ΠΑΝΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ
ΚΟΙΝΩΝΙΚΩΝ & ΠΟΛΙΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ
Π.Μ.Σ. ΔΙΚΑΙΟ ΕΠΙΧΕΙΡΗΣΕΩΝ ΚΑΙ ΔΙΟΙΚΗΣΗ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ:
«Ηλεκτρονικό Εμπόριο & Προστασία Προσωπικών Δεδομένων»
Η μετάβαση από την Οδηγία 95/46/ΕΚ στον Γενικό Κανονισμό 679/2016/ΕΕ

Μεταπτυχιακή Φοιτήτρια: Έλενα Δημάρκο του Μιχάλ
(ΑΜ: 7116Μ037)

Επιβλέπων Καθηγητής: Άγγελος Μπώλος, Επίκ. Καθηγητής

ΑΘΗΝΑ 2018

Πίνακας περιεχομένων

Συντομογραφίες

ΑΚ	Αστικός Κώδικας
βλ.	Βλέπε
ΓΟΣ	Γενικοί Όροι Συναλλαγών
ΔΕΕ	Δικαστήριο της Ευρωπαϊκής Ένωσης
ΔΕΚ	Δικαστήριο των Ευρωπαϊκών Κοινοτήτων
εδ.	εδάφιο
ΕΕ	Ευρωπαϊκή Ένωση
ΕΚ	Ευρωπαϊκή Κοινότητα
επ.	επόμενα
κλπ.	και τα λοιπά
ΚΠολΔ	Κώδικας Πολιτικής Δικονομίας
παρ.	παράγραφος
π.δ.	προεδρικό διάταγμα
π.χ.	παραδείγματος χάρη
σελ.	σελίδα

Εισαγωγή

Η προστασία των προσωπικών δεδομένων από την αθέμιτη επεξεργασία τους δεν είναι κάτι καινούριο ούτε στον ευρωπαϊκό, ούτε και στο διεθνή χώρο. Ήδη από τα τέλη της δεκαετίας του 1960, όταν οι ηλεκτρονικοί υπολογιστές άρχισαν να πρωτοεμφανίζονται η έννοια της επεξεργασίας άλλαξε εντελώς και τα πρώτα συναφή νομοθετήματα, είτε διεθνή είτε εθνικά, άρχισαν να τίθενται σε ισχύ. Παραδοσιακές νομικές έννοιες, όπως η προσωπική ελευθερία, το άσυλο της κατοικίας και η ιδιωτική ζωή άλλαξαν τελείως περιεχόμενο υφιστάμενες τη θεσμική διάβρωση που επέφερε η ανάπτυξη της τεχνολογίας. Η αθέμιτη επεξεργασία των προσωπικών δεδομένων έλαβε μεγαλύτερη διάσταση στον χώρο του ηλεκτρονικού εμπορίου και ειδικότερα κατά την κατάρτιση ηλεκτρονικών συμβάσεων με ηλεκτρονικά καταστήματα (e-shops). Ένας καταναλωτής προκειμένου να προβεί σε κάποια αγορά μέσω ενός ηλεκτρονικού καταστήματος (e-shop) είναι αναγκασμένος να κοινοποιήσει σε αυτό τα προσωπικά του στοιχεία, όπως το ονοματεπώνυμό του, την διεύθυνσή του, το email του κ.ά.. Θα πρέπει λοιπόν κατά την διαδικασία αυτή το ηλεκτρονικό κατάστημα να είναι σε θέση να του εγγυηθεί ότι τα προσωπικά του δεδομένα θα παραμείνουν ασφαλή κατά την κατάρτιση της ηλεκτρονικής σύμβασης. Το ηλεκτρονικό κατάστημα (e-shop) θα πρέπει να γνωστοποιεί στον καταναλωτή την πολιτική απορρήτου που ακολουθεί, καθώς και τα δικαιώματα που έχει ο τελευταίος, κατά την επεξεργασία των προσωπικών του δεδομένων. Κομβική σημασίας ως προς την άρση του άδικου χαρακτήρα της επεξεργασίας των προσωπικών δεδομένων αποτελεί η λήψη συγκατάθεσης από το υποκείμενο των δεδομένων. Ο Γενικός Κανονισμός Προστασίας των προσωπικών δεδομένων διευρύνει την διαφάνεια και τις υποχρεώσεις δημοσιοποίησης των παραβιάσεων από τις εταιρίες. Ο ορισμός υπεύθυνου προστασίας δεδομένων μπορεί σε κάθε περίπτωση να διευκολύνει την διαδικασία συμμόρφωσης με τον Γενικό Κανονισμό Προστασίας Δεδομένων. Τα ηλεκτρονικά καταστήματα (e-shops) θα πρέπει να υιοθετήσουν τεχνικά και οργανωτικά μέτρα ασφαλείας[1], προκειμένου να μην βρεθούν στην δυσμενή θέση, επιβολής σε αυτά, στην περίπτωση παραβίασης προσωπικών δεδομένων

[1] Ως «τεχνικά και οργανωτικά μέτρα ασφαλείας» νοούνται τα μέτρα που αποσκοπούν στην προστασία των δεδομένων προσωπικού χαρακτήρα από την τυχαία ή παράνομη καταστροφή, την τυχαία απώλεια, την αλλοίωση, τη μη εξουσιοδοτημένη κοινοποίηση ή πρόσβαση, ιδίως όταν η επεξεργασία συνεπάγεται τη διαβίβαση δεδομένων μέσω δικτύου, καθώς και στην προστασία από κάθε άλλη παράνομη μορφή επεξεργασίας.

καταναλωτών πρόστιμα ύψους 20 εκατομμυρίων ευρώ ή 4% του συνολικού ετήσιου παγκόσμιου τζίρου τους.

ΚΕΦΑΛΑΙΟ Α' Το ρυθμιστικό πλαίσιο των προσωπικών δεδομένων στο ηλεκτρονικό εμπόριο

1. Η Οδηγία 2000/31 για το Ηλεκτρονικό Εμπόριο

1.1. Γενικά

Το βασικότερο νομοθέτημα που διέπει τη λειτουργία των ηλεκτρονικών καταστημάτων είναι η Οδηγία 2000/31/ΕΕ. Η Οδηγία 2000/31/ΕΕ, γνωστή ως «οδηγία για το ηλεκτρονικό εμπόριο», η οποία αφορά τη ρύθμιση ορισμένων νομικών πτυχών των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά ψηφίστηκε από τα όργανα της ΕΕ και εκδόθηκε στις 8 Ιουνίου του 2000 για την απάλειψη των νομικών κινδύνων και της ανασφάλειας στο χώρο του ηλεκτρονικού εμπορίου. Αποτελείται από 24 άρθρα, τα οποία κατανέμονται σε τέσσερα κεφάλαια. Το πρώτο κεφάλαιο (άρθρα 1-3) αφορά γενικές διατάξεις σχετικά με το στόχο, το πεδίο εφαρμογής, τον ορισμό βασικών εννοιών, των μέτρων που πρέπει να λαμβάνουν τα κράτη μέλη και τις πληροφορίες που πρέπει να παρέχονται στους αποδέκτες των ηλεκτρονικών υπηρεσιών. Στο δεύτερο κεφάλαιο της Οδηγίας (άρθρα 4-15) αναλύονται οι αρχές που τη διέπουν και ιδίως οι σχετικές με τις εμπορικές επικοινωνίες, τις ηλεκτρονικές συμβάσεις, τις παρεχόμενες πληροφορίες, την ευθύνη των μεσαζόντων, ενώ στο τρίτο κεφάλαιο (άρθρα 16-20) περιλαμβάνονται οι διατάξεις σχετικά με την εφαρμογή των όρων της Οδηγίας, συμπεριλαμβανομένης της επίλυσης διαφορών που ανακύπτουν στις ηλεκτρονικές συναλλαγές. Τέλος, το τέταρτο κεφάλαιο (άρθρα 21-24) αφορά μόνο τελικές διατάξεις.

1.1.1 Το πεδίο εφαρμογής της Οδηγίας

Η Οδηγία εφαρμόζεται σε κάθε υπηρεσία, η οποία παρέχεται έναντι αμοιβής, από απόσταση με ηλεκτρονικά μέσα και μετά από προσωπική αίτηση ενός αποδέκτη υπηρεσιών[2]. Αν και η διατύπωση αυτή επιτρέπει την υπαγωγή σε αυτή ενός μεγάλου εύρους δραστηριοτήτων, αυτές περιορίζονται από μία σειρά εξαιρέσεων που προβλέπονται από την Οδηγία. Συγκεκριμένα, η Οδηγία δεν εφαρμόζεται στον φορολογικό τομέα, σε ζητήματα προστασίας προσωπικών δεδομένων, σε θέματα ή πρακτικές διεπόμενες από τη νομοθεσία περί καρτέλ, σε δραστηριότητες

[2]Άρθρα 1 και 2 παρ. α και την αιτιολογική σκέψη 17 της Οδηγίας 2000/31/ΕΕ.

συμβολαιογράφων και άλλων αντίστοιχων επαγγελμάτων σε περίπτωση που συνεπάγονται άμεση και ειδική σύνδεση με την άσκηση δημόσιας εξουσίας, την εκπροσώπηση πελάτη ενώπιον των δικαστηρίων, τη συμμετοχή σε τυχερά παιχνίδια[3]. Η εξαίρεση των τυχερών παιχνιδιών από το πεδίο εφαρμογής αφορά μόνο τα τυχερά παιχνίδια, τα λαχεία και τα στοιχήματα στα οποία ο παίκτης στοιχηματίζει νομισματική αξία και όχι τους διαφημιστικούς διαγωνισμούς ή τυχόν παιχνίδια που αποσκοπούν στην πώληση αγαθών ή υπηρεσιών και όπου οι πληρωμές χρησιμεύουν μόνο για την απόκτηση διαφημιζόμενων αγαθών ή υπηρεσιών. Μία ακόμα εξαίρεση διατυπώνεται στη σκέψη 18 του προοιμίου, σύμφωνα με την οποία αποκλείονται από το πεδίο εφαρμογής και οι δραστηριότητες που δεν πραγματοποιούνται σε απευθείας σύνδεση (on-line). Ο αποκλεισμός αυτός αφήνει εκτός πεδίου εφαρμογής το έμμεσο ηλεκτρονικό εμπόριο και στενεύει σε σημαντικό βαθμό το πλαίσιο εφαρμογής της οδηγίας σε σημείο αδικαιολόγητο.

1.1.2 Ο στόχος της Οδηγίας

Προκειμένου να εξασφαλιστούν η ασφάλεια δικαίου και η εμπιστοσύνη του καταναλωτή, η οδηγία επιχείρησε να καθορίσει ένα σαφές γενικό πλαίσιο που να καλύπτει ορισμένες νομικές πτυχές του ηλεκτρονικού εμπορίου στην εσωτερική αγορά. Πρωταρχικός στόχος της ήταν, η εξασφάλιση της ελεύθερης κυκλοφορίας των υπηρεσιών της κοινωνίας της πληροφορίας, μεταξύ των κρατών μελών και η ομαλή λειτουργία της εσωτερικής αγοράς[4], όπως αυτός διαγράφεται δια του άρθρου 1 παρ. 1. Επιδίωξε, δηλαδή, τη δημιουργία ενός χώρου χωρίς εθνικά σύνορα για τις υπηρεσίες αυτές.

Παρότι η Οδηγία αυτή δεν εμπίπτει στον κύκλο οδηγιών που έχουν εκδοθεί με σκοπό την προστασία του καταναλωτή, στο άρθρο 1 παρ. 3 ορίζεται ότι, αυτή «δεν θίγει το επίπεδο προστασίας, ιδίως της δημόσιας υγείας και των συμφερόντων του καταναλωτή, όπως θεσπίζεται στις κοινοτικές και εθνικές νομοθετικές πράξεις στο μέτρο που δεν υφίσταται περιορισμός της ελευθερίας παροχής υπηρεσιών της κοινωνίας της πληροφορίας». Πρόκειται για την εξασφάλιση της θεμελιώδους αρχής του κοινοτικού κεκτημένου (acquis communautaire), το οποίο εν προκειμένω εξειδικεύεται ως κεκτημένο προστασίας του καταναλωτή (aquis consommateur). Η αρχή αυτή ερμηνεύεται ως υποχρέωση των κρατών μελών να τηρούν το παράγωγο κοινοτικό και εναρμονισμένο προς αυτό εθνικό δίκαιο, που ρυθμίζει όλα τα επιμέρους ζητήματα της προστασίας του καταναλωτή.

---

[3] Άρθρο 1 παρ. 5 της Οδηγίας 2000/31/ΕΕ .

[4] *Καράκωστας Ι.*, Δίκαιο & Internet, Νομικά ζητήματα του Διαδικτύου, 2003, σελ. 169

Ο κανόνας, βέβαια, αυτός πρέπει να εφαρμόζεται πάντοτε με την επιφύλαξη του μη περιορισμού της ελεύθερης κυκλοφορίας των υπηρεσιών της κοινωνίας της πληροφορίας. Κύριο μέλημα των συντακτών της Οδηγίας, φαίνεται να υπήρξε, όχι ευθέως η επίτευξη στόχων κοινωνικής πολιτικής, αλλά η εγκαθίδρυση μιας αγοράς χωρίς εσωτερικά σύνορα, στον τομέα των υπηρεσιών της κοινωνίας της πληροφορίας, η οποία κατ' επέκταση θα μπορούσε να οδηγήσει στην επίτευξη υψηλού επιπέδου κοινοτικής ολοκλήρωσης. Η Οδηγία δεν θίγει το κοινοτικό κεκτημένο σε θέματα δημόσιας υγείας και προστασίας των καταναλωτών, καθώς έχει συμπληρωματικό χαρακτήρα προς το ισχύον ενωσιακό δίκαιο. Συνάμα δεν θεσπίζει πρόσθετους κανόνες, στον τομέα του Ιδιωτικού Διεθνούς Δικαίου, ούτε σχετίζεται με τη δικαιοδοσία των δικαστηρίων όπως διευκρινίζεται στο άρθρο 1 παρ. 4 της Οδηγίας. Αυτό σημαίνει, ότι για διαφορές που θα ανακύψουν στο πλαίσιο ηλεκτρονικών συναλλαγών, σε ενδοκοινοτικό επίπεδο και κατ' επέκταση σε συναλλαγές που λαμβάνουν χώρα σε ηλεκτρονικά καταστήματα μεταξύ μερών ευρισκόμενων σε κράτη μέλη της ΕΕ εξακολουθούν να εφαρμόζονται οι κανόνες του Ιδιωτικού Διεθνούς Δικαίου, ιδίως ο Κανονισμός 1215/2012/ΕΕ, ο Κανονισμός Ρώμη Ι και ο Κανονισμός Ρώμη ΙΙ.

1.1.3 Οι αρχές που διέπουν την Οδηγία

Ο κύριος στόχος της Οδηγίας, η εξασφάλιση της ελεύθερης κυκλοφορίας των υπηρεσιών της κοινωνίας της πληροφορίας μεταξύ των κρατών μελών εδράζεται δε σε τρεις πυλώνες-αρχές:

Αρχή της χώρας προέλευσης (country of origin principle). Η Οδηγία απηχεί δια μέσου του άρθρου 3 και ιδίως των παραγράφων 1 και 2 την αρχή της χώρας προέλευσης, σύμφωνα με την οποία, το κράτος, όπου ο φορέας μίας υπηρεσίας κοινωνίας πληροφοριών είναι εγκατεστημένος, είναι υπεύθυνο για την νομιμότητα της δραστηριότητας της. Ως εκ τούτου, οι δραστηριότητες του ηλεκτρονικού καταστήματος, στο πλαίσιο των on-line υπηρεσιών του, θα διέπονται από το δίκαιο του κράτους, όπου είναι εγκατεστημένο. Τα κράτη μέλη, οφείλουν να μην επιβάλλουν περιορισμούς στις υπηρεσίες κοινωνίας της πληροφορίας, που προέρχονται από άλλο κράτος μέλος, αλλά να εμπιστεύονται τις εθνικές νομοθεσίες των υπολοίπων κρατών και να εφαρμόζουν την αρχή της αμοιβαίας αναγνώρισης. Εντούτοις, προβλέπεται και δυνατότητα παρέκκλισης σε ορισμένες ειδικές περιπτώσεις για λόγους δημοσίας τάξεως, προστασίας της δημόσιας υγείας, προστασίας της δημόσιας ασφάλειας, προστασίας καταναλωτή/ επενδυτή. Τα λαμβανόμενα μέτρα ως παρέκκλιση, θα πρέπει όμως πάντοτε να είναι, σύμφωνα με την αρχή της αναλογικότητας και να περιορίζονται στα απολύτως αναγκαία.

Αρχή της μη αναγκαίας προηγούμενης άδειας. Το κεφάλαιο ΙΙ της οδηγίας που τιτλοφορείται «Αρχές» περιλαμβάνει αναφορά στην αρχή της μη αναγκαίας προηγούμενης άδειας στο άρθρο 4, με εξαίρεση τις περιπτώσεις καθεστώτων έγκρισης που δεν αφορούν ειδικά και αποκλειστικά τις υπηρεσίες κοινωνίας της πληροφορίας.

Υποχρεώσεις πληροφόρησης και διαφάνειας. Στο ίδιο κεφάλαιο σημειώνονται ως αρχές της Οδηγίας οι υποχρεώσεις πληροφόρησης και διαφάνειας. Πιο συγκεκριμένα, για να καταστεί εφικτή η διαφάνεια και η προστασία των καταναλωτών, προβλέπεται, η παροχή ορισμένων πληροφοριών, στις οποίες ο φορέας υπηρεσιών, και επί του πλαισίου της παρούσας εργασίας το ηλεκτρονικό κατάστημα, οφείλει να παρέχει στους αποδέκτες των υπηρεσιών του, άλλως καταναλωτές. Αξίζει να σημειωθεί, ότι ο κοινοτικός νομοθέτης, δίδει στη διαφάνεια και την παροχή ουσιώδους πληροφόρησης[5], ιδιαίτερα μεγάλη βαρύτητα, κυρίως όταν πρόκειται για καταναλωτικές συμβάσεις, θεωρώντας προφανώς, ότι με αυτόν τον τρόπο επέρχεται μετριασμός του γνωσιολογικού ελλείμματος του ως είθισται ανίδεου αποδέκτη και του δίδεται η δυνατότητα να λάβει συνειδητή και υπεύθυνη απόφαση.

1.1.4 Το ΠΔ 131/2003 για το ηλεκτρονικό εμπόριο

Η μεταφορά της Οδηγίας στα εθνικά δίκαια των κρατών μελών έπρεπε να γίνει έως 17.01.2002, σύμφωνα με το άρθρο 22 της Οδηγίας. Η Ελλάδα, ωστόσο, προσαρμόστηκε μετά από δεκαεξάμηνη καθυστέρηση, μεταφέροντας στο ΠΔ 131/2003 σχεδόν αυτολεξεί την Οδηγία, με πρόβλεψη στο άρθρο 21 του ΠΔ αναδρομικής ισχύς, ούτως ώστε να εξισορροπηθεί η καθυστέρηση. Μέσω του ΠΔ 131/2003 η Ελλάδα απέκτησε ένα σχετικά ολοκληρωμένο νομοθετικό πλαίσιο για τη ρύθμιση των νομικών προβλημάτων που εμφανίζονται στις ηλεκτρονικές συναλλαγές.

Ειδικότερα με το ΠΔ 131/2003 θεσπίστηκαν διατάξεις για τις υπηρεσίες της κοινωνίας της πληροφορίας, οι οποίες αφορούν την εσωτερική αγορά στην Ευρωπαϊκή Ένωση, την εγκατάσταση των φορέων παροχής υπηρεσιών, τις εμπορικές επικοινωνίες, τη σύναψη συμβάσεων με ηλεκτρονικά μέσα, την ευθύνη των μεσαζόντων παροχής υπηρεσιών της κοινωνίας της πληροφορίας, τους κώδικες δεοντολογίας, τον εξώδικο διακανονισμό διαφορών, τα μέσα έννομης προστασίας, τη συνεργασία μεταξύ κρατών μελών και τις κυρώσεις για την παραβίαση των διατάξεων.

[5] *Καράκωστας Ι.,* Προστασία του καταναλωτή (ν. 2251/1994), σελ. 89

Όπως καθίσταται σαφές, το ΠΔ 131/2003 επιχείρησε να καλύψει, μέσω μιας σφαιρικής προσέγγισης, γενικά τα θέματα που αφορούν την άσκηση επιχειρηματικής δραστηριότητας, στο πεδίο του ηλεκτρονικού εμπορίου. Από την άλλη, φρονώντας ο κοινοτικός νομοθέτης, ότι δύναται να εφαρμοστούν αναλογικά και στο ηλεκτρονικό εμπόριο, οι ρυθμίσεις του εθνικού δικαίου των κρατών μελών, η Οδηγία επικεντρώθηκε σε ορισμένα μόνο ζητήματα.

Η προσέγγιση της οδηγίας είναι «οριζόντια», δηλαδή δεν προβαίνει σε ρύθμιση συγκεκριμένων υπηρεσιών στην κοινωνία της πληροφορίας, όπως η πώληση καταναλωτικών αγαθών μέσω του διαδικτύου ή εξειδικευμένων τομέων του δικαίου, αλλά επιχειρεί με βάση ένα ενιαίο κανονιστικό πλαίσιο να καλύψει ορισμένες πτυχές της οικονομικής δραστηριότητας των φορέων παροχής υπηρεσιών στο διαδίκτυο. Το άρθρο 20 παρ. 3 του ΠΔ 131/2003, με σκοπό τη μεταφορά της διάταξης 1 παρ. 3 της Οδηγίας στην ελληνική νομοθεσία, αναφέρει ότι «καμία διάταξη του παρόντος ΠΔ δεν μπορεί να ερμηνευθεί κατά τρόπο που να θίγει το επίπεδο προστασίας της δημόσιας υγείας και των συμφερόντων του καταναλωτή, όπως θεσπίζεται σε κοινοτικές πράξεις και στις εθνικές νομοθεσίες που εκδόθηκαν κατ' εφαρμογή τους, στο μέτρο που δεν περιορίζεται έτσι η ελευθερία παροχής υπηρεσιών της κοινωνίας της πληροφορίας».

Στην ελληνική ρύθμιση, δεν τίθεται λοιπόν ρητά, η υποχρέωση εφαρμογής του κοινοτικού κεκτημένου, όσον αφορά στην προστασία του καταναλωτή, όπως συμβαίνει στο άρθρο 1 παρ. 3 της Οδηγίας, αλλά η ρύθμιση περιορίζεται στον τρόπο ερμηνείας των διατάξεων του διατάγματος αυτού. Η ερμηνεία θα πρέπει να γίνεται, με τρόπο που δεν θίγει, το επίπεδο προστασίας του καταναλωτή, στο μέτρο βεβαίως που δεν περιορίζεται η ελεύθερη κυκλοφορία των υπηρεσιών της κοινωνίας της πληροφορίας. Θα πρέπει μάλλον, να γίνει δεκτό, ότι η εν λόγω ρύθμιση δεν αποτελεί ακριβή μεταφορά της Οδηγίας στην εθνική μας νομοθεσία.

1.2 Η Οδηγία 95/46/ΕΚ και η ενσωμάτωσή της στην ελληνική έννομη τάξη με τον Νόμο 2472/1997

1.2.1 Οι κυριότερες ρυθμίσεις της Οδηγίας 95/46/ΕΚ

Η αρμοδιότητα της Κοινότητας, να νομοθετήσει επί του ζητήματος προστασίας των προσωπικών δεδομένων δεν της είχε απονεμηθεί με τα ιδρυτικά κείμενα. Παρόλα αυτά, στις 13 Σεπτεμβρίου του 1990, η Επιτροπή αποστέλλει στο Συμβούλιο επίσημη πρόταση[6], η οποία περιελάμβανε ένα πακέτο νομοθετικών μέτρων για την προστασία των προσωπικών δεδομένων. Μέσα στο κείμενο, η Επιτροπή προσπαθεί

[6] Η πρόταση με την αιτιολογική της έκθεση βρίσκεται δημοσιευμένη εδώ: http://aei.pitt.edu/3768/1/3768.pdf

να θεμελιώσει την αρμοδιότητά της, καταρχήν στο υψηλό επίπεδο που η ίδια εγγυάται για τα θεμελιώδη δικαιώματα και κατά δεύτερον στην ανάγκη συμπλήρωσης του κενού που άφηνε η Σύμβαση 108 του Συμβουλίου της Ευρώπης, η οποία ρύθμιζε μόνο την αυτοματοποιημένη προστασία προσωπικών δεδομένων. Επικαλέστηκε επίσης, τη μεγάλη διαφοροποίηση που παρατηρείτο στις επιμέρους εθνικές ρυθμίσεις των κρατών μελών και έκανε ιδιαίτερη μνεία στα Ψηφίσματα του Κοινοβουλίου που ζητούσαν από την Επιτροπή να αναλάβει νομοθετικές πρωτοβουλίες.

