

**ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΤΟΥ ΤΜΗΜΑΤΟΣ
ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ ΤΟΥ ΠΑΝΤΕΙΟΥ ΠΑΝΕΠΙΣΤΗΜΙΟΥ**

ΚΑΤΕΥΘΥΝΣΗ: ΝΟΜΙΚΟΣ ΠΟΛΙΤΙΣΜΟΣ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Θεσμικές εγγυήσεις προστασίας των δεδομένων προσωπικού
χαρακτήρα: το παράδειγμα του Ευρωπαϊκού Επόπτη

Άννα-Μαρία Βαγιάνου (Α.Μ. 7106Μ032)

Τριμελής Επιτροπή: Μ. Κουσκουνά
Α. Μαρκαντωνάτου-Σκαλτσά
Η. Νικολόπουλος

Αθήνα 30/6/2009

ΕΥΧΑΡΙΣΤΙΕΣ

Οφείλω ένα μεγάλο ευχαριστώ σε όλους τους καθηγητές και συμφοιτητές μου που με βοήθησαν και με στήριξαν στην ολοκλήρωση των μεταπτυχιακών μου σπουδών και ιδιαιτέρως την κυρία Κουσκουνά Μεταξία, Λέκτορα Ευρωπαϊκού Δικαίου στο Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών, που δέχτηκε να αναλάβει την επίβλεψη της διπλωματικής μου εργασίας.

Επίσης, θα ήθελα να ευχαριστήσω τον κύριο Μπόσκοβιτς Κοσμά για την πολύτιμη βοήθεια και την αμέριστη συμπαράστασή του στην διεκπεραίωση της παρούσας διπλωματικής εργασίας.

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΙΣΑΓΩΓΗ.....	1
ΚΕΦΑΛΑΙΟ Α: Το θεσμικό καθεστώς του Ευρωπαϊκού Επόπτη.....	3
1. Το νομικό πλαίσιο προστασίας των προσωπικών δεδομένων.....	3
1.1. Η ανάγκη προστασίας των προσωπικών δεδομένων.....	3
1.2. Το νομοθετικό πλαίσιο.....	4
1.2.1. Το εθνικό και διεθνές ρυθμιστικό πλαίσιο.....	4
1.2.2. Το κοινοτικό ρυθμιστικό πλαίσιο.....	8
α. Το κοινοτικό κεκτημένο: ελεύθερη ροή πληροφοριών και θεμελιώδες δικαίωμα στην προστασία των προσωπικών δεδομένων	9
β. Η οδηγία 95/46/ΕΚ.....	11
γ. Το άρθρο 286 ΣυνθΕΚ.....	12
δ. Ο Κανονισμός 45/2001/ΕΚ.....	13
1.3. Εννοιολογική προσέγγιση των προσωπικών δεδομένων.....	16
1.4. Κανόνες περί του θεμιτού της επεξεργασίας των προσωπικών δεδομένων.....	20
1.4.1. Αρχές αναφερόμενες στην ποιότητα των δεδομένων.....	20
1.4.2. Αρχές σχετικές με τη νομιμότητα της επεξεργασίας δεδομένων.....	21
1.4.3. Η ενημέρωση του υποκειμένου των δεδομένων.....	23
1.4.4. Τα δικαιώματα του υποκειμένου των δεδομένων.....	25
1.4.5. Εξαιρέσεις και περιορισμοί.....	27
1.4.6. Εμπιστευτικότητα και ασφάλεια της επεξεργασίας.....	28
2. Ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων: Σύσταση και Αρμοδιότητες.....	29
2.1. Η νομική θέση του ΕΕΠΔ.....	29

2.2.	Ο διορισμός και η διοικητική υποστήριξη του θεσμού.....	31
2.3.	Οι λόγοι καθιέρωσης του θεσμού.....	32
2.4.	Οι αρμοδιότητες του ΕΕΠΔ.....	33
2.4.1.	Εποπτεία (Supervision).....	34
2.4.1.1.	Ο τρόπος λειτουργίας της εποπτείας.....	35
2.4.2.	Διαβούλευση (Consultation).....	40
2.4.3.	Συνεργασία (Cooperation).....	43
3.	Η σχέση του ΕΕΠΔ με άλλες αρχές.....	44
3.1.	Οι Υπεύθυνοι Προστασίας Δεδομένων (DPOs).....	44
3.2.	Eurodac.....	46
3.3.	Ο Ευρωπαίος Διαμεσολαβητής (European Ombudsman).....	46
4.	Η νομική φύση του ΕΕΠΔ.....	48
4.1.	Οι πολλαπλές λειτουργίες του θεσμού.....	48
4.1.1.	Δεν είναι θεσμικό όργανο (institution).....	49
4.1.2.	Δεν είναι κοινοτική υπηρεσία (agency).....	49
4.1.3.	Δεν είναι ρυθμιστική αρχή (regulator).....	50
4.1.4.	Δεν είναι διαμεσολαβητής (ombudsman).....	52
4.1.5.	Δεν είναι δικαστική αρχή (judicial authority).....	53
4.1.6.	Τα βασικά χαρακτηριστικά του ΕΕΠΔ.....	55
5.	Ο Έλεγχος του ΕΕΠΔ.....	56
5.1.	Ο πολιτικός έλεγχος.....	56
5.2.	Ο δικαστικός έλεγχος.....	57

ΚΕΦΑΛΑΙΟ Β: Οι ουσιαστικές επιπτώσεις της λειτουργίας του Ευρωπαίου Επόπτη.....59

1.	Γνωμοδότηση του σχετικά με την πρόταση απόφασης-πλαισίου του Συμβουλίου για την ανταλλαγή πληροφοριών βάσει της αρχής της διαθεσιμότητας.....	60
----	---	----

2. Γνωμοδότηση του σχετικά με την πρωτοβουλία της Γερμανίας για τη θέσπιση απόφασης του Συμβουλίου για την εφαρμογή της απόφασης 2007/.../ΔΕΥ (η πρωτοβουλία του Prüm).....	64
3. Τρίτη γνωμοδότηση του για την πρόταση απόφασης-πλαισίου του Συμβουλίου για την προστασία των δεδομένων προσωπικού χαρακτήρα στα πλαίσια της αστυνομικής και δικαστικής συνεργασίας σε ποινικές υποθέσεις.....	68
4. Γνωμοδότηση του όσον αφορά το σχέδιο πρότασης απόφασης-πλαισίου του Συμβουλίου για τη χρήση των δεδομένων των καταστάσεων με τα ονόματα των επιβατών (PNR) με σκοπό την επιβολή του νόμου	73
5. Γνωμοδότηση του όσον αφορά την εφαρμογή ενός πολυετούς κοινοτικού προγράμματος για την προστασία των παιδιών κατά τη χρήση του διαδικτύου και άλλων επικοινωνιακών τεχνολογιών	78
ΕΠΙΛΟΓΟΣ.....	82
ΒΙΒΛΙΟΓΡΑΦΙΑ.....	85
ΠΑΡΑΡΤΗΜΑΤΑ.....	87

ΕΙΣΑΓΩΓΗ

Η παρούσα διπλωματική εργασία έχει ως στόχο να παρουσιάσει, να αναλύσει, σε επίπεδο πρωτογενών πηγών, και να αξιολογήσει, το ζήτημα της προστασίας των προσωπικών δεδομένων στα πλαίσια της Ευρωπαϊκής Ένωσης και ειδικότερα να εστιάσει στη λειτουργία και το ρόλο ενός νέου θεσμικού οργάνου επιφορτισμένου με την προστασία των δεδομένων αυτών, του **Ευρωπαϊού Επόπτη Προστασίας Δεδομένων**.

Πρόκειται για έναν θεσμό ο οποίος αναδεικνύει τη σημασία της προστασίας των προσωπικών δεδομένων στην κοινωνία της πληροφορίας, ο οποίος όμως δεν μπορεί να καταταχθεί εύκολα στην υφιστάμενη τυπολογία των οργάνων της Ένωσης. Ο Ευρωπαίος Επόπτης έχει αναλάβει να εκπληρώσει μια σειρά από λειτουργίες, όπως η προστασία των ατομικών δικαιωμάτων, η παροχή εμπειρογνωμοσύνης στα όργανα της Ένωσης, καθώς και η συνεργασία με εθνικούς θεσμούς προστασίας των προσωπικών δεδομένων. Κάποιες δε λειτουργίες του Επόπτη ενδεχομένως να έχουν και άμεσες πολιτικές επιπτώσεις όπως π.χ. όταν γνωμοδοτεί ως προς το εάν πρέπει να υιοθετηθεί μια πράξη του κοινοτικού νομοθέτη.

Ως καινούριος θεσμός με μόλις πέντε έτη παρουσίας στον ευρωπαϊκό χώρο, ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων δεν έχει ακόμη καταστεί αντικείμενο ενδελεχούς μελέτης και ικανής κριτικής τόσο στα πλαίσια της εγχώριας όσο και της ευρωπαϊκής βιβλιογραφίας. Για το λόγο αυτό θα γίνει μια

προσπάθεια μιας όσο το δυνατόν αρτιότερης και σφαιρικότερης παρουσίασης του θεσμού με βάση τις πρωτογενείς πηγές, όπως οι Συνθήκες, οι οδηγίες και οι κανονισμοί που αποτέλεσαν τη νομική βάση όχι μόνο για την ίδρυση του Ευρωπαϊκού Επόπτη αλλά και την κατοχύρωση του θεμελιώδους δικαιώματος της προστασίας των προσωπικών δεδομένων. Επίσης θα ληφθούν υπ' όψιν οι ομιλίες του ιδίου του Ευρωπαϊκού Επόπτη, οι ετήσιες εκθέσεις πεπραγμένων του προς το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο και την Επιτροπή στις οποίες περιγράφονται οι αποφάσεις και τα μέτρα που λαμβάνει αναφορικά πάντα με τα δεδομένα προσωπικού χαρακτήρα, καθώς και μια σειρά από γνωμοδοτήσεις επί νομοθετικών προτάσεων στο πλαίσιο του πρώτου και του τρίτου πυλώνα της Ένωσης.

Η παρούσα εργασία χωρίζεται σε δύο κεφάλαια: Το πρώτο κεφάλαιο αναφέρεται στο θεσμικό καθεστώς του Ευρωπαϊκού Επόπτη. Αρχικά θα γίνει μια σύντομη ιστορική αναδρομή που δείχνει τη σταδιακή παγίωση του εν λόγω θεσμού και κατόπιν μια αναλυτική παρουσίαση του δικαιώματος του κάθε πολίτη στην προστασία των προσωπικών του δεδομένων. Εν συνεχεία θα γίνει αναφορά στον Ευρωπαίο Επόπτη ως όργανο, στο ρόλο του, στις λειτουργίες του και στη συνεργασία του με τα άλλα όργανα της Ε.Ε. Στο τέλος του πρώτου αυτού κεφαλαίου μνεία θα γίνει για τη σχέση του με τις άλλες ανεξάρτητες αρχές (π.χ. με τον Ευρωπαίο Διαμεσολαβητή), τη νομική του φύση και τις μορφές ελέγχου στις οποίες υπόκειται. Στο δεύτερο κεφάλαιο θα γίνει μια παρουσίαση της κανονιστικής και πολιτικής του λειτουργίας ως εξειδικευμένου οργάνου σε θέματα προστασίας δεδομένων προσωπικού χαρακτήρα. Προς το σκοπό αυτό, θα αναλυθούν πέντε γνωμοδοτήσεις του έτσι ώστε να γίνουν αντιληπτοί οι τρόποι με τους οποίους προστατεύει τα θεμελιώδη δικαιώματα και συγχρόνως επηρεάζει την άσκηση της νομοθετικής λειτουργίας στα πλαίσια της Ευρωπαϊκής Ένωσης.

ΚΕΦΑΛΑΙΟ Α

ΤΟ ΘΕΣΜΙΚΟ ΚΑΘΕΣΤΩΣ ΤΟΥ ΕΥΡΩΠΑΙΟΥ ΕΠΟΠΤΗ

Όπως αναφέρθηκε και στην εισαγωγή, στο πρώτο αυτό κεφάλαιο θα ασχοληθούμε με το γενικό νομικό πλαίσιο της προστασίας των προσωπικών δεδομένων και στη συνέχεια με τον ίδιο τον Επόπτη ως θεσμό της Ευρωπαϊκής Ένωσης. Θα αναφερθούμε κυρίως στη σύσταση, τις αρμοδιότητες, τη σχέση του με άλλα όργανα και τη νομική του φύση. Βασική πηγή για την νομική ανάλυση που θα ακολουθήσει είναι ο Κανονισμός 45/2001/ΕΚ αλλά και η Οδηγία 95/46/ΕΚ που αποτέλεσαν την βάση για τη σύσταση και ανάπτυξη του θεσμού.

1. ΤΟ ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ ΠΡΟΣΤΑΣΙΑΣ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

1.1. Η ανάγκη προστασίας των προσωπικών δεδομένων.

Είναι γεγονός ότι τα τελευταία τριάντα χρόνια, έχει παρατηρηθεί μια έκρηξη τεχνολογικών ανακαλύψεων και πληροφοριακών συστημάτων τόσο σε παγκόσμιο επίπεδο, όσο και εντός του ευρωπαϊκού χώρου. Αυτή η έντονη

χρήση και διάδοση των νέων τεχνολογιών προκάλεσε –όχι άδικα- το φόβο μιας πιθανής αποδυνάμωσης ή της προσβολής των ανθρωπίνων δικαιωμάτων.

Ειδικότερα στις μέρες μας, η εμφάνιση της τρομοκρατίας, ως μια μορφή αόρατου πολέμου, επέτεινε την ανάγκη των κρατών για έλεγχο των προσωπικών στοιχείων πολιτών κυρίως στον τομέα των εναέριων μετακινήσεων και έπληξε σε μεγάλο βαθμό βασικά ανθρώπινα δικαιώματα, όπως π.χ. το δικαίωμα της ελευθερίας των πολιτών, την ελευθερία μετακίνησής τους, καθώς και την ελευθερία του εμπορίου, με απώτερο σκοπό να δημιουργήσουν ένα πλέγμα προστασίας από τις τρομοκρατικές αυτές ενέργειες.

Τα ευρωπαϊκά όργανα, όμως, από πολύ νωρίς αντιλήφθηκαν πως η διακίνηση και ανταλλαγή προσωπικών δεδομένων πολιτών μεταξύ των οργάνων και οργανισμών της Κοινότητας, επισείει τον κίνδυνο της ανεξέλεγκτης και παράνομης συλλογής, επεξεργασίας και χρήσης αυτών. Για το λόγο αυτό ξεκινά από πολύ νωρίς να συνάπτει συνθήκες, να θεσπίζει χάρτες και να εκδίδει οδηγίες και κανονισμούς για την προστασία του δικαιώματος των φυσικών προσώπων στα προσωπικά τους δεδομένα που γίνονται αντικείμενο χρήσης και επεξεργασίας από μια πλειάδα οργάνων και οργανισμών που δραστηριοποιούνται σε διάφορους τομείς εντός της Ευρωπαϊκής Κοινότητας.

Σκόπιμο κρίνεται επομένως, για την καλύτερη κατανόηση της σημερινής νομικής κατοχύρωσης του δικαιώματος των προσωπικών δεδομένων και τη σημερινή μορφή προστασίας τους μέσα από τη λειτουργία του Ευρωπαϊκού Επόπτη, να γίνει μια σύντομη αναφορά στα αρχικά νομοθετικά κείμενα στα πλαίσια της Ε.Ε. που έδωσαν τις πρώτες κατευθυντήριες γραμμές για τη δημιουργία των σύγχρονων οδηγιών και κανονισμών.

1.2. Το νομοθετικό πλαίσιο.

1.2.1. Το εθνικό και διεθνές ρυθμιστικό πλαίσιο.

Οι πρώτες κανονιστικές απαντήσεις στο αίτημα της προστασίας των προσωπικών δεδομένων καταγράφονται σε διεθνές και όχι σε κρατικό επίπεδο. Ωστόσο, το πρώτο νομοθέτημα παγκοσμίως, αναφορικά με την προστασία

προσωπικών δεδομένων, ήταν ο νόμος για την προστασία των δεδομένων του κρατιδίου της Hessen της Γερμανίας το 1970 και στην ίδια χώρα το 1974 ακολούθησε ο νόμος του κρατιδίου Rheinland-Pfalz. Ο πρώτος Ομοσπονδιακός Νόμος Προστασίας Δεδομένων (Bundesdatenschutzgesetz) τέθηκε σε ισχύ το 1979¹.

Επίσης, και το Ηνωμένο Βασίλειο είναι από τα πρώτα κράτη στο οποίο συναντάται το 1972 η νεότερη αναφορά της Επιτροπής σχετικά με την ιδιωτικότητα (The Report of the Committee on Privacy- “Younger Report”). Σ’ αυτήν διαμορφώνονται δέκα αρχές που προτείνεται να εφαρμόζονται σε περιπτώσεις που αφορούν πληροφορίες προσωπικού χαρακτήρα όταν γίνεται χρήση υπολογιστών. Οι αρχές αυτές κάνουν αναφορά στο σκοπό της συλλογής και αποθήκευσης των προσωπικών δεδομένων, για το χρονικό διάστημα διατήρησής τους, για την προστασία της ταυτότητας των ατόμων που συμμετέχουν σε στατιστικές έρευνες, τα υποκείμενα που έχουν πρόσβαση στα δεδομένα αυτά, για την ασφάλεια των διαδικασιών και την ακρίβεια των συλλεγόμενων στοιχείων. Τρία χρόνια μετά από το νομοθέτημα αυτό, η κυβέρνηση ανήγγειλε την ίδρυση της Επιτροπής Προστασίας Προσωπικών Δεδομένων².

Το 1978 τέθηκε σε ισχύ ο γαλλικός νόμος No 78-17 για την προστασία προσωπικών δεδομένων από την αθέμιτη επεξεργασία τους με υπολογιστή και με τον ίδιο νόμο ιδρύθηκε και η Commission nationale de l’ informatique et des libertés η οποία εγγυάται την εφαρμογή του οικείου νόμου. Το παράδειγμα των χωρών αυτών ακολούθησαν η Σουηδία, Νορβηγία, Αυστρία Δανία και Λουξεμβούργο. Σε αυτή τη χρονική περίοδο, ο Έλληνας νομοθέτης δεν συμμετέχει στην παραγωγή των πρώτων αυτών νομοθετημάτων.

Γενικά θα λέγαμε πως αυτές οι πρώτες νομοθετικές κατοχυρώσεις για την προστασία των προσωπικών δεδομένων δέχθηκαν μεγάλη κριτική για τις

¹ Βασίλης Σωτηρόπουλος, *Η συνταγματική προστασία των προσωπικών δεδομένων*, Αθήνα-Θεσ/κη 2006, εκδόσεις Σάκκουλα, σελ. 12.

² Rosemary Jay- Angus Hamilton, *Data Protection-Law and Practice*, London 1999, Sweet&Maxwell Publ., σελ. 2-3.

αυστηρές ρήτρες τους, τον έντονο έλεγχο και τις εξοντωτικές ποινικές, αστικές και διοικητικές κυρώσεις που προέβλεπαν³.

Το επόμενο νομικά δεσμευτικό διεθνές κείμενο για την προστασία των ανθρωπίνων δικαιωμάτων είναι η Σύμβαση του Συμβουλίου της Ευρώπης⁴ «για την προστασία των ατόμων από την αυτόματη επεξεργασία των προσωπικών πληροφοριών» που υπεγράφη στο Στρασβούργο το 1981 και είναι γνωστή ως **Σύμβαση 108**. Η Σύμβαση 108 περιέχει την πρώτη κωδικοποίηση του σκληρού πυρήνα της προστασίας προσωπικών δεδομένων, δηλαδή των αρχών και των εγγυήσεων που αποτελούν τη βάση κάθε σύγχρονου τότε- νομικού συστήματος σχετικών διατάξεων⁵.

Το περιεχόμενο της εν λόγω σύμβασης καθορίστηκε σε μεγάλο βαθμό από το κείμενο «Αρχές διέπουσες την προστασία της προσωπικής σφαίρας του ανθρώπου και τις διασυννοριακές ροές προσωπικών στοιχείων», το οποίο υιοθετήθηκε το 1980 από τον Οργανισμό για την Οικονομική Συνεργασία και την Ανάπτυξη (ΟΟΣΑ)⁶ και είχε περισσότερο συμβουλευτική παρά δεσμευτική νομική επιρροή.

Κατά τον Β. Σωτηρόπουλο, η Σύμβαση 108 είχε μια παράλειψη που σήμερα θα θεωρείτο αρκετά σοβαρή. Δεν προέβλεπε την καθιέρωση μιας αρχής ανεξάρτητου θεσμικού ελέγχου επιφορτισμένη με τη διασφάλιση της προστασίας των προσωπικών δεδομένων. Ο μηχανισμός ανεξάρτητου ελέγχου προστέθηκε ως παράμετρος της προστασίας των δεδομένων αυτών με το Πρόσθετο Πρωτόκολλο του 2001.

Γενικά θα λέγαμε πως το συγκεκριμένο νομοθέτημα επικεντρώθηκε κυρίως στα εξής θέματα:

1. Διαφοροποιεί την προστασία των δεδομένων ανάλογα με τη φύση τους, π.χ. αν υπάγονται σε ορισμένες «ειδικές κατηγορίες» (ευαίσθητα δεδομένα) ή όχι και ανάλογα με το σκοπό της

³ Βασίλης Αραβαντινός, *Η προστασία των στοιχείων προσωπικού χαρακτήρα από την αθέμιτη επεξεργασία τους με ηλεκτρονικό υπολογιστή*, Αθήνα- Κομοτηνή, 1997, εκδόσεις Σάκκουλα, σελ. 14.

⁴ Το Συμβούλιο της Ευρώπης είναι ένας πανευρωπαϊκός διακυβερνητικός οργανισμός που συστάθηκε το 1949 με σκοπό να εδραιώσει την πολιτική συνεργασία για την πρόοδο και προστασία των ατομικών δικαιωμάτων και ελευθεριών στο εσωτερικό της Ευρώπης.

⁵ Βασίλης Σωτηρόπουλος, *ό.π.*, σελ. 14.

⁶ Ο ΟΟΣΑ είναι ένας διεθνής οργανισμός (όχι αποκλειστικά ευρωπαϊκός) του οποίου βασικοί στόχοι είναι να καλλιεργήσει την οικονομική σταθερότητα και να ενισχύσει το εμπόριο. Η δράση του ξεκινά το 1960.

επεξεργασίας τους, ο οποίος μπορεί να είναι στατιστικός, ερευνητικός, ιστορικός κλπ. Ανάλογα, επομένως, με το σκοπό της επεξεργασίας γίνεται και μια διαβάθμιση της αυστηρότητας της ρύθμισης (αρ. 6 Σ. 108)

2. Ενοποιεί τη νομική αντιμετώπιση της προστασίας, είτε ο κύριος του αρχείου προσωπικών δεδομένων αποτελεί φορέα του δημοσίου είτε του ιδιωτικού τομέα (αρ. 3 παρ.1 Σ. 108).
3. Επεκτείνει τη νομική προστασία και στα αρχεία δεδομένων που δεν αποτελούν αντικείμενο αυτοματοποιημένης επεξεργασίας (αρ. 3 παρ. 2γ' Σ. 108).
4. Διατυπώνει βασικές αρχές για την ποιότητα των δεδομένων, όπως π.χ. η αρχή της θεμιτής και νόμιμης συλλογής και επεξεργασίας, η αρχή του καθορισμένου και νόμιμου σκοπού της επεξεργασίας, αρχές της αναγκαιότητας της επεξεργασίας, η αρχή της ακρίβειας των δεδομένων και οι αρχές της χρονικά πεπερασμένης διατήρησης των δεδομένων (αρ.5 Σ. 108).
5. Ανάγει τους κανόνες της πληροφορικής επιστήμης σχετικά με την ασφάλεια των δεδομένων σε νομικά δεσμευτικούς κανόνες (αρ. 7 Σ. 108).
6. Παρέχει συμπληρωματικές εγγυήσεις για το υποκείμενο των δεδομένων, όπως π.χ. το δικαίωμα γνώσης της επεξεργασίας των δεδομένων του, δικαίωμα πρόσβασης στα αρχεία που αφορούν τα προσωπικά του δεδομένα σε εύλογα χρονικά διαστήματα, το δικαίωμα διόρθωσης ή διαγραφής των δεδομένων που υπέστησαν επεξεργασία κατά παράβαση των διατάξεων και το δικαίωμα της προσφυγής σε περίπτωση μη ικανοποίησης των δικαιωμάτων του (αρ. 8 Σ. 108).
7. Περιγράφουν κατηγορίες θεμιτών περιορισμών της προστασίας των προσωπικών δεδομένων όπως π.χ. η κρατική και δημόσια ασφάλεια, τα νομισματικά συμφέροντα του κράτους, η καταστολή των ποινικών παραβάσεων, η προστασία του υποκειμένου των δεδομένων και

δικαιωμάτων τρίτων και οι περιπτώσεις επεξεργασίας δεδομένων για σκοπούς στατιστικούς ή επιστημονικούς (αρ. 9 Σ.108).

Γίνεται αντιληπτό, ότι οι αυστηρές ρυθμίσεις των νομοθετημάτων της πρώτης γενιάς υποχωρούν, ενώ χώρες που δεν είχαν ως τότε θεσπίσει νόμους για την προστασία των δεδομένων προσωπικού χαρακτήρα, συμμετέχουν στη σχετική παραγωγή⁷.

Σήμερα η σύμβαση αυτή έχει κυρωθεί από 38 κράτη μέλη του Συμβουλίου της Ευρώπης, περιλαμβανομένου και των 27 κρατών μελών της Ε.Ε., και μέχρι σήμερα ακόμα θεωρείται ως ο «ακρογωνιαίος λίθος» της προστασίας των προσωπικών δεδομένων⁸.

1.2.2. Το κοινοτικό ρυθμιστικό πλαίσιο

Σε αυτό το σημείο θα ασχοληθούμε με την ανάληψη νομοθετικής πρωτοβουλίας από την ίδια την Ε.Ε. και τη σύνδεση της προστασίας προσωπικών δεδομένων με το κοινοτικό κεκτημένο. Αυτό σημαίνει ότι πλέον η θέσπιση νομικών κανόνων προστασίας ανάγεται σε κοινοτική υποχρέωση των κρατών μελών. Είναι σε αυτή τη φάση που παγιώνεται η αντίληψη ότι η προστασία των προσωπικών δεδομένων χρειάζεται τη λειτουργία ενός ανεξάρτητου δημοσίου οργάνου με αποφασιστικές αρμοδιότητες παρέμβασης που να διασφαλίζει την εφαρμογή των νομοθετικών διατάξεων.

Βρισκόμαστε, λοιπόν, στην εποχή της *αυτορρύθμισης* της προστασίας εκ μέρους των υπευθύνων επεξεργασίας. Αυτορρύθμιση, υπό ευρεία έννοια, αποτελεί και η θέσπιση από την πλευρά της Ε.Ε. νομικών κανόνων προστασίας των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα όχι μόνο από τα όργανα της Κοινότητας αλλά και από τα όργανα του «Τρίτου Πυλώνα», όπως π.χ. Schengen, Europol, Eurojust, Customs), με την ίδρυση Κοινών Εποπτικών Αρχών που διασφαλίζουν την προστασία των δεδομένων από τα αντίστοιχα πληροφοριακά συστήματα. Η δυνατότητα

⁷ Βλ. Ιρλανδία, Ολλανδία, Ισπανία, Πορτογαλία, Βέλγιο. Η Ελλάδα κύρωσε τη Σύμβαση 108 με το Ν.2068/1992 και η ισχύς της άρχισε στη χώρα από την 1.1.1995.

⁸ Hustinx, P., "The Role of Data Protection Authorities", www.edps.europa.eu, Publications / Speeches & Articles, 23.12.2008, σελ.2.

αυτορρύθμισης είναι στενά συνδεδεμένη με το ρυθμιστικό και συμβουλευτικό ρόλο των Αρχών Προστασίας Προσωπικών Δεδομένων που έχουν ως αρμοδιότητα την παρότρυνση και επίβλεψη σωματείων, ενώσεων κλπ. στην κατάρτιση κωδίκων δεοντολογίας για την επαρκή προστασία των θεμελιωδών δικαιωμάτων των υποκειμένων των δεδομένων⁹.

Επιπλέον, στις τάσεις της *τρίτης γενιάς* εντάσσεται η πρόταση της «επεξεργασίας» ως πηγής κινδύνου για τα προσωπικά δεδομένα με τον σταδιακό παραμερισμό της ειδικότερης έννοιας του «αρχείου προσωπικών δεδομένων»¹⁰.

α. Το κοινοτικό κεκτημένο: ελεύθερη ροή πληροφοριών και θεμελιώδες δικαίωμα στην προστασία των προσωπικών δεδομένων

Με τη Συνθήκη περί Ιδρύσεως της Ευρωπαϊκής Κοινότητας (ΣυνθΕΚ) κατοχυρώνονται οι θεμελιώδεις ελευθερίες και μεταξύ άλλων η ελεύθερη κυκλοφορία των εμπορευμάτων, των προσώπων, των υπηρεσιών και των κεφαλαίων. Αυτές οι ελευθερίες προϋποθέτουν την ελεύθερη κυκλοφορία των πληροφοριών που εξατομικεύουν τα εν λόγω εμπορεύματα, πρόσωπα, υπηρεσίες και κεφάλαια. Η διαφορετική νομική μεταχείριση των πληροφοριών αυτών εκ μέρους των κρατών μελών, ενεργοποίησε την αρμοδιότητα του Συμβουλίου και του Ευρωπαϊκού Κοινοβουλίου να εκδώσουν μια οδηγία που να επιβάλλει μια ενοποιημένη ρύθμιση της προστασίας και της ελεύθερης κυκλοφορίας των προσωπικών πληροφοριών. Αυτή είναι η Οδηγία 95/46/ΕΚ.

Ενόψει της κρισιμότητας της διασυνοριακής ροής πληροφοριών εντός της Κοινότητας, σχετική διάταξη για την προστασία των προσωπικών δεδομένων περιλήφθηκε και στο ίδιο το σώμα της ΣυνθΕΚ.

Αξίζει επίσης ν' αναφερθεί πως τα προσωπικά δεδομένα αποτελούν πλέον αυτονομημένο έννομο αγαθό (αλλά και οικονομικό αγαθό-commodity- στα πλαίσια της αγοράς και της ελεύθερης κυκλοφορίας δεδομένων) το οποίο κατοχυρώνεται όχι μόνο ως νομική προϋπόθεση λειτουργίας της κοινής αγοράς,

⁹ Λ. Μήτρου, *Το δίκαιο στην Κοινωνία της Πληροφορίας*, Αθήνα-Θεσ/νίκη 2002, σελ 51 επ.

¹⁰ Β. Σωτηρόπουλος, *ό.π.*, σελ.19.

αλλά και ως αυτοτελής νομική εγγύηση που περιλαμβάνεται στο κοινοτικό κεκτημένο.

Έτσι και στον **Χάρτη Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης** αναφέρεται στο **άρθρο 8**¹¹ η προστασία των προσωπικών δεδομένων ως θεμελιώδες δικαίωμα και αυτονομείται σε σχέση με την προστασία του ιδιωτικού βίου (άρθρο 7 ΧΘΔΕΕ)¹².

Το άρθρο 8 του Χάρτη κατοχυρώνει ένα δικαίωμα που υπερβαίνει τους σκοπούς της **Οδηγίας 95/46/ΕΚ** και του **άρθρου 286 ΣυνθΕΚ** (τα οποία αναλύονται εκτενέστερα παρακάτω) και αυτό γίνεται αντιληπτό από το ότι εξαλείφεται από το κείμενο οποιαδήποτε αναφορά σε «ελεύθερη κυκλοφορία δεδομένων». Με αυτόν τον τρόπο απαγκιστρώνεται η προστασία προσωπικών δεδομένων από τους σκοπούς της λειτουργίας της «εσωτερικής αγοράς» της Κοινότητας και ανάγεται σε συνταγματική αυταξία, σε όλους τους τομείς δράσης της Ευρωπαϊκής Ένωσης. Με τον τρόπο αυτό η προστασία δεδομένων κατοχυρώνεται μέσω του άρθρου 8 του Χάρτη και ως προς τους τρεις πυλώνες της Ε.Ε¹³. Έτσι, σε επίπεδο Κοινότητας (Πρώτος Πυλώνας) ο ανεξάρτητος κεντρικός έλεγχος διενεργείται από τον αντίστοιχο θεσμό (Ευρωπαίος Επόπτης Προστασίας Δεδομένων), ενώ ο αποκεντρωμένος από τους Υπεύθυνους Προστασίας Δεδομένων που διορίζονται σε κάθε κοινοτικό όργανο και οργανισμό)¹⁴. Ως προς την Κοινή Εξωτερική Πολιτική και την Πολιτική Ασφάλειας (Δεύτερος Πυλώνας) και την Αστυνομική και Δικαστική Συνεργασία σε ποινικές υποθέσεις (Τρίτος Πυλώνας), η προστασία που διακηρύσσεται στα άρθρα 8 του Χάρτη και ΕΣΔΑ δεν εξειδικεύεται με ένα ενιαίο κείμενο και ο θεσμικός έλεγχος δεν ασκείται από μια ανεξάρτητη αρχή. Η προστασία

¹¹ «Προστασία των δεδομένων προσωπικού χαρακτήρα: **1.** Κάθε πρόσωπο έχει δικαίωμα στην προστασία των δεδομένων που το αφορούν **2.** Η επεξεργασία αυτών των δεδομένων πρέπει να γίνεται νομίμως, για καθορισμένους σκοπούς και με βάση τη συγκατάθεση του ενδιαφερομένου ή για άλλους θεμιτούς λόγους που προβλέπονται από το νόμο. Κάθε πρόσωπο έχει δικαίωμα να έχει πρόσβαση στα συλλεγμένα δεδομένα που το αφορούν και να επιτυγχάνει τη διόρθωσή τους **3.** Ο σεβασμός των κανόνων αυτών υπόκειται στον έλεγχο ανεξάρτητης αρχής.»

¹² Η έννοια της «προστασίας των δεδομένων» είναι ευρύτερη της «προστασίας της ιδιωτικής ζωής», αφού σχετίζεται και με άλλα θεμελιώδη δικαιώματα και ελευθερίες του ατόμου, ταυτόχρονα όμως και ειδικότερη, στο μέτρο που αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα, δηλαδή τις πληροφοριακές παραβιάσεις των θεμελιωδών δικαιωμάτων, όχι τις *corpora* προσβολές. (Βλ. Ετήσια Έκθεση ΕΕΠΔ 2004, σελ. 7)

¹³ Β. Σωτηρόπουλος, *ό.π.*, σελ.21.

¹⁴ Αυτό το σύστημα ιδρύεται με τον Κανονισμό 45/2001/ΕΚ, βάσει του άρθρου 286 ΣυνθΕΚ, για τον οποίο θα γίνει λόγος παρακάτω.

προσωπικών δεδομένων από την επεξεργασία που διενεργείται με τα πληροφοριακά συστήματα Schengen, Eurropol και Eurojust προβλέπεται από ειδικές διατάξεις που περιλαμβάνονται στις ιδρυτικές πράξεις τους ή σε μεταγενέστερα κείμενα και ο ανεξάρτητος έλεγχος ασκείται από Κοινές Εποπτικές Αρχές οι οποίες αποτελούνται από εκπροσώπους των εθνικών Αρχών Προστασίας Δεδομένων. Σήμερα πλέον έχει παγιωθεί σταδιακά και η συνεργασία ανάμεσα στους προέδρους των Κοινών Εποπτικών Αρχών και τον Ευρωπαϊό Επόπτη, ο οποίος, κατ' ορθή ερμηνεία του **Κανονισμού 45/2001**, ασκεί την γνωμοδοτική του αρμοδιότητα επί προτάσεων νομοθεσίας οργάνων που αφορούν και τον Τρίτο Πυλώνα¹⁵.

β. Η οδηγία 95/46/EK

Η οδηγία 95/46/EK είναι δημιούργημα του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, με την οποία εισάγεται ένα γενικό νομικό μοντέλο για την προστασία προσωπικών δεδομένων που δείχνει τις επιδιώξεις και τις προτεραιότητες της Ε.Ε. κατά την δεκαετία του 1990. Ο τίτλος της Οδηγίας είναι «Για την προστασία των ατόμων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και την ελεύθερη κυκλοφορία των δεδομένων αυτών». Απ' αυτό γίνεται αντιληπτό ότι η προστασία προσωπικών δεδομένων προβλέπεται όχι τόσο ως δικαίωμα, όσο ως περιορισμός της ελεύθερης κυκλοφορίας των προσωπικών δεδομένων¹⁶.

Κατά τα λεγόμενα του Β. Σωτηρόπουλου, η οδηγία αυτή αποτελεί μέχρι σήμερα το πιο αναλυτικό, συγκροτημένο και συγκεκριμένο των εθνικών νομοθεσιών δεσμευτικό νομικό κείμενο για την προστασία προσωπικών δεδομένων¹⁷. Αποτελεί το σύγχρονο μοντέλο ενός γενικού νομοθετήματος που περιέχει εκτεταμένες εξειδικεύσεις των δικαιωμάτων των υποκειμένων των δεδομένων, θέτοντας προστατευτικά όρια άσκησης των δικαιωμάτων αυτών και καθιερώνοντας τους νόμιμους όρους του επιτρεπτού της επεξεργασίας των

¹⁵ Αντιθέτως, η εποπτική του αρμοδιότητα περιορίζεται ρητά στον πρώτο πυλώνα της Ε.Ε. Βλ. http://www.edps.eu.int/publications/policy_papers/policy_paper_advisor_EN.pdf.

¹⁶ Rosemary Jay- Angus Hamilton, *ο.π.*, σελ. 9-14.

¹⁷ Β. Σωτηρόπουλος, *ό.π.*, σελ. 25.

δεδομένων. Τέλος, ανάγει σε κεντρικό ελεγκτικό όργανο για κάθε κράτος ένα ανεξάρτητο όργανο και ταυτοχρόνως ιδρύει τον φορέα συντονισμού των ανεξαρτήτων οργάνων, μέσω της «Ομάδας προστασίας των προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα»¹⁸, η οποία αποτελείται από εκπροσώπους των εθνικών αρχών προστασίας δεδομένων, από τον εκπρόσωπο του Ευρωπαϊκού Επόπτη και από έναν αντιπρόσωπο της Επιτροπής.

Με την εν λόγω Οδηγία, ιδρύεται η κοινοτική υποχρέωση των κρατών μελών για υιοθέτηση μέσων που, σε επίπεδο εσωτερικού δικαίου, υλοποιούν τις διατάξεις της ή, εφόσον υπάρχουν τα μέσα αυτά, υποχρέωση των μελών για εναρμόνιση των μέσων προς τις διατάξεις της Οδηγίας.

Κατόπιν, η **Οδηγία 97/66/ΕΚ** του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου τον Δεκέμβριο του 1999, αποτελεί ένα εξειδικευμένο πλέγμα κανόνων για την εφαρμογή των διατάξεων της Οδηγίας 95/46/ΕΚ σχετικά με τα προσωπικά δεδομένα που διακινούνται στον τηλεπικοινωνιακό τομέα. Η Οδηγία αυτή καταργήθηκε από την **Οδηγία 2002/58ΕΚ** του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου τον Ιούλιο του 2002. Με την Οδηγία αυτή αντιμετωπίζεται το ζήτημα της προστασίας των προσωπικών δεδομένων στο πεδίο της ελευθερίας της επικοινωνίας και της ανταπόκρισης που υποστηρίζεται από ηλεκτρονικά μέσα.

Με τις δύο αυτές τελευταίες Οδηγίες καθίσταται σαφές ότι μέρος της άσκησης του δικαιώματος της ελεύθερης επικοινωνίας και ανταπόκρισης αποτελεί η παραγωγή και χρήση των προσωπικών δεδομένων από τους χρήστες και ότι επομένως κατά την ενάσκηση του εν λόγω δικαιώματος επικοινωνίας, ενεργοποιούνται και οι προστατευτικές διατάξεις των προσωπικών δεδομένων.

γ. Το άρθρο 286 ΣυνθΕΚ

Κατά την τροποποίηση της Συνθήκης περί Ιδρύσεως της Ευρωπαϊκής Κοινότητας, στο Άμστερνταμ, το 1997, προστέθηκε το άρθρο 286, κατά το

¹⁸ Άρθρο 29 της Οδηγίας 95/46/ΕΚ.

οποίο η εφαρμογή των κοινοτικών πράξεων για την προστασία των προσωπικών δεδομένων και την ελεύθερη κυκλοφορία τους επεκτείνεται και στον «σκληρό πυρήνα» της Κοινότητας, δηλαδή στις οργανικές μονάδες ενάσκησης της κοινοτικής εξουσίας που έχουν ιδρυθεί από την Συνθήκη ή βάσει αυτής. Έτσι, στην §1 του εν λόγω άρθρου, προβλέπεται η αυτοδέσμευση της Κοινότητας, ως προς τον σεβασμό των κοινοτικών κανονιστικών διατάξεων για την προστασία προσωπικών δεδομένων από την ίδια, τα όργανα και τους οργανισμούς της. Με τη διάταξη αυτή γίνεται αντιληπτό ότι η προστασία των προσωπικών δεδομένων, δεν δεσμεύει μόνο τα κράτη μέλη, αλλά και την ίδια την Κοινότητα, ως προς τις πράξεις ή παραλείψεις των οργάνων της. Εναρκτήρια ημερομηνία της αυτοδέσμευσης αυτής ορίζεται η 1.1.1999¹⁹.

Στην §2 του ιδίου άρθρου, το Συμβούλιο συνιστά ένα «ανεξάρτητο εποπτικό όργανο» υπεύθυνο για την παρακολούθηση της εφαρμογής των διατάξεων για την προστασία των προσωπικών δεδομένων από τα όργανα και τους οργανισμούς της Κοινότητας. Σε εκτέλεση των διατάξεων του άρθρου 286, εκδίδεται ο Κανονισμός 45/2001/EK και ιδρύεται το προβλεπόμενο απ' αυτόν όργανο ανεξάρτητου θεσμικού ελέγχου, ο Ευρωπαϊός Επόπτης Προστασίας Προσωπικών δεδομένων, αλλά και ο θεσμός των Υπευθύνων Προστασίας Δεδομένων²⁰.

δ. Ο Κανονισμός 45/2001/EK

Όπως προαναφέρθηκε, ο εν λόγω κανονισμός θεσπίζεται από το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο την 18^η Δεκεμβρίου 2000 προκειμένου να εφαρμοσθεί το άρθρο 286 ΣυνθΕΚ. Αναφέρεται στην προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα όργανα και τους οργανισμούς της Κοινότητας και στην ελεύθερη διακίνηση των δεδομένων αυτών.

¹⁹ Βασίλης Σωτηρόπουλος, «Ο Ευρωπαϊός Επόπτης Προστασίας Δεδομένων», *Δικαιώματα του Ανθρώπου Νο 36/2007*, σελ. 1178.

²⁰ Hielke Hijmans, “The European Data Protection Supervisor: The institutions of the EC controlled by an independent authority”, *Common Market Law Review* 43, 2006, σελ. 1313-1314.

Σύμφωνα με την εξουσιοδοτική διάταξη του άρθρου 286 §1, την επεξεργασία προσωπικών δεδομένων από την Κοινότητα θα έπρεπε να διέπει η ήδη τότε υφιστάμενη νομοθεσία, δηλαδή οι Οδηγίες 95/46 και 97/66ΕΚ, ενώ νέα ρύθμιση προβλεπόταν μόνο για τη σύσταση και τις αρμοδιότητες του ανεξάρτητου εποπτικού οργάνου.

Ο κοινοτικός νομοθέτης θεμελιώνει την αναγκαιότητα της θέσπισης του Κανονισμού στο ότι «ένα πλήρες σύστημα προστασίας δεδομένων προσωπικού χαρακτήρα απαιτεί όχι μόνο την παροχή δικαιωμάτων στα υποκείμενα των δεδομένων και την επιβολή υποχρεώσεων στους φορείς που επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα, αλλά και την πρόβλεψη κατάλληλων κυρώσεων για τους παραβάτες καθώς και μιας ανεξάρτητης εποπτικής αρχής»²¹.

Οι διατάξεις του Κανονισμού έχουν καταρτισθεί με πρότυπο την Οδηγία 95/46, εισάγοντας ωστόσο λεπτομερέστερες διατυπώσεις σε ορισμένα σημεία προκειμένου να προσαρμοστούν στα καινούρια δεδομένα της εποχής και κυρίως σε σχέση με την επεξεργασία των προσωπικών δεδομένων από τα κοινοτικά όργανα.

Ο Κανονισμός ιδρύει δύο μορφές ανεξάρτητου θεσμικού ελέγχου, τον κεντρικό και τον αποκεντρωμένο. Για τον κεντρικό έλεγχο υπεύθυνος είναι ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων, ενώ ο αποκεντρωμένος έλεγχος ασκείται από τον Υπεύθυνο Προστασίας Δεδομένων. Κάθε κοινοτικό όργανο διορίζει ένα τουλάχιστον πρόσωπο ως υπεύθυνο για την προστασία των προσωπικών δεδομένων, ο οποίος είναι επιφορτισμένος να διασφαλίζει την εσωτερική εφαρμογή του Κανονισμού, να ενημερώνει τους υπεύθυνους επεξεργασίας και τα υποκείμενα για τα δικαιώματα και τις υποχρεώσεις τους, να τηρεί μητρώο επεξεργασιών και βέβαια να συνεργάζεται με τον Ευρωπαίο Επόπτη²².

Σύμφωνα με το άρθρο 3 §1 του 45/2001/ΕΚ, *«ο παρών Κανονισμός εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα από όλα τα όργανα και τους οργανισμούς της Κοινότητας, εφόσον η επεξεργασία αυτή*

²¹ Βλ. αιτιολογική σκέψη 2, προοιμίου του Κανονισμού.

²² Η πρόβλεψη των Υπευθύνων Προστασίας από τον Κανονισμό αποτελεί υλοποίηση της σχετικής δυνατότητας που είχε προβλέψει η Οδηγία 95/46/ΕΚ στο άρθρο 18§2.

πραγματοποιείται στα πλαίσια της άσκησης δραστηριοτήτων που εμπίπτουν , εν όλω ή εν μέρει, στο πεδίο εφαρμογής του κοινοτικού δικαίου».

Το πρώτο στοιχείο (κριτήριο *rationae personae*), καθιερώνει ειδικότερα ότι ο Κανονισμός εφαρμόζεται στην επεξεργασία δεδομένων από τα όργανα: Ευρωπαϊκό Κοινοβούλιο, Συμβούλιο της Ευρωπαϊκής Ένωσης, Ευρωπαϊκή Επιτροπή, Δικαστήριο των Ευρωπαϊκών Κοινοτήτων, Ελεγκτικό Συνέδριο και την Ευρωπαϊκή Κεντρική Τράπεζα. Επιπλέον, εφαρμόζεται στους ακόλουθους οργανισμούς: Ευρωπαϊκή Τράπεζα Επενδύσεων, Διαμεσολαβητή, Οικονομική και Κοινωνική Επιτροπή και Επιτροπή των Περιφερειών, Ευρωπαϊκό Κέντρο για την Ανάπτυξη και την Επαγγελματική Εκπαίδευση, Ευρωπαϊκό Οργανισμό για την βελτίωση των Βιοτικών και Εργασιακών Συνθηκών, Ευρωπαϊκή Υπηρεσία Περιβάλλοντος, Ευρωπαϊκό Εκπαιδευτικό Ίδρυμα, Ευρωπαϊκό Κέντρο για την παρακολούθηση των Ναρκωτικών και της Εξάρτησης από Ναρκωτικά, Ευρωπαϊκή Υπηρεσία για την Αξιολόγηση των Φαρμακευτικών Προϊόντων, Γραφείο για την Εναρμόνιση της Εσωτερικής Αγοράς, Ευρωπαϊκή Υπηρεσία για την Ασφάλεια και την Υγεία στην Εργασία, Κοινοτικό Γραφείο Ποικιλότητας Φυτών, Μεταφραστικό Κέντρο των Σωμάτων της Ένωσης, Ευρωπαϊκό Κέντρο Παρακολούθησης του Ρατσισμού και της Ξενοφοβίας, Ευρωπαϊκή Υπηρεσία για την Ανοικοδόμηση, Ευρωπαϊκή Αρχή Ασφάλειας Τροφίμων, Ευρωπαϊκή Υπηρεσία Ασφάλειας στη Θάλασσα και Ευρωπαϊκή Υπηρεσία Ασφάλειας στην Αεροπορία. Τέλος, και ο ίδιος ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων πρέπει να συμμορφώνεται²³.

Σύμφωνα με το δεύτερο στοιχείο (κριτήριο *rationae materiae*), οι δραστηριότητες αυτών των οργάνων και οργανισμών που εμπίπτουν ολικά εντός του δευτέρου και Τρίτου Πυλώνα της Συνθήκης ΕΕ δεν καλύπτονται από αυτόν τον Κανονισμό. Άλλωστε και στο άρθρο 16 του Προοιμίου του Κανονισμού τα μέτρα που θεσπίζονται από αυτόν δεν εφαρμόζονται σε αρχές που ιδρύθηκαν εκτός του κοινοτικού πλαισίου, όπως είναι η Ευροποι ή η Eurojust. Αυτές οι αρχές εφαρμόζουν τη Σύμβαση 108 και πρέπει να σέβονται τα θεμελιώδη δικαιώματα, σύμφωνα με το άρθρο 6 της Συνθήκης ΕΕ²⁴.

²³ Β. Σωτηρόπουλος, *Περαιτέρω Χρήση Πληροφοριών του Δημοσίου Τομέα*, Αθήνα- Θεσ/νίκη 2007, εκδόσεις Σάκκουλα, σελ.480-481.

²⁴ Βλ. αρ. 15 προοιμίου του Κανονισμού.

Η δεύτερη παράγραφος του ιδίου άρθρου αναφέρει ότι, «ο παρών Κανονισμός εφαρμόζεται στην, εν όλω ή εν μέρει, αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα, καθώς και στη μη αυτοματοποιημένη επεξεργασία τέτοιων δεδομένων, τα οποία περιλαμβάνονται ή πρόκειται να περιληφθούν σε αρχείο» (αρ. 3 §§1,2).

Αυτή η παράγραφος περιορίζει την εφαρμογή του Κανονισμού όσον αφορά την δια χειρός επεξεργασία. Ένα αρχείο καλύπτεται από τους κανόνες προστασίας δεδομένων, εφόσον είναι διαρθρωμένο σύμφωνα με ιδιαίτερα κριτήρια σχετιζόμενα με τα άτομα, έτσι ώστε να επιτρέπουν την εύκολη πρόσβαση στα απαιτούμενα δεδομένα. Στο μέτρο, λοιπόν, που ένα αρχείο επιτρέπει εύκολη πρόσβαση στα προσωπικά δεδομένα, εμπίπτει στο πεδίο εφαρμογής. Έτσι για παράδειγμα, οι κατάλογοι συμμετεχόντων στις τακτικές συναντήσεις που οργανώνονται από ένα όργανο και αποθηκεύονται σε χάρτινο αρχείο, συνήθως θα καλύπτονται²⁵.

1.3. Εννοιολογική προσέγγιση των προσωπικών δεδομένων

Μετά τη συνοπτική ανάλυση του νομικού υπόβαθρου του θεσμού του Ευρωπαϊκού Επόπτη και της προστασίας των προσωπικών δεδομένων και πριν προχωρήσουμε στην επί της ουσίας παρουσίαση της λειτουργίας του θεσμού αυτού μέσα από τις διατάξεις του Κανονισμού 45/2001, σκόπιμο θα ήταν να διευκρινιστούν κάποιοι ορισμοί που σχετίζονται με τα προσωπικά δεδομένα, έτσι ώστε να γίνει κατανοητό ποιο είναι το ακριβές αντικείμενο που τελεί υπό την εποπτεία-προστασία του Ευρωπαϊκού Επόπτη.

- **« Προσωπικά δεδομένα »**

Με τον όρο «προσωπικά δεδομένα» εννοούμε κάθε πληροφορία που αναφέρεται σε φυσικό πρόσωπο του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί (στο εξής αποκαλούμενο «υποκείμενο των δεδομένων»). Ως πρόσωπο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, λογίζεται το πρόσωπο εκείνο που μπορεί να προσδιοριστεί, άμεσα ή έμμεσα, ιδίως βάσει

²⁵ Β. Σωτηρόπουλος, *Περαιτέρω Χρήση Πληροφοριών του Δημοσίου Τομέα*, ό.π., σελ. 481.

αριθμού ταυτότητας ή βάσει ενός ή περισσότερων συγκεκριμένων στοιχείων που χαρακτηρίζουν την υπόστασή του από άποψη φυσική, βιολογική, ψυχική, οικονομική, πολιτιστική ή κοινωνική (άρθρο 2 § α' του Κανονισμού 45/2001/ΕΚ, και άρθρο 2^Α Οδηγίας 95/46/ΕΚ). Δεν λογίζονται ως δεδομένα προσωπικού χαρακτήρα τα στατιστικής φύσεως συγκεντρωτικά στοιχεία που συλλέχθηκαν στα πλαίσια στατιστικής έρευνας και από τα οποία δεν μπορούν πλέον να προσδιοριστούν τα υποκείμενα των δεδομένων. Παραδείγματα προσωπικών δεδομένων θα μπορούσαμε να αναφέρουμε τον αριθμό κυκλοφορίας ενός αυτοκινήτου, τον κάτοχο μιας κάρτας, τα στοιχεία ληξιαρχείου, ταυτότητας, στοιχεία οικογενειακής κατάστασης, δεδομένα εκπαίδευσης και επαγγελματικής εξειδίκευσης, πάσης φύσεως οικονομικά δεδομένα, εργασιακά στοιχεία κ.α.

Μια ειδική κατηγορία δεδομένων είναι τα λεγόμενα **«ευαίσθητα δεδομένα»**, αυτά δηλαδή που αφορούν στη φυλετική ή εθνική προέλευση, στα πολιτικά φρονήματα, στις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, στη συμμετοχή σε συνδικαλιστικές, επιστημονικές, φιλανθρωπικές οργανώσεις, στην υγεία, στην ερωτική ζωή και στις ποινικές διώξεις ή καταδίκες²⁶. Αναφορά στην κατηγορία αυτή των προσωπικών δεδομένων γίνεται στο άρθρο 10 § 1 του Κανονισμού 45/2001, όπου αναφέρεται ρητά η απαγόρευση επεξεργασίας των ευαίσθητων δεδομένων. Η απαγόρευση αυτή υπόκειται σε έναν αριθμό από εξαιρέσεις (αρ. 10 §2, περ. α-ε και §§§3,4,5), για παράδειγμα όταν το υποκείμενο έχει δώσει τη συγκατάθεσή του, αν η επεξεργασία αφορά δεδομένα που έχουν δημοσιευθεί πανηγυρικά από το υποκείμενο, η επεξεργασία είναι απαραίτητη για τη διασφάλιση ζωτικών συμφερόντων του υποκειμένου των δεδομένων κ.α.

- **«Επεξεργασία»**

Πρόκειται για κάθε εργασία ή σειρά εργασιών που πραγματοποιούνται (από τα όργανα και τους οργανισμούς της Κοινότητας) με ή χωρίς τη βοήθεια αυτοματοποιημένων μεθόδων και εφαρμόζονται σε δεδομένα προσωπικού χαρακτήρα, όπως η συλλογή, καταχώρηση, οργάνωση, διατήρηση,

²⁶ Ι. Ιγγλεζάκης, *Ευαίσθητα Προσωπικά Δεδομένα*, Αθήνα-Θεσ/κη, 2003, Εκδόσεις Σάκκουλας, σελ. 208 επ.,

προσαρμογή ή τροποποίηση, ανάκτηση, αναζήτηση πληροφοριών, χρήση, ανακοίνωση με διαβίβαση, διάδοση και κάθε άλλης μορφής διάθεσης, συσχέτιση ή συνδυασμός, καθώς και το κλείδωμα, η διαγραφή και η καταστροφή των δεδομένων αυτών (άρθρο 2 § β' του Κανονισμού).

Το ζήτημα της επεξεργασίας των προσωπικών δεδομένων αποτελεί τον βασικό άξονα γύρω από τον οποίο στρέφεται η προστασία των προσωπικών δεδομένων και αποτελεί τη βασική μέριμνα του Ευρωπαϊκού Επόπτη. Για τα θέματα που την αφορούν θα γίνει εκτενέστερα λόγος στη συνέχεια της παρούσας εργασίας.

- **«Αρχείο δεδομένων προσωπικού χαρακτήρα»**

Συναφής είναι και η έννοια του «αρχείου». Πρόκειται για κάθε διαρθρωμένο σύνολο δεδομένων προσωπικού χαρακτήρα το οποίο είναι προσιτά, με γνώμονα συγκεκριμένα κριτήρια, είτε το σύνολο αυτό είναι συγκεντρωμένο είτε αποκεντρωμένο είτε κατανεμημένο σε λειτουργική ή γεωγραφική βάση (άρθρο 2 § γ').

- **«Υπεύθυνος επεξεργασίας»**

Πρόκειται για το όργανο ή τον οργανισμό της Κοινότητας, τη Γενική Διεύθυνση, τη μονάδα ή κάθε άλλη διοικητική ενότητα που, αυτοτελώς ή από κοινού με άλλους, καθορίζει τους στόχους και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Όταν οι στόχοι και ο τρόπος της επεξεργασίας καθορίζονται σε ειδική κοινοτική πράξη, η ίδια αυτή πράξη είναι δυνατό να ορίζει τον υπεύθυνο της επεξεργασίας ή τα ειδικά κριτήρια που ισχύουν για το διορισμό του (άρθρο 2 § δ').

- **«Εκτελών την επεξεργασία»**

Είναι το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, υπηρεσία ή οποιοσδήποτε άλλος οργανισμός που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας (άρθρο 2 § ε').

- **«Τρίτος»**

Είναι το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή οποιοσδήποτε άλλος οργανισμός, εκτός από το υποκείμενο των δεδομένων, τον υπεύθυνο της επεξεργασίας, τον εκτελούντα την επεξεργασία και τα πρόσωπα τα οποία, υπό την άμεση εποπτεία του υπευθύνου της επεξεργασίας ή του εκτελούντος την επεξεργασία, που είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα αυτά (άρθρο 2 § στ').

- **«Αποδέκτης»**

Πρόκειται για το φυσικό ή νομικό πρόσωπο, δημόσια αρχή, υπηρεσία ή οποιοσδήποτε άλλος οργανισμός στον οποίο ανακοινώνονται τα δεδομένα, είτε πρόκειται για τρίτο, είτε όχι. Ωστόσο, οι αρχές στις οποίες ενδεχομένως ανακοινώνονται δεδομένα, στα πλαίσια ειδικής ερευνητικής αποστολής, δεν θεωρούνται ως αποδέκτες (άρθρο 2 § ζ').

- **«Συγκατάθεση»**

Είναι κάθε ελεύθερη, ρητή και εν πλήρη επίγνωση δήλωση βούλησης, με την οποία το υποκείμενο των δεδομένων, αφού προηγουμένως έχει ενημερωθεί, δέχεται να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν (άρθρο 2 § η'). Η ενημέρωση αυτή περιλαμβάνει πληροφόρηση τουλάχιστον για το σκοπό της επεξεργασίας, τα δεδομένα ή τις κατηγορίες δεδομένων που αφορά η επεξεργασία, τους αποδέκτες ή τις κατηγορίες αποδεκτών των προσωπικών δεδομένων, καθώς και το όνομα, την επωνυμία και τη διεύθυνση του υπευθύνου επεξεργασίας και του τυχόν εκπροσώπου του. Η συγκατάθεση μπορεί να ανακληθεί οποτεδήποτε, χωρίς αναδρομικό αποτέλεσμα²⁷.

Γενικά θα λέγαμε πως η συγκατάθεση του υποκειμένου των δεδομένων προσλαμβάνει ιδιαίτερη αξία, καθώς αποτελεί αυτοτελή όρο νομιμότητας της επεξεργασίας που προτάσσεται όλων των άλλων.

²⁷ Ι. Ιγγλεζάκης, *Δίκαιο της Πληροφορικής*, β' έκδοση, Αθήνα- Θεσ/νίκη 2008, εκδόσεις Σάκκουλα, σελ. 229.

1.4. Κανόνες περί του θεμιτού της επεξεργασίας των προσωπικών δεδομένων

1.4.1. Αρχές αναφερόμενες στην ποιότητα των δεδομένων

Στο δεύτερο κεφάλαιο του Κανονισμού 45/2001/EK, και πιο συγκεκριμένα στο άρθρο 4, αναφέρεται ότι τα δεδομένα προσωπικού χαρακτήρα πρέπει **α)** να υφίστανται **θεμιτή και νόμιμη επεξεργασία** και **β)** να συλλέγονται για **καθορισμένους, σαφείς και νόμιμους σκοπούς**, και η περαιτέρω επεξεργασία τους να συμβιβάζεται με τους σκοπούς αυτούς. Όπως αναφέρθηκε και παραπάνω, η επεξεργασία που γίνεται για ιστορικούς, στατιστικούς ή επιστημονικούς σκοπούς δεν θεωρείται ασυμβίβαστη, υπό την προϋπόθεση ότι ο υπεύθυνος της επεξεργασίας προβλέπει κατάλληλες εγγυήσεις, προκειμένου να διασφαλίζεται ότι η επεξεργασία των δεδομένων δεν πραγματοποιείται για άλλους σκοπούς και ότι τα δεδομένα δεν θα χρησιμοποιηθούν προς υποστήριξη μέτρων ή αποφάσεων που αφορούν ένα συγκεκριμένο πρόσωπο, **γ)** να είναι **πρόσφορα, συναφή** προς το θέμα και **όχι υπέρμετρα** σε σχέση με τους σκοπούς για τους οποίους συλλέγονται και επεξεργάζονται, **δ)** να είναι **ακριβή** και να ενημερώνονται, εφόσον χρειάζεται. Τα ανακριβή ή ελλιπή δεδομένα πρέπει να διαγράφονται ή να διορθώνονται, και **ε)** να διατηρούνται υπό μορφή που να επιτρέπει τον προσδιορισμό της ταυτότητας των υποκειμένων τους **μόνο κατά τη διάρκεια της περιόδου που είναι αναγκαία για την επίτευξη των σκοπών** για τους οποίους έχουν συλλεγεί και υφίστανται την επεξεργασία. Το όργανο ή ο οργανισμός της Κοινότητας προβλέπει ότι για τα δεδομένα που πρέπει να αποθηκευτούν πέραν της περιόδου αυτής, για τους προαναφερθέντες σκοπούς (ιστορικούς, στατιστικούς ή επιστημονικούς), πρέπει να διατηρούνται μόνο υπό μορφή που τα καθιστά ανώνυμα, είτε να αποθηκεύονται μόνο υπό τον όρο ότι η ταυτότητα του υποκειμένου τους τελεί υπό κρυπτογραφική μορφή.

Ρητά στον Κανονισμό αναφέρεται ότι ο υπεύθυνος της επεξεργασίας πρέπει να διασφαλίζει την τήρηση της παραγράφου αυτής.

1.4.2. Αρχές σχετικές με τη νομιμότητα της επεξεργασίας δεδομένων

α. Το θεμιτό της επεξεργασίας

Το άρθρο 5 του Κανονισμού παίζει κεντρικό ρόλο, αναφορικά με τη χορήγηση προσωπικών δεδομένων στο κοινό, διότι ορίζει πότε μια πράξη μπορεί να είναι νόμιμη ή όχι. Σύμφωνα λοιπόν με το εν λόγω άρθρο, η επεξεργασία των προσωπικών δεδομένων πραγματοποιείται μόνο εφόσον:

- είναι απαραίτητη για την εκπλήρωση καθήκοντος προς χάριν του δημοσίου συμφέροντος βάσει των Συνθηκών για την ίδρυση των Ευρωπαϊκών Κοινοτήτων ή άλλων νομοθετικών πράξεων που έχουν θεσπιστεί βάσει των συνθηκών αυτών ή για την εκπλήρωση καθήκοντος που ανάγεται στη νόμιμη άσκηση δημόσιας εξουσίας που έχει ανατεθεί στο όργανο ή στον οργανισμό της Κοινότητας ή σε τρίτον στον οποίον ανακοινώνονται τα δεδομένα,
- είναι απαραίτητη για την εκπλήρωση νόμιμης υποχρέωσης την οποία υπέχει ο υπεύθυνος της επεξεργασίας,
- είναι απαραίτητη για την εκτέλεση συμβάσεως στην οποία συμμετέχει το υποκείμενο των δεδομένων ή για την εφαρμογή προσυμβατικών μέτρων που λαμβάνονται κατόπιν αιτήσεώς του,
- το υποκείμενο των δεδομένων έχει παράσχει την αναμφισβήτητη συγκατάθεσή του,
- είναι απαραίτητη για τη διασφάλιση ζωτικών συμφερόντων του υποκειμένου των δεδομένων.

Η διάταξη αυτή προβλέπει διαζευκτικά τις πέντε «κλασσικές» νόμιμες βάσεις της επεξεργασίας, ενώ σημαντικό είναι ότι προτάσσει τους όρους αναγκαίας επεξεργασίας για συμμόρφωση προς την αρχή της νομιμότητας (όροι α και β, εκπλήρωση καθήκοντος χάριν του δημοσίου συμφέροντος, εκπλήρωση νόμιμης υποχρέωσης του υπευθύνου) και στη συνέχεια ακολουθούν οι όροι της εκτέλεσης σύμβασης, της «αδιαμφισβήτητης» συγκατάθεσης και της διασφάλισης ζωτικού συμφέροντος του υποκειμένου. Η διατύπωση αυτή εμπεριέχει κλιμάκωση των όρων επιτρεπτής επεξεργασίας, ανάλογα με το

βαθμό θεμιτής αναγκαιότητάς τους, ενόψει της φύσης των υπευθύνων επεξεργασίας ως οργάνων της δημόσιας εξουσίας που ασκεί η Κοινότητα²⁸.

β. Ο σκοπός της επεξεργασίας (άρθρο 6 του Κανονισμού)

Η αρχή του σκοπού είναι πολύ σημαντική για την προστασία των προσωπικών δεδομένων, διότι με τον καθορισμό του σκοπού της επεξεργασίας και με την προσήλωση σε αυτόν αποφεύγεται η «πολυλειτουργική» συλλογή και χρήση των προσωπικών δεδομένων, την οποία θα επιθυμούσαν οι υπεύθυνοι της επεξεργασίας και η οποία, όμως, συνιστά μη ανεκτή επέμβαση στα προσωπικά δεδομένα και στην ιδιωτική ζωή του ατόμου²⁹.

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα για σκοπούς άλλους εκτός από εκείνους για τους οποίους έχουν συλλεγεί, γίνεται μόνον εφόσον η μεταβολή του σκοπού επιτρέπεται ρητώς από τον εσωτερικό κανονισμό του οργάνου ή του οργανισμού της Κοινότητας.

Τα δεδομένα προσωπικού χαρακτήρα που συλλέγονται με αποκλειστικό σκοπό την κατοχύρωση της ασφάλειας ή του ελέγχου των συστημάτων ή των εργασιών επεξεργασίας, δεν επιτρέπεται να χρησιμοποιούνται για κανέναν άλλο σκοπό, με εξαίρεση την πρόληψη, τη διερεύνηση, τη διακρίβωση και τη δίωξη σοβαρών αξιόποινων πράξεων.

γ. Η διαβίβαση των προσωπικών δεδομένων (άρ. 7,8,9 του Κανονισμού)

Η διαβίβαση των δεδομένων διαχωρίζεται σε τρεις περιπτώσεις:

- 1) Η διαβίβαση στο εσωτερικό ή μεταξύ των οργάνων ή των οργανισμών της Κοινότητας, η οποία επιτρέπεται μόνο εφόσον τα δεδομένα είναι αναγκαία για τη νόμιμη εκτέλεση καθήκοντος που εμπίπτει στην αρμοδιότητα του αποδέκτη, δηλαδή στα πλαίσια της αρχής της νομιμότητας (άρθρο 7).

²⁸ Β. Σωτηρόπουλος, *Η συνταγματική προστασία των προσωπικών δεδομένων*, ό.π., σελ 31. (υποσημείωση αρ.75)

²⁹ Ι. Ιγγλεζάκης, *Δίκαιο της Πληροφορικής*, ό.π., σελ. 233.

- 2) Η διαβίβαση στο εσωτερικό της Κοινότητας, αλλά προς αποδέκτες εκτός των οργάνων της, οι οποίοι υπάγονται στην Οδηγία 95/46³⁰, είναι επιτρεπτή μόνο εφόσον ο αποδέκτης επικαλείται την αναγκαιότητά της για εκπλήρωση εννόμου συμφέροντος ή αποδεικνύει κάποιον άλλο νόμιμο λόγο που δεν θίγει τα δικαιώματα του υποκειμένου των δεδομένων (άρθρο 8).
- 3) Η διαβίβαση προς αποδέκτες οι οποίοι δεν υπάγονται στην Οδηγία 95/46, δηλαδή σε κράτη/οργανισμούς εκτός Ε.Ε. επιτρέπεται μόνο εφόσον κριθεί ότι εξασφαλίζουν επαρκές επίπεδο προστασίας προσωπικών δεδομένων και η διαβίβαση αποκλειστικά στο να διευκολύνει την εκτέλεση καθήκοντος του υπεύθυνου επεξεργασίας (άρθρο 9).

Η επάρκεια του βαθμού προστασίας που παρέχει η εκάστοτε χώρα ή ο συγκριμένος διεθνής οργανισμός αξιολογείται με γνώμονα το σύνολο των περιστάσεων που περιβάλλουν την εργασία ή το σύνολο των εργασιών της διαβίβασης των δεδομένων.

Ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων μπορεί να επιτρέψει διαβίβαση ή σύνολο διαβιβάσεων δεδομένων προσωπικού χαρακτήρα προς μια τρίτη χώρα ή ένα διεθνή οργανισμό που δεν παρέχει ικανοποιητικό επίπεδο προστασίας, σύμφωνα με τα ανωτέρω, όταν ο υπεύθυνος της επεξεργασίας παρέχει επαρκείς εγγυήσεις όσον αφορά την προστασία της ιδιωτικής ζωής και των θεμελιωδών δικαιωμάτων και ελευθεριών των προσώπων, καθώς και όσον αφορά την άσκηση των αντιστοίχων δικαιωμάτων οι εγγυήσεις αυτές μπορούν ιδίως να απορρέουν από κατάλληλες συμβατικές ρήτρες (αρ.9 §7).

1.4.3 Η ενημέρωση του υποκειμένου των δεδομένων

Ο Κανονισμός 45/2001/ΕΚ παρέχει στα υποκείμενα των δεδομένων έναν αριθμό ρητά προβλεπόμενων δικαιωμάτων. Οι αρχές αυτές αποτελούν υλοποίηση της γενικής αρχής της θεμιτής επεξεργασίας, όπως περιέχεται στο άρθρο 4 του Κανονισμού. Αφενός, το υποκείμενο των δεδομένων έχει το

³⁰ Βλ. σχετικά Θ. Σιδηρόπουλος, *Το δίκαιο του διαδικτύου*, β' έκδοση, Αθήνα-Θεσ/κη, 2008, εκδόσεις Σάκκουλα, σελ 247-248.

δικαίωμα να είναι ενημερωμένο και να υπερασπίζεται τα νόμιμα συμφέροντά του επί τη βάσει αυτών των πληροφοριών και αφετέρου, το όργανο ή ο οργανισμός που πρέπει να αποφασίσει για τη χορήγηση μπορεί να δράσει προληπτικά και να ενημερώσει το υποκείμενο των δεδομένων για τους σκοπούς του.

Παραπέρα, στα άρθρα 11 και 12 του Κανονισμού, γίνεται ένας διαχωρισμός της ενημέρωσης ανάμεσα στην περίπτωση που τα δεδομένα συλλέγονται παρά τω υποκειμένω των δεδομένων (αρ.11) και στην περίπτωση που τα δεδομένα δεν έχουν συλλεγεί παρά τω υποκειμένω (αρ.12).

Στην πρώτη περίπτωση ο υπεύθυνος της επεξεργασίας παρέχει στο πρόσωπο παρά τω οποίω συλλέγονται δεδομένα που το αφορούν πληροφορίες όπως: 1. η **ταυτότητα του υπευθύνου** επεξεργασίας, 2. ο **σκοπός** της επεξεργασίας των δεδομένων, 3. οι **αποδέκτες** των δεδομένων, 4. η ένδειξη αν η **απάντηση των ερωτήσεων** είναι υποχρεωτική ή προαιρετική, καθώς και οι συνέπειες παράλειψης απάντησης, 5. Το **δικαίωμα πρόσβασης** στα δεδομένα που το αφορούν και το **δικαίωμα διόρθωσης** αυτών, και 6. κάθε άλλη **συμπληρωματική πληροφορία** όπως π.χ. η νομική βάση της επεξεργασίας, η διάρκεια διατήρησης των δεδομένων και το δικαίωμα προσφυγής, ανά πάσα στιγμή στον Ευρωπαϊό Επόπτη.

Στη δεύτερη περίπτωση, ο υπεύθυνος της επεξεργασίας οφείλει, κατά την καταχώρηση των δεδομένων ή σε περίπτωση που προβλέπεται η ανακοίνωση των δεδομένων σε τρίτον, να παρέχει στο υποκείμενο των δεδομένων τουλάχιστον πληροφορίες όπως: α. την ταυτότητα του υπευθύνου της επεξεργασίας, β. τους σκοπούς αυτής, γ. τις κατηγορίες των σχετικών δεδομένων, δ. τους αποδέκτες των δεδομένων, ε. την ύπαρξη δικαιώματος πρόσβασης στα δεδομένα ή δικαίωμα διόρθωσης αυτών, στ. τις συμπληρωματικές πληροφορίες που προαναφέρθηκαν και επιπρόσθετα την ενημέρωση του υποκειμένου για την προέλευση των δεδομένων, εκτός αν ο υπεύθυνος της επεξεργασίας δεν δύναται να αποκαλύψει το στοιχείο αυτό για λόγους επαγγελματικού απορρήτου.

Τα ανωτέρω δεν εφαρμόζονται όταν η επεξεργασία γίνεται για σκοπούς στατιστικούς, ιστορικούς ή επιστημονικής έρευνας και η ενημέρωση του

υποκειμένου των δεδομένων αποδεικνύεται αδύνατη ή προϋποθέτει δυσανάλογες προσπάθειες ή εάν η καταχώρηση ή η ανακοίνωση των δεδομένων προβλέπεται ρητώς από την κοινοτική νομοθεσία. Στις περιπτώσεις αυτές, το όργανο ή ο οργανισμός της Κοινότητας προβλέπει τις κατάλληλες εγγυήσεις αφού ζητήσει τη γνώμη του Ευρωπαϊκού Επόπτη (άρθρο 12 § 2 του Κανονισμού).

1.4.4. Τα δικαιώματα του υποκειμένου των δεδομένων

Ο Κανονισμός δεν παραλείπει να κατοχυρώσει τα δικαιώματά του υποκειμένου. Έτσι κάνει ρητή αναφορά στα εξής δικαιώματα:

- 1) Το δικαίωμα πρόσβασης (άρθρο 13), δηλαδή το δικαίωμα που έχει καθένας να γνωρίζει εάν τα δεδομένα προσωπικού χαρακτήρα που τον αφορούν αποτελούν ή αποτέλεσαν αντικείμενο επεξεργασίας. Προς τούτο, το υποκείμενο των δεδομένων έχει δικαίωμα να ζητεί και να λαμβάνει από τον υπεύθυνο της επεξεργασίας εγγράφως, έγκυρα και έγκαιρα (εντός προθεσμίας τριών μηνών), τις ακόλουθες πληροφορίες:
 - ο Επιβεβαίωση για το κατά πόσον διενεργείται ή όχι επεξεργασία δεδομένων που το αφορούν,
 - ο Πληροφορίες σχετικά με τους σκοπούς της επεξεργασίας και τους αποδέκτες στους οποίους ανακοινώνονται τα δεδομένα,
 - ο Ανακοίνωση με εύληπτο τρόπο των υπό επεξεργασία δεδομένων καθώς και κάθε πληροφορίας για την προέλευσή τους,
 - ο Ενημέρωση σχετικά με τη λογική στην οποία στηρίζεται η αυτοματοποιημένη επεξεργασία των δεδομένων που το αφορούν.
- 2) Το δικαίωμα διόρθωσης (άρθρο 14), δηλαδή το δικαίωμα εκείνου του υποκειμένου να λαμβάνει από τον υπεύθυνο της επεξεργασίας αμελλητί τη διόρθωση δεδομένων προσωπικού χαρακτήρα που είναι ανακριβή ή ελλιπή.
- 3) Το δικαίωμα του κλειδώματος των δεδομένων (άρθρο 15), δηλαδή το δικαίωμα του υποκειμένου να λαμβάνει κλείδωμα των δεδομένων από τον υπεύθυνο, όταν:

- i. Το υποκείμενο αμφισβητεί την ακρίβειά τους.
- ii. Ο υπεύθυνος της επεξεργασίας δεν τα χρειάζεται πλέον για την εκτέλεση των καθηκόντων του.
- iii. Η επεξεργασία των δεδομένων είναι παράνομη.

Στην περίπτωση των αυτοματοποιημένων αρχείων, το κλείδωμα πραγματοποιείται με τεχνικές μεθόδους. Συνήθως, το κλείδωμα των δεδομένων θα αναγράφεται στο σύστημα με τρόπο σαφή, ώστε να αποτρέπεται οποιαδήποτε χρήση τους. Η επεξεργασία κλειδωμένων στοιχείων, επιτρέπεται μόνο για αποδεικτικούς σκοπούς ή με τη συγκατάθεση του υποκειμένου των δεδομένων ή για την προστασία δικαιωμάτων τρίτων (αρ. 15 §2,3).

- 4) Το δικαίωμα διαγραφής έχει το υποκείμενο όταν η επεξεργασία των δεδομένων που γίνεται αντικείμενο επεξεργασίας από τον υπεύθυνο είναι παράνομη και ειδικά όταν παραβιάζονται οι προαναφερθείσες διατάξεις σχετικά με την ποιότητα των δεδομένων, με τη νομιμοποίηση της επεξεργασίας και τα ευαίσθητα προσωπικά δεδομένα (άρθρο 16).
- 5) Το υποκείμενο έχει το δικαίωμα να λαμβάνει από τον υπεύθυνο την ανακοίνωση στους τρίτους στους οποίους έχουν γνωστοποιηθεί τα δεδομένα που το αφορούν, καθώς και κάθε διόρθωση, διαγραφή ή κλείδωμά τους, εκτός αν αυτό αποδεικνύεται αδύνατον ή προϋποθέτει δυσανάλογη προσπάθεια (άρθρο 17).
- 6) Το υποκείμενο έχει το δικαίωμα αντίταξης στην επεξεργασία των δεδομένων έχει το υποκείμενο α. για λόγους επιτακτικούς και νόμιμους σχετικούς με την προσωπική του κατάσταση, β. σε περίπτωση ανακοίνωσης ή χρησιμοποίησης των δεδομένων του σε/από τρίτους για σκοπούς προώθησης προϊόντων (άρθρο 18).
- 7) Το υποκείμενο έχει δικαίωμα να μη συμμορφώνεται με απόφαση η οποία παράγει έναντι αυτού έννομα αποτελέσματα ή το θίγει σε σημαντικό βαθμό και αφορά την αξιολόγηση ορισμένων πτυχών της προσωπικότητάς του, όπως είναι η απόδοσή του στην εργασία, η αξιοπιστία ή η διαγωγή του, εκτός και αν η απόφαση αυτή επιτρέπεται ρητά από το εθνικό ή κοινοτικό δίκαιο ή από τον Ευρωπαϊκό Επόπτη. Και

στις δύο περιπτώσεις, πρέπει να λαμβάνονται μέτρα που να εξασφαλίζουν τη διαφύλαξη των εννόμων συμφερόντων του υποκειμένου των δεδομένων, όπως τα μέτρα που του επιτρέπουν να διατυπώνει την άποψή του (άρθρο 19).

1.4.5. Εξαιρέσεις και περιορισμοί

Το άρθρο 20 του Κανονισμού 45/2001 παρέχει στα κοινοτικά όργανα και οργανισμούς τη δυνατότητα να περιορίσουν την εφαρμογή κάποιων από τις ανωτέρω διατάξεις (λ.χ. αρ.4 §1, αρ.11, αρ.12 §1, αρ.13-17 και αρ. 37 §1), εφόσον ο εκάστοτε περιορισμός αποτελεί αναγκαίο μέτρο. Οι περιπτώσεις αυτές απαριθμούνται στο εν λόγω άρθρο (αρ. 20 §1 περ. α-ε). Αν ο περιορισμός επιβληθεί, το υποκείμενο των δεδομένων θα ενημερωθεί για τους κύριους λόγους που αιτιολογούν τον περιορισμό αυτό και θα έχει δικαίωμα προσφυγής στον Ευρωπαϊό Επόπτη (αρ.20 §3).

Οι εξαιρέσεις και οι περιορισμοί του άρθρου 20 συνιστούν αποκλίσεις από το ισορροπημένο σύστημα του Κανονισμού 45/2001. Αποκλείουν το υποκείμενο των δεδομένων από ουσιώδη στοιχεία της προστασίας που του απονέμεται σύμφωνα με τον Κανονισμό. Με βάση το κοινοτικό δίκαιο, τέτοιες εξαιρέσεις πρέπει να ερμηνεύονται περιοριστικά. Πρέπει, επίσης, να τονιστεί ότι το άρθρο 20 αναφέρεται σε εξαιρετικές περιπτώσεις όπου η προστασία του υποκειμένου των δεδομένων που βασίζεται στο άρθρο 4 του Κανονισμού, θα μπορούσε να βλάψει άλλα θεμελιώδη δημόσια συμφέροντα. Ο εν λόγω Κανονισμός προβλέπει ρητή αιτιολογία σε κάθε ατομική περίπτωση όταν εφαρμόζεται ο περιορισμός του άρθρου 20. Αυτή η αιτιολογία υπόκειται σε έλεγχο από τον Ευρωπαϊό Επόπτη και σε τελικό επίπεδο από το Δικαστήριο των Ευρωπαϊκών Κοινοτήτων³¹.

³¹ Β. Σωτηρόπουλος, *Περαιτέρω χρήση πληροφοριών του Δημοσίου Τομέα*, ό.π., σελ.488.

1.4.6. Εμπιστευτικότητα και ασφάλεια της επεξεργασίας

Στο άρθρο 21 του Κανονισμού, αναφέρεται ρητά ότι τα πρόσωπα που απασχολούνται από όργανο ή οργανισμό της Κοινότητας καθώς και εκείνα που εκτελούν την επεξεργασία των προσωπικών δεδομένων και έχουν πρόσβαση σ' αυτά, μπορούν να τα επεξεργάζονται μόνο κατ' εντολή του υπευθύνου της επεξεργασίας.

Λαμβάνοντας υπόψη την πρόοδο της επιστήμης και το σχετικό κόστος εφαρμογής, ο υπεύθυνος επεξεργασίας εφαρμόζει τα κατάλληλα τεχνικά και οργανωτικά μέτρα για την κατοχύρωση κατάλληλου βαθμού ασφάλειας ενόψει των κινδύνων της επεξεργασίας και της φύσης των δεδομένων προσωπικού χαρακτήρα που πρέπει να προστατευθούν. Τα μέτρα αυτά λαμβάνονται κυρίως για να αποτρέπεται οποιαδήποτε μη επιτρεπόμενη διαβίβαση ή πρόσβαση, τυχαία ή παράνομη καταστροφή ή τυχαία απώλεια ή αλλοίωση, καθώς και οιαδήποτε άλλη μορφή παράνομης επεξεργασίας (άρθρο 22 §1).

Ο υπεύθυνος της επεξεργασίας οφείλει, όταν η επεξεργασία εκτελείται για λογαριασμό του, να επιλέγει ως εκτελούντα αυτής ένα πρόσωπο που να του παρέχει επαρκείς εγγυήσεις όσον αφορά τα τεχνικά και οργανωτικά μέτρα ασφάλειας που προβλέπονται στο άρθρο 22 και να μεριμνά για την τήρησή τους (άρθρο 23 §1).

Η ανάθεση της εκτέλεσης της επεξεργασίας πρέπει να διέπεται από σύμβαση ή νομική πράξη η οποία να συνδέει τον εκτελούντα την επεξεργασία με τον υπεύθυνο αυτής και να προβλέπει α) ότι ο εκτελών ενεργεί μόνο κατ' εντολή του υπευθύνου της επεξεργασίας και β) ότι οι υποχρεώσεις που προβλέπονται στα άρθρα 21-22 βαρύνουν τον εκτελούντα, εκτός αν, δυνάμει του άρθρου 16 ή 17 §3, δεύτερη περίπτωση της οδηγίας 95/46/EK, ο εκτελών υπόκειται ήδη σε υποχρεώσεις περί εμπιστευτικότητας και ασφάλειας που προβλέπονται από την εθνική νομοθεσία ενός κράτους μέλους (άρθρο 23 §2 περ. α' και β').

2. Ο ΕΥΡΩΠΑΙΟΣ ΕΠΟΠΤΗΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ: ΣΥΣΤΑΣΗ ΚΑΙ ΑΡΜΟΔΙΟΤΗΤΕΣ

2.1. Η νομική θέση του ΕΕΠΔ

Ο Ευρωπαίος Επόπτης είναι μια μονοπρόσωπη, ανεξάρτητη εποπτική αρχή, το νομικό καθεστώς της οποίας διέπεται κατ' αρχήν από τα άρθρα 41-48 (Κεφάλαιο V) του Κανονισμού 45/2001/ΕΚ. Η φύση της αρχής ως ανεξάρτητης θεμελιώνεται στα στοιχεία: α) προσωπικής και λειτουργικής ανεξαρτησίας, β) διοικητικής αυτοτέλειας, γ) δημοσιονομικής αυτοτέλειας, δ) των σχέσεων με το Ευρωπαϊκό Κοινοβούλιο.

Την προσωπική και λειτουργική ανεξαρτησία εγγυώνται οι διατάξεις που αναφέρονται στα κριτήρια επιλογής του Επόπτη και του Αναπληρωτή από το Ευρωπαϊκό Κοινοβούλιο. Σύμφωνα με το άρθρο 42 §2 του Κανονισμού, «Ο ευρωπαίος επόπτης προστασίας δεδομένων επιλέγεται μεταξύ προσώπων τα οποία παρέχουν εχέγγυα ανεξαρτησίας και διαθέτουν αξιόλογη εμπειρία και ικανότητες για την εκπλήρωση των καθηκόντων του ευρωπαίου επόπτη προστασίας δεδομένων, π.χ. διότι συμμετέχουν ή είχαν συμμετάσχει στις αρχές ελέγχου που αναφέρονται στο άρθρο 28 της οδηγίας 95/46/ΕΚ».

Ο Επόπτης, όπως οι δικαστές και ο γραμματέας του ΔΕΚ, απολαμβάνει τα προνόμια και τις ασυλίες του σχετικού Πρωτοκόλλου (άρθρα 12-15 και 18 που ισχύει για τις Ευρωπαϊκές Κοινότητες (άρθρο 42 § 7). Επίσης, σύμφωνα με το άρθρο 44 του Κανονισμού, ο ΕΕΠΔ δεν ζητά ούτε δέχεται εντολές από οποιονδήποτε κατά την εκτέλεση των καθηκόντων του. Απολαύει πλήρους ανεξαρτησίας, ενώ απέχει από οποιαδήποτε πράξη η οποία δεν συμβιβάζεται με τα καθήκοντά του και δεν ασκεί κατά τη διάρκεια της θητείας του, καμία άλλη επαγγελματική δραστηριότητα, αμειβόμενη ή μη (άρ.44 §§ 1-3). Όσον αφορά τις αποδοχές του, ο Επόπτης εξομοιώνεται με δικαστή του ΔΕΚ, ενώ ο Αναπληρωτής με τον Γραμματέα του ΔΕΚ³². Ο Αναπληρωτής επικουρεί τον Επόπτη στο σύνολο των καθηκόντων του και τον αναπληρώνει σε περίπτωση απουσίας ή κωλύματος.

³² Απόφαση 1247/2002/ΕΚ, άρθρα 1 και 2.

Υπόλογος μπορεί να είναι ο ΕΕΠΔ μόνο στο Ευρωπαϊκό Δικαστήριο, το οποίο δύναται να επιθεωρεί τις ενέργειές του, εάν αυτές αμφισβητούνται, και στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο στα οποία υποβάλλει την Ετήσια Έκθεσή του και ενώπιόν τους την παρουσιάζει³³.

Τη *διοικητική αυτοτέλεια* του οργάνου αυτού εγγυώνται οι διατάξεις που προβλέπουν ότι η αρχή επικουρείται από γραμματεία, το προσωπικό της οποίας διορίζεται από τον Επόπτη, ιεραρχικό προϊστάμενο στον οποίο υπάγεται αποκλειστικά. Το προσωπικό αυτό δεσμεύεται από τις κανονιστικές ρυθμίσεις που εφαρμόζονται γενικά στους υπαλλήλους των Ευρωπαϊκών Κοινοτήτων (άρθρο 43 §§ 4,5,6). Στα πλαίσια της διοικητικής ανεξαρτησίας της αρχής εντάσσεται η αρμοδιότητά του Επόπτη να θεσπίζει τον κανονισμό εσωτερικής λειτουργίας του (άρθρο 46 § 1α').

Τη *δημοσιονομική αυτοτέλεια* του οργάνου εγγυώνται οι διατάξεις που προβλέπουν ότι η αρμόδια επί του προϋπολογισμού αρχή φροντίζει για τους οικονομικούς πόρους που χρειάζονται για την εκτέλεση των καθηκόντων του ΕΕΠΔ και ο προϋπολογισμός αυτός περιλαμβάνεται σε ειδική γραμμή του γενικού προϋπολογισμού της Ε.Ε. (άρθρο 43 §§ 2,3).

Ο Επόπτης και ο Αναπληρωτής του διορίζονται από το *Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο* με κοινή συμφωνία, για θητεία πέντε ετών, βάσει καταλόγου που συντάσσει η Επιτροπή, κατόπιν δημόσιας πρόσκλησης για υποβολή υποψηφιοτήτων. Η θητεία αυτή δύναται να ανανεωθεί (άρθρο 42 §3). Όλοι οι ενδιαφερόμενοι στο σύνολο της Κοινότητας μπορούν να υποβάλλουν υποψηφιότητα, ενώ το Ευρωπαϊκό Κοινοβούλιο μπορεί ν' αποφασίσει να διοργανώσει ακρόαση για να διαμορφώσει γνώμη (άρθρο 42 §1). Η απαλλαγή του Επόπτη και του Αναπληρωτή από τα καθήκοντά του μπορεί να γίνει με απόφαση του ΔΕΚ, ύστερα από πρόταση του Ευρωπαϊκού Κοινοβουλίου, της Επιτροπής ή του Συμβουλίου. Κάθε χρόνο ο ΕΕΠΔ υποβάλλει στο Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο και την Επιτροπή έκθεση πεπραγμένων (Annual Report) την οποία οφείλει να δημοσιεύσει (άρθρο 48). Ο Επόπτης έχει τη δυνατότητα να προσφεύγει ενώπιον του Ευρωπαϊκού Κοινοβουλίου, του

³³ Interview of J. Bayo Delgado, published in "Hablemos de Europa", No 7, Δεκέμβριος 2008 και στο site: www.edps.europa.eu, Publications/ Speeches & Articles, σελ. 2.

Συμβουλίου και της Επιτροπής, όταν παρίσταται ανάγκη (άρθρο 47 §1 ζ'). Οι αποφάσεις του Επόπτη προσβάλλονται ενώπιον του ΔΕΚ (άρθρο 32 § 4).

2.2. Ο διορισμός και η διοικητική υποστήριξη του θεσμού

Η νομοθετική υλοποίηση της επιταγής του άρθρου 286 § 2 ΣυνΘΕΚ επήλθε πέντε χρόνια μετά τη Συνθήκη του Άμστερνταμ, με τον Κανονισμό 45/2001, ενώ η πραγματική λειτουργία του θεσμού του ΕΕΠΔ άρχισε το 2004, με το διορισμό του πρώτου Επόπτη, Peter Hustinx³⁴, και του Αναπληρωτή του Joaquín Bayo Delgado³⁵, την 22^α Δεκεμβρίου 2004. Η έδρα του ΕΕΠΔ και του Αναπληρωτή είναι στις Βρυξέλλες, όπου όταν αφίχθησαν, στις 2.2.2004, δεν είχε προβλεφθεί χώρος στέγασης του οργάνου και δεν είχε προσληφθεί γραμματεία για τη στήριξή του. Έτσι, αρχικά εγκαταστάθηκαν σ' ένα κτίριο του Ευρωπαϊκού Κοινοβουλίου. Κατόπιν, οι Γενικοί Γραμματείς των τριών μεγάλων θεσμικών οργάνων (Κοινοβούλιο, Επιτροπή και Συμβούλιο) υπέγραψαν με τον ΕΕΠΔ μια συμφωνία διοικητικής συνεργασίας προκειμένου να βοηθηθεί ο νέος θεσμός για τα πρώτα τρία έτη. Οι υπηρεσίες της Επιτροπής παρέχουν βοήθεια στον ΕΕΠΔ για όλα τα καθήκοντα που αφορούν την διαχείριση των προσώπων που συνδέονται με το όργανο καθώς και για την κατάρτιση και την εκτέλεση του προϋπολογισμού. Το Συμβούλιο επικουρεί στον τομέα της μετάφρασης³⁶.

Έως το τέλος του 2004 όλο το προσωπικό της Αρχής είχε προσληφθεί. Συνολικά προσλήφθηκαν 15 άτομα, από τα οποία τα 7 είναι υπάλληλοι και τα 8 έχουν σύμβαση εκτάκτου υπαλλήλου³⁷. Τα 5 από τα άτομα αυτά αποτελούν μια μονάδα επιφορτισμένη με διοικητικά καθήκοντα, ενώ τα υπόλοιπα 10 είναι μια μονάδα που έχει λειτουργικά καθήκοντα. Αυτή η δεύτερη μονάδα χωρίζεται σε

³⁴ Ο κ. Hustinx διετέλεσε Πρόεδρος της Εθνικής Αρχής Προστασίας Δεδομένων της Ολλανδίας από το Σεπτέμβριο του 2001 και από το 1996-2000 ήταν πρόεδρος της Ομάδας Εργασίας του άρθρου 29. Τον Ιανουάριο του 2009 επανεξελέγη για μια ακόμα πενταετία στη θέση του Ευρωπαϊού Επόπτη.

³⁵ Ο κ. Bayo Delgado, ήταν δικαστής από το 1989, πρόεδρος του δικαστικού συλλόγου της Βαρκελώνης και μέλος της Επιτροπής Πληροφοριών του Ισπανικού Συμβουλίου Δικαιοσύνης. Η θητεία του διήρκεσε έως το 2009, ενώ από τον Ιανουάριο του 2009 στη θέση του εξελέγη ο Giovanni Buttarelli για την επόμενη πενταετία. Ο G.Buttarelli εργάστηκε ως Γενικός Γραμματέας της ιταλικής Αρχής Προστασίας Δεδομένων από το 1997, ενώ το διάστημα μεταξύ 2002-2003 διετέλεσε Πρόεδρος της κοινής ελεγκτικής αρχής (Schengen Joint Supervisory Body) στο πλαίσιο του Schengen.

³⁶ Βασίλης Σωτηρόπουλος, «Ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων», *ό.π.*, σελ. 1186-1188.

³⁷ Ετήσια Έκθεση ΕΕΠΔ 2004, σελ. 14-17.

δύο τμήματα: σε αυτό που ασχολείται με τα καθήκοντα εποπτείας και το άλλο με γνωμοδοτικά και ενημερωτικά καθήκοντα.

Για την εύρυθμη λειτουργία του, ο ΕΕΠΔ θέσπισε εσωτερικούς διαδικαστικούς κανόνες, όπως α) κώδικα δεοντολογίας, σύμφωνα με τον οποίο κάθε υπάλληλος δεσμεύεται εγγράφως κατά την ανάληψη της υπηρεσίας να τηρεί την εμπιστευτικότητα των δεδομένων στα οποία έχει πρόσβαση κατά την ενάσκηση των καθηκόντων του, β) διοικητικό οδηγό (για εσωτερική ενημερωτική χρήση) και γ) διατάξεις εφαρμογής του κανονισμού υπηρεσιακής κατάστασης.

Τέλος, όσον αφορά την εσωτερική χρηματοοικονομική και δημοσιονομική διαχείριση, ο ΕΕΠΔ μεταβίβασε τα σχετικά καθήκοντα στον προϊστάμενο του τμήματος «Διοίκηση/Προσωπικό/Προϋπολογισμός», ο οποίος ενεργεί ως κύριος διατάκτης.

2.3. Οι λόγοι καθιέρωσης του θεσμού

Ο πρωταρχικός λόγος είναι η ιδιότητα της προστασίας των προσωπικών δεδομένων ως θεμελιώδους δικαιώματος. Όλα τα άτομα δικαιούνται αποτελεσματικής προστασίας των δικαιωμάτων τους είτε αναφερόμαστε στον δημόσιο, είτε στον ιδιωτικό τομέα. Ο ΕΕΠΔ έχει αναλάβει την αποστολή να διαφυλάττει τα προσωπικά δεδομένα και να αποκαθιστά κάθε παραβίασή τους από τα κοινοτικά όργανα και οργανισμούς.

Δεύτερος βασικός λόγος καθιέρωσης του θεσμού είναι η ανάγκη για εναρμόνιση των κανόνων/νομοθετικών διατάξεων που εφαρμόζονται από τις εθνικές ανεξάρτητες αρχές του κάθε κράτους μέλους και αφορούν την προστασία των προσωπικών δεδομένων. Για να επιτευχθεί αυτή η εναρμόνιση μεταξύ όλων των εθνικών συστημάτων προστασίας των δεδομένων, χρειάζεται η εποπτεία ενός ανεξαρτήτου οργάνου που θα λειτουργεί σε κοινοτικό επίπεδο.

Τρίτος λόγος είναι ότι το θεμελιώδες αυτό δικαίωμα δεν μπορεί να «αυτοπροστατευθεί». Επειδή η επεξεργασία και η χρήση των προσωπικών δεδομένων είναι στις μέρες μας πολύ συχνή, τόσο από ιδιωτικούς όσο και από δημόσιους φορείς, η ανάγκη για ένα όργανο ειδικά επιφορτισμένο με καθορισμό των κανόνων και των εγγυήσεων που πρέπει να τηρούνται πριν από κάθε

επεξεργασία προσωπικών δεδομένων, είναι σημαντική. Τον ρόλο αυτό αναλαμβάνει να διαδραματίσει ο ΕΕΠΔ.

Τέταρτος λόγος είναι ο σεβασμός των αρχών καλής διακυβέρνησης, απαιτεί ικανοποιητική προστασία των προσωπικών δεδομένων. Το δικαίωμα της «καλής διακυβέρνησης» ή αλλιώς της «χρηστής διοίκησης» (“good” or “sound administration”) έχει αναγνωριστεί ως βασική αρχή του Κοινοτικού δικαίου και γι’ αυτό τον λόγο έχει περιληφθεί στο άρθρο 41 του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ε.Ε. Στο ίδιο άρθρο γίνεται ειδική αναφορά στην προστασία των προσωπικών δεδομένων και συγκεκριμένα για το δικαίωμα του ατόμου να έχει πρόσβαση στο φάκελό του.

2.4. Οι αρμοδιότητες του ΕΕΠΔ

Ο Ευρωπαίος Επόπτης είναι επιφορτισμένος με την διασφάλιση της αποτελεσματικής εφαρμογής των κοινοτικών διατάξεων που έχουν τεθεί χάριν της προστασίας προσωπικών δεδομένων, στον τομέα των επεξεργασιών στις οποίες προβαίνουν οι οργανικές μονάδες της Ε.Ε. Αποστολή του είναι η προστασία της ακώλυτης ενάσκησης όλων των δικαιωμάτων των πολιτών της Ε.Ε., όσον αφορά την «πληροφοριακή» πτυχή τους, στο μέτρο που αυτή αποτελείται από όργανα και οργανισμούς της Κοινότητας. Επομένως, η αρμοδιότητα του ΕΕΠΔ επεκτείνεται στο σύνολο του «δημόσιου τομέα» της Ε.Ε (με εξαίρεση το ΔΕΚ όταν αυτό ασκεί δικαιοδοτικά καθήκοντα³⁸) και όχι στο δημόσιο και ιδιωτικό τομέα των κρατών –μελών, για τον οποίο αρμόδιες είναι οι εθνικές αρχές ελέγχου.

Εκτός των αρμοδιοτήτων του παραμένουν οι επεξεργασίες προσωπικών δεδομένων που διενεργούνται στα πλαίσια διεθνών συμφωνιών, όπως είναι π.χ. η σύμβαση Ευροpol. Αντιθέτως, για τη Eurodac ο ΕΕΠΔ επέχει θέση κοινής εποπτικής αρχής³⁹.

³⁸ Κανονισμός 45/2001/ΕΚ, Κεφάλαιο V, ΕΕΠΔ, άρθρο 46 γ’. Ο ΕΕΠΔ έχει δηλαδή αρμοδιότητα για τα προσωπικά δεδομένα π.χ. των υπαλλήλων του ΔΕΚ, καθώς αυτά ανάγονται στις διοικητικές εξουσίες του οργάνου.

³⁹ Βασίλης Σωτηρόπουλος, «Ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων», ό.π., σελ. 1181-1182.

Η «παιδαγωγική» και γενικότερα πολιτική αποστολή με την οποία είναι επιφορτισμένος ο ΕΕΠΔ εκπληρώνονται μέσα από τις αρμοδιότητές του που ταξινομούνται σε τρεις γενικές κατηγορίες: εποπτεία, διαβούλευση, συνεργασία. Με βάση τις τρεις αυτές κατηγορίες θα κριθεί και η αποτελεσματικότητα του θεσμού.

2.4.1 Εποπτεία (Supervision)

Η εποπτεία ασκείται από τον ΕΕΠΔ αποκλειστικά προς τα όργανα και τους οργανισμούς της Κοινότητας. Η εποπτεία, αντίθετα, των οργάνων των κρατών μελών και των ιδιωτικών φορέων ανήκει στην εθνική και υπο-εθνική αρχή προστασίας δεδομένων, βάσει της Οδηγίας 95/46. Ο τομέας της εποπτείας αποτελεί τον κορμό των ελεγκτικών, αποφασιστικών και διαδικαστικών αρμοδιοτήτων της αρχής. Στα πλαίσια αυτής της αρμοδιότητάς του, ο ΕΕΠΔ δέχεται και εξετάζει ενστάσεις πολιτών σε σχέση με ζητήματα προστασίας προσωπικών δεδομένων, διενεργεί προκαταρκτικούς ελέγχους και έρευνες αυτεπαγγέλτως ή κατόπιν αιτήσεως, ενημερώνει τα υποκείμενα για τα δικαιώματά τους, ακούει και εξετάζει παράπονά τους και παρακολουθεί τις τεχνολογικές εξελίξεις που μπορεί να έχουν αντίκτυπο στην προστασία των προσωπικών δεδομένων. Τέλος, λαμβάνει όλα τα κατάλληλα μέτρα που είναι απαραίτητα για την αποφυγή προσβολής των προσωπικών δεδομένων⁴⁰. Προς το σκοπό αυτό, ο ΕΕΠΔ είναι εξοπλισμένος με ευχέρεια πρόσβασης σε όλα τα προσωπικά δεδομένα και τις πληροφορίες που είναι αναγκαίες για τις έρευνές του, καθώς και σε όλους τους χώρους στους οποίους ασκούνται οι δραστηριότητες των υπευθύνων επεξεργασίας. Ο ΕΕΠΔ έχει αρμοδιότητα να εντέλλεται τον υπεύθυνο επεξεργασίας να επιληφθεί σε περίπτωση προβαλλόμενης παραβίασης των διατάξεων που διέπουν την επεξεργασία προσωπικών δεδομένων και να εντέλλεται την ικανοποίηση των αιτημάτων για την άσκηση δικαιωμάτων των υποκειμένων. Για την επιβολή των εντολών αυτών, ο ΕΕΠΔ είναι εξοπλισμένος με περιορισμένες κυρωτικές αρμοδιότητες, όπως η προειδοποίηση ή επίπληξη, η εντολή διόρθωσης, κλειδώματος,

⁴⁰ Hielke Hijmans, “The European Data Protection Supervisor:”, *ό.π.*, σελ. 1316.

διαγραφής ή καταστροφής δεδομένων που έτυχαν παράνομης επεξεργασίας και η επιβολή προσωρινής ή οριστικής απαγόρευσης της επεξεργασίας⁴¹. Σε περίπτωση που δεν γίνουν σεβαστές οι διαταγές του, έχει την δυνατότητα να προσφεύγει στο οικείο όργανο ή οργανισμό και αν είναι αναγκαίο, στο Ευρωπαϊκό Κοινοβούλιο, στο Συμβούλιο, στην Επιτροπή ή στο ΔΕΚ. Ενώπιον του τελευταίου έχει και δικαίωμα άσκησης παρέμβασης (αρ. 47 Κανονισμού 45/2001/ΕΚ). Ο ΕΕΠΔ έχει επίσης, ειδική εποπτική λειτουργία επί της Κεντρικής Μονάδας της Eurodac (αρ. 20 του Κανονισμού της Eurodac).

Σχετικά με την επίβλεψη και τον έλεγχο της συμμόρφωσης των οργάνων και οργανισμών της Κοινότητας με τους κανόνες προστασίας των προσωπικών δεδομένων, υπάρχουν, εκτός από τον ΕΕΠΔ που ενεργεί ως ανεξάρτητη εξωτερική προς τα κοινοτικά όργανα και τους οργανισμούς αρχή, και άλλα όργανα επιφορτισμένα με το ίδιο έργο, όπως π.χ. κάποιες οργανωμένες οντότητες εντός των οργάνων και οργανισμών που αποκαλούνται «ελεγκτές», οι Υπεύθυνοι Προστασίας Δεδομένων (Data Protection Officers-DPOs) οι οποίοι βρίσκονται εντός των οργάνων ή οργανισμών της Κοινότητας και παρόλο που είναι διορισμένα (εσωτερικά) πρόσωπα, απολαύουν ανεξαρτησίας και δεν λαμβάνουν εντολές από κανέναν κατά την εκτέλεση των καθηκόντων τους (άρθρο 24 §7)⁴², και τέλος το Ευρωπαϊκό Δικαστήριο που προσφέρει νομική προστασία⁴³.

2.4.1.1. Ο τρόπος λειτουργίας της εποπτείας

Η εποπτεία από τον ΕΕΠΔ, από πολλές απόψεις, είναι παρόμοια με τον τρόπο που ο Ευρωπαίος Διαμεσολαβητής ενεργεί σε περιπτώσεις κακοδιοίκησης. Ο ΕΕΠΔ συνεργάζεται με τα όργανα και τους οργανισμούς της

⁴¹ Οι κυρωτικές αρμοδιότητες που δεν έχει ο ΕΕΠΔ και έχουν οι περισσότερες εθνικές αρχές προστασίας δεδομένων είναι εκείνη της (οριστικής ή προσωρινής) ανάκλησης αδείας και της επιβολής χρηματικού προστίμου. Κατά τον Β. Σωτηρόπουλο, η αρμοδιότητα επιβολής προστίμου προς ένα όργανο της Κοινότητας, το οποίο θα υποχρεούτο να καταβάλει σ' ένα άλλο όργανο της Κοινότητας (ΕΕΠΔ) θα ήταν μάλλον υποκριτική και αναποτελεσματική για το σκοπό της συμμόρφωσης του οργάνου προς την κείμενη νομοθεσία της προστασίας προσωπικών δεδομένων. Όσο για τους υπαλλήλους που θα προβούν σε παραβάσεις του Κανονισμού 45/2001, υπάρχει πειθαρχική ποινή (αρ. 49) σύμφωνα με τον κανονισμό υπηρεσιακής κατάστασης των υπαλλήλων των Ε.Κ.

(βλ. Β. Σωτηρόπουλος, «Ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων», *υποσημ.*, σελ. 1182-1183.

⁴² Για τη λειτουργία των DPOs και τη σχέση τους με τον ΕΕΠΔ θα γίνει λόγος αναλυτικότερα παρακάτω.

⁴³ Hielke Hijmans, "The European Data Protection Supervisor: ...", *ό.π.*, σελ. 1317.

Κοινότητας προκειμένου να βελτιώσει την ποιότητα της επεξεργασίας των προσωπικών δεδομένων. Προς αυτήν την κατεύθυνση, η εποπτεία μπορεί να πραγματοποιηθεί με τρεις τρόπους:

α) Κατόπιν πρωτοβουλίας των κοινοτικών οργάνων και οργανισμών: προληπτικός έλεγχος (prior checking) των επεξεργασιών (αρ. 27 §1-5).

Κάθε νέα διενέργεια επεξεργασίας από τα κοινοτικά όργανα ή οργανισμούς, πρέπει να γνωστοποιηθεί στον υπεύθυνο προστασίας δεδομένων, προτού ξεκινήσει (αρ. 25). Ο υπεύθυνος της προστασίας δεδομένων πρέπει πρώτα να ερευνήσει το εγχείρημα. Αυτό σημαίνει ότι αν η επικείμενη επεξεργασία παρουσιάζει ιδιαίτερους κινδύνους για τα δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων, λόγω της φύσης και της εμβέλειας των σκοπών της, είναι υποχρεωμένος να κοινοποιήσει αυτό στον ΕΕΠΔ (άρ. 27 §1). Μία τέτοια περίπτωση, παραδείγματος χάρη, μπορεί ν' αφορά τη διερεύνηση υπονοιών ανάρμοστης χρήσης του διαδικτύου και του ηλεκτρονικού ταχυδρομείου⁴⁴. Επίσης, η χρήση μοναδικού ταυτοποιητή (του προσωπικού αναγνωριστικού αριθμού) δικαιολογεί τον προληπτικό έλεγχο μιας επεξεργασίας που δεν εντάσσεται στον ενδεικτικό κατάλογο⁴⁵.

Ο ΕΕΠΔ έχει εκπονήσει ειδικό έντυπο κοινοποίησης των επεξεργασιών που χρήζουν προληπτικού ελέγχου, ώστε να επιτευχθεί η ομοιόμορφη άσκηση της σχετικής αρμοδιότητας των υπευθύνων των προσωπικών δεδομένων και για να κερδηθεί ο χρόνος που απαιτείται για τη συμπλήρωση των κοινοποιήσεων με επιπρόσθετες πληροφορίες⁴⁶.

Αφού λοιπόν, ο ΕΕΠΔ κάνει τον προληπτικό έλεγχο, διατυπώνει γνώμη, μέσα σε διάστημα δύο μηνών από τη λήψη της κοινοποίησης. Η προθεσμία αυτή μπορεί ν' ανασταλεί αν ο ΕΕΠΔ χρειάζεται συμπληρωματικές πληροφορίες ή να παραταθεί για δύο μήνες επιπλέον, εάν το απαιτεί η πολυπλοκότητα της υπόθεσης. Αν μετά το πέρας των ανωτέρω προθεσμιών δεν υπάρξει

⁴⁴ Ετήσια Έκθεση ΕΕΠΔ 2004, σελ. 23, υπόθεση 2004-0013, για την οποία ο ΕΕΠΔ εξέδωσε γνώμη με την οποία έκανε δεκτή την επεξεργασία υπό ορισμένες προϋποθέσεις.

⁴⁵ Υπόθεση 2004-0196, ό.π.

⁴⁶ Βασίλης Σωτηρόπουλος, «Ο Ευρωπαϊός Επόπτης Προστασίας Δεδομένων», ό.π., σελ. 1192.

γνωμοδότηση, τότε αυτή τεκμαίρεται θετική⁴⁷. Αν ο ΕΕΠΔ γνωμοδοτήσει ότι η επεξεργασία ενδέχεται να παραβιάζει κάποιες διατάξεις του εν λόγω Κανονισμού, τότε υποβάλλει ο ίδιος προτάσεις για ν' αποφευχθεί μια τέτοια παράβαση (αρ.27 §4). Οι γνώμες του ΕΕΠΔ έχουν την εξής δομή: α. την περιγραφή της διαδικασίας, β. την περίληψη των γεγονότων, γ. τη νομική ανάλυση και δ. τα συμπεράσματα⁴⁸.

Σύμφωνα με την Ετήσια Έκθεση 2005 του ΕΕΠΔ, τα περισσότερα θέματα που εισήχθησαν για προληπτικό έλεγχο στον ΕΕΠΔ, αφορούσαν ιατρικά δεδομένα και άλλους είδους δεδομένων υγείας, δεδομένα σχετικά με την αξιολόγηση του προσωπικού των κοινοτικών οργάνων και οργανισμών, καθώς και προσωπικά δεδομένα σχετιζόμενα με διοικητικές έρευνες και πειθαρχικές διαδικασίες.

Σύμφωνα με την τελευταία δημοσιευμένη Ετήσια Έκθεση του 2007, εισήχθησαν το έτος αυτό για προληπτικό έλεγχο 101 υποθέσεις και εκδόθηκαν από τον ΕΕΠΔ 90 γνωμοδοτήσεις. Οι αριθμοί αυτοί παρουσιάζουν μια αύξηση 77,19% των προκαταρκτικών ελέγχων σε σχέση με το έτος 2006. Αυτό ενδεχομένως να οφείλεται στη συνεχή ενθάρρυνση των υπευθύνων προστασίας δεδομένων (DPOs) από τον ΕΕΠΔ για συχνότερη ενημέρωσή του σε θέματα επεξεργασίας προσωπικών δεδομένων που περικλείουν κινδύνους⁴⁹. Τα θέματα τα οποία απασχόλησαν περισσότερο τον ΕΕΠΔ κατά το έτος 2007 αφορούσαν υποθέσεις ιατρικών φακέλων (medical files), εκτιμήσεις προσωπικού (staff evaluation), ενστάσεις (offences), πειθαρχικές διαδικασίες (disciplinary procedures), κοινωνικές υπηρεσίες (social services) και ηλεκτρονική παρακολούθηση (e-monitoring)⁵⁰.

Ο Κανονισμός 45/2001, δεν απαιτεί ρητά από τα όργανα και τους οργανισμούς της Κοινότητας να αναβάλλουν την διαδικασία της επεξεργασίας κάποιων δεδομένων μέχρι ο ΕΕΠΔ να γνωμοδοτήσει. Η χρήση της λέξης «γνώμη» αντί για τη λέξη «εξουσιοδότηση» μπορεί να θεωρηθεί βάσιμο επιχείρημα για την απουσία τέτοιας υποχρέωσης από την πλευρά του οργάνου

⁴⁷ Σύμφωνα με την Ετήσια Έκθεση ΕΕΠΔ 2007, σελ. 14, μέχρι σήμερα δεν έχει υπάρξει τέτοια σιωπηρά θετικά τεκμαιρόμενη γνώμη εκ μέρους του ΕΕΠΔ.

⁴⁸ Ετήσια Έκθεση ΕΕΠΔ 2007, σελ. 15.

⁴⁹ Ο.π., σελ. 16.

⁵⁰ Ο.π., σελ. 16-18.

ή του οργανισμού. Παρά ταύτα, οι αυστηρές προθεσμίες που τάσσονται στον ΕΕΠΔ για να γνωμοδοτήσει, συντείνουν στο συμπέρασμα ότι τα όργανα αυτά είναι υποχρεωμένα να περιμένουν τη γνώμη του ΕΕΠΔ πριν προχωρήσουν σε οποιαδήποτε επεξεργασία δεδομένων προσωπικού χαρακτήρα⁵¹.

Ο προληπτικός αυτός έλεγχος αποδεικνύει τη συνεργασία που πρέπει να υπάρχει ανάμεσα σε δύο διοικητικά σώματα. Το ένα (ο ΕΕΠΔ) μπορεί να κάνει προτάσεις σχετικά με μια επιχειρούμενη επεξεργασία δεδομένων, και το άλλο (όργανο ή οργανισμός) να ζητά τη γνώμη του και να προχωρά σύμφωνα με τις υποδείξεις του πρώτου και να τροποποιεί ή ενδεχομένως να απέχει τελείως από οποιαδήποτε διαδικασία επεξεργασίας. Στην περίπτωση όμως που το όργανο ή οργανισμός δεν μεταβάλλει τον τρόπο της επεξεργασίας των δεδομένων σύμφωνα με τις οδηγίες του ΕΕΠΔ, τότε ο τελευταίος μπορεί να ασκήσει τις εξουσίες που του απονέμονται από το άρθρο 47 §1 του Κανονισμού όπως π.χ. να του παρέχει συμβουλές, να δίνει εντολές συμμόρφωσης και προειδοποιήσεις, να επιβάλλει επιπλήξεις, απαγορεύσεις και να προσφεύγει αφενός στο οικείο όργανο ή οργανισμό και αφετέρου στο Ευρωπαϊκό Κοινοβούλιο, στο Συμβούλιο, στην Επιτροπή και στο Δικαστήριο των Ευρωπαϊκών Κοινοτήτων όταν παρίσταται μεγάλη ανάγκη.

β) Με πρωτοβουλία των υποκειμένων των δεδομένων: ενστάσεις (complaints).

Κάθε φυσικό πρόσωπο, ανεξαρτήτου εθνικότητας και τόπου διαμονής, μπορεί να προσφεύγει στον ΕΕΠΔ σχετικά με οποιαδήποτε παραβίαση του Κανονισμού 45/2001 από κάποιο κοινοτικό όργανο ή οργανισμό. Σύμφωνα με το αρ. 32 §2 του Κανονισμού, κάθε υποκείμενο δεδομένων μπορεί να καταθέτει ένσταση στον ΕΕΠΔ εφόσον θεωρεί ότι τα δικαιώματα που του παρέχει το άρθρο 286 της συνθήκης παραβιάσθηκαν εξαιτίας της επεξεργασίας δεδομένων προσωπικού χαρακτήρα που το αφορούν, εκ μέρους ενός οργάνου ή οργανισμού της Κοινότητας⁵². Οι αποφάσεις του ΕΕΠΔ επί των ενστάσεων

⁵¹ Hielke Hijmans, *ό.π.*, σελ. 1318.

⁵² Το έτος 2004 κατατέθηκαν μόνο οκτώ προσφυγές, συγκριτικά με την τελευταία Ετήσια Έκθεση του 2007 στην οποία αναφέρεται ότι κατατέθηκαν 65 προσφυγές, εκ των οποίων οι 29 έγιναν δεκτές και προχώρησαν σε περαιτέρω έλεγχο από τον ΕΕΠΔ, ενώ οι άλλες 36 κρίθηκαν εκτός του πεδίου δράσης του ΕΕΠΔ (βλ. Ετήσια Έκθεση ΕΕΠΔ 2007, σελ. 28 και 31).

αυτών δύναται να προσβάλλονται ενώπιον του Δικαστηρίου των Ευρωπαϊκών Κοινοτήτων (§3). Εννοείται πως η παραβίαση πρέπει ν' αφορά το υποκείμενο άμεσα και προσωπικά. Αν ο ΕΕΠΔ κρίνει ότι η ένσταση δεν αφορά φυσικό πρόσωπο και παραβίαση προσωπικών δεδομένων από κοινοτικά όργανα και οργανισμούς κατά την επεξεργασία, δεν προχωρά στην εξέταση αυτής και την απορρίπτει (declared inadmissible)⁵³.

Στο αρ. 33 του Κανονισμού αναφέρεται ότι ενστάσεις μπορεί να υποβάλει και κάθε πρόσωπο που απασχολείται από όργανο ή οργανισμό της Κοινότητας (members of staff), επικαλούμενο παράβαση των διατάξεων του παρόντος Κανονισμού που διέπει την επεξεργασία δεδομένων προσωπικού χαρακτήρα, χωρίς ν' ακολουθηθεί η επίσημη οδός.

Αναφορικά με τη διαδικασία κατάθεσης ένστασης θα λέγαμε ότι είναι πιο ευέλικτη σε σχέση με τον προληπτικό έλεγχο. Η εν λόγω διάταξη δεν περιέχει κάποιο χρονικό περιορισμό για την υποβολή εντάσεων από το υποκείμενο των δεδομένων. Ενστάσεις μπορούν να κατατεθούν οποτεδήποτε. Από την άλλη πλευρά το χρονικό περιθώριο που έχει ο ΕΕΠΔ για ν' απαντήσει είναι αρκετά μεγάλο. Ενώ δηλαδή ο ΕΕΠΔ στον προληπτικό έλεγχο πρέπει να ενεργήσει εντός δύο μηνών, στην προκειμένη περίπτωση έχει περιθώριο έξι μηνών για ν' αποφασίσει επί της ένστασης.

Αφού, λοιπόν, ο ΕΕΠΔ εξετάσει την υπόθεση και κρίνει ότι πρόκειται για παραβίαση των διατάξεων περί προστασίας δεδομένων, έρχεται σε επαφή με το όργανο ή τον οργανισμό που έχει κάνει την παραβίαση και προτείνει τρόπους ίασης της παραβίασης, προειδοποιεί τους αρμόδιους της επεξεργασίας, τους συμβουλεύει σχετικά με τον προσήκοντα τρόπο επεξεργασίας των προσωπικών δεδομένων, ζητά διορθώσεις, απαγορεύει επεξεργασίες, κάνει αναφορά του ζητήματος στο Κοινοβούλιο, την Επιτροπή, το Συμβούλιο ή το Δικαστήριο των Ευρωπαϊκών Κοινοτήτων⁵⁴.

Εκτός από την ένσταση που υποβάλλεται ενώπιον του ΕΕΠΔ για παραβιάσεις των διατάξεων του Κανονισμού, το υποκείμενο μπορεί να δράσει και με τους εξής παρακάτω τρόπους:

⁵³ Ετήσια Έκθεση ΕΕΠΔ 2007, σελ. 28

⁵⁴ Ετήσια Έκθεση, ό.π.

αα. Το υποκείμενο των δεδομένων μπορεί να ζητήσει από το Πρωτοδικείο των Ευρωπαϊκών Κοινοτήτων (ΠΕΚ), να ακυρώσει την απόφαση του υπό κρίση οργάνου, δεδομένου ότι αυτή η απόφαση έχει ήδη ληφθεί. Η προσφυγή προς το ΠΕΚ πρέπει να υποβληθεί εντός δύο μηνών αφότου λήφθηκε η απόφαση (αρ. 230 (4) και (5) ΕΚ).

ββ. Το υποκείμενο μπορεί να υποβάλει παράπονα στον Ευρωπαϊό Διαμεσολαβητή που να αφορούν αγωγή κακοδιοίκησης εντός δύο ετών από την κατάθεσή της (αρ. 2 (2) του νόμου για τον Ευρωπαϊό Διαμεσολαβητή).

γγ. Το υποκείμενο μπορεί να υποβάλει ένσταση ενώπιον του ΕΕΠΔ σχετικά με μια αμφισβητούμενη επεξεργασία των προσωπικών του δεδομένων (όχι αποκλειστικά εναντίον μιας απόφασης) που διεξήχθη ή πρόκειται να διεξαχθεί από κάποιο όργανο ή οργανισμό της Κοινότητας (αρ. 32 (2) του Κανονισμού).

δδ. Το υποκείμενο μπορεί επίσης, να προσεγγίσει τον Υπεύθυνο των προσωπικών δεδομένων (DPO), πριν προχωρήσει σε οποιαδήποτε από τις τρεις προαναφερθείσες ενέργειες.

εε. Επίσης, το υποκείμενο το δεδομένων μπορεί πρώτα να προσεγγίσει το κοινοτικό όργανο ή οργανισμό, πριν προχωρήσει στις παραπάνω αναφερθείσες ενέργειες.

Για τα μέλη του προσωπικού που απασχολούνται από τα όργανα και τους οργανισμούς των Ευρωπαϊκών Κοινοτήτων, η κατάσταση είναι ακόμη πιο περίπλοκη. Παραδείγματος χάριν, ένα μέλος του προσωπικού μπορεί να υποβάλει παράπονο προς τον ΕΕΠΔ, βάσει του αρ. 90β' του Κανονισμού Προσωπικού, όπως επίσης και βάσει του αρ. 33 του Κανονισμού⁵⁵.

2.4.2. Διαβούλευση (Consultation)

Ο τομέας της διαβούλευσης περιλαμβάνει τις ευρείες συμβουλευτικές αρμοδιότητες της αρχής, τόσο σε επίπεδο παροχής κατευθυντήριων οδηγιών προς τους υπευθύνους επεξεργασίας, όσο και σε επίπεδο παροχής γνωμοδοτήσεων πριν από κάθε κανονιστική ρύθμιση που σχετίζεται με την

⁵⁵ Hielke Hijmans, *ό.π.*, σελ. 1320.

προστασία προσωπικών δεδομένων. Οι συμβουλευτικές αρμοδιότητες του ΕΕΠΔ είναι ευρύτερες από τις εποπτικές, οι οποίες αφορούν μόνο την επεξεργασία των προσωπικών δεδομένων από τα κοινοτικά όργανα και τους οργανισμούς. Η προηγούμενη γνώμη του ΕΕΠΔ είναι ουσιώδης τύπος για τη θεσμοθέτηση από την Κοινότητα μιας ρύθμισης που επηρεάζει την προστασία προσωπικών δεδομένων. Παρατηρείται όμως, ότι ο ΕΕΠΔ δεν έχει άμεση κανονιστική αρμοδιότητα όπως ορισμένες εθνικές αρχές προστασίας δεδομένων.

Οι συμβουλευτικές και γνωμοδοτικές αρμοδιότητες του ΕΕΠΔ ανάγονται στην αποστολή μιας ανεξάρτητης αρχής, ως παράγοντας καλής διακυβέρνησης και καλής νομοθεσίας. Ως προς την πρώτη αποστολή, ο ΕΕΠΔ συμβουλεύει τα όργανα, είτε αυτεπαγγέλτως είτε κατόπιν αιτήματος, σχετικά με ζητήματα προστασίας δεδομένων. Τα όργανα πριν επιβάλλουν ένα διοικητικό μέτρο που έχει αντίκτυπο στην προστασία των προσωπικών δεδομένων, οφείλουν να κοινοποιούν στον ΕΕΠΔ τους όρους με τους οποίους θα επιβληθούν αυτά (αρ. 28 §1). Όσον αφορά το ζήτημα της καλής νομοθεσίας, η Επιτροπή όταν υποβάλλει νομοθετική πρόταση που μπορεί να επηρεάζει την προστασία των προσωπικών δεδομένων, συμβουλεύεται τον ΕΕΠΔ (αρ. 28 §2).

Ειδικότερα:

α. Ο ΕΕΠΔ έχει το καθήκον να συμβουλεύει τα κοινοτικά όργανα και τους οργανισμούς όταν αυτά λαμβάνουν διοικητικά μέτρα που σχετίζονται με την επεξεργασία προσωπικών δεδομένων. Μια τέτοια περίπτωση είναι η θέσπιση εσωτερικών κανόνων (κανονισμών λειτουργίας, κωδίκων δεοντολογίας κλπ.), μία δράση που σχετίζεται με την κανονιστική λειτουργία των οργάνων αυτών. Αυτό βέβαια δεν σημαίνει ότι κάμπτεται η διοικητική αυτοτέλεια των οργάνων, αφού ο ρόλος του ΕΕΠΔ είναι συμβουλευτικός.

Τα θέματα που απασχόλησαν τον ΕΕΠΔ, στον εν λόγω τομέα, αφορούσαν την κατηγοριοποίηση φακέλων και την περίοδο διατήρησής τους, την ασφάλεια του διαδικτύου, τις ελεγκτικές διαδικασίες ενάντια στην απάτη και τη διαφθορά, την ανταλλαγή πληροφοριών, τους κανόνες εφαρμογής της προστασίας των δεδομένων κ.α⁵⁶.

⁵⁶ Ετήσια Έκθεση ΕΕΠΔ 2007, σελ. 36.

β. Η Επιτροπή υποχρεούται να συμβουλευέται τον ΕΕΠΔ κάθε φορά που εγκρίνει μια νομοθετική πρόταση. Αυτό δεν ισχύει μόνο για προτάσεις που αφορούν κυρίως την προστασία των προσωπικών δεδομένων, αλλά και προτάσεις που αναπτύσσουν, συμπληρώνουν ή τροποποιούν το υπάρχον νομικό πλαίσιο προστασίας δεδομένων και για προτάσεις οι οποίες, ενώ έχουν σημαντικό αντίκτυπο στην προστασία δεδομένων, δεν λαμβάνουν υπόψη το παρόν νομοθετικό πλαίσιο.

Επιπλέον, η γνωμοδοτική αρμοδιότητα του ΕΕΠΔ σε θέματα νομοσχεδίων μπορεί να ασκείται αυτεπαγγέλτως και σε οποιοδήποτε στάδιο της νομοθετικής διαδικασίας. Υπάρχει η δυνατότητα να ενεργοποιηθεί ο ΕΕΠΔ χωρίς να του ζητηθεί, για να διευκρινίζει την έκταση της αρμοδιότητάς του και για να υπενθυμίζει τον κεντρικό εποπτικό του ρόλο στο επίπεδο της Ε.Ε.⁵⁷ (ακόμα και σε σχέση με τη νομοθεσία του Τρίτου Πυλώνα⁵⁸). Παραδείγματός χάρη, πριν ολοκληρωθεί η Συνθήκη της Λισσαβόνας, ο ΕΕΠΔ έθεσε υπόψη της πορτογαλικής προεδρίας ορισμένα πιο συγκεκριμένα ζητήματα τα οποία έκρινε ότι έχρηζαν ιδιαίτερης προσοχής για την προστασία των προσωπικών δεδομένων⁵⁹.

Το έτος 2007 ο ΕΕΠΔ γνωμοδότησε σε 12 αποφάσεις που αφορούσαν την προστασία των προσωπικών δεδομένων και ειδικότερα τους τομείς της ελευθερίας, της ασφάλειας και της δικαιοσύνης. Οι 5 από αυτές αφορούσαν υποθέσεις που ενέπιπταν στον Τρίτο Πυλώνα, δηλαδή στον τομέα της αστυνομικής και δικαστικής συνεργασίας για ποινικά θέματα. Οι υπόλοιπες αφορούσαν αποφάσεις της Ευροπλ για θέματα διασυνοριακής συνεργασίας (Συνθήκη του Prüm) και την πρόταση για το Ευρωπαϊκό Αρχείο Ονομάτων Επιβατών (European PNR System)⁶⁰, για τις οποίες θα γίνει λόγος αναλυτικότερα στο επόμενο κεφάλαιο.

⁵⁷ Βασίλης Σωτηρόπουλος, «Ο Ευρωπαϊός Επόπτης Προστασίας Δεδομένων», *ό.π.*, σελ. 1196-1198.

⁵⁸ Υποθέσεις PNR, ανταλλαγής πληροφοριών ποινικού μητρώου κπλ.

⁵⁹ Ετήσια Έκθεση *ό.π.*, σελ. 41.

⁶⁰ Ετήσια Έκθεση *ό.π.*, σελ. 44.

2.4.3. Συνεργασία (Cooperation)

Σύμφωνα με τη σκέψη αρ. 17 του προοιμίου του Κανονισμού 45/2001, ο ΕΕΠΔ, ως κεντρικό όργανο για την προστασία των προσωπικών δεδομένων σε επίπεδο Ευρωπαϊκής Κοινότητας, οφείλει να προωθεί την συνεκτικότητα των κανόνων και των διαδικασιών που εφαρμόζονται στο πεδίο της Ε.Ε. Επειδή όμως ο ΕΕΠΔ δεν είναι το μόνο επιφορτισμένο όργανο για την προστασία των προσωπικών δεδομένων, ο ίδιος Κανονισμός του επιβάλλει το καθήκον να συνεργάζεται με τη λεγόμενη **Ομάδα Εργασίας** του άρθρου 29 της Οδηγίας 95/46/ΕΚ. Η Ομάδα Εργασίας είναι ένα ανεξάρτητο συμβουλευτικό όργανο που αποτελείται από τις εθνικές αρχές προστασίας δεδομένων (ένα άτομο από κάθε κράτος μέλος), τον ΕΕΠΔ⁶¹ και την Επιτροπή. Στόχο έχει την ομοιόμορφη εφαρμογή της Οδηγίας σε όλα τα κράτη μέλη και την παροχή συμβουλών και προτάσεων επί θεμάτων προστασίας των προσωπικών δεδομένων, τόσο προς τα όργανα και τους οργανισμούς της Κοινότητας, όσο και προς την Επιτροπή. Ο ΕΕΠΔ συμμετέχει στις συνεδριάσεις αυτής της Ομάδας και του έχει δοθεί δικαίωμα ψήφου, ενώ στην Επιτροπή δεν έχει δοθεί⁶². Η Ομάδα Εργασίας μετράει πάνω από δέκα χρόνια ύπαρξης στον ευρωπαϊκό χώρο και έχει μέχρι σήμερα παράγει μεγάλο αριθμό γνωμών και αποφάσεων, κυρίως αναφορικά με θέματα διασυννοριακής ροής προσωπικών δεδομένων⁶³. Ειδικότερα, οι γνωμοδοτήσεις του θεωρούνται το ίδιο χρήσιμες με εκείνες του ΕΕΠΔ, διότι εξετάζουν τα σημεία των υποθέσεων από εθνική σκοπιά.