Αντικείμενο της ρύθμισης ήταν, τόσο η αυτοματοποιημένη[7] επεξεργασία, όσο και η μη αυτοματοποιημένη, τόσο στο δημόσιο όσο και στον ιδιωτικό τομέα. Υπήρχε επίσης ρητή σύνδεση με το δικαίωμα στην ιδιωτικότητα. Η σύνδεση αυτή απασχόλησε περισσότερο και την Οικονομική και Κοινωνική Επιτροπή κατά την επεξεργασία της πρότασης και τη διατύπωση της γνώμης της, η οποία θεωρούσε ότι θα έπρεπε να υπάρχει αναφορά και σε άλλα θεμελιώδη δικαιώματα και ελευθερίες, εφόσον η πρόταση είχε ως στόχο και την προστασία της ιδιωτικότητας.

Η Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών εγκρίθηκε στις 24 Οκτωβρίου 1995 και τέθηκε σε ισχύ τον Δεκέμβριο του ίδιου έτους.

Η Οδηγία αυτή, αποτελεί το σημαντικότερο κείμενο προστασίας προσωπικών δεδομένων και έχει συμβάλλει σε πολύ μεγάλο βαθμό στην κατοχύρωση του δικαιώματος αυτού ως θεμελιώδους. Αξιοσημείωτο είναι το γεγονός, ότι το παράγωγο ενωσιακό δίκαιο προηγήθηκε ιστορικά του πρωτογενούς. Όταν το δικαίωμα προστασίας των προσωπικών δεδομένων έτυχε αναγνώρισης και στο πρωτογενές ενωσιακό δίκαιο τόσο στον Χάρτη Θεμελιωδών Δικαιωμάτων της Ε.Ε., όσο και με τη Συνθήκη της Λισαβόνας, η Οδηγία 95/46/ΕΚ μετρούσε ήδη πολλά χρόνια εφαρμογής. Η επιρροή της ήταν τεράστια και στα εθνικά νομικά συστήματα των κρατών μελών, τα οποία σε πολλές περιπτώσεις υιοθέτησαν ρυθμίσεις πολύ αυστηρότερες από αυτές που προβλέπονταν στην Οδηγία.

[7] Στην υπόθεση Bodil Lindqvist, το ΔΕΕ έκρινε ότι: «η εργασία που συνίσταται στην αναφορά, επί ιστοσελίδας του διαδικτύου, σε διάφορα πρόσωπα και στον προσδιορισμό τους είτε με το όνομά τους είτε με άλλα μέσα, για παράδειγμα με τον αριθμό τηλεφώνου τους ή με στοιχεία σχετικά με τις συνθήκες εργασίας τους και τις ασχολίες τους κατά τον ελεύθερο χρόνο, συνιστά αυτοματοποιημένη, εν όλω ή εν μέρει, επεξεργασία δεδομένων προσωπικού χαρακτήρα, κατά την έννοια του άρθρου 3 παράγραφος 1 της οδηγίας 95/46».

Αντικείμενο προστασίας της Οδηγίας δεν είναι τα προσωπικά δεδομένα εν γένει, αλλά τα φυσικά πρόσωπα[8] κατά την επεξεργασία των προσωπικών τους δεδομένων. Υπόχρεος να παράσχει την προστασία των θεμελιωδών δικαιωμάτων και ελευθεριών, ιδίως του δικαιώματος στην ιδιωτικότητα κατά την επεξεργασία των δεδομένων των φυσικών προσώπων είναι τα κράτη μέλη. Πέρα από το αμυντικό περιεχόμενο του δικαιώματος, η Οδηγία θέτει και ένα διεκδικητικό, την κατάργηση δηλαδή όλων των περιορισμών στην ελεύθερη ροή των προσωπικών δεδομένων μεταξύ των κρατών μελών.

Ως δεδομένα προσωπικού χαρακτήρα[9], η Οδηγία θεωρεί κάθε πληροφορία που αναφέρεται σε φυσικό πρόσωπο του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί. Ιδιαίτερο προβληματισμό έχει προκαλέσει στη νομολογία και τη θεωρία το ζήτημα των βιομετρικών δεδομένων[10].

Η επεξεργασία των δεδομένων συνίσταται σε κάθε εργασία ή σειρά εργασιών, αυτοματοποιημένων ή μη, όπως η συλλογή, η καταχώρηση, η αποθήκευση, η διαβίβαση, ο συνδυασμός, η διαγραφή, ακόμα και η καταστροφή.

Κάθε επεξεργασία προσωπικών δεδομένων είναι μη νόμιμη, εκτός αν υπακούει σε ορισμένες αρχές. Συναφώς, στο άρθρο 7 της Οδηγίας, προβλέπονται οι

---

[8] Το δικαίωμα προστασίας προσωπικών δεδομένων απονέμεται σε φυσικά και όχι νομικά πρόσωπα. Η μόνη δυνατότητα να υπερκεραστεί αυτό το τυπικό εμπόδιο, είναι το να καταφέρουν οι προσφεύγοντες, να αποδείξουν, ότι εκφράζουν τα μέλη τους, τα οποία είναι φυσικά πρόσωπα. Με αγωνία αναμένεται επί του ζητήματος αυτού η απόφαση επί της προσφυγής της Digital Rights Ireland Ltd κατά της Επιτροπής ενώπιον του Γενικού Δικαστηρίου ζητώντας την ακύρωση της απόφασης (ΕΕ) 2016/1250 της Επιτροπής σχετικά με την επάρκεια της προστασίας που παρέχεται από την Privacy Shield. Έναν μήνα αργότερα, διάφοροι γαλλικοί φορείς προσέφυγαν ενώπιον του ΔΕΕ εναντίον της ίδιας απόφασης για λόγους παρόμοιους με αυτούς που προέβαλε η Digital Rights. Οι αποφάσεις του Δικαστηρίου αναμένονται με μεγάλο ενδιαφέρον, αν και πιθανολογούνται αβάσιμες, καθώς οι προσφεύγοντες και στις δυο υποθέσεις είναι νομικά και όχι φυσικά πρόσωπα.

[9] Διαφωτιστική σχετικά με την έννοια των προσωπικών δεδομένων είναι και η απόφαση Lindqvist (C-101-01) στην οποία το Δικαστήριο έκρινε ότι το όνομα ενός φυσικού προσώπου σε συνδυασμό με τον αριθμό του τηλεφώνου του και με πληροφορίες σχετικά με τις συνθήκες εργασίας του ή τα προσωπικά του ενδιαφέροντα είναι προσωπικά δεδομένα. Συναφώς και στην Tietosuojavaltuutetuu (C-73/07), το Δικαστήριο θεώρησε ως προσωπικά δεδομένα για τους σκοπούς της Οδηγίας τη μισθοδοσία φυσικών προσώπων, ακόμα και το σημείο αναφοράς το οποίο ξεπερνά η μισθοδοσία τους.

[10] *Παναγόπουλου – Κουτνατζή Φ.,* Βιομετρικές μέθοδοι και προστασία ιδιωτικότητας : Σκέψεις με αφορμή την απόφαση του ΔΕΕ Michael Schwarz κατά Κρατιδίου του Bochum (C-291/2012), ΔίΜΜΕ 2013, σελ. 482

νομιμοποιητικές βάσεις της επεξεργασίας. Δεν είναι, λοιπόν, παράνομη η επεξεργασία προσωπικών δεδομένων όταν:

α) βασίζεται στη συγκατάθεση του υποκειμένου των δεδομένων,

β) είναι απαραίτητη για την εκτέλεση σύμβασης στην οποία το υποκείμενο είναι συμβαλλόμενο μέρος,

γ) είναι εκ του νόμου επιβεβλημένη,

δ) γίνεται προς το συμφέρον του υποκειμένου,

ε) επιβάλλεται για λόγους δημοσίου συμφέροντος και

στ) επιδιώκεται η ικανοποίηση εννόμου συμφέροντος αυτού που έχει την ευθύνη της επεξεργασίας ή τρίτων, υπό την απαραίτητη προϋπόθεση, το έννομο συμφέρον αυτό να μην έρχεται σε αντίθεση, με το αντίστοιχο, του υποκειμένου των δεδομένων.

Προς περαιτέρω προστασία των υποκειμένων των δεδομένων, η Οδηγία προβλέπει σειρά επιμέρους δικαιωμάτων για τα υποκείμενα, τα οποία σχετίζονται με την επεξεργασία και έχουν ως στόχο να εξασφαλίσουν, ότι αυτή, θα υπακούει καθ' όλη τη διάρκεια της, σε ορισμένες θεμελιώδεις αρχές.

Η ευθύνη της τήρησης της υποχρέωσης για το νομότυπο της επεξεργασίας ανήκει στο πρόσωπο που φέρει την ευθύνη αυτής. Το πρόσωπο αυτό ονομάζεται «υπεύθυνος επεξεργασίας» και είναι το πρόσωπο (φυσικό ή νομικό, δημοσίου ή ιδιωτικού δικαίου) που μόνος ή από κοινού με άλλους καθορίζει τους στόχους και τον τρόπο της επεξεργασίας των δεδομένων. Η έννοια[11] του υπεύθυνου

[11] Στις πρόσφατα δημοσιευμένες προτάσεις του, επί της υπόθεσης Facebook Ireland (C-210/16), ο γενικός εισαγγελέας Yves Bot πρότεινε στο Δικαστήριο να κρίνει πως ο διαχειριστής fanpage κοινωνικού δικτύου (εν προκειμένω το Facebook), είναι υπεύθυνος επεξεργασίας, κατά την έννοια της Οδηγίας 95/46/ΕΚ, όσον αφορά το στάδιο επεξεργασίας δεδομένων προσωπικού χαρακτήρα που συνίσταται στη συλλογή από το κοινωνικό δίκτυο των δεδομένων που αφορούν τα πρόσωπα που επισκέπτονται την ενλόγω σελίδα με σκοπό την κατάρτιση στατιστικών επισκεψιμότητας της συγκεκριμένης σελίδας. Η πρακτική αυτή ονομάζεται web tracking και συνίσταται στην παρατήρηση και ανάλυση της συμπεριφοράς των χρηστών του διαδικτύου για εμπορικούς κυρίως σκοπούς. Ο γενικός εισαγγελέας διατύπωσε στην πρότασή του και την άποψη, πως η δραστηριότητά του υπεύθυνου επεξεργασίας στρέφεται προς τους κατοίκους του κράτους μέλους που αποτελούν στόχους της προωθητικής και διαφημιστικής δραστηριότητας, ακόμα και αν ο υπεύθυνος επεξεργασίας βρίσκεται εγκαταστημένος σε άλλο κράτος μέλος. Αυτό σημαίνει ότι αρμόδια να επιληφθεί της υπόθεσης είναι η αρχή ελέγχου του κράτους μέλους στο οποίο βρίσκονται εγκαταστημένα τα υποκείμενα των δεδομένων και ότι μπορεί, σύμφωνα πάντα με το γενικό εισαγγελέα , αυτή να ασκεί την εξουσία παρεμβάσεως που διαθέτει βάσει της Οδηγίας, χωρίς να υποχρεούται να

επεξεργασίας αντιδιαστέλλεται προς αυτή του εκτελούντος την επεξεργασία, ο οποίος είναι το πρόσωπο (φυσικό ή νομικό, δημοσίου ή ιδιωτικού δικαίου) το οποίο επεξεργάζεται τα δεδομένα για λογαριασμό του υπεύθυνου επεξεργασίας.

Η Οδηγία προβλέπει και ειδικούς κανόνες για την επεξεργασία δεδομένων ειδικών κατηγοριών. Στο άρθρο 8, υπάρχει πρόβλεψη για τα ευαίσθητα προσωπικά δεδομένα, όπως είναι η φυλετική καταγωγή, τα πολιτικά φρονήματα, η σεξουαλική ζωή, τα δεδομένα που αφορούν σε ποινικές καταδίκες. Τα κράτη μέλη, υποχρεούνται καταρχήν, να απαγορεύουν οποιαδήποτε επεξεργασία τέτοιου είδους προσωπικών δεδομένων. Φυσικά, υπάρχει πρόβλεψη στο κείμενο της Οδηγίας για κάμψη της απαγόρευσης αυτής, για συγκεκριμένους περιοριστικά αναφερόμενους λόγους. Ως δικαιολογητική βάση, για την θέσπιση ειδικών κατηγοριών προσωπικών δεδομένων, οι οποίες μάλιστα, απολαμβάνουν και ευρύτερης προστασίας, μπορεί να θεωρηθεί η αρχή της απαγόρευσης των διακρίσεων. Ειδικότερα, ο κοινοτικός νομοθέτης προσπάθησε να αποτρέψει τυχόν δημιουργία διακρίσεων που θα είχαν ως βάση τις ευαίσθητες αυτές πληροφορίες του φυσικού προσώπου.

Όπως, κάθε δικαίωμα, το οποίο τυγχάνει αναγνώρισης σε Ενωσιακό επίπεδο, έτσι και το δικαίωμα προστασίας προσωπικών δεδομένων, υπόκειται σε περιορισμούς. Το άρθρο 13 της Οδηγίας προβλέπει επτά λόγους, για τους οποίους, ένα κράτος μέλος μπορεί να περιορίζει με νομοθετικά μέτρα την εμβέλεια των υποχρεώσεών του όσον αφορά στην υποχρέωση προστασίας των προσωπικών δεδομένων. Η γραμματική διατύπωση του άρθρου «εμβέλεια των υποχρεώσεων» φανερώνει, ότι οι περιορισμοί μπορούν να αφορούν, τόσο το αμυντικό όσο και το διεκδικητικό περιεχόμενο του δικαιώματος. Εφόσον όμως, η Οδηγία μιλάει για περιορισμό μονάχα της εμβέλειας των υποχρεώσεων των κρατών μελών, τούτο σημαίνει πως υπάρχει ένα κομμάτι των υποχρεώσεων αυτών που δεν δύνανται να περιοριστεί. Το κομμάτι αυτό ανήκει στο λεγόμενο «πυρήνα» του δικαιώματος.

Η Οδηγία αφήνει μεγάλο περιθώριο στα κράτη μέλη να εκτιμήσουν την αναγκαιότητα και την καταλληλότητα ενός περιορισμού και εναπόκειται προφανώς στο Δικαστήριο ή στις αρχές ελέγχου να κρίνουν κατά πόσο τηρήθηκε η αρχή της αναλογικότητας σε κάθε περίπτωση. Το σύστημα αυτό των περιορισμών εμφανίζει πολλά κοινά στοιχεία με το αντίστοιχο που ισχύει στο άρθρο 8 της ΕΣΔΑ.

Η Οδηγία 95/46/ΕΚ αφιερώνει το τέταρτο κεφάλαιό της στη ρύθμιση της διαβίβασης δεδομένων προσωπικού χαρακτήρα προς τρίτες χώρες και τις συναφείς υποχρεώσεις των κρατών μελών. Αναφέρθηκε πιο πάνω, ότι η ροή δεδομένων εντός

ζητήσει από την αντίστοιχη αρχή του κράτους μέλους του υπεύθυνου επεξεργασίας να την ασκήσει εκείνη.

των κρατών μελών της Ένωσης, είναι ελεύθερη. Η μεταφορά, όμως δεδομένων προς τρίτες χώρες επιτρέπεται μόνον εάν η τρίτη χώρα εξασφαλίζει[12] ικανοποιητικό επίπεδο προστασίας για τα μεταφερόμενα δεδομένα. Ωστόσο, υπάρχουν εξαιρέσεις από τον κανόνα του ικανοποιητικού επιπέδου προστασίας, περιπτώσεις δηλαδή στις οποίες η μεταφορά δεδομένων είναι δυνατή ακόμα και εάν δεν εξασφαλίζεται τέτοιο επίπεδο.

Μία από τις σημαντικότερες ρυθμίσεις της Οδηγίας 95/46/ΕΚ, αποτελεί και η επιβολή στα κράτη μέλη της υποχρέωσης, να προβλέπουν ότι μία ή περισσότερες δημόσιες αρχές, επιφορτίζονται με τον έλεγχο της εφαρμογής των επιμέρους εθνικών διατάξεων, που θεσπίζονται κατ' εφαρμογή της Οδηγίας. Οι αρχές αυτές, ονομάζονται στο κείμενο της Οδηγίας, ως αρχές ελέγχου. Οι αρχές αυτές, θα πρέπει να είναι εξοπλισμένες, τόσο με αρμοδιότητες ελέγχου όσο και με αρμοδιότητες παρέμβασης και εμπλοκής σε νομικές ενέργειες. Καθίστανται επιπλέον, υπεύθυνες να δέχονται παράπονα σχετικά με την προστασία δικαιωμάτων και ελευθεριών κατά την επεξεργασία προσωπικών δεδομένων. Για το καθεστώς των αρχών ελέγχου, η Οδηγία χρησιμοποιεί τον όρο «απόλυτη ανεξαρτησία».

Η συνολική επιρροή της Οδηγίας 95/46/ΕΚ στην εξέλιξη του δικαίου προστασίας των προσωπικών δεδομένων είναι αναμφίβολα πολύ σημαντική. Δεν είναι τυχαίο, ότι εφαρμόζεται απρόσκοπτα για παραπάνω από μια εικοσαετία, και ότι ακόμα και μετά την κατάργηση της, θα εξακολουθεί να παραμένει, το σημαντικότερο νομοθέτημα προστασίας προσωπικών δεδομένων στον ευρωπαϊκό χώρο.

1.2.2. Το πεδίο εφαρμογής και τα βασικά χαρακτηριστικά του Νόμου 2472/1997

Η κοινοτική Οδηγία για την προστασία των προσώπων έναντι της επεξεργασίας προσωπικών δεδομένων και την ελεύθερη κυκλοφορία των δεδομένων αυτών ενσωματώθηκε στην εσωτερική έννομη τάξη με τον Νόμο 2472/1997 για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Ο έλληνας νομοθέτης «εμπνεύστηκε» από την Οδηγία και προσανατολίστηκε στις ρυθμίσεις της, χωρίς να έχει προβεί σε αδιαμεσολάβητη «μεταφορά» των ρυθμίσεων στο εσωτερικό δίκαιο, όπως ίσως θα ανέμενε κανείς, με δεδομένη την απειρία και την έλλειψη συναφούς νομοθετικής παράδοσης. Όπου σημειώνονται αποκλίσεις από τις κοινοτικές ρυθμίσεις, αυτό έγινε, καθώς ο νομοθέτης αξιοποίησε την ευχέρειά που

[12] Αρμόδια, για την διαπίστωση του αν μια χώρα πληροί το κριτήριο της επαρκούς προστασίας των προσωπικών δεδομένων, είναι η Επιτροπή με τη διαδικασία της δεύτερης παραγράφου του άρθρου 31 της Οδηγίας.

του παρείχε η Οδηγία, να επιδιώξει ένα επίπεδο προστασίας, υψηλότερο αυτού που συγκροτούν οι κοινοτικές ρυθμίσεις.

Με τον νόμο αυτό ιδρύθηκε η Ανεξάρτητη Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, έργο της οποίας είναι η εποπτεία της εφαρμογής του Νόμου 2472/1997 και άλλων ρυθμίσεων που αφορούν την προστασία του πολίτη από την παράνομη επεξεργασία προσωπικών δεδομένων του και η ενάσκηση των αρμοδιοτήτων που της ανατίθενται από τους εκάστοτε σχετικούς νόμους.

Ο Νόμος 2472/1997 ορίζει τις προϋποθέσεις για την επεξεργασία δεδομένων προσωπικού χαρακτήρα, ιδίως ότι πρέπει αυτά να συλλέγονται κατά τρόπο θεμιτό και νόμιμο και να υφίστανται νόμιμη επεξεργασία, να είναι ακριβή και να ενημερώνονται, όταν χρειάζεται (άρθρ. 4 παρ. 1). Επίσης το υποκείμενο των δεδομένων θα πρέπει να έχει δώσει τη συγκατάθεσή του, εκτός αν συντρέχει μια από τις εξαιρέσεις που προβλέπονται στο νόμο (άρθρ. 5 παρ. 1). Αυστηρότερη προστασία επιβάλλεται, όταν πρόκειται για ευαίσθητα προσωπικά δεδομένα (άρθρ. 7).

Επίσης, καθιερώνεται δικαίωμα του υποκειμένου των δεδομένων, να ενημερώνεται με τρόπο πρόσφορο και σαφή για το σκοπό της επεξεργασίας, για τις κατηγορίες δεδομένων που πρόκειται να αποτελέσουν αντικείμενο επεξεργασίας, για τους αποδέκτες των δεδομένων αυτών και για τα στοιχεία του υπεύθυνου επεξεργασίας των δεδομένων. Ιδιαίτερη σημασία έχει και η καθιέρωση του δικαιώματος του υποκειμένου της επεξεργασίας να έχει πρόσβαση σε όλα τα δεδομένα προσωπικού χαρακτήρα που τον αφορούν και επίσης, να πληροφορείται την πηγή προέλευσης τους. Μάλιστα, μπορεί να ασκεί το δικαίωμα του αυτό και με τη συνδρομή προσώπου, που διαθέτει ειδικές γνώσεις. Τέλος, στο υποκείμενο της επεξεργασίας αναγνωρίζεται, αφενός μεν το δικαίωμα να προβάλει οποτεδήποτε αντιρρήσεις για την επεξεργασία των δεδομένων, που τον αφορούν, αφετέρου δε το δικαίωμα προσωρινής δικαστικής προστασίας. Το τελευταίο δικαίωμα μπορεί να το ασκήσει, όταν πρόκειται για πράξη ή απόφαση που τον θίγει, εφόσον η επεξεργασία αποβλέπει στην αξιολόγηση της προσωπικότητάς του και ιδίως της αποδοτικότητας του στην εργασία, της οικονομικής φερεγγυότητάς του, της αξιοπιστίας του και της εν γένει συμπεριφοράς του (άρθρ. 11 έως 14).

Για την περίπτωση παράβασης των υποχρεώσεων τους, οι υπεύθυνοι επεξεργασίας υπόκεινται σε ποινικές και διοικητικές κυρώσεις. Ο νόμος καθιερώνει και ευθύνη για αποζημίωση του προσώπου, που προκάλεσε περιουσιακή ή ηθική βλάβη στο υποκείμενο των προσωπικών δεδομένων (άρθρ. 21)[13].

[13] *Αλεξανδρίδου Ε.,* Το δίκαιο του ηλεκτρονικού εμπορίου, 2004, σελ. 190

1.3 Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (ΓΚΠΔ)

1.3.1 Γενικά

Το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο της Ευρωπαϊκής Ένωσης αποφάσισαν στις 27 Απριλίου 2016 την υιοθέτηση ενός νέου νομικού πλαισίου στην Ε.Ε. για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα. Το νομικό αυτό πλαίσιο αποτελείται από μια Οδηγία (2016/680) και έναν Κανονισμό. Αμφότερα τα νομοθετήματα, αποτελούν πραγματικές τομές, στην προστασία των προσωπικών δεδομένων σε Ενωσιακό επίπεδο, αλλά ο Κανονισμός 2016/679 ή Γενικός Κανονισμός για την Προστασία Δεδομένων (ΓΚΠΔ) απαριθμεί 99 άρθρα έναντι 34 της Οδηγίας και προβάλλει ως το πλέον βασικό ευρωπαϊκό κείμενο για την προστασία των προσωπικών δεδομένων στην Ε.Ε. Ο ΓΚΠΔ τέθηκε σε ισχύ στις 25 Μαΐου 2018.

1.3.2 Η επιλογή του Κανονισμού ως ρυθμιστικού εργαλείου

Η Επιτροπή πρότεινε ως νομοθετικό εργαλείο έναν Κανονισμό, εγκαταλείποντας την μέθοδο της προσαρμογής δια των Οδηγιών, διότι απέβλεπε στην συνεκτικότητα της ρύθμισης. Ο Κανονισμός αναμφίβολα οδηγεί σε μεγαλύτερο βαθμό εναρμόνισης, καθώς καθίσταται μέρος του εθνικού κανονιστικού συστήματος, χωρίς την ανάγκη υιοθέτησης εθνικών κανόνων, έχει άμεσο αποτέλεσμα, ανεξάρτητο από το εθνικό δίκαιο και υπερισχύει τυχόν αντίθετων εθνικών κανόνων. Η υιοθέτηση του μοντέλου του Κανονισμού, αποσκοπούσε στην απλούστευση των διαδικασιών αλλά και στη μείωση του «κόστους συμμόρφωσης», ιδίως για τις εταιρίες που δραστηριοποιούνται σε περισσότερες χώρες της Ε.Ε.