Παράλληλα, το καθήκον του ΕΕΠΔ για συνεργασία επεκτείνεται και στο επίπεδο του Τρίτου Πυλώνα της Ε.Ε. δηλαδή σε θέματα που αφορούν την προστασία δεδομένων προσωπικού χαρακτήρα στον τομέα της δικαστικής συνεργασίας επί ποινικών υποθέσεων και της αστυνομικής και τελωνειακής συνεργασίας. Για τα θέματα αυτά συνεργάζονται με τον ΕΕΠΔ οι κεντρικές εποπτικές αρχές του Τρίτου Πυλώνα, όπως η αρχές Europol, Eurojust, Schengen και το Τελωνειακό Σύστημα Πληροφοριών⁶⁴. Οι αρχές αυτές

⁶¹ Κανονισμός 45/2001, άρθρο 46 § στ' (i) και (ii) και § ζ'. Ο ΕΕΠΔ είναι μέλος από το 2004.

⁶² Hielke Hijmans, *ό.π.*, σελ. 1322.

⁶³ Βλ. www.europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/index_en.htm.

⁶⁴ Σκέψη αρ. 17 του προοιμίου του Κανονισμού 45/2001.

αποτελούνται από εκπροσώπους των εθνικών εποπτικών αρχών. Η ανάγκη αυτή για στενή συνεργασία των εθνικών αρχών με τον ΕΕΠΔ είναι εμφανής τα τελευταία χρόνια κυρίως λόγω της αύξησης των ενεργειών, σε ευρωπαϊκό επίπεδο, για την καταπολέμηση του οργανωμένου εγκλήματος και της τρομοκρατίας⁶⁵.

3. Η ΣΧΕΣΗ ΤΟΥ ΕΕΠΔ ΜΕ ΑΛΛΕΣ ΑΡΧΕΣ

3.1. Οι Υπεύθυνοι Προστασίας Δεδομένων (DPOs)

Η λειτουργία ενός κεντρικού μονοπρόσωπου εποπτικού οργάνου όπως είναι ο ΕΕΠΔ, θα έκανε αμφίβολη την ταχεία και αποτελεσματική προστασία των προσωπικών δεδομένων. Για το λόγο αυτό επιβλήθηκε η εισαγωγή του παράλληλου αποκεντρωμένου ελέγχου. Ο αποκεντρωμένος έλεγχος ασκείται από τους Υπευθύνους Προστασίας Δεδομένων (εφεξής ΥΠΔ), ένας-τουλάχιστον- εκ των οποίων διορίζεται σε κάθε όργανο ή οργανισμό της Κοινότητας (αρ. 24 §1 Κανονισμού) για θητεία 2-5 ετών ανανεώσιμη, η οποία όμως δεν μπορεί να ξεπερνά τα 10 έτη (αρ. 24 §4). Τα μεγαλύτερα όργανα, όπως είναι η Επιτροπή, το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο της Ε.Ε. και το Δικαστήριο των Ευρωπαϊκών Κοινοτήτων, έχουν διορίσει και έναν αναπληρωτή ΥΠΔ⁶⁶.

Η προσωπική και λειτουργική ανεξαρτησία του ΥΠΔ αποτελούν εγγυήσεις για την απρόσκοπτη άσκηση των αρμοδιοτήτων του. Σύμφωνα με το αρ. 24 §7 του Κανονισμού, ο ΥΠΔ δεν είναι δυνατόν να λαμβάνει εντολές κατά την εκτέλεση των καθηκόντων του. Στις αρμοδιότητές του εντάσσεται η φροντίδα για την ενημέρωση του υπευθύνου επεξεργασίας και των υποκειμένων των δεδομένων, η συνεργασία του με τον ΕΕΠΔ, η διασφάλιση της εσωτερικής εφαρμογής του Κανονισμού 45/2001 από το όργανο ή τον οργανισμό στον οποίο είναι διορισμένος και η τήρηση του μητρώου

⁶⁵ Ετήσια Έκθεση ΕΕΠΔ 2007, σελ. 63-64.

⁶⁶ Ετήσια Έκθεση 2007, σελ. 34.

επεξεργασιών που διενεργεί ο υπεύθυνος της επεξεργασίας (αρ. 24 §1 περ. α, β, γ, δ.).

Η σχέση του ΥΠΔ με τον ΕΕΠΔ συνίσταται στην υποχρέωση του πρώτου να κοινοποιεί στον δεύτερο ορισμένα βασικά στοιχεία πριν από τη διενέργεια οποιασδήποτε επεξεργασίας προσωπικών δεδομένων. Ειδικότερα, ο ΥΠΔ κοινοποιεί στον ΕΕΠΔ τις εργασίες επεξεργασίας οι οποίες ενδέχεται να παρουσιάζουν ιδιαίτερους κινδύνους για τα δικαιώματα των υποκειμένων των δεδομένων⁶⁷. Η υποχρέωση κοινοποίησης συνδέεται με την διαπίστωση αναγκαιότητας διενέργειας ενός προληπτικού ελέγχου της επεξεργασίας. Στην περίπτωση αυτή, αφού διενεργηθεί ο προληπτικός έλεγχος, ο ΕΕΠΔ γνωμοδοτεί εντός δύο μηνών από την κοινοποίηση για την ασφάλεια της επιχειρούμενης επεξεργασίας. Παρατηρείται, επίσης, ότι ο ΥΠΔ υπόκειται στην εξουσία του ΕΕΠΔ, παρόλο που αυτό δεν επιβάλλεται από μια επίσημη ιεραρχία. Αυτή η υπεροχή του ΕΕΠΔ έναντι του ΥΠΔ δικαιολογείται από το γεγονός ότι ο εσωτερικός έλεγχος δεν είναι το ίδιο με τον εξωτερικό, διότι ο ΥΠΔ, παρόλο που κατέχει μια ανεξάρτητη θέση, δεν παύει να είναι μέρος ενός οργάνου ή οργανισμού. Σύμφωνα με την Ετήσια Έκθεση 2007⁶⁸, ο ΕΕΠΔ υποχρέωσε τα όργανα και τους οργανισμούς που δεν είχαν διορίσει έναν ΥΠΔ, να προχωρήσουν σ' ένα τέτοιο διορισμό και να αντλήσουν πόρους και προσωπικό για την καταλληλότερη εκπλήρωση των καθηκόντων του. Ακόμα και η απόλυση ενός ΥΠΔ γίνεται κατόπιν συναινέσεως του ΕΕΠΔ⁶⁹.

Ο ρόλος του ΥΠΔ είναι σημαντικός για το επίπεδο προστασίας των προσωπικών δεδομένων στις οργανικές μονάδες της Ε.Ε. Για την ακρίβεια, ο ΥΠΔ διαδραματίζει ένα ρόλο μεσάζοντα μεταξύ των οργάνων ή των οργανισμών της Κοινότητας και του ΕΕΠΔ.

⁶⁷ Ενδεικτικός κατάλογος των «επικίνδυνων» εργασιών περιλαμβάνεται στο άρθρο 27 του Κανονισμού 45/2001.

⁶⁸ Βλ. σελ. 35.

⁶⁹ Hielke Hijmans, *ό.π.*, σελ. 1317.

3.2. Eurodac

Η Eurodac είναι μια μεγάλη βάση δεδομένων με αποτυπώματα αιτούντων ασύλου και παράνομων μεταναστών που βρίσκονται εντός της Ε.Ε. Η βάση αυτή δεδομένων, που ιδρύθηκε με τον Κανονισμό 2725/2000 του Συμβουλίου, βοηθά στην αποτελεσματικότερη εφαρμογή της Συνθήκης του Δουβλίνου⁷⁰ που αφορά ζητήματα αιτήσεων ασύλου. Όπως και για τα συστήματα των Eurosol και Schengen, έτσι και για το Eurodac, προβλέπεται η λειτουργία μιας κοινής εποπτικής αρχής για την προστασία των προσωπικών δεδομένων που υφίστανται επεξεργασία στο πλαίσιο του ρυθμιστικού πεδίου του συστήματος.

Ο ΕΕΠΔ εποπτεύει την Κεντρική Μονάδα της Eurodac και παρακολουθεί τη νομιμότητα της διαβίβασης προσωπικών δεδομένων από την Κεντρική Μονάδα στα κράτη μέλη. Οι κυριότερες παρατηρήσεις του ΕΕΠΔ ως εποπτικού οργάνου αφορούν τα μέτρα ασφάλειας που πρέπει να περιβάλλουν τις επεξεργασίες των προσωπικών δεδομένων στην Κεντρική Μονάδα και τα αρχεία που πρέπει να τηρεί η τελευταία.

3.3. Ο Ευρωπαίος Διαμεσολαβητής (European Ombudsman)

Από το 1995, ο Ευρωπαίος Διαμεσολαβητής (εφεξής ΕΔ) ασκεί την αρμοδιότητα διεξαγωγής ερευνών σχετικά με περιπτώσεις κακοδιοίκησης στις δραστηριότητες των κοινοτικών θεσμικών οργάνων ή οργανισμών, με εξαίρεση το Δικαστήριο και το Πρωτοδικείο κατά την άσκηση της δικαιοδοτικής τους λειτουργίας. Οι έρευνες αυτές μπορεί να διεξάγονται αυτεπάγγελα από τον ίδιο τον ΕΔ ή κατόπιν καταγγελίας φυσικού ή νομικού προσώπου.

Σύμφωνα με το μνημόνιο συνεργασίας που υπεγράφη μεταξύ του ΕΕΠΔ και του ΕΔ το Νοέμβριο του 2006⁷¹, κοινός στόχος και των δύο είναι να επιτύχουν τη βέλτιστη χρήση των κοινοτικών πόρων και να διευκολύνουν μια συνεπή προσέγγιση στις νομικές και διοικητικές πτυχές της προστασίας δεδομένων, προάγοντας έτσι τα δικαιώματα και το συμφέρον των πολιτών και των καταγγελλόντων. Παράλληλα, επειδή οι περιπτώσεις κακοδιοίκησης μπορεί

⁷⁰ Υπεγράφη στο Δουβλίνο στις 15 Ιουνίου 1990.

⁷¹ Βλ. ΕΕ 7.2. 2007 C 27, σελ. 21-23.

να περιέχουν και επεξεργασία προσωπικών δεδομένων, πολλές φορές και τα δύο όργανα κρίνονται αρμόδια να εξετάσουν τις υποθέσεις αυτές. Για να αποφευχθεί όμως η άσκοπη επανάληψη διαδικασιών και κατ' επέκταση διιστάμενες ερμηνείες, το εν λόγω μνημόνιο έρχεται να ορίσει ευέλικτες ρυθμίσεις συνεργασίας. Συνεπώς, το μνημόνιο αυτό παρέχει μια βάση για εποικοδομητική συνεργασία για την επίτευξη του στόχου αυτού και δεν προορίζεται να δημιουργήσει νόμιμα δικαιώματα ή υποχρεώσεις.

Όταν, λοιπόν, οι καταγγελίες μπορούν να εξεταστούν είτε από τον ΕΔ είτε από τον ΕΕΠΔ, οι καταγγέλλοντες μπορούν να επιλέγουν την αρχή στην οποία θα απευθύνουν την καταγγελία τους. Επιπλέον, οι δύο αρχές υποχρεούνται: **1.** να αποφεύγουν, στο μέτρο του δυνατού, τις άσκοπες επαναλήψεις διαδικασιών και τις αποκλίνουσες προσεγγίσεις, **2.** να ανταλλάσσουν πληροφορίες και **3.** να σέβονται τις απαιτήσεις εμπιστευτικότητας που διέπουν τις δραστηριότητές τους.

Με τον τρόπο αυτό, αν μια αρχή εξετάζει ή έχει εξετάσει μια καταγγελία, η άλλη αρχή δεν ξεκινά νέα έρευνα επ' αυτής, εκτός και αν ο καταγγέλλων προσκομίσει νέα σημαντικά στοιχεία για αυτήν και η άλλη αρχή έχει ήδη περατώσει την έρευνά της. Στο μνημόνιο συνεργασίας, τα δύο όργανα δηλώνουν την πρόθεσή τους να ενημερώνει το ένα το άλλο για τα πορίσματα των ερευνών τους. Στις υποθέσεις που αφορούν την προστασία των προσωπικών δεδομένων, όταν ο ΕΔ αποφασίζει για αυτές, λαμβάνει υπόψη του την γνώμη του ΕΕΠΔ. Τέλος, και οι δύο αρχές δηλώνουν την πρόθεσή τους για τακτικές συναντήσεις, τουλάχιστον μια φορά ετησίως προκειμένου να ανταλλάσσουν απόψεις για τη βελτίωση της συνεργασίας τους.

4. Η ΝΟΜΙΚΗ ΦΥΣΗ ΤΟΥ ΕΕΠΔ

4.1. Οι πολλαπλές λειτουργίες του θεσμού.

Ο Ευρωπαϊός Επόπτης έχει πολλές διαφορετικές λειτουργίες όπως μπορούμε να συμπεράνουμε από τα άρθρα 46 και 47 του Κανονισμού 45/2001.

Ας αναφερθούμε, λοιπόν, σε κάποιες από αυτές:

- Είναι σύμβουλος των κοινοτικών οργάνων και οργανισμών.
- Είναι δέκτης ενστάσεων και καταγγελιών.
- Είναι εξειδικευμένος σύμβουλος σε θέματα ελέγχου της λειτουργίας των δικτύων και των νέων τεχνολογιών.
- Διασφαλίζει τη σωστή εφαρμογή του Κανονισμού και των άλλων σχετικών κοινοτικών πράξεων.
- Επιβάλλει μέτρα για την εφαρμογή του νόμου, τα οποία είναι δεσμευτικά για τα κοινοτικά όργανα και οργανισμούς (άρθρο 47, περ. γ'-στ' Κανονισμού).
- Προσφέρει νομική προστασία στον πολίτη (άρθρα 32 και 33 Κανονισμού) όταν επιλύει διαμάχες μεταξύ των υποκειμένων των δεδομένων και των οργάνων ή οργανισμών της Κοινότητας.
- Προτείνει μέτρα συμμόρφωσης όταν τα κοινοτικά όργανα και οργανισμοί δεν συμβαδίζουν με τις αποφάσεις του.
- Έχει κανονιστική λειτουργία, αφού έχει την εξουσία να δίνει κατευθυντήριες οδηγίες και σε συγκεκριμένα θέματα να εισάγει γενικούς κανόνες.
- Σε κάποιες περιπτώσεις, θα λέγαμε ότι ο ΕΕΠΔ έχει και «συνταγματική» λειτουργία, αφού διασφαλίζει τον σεβασμό των θεμελιωδών δικαιωμάτων. Αυτό επιβεβαιώνεται και από το γεγονός ότι μπορεί να παρεμβαίνει όταν τέτοιου είδους υποθέσεις εισάγονται προς επίλυση ενώπιον του Δικαστηρίου των ΕΚ⁷².

Ανακεφαλαιώνοντας, θα λέγαμε πως ο ανωτέρω κατάλογος δείχνει ότι έχει δοθεί στον ΕΕΠΔ μια πληθώρα λειτουργιών. Το σύνολο, όμως, αυτών των

⁷² Βλ. Υποθέσεις C-317/04 και C-318/04.

λειτουργιών δεν βοηθά στο να αντιληφθούμε επακριβώς ποια είναι η νομική φύση του ΕΕΠΔ, αφού παρόμοιες λειτουργίες έχουν και άλλα όργανα και οργανισμοί της Κοινότητας. Για να μπορέσουμε, λοιπόν, να καταλήξουμε σ' ένα συμπέρασμα, πρέπει να πρώτα να ερευνήσουμε τη φύση του με αφαιρετικό τρόπο, δηλαδή να ξεκαθαρίσουμε τι δεν είναι ο ΕΕΠΔ.

4.1.1. Δεν είναι θεσμικό όργανο (institution)

Ο ΕΕΠΔ δεν είναι θεσμικό όργανο, εν στενή εννοία, εφόσον δεν περιλαμβάνεται στον κατάλογο του άρθρου 7, παρ. 1 της ΣυνθΕΚ που απαριθμεί τα κοινοτικά θεσμικά όργανα. Αυτό το στοιχείο έχει σημασία διότι ορισμένες εξουσίες απονέμονται από τη Συνθήκη αποκλειστικά και μόνο σε θεσμικά όργανα. Σημαντικό είναι, επίσης, ότι η ΕΚ λειτουργεί σε μια βάση οργανικής ισορροπίας μεταξύ του Συμβουλίου και του Ευρωπαϊκού Κοινοβουλίου. Αυτή την ισορροπία επιβλέπει το Δικαστήριο των ΕΚ. Ο ΕΕΠΔ, χωρίς να είναι ο ίδιος θεσμικό όργανο, οφείλει να σέβεται την ισορροπία αυτή.

Παρόλα αυτά, για κάποιους πολύ συγκεκριμένους σκοπούς, ο ΕΕΠΔ έχει την ίδια μεταχείριση με τα θεσμικά όργανα. Για θέματα που αφορούν, παραδείγματος χάρη, το προσωπικό του, ο ΕΕΠΔ εξομοιούται με τα θεσμικά όργανα⁷³. Ακόμα και σε θέματα προϋπολογισμού, η Κοινότητα κατατάσσει τον ΕΕΠΔ σε ξεχωριστό τομέα σε σχέση με τους άλλους οργανισμούς⁷⁴.

Συμπερασματικά θα λέγαμε ότι ο ΕΕΠΔ, έχει ορισμένα χαρακτηριστικά ενός θεσμικού οργάνου.

4.1.2. Δεν είναι κοινοτική υπηρεσία (agency)

Τα τελευταία χρόνια, στους κόλπους της ΕΚ, έχει κάνει την εμφάνισή του ένας αρκετά μεγάλος αριθμός κοινοτικών υπηρεσιών/οργανισμών. Το ευρωπαϊκό διαδίκτυο ερμηνεύει τον όρο «κοινοτική υπηρεσία» ως ένα σώμα που διέπεται από το δημόσιο ευρωπαϊκό δίκαιο, διαχωρίζεται από τα κοινοτικά θεσμικά όργανα και έχει τη δική του νομική προσωπικότητα. Ιδρύεται με

⁷³ Κανονισμός 45/2001, αρ. 43 περ.6.

⁷⁴ Hielke Hijmans, *ό.π.*, σελ. 1324-1325.

δευτερογενή νομοθετική πράξη, με σκοπό να εκπληρώσει μια συγκεκριμένη τεχνική, επιστημονική ή διοικητική αποστολή η οποία καθορίζεται από σχετική κοινοτική πράξη. Σήμερα, είκοσι δύο όργανα ανταποκρίνονται στην έννοια του της «κοινοτικής υπηρεσίας»⁷⁵. Όμως, μερικά από αυτά έχουν τη δυνατότητα να παίρνουν αποφάσεις που να δεσμεύουν αυτούς τους οποίους απευθύνονται αυτές. Ένα χαρακτηριστικό παράδειγμα κοινοτικής υπηρεσίας είναι το Γραφείο Εναρμόνισης της Εσωτερικής Αγοράς (OHIM) στην πόλη Αλικάντε το οποίο ιδρύθηκε με τον Κανονισμό 40/94 του Συμβουλίου της ΕΚ.

Ο ΕΕΠΔ δεν εντάσσεται σ' αυτήν την κατηγορία για τρεις λόγους:

1. Παρόλο που έχει συσταθεί με δευτερογενή νομοθετική πράξη, η πρόβλεψη για την ίδρυσή του έχει ως νομική βάση απευθείας τη Συνθήκη της ΕΚ.
2. Ο ΕΕΠΔ δεν έχει ιδρυθεί για να πραγματοποιήσει κάποιον τεχνικό, επιστημονικό ή διοικητικό σκοπό ο οποίος να προέρχεται από ένα θεσμικό όργανο της ΕΚ. Αντιθέτως, ο ΕΕΠΔ έχει συσταθεί για να εποπτεύει τα κοινοτικά θεσμικά όργανα και τις λοιπές κοινοτικές υπηρεσίες και οργανισμούς.
3. Οι κοινοτικές υπηρεσίες δεν έχουν υποχρέωση να επιβλέπουν τα θεσμικά όργανα της Κοινότητας. Άλλωστε, δεν θα μπορούσαν να έχουν μια τέτοια υποχρέωση, διότι με αυτόν τον τρόπο θα αδυνατούσαν τα κοινοτικά θεσμικά όργανα να ασκήσουν τις εξουσίες που τους έχουν δοθεί από τη Συνθήκη.

Από τα παραπάνω συνάγεται ότι ο ΕΕΠΔ δεν έχει τη νομική φύση μιας κοινοτικής υπηρεσίας, απλώς υπάρχει περίπτωση κάποιες λειτουργίες των υπηρεσιών αυτών να είναι παρόμοιες με αυτές του ΕΕΠΔ⁷⁶.

4.1.3. Δεν είναι ρυθμιστική αρχή (regulator)

Το φαινόμενο των ρυθμιστικών αρχών έχει τις ρίζες του στις Ηνωμένες Πολιτείες. Ένα κυβερνητικό όργανο ονομάζεται «ρυθμιστικό» όταν έχει την

⁷⁵ Βλ. www.europa.eu/agencies/index_en.htm.

⁷⁶ Hielke Hijmans, *ό.π.*, σελ. 1325-1326.

εξουσία να ρυθμίζει τον τρόπο με τον οποίο οργανώνονται και ασκούνται τα ιδιωτικά συμφέροντα και δικαιώματα. Στις Ηνωμένες Πολιτείες, στις αρμοδιότητες των «ρυθμιστών» περιλαμβάνεται η εξουσία να παίρνουν δεσμευτικές αποφάσεις σε υποθέσεις ιδιωτών, όπως επίσης και να διαμορφώνουν κανόνες.

Στο κοινοτικό δίκαιο, ο όρος «ρυθμιστική αρχή» χρησιμοποιείται για όργανα των κρατών μελών τα οποία συστήνονται με σκοπό να προωθήσουν τη διεύρυνση και τον ανταγωνισμό σε συγκεκριμένους τομείς της αγοράς όπου υπάρχουν μονοπωλιακές ή ολιγοπωλιακές καταστάσεις, όπως π.χ. στις τηλεπικοινωνίες, τον ηλεκτρισμό, τα καύσιμα κλπ. Αυτά τα όργανα πρέπει να είναι ανεξάρτητα από τους τομείς αυτούς της αγοράς (όχι όμως και αναγκαία ανεξάρτητα από τις εθνικές κυβερνήσεις) και έχουν αρμοδιότητα να θεσπίζουν κανόνες, κυρίως τεχνικής φύσεως.

Με βάση τα προαναφερθέντα, είναι σαφές πως ο ΕΕΠΔ έχει και αρκετές «ρυθμιστικές» αρμοδιότητες. Αυτό αποδεικνύεται από το γεγονός ότι ο ΕΕΠΔ μπορεί να αποφαινεται επί ιδιωτικών υποθέσεων, όπως π.χ. επί ενστάσεως ενός υποκειμένου δεδομένων. Επίσης, μπορεί να επιβάλλει την εφαρμογή των νόμων περί προστασίας προσωπικών δεδομένων (αρ. 47 γ'-στ' του Κανονισμού 45/2001). Κατά τη διαδικασία του προκαταρκτικού ελέγχου μπορεί να γνωμοδοτεί, πράγμα το οποίο μπορεί να έχει νομικές συνέπειες (αρ. 27 του Κανονισμού). Επιπλέον, έχει την δυνατότητα να δίνει κατευθυντήριες οδηγίες προς τα κοινοτικά όργανα και οργανισμούς, καθώς και προς τα υποκείμενα των δεδομένων σχετικά με την σωστή ερμηνεία των διατάξεων που αναφέρονται στην προστασία των προσωπικών δεδομένων. Οι νομικές αυτές πράξεις του ΕΕΠΔ θεωρούνται μη δεσμευτικό δίκαιο (soft law). Μπορεί, επίσης, σε πολύ συγκεκριμένα θέματα, να θεσπίζει κανόνες που έχουν γενική εφαρμογή και έτσι να θεωρείται *οιονεί* νομοθετικό όργανο. Ένα χαρακτηριστικό παράδειγμα είναι το άρθρο 37 § 2 του Κανονισμού, όπου ο ΕΕΠΔ οφείλει να ορίσει έναν κατάλογο με τις επεξεργασίες που έχουν σχέση με την κίνηση δεδομένων. Γενικότερα, θα λέγαμε ότι με βάση το άρθρο 46 η' του Κανονισμού, ο ΕΕΠΔ έχει την εξουσία να καθορίζει, να αιτιολογεί και να δημοσιοποιεί τις εξαιρέσεις, τις εγγυήσεις, τις άδειες και τις προϋποθέσεις σχετικά με τα οριζόμενα στα άρθρα

10 § 2 περ. β', § 4, 5, 6, στο άρθρο 12 § 2, στο άρθρο 19 και 37 § 2 του Κανονισμού 45/2001.

Παρόλα αυτά, η ύπαρξη αυτών των εξουσιών δεν χαρακτηρίζει τον ΕΕΠΔ ως ρυθμιστική αρχή. Οι εξουσίες που προαναφέρθηκαν καλύπτουν ένα μέρος μόνο του συνόλου των αρμοδιοτήτων του και στην πράξη, ο ΕΕΠΔ διασφαλίζει καλύτερα τη σωστή εφαρμογή των διατάξεων περί προστασίας των δεδομένων με το να προσπαθεί να επιτύχει έναν φιλικό διακανονισμό. Τέλος, θα καταλήγαμε πως ο ΕΕΠΔ δεν είναι «ρυθμιστής», αφού οι «ρυθμιστές» συνήθως συστήνονται με σκοπό τον ανεξάρτητο έλεγχο της αγοράς, ενώ αντίθετα ο ΕΕΠΔ έχει ως βασική λειτουργία να εποπτεύει δημόσιες οντότητες⁷⁷.

4.1.4. Δεν είναι διαμεσολαβητής (ombudsman)

Είναι γεγονός ότι ο ΕΕΠΔ έχει κάποια στοιχεία διαμεσολαβητή, ειδικά όταν χειρίζεται ενστάσεις υποκειμένων των δεδομένων. Όπως ήδη αναφέρθηκε (βλ. κεφ. 3.3), βάσει της ΣυνθΕΚ, ο Ευρωπαϊός Διαμεσολαβητής (ΕΔ) έχει την εξουσία να διεξάγει έρευνες που αφορούν περιστατικά κακοδιοίκησης στις δραστηριότητες των κοινοτικών οργάνων ή οργανισμών. Και ο ΕΕΠΔ όμως, έχει την δυνατότητα να διεξάγει έρευνες είτε με δική του πρωτοβουλία, είτε μετά από ένσταση του ενδιαφερόμενου. Οι έρευνες αυτές παρουσιάζουν ομοιότητες με εκείνες του ΕΔ αφού και στις δύο περιπτώσεις το σημείο εκκίνησης είναι η κακοδιοίκηση.

Ένα από τα αντικείμενα του ΕΔ είναι να προσφέρει ένα πολιτικό δικαίωμα στον πολίτη να παρεμβαίνει για την αποκατάσταση της εις βάρος του διοικητικής παράβασης. Αντίθετα, η έννομη προστασία που προσφέρει ο ΕΕΠΔ είναι το δικαίωμα ένστασης του υποκειμένου των δεδομένων ως ενδικοφανούς προσφυγής, γεγονός που επιβεβαιώνεται και από το άρθρο 32 του Κανονισμού 45/2001 όπου εντάσσεται στο κεφάλαιο III με τον τίτλο «Ένδικα Μέσα».

Επιπλέον, ο ΕΕΠΔ προσφέρει ένα μέσο έννομης προστασίας στον πολίτη (βάσει του άρθρου 32 του Κανονισμού) του οποίου η φύση είναι

⁷⁷ Hielke Hijmans, *ό.π.*, σελ. 1327-1328.

διαφορετική από αυτό που προσφέρει ο ΕΔ. Στην ουσία δηλαδή, δεν πρόκειται για μια εναλλακτική μορφή έννομης προστασίας, αλλά είναι μέρος της έννομης προστασίας, περιλαμβάνοντας και τη δυνατότητα να τεθεί η υπόθεση ενώπιον του Δικαστηρίου των ΕΚ. Και τα δύο όργανα όμως, κάνουν προσπάθεια για να επιτευχθεί εξωδικαστική επίλυση των διαφορών που προκύπτουν μεταξύ των καταγγελλόντων και των κοινοτικών θεσμικών οργάνων.

Επιπροσθέτως, ο ΕΕΠΔ και ο ΕΔ προσπαθούν και οι δύο να βελτιώσουν την ποιότητα της διοίκησης εν γένει. Οι λειτουργίες όμως, του ΕΕΠΔ είναι πιο εκτενείς και έχουν διαφορετική φύση από αυτές του ΕΔ. Επίσης, η θέση του ΕΔ είναι άμεσα συνδεδεμένη με το Ευρωπαϊκό Κοινοβούλιο, αφού και η ίδια η ΣυνθΕΚ αναφέρεται σε αυτόν στο κεφάλαιο για το Ευρωπαϊκό Κοινοβούλιο. Αντιθέτως, ο ΕΕΠΔ εκπληρώνει τις λειτουργίες του έναντι όλων των θεσμικών οργάνων της Κοινότητας ισάξια. Αυτό άλλωστε προκύπτει από το αρ. 286 ΕΚ και από το αρ. 41 του Κανονισμού⁷⁸.

Συνοψίζοντας, θα λέγαμε πως σε καμία περίπτωση δεν θα πρέπει να χαρακτηρίσουμε τον ΕΕΠΔ ως έναν Ευρωπαϊό Διαμεσολαβητή εξειδικευμένο σε θέματα προστασίας προσωπικών δεδομένων, αλλά ως ένα διαφορετικής φύσης όργανο που απλώς χειρίζεται θέματα που εμπίπτουν και στις αρμοδιότητες του ΕΔ.

4.1.5. Δεν είναι δικαστική αρχή (judicial authority)

Με μια πρώτη ματιά, φαίνεται ξεκάθαρα πως ο ΕΕΠΔ δεν είναι δικαστική αρχή. Όμως, δεν πρέπει να παραβλέπουμε το γεγονός ότι ο ΕΕΠΔ μπορεί να παρεμβαίνει σε δικαστικές υποθέσεις ή να εισάγει υποθέσεις προς επίλυση, ενώπιον του ΔΕΚ, με δική του πρωτοβουλία. Αυτή τη λειτουργία εκ φύσεως δεν την έχει ένα κοινό δικαστήριο, αφού μόνη του υποχρέωση είναι να αποφασίζει επί αγωγών που υποβάλλονται σ' αυτό από άλλους (υπό μία έννοια, ο επόπτης έχει και στοιχεία εισαγγελικής αρχής που παρεμβαίνει σε δικαστικές υποθέσεις υπέρ του νόμου). Ο ΕΕΠΔ δεν χρειάζεται να είναι απαραίτητα δικηγόρος ή δικαστής. Το άρθρο 42 του Κανονισμού απαιτεί απλώς εμπειρία και ικανότητες

⁷⁸ Hielke Hijmans, *ό.π.*, σελ. 1329-1330.

για την εκπλήρωση των καθηκόντων του. Η ερμηνεία και εφαρμογή του κοινοτικού δικαίου αποτελούν αποκλειστική αρμοδιότητα του ΔΕΚ και των εθνικών δικαστηρίων. Μέσα από την ερμηνεία του Κανονισμού 45/2001 δεν διαφαίνεται η πρόθεση να δοθεί στον ΕΕΠΔ μέρος από αυτή την αποκλειστικότητα του ΔΕΚ.

Παρόλα αυτά, δεν θα πρέπει να παραβλέψουμε ότι ορισμένα χαρακτηριστικά του ΕΕΠΔ προσιδιάζουν σε αυτά ενός δικαστηρίου, σύμφωνα, τουλάχιστον, με τον ορισμό ενός (εθνικού) δικαστηρίου που έχει υιοθετήσει το ΔΕΚ στο πλαίσιο της προδικαστικής παραπομπής του άρθρου 234 ΕΚ. Στην απόφαση C-54/96, *Dorsch Consult*⁷⁹, ορίζονται τα χαρακτηριστικά που πρέπει να πληροί μια αρχή για να χαρακτηρίζεται ως δικαστική. Αυτά είναι τα εξής:

1. Να έχει συσταθεί με νόμο
2. Να έχει μονιμότητα
3. Η διαδικασία να διεξάγεται μεταξύ των μερών (*inter partes*)
4. Να είναι ανεξάρτητο
5. Να εφαρμόζει νομικούς κανόνες
6. Να έχει αναγκαστική δικαιοδοσία

Από τα χαρακτηριστικά αυτά, ο ΕΕΠΔ πληροί όλες τις προϋποθέσεις για τον χαρακτηρισμό του ως δικαστική αρχή, εκτός από την τελευταία, διότι σύμφωνα με το αρ. 32 του Κανονισμού 45/2001, το υποκείμενο των δεδομένων δεν είναι υποχρεωμένο να προσφύγει ενώπιον του ΕΕΠΔ, αλλά μπορεί να κινήσει τη διαδικασία απευθείας ενώπιον του Δικαστηρίου κατά οποιασδήποτε απόφασης οργάνου ή οργανισμού της Κοινότητας. Επιπλέον, ούτε και ως διαιτητική αρχή θα μπορούσε να χαρακτηριστεί ο ΕΕΠΔ⁸⁰.

Κατά συνέπεια, και με βάση τις διατάξεις του Κανονισμού, δεν αποδεικνύεται ότι η πρόθεσή του ήταν να συστήσει μια δικαστική αρχή, αφού οι βασικές του λειτουργίες δεν εξαντλούνται μόνο στην προσφορά νομικής προστασίας προς τα υποκείμενα των δεδομένων, αλλά επικεντρώνονται περισσότερο στην εποπτεία των κοινοτικών οργάνων και οργανισμών.

⁷⁹ Βλ. C- 54/96, 17.09.1997, Συλλογή 1997, I-4961.

⁸⁰ Hielke Hijmans, *ό.π.*, σελ. 1330-1332.

4.1.6. Τα βασικά χαρακτηριστικά του ΕΕΠΔ

Αφού ολοκληρώσαμε τον έλεγχο περί του τι δεν είναι ο ΕΕΠΔ μπορούμε να καταλήξουμε στο συμπέρασμα ότι ο ΕΕΠΔ δεν εμπίπτει σε καμία από τις παραπάνω κατηγορίες, αλλά απλώς τυχαίνει να παρουσιάζει κοινά στοιχεία με άλλες αρχές ή οργανισμούς της ΕΚ, πράγμα που συχνά προκαλεί σύγχυση ως προς την οριοθέτηση των εξουσιών του και τον καθορισμό της νομικής του φύσης. Αν όμως κρίναμε με μια πιο θετική ματιά, θα μπορούσαμε να πούμε ότι ο επόπτης παρουσιάζει τα στοιχεία ενός *suī generis* οργανισμού ή δημόσιας αρχής ο οποίος χαρακτηρίζεται από τη σώρευση διαφορετικών λειτουργιών με πρωτεύον όμως χαρακτηριστικό αυτό της **εποπτείας** και του **ελέγχου**. Ο επόπτης είναι πρωτίστως εποπτική αρχή.

Για να κατανοήσουμε, όμως, επαρκώς τη φύση του, σκόπιμο θα ήταν να συνοψίσουμε τα βασικά χαρακτηριστικά της αρχής αυτής⁸¹.

- ✓ Πρώτον, πρέπει να τονιστεί ότι η αρχή αυτή είναι **μονοπρόσωπη**. Ένα άτομο ορίζεται ως «Επόπτης» (Supervisor) το οποίο αντιπροσωπεύει την προστασία των προσωπικών δεδομένων σε επίπεδο Ε.Ε. Επικουρείται και εκπροσωπείται σε περίπτωση απουσίας του από τον «Αναπληρωτή Επόπτη». Και τα δύο αυτά πρόσωπα εργάζονται μαζί ως μια ομάδα και άρα θα μπορούσε κάποιος να πει ότι στην ουσία έχει και στοιχεία συλλογικού οργάνου.
- ✓ Δεύτερον, η αρχή είναι **ανεξάρτητη**. Αυτό έχει ήδη τονιστεί στο άρθρο 286 της ΣυνθΕΚ, όπως και στο Κεφάλαιο V του Κανονισμού 45/2001. Η σπουδαιότητα αυτού του στοιχείου φαίνεται και από την αναφορά που γίνεται σ' αυτό στα άρθρα 28 και 29 της Οδηγίας 95/46 ως το *κύριο χαρακτηριστικό* της εποπτείας⁸².

⁸¹ Hielke Hijmans, *ό.π.*, σελ. 1334-1335.

⁸² Βλ σχετικά Peter Hustinx, "Perspectives of Independent Authorities: independence and more effectiveness", λόγος που εκφωνήθηκε στις 2 Απριλίου 2007 στο διήμερο νομικό συμπόσιο στο Μέγαρο Μουσικής Αθηνών με θέμα: «Οι ανεξάρτητες αρχές στη σύγχρονη δημοκρατία».

- ✓ Τρίτον, η αρχή είναι **εξειδικευμένη στην παροχή εμπειρογνωμοσύνης** (expert) σε θέματα προστασίας δεδομένων. Το προσόν αυτό κρίνεται ως προαπαιτούμενο για το διορισμό του ΕΕΠΔ⁸³. Όλες οι εξουσίες του ΕΕΠΔ μπορούν να ασκηθούν μόνο εφόσον κριθεί πως αυτός διαθέτει την απαιτούμενη εμπειρία και γνώσεις επί θεμάτων που αφορούν τα προσωπικά δεδομένα.
- ✓ Τέταρτον, έχει ίδια **εξουσία**. Ο ΕΕΠΔ κατέχει μια ακλόνητη θέση εντός του οργανωμένου νομικού πλέγματος της ΕΚ. Οι εξουσίες αυτές (οι οποίες έχουν αναλυτικά παρουσιασθεί στα πλαίσια της παρούσας εργασίας) δεν έχουν μεταβιβαστεί στον ΕΕΠΔ, αλλά του έχουν απευθείας αποδοθεί από το άρθρο 286 ΣυνθΕΚ. Τα θεσμικά όργανα και οι άλλοι οργανισμοί της Κοινότητας πρέπει να σέβονται τις εξουσίες αυτές του ΕΕΠΔ και αυτός με τη σειρά του οφείλει να σέβεται τις δικές τους έτσι ώστε να διατηρείται η οργανική ισορροπία στους κόλπους της ΕΚ⁸⁴.

5. Ο ΕΛΕΓΧΟΣ ΤΟΥ ΕΕΠΔ

5.1. Ο πολιτικός έλεγχος

Στο άρθρο 42 του Κανονισμού, αναφέρεται στον διορισμό και στην λήξη της θητείας του ΕΕΠΔ (άρθρα 1-6). Το ΔΕΚ είναι το μόνο όργανο που δύναται ν' απαλλάξει τον ΕΕΠΔ από τα καθήκοντά του ή να τον κηρύξει έκπτωτο, σε εξαιρετικές περιπτώσεις που κρίνεται ένοχος για κακοδιοίκηση ή όταν η ανεξαρτησία του τίθεται υπό αμφισβήτηση. Αυτές οι εγγυήσεις απομακρύνουν τον ΕΕΠΔ από κάθε είδους εξωτερικές υποδείξεις ή πιέσεις, εμφανείς ή κεκρυμμένες⁸⁵.

⁸³ Κανονισμός 45/2001, αρ. 42 § 2.

⁸⁴ Hielke Hijmans, *ό.π.*, σελ. 1335-1336.

⁸⁵ Hielke Hijmans, *ό.π.*, σελ. 1338.

Σημαντικό είναι επίσης και το άρθρο 44 § 2 του Κανονισμού, το οποίο απαγορεύει στον ΕΕΠΔ να ζητήσει και να λάβει εντολές από οιονδήποτε κατά την εκτέλεση των καθηκόντων του. Ο έλεγχος της απόδοσής του από κάποιο πολιτικό όργανο, όπως π.χ. από το Ευρωπαϊκό Κοινοβούλιο ή το Συμβούλιο (τα οποία είναι οι οργανισμοί που διορίζουν τον ΕΕΠΔ), κατά τρόπο που θα μπορούσε να επηρεάσει την μελλοντική του απόδοση, θα ερχόταν σε αντίθεση με τις εγγυήσεις αυτές.

Οι προβλέψεις αυτές του Κανονισμού, διασφαλίζουν κατά τρόπο ικανοποιητικό ότι η άσκηση των καθηκόντων του ΕΕΠΔ δεν υπόκειται σε κανέναν πολιτικό έλεγχο. Στην πραγματικότητα βέβαια, ο πολιτικός έλεγχος δεν αποκλείεται τελείως (αφού κάποιοι μηχανισμοί περιέχουν στοιχεία ελέγχου) απλώς δεν είναι τόσο έντονος ώστε να καταλύει το περιεχόμενο των ανωτέρω διατάξεων του Κανονισμού. Μία τέτοια περίπτωση είναι και η υποχρέωση του ΕΕΠΔ να υποβάλει κάθε χρόνο στο Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Επιτροπή (αρ. 48 §1) καθώς και σε όλα τα όργανα και οργανισμούς της Κοινότητας (αρ. 48 §2) μια έκθεση πεπραγμένων (Annual Report) και να τη δημοσιεύει. Στο στην ίδια παράγραφο του ιδίου άρθρου αναφέρεται η πιθανή εξέταση της έκθεσης από το Ευρωπαϊκό Κοινοβούλιο. Αυτή η εξέταση έχει, κατά την άποψή μου, την έννοια της αποτίμησης του έργου του ΕΕΠΔ και την κριτική των μέτρων που λαμβάνονται για την αποτελεσματικότερη προστασία των προσωπικών δεδομένων.

Εκτός από την ετήσια αυτή έκθεση, σε πολλές περιπτώσεις η ενέργειες που κάνει ο ΕΕΠΔ συνοδεύονται και από ένα δημόσιο έγγραφο. Αυτό εξυπηρετεί στο να αποδεικνύεται η διαφάνεια που πρέπει να τηρεί ο ΕΕΠΔ κατά την ενάσκηση των καθηκόντων του⁸⁶.

5.2. Ο δικαστικός έλεγχος

Όπως έχει πολλάκις αναφερθεί εντός της παρούσας εργασίας, ο ΕΕΠΔ είναι μεν μια ανεξάρτητη αρχή. Αυτό όμως, δεν συνεπάγεται και αποκλεισμό οποιασδήποτε μορφής ελέγχου από το ΔΕΚ. Όσο ο ΕΕΠΔ ενεργεί με δέσμια

⁸⁶ Hielke Hijmans, *ό.π.*, σελ. 1339.

αρμοδιότητα, είναι κατανοητό ότι πρέπει να υπόκειται σε νομικό έλεγχο από τα δικαστήρια της ΕΚ. Άλλωστε, ο δικαστικός έλεγχος είναι μια απαίτηση από την πλευρά των πολιτών για αποτελεσματική δικαστική προστασία. Άλλωστε πρόκειται για ένα θεμελιώδες δικαίωμα που έχει αναχθεί σε γενική αρχή και είναι κοινό στα Συντάγματα όλων των κρατών μελών.

Επιπλέον, όπως έχει ήδη ειπωθεί, ο ΕΕΠΔ έχει την εξουσία να ερμηνεύει το κοινοτικό δίκαιο κατά τρόπο δεσμευτικό για τα όργανα και τους οργανισμούς της ΕΚ. Σ' αυτήν την περίπτωση το ΔΕΚ οφείλει να ελέγχει και να εξασφαλίζει ότι οι ερμηνείες που δίνει ο ΕΕΠΔ είναι σύμφωνοι με την ερμηνεία του κοινοτικού δικαίου⁸⁷.

Τέλος, και το άρθρο 32 §2 του Κανονισμού συντείνει στο συμπέρασμα ότι και οι αποφάσεις του ΕΕΠΔ ελέγχονται, εφόσον υπάρχει δυνατότητα προσβολής τους ενώπιον του ΔΕΚ.

⁸⁷ Hielke Hijmans, *ό.π.*, σελ. 1339-1340.

ΚΕΦΑΛΑΙΟ Β

ΟΙ ΟΥΣΙΑΣΤΙΚΕΣ ΕΠΙΠΤΩΣΕΙΣ ΤΗΣ ΛΕΙΤΟΥΡΓΙΑΣ ΤΟΥ

ΕΥΡΩΠΑΙΟΥ ΕΠΟΠΤΗ

Αφού ολοκληρώθηκε η αναλυτική παρουσίαση του θεσμικού καθεστώτος του Ευρωπαϊκού Επόπτη, θα ήταν αναγκαίο, για την καλύτερη κατανόηση του ρόλου που αυτός επιτελεί και ειδικότερα της «κανονιστικής» του λειτουργίας, να γίνει μια αναφορά σε ορισμένες γνωμοδοτήσεις του ΕΕΠΔ επί προτάσεων νομοθετικών πράξεων του Συμβουλίου, οι οποίες καταδεικνύουν τον τρόπο με τον οποίο προσεγγίζει τα καθήκοντά του ο ΕΕΠΔ, τη βαρύτητα που δίνει στην προστασία των ανθρωπίνων δικαιωμάτων και τον αντίκτυπο που έχουν στην υιοθέτηση των τελικών αποφάσεων του κοινοτικού νομοθέτη. Οι γνωμοδοτήσεις που θα αναλυθούν εν συνεχεία αφορούν: **1.** την ανταλλαγή πληροφοριών βάσει της αρχής της διαθεσιμότητας, **2.** την προστασία των δεδομένων προσωπικού χαρακτήρα που τυγχάνουν επεξεργασίας στο πλαίσιο του Τρίτου Πυλώνα, **3.** τη Σύμβαση του Prüm, **4.** τη χρήση των δεδομένων των καταστάσεων με τα ονόματα επιβατών (PNR) και **5.** την προστασία των παιδιών κατά τη χρήση του διαδικτύου και άλλων τηλεπικοινωνιακών τεχνολογιών.

1. Γνωμοδότηση σχετικά με την πρόταση απόφασης-πλαίσιου του Συμβουλίου για την ανταλλαγή πληροφοριών βάσει της αρχής της διαθεσιμότητας (COM 2005/490 τελικό)⁸⁸.

Η εν λόγω πρόταση απόφασης πλαισίου του Συμβουλίου διαβιβάσθηκε με επιστολή από την Επιτροπή στον ΕΕΠΔ τον Οκτώβριο του 2005. Ο ΕΕΠΔ θεώρησε την επιστολή αυτή ως αίτηση παροχής συμβουλών προς όργανα και οργανισμούς της Κοινότητας, όπως προβλέπεται από το αρ. 28 § 2 του Κανονισμού 45/2001 ΕΚ.

Το θέμα της διαθεσιμότητας πληροφοριών αστυνομικού χαρακτήρα πέραν των εθνικών συνόρων ή η ανταλλαγή αυτών των πληροφοριών, κατέχει υψηλή θέση στο πρόγραμμα δράσης των κρατών μελών, τόσο εντός όσο και εκτός του Συμβουλίου, καθώς επίσης στο πλαίσιο του Ευρωπαϊκού Κοινοβουλίου. Επίσης, εντός της γνωμοδότησης αναφέρεται ρητά⁸⁹ ότι το θέμα αυτό κρίνεται ιδιαιτέρως σημαντικό από την άποψη της προστασίας των προσωπικών δεδομένων και είναι άμεσα συνδεδεμένο με την πρόταση απόφασης πλαισίου του Συμβουλίου σχετικά με την προστασία δεδομένων προσωπικού χαρακτήρα στο πλαίσιο της αστυνομικής και δικαστικής συνεργασίας σε ποινικές υποθέσεις (θα γίνει αναλυτική αναφορά παρακάτω υπό 3).

Η έννοιά της αρχής της διαθεσιμότητας είναι ότι οι απαιτούμενες πληροφορίες για την καταπολέμηση του εγκλήματος πρέπει να διακινούνται χωρίς εμπόδια διαμέσου των εσωτερικών συνόρων της Ε.Ε. Στόχος της εν λόγω πρότασης είναι η εφαρμογή της αρχής αυτής υπό μορφή δεσμευτικού νομοθετικού μέσου. Κατά την άποψη όμως του ΕΕΠΔ, δεν πρέπει να εκδοθεί νομοθετικό μέσο αυτού του είδους χωρίς ουσιώδεις διασφαλίσεις για την προστασία δεδομένων. Την ίδια θέση λαμβάνει ο ΕΕΠΔ όσον αφορά την έκδοση άλλων νομοθετικών μέσων που διευκολύνουν τη ροή πληροφοριών αστυνομικού χαρακτήρα εντός των εσωτερικών συνόρων της Ε.Ε.

⁸⁸ ΕΕ 17.5. 2006 C 116, σελ. 8.

⁸⁹ C 116, σελ. 8, § 4.

Ειδικότερα, η αρχή της διαθεσιμότητας αναφέρει πως οι πληροφορίες οι οποίες είναι διαθέσιμες σε ορισμένες αρχές κάποιου κράτους μέλους πρέπει να παρέχονται και σε ανάλογες αρχές άλλων κρατών μελών. Η ανταλλαγή αυτή πρέπει να γίνεται με τον ταχύτερο και ευκολότερο τρόπο μεταξύ των αρχών των κρατών μελών. Αυτή η ανταλλαγή, όμως, εμφανίζει συχνά δυσχέρειες που σχετίζονται με την ανομοιόμορφη οργάνωση της αστυνομίας και της δικαιοσύνης σε κάθε κράτος μέλος, τους διαφορετικούς τύπους ευαίσθητων πληροφοριών και τρόπων πρόσβασης σε αυτές και την ερμηνεία αυτών σε διαφορετικές γλώσσες και νομικά συστήματα.

Προς το σκοπό της άμεσης και τάχιστα ανταλλαγής πληροφοριών, η πρόταση απόφασης πλαισίου για τη διαθεσιμότητα εισάγει τα «δεδομένα καταλόγου», δηλαδή συγκεκριμένα δεδομένα που επιδέχονται άμεση διασυννοριακή πρόσβαση⁹⁰. Τα κράτη μέλη πρέπει να επιτρέπουν οι πληροφορίες να είναι διαθέσιμες. Με τον τρόπο αυτό, όμως, χάνουν την αρμοδιότητα ελέγχου της ροής των πληροφοριών και γι' αυτό απαιτείται ιδιαίτερη προσοχή από την άποψη της προστασίας δεδομένων προσωπικού χαρακτήρα.

Η αρχή της διαθεσιμότητας εφαρμόζεται: **α)** σε υφιστάμενες πληροφορίες, **β)** σε έξι τύπους πληροφοριών που απαριθμούνται στο παράρτημα II της πρότασης της Επιτροπής⁹¹, **γ)** σε πληροφορίες διαθέσιμες

⁹⁰ Δεδομένα καταλόγου νοούνται «τα δεδομένα που έχουν ως στόχο να εντοπίζουν με σαφήνεια πληροφορίες και στα οποία μπορεί να τεθεί το ερώτημα μέσω διαδικασίας αναζήτησης για να διαπιστωθεί εάν οι πληροφορίες είναι διαθέσιμες ή όχι.» (Βλ. ό.π. σελ. 14, § 54).

⁹¹ Σύμφωνα με τους όρους που τίθενται στην παρούσα απόφαση-πλαίσιο μπορούν να ληφθούν τα ακόλουθα είδη πληροφοριών:

1. Προφίλ DNA, ήτοι ένας κωδικός αριθμός και γραμμάτων ο οποίος καταρτίζεται βάσει των επτά ιχνηθετών DNA που αποτελούν την ευρωπαϊκή δέσμη προτύπων όπως ορίζεται στο ψήφισμα του Συμβουλίου 2001/C/187/01 της 25ης Ιουνίου 2001 για την ανταλλαγή αποτελεσμάτων ανάλυσης του DNA[9]. Οι ιχνηθέτες αυτοί δεν θα περιλαμβάνουν πληροφορίες σχετικά με συγκεκριμένα κληρονομικά χαρακτηριστικά.
2. Δακτυλικά αποτυπώματα.
3. Βαλλιστικά στοιχεία.
4. Πληροφορίες σχετικά τον αριθμό κυκλοφορίας του οχήματος
5. Αριθμοί τηλεφώνου και άλλα δεδομένα επικοινωνιών, με την εξαίρεση των δεδομένων περιεχομένου και των δεδομένων κίνησης εκτός εάν τα τελευταία δεδομένα ελέγχονται από την ορισθείσα αρχή.
6. Ελάχιστα δεδομένα για την αναγνώριση των προσώπων που περιλαμβάνονται στα μητρώα του ληξιαρχείου.

στις αρμόδιες αρχές. Η αρχή αυτή περιορίζει την εφαρμογή της αρχής της διαθεσιμότητας στη φάση πριν την έναρξη της δίκωξης⁹².

Η εφαρμογή μιας τόσο ευρείας αρχής όπως η εν λόγω αρχή, απαιτεί σαφή και ακριβή καθορισμό των δεδομένων που θεωρούνται διαθέσιμα. Για τον λόγο αυτό, ο ΕΕΠΔ συνιστά την αποσαφήνιση των ανωτέρω τριών πεδίων εφαρμογής, τον περιορισμό του πεδίου εφαρμογής της αρχής σε πληροφορίες ελεγχόμενες από αρμόδιες αρχές και τη λήψη μέριμνας για επαρκείς διασφαλίσεις όσον αφορά την προστασία δεδομένων προσωπικού χαρακτήρα⁹³.

Επιπλέον, ο ΕΕΠΔ ζητά να διασφαλιστεί ότι η πρόταση δεν θα προάγει την άνευ όρων διασύνδεση των βάσεων δεδομένων, οδηγώντας τελικά σ' ένα δίκτυο βάσεων δεδομένων του οποίου η εποπτεία θα είναι δυσχερής.

Η πρόταση στα άρθρα 9 και 10, προβλέπει την άμεση και έμμεση (αντίστοιχα) πρόσβαση στις πληροφορίες. Άμεση ηλεκτρονική πρόσβαση (direct on line consultation) υπάρχει σε πληροφορίες περιεχόμενες σε βάσεις δεδομένων όπου οι αντίστοιχες εθνικές αρχές έχουν άμεση ηλεκτρονική πρόσβαση. Όταν η αναζήτηση σε δεδομένα καταλόγου αποβαίνει επιτυχής, η ενδιαφερόμενη αρχή μπορεί να διατυπώνει αίτηση πληροφοριών και να τη διαβιβάζει στην ορισθείσα αρχή, ώστε να λάβει τις πληροφορίες που προσδιορίζονται από τα δεδομένα καταλόγου.

Η άμεση πρόσβαση δεν δημιουργεί νέες βάσεις δεδομένων, απαιτεί όμως τη διαλειτουργικότητα των συστημάτων των ισοδύναμων αρμόδιων αρχών στα κράτη μέλη. Η πρόσβαση αυτή θα εισαγάγει νέα χρήση των ήδη υφιστάμενων βάσεων με την παροχή σε όλες τις αρμόδιες αρχές των κρατών μελών μιας ευχέρειας την οποία διέθεταν μέχρι πρότινος μόνο οι εθνικές αρμόδιες αρχές. Αυτό όμως, θα σήμαινε αυτομάτως ότι πρόσβαση στις βάσεις δεδομένων θα έχουν ένα αυξημένο πλήθος προσώπων, γεγονός που θα αύξανε τον κίνδυνο να σημειωθούν καταχρήσεις. Έτσι φαίνεται ότι αναιρείται η εξουσία των εθνικών αρχών να αρνούνται την παροχή πληροφοριών, εγείρονται αμφιβολίες ως προς την επικαιροποίηση των δεδομένων και τέλος προκύπτουν

⁹² Άρθρο 2 § 1 COM (2005) 490 τελικό.

⁹³ C 116, σελ. 11, § 27 και 28.

προβλήματα όταν οι ορισθείσες αρχές που έχουν πρόσβαση σε βάσεις δεδομένων δεν είναι αστυνομικές. Ακόμη όμως και να είναι αστυνομικές, η εθνική αρχή για την προστασία δεδομένων στο οικείο κράτος μέλος στερείται οποιασδήποτε αρμοδιότητας εποπτείας έναντι των αστυνομικών αρχών άλλων κρατών μελών. Υπάρχει δε ο κίνδυνος να αποκαλυφθεί ότι για κάποια φυσικά πρόσωπα υπάρχει αστυνομικός φάκελος σχετικός με αξιόποινες πράξεις⁹⁴.

Για τους ανωτέρω λόγους, ο ΕΕΠΔ έκρινε ότι υπάρχει ανάγκη θέσπισης μιας άλλης απόφασης πλαισίου σχετικά με την προστασία των προσωπικών δεδομένων από την οποία θα εξαρτάται η θέσπιση της προκειμένης πρότασης. Κρίνεται, επίσης, αναγκαίο, να προβλέψει ο ευρωπαϊός νομοθέτης τους δέοντες κανόνες αναφορικά με τη σύσταση των καταλόγων, τη διαχείριση των συστημάτων αρχειοθέτησης και την κατάλληλη οργάνωση της πρόσβασης στα δεδομένα καταλόγου. Κατά την άποψη του ΕΕΠΔ, η πρόταση δεν είναι ικανοποιητική όσον αφορά τα σημεία αυτά⁹⁵.

Επιπροσθέτως, ο ΕΕΠΔ αναφέρει ότι η αρχή της διαθεσιμότητας θα πρέπει να μη θίγει την βάσει της εθνικής νομοθεσίας υποχρέωση να λαμβάνεται προηγούμενη άδεια για τις πληροφορίες από τις δικαστικές αρχές.

Ολοκληρώνοντας, θα λέγαμε ότι ο ΕΕΠΔ δράττεται της ευκαιρίας να παρουσιάσει μέσα από την παρούσα γνώμη, ορισμένες περισσότερο γενικές και θεμελιώδεις απόψεις σχετικά με το θέμα της ανταλλαγής πληροφοριών αστυνομικού χαρακτήρα. Κατά τον ΕΕΠΔ, θα πρέπει η αρχή της διαθεσιμότητας να εφαρμοστεί υπό μορφή δεσμευτικού νομοθετικού μέσου με περισσότερο συντηρητική, σταδιακή προσέγγιση, βάσει της οποίας να καλύπτεται ένας τύπος δεδομένων με παρακολούθηση αφενός του βαθμού στον οποίο η αρχή της διαθεσιμότητας μπορεί όντως να στηρίζει την αστυνόμευση και αφετέρου των συγκεκριμένων κινδύνων για την προστασία των δεδομένων προσωπικού χαρακτήρα. Επίσης, οποιοδήποτε νομοθετικό μέσο εφαρμογής της εν λόγω

⁹⁴ Σύμφωνα με την άποψη του Β. Σωτηρόπουλου: «...η αρχή της διαθεσιμότητας συνιστά στην ουσία κατάργηση της αρχής της νομιμότητας των επεξεργασιών των προσωπικών δεδομένων (ειδικά στο επίπεδο του τρίτου πυλώνα). Όπως και η υποχρεωτική διατήρηση των τηλεπικοινωνιακών δεδομένων, έτσι και η αρχή της διαθεσιμότητας, με την ευρύτητά της και τις τεράστιες εξαιρέσεις που εισάγει από την προστασία, επηρεάζει το κοινοτικό κεκτημένο προστασίας δεδομένων. Η θεμελιώδης προστασία προσωπικών δεδομένων στην Ευρώπη δεν θα είναι η ίδια, ύστερα από την ψήφιση αυτής της απόφασης-πλαίσιο.» (*Η συνταγματική προστασία των προσωπικών δεδομένων*, Αθήνα 2006, σελ. 199-200).

⁹⁵ C 116, σελ. 12, § 39.

αρχής δεν θα πρέπει να θεσπιστεί χωρίς την προηγούμενη θέσπιση ουσιαστικών διασφαλίσεων για την προστασία δεδομένων⁹⁶.

Καταδεικνύεται, επομένως, ότι ο επόπτης δεν παρέχει απλώς τεχνική εμπειρογνωμοσύνη, αλλά ελέγχει, από ουσιαστικής πλευράς, και την αναγκαιότητα της εισαγωγής ή μη μιας νομοθετικής πράξης υπό το πρίσμα της επαρκούς προστασίας των θεμελιωδών δικαιωμάτων, καθώς και το πρόσφορο και την αναλογικότητα των επιμέρους ρυθμίσεων.

Κλείνοντας τη γνωμοδότηση του ο ΕΕΠΔ κάνει ορισμένες συστάσεις με στόχο την τροποποίηση της συγκεκριμένης πρότασης και ειδικότερα μια κωδικοποίηση των αρχών προστασίας που θα πρέπει να εφαρμοσθούν⁹⁷.

2. Γνωμοδότηση σχετικά με την πρωτοβουλία της Γερμανίας για τη θέσπιση απόφασης του Συμβουλίου για την εφαρμογή της απόφασης 2007/.../ΔΕΥ (η πρωτοβουλία του Prüm)⁹⁸.

Σχετικά με την πρωτοβουλία αυτή της Γερμανίας για απόφαση εφαρμογής, δεν ζητήθηκε η γνωμοδότηση του ΕΕΠΔ. Επομένως, ο ΕΕΠΔ γνωμοδότησε κατόπιν ιδίας πρωτοβουλίας. Όπως, έχει ήδη αναφερθεί (βλ. ανωτέρω υπό 2.4.2) ο ΕΕΠΔ έχει δικαίωμα να γνωμοδοτεί επί νομοσχεδίων αυτεπαγγέλτως και να παρεμβαίνει σε οποιοδήποτε στάδιο της νομοθετικής διαδικασίας χωρίς να του έχει ζητηθεί. Αν και τα κράτη μέλη είναι αυτά που παίρνουν την πρωτοβουλία για τη θέσπιση ενός νομοθετικού μέτρου, δυνάμει του τίτλου VI της Συνθήκης της Ευρωπαϊκής Ένωσης, δεν υπέχουν νομική υποχρέωση να ζητήσουν τη γνωμοδότηση του ΕΕΠΔ⁹⁹.

Στην προκειμένη περίπτωση, στόχος του Συμβουλίου είναι να τροποποιηθεί η πρωτοβουλία όσο το δυνατόν λιγότερο, ώστε να είναι απολύτως σύμφωνη με το κείμενο της **σύμβασης του Prüm** που έχει

⁹⁶ C 116 σελ. 17, §§ 69 και 70.

⁹⁷ C 116 σελ. 16 § 67.

⁹⁸ ΕΕ 10.4. 2008 C 89, σελ.1.

⁹⁹ C 89, σελ. 1, §§ 2 και 3.

υπογραφεί ήδη από ορισμένα κράτη μέλη. Ο ΕΕΠΔ αναλαμβάνει να εξετάσει τον δημοκρατικό αντίκτυπο της προσέγγισης αυτής.

Η σύμβαση του Prüm υπεγράφη το Μάιο του 2005 από επτά κράτη μέλη, εκτός του πλαισίου της συνθήκης της Ευρωπαϊκής Ένωσης. Εν συνεχεία προσχώρησαν και άλλα κράτη μέλη. Η εν λόγω σύμβαση συμπληρώνεται από μια συμφωνία που είναι απαραίτητη για την εφαρμογή της. Τα κύρια στοιχεία της σύμβασης του Prüm θα ενσωματωθούν στο νομικό πλαίσιο της Ε.Ε, μετά την έκδοση της απόφασης 2007/.../ΔΕΥ του Συμβουλίου σχετικά με την πρωτοβουλία 15 κρατών μελών («πρωτοβουλία του Prüm»), επί της οποίας έχει ήδη επιτευχθεί πολιτική συμφωνία στο Συμβούλιο. Κατά τη νομοθετική διαδικασία για την προετοιμασία της έκδοσης της απόφασης του Συμβουλίου, στόχος ήταν να επιτευχθεί συμφωνία ως προς το κεκτημένο της σύμβασης του Prüm¹⁰⁰.

Επί της ουσίας τώρα, η παρούσα γνωμοδότηση εστιάζει στο σχέδιο απόφασης του Συμβουλίου για τους κανόνες εφαρμογής. Οι κανόνες εφαρμογής έχουν ιδιαίτερη σημασία διότι προσδιορίζουν κρίσιμες πτυχές και μέσα του συστήματος και της λειτουργίας του. Οι κανόνες εφαρμογής θεσπίζουν κοινές διατάξεις για την ανταλλαγή δεδομένων (κεφ.2) και καθορίζουν τα ειδικά χαρακτηριστικά της ανταλλαγής δεδομένων DNA (κεφ.3), δεδομένων σχετικών με δακτυλικά αποτυπώματα (κεφ.4) και δεδομένων σχετικών με άδειες κυκλοφορίας οχημάτων (κεφ. 5)¹⁰¹.

Ο ΕΕΠΔ επισημαίνει ότι η εκ των προτέρων ύπαρξη κανόνων εφαρμογής που ήδη ισχύουν για τη σύμβαση του Prüm φαίνεται ότι περιορίζει κατά πολύ το περιθώριο ουσιαστικών χειρισμών του Συμβουλίου. Συνεπώς, τα 27 κράτη μέλη θα πρέπει να ακολουθήσουν την πορεία που είναι ήδη καθορισμένη από τα 7 κράτη μέλη που υπέγραψαν τη σύμβαση του Prüm. Όμως η προσέγγιση αυτή εμποδίζει την ανάπτυξη μιας διαφανούς και δημοκρατικής νομοθετικής διαδικασίας, δεδομένου ότι περιορίζει σημαντικά τη δυνατότητα να πραγματοποιηθεί μια γενική συζήτηση και να ληφθούν ουσιαστικά υπόψη ο νομοθετικός ρόλος του Ευρωπαϊκού Συμβουλίου και ο συμβουλευτικός του ΕΕΠΔ. Για το λόγο αυτό, ο ΕΕΠΔ ζητά να συζητηθούν ανοιχτά η πρωτοβουλία

¹⁰⁰ Βλ. σχετικά Ετήσια Έκθεση 2007, “Cross-border cooperation”, σελ 47.