Η επιλογή αυτή δεν συνάντησε μόνο αποδοχή αλλά και επιφυλάξεις. Η επιλογή του Κανονισμού επικρίθηκε, καθώς η δεσμευτική ισχύς του, ερχόταν σε αντίθεση με τις εθνικές αντιλήψεις και προτιμήσεις αναφορικά με το επίπεδο προστασίας των προσωπικών δεδομένων. Οι επιφυλάξεις, αφορούσαν κυρίως, τον κίνδυνο πλήρους αποκλεισμού των εθνικών ρυθμίσεων, η οποία οδηγούσε σε μια αντίληψη «συγκεντρωτικής και μονοπωλιακής νομοθέτησης», καταργώντας μια βασική συνιστώσα του ενωσιακού δικαίου, ήτοι την αρχή της επικουρικότητας.

Οι αντιδράσεις περαιτέρω, οφείλονταν σε μεγάλο βαθμό και στο γεγονός, ότι η πρόταση του Κανονισμού, έδινε στην Ευρωπαϊκή Επιτροπή ευρύτατη κανονιστική αρμοδιότητα, ώστε να προσδιορίζει το ειδικότερο περιεχόμενο των ρυθμίσεων και των υποχρεώσεων. Στην ουσία οι αντιδράσεις είχαν προκύψει εκ του γεγονότος ότι «αναγνωρίζονταν» στην Επιτροπή να υιοθετεί πράξεις κατ' εξουσιοδότηση και εκτελεστικές πράξεις, μία αρμοδιότητα που ήταν ιδιαίτερα κρίσιμη. Το διακυβευόμενο

αγαθό άλλωστε αποτελούσε και αποτελεί ένα θεμελιώδες δικαίωμα, επομένως θεωρήθηκε, ότι ενέπιπτε στην αρμοδιότητα του νομοθέτη (Συμβούλιο και Κοινοβούλιο).

Πέραν των επιφυλάξεων για την ενίσχυση της κανονιστικής εξουσίας της Επιτροπής, μια ουσιαστική επιφύλαξη αφορούσε την δυνατότητα της Επιτροπής, να επεμβαίνει ακόμη και σε μεμονωμένες περιπτώσεις, καταστρατηγώντας τον ρόλο των εθνικών ανεξάρτητων αρχών. Η επιλογή του Κανονισμού, ως ρυθμιστικού εργαλείου, ώστε να εξασφαλίζεται «συνεκτικό και υψηλό επίπεδο προστασίας», «ισοδύναμο σε όλα τα κράτη μέλη» μέσω της «συνεκτικής και ομοιόμορφης εφαρμογής» επικράτησε εν τέλει, επιβεβαιώνοντας την κεντρική θέση που λαμβάνει το πεδίο της προστασίας προσωπικών δεδομένων μεταξύ των πολιτικών της Ε.Ε. και την μετάβαση από την εθνική στην ενωσιακή ρυθμιστική σφαίρα.

Ωστόσο, παρά τον συμβιβασμό αυτό και τη φύση του Κανονισμού, ο Γενικός Κανονισμός Προστασίας Δεδομένων, περιέχει αρκετές «ρήτρες ευελιξίας», αναγνωρίζοντας στα κράτη μέλη, την ευχέρεια να εξειδικεύσουν τους κανόνες του, συμπεριλαμβανομένων αυτών, που αφορούν την επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα, και να προσδιορίζουν τις περιστάσεις ειδικών καταστάσεων επεξεργασίας, μεταξύ άλλων τον ακριβέστερο καθορισμό των προϋποθέσεων, υπό τις οποίες η επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι σύννομη[14].

1.3.3 Οι βασικές απαιτήσεις του ΓΚΠΔ

Ο Γενικός Κανονισμός Προστασίας Δεδομένων επιβάλλει ένα ευρύ φάσμα απαιτήσεων σε εταιρείες που συλλέγουν ή επεξεργάζονται δεδομένα προσωπικού χαρακτήρα, συμπεριλαμβανομένης της απαίτησης συμμόρφωσης, με έξι βασικές αρχές:

1. Διαφάνεια, δικαιοσύνη και νομιμότητα στο χειρισμό και τη χρήση προσωπικών δεδομένων. Θα πρέπει να γίνεται σαφές στα άτομα, το πώς χρησιμοποιούνται τα προσωπικά τους δεδομένα και θα χρειαστεί επίσης μια "νόμιμη βάση" για την επεξεργασία αυτών των δεδομένων.
2. Περιορισμός της επεξεργασίας των προσωπικών δεδομένων σε καθορισμένους, σαφείς και νόμιμους σκοπούς. Δεν θα επιτρέπεται να επαναχρησιμοποιούνται ή να αποκαλύπτονται προσωπικά δεδομένα για σκοπούς που δεν είναι "συμβατοί" με το σκοπό για τον οποίο συλλέχθηκαν αρχικά τα δεδομένα.

[14] *Μήτρου Λ.*, Ο γενικός κανονισμός προστασίας προσωπικών δεδομένων, 2017, σελ. 33

3. Ελαχιστοποίηση της συλλογής και αποθήκευσης δεδομένων προσωπικού χαρακτήρα σε εκείνα που είναι επαρκή και σχετικά για τον επιδιωκόμενο σκοπό.
4. Εξασφάλιση της ακρίβειας των προσωπικών δεδομένων και της δυνατότητας διαγραφής ή διόρθωσης. Θα χρειαστεί η λήψη μέτρων για να βεβαιωθεί το άτομο, ότι τα προσωπικά του δεδομένα είναι ακριβή και μπορούν να διορθωθούν αν προκύψουν σφάλματα.
5. Περιορισμός της αποθήκευσης προσωπικών δεδομένων. Θα χρειαστεί η διασφάλιση, ότι διατηρούνται προσωπικά δεδομένα, μόνο για όσο διάστημα είναι απαραίτητο για την επίτευξη των σκοπών για τους οποίους συλλέχθηκαν τα δεδομένα.
6. Διασφάλιση της ασφάλειας, της ακεραιότητας και της εμπιστευτικότητας των προσωπικών δεδομένων. Η εταιρεία πρέπει να λάβει μέτρα για την ασφαλή φύλαξη των προσωπικών δεδομένων μέσω τεχνικών και οργανωτικών μέτρων ασφαλείας.

1.3.4 Τα δικαιώματα του υποκειμένου των δεδομένων

1.3.4.1 Το δικαίωμα ενημέρωσης

Το υποκείμενο των δεδομένων πρέπει να ενημερώνεται για την ύπαρξη της πράξης επεξεργασίας και τους σκοπούς της, καθώς η πληροφόρηση ήδη κατά την φάση της συλλογής, του δίνει τη δυνατότητα να εκτιμήσει την κατάσταση, να προσδιορίσει την πληροφοριακή συμπεριφορά του αλλά και να ασκήσει τα δικαιώματα που κατοχυρώνει ο νόμος[15]. Η ενημέρωση που είχε εισαχθεί με την Οδηγία 95/46/ΕΚ ως δικαίωμα «δεύτερης γενιάς»[16] είναι διατυπωμένη ταυτόχρονα ως δικαίωμα του υποκειμένου των δεδομένων και υποχρέωση του υπευθύνου επεξεργασίας. Η υποχρέωση ενημέρωσης υπάρχει, είτε οι σχετικές πληροφορίες προς επεξεργασία συλλέγονται από το ίδιο το υποκείμενο (άρθρο 13), είτε από άλλες πηγές (άρθρο 14). Ο Κανονισμός περιλαμβάνει σχετικά λεπτομερείς ρυθμίσεις για το εύρος της πληροφορίας που πρέπει να παρέχεται σε κάθε περίπτωση, ήτοι πληροφόρηση για την ταυτότητα του υπεύθυνου επεξεργασίας, τους σκοπούς και τη νομική βάση της επεξεργασίας, το χρονικό διάστημα τήρησης, τους αποδέκτες, την πρόθεση διασυνοριακής διαβίβασης καθώς και τα δικαιώματα του προσώπου.

---

[15] Ο ελληνικός νόμος (ν.2472/97) προέβλεπε ρητά την υποχρέωση ενημέρωσης του υποκειμένου πριν από τη διαβίβαση των δεδομένων του σε τρίτον (άρθρο 11 παρ. 3), ώστε το υποκείμενο των δεδομένων να είναι σε θέση να εκτιμήσει την βαρύτητα των χορηγούμενων προσωπικών του δεδομένων, να προετοιμάσει την άμυνά του και να ασκήσει τα δικαιώματά του.

[16] Δικαίωμα, το οποίο αγνοούσαν οι εθνικές νομοθεσίες ως την υιοθέτηση της Οδηγίας.

Άξιο αναφοράς είναι, ότι έχει ρητά εισαχθεί υποχρέωση ενημέρωσης και στην περίπτωση που τα δεδομένα, θα χρησιμοποιηθούν για άλλο σκοπό από εκείνον για τον οποίον συλλέχθηκαν. Ο Κανονισμός αναφέρεται με λεπτομέρειες και στο χρονικό σημείο και διάστημα εντός του οποίου, πρέπει να λαμβάνει χώρα η ενημέρωση αυτή[17].

Υφίστανται εξαιρέσεις ως προς το δικαίωμα ενημέρωσης, αυτές είναι: 1. όταν η παροχή τέτοιων πληροφοριών αποδεικνύεται αδύνατη ή συνεπάγεται δυσανάλογη προσπάθεια, 2. όταν η επεξεργασία αφορά σκοπούς αρχειοθέτησης ή επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς, 3. όταν η απόκτηση ή κοινοποίηση της πληροφορίας έχει ως έρεισμα διάταξη νόμου ή θα διακύβευε την εμπιστευτικότητα που επιβάλλεται από υποχρεώσεις τήρησης επαγγελματικού απορρήτου.

Η ευρύτητα των ανωτέρω εξαιρέσεων έχει ως φυσικό επακόλουθο τον κίνδυνο αποδυνάμωσης του δικαιώματος ενημέρωσης.

1.3.4.2 Το δικαίωμα πρόσβασης και αντίταξης

Η έγκαιρη και κατανοητή πληροφόρηση αποτελεί προϋπόθεση για την άσκηση του δικαιώματος πρόσβασης. Το δικαίωμα πρόσβασης καταλαμβάνει μια σημαντική θέση στο σύνολο των δικαιωμάτων, καθώς διασφαλίζει τη δυνατότητα ενός προσώπου να ζητά επιβεβαίωση για το κατά πόσον ή όχι τα δεδομένα προσωπικού χαρακτήρα, που το αφορούν, υφίστανται επεξεργασία και, εάν συμβαίνει αυτό, την πρόσβαση στα δεδομένα προσωπικού χαρακτήρα και σε πληροφορίες που αφορούν τους σκοπούς της επεξεργασίας, τις κατηγορίες των δεδομένων, τους αποδέκτες και σε λοιπά στοιχεία (άρθρο 15 ΓΚΠΔ)[18].

Το δικαίωμα πρόσβασης, θα ήταν ατελέσφορο, αν δεν συνοδευόταν από τα δικαιώματα διόρθωσης και διαγραφής των προσωπικών δεδομένων. Το δικαίωμα διόρθωσης, σύστοιχο της αρχής της ακρίβειας των προσωπικών δεδομένων (άρθρο 5 παρ. 1 δ), συνίσταται στο δικαίωμα διόρθωσης ανακριβών ή και συμπλήρωσης ελλιπών προσωπικών δεδομένων (άρθρο 16). Το πλέγμα των δικαιωμάτων, μέσω των οποίων ένα πρόσωπο, μπορεί να ασκήσει έλεγχο στην επεξεργασία των δεδομένων του, συμπληρώνεται με το δικαίωμα διαγραφής (άρθρο 17), του

[17] Στην περίπτωση συλλογής από το ίδιο το υποκείμενο το χρονικό σημείο της ενημέρωσης είναι η λήψη των σχετικών πληροφοριών, ενώ στην περίπτωση συλλογής από άλλες πηγές ο Κανονισμός αναφέρεται σε «εύλογη προθεσμία» από τη συλλογή, στην πρώτη «επικοινωνία με το υποκείμενο» ή στην «πρώτη κοινοποίηση» σε αποδέκτη δεδομένων.

[18] Ρητά προβλέπεται η υποχρέωση παροχής αντιγράφου, η οποία δεν αναγνωριζόταν υπό το προϊσχύσαν καθεστώς.

περιορισμού της επεξεργασίας (άρθρο 18), της φορητότητας (άρθρο 20), της εναντίωσης[19] (άρθρο 21) και της μη αυτοματοποιημένης λήψης απόφασης (άρθρο 22).

Ένα πρόσωπο δικαιούται να αντιτάσσεται ανά πάσα στιγμή στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που το αφορούν, η οποία επεξεργασία επιβάλλεται για λόγους είτε εκπλήρωσης δημοσίου συμφέροντος (άρθρο 6 παρ. 1 ε) είτε ικανοποίησης εννόμου συμφέροντος (άρθρο 6 παρ. 1 στ.). Ο υπεύθυνος επεξεργασίας φέρει το βάρος να αποδείξει την συνδρομή επιτακτικών και νόμιμων λόγων για την επεξεργασία, οι οποίοι υπερισχύουν των συμφερόντων, των δικαιωμάτων και των ελευθεριών του υποκειμένου των δεδομένων[20] .

Το δικαίωμα του περιορισμού της επεξεργασίας αντιστοιχεί σε ένα δικαίωμα «μερικής ή προσωρινής εναντίωσης», έχει ουσιαστικά τον χαρακτήρα των ασφαλιστικών μέτρων. Το υποκείμενο λοιπόν, μπορεί να παρεμβαίνει αναστέλλοντας την επεξεργασία των δεδομένων του, εάν εκκρεμεί η επαλήθευση της ακρίβειας αυτών ή και της ίδιας της νομιμότητας της επεξεργασίας. Ως προς το δικαίωμα αυτό υφίσταται το παράδοξο, το υποκείμενο των δεδομένων να έχει την δυνατότητα να ζητήσει την διατήρηση των δεδομένων, προκειμένου να τα χρησιμοποιήσει στην θεμελίωση, την άσκηση ή την υποστήριξη νομικών αξιώσεων.

1.3.4.3 Το δικαίωμα στη λήθη

Το δικαίωμα στη λήθη αποτελεί ένα νέο ψηφιακό δικαίωμα, το οποίο περιλαμβάνεται στο άρθρο 17 του ΓΚΠΔ. Η Viviane Reding, ωστόσο, πρώην Επίτροπος Δικαιοσύνης της Ε.Ε. και πρώην Αντιπρόεδρος της Επιτροπής έχει τονίσει, πως το δικαίωμα στη λήθη βασίζεται σε ήδη υπάρχοντες κανόνες και δεν αποτελεί δικαίωμα ex novo .

Το δικαίωμα στη λήθη αναγνωρίστηκε σε Ενωσιακό επίπεδο με την απόφαση της 13ης Μαΐου 2014 του Δικαστηρίου της Ε.Ε.. Η υπόθεση αυτή αφορούσε στις μηχανές αναζήτησης και την υποχρέωσή τους να αφαιρούν συνδέσμους προς ιστοσελίδες από τις λίστες των αποτελεσμάτων τους, έπειτα από αιτήματα των υποκειμένων των

[19] Τα δικαιώματα του περιορισμού και της εναντίωσης είχε υιοθετήσει τόσο η Οδηγία 95/46/ΕΚ στο άρθρο 14, όσο και η ελληνική νομοθεσία στο άρθρο 13 του ν. 2472/97.

[20] Η ρύθμιση του ν. 2472/97 σε αντίθεση με την κοινοτική Οδηγία 95/46/ΕΚ δεν απαιτούσε από τα πρόσωπα να επικαλεστούν νόμιμους και επιτακτικούς λόγους για να ασκήσουν το δικαίωμα αντίρρησης, ενώ σε περίπτωση μη ανταπόκρισης του υπεύθυνου επεξεργασίας μετέθετε ρητά στην Αρχή Προστασίας Προσωπικών Δεδομένων τη στάθμιση των αντιτιθέμενων δικαιωμάτων και συμφερόντων ως προς την επεξεργασία.

δεδομένων, με το επιχείρημα, ότι οι πληροφορίες αυτές δε θα πρέπει πλέον να συνδέονται με το όνομά τους μέσω ενός τέτοιου καταλόγου.

Πιο συγκεκριμένα, στις 5 Μαρτίου 2010 ο M. Costeja González, ισπανικής ιθαγένειας και κάτοικος Ισπανίας, υπέβαλε στην Ισπανική Αρχή Προστασίας Δεδομένων (εφεξής AEPD) καταγγελία κατά της La Vanguardia Ediciones SL, η οποία εκδίδει καθημερινή εφημερίδα μεγάλης κυκλοφορίας, καθώς και κατά της Google Spain και της Google Inc. Η καταγγελία αυτή υποβλήθηκε, επειδή όταν ένας χρήστης του διαδικτύου εισήγε το ονοματεπώνυμο του M. Costeja González στη μηχανή αναζήτησης της Google, εμφανίζονταν σύνδεσμοι προς δύο σελίδες της εφημερίδας La Vanguardia, στις οποίες περιλαμβανόταν ανακοίνωση, με μνεία του ονοματεπωνύμου του M. Costeja González, για πλειστηριασμούς ακινήτων κατόπιν κατάσχεσης που επιβλήθηκε λόγω κοινωνικοασφαλιστικών οφειλών[21].

Η AEPD απέρριψε την εν λόγω καταγγελία στις 30 Ιουλίου του ίδιου έτους κατά το μέρος που αφορούσε την La Vanguardia, εκτιμώντας ότι η εκ μέρους της δημοσίευση των επίμαχων πληροφοριών ήταν από νομικής άποψης δικαιολογημένη, την έκανε όμως δεκτή κατά το μέρος που αφορούσε την Google Spain και την Google Inc.

Η AEPD έκρινε, ότι οι φορείς εκμετάλλευσης μηχανών αναζήτησης, υπόκεινται στη νομοθεσία περί προστασίας των δεδομένων, δεδομένου ότι, προβαίνουν σε επεξεργασία δεδομένων για την οποία φέρουν ευθύνη και ότι ασκούν δραστηριότητες ενδιάμεσου στην κοινωνία της πληροφορίας.

Η Google Spain και η Google Inc. προσέβαλαν, καθεμία χωριστά, την εν λόγω απόφαση ενώπιον του Audiencia Nacional, το οποίο ανέστειλε την ενώπιόν του διαδικασία και υπέβαλε στο Δικαστήριο σειρά προδικαστικών ερωτημάτων, ως προς το κατά πόσον οι σχετικές διατάξεις της Οδηγίας, θα μπορούσαν να χρησιμεύσουν ως νομική βάση για τις αξιώσεις του M. Costeja González περί αφαίρεσης των προσωπικών του δεδομένων από τη λίστα αποτελεσμάτων αναζήτησης που πραγματοποιείται στο διαδίκτυο. Η επιρροή του Δικαστηρίου από την ήδη δημοσιευμένη τότε Πρόταση της Επιτροπής και τη σκοπούμενη κατοχύρωση του δικαιώματος στη λήθη και η επακόλουθη δέσμευσή του στη διαδικασία μεταρρύθμισης του νομικού πλαισίου για την προστασία δεδομένων είναι εμφανής και από το επιχείρημά του, ότι ακόμη και η αρχικώς νόμιμη επεξεργασία, μπορεί να καταστεί ασυμβίβαστη με την Οδηγία, σε περίπτωση που τα εν λόγω δεδομένα δεν είναι πλέον απαραίτητα σύμφωνα με τους σκοπούς για τους οποίους συλλέχθηκαν ή υπέστησαν επεξεργασία.

[21] Υπόθεση C-131/12, Google Spain κατά AEPD

Προσφεύγοντας δε και σε ρυθμίσεις του πρωτογενούς Ενωσιακού δικαίου, τόνισε ότι το δικαίωμα του υποκειμένου των δεδομένων να ζητά την αφαίρεση των πληροφοριών που το αφορούν από τα αποτελέσματα των μηχανών αναζήτησης βασίζεται στα άρθρα 7 και 8 του Χάρτη και τα ότι τα δικαιώματα αυτά παρακάμπτουν, όχι μόνο το οικονομικό συμφέρον του χειριστή της μηχανής αναζήτησης, αλλά και το ενδιαφέρον του ευρύτερου κοινού για την εξεύρεση πληροφοριών σχετικά με το υποκείμενο των δεδομένων. Εξαίρεση αποτελούν τα δημόσια πρόσωπα, καθώς η παρέμβαση στα θεμελιώδη δικαιώματά τους δικαιολογούνται από το επικρατέστερο ενδιαφέρον του ευρύτερου κοινού να έχει πρόσβαση στις εν λόγω πληροφορίες. Κάνοντας, τέλος, υπαγωγή των πραγματικών περιστατικών της κύριας δίκης στα αποτελέσματα της ερμηνευτικής του προσέγγισης, το Δικαστήριο έκρινε πως πράγματι θεμελιώνεται το δικαίωμα του υποκειμένου των δεδομένων να μη συνδέονται πλέον οι πληροφορίες αυτές με το όνομά του μέσω των αποτελεσμάτων αναζήτησης.

Οι μηχανές αναζήτησης έχουν συμμορφωθεί με την απόφαση του Δικαστηρίου και ανταποκρίνονται, πλέον, στα αιτήματα διαγραφής. Μετά την Google, τόσο η Bing όσο και η Yahoo έχουν δημοσιεύσει ηλεκτρονική αίτηση για διαγραφή. Ωστόσο, το ψηφιακό δικαίωμα στη λήθη δεν αφορά μόνο στην υποχρέωση των παρόχων μηχανών αναζήτησης να αφαιρούν συνδέσμους που αφορούν προσωπικά δεδομένα. Και αυτό, καθότι ενσαρκώνει στην ουσία, το αίτημα των ατόμων, να έχουν τη δυνατότητα να επιτυγχάνουν την αφαίρεση των προσωπικών τους δεδομένων, ιδίως εκείνων που έχουν δημοσιευθεί σε μέσα κοινωνικής δικτύωσης, εκτός εάν υπάρχει επιτακτικός λόγος για τη διατήρησή τους.

Στην πράξη, το δικαίωμα στη λήθη αφορά τη δυνατότητα αποτελεσματικής αντιμετώπισης των συνεπειών του Διαδικτύου που «δεν ξεχνά ποτέ», εξασφαλίζοντας την προσωπική αυτονομία του ατόμου και την προστασία της ιδιωτικής ζωής. Στον ψηφιακό κόσμο, το δικαίωμα αυτό παίρνει μια πιο ρεαλιστική μορφή: γίνεται αντιληπτό ως το αίτημα ενός ατόμου σε διαγραφή των δεδομένων που τον αφορούν και μπορεί κάλλιστα να αναδιατυπωθεί ως «δικαίωμα στη λήθη του κυβερνοχώρου» .

Παρά τη φιλοδοξία της Επιτροπής και τις προσδοκίες που καλλιεργήθηκαν η τελική αποτύπωση του δικαιώματος δεν συνιστά προφανώς μια «αλλαγή παραδείγματος» ως προς την προστασία των προσώπων. Το «δικαίωμα στη λήθη» αντιμετωπίζεται από αρκετούς περισσότερο ως μια επέκταση, μια επεξήγηση του δικαιώματος διαγραφής των δεδομένων. Πράγματι στον Κανονισμό εντάσσεται στο δικαίωμα διαγραφής (άρθρο 17) που ωστόσο φέρει ως –κατά τι αληθή εντός παρενθέσεως και εισαγωγικών – παράτιτλο «δικαίωμα στη λήθη».

Σύμφωνα με τη ρύθμιση, ο υπεύθυνος επεξεργασίας υποχρεούται να διαγράφει τα δεδομένα, εφόσον: α) στερούνται νόμιμης βάσης (ανάκληση συγκατάθεσης, παράνομη επεξεργασία, υπέρβαση αναγκαίου για τον σκοπό χρόνου τήρησης), β) η διαγραφή επιβάλλεται εκ του νόμου, γ) ασκείται λυσιτελώς το δικαίωμα εναντίωσης στην επεξεργασία, δ) πρόκειται για δεδομένα που είχαν συλλεχθεί σε σχέση με την προσφορά υπηρεσιών της κοινωνίας των πληροφοριών σε παιδί.