¹⁰¹ C 89, σελ. 2, §10.

και το παράρτημά της, αξιοποιώντας ουσιαστικά τις προτάσεις όλων των θεσμικών φορέων.

Στο κεφ. 6 της απόφασης του Συμβουλίου σχετικά με την πρωτοβουλία του Prüm καθορίζονται ορισμένες εγγυήσεις και ειδικοί κανόνες όσον αφορά την προστασία των δεδομένων. Ωστόσο, οι κανόνες αυτοί δεν μπορούν να λειτουργήσουν σωστά από μόνοι τους, αλλά πρέπει να στηριχτούν σε ένα πλήρως ανεπτυγμένο και γενικότερο πλαίσιο για τη προστασία των προσωπικών δεδομένων τα οποία επεξεργάζονται οι αστυνομικές και δικαστικές αρχές. Το άρθρο 25 της απόφασης του Συμβουλίου για την πρωτοβουλία του Prüm παραπέμπει στη σύμβαση αριθ. 108 του Συμβουλίου της Ευρώπης (βλ. ανωτέρω υπό 1.2.1). Ο ΕΕΠΔ έχει, όμως, επανειλημμένα τονίσει ότι οι αρχές που περιέχονται στην σύμβαση 108, πρέπει να συγκεκριμενοποιηθούν, ώστε να εξασφαλιστεί υψηλό επίπεδο προστασίας των δεδομένων προσωπικού χαρακτήρα το οποίο θα μπορεί να εγγυάται τόσο τα δικαιώματα των πολιτών, όσο και την αποτελεσματική επιβολή του νόμου σε ένα χώρο ελευθερίας, ασφάλειας και δικαιοσύνης¹⁰².

Επιπλέον, ο ΕΕΠΔ θεωρεί πως οι αποφάσεις του Συμβουλίου σχετικά με τη σύμβαση του Prüm δεν θα πρέπει να τεθούν σε ισχύ προτού τα κράτη μέλη θέσουν σε εφαρμογή μια γενική απόφαση-πλαίσιο για την προστασία των δεδομένων στον τρίτο πυλώνα. Κρίνει, επίσης, αναγκαίο, οι σχέσεις μεταξύ των νομικών πράξεων να είναι απολύτως σαφείς έτσι ώστε να διασφαλιστεί ότι η εν λόγω απόφαση πλαίσιο αποτελεί το γενικό νομικό πλαίσιο «lex generalis», ενώ παράλληλα επιτρέπεται η εφαρμογή περαιτέρω ειδικών εγγυήσεων και αυστηρότερων κανόνων που θεσπίζονται με την απόφαση σχετικά με την πρωτοβουλία του Prüm¹⁰³.

Επιπρόσθετα, θα πρέπει ο νομοθέτης να διευκρινίσει ότι οι ειδικοί κανόνες προστασίας δεδομένων σχετικών με το DNA, τα δακτυλικά αποτυπώματα και τις άδειες κυκλοφορίας οχημάτων, δεν ισχύουν μόνο για την ανταλλαγή αυτών των δεδομένων αλλά και για τη συλλογή, αποθήκευση και επεξεργασία τους εντός του κράτους μέλους, καθώς και για την παροχή

¹⁰² C 89, σελ. 2, §14.

¹⁰³ C 89, σελ. 3, §17.

περαιτέρω δεδομένων προσωπικού χαρακτήρα εντός του πεδίου εφαρμογής της απόφασης του Συμβουλίου σχετικά με την πρωτοβουλία του Prüm¹⁰⁴.

Ο ΕΕΠΔ, καλεί επομένως, το νομοθέτη να διασφαλίσει (σύμφωνα με το άρθρο 30 §1 στοιχείο β' της Συνθήκης της Ευρωπαϊκής Ένωσης¹⁰⁵) ότι πριν από την έναρξη ισχύος της παρούσας πρωτοβουλίας, θα έχει θεσπιστεί ένα σαφές, αποτελεσματικό και συνολικό νομικό πλαίσιο για την προστασία των προσωπικών δεδομένων, το οποίο θα συνδυάζει διάφορες νομικές πράξεις με γενικές διατάξεις και ειδικές εγγυήσεις.

Τα στοιχεία, λοιπόν, αυτά που θεωρεί ο ΕΕΠΔ ότι δεν καλύπτονται από το σχέδιο της απόφασης-πλαισίου για την προστασία των δεδομένων στον τρίτο πυλώνα και τα οποία πρέπει να ληφθούν υπόψη για την εφαρμογή του συστήματος που θεσπίζει η παρούσα πρωτοβουλία είναι τα εξής:

α. Η διαφάνεια, η οποία αποτελεί ουσιώδες στοιχείο της διαδικασίας λήψης αποφάσεων και της εφαρμογής των κανόνων. Θα πρέπει δηλαδή να ενισχυθεί η διαφάνεια των μέτρων, να θεσπισθούν μηχανισμοί ενημέρωσης των πολιτών σχετικά με τα δικαιώματά τους και τον τρόπο άσκησής τους.

β. Η κλίμακα του συστήματος, δηλαδή η ανταλλαγή των δεδομένων μεταξύ πολλών ή λίγων κρατών. Κατά τον ΕΕΠΔ, ο νομοθέτης οφείλει να λάβει υπόψη του την κλίμακα αυτή, διασφαλίζοντας ότι η αύξηση του αριθμού των συμμετεχόντων κρατών μελών δεν θα οδηγήσει σε μειωμένη αποτελεσματικότητα. Θα πρέπει, συνεπώς, να οριστούν συγκεκριμένοι μορφότυποι για τη διαβίβαση των δεδομένων και να παρακολουθείται συνέχεια η ορθότητα των ανταλλαγών δεδομένων.

γ. Ο σημαντικός ρόλος των ανεξάρτητων εποπτικών αρχών στο πλαίσιο των διασυνοριακών ανταλλαγών δεδομένων μεγάλης κλίμακας. Ο ΕΕΠΔ συνιστά να αναγνωριστεί ρητά εντός της πρωτοβουλίας ο ουσιαστικός συμβουλευτικός ρόλος των αρχών αυτών.

¹⁰⁴ C 89, σελ. 3, §18.

¹⁰⁵ «1. Η από κοινού δράση στον τομέα της αστυνομικής συνεργασίας περιλαμβάνει:

β) τη συλλογή, αποθήκευση, επεξεργασία, ανάλυση και ανταλλαγή σχετικών πληροφοριών, συμπεριλαμβανομένων των πληροφοριών που κατέχουν οι υπηρεσίες επιβολής του νόμου για αναφορές ως προς τις καταχωρήσεις ύποπτων οικονομικών συναλλαγών, ιδίως μέσω της Ευρωπόλ, υπό την επιφύλαξη των κατάλληλων διατάξεων για την προστασία δεδομένων προσωπικού χαρακτήρα».

Επιπλέον, ο ΕΕΠΔ καλεί το νομοθέτη να συμπεριλάβει ένα σαφή και περιεκτικό ορισμό των δεδομένων προσωπικού χαρακτήρα και να ληφθεί υπόψη η ακρίβεια της διαδικασίας αντιστοίχισης στα πλαίσια των αυτοματοποιημένων αναζητήσεων και συγκρίσεων DNA και δακτυλικών αποτυπωμάτων.

Τέλος, ο ΕΕΠΔ συνιστά να συμμορφωθεί η πρωτοβουλία με τον Κανονισμό 45/2001/ΕΚ και να δοθεί έμφαση στην αξιολόγηση των προσωπικών δεδομένων, εστιάζοντας κυρίως στους σκοπούς, τις μεθόδους, την ακρίβεια των ανταλλασσόμενων δεδομένων καθώς και την διάρκεια της αποθήκευσής τους.

Ο Επόπτης παρεμβαίνει ακόμη μια φορά σε ό,τι αφορά την σκοπιμότητα της υιοθέτησης της πράξης (κρίνει ότι δεν θα πρέπει να υιοθετηθεί πριν τεθεί ένα γενικό πλαίσιο προστασίας), καλύπτει δε ακόμη τη δομή του όλου συστήματος προστασίας (σχέση γενικού ειδικού μεταξύ πράξεων) καθώς και τις συγκεκριμένες εγγυήσεις της υπό κρίση πράξης.

3. Τρίτη γνωμοδότηση για την πρόταση απόφασης-πλαισίου του Συμβουλίου για την προστασία των δεδομένων προσωπικού χαρακτήρα στα πλαίσια της αστυνομικής και δικαστικής συνεργασίας σε ποινικές υποθέσεις¹⁰⁶.

Τον Δεκέμβριο του 2005 και το Νοέμβριο του 2006, ο ΕΕΠΔ εξέδωσε δύο γνώμες¹⁰⁷ για την πρόταση απόφασης πλαισίου του Συμβουλίου για την προστασία των δεδομένων προσωπικού χαρακτήρα που τυγχάνουν επεξεργασίας στο πλαίσιο της αστυνομικής και δικαστικής συνεργασίας σε ποινικές υποθέσεις, την οποία υπέβαλε η Επιτροπή. Στις γνώμες αυτές, ο ΕΕΠΔ επεσήμανε τη σημασία της πρότασης αυτής ως αποτελεσματικού μέσου για την προστασία των δεδομένων προσωπικού χαρακτήρα στο πεδίο που καλύπτεται από τον Τίτλο IV της Συνθήκης ΕΕ. Τον Ιανουάριο του 2007 η Γερμανική Προεδρία καθόρισε ορισμένα βασικά σημεία για την αναθεώρηση της

¹⁰⁶ ΕΕ 23.6. 2007 C139, σελ. 1.

¹⁰⁷ Βλ. ΕΕ C 47 της 25.2.2006, σελ.27 η πρώτη γνώμη και στην ιστοσελίδα www.edps.europa.eu η δεύτερη.

πρότασης, με στόχο την άρση των εκκρεμών επιφυλάξεων και τη βελτίωση της προστασίας των δεδομένων στο πλαίσιο του τρίτου πυλώνα. Λόγω των ουσιαστικών αλλαγών που περιέχονται στην αναθεωρημένη πρόταση, καθώς και της σημασίας της, απαιτήθηκε και τρίτη γνωμοδότηση του ΕΕΠΔ, ο οποίος αναφέρεται στις κυριότερες ανησυχίες του, χωρίς να επαναλαμβάνει τα σημεία που επισημάνθηκαν στις άλλες δύο γνώμες του¹⁰⁸.

Επί της ουσίας, λοιπόν, ο ΕΕΠΔ εκφράζει την απογοήτευσή του για το περιεχόμενο του κειμένου που υπέβαλε η Γερμανική Προεδρία, διότι δεν ανταποκρίνεται στις προσδοκίες του για τους εξής λόγους¹⁰⁹:

α. Το κείμενο εξασθενεί το επίπεδο προστασίας του πολίτη, δεδομένου ότι έχουν αφαιρεθεί ορισμένες ουσιώδεις διατάξεις για την προστασία του και οι οποίες υπήρχαν στην πρόταση της Επιτροπής.

β. Το επίπεδο προστασίας που παρέχει η αναθεωρημένη πρόταση είναι χαμηλότερο και από το αντίστοιχο επίπεδο που παρέχει η Σύμβαση αριθ. 108¹¹⁰.

γ. Το κείμενο καθιστά το φάκελο ακόμη πιο περίπλοκο, αφού καλύπτει την επεξεργασία δεδομένων από την Europol, Eurojust και το Τελωνειακό Σύστημα Πληροφοριών του τρίτου πυλώνα και ανοίγει συζήτηση για την εποπτεία των φορέων αυτών.

δ. Η νομοθετική ποιότητα του κειμένου δεν είναι ικανοποιητική. Συγκεκριμένα, το κείμενο δεν είναι διατυπωμένο με σαφήνεια, απλότητα και ακρίβεια, γεγονός που εμποδίζει τους πολίτες να κατανοήσουν με σαφήνεια τα δικαιώματα και τις υποχρεώσεις τους.

ε. Το χαμηλό επίπεδο προστασίας που παρέχει η πρόταση δεν μπορεί να συμβάλει ορθώς στη δημιουργία χώρου ελευθερίας, ασφάλειας και δικαιοσύνης εντός του οποίου είναι δυνατή η διασυνοριακή ανταλλαγή πληροφοριών επιβολής του νόμου μεταξύ των αστυνομικών και δικαστικών αρχών. Ειδικότερα, η πρόταση εξαρτά την ανταλλαγή πληροφοριών από διαφόρους εθνικούς «κανόνες καταγωγής» και «δύο μέτρα και δύο σταθμά»

¹⁰⁸ Βλ. σχετικά Ετήσια Έκθεση 2007, σελ. 44-45 (υπό 3.3.1)

¹⁰⁹ C139, σελ. 2, § 5.

¹¹⁰ Σύμβαση του Συμβουλίου της Ευρώπης για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία πληροφοριών προσωπικού χαρακτήρα, 28.1.1981 (βλ. ανωτέρω υπό 1.2.1).

που επηρεάζουν σημαντικά τη συνεργασία στο πεδίο της επιβολής του νόμου χωρίς να βελτιώνουν την προστασία των προσωπικών δεδομένων¹¹¹.

Η αυξημένη σημασία της αστυνομικής και δικαστικής συνεργασίας σε ποινικές υποθέσεις καθώς και οι δράσεις που απορρέουν από το Πρόγραμμα της Χάγης για την ενίσχυση της ελευθερίας, της ασφάλειας και της δικαιοσύνης στην ΕΕ¹¹², προβάλλουν την ανάγκη για κοινά πρότυπα προστασίας των προσωπικών δεδομένων στο πλαίσιο του τρίτου πυλώνα. Όμως, ο ΕΕΠΔ έχει επανειλημμένα τονίσει ότι τα υφιστάμενα μέσα ευρωπαϊκού επιπέδου δεν επαρκούν. Η σύμβαση 108 του Συμβουλίου της Ευρώπης η οποία είναι μεν δεσμευτική για τα κράτη μέλη, αλλά δεν παρέχει την απαιτούμενη ακρίβεια. Επίσης, η οδηγία 95/46/EK στην οποία ενσωματώνονται και διευκρινίζονται οι αρχές της σύμβασης 108 όσον αφορά στην εσωτερική αγορά, δεν εφαρμόζεται σε δραστηριότητες που εμπίπτουν στο πεδίο εφαρμογής του τρίτου πυλώνα. Για τον τομέα της αστυνομικής και δικαστικής συνεργασίας, όλα τα κράτη μέλη έχουν υπογράψει τη σύσταση αριθ. R (87) 15 της Επιτροπής των Υπουργών του Συμβουλίου της Ευρώπης προς τα κράτη μέλη για τη ρύθμιση της χρήσης δεδομένων προσωπικού χαρακτήρα στον αστυνομικό τομέα¹¹³, η οποία όμως δεν είναι δεσμευτική πράξη¹¹⁴.

Για τους λόγους αυτούς ο ΕΕΠΔ υποστηρίζει την άποψη ότι ένα γενικό πλαίσιο για την προστασία των δεδομένων στο πλαίσιο του τρίτου πυλώνα πρέπει να εξασφαλίζει ένα υψηλό και συνεκτικό επίπεδο προστασίας δεδομένων βασιζόμενα στις αρχές προστασίας δεδομένων που κατοχυρώνονται με τη σύμβαση 108 και την οδηγία 95/46/EK, λαμβάνοντας υπόψη και τις ιδιαιτερότητες των δραστηριοτήτων επιβολής του νόμου. Η συνεκτικότητα αυτή είναι ακόμη σημαντικότερη όταν διαβιβάζονται δεδομένα προσωπικού χαρακτήρα από τον πρώτο στον τρίτο πυλώνα, όπως συμβαίνει π.χ. στην περίπτωση των PNR. Η χρήση καταλόγων ατόμων των οποίων απαγορεύεται η επιβίβαση σε αεροσκάφη («no flying lists») τους οποίους καταρτίζουν οι αερομεταφορείς για τις αρχές επιβολής του νόμου για σκοπούς

¹¹¹ Π.χ. άρθρο 13 περί συμμόρφωσης προς τους εθνικούς περιορισμούς εθνικής επεξεργασίας.

¹¹² Βλ. ΕΕ C 198 της 12.8.2005, σελ.1.

¹¹³ Η σύσταση αυτή εκδόθηκε το Σεπτέμβριο του 1987 και υπάρχει στην ιστοσελίδα www.coe.int/dataprotection/.

¹¹⁴ C 139, σελ. 3, § 8.

εμπορικούς και ασφάλειας των πτήσεων (πρώτος πυλώνας). Επομένως, ο ΕΕΠΔ κρίνει πως οι αρχές προστασίας δεδομένων του πρώτου πυλώνα πρέπει να εφαρμόζονται και στον τρίτο¹¹⁵.

Αναφορικά με την δυνατότητα εφαρμογής δεδομένων προσωπικού χαρακτήρα στην επεξεργασία που λαμβάνει χώρα στο εσωτερικό των κρατών μελών, ο ΕΕΠΔ επισημαίνει ότι το σημερινό σχέδιο το οποίο παρέχει στα κράτη μέλη πλήρη διακριτική ευχέρεια κατά την εφαρμογή των ομοιόμορφων αρχών προστασίας δεδομένων και δεν τα υποχρεώνει να εφαρμόζουν τους ίδιους κοινούς κανόνες προστασίας δεδομένων εντός του χώρου της αστυνομικής και δικαστικής συνεργασίας, περικλείει τον κίνδυνο να υπάρξουν διαφορετικά επίπεδα προστασίας των δεδομένων στα διάφορα κράτη μέλη. Αυτό είναι ασυμβίβαστο προς τη δημιουργία ενός χώρου ελευθερίας, ασφάλειας και δικαιοσύνης και ακατάλληλο για την προστασία των δεδομένων προσωπικού χαρακτήρα, σύμφωνα με το άρθρο 30 §1 στ. β' ΣΕΕ. Επίσης, οι αρχές επιβολής του νόμου θα αντιμετωπίζουν προβλήματα λόγω των δυσεφάρμοστων διακρίσεων μεταξύ εγχώριων δεδομένων και δεδομένων που διαβιβάζονται. Για τους ανωτέρω λόγους, ο ΕΕΠΔ καλεί το νομοθέτη να υποχρεώσει τα κράτη μέλη να εφαρμόζουν την απόφαση-πλαίσιο στην επεξεργασία των προσωπικών δεδομένων¹¹⁶.

Επιπρόσθετα, ο ΕΕΠΔ κρίνει ότι οι σημερινές διατάξεις για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα, θίγουν τη βασική αρχή του περιορισμού του σκοπού και μάλιστα υπολείπονται των υφιστάμενων κανόνων που θεσπίζει η σύμβαση 108. Στην υπό εξέταση πρόταση, οι διατάξεις για τον περιορισμό του σκοπού περιέχονται στα άρθρα 3 και 12. ωστόσο, το άρθρο 3 είναι υπερβολικά ευρύ και δεν καλύπτει έναν κατάλληλο περιορισμό των σκοπών για την αποθήκευση των δεδομένων, όπως απαιτεί το άρθρο 5 στ. β' της σύμβασης 108¹¹⁷. Παράλληλα, το εν λόγω άρθρο δεν προβλέπει και

¹¹⁵ C 139, σελ. 4, § 13.

¹¹⁶ C 139, σελ. 4-5, § § 18 και 19.

¹¹⁷ «Τα δεδομένα προσωπικού χαρακτήρα αποθηκεύονται για συγκεκριμένους και θεμιτούς σκοπούς και δεν χρησιμοποιούνται κατά τρόπο ασυμβίβαστο προς τους σκοπούς αυτούς».

παρεκκλίσεις σύμφωνα με το άρθρο 9 § 2 της σύμβασης 108¹¹⁸. Το άρθρο 12 καθορίζει μια ευρεία αλλά όχι σαφώς καθορισμένη σειρά παρεκκλίσεων από την αρχή του περιορισμού του σκοπού. Συγκεκριμένα το άρθρο δεν προβλέπει την προϋπόθεση να είναι οι παρεκκλίσεις αναγκαίες. Στην § 1 στοιχείο β' του άρθρου αυτού αναφέρεται ότι επιτρέπεται η επεξεργασία για «κάθε άλλον σκοπό» υπό την προϋπόθεση της συγκατάθεσης της αρμόδιας αρχής που διαβίβασε τα προσωπικά δεδομένα. Όμως, σε καμία περίπτωση η συγκατάθεση της διαβιβάζουσας αρχής δεν μπορεί να αντικαθιστά τη συγκατάθεση του υποκειμένου των δεδομένων. Συνεπώς, ο ΕΕΠΔ συνιστά στο νομοθέτη να αναδιατυπώσει τις σχετικές διατάξεις βάσει των ισχυόντων διεθνών κανόνων προστασίας δεδομένων¹¹⁹.

Παρόμοιες είναι και οι απόψεις του ΕΕΠΔ σχετικά με τις διαβιβάσεις προσωπικών δεδομένων σε τρίτες χώρες ή διεθνείς οργανισμούς. Συγκεκριμένα, ο ΕΕΠΔ θεωρεί ότι οι διατάξεις της πρότασης που αφορούν τις διαβιβάσεις αυτές δεν είναι κατάλληλες για την προστασία των δεδομένων προσωπικού χαρακτήρα και παράλληλα είναι δυσεφάρμοστες για τις αρχές επιβολής του νόμου, αφού αυτές δεν θα πρέπει να εξετάζουν μόνο την καταλληλότητα της τρίτης χώρας που ζητά τη διαβίβαση των δεδομένων, αλλά να λαμβάνουν υπόψη και το εάν τα άλλα κράτη μέλη που έχουν συνεισφέρει στο φάκελο, συγκατατίθενται μετά από δική του αξιολόγηση για την καταλληλότητα της συγκεκριμένης τρίτης χώρας. Γι' αυτό ο ΕΕΠΔ προτείνει να ακολουθούνται κοινά πρότυπα και να λαμβάνονται συντονισμένες αποφάσεις όσον αφορά την καταλληλότητα¹²⁰.

Επίσης, ο ΕΕΠΔ τονίζει πως ούτε η ποιότητα των δεδομένων ορίζεται κατάλληλα και επαρκώς στις διατάξεις της παρούσας πρότασης. Για την ακρίβεια αναφέρει πως υστερούν σε σχέση με το επίπεδο προστασίας που απαιτεί η σύμβαση 108, αφού δεν περιέχει διατάξεις σχετικά με τη διάκριση των διαφόρων κατηγοριών δεδομένων (ανάλογα, δηλαδή, με το βαθμό ακρίβειας και

¹¹⁸ «Παρέκλιση από τις διατάξεις των άρθρων... και 8 της παρούσας σύμβασης είναι δυνατή, όταν αυτή προβλέπεται από διάταξη νόμου του Συμβαλλόμενου Μέρους και αποτελεί απαραίτητο αναγκαίο μέτρο σε μια δημοκρατική κοινωνία:

α.... για την προστασία της ασφάλειας του Κράτους, τη δημόσιας ασφάλεια ή την καταστολή των ποινικών παραβάσεων.»

¹¹⁹ C 139, σελ. 5, § § 18 και 19.

¹²⁰ C139, σελ. 6, § 30.

αξιοπιστίας τους) και τη διάκριση των διαφορετικών κατηγοριών υποκειμένων των δεδομένων (δηλαδή, εγκληματίες, υπόπτους, θύματα, μάρτυρες κλπ). Οι διακρίσεις αυτές πρέπει να γίνονται όχι μόνο για την προστασία των προσωπικών δεδομένων του πολίτη, αλλά και να μπορούν οι παραλήπτες να κάνουν πλήρη και ορθή χρήση των δεδομένων που παραλαμβάνουν¹²¹.

Γενικά θα λέγαμε ότι ο ΕΕΠΔ δεν μένει ικανοποιημένος από την αναθεωρημένη αυτή πρόταση λόγω του χαμηλού επιπέδου προστασίας των δεδομένων και του μη ικανοποιητικού χαρακτήρα της νομοθετικής ποιότητας του κειμένου. Ειδικότερα, η πρόταση περιπλέκει περισσότερο την κατάσταση, διευρύνοντας την εφαρμογή της απόφασης πλαισίου στην Eurorol, Eurojust και το Τελωνειακό Σύστημα Πληροφοριών του τρίτου πυλώνα και προτείνοντας τη δημιουργία Κοινής Αρχής Ελέγχου βάσει ακατάλληλης νομικής πράξης. Ο Επόπτης φαίνεται να θεωρεί ότι δεν μπορεί να συσταθεί με απόφαση-πλαίσιο νέο όργανο αλλά μόνο να εναρμονιστούν οι εθνικές διατάξεις.

Για τους ανωτέρω λόγους, ο ΕΕΠΔ προτείνει να δοθεί προστιθέμενη αξία στις διατάξεις της σύμβασης 108, να τηρούνται οι αρχές του πρώτου πυλώνα και της σύστασης αριθ. R (87) 15 και τέλος να ρυθμισθούν όλα τα ζητήματα τα όποια επισημάνθηκαν στην παρούσα γνωμοδότηση αλλά και στις δύο προηγούμενες.

4. Γνωμοδότηση όσον αφορά το σχέδιο πρότασης απόφασης-πλαισίου του Συμβουλίου για τη χρήση των δεδομένων των καταστάσεων με τα ονόματα των επιβατών (PNR) με σκοπό την επιβολή του νόμου¹²².

Σύμφωνα με το άρθρο 28 § 2 του Κανονισμού 45/2001/ΕΚ¹²³, η Επιτροπή απέστειλε στον ΕΕΠΔ προς γνωμοδότηση το σχέδιο πρότασης απόφασης-πλαισίου του Συμβουλίου για τη χρήση των δεδομένων των καταστάσεων με τα ονόματα των επιβατών (PNR) με σκοπό την επιβολή του νόμου.

¹²¹ C 139, σελ. 7, § 32.

¹²² Βλ. ΕΕ 1.5. 2008 C 110, σελ. 1.

¹²³ «Η Επιτροπή, οσάκις εγκρίνει νομοθετική πρόταση σχετικά με την προστασία των δικαιωμάτων και των ελευθεριών των προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, συμβουλεύεται τον ευρωπαϊκό επόπτη προστασίας δεδομένων.»

Η πρόταση αυτή αφορά την επεξεργασία δεδομένων PNR εντός της Ε.Ε. και συνδέεται στενά με άλλα συστήματα συλλογής και χρήσης δεδομένων των επιβατών, ιδίως δε τη συμφωνία μεταξύ της Ε.Ε. και των Ηνωμένων Πολιτειών της Αμερικής του Ιουλίου του 2007. Πρόκειται δηλαδή για την πρόταση δημιουργίας ενός συστήματος PNR εντός του χώρου της Ε.Ε.

Στόχος της πρότασης είναι η εναρμόνιση των διατάξεων των κρατών μελών οι οποίες διέπουν τις υποχρεώσεις των αερομεταφορέων που εκτελούν πτήσεις από ή προς την επικράτεια ενός τουλάχιστον κράτους μέλους αναφορικά με τη διαβίβαση δεδομένων PNR στις αρμόδιες αρχές με σκοπό την πρόληψη και την καταπολέμηση των τρομοκρατικών εγκλημάτων και του οργανωμένου εγκλήματος. Η Ε.Ε. έχει συνάψει με τις ΗΠΑ καθώς και με τον Καναδά διευθετήσεις όσον αφορά τη διαβίβαση δεδομένων PNR για ανάλογους σκοπούς και αναμένεται να αρχίσουν διαπραγματεύσεις μεταξύ Ε.Ε. και Αυστραλίας.

Η εν λόγω πρόταση συμπληρώνει την οδηγία 82/2004/ΕΚ του Συμβουλίου σχετικά με την υποχρέωση των μεταφορέων να κοινοποιούν τα στοιχεία των επιβατών που είναι γνωστά ως δεδομένα API (Advanced Passenger Information) για να καταπολεμηθεί η παράνομη μετανάστευση και να βελτιωθεί ο συνοριακός έλεγχος.

Αντίθετα με τα δεδομένα API που υποτίθεται ότι διευκολύνουν τον εντοπισμό φυσικών προσώπων, τα δεδομένα PNR που αναφέρονται στην πρόταση θα συνέβαλλαν στη διενέργεια εκτιμήσεων επικινδυνότητας για πρόσωπα, στην απόκτηση απορρήτων πληροφοριών και στην πραγματοποίηση συσχετισμών μεταξύ γνωστών και αγνώστων ατόμων¹²⁴.

Ο ΕΕΠΔ σημειώνει ότι για την πρόταση αυτή έχουν υποβάλλει κοινή γνωμοδότηση η Ομάδα του άρθρου 29 (βλ. ανωτέρω υπό 2.4.3) και η Ομάδα «Αστυνομία και Δικαιοσύνη». Με τη γνωμοδότηση αυτή ο ΕΕΠΔ συμφωνεί.

Στην γνωμοδότηση αυτή, τον ΕΕΠΔ θα απασχολήσουν τέσσερα κύρια ζητήματα¹²⁵:

¹²⁴ C 110, σελ. 2, § 6.

¹²⁵ C 110, σελ. 2, § 10 και Ετήσια Έκθεση 2007, σελ. 51.

1. Η νομιμότητα των προβλεπόμενων μέτρων, το ζήτημα του σκοπού, της αναγκαιότητας και της αναλογικότητας της πρότασης θα εκτιμηθούν σύμφωνα με τα κριτήρια του άρθρου 8 του Χάρτη Θεμελιωδών Δικαιωμάτων της Ε.Ε, καθώς και των άρθρων 5 και 8 της σύμβασης αριθ. 108 του Συμβουλίου της Ευρώπης.
2. Το κατά πόσο δίκαιη είναι η προτεινόμενη πράξη επεξεργασίας και ο αντίκτυπος του εφαρμοστέου καθεστώτος προστασίας δεδομένων στην άσκηση των δικαιωμάτων του προσώπου που αφορούν τα δεδομένα.
3. Η ιδιότητα των παραληπτών δεδομένων σε εθνικό επίπεδο. Ιδιαίτερες ανησυχίες προκύπτουν για την ιδιότητα των PIU (μονάδα στοιχείων επιβατών σε κάθε κράτος μέλος, υπεύθυνη για τη συλλογή δεδομένων PNR από τους αερομεταφορείς), των ενδιαμέσων και των αρμοδίων αρχών που αναλαμβάνουν να εκτιμήσουν την επικινδυνότητα των επιβατών.
4. Οι προϋποθέσεις της διαβίβασης δεδομένων προς τρίτες χώρες.

Ως προς το θεμιτό χαρακτήρα των προτεινόμενων μέτρων, ο ΕΕΠΔ καταλήγει στο συμπέρασμα ότι η πρόταση βασίζεται σε διάφορες βάσεις δεδομένων χωρίς συνολική εκτίμηση των απτών αποτελεσμάτων και ελλείψεών τους. Αυτό είναι αντίθετο με μια ορθολογική νομοθετική πολιτική στο πλαίσιο της οποίας δεν πρέπει να θεσπίζονται νέες πράξεις πριν εφαρμοσθούν πλήρως οι υφιστάμενες και αποδειχθούν ανεπαρκείς. Αυτό άλλωστε, θα μπορούσε και να οδηγήσει σε μια κοινωνία γενικευμένης επιτήρησης.

Από τη μία πλευρά, λοιπόν, η καταπολέμηση της τρομοκρατίας μπορεί ασφαλώς να αποτελέσει θεμιτό λόγο για την εφαρμογή εξαιρέσεων από τα θεμελιώδη δικαιώματα του σεβασμού της ιδιωτικής ζωής και της προστασίας των δεδομένων, από την άλλη όμως, για να μπορεί να γίνει δεκτή μια τέτοια παραβίαση της ιδιωτικής ζωής, πρέπει να στηρίζεται σε σαφή και αναντίρρητα

στοιχεία, ενώ πρέπει να αποδεικνύεται και η αναλογικότητα της επεξεργασίας¹²⁶.

Η τήρηση της αρχής της αναλογικότητας σημαίνει όχι μόνο ότι το προτεινόμενο μέτρο πρέπει να είναι αποτελεσματικό, αλλά και ότι ο σκοπός που επιδιώκεται με την πρόταση δεν είναι δυνατόν να επιτευχθεί με μέσα που παραβιάζουν λιγότερο την ιδιωτική ζωή. Κατά τον ΕΕΠΔ, δεν διενεργήθηκε στην παρούσα πρόταση μια συνολική εκτίμηση για την ύπαρξη εναλλακτικών λύσεων πριν τεθούν σε εφαρμογή νέα μέτρα για την επεξεργασία πληροφοριών προσωπικού χαρακτήρα¹²⁷.

Δυστυχώς, όμως, ο ΕΕΠΔ, διαπιστώνει ότι η συγκεκριμένη πρόταση δεν περιλαμβάνει τα απαραίτητα στοιχεία αιτιολόγησης και δεν πληρούνται τα κριτήρια της αναγκαιότητας και της αναλογικότητας. Τα δύο αυτά κριτήρια αποτελούν προϋπόθεση για να τεθεί σε ισχύ η εν λόγω πρόταση.

Αναφορικά με το δεύτερο ζήτημα, ο ΕΕΠΔ φρονεί ότι πρέπει να αποσαφηνισθεί στην πρόταση ποιο νομικό καθεστώς έχει εφαρμογή σε κάθε στάδιο της επεξεργασίας και να διευκρινισθεί ενώπιον ποιου φορέα ή αρχής ασκείται το δικαίωμα πρόσβασης ή διόρθωσης. Και πάλι ο ΕΕΠΔ υπενθυμίζει ότι σύμφωνα με το άρθρο 30 § 1 στοιχείο β' της ΣυνθΕΕ, οι διατάξεις θα πρέπει να είναι κατάλληλες και να καλύπτουν όλο το φάσμα των επεξεργασιών που προβλέπει η πρόταση. Εκφράζει δε τη λύπη του για την αβεβαιότητα που υπάρχει εντός της πρότασης όσον αφορά την άσκηση των θεμελιωδών δικαιωμάτων του προσώπου στο οποίο αναφέρονται τα δεδομένα. Αυτό συμβαίνει συνήθως, λόγω του ότι τα στοιχεία επεξεργάζονται ενδιάμεσοι φορείς με ασαφές νομικό καθεστώς και έτσι ο ενδιαφερόμενος κινδυνεύει να βρεθεί ενώπιον διαφόρων παραληπτών δεδομένων. Και το ερώτημα που τίθεται είναι: ενώπιον ποιού κράτους μέλους θα ασκήσει τα δικαιώματά του; Εφαρμογή θα έχουν οι εθνικοί κανόνες προστασίας δεδομένων ή θα πρέπει να ληφθεί υπόψη κάποια ειδική κατασταλτική νομοθεσία¹²⁸;

¹²⁶ Βλ. σχετικά Peter Hustinx, “Can we put limits on the freedom of movement and intervene in peoples private lives in the fight against serious threats?”, 6th Parliamentary Colloquy Paris-Berlin: “Collective security and individual liberties”, Lyon, 4 April 2008.

¹²⁷ C 110., σελ. 5, § 31.

¹²⁸ C 110., σελ. 8 και 9, § 64-67.

Ως προς το ζήτημα της ιδιότητας των παραληπτών, ο ΕΕΠΔ σημειώνει ότι η πρόταση δεν προβλέπει τίποτα συγκεκριμένο σχετικά με την ιδιότητα των παραληπτών των δεδομένων προσωπικού χαρακτήρα που συλλέγονται από τις αεροπορικές εταιρείες, είτε πρόκειται για ενδιάμεσους φορείς, είτε για μονάδες στοιχείων επιβατών (PIU), είτε για αρμόδιες αρχές. Η ιδιότητα του παραλήπτη σχετίζεται άμεσα με τις εγγυήσεις προστασίας δεδομένων που ισχύουν για το συγκεκριμένο παραλήπτη.

Γενικά, ο ΕΕΠΔ παρατηρεί ότι η επιβολή συστήματος PNR της Ε.Ε. δυσχεραίνεται περισσότερο επειδή οι αρχές επιβολής του νόμου έχουν διαφορετικές αρμοδιότητες ανάλογα με το εθνικό δίκαιο κάθε κράτους μέλους. Για το λόγο αυτό ο ΕΕΠΔ συνιστά να γίνει η πρόταση σαφέστερη όσον αφορά την ιδιότητα των αναφερομένων φορέων και τις εγγυήσεις που προβλέπονται για τον έλεγχο άσκησης των αρμοδιοτήτων τους. Ειδικότερα, θα πρέπει να προστεθούν, κατά την άποψή του, διατάξεις στις οποίες θα ορίζονται περιοριστικά οι αρμοδιότητες και οι νομικές υποχρεώσεις των ενδιάμεσων φορέων, PIU και των άλλων αρμοδίων αρχών.

Τέλος, σχετικά με τις προϋποθέσεις διαβίβασης των δεδομένων PNR σε τρίτες χώρες, η πρόταση προβλέπει κάποιες διασφαλίσεις (άρθρο 8 της πρότασης). Προβλέπει ρητά την εφαρμογή της απόφασης-πλαισίου για την προστασία των δεδομένων στις διαβιβάσεις, εισάγει περιορισμό ειδικού σκοπού και ορίζει ότι απαιτείται η συναίνεση του κράτους μέλους σε περίπτωση περαιτέρω διαβίβασης. Παράλληλα, η διαβίβαση θα πρέπει να είναι σύμφωνη με το εθνικό δίκαιο του συγκεκριμένου κράτους μέλους. Ωστόσο, εκκρεμούν πολλά θέματα όπως π.χ. από ποιόν και υπό ποιες προϋποθέσεις θα παρέχεται η συναίνεση αυτή. Ο ΕΕΠΔ επ' αυτού κρίνει ότι ο τρόπος παροχής της συναίνεσης θα πρέπει τουλάχιστον να είναι σύμφωνος με το εθνικό δίκαιο και το τρίτο κράτος να εξασφαλίζει ένα κατάλληλο επίπεδο προστασίας από την παραλήπτρια χώρα για τη σχεδιαζόμενη επεξεργασία.

Επιπλέον, αναφορικά με την εφαρμογή της απόφασης-πλαισίου για την προστασία των δεδομένων, ο ΕΕΠΔ φρονεί πως πρέπει να αναφέρεται ρητώς στο διατακτικό της πρότασης ότι οι σαφέστερες εγγυήσεις της πρότασης

υπερέχουν των γενικών προϋποθέσεων και εξαιρέσεων της απόφασης-πλαισίου για την προστασία των δεδομένων.

Παρατηρούμε, λοιπόν, ότι και στην συγκεκριμένη γνωμοδότηση, ο ΕΕΠΔ προβάλλει αντιρρήσεις επί των αρχών και δεν κάνει απλή εφαρμογή του δικαίου, αλλά η γνώμη του έχει ευρύτερες πολιτικές επιπτώσεις, ιδιαιτέρως όσον αφορά την τήρηση της αρχής της αναλογικότητας και της αναγκαιότητας της επεξεργασίας και την απαίτηση περισσότερων εγγυήσεων για την όσο το δυνατόν καλύτερη προστασία των θεμελιωδών δικαιωμάτων του προσώπου στο οποίο αφορούν τα δεδομένα.

5. Γνωμοδότηση όσον αφορά την εφαρμογή ενός πολυετούς κοινοτικού προγράμματος για την προστασία των παιδιών κατά τη χρήση του διαδικτύου και άλλων επικοινωνιακών τεχνολογιών¹²⁹.

Η υπό κρίση πρόταση του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου στάλθηκε από την Επιτροπή στον ΕΕΠΔ για γνωμοδότηση στις 4.3.2008, βάσει του άρθρου 28 § 2 του Κανονισμού 45/2001. Το εν λόγω πρόγραμμα επικεντρώνεται περισσότερο στην δράση για την προστασία των παιδιών κατά τη χρήση νέων τεχνολογιών παρά στη λήψη ρυθμιστικών μέτρων. Στόχοι του είναι η μείωση του παράνομου και επιβλαβούς περιεχομένου των διαδικτυακών τόπων, η προώθηση ενός ασφαλέστερου διαδικτυακού περιβάλλοντος και η ενημέρωση του κοινού.

Καταρχήν, ο ΕΕΠΔ θεωρεί πως η πρόταση πρέπει να κινηθεί εντός των νομικού πλαισίου που έχουν χαράξει η οδηγία 200/31/EK για το ηλεκτρονικό εμπόριο, η οδηγία 2002/58/EK για το ηλεκτρονικό απόρρητο και η οδηγία 95/46/EK για την προστασία των προσωπικών δεδομένων.

Τα βασικά ζητήματα που απασχόλησαν τον ΕΕΠΔ σχετικά με την πρόταση αυτή είναι:

- Η σχέση της προστασίας των προσωπικών δεδομένων και της ασφάλειας των παιδιών, με σκεπτικό ότι η προστασία των

¹²⁹ Βλ. ΕΕ 7.1. 2009 C 2, σελ. 2.

δεδομένων των παιδιών είναι ένα απαραίτητο πρώτο βήμα για την πρόληψη της εκμετάλλευσής τους.

- Η επεξεργασία των προσωπικών δεδομένων η οποία είναι σύμφυτη με την αναφορά, το φιλτράρισμα και τη διακοπή ύποπτων περιεχομένων και προσώπων εντός του διαδικτύου.
- Το ερώτημα κατά πόσον η αναφορά ύποπτων ατόμων ή γεγονότων παραβιάζουν τις διατάξεις για τα προσωπικά δεδομένα.
- Ο ρόλος των τεχνολογικών μέσων και εργαλείων.
- Η ευθύνη της βιομηχανίας του διαδικτύου σε σχέση με τον έλεγχο των χρηστών των δεδομένων.

Βασικό σημείο εκκίνησης είναι η διαπίστωση ότι υπάρχει ανάγκη προστασίας της αξιοπρέπειας, της ασφάλειας και του απορρήτου των δεδομένων των παιδιών κατά τη χρήση του διαδικτύου¹³⁰.

Άποψη του ΕΕΠΔ είναι ότι πρέπει να εντατικοποιηθεί η ενημέρωση των παιδιών σχετικά με τους κινδύνους που ελλοχεύουν από την κάθε είδους επικοινωνία που έχουν μέσω διαδικτύου και την αυθαίρετη χρήση των προσωπικών τους στοιχείων, όπως είναι το πραγματικό τους όνομα, ηλικία και ο τόπος κατοικίας. Η ανίχνευση της παιδικής δραστηριότητας από άλλους χρήστες, μπορεί οδηγήσει τους ανήλικους σε εγκληματικές δραστηριότητες. Υπάρχει ο κίνδυνος του δολοφονικού τους από επιτήδειους χρήστες με σκοπό τη σεξουαλική τους παρενόχληση και γενικά το ρίσκο να προβούν σε διάφορων ειδών παράνομες ενέργειες¹³¹.

Για την αποφυγή των κινδύνων αυτών και την προστασία της παιδικής ηλικίας, η παρούσα πρόταση προτείνει τη διαγραφή των στοιχείων που καταγράφονται στους διάφορους διαδικτυακούς τόπους ανά τακτά χρονικά διαστήματα καθώς και τη συχνή ενημέρωση τόσο των ανήλικων χρηστών, όσο και των γονέων και των εκπαιδευτικών. Αυτό μπορεί να επιτευχθεί με την διασπορά κατάλληλων πληροφοριών και τη πρόβλεψη online επαφής ώστε γονείς και τέκνα να μπορούν να υποβάλλουν ερωτήματα και να λάβουν

¹³⁰ Βλ. σχετικά την διακήρυξη του Υπουργικού Συμβουλίου της Ε.Ε. στις 20.2.2008.

¹³¹ C 2, σελ. 3, § 11-12.

απαντήσεις σχετικά με το πώς μπορούν να προστατευθούν τα προσωπικά δεδομένα των ανηλίκων¹³².

Ο ΕΕΠΔ τονίζει ότι προς αυτή την κατεύθυνση πρέπει να κινηθούν όλες οι αρχές προστασίας δεδομένων και να υπάρξει ομαλή συνεργασία, ανταλλαγή πληροφοριών και εμπειρίας τόσο σε εθνικό, όσο και σε Ευρωπαϊκό επίπεδο.

Από την άλλη πλευρά, όμως, ο ΕΕΠΔ επισημαίνει ότι ναι μεν η προστασία των παιδικών προσωπικών δεδομένων είναι αναμφισβήτητο το κύριο ζητούμενο, δεν πρέπει όμως να παραβλέπουμε το γεγονός ότι η προστασία των παιδιών συμβαίνει σ' ένα περιβάλλον που μπορεί να διακυβεύονται τα δικαιώματα άλλων ατόμων. Επομένως, κάθε είδους παρακολούθηση θα πρέπει να πραγματοποιείται με απόλυτο σεβασμό στα ανθρώπινα δικαιώματα όλων όσων εμπλέκονται στο διαδίκτυο.

Παράλληλα, θα πρέπει κάθε σύστημα αναφοράς, το οποίο ενημερώνει για την ύπαρξη παράνομου ή επικίνδυνου δικτυακού περιεχομένου, να λαμβάνει υπόψη του το υπάρχον νομικό πλαίσιο προστασίας των προσωπικών δεδομένων. Κάθε επεξεργασία, λοιπόν, που αφορά άτομα που κρίνονται ύποπτα για παράνομη συμπεριφορά ή για προώθηση παράνομου υλικού στο διαδίκτυο, καθώς και τα στοιχεία των θυμάτων δικτυακής εκμετάλλευσης, πρέπει να γίνεται με βάση τις αρχές για την προστασία των ευαίσθητων δεδομένων¹³³.

Τέλος, ο ΕΕΠΔ επισημαίνει ότι και τα συστήματα φιλτραρίσματος ή απαγόρευσης πρόσβασης στα δίκτυα, θα πρέπει να χρησιμοποιούνται με επιφύλαξη, έχοντας πάντα υπόψη το ενδεχόμενο να προκαλέσουν τα αντίθετα αποτελέσματα, όπως για παράδειγμα, να αποτρέψουν την πρόσβαση σε απολύτως νόμιμες πληροφορίες¹³⁴. Παράλληλα κρίνει πως οι επιλογές που κάνει η πρόταση για την προστασία των παιδιών, δεν πρέπει να επηρεάζουν το δικαίωμα της ελεύθερης έκφρασης και να αποτρέπουν το χρήστη από την απόλαυση των ευκαιριών που του προσφέρουν οι νέες τεχνολογίες, όπως είναι η ελεύθερη πρόσβαση στη γνώση, η ανταλλαγή πολιτιστικών πληροφοριών και γενικά η συμμετοχή στην κοινωνία της πληροφορίας.

¹³² C 2, σελ. 3, § 14.

¹³³ Βλ. άρθρο 8 της οδηγίας 95/46/EK.

¹³⁴ C 2, σελ. 5, § 25.

Καταλήγει, επομένως, ο ΕΕΠΔ στο συμπέρασμα ότι πρέπει να βρεθεί μια ισορροπία μεταξύ της μάχης για την καταπολέμηση των παράνομων δικτυακών περιεχομένων και την καταλληλότητα των μέτρων που θα ληφθούν για την προστασία της παιδικής ηλικίας, ώστε να μην θίγονται τα θεμελιώδη δικαιώματα όλων όσων χρησιμοποιούν το διαδίκτυο.

Και στην υπόθεση αυτή είναι εμφανής ο ρόλος του Επόπτη ως εποπτικού οργάνου το οποίο ελέγχει την προστασία θεμελιωδών δικαιωμάτων (συνταγματικός ρόλος) και το οποίο συγχρόνως θέτει κατευθυντήριες γραμμές και κριτήρια για τον τρόπο εξισορρόπησης και στάθμισης μεταξύ διαφορετικών θεμελιωδών δικαιωμάτων.

ΕΠΙΛΟΓΟΣ

Στην παρούσα διπλωματική εργασία έγινε μια προσπάθεια να εστιάσουμε στη νεοσυσταθείσα αρχή που ονομάζεται Ευρωπαϊός Επόπτης Προστασίας Δεδομένων και εποπτεύει από το 2004 έως σήμερα, κατά τρόπο ανεξάρτητο, τα όργανα και τους οργανισμούς της Ευρωπαϊκής Κοινότητας. Ο Ευρωπαϊός Επόπτης αναλύθηκε ως ένα νέο θεσμικό φαινόμενο στα πλαίσια της Ε.Ε.

Όπως προαναφέρθηκε, ο ΕΕΠΔ έχει τέσσερα βασικά χαρακτηριστικά: προσωποποιεί την προστασία των προσωπικών δεδομένων, απολαύει ανεξαρτησίας, διαθέτει τεχνική εμπειρία και έχει εξοπλιστεί με σειρά εξουσιών. Αυτό καταδεικνύει πως ο ΕΕΠΔ εκπληρώνει διάφορες λειτουργίες (με κύρια αυτή της εποπτικής αρχής), οι οποίες οδηγούν όλες σε έναν κοινό στόχο: την προστασία των προσωπικών δεδομένων.

Όσον αφορά την επιτυχία του θεσμού αυτού στον τομέα αυτό, θα λέγαμε ότι αυτή κρίνεται από την αποτελεσματικότητά του κατά την εκτέλεση της αποστολής του. Κατά την άποψη του Β. Σωτηρόπουλου: «Η επιτυχία των ανεξαρτήτων αρχών κρίνεται βάσει της κατάκτησης της εμπιστοσύνης των πολιτών»¹³⁵.

Είναι γεγονός ότι τόσο ο Ευρωπαϊός Διαμεσολαβητής, όσο και ο Ευρωπαϊός Επόπτης, είναι εντεταλμένοι για την εύρυθμη λειτουργία των

¹³⁵ Βασίλης Σωτηρόπουλος, «Ο Ευρωπαϊός Επόπτης Προστασίας Δεδομένων», *Δικαιώματα του Ανθρώπου Νο 36/2007*, σελ. 1201.

οργάνων κατά την επαφή τους με τους πολίτες της Ε.Ε. Επομένως, θεωρούμε πως η αποτελεσματικότητα του ΕΕΠΔ θα κριθεί τελικά με γνώμονα το κατά πόσον ο θεσμός αυτός θα λειτουργήσει ως ένα ταχύ και αποτελεσματικό μέσο επίλυσης υποθέσεων χωρίς να χρειάζεται να επιληφθούν τα κοινοτικά δικαστήρια. Αυτό θα φανεί και από το κατά πόσον οι πολίτες θα αποφύγουν την απευθείας προσφυγή στα δικαστικά όργανα και θα προτιμήσουν να προσφύγουν ενώπιον του ΕΕΠΔ, υπολογίζοντας στην αμεσότητα της προστασίας της οποίας θα τύχουν. Αν, λοιπόν, τα στατιστικά στοιχεία, μέσα και από τις ετήσιες εκθέσεις του αποδεικνύουν κάτι τέτοιο, τότε θα μπορούμε να μιλάμε για επιτυχία του εν λόγω θεσμού.

Προς αυτήν την κατεύθυνση κινείται και ο ίδιος ο Επόπτης όταν σε κάποιο άρθρο του αναφέρει ότι: «...πρέπει να ασχοληθούμε με το ερώτημα αν υπάρχουν κάποιοι τομείς όπου ο τρέχων ρόλος των αρχών προστασίας δεδομένων μπορεί να υποβληθεί σε βελτίωση ώστε να γίνει η δράση τους πιο αποτελεσματική...και κατά πόσο οι κανόνες και οι αρχές για την προστασία των προσωπικών δεδομένων μπορούν να γίνουν πραγματικότητα»¹³⁶.

Κατά την προσωπική μου άποψη, για να πετύχει ο ΕΕΠΔ το στόχο του και να βελτιώσει το επίπεδο προστασίας των προσωπικών δεδομένων, θα πρέπει να αναβαθμίσει τη δράση του παρέχοντας στον πολίτη ευέλικτες και απλές διαδικασίες προσφυγής και να εξασφαλίσει την καλύτερη δυνατή συνεργασία του τόσο με τις εθνικές αρχές προστασίας δεδομένων, όσο και με τους υπευθύνους επεξεργασίας προσωπικών δεδομένων που δρουν εντός των οργάνων και των οργανισμών της ΕΚ. Παράλληλα, θα πρέπει να δημιουργήσει ένα κλίμα εμπιστοσύνης στον πολίτη, μέσω της διαφάνειας των διαδικασιών που και ο ίδιος, άλλωστε, πρεσβεύει στις γνωμοδοτήσεις του. Με τον τρόπο αυτό θα καταφέρει να αποκτήσει αξιοπιστία στον ευρωπαϊκό χώρο και να αναχθεί σε κύριο όργανο προστασίας των προσωπικών δεδομένων.

Παράλληλα, μέσα από τις αναλυθείσες γνωμοδοτήσεις προκύπτει ότι ο Επόπτης ασκεί συγχρόνως μια αξιοσημείωτη θεσμική λειτουργία εφόσον παρεμβαίνει άμεσα στη νομοθετική λειτουργία και παίρνει θέση στο εάν μια

¹³⁶ Hustinx, P., "The Role of Data Protection Authorities", www.edps.europa.eu, Publications / Speeches & Articles, 23.12.2008, σελ.7.

συγκεκριμένη νομοθετική πρόταση πρέπει να υιοθετηθεί ή όχι και υπό ποιους όρους. Επιπλέον, εκπληρώνει εμμέσως και μια κανονιστική λειτουργία, δεδομένου ότι εισάγει κριτήρια, όρους και κατευθύνσεις σε ό,τι αφορά τους θεμιτούς τρόπους επεξεργασίας δεδομένων προς χρήση από τον κοινοτικό νομοθέτη.

Συμπερασματικά, πρόκειται για ένα εποπτικό όργανο που καλείται να συμβάλει στην πράξη, τόσο στην αποτελεσματική προστασία των ατομικών δικαιωμάτων, όσο και στην ανάπτυξη της πολιτικής προστασίας των ανθρωπίνων δικαιωμάτων εκ μέρους των οργάνων της Ένωσης. Αυτό σημαίνει πως ο Ευρωπαίος Επόπτης αφενός μεν προστατεύει τα ατομικά δικαιώματα θέτοντας όρια στη δράση του κοινοτικού νομοθέτη, αφετέρου δε, καλείται να κατευθύνει το έργο του νομοθέτη προς την κατεύθυνση της ενεργητικής προστασίας της ιδιωτικής ζωής στην κοινωνία της πληροφορίας.

ΒΙΒΛΙΟΓΡΑΦΙΑ

A. Ελληνική

- **Αραβαντινός Βασίλης**, *Η προστασία των στοιχείων προσωπικού χαρακτήρα από την αθέμιτη επεξεργασία τους με ηλεκτρονικό υπολογιστή*, Αθήνα- Κομοτηνή, 1997, εκδόσεις Σάκκουλα.
- **Ιγγλεζάκης Ι.**, *Ευαίσθητα Προσωπικά Δεδομένα*, Αθήνα-Θεσ/κη, 2003, Εκδόσεις Σάκκουλα.
- **Ιγγλεζάκης Ι.**, *Δίκαιο της Πληροφορικής*, β' έκδοση, Αθήνα- Θεσ/νίκη 2008, εκδόσεις Σάκκουλα.
- **Μήτρου Λίλιαν**, *Το δίκαιο στην Κοινωνία της Πληροφορίας*, Αθήνα-Θεσ/νίκη 2002, εκδόσεις Σάκκουλα.
- **Σιδηρόπουλος Θ.**, *Το δίκαιο του διαδικτύου*, β' έκδοση, Αθήνα-Θεσ/κη, 2008, εκδόσεις Σάκκουλα.
- **Σωτηρόπουλος Βασίλης**, *Η συνταγματική προστασία των προσωπικών δεδομένων*, Αθήνα-Θεσ/κη 2006, εκδόσεις Σάκκουλα.
- **Σωτηρόπουλος Βασίλης**, «Ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων», *Δικαιώματα του Ανθρώπου Νο 36/2007*, σελ.1173-1203.
- **Σωτηρόπουλος Βασίλης**, *Περαιτέρω Χρήση Πληροφοριών του Δημοσίου Τομέα*, Αθήνα- Θεσ/νίκη 2007, εκδόσεις Σάκκουλα.

B. Ξενόγλωσση

- **Chalton Simon/ Gaskill Shelagh, Sterling J. A. L.**, *Encyclopedia of data Protection*, London, 1988-1997, Sweet & Maxwell.
- **Delgado J. Bayo**, Interview published in "Hablemos de Europa", No 7, Δεκέμβριος 2008.
- **Hijmans Hielke**, "The European Data Protection Supervisor: The institutions of the EC controlled by an independent authority", *Common Market Law Review* 43, p. 1313-1342, 2006.

- **Hustinx, P.**, “All data breaches must be made public”, published in ZDNet.co.uk, 29.01.2009.
- **Hustinx, P.**, “The Role of Data Protection Authorities”, www.edps.europa.eu , Publications / Speeches & Articles, 23.12.2008.
- **Hustinx P.**, “Can we put limits on the freedom of movement and intervene in peoples private lives in the fight against serious threats?”, 6th Parliamentary Colloquium Paris-Berlin: “Collective security and individual liberties”, Lyon, 4 April 2008.
- **Hustinx P.**, “Perspectives of Independent Authorities: independence and more effectiveness”, λόγος που εκφωνήθηκε στις 2 Απριλίου 2007 στο διήμερο νομικό συμπόσιο στο Μέγαρο Μουσικής Αθηνών με θέμα: «Οι ανεξάρτητες αρχές στη σύγχρονη δημοκρατία», www.edps.europa.eu.
- **Rosemary Jay- Angus Hamilton**, *Data Protection-Law and Practice*, London 1999, Sweet & Maxwell Publications.

Γ. Νομοθετικά Κείμενα και Εκθέσεις

- Κανονισμός 45/2001/EK
- Οδηγία 95/46/EK
- Σύμβαση 108 του Συμβουλίου της Ευρώπης 1981
- Χάρτης Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης
- Report of the Committee on Privacy 1971
- Ετήσιες Εκθέσεις ΕΕΠΔ 2004-2007

Δ. Δικτυακοί τόποι

- www.edps.europa.eu
- www.europa.eu
- www.eur-lex.europa.eu

ΠΑΡΑΡΤΗΜΑΤΑ

- ΚΑΝΟΝΙΣΜΟΣ 45/2001/ΕΚ
- ΓΝΩΜΟΔΟΤΗΣΕΙΣ ΕΥΡΩΠΑΙΟΥ ΕΠΟΠΤΗ

I

(Πράξεις για την ισχύ των οποίων απαιτείται δημοσίευση)

**ΚΑΝΟΝΙΣΜΟΣ (ΕΚ) αριθ. 45/2001 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ
της 18ης Δεκεμβρίου 2000**

σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα όργανα και τους οργανισμούς της Κοινότητας και σχετικά με την ελεύθερη κυκλοφορία των δεδομένων αυτών

ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ ΚΑΙ ΤΟ ΣΥΜΒΟΥΛΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ,

Έχοντας υπόψη:

τη συνθήκη για την ίδρυση της Ευρωπαϊκής Κοινότητας, και ιδίως το άρθρο 286,

την πρόταση της Επιτροπής ⁽¹⁾,

τη γνώμη της Οικονομικής και Κοινωνικής Επιτροπής ⁽²⁾,

Αποφασίζοντας σύμφωνα με τη διαδικασία του άρθρου 251 της συνθήκης ⁽³⁾,

Εκτιμώντας τα ακόλουθα:

- (1) Το άρθρο 286 της συνθήκης ορίζει ότι, οι κοινοτικές πράξεις για την προστασία των φυσικών προσώπων όσον αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα και την ελεύθερη κυκλοφορία αυτών, εφαρμόζονται στα όργανα και τους οργανισμούς της Κοινότητας.
- (2) Ένα πλήρες σύστημα προστασίας των δεδομένων προσωπικού χαρακτήρα απαιτεί όχι μόνο την παροχή δικαιωμάτων στα υποκείμενα των δεδομένων και την επιβολή υποχρεώσεων στους φορείς που επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα, αλλά και την πρόβλεψη κατάλληλων κυρώσεων για τους παραβάτες καθώς και μιας ανεξάρτητης εποπτικής αρχής.
- (3) Το άρθρο 286, παράγραφος 2 της συνθήκης προβλέπει τη σύσταση ανεξάρτητου εποπτικού οργάνου, επιφορτισμένου με την παρακολούθηση της εφαρμογής των εν λόγω κοινοτικών πράξεων στα όργανα και τους οργανισμούς της Κοινότητας.
- (4) Το άρθρο 286 παράγραφος 2 της συνθήκης προβλέπει, εξάλλου, τη θέσπιση κάθε άλλης χρήσιμης διάταξης, ανάλογα με την περίπτωση.
- (5) Εν προκειμένω, απαιτείται ένας κανονισμός προκειμένου να δοθούν στα πρόσωπα νομικώς προστατευόμενα δικαιώματα, να καθορισθούν οι υποχρεώσεις των υπευθύνων επεξεργα-

σίας δεδομένων στο πλαίσιο των οργάνων και οργανισμών της Κοινότητας, και να συσταθεί μια ανεξάρτητη εποπτική αρχή, υπεύθυνη για την εποπτεία της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα όργανα και τους οργανισμούς της Κοινότητας.

- (6) Ζητήθηκε η γνώμη της ομάδας προστασίας των προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, η οποία έχει συσταθεί δυνάμει του άρθρου 29 της οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Οκτωβρίου 1995, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών ⁽⁴⁾.
- (7) Τα πρόσωπα που μπορούν να προστατεύονται είναι εκείνα των οποίων δεδομένα προσωπικού χαρακτήρα επεξεργάζονται τα όργανα ή οι οργανισμοί της Κοινότητας σε οιοδήποτε πλαίσιο, παραδείγματος χάριν, διότι τα πρόσωπα αυτά απασχολούνται από αυτά τα όργανα ή τους οργανισμούς.
- (8) Οι αρχές της προστασίας των δεδομένων θα πρέπει να ισχύουν για όλες τις πληροφορίες που αφορούν ένα πρόσωπο του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί για να κριθεί κατά πόσον είναι δυνατή η εξακρίβωση της ταυτότητας ενός προσώπου, είναι σκόπιμο να λαμβάνονται υπόψη όλα τα μέσα που είναι δυνατό να χρησιμοποιήσει ευλόγως ο υπεύθυνος της επεξεργασίας ή οποιοδήποτε άλλο πρόσωπο για να εξακριβώσει την ταυτότητα του εν λόγω προσώπου οι αρχές της προστασίας δεν θα πρέπει να ισχύουν για τα δεδομένα τα οποία έχουν καταστεί επαρκώς ανώνυμα ώστε να μην είναι πλέον δυνατή η εξακρίβωση της ταυτότητας του υποκειμένου των δεδομένων.
- (9) Η οδηγία 95/46/ΕΚ επιβάλλει στα κράτη μέλη να εξασφαλίζουν την προστασία των θεμελιωδών δικαιωμάτων και ελευθεριών των φυσικών προσώπων, και ιδίως της ιδιωτικής τους ζωής, έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, ούτως ώστε να εξασφαλίζεται η ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα στην Κοινότητα.

⁽¹⁾ ΕΕ C 376 Ε της 28.12.1999, σ. 24.

⁽²⁾ ΕΕ C 51 της 23.2.2000, σ. 48.

⁽³⁾ Γνώμη του Ευρωπαϊκού Κοινοβουλίου της 14ης Νοεμβρίου 2000 και απόφαση του Συμβουλίου της 30ής Νοεμβρίου 2000.

⁽⁴⁾ ΕΕ L 281 της 23.11.1995, σ. 31.

- (10) Η οδηγία 97/66/EK του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 15ης Δεκεμβρίου 1997, περί επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και προστασίας της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα ⁽¹⁾, διευκρινίζει και συμπληρώνει την οδηγία 95/46/EK σε ό,τι αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα στον τομέα των τηλεπικοινωνιών.
- (11) Διάφορες άλλες κοινοτικές διατάξεις, ιδίως στον τομέα της αμοιβαίας συνδρομής μεταξύ των εθνικών διοικήσεων και της Επιτροπής, αποβλέπουν ομοίως στη διευκρίνιση και τη συμπλήρωση της οδηγίας 95/46/EK στους οικείους τομείς.
- (12) Είναι απαραίτητο να διασφαλιστεί στο σύνολο της Κοινότητας η συνεκτική και ομοιόμορφη εφαρμογή των κανόνων προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών των προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα.
- (13) Σκοπός είναι να διασφαλισθεί τόσο η ουσιαστική τήρηση των κανόνων προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών των προσώπων, όσο και η ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα μεταξύ των κρατών μελών και των οργάνων και οργανισμών της Κοινότητας, ή μεταξύ των οργάνων και οργανισμών της Κοινότητας, στο πλαίσιο της άσκησης των αντίστοιχων αρμοδιοτήτων τους.
- (14) Θα πρέπει, για το σκοπό αυτό, να θεσπισθούν αναγκαστικές διατάξεις όσον αφορά τα όργανα και τους οργανισμούς της Κοινότητας οι εν λόγω διατάξεις θα πρέπει να ισχύουν για κάθε είδους επεξεργασία δεδομένων προσωπικού χαρακτήρα την οποία διενεργούν όλα τα όργανα και όλοι οι οργανισμοί της Κοινότητας, στο μέτρο που η επεξεργασία αυτή εκτελείται για την άσκηση δραστηριοτήτων που εμπíπτουν, εν όλω ή εν μέρει, στο πεδίο εφαρμογής του κοινοτικού δικαίου.
- (15) Όταν η επεξεργασία αυτή διενεργείται από τα όργανα και τους οργανισμούς της Κοινότητας για την άσκηση δραστηριοτήτων που δεν εμπíπτουν στο πεδίο εφαρμογής του παρόντος κανονισμού, ιδίως εκείνων που προβλέπονται στους τίτλους V και VI της συνθήκης για την Ευρωπαϊκή Ένωση, η προστασία των θεμελιωδών δικαιωμάτων και ελευθεριών εξασφαλίζεται, τηρουμένου του άρθρου 6 της συνθήκης για την Ευρωπαϊκή Ένωση. Η πρόσβαση στα έγγραφα, συμπεριλαμβανομένων των όρων πρόσβασης στα έγγραφα που περιέχουν δεδομένα προσωπικού χαρακτήρα, διέπεται από τις ρυθμίσεις που έχουν θεσπιστεί δυνάμει του άρθρου 255 της συνθήκης ΕΚ το πεδίο εφαρμογής του οποίου εκτείνεται στους τίτλους V και VI της συνθήκης για την Ευρωπαϊκή Ένωση.
- (16) Οι διατάξεις αυτές δεν εφαρμόζονται σε φορείς που έχουν συσταθεί εκτός του κοινοτικού πλαισίου και ο ευρωπαίος επόπτης προστασίας δεδομένων δεν είναι αρμόδιος να παρακολουθεί την επεξεργασία δεδομένων προσωπικού χαρακτήρα από τους φορείς αυτούς.
- (17) Η αποτελεσματικότητα της προστασίας των προσώπων από την επεξεργασία δεδομένων προσωπικού χαρακτήρα μέσα στην Ένωση, προϋποθέτει τη συνεκτικότητα των κανόνων και των διαδικασιών που εφαρμόζονται ως προς το θέμα αυτό στις δραστηριότητες που υπάγονται σε διαφορετικά νομικά πλαίσια. Η εκπόνηση θεμελιωδών αρχών που αφορούν την προστασία των δεδομένων προσωπικού χαρακτήρα στον τομέα της δικαστικής συνεργασίας επί ποινικών υποθέσεων και της αστυνομικής και τελωνειακής συνεργασίας και η σύσταση μιας γραμματείας για τις κοινές εποπτικές αρχές, τις οποίες εισάγουν η σύμβαση Ευρωπαϊκή, η σύμβαση για τη χρήση της πληροφορικής στον τομέα των τελωνείων και η σύμβαση Σένγκεν, αποτελούν, προς τούτο, το πρώτο στάδιο.
- (18) Ο παρών κανονισμός δεν θα πρέπει να θίγει τα δικαιώματα και τις υποχρεώσεις των κρατών μελών βάσει των οδηγιών 95/46/EK και 97/66/EK και δεν αποσκοπεί στην τροποποίηση των πρακτικών και διαδικασιών οι οποίες έχουν καθιερωθεί νομίμως από τα κράτη μέλη στον τομέα της εθνικής ασφάλειας, της προάσπισης της τάξης καθώς και της πρόληψης, ανίχνευσης, έρευνας και δίωξης των αξιόποινων πράξεων, τηρουμένων των διατάξεων του πρωτοκόλλου περί προνομίων και ασυλιών των Ευρωπαϊκών Κοινοτήτων και του διεθνούς δικαίου.
- (19) Τα όργανα και οι οργανισμοί της Κοινότητας απευθύνονται στις αρμόδιες αρχές των κρατών μελών, όταν κρίνουν ότι πρέπει να πραγματοποιηθούν παρακολουθήσεις επικοινωνιών στα δίκτυα τηλεπικοινωνιών τους, σύμφωνα με τις ισχύουσες εθνικές διατάξεις.
- (20) Οι διατάξεις που εφαρμόζονται στα όργανα και τους οργανισμούς της Κοινότητας θα πρέπει να αντιστοιχούν προς εκείνες οι οποίες διέπουν την εναρμόνιση των εθνικών νομοθεσιών ή την εφαρμογή άλλων κοινοτικών πολιτικών, ιδίως στον τομέα της αμοιβαίας συνδρομής. Παρόλα αυτά, είναι δυνατόν να απαιτούνται διευκρινίσεις και συμπληρωματικές διατάξεις για την πραγμάτωση της προστασίας στην περίπτωση των επεξεργασιών δεδομένων προσωπικού χαρακτήρα που πραγματοποιούν τα όργανα και οι οργανισμοί της Κοινότητας.
- (21) Αυτό ισχύει εξίσου για τα δικαιώματα των προσώπων τα δεδομένα των οποίων υφίστανται επεξεργασία, για τις υποχρεώσεις των οργάνων και οργανισμών της Κοινότητας που είναι υπεύθυνα για την επεξεργασία, και για τις εξουσίες που ανατίθενται στην ανεξάρτητη εποπτική αρχή η οποία είναι επιφορτισμένη να μεριμνά για την προσήκουσα εφαρμογή του παρόντος κανονισμού.
- (22) Τα δικαιώματα που παρέχονται στο υποκείμενο των δεδομένων και η άσκηση των δικαιωμάτων αυτών δεν θα πρέπει να θίγουν τις υποχρεώσεις που επιβάλλονται στον υπεύθυνο της επεξεργασίας.
- (23) Η ανεξάρτητη εποπτική αρχή ασκεί τα εποπτικά της καθήκοντα σύμφωνα με τη συνθήκη και σεβόμενη τα ανθρώπινα δικαιώματα και τις θεμελιώδεις ελευθερίες. Διενεργεί τις έρευνές της τηρουμένου του πρωτοκόλλου περί προνομίων και ασυλιών και του κανονισμού υπηρεσιακής κατάστασης των υπαλλήλων των Ευρωπαϊκών Κοινοτήτων και του καθεστώτος που εφαρμόζεται στο λοιπό προσωπικό των Κοινοτήτων αυτών.
- (24) Θα πρέπει να ληφθούν τα τεχνικά μέτρα που απαιτούνται για να καταστεί δυνατή η πρόσβαση στα μητρώα επεξεργασίας που τηρούν οι υπεύθυνοι προστασίας δεδομένων μέσω της ανεξάρτητης εποπτικής αρχής.

⁽¹⁾ ΕΕ L 24 της 30.1.1998, σ. 1.

- (25) Οι αποφάσεις της ανεξάρτητης εποπτικής αρχής σχετικά με τις εξαιρέσεις, τις εγγυήσεις, τις άδειες και τους όρους που αφορούν τις επεξεργασίες δεδομένων, όπως ορίζονται στον παρόντα κανονισμό, θα πρέπει να δημοσιεύονται στην έκδοση πεπραγμένων. Ανεξάρτητα από την ετήσια δημοσίευση της έκθεσης πεπραγμένων, η ανεξάρτητη εποπτική αρχή μπορεί να δημοσιεύει εκδόσεις για ειδικά θέματα.
- (26) Ορισμένες επεξεργασίες που ενδέχεται να παρουσιάζουν ιδιαίτερο κίνδυνο όσον αφορά τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων, υπόκεινται στον προκαταρκτικό έλεγχο της ανεξάρτητης εποπτικής αρχής. Η γνώμη που διατυπώνεται στα πλαίσια του προκαταρκτικού αυτού ελέγχου, συμπεριλαμβανομένης της γνώμης που προκύπτει από την έλλειψη απάντησης εντός της προβλεπόμενης προθεσμίας, θα πρέπει να μην προδικάσει τη μεταγενέστερη άσκηση των εξουσιών της ανεξάρτητης εποπτικής αρχής σε σχέση με την εν λόγω επεξεργασία.
- (27) Η επεξεργασία δεδομένων προσωπικού χαρακτήρα για την εκτέλεση καθήκοντος που ασκούν χάριν του δημόσιου συμφέροντος τα όργανα και οι οργανισμοί της Κοινότητας, περιλαμβάνει την επεξεργασία δεδομένων προσωπικού χαρακτήρα, που είναι αναγκαία για τη διαχείριση και τη λειτουργία των εν λόγω οργάνων και οργανισμών.
- (28) Σε ορισμένες περιπτώσεις, ενδείκνυται να προβλεφθεί ότι η επεξεργασία δεδομένων θα πρέπει να επιτρέπεται βάσει κοινοτικών διατάξεων ή πράξεων μεταφοράς κοινοτικών διατάξεων. Ωστόσο, όταν τέτοιες διατάξεις δεν υφίστανται και εν αναμονή της θεσπίσεώς τους, ο ευρωπαίος επόπτης προστασίας των δεδομένων μπορεί, μεταβατικά, να επιτρέψει την επεξεργασία τέτοιων δεδομένων με την υιοθέτηση καταλλήλων εγγυήσεων. Εν προκειμένω, λαμβάνει ιδίως υπόψη τις διατάξεις που έχουν θεσπίσει τα κράτη μέλη για τη ρύθμιση ανάλογων περιπτώσεων.
- (29) Οι περιπτώσεις αυτές αφορούν την επεξεργασία δεδομένων τα οποία δηλώνουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, τη συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και την επεξεργασία δεδομένων σχετικά με την υγεία ή τη σεξουαλική ζωή και τα οποία είναι αναγκαία προκειμένου να γίνονται σεβαστές οι υποχρεώσεις και τα ειδικά δικαιώματα του υπευθύνου της επεξεργασίας σε θέματα εργατικού δικαίου ή για σημαντικό λόγο δημοσίου συμφέροντος. Πρόκειται επίσης για την επεξεργασία δεδομένων σχετικά με αδικήματα, ποινικές καταδίκες ή μέτρα ασφαλείας ή ακόμα για την άδεια να υπαχθεί ένα υποκείμενο δεδομένων σε απόφαση η οποία παράγει νομικά αποτελέσματα έναντι αυτού ή το θίγει σε σημαντικό βαθμό, και έχει ληφθεί μόνο βάσει μιας αυτοματοποιημένης επεξεργασίας δεδομένων, η οποία έχει σκοπό να αξιολογήσει ορισμένες πτυχές της προσωπικότητάς του.
- (30) Ενδέχεται να χρειάζεται ο έλεγχος των δικτύων υπολογιστών που λειτουργούν υπό την ευθύνη των οργάνων και των οργανισμών της Κοινότητας, προκειμένου να αποτρέπεται η τυχόν μη επιτρεπόμενη χρήση τους ο ευρωπαίος επόπτης προστασίας δεδομένων καθορίζει το αν και υπό ποιους όρους αυτό είναι δυνατόν.
- (31) Η ευθύνη για την παραβίαση του παρόντος κανονισμού διέπεται από το άρθρο 288 δεύτερο εδάφιο της συνθήκης.
- (32) Ένας ή πλείονες υπεύθυνοι για την προστασία των δεδομένων μερμούν, στο πλαίσιο κάθε οργάνου ή οργανισμού της Κοινότητας, για την εφαρμογή των διατάξεων του παρόντος κανονισμού και συμβουλευούν τους υπευθύνους της επεξεργασίας κατά την εκτέλεση των υποχρεώσεών τους.
- (33) Σύμφωνα με το οικείο άρθρο 21, ο κανονισμός (ΕΚ) αριθ. 322/97 του Συμβουλίου, της 17ης Φεβρουαρίου 1997, περί κοινοτικών στατιστικών⁽¹⁾, εφαρμόζεται υπό την επιφύλαξη της οδηγίας 95/46/ΕΚ.
- (34) Σύμφωνα με το οικείο άρθρο 8 παράγραφος 8, ο κανονισμός (ΕΚ) αριθ. 2533/98 του Συμβουλίου, της 23ης Νοεμβρίου 1998, όσον αφορά τη συλλογή στατιστικών πληροφοριών από την Ευρωπαϊκή Κεντρική Τράπεζα⁽²⁾, εφαρμόζεται υπό την επιφύλαξη της οδηγίας 95/46/ΕΚ.
- (35) Σύμφωνα με το οικείο άρθρο 1 παράγραφος 2, ο κανονισμός (ΕΟΚ, Ευρατόμ) αριθ. 1588/90 του Συμβουλίου, της 11ης Ιουνίου 1990, σχετικά με τη διαβίβαση στη στατιστική Υπηρεσία των Ευρωπαϊκών Κοινοτήτων πληροφοριών που καλύπτονται από το στατιστικό απόρρητο⁽³⁾, δεν παρεκκλίνει από τις ειδικές κοινοτικές ή εθνικές διατάξεις που άπτονται της διαφύλαξης άλλων απορρήτων εκτός του στατιστικού.
- (36) Ο παρών κανονισμός δεν αποβλέπει να περιορίσει τη διακριτική ευχέρεια των κρατών μελών κατά την κατάρτιση της εθνικής τους νομοθεσίας στον τομέα της προστασίας δεδομένων, που θεσπίζεται δυνάμει του άρθρου 32 της οδηγίας 95/46/ΕΚ, σύμφωνα με το άρθρο 249 της συνθήκης.

ΕΞΕΔΩΣΑΝ ΤΟΝ ΠΑΡΟΝΤΑ ΚΑΝΟΝΙΣΜΟ:

ΚΕΦΑΛΑΙΟ Ι

ΓΕΝΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 1

Αντικείμενο του κανονισμού

1. Τα όργανα και οι οργανισμοί που συνιστώνται από τις συνθήκες για την ίδρυση των Ευρωπαϊκών Κοινοτήτων ή βάσει αυτών, στο εξής αποκαλούμενα: «όργανα και οργανισμοί της Κοινότητας», εξασφαλίζουν,

⁽¹⁾ ΕΕ L 52 της 22.2.1997, σ. 1.

⁽²⁾ ΕΕ L 318 της 27.11.1998, σ. 8.

⁽³⁾ ΕΕ L 151, 15.6.1990, σ. 1· κανονισμός όπως τροποποιήθηκε από τον κανονισμό (ΕΚ) αριθ. 322/97 (ΕΕ L 52 της 22.2.1997, σ. 1).

σύμφωνα με τον παρόντα κανονισμό, την προστασία των θεμελιωδών δικαιωμάτων και ελευθεριών των φυσικών προσώπων, και ιδίως της ιδιωτικής τους ζωής, έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, και δεν περιορίζουν ούτε απαγορεύουν την ελεύθερη κυκλοφορία δεδομένων προσωπικού χαρακτήρα μεταξύ τους ή προς αποδέκτες οι οποίοι υπόκεινται στην εθνική νομοθεσία των κρατών μελών που εφαρμόζουν την οδηγία 95/46/EK.

2. Η ανεξάρτητη εποπτική αρχή, η οποία συνιστάται με τον παρόντα κανονισμό, εφεξής αποκαλούμενη «ευρωπαϊός επόπτης προστασίας δεδομένων», ελέγχει την εφαρμογή των διατάξεων του παρόντος κανονισμού σε κάθε επεξεργασία δεδομένων που πραγματοποιείται από όργανο ή οργανισμό της Κοινότητας.

Άρθρο 2

Ορισμοί

Για τους σκοπούς του παρόντος κανονισμού, νοούνται ως:

- α) «δεδομένα προσωπικού χαρακτήρα»: κάθε πληροφορία που αναφέρεται σε φυσικό πρόσωπο του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί (στο εξής αποκαλούμενο «υποκείμενο των δεδομένων»)· ως πρόσωπο του οποίου η ταυτότητα μπορεί να εξακριβωθεί λογίζεται το πρόσωπο εκείνο που μπορεί να προσδιοριστεί, άμεσα ή έμμεσα, ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός ή περισσότερων συγκεκριμένων στοιχείων που χαρακτηρίζουν την υπόστασή του από άποψη φυσική, βιολογική, ψυχική, οικονομική, πολιτιστική ή κοινωνική,
- β) «επεξεργασία δεδομένων προσωπικού χαρακτήρα» (στο εξής αποκαλούμενη «επεξεργασία»): κάθε εργασία ή σειρά εργασιών που πραγματοποιούνται με ή χωρίς τη βοήθεια αυτοματοποιημένων μεθόδων και εφαρμόζονται σε δεδομένα προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διατήρηση, η προσαρμογή ή η τροποποίηση, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η ανακοίνωση με διαβίβαση, η διάδοση και κάθε άλλη μορφή διάδοσης, η συσχέτιση ή ο συνδυασμός, καθώς και το κλείδωμα, η διαγραφή ή η καταστροφή,
- γ) «αρχείο δεδομένων προσωπικού χαρακτήρα» (στο εξής αποκαλούμενο «αρχείο»): κάθε διαρθρωμένο σύνολο δεδομένων προσωπικού χαρακτήρα τα οποία είναι προσβάσιμα με γνώμονα συγκεκριμένα κριτήρια, είτε το σύνολο αυτό είναι συγκεντρωμένο είτε αποκεντρωμένο είτε καταναμημένο σε λειτουργική ή γεωγραφική βάση,
- δ) «υπεύθυνος της επεξεργασίας»: το όργανο ή ο οργανισμός της Κοινότητας, η Γενική Διεύθυνση, η μονάδα ή κάθε άλλη διοικητική ενότητα που, αυτοτελώς ή από κοινού με άλλους, καθορίζει τους στόχους και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Όταν οι στόχοι και ο τρόπος της επεξεργασίας καθορίζονται σε ειδική κοινοτική πράξη, η ίδια κοινοτική πράξη είναι δυνατό να ορίζει τον υπεύθυνο της επεξεργασίας ή τα ειδικά κριτήρια που ισχύουν για το διορισμό του,
- ε) «εκτελών την επεξεργασία»: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή οποιοσδήποτε άλλος οργανισμός που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας,
- στ) «τρίτος»: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή οποιοσδήποτε άλλος οργανισμός, εκτός από το υποκείμενο των δεδομένων, τον υπεύθυνο της επεξεργασίας, τον εκτελούντα την επεξεργασία και τα πρόσωπα τα οποία, υπό την άμεση εποπτεία του υπευθύνου της επεξεργασίας ή του εκτελούντος την επεξεργασία, είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα,
- ζ) «αποδέκτης»: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή οποιοσδήποτε άλλος οργανισμός στον οποίο ανακοινώνονται τα δεδομένα, είτε πρόκειται για τρίτο, είτε όχι. Ωστόσο, οι αρχές στις οποίες ενδεχομένως ανακοινώνονται δεδομένα, στα πλαίσια ειδικής ερευνητικής αποστολής, δεν θεωρούνται ως αποδέκτες,
- η) «συγκατάθεση του υποκειμένου των δεδομένων»: κάθε ελεύθερη, ρητή και εν πλήρη επιγνώσει δήλωση βούλησής, με την οποία το υποκείμενο των δεδομένων δέχεται να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν.

Άρθρο 3

Πεδίο εφαρμογής

1. Ο παρών κανονισμός εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα από όλα τα όργανα και τους οργανισμούς της Κοινότητας, εφ' όσον η επεξεργασία αυτή πραγματοποιείται στα πλαίσια της άσκησης δραστηριοτήτων που εμπίπτουν, εν όλω ή εν μέρει, στο πεδίο εφαρμογής του κοινοτικού δικαίου.

2. Ο παρών κανονισμός εφαρμόζεται στην, εν όλω ή εν μέρει, αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα, καθώς και στη μη αυτοματοποιημένη επεξεργασία τέτοιων δεδομένων, τα οποία περιλαμβάνονται ή πρόκειται να περιληφθούν σε αρχείο.

ΚΕΦΑΛΑΙΟ II

ΓΕΝΙΚΟΙ ΚΑΝΟΝΕΣ ΠΕΡΙ ΤΟΥ ΘΕΜΙΤΟΥ ΤΗΣ ΕΠΕΞΕΡΓΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

ΤΜΗΜΑ 1

ΑΡΧΕΣ ΑΝΑΦΕΡΟΜΕΝΕΣ ΣΤΗΝ ΠΟΙΟΤΗΤΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ

Άρθρο 4

Ποιότητα των δεδομένων

1. Τα δεδομένα προσωπικού χαρακτήρα πρέπει:
 - α) να υφίστανται θεμιτή και νόμιμη επεξεργασία,
 - β) να συλλέγονται για καθορισμένους, σαφείς και νόμιμους σκοπούς, και η περαιτέρω επεξεργασία τους να συμβιβάζεται με τους σκοπούς αυτούς. Η περαιτέρω επεξεργασία, για ιστορικούς, στατιστικούς ή επιστημονικούς σκοπούς, δεν θεωρείται ασυμβίβαστη, υπό την προϋπόθεση ότι ο υπεύθυνος της επεξεργασίας προβλέπει κατάλληλες εγγυήσεις, προκειμένου να διασφαλίζεται ιδίως ότι η επεξεργασία των δεδομένων δεν πραγματοποιείται για άλλους σκοπούς και ότι τα δεδομένα δεν θα χρησιμοποιηθούν προς υποστήριξη μέτρων ή αποφάσεων που αφορούν ένα συγκεκριμένο πρόσωπο,
 - γ) να είναι πρόσφορα, συναφή προς το θέμα και όχι υπέρμετρα σε σχέση με τους σκοπούς για τους οποίους συλλέγονται και υφίστανται περαιτέρω επεξεργασία,
 - δ) να είναι ακριβή και, εφόσον χρειάζεται, να ενημερώνονται· λαμβάνονται όλα τα εύλογα μέτρα ώστε δεδομένα ανακριβή ή ελλιπή, σε σχέση με τους σκοπούς για τους οποίους έχουν συλλεγεί ή υφίστανται περαιτέρω επεξεργασία, να διαγράφονται ή να διορθώνονται,
 - ε) να διατηρούνται υπό μορφή που να επιτρέπει τον προσδιορισμό της ταυτότητας των υποκειμένων τους μόνο κατά τη διάρκεια της περιόδου που είναι αναγκαία για την επίτευξη των σκοπών για τους οποίους έχουν συλλεγεί ή υφίστανται περαιτέρω επεξεργασία. Το όργανο ή ο οργανισμός της Κοινότητας προβλέπει, για τα δεδομένα προσωπικού χαρακτήρα που πρέπει να αποθηκευθούν πέραν της περιόδου αυτής, για σκοπούς ιστορικούς, στατιστικούς ή επιστημονικούς, είτε να διατηρούνται μόνον υπό μορφήν η οποία τα καθιστά ανώνυμα, είτε, εάν αυτό είναι αδύνατο, να αποθηκεύονται μόνον υπό τον όρο ότι η ταυτότητα του υποκειμένου τους τελεί υπό κρυπτογραφική μορφή. Τα δεδομένα δεν πρέπει πάντως να χρησιμοποιούνται για άλλους σκοπούς εκτός από σκοπούς ιστορικούς, στατιστικούς ή επιστημονικούς.
2. Ο υπεύθυνος της επεξεργασίας διασφαλίζει την τήρηση της παραγράφου 1.

ΤΜΗΜΑ 2

ΑΡΧΕΣ ΣΧΕΤΙΚΕΣ ΜΕ ΤΗ ΝΟΜΙΜΟΠΟΙΗΣΗ ΤΗΣ ΕΠΕΞΕΡΓΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

Άρθρο 5

Θεμιτό της επεξεργασίας

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα πραγματοποιείται μόνον εφόσον:

- α) είναι απαραίτητη για την εκπλήρωση καθήκοντος προς χάριν του δημόσιου συμφέροντος βάσει των συνθηκών για την ίδρυση των Ευρωπαϊκών Κοινοτήτων ή άλλων νομοθετικών πράξεων που έχουν θεσπισθεί βάσει των συνθηκών αυτών ή για την εκπλήρωση καθήκοντος που ανάγεται στη νόμιμη άσκηση δημόσιας εξουσίας που έχει ανατεθεί στο όργανο ή στον οργανισμό της Κοινότητας ή σε τρίτον στον οποίον ανακοινώνονται τα δεδομένα, ή

- β) είναι απαραίτητη για την εκπλήρωση νόμιμης υποχρέωσης την οποία υπέχει ο υπεύθυνος της επεξεργασίας, ή
- γ) είναι απαραίτητη για την εκτέλεση συμβάσεως στην οποία συμμετέχει το υποκείμενο των δεδομένων ή για την εφαρμογή προσυμβατικών μέτρων που λαμβάνονται κατόπιν αιτήσεώς του, ή
- δ) το υποκείμενο των δεδομένων έχει παράσχει την αναμφισβήτητη συγκατάθεσή του, ή
- ε) είναι απαραίτητη για τη διασφάλιση ζωτικών συμφερόντων του υποκειμένου των δεδομένων.

Άρθρο 6

Μεταβολή σκοπού

Με την επιφύλαξη των άρθρων 4, 5 και 10:

1. Η επεξεργασία δεδομένων προσωπικού χαρακτήρα για σκοπούς άλλους εκτός από εκείνους για τους οποίους έχουν συλλεγεί, γίνεται μόνον εφόσον η μεταβολή του σκοπού επιτρέπεται ρητώς από τον εσωτερικό κανονισμό του οργάνου ή του οργανισμού της Κοινότητας.
2. Τα δεδομένα προσωπικού χαρακτήρα που συλλέγονται με αποκλειστικό σκοπό την κατοχύρωση της ασφάλειας ή του ελέγχου των συστημάτων ή των εργασιών επεξεργασίας, δεν επιτρέπεται να χρησιμοποιούνται για κανέναν άλλο σκοπό, με εξαίρεση την πρόληψη, τη διερεύνηση, τη διακρίβωση και τη δίωξη σοβαρών αξιόποινων πράξεων.

Άρθρο 7

Διαβίβαση δεδομένων προσωπικού χαρακτήρα στο εσωτερικό ή μεταξύ οργάνων ή οργανισμών της Κοινότητας

Με την επιφύλαξη των άρθρων 4, 5, 6 και 10:

1. Η διαβίβαση δεδομένων προσωπικού χαρακτήρα στο εσωτερικό ή μεταξύ οργάνων ή οργανισμών της Κοινότητας, επιτρέπεται μόνον εφόσον τα δεδομένα είναι αναγκαία για τη νόμιμη εκτέλεση καθήκοντος που εμπίπτει στην αρμοδιότητα του αποδέκτη.
2. Όταν τα δεδομένα διαβιβάζονται κατόπιν αιτήσεως του αποδέκτη, υπεύθυνοι για το σύννομο χαρακτήρα της διαβίβασης είναι τόσο ο υπεύθυνος της επεξεργασίας όσο και ο αποδέκτης.

Ο υπεύθυνος της επεξεργασίας υποχρεούται να ελέγχει την αρμοδιότητα του αποδέκτη και να αξιολογεί προσωρινά την αναγκαιότητα διαβίβασης των δεδομένων. Εάν ανακύπτουν αμφιβολίες ως προς την αναγκαιότητα της διαβίβασης αυτής, ο υπεύθυνος της επεξεργασίας ζητά περαιτέρω διευκρινίσεις από τον αποδέκτη.

Ο αποδέκτης μεριμνά ώστε η αναγκαιότητα της διαβίβασης των δεδομένων να μπορεί να επαληθευτεί μεταγενέστερα.

3. Ο αποδέκτης επεξεργάζεται τα δεδομένα προσωπικού χαρακτήρα μόνον για τους σκοπούς οι οποίοι αιτιολογούν τη διαβίβασή τους.

Άρθρο 8

Διαβίβαση δεδομένων προσωπικού χαρακτήρα προς αποδέκτες άλλους, εκτός από τα όργανα και τους οργανισμούς της Κοινότητας, οι οποίοι υπάγονται στην οδηγία 95/46/EK

Με την επιφύλαξη των άρθρων 4, 5, 6 και 10, τα δεδομένα προσωπικού χαρακτήρα διαβιβάζονται σε αποδέκτες οι οποίοι εμπίπτουν στην εθνική νομοθεσία που θεσπίζεται κατ' εφαρμογή της οδηγίας 95/46/EK, μόνον εάν:

- α) Ο αποδέκτης αποδεικνύει την αναγκαιότητα των δεδομένων για την εκπλήρωση καθήκοντος προς χάριν του δημόσιου συμφέροντος ή την εκπλήρωση καθήκοντος που ανάγεται στην άσκηση δημόσιας εξουσίας, ή
- β) εάν ο αποδέκτης αποδεικνύει την αναγκαιότητα της διαβίβασης των δεδομένων και δεν υφίστανται λόγοι να υποτεθεί ότι η διαβίβαση αυτή μπορεί να θίξει τα νόμιμα συμφέροντα του υποκειμένου των δεδομένων.

Άρθρο 9

Διαβίβαση δεδομένων προσωπικού χαρακτήρα προς αποδέκτες άλλους, εκτός από τα όργανα και τους οργανισμούς της Κοινότητας, οι οποίοι δεν υπόκεινται στην οδηγία 95/46/ΕΚ

1. Η διαβίβαση δεδομένων προσωπικού χαρακτήρα προς αποδέκτες άλλους, εκτός από τα όργανα και τους οργανισμούς της Κοινότητας, οι οποίοι δεν υπόκεινται στην εθνική νομοθεσία που θεσπίζεται κατ' εφαρμογή της οδηγίας 95/46/ΕΚ, επιτρέπεται μόνον εφόσον διασφαλίζεται επαρκής βαθμός προστασίας στη χώρα του αποδέκτη ή στο πλαίσιο του αποδέκτη διεθνούς οργανισμού και εφόσον η διαβίβαση αποβλέπει αποκλειστικά στο να διευκολύνει την εκτέλεση καθήκοντος που εμπίπτει στην αρμοδιότητα του υπεύθυνου της επεξεργασίας.
2. Η επάρκεια του βαθμού προστασίας που παρέχει η εκάστοτε τρίτη χώρα ή ο συγκεκριμένος διεθνής οργανισμός αξιολογείται με γνώμονα το σύνολο των περιστάσεων που περιβάλλουν την εργασία ή το σύνολο εργασιών της διαβίβασης δεδομένων. Ιδιαίτερος, λαμβάνεται υπόψη το είδος των δεδομένων, ο σκοπός και η διάρκεια της προτεινόμενης επεξεργασίας ή των προτεινόμενων επεξεργασιών η τρίτη χώρα ή ο αποδέκτης διεθνής οργανισμός, η νομοθεσία, τόσο γενική όσο και ειδική, η οποία ισχύει στη συγκεκριμένη τρίτη χώρα ή εφαρμόζεται έναντι του συγκεκριμένου διεθνούς οργανισμού καθώς και οι κανόνες δεοντολογίας και τα μέτρα ασφαλείας που εφαρμόζονται στη συγκεκριμένη τρίτη χώρα ή στο πλαίσιο του συγκεκριμένου διεθνούς οργανισμού.
3. Τα όργανα και οι οργανισμοί της Κοινότητας ενημερώνουν την Επιτροπή και τον ευρωπαϊό επόπτη προστασίας δεδομένων σε περίπτωση που κρίνουν ότι η τρίτη χώρα ή ο συγκεκριμένος διεθνής οργανισμός δεν διασφαλίζουν επαρκή βαθμό προστασίας κατά την έννοια της παραγράφου 2.
4. Η Επιτροπή ενημερώνει τα κράτη μέλη για τις περιπτώσεις που αναφέρονται στην παράγραφο 3.
5. Τα όργανα και οι οργανισμοί της Κοινότητας λαμβάνουν τα μέτρα που είναι απαραίτητα για να συμμορφωθούν με τις αποφάσεις που λαμβάνει η Επιτροπή όταν διαπιστώνει, κατ' εφαρμογήν του άρθρου 25, παράγραφοι 4 και 6 της οδηγίας 95/46/ΕΚ, ότι τρίτη χώρα ή διεθνής οργανισμός διασφαλίζει ή όχι επαρκή βαθμό προστασίας.
6. Κατά παρέκκλιση από τις παραγράφους 1 και 2, το όργανο ή ο οργανισμός της Κοινότητας δύναται να διαβιβάζει δεδομένα προσωπικού χαρακτήρα εάν:
 - α) το υποκείμενο των δεδομένων έχει παράσχει την αναμφισβήτητη συγκατάθεσή του για την προτεινόμενη διαβίβαση, ή
 - β) η διαβίβαση είναι αναγκαία για την εκτέλεση συμβάσεως μεταξύ του υποκειμένου των δεδομένων και του υπευθύνου της επεξεργασίας ή για την εφαρμογή προσυμβατικών μέτρων που λαμβάνονται κατόπιν αιτήσεως του υποκειμένου των δεδομένων, ή
 - γ) η διαβίβαση είναι αναγκαία για τη σύναψη ή την εκτέλεση συμβάσεως προς το συμφέρον του υποκειμένου των δεδομένων, μεταξύ του υπευθύνου της επεξεργασίας και τρίτου, ή
 - δ) η διαβίβαση είναι αναγκαία ή επιβάλλεται εκ του νόμου για σημαντικούς λόγους δημόσιου συμφέροντος ή για την αναγνώριση, άσκηση ή υπεράσπιση δικαιώματος ενώπιον δικαστηρίου, ή
 - ε) η διαβίβαση είναι αναγκαία για τη διασφάλιση ζωτικών συμφερόντων του υποκειμένου των δεδομένων, ή
 - στ) η διαβίβαση πραγματοποιείται από αρχείο το οποίο, κατά το κοινοτικό δίκαιο, χρησιμεύει για την ενημέρωση του κοινού και το οποίο μπορεί να συμβουλευθεί το κοινό εν γένει ή κάθε πρόσωπο που αποδεικνύει ότι έχει έννομο συμφέρον, εφόσον πληρούνται στη συγκεκριμένη περίπτωση οι προϋποθέσεις του κοινοτικού δικαίου που διέπουν την αναζήτηση πληροφοριών.
7. Με την επιφύλαξη της παραγράφου 6, ο ευρωπαίος επόπτης προστασίας δεδομένων μπορεί να επιτρέπει διαβίβαση ή σύνολο διαβιβάσεων δεδομένων προσωπικού χαρακτήρα προς μια τρίτη χώρα ή ένα διεθνή οργανισμό που δεν παρέχει ικανοποιητικό επίπεδο προστασίας κατά την έννοια των παραγράφων 1 και 2, όταν ο υπεύθυνος της επεξεργασίας παρέχει επαρκείς εγγυήσεις όσον αφορά την προστασία της ιδιωτικής ζωής και των θεμελιωδών δικαιωμάτων και ελευθεριών των προσώπων, καθώς και όσον αφορά την άσκηση των αντιστοίχων δικαιωμάτων οι εγγυήσεις αυτές μπορούν ιδίως να απορρέουν από κατάλληλες συμβατικές ρήτρες.
8. Τα όργανα και οι οργανισμοί της Κοινότητας γνωστοποιούν στον ευρωπαϊό επόπτη προστασίας δεδομένων κατηγορίες περιπτώσεων στις οποίες εφήρμοσαν τις παραγράφους 6 και 7.

ΤΜΗΜΑ 3

ΕΙΔΙΚΕΣ ΚΑΤΗΓΟΡΙΕΣ ΕΠΕΞΕΡΓΑΣΙΑΣ

Άρθρο 10

Επεξεργασία ειδικών κατηγοριών δεδομένων

1. Απαγορεύεται η επεξεργασία δεδομένων προσωπικού χαρακτήρα που δηλώνουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις και τη συμμετοχή σε συνδικαλιστικές οργανώσεις καθώς και η επεξεργασία δεδομένων που αναφέρονται στην υγεία και τη σεξουαλική ζωή.
2. Η παράγραφος 1 δεν εφαρμόζεται εφόσον:
 - α) το υποκείμενο των δεδομένων έχει δώσει ρητά τη συγκατάθεσή του για την επεξεργασία τους, εκτός εάν ο εσωτερικός κανονισμός του οικείου οργάνου ή οργανισμού της Κοινότητας ορίζει ότι η απαγόρευση της παραγράφου 1 δεν μπορεί να αρθεί με την παροχή της συγκατάθεσης του υποκειμένου των δεδομένων, ή
 - β) η επεξεργασία είναι απαραίτητη προκειμένου να γίνουν σεβαστές οι υποχρεώσεις και τα ειδικά δικαιώματα του υπευθύνου της επεξεργασίας σε θέματα εργατικού δικαίου, εφόσον αυτό επιτρέπεται από τις συνθήκες για την ίδρυση των Ευρωπαϊκών Κοινοτήτων ή άλλες νομοθετικές πράξεις θεσπιζόμενες βάσει των συνθηκών αυτών ή, εάν αυτό παρίσταται αναγκαίο, εφόσον η επεξεργασία έχει γίνει δεκτή από τον ευρωπαϊό επόπτη προστασίας δεδομένων, μέσω επαρκών εγγυήσεων, ή
 - γ) η επεξεργασία είναι απαραίτητη για τη διασφάλιση ζωτικών συμφερόντων του υποκειμένου των δεδομένων ή άλλου προσώπου, εφόσον το υποκείμενο των δεδομένων τελεί σε φυσική ή νομική αδυναμία να δηλώσει τη συγκατάθεσή του, ή
 - δ) η επεξεργασία αφορά δεδομένα τα οποία προδήλως έχει δημοσιοποιήσει το υποκείμενο των δεδομένων ή είναι αναγκαία για την αναγνώριση, την άσκηση ή την υπεράσπιση δικαιώματος ενώπιον δικαστηρίου, ή
 - ε) η επεξεργασία εκτελείται, στο πλαίσιο των νόμιμων δραστηριοτήτων του και με επαρκείς εγγυήσεις, από φορέα ο οποίος δεν έχει κερδοσκοπικό σκοπό, συνιστά μονάδα ενσωματωμένη σε όργανο ή οργανισμό της Κοινότητας, δεν υπόκειται στην εθνική νομοθεσία περί προστασίας των δεδομένων η οποία εφαρμόζεται δυνάμει του άρθρου 4 της οδηγίας 95/46/EK και επιδιώκει πολιτικούς, φιλοσοφικούς, θρησκευτικούς ή συνδικαλιστικούς σκοπούς, υπό τον όρο ότι η εν λόγω επεξεργασία αφορά μόνον τα μέλη του ή τα πρόσωπα με τα οποία ο φορέας διατηρεί, ως εκ του σκοπού του, τακτικές επαφές, και τα δεδομένα κοινολογούνται σε τρίτους μόνον με τη συγκατάθεση των υποκειμένων των δεδομένων.
3. Η παράγραφος 1 δεν εφαρμόζεται όταν η επεξεργασία των δεδομένων είναι αναγκαία για λόγους προληπτικής ιατρικής, ιατρικής διάγνωσης, για την παροχή ιατροφαρμακευτικής νοσηλείας ή θεραπείας ή για τη διαχείριση υπηρεσιών υγείας, η δε επεξεργασία των δεδομένων αυτών εκτελείται από πρόσωπο που ασχολείται κατ' επάγγελμα με τη θεραπεία της υγείας, υποκείμενο στην υποχρέωση τήρησης του επαγγελματικού απορρήτου ή από άλλο πρόσωπο το οποίο ομοίως υπέχει αντίστοιχη υποχρέωση τήρησης απορρήτου.
4. Εφόσον παρέχονται οι δέουσες εγγυήσεις, και για λόγους σοβαρού δημοσίου συμφέροντος, μπορούν να θεσπίζονται και άλλες παρεκκλίσεις, εκτός από τις προβλεπόμενες στην παράγραφο 2, από τις συνθήκες για την ίδρυση των Ευρωπαϊκών Κοινοτήτων ή άλλες νομοθετικές πράξεις θεσπιζόμενες βάσει των συνθηκών αυτών, ή, εφόσον αυτό παρίσταται αναγκαίο, με απόφαση του ευρωπαϊού επόπτη προστασίας δεδομένων.
5. Η επεξεργασία δεδομένων σχετικών με αδικήματα, ποινικές καταδίκες ή μέτρα ασφαλείας μπορεί να πραγματοποιείται μόνον εάν επιτρέπεται από τις συνθήκες για την ίδρυση των Ευρωπαϊκών Κοινοτήτων ή άλλες νομοθετικές πράξεις θεσπιζόμενες βάσει των συνθηκών αυτών ή, εφόσον αυτό παρίσταται αναγκαίο, από τον ευρωπαϊό επόπτη προστασίας των δεδομένων, υπό την επιφύλαξη ειδικών και κατάλληλων εγγυήσεων.
6. Ο ευρωπαίος επόπτης προστασίας δεδομένων καθορίζει τις προϋποθέσεις υπό τις οποίες επιτρέπεται η επεξεργασία, από όργανο ή οργανισμό της Κοινότητας, προσωπικού κωδικού αριθμού ή κάθε άλλου αναγνωριστικού στοιχείου το οποίο τυγχάνει γενικής εφαρμογής.

ΤΜΗΜΑ 4

ΕΝΗΜΕΡΩΣΗ ΤΟΥ ΥΠΟΚΕΙΜΕΝΟΥ ΤΩΝ ΔΕΔΟΜΕΝΩΝ

Άρθρο 11

Ενημέρωση σε περίπτωση που τα δεδομένα συλλέγονται παρά τω υποκειμένω των δεδομένων

1. Ο υπεύθυνος της επεξεργασίας παρέχει στο πρόσωπο παρά τω οποίω συλλέγονται δεδομένα που το αφορούν, τουλάχιστον τις πληροφορίες που απαριθμούνται κατωτέρω, εκτός εάν το υποκείμενο έχει ήδη ενημερωθεί:

- α) την ταυτότητα του υπευθύνου της επεξεργασίας,
- β) τους σκοπούς της επεξεργασίας για τους οποίους προορίζονται τα δεδομένα,
- γ) τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων,
- δ) ένδειξη εάν η απάντηση των ερωτήσεων είναι υποχρεωτική ή προαιρετική, καθώς και τις ενδεχόμενες συνέπειες παράλειψης απάντησης,
- ε) την ύπαρξη δικαιώματος πρόσβασης στα δεδομένα που το αφορούν και δικαιώματος διόρθωσης των δεδομένων αυτών,

στ) οποιαδήποτε συμπληρωματική πληροφορία, όπως:

- i) τη νομική βάση της επεξεργασίας για την οποία προορίζονται τα δεδομένα,
- ii) τις προθεσμίες διατήρησης των δεδομένων,
- iii) το δικαίωμα προσφυγής, ανά πάσα στιγμή, στον ευρωπαϊό επόπτη προστασίας δεδομένων,

στο μέτρο που, λαμβανομένων υπόψη των ειδικών συνθηκών υπό τις οποίες συλλέγονται τα δεδομένα, αυτές οι συμπληρωματικές πληροφορίες είναι αναγκαίες, για τη διασφάλιση της θεμιτής επεξεργασίας των δεδομένων έναντι του υποκειμένου των δεδομένων.

2. Κατά παρέκκλιση από την παράγραφο 1, η παροχή πληροφοριών ή μέρους αυτών, εκτός των πληροφοριών που αναφέρονται στην παράγραφο 1, σημεία α), β) και δ), μπορεί να αναβάλλεται για όσον χρόνο αυτό είναι αναγκαίο για στατιστικούς σκοπούς. Οι πληροφορίες πρέπει να παρέχονται μόλις εκλείψει ο λόγος για τον οποίο δεν παρασχέθηκαν.

Άρθρο 12

Ενημέρωση σε περίπτωση που τα δεδομένα δεν έχουν συλλεγεί παρά τω υποκειμένω των δεδομένων

1. Όταν τα δεδομένα δεν έχουν συλλεγεί παρά τω υποκειμένω των δεδομένων, ο υπεύθυνος της επεξεργασίας οφείλει, κατά την καταχώρηση των δεδομένων ή σε περίπτωση που προβλέπεται η ανακοίνωση των δεδομένων σε τρίτον, και το αργότερο κατά την πρώτη ανακοίνωσή τους, να παρέχει στο υποκείμενο των δεδομένων τουλάχιστον τις κατωτέρω απαριθμούμενες πληροφορίες, εκτός εάν το υποκείμενο έχει ήδη ενημερωθεί:

- α) την ταυτότητα του υπευθύνου της επεξεργασίας,
- β) τους σκοπούς της επεξεργασίας,
- γ) τις κατηγορίες των σχετικών δεδομένων,
- δ) τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων,
- ε) την ύπαρξη δικαιώματος πρόσβασης στα δεδομένα που το αφορούν και δικαιώματος διόρθωσης αυτών των δεδομένων,

στ) οποιαδήποτε συμπληρωματική πληροφορία, όπως:

- i) τη νομική βάση της επεξεργασίας για την οποία προορίζονται τα δεδομένα,
- ii) τις προθεσμίες διατήρησης των δεδομένων,
- iii) το δικαίωμα προσφυγής, ανά πάσα στιγμή, στον ευρωπαϊό επόπτη προστασίας δεδομένων,

iv) την προέλευση των δεδομένων, εκτός εάν ο υπεύθυνος της επεξεργασίας δεν δύναται να αποκαλύψει το στοιχείο αυτό για λόγους επαγγελματικού απορρήτου,

στο μέτρο που, λαμβανομένων υπόψη των ειδικών συνθηκών υπό τις οποίες συλλέγονται τα δεδομένα, αυτές οι συμπληρωματικές πληροφορίες είναι αναγκαίες, για τη διασφάλιση της θεμιτής επεξεργασίας των δεδομένων έναντι του υποκειμένου των δεδομένων.

2. Η παράγραφος 1 δεν εφαρμόζεται όταν, ιδίως στην περίπτωση της επεξεργασίας για σκοπούς στατιστικούς ή ιστορικής ή επιστημονικής έρευνας, η ενημέρωση του υποκειμένου των δεδομένων αποδεικνύεται αδύνατη ή προϋποθέτει δυσανάλογες προσπάθειες ή εάν η καταχώρηση ή η ανακοίνωση των δεδομένων προβλέπεται ρητώς από την κοινοτική νομοθεσία. Στις περιπτώσεις αυτές, το όργανο ή ο οργανισμός της Κοινότητας προβλέπει τις κατάλληλες εγγυήσεις αφού ζητήσει τη γνώμη του ευρωπαϊού εφόπτη προστασίας δεδομένων.

ΤΜΗΜΑ 5

ΔΙΚΑΙΩΜΑΤΑ ΤΟΥ ΥΠΟΚΕΙΜΕΝΟΥ ΤΩΝ ΔΕΔΟΜΕΝΩΝ

Άρθρο 13

Δικαίωμα πρόσβασης

Το υποκείμενο των δεδομένων έχει το δικαίωμα να λαμβάνει ανεμπόδιστα, ανά πάσα στιγμή εντός προθεσμίας τριών μηνών από την παραλαβή της αίτησης παροχής πληροφοριών και ατελώς από τον υπεύθυνο της επεξεργασίας:

- α) επιβεβαίωση για το κατά πόσον διενεργείται ή όχι επεξεργασία δεδομένων που το αφορούν,
- β) πληροφορίες τουλάχιστον σχετικά με τους σκοπούς της επεξεργασίας, τις κατηγορίες δεδομένων που αφορά και τους αποδέκτες ή τις κατηγορίες αποδεκτών στους οποίους ανακοινώνονται τα δεδομένα,
- γ) ανακοίνωση, με εύληπτο τρόπο, των υπό επεξεργασία δεδομένων καθώς και κάθε διαθέσιμης πληροφορίας σχετικά με την προέλευσή τους,
- δ) ενημέρωση σχετικά με τη λογική στην οποία στηρίζεται η αυτοματοποιημένη επεξεργασία των δεδομένων που το αφορούν.

Άρθρο 14

Διόρθωση

Το υποκείμενο των δεδομένων έχει το δικαίωμα να λαμβάνει, από τον υπεύθυνο της επεξεργασίας, αμελλητί τη διόρθωση δεδομένων προσωπικού χαρακτήρα που είναι ανακριβή ή ελλιπή.

Άρθρο 15

Κλείδωμα των δεδομένων

1. Το υποκείμενο των δεδομένων έχει το δικαίωμα να λαμβάνει, από τον υπεύθυνο της επεξεργασίας, το κλείδωμα των δεδομένων, όταν:

- α) η ακρίβειά τους αμφισβητείται από το υποκείμενο των δεδομένων, κατά τη διάρκεια προθεσμίας που επιτρέπει στον υπεύθυνο της επεξεργασίας να εξακριβώσει το ακριβές των δεδομένων, συμπεριλαμβανομένης της πληρότητας αυτών, ή
- β) ο υπεύθυνος της επεξεργασίας δεν τα χρειάζεται πλέον για την εκτέλεση των καθηκόντων του, αλλά τα δεδομένα πρέπει να διατηρηθούν για αποδεικτικούς σκοπούς, ή
- γ) η επεξεργασία των δεδομένων είναι παράνομη, και το υποκείμενο των δεδομένων αντιτάσσεται στη διαγραφή τους και ζητά αντ' αυτής το κλείδωμά τους.

2. Στην περίπτωση των αυτοματοποιημένων αρχείων, το κλείδωμα πραγματοποιείται κατ' αρχήν με τεχνικές μεθόδους. Το γεγονός ότι τα συγκεκριμένα δεδομένα προσωπικού χαρακτήρα έχουν κλειδωθεί αναγράφεται στο σύστημα κατά τρόπον ώστε να καθίσταται σαφές ότι τα δεδομένα αυτά δεν επιτρέπεται να χρησιμοποιηθούν.

3. Η επεξεργασία κλειδωμένων κατ' εφαρμογήν του παρόντος άρθρου δεδομένων προσωπικού χαρακτήρα, με εξαίρεση την αποθήκευσή τους, επιτρέπεται μόνον για αποδεικτικούς σκοπούς, ή με τη συγκατάθεση του υποκειμένου των δεδομένων, ή για την προστασία δικαιωμάτων τρίτων.

4. Ο υπεύθυνος της επεξεργασίας ενημερώνει το υποκείμενο των δεδομένων, το οποίο ζήτησε και εξασφάλισε το κλειδί των δεδομένων που το αφορούν, πριν από την άρση του κλειδώματος.

Άρθρο 16

Διαγραφή

Το υποκείμενο των δεδομένων έχει το δικαίωμα να λαμβάνει, από τον υπεύθυνο της επεξεργασίας, τη διαγραφή δεδομένων εάν η επεξεργασία τους είναι παράνομη, ιδίως όταν παραβιάζονται οι διατάξεις των τμημάτων 1, 2 και 3 του κεφαλαίου II.

Άρθρο 17

Κοινοποίηση σε τρίτους

Το υποκείμενο των δεδομένων έχει το δικαίωμα να λαμβάνει από τον υπεύθυνο της επεξεργασίας, την ανακοίνωση στους τρίτους, στους οποίους έχουν γνωστοποιηθεί τα δεδομένα, κάθε διόρθωσης, διαγραφής, ή κλειδώματός τους, σύμφωνα με τα άρθρα 13 έως 16, εκτός αν αυτό αποδεικνύεται αδύνατο ή προϋποθέτει δυσανάλογη προσπάθεια.

Άρθρο 18

Δικαίωμα αντίταξης του υποκειμένου των δεδομένων

Το υποκείμενο των δεδομένων έχει το δικαίωμα:

- α) να αντιτάσσεται ανά πάσα στιγμή, για επιτακτικούς και νόμιμους λόγους σχετικούς με την προσωπική του κατάσταση, στην επεξεργασία δεδομένων που το αφορούν, με εξαίρεση τις περιπτώσεις που εμπίπτουν στο άρθρο 5, στοιχεία β), γ) και δ). Σε περίπτωση αιτιολογημένης αντίταξης, η εν λόγω επεξεργασία δεν επιτρέπεται πλέον να αφορά τα εν λόγω δεδομένα,
- β) να ενημερώνεται πριν διαβιβαστούν για πρώτη φορά δεδομένα προσωπικού χαρακτήρα σε τρίτους ή γίνει χρήση για λογαριασμό τρίτων, για σκοπούς προώθησης προϊόντων, και να του παρέχεται ρητά το δικαίωμα να αντιτάσσεται ατελώς στην ανακοίνωση ή τη χρησιμοποίηση αυτή.

Άρθρο 19

Αυτοματοποιημένες ατομικές αποφάσεις

Το υποκείμενο των δεδομένων έχει το δικαίωμα να μη συμμορφώνεται με απόφαση η οποία παράγει έναντι αυτού νομικά αποτελέσματα ή το θίγει σε σημαντικό βαθμό, και η οποία βασίζεται αποκλειστικά και μόνο στην αυτοματοποιημένη επεξεργασία δεδομένων με σκοπό την αξιολόγηση ορισμένων πτυχών της προσωπικότητάς του, όπως είναι η απόδοσή του στην εργασία, η αξιοπιστία ή η διαγωγή του, εκτός αν η απόφαση αυτή επιτρέπεται ρητά από το εθνικό ή κοινοτικό δίκαιο ή από τον ευρωπαϊκό επόπτη προστασίας δεδομένων, αν αυτό αποδεικνύεται αναγκαίο. Και στις δύο περιπτώσεις, πρέπει να λαμβάνονται μέτρα που να εξασφαλίζουν τη διαφύλαξη των εννόμων συμφερόντων του υποκειμένου των δεδομένων, όπως τα μέτρα που του επιτρέπουν να διατυπώνει την άποψή του.

ΤΜΗΜΑ 6

ΕΞΑΙΡΕΣΕΙΣ ΚΑΙ ΠΕΡΙΟΡΙΣΜΟΙ

Άρθρο 20

Εξαιρέσεις και περιορισμοί

1. Τα όργανα και οι οργανισμοί της Κοινότητας δύνανται να θέτουν περιορισμούς στην εφαρμογή του άρθρου 4 παράγραφος 1, του άρθρου 11, του άρθρου 12 παράγραφος 1, των άρθρων 13 έως 17 και του άρθρου 37 παράγραφος 1, εφόσον ο εκάστοτε περιορισμός αποτελεί αναγκαίο μέτρο για:

- α) τη διασφάλιση της πρόληψης, διερεύνησης, διακρίβωσης και δίωξης αξιόποινων πράξεων,
- β) τη διασφάλιση σημαντικού οικονομικού ή χρηματοοικονομικού συμφέροντος ενός κράτους μέλους ή των Ευρωπαϊκών Κοινοτήτων, μεταξύ άλλων στο νομισματικό, δημοσιονομικό και φορολογικό τομέα,
- γ) την εξασφάλιση της προστασίας του υποκειμένου των δεδομένων ή των δικαιωμάτων και ελευθεριών άλλων προσώπων,

- δ) τη διασφάλιση της εθνικής ασφάλειας, της δημόσιας ασφάλειας και της άμυνας των κρατών μελών,
- ε) την εξασφάλιση ελέγχου, επιθεώρησης ή κανονιστικής λειτουργίας που συνδέεται, έστω και περιστασιακά, με την άσκηση δημόσιας εξουσίας, στις περιπτώσεις που αναφέρονται στα στοιχεία α) και β).

2. Τα άρθρα 13 έως 16 δεν εφαρμόζονται οσάκις η επεξεργασία των δεδομένων γίνεται με αποκλειστικό σκοπό την επιστημονική έρευνα ή τα δεδομένα αποθηκεύονται υπό μορφήν δεδομένων προσωπικού χαρακτήρα για χρονικό διάστημα που δεν υπερβαίνει αυτό που είναι απαραίτητο για την απλή κατάρτιση στατιστικών, υπό την επιφύλαξη ότι είναι σαφές πως δεν υπάρχει κίνδυνος για παραβίαση της ιδιωτικής ζωής του υποκειμένου των δεδομένων και ότι ο υπεύθυνος της επεξεργασίας παρέχει κατάλληλες νομικές εγγυήσεις, οι οποίες αποκλείουν ιδίως τη δυνατότητα χρησιμοποίησης των δεδομένων για τη λήψη μέτρων ή αποφάσεων που αφορούν συγκεκριμένο πρόσωπο.

3. Όταν επιβάλλεται περιορισμός που προβλέπεται στην παράγραφο 1, το υποκείμενο των δεδομένων ενημερώνεται, σύμφωνα με το κοινοτικό δίκαιο, για τους ουσιώδεις λόγους που αιτιολογούν τον περιορισμό αυτό, καθώς και για το δικαίωμά του να προσφύγει στον ευρωπαϊό επόπτη προστασίας δεδομένων.

4. Όταν γίνεται επίκληση περιορισμού προβλεπόμενου στην παράγραφο 1 για να απαγορευθεί η πρόσβαση στο υποκείμενο των δεδομένων, ο ευρωπαίος επόπτης προστασίας δεδομένων του γνωστοποιεί απλώς, όταν εξετάζει την ένσταση, εάν η επεξεργασία των δεδομένων έγινε με τον προσηκόντα τρόπο και, εάν όχι, για το κατά πόσον πραγματοποιήθηκαν όλες οι αναγκαίες διορθώσεις.

5. Η ενημέρωση η οποία προβλέπεται στις παραγράφους 3 και 4 μπορεί να αναβάλλεται εφόσον στερεί από τον περιορισμό που επιβάλλεται βάσει της παραγράφου 1 την ισχύ του.

ΤΜΗΜΑ 7

ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΤΗΣ ΕΠΕΞΕΡΓΑΣΙΑΣ

Άρθρο 21

Εμπιστευτικότητα της επεξεργασίας

Το πρόσωπο που απασχολείται από όργανο ή οργανισμό της Κοινότητας, καθώς και τα όργανα ή οργανισμοί της Κοινότητας που ενεργούν αυτά καθ' εαυτά ως εκτελούντα την επεξεργασία και έχουν πρόσβαση σε δεδομένα προσωπικού χαρακτήρα, μπορούν να τα επεξεργάζονται μόνον κατ' εντολήν του υπεύθυνου της επεξεργασίας, εκτός εάν τούτο απαιτείται από το εθνικό ή το κοινοτικό δίκαιο.

Άρθρο 22

Ασφάλεια της επεξεργασίας

1. Λαμβάνοντας υπόψη την πρόοδο της επιστήμης και το σχετικό κόστος εφαρμογής, ο υπεύθυνος της επεξεργασίας εφαρμόζει τα κατάλληλα τεχνικά και οργανωτικά μέτρα για την κατοχύρωση κατάλληλου βαθμού ασφάλειας ενόψει των κινδύνων της επεξεργασίας και της φύσης των δεδομένων προσωπικού χαρακτήρα που πρέπει να προστατευθούν.

Τα μέτρα αυτά λαμβάνονται ιδίως για να αποτρέπεται οποιαδήποτε μη επιτρεπόμενη διαβίβαση ή πρόσβαση, τυχαία ή παράνομη καταστροφή ή τυχαία απώλεια ή αλλοίωση, καθώς και οιαδήποτε άλλη μορφή παράνομης επεξεργασίας.

2. Όταν τα δεδομένα προσωπικού χαρακτήρα αποτελούν αντικείμενο αυτοματοποιημένης επεξεργασίας, λαμβάνονται μέτρα, εφόσον απαιτούνται, ανάλογα με τον κίνδυνο, ιδίως με σκοπό:

- α) να μην αποκτά μη εξουσιοδοτημένο προς τούτο πρόσωπο πρόσβαση σε συστήματα πληροφορικής που χρησιμοποιούνται για την επεξεργασία δεδομένων προσωπικού χαρακτήρα,
- β) να αποτρέπεται κάθε ανάγνωση, αντιγραφή, αλλοίωση ή απομάκρυνση υποθεμάτων αποθήκευσης, χωρίς εξουσιοδότηση,
- γ) να αποτρέπεται κάθε εισαγωγή δεδομένων στη μνήμη, χωρίς εξουσιοδότηση, καθώς και κάθε γνωστοποίηση, αλλοίωση ή διαγραφή αποθηκευμένων δεδομένων προσωπικού χαρακτήρα, χωρίς εξουσιοδότηση,

- δ) να αποτρέπεται η χρήση συστημάτων επεξεργασίας δεδομένων από μη εξουσιοδοτημένα προς τούτο πρόσωπα μέσω εγκαταστάσεων διαβίβασης δεδομένων,
- ε) να εξασφαλίζεται ότι οι εξουσιοδοτημένοι χρήστες συστήματος επεξεργασίας δεδομένων δεν διαθέτουν πρόσβαση σε άλλα δεδομένα προσωπικού χαρακτήρα πλην εκείνων που καλύπτονται από το δικαίωμα πρόσβασης που τους παρέχεται,
- στ) να καταγράφονται ίχνη των δεδομένων προσωπικού χαρακτήρα τα οποία έχουν ανακοινωθεί, της χρονικής στιγμής της ανακοίνωσής τους και του αποδέκτη τους,
- ζ) να διασφαλίζεται ότι θα μπορεί να εξακριβώνεται εκ των υστέρων ποια δεδομένα προσωπικού χαρακτήρα έχουν υποστεί επεξεργασία, ποια χρονική στιγμή και από ποια πρόσωπα,
- η) να διασφαλίζεται ότι τα δεδομένα προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία για λογαριασμό τρίτων υφίστανται μόνο την επεξεργασία η οποία προβλέπεται από το αναθέτον όργανο ή οργανισμό,
- θ) να εξασφαλίζεται ότι, κατά την ανακοίνωση δεδομένων προσωπικού χαρακτήρα και κατά τη διαβίβαση των υποθεμάτων της αποθήκευσης, δεν είναι δυνατή η ανάγνωση, αντιγραφή ή διαγραφή των δεδομένων, χωρίς εξουσιοδότηση,
- ι) η εσωτερική οργανωτική δομή ενός οργάνου ή οργανισμού να σχεδιάζεται κατά τρόπο ώστε να πληρούνται οι ειδικές προϋποθέσεις που ισχύουν για την προστασία των δεδομένων.

Άρθρο 23

Επεξεργασία δεδομένων προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας

1. Ο υπεύθυνος της επεξεργασίας οφείλει, σε περίπτωση που η επεξεργασία πραγματοποιείται για λογαριασμό του, να επιλέγει ως εκτελούντα την επεξεργασία ένα πρόσωπο το οποίο να παρέχει επαρκείς εγγυήσεις όσον αφορά τα τεχνικά και οργανωτικά μέτρα ασφάλειας που προβλέπονται από το άρθρο 22 και να μεριμνά για την τήρηση των μέτρων αυτών.
2. Η εκτέλεση επεξεργασιών μέσω ανάθεσης της εκτέλεσης της επεξεργασίας πρέπει να διέπεται από σύμβαση ή νομική πράξη η οποία να συνδέει τον εκτελούντα την επεξεργασία με τον υπεύθυνο της επεξεργασίας και να προβλέπει ιδίως:
 - α) ότι ο εκτελών την επεξεργασία ενεργεί μόνον κατ' εντολή του υπευθύνου της επεξεργασίας,
 - β) ότι οι υποχρεώσεις που προβλέπονται στα άρθρα 21 και 22 βαρύνουν και τον εκτελούντα την επεξεργασία, εκτός εάν, δυνάμει του άρθρου 16 ή του άρθρου 17 παράγραφος 3, δεύτερη περίπτωση της οδηγίας 95/46/EK, ο εκτελών την επεξεργασία υπόκειται ήδη σε υποχρεώσεις περί εμπιστευτικότητας και ασφαλείας που προβλέπονται από την εθνική νομοθεσία ενός κράτους μέλους.
3. Για τους σκοπούς της διατήρησης των αποδείξεων, τα τμήματα της σύμβασης ή της νομικής πράξης που αφορούν την προστασία των δεδομένων και τις προϋποθέσεις σχετικά με τα μέτρα που προβλέπονται στο άρθρο 22, καταρτίζονται εγγράφως ή υπό άλλη ισοδύναμη μορφή.

ΤΜΗΜΑ 8

ΥΠΕΥΘΥΝΟΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

Άρθρο 24

Διορισμός και καθήκοντα του υπευθύνου προστασίας δεδομένων

1. Κάθε όργανο και κάθε οργανισμός της Κοινότητας διορίζει ένα τουλάχιστον πρόσωπο, ως υπεύθυνο για την προστασία των δεδομένων προσωπικού χαρακτήρα. Τα καθήκοντα του εν λόγω υπευθύνου είναι τα εξής:
 - α) φροντίζει ώστε οι υπεύθυνοι της επεξεργασίας και τα υποκείμενα των δεδομένων να ενημερώνονται όσον αφορά τα δικαιώματα και τις υποχρεώσεις τους, δυνάμει του παρόντος κανονισμού,
 - β) ανταποκρίνεται στα αιτήματα του ευρωπαίου επόπτη προστασίας δεδομένων και, στα πλαίσια της αρμοδιότητάς του, συνεργάζεται με τον ευρωπαίο επόπτη προστασίας δεδομένων, είτε κατόπιν αιτήματος του τελευταίου, είτε με δική του πρωτοβουλία,
 - γ) διασφαλίζει, κατά τρόπο ανεξάρτητο, την εσωτερική εφαρμογή των διατάξεων του παρόντος κανονισμού,

- δ) τηρεί μητρώο με τις επεξεργασίες που διενεργεί ο υπεύθυνος της επεξεργασίας, περιλαμβανομένων των πληροφοριακών στοιχείων που μνημονεύονται στο άρθρο 25 παράγραφος 2,
- ε) κοινοποιεί στον ευρωπαϊό επόπτη προστασίας δεδομένων τις εργασίες επεξεργασίας οι οποίες ενδέχεται να παρουσιάζουν ιδιαίτερους κινδύνους κατά την έννοια του άρθρου 27.

Με τον τρόπο αυτό, ο εν λόγω υπεύθυνος φροντίζει ώστε η επεξεργασία να μην μπορεί να θίξει τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων.

2. Η επιλογή του υπεύθυνου προστασίας δεδομένων γίνεται με κριτήριο τα προσωπικά και επαγγελματικά του προσόντα και, ιδίως, τις ειδικές του γνώσεις στον τομέα της προστασίας δεδομένων.

3. Η επιλογή του υπευθύνου προστασίας δεδομένων δεν πρέπει να μπορεί να έχει ως συνέπεια σύγκρουση συμφερόντων μεταξύ της ιδιότητάς του ως υπευθύνου και άλλων επισήμων καθηκόντων που μπορεί ενδεχομένως να ασκεί, ειδικότερα στα πλαίσια της εφαρμογής των διατάξεων του παρόντος κανονισμού.

4. Η διάρκεια της θητείας του υπευθύνου προστασίας δεδομένων είναι από 2 ως 5 έτη. Η θητεία του μπορεί να ανανεώνεται, χωρίς όμως η συνολική διάρκεια της θητείας να μπορεί να υπερβαίνει τα δέκα έτη. Ο υπεύθυνος προστασίας δεδομένων είναι δυνατό να απαλλάσσεται από τα καθήκοντά του ως υπευθύνου προστασίας δεδομένων από το όργανο ή οργανισμό της Κοινότητας που τον διόρισε μόνο με τη συγκατάθεση του ευρωπαϊού επόπτη προστασίας δεδομένων, εφόσον έχει παύσει να πληροί τις προϋποθέσεις που απαιτούνται για την άσκηση των καθηκόντων του.

5. Το όργανο ή ο οργανισμός που διορίζει τον υπεύθυνο προστασίας δεδομένων, γνωστοποιεί εν συνεχεία το όνομα αυτού στον ευρωπαϊό επόπτη προστασίας δεδομένων.

6. Το όργανο ή ο οργανισμός της Κοινότητας που διορίζει τον υπεύθυνο προστασίας δεδομένων, του παρέχει το αναγκαίο προσωπικό και πόρους για την εκτέλεση της αποστολής του.

7. Ο υπεύθυνος προστασίας δεδομένων δεν είναι δυνατό να λαμβάνει εντολές κατά την εκτέλεση των καθηκόντων του.