Το δικαίωμα διαγραφής δεν είναι απεριόριστο: οριοθετείται από την ύπαρξη νομικής υποχρέωσης προς επεξεργασία, το δημόσιο συμφέρον ή τα δικαιώματα ή (και) τα έννομα συμφέροντα άλλων προσώπων (ελευθερία έκφρασης, δικαίωμα ενημέρωσης, δικαίωμα στην έννομη προστασία) καθώς και για σκοπούς που αφορούν την επιστημονική ή ιστορική έρευνα που επιβάλλουν την διατήρηση των δεδομένων και την απόρριψη του αιτήματος διαγραφής.

Μία ειδοποιός διαφορά του δικαιώματος έναντι των άλλων δικαιωμάτων (εναντίωση, περιορισμός) εντοπίζεται στην αναδρομικότητά του. Η διαγραφή αλλάζει εν τέλει την έκταση της επεξεργασίας, ακόμη κι αν αυτή είχε πραγματοποιηθεί σύννομα στο παρελθόν.

1.3.4.4 Το δικαίωμα στη φορητότητα

Το δικαίωμα στη φορητότητα αποτελεί καινοτομία του Κανονισμού και συνίσταται σε δύο βασικές πτυχές: το δικαίωμα του προσώπου να λαμβάνει δεδομένα που έχει παράσχει σε υπεύθυνο επεξεργασίας και το δικαίωμα να διαβιβάζει τα δεδομένα του σε άλλο υπεύθυνο επεξεργασίας, χωρίς να εμποδίζεται σε αυτό από τον υπεύθυνο επεξεργασίας, στον οποίο αρχικά παρασχέθηκαν (άρθρο 20).

Η Επιτροπή φιλοδοξούσε να καταστήσει δυνατή την ευχερή «μετακίνηση» δεδομένων από πάροχο σε πάροχο, κυρίως με αναφορά τα ψηφιακά κοινωνικά δίκτυα[22]. Χαρακτηριστικό παράδειγμα, είναι η παροχή στον χρήστη υπηρεσιών κοινωνικής δικτύωσης, όπως το Facebook, του δικαιώματος αλλά και της δυνατότητας, αφενός να ελέγχει όλες τις πληροφορίες που έχει αναρτήσει στη συγκεκριμένη πλατφόρμα και αφετέρου να ζητήσει τη μεταφορά τους σε άλλη πλατφόρμα.

Η Επιτροπή επιδίωκε να αντιμετωπίσει το λεγόμενο lock – in των χρηστών και κατ΄ αποτέλεσμα να αυξήσει τον ανταγωνισμό μεταξύ των παρόχων κοινωνικών δικτύων.

[22]Όπως αναφέρεται στην οικεία έκθεση αποτίμησης συνεπειών, τα προσωπικά δεδομένα τα οποία μπορούν να μεταφέρονται μπορούν να είναι φωτογραφίες, λίστες «φίλων», πληροφορίες επαφών, ημερολόγιο , διαπροσωπικές επικοινωνίες ή άλλα είδη προσωπικά ή κοινωνικά σημαντικών δεδομένων.

Η εισαγωγή του δικαιώματος αντιμετωπίστηκε με επιφύλαξη, διότι προσιδίαζε περισσότερο στο δίκαιο του ανταγωνισμού και στο δίκαιο του καταναλωτή.

Το δικαίωμα αυτό εφαρμόζεται σε κάθε υπεύθυνο επεξεργασίας που επεξεργάζεται προσωπικά δεδομένα με ηλεκτρονικά μέσα, αποκλείοντας από το πεδίο εφαρμογής του δικαιώματος τα έντυπα και έγχαρτα αρχεία. Γίνεται μάλιστα δεκτό, ότι εφαρμόζεται και στην περίπτωση των παρόχων υπηρεσιών υπολογιστικού νέφους.

Παρόλο, που το δικαίωμα φορητότητας προβλέφθηκε προκειμένου να ενισχύσει την θέση του υποκειμένου, το πεδίο εφαρμογής του είναι ιδιαίτερα στενό και περιορίζεται στις περιπτώσεις που η επεξεργασία θεμελιώνεται στη συγκατάθεση του προσώπου ή σε μια συμβατική σχέση με αυτό. Περαιτέρω το δικαίωμα περιορίζεται στα δεδομένα που έχει παράσχει το ίδιο το πρόσωπο και δεν επεκτείνεται σε αυτά που παράγονται από τον πάροχο για το πρόσωπο. Η άσκηση του δικαιώματος φορητότητας δεν θα πρέπει να επηρεάζει τα δικαιώματα και τις ελευθερίες τρίτων[23].

Όσον αφορά την απευθείας διαβίβαση μεταξύ παρόχων, η εφαρμογή της εξαρτάται εν τέλει από το εάν είναι τεχνικά εφικτή (άρθρο 20 παρ. 2)[24].

1.3.5 Ο Υπεύθυνος Προστασίας (Data Protection Officer)

Με το άρθρο 37 του ΓΚΠΔ καθιερώνεται στο πλαίσιο προστασίας δεδομένων στο Ενωσιακό δίκαιο, ο θεσμός του Υπεύθυνου Προστασίας. Ο Υπεύθυνος Προστασίας αναμένεται να αποτελέσει θεμέλιο λίθο του συστήματος επιμερισμού της ευθύνης, που θεσπίζει ο ΓΚΠΔ. Αν και η προσωπική ευθύνη του Υπεύθυνου Προστασίας για οποιαδήποτε μη συμμόρφωση αποκλείεται εξαρχής, η παρουσία του σε συνδυασμό με τον αυξημένο βαθμό αυτονομίας, που εκ νόμου απαιτείται να απολαμβάνει, σκοπούν στην εξασφάλιση, ότι ο Υπεύθυνος και ο Εκτελών την επεξεργασία έχουν επαρκή και εξειδικευμένη βοήθεια στο έργο που καλούνται να επιτελέσουν.

Σύμφωνα με τα προβλεπόμενα στο άρθρο 37 ο διορισμός Υπευθύνου Προστασίας[25] είναι υποχρεωτικός σε τρεις περιπτώσεις: α) στην περίπτωση που η

[23]Τα δικαιώματα πνευματικής ιδιοκτησίας ή τα εταιρικά απόρρητα, θα πρέπει να ερμηνεύονται στενά και η επίκλησή τους να μην γίνεται προσχηματικά.

[24] Κρίσιμο στοιχείο είναι η διασφάλιση της διαλειτουργικότητας, καθώς ελλείψει αυτής είναι αναμφίβολο, εάν εν τοις πράγμασι μπορεί να βρει εφαρμογή το δικαίωμα της φορητότητας.

[25] Στη Γερμανία, σύμφωνα με το άρθρο 4στ, παράγραφος 1 του γερμανικού ομοσπονδιακού νόμου για την προστασία των προσωπικών δεδομένων (Bundesdatenschutzgesetz), οι εταιρίες του ιδιωτικού τομέα υποχρεούνται να διορίζουν εσωτερικό υπεύθυνο για την προστασία των προσωπικών δεδομένων, εφόσον απασχολούν μόνιμα τουλάχιστον 10 εργαζομένους για την αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων.

επεξεργασία διενεργείται από δημόσια αρχή ή φορέα, (β) στην περίπτωση που οι βασικές (core) δραστηριότητες επεξεργασίας προσωπικών δεδομένων, απαιτούν τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε μεγάλη κλίμακα ή (γ) όταν απαιτούν μεγάλης κλίμακας επεξεργασία κατηγοριών ευαίσθητων δεδομένων (άρθρα 9 και 10 ΓΚΠΔ). Η πρώτη κατηγορία είναι περισσότερο ξεκάθαρη[26], αλλά οι άλλες δύο απαιτούν μια κάποια διασάφηση. Συναφώς, ως βασικές δραστηριότητες (core activities) μπορούν να χαρακτηριστούν εκείνες, στις οποίες λαμβάνει χώρα συλλογή και επεξεργασία δεδομένων, που καταλήγει στη δημιουργία σχετικού αρχείου, όπως για παράδειγμα, συμβαίνει σε ένα νοσοκομείο ή μια εταιρεία παροχής υπηρεσιών ασφάλειας. Αντίστοιχα, ως δραστηριότητες μεγάλης κλίμακας, μπορούν να χαρακτηριστούν οι περιπτώσεις διαδικτυακής επεξεργασίας, με σκοπό την εμπορική προώθηση, οι τραπεζικές και οι ασφαλιστικές δραστηριότητες. Ένα σημείο που χρήζει διευκρίνισης είναι το συνδετικό «και» στην τρίτη κατηγορία (υπό (γ)).

Σημειώνεται εδώ, ότι η υποχρέωση διορισμού Υπεύθυνου Προστασίας δεν υφίσταται στην περίπτωση σωρευτικής επεξεργασίας τόσο ειδικών κατηγοριών προσωπικών δεδομένων (άρθρο 9) όσο και δεδομένων που αφορούν ποινικές καταδίκες (άρθρο 10). Η δικαιοπολιτικά ορθή ερμηνεία του ΓΚΠΔ επιβάλλει να θεωρήσουμε, πως η υποχρέωση διορισμού Υπεύθυνου Προστασίας, υφίσταται σε οποιαδήποτε από τις δύο περιπτώσεις επεξεργασίας. Η γενικότερη κατεύθυνση, την οποία ακολουθεί η Ομάδα Εργασίας του άρθρου 29, υποστηρίζει το διορισμό Υπεύθυνου Προστασίας σε όλες τις περιπτώσεις, πέρα από εκείνες στις οποίες είναι ξεκάθαρο, ότι δεν απαιτείται. Ωστόσο, ο διορισμός του, ακόμα και αν είναι προαιρετικός, επισύρει όλες τις υποχρεώσεις που προβλέπονται στα άρθρα 37-39.

Σε κάθε περίπτωση, η επιλογή για μη διορισμό Υπεύθυνου Προστασίας, πρέπει να αιτιολογείται επαρκώς και εγγράφως σύμφωνα με την αρχή της λογοδοσίας. Το άρθρο 37 εφαρμόζεται τόσο για τους Υπεύθυνους Επεξεργασίας όσο και τους Εκτελούντες την επεξεργασία. Αυτό σημαίνει, ότι η υποχρέωση για διορισμό

[26] Η Ομάδα Εργασίας του άρθρου 29 θεωρεί πως το τι θεωρείται δημόσια αρχή ή φορέας πρέπει να ερμηνευθεί υπό το πρίσμα του εθνικού δικαίου. Η άποψη αυτή είναι μάλλον επιφυλακτική. Αν λάβουμε υπόψη το γεγονός, ότι η ερμηνεία της έννοιας του δημόσιου οργανισμού έχει εναρμονιστεί σημαντικά, ιδίως στον τομέα των δημοσίων συμβάσεων και ότι ο διορισμός Υπεύθυνου Προστασίας δρα προστατευτικά για το υπό εξέταση δικαίωμα, θα ήταν νομικά λυσιτελές να υιοθετήσουμε Ενωσιακή, ευρύτερη ερμηνεία για την έννοια του δημόσιου φορέα. Σε κάθε περίπτωση και σύμφωνα με το άρθρο 6 του ΓΚΠΔ η αυτονομία των κρατών μελών να θεσπίζουν ειδικότερες ρυθμίσεις είναι ελεύθερη, στο μέτρο που οι ρυθμίσεις αυτές είναι πιο εξειδικευμένες από όσα ορίζονται στον Κανονισμό.

Υπεύθυνου Επεξεργασίας, μπορεί να βαρύνει αμφότερους ή τον έναν από τους δύο. Ο Υπεύθυνος Προστασίας, απολαμβάνει μιας ιδιότυπης ασυλίας, έναντι των κυρώσεων του ΓΚΠΔ, ωστόσο μπορεί να ευθύνεται αστικά έναντι του Υπεύθυνου ή του Εκτελούντα την επεξεργασία για τυχόν παροχή εσφαλμένων συμβουλών. Πάντως, χαίρει λειτουργικής και οικονομικής ανεξαρτησίας, αυτονομίας και ασυλίας. Υποχρεούται να έχει ως προτεραιότητα τα καθήκοντα του Υπευθύνου Προστασίας .

Τα στοιχεία επικοινωνίας με τον Υπεύθυνο Επεξεργασίας, πρέπει να είναι διαθέσιμα, τόσο στα υποκείμενα των δεδομένων, για να διευκολύνεται η ενάσκηση των δικαιωμάτων τους, ιδίως των δικαιωμάτων διόρθωσης, φορητότητας, πρόσβασης και διαγραφής, όσο και στην επιβλέπουσα αρχή ώστε να καθίσταται δυνατή η συνεργασία μαζί του.

Τα επαγγελματικά/τυπικά προσόντα του Υπεύθυνου Προστασίας δε διευκρινίζονται επαρκώς στον Κανονισμό, ωστόσο είναι δεδομένο, πως θα πρέπει να έχει μεγάλη εμπειρία στο δίκαιο προσωπικών δεδομένων και εξαιρετικές επικοινωνιακές και οργανωτικές δεξιότητες, ειδικά στην περίπτωση μεγάλων επιχειρήσεων των οποίων διάφορα τμήματα θα πρέπει να συνεργαστούν[27]. Παρόλα αυτά, η Ελληνική Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα έχει ισχυριστεί, πως ο ΓΚΠΔ δε θέτει κάποια υποχρεωτική απαίτηση για προηγούμενη πιστοποίηση του Υπεύθυνου Προστασίας. Στην ίδια κατεύθυνση, κινήθηκε και η Βελγική Αρχή με την υπ' αριθ. 4/2017 γνωμοδότησή της. Αντιθέτως η Ισπανική Αρχή υιοθέτησε ορισμένες κατευθυντήριες γραμμές που θα πρέπει να διέπουν το σύστημα πιστοποίησης προσώπων ως Υπεύθυνων Προστασίας.

Η θέση του Υπεύθυνου Επεξεργασίας μέσα στην επιχείρηση έχει δημιουργήσει ζητήματα. Ο διορισμός κάποιου ήδη υπάρχοντα υπαλλήλου ως υπεύθυνου Προστασίας καταρχήν δεν απαγορεύεται. Ωστόσο, για να μην υπάρχει ζήτημα σύγκρουσης συμφερόντων, δε μπορεί να διοριστεί Υπεύθυνος Επεξεργασίας ο νομικός σύμβουλος της επιχείρησης που παρέχει τις υπηρεσίες του in house ή υπάλληλος τμήματος που αποτελεί τον υπεύθυνο ή τον εκτελούντα την επεξεργασία δεδομένων[28]. Αξίζει να σημειωθεί και το ότι, σε περίπτωση που οι υπηρεσίες Υπευθύνου Επεξεργασίας παρέχονται οργανωμένα από κάποια εταιρεία ως εξωτερικού παρόχου, οι Υπεύθυνοι Προστασίας, θα πρέπει να μην έχουν πρόσβαση

[27] *Γιαννακάκης Ι.*, Ο ρόλος και οι ευθύνες του Data Protection Officer, http://www.cyberinsurancequote.gr/insurance/nomothesia/

[28] Έτσι ο Δ. Ζωγραφόπουλος στην εισήγησή του στο «Προστασία Δεδομένων Προσωπικού Χαρακτήρα – Οι προκλήσεις του Κανονισμού (Ε.Ε.) 2016/679 – Γενικός Κανονισμός για την Προστασία Δεδομένων –GDPR» στη Νομική Βιβλιοθήκη.

στο έργο των συναδέλφων τους και να μην αναλαμβάνουν θέση Υπεύθυνου Επεξεργασίας σε επιχειρήσεις ανταγωνιστές.

Εν κατακλείδι, ο ρόλος του Υπεύθυνου Επεξεργασίας αναδεικνύεται μέσα από τη συμμετοχή που, δυνάμει της παραγράφου 1 του άρθρου 39, καλείται να έχει στην τήρηση του αρχείου επεξεργασίας του άρθρου 30. Σύμφωνα με το τελευταίο, ο υπεύθυνος επεξεργασίας έχει την υποχρέωση να τηρεί αρχείο καταγραφής όλων των επεξεργασιών για τις οποίες είναι υπεύθυνος, τίποτα όμως δεν τον εμποδίζει να αναθέτει στον Υπεύθυνο Προστασίας την καταγραφή αυτή. Φυσικά, ο τελικώς υπεύθυνος είναι ο υπεύθυνος επεξεργασίας.

Σύμφωνα με την άποψη της Ομάδας Εργασίας του άρθρου 29, το ίδιο ισχύει mutatis mutandis και κατά την κατάρτιση της αξιολόγησης επίπτωσης στα προσωπικά δεδομένα (data protection impact assessment, DPIA). Όπως ορθά παρατηρεί και ο Αλ. Νούσιας : *«η συμμόρφωση με τον Κανονισμό είναι η μία όψη του νομίσματος. Η άλλη αφορά στη σωστή ανάγνωση των δεδομένων, προκειμένου μέσα από αυτή να εντοπιστεί το σημείο που συναντώνται η τεχνολογία, η κοινωνία και η αγορά. Ο ρόλος του Υπεύθυνου Προστασίας είναι η παροχή βοήθειας στους διαφόρους οργανισμούς- υπεύθυνους επεξεργασίας να εντοπίσουν το σημείο αυτό.»*

1.3.6 Η υποχρέωση λογοδοσίας του υπεύθυνου επεξεργασίας δεδομένων

Μία κομβική επιλογή του Κανονισμού είναι η υιοθέτηση της αρχής της λογοδοσίας. Ο Κανονισμός εντάσσει τη λογοδοσία στη ρύθμιση που αφορά τις αρχές που διέπουν την επεξεργασία προσωπικών δεδομένων αλλά κυρίως προσδίδει σε αυτήν τη λειτουργία ενός μηχανισμού εγγύησης της τήρησής τους, σύμφωνα με το άρθρο 5 παρ. 2, ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και είναι σε θέση να αποδείξει τη συμμόρφωση με τις αρχές της προστασίας προσωπικών δεδομένων, όπως κατοχυρώνονται στην πρώτη παράγραφο του άρθρου[29].

Η αρχή αυτή είχε συμπεριληφθεί και στις Κατευθυντήριες Αρχές του ΟΟΣΑ και η ένταξή της στο νέο πλαίσιο του Κανονισμού έγινε προκειμένου να ενισχυθεί ο ρόλος του υπεύθυνου επεξεργασίας και να αυξηθεί η ευθύνη του. Η αρχή αυτή συνδέθηκε με τον περιορισμό των διοικητικών διατυπώσεων, ερμηνεύτηκε μάλιστα ως αντιστάθμισμα κατάργησης αυτών. Η λογοδοσία έχει πολλές διαστάσεις και γίνεται αντιληπτή διαφορετικά από διαφορετικούς ανθρώπους. Η λογοδοσία σχετίζεται περισσότερο με την υποχρέωση να αιτιολογεί κανείς τη συμπεριφορά ή τις ενέργειές

[29] Δηλαδή τη «νομιμότητα, αντικειμενικότητα και διαφάνεια», τον περιορισμό του σκοπού», την «ελαχιστοποίηση των δεδομένων», την «ακρίβεια», το «περιορισμό του χρόνου τήρησης» και την «ακεραιότητα και εμπιστευτικότητα».

του. Λόγω της πολυπλοκότητας και της πολυσημίας του όρου η Ομάδα του άρθρου 29 επιχείρησε να προσδιορίσει τη σημασία του, επισημαίνοντας ότι ο «όρος δίνει έμφαση στην παρουσίαση του τρόπου με τον οποίο ασκείται η ευθύνη και στη δυνατότητα σχετικής επαλήθευσης».Η λογοδοσία εισάγεται ως μια γενική υποχρέωση του υπεύθυνου να επιδεικνύει συμμόρφωση. Ο υπεύθυνος επεξεργασίας έχει το βάρος να αποδείξει, ότι πράγματι επιδεικνύει συμμόρφωση. Ο Κανονισμός προβλέπει ρητά, ότι ο υπεύθυνος επεξεργασίας, έχει το βάρος να αποδείξει μόνο, ότι υφίσταται συγκατάθεση του υποκειμένου για επεξεργασία των προσωπικών του δεδομένων.

Στο άρθρο 24 παρ. 1 του Κανονισμού διατυπώνεται ως στοιχείο «ευθύνης» του υπεύθυνου επεξεργασίας η υποχρέωση να εφαρμόζει τα κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζει και να μπορεί να αποδεικνύει, ότι η επεξεργασία διενεργείται σύμφωνα με τον Κανονισμό». Τα μέτρα οργάνωσης και επίδειξης συμμόρφωσης περιλαμβάνουν:

1.την εκτίμηση αντίκτυπου της επεξεργασίας,

2.την προηγούμενη διαβούλευση,

3.την εφαρμογή μέτρων ασφαλείας,

4.την υιοθέτηση κωδίκων δεοντολογίας και μηχανισμών πιστοποίησης,

5.τον ορισμό (εσωτερικού) υπεύθυνου προστασίας δεδομένων,

6.την τήρηση αρχείων επεξεργασίας,

7.την τήρηση υποχρεώσεων κοινοποίησης της παραβίασης δεδομένων.

1.3.7 Οι περιορισμοί του δικαιώματος προστασίας προσωπικών δεδομένων

Το δικαίωμα προστασίας των προσωπικών δεδομένων επιδέχεται περιορισμούς . Η ρύθμιση του άρθρου 23 είναι ενδεικτική. Ο περιοριστικός κατάλογος των δυνητικών εξαιρέσεων είναι μάλιστα ευρύτερος του αντίστοιχου καταλόγου του άρθρου 13 της Οδηγίας 95/46/ΕΚ, καθώς ως λόγους εξαίρεσης, προβλέπει τη διασφάλιση της ασφάλειας του κράτους, της εθνικής άμυνας, της δημόσιας ασφάλειας, της πρόληψης, της διερεύνησης, της ανίχνευσης ή της δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων, άλλων σημαντικών στόχων γενικού δημοσίου συμφέροντος της Ένωσης ή κράτους μέλους, ιδίως σημαντικού οικονομικού ή χρηματοοικονομικού συμφέροντος της Ένωσης ή κράτους μέλους, συμπεριλαμβανομένων των νομισματικών, δημοσιονομικών και φορολογικών θεμάτων, της δημόσιας υγείας και της κοινωνικής ασφάλισης, της προστασίας της ανεξαρτησίας της δικαιοσύνης και των δικαστικών διαδικασιών, της πρόληψης, της διερεύνησης, της ανίχνευσης και της δίωξης παραβάσεων δεοντολογίας σε νομοθετικά κατοχυρωμένα επαγγέλματα, της παρακολούθησης, της επιθεώρησης ή

της κανονιστικής λειτουργίας που συνδέεται, έστω περιστασιακά, με την άσκηση δημόσιας εξουσίας, της προστασίας του υποκειμένου των δεδομένων ή των δικαιωμάτων και των ελεύθερων τρίτων και τέλος της εκτέλεσης αστικών αξιώσεων.

Ο ενωσιακός νομοθέτης εξισορροπεί την ευρύτητα του καταλόγου και την αοριστία ορισμένων διατυπώσεων με την επιταγή να εισάγεται η εξαίρεση με νομοθετικό μέτρο[30].

1.3.8 Το κυρωτικό οπλοστάσιο του Κανονισμού

Βασικός πυλώνας του συστήματος προστασίας προσωπικών δεδομένων είναι οι κυρώσεις. Η πρόβλεψη και η πιθανότητα επιβολής κυρώσεων αναπτύσσουν αναμφίβολα, μια αποτρεπτική λειτουργία. Η συνεκτικότητα και η αποτελεσματικότητα της προστασίας των προσωπικών δεδομένων συνδέεται άμεσα με την δυνατότητα επιβολής «ισοδύναμων κυρώσεων».Η κανονιστική παρέμβαση στο ζήτημα των κυρώσεων και ιδίως η ρύθμιση αναφορικά με τα πρόστιμα, είναι μια από τις πλέον εμφανείς αλλαγές που επήλθαν στο προηγούμενο νομικό καθεστώς[31].

Το καθεστώς των κυρώσεων ρυθμιζόταν στην Οδηγία 95/46/ΕΚ κατά τρόπο ιδιαζόντως γενικό, πιο συγκεκριμένα όριζε ότι «οι εθνικοί νομοθέτες όφειλαν να λάβουν τα κατάλληλα μέτρα για να εξασφαλίσουν την πλήρη εφαρμογή των διατάξεων της Οδηγίας και να προβλέπουν ιδίως κυρώσεις για παράβαση των διατάξεων εφαρμογής της». Η ρύθμιση ήταν γενική και κατέλειπε ευρεία διακριτική ευχέρεια στα κράτη μέλη για την επιλογή της φύσης και της έντασης των κυρώσεων. Η ενσωμάτωση των αόριστων επιταγών της κοινοτικής νομοθεσίας στην εθνική έννομη τάξη είχε ως αποτέλεσμα αξιοσημείωτες διαφορές και αποκλίσεις μεταξύ των

[30] Δέσμευση που περιλαμβανόταν ήδη στο άρθρο 13 της Οδηγίας 95/46/ΕΚ, χωρίς ωστόσο να προσδιορίζεται εγγύτερα το είδος των μέτρων.

[31] Στην υπόθεση Von Colson και Kamann κατά Land NordrheinWestfalen, το ΔΕΕ επεσήμανε ότι όλα τα κράτη μέλη προς τα οποία απευθυνόταν η Οδηγία υποχρεούνταν να θεσπίσουν στην εθνική έννομη τάξη τους κάθε αναγκαίο μέτρο ώστε να διασφαλίζεται η πλήρης εφαρμογή της, σύμφωνα με τον επιδιωκόμενο στόχο. Το Δικαστήριο έκρινε ότι, αν και εναπόκειται στα κράτη μέλη να επιλέξουν τους τρόπους και τα μέσα που θα διασφαλίσουν την εφαρμογή της Οδηγίας, η ελευθερία αυτή αναιρεί την υποχρέωση που τους επιβάλλεται. Ειδικότερα, το αποτελεσματικό ένδικο μέσο πρέπει να δίνει στο πρόσωπο τη δυνατότητα να διεκδικεί και να ασκεί το εν λόγω δικαίωμα στην πλήρη έκταση του περιεχομένου του. Για την επίτευξη πραγματικής και ουσιαστικής προστασίας, τα ένδικα μέσα πρέπει να κινούν ποινικές διαδικασίες και/ή διαδικασίες αποζημίωσης, οι οποίες θα οδηγούν στην επιβολή αποτρεπτικών κυρώσεων.

κρατών μελών. Σε ορισμένες χώρες δόθηκε έμφαση στις διοικητικές κυρώσεις[32], σε άλλες προβλέφθηκαν ποινικές παραβάσεις.

Υπό τον Κανονισμό οι ρυθμίσεις αναφορικά με τις κυρώσεις υπερβαίνουν ουσιαστικά αυτές του προηγούμενου νομικού καθεστώτος, υφίσταται επίσης λεπτομερή παράθεση της κλίμακας των προστίμων που επιβάλλονται. Ο ΓΚΠΔ εισάγει περισσότερους και σημαντικά λεπτομερέστερους κανόνες για την αντιμετώπιση των παραβάσεων του νόμου αλλά και την εναρμόνιση της αντίστοιχης αντιμετώπισης από τα κράτη μέλη. Εναρμόνιση, η οποία επιτυγχάνεται με τον περιορισμό της κανονιστικής ευχέρειας του εθνικού νομοθέτη αλλά και με την επιβεβαίωση του κομβικού ρόλου των ανεξάρτητων αρχών στην εφαρμογή του νόμου.

Ο Κανονισμός εντάσσει τις κυρώσεις σε ένα πλέγμα κανόνων προς επιβολή της συμμόρφωσης, στο οποίο συμπεριλαμβάνονται και οι λεγόμενες «διορθωτικές εξουσίες» των ανεξάρτητων αρχών. Οι κυρώσεις θα πρέπει να επιβάλλονται «επιπρόσθετα ή αντί των κατάλληλων μέτρων που επιβάλλονται από την εποπτική αρχή». Η ρύθμιση είναι εξαντλητικά λεπτομερής αναφορικά με την επιβολή των διοικητικών προστίμων, ενώ ως προς τις άλλες κυρώσεις ο ενωσιακός νομοθέτης παραπέμπει στην εθνική ρύθμιση (άρθρο 84).

Τα διοικητικά πρόστιμα συνιστούν το ισχυρότερο κυρωτικό εργαλείο του Κανονισμού. Οι ρυθμίσεις του άρθρου 83 επιβάλλουν δεσμευτικά τόσο το ύψος των προστίμων όσο και το πεδίο των παραβάσεων για τις οποίες αυτά επιβάλλονται. Ο Κανονισμός προσδιορίζει επακριβώς τις ρυθμίσεις, η παράβαση των οποίων επισύρει διοικητικά πρόστιμα: 1. έως δέκα εκατομμύρια ευρώ ή σε περίπτωση επιχειρήσεων, έως το 2% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους και 2. πρόστιμα έως είκοσι εκατομμύρια ευρώ ή σε περίπτωση επιχειρήσεων, έως το 4% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους. Σε αμφότερες τις περιπτώσεις, ο Κανονισμός προβλέπει ότι επιβάλλεται το κάθε φορά υψηλότερο ποσό. Άξιο αναφοράς είναι ότι το υψηλότερο ποσό επιβάλλεται και σε περίπτωση παρεμπόδισης της άσκησης των ελεγκτικών εξουσιών της εποπτικής αρχής ή και μη συμμόρφωσης προς τις εντολές της.

Ο ενωσιακός νομοθέτης όρισε το ανώτατο ύψος αλλά ανέθεσε στις εποπτικές αρχές τη μέριμνα, ώστε η επιβολή διοικητικών προστίμων να είναι για κάθε μεμονωμένη περίπτωση αποτελεσματική, αναλογική και αποτρεπτική (άρθρο 83

[32] Σημαντικές διαφοροποιήσεις είχαν καταγραφεί αναφορικά με τις διοικητικές κυρώσεις που προβλέπονταν στα διάφορα κράτη μέλη, όπως π.χ. σε σχέση με το ύψος των προστίμων.

παρ. 1). Η ευχέρεια που παρέχεται στις εποπτικές αρχές είναι ευρεία, γι' αυτό αυτή πρέπει να ασκείται αφενός υπό τους όρους της αναλογικότητας και αφετέρου επί τη βάσει των συγκεκριμένων κριτηρίων που παραθέτει ο Κανονισμός (άρθρο 83 παρ. 2).

Κρίσιμα στοιχεία είναι η φύση, η βαρύτητα και η διάρκεια της παράβασης, λαμβανομένων υπόψη της φύσης, της έκτασης ή του σκοπού της επεξεργασίας, του αριθμού των θιγόμενων προσώπων και του βαθμού ζημίας των υποκειμένων των δεδομένων που έθιξε η παράβαση και τον βαθμό ζημίας που υπέστησαν καθώς επίσης και η κατηγορία των δεδομένων που επηρεάζονται από την παράβαση. Σημαντικοί παράγοντες για τον προσδιορισμό του ύψους του προστίμου αφορούν την ύπαρξη δόλου ή αμέλειας, τον βαθμό ευθύνης του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία αναφορικά με την λήψη τεχνικών και οργανωτικών μέτρων προστασίας (άρθρα 25 και 32), τις προσπάθειες και ενέργειες μετριασμού των επιπτώσεων της παράβασης, την ύπαρξη προηγούμενων παραβάσεων αλλά και τον βαθμό συνεργασίας με την εποπτική αρχή καθώς και τη συμμόρφωση με τα μέτρα που αυτή επέδειξε.

Ως κριτήριο παρατίθεται επιπλέον το εξής: «κάθε άλλο επιβαρυντικό ή ελαφρυντικό στοιχείο που προκύπτει από τις περιστάσεις της συγκεκριμένης περίπτωσης». Στο γενικό αυτό κριτήριο ο Κανονισμός εντάσσει τα οικονομικά οφέλη που αποκομίστηκαν ή τις ζημίες που αποφεύχθηκαν, άμεσα ή έμμεσα, από την παράβαση, θέτοντας εμμέσως την αρχή ότι η κύρωση θα πρέπει να είναι τέτοιας τάξεως, ώστε να μην είναι οικονομικά συμφέρουσα η παρανομία. Ο Κανονισμός καλεί επίσης την εποπτική αρχή να λαμβάνει υπόψη το γενικό επίπεδο εισοδημάτων στο κράτος μέλος, καθώς και την οικονομική κατάσταση του προσώπου, όταν εξετάζει το ενδεδειγμένο ποσό του προστίμου. Με βάση την αρχή της αναλογικότητας ο Κανονισμός επιτρέπει την επιβολή επίπληξης αντί προστίμου, εφόσον πρόκειται για παράβαση ελάσσονος σημασίας ή αν το πρόστιμο που ενδέχεται να επιβληθεί θα αποτελούσε δυσανάλογη επιβάρυνση σε φυσικό πρόσωπο[33].

Κεφάλαιο Β' Ειδικά ζητήματα προστασίας προσωπικών δεδομένων στο ηλεκτρονικό εμπόριο

2. Η συγκατάθεση ως ουσιαστική προϋπόθεση νόμιμης επεξεργασίας των προσωπικών δεδομένων

[33] *Μήτρου*, 2017, σελ.169

Ο όρος «συγκατάθεση» εμφανίζεται σε πολλούς κλάδους του δικαίου, ως νομιμοποιητικό γεγονός, ως όρος δηλαδή που άρει την απαγόρευση μιας καταρχήν μη επιτρεπόμενης ενέργειας. Στο δίκαιο των προσωπικών δεδομένων, δεν εισάγεται για πρώτη φορά με τον ΓΚΠΔ. Υπό το καθεστώς της Οδηγίας 95/46/ΕΚ η συγκατάθεση του υποκειμένου, έχει την έννοια δήλωσης βουλήσεως του υποκειμένου των δεδομένων, η οποία είναι ελεύθερη, ρητή και δίδεται υπό καθεστώς πλήρους επίγνωσης για τα έννομα αποτελέσματά της και με την οποία το υποκείμενο των δεδομένων δηλώνει ότι δέχεται, ότι τα δεδομένα του, δύνανται να αποτελέσουν αντικείμενο επεξεργασίας.

Ο ΓΚΠΔ, στο στοιχείο 11' του άρθρου 4 δίνει τον ορισμό της συγκατάθεσης, ο οποίος εν πολλοίς αποτελεί αντιγραφή της προηγούμενης ρύθμισης. Έτσι λοιπόν, ως συγκατάθεση του υποκειμένου των δεδομένων ορίζεται κάθε ένδειξη βουλήσεως, ελεύθερη[34], συγκεκριμένη[35], ρητή και εν πλήρει επιγνώσει[36] με την οποία το υποκείμενο των δεδομένων εκδηλώνει, ότι συμφωνεί, με δήλωση ή σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού

[34] Η ελεύθερη συγκατάθεση συντρέχει μόνον «εάν το υποκείμενο των δεδομένων είναι σε θέση να επιλέξει πραγματικά και δεν διατρέχει κίνδυνο εξαπάτησης, εκφοβισμού, εξαναγκασμού ή σημαντικών αρνητικών συνεπειών εφόσον δεν συγκατατεθεί».

[35] Για να είναι έγκυρη η συγκατάθεση πρέπει να είναι και ειδική. Τούτο είναι σε άμεση συνάρτηση με την ποιότητα της παρεχόμενης πληροφόρησης ως προς το αντικείμενο της συγκατάθεσης, λαμβάνοντας υπ' όψιν τις εύλογες προσδοκίες του μέσου υποκειμένου των δεδομένων. Η συγκατάθεση του υποκειμένου των δεδομένων πρέπει να ζητηθεί εκ νέου εφόσον πρόκειται να προστεθούν νέες δραστηριότητες επεξεργασίας ή να μεταβληθούν οι υπάρχουσες κατά τρόπο, ο οποίος δεν θα μπορούσε εύλογα να έχει προβλεφθεί όταν χορηγήθηκε η συγκατάθεση.

[36] Πριν λάβει απόφαση, το υποκείμενο των δεδομένων πρέπει να έχει λάβει επαρκή πληροφόρηση. Το κατά πόσον η παρεχόμενη πληροφόρηση είναι επαρκής κρίνεται μόνο κατά περίπτωση. Συνήθως η εν πλήρη επιγνώσει συγκατάθεση προϋποθέτει επακριβή και εύληπτη επεξήγηση του θέματος για το οποίο ζητείται η συγκατάθεση, καθώς και βασικές πληροφορίες για τις συνέπειες της παροχής ή της άρνησης της συγκατάθεσης. Το γλωσσικό ύφος της παρεχόμενης πληροφόρησης θα πρέπει να είναι προσαρμοσμένο στους αναμενόμενους αποδέκτες της. Επίσης, οι πληροφορίες θα πρέπει να είναι άμεσα διαθέσιμες στο υποκείμενο των δεδομένων. Η εύκολη πρόσβαση και η εύκολη εύρεση των πληροφοριών είναι σημαντικά στοιχεία. Σε ένα διαδικτυακό περιβάλλον, η αποκαλούμενη πολυεπίπεδη ενημέρωση μπορεί να αποτελεί μια καλή λύση αφού, πέρα από τη συνοπτική έκδοση των πληροφοριών, το υποκείμενο των δεδομένων μπορεί να έχει πρόσβαση και σε μια αναλυτικότερη έκδοση.

χαρακτήρα, που το αφορούν. Η πρώτη μεγάλη διαφορά είναι, πως η συγκατάθεση του υποκειμένου, πρέπει να έχει τη μορφή δήλωσης ή σαφούς θετικής ενέργεια.

Ακολουθώντας μια μακρά ερμηνευτική προσέγγιση των εποπτικών αρχών επί του ζητήματος, ο Ενωσιακός νομοθέτης προχωρά στην περαιτέρω διευκρίνηση της συγκατάθεσης, στο άρθρο 7 του ΓΚΠΔ, για την περίπτωση που αυτή (η συγκατάθεση) αποτελεί τη νομιμοποιητική βάση της επεξεργασίας.

Πλέον, ο υπεύθυνος επεξεργασίας πρέπει να είναι σε θέση να αποδείξει, ότι το υποκείμενο των δεδομένων, έχει δώσει τη συγκατάθεσή του για την επεξεργασία. Το υποκείμενο, διατηρεί το δικαίωμα να ανακαλέσει τη συγκατάθεσή του, ανά πάσα στιγμή, χωρίς η ανάκληση αυτή να θίγει τη νομιμότητα της επεξεργασίας. Το υποκείμενο πρέπει να ενημερώνεται σχετικά για την ύπαρξη του δικαιώματος ανάκλησης και για τον τρόπο που αυτή θα ανακαλείται, ο οποίος μάλιστα θα πρέπει να είναι ο ίδιος με αυτόν της αρχικής χορήγησης της συγκατάθεσης.

Άξιο αναφοράς είναι και το γεγονός πως για να θεωρηθεί μια συγκατάθεση ότι έχει ληφθεί σύννομα, σε περίπτωση που παρέχεται στο πλαίσιο γραπτής δήλωσης που αφορά και άλλα θέματα, το αίτημα για συγκατάθεση πρέπει να υποβάλλεται κατά διακριτό τρόπο από τα υπόλοιπα θέματα και σε κατανοητή και εύκολα προσβάσιμη μορφή. Χαρακτηριστική καινοτομία είναι και η ειδική ρύθμιση. Όσον αφορά περιπτώσεις συγκατάθεσης που ελήφθησαν μέχρι και την ημέρα εφαρμογής του ΓΚΠΔ και αφορούν επεξεργασία που συνεχίζεται και μετά από την ημέρα αυτή ορθότερο είναι να δεχθούμε πως δεν απαιτείται συγκατάθεση εάν καλύπτονται οι αυστηρότερες προϋποθέσεις που θέτει ο Κανονισμός[37].

Επίσης, η εγκυρότητα της συναίνεσης εκτιμάται κατ' αναλογία με τις ρυθμίσεις του δικαίου των δικαιοπραξιών. Δηλαδή, η συναίνεση πρέπει να είναι ελεύθερη, γεγονός, το οποίο αναλύεται όχι μόνο στο πλαίσιο του θεσμού του εξαναγκασμού ή της ψυχικής πίεσης, αλλά το άρθρο 7 (5) ευρύτερα ορίζει ότι ουσιώδες στοιχείο για την εκτίμηση της ελευθερίας της συναίνεσης του υποκειμένου των δεδομένων είναι το γεγονός, ότι η εφαρμογή όλης της σύμβασης, εξαρτάται από την αποδοχή της επεξεργασίας, ενώ η ίδια η επεξεργασία, δεν είναι στην ουσία απαραίτητη για την εκτέλεση της σύμβασης. Για παράδειγμα, αμφισβητείται η νομιμότητα της πρακτικής ενός ιστοτόπου, ο οποίος απαγορεύει σε ένα χρήστη γενική πρόσβαση στις ιστοσελίδες του, εάν αυτός δεν δεχθεί πρώτα τα "cookies"[38] του, ενώ ο ιστοτόπος δεν

[37] *Ιωάννης Δημ. Ιγγλεζάκης*, Δίκαιο πληροφορικής, 2018, σελ. 292

[38] Τα «cookies" είναι μικρά αρχεία με πληροφορίες που μια ιστοσελίδα (συγκεκριμένα ο εξυπηρετητής ιστού – web server) αποθηκεύει στον υπολογιστή ενός χρήστη, ώστε κάθε

προορίζεται ειδικά σε παροχή υπηρεσιών επεξεργασίας προσωπικών δεδομένων. Σε αυτή την περίπτωση, η συναίνεση του επισκέπτη είναι δυνατό να κριθεί ως πλασματική.

Συνεπάγεται, ότι απαιτείται μια θετική ενέργεια, η οποία πρέπει να καταγράφεται και η οποία μπορεί να λάβει τη μορφή μιας γραπτής δήλωσης αλλά και ενός κλικ, ενός πατήματος στην οθόνη, μιας κίνησης, κ.λπ.[39] Αντιθέτως, δεν είναι συμβατός με τον θεσμό προστασίας ο μηχανισμός ο οποίος εξ αρχής (by default, «πλην ρητής αρνήσεως») προϋποθέτει την συναίνεση του υποκειμένου των δεδομένων. Αντίθετα, προωθείται από τον Κανονισμό, η έννοια της ενσωματωμένης πρόβλεψης της προστασίας («privacy by design»), παρόλο που αυτή η μορφή «κωδικοποίησης» του θεσμού προστασίας σε τεχνικά μέτρα προκαλεί ήδη κάποιες αντιδράσεις σε θεωρητικό επίπεδο[40].

2.1 Ειδικοί λόγοι επιτρεπτού της επεξεργασίας (λόγοι άρσης του άδικου χαρακτήρα της επεξεργασίας)

Όταν απουσιάζει η έγκυρη συγκατάθεση του υποκειμένου, τότε η άρση του άδικου χαρακτήρα της επεξεργασίας, θα πρέπει να υπαγορεύεται απευθείας από το νόμο, ήτοι να στηρίζεται σε στάθμιση ανάμεσα στα συμφέροντα του υποκειμένου και του υπεύθυνου επεξεργασίας ή τρίτου. Συνοπτικά, για την επεξεργασία των απλών δεδομένων αρκεί η ανάγκη ικανοποίησης ενός υπερέχοντος συμφέροντος, είτε αυτό υπαγορεύεται από διάταξη νόμου ή όχι, ενώ για την επεξεργασία των ευαίσθητων δεδομένων, προαπαιτείται να υπαγορεύεται αυτή ή το διαμέσου αυτής ικανοποιούμενο συμφέρον από διάταξη νόμου υπερισχύουσα της καταρχήν απαγόρευσης της επεξεργασίας, δηλαδή να υπαγορεύεται από διάταξη υπέρτερου

φορά που ο χρήστης συνδέεται στην ιστοσελίδα, η τελευταία να ανακτά τις εν λόγω πληροφορίες και να προσφέρει στο χρήστη σχετικές με αυτές υπηρεσίες. Χαρακτηριστικό παράδειγμα τέτοιων πληροφοριών είναι οι προτιμήσεις του χρήστη σε μια ιστοσελίδα, όπως αυτές δηλώνονται από τις επιλογές που κάνει ο χρήστης στη συγκεκριμένη ιστοσελίδα (π.χ. επιλογή συγκεκριμένων «κουμπιών», αναζητήσεων, διαφημίσεων, κλπ.

[39] Απαίτηση συμφωνίας με checkboxes σε κάθε σημείο που ο χρήστης εισάγει προσωπικά δεδομένα, όπως στο ταμείο, στη σελίδα δημιουργίας προφίλ, στο σημείο εγγραφής στο newsletter και αλλού. Κάθε αποδοχή πρέπει να καταγράφεται στο σύστημα, με την ακριβή ώρα και το ακριβές κείμενο πάνω στο οποίο δόθηκε η συγκατάθεση. Έτσι δημιουργείται ένα ιστορικό συγκατάθεσης για κάθε χρήστη.

[40] *Philippe Jougleux*, Ευρωπαϊκό δίκαιο του διαδικτύου, 2016, σελ. 77

τυπικού κύρους είτε διάταξη ειδική ή υπερισχύουσα είτε μετά από στάθμιση in concreto.

Στην περίπτωση που η επεξεργασία αφορά ευαίσθητα προσωπικά δεδομένα, οι προϋποθέσεις είναι ακόμα πιο αυστηρές: σε περίπτωση που δεν υπάρχει γραπτή συγκατάθεση του υποκειμένου, η επεξεργασία είναι νόμιμη, μόνο αν γίνεται για διαφύλαξη ζωτικού συμφέροντος του υποκειμένου, αν τα δεδομένα έχουν δημοσιοποιηθεί από το ίδιο το υποκείμενο, αν πρόκειται να χρησιμοποιηθούν για την άσκηση δικαιώματος ενώπιον δικαστηρίου, αν αφορούν την παροχή υπηρεσιών υγείας, αν αφορούν επεξεργασία από δημόσια αρχή για λόγους εθνικής ασφάλειας, εγκληματολογικής πολιτικής, προστασία της δημόσιας υγείας, δημόσιους φορολογικούς ελέγχους ή ελέγχους κοινωνικών παροχών, ερευνητικούς και επιστημονικούς σκοπούς, δημοσιογραφικούς σκοπούς σε σχέση με δεδομένα δημοσίων προσώπων κατά την άσκηση δημοσίου λειτουργήματος και τέλος αν αφορούν την επεξεργασία δεδομένων τέχνης. Στην επεξεργασία ευαίσθητων δεδομένων δεν ισχύει το σχήμα κανόνας-εξαίρεση (δηλαδή συγκατάθεση-εξαίρεση όπως αναφέρθηκε παραπάνω), διότι ακόμα και αν το υποκείμενο συγκατατίθεται στην επεξεργασία των ευαίσθητων δεδομένων του, αυτή δεν είναι νόμιμη χωρίς την άδεια της Αρχής, ισχύει δηλαδή η αρχή της κατ' αρχήν απαγόρευσης επεξεργασίας των ευαίσθητων δεδομένων.

Οι λόγοι άρσης του άδικου χαρακτήρα της επεξεργασίας είναι οι εξής:

I. Η σύμβαση και το ζωτικό συμφέρον του υποκειμένου. Η εκτέλεση της σύμβασης με το πρόσωπο, στο οποίο αναφέρονται τα δεδομένα και η προστασία ζωτικών του συμφερόντων, αποτελούν βάσεις νόμιμης επεξεργασίας που αναφέρονται, καταρχήν στο ίδιο το υποκείμενο των δεδομένων. Σχετικά με τη σύμβαση, η επεξεργασία θεωρείται σύννομη, εφόσον γίνεται ως αναγκαία προϋπόθεση για την εκτέλεσή της ή διενεργείται κατά το προσυμβατικό στάδιο πριν τη σύναψή της και εφόσον το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος. Εν προκειμένω η αναγκαιότητα της είναι το νομιμοποιητικό στοιχείο της επεξεργασίας, συνεπώς πρέπει να ερμηνεύεται συσταλτικά λαμβάνοντας υπόψη το σκοπό και τη φύση της σύμβασης, ώστε να προστατεύεται το υποκείμενο από τυχόν επεξεργασία που του επιβάλλεται εν τέλει μονομερώς διά της συμβατικής οδού. Σχετικά με το ζωτικό συμφέρον του υποκειμένου, νοείται πως η επεξεργασία είναι νόμιμη εφόσον κρίνεται απαραίτητη για τη διαφύλαξη ουσιώδους για τη ζωή συμφέροντος του και εφόσον το πρόσωπο είναι σωματικά ή νομικά αδύνατο να συγκατατεθεί.