8. Κάθε όργανο ή οργανισμός της Κοινότητας θεσπίζει, σύμφωνα με τις διατάξεις που περιλαμβάνονται στο παράρτημα, συμπληρωματικές διατάξεις εφαρμογής. Αυτές οι συμπληρωματικές διατάξεις αφορούν, ειδικότερα, τα καθήκοντα, τις αρμοδιότητες και τις εξουσίες του υπευθύνου προστασίας δεδομένων.

Άρθρο 25

Κοινοποίηση στον υπεύθυνο προστασίας δεδομένων

1. Ο υπεύθυνος της επεξεργασίας ενημερώνει σχετικά τον υπεύθυνο προστασίας δεδομένων, πριν από τη διενέργεια οιασδήποτε επεξεργασίας ή σειράς επεξεργασιών, οι οποίες επιδιώκουν τον ίδιο σκοπό ή συναφείς σκοπούς.
2. Τα παρεχόμενα πληροφοριακά στοιχεία περιλαμβάνουν:
 - α) το όνομα και τη διεύθυνση του υπευθύνου της επεξεργασίας καθώς και μνεία των υπηρεσιών ενός οργάνου ή οργανισμού που είναι επιφορτισμένο με την επεξεργασία δεδομένων προσωπικού χαρακτήρα για έναν συγκεκριμένο σκοπό,
 - β) τον σκοπό ή τους σκοπούς της επεξεργασίας,
 - γ) περιγραφή της κατηγορίας ή των κατηγοριών των υποκειμένων των δεδομένων και των δεδομένων ή κατηγοριών δεδομένων στα οποία αναφέρονται,
 - δ) τη νομική βάση της επεξεργασίας για την οποία προορίζονται τα δεδομένα,
 - ε) τους αποδέκτες ή τις κατηγορίες αποδεκτών στους οποίους ενδέχεται να ανακοινωθούν τα δεδομένα,
 - στ) μια γενική ένδειξη των καταληκτικών ημερομηνιών για το κλειδωμά και τη διαγραφή των διαφόρων κατηγοριών δεδομένων,
 - ζ) τις προτεινόμενες διαβιβάσεις δεδομένων προς τρίτες χώρες ή διεθνείς οργανισμούς,
 - η) γενική περιγραφή που να επιτρέπει την προκαταρκτική αξιολόγηση σχετικά με την καταλληλότητα των μέτρων που λαμβάνονται κατ' εφαρμογή του άρθρου 22 με σκοπό την κατοχύρωση της ασφάλειας της επεξεργασίας.

3. Οποιαδήποτε μεταβολή η οποία επηρεάζει τα αναφερόμενα στην παράγραφο 2 πληροφοριακά στοιχεία, γνωστοποιείται ταχέως στον υπεύθυνο προστασίας δεδομένων.

Άρθρο 26

Μητρώο

Κάθε υπεύθυνος προστασίας δεδομένων τηρεί μητρώο των επεξεργασιών που του κοινοποιούνται δυνάμει του άρθρου 25.

Τα μητρώα περιέχουν τουλάχιστον τις πληροφορίες που αναφέρονται στο άρθρο 25 παράγραφος 2 σημεία α) έως ζ). Οποιοσδήποτε μπορεί να συμβουλευτεί τα μητρώα με άμεσο ή έμμεσο τρόπο, μέσω του ευρωπαϊού επόπτη προστασίας δεδομένων.

ΤΜΗΜΑ 9

ΠΡΟΚΑΤΑΡΚΤΙΚΟΣ ΕΛΕΓΧΟΣ ΕΚ ΜΕΡΟΥΣ ΤΟΥ ΕΥΡΩΠΑΙΟΥ ΕΠΟΠΤΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΥΠΟΧΡΕΩΣΗ ΣΥΝΕΡΓΑΣΙΑΣ

Άρθρο 27

Προκαταρκτικοί έλεγχοι

1. Οι επεξεργασίες, οι οποίες ενδέχεται να παρουσιάσουν ιδιαίτερους κινδύνους για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων λόγω της φύσης, της εμβέλειας ή των σκοπών τους, υποβάλλονται σε προκαταρκτικό έλεγχο εκ μέρους του ευρωπαϊού επόπτη προστασίας δεδομένων.

2. Οι επεξεργασίες που ενδέχεται να παρουσιάσουν τέτοιους κινδύνους είναι οι ακόλουθες:

- α) οι επεξεργασίες δεδομένων σχετικά με την υγεία και οι επεξεργασίες δεδομένων σχετικά με υποψία τέλεσης αδικήματος, αδικήμα, ποινική καταδίκη ή μέτρα ασφαλείας,
- β) οι επεξεργασίες που αποσκοπούν στην αξιολόγηση της προσωπικότητας των υποκειμένων των δεδομένων, όπως οι ικανότητές τους, η απόδοσή τους ή η συμπεριφορά τους,
- γ) οι επεξεργασίες που επιτρέπουν διασυνδέσεις μεταξύ δεδομένων που αποτελούν αντικείμενο επεξεργασίας για διαφορετικούς σκοπούς και οι οποίες δεν προβλέπονται από το εθνικό ή το κοινοτικό δίκαιο,
- δ) οι επεξεργασίες που έχουν ως σκοπό τον αποκλεισμό ενός ατόμου από κάποιο δικαίωμα, παροχή ή σύμβαση.

3. Οι προκαταρκτικοί έλεγχοι διενεργούνται από τον ευρωπαίο επόπτη προστασίας δεδομένων μετά τη λήψη της κοινοποίησης από τον υπεύθυνο προστασίας δεδομένων, ο οποίος, σε περίπτωση αμφιβολίας όσον αφορά την ανάγκη προκαταρκτικού ελέγχου, συμβουλευτεί τον ευρωπαίο επόπτη προστασίας δεδομένων.

4. Ο ευρωπαίος επόπτης προστασίας δεδομένων γνωμοδοτεί εντός δύο μηνών από τη λήψη της κοινοποίησης. Η προθεσμία αυτή μπορεί να αναστέλλεται έως ότου λάβει τις ζητηθείσες συμπληρωματικές πληροφορίες ο ευρωπαίος επόπτης προστασίας δεδομένων. Εφ' όσον το απαιτεί η πολυπλοκότητα του φακέλου, η προθεσμία αυτή μπορεί επίσης να παραταθεί για νέα περίοδο δύο μηνών κατόπιν απόφασης του ευρωπαϊού επόπτη προστασίας των δεδομένων. Η εν λόγω απόφαση κοινοποιείται στον υπεύθυνο επεξεργασίας πριν από τη λήξη της αρχικής περιόδου των δύο μηνών.

Εάν, στο πέρας της δίμηνης προθεσμίας, η οποία ενδεχομένως παρατείνεται, δεν υπάρχει γνωμοδότηση, τότε η γνώμη τεκμαίρεται θετική.

Εάν ο ευρωπαίος επόπτης προστασίας δεδομένων γνωμοδοτήσει ότι, η κοινοποιηθείσα επεξεργασία ενδέχεται να συνιστά παράβαση κάποιας διάταξης του παρόντος κανονισμού, τότε ο ευρωπαίος επόπτης υποβάλλει, ανάλογα με την περίπτωση, προτάσεις για να αποφευχθεί μια τέτοια παράβαση. Εάν ο υπεύθυνος της επεξεργασίας δεν μεταβάλει αναλόγως την επεξεργασία, τότε ο ευρωπαίος επόπτης προστασίας δεδομένων μπορεί να ασκήσει τις εξουσίες που του απονέμονται από το άρθρο 47 παράγραφος 1.

5. Ο ευρωπαίος επόπτης προστασίας δεδομένων τηρεί μητρώο με όλες τις επεξεργασίες που του κοινοποιούνται δυνάμει της παραγράφου 2. Το μητρώο περιλαμβάνει τις πληροφορίες που αναφέρονται στο άρθρο 25. Οποιοσδήποτε μπορεί να συμβουλευθεί το μητρώο.

Άρθρο 28**Διαβούλευση**

1. Τα όργανα και οι οργανισμοί της Κοινότητας ενημερώνουν τον ευρωπαϊό επόπτη προστασίας δεδομένων οσάκις εκπονούν διοικητικά μέτρα που σχετίζονται με την επεξεργασία δεδομένων προσωπικού χαρακτήρα στην οποία μετέχει όργανο ή οργανισμός της Κοινότητας, είτε αυτοτελώς, είτε από κοινού με άλλους.
2. Η Επιτροπή, οσάκις εγκρίνει νομοθετική πρόταση σχετικά με την προστασία των δικαιωμάτων και των ελευθεριών των προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, συμβουλευεται τον ευρωπαϊό επόπτη προστασίας δεδομένων.

Άρθρο 29**Υποχρέωση ενημέρωσης**

Τα όργανα και οι οργανισμοί της Κοινότητας γνωστοποιούν στον ευρωπαϊό επόπτη προστασίας δεδομένων τα μέτρα που λαμβάνουν κατόπιν αποφάσεως ή αδείας του τελευταίου που προβλέπεται στο άρθρο 46 σημείο η).

Άρθρο 30**Υποχρέωση συνεργασίας**

Κατόπιν αιτήσεώς του, οι υπεύθυνοι της επεξεργασίας επικουρούν τον ευρωπαϊό επόπτη προστασίας δεδομένων κατά την εκτέλεση των καθηκόντων του, ιδίως παρέχοντάς του τις πληροφορίες που αναφέρονται στο άρθρο 47 παράγραφος 2 σημείο α) και δίδοντάς του την πρόσβαση, η οποία προβλέπεται στο άρθρο 47 παράγραφος 2 σημείο β).

Άρθρο 31**Υποχρέωση απάντησης σε καταγγελίες παραβάσεων**

Σε απάντηση της άσκησης των αρμοδιοτήτων του ευρωπαϊού επόπτη προστασίας δεδομένων δυνάμει του άρθρου 47 παράγραφος 1 σημείο β), ο υπεύθυνος της συγκεκριμένης επεξεργασίας τον ενημερώνει για την άποψή του, εντός ευλόγου προθεσμίας την οποία τάσσει ο ευρωπαίος επόπτης προστασίας δεδομένων. Η γνώμη αυτή περιλαμβάνει επίσης περιγραφή των μέτρων που έχουν ενδεχομένως ληφθεί, σε απάντηση των παρατηρήσεων του ευρωπαϊού επόπτη προστασίας δεδομένων.

ΚΕΦΑΛΑΙΟ III**ΕΝΔΙΚΑ ΜΕΣΑ****Άρθρο 32****Προσφυγή**

1. Το Δικαστήριο των Ευρωπαϊκών Κοινοτήτων είναι αρμόδιο για την εκδίκαση κάθε διαφοράς που σχετίζεται με τις διατάξεις του παρόντος κανονισμού, συμπεριλαμβανομένων των αιτήσεων αποζημίωσης.
2. Με την επιφύλαξη δικαστικής προσφυγής, κάθε υποκείμενο δεδομένων μπορεί να καταθέτει ένσταση στον ευρωπαϊό επόπτη προστασίας δεδομένων εφόσον θεωρεί ότι τα δικαιώματα που του παρέχει το άρθρο 286 της συνθήκης παραβιάστηκαν εξαιτίας της επεξεργασίας δεδομένων προσωπικού χαρακτήρα που το αφορούν, εκ μέρους ενός οργάνου ή οργανισμού της Κοινότητας.
Η έλλειψη απάντησης του ευρωπαϊού επόπτη προστασίας δεδομένων εντός προθεσμίας έξι μηνών, ισοδυναμεί με απόφαση απόρριψης της ένστασης.
3. Οι αποφάσεις του ευρωπαϊού επόπτη προστασίας δεδομένων, δύνανται να προσβάλλονται ενώπιον του Δικαστηρίου των Ευρωπαϊκών Κοινοτήτων.
4. Κάθε πρόσωπο που έχει υποστεί ζημία λόγω παράνομης επεξεργασίας ή λόγω οιασδήποτε ενέργειας ασυμβίβαστης με τον παρόντα κανονισμό, έχει το δικαίωμα να απαιτήσει την επανόρθωση της ζημίας που υπέστη σύμφωνα με το άρθρο 288 της συνθήκης.

Άρθρο 33**Ενστάσεις του προσωπικού των Κοινοτήτων**

Κάθε πρόσωπο το οποίο απασχολείται από όργανο ή οργανισμό της Κοινότητας δύναται να υποβάλλει ένσταση στον ευρωπαϊό επόπτη προστασίας δεδομένων επικαλούμενο παράβαση των διατάξεων του παρόντος κανονισμού που διέπει την επεξεργασία δεδομένων προσωπικού χαρακτήρα, χωρίς να ακολουθηθεί η επίσημη οδός. Κανείς δεν επιτρέπεται να υποστεί ζημία διότι έχει υποβάλλει ένσταση προς τον ευρωπαϊό επόπτη προστασίας δεδομένων, με την οποία επικαλείται παραβίαση των διατάξεων που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

ΚΕΦΑΛΑΙΟ IV

ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ ΚΑΙ ΤΗΣ ΙΔΙΩΤΙΚΗΣ ΖΩΗΣ ΣΤΟ ΠΛΑΙΣΙΟ ΕΣΩΤΕΡΙΚΩΝ ΔΙΚΤΥΩΝ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

Άρθρο 34

Πεδίο εφαρμογής

Υπό την επιφύλαξη των άλλων διατάξεων του παρόντος κανονισμού, το παρόν κεφάλαιο διέπει την επεξεργασία δεδομένων προσωπικού χαρακτήρα η οποία σχετίζεται με τη χρήση τηλεπικοινωνιακών δικτύων ή τερματικών εξοπλισμών που λειτουργούν υπό τον έλεγχο οργάνου ή οργανισμού της Κοινότητας.

Για τους σκοπούς του παρόντος κεφαλαίου, ως «χρήστης» νοείται κάθε φυσικό πρόσωπο που χρησιμοποιεί ένα τηλεπικοινωνιακό δίκτυο ή έναν τερματικό εξοπλισμό που λειτουργούν υπό τον έλεγχο οργάνου ή οργανισμού της Κοινότητας.

Άρθρο 35

Ασφάλεια

1. Τα όργανα και οι οργανισμοί της Κοινότητας λαμβάνουν τα ενδεδειγμένα τεχνικά και οργανωτικά μέτρα με σκοπό την κατοχύρωση της ασφαλούς χρήσης των τηλεπικοινωνιακών δικτύων και του τερματικού εξοπλισμού, ενδεχομένως σε συνεννόηση με τους φορείς παροχής κοινόχρηστων τηλεπικοινωνιακών υπηρεσιών ή τους φορείς παροχής δημόσιων τηλεπικοινωνιακών δικτύων. Τα εν λόγω μέτρα είναι ικανά να κατοχυρώνουν ένα βαθμό ασφάλειας ανάλογο με το μέγεθος του κινδύνου, λαμβανομένης υπόψη της πλέον πρόσφατης επιστημονικής πρόοδου και του κόστους της εφαρμογής των εν λόγω μέτρων.

2. Όταν συντρέχει ιδιαίτερος κίνδυνος παραβίασης της ασφάλειας του δικτύου και του τερματικού εξοπλισμού, το οικείο όργανο ή οργανισμός της Κοινότητας ενημερώνει τους χρήστες του δικτύου για τον κίνδυνο αυτό, καθώς και για τα μέτρα που είναι δυνατόν να άρουν τον κίνδυνο και τα εναλλακτικά μέσα επικοινωνίας που μπορούν να χρησιμοποιηθούν.

Άρθρο 36

Εμπιστευτικός χαρακτήρας των επικοινωνιών

Τα όργανα και οι οργανισμοί της Κοινότητας διασφαλίζουν τον εμπιστευτικό χαρακτήρα των επικοινωνιών μέσω τηλεπικοινωνιακών δικτύων και τερματικού εξοπλισμού, τηρουμένων των γενικών αρχών του κοινοτικού δικαίου.

Άρθρο 37

Δεδομένα κίνησης και χρέωσης

1. Με την επιφύλαξη των παραγράφων 2, 3 και 4, τα αναφερόμενα στους χρήστες δεδομένα κινήσεως τα οποία υποβάλλονται σε επεξεργασία και εισάγονται στη μνήμη με σκοπό την καταγραφή των κλήσεων ή των λοιπών συνδέσεων μέσω του εκάστοτε τηλεπικοινωνιακού δικτύου, διαγράφονται ή καθίστανται ανώνυμα κατά το πέρας της συγκεκριμένης κλήσης ή άλλης σύνδεσης.

2. Εάν απαιτείται, για τους σκοπούς της διαχείρισης του προϋπολογισμού των τηλεπικοινωνιακών δικτύων και της διαχείρισης της κίνησης, συμπεριλαμβανομένου του ελέγχου της επιτρεπόμενης χρήσης του τηλεπικοινωνιακού συστήματος, επιτρέπεται η επεξεργασία των σχετικών με την κίνηση δεδομένων, όπως ορίζονται σε κατάλογο ο οποίος εγκρίνεται από τον ευρωπαϊκό επόπτη προστασίας δεδομένων. Αυτά τα δεδομένα διαγράφονται ή καθίστανται ανώνυμα το συντομότερο δυνατό, το αργότερο σε έξι μήνες μετά τη συλλογή τους, εκτός εάν η μεταγενέστερη διατήρησή τους είναι απαραίτητη για την αναγνώριση, την άσκηση ή την υπεράσπιση δικαιώματος στο πλαίσιο αγωγής υπό εκδίκαση ενώπιον δικαστηρίου.

3. Η επεξεργασία των δεδομένων κίνησης και χρέωσης γίνεται μόνον από πρόσωπα που είναι υπεύθυνα για τη διαχείριση της χρέωσης, της κίνησης ή του προϋπολογισμού.

4. Οι χρήστες τηλεπικοινωνιακών δικτύων έχουν το δικαίωμα να λαμβάνουν τιμολόγια ή μη αναλυτικούς λογαριασμούς των κλήσεων που πραγματοποιήθηκαν.

Άρθρο 38

Κατάλογοι χρηστών

1. Τα δεδομένα προσωπικού χαρακτήρα που περιλαμβάνονται σε έντυπους ή ηλεκτρονικούς καταλόγους χρηστών και η πρόσβαση στους καταλόγους αυτούς, περιορίζονται σε ό,τι είναι απολύτως αναγκαίο για τους ειδικούς σκοπούς του καταλόγου.

2. Τα όργανα και οι οργανισμοί της Κοινότητας λαμβάνουν όλα τα αναγκαία μέτρα προκειμένου τα δεδομένα προσωπικού χαρακτήρα που περιέχονται στους καταλόγους, να μην χρησιμοποιούνται για άμεση προώθηση προϊόντων, ανεξάρτητα από το εάν τα δεδομένα αυτά είναι ή όχι προσιτά στο κοινό.

Άρθρο 39

Ένδειξη και περιορισμός της αναγνώρισης καλούσας και καλούμενης γραμμής

1. Όταν παρέχεται ένδειξη της αναγνώρισης της καλούσας γραμμής, ο καλών χρήστης πρέπει να έχει τη δυνατότητα, με απλά μέσα και ατελώς, να απαλείφει την ένδειξη της αναγνώρισης της καλούσας γραμμής.
2. Όταν παρέχεται ένδειξη της αναγνώρισης της καλούσας γραμμής, ο καλούμενος χρήστης πρέπει να έχει τη δυνατότητα, με απλά μέσα και ατελώς, να εμποδίζει την ένδειξη της αναγνώρισης της καλούσας γραμμής για τις εισερχόμενες κλήσεις.
3. Όταν παρέχεται ένδειξη της αναγνώρισης της καλούμενης γραμμής, ο καλούμενος χρήστης πρέπει να έχει τη δυνατότητα, με απλά μέσα και ατελώς, να απαλείφει την ένδειξη της αναγνώρισης της καλούμενης γραμμής στον καλούντα χρήστη.
4. Όταν παρέχεται ένδειξη της αναγνώρισης της καλούσας ή καλούμενης γραμμής, τα όργανα και οι οργανισμοί της Κοινότητας ενημερώνουν τους χρήστες για το γεγονός αυτό, καθώς και για τις δυνατότητες που προβλέπονται στις παραγράφους 1, 2 και 3.

Άρθρο 40

Παρεκκλίσεις

Τα όργανα και οι οργανισμοί της Κοινότητας διασφαλίζουν ότι υπάρχουν διαφανείς διαδικασίες οι οποίες διέπουν τον τρόπο με τον οποίο μπορούν να αντιτάσσονται στην απόρριψη της ένδειξης της αναγνώρισης της καλούσας γραμμής, ως εξής:

- α) προσωρινώς, κατόπιν αιτήσεως του χρήστη που ζητά τον εντοπισμό των κακόβουλων ή ενοχλητικών κλήσεων,
- β) για κάθε γραμμή χωριστά, προκειμένου για τους οργανισμούς που ασχολούνται με τις κλήσεις άμεσης επέμβασης, ώστε να δίδεται απάντηση σε τέτοιου είδους κλήσεις.

ΚΕΦΑΛΑΙΟ V

ΑΝΕΞΑΡΤΗΤΗ ΕΠΟΠΤΙΚΗ ΑΡΧΗ: ΕΥΡΩΠΑΙΟΣ ΕΠΟΠΤΗΣ ΠΡΟΣΤΑΣΙΑΣ ΤΩΝ ΔΕΔΟΜΕΝΩΝ

Άρθρο 41

Ευρωπαίος επόπτης προστασίας των δεδομένων

1. Συνιστάται ανεξάρτητη εποπτική αρχή, καλούμενη στο εξής «ευρωπαίος επόπτης προστασίας δεδομένων».
2. Όσον αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα, ο ευρωπαίος επόπτης προστασίας δεδομένων είναι επιφορτισμένος να εξασφαλίζει ότι τα όργανα και οι οργανισμοί της Κοινότητας σέβονται τα θεμελιώδη δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ιδίως την ιδιωτική τους ζωή.

Ο ευρωπαίος επόπτης προστασίας δεδομένων είναι επιφορτισμένος με την παρακολούθηση και την εξασφάλιση της εφαρμογής των διατάξεων του παρόντος κανονισμού και κάθε άλλης κοινοτικής πράξης στον τομέα της προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα που πραγματοποιείται από ένα όργανο ή έναν οργανισμό της Κοινότητας, και για την παροχή συμβουλών προς τα όργανα και τους οργανισμούς της Κοινότητας και προς τα υποκείμενα των δεδομένων για κάθε θέμα που αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Προς το σκοπό αυτό, ο ευρωπαίος επόπτης προστασίας δεδομένων εκτελεί τα καθήκοντα που προβλέπονται στο άρθρο 46 και ασκεί τις αρμοδιότητες που του παρέχονται από το άρθρο 47.

Άρθρο 42

Διορισμός

1. Το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο διορίζουν, με κοινή συμφωνία, τον ευρωπαίο επόπτη προστασίας δεδομένων για πέντε έτη, βάσει καταλόγου που συντάσσει η Επιτροπή κατόπιν δημόσιας πρόσκλησης για υποβολή υποψηφιοτήτων.

Διορίζεται αναπληρωτής επόπτης σύμφωνα με την ίδια διαδικασία και για την ίδια χρονική διάρκεια. Επικουρεί τον επόπτη στο σύνολο των καθηκόντων του και τον αναπληρώνει σε περίπτωση απουσίας ή κωλύματος.

2. Ο ευρωπαίος επόπτης προστασίας δεδομένων επιλέγεται μεταξύ προσώπων τα οποία παρέχουν εχέγγυα ανεξαρτησίας και διαθέτουν αξιόλογη εμπειρία και ικανότητες για την εκπλήρωση των καθηκόντων του ευρωπαϊού επόπτη προστασίας δεδομένων, πχ. διότι συμμετέχουν ή είχαν συμμετάσχει στις αρχές ελέγχου που αναφέρονται στο άρθρο 28 της οδηγίας 95/46/ΕΚ.
3. Η θητεία του ευρωπαϊού επόπτη προστασίας δεδομένων δύναται να ανανεωθεί.
4. Εκτός από την κανονική ανανέωση και τον θάνατο, η θητεία του ευρωπαϊού επόπτη προστασίας δεδομένων λήγει σε περίπτωση παραίτησης ή υποχρεωτικής συνταξιοδότησης σύμφωνα με την παράγραφο 5.
5. Το Δικαστήριο δύναται να απαλλάξει τον ευρωπαίο επόπτη προστασίας δεδομένων από τα καθήκοντά του ή να τον κηρύξει έκπτωτο από το δικαίωμα παροχής συντάξεως ή άλλων ευεργετημάτων που εξομοιούνται με σύνταξη, κατόπιν αιτήσεως του Ευρωπαϊκού Κοινοβουλίου, του Συμβουλίου ή της Επιτροπής, εάν παύσει να πληροί τις προϋποθέσεις που απαιτούνται για την άσκηση των καθηκόντων του ή εάν διαπράξει βαρύ παράπτωμα.
6. Στις περιπτώσεις κανονικής ανανέωσης και εκούσιας παραίτησης, ο ευρωπαίος επόπτης προστασίας δεδομένων παραμένει ωστόσο εν υπηρεσία μέχρι την αντικατάστασή του.
7. Τα άρθρα 12 έως και 15 και 18 του πρωτοκόλλου περί των προνομίων και ασυλιών των Ευρωπαϊκών Κοινοτήτων, ισχύουν και για τον ευρωπαίο επόπτη προστασίας δεδομένων.
8. Οι παράγραφοι 2 έως 7 ισχύουν και για τον αναπληρωτή επόπτη.

Άρθρο 43

Καθεστώς και γενικοί όροι άσκησης των καθηκόντων του ευρωπαϊού επόπτη προστασίας δεδομένων, ανθρώπινο δυναμικό και οικονομικοί πόροι

1. Το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο και η Επιτροπή καθορίζουν, με κοινή συμφωνία, το καθεστώς και τους γενικούς όρους άσκησης των καθηκόντων του ευρωπαϊού επόπτη προστασίας δεδομένων, και ιδίως το μισθό, τα επιδόματα και οποιαδήποτε άλλη παροχή εξομοιούμενη με αποδοχές.
2. Η αρμόδια επί του προϋπολογισμού αρχή φροντίζει ώστε ο ευρωπαίος επόπτης προστασίας δεδομένων να διαθέτει το ανθρώπινο δυναμικό και τους οικονομικούς πόρους που χρειάζονται για την εκτέλεση των καθηκόντων του.
3. Ο προϋπολογισμός του ευρωπαϊού επόπτη προστασίας δεδομένων περιλαμβάνεται σε ειδική γραμμή του τμήματος VIII του γενικού προϋπολογισμού της Ευρωπαϊκής Ένωσης.
4. Ο ευρωπαίος επόπτης προστασίας δεδομένων επικουρείται από γραμματεία. Οι υπάλληλοι και τα μέλη του λοιπού προσωπικού της γραμματείας διορίζονται από τον ευρωπαίο επόπτη προστασίας δεδομένων, των οποίων είναι ο ιεραρχικά προϊστάμενος και στον οποίο υπάγονται αποκλειστικά. Ο αριθμός τους καθορίζεται κάθε χρόνο στα πλαίσια της διαδικασίας του προϋπολογισμού.
5. Οι υπάλληλοι και τα μέλη του λοιπού προσωπικού της γραμματείας του ευρωπαϊού επόπτη προστασίας δεδομένων, υπόκεινται στους κανονισμούς και τις ρυθμίσεις που εφαρμόζονται στους υπαλλήλους και το λοιπό προσωπικό των Ευρωπαϊκών Κοινοτήτων.
6. Για τα θέματα που αφορούν το προσωπικό του, ο ευρωπαίος επόπτης προστασίας δεδομένων εξομοιούται με τα όργανα κατά την έννοια του άρθρου 1 του κανονισμού υπηρεσιακής κατάστασης των υπαλλήλων των Ευρωπαϊκών Κοινοτήτων.

Άρθρο 44

Ανεξαρτησία

1. Ο ευρωπαίος επόπτης προστασίας δεδομένων απολαύει πλήρους ανεξαρτησίας κατά την εκτέλεση των καθηκόντων του.
2. Κατά την εκτέλεση των καθηκόντων του, ο ευρωπαίος επόπτης προστασίας δεδομένων δεν ζητά ούτε δέχεται εντολές από οιονδήποτε.
3. Ο ευρωπαίος επόπτης προστασίας δεδομένων απέχει από οποιαδήποτε πράξη η οποία δεν συμβιβάζεται με τα καθήκοντά του και δεν ασκεί, κατά τη διάρκεια της θητείας του, καμία άλλη επαγγελματική δραστηριότητα, αμειβόμενη ή μη.

4. Μετά τη λήξη της θητείας του, ο ευρωπαίος επόπτης προστασίας δεδομένων υποχρεούται να συμπεριφέρεται με ακεραιότητα και διακριτικότητα σε σχέση με την αποδοχή ορισμένων θέσεων και ευεργετημάτων.

Άρθρο 45

Επαγγελματικό απόρρητο

Ο ευρωπαίος επόπτης προστασίας δεδομένων και το προσωπικό του υποχρεούνται, τόσο κατά τη διάρκεια της θητείας τους όσο και μετά τη λήξη της, να τηρούν το επαγγελματικό απόρρητο όσον αφορά οιοσδήποτε εμπιστευτικές πληροφορίες που έχουν περιέλθει σε γνώση τους κατά την εκτέλεση των καθηκόντων τους.

Άρθρο 46

Καθήκοντα

Ο ευρωπαίος επόπτης προστασίας δεδομένων:

- α) ακούει και εξετάζει τις ενστάσεις και ενημερώνει το υποκείμενο των δεδομένων για τα αποτελέσματα της έρευνάς του εντός ευλόγου προθεσμίας,
- β) διενεργεί έρευνες είτε με δική του πρωτοβουλία είτε βάσει ένστασης, και ενημερώνει τα υποκείμενα των δεδομένων για τα αποτελέσματα της έρευνάς του εντός εύλογου προθεσμίας,
- γ) ελέγχει και διασφαλίζει την εφαρμογή του παρόντος κανονισμού και κάθε άλλης κοινοτικής πράξης που αφορά την προστασία φυσικών προσώπων από την επεξεργασία δεδομένων προσωπικού χαρακτήρα από όργανο ή οργανισμό της Κοινότητας, με εξαίρεση το Δικαστήριο των Ευρωπαϊκών Κοινοτήτων, στα πλαίσια της άσκησης των δικαιωμάτων του καθηκόντων,
- δ) συμβουλεύει το σύνολο των οργάνων και οργανισμών της Κοινότητας, είτε με δική του πρωτοβουλία είτε αφού ζητηθεί η γνώμη του επί όλων των θεμάτων που άπτονται της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, ιδίως πριν από τη θέσπιση εσωτερικών κανόνων σχετικά με την προστασία των θεμελιωδών δικαιωμάτων και ελευθεριών έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα εν λόγω όργανα και οργανισμούς,
- ε) παρακολουθεί τις εξελίξεις που παρουσιάζουν ενδιαφέρον, στο μέτρο που έχουν επιπτώσεις για την προστασία των δεδομένων προσωπικού χαρακτήρα, ιδίως τις εξελίξεις της τεχνολογίας της πληροφορίας και των επικοινωνιών,
- στ) i) συνεργάζεται με τις εθνικές εποπτεύουσες αρχές, που αναφέρονται στο άρθρο 28 της οδηγίας 95/46/EK, των χωρών στις οποίες εφαρμόζεται η εν λόγω οδηγία, στο βαθμό που τούτο είναι αναγκαίο για την εκτέλεση των αντιστοίχων καθηκόντων τους, ιδίως ανταλλάσσοντας κάθε χρήσιμη πληροφορία, καλώντας τις αρχές ή τους φορείς αυτούς να ασκήσουν τις εξουσίες τους ή ανταποκρινόμενος σε αιτήματα των αρχών ή φορέων αυτών,
ii) συνεργάζεται επίσης με τους εποπτικούς φορείς προστασίας δεδομένων που συνιστώνται δυνάμει του τίτλου VI της συνθήκης για την Ευρωπαϊκή Ένωση, ιδίως προκειμένου να βελτιωθεί η συνοχή στην εφαρμογή των κανόνων και διαδικασιών των οποίων την τήρηση έχουν αντιστοίχως αναλάβει να εξασφαλίζουν.
- ζ) συμμετέχει στις εργασίες της ομάδας προστασίας των προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, η οποία έχει συσταθεί δυνάμει του άρθρου 29 της οδηγίας 95/46/EK,
- η) καθορίζει, αιτιολογεί και δημοσιοποιεί τις εξαιρέσεις, τις εγγυήσεις, τις άδειες και τις προϋποθέσεις που αναφέρονται στο άρθρο 10 παράγραφος 2 στοιχείο β), παράγραφοι 4, 5 και 6, στο άρθρο 12 παράγραφος 2, στο άρθρο 19 και στο άρθρο 37 παράγραφος 2,
- θ) τηρεί μητρώο με τις επεξεργασίες οι οποίες του κοινοποιούνται δυνάμει του άρθρου 27 παράγραφος 2 και οι οποίες καταγράφονται σύμφωνα με το άρθρο 27 παράγραφος 5, και παρέχει τα μέσα πρόσβασης στα μητρώα που τηρούν οι υπεύθυνοι προστασίας δεδομένων κατ' εφαρμογήν του άρθρου 26,
- ι) διενεργεί προκαταρκτικό έλεγχο επί των επεξεργασιών που του κοινοποιούνται,
- ια) θεσπίζει τον εσωτερικό του κανονισμό.

Άρθρο 47

Αρμοδιότητες

1. Ο ευρωπαίος επόπτης προστασίας δεδομένων μπορεί:
 - α) να παρέχει συμβουλές στα υποκείμενα των δεδομένων κατά την άσκηση των δικαιωμάτων τους,
 - β) να εντέλλεται τον υπεύθυνο της επεξεργασίας δεδομένων να επιληφθεί σε περίπτωση προβαλλόμενης παραβίασης των διατάξεων που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα και, ενδεχομένως, να διατυπώνει προτάσεις για την επανόρθωση αυτής της παραβίασης και τη βελτίωση της προστασίας των υποκειμένων των δεδομένων,
 - γ) να εντέλλεται την ικανοποίηση των αιτημάτων για την άσκηση ορισμένων δικαιωμάτων όσον αφορά τα δεδομένα εάν τα εν λόγω αιτήματα έχουν απορριφθεί κατά παράβαση των άρθρων 13 έως 19,
 - δ) να προειδοποιεί ή να επιπλήττει τον εκάστοτε υπεύθυνο της επεξεργασίας,
 - ε) να εντέλλεται τη διόρθωση, το κλείδωμα, τη διαγραφή ή την καταστροφή οιοδήποτε δεδομένου που έχει τύχει επεξεργασίας κατά παράβαση των διατάξεων που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα και την κοινοποίηση των μέτρων αυτών στους τρίτους στους οποίους έχουν κοινολογηθεί τα δεδομένα,
 - στ) να επιβάλλει προσωρινή ή οριστική απαγόρευση της επεξεργασίας,
 - ζ) να προσφεύγει στο οικείο όργανο ή οργανισμό και, εάν παρίσταται αναγκαίο, στο Ευρωπαϊκό Κοινοβούλιο, στο Συμβούλιο και στην Επιτροπή,
 - η) να προσφεύγει στο Δικαστήριο των Ευρωπαϊκών Κοινοτήτων υπό τους όρους που προβλέπει η συνθήκη,
 - θ) να παρεμβαίνει στις υποθέσεις που φέρονται ενώπιον του Δικαστηρίου των Ευρωπαϊκών Κοινοτήτων.
2. Ο επόπτης της προστασίας δεδομένων είναι εξουσιοδοτημένος:
 - α) να απαιτεί από έναν υπεύθυνο της επεξεργασίας ή από ένα όργανο ή οργανισμό της Κοινότητας, πρόσβαση σε όλα τα δεδομένα προσωπικού χαρακτήρα και σε όλες τις πληροφορίες που απαιτούνται για τις έρευνές του,
 - β) να απαιτεί πρόσβαση σε όλους τους χώρους στους οποίους ασκεί τις δραστηριότητές του ένας υπεύθυνος επεξεργασίας ή ένα όργανο ή οργανισμός της Κοινότητας, εφόσον ευλόγως εικάζεται ότι ασκείται δραστηριότητα διεπόμενη από τον παρόντα κανονισμό.

Άρθρο 48

Έκθεση πεπραγμένων

1. Ο ευρωπαίος επόπτης προστασίας δεδομένων υποβάλλει κάθε χρόνο στο Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο και την Επιτροπή έκθεση πεπραγμένων και ταυτόχρονα τη δημοσιεύει.
2. Ο ευρωπαίος επόπτης διαβιβάζει την έκθεση πεπραγμένων στα άλλα όργανα και τους οργανισμούς της Κοινότητας, τα οποία μπορούν να υποβάλλουν σχόλια ενόψει της ενδεχόμενης εξέτασης της έκθεσης στο Ευρωπαϊκό Κοινοβούλιο, ιδίως σε σχέση με την περιγραφή των μέτρων που λαμβάνονται σε απάντηση των παρατηρήσεων του ευρωπαίου επόπτη προστασίας δεδομένων δυνάμει του άρθρου 31.

ΚΕΦΑΛΑΙΟ VI

ΤΕΛΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 49

Κυρώσεις

Κάθε παράλειψη των υποχρεώσεων τις οποίες υπέχει υπάλληλος ή άλλο μέλος του προσωπικού των Ευρωπαϊκών Κοινοτήτων δυνάμει του παρόντος κανονισμού, η οποία διαπράττεται εκ προθέσεως ή εξ αμελείας, επισύρει πειθαρχική κύρωση, σύμφωνα με τις διατάξεις του κανονισμού υπηρεσιακής κατάστασης των υπαλλήλων των Ευρωπαϊκών Κοινοτήτων ή του καθεστώτος που εφαρμόζεται στο λοιπό προσωπικό.

Άρθρο 50

Μεταβατική περίοδος

Τα όργανα και οι οργανισμοί της Κοινότητας λαμβάνουν τα αναγκαία μέτρα προκειμένου όλες οι εργασίες επεξεργασίας που έχουν ήδη αρχίσει κατά την ημερομηνία έναρξης ισχύος του παρόντος κανονισμού, να συμμορφούνται με τις διατάξεις του, εντός προθεσμίας ενός έτους από την εν λόγω ημερομηνία.

Άρθρο 51

Έναρξη ισχύος

Ο παρών κανονισμός αρχίζει να ισχύει την εικοστή ημέρα από τη δημοσίευσή του στην *Επίσημη Εφημερίδα των Ευρωπαϊκών Κοινοτήτων*.

Ο παρών κανονισμός είναι δεσμευτικός ως προς όλα τα μέρη του και ισχύει άμεσα σε κάθε κράτος μέλος.

Βρυξέλλες, 18 Δεκεμβρίου 2000.

Για το Ευρωπαϊκό Κοινοβούλιο

Η Πρόεδρος

N. FONTAINE

Για το Συμβούλιο

Ο Πρόεδρος

D. VOYNET

ΠΑΡΑΡΤΗΜΑ

1. Ο υπεύθυνος προστασίας δεδομένων δύναται να διατυπώνει συστάσεις, για τη βελτίωση της προστασίας δεδομένων από πρακτική άποψη, προς το όργανο ή τον οργανισμό της Κοινότητας που τον διόρισε και να τα συμβουλεύει, καθώς και τον υπεύθυνο της εκάστοτε επεξεργασίας, σχετικά με θέματα που άπτονται της εφαρμογής των διατάξεων περί της προστασίας δεδομένων. Πέραν αυτού, μπορεί να προβαίνει, είτε με δική του πρωτοβουλία, είτε κατόπιν αιτήσεως του οργάνου ή του οργανισμού της Κοινότητας που τον διόρισε, του υπευθύνου της επεξεργασίας, της οικείας επιτροπής προσωπικού ή κάθε φυσικού προσώπου, στη διερεύνηση ζητημάτων και περιστατικών που σχετίζονται ευθέως με τα καθήκοντά του και που υποπίπτουν στην αντίληψή του και να αναφέρει στο πρόσωπο το οποίο ζήτησε την έρευνα ή στον υπεύθυνο της επεξεργασίας.
 2. Είναι δυνατόν να ζητείται άμεσα η γνώμη του υπευθύνου προστασίας δεδομένων, χωρίς να ακολουθηθεί η επίσημη οδός, σχετικά με οποιοδήποτε θέμα άπτεται της ερμηνείας ή της εφαρμογής του παρόντος κανονισμού, από το όργανο ή τον οργανισμό της Κοινότητας που τον διόρισε, τον υπεύθυνο της επεξεργασίας ή την οικεία επιτροπή προσωπικού ή ακόμα από κάθε φυσικό πρόσωπο.
 3. Ουδείς επιτρέπεται να υποστεί ζημία διότι φέρει εις γνώσιν του υπευθύνου προστασίας δεδομένων που είναι αρμόδιος, γεγονός το οποίο ισχυρίζεται ότι συνιστά παραβίαση των διατάξεων του παρόντος κανονισμού.
 4. Κάθε αφορώμενος υπεύθυνος επεξεργασίας υποχρεούται να επικουρεί τον υπεύθυνο προστασίας δεδομένων στην εκπλήρωση των καθηκόντων του και να του παρέχει τις πληροφορίες που ζητάει. Κατά την εκτέλεση των καθηκόντων του, ο υπεύθυνος προστασίας δεδομένων έχει πρόσβαση, ανά πάσα στιγμή, στα δεδομένα που αποτελούν αντικείμενο των εργασιών επεξεργασίας, σε όλους τους χώρους, εγκαταστάσεις επεξεργασίας δεδομένων και υποθέματα πληροφοριών.
 5. Ο υπεύθυνος προστασίας δεδομένων απαλλάσσεται από άλλα καθήκοντα στο βαθμό που τούτο είναι αναγκαίο. Ο υπεύθυνος προστασίας δεδομένων και το προσωπικό του, στους οποίους εφαρμόζεται το άρθρο 287 της συνθήκης, υποχρεούνται να μην κοινολογούν πληροφορίες ή έγγραφα τα οποία περιέρχονται εις γνώσιν ή στην κατοχή τους στο πλαίσιο της άσκησης των καθηκόντων τους.
-

EUROPEAN DATA PROTECTION SUPERVISOR

Opinion of the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the exchange of information under the principle of availability (COM (2005) 490 final)

(2006/C 116/04)

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty establishing the European Community, and in particular its Article 286,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular its Article 8,

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data,

Having regard to the request for an opinion in accordance with Article 28(2) of Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data,

HAS ADOPTED THE FOLLOWING OPINION:

I. PRELIMINARY REMARKS

1. The Proposal for a Council Framework Decision on the exchange of information under the principle of availability has been sent by the Commission to the EDPS by letter of 12 October 2005. The EDPS understands this letter as a request to advise Community institutions and bodies, as foreseen in Article 28(2) of Regulation (EC) No 45/2001. According to the EDPS, the present opinion should be mentioned in the preamble of the Framework Decision.
2. The nature of this opinion has to be seen in the context described under II. As indicated under II, it is far from obvious that the present proposal — or the approach to availability taken by the proposal — will eventually lead to the adoption of a legal instrument. Other approaches are advocated by a considerable number of Member States.
3. However, it is obvious that the subject of the availability of law enforcement information across the internal borders

— or, more widely, the exchange of this information — is high on the agenda of the Member States, inside as well as outside the Council, and within the European Parliament.

4. It is equally obvious that this subject is highly relevant from the perspective of the protection of personal data, as the present opinion itself will illustrate. The EDPS recalls that the present proposal was presented by the Commission with a close link to the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, object of an opinion of the EDPS, presented on 19 December 2005.
5. The EDPS will use this occasion to present in this opinion some general and more fundamental points of view on the subject of exchange of law enforcement information and on the approaches for regulating this subject. By presenting this opinion, the EDPS envisages ensuring that the perspective of data protection will be duly taken into account in future discussions on the subject.
6. The EDPS will be available for further consultation at a later stage, following relevant developments in the legislative process on this proposal as well as on other related proposals.
7. The principle of availability has been introduced as an important new principle of law in the Hague Programme. It entails that information needed for the fight against crime should cross the internal borders of the EU without obstacles. The objective of the present proposal is to implement this principle in a binding legal instrument.
8. The exchange of police information between different countries is a popular subject for legislators, within and outside the framework of the EU. Recently, the following initiatives drew the attention of the EDPS.

II. THE PROPOSAL IN ITS CONTEXT

9. In the first place, on 4 June 2004 Sweden proposed a Framework Decision on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union. On this proposal, the Council has reached an agreement on a general approach in its meeting of 1 December 2005.
 10. In the second place, on 27 May 2005, seven Member States signed a Convention in Prüm (Germany) on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration. It introduces *inter alia* measures to improve information exchange for DNA and fingerprints. The Convention is open for any Member State of the European Union to join. The Contracting Parties aim to incorporate the provisions of the Convention into the legal framework of the European Union.
 11. In the third place, the availability of law enforcement information across the internal borders of the European Union will also be further facilitated by other legal instruments, such as the proposals regarding a Second Generation Schengen Information System (SIS II), the proposal for access for consultation to the Visa Information System (VIS) and the proposal for a Framework Decision on the organisation and content of the exchange of information extracted from criminal records between Member States. In this respect, it is also useful to mention the Communication on improved effectiveness, enhanced operability and synergies among European databases in the area of Justice and Home Affairs, issued by the Commission on 25 November 2005.
 12. Because all of these initiatives have been issued, it follows that the present proposal for a Framework Decision on availability should not be examined by itself, but other approaches to the exchange of law enforcement information should also be taken into account. This is even more important since it is the current tendency within the Council to give preference to other approaches to information exchange and to the concept of availability than the general approach proposed by the Commission in the present proposal. The present text of the proposal might even not be the object of discussion in the Council.
 13. Furthermore, this proposal is closely linked to the Proposal for a Framework Decision on the protection of personal data. The present opinion must be understood in connection with the more profound opinion on the latter Framework Decision.
 14. In his opinion on the Proposal for a Framework Decision on the protection of personal data, the EDPS underlined the importance of adequate data protection as a necessary consequence of a legal instrument on availability. According to the EDPS, such a legal instrument should not be adopted without essential guarantees on data protection.
 15. The EDPS takes the same position in respect of the adoption of other legal instruments that facilitate the flow of law enforcement information across the internal borders of the EU. The EDPS therefore welcomes that the Council as well as the European Parliament have dedicated priority to the aforementioned proposal for a Framework Decision on the protection of personal data.
- ### III. THE AVAILABILITY PRINCIPLE AS SUCH
16. The availability principle is in itself a simple principle. The information that is available to certain authorities in a Member State must also be provided to equivalent authorities in other Member States. The information must be exchanged as swiftly and easily as possible between the authorities of the Member States and preferably by allowing direct online access.
 17. The difficulties arise because of the environment in which the principle of availability has to be made effective:
 - A heterogeneous organisation of the police and the judiciary in the Member States, with different checks and balances.
 - Different types of (sensitive) information are included (such as DNA or fingerprints).
 - Different ways of access to relevant information for competent authorities even within Member States.
 - It is difficult to ensure that information originating from another Member State will be properly interpreted due to differences in languages, in technological systems (interoperability) and in legal systems.
 - It has to be included in the existing and extensive patchwork of legal provisions that deal with the exchange of law enforcement information between countries.
 18. Irrespective of this complex environment, it is common understanding that the principle can not work by itself. Additional measures are needed to ensure that information can effectively be found and accessed. In any case, those measures must make it easier for law enforcement authorities to find out whether law enforcement authorities in other Member States have relevant information at their disposal and where this relevant information can be found. Such additional measures could consist of interfaces that deliver direct access to all or specific data held by other Member States. The proposal for a Framework Decision on availability introduces for this reason 'index data', specific data that can be accessed directly across the borders.

19. In general terms, the availability principle should facilitate the flow of information between the Member States. The internal borders will be abolished and the Member States have to allow that information available to their police authorities will increasingly become accessible for other authorities. The Member States lose competence to control the flow of information, which also results in the fact that they no longer can rely on their national legislation as a sufficient instrument for an adequate protection of the information.
20. It is for this reason that the proposal needs specific attention from the perspective of the protection of personal data. In the first place, information that is normally confidential and well secured must be provided to authorities in other Member States. In the second place, to make the system work index data must be established and made available to authorities in other Member States. The implementation of this principle will, as a consequence, generate more data than currently available.
23. The proposal does not specify whether 'available information' consists merely of information already controlled by competent authorities or also includes information that can be potentially obtained by these authorities. However, according to the EDPS, the proposal could be interpreted as comprising both.
24. Indeed, while Article 2(2) seems to suggest a narrower scope, by specifying that the Framework Decision 'does not entail any obligation to collect and store information [...] for the sole purpose of making it available', Article 3(a) allows a broader interpretation, by stating that 'information' shall mean 'existing information, listed in Annex II'.
25. Annex II mentions at least two categories of data that are commonly controlled by others than the police. The first category is vehicle registration information. In many Member States, the databases containing this information are not controlled by law enforcement authorities, even though they are regularly accessed by these authorities. Should this kind of information fall within the scope of the 'available information' which, according to Article 1, shall be provided to equivalent competent authorities of other Member States? The second category of data listed in Annex II to be mentioned are telephone numbers and other communications data: should these data be considered to be 'available' even when these data are not controlled by competent authorities, but by private companies?

IV. MAIN ELEMENTS

Scope of the principle of availability

21. First of all, it is essential to define to which kind of information the principle of availability will apply. The field of application of this principle is defined in general terms in Article 2 of the proposal, in combination with Article 1(1) and Article 3(a). The principle shall apply to information that is:
 - existing information;
 - listed in Annex II which defines six types of information;
 - available to competent authorities.

These are the three essential elements of the scope of the principle in the proposal by the Commission. The scope is further refined in Article 2. Article 2(1) limits the application of the principle of availability to the stage prior to the commencement of a prosecution, whereas Article 2(2), (3) and (4) provide some more specific restrictions.
22. To understand the consequences of the proposal, a more profound analysis of the three essential elements mentioned above is needed. The first two elements of the scope are by themselves reasonably clear. The definition of 'existing information' is elaborated in Article 2(2) stating that the Framework Decision does not entail any obligation to collect and store information for the sole purpose of making it available, whereas the list in Annex II can not be interpreted in different ways. It is the third essential element, by itself and in combination with the first two elements that needs further clarification.
26. Moreover, other provisions of the proposal, and more particular Articles 3(d) and 4(1)(c) of the proposal, support the view that 'designated authorities' and even 'designated parties' may control information that is 'available' for 'competent authorities'. It also follows from the text of the proposal that a 'competent authority' of a Member State is an authority covered by Article 29, first hyphen, of the EU-Treaty whereas any national authority can qualify as a 'designated authority'.
27. According to the EDPS, application of the availability principle to information that is controlled by designated authorities and designated parties, entails the following questions:
 - Does Article 30(1)(b) provide for a sufficient legal basis, since information has to be made available by designated authorities and designated parties and from databases that do not fall within the framework of the third pillar?
 - Will the Framework Decision on the protection of personal data apply, as is assumed e.g. in Article 8 of the proposal?
 - If not, is the processing in accordance with the obligations under Directive 95/46/EC?

28. The implementation of such a broad principle as the 'principle of availability' requires a clear and precise definition of the data that shall be considered available. Therefore, the EDPS recommends:

- Clarifying the scope.
- As a first option, limiting the scope of the principle of availability to information controlled by competent authorities.
- As a second option, in case of a broader scope, ensuring sufficient safeguards for the protection of personal data. The questions raised in point 27 hereinabove have to be taken into consideration.

Other issues related to the scope

29. According to Article 2(1) of the proposal, the Framework Decision shall apply to the processing of information prior to the commencement of a prosecution. Its scope is more limited than the proposal for a Framework Decision on the protection of personal data that fully applies to judicial cooperation in criminal matters.

30. However, according to the EDPS this limitation does not by itself limit the scope of the proposal to police cooperation. It could also include judicial cooperation in criminal matters since in a number of Member States judicial authorities also have competences on criminal investigations, before the commencement of a prosecution. However, the fact that the proposal is solely based on Article 30(1)(b) TEU seems to indicate that it only applies to police cooperation. A clarification on this aspect would be welcomed.

31. The present proposal applies to providing information to Europol whereas the proposal for a Framework Decision on the protection of personal data excludes the processing of personal data by Europol. The EDPS advises limiting the information exchange with Europol to the purposes of Europol itself, as mentioned in Article 2 of the Europol Convention and the Annex thereof. Moreover, account should be taken of the detailed rules for exchange of data with Europol, which are already laid down in several Council Acts.

No new databases containing personal data

32. The starting point of the proposal is that it will not lead to the construction of new databases containing personal data. To that effect, Article 2(2) is clear: it does not entail any obligation to collect and store information for the sole

purpose of making it available. From the perspective of data protection, this is an important and positive element of the proposal. The EDPS recalls his opinion on the proposal for a directive on the retention of data processed in connection with the provision of public electronic communication ⁽¹⁾ in which he emphasised that legal obligations that lead to substantial databases run particular risks for the data subject, *inter alia* because of risks of illegitimate use.

33. However:

- It is important to ensure that the proposal will not promote an unconditional interconnection of databases and thus a network of databases which will be hard to supervise.
- There is an exception to the starting point mentioned above: Article 10 of the proposal which ensures that index data are available on line. Index data may contain personal data or in any case reveal their existence.

Direct and indirect access to information

34. The proposal provides for direct and indirect access to information. Article 9 of the proposal foresees direct on line access to information contained in databases to which corresponding national authorities have direct on line access. Article 10 entails an indirect access. Index data of information that is not accessible online shall be available for online consultation by equivalent competent authorities of other Member States and Europol. When consultation of index data results in a match, this authority may issue an information demand and send it to the designated authority in order to obtain the information identified by the index data.

35. Direct access does not lead to new databases, but it requires the interoperability of the databases of the equivalent competent systems within the Member States. Moreover, it will necessarily introduce a new usage of already existing databases by providing a facility to all competent authorities of the Member States which until now had only been open to national competent authorities. Direct access will automatically mean that an increased number of persons will have access to a database and therefore encompasses a growing risk of misuse.

⁽¹⁾ Opinion of 26 September 2005 on the Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC (COM (2005) 438 final).

36. In case of direct access by a competent authority of another Member State, the designated authorities of the originating Member State have no control over the access and the further use of the data. This consequence of direct access as foreseen by the proposal has to be properly addressed, since:

- It seems to invalidate the powers of the designated authorities to refuse the provision of information (under Article 14).
- It raises questions as to responsibilities for the accuracy and the keeping up to date of data, once they have been accessed. How can a designated authority of the originating Member State ensure that data are kept up to date?
- It is not only the designated authority that is no longer capable of fulfilling all its obligations under data protection law, but also the national data protection authority of the originating Member State can no longer supervise the application of the obligations since it lacks any competence *vis-a-vis* law enforcement authorities of other Member States.
- These problems are even more predominant in case of access to databases of designated authorities and designated parties, not being law enforcement authorities (see points 25-28 of this opinion).

This consequence of direct access is an important reason why the adoption of the present proposal should depend on the adoption of a Framework Decision on the protection of personal data. One problem remains: it is difficult to see how designated authorities could refuse the provision of information under Article 14.

37. As concerns indirect access through index data that give information on a hit/no hit system: this is not a new phenomenon. It is the basis of the functioning of European large scale information systems, such as the Schengen Information System. The establishment of a system of index data has the advantage that it allows the originating Member States to control the exchange of information from their police files. If consultation of index data results in a match, the requesting authority may issue an information demand concerning the data subject involved. This demand can be properly assessed by the requested authority.

38. Nevertheless, a proper analysis is needed since the establishment of a system of index data — in areas where those

systems until now did not exist, other than the European large scale information systems — can create new risks for the data subject. The EDPS emphasises that although index data do not contain much information about the data subject, consultation of index data can lead to a highly sensitive result. It may reveal that a person is included in a police file in relation to criminal offences.

39. Therefore, it is of the utmost importance that the European legislator provides for adequate rules, at least on the creation of index data, on the management of the filing systems of index data and on the adequate organisation of the access to the index data. According to the EDPS, the proposal is not satisfactory on these points. At this stage, the EDPS makes three observations:

- The definition of index data is unclear. It is not clear whether index data are seen as meta-data, primary keys or even both? The notion of index data needs to be clarified, as it has a direct impact on the level of data protection and the required safeguards.
- The proposal should clarify the role of national contact points as regards index data. Involvement of national contact points could be necessary, in particular in cases when the interpretation of the index data requires specialised knowledge for instance in case of the possible matching of fingerprints.
- The proposal leaves the adoption of rules necessary for the creation of index data to implementing legislation in accordance with the comitology-procedure foreseen in Article 19. Although implementing rules might be needed, the basic rules for the creation of index data should be included in the Framework Decision itself.

Prior authorisation by judicial authorities

40. The information exchange shall not prevent Member States requiring prior authorisation by judicial authorities to transmit the information to the requesting authority when this information is under judicial control in the requested country. This is important since, according to a survey on police powers to exchange personal data⁽¹⁾, not in all Member States police can autonomously access these data. According to the EDPS, the availability principle should not undermine the obligation under national law to obtain a prior authorisation for the information, or at least establish specific rules concerning the categories of data for which prior authorisation has to be obtained, that will be applicable in all Member States.

⁽¹⁾ Replies to questionnaire on Framework Decision on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the EU, in particular as regards serious offences including terrorist acts (Council Doc No 5815/1/05).

41. This obligation should be interpreted in connection with Article 11(2) of the Proposal for a Framework Decision on the protection of personal data that also envisages that the transmitting Member State has a say in the further use of the data in the Member State to which the data have been transmitted. The EDPS notes the importance of this principle, which is needed to ensure that availability will not lead to circumventing restrictive national legislation on the further use of personal data.

Final remark

42. These elements require high standards of data protection. Special attention should be given to ensure the principles of purpose limitation and further processing as well as to the accuracy and the reliability of the information that is accessed (see the opinion of the EDPS on the Framework Decision on the protection of personal data, IV.2 and IV.6).

V. OTHER APPROACHES

Swedish proposal

43. The Swedish proposal is not limited to specific types of information but covers all information *and intelligence*, even information and intelligence that is kept by others than competent law enforcement authorities. The proposal advances cooperation by setting time limits to answer requests for information and by abolishing discrimination between the exchange within one Member State and cross border exchange of information. It does not provide for additional measures ensuring that the information can effectively be accessed. It is for this reason understandable that the Commission was not satisfied by the Swedish proposal in itself, as an adequate instrument for availability⁽¹⁾.

44. The approach in the Swedish proposal has the following general implications, from the perspective of data protection:

- It is welcomed that the proposal is strictly limited to the processing of existing data and does not lead to any new databases, not even to 'index data'.
- However, the absence of 'index data' is not by definition a positive element. Index data, if adequately secured, can facilitate a targeted and therefore less intrusive research of data with a sensitive nature. It can also allow for better filtering of requests and for better supervision.
- In any case, the proposal leads to an increase of the cross border exchange of personal data, with risks for the protection of personal data, *inter alia* because the

competence of the Member States to fully control the exchanger of data is affected. It should not be adopted independently of the adoption of the Framework Decision on the protection of personal data.

Prüm Convention

45. The Prüm Convention takes another approach to implementing the principle of availability. Whereas the present proposal for a Framework Decision has a general approach — not providing for specific rules for the exchange of specific types of information but applicable to all types of information, in so far as they are listed in Annex II (see points 21-28 of this opinion) —, the approach of the Prüm Convention is gradual.

46. This approach it is sometimes called a 'data field-by-data field approach'. It applies to specific types of information (DNA, fingerprinting data and vehicle registration data) and it lays down the obligation to take into account the specific nature of the data. The Convention lays down the obligation to open and keep DNA analysis files for the investigation of criminal offences. A similar obligation applies to fingerprinting data. As to vehicle registration data, direct access has to be given to national contact points of other Member States.

47. The approach of the Prüm Convention gives rise to three types of observations.

48. In the first place, it goes without saying that the EDPS does not endorse the process leading up to this Convention, outside the institutional framework of the European Union, and therefore without substantive involvement of the Commission. Moreover, this means no democratic control by the European Parliament and no judicial control by the Court of Justice and as a result there are less guarantees that all the (public) interests are equally balanced. This includes the perspective of data protection. In other words, the institutions of the European Union do not have the opportunity to assess — before the system is established — the impact of the policy choices on the protection of personal data.

49. In the second place, it is obvious that some elements of the Prüm Convention are clearly more intrusive to the data subject than the proposal for a Framework Decision on availability. The Convention necessarily leads to the establishment of new databases which in itself presents risks to the protection of personal data. The necessity and proportionality of the establishment of these new databases should be demonstrated. Adequate safeguards for the protection of personal data should be provided.

⁽¹⁾ See Commission Staff Working Document Annex to the Proposal for a Council Framework Decision on the exchange of information under the principle of availability, SEC 2005 (1207) of 12.10.2005.

A 'data field-by-data field approach'

50. In the third place, as said before, the Convention takes a 'data field-by-data field approach'. Hereinabove, the EDPS mentioned the difficulties and uncertainties related to the environment in which the principle of availability has to be made effective. Under those circumstances, it is according to the EDPS preferable not to set up a system for a range of data, but to start with a more cautious approach which involves one type of data and to monitor to what extent the principle of availability can effectively support law enforcement, as well as the specific risks for the protection of personal data. Based on these experiences, the system could possibly be extended to other types of data and/or modified in order to be more effective.

51. This 'data field-by-data field approach' would also better fulfil the requirements of the principle of proportionality. According to the EDPS, the needs for a better cross border exchange of data for the purpose of law enforcement could justify the adoption of a legal instrument on EU level, but to be proportional the instrument should be appropriate to achieve its goal which can be more properly established after a period of practical experiences. Furthermore, the instrument should not disproportionately harm the data subject. The exchange should not relate to more types of data than strictly necessary, with a possibility of an anonymous exchange of data, and should take place under strict conditions of data protection.

52. Moreover, a more cautious approach as advocated by the EDPS could — possibly in addition to the 'data field-by-data field approach' — include starting the implementation of the availability principle only by way of indirect access, via index data. The EDPS mentions this as a point for consideration in the further legislative process.

VI. WHICH DATA?

53. Annex II enumerates the types of information that may be obtained under the proposed Framework Decision. All of the six types of information listed there are personal data under most circumstances because they all involve a relation to an identified or identifiable person.

54. Under Article 3(g) of the Proposal, index data shall mean 'data the purpose of which is to distinctively identify information and that can be queried by means of a search

routine to ascertain whether or not information is available'. In the 'Approach for the implementation of the principle of availability' ⁽¹⁾ the following data are qualified as index data:

- the identification of the persons concerned;
- an identifying number for the objects concerned (vehicles/documents);
- fingerprints/digital photos.

Another type of data that could qualify as index data would be DNA-profiles. This list of index data reveals that index data may contain personal data and thus, an adequate protection is required.

55. The EDPS specifically addresses the issue of DNA-profiles. DNA analysis has proved to be of significant value for the investigation of crime and efficient exchange of DNA data can be essential to the fight against crime. However, it is essential that the concept of DNA data is clearly defined and that the specific characteristics of these data are properly taken into account. Indeed, from a data protection point of view, there is a big difference between DNA samples and DNA profiles.

56. DNA samples (often collected and stored by law enforcement authorities) should be considered as particularly sensitive, since they are more likely to contain the whole DNA 'picture'. They can provide information on genetic characteristics and the health status of a person, as may be required for totally different purposes such as giving medical advices to individuals or young couples.

57. On the contrary, DNA profiles only contain some partial DNA information extracted from the DNA sample: they can be used to verify the identity of a person, but in principle they do not reveal genetic characteristics of a person. Nonetheless, progress in science may increase the information that can be revealed by DNA profiles: what is considered as an 'innocent' DNA profile at a certain moment in time, may at a later stage reveal much more information than expected and needed, and in particular information concerning genetic characteristics of a person. The information that can be revealed by DNA profiles should thus be considered as dynamic.

58. In this perspective, the EDPS notes that both the Prüm Convention and the Commission proposal promote the exchange of DNA data between law enforcement, but there are substantial differences in the way they do so.

⁽¹⁾ Document from the Presidency to the Council of 5 April 2005 (Doc. No.: 7641/05).

59. The EDPS welcomes that the Commission proposal does not establish any obligation to collect DNA data and that it clearly limits the exchange of DNA data to DNA profiles. Annex II defines DNA profiles through an initial common list of DNA markers used in forensic DNA analysis in Member States. This list — based on the seven DNA markers of the European Standard Set as defined Annex I of the Council Resolution of 25 June 2001 on the exchange of DNA analysis results⁽¹⁾ — guarantees that DNA profiles will not contain, when they are extracted, any information about specific hereditary characteristics.
60. The EDPS highlights that this Council Resolution lays down some very important safeguards which are specifically related to the dynamic nature of DNA profiles. Indeed, section III of the Resolution, after limiting the exchanges of DNA analysis results to 'chromosome zones [...] not known to provide information about specific hereditary characteristics', further recommends Member States to no longer use those DNA markers which, due to science developments, may provide information on specific hereditary characteristics.
61. The Prüm Convention provides for a different approach, since it obliges the Contracting Parties to open and keep DNA analysis files for the investigation of criminal offences. It therefore entails the creation of new DNA databases and an increased collection of DNA data. Furthermore, it is unclear which kind of data are included in the 'DNA analysis files' and the Convention does not take into account the dynamic evolution of DNA profiles.
62. The EDPS points out that any legal instrument laying down exchanges of DNA data should:
- Clearly limit and define the type of DNA information which may be exchanged (also with regard to the fundamental difference between DNA samples and DNA profiles).
 - Set up common technical standards aimed at avoiding that variations in practices on forensic DNA databases in Member States could lead to difficulties and inaccurate results when data are exchanged.
 - Provide for appropriate legally binding safeguards aimed at preventing that the developments of science would result in obtaining from DNA profiles personal data which are not only sensitive, but also unnecessary for the purpose for which they were collected.
63. In this perspective, the EDPS hereby confirms and integrates the remarks already made in his opinion on the Framework Decision on the protection of personal data (point 80). In that Opinion, the EDPS pointed out, with regard to DNA data, that specific safeguards should be provided, so as to guarantee that: the available information may only be used to identify individuals for the prevention, detection, or investigation of criminal offences; the level of accuracy of DNA profiles is carefully taken into account and might be challenged by the data subject through readily available means; the respect of the dignity of persons must be fully ensured⁽²⁾.
64. These considerations lead furthermore to the conclusion that legislation on the establishment of DNA-files and the exchange of data from these files should only be adopted after an impact assessment in which the benefits and the risks could have been properly assessed. The EDPS recommends that this legislation contains obligations for a regular evaluation after its entry into force.
65. Finally, Annex II includes other types of information that may be exchanged. It includes information that originates from private parties since telephone numbers and other communication data, as well as traffic data do normally originate from telephone operators. The explanatory memorandum confirms that Member States are obliged to ensure that law enforcement relevant information controlled by authorities or by private parties designated for this purpose, is shared with equivalent competent authorities of other Member States and Europol. Whereas the proposal applies to personal data originating from private parties, the applicable legal framework should — according to the EDPS — contain additional safeguards to protect the data subject so as to ensure the accuracy of the data.

VII. PRINCIPLES OF DATA PROTECTION

66. The rules on the protection of personal data are not specifically laid down in the proposed Council Framework Decision, while in other instruments, like the Prüm Convention or the Swedish proposal, there are some specific provisions on the protection of personal data. The lack of specific rules on the protection of personal data in the availability proposal is acceptable only insofar as the general rules contained in the proposal for a Framework Decision on data protection in third pillar are fully applicable and provide for a sufficient protection. Moreover, rules on personal data protection laid down by specific instruments — such as the Swedish proposal and the Prüm Convention — should not lower the level of protection ensured by the general framework. The EDPS recommends adding a specific clause on possible conflicts between the different rules on data protection.

⁽¹⁾ OJ C 187, p. 1.

⁽²⁾ In the same line, see also the Council of Europe's 'Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of personal biometric data', February 2005.

67. At this point, the EDPS would like to highlight again, by recalling his opinion with regard to the Framework Decision on the protection of personal data, the importance of having consistent and comprehensive data protection rules in place with regard to law enforcement cooperation that apply to all processing. Subsequently, the EDPS reiterates the other points made in that opinion. In this paragraph, the following data protection issues are emphasised:

- Lawful processing of personal data. The EDPS supports the approach that information can be available only if it has been collected lawfully (as mentioned by Article 2.2 with regard to information collected through coercive measures). Lawful processing of personal data would also ensure that information made available and exchanged can be properly used also in a judicial proceeding. Indeed, although information processed after the commencement of a prosecution falls outside the scope of the proposed instrument, it is still likely that information exchanged before by law enforcement authorities ends up in judicial proceedings.
- Quality of personal data is of specific importance since the availability principle favours that information will be used by law enforcement authorities operating outside the context in which the data were collected. Those authorities even have direct access to databases of other Member States. The quality of the personal data can only be ensured if its accuracy is regularly and properly checked, if information is distinguished according to the different categories of persons concerned (victims, suspects, witnesses, etc), and if, when necessary, the degree of accuracy is indicated (see EDPS Opinion on the protection of personal data, IV.6).

These points make once more clear why data protection rules, and especially rules on accuracy, should be applicable to all kinds of processing, also to domestic ones. Otherwise, personal data which are directly accessed could be incorrect, out of date and thus impinge both on the data subjects' rights and on the efficiency of investigations.

- Purpose limitation. According to the principle of availability, personal data may be accessed by equivalent competent authorities of other Member States. However, the competences of law enforcement authorities may substantially differ from country to country. It is therefore essential to ensure that the basic principle of purpose limitation is respected in spite of the different scope of competences of the various competent authorities exchanging the data. Information which is collected and processed by a certain authority with a specific purpose can not then be used for a

different purpose just by virtue of the different, maybe broader, competences of the receiving authority.

Therefore, the EDPS welcomes Article 7 of the proposed Framework Decision, which should be read as a specification of the general rules laid down in the proposed Framework Decision on the protection of personal data. Furthermore, the EDPS notes that the assessment of the equivalence between different authorities (which in the current proposal is left to a comitology procedure) should be carried out carefully and with due respect to the purpose limitation principle.

- Time limits for storing exchanged information shall also be seen in the light of the purpose limitation principle: information accessed or exchanged for one purpose should be deleted as soon as it is no longer necessary for that purpose. This would avoid unnecessary duplication of databases, while still allowing competent authorities to access (updated) available information again, in case it is necessary for another legitimate purpose.
- Logging of information transmitted according to the principle of availability. Logging should take place on both sides: in the requested as well as in the requesting Member State. Access logs, not only exchange logs, should be kept (see EDPS Opinion on the protection of personal data, point 133), also with a view to ensuring that national competent authorities trust each other and do not completely lose control over the information available. The need for traceability of information also implies a possibility to update and/or correct information.
- Rights of data subjects. Systems for exchange of information between EU law enforcement authorities increase situations whereby personal data are (temporarily) processed at the same time by competent authorities in different Member States. This means on one hand that common EU-standards on data subjects' rights should be established, and on the other hand that data subjects should be able to exercise their rights, to the extent allowed by rules on data protection in third pillar, with regard to both authorities that make data available and authorities that access and process these data.
- Supervision. The EDPS points out that, depending on the case, more than one national supervisory authority may be competent to monitor the processing of personal data carried out on the basis of the current proposals. In this regard, direct online access to law enforcement information calls for an enhanced supervision and coordination by relevant national data protection authorities.

VIII. CONCLUSIONS

General conclusions relating to the principle of availability

68. The EDPS uses the occasion to present in this opinion some general and more fundamental points of view on the subject of exchange of law enforcement information and on the approaches for regulating this subject. The EDPS will be available for further consultation at a later stage, following relevant developments in the legislative process on this proposal or on other related proposals.
69. According to the EDPS, the principle of availability should be implemented into a binding legal instrument by way of a more cautious, gradual approach which involves one type of data and to monitor to what extent the principle of availability can effectively support law enforcement, as well as the specific risks for the protection of personal data. This more cautious approach could include starting with the implementation of the availability principle only by way of indirect access, via index data. Based on these experiences, the system could possibly be extended to other types of data and/or modified in order to be more effective.
70. Any legal instrument implementing the principle of availability should not be adopted without the prior adoption of essential guarantees on data protection as included in the Proposal for a Framework Decision on the protection of personal data.

Recommendations aiming to modify the present proposal

71. The EDPS recommends clarifying the scope of the principle of availability as follows:
- Adding a clear and precise definition of the data that will be considered available.
 - As a first option, limiting the scope of the principle of availability to information controlled by competent authorities.
 - As a second option, in case of a broader scope, ensuring sufficient safeguards for the protection of personal data. The questions raised in point 27 of this opinion have to be taken into consideration.
72. The EDPS makes the following observations on direct access to databases by a competent authority of another Member State:
- The issue has to be properly addressed since, in case of direct access, the designated authorities of the originating Member State have no control over the access and the further use of the data.

- The proposal may not promote an unconditional inter-connection of databases and thus a network of databases which will be hard to supervise
73. The Framework Decision should be more precise on the establishment of a system of index data. More in particular:
- The proposal should provide for adequate rules, at least on the creation of index data, on the management of the filing systems of index data and on the adequate organisation of the access to the index data.
 - The definition of index data needs to be clarified.
 - The proposal should clarify the role of national contact points as regards index data.
 - The basic rules for the creation of index data should be included in the Framework Decision itself and not left to implementing legislation in accordance with the comitology-procedure.
74. The EDPS points out that the proposal -in so far as it lays down exchanges of DNA data — should:
- Clearly limit and define the type of DNA information which may be exchanged (also with regard to the fundamental difference between DNA samples and DNA profiles).
 - Set up common technical standards aimed at avoiding that variations in practices on forensic DNA databases in Member States could lead to difficulties and inaccurate results when data are exchanged
 - Provide for appropriate legally binding safeguards aimed at preventing that the developments of science would result in obtaining from DNA profiles personal data which are not only sensitive, but also unnecessary for the purpose for which they were collected.
 - Only be adopted after an impact assessment.
75. The EDPS advises limiting the information exchange with Europol to the purposes of Europol itself, as mentioned in Article 2 of the Europol Convention and the Annex thereof.

Done at Brussels on 28 February 2006.

Peter HUSTINX

European Data protection Supervisor

I

(Resolutions, recommendations and opinions)

OPINIONS

EUROPEAN DATA PROTECTION SUPERVISOR

Opinion of the European Data Protection Supervisor on the Initiative of the Federal Republic of Germany, with a view to adopting a Council Decision on the implementation of Decision 2007/.../JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime

(2008/C 89/01)

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty establishing the European Community, and in particular its Article 286,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular its Article 8,

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data,

Having regard to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, and in particular its Article 41,

HAS ADOPTED THE FOLLOWING OPINION:

I. INTRODUCTION

1. On 9 November 2007, the Official Journal published the Federal Republic of Germany's initiative for a Council Decision on the implementation of Decision 2007/.../JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime ⁽¹⁾ ('the initiative'). This initiative is supplemented by an Annex of 18 October 2007 containing further details concerning the implementation of Decision 2007/.../JHA ('the Annex') ⁽²⁾.

⁽¹⁾ OJ C 267, 9.11.2007, p. 4.

⁽²⁾ The Annex has not yet been published in the Official Journal, but is publicly available, as document number 11045/1/07 REV 1 ADD 1, at the Council register.

2. The EDPS was not asked for advice on this initiative for an implementing decision. Therefore he issues this opinion on his own initiative, in the same way as his opinion on the initiative for a Council Decision was issued, on 4 April 2007 ⁽³⁾.
3. Although there is no legal obligation for a Member State that takes the initiative for a legislative measure under Title VI of the EU Treaty to ask the EDPS for advice, the procedure does not preclude the request for such an advice either. Moreover, in his Opinion of 4 April 2007, the EDPS recommended adding the following sentence to Article 34 of that Council Decision: 'The Council shall consult the EDPS on such an implementing measure'. Unfortunately, this recommendation has not been followed, despite the logic behind it: implementing measures will in this case most often affect the processing of personal data. The present initiative by the Federal Republic of Germany is a clear illustration of this logic.
4. The EDPS does not draw any substantive conclusion from this result. It fits within the approach chosen by the Council to modify the initiative as little as possible, in order to ensure full compatibility with the text of the Treaty of Prüm which had been signed previously by a number of Member States. The EDPS will discuss the democratic impact of this approach further on in this opinion.

II. CONTEXT AND LEGAL FRAMEWORK

5. The Treaty of Prüm was signed in May 2005 by seven Member States, outside of the framework of the EU Treaty. Subsequently, other Member States have acceded to the Treaty.

⁽³⁾ OJ C 169, 21.7.2007, p. 2.

6. The Treaty of Prüm is complemented by an implementing agreement, based on Article 44 of that Treaty and concluded on 5 December 2006. This implementing agreement is necessary for the functioning of the Prüm Treaty.
7. The main elements of the Prüm Treaty will be included in the legal framework of the European Union, after the adoption of Council Decision 2007/.../JHA on the initiative of 15 Member States ('the Prüm initiative'), on which a political agreement in the Council has already been reached. This inclusion was right from the start the intention of the Contracting Parties to the EU Treaty, as confirmed by the preamble of the Prüm Treaty.
8. The intention during the legislative procedure leading to the adoption of the Council decision was not to discuss major issues any more, but to reach agreement on the *acquis* of the Prüm Treaty. This intention was all the more important since — pending this legislative procedure — the ratification process of the Treaty continued in a number of Member States and the Treaty entered into force.

III. OBJECT AND FOCUS OF THIS OPINION

9. This opinion will focus on the draft Council decision on the implementing rules. The points made in the previous EDPS opinion on the Council decision on the Prüm initiative are still valid and will not be repeated, unless this is necessary to highlight those issues that the legislator could still address through the implementing rules.
10. In this context, it is important to stress that the implementing rules vest a specific importance, because, besides some administrative and technical provisions, they define crucial aspects and tools of the system and of its functioning. For example, Chapter 1 of the implementing rules lays down the definitions of the terms used in the Council decision on Prüm. Furthermore, the implementing rules establish common provisions for data exchange (Chapter 2), and then define the specific characteristics of the exchange of DNA (Chapter 3), dactyloscopic (Chapter 4) and vehicle registration data (Chapter 5). The final provisions of Chapter 6 contain important provisions on the adoption of further implementing rules in manuals as well as on the evaluation of the application of the decision.
11. Furthermore, the Annex will be considered insofar as it contributes, or should contribute, to defining the features of the proposed system and the guarantees for the data subjects.

IV. GENERAL POINTS

Limited margin of manoeuvre

12. The EDPS notes that also in this case the pre-existence of implementing rules already in force for the Prüm Conven-

tion seems to strongly reduce the real margin of manoeuvre left to the Council. Indeed, Recital 3 and Article 18 of the initiative state that both the implementing decision and the manuals shall be based on the implementing provisions agreed on 5 December 2006 concerning the administrative and technical implementation of the Prüm Treaty. Therefore, according to the present initiative, the 27 Member States will have to follow the path already defined by the 7 Member States that signed the Prüm Treaty.

13. This approach obstructs the development of a really transparent and democratic legislative process, since it considerably reduces the possibility of having a broad debate and of effectively taking into account the legislative role of the European Parliament and the advisory role of other institutions, such as the EDPS. The EDPS recommends that the initiative and its Annex are openly discussed by effectively profiting from the contributions of all institutional actors, also in consideration of the role of full co-legislator that the European Parliament will enjoy in this area once the Reform Treaty — signed in Lisbon on 13 December — enters into force.

Data protection legal framework and relations with the Draft framework decision on data protection in third pillar

14. The applicable legal framework on data protection is complex and fluctuant. Indeed, Chapter 6 of the Prüm initiative lays down some guarantees and specific rules with regard to data protection. However, these specific rules are not stand-alone and need to base themselves for their proper functioning on a full-fledged and general framework for the protection of personal data processed by police and judicial authorities. Currently, Article 25 of the Prüm initiative refers to Convention 108 of the Council of Europe. However, the EDPS has repeatedly stressed the need to further specify the principles contained in Convention 108, thus ensuring a level of data protection which is high, harmonized, and therefore appropriate to guarantee both citizens rights and law enforcement effectiveness in an area of Freedom, Security and Justice ⁽¹⁾.
15. In this perspective, the Commission proposed already in October 2005 a general instrument, the draft Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters ('the draft framework decision on data protection in third pillar'). This proposal has not been adopted yet by the Council and is thus still subject to discussion and possible amendments, let alone further delay in adoption and implementation. However, it is clear by now that this Framework Decision, as it currently stands, would only be applicable to personal data exchanged with other Member States and not to the domestic processing of those data ⁽²⁾.

⁽¹⁾ See, more recently, EDPS opinion on Prüm, § 57-76 and EDPS Third opinion of 27 April 2007 on the proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters, § 14 (OJ C 139, 23.6.2007, p. 1).

⁽²⁾ The latest draft of this proposal is available on Council register as document number 16397/07.

16. Furthermore, the current text of the draft framework decision on data protection in third pillar, in spite of its objective of ensuring a high level of data protection, provides only minimal harmonization and guarantees. This means that some instruments, such as the current initiative, which could have benefited from a comprehensive general framework on data protection, are now called to deal with the lacunae left by the draft framework decision on data protection in third pillar.
17. Therefore, the EDPS on the one hand reiterates that the Council decisions on Prüm should not enter into force before Member States have implemented a general framework decision on data protection in the third pillar. This condition should be specifically laid down in the initiative, and subject to appropriate prior verification of the proper functioning of the data protection guarantees within the data exchange system. In this context, it is also essential to guarantee that relations between legal instruments are clarified with a view to ensuring that the framework decision on data protection in third pillar acts as '*lex generalis*' while allowing the applicability of further specific guarantees and tailored stricter standards laid down by the Prüm initiative ⁽¹⁾.
18. On the other hand, the legislator should clarify that the specific data protection rules relating to DNA, fingerprints and vehicle registration data in Chapter 6 of the Prüm initiative, are applicable not only to the exchange of these data, but also to their collection, storing and domestic processing, as well as to the supply of further personal data within the scope of the Council decision. This clarification would be in line with Article 24(2) of the Prüm initiative, as well as a logical consequence of the obligation for Member States to collect, store and share the abovementioned kinds of data.
19. This is even more important when considering that the scope of the draft framework decision on data protection in third pillar will probably not apply to domestic processing of personal data. The Council took this decision but at the same time specified that this choice does not limit the ability of the legal basis to cover this kind of processing operations. Against this background, since the current package of initiatives — comprising the Prüm initiative and the implementing rules — imposes the obligation to create and maintain certain databases, such as the DNA database, it should also contain guarantees concerning the processing operations — notably, the collection and storage of DNA profiles — stemming from the collection and the storage. Otherwise, if their application were to be limited to exchanged data, these legal instruments would not contain the appropriate provisions on the protection of personal data to which any action based on Article 30(1)(b) of the EU Treaty should be subject.
20. The EDPS calls on the legislator to ensure, pursuant to Article 30(1)(b) of the EU Treaty, that a clear, effective and comprehensive legal framework with regard to data protection — combining different legal instruments with general provisions and specific guarantees — is in place before the current initiative enters into force.
21. In this opinion, the EDPS will therefore make reference, where relevant, to those issues that have not been (completely) addressed by the draft framework decision on data protection in third pillar and should therefore be considered in the implementation of the system laid down by the current initiative.
- Transparency of decision making process and of implementing rules**
22. The EDPS stresses that transparency is an essential element both in the decision-making process and in the implementation of the rules. Transparency therefore should allow on one hand a full and effective participation of all the relevant institutional actors involved and on the other hand should favour public debate and adequate information of the citizens.
23. Unfortunately, in this case a series of circumstances affect transparency: there is no explanatory memorandum explaining the reasons behind the proposed measures, their effectiveness and the possible policy alternatives; the text of the Annex is still incomplete — for example, it has not yet been published in the Official Journal, is not translated in all official languages, references to articles and terminology are often inaccurate and declarations of Member States on the content of DNA databases are not available; the initiative itself does not lay down obligations or mechanisms to adequately inform citizens about the measures taken and amendments to those measures.
24. Therefore, the EDPS recommends enhancing the transparency of the measures, by providing a definitive version of the Annex as soon as possible and by establishing mechanisms to inform citizens about the features of the systems, their rights and how to exercise them. The latter information campaigns should be explicitly laid down in the initiative or its Annex.
- Scale of the system**
25. The current initiative closely mirrors the implementing rules established under the Prüm Treaty. However, as already noticed in the opinion on the Council Prüm initiative (§ 33-35), mechanisms that are designed for information exchange between a few Member States are not necessarily appropriate — and may therefore have to be adapted — when they are to be applied to a much larger scale system, such as an information exchange between 27 Member States.

⁽¹⁾ With regard to this point, the text of Article 27b of the latest draft of the Draft framework decision on data protection in the third pillar should be carefully considered and discussed.

26. Indeed, small scale favours close contacts between Member States involved, both with regard to law enforcement and with regard to monitoring the risks for the protection of personal data of the persons concerned. This is not the case in a larger system, in which national practices and legal regimes broadly differ as to the collection, storage and processing of data, especially with regard to DNA profiles and fingerprints. Furthermore, the use of different languages and of different legal concepts may affect the accuracy in the exchanges of data between countries with different legal traditions. Therefore, the EDPS invites the legislator to properly take into account the scale of the system when further discussing the current initiative, by ensuring that the increase in the number of participating Member States does not entail a decrease in effectiveness. In particular specific formats for communication of data, also taking into account the language differences, should be established in the implementing rules, and the accuracy of the data exchanges should be constantly monitored.

The involvement of data protection authorities

27. The initiative should recognize the important role to be played by the independent supervisory authorities in the context of large scale trans-border data exchanges, and should put them in a position to effectively carry out their tasks.
28. First of all, the current legal framework does not provide for any consultation or involvement of the competent supervisory authorities about amendments to the implementing rules and their Annexes (Article 18 of the initiative), about the implementation of the data protection rules by the Member States (Article 20), or about the evaluation of data exchange (Article 21). It is, for example, particularly unfortunate that Chapter IV of the Annex, which lays down in detail the rules for assessing the implementation, does not mention at all the competent data protection authorities. The EDPS recommends that the essential advisory role played by these authorities be explicitly recognized by the abovementioned Articles.
29. Secondly, the initiative should ensure that Member States provide data protection authorities with the (additional) resources necessary to carry out the supervisory tasks stemming from the implementation of the proposed system.
30. Thirdly, the initiative should provide that competent data protection authorities regularly meet at EU level with a view to coordinate their activities and harmonize the application of these instruments. This opportunity should be expressly laid down by the initiative, to the extent that the Framework Decision on data protection in the third pillar does not establish a more general forum of data protection authorities at EU level.

V. SPECIFIC ISSUES

Definitions

31. Article 2 of the initiative lays down a series of definitions, which in part mirror those contained in the Council decision. First of all, it should be underlined that the definitions contained in Article 2 of the initiative do not correspond exactly to the definitions laid down by the Council decision, in particular by its Article 24. The legislator should align the formulations of the two texts in order to prevent implementation problems.
32. Secondly, the EDPS, already in his opinion on the Prüm initiative, regretted the lack of a clear definition of personal data (§ 41-43). This lack is even more regrettable in the implementing rules, which are proposed when it is already clear that the draft framework decision on data protection in third pillar will not be applicable to domestic collection and processing of personal data, and in particular of DNA profiles. The EDPS therefore calls upon the legislator once more to introduce a clear and inclusive definition of personal data.
33. In this perspective, the implementing provisions should also clarify the applicability of data protection rules to unidentified DNA profiles — which have not yet been attributed to an identified person. Indeed, these data are collected, exchanged, cross-matched with a view to attribute them to the persons to which they belong. Therefore, since the objective of the system is to identify these persons and these data are in principle bound to be only temporarily 'unidentified', they should as well be covered by most, if not all provisions and guarantees applicable to personal data ⁽¹⁾.
34. Also with regard to the definition of the 'non-coding part of DNA' (Article 2(e)), the EDPS recalls once again ⁽²⁾ that the capacity of some chromosome regions to provide for sensitive hereditary characteristics of an organism can improve with the developments of science. Therefore, the definition of 'non-coding part' should be dynamic, by including an obligation to no longer use those DNA markers which, due to science developments, may provide information on specific hereditary characteristics ⁽³⁾.

⁽¹⁾ On the applicability of data protection rules to DNA profiles, see Article 29 Working Party Opinion No 4/2007 of 20 June 2007 on the concept of personal data, WP136, p. 8-9; in the same opinion clarifications are also provided on the analogous case of the applicability of data protection rules to dynamic IP addresses, p. 16-17.

⁽²⁾ See also EDPS Opinion of 28 February 2006 on the Proposal for a Council Framework Decision on the exchange of information under the principle of availability (COM(2005) 490 final), § 58-60 (OJ C 116, 17.5.2006).

⁽³⁾ See, in the same line, Annex I of the Council Resolution of 25 June 2001 on the exchange of DNA analysis results (OJ C 187, 3.7.2001, p. 1).

Accuracy in automated searches and comparisons

35. Article 8 of the initiative regulates automated search and comparison of DNA profiles, by establishing that automated notification of a match *'shall only be provided if the automated search or comparison has resulted in a match of a minimum number of loci'*. This minimum is set out in Chapter I of the Annex: each Member State shall ensure that DNA profiles made available contain at least 6 out of the 7 EU 'standard' loci (§ 1.1 of Chapter I of Annex); the comparison will take place between the values of the compared loci commonly contained in the requesting and requested DNA-profiles (§ 1.2); there will be a match if all values of compared loci are the same ('full match') or if only one value is different ('near match') (§ 1.2); both full matches and near matches will be reported (§ 1.3).
36. With regard to this mechanism, the EDPS notes that accuracy of the match is an essential condition. The higher is the number of loci that match, the less likely it is that there is a false match between DNA profiles that have been compared. In the current European Union context, the existence and the structure of DNA databases vary from country to country. Different numbers and different sets of loci are used in different countries. The Annex sets the minimum number of loci for a match at 6, without providing information about the envisaged error rate for this system. With regard to this issue, the EDPS notes that in many countries a higher number of loci is used with a view to increase the accuracy of the matches and reduce the false matches⁽¹⁾. Therefore, in order to properly assess the degree of accuracy of the envisaged system, it would be essential that information be provided about the envisaged error rate for each number of loci compared.
37. This also means that the minimum number of loci is an essential element and it should therefore be established in the text of the current initiative rather than in the Annex (which, pursuant to Article 18 of the initiative, can be modified by the Council acting on qualified majority and without consulting the Parliament), in order to avoid that a decrease in the number of loci may affect the accuracy. The possibility of errors and false matches should be duly taken into account, by providing that near matches are explicitly reported as such (and therefore receiving authorities are aware that this match is not as reliable as a full match).
38. Furthermore, the initiative itself recognizes the possibility that searches and comparisons generate multiple matches, as explicitly laid down by Article 8 of the initiative with regard to DNA profiles and by Chapter 3 (point 1.2) of the Annex with regard to vehicles. In all these cases, further checks and verifications should take place in order to determine which are the reasons for a multiple match and which of these matches is accurate, before carrying out further exchange of personal data based on that match.
39. In the same perspective, the EDPS recommends that awareness is raised, in particular among law enforcement operators dealing with DNA comparisons and searches, about the fact that DNA profiles are not unique identifiers: even full matches in a certain number of loci do not exclude the possibility of false matches, i.e. the possibility that a person is wrongly linked to a DNA profile. Indeed, DNA-profiles comparisons and searches are subject to possible errors at different stages: the scarce quality of the DNA samples at the moment of collection, possible technical errors in the DNA analysis, input errors, or just because a chance match occurs in the specific loci considered in the comparison. With regard to the last point, the error rate is likely to be higher when the number of loci diminishes and when the database expands.
40. A similar reasoning can be applied with regard to the accuracy of fingerprints matching. Article 12 of the initiative establishes that the digitalisation and transmission of dactyloscopic data will be carried out in accordance with a uniform data format specified in Chapter II of the Annex. Furthermore, Member States shall ensure that dactyloscopic data are of sufficient quality for comparison by the automated fingerprint identification system (AFIS). Chapter II of the Annex provides some details on the format to be used. Against this background, the EDPS notes that, with a view to ensure accuracy of the matching process, the initiative and its Annex should harmonize as much as possible the different AFIS systems in use in the Member States and the way these systems are used, in particular with regard to the false rejection rate. According to the EDPS, this information should be included in the Manual established pursuant to Article 18(2) of the initiative.
41. Another crucial element is that DNA (and fingerprints) databases should be precisely circumscribed, since they can contain, depending on the Member States, DNA profiles or fingerprints of different kinds of data subjects (criminals, suspects, other people present on the crime scene, etc.). In spite of these differences, the current initiative does not circumscribe the kinds of databases that will be used by each Member States, and declarations to this effect are not yet included in the Annex. Therefore, matches can occur between DNA and fingerprint data relating to non homogeneous, and often non relevant, categories of data subjects.
42. According to the EDPS, the initiative should specify which kinds of data subjects will be involved in the exchanges of data and how their different status will be communicated to other Member States in the context of a comparison or search. For example, the initiative could establish an obligation to provide in the matching report information about which kind of data subject the DNA data or fingerprints have been matched with, to the extent this information is available to the requested authorities.

⁽¹⁾ For example, in the UK the National DNA Database has increased the number of loci used for DNA profiles from 6 to 10, also with a view to enhance the reliability of the system.

The evaluation of the data exchange

43. The evaluation of the data exchange, pursuant to Article 21 of the initiative and Chapter 4 of the Annex, is welcome. However, these provisions focus merely on administrative, technical and financial implementation of automated data exchanges without even mentioning the evaluation of the implementation of the data protection rules.
44. Therefore, the EDPS suggests that specific emphasis be given to the evaluation of data protection aspects of data exchanges, with specific attention to purposes for which data have been exchanged, methods of information of data subjects, accuracy of exchanged data and false matches, requests of access to personal data, length of storage periods and effectiveness of security measures. In this context, relevant data protection authorities and experts should be duly involved, for example by providing that data protection experts take part in the evaluation visits established by Chapter 4 of the Annex and that relevant data protection authorities receive the evaluation report referred to in Article 20 of the initiative and in Chapter 4 of the Annex.

Communications network and technical aspects of the system

45. Article 4 of the initiative establishes that all the electronic exchanges of data will take place using the 'TESTA II' communications network. In this context, the Annex mentions at page 76, point 54, that 'The system is compliant with data protection issues as stated in Regulation (EC) No 45/2001 (Articles 21, 22 and 23) and Directive 95/46/EC'. The EDPS recommends that this information be clarified, also with regard to the role that Community institutions will play in the system. In this context, both the supervisory and the advisory roles of the EDPS stemming from Regulation (EC) No 45/2001 should be fully taken into account.
46. Furthermore, once the Annex is finalized and contains all the details and the declarations clarifying the features of the systems, the EDPS will consider whether to provide further advice on the more technical aspects of the system.

VI. CONCLUSIONS

- The EDPS recommends that the initiative and its Annex are openly discussed by effectively profiting from the contributions of all institutional actors, also in consideration of the role of full co-legislator that the European Parliament will enjoy in this area once the Reform Treaty — signed in Lisbon on 13 December — enters into force.
- The EDPS calls on the legislator to ensure, pursuant to Article 30(1)(b) of the EU Treaty, that a clear, effective and comprehensive legal framework with regard to data protection — combining different legal instruments with general provisions and specific guarantees — is in place before the current initiative enters into force.

- In this perspective, the EDPS on the one hand reiterates that the Council decisions on Prüm should not enter into force before Member States have implemented a general framework decision on data protection in the third pillar that would be a '*lex generalis*' on top of which those provisions of the Prüm initiative ensuring specific guarantees and tailored stricter standards should apply.
- On the other hand, the legislator should clarify that the specific data protection rules relating to DNA, fingerprints and vehicle registration data in Chapter 6 of the Prüm initiative, are applicable not only to the exchange of these data, but also to their collection, storing and domestic processing, as well as to the supply of further personal data within the scope of the Council decision.
- The EDPS recommends enhancing the transparency of the measures, by providing a definitive version of the Annex as soon as possible and by establishing mechanisms to inform citizens about the features of the systems, their rights and how to exercise them.
- The EDPS invites the legislator to properly take into account the scale of the system when further discussing the current initiative, by ensuring that the increase in the number of participating Member States does not entail a decrease in effectiveness. In particular specific formats for communication of data, also taking into account the language differences, should be established in the implementing rules, and the accuracy of the data exchanges should be constantly monitored.
- The EDPS recommends that the essential advisory role played by relevant data protection authorities be explicitly recognized by the Articles about amendments to the implementing rules and their Annexes (Article 18), about the implementation of the data protection rules by the Member States (Article 20), and about the evaluation of data exchange (Article 21). Furthermore, the initiative should ensure that Member States provide data protection authorities with the (additional) resources necessary to carry out the supervisory tasks stemming from the implementation of the proposed system and that competent data protection authorities regularly meet at EU level with a view to coordinate their activities and harmonize the application of these instruments.
- The EDPS therefore calls upon the legislator once more to introduce a clear and inclusive definition of personal data. In this perspective, the implementing provisions should also clarify the applicability of data protection rules to unidentified DNA profiles — which have not yet been attributed to an identified person. The EDPS also recalls once again that the definition of 'non-coding part' should be dynamic, by including an obligation to no longer use those DNA markers which, due to science developments, may provide information on specific hereditary characteristics

- The EDPS recommends that, in the context of automated searches and comparisons, accuracy of the matching process is duly taken into account.
 - This means that, with regard to DNA comparisons and searches, information should be provided about the envisaged error rate for each number of *loci* compared, that near matches should be explicitly reported as such, that further checks should be carried out in case of multiple matches, and that awareness is raised about the fact that DNA profiles are not unique identifiers. With regard to fingerprints, the initiative should harmonize as much as possible the different AFIS systems in use in the Member States and the way these systems are used, in particular with regard to false rejection rates.
 - Furthermore, DNA and fingerprints databases should be precisely circumscribed, since they can contain, depending on the Member States, DNA profiles or fingerprints of different kinds of data subjects. The initiative should specify which kinds of data subjects will be involved in the exchanges of data and how their different status will be communicated to other Member States in the context of a comparison or search.
 - The EDPS suggests that specific emphasis be given to the evaluation of data protection aspects of data exchanges, with specific attention to purposes for which data have been exchanged, methods of information of data subjects, accuracy of exchanged data and false matches, requests of access to personal data, length of storage periods and effectiveness of security measures. In this context, relevant data protection authorities and experts should be duly involved.
 - The EDPS recommends that the use of the 'TESTA II' communications network and its compliance with Regulation (EC) No 45/2001 be clarified, also with regard to the role that Community institutions will play in the system.
- Done at Brussels, 19 December 2007.
- Peter HUSTINX
European Data Protection Supervisor
-

I

(Resolutions, recommendations, guidelines and opinions)

OPINIONS

EUROPEAN DATA PROTECTION SUPERVISOR

Third opinion of the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters

(2007/C 139/01)

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty establishing the European Community, and in particular its Article 286,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular its Article 8,

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ⁽¹⁾,

Having regard to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data ⁽²⁾, and in particular its Article 41,

HAS ADOPTED THE FOLLOWING OPINION:

I. INTRODUCTION

1. On 19 December 2005 and on 29 November 2006, the EDPS issued two opinions ⁽³⁾ on the Proposal of the Commission for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters. In these opinions, he underlined the importance of the proposal as an effective instrument for the protection of personal data in the area covered by Title VI of the EU-Treaty. In particular, in his second opinion the EDPS voiced his concerns that developments in the negotiations were leading towards a level of protection of personal data not only below the standards laid down in Directive 95/46/EC, but also incompatible with the more generally formulated Council of Europe Convention No 108 ⁽⁴⁾.
2. In January 2007, the German Presidency set out a series of basic points to revise the proposal, with a view to remove outstanding reservations and improve data protection in the third pillar ⁽⁵⁾. The revised draft proposal ⁽⁶⁾ was submitted to the EP for a second consultation on 13 April 2007.

⁽¹⁾ OJ L 281, 23.11.1995, p. 31.

⁽²⁾ OJ L 8, 12.1.2001, p. 1.

⁽³⁾ The first Opinion can be found in the OJ C 47, 25.2.2006, p. 27; the second Opinion is available on EDPS website: www.edps.europa.eu

⁽⁴⁾ Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe, 28 January 1981.

⁽⁵⁾ Council document 5435/07 of 18 January 2007, available at: register.consilium.europa.eu

⁽⁶⁾ Council document 7315/07 of 13 March 2007, available at: register.consilium.europa.eu

3. The substantive changes contained in the revised proposal, as well as its importance, call for a new opinion of the EDPS. This opinion will concentrate on the EDPS main concerns and will not revisit all the points made in his previous opinions, as these remain valid for this revised proposal.

II. THE NEW IMPETUS BY THE GERMAN PRESIDENCY

4. The EDPS welcomes the fact that the German Presidency is putting a lot of effort into the negotiations on this Council Framework Decision. It is common knowledge that the negotiations were blocked in Council, because of fundamental differences in opinion between the Member States on essential issues. It was therefore a wise decision of the Presidency to give these negotiations a new impetus by presenting a fresh text.
5. The fact that the German Presidency gave a new impetus to the negotiations is in itself very positive. However, after a thorough examination of the latest text, the EDPS is disappointed about the content. The text presented by the German Presidency does not fulfil expectations. This is for the following reasons:
 - The text weakens the level of protection of the citizen, since a number of essential provisions for their protection which were included in the Commission proposal have been taken out.
 - In many aspects the revised proposal even falls below the level of protection afforded by Convention 108. It is thus both unsatisfactory and will even be incompatible with international obligations of the Member States.
 - The text adds new complexities to the dossier, since it covers data processing by Europol, Eurojust and the third-pillar Customs Information System, and it opens up the debate on the supervision on these bodies. Notably, this opinion will discuss whether a Council Framework Decision is an appropriate legal instrument for these topics.
 - The legislative quality of the text is unsatisfactory. Apart from the choice of legal instrument, several provisions do not fulfil the requirements of the common guidelines for the quality of drafting of Community legislation ⁽⁷⁾. In particular, the text is not drafted clearly, simply and precisely, which makes it difficult for the citizens to identify their rights and obligations unambiguously.
 - The low level of protection afforded by the proposal cannot properly serve the creation of an area of freedom, security and justice in which law enforcement information can be exchanged between police and judicial authorities disregarding national borders. Indeed, in the absence of a high and broadly applicable level of data protection, the proposal makes exchanges of information still subject to different national 'rules of origin' and 'double standards' that strongly affect efficiency in law enforcement cooperation while not improving the protection of personal data ⁽⁸⁾.
6. The EDPS is well aware of the difficulties in reaching unanimity in the Council. However, the decision-making procedure cannot justify a lowest common denominator approach that would hinder the fundamental rights of EU citizens as well as hamper the efficiency of law enforcement. In this context, it would be desirable that data protection expertise would be fully taken into account and that the recommendations made by the European Parliament in its resolutions ⁽⁹⁾ would be duly integrated.

⁽⁷⁾ Interinstitutional Agreement of 22 December 1998 on common guidelines for the quality of drafting of Community legislation (OJ C 73, 17.3.1999, p. 1). Examples can be found in chapter V of this opinion.

⁽⁸⁾ See for example, Article 14 on transfers to third countries and international bodies; Article 12(1)(d) on further processing of personal data; Article 10 on compliance with time-limits for erasure and review; Article 13 on compliance with national processing restrictions.

⁽⁹⁾ The European Parliament adopted its first resolution on the initial Commission proposal on 27 September 2006. A second resolution, on the revised proposal, is expected by June.

III. LEGAL FRAMEWORK AND FOCUS OF THIS OPINION

7. A Framework Decision on the protection of personal data in the third pillar is an essential element in the development of an area of freedom, security and justice. The growing importance of the police and judicial cooperation in criminal matters as well as the actions stemming from the Hague Programme ⁽¹⁰⁾ have highlighted the necessity of common standards in the protection of personal data in the third pillar.
8. Unfortunately, as repeatedly affirmed by the EDPS and other relevant actors ⁽¹¹⁾, the existing instruments at European level are not sufficient. Council of Europe Convention 108, which is binding on Member States, lays down fundamental general principles of data protection, but, even though it must be interpreted in the light of the ECHR case law, does not provide for the necessary preciseness, as has been stated before by the EDPS on several occasions ⁽¹²⁾. Directive 95/46/EC, which integrated and specified the principles of Convention 108 with regard to the internal market, has been adopted already in 1995. This directive does not apply to activities which fall within the scope of the third pillar. For activities within the area of police and judicial cooperation all Member States have subscribed to Recommendation No R (87) 15 ⁽¹³⁾, which specifies Convention 108 to a certain extent for the police sector, but this is not a binding legal instrument.
9. In this context, Article 30(1)(b) of the EU-Treaty requires that common actions in the field of police cooperation entailing the processing of information by law enforcement authorities shall be subject to 'appropriate provisions on the protection of personal data'. Such appropriate provisions do not exist, in the absence of a Council Framework Decision with a satisfactory content.
10. A parallel can be easily drawn with the development of the internal market, where a high level of protection of personal data throughout the Community was considered to be an essential element to eliminate obstacles in the free circulation of goods, services, capitals, and persons, and led to the adoption of Directive 95/46/EC. By analogy, an area of freedom, security and justice in which information should freely flow between authorities dealing with law enforcement both at national and EU level requires a high and uniform level of protection of personal data in all Member States.
11. These considerations are in contrast with the current situation, in which there is not such a general framework and in which the provisions on the protection of personal data in the third pillar are 'sector specific' and dispersed in different legal instruments ⁽¹⁴⁾. Some recent proposals ⁽¹⁵⁾ confirm and enhance the already existing fragmentation of data protection provisions in this area and put at risk their consistency. Furthermore, the lack of a general framework affects the swift adoption of many proposals in the area of police and judicial cooperation.
12. For these reasons the EDPS has strongly supported the Commission proposal in his previous opinions and has put forward appropriate recommendations in order to improve the proposal which was needed to ensure an appropriate level of protection of the citizen. The EDPS has constantly held that a general framework for data protection in the third pillar must ensure a high and consistent standard of data protection, by building on data protection principles laid down by Convention 108 and Directive 95/46/EC, whilst also taking into account, where necessary, the specificities of law enforcement activities.
13. Consistency of this general framework with first pillar data protection principles is all the more important in a context in which the growing involvement of the private sector in law enforcement entails that personal data move from the first pillar to the third pillar (like in the case of PNR) or from the third

⁽¹⁰⁾ See also the Council and Commission Action Plan implementing the Hague Programme on strengthening freedom, security and justice in the European Union (OJ C 198, 12.8.2005, p. 1).

⁽¹¹⁾ The Conference of European Data Protection Authorities, delivered an opinion on 24 January 2006, available as document No 6329/06 at register.consilium.europa.eu. The Council of Europe's Consultative Committee on the Convention for the Protection of Individuals with regard to automatic processing of personal data (T-PD) adopted on 20 March 2007 a paper outlining its initial remarks, which is available at: www.coe.int/dataprotection/

⁽¹²⁾ See, more recently, the opinion of the EDPS of 4 April 2007 on the initiative of 15 Member States with a view to adopting a Council Decision on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, point 60.

⁽¹³⁾ Recommendation No R (87) 15 of the Committee of Ministers to Member States regulating the use of personal data in the police sector, adopted on 17 September 1987 and available at: www.coe.int/dataprotection/

⁽¹⁴⁾ Such as the legal instruments regulating Europol, Eurojust, the third pillar Customs Information System.

⁽¹⁵⁾ Such as the recent initiatives concerning Europol, the Prüm Treaty and access by law enforcement to VIS database.

pillar to the first pillar. Relevant examples can be easily found: the use of 'no fly lists' including persons who should not be allowed on airplanes and established for law enforcement by airlines for purposes within the first pillar (commercial purposes as well as flight security), as well as the proposal on access by law enforcement authorities to the VIS database, established as an instrument of a common visa policy ⁽¹⁶⁾. Therefore, the EDPS stresses that data protection principles in the first pillar must apply also to the third pillar. However, the specificities of law enforcement activities may make additional or exceptional provisions necessary ⁽¹⁷⁾.

14. Appropriate, consistent and broadly applicable safeguards for data protection in the third pillar are essential not only to guarantee the fundamental right of data protection of individuals, but also to foster efficiency in law enforcement cooperation within the area of freedom, security and justice.
15. Against this background, this opinion assesses to what extent the current revised proposal lays down appropriate provisions on the protection of personal data, pursuant to Article 30(1)(b) of the EU-Treaty. In doing so, the EDPS will refer to some of the recommendations made in his previous opinions. This opinion will also assess whether the revised proposal respects the international obligations of Member states stemming from Council of Europe Convention 108 and ECHR case law, as well as the principles laid down in Recommendation No R (87) 15 on the use of personal data in the police sector. Furthermore, the EDPS will consider to what extent the provisions of the proposal would have an impact on efficiency in police and judicial cooperation.

IV. MAIN CONCERNS

IV.1. Applicability to domestic processing of personal data

16. The proposal now includes a recital stating that Member States will apply the rules of the Framework Decision to national data-processing, so that conditions for transmitting data *may* already be met when the data are collected (Recital 6a). This recital tries to address the concerns voiced not only by the EDPS in his previous opinions, but also by many other stakeholders. Indeed, the European Parliament, the Conference of data protection authorities, and even the Council of Europe's T-PD Consultative Committee — consisting of data protection representatives of European governments — have all made clear in various occasions that the applicability of the Framework Decision to domestic processing of personal data is an essential condition not only to ensure a sufficient protection of personal data but also to allow an efficient cooperation between law enforcement authorities ⁽¹⁸⁾.
17. However, the recital as such cannot impose an obligation which is not explicitly laid down in the provisions. Unfortunately, Article 1 (Purpose and scope) explicitly limits the applicability of the proposal to data exchanged between Member States or EU bodies, by guaranteeing that *'the basic rights and freedoms, and in particular the privacy, of data subjects are fully protected when personal data are transmitted [...]'*.
18. Therefore, the current draft leaves to Member States' full discretion in the application of uniform data protection principles to domestic processing of personal data and does not bind Member States to implement the same common data protection standards, this all within an area of police and judicial cooperation, where internal borders must be lifted. Against this background, the EDPS highlights again that the possibility of having different levels of data protection in different Member States within the third pillar would be:
 - inconsistent with the creation of an area of freedom, security and justice within which citizens move freely and with a proper approximation of the laws pursuant to Article 34(2)(b) of the EU-Treaty,
 - not appropriate for the protection of personal data, in light of Article 30(1)(b) of the EU-Treaty,

⁽¹⁶⁾ See Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences (COM(2005)600 final).

⁽¹⁷⁾ In the same line, see also the Explanatory memorandum of Recommendation No R (87) 15, point 37.

⁽¹⁸⁾ See documents mentioned in footnote 9.

- inefficient and unworkable for law enforcement authorities, which would be unduly burdened by unmanageable distinctions between domestic data and data transmitted or available for transmission, which in most cases will be part of the same file ⁽¹⁹⁾.
19. The EDPS strongly advises the legislator to extend the scope of applicability, by obliging — not only inviting — Member States to apply the Framework Decision to domestic processing of personal data. Moreover, there are no compelling legal arguments supporting the view that application to domestic data would not be allowed under Article 34 of the EU-Treaty.

IV.2. Limitation of the further purposes for which personal data may be processed

20. The principle of purpose limitation is one of the basic principles of data protection. In particular, Convention 108 states that personal data shall be '*stored for specified and legitimate purposes and not used in a way incompatible with those purposes*' (Article 5(b)). Derogations to this principle are allowed only insofar as they are provided for by law and constitute a necessary measure in a democratic society in the interests of, inter alia, the 'suppression of criminal offences' (Article 9). The case law of the European Court of Human Rights has made clear that these derogations shall be proportionate, precise and foreseeable, pursuant to Article 8, paragraph 2 of the European Convention on Human Rights ⁽²⁰⁾.
21. In the current proposal, the provisions on purpose limitation are laid down both in Article 3 and Article 12. Article 3 allows further processing for purposes compatible with the one for which data were collected, and is thus, in this respect, in line with basic data protection principles.
22. However, Article 3 is far too broad and does not cover an appropriate limitation of the purposes for storage, also required by Article 5(b) of Convention 108, mentioned above. The general reference to the purposes of Title VI of the EU-Treaty can not be seen as specified and legitimate purposes. The purpose of police and judicial cooperation is not by nature legitimate ⁽²¹⁾, and certainly not specified.
23. Article 3 does not contain any derogation as would be possible pursuant to Article 9 of Convention 108. However, Article 12 of the proposal lays down a very broad and not clearly defined series of derogations to the purpose limitation principle in the context of personal data received from or made available by another Member State. In particular, the condition that derogations shall be necessary is not explicitly laid down in the article. Secondly, it is not clear which are the 'other [...] administrative proceedings' for which Article 12(1)(b) allows processing of personal data collected and transmitted for a different purpose. Furthermore, Article 12(1)(d) allows processing for 'any other purpose' with the sole condition that the competent authority that has transmitted the personal data gives its consent. In this context, it shall be noted that the consent of the transmitting authority cannot be considered under any circumstances as replacing the consent of the data subject or providing legal grounds to derogate from the purpose limitation principle. Therefore, the EDPS would like to stress that this broad and open derogation does not fulfil the basic requirements of adequate data protection and even contradicts the basic principles of Convention 108. Therefore, the EDPS recommends the legislator to redraft the relevant provisions.
24. A last remark concerns Article 12(2), which allows the possibility that third pillar Council decisions take precedence over paragraph 1 where appropriate conditions are laid down for the processing of personal data. The EDPS notes that the formulation of this paragraph is very general and does not do justice to the nature of the Council Framework Decision as a *lex generalis* for police and judicial cooperation. This *lex generalis* should apply to all processing of personal data in this area.
25. The EDPS believes that the current provisions on further processing of personal data impinge on the basic purpose limitation principle and even fall below the existing standard laid down by Convention 108. Therefore, the EDPS recommends the legislator to redraft the relevant provisions in the light of the existing international data protection rules and of the relevant case law.

⁽¹⁹⁾ For a more detailed reasoning, see EDPS second opinion, points 11-13.

⁽²⁰⁾ Among the consolidated case law in this domain, the most explicit case is *Rotaru v. Romania*.

⁽²¹⁾ It is not sufficient to start from the assumption that the police under all circumstances and in all cases operates within the limits of its legal obligations.

IV.3. Adequate protection in the exchange of personal data with third countries

26. Convention 108 also deals with transfers to third countries. The Additional protocol regarding supervisory authorities and transborder data flows lays down the general principle — subject to certain derogations — that transfer of personal data to third party is permitted only if that party ‘ensures an adequate level of protection for the intended data transfer’. The principle of ‘adequate protection’ has been implemented and specified within several legal instruments of the European Union, not only in first pillar instruments on data protection, like Directive 95/46/EC ⁽²³⁾, but also in legal instruments within the third pillar, such as the legal instruments establishing Europol and Eurojust.
27. Recital 12 of the current proposal states that, in case of transfer of personal data to third countries or international bodies, ‘these data should, in principle, benefit from an adequate level of protection’. Furthermore, Article 14 allows personal data transmitted from another Member State to be transferred to third countries or international bodies when the transmitting authority has given its consent to the transfer in compliance with its national law. Therefore, the provisions of the proposal do not establish any need for adequate protection, nor foresee any common criteria or mechanisms in order to assess adequacy. This means that each Member State will assess at its own discretion the level of adequacy provided for by the third country or international organisation. As a consequence, the list of adequate countries and international organisations — to which a transfer is allowed — will considerably vary from Member State to Member State.
28. This legal framework would also hinder police and judicial cooperation. Indeed, law enforcement authorities of a Member State, when deciding on a request for a certain criminal file by a third country, will not only have to consider the adequacy of that country, but shall also take into account whether or not each of the other (up to 26) Member States that contributed to the file has given its consent, according to its own adequacy assessment of the relevant third country.
29. In this context, Article 27 of the proposal, on Relationship to agreements with third States, adds more uncertainty, stating that the Framework Decision is without prejudice to obligations and commitments incumbent upon Member States or upon EU by virtue of bilateral and/or multilateral agreements with third States. According to the EDPS, this provision should be clearly limited to existing agreements and should lay down that future agreements shall be in line with the provisions of this proposal.
30. The EDPS believes that current provisions on transfers of personal data to third countries and international organisations would not be appropriate to protect personal data as well as unworkable for law enforcement authorities. Therefore, the EDPS reiterates ⁽²³⁾ the need to ensure an adequate level of protection when personal data are transferred to third countries or international organizations, and that mechanisms ensuring common standards and coordinated decisions with regard to adequacy are put in place. The same opinion has been expressed before by the European Parliament and the T-PD Committee of the Council of Europe.

IV.4. Quality of data

31. Article 5 of Convention 108 lays down the principles for ensuring the quality of personal data. Further details are provided in other non binding instruments like Recommendation No R (87) 15 and in its three evaluations carried out so far.
32. When comparing the current proposal with the aforementioned legal instruments, it is clear that some important guarantees, in some cases already provided by the Commission proposal, are lacking in the revised version:
- Article 3 of the proposal does not guarantee that data are obtained and processed fairly, as required by Article 5 of Convention 108.

⁽²²⁾ With regard to this point, it should be noted that the Commission has recently stated, in its *Communication of 7 March 2007 on the follow-up of the Work Programme for better implementation of the Data Protection Directive*, that the rules laid down by Directive 95/46/EC in relation to transfers of personal data to third countries are substantially appropriate and need not to be modified.

⁽²³⁾ See the concerns already expressed in the first opinion, paragraph IV.8, and in the second opinion, points 22-23.

- The proposal no longer includes any provisions laying down — as required by Principle 3.2 of Recommendation No R (87) 15 — that different categories of data are distinguished in accordance with their degree of accuracy and reliability and that data based on facts are distinguished from data based on opinions or personal assessments ⁽²⁴⁾. The lack of such a common requirement could actually undermine the data being exchanged between police authorities as they will not be able to ascertain whether the data can be construed as ‘evidence’, ‘fact’, ‘hard intelligence’ or ‘soft intelligence’. This could have the consequence of not only hampering security operations and intelligence gathering which rely on these distinctions but also making it more difficult for courts to secure convictions.
 - There are no distinctions between different categories of data subjects (criminals, suspects, victims, witnesses, etc.) nor specific guarantees for data relating to non-suspects, contrary to Principle 2 of Recommendation No R (87) 15 and its evaluation reports ⁽²⁵⁾. Again, these distinctions are not only necessary for the protection of the personal data of the citizen, but also for the ability of the recipients to be able to make full use of the data they receive. Without these distinctions, the receiving police services can not immediately use the data, but have first to ascertain how the data must be qualified and subsequently how they can be used and shared for different law enforcement purposes.
 - The periodic review provided for by Article 6 does not ensure the periodic verification of data quality and that police files are purged of superfluous or inaccurate data and kept up to date, as required by Recommendation No R (87) 15 ⁽²⁶⁾. The importance of such review for data protection is obvious, but again this is also vital for the efficient operation of police services. Old and out of date intelligence is at best useless and at worst can shift resources away from current priorities to matters which are not, and should not, be the focus of investigation.
 - If personal data — transmitted from another Member State — are found to be inaccurate, there are no obligations or mechanisms to ensure their rectification in the originating Member State. Again the issue of accuracy is vital to the effective operation of the police and judiciary. If the quality of data cannot be guaranteed, it will harm the usefulness of data transfer as a tool for fighting crime across borders.
33. Against this background, the EDPS believes that the provisions relating to data quality of the current proposal are neither appropriate nor complete — specifically taking into account Recommendation No R (87) 15 which has been subscribed by all the Member States —, and they even fall below the level of protection required by Convention 108. It is also useful to recall once more that accuracy of personal data is in the interest of both the law enforcement itself as well as the individual ⁽²⁷⁾.

IV.5. Exchanges of personal data with non competent authorities and private parties

34. According to Principle 5 (Communication of data) of Recommendation No R (87) 15, communication of personal data from law enforcement authorities to other public bodies or to private parties should only be permissible under specific and strict conditions. Such provisions, laid down in the initial Commission proposal and welcomed by the EDPS and the European Parliament, have been now deleted by the revised version. Therefore, the new text does not lay down any specific guarantees for transfers of personal data to private parties or non law enforcement authorities.

⁽²⁴⁾ Point 52 of explanatory Memorandum to Recommendation states that ‘[i]t should be possible to distinguish between corroborated data and uncorroborated data, including assessment of human behaviour, between facts and opinions, between reliable information (and the various shades thereof) and conjecture, between reasonable cause to believe that information is accurate and a groundless belief in its accuracy’. See also the Second evaluation of the relevance of recommendation No R (87) 15 regulating the use of personal data in the police sector (1998), point 5.1.

⁽²⁵⁾ See in particular, point 5.2 of the Second evaluation, mentioned above, and points 24-27 of the Third evaluation of Recommendation No R (87) 15 regulating the use of personal data in the police sector (2002).

⁽²⁶⁾ See principle 7 (Length of storage and updating of data) and the Explanatory Memorandum, points 96-98.

⁽²⁷⁾ Explanatory memorandum to Recommendation No R (87) 15, point 74.

35. In addition, access and further use by law enforcement authorities of personal data controlled by private parties shall be permitted only on the basis of well defined conditions and limitations. In particular, as the EDPS already mentioned in his previous opinions, access by law enforcement authorities shall be allowed only on a case-by-case basis, under specified circumstances, for specified purposes, and be under judicial control in the Member States. Recent developments, such as Directive 2006/24/EC ⁽²⁸⁾ on data retention, the PNR agreement with the United States ⁽²⁹⁾, and the access by law enforcement authorities to data held by SWIFT ⁽³⁰⁾ confirm the fundamental importance of these guarantees. It is unfortunate that the current proposal does not provide for any specific guarantees on access and further use by law enforcement authorities of personal data collected by private parties.
36. Against this background, the EDPS notes that, with regard to exchanges of personal data with private parties and non competent authorities, the current proposal fails to comply with the principles of Recommendations No R (87) 15 and to address the fundamental issue of access and further use by law enforcement authorities of personal data controlled by private parties.

IV.6. Other substantive points

37. Besides the abovementioned main concerns, the EDPS would like to draw the legislator's attention to the following points, which in most of the cases have already been addressed in more details in his previous opinions:
- **Special categories of data.** Article 7 of the revised proposal contradicts the in-principle prohibition laid down by Article 6 of Convention 108. Furthermore, it fails to refer to personal data relating to criminal convictions, which are undoubtedly very relevant in the context of police and judicial cooperation, and does not provide for specific safeguards with regard to biometric data and DNA-profiles.
 - **Automated individual decisions.** EDPS welcomes that Article 8 integrates this provision into the revised proposal.
 - **Logging and documentation.** Article 11, in order to be effective for the purposes of verification of the lawfulness of data processing, shall lay down appropriate mechanisms for logging or documenting not only all transmissions of data, but also *all accesses* to data.
 - **Right to be informed.** Article 16 is incomplete, since it does not mention information about the identity of the controller and the recipients. Furthermore, Recital 13 ('[...] it may be necessary to inform data subjects [...]') depicts information as a mere possibility rather than a basic obligation of the controller.
 - **Right of access.** Article 17 is incomplete, since access shall include also the *purposes* for which data are processed and communication in an *intelligible form*. Furthermore, exceptions laid down by paragraph 2 — such as the case when access would 'otherwise be detrimental to national interests' — are too broad and unforeseeable. Lastly, there is no mechanism ensuring that the appeal to the supervisory authority results in granting access, when it had been unlawfully denied.

V. NEW ISSUES RAISED BY THE REVISED PROPOSAL

38. The revised proposal includes as a fully new element, in comparison with the Commission proposal. It covers activities by European institutions and bodies in the third pillar (Article 1(2) of the proposal). According to the 20th Recital, this includes data processing by Europol, Eurojust and the third pillar Customs Information System. Article 1(2) does not only mention European bodies but also institutions, which means that for instance data processing within the Council should be subject to the Council

⁽²⁸⁾ Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ L 105, 13.4.2006, p. 54).

⁽²⁹⁾ Agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security (OJ L 298, 27.10.2006, p. 29).

⁽³⁰⁾ See Working Party 29 Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp128_en.pdf, and EDPS Opinion on the role of the European Central Bank in the SWIFT case, available at EDPS website.

Framework Decision. It is not clear whether the drafters intended such a wide scope, or that they intended to limit the application to the three bodies mentioned in the 20th Recital. It would in any event be needed to specify the text, in order to avoid legal uncertainty.

39. This leads to a more general remark. According to the EDPS, it is of utmost importance that an appropriate level of data protection is guaranteed throughout the whole third pillar, since only under such condition a free exchange of information within an area of freedom, security and justice without internal borders would be facilitated in a sufficient manner. This includes applying the general framework on data protection to the European bodies in the third pillar. The EDPS underlined this need earlier in Part IV of his Opinion on the proposal for a Council Decision on Europol.
40. However, for reasons of effective law making the EDPS has serious doubts whether the present Council Framework Decision should cover the activities of the European bodies that operate in the third pillar. The first argument against this wide scope has to do with legislative policy. The EDPS fears that including the European bodies in the present text would run the risk that the discussions in Council will concentrate on this new element, instead of on the substantive provisions on data protection. It will complicate the legislative process. The second argument is of a legal nature. At first sight, it seems that a Council Framework Decision — an instrument which is comparable to a directive under the EC-Treaty — is not an appropriate legal instrument to regulate the rights and obligations of European bodies. Article 34 of the EU-Treaty introduces this instrument for the approximation of the laws and regulations of the Member States. In any event, there is a serious risk that the legal basis will be challenged during the legislative process, or afterwards.
41. The EDPS has a similar view, also with regard to the legal instrument chosen, on Article 26 of the draft, which foresees the establishment of a new joint supervisory authority, replacing the existing authorities that supervise the data processing within third pillar bodies. By itself, the intention to set up such an authority may seem logical. It might lead to an even more efficient system of supervision, and further ensure consistency of the level of protection within the bodies established under the third pillar.
42. However, at this moment there is no immediate need for such a new supervisory body. The supervision itself functions satisfactorily. Moreover, the president of Eurojust has put forward objections against application of this system of supervision to Eurojust. Without entering into the substance of these objections, it is clear that adding the subject matter of supervision on EU-bodies to the Council Framework Decision would make the legislative process even more difficult. In addition, this approach would not be consistent with other proposals in this area that are presently on the table ⁽³¹⁾ or have been recently adopted ⁽³²⁾.
43. In short, the EDPS advises not to add provisions relating to data processing by EU-bodies to the text of the Council Framework Decision. The EDPS gives this advice for reasons of effective law making. It is important that all efforts in Council will be concentrated on the substantive provisions of data protection in order to give the citizen the necessary protection.

VI. CONCLUSIONS

44. The EDPS welcomes the new impetus given by the German Presidency. Adopting a general framework for data protection in the third pillar is essential, as the EDPS and other relevant actors have already highlighted in several occasions, in order to support the development an area of freedom, security and justice in which citizens' right to protection of personal data is uniformly guaranteed and cooperation between law enforcement authorities can take place disregarding national borders.
45. However, the revised proposal does not meet either of these objectives. Indeed, in the absence of a high and broadly applicable level of data protection, the proposal makes exchanges of information still subject to different national 'rules of origin' and 'double standards' that strongly affect efficiency in law enforcement cooperation while not improving the protection of personal data.

⁽³¹⁾ Such as the recent Commission proposal on establishing the European Police Office, COM(2006)817 final.

⁽³²⁾ Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II) (OJ L 381 of 28.12.2006, p. 4).

46. To give a concrete example, this would mean that a law enforcement body at national or EU level, when dealing with a criminal file — consisting of information originating from various national, other Member States' and EU authorities — would have to apply different processing rules for different pieces of information depending on whether: personal data have been collected domestically or not; each of the transmitting bodies has given its consent for the envisaged purpose; the storage is compliant with time limits laid down by applicable laws of each of the transmitting bodies; further processing restrictions requested by each of the transmitting bodies do not prohibit the processing; in case of a request from a third country, each transmitting body has given its consent according to its own evaluation of adequacy and/or international commitments. In addition, citizens' protection and rights will vary enormously and be subject to different broad derogations depending on the Member State where processing takes place.
47. Furthermore, the EDPS regrets that the legislative quality of the text is unsatisfactory and that the proposal adds new complexities to the dossier, by extending the applicability of the Framework Decision to Europol, Eurojust and the third-pillar Customs Information System as well as proposing the creation of a Joint Supervisory Body on the basis of an inappropriate legal instrument.
48. The EDPS is concerned because the current text takes out essential provisions for the protection of personal data which were included in the Commission proposal. By doing so, it significantly weakens the level of protection of the citizens. Firstly, it fails to provide the added value to Convention 108 which would make its provisions appropriate from a data protection point of view, as required by Article 30(1) of the EU-Treaty. Secondly, it also fails to meet in many aspects the level of protection required by Convention 108. Therefore, the EDPS believes that this proposal would need substantial improvements before it could be the basis for the discussion of an adequate general framework on data protection in the third pillar. These improvements should make sure that this general framework:
- Provides added value to Convention 108, by laying down the appropriate provisions on the protection of personal data required by Article 30(1) of the EU-Treaty.
 - Is applicable to domestic processing of personal data by law enforcement authorities.
 - Is consistent with first pillar data protection principles, whilst also taking into account, where necessary, the specificities of law enforcement activities.
 - Is in line with the principles laid down by Convention 108 and Recommendation No R (87) 15, in particular with regard to:
 - Limitation of the further purposes for which personal data may be processed.
 - Quality of data, including distinction between different categories of data subjects (criminals, suspects, victims, witnesses, etc.), assessment of the different degree of accuracy and reliability of personal data, mechanisms to ensure periodic verification and rectification.
 - Conditions for transfers of personal data to non competent authorities and private parties, as well as for access and further use by law enforcement authorities of personal data controlled by private parties.
 - Ensures adequate protection in the exchange of personal data with third countries, also with regard to international agreements.
 - Addresses the other points mentioned in this as well as previous EDPS opinions.
49. The EDPS is well aware of the difficulties in reaching unanimity in the Council. However, the decision making procedure cannot justify a lowest common denominator approach that would hinder the fundamental rights of EU citizens as well as hamper the efficiency of law enforcement.

Done at Brussels, 27 April 2007.

Peter HUSTINX

European Data Protection Supervisor

I

(Resolutions, recommendations and opinions)

OPINIONS

EUROPEAN DATA PROTECTION SUPERVISOR

Opinion of the European Data Protection Supervisor on the draft Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes

(2008/C 110/01)

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty establishing the European Community, and in particular its Article 286,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular its Article 8,

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ⁽¹⁾,

Having regard to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data ⁽²⁾, and in particular its Article 41,

Having regard to the request for an opinion in accordance with Article 28(2) of Regulation (EC) No 45/2001 received on 13 November 2007 from the European Commission,

HAS ADOPTED THE FOLLOWING OPINION

I. INTRODUCTION

Consultation of the EDPS

1. The draft Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law

enforcement purposes was sent by the Commission to the EDPS for consultation, in accordance with Article 28(2) of Regulation No 45/2001/EC (hereinafter 'the proposal').

2. The proposal concerns the processing of PNR data within the EU and is closely related to other schemes of collection and use of passengers' data, in particular the EU-US agreement of July 2007. These schemes are of great interest to the EDPS, who already had the opportunity to send some preliminary comments on the Commission's questionnaire on the intended EU PNR system, sent in December 2006 to relevant stakeholders ⁽³⁾. The EDPS welcomes the consultation of the Commission. According to the EDPS, the present opinion should be mentioned in the preamble of the Council Decision.

The proposal in its context

3. The proposal intends to harmonise Member States' provisions on obligations for air carriers operating flights to or from the territory of at least one Member State regarding the transmission of PNR data to the competent authorities for the purpose of preventing and fighting terrorist offences and organised crime.
4. Arrangements for transmission of PNR data for comparable purposes have been concluded by the European Union with the USA, as well as with Canada. A first agreement concluded with the USA in May 2004 was replaced

⁽¹⁾ OJ L 281, 23.11.1995, p. 31.

⁽²⁾ OJ L 8, 12.1.2001, p. 1.

⁽³⁾ Including Member States, Data Protection Authorities and airlines associations. This questionnaire had been prepared in view of the preparation of an impact assessment by the European Commission on the present proposal.

by a new agreement in July 2007 ⁽¹⁾. A similar agreement was concluded with Canada in July 2005 ⁽²⁾. In addition, negotiations are due to start between the EU and Australia for an agreement on the exchange of PNR data, and South Korea is also requiring PNR data from flights to its territory, without any plan for negotiation at European level at this stage.