II. Ο νόμος ως θεμέλιο σύννομης επεξεργασίας. Η υποχρέωση μπορεί να επιβάλλεται τόσο από τον κοινοτικό όσο και από τον εθνικό νομοθέτη. Στην περίπτωση αυτή η στάθμιση μεταξύ του δικαιώματος προστασίας των προσωπικών δεδομένων και του επιδιωκόμενου με τη ρύθμιση σκοπού έχει ήδη γίνει από τον νομοθέτη. Μάλιστα με τον νέο Κανονισμό επιχειρείται μια εγγύτερη οριοθέτηση των απαιτήσεων της εν λόγω νομικής βάσης, καθώς απαιτείται να καθορίζεται στο νόμο ο σκοπός της επεξεργασίας και να υπάρχει δυνητική πρόβλεψη της νομικής βάσης σ' αυτόν (άρθρο 6 § 3 ΓΚΠΔ).

III. Η εξισορρόπηση της προστασίας προσωπικών δεδομένων και του δημοσίου συμφέροντος. Το δικαίωμα προστασίας των προσωπικών δεδομένων του υποκειμένου υπόκειται σε περιορισμούς, τα όρια των οποίων, τίθενται από το Σύνταγμα λαμβανομένης υπόψη της αρχής της αναλογικότητας, από την ΕΣΔΑ (αρ. 8 § 2), αλλά και από τον Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (αρ. 52). Οι περιορισμοί αυτοί, πρέπει να αναφέρονται στο νόμο και να είναι αναγκαίοι σε μια δημοκρατική κοινωνία για την άσκηση και προστασία του δημοσίου συμφέροντος. Η έννοια είναι εξαιρετικά αόριστη και γι' αυτό πρέπει να οριοθετείται με βάση την αναγωγή της σε νομοθετικές διατάξεις, οι οποίες αφορούν την εθνική οικονομία, τη λειτουργία του δημοκρατικού πολιτεύματος, την εθνική άμυνα, την δημόσια υγεία, τη δημόσια εκπαίδευση, την εσωτερική ασφάλεια και την προστασία του περιβάλλοντος. Η εκτέλεση του έργου πρέπει να γίνεται από δημόσια αρχή ή να έχει ανατεθεί από αυτή σε υπεύθυνο επεξεργασίας ή σε τρίτο (ΟΤΑ, ανεξάρτητες αρχές). Οι λόγοι αυτοί, τιθέμενοι ως περιορισμοί ατομικού δικαιώματος, πρέπει να ερμηνεύονται στενά. Οι λόγοι αυτοί, είναι η εθνική ασφάλεια (ασφάλεια του κράτους, άμυνα), η εγκληματολογική και σωφρονιστική πολιτική, λόγοι προστασίας της δημόσιας υγείας και λόγοι σχετικοί με την άσκηση δημόσιου φορολογικού ελέγχου ή δημόσιου ελέγχου κοινωνικών παροχών. Σε σύγκριση του ν. 2472/97 με τον Κανονισμό, ο ΓΚΠΔ αναφέρεται σε ουσιαστικό δημόσιο συμφέρον, το οποίο πρέπει να είναι ανάλογο, προς τον επιδιωκόμενο στόχο, οφείλει να σέβεται την ουσία του δικαιώματος, την προστασία των δεδομένων, ενώ (ο Κανονισμός) προβλέπει επίσης κατάλληλα και συγκεκριμένα μέτρα για τη διασφάλιση των θεμελιωδών δικαιωμάτων και συμφερόντων του υποκειμένου των δεδομένων. Παράλληλα γίνεται ειδικότερη μνεία στη δημόσια υγεία (αρ 9. § 2 θ), καθώς θεωρείται επιτρεπτή η επεξεργασία για σκοπούς προληπτικής ή επαγγελματικής ιατρικής εκτίμησης της ικανότητας προς εργασία του εργαζομένου, ιατρικής διάγνωσης, παροχής υγειονομικής ή κοινωνικής περίθαλψης ή θεραπείας, διαχείρισης

υγειονομικών και κοινωνικών συστημάτων και υπηρεσιών, καθώς οι απαριθμούμενοι σκοποί αντιστοιχούν τόσο στην εξυπηρέτηση και προστασία του υποκειμένου, όσο και σε ευρύτερους στόχους. Το δημόσιο συμφέρον υπηρετούν εξάλλου και οι εξαιρέσεις που αφορούν επεξεργασία απαραίτητη για σκοπούς αρχειοθέτησης, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς.

IV. Τα δικαιώματα και τα έννομα συμφέροντα τρίτων ως θεμέλιο της νόμιμης επεξεργασίας. Εκτός από το δημόσιο συμφέρον και τα δικαιώματα των άλλων συνιστούν βάση περιορισμού του δικαιώματος προστασίας των προσωπικών δεδομένων. Το έννομο συμφέρον του υπεύθυνου επεξεργασίας[41] ή τρίτου θα

[41] Στην υπόθεση ASNEF και FECEMD, το ΔΕΕ αποσαφήνισε ότι το εθνικό δίκαιο απαγορεύεται να θεσπίζει επιπλέον προϋποθέσεις για τη νόμιμη επεξεργασία δεδομένων από εκείνες που αναφέρονται στο άρθρο 7 στοιχείο στ) της οδηγίας. Η προσφυγή αφορούσε διάταξη του ισπανικού νόμου για την προστασία των δεδομένων σύμφωνα με την οποία ιδιώτες τρίτοι μπορούσαν να επικαλεστούν έννομο συμφέρον για την επεξεργασία προσωπικών δεδομένων μόνον εάν αυτά περιλαμβάνονταν ήδη σε δημόσια προσβάσιμες πηγές. Το Δικαστήριο υπενθύμισε καταρχάς ότι η οδηγία 95/46 έχει ως σκοπό να καταστήσει ισοδύναμο σε όλα τα κράτη μέλη το επίπεδο προστασίας των δικαιωμάτων και των ελευθεριών των προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Η προσέγγιση των εθνικών νομοθεσιών που ισχύουν στον τομέα αυτό δεν πρέπει να έχει ως αποτέλεσμα την εξασθένιση της προστασίας που αυτές εξασφαλίζουν, αλλά πρέπει, αντιθέτως, να έχει ως σκοπό την κατοχύρωση υψηλού επιπέδου προστασίας στην Ένωση. Επομένως, κατά το ΔΕΕ, «από τον σκοπό που συνίσταται στη διασφάλιση ισοδύναμου επιπέδου προστασίας σε όλα τα κράτη μέλη προκύπτει ότι το άρθρο 7 της οδηγίας 95/46 προβλέπει εξαντλητικό και περιοριστικό κατάλογο των περιπτώσεων κατά τις οποίες η επεξεργασία δεδομένων προσωπικού χαρακτήρα μπορεί να θεωρηθεί νόμιμη». Επιπλέον, «τα κράτη μέλη δεν μπορούν ούτε να προσθέτουν νέες αρχές σχετικά με τη νομιμοποίηση επεξεργασιών δεδομένων προσωπικού χαρακτήρα στο άρθρο 7 της οδηγίας 95/46, ούτε να προβλέπουν πρόσθετες απαιτήσεις που τροποποιούν το περιεχόμενο μιας εκ των έξι αρχών που προβλέπει το εν λόγω άρθρο».Το Δικαστήριο κάνει δεκτό ότι «όσον αφορά τη στάθμιση που είναι απαραίτητη δυνάμει του άρθρου 7 στοιχείο στ) της οδηγίας 95/46, είναι δυνατόν να ληφθεί υπόψη το γεγονός ότι η σοβαρότητα της προσβολής των θεμελιωδών δικαιωμάτων του προσώπου που προκαλείται από την εν λόγω επεξεργασία μπορεί να ποικίλλει ανάλογα με το εάν τα επίμαχα δεδομένα περιλαμβάνονται ήδη ή όχι σε δημόσια προσβάσιμες πηγές». Ωστόσο, «το άρθρο 7 στοιχείο στ) της οδηγίας αυτής απαγορεύει σε κράτος μέλος να αποκλείει κατηγορηματικώς και γενικώς τη δυνατότητα επεξεργασίας ορισμένων κατηγοριών δεδομένων προσωπικού χαρακτήρα, χωρίς να επιτρέπει τη στάθμιση των αντικρουόμενων δικαιωμάτων και συμφερόντων στο πλαίσιο συγκεκριμένης περίπτωσης». Κατόπιν των

αποτελέσει βάση της νόμιμης επεξεργασίας, όταν αυτή η επεξεργασία είναι απολύτως απαραίτητη για την εξυπηρέτηση του, αλλά και όταν προκύπτει ως αποτέλεσμα μιας επιβεβλημένης στάθμισης με το συμφέρον ή τα θεμελιώδη δικαιώματα και τις ελευθερίες του υποκειμένου στην οποία προκύπτει πως το έννομο συμφέρον του υπεύθυνου ή του τρίτου υπερέχει προφανώς των δικαιωμάτων του υποκειμένου. Τα συμφέροντα θα πρέπει να είναι έννομα, δηλαδή να προστατεύονται από τον νόμο. Μπορεί να ποικίλλουν και να περιλαμβάνουν θεμελιώδη δικαιώματα, όπως το δικαίωμα της πληροφόρησης, της πρόσβασης σε δημόσια έγγραφα, της έρευνας κ.α. Ειδικά για τα ευαίσθητα δεδομένα, έννομο θεωρείται το συμφέρον του υπεύθυνου επεξεργασίας, όταν αυτός προβαίνει σε επεξεργασία προσωπικών δεδομένων του υποκειμένου, με σκοπό να την αξιοποιήσει για την υπεράσπιση δικαιώματος του, ενώπιον δικαστηρίου. Ειδικά για τον τύπο και τη δημοσιογραφική έρευνα πρέπει να σημειωθούν τα εξής: για να είναι νόμιμη η επεξεργασία, πρέπει να υπάρχει δικαιολογημένο ενδιαφέρον του κοινού προς ενημέρωση και μια ηθική απαξία του συγκεκριμένου προσωπικού δεδομένου του υποκειμένου που τελεί υπό συλλογή και επεξεργασία. Προκειμένου να διαπιστωθεί το δικαιολογημένο ενδιαφέρον του κοινού, ο ερμηνευτής θα πρέπει να αναχθεί στις γενικές αρχές της δημόσιας τάξης και να κρίνει κατά περίπτωση, λαμβάνοντας σοβαρά υπόψη την ιδιότητα του υποκειμένου ως δημόσιο πρόσωπο .

2.2 Πολιτική Προστασίας Προσωπικών Δεδομένων

Το ηλεκτρονικό κατάστημα, ως Υπεύθυνος Επεξεργασίας των δεδομένων των επισκεπτών/πελατών που συλλέγει και εν γένει επεξεργάζεται έχει έναντι αυτών υποχρέωση πληροφόρησης. Ιδιαίτερα σημαντικό είναι το άρθρο 13 του Κανονισμού 679/2016/ΕΕ, το οποίο αναφέρει όλες τις πληροφορίες, που πρέπει να δίδονται στο υποκείμενο των δεδομένων, πριν από τη συλλογή των προσωπικών του δεδομένων.

εκτιμήσεων αυτών, το Δικαστήριο αποφάνθηκε ότι «το άρθρο 7 στοιχείο στ) της οδηγίας 95/46 έχει την έννοια ότι απαγορεύει εθνική νομοθεσία η οποία, ελλείψει της συγκαταθέσεως του ενδιαφερομένου προσώπου και προκειμένου να επιτραπεί η επεξεργασία των δεδομένων προσωπικού χαρακτήρα η οποία είναι απαραίτητη για την επίτευξη του εννόμου συμφέροντος που επιδιώκει ο υπεύθυνος της επεξεργασίας αυτής ή ο τρίτος ή οι τρίτοι στους οποίους ανακοινώνονται τα δεδομένα αυτά, απαιτεί, πέραν του σεβασμού των θεμελιωδών δικαιωμάτων και ελευθεριών του τελευταίου, τα εν λόγω δεδομένα να περιλαμβάνονται σε δημόσια προσβάσιμες πηγές, αποκλείοντας έτσι κατηγορηματικώς και γενικώς οποιαδήποτε επεξεργασία δεδομένων που δεν περιλαμβάνονται σε αυτές τις πηγές».

Πιο συγκεκριμένα, κατά τη λήψη των δεδομένων προσωπικού χαρακτήρα, το ηλεκτρονικό κατάστημα θα πρέπει να παρέχει στο υποκείμενο των δεδομένων, όλες τις ακόλουθες πληροφορίες:

α) την ταυτότητα και τα στοιχεία επικοινωνίας του υπευθύνου επεξεργασίας (δηλαδή της επιχείρησης/ εταιρείας που διατηρεί το ηλεκτρονικό κατάστημα),

β) τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων (αν έχει οριστεί),

γ) τους σκοπούς της επεξεργασίας για τους οποίους προορίζονται τα δεδομένα προσωπικού χαρακτήρα. Ο κύριος σκοπός που συναντάται σε ένα ηλεκτρονικό κατάστημα είναι η σύναψη και εκτέλεση της πώλησης προϊόντος του ηλεκτρονικού καταστήματος, ενώ συχνά συναντώνται και επιμέρους σκοποί, όπως η αποστολή ενημερωτικού υλικού για προώθηση προϊόντων, η επικοινωνία για επίλυση αποριών σχετικά με τα εμπορεύματα, η απόλαυση προνομίων πελάτη, η διεξαγωγή έρευνας αγοράς κ.ά.,

δ) τη νομική βάση για την επεξεργασία. Η κυριότερη νομιμοποιητική βάση για την επεξεργασία είναι η εκτέλεση της σύμβασης ή η λήψη μέτρων πριν την εκτέλεση της σύμβασης, ωστόσο ενδέχεται να αποτελούν νομιμοποιητικές βάσεις και το έννομο συμφέρον του καταστήματος, η συγκατάθεση των υποκειμένων των δεδομένων (όπως στις περιπτώσεις αποστολής ενημερωτικού δελτίου, συμμετοχής σε έρευνα αγοράς, αποδοχής χρήσης cookies), η έννομη υποχρέωση του ηλεκτρονικού καταστήματος (π.χ. όπως αυτή πηγάζει από τη φορολογική νομοθεσία),

δ) τα έννομα συμφέροντα που επιδιώκονται από τον υπεύθυνο επεξεργασίας ή από τρίτο, στις περιπτώσεις που η νομιμοποιητική βάση της επεξεργασίας είναι το έννομο συμφέρον,

ε) τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων προσωπικού χαρακτήρα, εάν υπάρχουν,

στ) την τυχόν πρόθεση του υπευθύνου επεξεργασίας να διαβιβάσει δεδομένα προσωπικού χαρακτήρα σε τρίτη χώρα ή διεθνή οργανισμό και την ύπαρξη ή την απουσία απόφασης επάρκειας της Επιτροπής ή άλλων κατάλληλων εγγυήσεων ασφαλούς διαβίβασης δεδομένων.

ζ) το χρονικό διάστημα για το οποίο θα αποθηκευτούν τα δεδομένα προσωπικού χαρακτήρα ή, όταν αυτό είναι αδύνατο, τα κριτήρια που καθορίζουν το εν λόγω διάστημα. Το χρονικό διάστημα που ορίζεται πρέπει να είναι σύμφωνο με την αρχή του περιορισμού του χρόνου αποθήκευσης, δηλαδή το ηλεκτρονικό κατάστημα θα πρέπει σε περίπτωση ελέγχου από την αρμόδια αρχή να δύναται να αποδείξει την αναγκαιότητα της διατήρησης των δεδομένων γι’ αυτό το χρονικό διάστημα.

η) τα δικαιώματα τα οποία αναγνωρίζονται στον επισκέπτη ή πελάτη του ηλεκτρονικού καταστήματος: πρόσβασης, διόρθωσης, διαγραφής, φορητότητας, περιορισμού, εναντίωσης ή και ανάκλησης της συγκατάθεσης.

θ) το δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή. Σύμφωνα με τις οδηγίες που έχουν δοθεί από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, η δυνατότητα υποβολής καταγγελίας αναγνωρίζεται στα πρόσωπα, μόνο υπό την προϋπόθεση, ότι έχουν προηγουμένως ασκήσει τα δικαιώματα τους και είτε δεν έλαβαν απάντηση εντός ενός μηνός - με υπό προϋποθέσεις παράταση δύο μηνών- είτε η απάντηση που έλαβαν δεν είναι ικανοποιητική.

ι) κατά πόσο η παροχή δεδομένων προσωπικού χαρακτήρα αποτελεί νομική ή συμβατική υποχρέωση ή απαίτηση για τη σύναψη σύμβασης, καθώς και κατά πόσο το υποκείμενο των δεδομένων υποχρεούται να παρέχει τα δεδομένα προσωπικού χαρακτήρα και ποιες ενδεχόμενες συνέπειες θα είχε η μη παροχή των δεδομένων αυτών,

κ) την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων, η οποία ενδέχεται να έχει έννομα αποτελέσματα στο υποκείμενο των δεδομένων, συμπεριλαμβανομένης της κατάρτισης προφίλ, καθώς και τη σημασία και τις προβλεπόμενες συνέπειες της εν λόγω επεξεργασίας για το υποκείμενο των δεδομένων. Στην πράξη όλη η ανωτέρω πληροφόρηση καθώς και πληροφορίες που αφορούν τα κατάλληλα τεχνικά και οργανωτικά μέτρα ασφαλείας που εφαρμόζονται, αλλά και η περιγραφή του τρόπου άσκησης των δικαιωμάτων περιλαμβάνονται στην Πολιτική Προστασίας Προσωπικών Δεδομένων που βρίσκεται αναρτημένη σε εμφανές σημείο στην ιστοσελίδα του ηλεκτρονικού καταστήματος.

2.3 Γενικοί Όροι Συναλλαγών (ΓΟΣ)

2.3.1 Έννοια και χαρακτηριστικά

Οι ΓΟΣ συνιστούν τυποποιημένους όρους που προορίζονται να αποτελέσουν περιεχόμενο μεγάλου αριθμού ομοιόμορφων συμβάσεων έχοντας διαμορφωθεί πριν από τη σύναψή τους από τον κατά τεκμήριο οικονομικά και οργανωτικά ισχυρότερο συμβαλλόμενο. Η έννοιά τους νομοθετικά ορίζεται στο άρθ. 2 παρ. 1 του ν. 2251/1994, όπου χαρακτηρίζονται ως ΓΟΣ, οι «όροι που έχουν διατυπωθεί εκ των προτέρων για μελλοντικές συμβάσεις» ανάμεσα στους προμηθευτές και τους καταναλωτές.

Στην παρ. 10 του ίδιου άρθρου μάλιστα, ο νόμος διευρύνει το πεδίο εφαρμογής του, ορίζοντας ότι οι διατάξεις του «εφαρμόζονται και για κάθε όρο σύμβασης που δεν αποτέλεσε αντικείμενο ατομικής διαπραγμάτευσης», δηλαδή όταν ο καταναλωτής

δεν μπόρεσε να επηρεάσει το περιεχόμενό του[42]. Παρά τα πλεονεκτήματα που προσφέρει η χρήση των ΓΟΣ (όπως π.χ. η επιτάχυνση των διαδικασιών διαπραγμάτευσης και της κατάρτισης των συμβάσεων, η απλοποίηση των συναλλαγών, η ασφάλεια δικαίου κλπ.), παραμονεύουν πολλοί κίνδυνοι για τους καταναλωτές, ακριβώς επειδή οι ΓΟΣ προδιατυπώνονται μονομερώς από τους προμηθευτές, οι οποίοι περιορίζουν τις δικές τους υποχρεώσεις ή θέτουν στους καταναλωτές συμβατικά βάρη που, σύμφωνα με το ενδοτικό δίκαιο του ΑΚ, οι ίδιοι έπρεπε να φέρουν[43]. Για παράδειγμα, είναι σύνηθες να επιβάλλουν απαλλακτικές ρήτρες για την ευθύνη τους λόγω εσφαλμένης διαβίβασης των μηνυμάτων ή λόγω αλλοίωσης, διαρροής ή υποκλοπής των δεδομένων που αποστέλλονται μέσω του Διαδικτύου, εξαιτίας δικής τους αμέλειας ή δόλιας ενέργειας τρίτων[44]. Έτσι, δημιουργείται μια ανισορροπία μεταξύ των εκατέρωθεν δικαιωμάτων και υποχρεώσεων των μερών εις βάρος των ασθενέστερων μερών, δηλαδή των καταναλωτών. Εξάλλου, οι τελευταίοι δεν μπορούν να διαπραγματευθούν τους ΓΟΣ, απλώς έχουν την ελευθερία είτε να προσχωρήσουν σε αυτούς και να καταρτίσουν τη σύμβαση δεχόμενοι τους επιβαλλόμενους όρους, ως έχουν, χωρίς αλλαγές, είτε να απέχουν από την ολοκλήρωση της συμφωνίας[45].

2.3.2. Οι ΓΟΣ στο ηλεκτρονικό εμπόριο

Στον χώρο του Διαδικτύου οι συμβάσεις καταρτίζονται κατά κανόνα βάσει προσυντεταγμένων ΓΟΣ, οι οποίοι περιλαμβάνονται συνήθως είτε στην ιστοσελίδα του προμηθευτή ή στη φόρμα παραγγελίας είτε στα e-mail, που αυτός αποστέλλει στους χρήστες - πελάτες. Μάλιστα, εξαιτίας της έλλειψης προσωπικής επαφής και της παρεμβολής του τηλεπικοινωνιακού μέσου στην επικοινωνία των συμβαλλομένων, οι καταναλωτές επέρχονται σε ακόμη δυσμενέστερη θέση, καθώς εκμηδενίζεται κάθε δυνατότητα διαπραγμάτευσης των όρων της σύμβασης και η επιχείρηση απολαμβάνει την απεριόριστη σχεδόν δυνατότητα, να διαμορφώσει το συμβατικό περιεχόμενό της, όπως εκείνη επιθυμεί[46]. Κατά κύριο λόγο, οι ΓΟΣ που χρησιμοποιούνται στο Διαδίκτυο έχουν το ακόλουθο περιεχόμενο[47] :

---

[42] *Γεωργιάδης Απ.*, Γενικές αρχές αστικού δικαίου, 2012, σελ. 472-473

[43] *Δέλλιος Γ.*, σε Αλεξανδρίδου Ελίζα, Δίκαιο προστασίας καταναλωτή, ελληνικό – ενωσιακό, κατ' άρθρο ερμηνεία του Ν. 2251/1994 και άλλων σχετικών νομοθετημάτων, 2015, σελ.100

[44] *Γεωργιάδης*, 2012, σελ. 500

[45] *Δελούκα – Ιγγλέση Κ.*, Δίκαιο του καταναλωτή (ενωσιακό και ελληνικό), 2014, σελ. 225

[46] Επειδή οι ηλεκτρονικές συμβάσεις έχουν ως χαρακτηριστικό την τυποποίηση του περιεχομένου τους και δεν λαμβάνονται υπόψη οι ιδιαίτερες ανάγκες των συμβαλλομένων, η προστασία απέναντι σε καταχρηστικούς ΓΟΣ δεν διαφοροποιείται ουσιαστικά ανάλογα με την

- Ενημέρωση του καταναλωτή για την ύπαρξη ΓΟΣ στη συγκεκριμένη ιστοσελίδα και ανάλυση του τρόπου με τον οποίο αυτός μπορεί να λάβει γνώση του περιεχομένου τους.
- Διασφάλιση από τον επιχειρηματία της δυνατότητάς του για μονομερή τροποποίηση ή ανανέωση των ΓΟΣ.
- Έμφαση στο δικαίωμα υπαναχώρησης του αγοραστή από τη σύμβαση.
- Εξαίρεση από τη δυνατότητα επιστροφής ορισμένων προσωποποιημένων αγαθών που έχουν παραγγελθεί για την κάλυψη συγκεκριμένων αναγκών και κατά παρέκκλιση από τα κοινώς πωλούμενα.
- Αποκλεισμός ή περιορισμός της ευθύνης του πωλητή για ζημίες από τη μη εκτέλεση ή την καθυστέρηση εκτέλεσης της σύμβασης.
- Καθορισμός τρόπων πληρωμής και κατοχύρωση της ασφάλειάς τους.
- Υπενθύμιση των νομοθετικών διατάξεων για την προστασία της προσωπικής ασφάλειας από τη χρήση ηλεκτρονικών δεδομένων προσωπικού χαρακτήρα.
- Εγγυήσεις για την καταλληλότητα των προϊόντων και την ανταπόκρισή τους σε διεθνείς και ευρωπαϊκούς κανόνες ασφαλείας (π.χ. πρότυπα ISO).
- Μονομερής καθορισμός εκ μέρους του πωλητή της διεθνούς δικαιοδοσίας και του εφαρμοστέου δικαίου για την επίλυση μελλοντικών διαφορών[48].