5. Within the EU, the proposal comes as an addition to Council Directive 2004/82/EC ⁽³⁾ on the obligation of carriers to communicate passengers' data known as API data, in order to combat illegal immigration and improve border control. This directive should have been transposed in national law of Member States not later than 5 September 2006. Implementation is however not ensured yet in all Member States.

6. Contrary to Advanced Passenger Information (API) data that are supposed to help identifying individuals, PNR data mentioned in the proposal would contribute to carrying out risk assessments of persons, obtaining intelligence and making associations between known and unknown people.

7. The proposal includes the following main elements:

- It provides for the making available by air carriers of PNR data to the competent authorities of Member States, for the purpose of preventing and combating terrorist offences and organised crime.
- It foresees the designation of a Passenger Information Unit (PIU) in principle in each Member State, responsible for collecting the PNR data from air carriers (or designated intermediaries) and for carrying out a risk assessment of passengers.
- Information assessed accordingly will be transmitted to competent authorities in each Member State. This information will be exchanged with other Member States on a case by case basis and for the purpose indicated above.
- Transfer to countries outside the European Union is subject to additional conditions.

— Data will be retained for thirteen years, eight of which in a dormant database.

— The processing is to be governed by the (draft) Council Framework decision on the Protection of Personal Data Processed in the Framework of Police and Judicial Cooperation in Criminal Matters (hereafter the 'data protection framework decision') ⁽⁴⁾.

— A Committee with representatives of Member States will assist the Commission with regard to protocol and encryption issues, as well as with regard to criteria and practice for risk assessment.

— A review of the decision is to take place within three years after its entry into force.

Focus of the opinion

8. The proposal on which the EDPS is consulted is a further step in a movement towards a routine collection of data of individuals who are in principle not suspected of any crime. As mentioned above, this evolution is taking place at international and European level.

9. The EDPS notes that also the Article 29 Working Party and the Working Party on Police and Justice have presented a joint opinion on the proposal ⁽⁵⁾. The EDPS supports that opinion. The present opinion emphasises and develops a number of additional points.

10. While the opinion of the EDPS will analyse all relevant aspects of the proposal, it will concentrate on four main issues.

— The first of these issues is the legitimacy of the intended measures. The question of the purpose, necessity and proportionality of the proposal will be assessed against the criteria of Article 8 of the Charter of Fundamental Rights of the European Union.

— The opinion will also analyse the question of the law applicable to the proposed processing operation. In particular, the scope of application of the data protection framework decision in relation to the application of first pillar data protection legislation deserves specific attention. The consequence of the applicable data protection regime with regard to the exercise of data subject's rights will also be questioned.

⁽¹⁾ Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement) (OJ L 204, 4.8.2007, p. 18).

⁽²⁾ Agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information and Passenger Name Record data (OJ L 82, 21.3.2006, p. 15).

⁽³⁾ Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data (OJ L 261, 6.8.2004, p. 24).

⁽⁴⁾ The latest draft of this proposal is available on Council register as document number 16397/07.

⁽⁵⁾ Joint opinion on the proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, presented by the Commission on 6 November 2007, adopted by the Article 29 Working Party on 5 December 2007 and by the Working Party on Police and Justice on 18 December 2007, WP 145, WPPJ 01/07.

- The opinion will then focus on the quality of recipients of data at national level. In particular, the quality of PIUs, of intermediaries and of competent authorities designated to perform risk assessment and analyse passenger data raises specific concerns as no precision is given in the proposal in this respect.
- The fourth issue relates to the conditions of transfer of data to third countries. It is not clear what conditions will apply to such transfers where different sets of rules exist: the conditions of transfer under the present proposal, together with those of the data protection framework decision, and the existing international agreements (with the USA and Canada).

11. Other substantive points will be identified in a last part, including positive steps in terms of data protection but also additional sources of concern in the proposal.

II. LEGITIMACY OF THE PROPOSED MEASURES

12. In order to analyse the legitimacy of the proposed measures in accordance with fundamental data protection principles, and notably Article 8 of the European Charter of Fundamental Rights and Articles 5 to 8 of Council of Europe Convention No 108 ⁽¹⁾, it is necessary to identify clearly the purpose of the intended processing of personal data, to assess its necessity and its proportionality. It should be ensured that no other means is available, that would be less invasive, to reach the envisaged purpose.

Identification of purpose

13. The wording of the proposal and its impact assessment indicate that the objective is not simply to identify known terrorists or known criminals involved in organised crime, by comparing their names with those included in lists managed by law enforcement authorities. The purpose is to gather intelligence with regard to terrorism or organised crime, and more precisely 'to carry out risk assessment of persons, obtain intelligence and make association between known and unknown people' ⁽²⁾. The purpose stated in Article 3(5) of the proposal is, in the same line and firstly, 'to identify persons who are *or may be* involved in a terrorist or organised crime offence, *as well as their associates*.'
14. This is the reason invoked to explain that API data are not sufficient to reach the alleged purpose. Indeed, as already mentioned, while API data are supposed to help identifying individuals, PNR data do not have an identification purpose, but the details of the PNR would contribute to carrying out risk assessments of the persons, obtaining

intelligence and making associations between known and unknown people.

15. The purpose of the measures envisaged does not only cover the catching of *known* persons but also the locating of persons that *may* fall within the criteria of the proposal.

In order to identify these persons, risk analysis and identification of patterns are at the core of the project. Recital 9 of the proposal states explicitly that data must be kept 'for a sufficiently long period as to fulfil the purpose of developing risk indicators and establishing patterns of travel and behaviour'.

16. The purpose is thus described in two layers: the first layer consists of the global objective to fight against terrorism and organised crime, while the second layer includes the means and measures inherent to the achievement of this objective. While the purpose of fighting terrorism and organised crime appears to be clear enough and legitimate, the means used to reach this purpose leave room for discussion.

Establishing patterns and risk assessment

17. The proposal gives no indication on the way patterns will be established and risk assessment will be performed. The impact assessment gives the following precision as to the way PNR data will be used: to run the data of passengers 'against a combination of characteristics and behavioural patterns, aimed at creating a risk-assessment. When a passenger fits within a certain risk-assessment, then he could be identified as a high-risk passenger' ⁽³⁾.
18. Suspected persons could be selected according to concrete elements of suspicion included in their PNR data (e.g. contact with a suspicious travel agency, reference of a stolen credit card), as well as on the basis of 'patterns' or an abstract profile. Different standard profiles could indeed be constituted on the basis of travel patterns, for 'normal passengers' or 'suspicious passengers'. These profiles would enable investigating further those passengers who do not fall within the 'normal passenger category', all the more so if their profile is associated with other suspicious elements such as a stolen credit card.
19. Although it cannot be assumed that passengers would be targeted according to their religion or other sensitive data, it appears nevertheless that they would be subject to investigation on the basis of a mix of *in concreto* and *in abstracto* information, including standard patterns and abstract profiles.

⁽¹⁾ Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe, 28 January 1981.

⁽²⁾ Explanatory Memorandum of the proposal, Chapter I.

⁽³⁾ Impact assessment, Chapter 2.1, 'Description of the problem'.

20. One could discuss whether this type of investigation would qualify as profiling. Profiling would consist of a 'computer method making use of data mining on a data warehouse, enabling or intended to enable the classification, with some probability — and thus with some margin of error — of an individual in a specific category in order to take individual decisions towards that person' ⁽¹⁾.
21. The EDPS is aware that there are ongoing discussions on the definition of profiling. Whether or not it is officially recognised that the proposal aims at *profiling* passengers, the main point at stake is not about definitions. It is about the impact on individuals.
22. The main concern of the EDPS relates to the fact that decisions on individuals will be taken on the basis of patterns and criteria established using the data of passengers in general. Thus decisions on one individual might be taken, using as a reference (at least partially), patterns derived from the data of *other* individuals. It is thus in relation to an abstract context that decisions will be taken, which can greatly affect data subjects. It is extremely difficult for individuals to defend themselves against such decisions.
23. In addition, the risk assessment is to be performed in absence of uniform standards of identification of suspects. The EDPS seriously questions the legal certainty of the whole filtering process, considering that the criteria against which every passenger will be scanned are so poorly defined.
24. The EDPS recalls the jurisprudence of the European Court of Human Rights, according to which domestic law must be sufficiently precise to indicate to citizens in what circumstances and on what terms the public authorities are empowered to file information on their private life

and make use of it. The information 'should be accessible to the person concerned and foreseeable as to its effects'. A rule is 'foreseeable' 'if it is formulated with sufficient precision to enable any individual — if need be with appropriate advice — to regulate his conduct' ⁽²⁾.

25. To conclude, it is notably because of these types of risks, that the present proposal needs careful consideration. While the general purpose to fight against terrorism and organised crime is in itself clear and legitimate, the core of the processing to be put in place does not appear to be sufficiently circumscribed and justified. The EDPS therefore urges the EU-legislator to clearly address this issue, before adoption of the Framework Decision.

Necessity

26. The intrusive character of the measures is evident, as shown above. On the other hand, their utility is far from being demonstrated.
27. The impact assessment on the proposal concentrates on the best way to establish an EU PNR, more than on the necessity of such PNR. Reference is made in the assessment ⁽³⁾ to PNR systems in place in other countries, namely the USA and the United Kingdom. One can however deplore the lack of precise facts and figures related to those systems. 'Numerous arrests' are reported with regard to 'various crimes' in the UK semaphore system, without precision as to the link with terrorism or organised crime. No details are given with regard to the US programme, except that 'the EU has been able to assess the value of PNR data and to realise its potential for law enforcement purposes'.
28. Not only is there a lack of precise information *in the proposal* on the concrete results of such PNR systems, but reports published by *other agencies*, e.g. the GAO in the United States, do not confirm at this stage the efficiency of the measures ⁽⁴⁾.

⁽¹⁾ This definition comes from a recent study on profiling of the Council of Europe: *L'application de la Convention 108 au mécanisme de profilage, Éléments de réflexion destinés au travail futur du Comité consultatif (T-PD)*, Jean-Marc Dinant, Christophe Lazaro, Yves Pouillet, Nathalie Lefever, Antoinette Rouvroy, November 2007 (not published yet). See also the definition by Lee Bygrave: 'Generally speaking, profiling is the process of inferring a set of characteristics (typically behavioural) about an individual person or collective entity and then treating that person/entity (or other persons/entities) in the light of these characteristics. As such, the profiling process has two main components: (i) profile generation — the process of inferring a profile; (ii) profile application — the process of treating persons/entities in light of this profile'. L. A. BYGRAVE, *Minding the machine: Article 15 of the EC Data Protection Directive and Automated Profiling*, *Computer Law & Security Report*, 2001, vol. 17, pp. 17-24 <http://www.austlii.edu.au/au/journals/PLPR/2000/40.html>

⁽²⁾ *Rotaru v. Romania*, No 28341/95, §§ 50, 52 and 55.
See also *Amann v. Switzerland*, No 27798/95, §§ 50 *et s.*

⁽³⁾ Chapter 2.1., 'Description of the problem'.

⁽⁴⁾ See e.g. the report of the United States Government Accountability Office to congressional requesters, May 2007, 'Aviation Security: Efforts to Strengthen International Passenger Prescreening are Under Way, but Planning and Implementation Issues remain' <http://www.gao.gov/new.items/d07346.pdf>

29. The EDPS considers that techniques consisting of assessing the risk presented by individuals using data mining tools and behavioural patterns need to be further assessed, and their utility be clearly established in the framework of the fight against terrorism, before they are used on such a wide scale.

Proportionality

30. In order to appreciate the balance between the intrusion in the privacy of the individual and the necessity of the measure ⁽¹⁾, the following elements are taken into account:
- The measures apply to all passengers, be they under investigation or not by law enforcement authorities. It constitutes proactive research, on an unprecedented scale.
 - Decisions on individuals can be based on abstract profiles, thus including a significant margin of error.
 - The nature of the measures to be taken against the individual relate to law enforcement: the consequences in terms of exclusion or coercion are therefore much more intrusive than in other contexts, like credit card fraud or marketing.
31. Compliance with the proportionality principle implies not only that the proposed measure is effective, but also that the purpose envisaged by the proposal can not be reached using the less privacy invasive tools. The effectiveness of the intended measures has not been demonstrated. The existence of alternatives must be carefully assessed before additional/new measures are put in place to process personal information. According to the EDPS, such comprehensive assessment has not taken place.
32. The EDPS wishes to recall the other large scale systems monitoring the movements of individuals within or at the borders of the EU, whether in operation or about to be implemented, including in particular the Visa Information System ⁽²⁾ and the Schengen Information System ⁽³⁾.

⁽¹⁾ According to article 9 of Convention 108, 'derogation from the provisions of Articles 5, 6 and 8 of this convention shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of:

1. protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences;

2. protecting the data subject or the rights and freedoms of others.'

⁽²⁾ Council decision 2004/512/EC of 8 June 2004 establishing the Visa Information System (VIS) (OJ L 213, 15.6.2004, p. 5). Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas, COM(2005) 0835 final; Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, COM(2005) 0600 final.

⁽³⁾ See in particular Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) (OJ L 205, 7.8.2007).

While these instruments do not have as a main goal the fight against terrorism or organised crime, they are or will be to some extent accessible to law enforcement authorities for the broader scope of the fight against crime ⁽⁴⁾.

33. Another example concerns the availability of personal data included in national police data bases — especially with regard to biometric information — in the framework of the Prüm Treaty signed in May 2005, that is being extended to all Member states of the European Union ⁽⁵⁾.

34. These different instruments all have in common that they enable a global monitoring of movements of individuals, even if from different perspectives. The way in which they can already contribute to the fight against specific forms of crimes, including terrorism, should be subject to in-depth and comprehensive analysis, before deciding to establish a new form of systematic scanning of all persons leaving or entering the EU by plane. The EDPS recommends that the Commission conducts such an analysis, as a necessary step in the legislative procedure.

Conclusion

35. In the light of the foregoing, the EDPS concludes as follows on the legitimacy of the proposed measures. Building upon different data bases without a global view on the concrete results and shortcomings:
- Is contrary to a rational legislative policy in which new instruments must not be adopted before those existing have been fully implemented and proved to be insufficient ⁽⁶⁾.
 - Might otherwise lead to a move towards a total surveillance society.
36. The fight against terrorism can certainly be a legitimate ground to apply exceptions to the fundamental rights to privacy and data protection. However, to be valid, the necessity of the intrusion must be supported by clear and

⁽⁴⁾ See on this issue: Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences (COM(2005) 600 final) (OJ C 97, 25.4.2006, p. 6).

⁽⁵⁾ See the EDPS Opinions on the Prüm Decisions: Opinion of 4 April 2007 on the initiative of 15 Member States with a view to adopting a Council Decision on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (OJ C 169, 21.7.2007, p. 2), and Opinion of 19 December 2007 on the Initiative of the Federal Republic of Germany, with a view to adopting a Council Decision on the implementation of Decision 2007/.../JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, available at: <http://www.edps.europa.eu>

⁽⁶⁾ This point has been made several times by the EDPS, most recently in its opinion of 25 July 2007 on the Implementation of the Data Protection Directive (OJ C 255, 27.10.2007, p. 1).

undeniable elements, and the proportionality of the processing must be demonstrated. This is all the more required in case of extensive intrusion in the privacy of individuals, as foreseen in the proposal.

37. It can only be noted that such elements of justification are missing in the proposal and that the necessity and proportionality tests are not fulfilled.
38. The EDPS insists on the essential character of the necessity and proportionality tests developed above. They represent a *condicio sine qua non* to the entry into force of the present proposal. Any further comment of the EDPS in the present opinion must be taken in the light of this preliminary condition.

III. APPLICABLE LAW — EXERCISE OF DATA SUBJECT'S RIGHTS

Applicable law

39. The analysis below will concentrate on three points:

- a description of the different steps of the processing foreseen in the proposal, with a view to identifying the law applicable at each stage,
- the limitations of the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters in terms of scope and in terms of rights of the data subject,
- a more general analysis of the extent to which a third pillar instrument can apply to private actors processing data in a first pillar framework.

Applicable law at different steps of the processing

40. Article 11 of the proposal states that 'Member States shall ensure that the Council Framework Decision on the Protection of Personal data Processed in the Framework of Police and Judicial Cooperation in Criminal Matters (...) is applicable to the processing of personal data under this Framework Decision.'
41. However, in spite of this provision it is not clear to what extent the data protection framework decision — an instrument under the third pillar of the EU Treaty — will be applicable to data processed by airlines, collected by PIUs, and further used by other competent authorities.
42. The first step in the processing of personal data foreseen by the proposal is processing by the airlines, which are obliged to make PNR data available — using in principle a push system — to national PIUs. It seems from the

wording of the proposal and the impact assessment ⁽¹⁾ that data could also be transmitted in bulk by airlines to intermediaries. Airlines are primarily active in a commercial environment, subject to national data protection legislation implementing Directive 95/46/EC ⁽²⁾. Questions on the applicable law will arise when data collected are used for law enforcement purposes ⁽³⁾.

43. Data would then be filtered by an intermediary (to be formatted and to exclude PNR data not included in the list of data required by the proposal) or sent directly to PIUs. Intermediaries could also be actors from the private sector, as is the case for SITA, operating in that sense in the framework of the PNR Agreement with Canada.

44. When it comes to PIUs, responsible for the risk assessment of the whole amount of data, it is not clear who will be responsible for the processing. Customs and border authorities might be involved, and not necessarily law enforcement authorities.

45. The subsequent transmission of filtered data to 'competent' authorities would probably happen in a law enforcement context. The proposal states that 'competent authorities shall only include authorities responsible for the prevention or combating of terrorist offences and organised crime'.

46. While moving forward through the steps of the processing, the actors involved and the purpose followed have a closer link with police and judicial cooperation in criminal matters. The proposal does not explicitly mention, however, when precisely the data protection framework decision will apply. The wording would even lead to think that it applies to the whole processing, and even to the airlines ⁽⁴⁾. However, the framework decision on the protection of personal data includes in itself some limitations.

⁽¹⁾ Article 6.3 of the proposal and Impact assessment, Annex A, 'Method of transmission of the data by the carriers'.

⁽²⁾ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

⁽³⁾ See in this respect the consequences of the PNR judgement. Judgement of the Court of 30 May 2006, European Parliament v Council (C-317/04) and Commission (C-318/04), Joined cases C-317/04 and C-318/04, ECR [2006], Point 56.

⁽⁴⁾ Article 11 of the proposal. See also recital 10 of the preamble: 'The Council Framework Decision on the Protection of Personal Data Processed in the Framework of Police and Judicial Cooperation in Criminal Matters (...) should be applicable to all the data processed in accordance with this Framework Decision. The rights of the data subjects in relation to such processing, such as the right to information, the right of access, the right of rectification, erasure and blocking, as well as the rights to compensation and judicial remedies should be those provided under that framework decision'.

47. In this context, the EDPS fundamentally questions the fact whether Title VI of the EU-Treaty can serve as a legal basis for legal obligations on a routine basis and for law enforcement purposes upon private sector actors. Additionally, the question is relevant whether Title VI of the EU-Treaty can serve as a legal basis for legal obligations on public authorities which are in principle outside the framework of law enforcement cooperation. These questions will be elaborated further on in this opinion.

Limitations of the data protection framework decision

48. The text of the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters contains at least two limitations which are relevant in terms of scope.
49. In the first place, the scope of the data protection framework decision is well defined in the framework decision itself: it applies 'only to data gathered or processed by competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties' ⁽¹⁾.
50. In the second place, the data protection framework decision is not supposed to apply to data processed purely at domestic level, but is limited to data exchanged between Member States and further transfer to third countries ⁽²⁾.
51. The data protection framework decision also includes some drawbacks compared to Directive 95/46/EC, in particular a wide exception to the purpose limitation principle. With regard to this purpose principle, the proposal clearly limits the purpose of the processing to the fight against terrorism and organised crime. However, the data protection framework decision allows processing for wider purposes. In such a case, the *lex specialis* (the proposal) should prevail over the *lex generalis* (the data protection framework decision) ⁽³⁾. This should be made explicit in the text of the proposal.
52. For this reason, the EDPS recommends adding the following provision to the proposal: 'Personal data transmitted by airlines according to this Framework Decision may not be processed for purposes other than the fight against terrorism and organised crime. The exceptions foreseen with regard to the purpose principle in the Council Framework Decision on the protection of

personal data processed in the framework of police and judicial cooperation in criminal matters do not apply'.

53. As a conclusion, the EDPS notes a serious lack of legal certainty with regard to the data protection regime applicable to the different actors involved in the project, and in particular to airlines and other first pillar actors: be it the rules of the proposal, the rules of the data protection framework decision or the national legislation implementing Directive 95/46/EC. The legislator should make clear at what moment of the processing precisely these different rules will apply.

Conditions of application of first and third pillar rules

54. The EDPS fundamentally questions the fact that a third pillar instrument creates legal obligations on a routine basis and for law enforcement purposes upon private or public sector actors which are in principle outside the framework of law enforcement cooperation.
55. A comparison could be made here with two other cases where the private sector was involved in the retention or transfer of data in a perspective of law enforcement:
- *The US-PNR case where a systematic transfer of PNR data by airlines to law enforcement authorities was foreseen.* The judgement of the Court of Justice in the PNR case excluded Community competence to conclude the PNR agreement. One of the justifications was that the transfer of PNR data to the US CBP constituted processing operations concerning public security and the activities of the State in areas of criminal law ⁽⁴⁾. In this case, the processing operation was a transfer to the CBP in a systematic fashion, which makes a difference with the following case:
 - *The general retention of data by electronic communication operators.* With regard to the Community competence to establish such a retention period, a difference can be made with the US-PNR case, considering that Directive 2006/24/EC ⁽⁵⁾ only foresees an obligation of retention, with data remaining under the control of the operators. No systematic transfer of data to law enforcement authorities is envisaged. It can be concluded that, as far as the data remain under the control of the service providers, those providers also remain responsible for the respect of personal data protection obligations vis-à-vis the data subject.

⁽¹⁾ Recital 5(a), version of 11 December 2007 of the data protection framework decision.

⁽²⁾ Article 1.

⁽³⁾ With regard to this point, the text of Article 27b of the latest draft of the Framework decision on data protection in the third pillar should be carefully considered and discussed.

⁽⁴⁾ Judgement of the Court of 30 May 2006, European Parliament v Council (C-317/04) and Commission (C-318/04), joined cases C-317/04 and C-318/04, ECR [2006], Point 56.

⁽⁵⁾ Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ L 105, 13.4.2006, p. 54).

56. In the present EU PNR proposal, airlines have to make available in a systematic way the PNR data of all passengers. However, these data are not transferred directly in bulk to law enforcement authorities: they can be sent to an intermediary and they are assessed by a third party, the statute of which remains unclear, before selected information is sent to competent authorities.

57. The main part of the processing happens in a grey zone, having material links with the first as well as with the third pillar. As it will be developed in Chapter IV, the quality of actors processing the data is not clear. Airlines are obviously no enforcement authorities, and intermediaries could be actors of the private sector. Even with regard to PIUs which would be public authorities, it must be stressed that not every public authority has the quality and the competences to perform law enforcement tasks on a routine basis.

58. Traditionally, a clear separation has existed between law enforcement and private sector activities, where law enforcement tasks are performed by specifically dedicated authorities, in particular police forces, and private actors are solicited on a case by case basis to communicate personal data to these enforcement authorities. There is now a trend to impose cooperation for law enforcement purposes on private actors on a systematic basis, which raises the question which data protection framework (first or third pillar) applies to the conditions of this cooperation: should the rules be based on the quality of the data controller (private sector) or on the purpose followed (law enforcement)?

59. The EDPS has already recalled the risk of a legal loophole between the first and third pillar activities ⁽¹⁾. It is indeed far from clear whether activities by private companies, in some way connected with enforcement of criminal law, are covered by the field of action of the European Union legislator under the Articles 30, 31 and 34 TEU.

60. If the general (first pillar) framework would not apply, a service provider should have to make difficult distinctions within his data bases. Under the current regime, it is clear that the data controller has to respect the same data protection vis-à-vis the data subjects irrespectively of the purposes that justify the retention of data. An outcome in which processing by service providers for different purposes would be subject to different frameworks for data protection should therefore be avoided.

⁽¹⁾ See the Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive (OJ C 255, 27.10.2007, p. 1). See also the Annual Report 2006, p. 47.

Exercise of data subject's rights

61. The different legal regimes that would apply at national level would have a major impact primarily on the exercise of his/her rights by the data subject.

62. It is stated in the preamble of the proposal that 'information, access, rectification, erasure and blocking, compensation and judicial remedies are to be provided under the data protection framework decision'. However, this statement does not answer the question of who the controller in charge of answering data subjects' requests is.

63. While information on the processing could be communicated by airlines, the issue is more complex when it comes to access or rectification of data. These rights are indeed restricted under the data protection framework decision. As stated above, it is doubtful that a service provider such as an airline could be obliged to give differentiated access and rectification rights to the data it holds, depending on the purpose (commercial or law enforcement) followed. One might argue that these rights are to be exercised before the PIU or the otherwise designated competent authorities. The proposal however gives no further indication in this respect, and as already mentioned, it is not clear either that these authorities (at least PIUs) will be law enforcement authorities normally entrusted with restricted (possibly indirect) access procedures.

64. The individual also risks being confronted with different recipients of data, as far as PIUs are concerned: the data are indeed transmitted to the PIU of the country of departure/arrival of flights, but also possibly to PIUs of other Member States on a case by case basis. Moreover, it is possible that several member States may establish or designate one single and common PIU. The data subject might in that case have to exercise redress before an authority of another Member State. Here again, it is not clear whether the national data protection rules will apply (these are supposed to be harmonised within the EU), or if specific law enforcement legislation will have to be taken into account (given the lack of comprehensive harmonisation in the third pillar at national level).

65. The question is the same with regard to access to data processed by intermediaries, the statute of which is unclear, and which could also be common to airlines in different countries of the EU.

66. The EDPS deplores the uncertainty that remains with regard to the exercise of these fundamental rights of the data subject. He stresses the fact that this situation is mostly due to the fact that actors who do not have law enforcement as a principal task are entrusted with such responsibilities.

Conclusion

67. The EDPS considers that the proposal should make clear what legal regime is applicable at which stage of the processing, and specify vis-à-vis which actor or authority access and redress shall be exercised. The EDPS recalls that according to Article 30.1. b) TEU, provisions on data protection should be appropriate and cover the full range of processing operations established by the proposal. A simple reference to the data protection framework decision is not sufficient, given the limited scope of that framework decision and the restriction of rights it contains. As far as law enforcement authorities are involved, the rules of the data protection framework decision should at least apply to the whole processing foreseen in the proposal, in order to guarantee the coherence of the application of data protection principles.

IV. QUALITY OF RECIPIENTS

68. The EDPS notes that the proposal does not provide for any specification with regard to the quality of the recipients of personal data collected by airlines, be it for intermediaries, Passenger Information Units, or competent authorities. It must be stressed that the quality of the recipient is in direct relation with the type of data protection guarantees applying to that recipient. The difference between guarantees provided in particular by first and third pillar rules has already been mentioned. It is essential that the applicable regime be clear for all actors involved, including national governments, law enforcement agencies, the data protection authorities, as well as data controllers and data subjects involved.

Intermediaries

69. No indication is given in the proposal with regard to the quality of intermediaries⁽¹⁾. The role of intermediaries as controllers or processors is not specified either. From experience, it seems that a private sector entity, be it a Computer Reservation System or another entity, could perfectly be entrusted with the task of gathering PNR data directly from the airlines to redirect them to PIUs. It is

indeed the way data are processed under the PNR Agreement with Canada. SITA⁽²⁾ is the company responsible for the processing of the information. The role of the intermediary is decisive, as it could be responsible for the filtering out/reformatting of data that are transmitted in bulk by airlines⁽³⁾. Even if intermediaries are obliged to cancel the processed information once it has been transferred to PIUs, the processing in itself is highly sensitive: a consequence of the intervention of intermediaries is the creation of an additional database including massive amounts of data, and even, according to the proposal, sensitive data (intermediaries being obliged then to delete those sensitive data). For these reasons, the EDPS recommends that no intermediaries should be involved in the processing of passenger data, unless their quality and tasks are strictly specified.

Passenger information units

70. PIUs have a decisive role in identifying persons that are or may be involved or associated with terrorism or organised crime. According to the proposal, they will be responsible for creating risk indicators and providing intelligence on travel patterns⁽⁴⁾. Where the risk assessment is based on standardised travel patterns and not on material evidence linked with a concrete case, the analysis can be considered as constituting proactive investigation. The EDPS stresses that this kind of processing is in principle strictly regulated in Member State legislation (if not prohibited), and it is the task of specific public authorities the functioning of which is also strictly regulated.
71. PIUs are therefore entrusted with very sensitive processing of information, without the proposal giving any detail on their quality and the conditions in which they would exercise this competence. Although it is likely that this task will be performed by a governmental body, possibly customs or border control, the proposal does not explicitly prevent Member States to entrust intelligence agencies or even any kind of processor with its performance. The EDPS underlines the fact that the transparency and guarantees applying to intelligence agencies are not always identical to those applicable to traditional law enforcement authorities. Details on the quality of PIUs are decisive, as this will have direct consequences on the applicable legal framework and the conditions of supervision. The EDPS considers that the proposal must include an additional provision detailing the specificities of PIUs.

⁽²⁾ SITA was created in 1949 by 11 member airlines. Value-added solutions are provided to air transport industry through the commercial company SITA INC (Information, Networking Computing) and network services through SITA SC on a co-operative basis.

⁽³⁾ Impact assessment, Annex A, 'Method of transmission of the data by the carriers'.

⁽⁴⁾ Article 3 of the proposal.

⁽¹⁾ Article 6 of the proposal.

Competent authorities

72. It appears from Article 4 of the proposal that any authority responsible for the prevention or combating of terrorist offences and organised crime can receive the data. While the purpose is clearly defined, the quality of the authority is missing. The proposal does not foresee any limitation of recipients to law enforcement authorities.

As mentioned above with regard to PIUs, it is decisive that the sensitive information at stake be processed in an environment with a clear legal framework. This is much more the case, e.g., for law enforcement authorities than for intelligence agencies. Considering the data mining elements and the proactive research included in the proposal, it cannot be excluded that such intelligence agencies be involved in the processing of the data, without exclusion of any other type of authorities.

Conclusion

73. As a general comment, the EDPS notes that the enforcement of an EU PNR system is rendered even more difficult considering that law enforcement authorities have different competences depending on the national law of the Member States, including or not intelligence, tax, immigration or police. This is however a supplementary reason to recommend that the proposal be much more precise with regard to the quality of the mentioned actors and the guarantees to control the performance of their tasks. Additional provisions should be integrated in the proposal, to specify strictly the competences and the legal obligations of intermediaries, PIUs and other competent authorities.

V. CONDITIONS OF TRANSFER TO THIRD COUNTRIES

74. The proposal provides for some safeguards in relation to the transfer of PNR data to third countries⁽¹⁾. In particular, it foresees explicitly the application of the data protection framework decision to data transfers, it provides for a specific purpose limitation and it states the need for consent of the Member State in case of onward transfer. The transfer should also comply with national legislation of the Member State concerned, as well as any applicable international agreement.
75. Many questions remain however, in particular with regard to the quality of consent, the conditions of application of the data protection framework decision and the question of 'reciprocity' in the transmission of data to third countries.

Quality of consent

76. The Member State of origin must give express consent for onward transfer of data from a third country to another third country. The proposal does not specify under what conditions and by whom this consent will be given, and whether national DPAs should be involved in the decision. The EDPS considers that the way consent will be given should at least be in conformity with national laws stating conditions of transfer of personal data to third countries.
77. Besides, consent of a Member State should not prevail over the principle according to which an adequate level of protection must be foreseen by the recipient country for the intended processing. These conditions should be cumulative, as they are in the data protection framework decision (Article 14). The EDPS therefore suggests adding a point (c) to paragraph 1 of Article 8 that would read 'and (c) the third State ensures an adequate level of protection for the intended data processing.' The EDPS recalls in this respect that mechanisms ensuring common standards and coordinated decisions with regard to adequacy must be put in place⁽²⁾.

Application of the data protection framework decision

78. The proposal refers to the conditions and safeguards contained in the data protection framework decision while also specifying explicitly some conditions, in particular the above mentioned consent of the Member State concerned, and a limitation of the purpose to preventing and fighting terrorist offences and organised crime.
79. The data protection framework decision itself provides for conditions to the transfer of personal data to third countries, namely with regard to the purpose limitation, the quality of recipients, the consent of Member State, and the adequacy principle. However, it also foresees derogations to these conditions of transfer: legitimate prevailing interests, especially important public interests, can be a sufficient basis for transfer even if the conditions listed above are not fulfilled.
80. As already mentioned in Chapter III of this opinion, the EDPS considers that it must be stated clearly in the text of the proposal that the more precise guarantees of the proposal prevail over the general conditions — and exceptions — of the data protection framework decision, where it applies.

⁽¹⁾ Article 8 of the proposal.

⁽²⁾ Opinion of the EDPS of 26 June 2007 on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters, points 27 to 30 (OJ C 139, 23.6.2007, p. 1).

Reciprocity*Countries having a bilateral agreement with the EU*

81. The proposal addresses the issue of possible 'retaliation requests' of countries that might ask the EU for PNR data for flights from the EU to their territory. Where the EU requests data from databases of airlines of such third countries, because they operate a flight to or from the EU, such third country could ask the same from airlines based in the EU, including data from citizens of the EU. Although the Commission considers this eventuality as 'very remote', it allows for it. The proposal refers in this regard to the fact that the agreement with the US and with Canada foresee such reciprocal treatment 'which may be enforced automatically' ⁽¹⁾. The EDPS questions the significance of such an automatic reciprocity and the application of safeguards to such transfers, notably taking into account the existence of an adequate level of protection of the country concerned.
82. A distinction should be made between third countries which have already concluded an agreement with the EU, and those countries which do not have such agreement.

Countries having no agreement with the EU

83. The EDPS notes that reciprocity might lead to transfer personal data to countries where no guarantees can be provided in terms of democratic standards and adequate level of data protection.
84. The impact assessment gives further elements with regard to the conditions of transfer of data to third countries: the advantage of the EU-PNR system, where data are filtered by PIUs, is emphasised. Only selected data of suspected individuals (and not bulk data) would be transferred to the competent authorities of Member States and presumably to third countries as well ⁽²⁾. The EDPS recommends clarifying this point in the text of the proposal. A simple statement in the impact assessment does not provide for the necessary protection.
85. While the selection of data would contribute to minimise the impact on the privacy of passengers, it must be recalled that data protection principles go far beyond data minimisation, and include principles such as necessity, transparency and exercise of data subject rights, all principles to be taken into account when determining whether a third country provides for an adequate level of protection.

86. The impact assessment indicates that such processing will provide the EU with the ability 'to insist on certain standards and to ensure consistency in such bilateral agreements with third countries. It will also provide for the possibility of requesting reciprocal treatment from third countries with which the EU has an agreement, something that is not possible today' ⁽³⁾.
87. From these observations arises the question of the impact of the proposal on the existing agreements with Canada and the USA. The conditions of access to data in these agreements are indeed much broader, as they are not subject to a similar selection before being transferred to those third countries.
88. The impact assessment indicates that 'in cases in which the EU has an international agreement with a third country for the exchange/transmission of PNR data to such third country, such agreements shall be duly taken into account. The carriers should send the PNR data to the Passengers Information Units according to the normal practice under the current measure. The PIU which receives such data shall transmit them to the competent authority of the third country with which such an agreement exists' ⁽⁴⁾.
89. While on the one hand, the proposal seems to aim at a transfer of *only selected* data to any competent authority, be it within the EU or outside, on the other hand, the impact assessment, the preamble of the proposal (recital 21) and Article 11 itself recall that existing agreements should be duly taken into account. This might lead to the conclusion that filtering may only be a valid measure for agreements to be concluded in the future. It could be foreseen in this perspective that bulk access will still be the rule for access e.g. by US authorities to PNR data, in conformity with the provisions of the EU-US agreement, but that in parallel and on a case by case basis, a transfer of data to the US could occur, relating to specific data identified by PIUs, including but not limited to data concerning flights to the US.
90. The EDPS regrets the lack of clarity on this decisive point of the proposal. He considers of the utmost importance that the conditions of transfer of PNR data to third countries be coherent and subject to a harmonised level of protection. Besides, for reasons of legal certainty, precautions with regard to the guarantees applying to the transfer of data should be included in the proposal itself and not only in the impact assessment, as it is the case now.

⁽¹⁾ Explanatory Memorandum of the proposal, Chapter 2.

⁽²⁾ Impact assessment, Chapter 5.2., 'Protection of privacy'.

⁽³⁾ Impact assessment, Chapter 5.2., 'Relations with third countries'.

⁽⁴⁾ Impact assessment, Annex A, 'Bodies receiving data from the Passenger Information Units'.

VI. OTHER SUBSTANTIVE POINTS

Automated processing

91. The EDPS notes that the proposal explicitly excludes that enforcement actions be taken by the Passenger Information Units and the competent authorities of the Member States only by reason of the automated processing of PNR data or by reason of a person's race or ethnic origin, religious or philosophical belief, political opinion or sexual orientation ⁽¹⁾.
92. Such precision is welcome as it limits the risks of arbitrary measures against individuals. The EDPS however notes that its scope is limited to *enforcement actions* by PIUs or competent authorities. It does not exclude, in its present wording, the automated filtering of individuals according to standard profiles, nor does it prevent the automated constitution of lists of suspected persons and the taking of measures such as extended surveillance, as long as these measures are not considered as enforcement actions.
93. The EDPS considers that the notion of *enforcement actions* is too vague, and that, as a principle, *no decision* should be taken with regard to individuals *only* by reason of the automated processing of their data ⁽²⁾. The EDPS recommends modifying the text accordingly.

Quality of data

94. The proposal gives in Article 5.2 an important precision as it makes clear that no obligation is put on airlines to collect or retain additional data to those collected for the initial commercial purpose.
95. Several aspects of the processing of these data still deserve further comment:
 - The data to be made available, as listed in Annex 1 of the proposal, are very extensive, and the list is similar to the list of data available to US authorities in the EU-US agreement. The quality of some of the data requested has already been questioned at several occasions by Data Protection Authorities, and especially by the Article 29 Working Party ⁽³⁾.

⁽¹⁾ Recital 20 and Article 3.3 and 3.5 of the proposal.

⁽²⁾ See in this respect Article 15.1 of Directive 95/46/EC. The Directive prohibits such automated decisions in cases where the individual would be affected by the decision. With regard to the context of the proposal, decisions in a law enforcement framework are likely to affect severely the data subjects in any case. Also the fact of being subject to secondary checks can affect the data subject, especially if these actions are taken repeatedly.

⁽³⁾ See in particular Opinion No 5/2007 of 17 August 2007 on the follow-up agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security concluded in July 2007, WP 138.

— It seems from the wording of the impact assessment ⁽⁴⁾ and Article 6.3 of the proposal that data could also be transmitted in bulk by airlines to intermediaries. In a first stage, data transmitted to a third party would not even be limited in compliance with the PNR data listed in Annex 1 of the proposal.

— With regard to the processing of sensitive data, even if these data might be filtered out at the stage of intermediaries, the question still remains whether the transfer of the open field by airlines is strictly necessary.

The EDPS supports the points made in the WP29-opinion in this respect.

Method of transfer of PNR data

96. Air carriers established outside the EU are required to *push* data to PIUs or intermediaries as long as they possess the technical architecture to do it. If this is not the case they will have to permit the extraction of data through the *pull* method.
97. Allowing for different methods of communication of data depending on the airlines concerned will only raise more difficulties with regard to the control of the compliance of transfer of PNR data with data protection rules. This risks as well to distort competition between EU and non-EU airlines.
98. The EDPS recalls that the push method, allowing airlines to keep control on the quality of data transferred and the circumstances of transfers, is the only admissible method with regard to the proportionality of the processing. Besides, it must consist of an effective push, that is, the data should not be sent in bulk to an intermediary but filtered at the very first step of the processing. It is not admissible that non necessary data — and data not included in Annex 1 of the proposal — be sent to a third party, even if those data are to be deleted immediately by this third party.

Data retention

99. Article 9 of the proposal foresees a 5 years retention period of PNR data, with an additional 8 years period where data are to be kept in a 'dormant' database that will be accessible in restricted conditions.

⁽⁴⁾ Impact assessment, Annex A, 'Method of transmission of the data by the carriers'.

100. The EDPS questions the difference between the two types of data bases: it is questionable whether the dormant database constitutes a real archive, with different methods of storage and retrieval of data. Indeed, most of the conditions put to the access to the dormant database consist of security requirements that could be applicable to the 'five years retention database' as well.

101. The total duration of storage — that is 13 years — is in any case excessive. It is justified in the impact assessment by the need to develop risk indicators and establish patterns of travel and behaviour ⁽¹⁾, the efficiency of which deserves further demonstration. While it is obvious that data can be retained as long as necessary in a specific case as far as an investigation is ongoing, no justification can support the retention of data of all passengers in total absence of suspicion for 13 years.

102. The EDPS further notes that this retention period is not supported by the answers of Member States to the questionnaire of the Commission, according to which the average duration of storage required would be 3,5 years ⁽²⁾.

103. Moreover, the period of 13 years is comparable to the retention period of 15 years in the most recent agreement with the United States. The EDPS has always understood that this long retention period was only agreed upon because of strong pressure by the US Government to have a much longer period than 3.5 years, not because it was in any stage defended by the Council or the Commission. There is no reason to transpose such a compromise — that only has been justified as a necessary result of negotiations — to a legal instrument within the EU itself.

Role of the Committee of Member States

104. The Committee of Member States established under Article 14 of the proposal will be competent with regard to security issues including protocol and encryption of PNR data, but also with regard to guidance for common general criteria, methods and practices related to risk assessment.

105. Apart from these indications, the proposal does not include any element or criteria with regard to the concrete conditions and framework of the risk assessment process. The impact assessment mentions that the criteria will ultimately depend on intelligence held by each Member State,

which is constantly evolving. The risk assessment is to be performed in absence of uniform standards of identification of suspects. The extent to which the Committee of Member States will be able to play a role in this regard thus appears questionable.

Security

106. The proposal details a series of security measures ⁽³⁾ to be taken by PIUs, intermediaries and other competent authorities in order to protect the data. Considering the importance of the data base and the sensitivity of the processing, the EDPS considers that in addition to the measures envisaged, the entity processing the data should also be obliged to officially notify any security breach.

107. The EDPS is aware of the project to establish such a notification procedure in the sector of electronic communications at European level. He advises to include such safeguard in the present proposal, and refers in this respect to the security breach system put in place in the United States with regard to state agencies ⁽⁴⁾. Security incidents can indeed happen in any field of activity, and in the private as well as the public sector, as the recent loss of a whole citizens' database by the British administration has shown ⁽⁵⁾. Large scale databases such as the one envisaged in the proposal would be first on a priority list to benefit from such an alert system.

Review and Sunset Clause

108. The EDPS notes that a review is to take place within three years of the entry into force of the framework decision, on the basis of a report prepared by the Commission. He acknowledges the fact that this review, based on information provided by Member States, will give specific attention to data protection safeguards, and include the implementation of the 'push' method, the data retention and the quality of the risk assessment. Such review should, to be comprehensive, include the results of an analysis of the statistical data produced on the basis of the processing of PNR information. These statistics should, in addition to the elements mentioned in Article 18 of the proposal, include statistical details on the identification of high risk persons, such as the criteria for such identification and the concrete results of any law enforcement action resulting of the identification.

⁽³⁾ Article 12 of the proposal.

⁽⁴⁾ See in particular the works of the American 'Identity Theft Task Force':
<http://www.idtheft.gov/>

⁽⁵⁾ See the link to the British HM Revenue and Customs website:
<http://www.hmrc.gov.uk/childbenefit/update-faqs.htm>
See also:
http://news.bbc.co.uk/1/hi/uk_politics/7103566.stm

⁽¹⁾ Impact assessment, Annex A, 'Data retention period'.

⁽²⁾ Impact assessment, annex B.

109. The EDPS has already insisted in this opinion on the absence of concrete elements to establish the necessity of the system proposed. He considers however that, should the framework decision enter into force, it should as a minimum be complemented by a sunset clause. At the end of the three years period, the Framework Decision should be repealed in case no element would come to support its continuation.

Impact on other legal instruments

110. In its final provisions the proposal puts a condition to the further application of already existing bilateral or multilateral agreements or arrangements. Those instruments can only be applied as far as they are compatible with the objectives of the proposed framework decision.

111. The EDPS questions the scope of this provision. As already mentioned in Chapter V under Reciprocity, it is not clear what the impact of this provision will be on the content of agreements with third countries, such as the agreement with the US. In a different perspective, it is not clear either whether the provision could have an impact on the conditions of application of instruments with a broader scope, such as Council of Europe Convention No 108. Although this might appear unlikely in view of the difference of institutional context and actors involved, any risk of misinterpretation should be avoided and the proposal should make clear that it does not have any impact on instruments with a broader scope, notably those having as object the protection of fundamental rights.

VII. CONCLUSION

112. The EDPS stresses the major impact in terms of data protection of the present proposal. He has concentrated his analysis on four fundamental issues raised by the proposal, and insists on the fact that the issues raised need to be addressed in a comprehensive manner. Under the present circumstances, the proposal is not in conformity with fundamental rights, notably Article 8 of the Charter of the Fundamental Rights of the Union, and should not be adopted.

113. Should the comments above be complied with, especially the legitimacy test, some drafting proposals have been made in the present opinion that should be taken into account by the legislator. Reference is made in particular to points 67, 73, 77, 80, 90, 93, 106, 109 and 111 of the opinion.

Legitimacy of the proposed measures

114. While the general purpose to fight against terrorism and organised crime is in itself clear and legitimate, the core of the processing to be put in place is not sufficiently circumscribed and justified.

115. The EDPS considers that techniques consisting of assessing the risk presented by individuals using data mining tools and behavioural patterns need to be further assessed, and their utility be clearly established in the framework of the fight against terrorism, before they are used on such a wide scale.

116. Building upon different data bases without a global view on the concrete results and shortcomings:

- Is contrary to a rational legislative policy in which new instruments must not be adopted before existing instruments have been fully implemented and proved to be insufficient.

- Might otherwise lead to a move towards a total surveillance society.

117. The fight against terrorism can certainly be a legitimate ground to apply exceptions to the fundamental rights to privacy and data protection. However, to be valid, the necessity of the intrusion must be supported by clear and undeniable elements, and the proportionality of the processing must be demonstrated. This is all the more required in case of extensive intrusion in the privacy of individuals, as foreseen in the proposal.

118. These elements of justification are missing in the proposal and the necessity and proportionality tests are not fulfilled.

119. The EDPS insists on the essential character of the necessity and proportionality tests developed above. They represent a *condicio sine qua non* to the entry into force of the proposal.

Applicable legal framework

120. The EDPS notes a serious lack of legal certainty as to the regime applicable to the different actors involved in the project, and in particular to airlines and other first pillar actors: be it the rules of the proposal, the rules of the data protection framework decision or the national legislation implementing Directive 95/46/EC. The legislator should make clear at what stages of the processing these different rules will apply.

121. The present trend to impose cooperation for law enforcement purposes on private actors on a systematic basis raises the question which data protection framework (first or third pillar) applies to the conditions of this cooperation: it is not clear whether the rules should be based on the quality of the data controller (private sector) or on the purpose followed (law enforcement).

122. The EDPS has already stressed the risk of a legal loophole between the first and third pillar activities ⁽¹⁾. It is indeed far from clear whether activities by private companies, in some way connected with enforcement of criminal law, are covered by the field of action of the European Union legislator under the Articles 30, 31 and 34 TEU.
123. An outcome in which processing by service providers for different purposes would be subject to different frameworks for data protection should be avoided, especially considering the difficulties this would create in terms of exercise of rights by data subjects.

Quality of recipients

124. The proposal should provide for a specification with regard to the quality of the recipients of personal data collected by airlines, be it for intermediaries, Passenger Information Units, or competent authorities.
125. The quality of the recipient, that could in some cases be private sector actors, is in direct relation with the type of data protection guarantees applying to that recipient. It is essential that the applicable regime be clear for all actors involved, including the legislator, the data protection authorities, as well as data controllers and data subjects involved.

Transfer of data to third countries

126. The EDPS stresses the need to ensure that an adequate level of protection is provided in the recipient country. He also questions the significance of the 'reciprocity' principle mentioned in the proposal, and its application to countries already bound by an agreement with the EU, like Canada or the US. He considers it to be of the utmost importance that the conditions of transfer of PNR data to third countries be coherent and subject to a harmonised level of protection.

Other substantive points

127. The EDPS also draws the attention of the legislator to specific aspects of the proposal that need more precision

or a better taking into account of data protection principle. This is the case in particular with regard the following aspects:

- the conditions in which automated decisions can be taken should be restricted,
- the quantity of data processed should be reduced,
- the method of transfer of data should solely rely on *push*,
- the data retention period is considered as excessive and not justified,
- the role of the committee of Member States could be more precise with regard to its guidance on 'risk assessment',
- the security measures should include a 'security breach notification' procedure,
- the review of the decision should include a sunset clause,
- the proposal should make clear that it does not have any impact on instruments with a broader scope having namely as object the protection of fundamental rights.

Final observations

128. The EDPS notes that the present proposal is made at a moment when the institutional context of the European Union is about to change fundamentally. The consequences of the Lisbon Treaty in terms of decision making will be fundamental, especially with regard to the role of the Parliament.
129. Considering the unprecedented impact of the proposal in terms of fundamental rights, the EDPS advises not to adopt it under the present Treaty Framework, but to ensure it follows the co-decision procedure foreseen by the new Treaty. This would strengthen the legal grounds on which the decisive measures envisaged in the proposal would be taken.

⁽¹⁾ See the Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive (OJ C 255, 27.10.2007, p. 1). See also Annual Report 2006, p. 47.

EUROPEAN DATA PROTECTION SUPERVISOR

Opinion of the European Data Protection Supervisor on the Proposal for a Decision of the European Parliament and of the Council establishing a multiannual Community programme on protecting children using the Internet and other communication technologies

(2009/C 2/02)

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty establishing the European Community, and in particular its Article 286,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular its Article 8,

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ⁽¹⁾,

Having regard to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data ⁽²⁾, and in particular its Article 41,

Having regard to the request for an opinion in accordance with Article 28(2) of Regulation (EC) No 45/2001 received on 4 March 2008 from the European Commission,

HAS ADOPTED THE FOLLOWING OPINION:

I. INTRODUCTION

Consultation of the EDPS

1. The Proposal for a Decision of the European Parliament and of the Council establishing a multiannual Community programme on protecting children using the Internet and other communication technologies (hereinafter 'the proposal') was sent by the Commission to the EDPS for consultation on 4 March 2008, in accordance with Article 28(2) of Regulation (EC) No 45/2001. This consultation should be explicitly mentioned in the preamble of the decision.

⁽¹⁾ OJ L 281, 23.11.1995, p. 31.

⁽²⁾ OJ L 8, 12.1.2001, p. 1.

The proposal in its context

2. The new multiannual programme (hereinafter 'the programme') is presented in the continuity of the Safer Internet (1999-2004) and the Safer Internet Plus programmes (2005-2008).
3. Four orientations are defined:
 - reducing illegal content and tackling harmful conduct online,
 - promoting a safer online environment,
 - ensuring public awareness,
 - establishing a knowledge database.
4. The programme is presented as consistent and complementary to relevant Community policies, programmes and actions. Considering the number of existing regulatory measures in the field of the protection of children in the context of new technologies, this programme concentrates on action rather than regulation. Focus is put on the efficiency and effectiveness of initiatives to be taken, and adaptation to the evolution of new technologies. In this perspective, it foresees enhanced exchanges of information and best practices.
5. As a framework instrument, the programme does not go into the details of the actions to be taken, but allows for calls for proposals and calls for tenders in line with the four orientations defined.

Focus of the opinion

6. The general orientations of the programme address the protection of children using the Internet and other communication technologies without putting emphasis on the privacy aspects of the issue ⁽³⁾. While being totally supportive of the objective of the proposal, the EDPS will in this opinion highlight these privacy aspects.

⁽³⁾ Some references to privacy can be found in the Impact Assessment (3.2. Specific risks: disclosure of personal information; 3.3. Target groups; 5.2. Analysis of the impact of the policy options) but they are not significantly developed.

7. The EDPS considers as essential that the initiatives planned be consistent with the existing legal framework as cited in the proposal ⁽¹⁾, and in particular Directive 2000/31/EC on e-commerce, Directive 2002/58/EC on e-privacy, and Directive 95/46/EC on data protection ⁽²⁾.
8. The protection of personal data should be taken into account with regard to different aspects and different actors involved in the programme: the protection of personal data of children is of course the main issue, but not the only one: personal data related to persons and contents under scrutiny for the purpose of protecting children should also be taken into consideration.
9. These issues will be developed as follows in this opinion:
 - Chapter II will develop the link between data protection and the safety of children, highlighting the fact that the protection of children's data is an indispensable step towards more safety and prevention of abuse,
 - in Chapter III, the opinion will stress the fact that processing of personal data is also inherent to the reporting, filtering or blocking of suspicious contents or persons on the Internet:
 - in a first point, the question of the reporting of suspected persons or facts will be analysed in a data protection perspective,
 - the second point will focus on the role of technical tools,
 - the responsibility of the industry, in relation with their control on users' data and on content data will be the subject of the last point.
10. The EDPS fully supports the objective of the programme and the orientations defined in order to enhance the protection of children online. In particular, reducing illegal or harmful content and raising awareness of children and other actors involved are decisive measures which should be further developed.
11. The EDPS wishes to recall that an appropriate protection of the personal information of the child is an essential preliminary step to ensure safety while being online. This interconnection between privacy and security of children is explicit in the recent Declaration of the Committee of Ministers 'on protecting the dignity, security and privacy of children using the Internet' ⁽³⁾. The declaration recalls the right of children to dignity, special protection and care as is necessary for their well being, 'to protection against all forms of discrimination or arbitrary or unlawful interference with their privacy and to unlawful attacks on their honour and reputation'.
12. As examples of risks associated with the protection of the privacy of children, the declaration cites the traceability of children's activities that may expose them to criminal activities, such as solicitation for sexual purposes or other illegal activities. Profiling and retention of personal data regarding children's activities are also presented as leading to a potential risk of misuse, e.g. for commercial purposes, or for searches by educational establishments or prospective employers. The declaration therefore calls for removal or deletion in a reasonably short period of time of content and traces left by children online, and for the development and promotion of information to children, especially on the competent use of tools providing access to information, the development of critical analysis of content and the appropriation of adequate communication skills.
13. The EDPS supports these findings. In particular, he considers as essential to raise the awareness of the child as to the risks linked with a spontaneous communication of personal details such as real name, age or place of residence.
14. Point 3 of the measures ⁽⁴⁾ proposed by the multiannual programme is specifically dedicated to 'Ensuring public awareness', through actions directed to children, parents, carers and educators, as to opportunities and risks related to the use of online technologies and 'means of staying safe online'. Among the means indicated in the proposal, the dissemination of appropriate information and the provision of contact points where parents and children can receive answers to questions about how to stay safe online, are two useful tools that should integrate explicitly this dimension of the protection of the child's personal data.
15. The EDPS wishes to stress that data protection authorities are relevant interlocutors in this context. They should be mentioned as such in the proposal, especially where it foresees the promotion of cooperation and sharing of information, experience and good practice at national and European level ⁽⁵⁾.

II. PROTECTION OF PERSONAL DATA AND SAFETY OF CHILDREN

⁽¹⁾ Explanatory Memorandum, 2.1. The legislative context; Summary of the Impact Assessment, 1.2. State of play: legislation.

⁽²⁾ — Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (OJ L 178, 17.7.2000, p. 1).

— Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

— Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

⁽³⁾ Declaration adopted by the Council of Ministers on 20 February 2008 at the 1018th meeting of the Ministers' Deputies, available at: [wcd.coe.int/ViewDoc.jsp?Ref=Decl\(20.02.2008\)&Ver=0001](http://wcd.coe.int/ViewDoc.jsp?Ref=Decl(20.02.2008)&Ver=0001)

⁽⁴⁾ Annex 1, Actions, point 3.

⁽⁵⁾ Annex 1, Actions, point 1.

16. Several initiatives can be mentioned as an illustration of recent actions taken in this perspective in Member States or Members of the EEA. The Swedish DPA is conducting a yearly survey on young peoples' attitudes towards internet and surveillance, just like the DPA of the United Kingdom ⁽¹⁾ which conducted a survey directed to 2 000 children between 14 and 21 years old. In January 2007, together with the Ministry of Education, the Norwegian DPA has launched an education campaign directed at schools ⁽²⁾. In Portugal, a protocol has been signed between the DPA and the Ministry of Education, to promote a data protection culture on the Internet and especially on social networks ⁽³⁾. Following this project, Portuguese social networks have integrated an interface and a mascot dedicated to children between 10 and 15 years old.
17. These examples illustrate the active and decisive role played by data protection actors when it comes to the protection of children online, and the need to include them explicitly as interlocutors in the multiannual programme.

III. PROTECTION OF PERSONAL DATA AND RIGHTS OF OTHER STAKEHOLDERS

I. Reporting and exchange of information

18. The first point of the proposal ('Reducing illegal content and tackling harmful conduct online' ⁽⁴⁾) includes as one of its main actions the provision of contact points for reporting online illegal content and harmful conduct. It is not questionable that to be fought efficiently, illegal content or harmful conduct must be brought to the attention of the competent authorities. Contact points have actually already been established in relation with the protection of children but also, e.g. for the fight against spam ⁽⁵⁾.
19. The EDPS notes nevertheless that the notion of harmful content remains unclear: no indication is given on who is responsible for defining what harmful content is, and according to what criteria. This is all the more worrying considering the implications of a possible reporting of such content.
20. In addition, as already mentioned above, in the framework of a programme like the present one not only personal data of children are at stake, but also personal data of all persons who are connected in some way with the information circulating on the network. It can be, for instance, the person suspected of misbehaviour and reported as suspect, but also the person reporting a suspicious conduct or content, or the victim of the abuse. While this information

is necessary to an efficient reporting system, the EDPS considers it important to recall that it should always be processed in accordance with data protection principles.

21. Some data at stake might even need specific protection, if they can be considered as sensitive data in the sense of Article 8 of Directive 95/46/EC. This can be the case for data related to authors of infringements as well as victims of abuse, especially when it comes to child pornography. It must be noted that at national level, some systems of reporting have required modification of the data protection legislation in order to enable the processing of judicial data of suspected offenders or victims ⁽⁶⁾. The EDPS insists on the fact that any reporting system to be put in place takes into account the existing data protection framework. The demonstration of a public interest, as well as guarantees related to the supervision of the system, in principle by law enforcement authorities, are decisive elements to comply with this framework.

II. The role of technical tools in a privacy perspective

22. The use of technical tools is promoted as one of the solutions to deal with illegal content and harmful conduct ⁽⁷⁾. Examples of such tools are given in the impact assessment ⁽⁸⁾, including age recognition, face recognition (for victim identification by law enforcement authorities) or filtering technologies. According to the proposal these tools should be better adapted to practical needs and accessible to relevant stakeholders.
23. The EDPS has already taken a clear position ⁽⁹⁾ in favour of the use of new technologies to enhance the protection of the rights of individuals. He considers that the principle of 'privacy by design' should constitute an inherent part of technological development which implies the processing of personal data. The EDPS therefore strongly encourages the development of projects aiming at developing technologies in that sense.
24. It is especially important to develop systems that will reduce as much as possible the exposure of children's personal data providing them a reliable protection and to offer them accordingly the opportunity to use new tools of the Information Society like social networks in a safer way.

⁽¹⁾ See 'www.ico.gov.uk/youngpeople'.

⁽²⁾ See 'www.dubestemmer.no'.

⁽³⁾ See 'dadus.cnpd.pt/'.

⁽⁴⁾ Annex 1 of the proposal.

⁽⁵⁾ See e.g. the website put in place by the Belgian authorities for these purposes: www.ecops.be

⁽⁶⁾ See the Belgian Law on Data Protection of 8 December 1992, Article 3(6) related to the processing of data by the Centre for the reporting of missing or sexually abused children.

⁽⁷⁾ Annex 1, Actions, point 1.

⁽⁸⁾ Impact assessment, point 3.1.

⁽⁹⁾ 2006 EDPS annual report part 3.5.1 Technological developments.

25. It should nevertheless be recalled that, depending on the way they are used, technological tools can have a variety of impacts on individuals. If they are used in order to filter or to block information, they can stop the access by children to content that could be potentially damaging, but they can also prevent someone to get access to legitimate information.
26. Even if the major concern here relates to freedom of access to information, there is still a consequence in a privacy perspective. Indeed, filtering, especially in its most recent developments using identity management, can function on the basis of given criteria, including personal data such as the age of the individual connected to the network (to prevent access by adults or children to specified content), the content of the information and traffic data linked with the identity of the author of the information. Depending on the way this personal information will — automatically — be processed, the individuals concerned could face consequences with regard to their right to communicate online.
27. The use of filtering or blocking tools to control the access to networks must therefore be used in a cautious way, taking into account their possible adverse effects and taking full profit of the privacy enhancing opportunities offered by the technology.
28. The EDPS welcomes the precision given in the impact assessment ⁽¹⁾ according to which none of the proposed options should affect the rights to privacy and freedom of expression. He also shares the view expressed therein that one of the main objectives is user empowerment, i.e. 'empowerment for making better choices and taking appropriate actions' to protect children ⁽²⁾.
- III. *The responsibility of service providers*
29. The collaboration of all stakeholders is considered in the proposal as a necessary element to enhance the protection of children using communication technologies. Among these stakeholders, the proposal ⁽³⁾ foresees the participation and the involvement of the industry especially through self-regulation.
30. Being responsible for the provision of telecommunication and content services, the industry in this sector could have some influence on the reporting, filtering or blocking of information when it is considered as illegal or harmful. The extent to which it can actually be entrusted with such a task, in a legal perspective, could nevertheless lead to discussion.
31. The collaboration of the industry in the perspective of raising the awareness of children and other actors concerned, like parents or educators, is of course welcome. Putting in place alert systems and moderators on websites allowing for the exclusion of inappropriate content, is also an essential aspect of the responsibility of content providers.
32. As far as *telecommunication* service providers are concerned, the monitoring of telecommunications is however a debatable question, either aimed at the control of content protected by intellectual property rights or other illegal content. The issue raises the question of the intervention of a commercial actor, offering a specific (telecommunication) service, in a sphere where it is in principle not supposed to intervene, that is, the control of the content of the telecommunications. The EDPS recalls that such control should in principle not be done by service providers, and certainly not in a systematic way. When it is necessary in specific circumstances, it should in principle be the task of law enforcement authorities.
33. In its opinion of 18 January 2005, the Article 29 Working Party has recalled in relation with this issue ⁽⁴⁾ that 'no systematic obligation of surveillance and collaboration can be imposed on ISPs, pursuant to Article 15 of Directive 2000/31/EC on electronic commerce. (...) As stated in Article 8 of the Data protection Directive, processing of data related to offences, criminal convictions or security measures can be processed only under strict conditions as implemented by Member States. While any individual obviously has the right to process judicial data in the process of his/her own litigation, the principle does not go as far as permitting in depth investigation, collection and centralisation of personal data by third parties, including in particular, systematic research on a general scale such as the scanning of the Internet (...). Such investigation falls within the competence of judicial authorities'.
34. In an area where freedom of speech, access to information, privacy and other fundamental rights are at stake, this intervention of private actors raises the question of the proportionality of the means used. The European Parliament has recently adopted a resolution stressing the need for a solution in compliance with the fundamental rights of individuals ⁽⁵⁾. In point 23 of its resolution, it states that 'the Internet is a vast platform for cultural expression, access to knowledge, and democratic participation in European creativity, bringing generations together through the information society; [the Parliament] calls on the Commission and the Member States, to avoid adopting measures conflicting with civil liberties and human rights and with the principles of proportionality, effectiveness and dissuasiveness, such as the interruption of Internet access'.

⁽¹⁾ Impact assessment, point 5.2.

⁽²⁾ In that sense, filters would be meant to be initialised by parents, and could be de-activated, so that the adult remains in full control of the filtering effect.

⁽³⁾ Recital 8 of the preamble; Annex 1, point 1.4; Summary of the impact assessment, point 3.1.

⁽⁴⁾ Working document of the Article 29 Working Party on data protection issues related to intellectual property rights, WP 104.

⁽⁵⁾ European Parliament resolution of 10 April 2008 on cultural industries in Europe (2007/2153(INI)), point 23.

35. The EDPS considers that a balance has to be found between the legitimate objective to fight against illegal content and the appropriate nature of the means used. He recalls that any action of surveillance of telecommunication networks, where necessary in specific cases, should be the task of law enforcement authorities.

IV. CONCLUSION

36. The EDPS supports the proposal for a multiannual programme to protect children using the Internet and other communication technologies. He welcomes the fact that this programme intends to focus on the development of new technologies and on the elaboration of concrete actions to enhance the effectiveness of the protection of children.

37. The EDPS recalls that the protection of personal data is an essential prerequisite to the safety of children online. Misuse of children's personal information must be prevented, using the orientations proposed in the programme, and especially the following:

- ensuring awareness of children and other stakeholders like parents and educators,
- promoting the development of best practice by the industry,
- promoting the development of privacy compliant technological tools,

— favouring the exchange of good practice and practical experience amongst relevant authorities, including data protection authorities.

38. These actions should be developed without overlooking the fact that the protection of children takes place within an environment where the rights of others might be at stake. Any initiative of collecting, blocking or reporting information should only be taken in the respect of the fundamental rights of all individuals involved and in compliance with the data protection legal framework. In particular, the EDPS recalls that the surveillance of telecommunication networks, where necessary in specific circumstances, should be the task of law enforcement authorities.

39. The EDPS notes that this programme constitutes a general framework for further concrete actions. He considers that some observations made in this opinion are a first step and could be developed in a practical way, by reference to the projects still to be put in place, in line with the orientations of the programme. He recommends that data protection authorities be closely involved when it comes to the definition of these practical projects. He also refers to the activities of the Article 29 Working Party on the subject, and in particular to the present work of the Working Party on social networks ⁽¹⁾.

Done at Brussels, 23 June 2008.

Peter HUSTINX
European Data Protection Supervisor

⁽¹⁾ See the Working Document 1/2008 of 18 February 2008 on the protection of Children's Personal Data, WP 147, and for a more general view, the work programme 2008-2009 of the Working Party including social networks, available at: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2008_en.htm