2.3.3 Ο έλεγχος των ΓΟΣ

Οι διατάξεις του άρθ. 2 του ν. 2251/1994 στοχεύουν κατά κύριο λόγο, στον έλεγχο του κύρους των ΓΟΣ, σε μια σύμβαση και στην προστασία των καταναλωτών από τους ως άνω κινδύνους. Ο έλεγχος αυτός γίνεται σε τρία στάδια. Σε πρώτο στάδιο,

---

ιδιότητα των αντισυμβαλλομένων των προμηθευτών. Συνεπώς, η έννοια του καταναλωτή θα πρέπει να νοηθεί εδώ με την ευρεία έννοια, ώστε ο κύκλος προστασίας να περιλαμβάνει όχι μόνο τις καταναλωτικές, αλλά και τις αμφιμερώς εμπορικές συμβάσεις. Πάντως ο δικαστικός έλεγχος της καταχρηστικότητας των ΓΟΣ πρέπει να είναι απόλυτα εξατομικευμένος και με βάση τα ατομικά δεδομένα της κάθε περίπτωσης, δηλαδή κάθε καταναλωτής θα πρέπει να αξιολογείται με βάση εμπειρικά και δεοντολογικά στοιχεία για να κριθεί εάν πρόκειται για πρόσωπο που δικαιούται της ειδικής νομοθετικής προστασίας ή όχι. Έτσι, λαμβάνεται υπόψη το πρότυπο του επιφανειακά προσλαμβάνοντος κατά το στάδιο της παρατήρησης και λογικά σκεπτόμενου κατά το στάδιο λήψης απόφασης για μια συγκεκριμένη δικαιοπρακτική συμπεριφορά καταναλωτή.

[47] *Τζίβα Ε.*, Το ηλεκτρονικό εμπόριο και η προστασία των καταναλωτών απέναντι σε γενικούς όρους συναλλαγών, ΔΕΕ 10/2003, σελ. 1047 - 1048

[48] Σε αμφιμερώς εμπορικές συμβάσεις (και σπανιότερα σε καταναλωτικές) περιέχονται και όροι για τη διαιτητική επίλυση τυχόν αναφυόμενων διαφορών.

ελέγχεται η ένταξη των ΓΟΣ στη σύμβαση μεταξύ προμηθευτή και καταναλωτή, δηλαδή εάν ενσωματώθηκαν ορθώς στη σύμβαση, ώστε ο καταναλωτής να δεσμεύεται από αυτούς. Η ενσωμάτωση είναι κατ' αρχήν αναμφισβήτητη, όταν οι ΓΟΣ περιλαμβάνονται σε εμφανές σημείο της ιστοσελίδας ή στο e-mail του προμηθευτή, οπότε γίνεται λόγος για ρητή αποδοχή τους από τους καταναλωτές. Επίσης, δεκτή γίνεται η ενσωμάτωση και όταν οι ΓΟΣ δεν αναγράφονται καθ' ολοκληρίαν στην ιστοσελίδα ή στη φόρμα παραγγελίας, όμως σε αυτές υπάρχει ειδική μνεία και παραπομπή στους γενικούς όρους (π.χ. όταν υπάρχει μια σαφής επισήμανση με σύνδεσμο / «link»[49]).

Τέλος, εξ αντιδιαστολής από το άρθ. 2 § 1 του ν. 2251/1994, συνάγεται ότι οι ΓΟΣ σε κάθε περίπτωση ενσωματώνονται στη σύμβαση, όταν ο καταναλωτής γνώριζε για την ύπαρξη και το περιεχόμενό τους, πριν από το χρόνο σύναψης της σύμβασης ή όφειλε να γνωρίζει, σύμφωνα με την καλή πίστη και τα συναλλακτικά ήθη, ότι συνηθίζεται η χρήση ΓΟΣ στη συγκεκριμένη κατηγορία συναλλαγών και η δυνατότητα γνώσης τους, του είχε παρασχεθεί από τον προμηθευτή. Εξάλλου, η διάταξη αυτή ορίζει ότι οι ΓΟΣ δεν δεσμεύουν τον καταναλωτή μόνο εάν ο τελευταίος κατά την κατάρτιση της σύμβασης «τους αγνοούσε ανυπαιτίως», επειδή, για παράδειγμα, «ο προμηθευτής δεν του υπέδειξε την ύπαρξή τους ή του στέρησε τη δυνατότητα να λάβει πραγματική γνώση του περιεχομένου τους[50]».

Την τυπική γνώση της ύπαρξης των ΓΟΣ εξασφαλίζει, άλλωστε, και το π.δ. 131/2003 στο άρθ. 9 § 2, όπου ορίζεται ότι «ατομικοί όροι της σύμβασης και γενικοί όροι συναλλαγών που παρέχονται στον αποδέκτη πρέπει να διατίθενται κατά τρόπο επιτρέποντα την αποθήκευση και την αναπαραγωγή τους». Έτσι, για την παροχή των υπηρεσιών της κοινωνίας της πληροφορίας, δεν αρκεί απλώς η εμφάνιση των ΓΟΣ στην οθόνη του χρήστη των υπηρεσιών, αλλά θα πρέπει ο τελευταίος να μπορεί να τους «κατεβάζει» (download), να τους διαβάζει σε απευθείας σύνδεση (on line), να τους αποθηκεύει και να τους εκτυπώνει.

Ούτε αρκεί, επίσης, η υπόδειξή τους από τον προμηθευτή μόνο στην πρώτη σελίδα (σελίδα υποδοχής) του διαδικτυακού τόπου του προμηθευτή, αλλά πρέπει να γίνεται και στη σελίδα, στην οποία υπάρχει το έντυπο της παραγγελίας προς συμπλήρωση ή τουλάχιστον, να υπάρχει σε αυτήν ένας εμφανής υπερσύνδεσμος (hyperlink), μέσω του οποίου να γίνεται μετάβαση στην ιστοσελίδα που περιλαμβάνει τους γενικούς όρους.

---

[49] *Αλεξανδρίδου*, 2004, σελ. 74

[50] *Αλεξανδρίδου*, 2004, σελ. 74

Επιπλέον, προκειμένου να εξασφαλιστεί και η ουσιαστική γνώση των ΓΟΣ και αυτοί να θεωρηθούν ενσωματωμένοι στη σύμβαση, θα πρέπει, σύμφωνα με το άρθρ. 2 § 1 του ν. 2251/1994, το κείμενό τους να είναι ευανάγνωστο, σαφές και κατανοητό ακόμα και σε έναν μέσο καταναλωτή χωρίς νομικές γνώσεις. Επίσης, θα πρέπει να είναι γραμμένο στην ελληνική γλώσσα, εφόσον η γλώσσα της κύριας σύμβασης είναι η ελληνική και η επιχείρηση του προμηθευτή είναι επίσης ελληνική και απευθύνεται σε Έλληνες καταναλωτές[51].

Μάλιστα, με σχετική τροποποίηση που επέφερε ο ν. 3587/2007, και οι γενικοί όροι των διεθνών συναλλαγών που εφαρμόζονται στην ελληνική αγορά αποτυπώνονται υποχρεωτικά και στην ελληνική γλώσσα. Έτσι, λοιπόν, το κριτήριο ενσωμάτωσης των ΓΟΣ σε μια ηλεκτρονική σύμβαση είναι η δυνατότητα του καταναλωτή να εναντιωθεί σε αυτούς προτού προχωρήσει σε συμβατική δέσμευση ή, τουλάχιστον, να απόσχει από την κατάρτιση της σύμβασης. Κατ' αυτόν τον τρόπο διασφαλίζεται, ότι δεν βρίσκεται δεσμευμένος, από όρους που δεν γνώριζε.

Σε δεύτερο επίπεδο, το δικαστήριο προχωρά σε έλεγχο ερμηνείας των ΓΟΣ, ώστε να εξακριβώσει το ακριβές νόημά τους. Σύμφωνα με το άρθ. 2 § 4 του ν. 2251/1994, κατά την ερμηνεία λαμβάνεται υπόψη, η ανάγκη προστασίας των καταναλωτών και, σε περίπτωση αμφιβολίας, οι ΓΟΣ ερμηνεύονται υπέρ των τελευταίων στην προσπάθεια εξισορρόπησης των συμφερόντων τους με αυτά των προμηθευτών. Έτσι, εάν δεν μπορούν να εξαχθούν ασφαλή συμπεράσματα σχετικά με το νόημα των ΓΟΣ εφαρμόζοντας τους γενικούς κανόνες ερμηνείας των δικαιοπραξιών (ΑΚ 173 και 200)[52], τότε μεταξύ των διαφόρων ερμηνευτικών εκδοχών επιλέγεται αυτή που αποβαίνει εις όφελος του καταναλωτή[53].

Τέλος, το γεγονός ότι ο καταναλωτής γνωρίζει το περιεχόμενο των ΓΟΣ δεν συνεπάγεται από μόνο του τη μη εκμετάλλευσή του από τον προμηθευτή, καθώς, όπως αναφέρθηκε, ακόμα και εάν είναι ενημερωμένος, δεν έχει τη δυνατότητα να

[51] Το γεγονός ότι ο server μιας ελληνικής επιχείρησης του προμηθευτή είναι εγκαταστημένος σε Τρίτη χώρα δεν αρκεί ώστε να προσδώσει αλλοδαπό χαρακτήρα στη σύμβαση, οπότε και σε αυτή την περίπτωση θα πρέπει οι όροι να αποτυπώνονται στα ελληνικά.

[52] ΑΚ 173: «Κατά την ερμηνεία της δήλωσης βουλήσεως αναζητείται η αληθινή βούληση χωρίς προσήλωση στις λέξεις», ΑΚ 200: «Οι συμβάσεις ερμηνεύονται όπως απαιτεί η καλή πίστη, αφού ληφθούν υπόψη και τα συναλλακτικά ήθη».

[53] Η παρ. 5 του άρθρου 2 εισάγει και έναν τρίτο ερμηνευτικό κανόνα, κατά τον οποίο, όταν ελέγχεται το περιεχόμενο ΓΟΣ στο πλαίσιο άσκησης συλλογικής αγωγής από ενώσεις καταναλωτών ή επιβολής διοικητικής κύρωσης στον προμηθευτή, επιλέγεται η δυσμενέστερη ερμηνευτική εκδοχή για τον καταναλωτή, εφόσον οδηγεί σε απαγόρευση διατύπωσης και χρήσης του όρου.

διαπραγματευτεί τους όρους της σύμβασης. Έτσι, σε τρίτο επίπεδο, το δικαστήριο ελέγχει το κύρος του περιεχομένου των ΓΟΣ, προκειμένου να εντοπίσει τυχόν καταχρηστικότητά τους. Ως καταχρηστικοί χαρακτηρίζονται οι ΓΟΣ, οι οποίοι οδηγούν στη διατάραξη της ισορροπίας των υποχρεώσεων και των δικαιωμάτων των μερών δημιουργώντας γόνιμο έδαφος για την εκμετάλλευση του συναλλακτικά μειονεκτούντος καταναλωτή και συνεπώς, είναι άκυροι (άρθ. 2 § 6). Ο καταχρηστικός χαρακτήρας των ΓΟΣ κρίνεται, αφού ληφθούν υπόψη, η φύση των αγαθών ή υπηρεσιών που αφορά η σύμβαση, ο σκοπός της, το σύνολο των ειδικών συνθηκών κατά τη σύναψή της και όλες οι υπόλοιπες συναφείς ρήτρες της. Συνεπώς, είναι άκυροι, ως καταχρηστικοί οι όροι, που κατανέμουν ανισομερώς τους κινδύνους και τα βάρη θέτοντας τον καταναλωτή σε δυσμενέστερη θέση, καθώς και όσοι αποκλίνουν, χωρίς εύλογη αιτία, από τις ρυθμίσεις του ενδοτικού δικαίου κατά τρόπο που μεταβάλλουν τα δικαιώματα και τις υποχρεώσεις των μερών εις βάρος του καταναλωτή, όπως αυτά ισχύουν με βάση τους κανόνες του ενδοτικού δικαίου.

Ειδικότερα, στην § 7 του άρθ. 2, ο νόμος παραθέτει έναν λεπτομερή ενδεικτικό κατάλογο καταχρηστικών ΓΟΣ, οι οποίοι σε κάθε περίπτωση απαγορεύονται και είναι αυτοδικαίως άκυροι, με την ακυρότητα να λαμβάνεται υπόψη αυτεπαγγέλτως από το δικαστήριο (απόλυτη ακυρότητα). Παραδείγματος χάρη, είναι καταχρηστικός ο όρος σύμβασης, κατά τον οποίο σε περίπτωση υπαίτιας πλημμελούς εκπλήρωσης της παροχής του προμηθευτή, εκείνος ευθύνεται έως την αξία του πωλούμενου πράγματος, καθώς ο όρος αυτός συνεπάγεται παραίτηση του καταναλωτή από το δικαίωμά του να ζητήσει την αποκατάσταση της θετικής όσο και της αποθετικής ζημίας του κατά την ΑΚ 298 (άρθ. 2 § 7 στ. ιζ' του ν. 2251/1994). Το ίδιο ισχύει και για έναν όρο που περιορίζει τις ανειλημμένες συμβατικές υποχρεώσεις και ευθύνες του προμηθευτή (στ. β'). Αν, αντιθέτως, ο εκάστοτε ελεγχόμενος ΓΟΣ δεν εμπίπτει σε αυτήν τη «μαύρη λίστα», τότε η καταχρηστικότητά του ελέγχεται σύμφωνα με τη γενική απαγορευτική ρήτρα της προηγούμενης παραγράφου (άρθ. 2 § 6).

Κεφάλαιο Γ'

Τεχνικά και οργανωτικά μέτρα συμμόρφωσης με τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR)

3.1 Καταγραφή – ροή δεδομένων (Data Inventory - Flows)

3.1.1 Υποχρέωση καταγραφής δεδομένων

Ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) φέρνει το ζήτημα της Προστασίας των προσωπικών δεδομένων στο επίκεντρο, όπως ήδη έχει διατυπωθεί. Ο GDPR απαιτεί από τις εταιρείες που δρουν είτε ως υπεύθυνοι επεξεργασίας είτε

ως εκτελούντες την επεξεργασία, να διασφαλίζουν την ασφάλεια των προσωπικών δεδομένων, που έχουν συλλέξει ή τους έχουν παραχωρηθεί προς επεξεργασία. Απαιτείται από τον κανονισμό, οι εταιρείες που επεξεργάζονται προσωπικά δεδομένα να τεκμηριώνουν και να υποδεικνύουν, από που προέρχονται τα δεδομένα καθώς και το πως διαφυλάσσονται κατά την επεξεργασία και την μεταφορά τους καθ' όλη τη διάρκεια του κύκλου ζωής τους. Στο πλαίσιο του κανονισμού, δίνεται έμφαση στο γεγονός, ότι όλα τα προσωπικά δεδομένα, πρέπει να καταγράφονται και κάθε εταιρεία, πρέπει να διαθέτει ένα σύστημα, που να παρακολουθεί σε μόνιμη βάση τις διάφορες πράξεις, που διεξάγονται στα δεδομένα προσωπικού χαρακτήρα. Για να γίνει αυτό, απαιτείται από τις εταιρείες να διατηρούν ένα μητρώο δεδομένων (Data Inventory) το οποία θα περιγράφει την δραστηριότητα των δεδομένων, έτσι ώστε να γίνεται η διακυβέρνηση αυτών καθώς και να μπορούν να εφαρμόζονται οι σωστές διαδικασίες για την ορθή διαφύλαξη τους.

Ο GDPR απαιτεί όχι μόνο να είναι σε θέση μια εταιρεία, να προσδιορίσει και να προστατεύσει τα δεδομένα, όπου και αν βρίσκονται αλλά και να είναι υπεύθυνη, για την ακρίβεια των δεδομένων που κατέχει.

Για την εφαρμογή των κανονιστικών απαιτήσεων πρέπει πρώτα να εντοπιστούν αυτά τα δεδομένα στα συστήματά που φιλοξενούνται, εφόσον πρόκειται για ηλεκτρονικά δεδομένα και να περιγράφει σε ποια επεξεργασία υπόκεινται. Αυτή η διαδικασία ονομάζεται χαρτογράφηση δεδομένων (data mapping) ή καταγραφή δεδομένων (data inventorying) και είναι απαραίτητη, ώστε να τεκμηριώνονται, αυτές οι πληροφορίες. Το άρθρο 30 του GDPR (καταγραφή των δραστηριοτήτων επεξεργασίας) είναι η χαρτογράφηση δεδομένων. Χωρίς χαρτογράφηση δεδομένων και την ακριβή απογραφή των δεδομένων, την επεξεργασία τους, τις ροές τους, τα μέσα με τα οποία μεταδίδονται, τα άτομα που επεξεργάζονται τα δεδομένα, είναι αδύνατο για μια εταιρεία ή οργανισμό να εκπληρώσει τις απαιτήσεις της σύμφωνα με το GDPR.

3.1.2 Ροές δεδομένων (Data Flows)

Η δημιουργία ροών δεδομένων είναι ένα βασικό βήμα που θα πρέπει να πραγματοποιηθεί από την επιχείρηση-οργανισμό με βάση το GDPR. Με αυτή την ανάλυση η εταιρεία μπορεί να ανακαλύψει πού είναι τα βασικά κενά της, και να κάνει τα βήματα που πρέπει για να εντοπίσει τα δεδομένα που διαθέτει και τους τόπους που αυτά διακινούνται. Μια ροή δεδομένων είναι μια μεταφορά πληροφοριών από μια τοποθεσία στην άλλη. Για παράδειγμα, από τους προμηθευτές και τους δευτερεύοντες προμηθευτές μέσω των πελατών εντός ή εκτός της ΕΕ. Είναι δεδομένο, πως η καταγραφή μαζί με την ροή δεδομένων, αποτελούν πρωταρχικό

βήμα για την συμμόρφωση με τον κανονισμό. Ένας οργανισμός, πρέπει να γνωρίζει τα προσωπικά δεδομένα, που επεξεργάζεται και ότι τα δεδομένα υποβάλλονται σε επεξεργασία σύμφωνα με το νομικό πλαίσιο.

Κατά την χαρτογράφηση της ροής πληροφοριών, θα πρέπει να εντοπιστούν τα σημεία αλληλεπίδρασης μεταξύ των ενδιαφερόμενων μέρων. Είναι σημαντικό να κινούμαστε μέσω του κύκλου ζωής των πληροφοριών για τον εντοπισμό απρόβλεπτων ή ακούσιων χρήσεων δεδομένων. Μια εταιρεία θα πρέπει να εξετάσει επίσης τις πιθανές μελλοντικές χρήσεις των πληροφοριών που συλλέγει ακόμη και αν δεν είναι άμεσα αναγκαίο.

Ο πρώτος στόχος, μιας ροής δεδομένων είναι να προσδιοριστεί, ο τρόπος με τον οποίο χρησιμοποιούνται τα δεδομένα και να βεβαιωθούμε, όταν είναι απαραίτητο, πως τα άτομα για τα οποία γίνεται συλλογή δεδομένων είναι ενήμερα για την χρήση των δεδομένων που έχουν συλλεχθεί. Εάν ένας οργανισμός συλλέγει δεδομένα για το λόγο, ότι μια μέρα μπορεί να τα χρησιμοποιήσει, ο GDPR απαγορεύει αυτή τη συλλογή. Υπάρχουν διάφοροι τρόποι με τους οποίους τα δεδομένα μπορούν να συλλεχθούν, και είναι σημαντικό να ξέρει η εταιρεία τι συμβαίνει πραγματικά με καθένα από αυτούς τους τρόπους καθώς και με τις τεχνικές συλλογής που ακολουθούνται.

Τα δεδομένα για την δημιουργία της ροής δεδομένων μπορούν να συλλεχθούν κατά την επιθεώρηση των υπαρχόντων εγγράφων του οργανισμού, μέσω στοχευμένων συναντήσεων με το προσωπικό που διαχειρίζεται προσωπικά δεδομένα, μέσω συμπλήρωσης ερωτηματολογίων ή ακόμη και από εσωτερική παρατήρηση διεργασιών. Εάν η αποτύπωση της ροής ενός οργανισμού, σχετικά με τον τρόπο με τον οποίο ρέουν τα δεδομένα του, είναι διαφορετική από την πραγματικότητα, τότε υπάρχει παραβίαση με βάση τον κανονισμό και θα μπορούσε να επιβληθεί πρόστιμο. Ο οργανισμός θα πρέπει να διοργανώνει συναντήσεις με όλα τα μέλη των ομάδων που διαχειρίζονται δεδομένα και να συζητούν τι συμβαίνει σε κάθε στάδιο της διαδικασίας συλλογής δεδομένων, καθώς και για το που πηγαίνουν τα δεδομένα όπως και ποιος έχει πρόσβαση σε αυτά. Τυπικά, η έξοδος μιας διαδικασίας ή μιας ροή εργασίας είναι μια είσοδος σε μια άλλη επεξεργασία ή διαδικασία. Όπως και με τα βασικά στοιχεία ενός δεδομένου στην καταγραφή, ο οργανισμός πρέπει να εξετάσει τα προσωπικά δεδομένα που συλλέγονται και σε τι μορφή έχουν συλλεχθεί. Χρειάζεται επίσης να δούμε, πώς συλλέχθηκαν τα δεδομένα, ποιος είναι υπεύθυνος γι' αυτά, πού βρίσκονται και ποιος έχει πρόσβαση σε αυτά. Η εταιρεία θα πρέπει να είναι σε θέση να γνωρίζει αν τα δεδομένα έχουν αποκαλυφθεί ή μοιραστεί με οποιονδήποτε άλλο και εάν το σύστημα αλληλεπιδρά ή μεταφέρει πληροφορίες σε οποιοδήποτε άλλο σύστημα.

3.1.3 Αρχεία δραστηριοτήτων επεξεργασίας

Κάθε υπεύθυνος επεξεργασίας θα πρέπει να τηρεί αρχείο των δραστηριοτήτων επεξεργασίας στο πλαίσιο της ευθύνης του για τα δεδομένα που επεξεργάζεται, συμπεριλαμβανομένων:

- Όνομα και στοιχεία επικοινωνίας του controller και, κατά περίπτωση, του joint controller, τον εκπρόσωπο του controller και τον υπεύθυνο προστασίας δεδομένων (DPO).
- Τους σκοπούς της επεξεργασίας.
- Περιγραφή των κατηγοριών των υποκειμένων των δεδομένων.
- Περιγραφή των κατηγοριών προσωπικών δεδομένων.
-Κατηγορίες αποδεκτών στους οποίους έχουν διαβιβαστεί ή πρόκειται να αποκαλυφθούν τα προσωπικά δεδομένα συμπεριλαμβανομένων των αποδεκτών σε τρίτες χώρες ή διεθνείς οργανισμούς.
- Κατά περίπτωση, διαβιβάσεις δεδομένων προσωπικού χαρακτήρα προς τρίτη χώρα, συμπεριλαμβανομένης την γνωστοποίηση της εν λόγω τρίτης χώρας και τον μηχανισμό μεταβίβασης που επικαλείται.
- Όπου είναι δυνατόν, τις προβλεπόμενες προθεσμίες για τη διαγραφή των διαφόρων κατηγοριών δεδομένων.
- Όπου είναι δυνατόν, γενική περιγραφή της τεχνικής και οργανωτικής ασφάλειας – μέτρα.

3.1.4 Μεθοδολογία καταγραφής δεδομένων

Η μεθοδολογία καταγραφής δεδομένων (data inventorying) είναι ακρογωνιαίος λίθος της συμμόρφωσης με το GDPR και θα πρέπει να εκτελείται σε συγκεκριμένα βήματα, καθώς και να διατηρεί ακριβές το αποτέλεσμα ώστε να αποτυπώνεται ορθά. Για αυτό τον λόγο, θα πρέπει ο εκτελών την μεθοδολογία να καταρτίζει ένα ακριβές πλάνο εκτέλεσης, το οποίο θα συλλέγει από όλες τις πήγες ενός οργανισμού ή μιας εταιρείας τις κατάλληλες πληροφορίες που θα κάνουν την καταγραφή των δεδομένων ακριβή.

Οι βασικές μέθοδοι που χρησιμοποιούνται για την εκτέλεση της μεθοδολογίας καταγραφής δεδομένων είναι κυρίως οι :

1. Διαδικασία συνεντεύξεων,
2. Αυτόματος εντοπισμός των δεδομένων με χρήση λογισμικού,
3. Ανατροφοδότηση από άλλα συστήματα.

Φυσικά μπορεί να χρησιμοποιηθεί και συνδυασμός, ώστε να γίνει διασταύρωση ή εμπλουτισμός του data inventory από διαφορετικές πηγές. Η διαδικασία των

συνεντεύξεων θα πρέπει να είναι οργανωμένη με ερωτήσεις, που να απευθύνονται σε μέρη που επεξεργάζονται ή παίρνουν μέρος στην επεξεργασία και να απαντούν κατά βάση στα Γιατί - Ποιος - Πότε – Που (Why-Who-When-Where). Με βάση την μεθοδολογία των 5W's όπως την ονομάζουμε δημιουργούμε σετ ερωτήσεων οι οποίες θα μας δώσουν απαντήσεις ώστε να συμπληρώσουμε το data inventory μας.

3.1.5 Αντιστοίχιση με βάση τα 5 W's

Αυτή η ενότητα παρέχει βασικά βήματα στους controllers - processors για τη δημιουργία ενός data inventory - mapping των δραστηριοτήτων επεξεργασίας δεδομένων. Σε πολλές περιπτώσεις, οι φόρμες αίτησης / επικοινωνίας (έντυπη ή ηλεκτρονική) παρέχουν συχνά ένα καλό σημείο από το οποίο μπορούμε να ακολουθήσουμε την διαδρομή των δεδομένων. Ο τύπος, η πολυπλοκότητα, ο όγκος, η ευαισθησία ή ο κίνδυνος της επεξεργασίας μπορεί να απαιτούν μια πιο «σε βάθος» ή εξελιγμένη προσέγγιση. Οι πληροφορίες που συγκεντρώνονται θα βοηθήσουν να ενημερωθούν τα επόμενα βήματα - συμμόρφωση με τις αρχές και τα δικαιώματα και δημιουργία των "αρχείων των δραστηριοτήτων επεξεργασίας" που απαιτούνται από το άρθρο 30 του GDPR.

Α) Γιατί επεξεργάζονται δεδομένα προσωπικού χαρακτήρα ; (Why)

Τα προσωπικά δεδομένα καθορίζονται ευρέως στο GDPR και σημαίνει κάθε πληροφορία σχετικά με ένα φυσικό πρόσωπο που μπορεί να εντοπιστεί, άμεσα ή έμμεσα, ιδίως με αναφορά σε ένα αναγνωριστικό όπως όνομα, αναγνωριστικό αριθμό, δεδομένα θέσης, ηλεκτρονικό αναγνωριστικό ή σε ένα ή περισσότερους παράγοντες που σχετίζονται με τη φυσική, φυσιολογική, γενετική, ψυχική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα αυτού του προσώπου. Εξετάζοντας όλους τους τομείς της επιχείρησης ή της υπηρεσίας θα πρέπει να είμαστε σε θέση να απαριθμήσουμε όλους τους λόγους για τους οποίους χρησιμοποιούνται προσωπικά δεδομένα.

Β) Ποιου τα προσωπικά δεδομένα επεξεργάζονται; (Who)

Θα πρέπει να είμαστε σε θέση να απαντήσουμε στην ερώτηση αυτή, ώστε να προσδιορίσουμε το υποκείμενο των δεδομένων και να το καταγράψουμε. Για καθέναν από τους λόγους που αναφέρονται, απαριθμούνται όλες οι διάφορες κατηγορίες προσώπων για τα οποία γίνεται η επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Γ) Τι είδους προσωπικά δεδομένα επεξεργάζονται ; (What)

Θα πρέπει να είμαστε σε θέση να απαντήσουμε και να περιγράψουμε τις διαφορετικές υποκατηγορίες προσωπικών δεδομένων που επεξεργάζονται από το σύστημα ή την επιχείρηση, να προσδιορίσουμε την πηγή καθώς και την νομική υπόσταση των δεδομένων.

Δ) Πότε γίνεται η επεξεργασία δεδομένων προσωπικού χαρακτήρα; (When)

Δεν πρέπει να ξεχνούμε πως με την έννοια επεξεργασία ο κανονισμός περιλαμβάνει τις ενέργειες απόκτησης, αποκάλυψης και διαγραφής προσωπικών δεδομένων. Είναι σημαντικό λοιπόν και θα πρέπει να ορίσουμε το πότε συμβαίνουν όλες οι παραπάνω ενέργειες.

Ε) Που γίνεται η επεξεργασία δεδομένων προσωπικού χαρακτήρα; (Where)

Εξίσου σημαντικό με τα προηγούμενα τέσσερα είναι και το σημείο, στο οποίο γίνεται η επεξεργασία και σε πολλές περιπτώσεις, η επεξεργασία μπορεί να λαμβάνει μέρος σε παραπάνω από ένα σημεία.

3.2 Εκτίμηση των επιπτώσεων σχετικά με την προστασία των δεδομένων (DPIA)

3.2.1 Εκτέλεση της DPIA

Με σκοπό να εφαρμοστεί η DPIA σε ένα νέο πληροφοριακό σύστημα επεξεργασίας δεδομένων, διατυπώνεται στη συνέχεια μια γενική προσέγγιση μεθοδολογίας, η οποία θα αποτελείται από τις κατάλληλες δραστηριότητες, ώστε η εκτίμηση των επιπτώσεων, σχετικά με τη προστασία των δεδομένων, να εκτελείται με όσον το δυνατόν περισσότερη σαφήνεια και μεθοδικότητα. Η διαδικασία αυτή αποτελείται από τα εξής βήματα: καθορισμός της ανάγκης για την διενέργεια της DPIA (Τι είδους προσωπικά δεδομένα επεξεργάζονται; Ποιος ο υπεύθυνος επεξεργασίας; Ενδέχεται να υπάρξουν αρνητικές επιπτώσεις για τα φυσικά πρόσωπα; Έχουν ληφθεί μέτρα προστασίας;), προσδιορισμός της ομάδας εκτέλεσης της DPIA, αναγνώριση και περιγραφή της εφαρμογής / διαδικασίας (Περιγραφή του σχεδιασμού της εφαρμογής και των διεπαφών της με άλλα συστήματα και της διαδικασίας, της ροής των δεδομένων, των εμπλεκόμενων χρηστών και των επιμέρους υποσυστημάτων της εφαρμογής), σύσκεψη με τους εμπλεκόμενους (Άτομα από το εσωτερικό και εξωτερικό του οργανισμού επισημαίνουν τους κινδύνους που αφορούν το δικό τους πεδίο εξειδίκευσης), αναγνώριση των σχετικών κινδύνων (Αναγνώριση των συνθηκών και των πιθανών κινδύνων που μπορεί να απειλήσουν τα προσωπικά δεδομένα των ατόμων και να επηρεάσουν την ιδιωτικότητά τους), διαχείριση των κινδύνων (Αξιολόγηση των ενδεχόμενων απειλών και των δυσμενών γεγονότων που

έχουν αρνητικές επιπτώσεις για τα φυσικά πρόσωπα, λήψη μέτρων αντιμετώπισης και ασφάλειας), έλεγχος νομοθετικής συμμόρφωσης, τεκμηρίωση και ολοκλήρωση της σχετικής έκθεσης, εξωτερικός έλεγχος και ανασκόπηση.

Κάθε επεξεργασία δεδομένων εντός της εταιρείας πρέπει να συμμορφώνεται με τις απαιτήσεις προστασίας δεδομένων και κάθε εταιρεία πρέπει να είναι σε θέση να αποδείξει την συμμόρφωση της. Το θέμα της εκτίμησης των επιπτώσεων στην αξιολόγηση κινδύνου / προστασία δεδομένων ("DPIA"), αποτελεί στοιχείο της γενικής έννοιας του GDPR για την προστασία δεδομένων. Το άρθρο 32 του GDPR διευκρινίζει την "ασφάλεια στην επεξεργασία" και στο άρθρο 35 του GDPR, την αξιολόγηση των επιπτώσεων στην προστασία δεδομένων.

Και τα δύο άρθρα περιγράφουν τις ευθύνες του υπεύθυνου επεξεργασίας, σύμφωνα με το οποίο το άρθρο 32 του GDPR ισχύει και για τους εκτελούντες της επεξεργασία. Σύμφωνα με το άρθρο 32 του GDPR, η αξιολόγηση βασίζεται στην πιθανότητα εμφάνισης και τη σοβαρότητα του κινδύνου για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Σε πολλές εταιρείες, τα μέτρα που πρέπει να εφαρμοστούν έχουν ήδη αξιολογηθεί όσον αφορά τις πτυχές, που σχετίζονται με τον κίνδυνο - συχνά σε συμφωνία με την ασφάλεια των πληροφοριών σύστημα διαχείρισης ("ISMS").

Όσον αφορά το άρθρο 32 του GDPR, η μεθοδολογία που χρησιμοποιείται σήμερα, είναι αυτή, που ήδη εφαρμόζεται και είναι διαδεδομένη από την κλασσική ανάλυση και εκτίμηση κινδύνου. Όπως έχει ήδη καθιερωθεί σε πολλές εταιρείες, μπορεί να γίνει διάκριση μεταξύ βασικής ασφάλειας πληροφοριών, η οποία βασικά ισχύει για όλες τις διαδικασίες και εισαγωγή ειδικών μέτρων για την διαδικασία επεξεργασίας πληροφοριών. Η αξιολόγηση αντίκτυπου για την προστασία των δεδομένων (άρθρο 35 του GDPR) είναι το αντίστοιχο του προηγούμενου (άρθρο 20 της οδηγίας 95/46/ ΕΚ).

Μια σημαντική καινοτομία που επιφέρει ο ΓΚΠΔ, συνίσταται στην καταρχήν κατάργηση της γενικής υποχρέωσης γνωστοποίησης προς την αρχή ελέγχου (εκάστοτε αρμόδια ΑΠΔΠΧ) της επεξεργασίας, που προέβλεπε η Οδηγία 95/46/ΕΚ και η οποία βάρυνε τους υπευθύνους επεξεργασίας, και στην αντικατάστασή της:

α. αφενός, από την υποχρέωση για τους υπευθύνους επεξεργασίας να τηρούν αρχεία των δραστηριοτήτων επεξεργασίας, για τις οποίες είναι υπεύθυνοι, καθώς και την υποχρέωση για τους εκτελούντες την επεξεργασία να τηρούν αρχεία όλων των κατηγοριών δραστηριοτήτων επεξεργασίας, που διεξάγονται για λογαριασμό υπευθύνου επεξεργασίας,

β. αφετέρου, από την υποχρέωση για τους υπευθύνους επεξεργασίας να διενεργούν εκτίμηση αντικτύπου (Data protection impact assessment - DPIA) σχετικά με την προστασία δεδομένων σε συγκεκριμένες κατηγορίες επεξεργασιών.

Η κατάργηση της γενικής υποχρέωσης γνωστοποίησης της επεξεργασίας δεδομένων προσωπικού χαρακτήρα προς τις ΑΠΔΠΧ δικαιολογήθηκε, από τη διαπίστωση, ότι η υποχρέωση αυτή, παρά το ότι επιφέρει στις αρχές ελέγχου και, ιδίως, στους υπευθύνους επεξεργασίας διοικητικό και οικονομικό φόρτο, δεν συνέβαλε σε όλες τις περιπτώσεις, στη βελτίωση της προστασίας των δεδομένων προσωπικού χαρακτήρα. Προκρίθηκε, συνεπώς, η αντικατάσταση αυτής της γενικής υποχρέωσης γνωστοποίησης από «αποτελεσματικές διαδικασίες και μηχανισμούς που επικεντρώνονται σε εκείνους τους τύπους πράξεων επεξεργασίας που ενδέχεται να έχουν ως αποτέλεσμα υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων λόγω της φύσης, του πεδίου εφαρμογής, του πλαισίου και των σκοπών τους».

Ως «τύποι πράξεων» επεξεργασίας, από τους οποίους ενδέχεται να προκύψουν κίνδυνοι για τα υποκείμενα των δεδομένων, χαρακτηρίζονται, ιδίως, εκείνοι που περιλαμβάνουν τη χρήση νέων τεχνολογιών ή είναι νέου τύπου και δεν έχει διενεργηθεί προηγούμενη εκτίμηση αντικτύπου ως προς την προστασία των δεδομένων από τον υπεύθυνο επεξεργασίας ή παρίσταται αναγκαία η αξιολόγησή τους, λόγω του χρόνου που έχει παρέλθει από την αρχική επεξεργασία.

Στο πλαίσιο αυτό, η ρητή θέσπιση υποχρέωσης διενέργειας DPIA παρίσταται, καταρχάς, ως ένα αντιστάθμισμα στην κατάργηση της γενικής υποχρέωσης γνωστοποίησης της επεξεργασίας, με σκοπό την αντιμετώπιση των υψηλών κινδύνων, που ενδέχεται να προκύψουν, για τα υποκείμενα των δεδομένων από συγκεκριμένες κατηγορίες επεξεργασιών, λόγω της φύσης, του πεδίου εφαρμογής, του πλαισίου και των σκοπών τους.

Υπό την έννοια αυτή η υποχρέωση διενέργειας DPIA σημαίνει, ότι ο υπεύθυνος επεξεργασίας, έχει την υποχρέωση να αξιολογήσει όλες τις παραμέτρους των κρίσιμων πράξεων επεξεργασίας πριν από την έναρξή τους, προκειμένου να διασφαλίσει την αποτελεσματική προστασία των υποκειμένων. Επιπλέον, εάν απαιτείται από τις περιστάσεις, ο υπεύθυνος επεξεργασίας υποχρεούται να πραγματοποιεί σχετικά διαβούλευση με την αρμόδια ΑΠΔΠΧ, πριν από την έναρξη της επεξεργασίας. Συνακόλουθα, η υποχρέωση διενέργειας DPIA σημαίνει, επίσης, ότι πρόκειται για ένα μέτρο, το οποίο είναι πλήρως ενταγμένο στην ανάγκη προστασίας των δεδομένων ήδη από το σχεδιασμό και εξορισμού (Privacy by design

/Privacy by default), σύμφωνα με τα οριζόμενα στις διατάξεις του άρθρου 25 του ΓΚΔΠ.

3.2.2 Έννοια και περιεχόμενο της υποχρέωσης διενέργειας DPIA

Ο υπεύθυνος επεξεργασίας υποχρεούται ρητά σε διενέργεια DPIA, πριν από την κρίσιμη επεξεργασία, κάθε φορά που ένα είδος επεξεργασίας, ιδίως με χρήση νέων τεχνολογιών, και συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας αυτής, ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων. Είναι δυνατό η διενέργεια DPIA να μην αφορά μεμονωμένη επεξεργασία, αλλά ένα σύνολο πράξεων επεξεργασίας, εφόσον αυτές είναι παρόμοιες και ενέχουν παρόμοιους υψηλούς κινδύνους για τα ενδιαφερόμενα υποκείμενα. Ο ΓΚΠΔ, εξειδικεύοντας την έννοια των επεξεργασιών δυνάμενων να επιφέρουν ως άνω υψηλούς κινδύνους καθιστά, κατά τρόπο ενδεικτικό («ιδίως») και όχι περιοριστικό, τη διενέργεια DPIA υποχρεωτική σε τρεις τουλάχιστον τύπους επεξεργασιών:

α. της συστηματικής και εκτενούς αξιολόγησης προσωπικών πτυχών των υποκειμένων, που βασίζεται σε αυτοματοποιημένη επεξεργασία (συμπεριλαμβανομένης της τεχνικής profiling) και στην οποία βασίζονται αποφάσεις που παράγουν έννομα αποτελέσματα για τα υποκείμενα αυτά ή τα επηρεάζουν σε σημαντικό βαθμό,

β. της μεγάλης κλίμακας επεξεργασίας των ειδικών κατηγοριών δεδομένων που αναφέρονται στο άρθρο 9 παρ. 1 ή δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα που αναφέρονται στο άρθρο 10 (δηλαδή, σχετικών με ευαίσθητα δεδομένα προσωπικού χαρακτήρα) και

γ. της συστηματικής παρακολούθησης δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα.

Πέρα από τους ως άνω τύπους επεξεργασιών που προσδιορίζονται ρητά, θεσπίζεται υποχρέωση για κάθε ΑΠΔΠΧ να καταρτίζει και να δημοσιοποιεί κατάλογο με τους τύπους επεξεργασίας, που υπόκεινται -κατά την κρίση της- στην υποχρέωση για διενέργεια DPIA.

Θεσπίζεται, επίσης, ευχέρεια για κάθε ΑΠΔΠΧ να καταρτίζει και να δημοσιοποιεί κατάλογο με τους τύπους επεξεργασίας, που –πάντοτε κατά την κρίση της- εξαιρούνται από την υποχρέωση για διενέργεια DPIA. Τόσο ο κατάλογος, με τους τύπους επεξεργασίας για τους οποίους απαιτείται η διενέργεια DPIA, όσο και ο κατάλογος με εκείνους που εξαιρούνται από τη διενέργεια DPIA, ανακοινώνονται από την αρμόδια ΑΠΔΠΧ στο Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων.

Το ελάχιστο περιεχόμενο της DPIA, που διενεργείται υποχρεωτικά κατά τα προαναφερόμενα, σύμφωνα με το ΓΚΠΔ συνίσταται σε:

α. συστηματική περιγραφή των προβλεπόμενων πράξεων επεξεργασίας και των σκοπών αυτών, καθώς και του εννόμου συμφέροντος που επιδιώκει, κατά περίπτωση, ο υπεύθυνος επεξεργασίας,

β. εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας σε σχέση με τους σκοπούς τους,

γ. εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων

δ. τα προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων, συμπεριλαμβανομένων των εγγυήσεων, των μέτρων και μηχανισμών ασφάλειας, ώστε να διασφαλίζεται η προστασία των δεδομένων και να αποδεικνύεται η συμμόρφωση προς το ΓΚΠΔ, λαμβάνοντας υπόψη τα δικαιώματα και τα έννομα συμφέροντα τόσο των υποκειμένων των δεδομένων όσο και άλλων ενδιαφερόμενων προσώπων.

Προσθέτουμε ότι, εφόσον υπάρχει εκτελών την επεξεργασία, αυτός θα πρέπει να παρέχει συνδρομή στον υπεύθυνο επεξεργασίας, όταν χρειάζεται και αφού του ζητηθεί, ώστε να διασφαλίζει τη συμμόρφωση προς τις υποχρεώσεις, που απορρέουν από τη διενέργεια DPIA, σχετικά με την προστασία των δεδομένων, και από την προηγούμενη διαβούλευση με την αρμόδια ΑΠΔΠΧ

3.2.3 Απόφαση για διενέργεια DPIA

Οι αρχές προστασίας δεδομένων μπορούν να καταρτίσουν κατάλογο των δραστηριοτήτων επεξεργασίας για τις οποίες, γενικά, δεν απαιτείται εκτίμηση επιπτώσεων για την προστασία των δεδομένων (whitelist) και των ειδών επεξεργασίας δραστηριότητες που υπόκεινται πάντοτε στην απαίτηση για αξιολόγηση των επιπτώσεων στην προστασία των δεδομένων (blacklist). Σε ορισμένες περιπτώσεις, ο υπεύθυνος επεξεργασίας υποχρεούται να διεξάγει αξιολόγηση των επιπτώσεων στην προστασία δεδομένων. Η σοβαρότητα της παρέμβασης στα θεμελιώδη δικαιώματα χρησιμεύει ως προσανατολισμός για την ταξινόμηση υψηλών κινδύνων για τα δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων. Ο GDPR απαιτεί από τον ελεγκτή να αξιολογεί τον κίνδυνο προστασίας δεδομένων βάσει αντικειμενικών κριτηρίων. Η άποψη του ευρωπαϊκού νομοθέτη είναι, ότι ιδίως, οι νέες τεχνολογίες αποτελούν έναυσμα για την υποχρέωση διενέργειας αξιολόγησης αντικτύπου για την προστασία των δεδομένων. Ανεξαρτήτως της υποχρέωσης διεξαγωγής αξιολόγησης των επιπτώσεων στην προστασία των δεδομένων, αυτό μπορεί πάντα να γίνει εθελοντικά ως προσθήκη στην αξιολόγηση κινδύνου σύμφωνα με το άρθρο 32 του GDPR. Ως απλοποίηση της

διαδικασίας, πολλές δραστηριότητες επεξεργασίας δεδομένων με παρόμοιο υψηλό κίνδυνο μπορούν να εξεταστούν σε μία μόνο αξιολόγηση.

3.2.4 Οφέλη από την εκτέλεση της DPIA

Από την εκτέλεση και την ολοκλήρωση της εκτίμησης των επιπτώσεων σχετικά με την προστασία των προσωπικών δεδομένων προκύπτουν σημαντικά πλεονεκτήματα ουσιαστικής σημασίας για τον οργανισμό. Αυτά τα πλεονεκτήματα αφορούν το εσωτερικό και εξωτερικό περιβάλλον του οργανισμού και θα μπορούσαν να καταγραφούν ως εξής :

Εσωτερικά:

1. διαχείριση του κινδύνου (αναγνώριση και περιορισμός),
2. αποφυγή κοστοβόρων επαναπροσδιορισμών της διαδικασίας επεξεργασίας αλλά και της ίδιας της εφαρμογής εάν από την αρχή έχουν προσδιοριστεί οι ενδεχόμενοι κίνδυνοι και απειλές,
3. αποφυγή επιβολής κυρώσεων αλλά και αποφυγή της διακοπής ή απαγόρευσης του εγχειρήματος από την αρμόδια Αρχή Προστασίας Προσωπικών Δεδομένων λόγω μη συμμόρφωσης στους υφιστάμενους κανονισμούς και στη νομοθεσία της Ε.Ε,
4. βελτίωση της προστασίας των προσωπικών δεδομένων και της αποδοτικότητας της συγκεκριμένης υπηρεσίας,
5. βελτίωση του τρόπου διαχείρισης των δεδομένων γνωρίζοντας τις πιθανές απειλές και αστοχίες,
6. αύξηση της ασφάλειας του συστήματος όσον αφορά την προστασία των δεδομένων και των γενικότερων λειτουργιών του οργανισμού που βασίζονται σε αυτό,
7. βελτίωση της τεχνογνωσίας σε θέματα προστασίας προσωπικών δεδομένων και ασφάλειας πληροφοριακών συστημάτων.

Εξωτερικά:

1. ενίσχυση της αξιοπιστίας του οργανισμού από την πλευρά των εμπλεκόμενων μερών,
2. υπόδειξη συμμόρφωσης με την νομοθεσία περί προστασίας προσωπικών δεδομένων και επιβεβαίωση ότι η ασφάλεια λαμβάνεται σοβαρά υπόψη.

3.2.5 Μεθοδολογία διενέργειας DPIA

Ο κανονισμός δεν υποδεικνύει συγκεκριμένη μεθοδολογία για την διενέργεια μιας DPIA, σαφώς και υπάρχουν δοκιμασμένες βέλτιστες πρακτικές της οποίες μπορούμε να ακολουθήσουμε, ώστε να πετύχουμε τον σκοπό της DPIA. Αυτό φυσικά δίνει τη δυνατότητα σε αυτόν που διενεργεί την DPIA να επιλέξει μεταξύ πληθώρας και

δοκιμασμένων τεχνικών που θα του δώσουν την δυνατότητα να επιτύχει ένα σωστό αποτέλεσμα. Μπορεί ο κανονισμός, να μην προτείνει συγκεκριμένη μεθοδολογία, όπως προαναφέρθηκε, όμως είναι σαφής ως προς τα κριτήρια και τα χαρακτηριστικά τα οποία θα πρέπει να περιλαμβάνονται σε μία σωστή DPIA. Ο κανονισμός ορίζει το ελάχιστο περιεχόμενο της DPIA (άρθρο 35 παράγραφος 7 και αιτιολογικές σκέψεις 84 και 90):

1. «περιγραφή των προβλεπόμενων πράξεων επεξεργασίας και των σκοπών της επεξεργασίας»·
2. «εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας»·
3. «εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων»·
4. «τα προβλεπόμενα μέτρα»:

α) «αντιμετώπισης των κινδύνων»·

β) «απόδειξης της συμμόρφωσης με τον παρόντα κανονισμό».

Κατά την εκτίμηση του αντικτύπου μιας πράξης επεξεργασίας δεδομένων πρέπει να λαμβάνεται υπόψη (άρθρο 35 παράγραφος 8) η συμμόρφωση με έναν κώδικα δεοντολογίας (άρθρο 40). Τούτο μπορεί επίσης να χρησιμεύσει στην απόδειξη ότι έχουν επιλεγεί ή ληφθεί τα κατάλληλα μέτρα, με τον όρο ότι ο κώδικας δεοντολογίας ενδείκνυται για την πράξη επεξεργασίας.

Θα πρέπει επίσης να λαμβάνονται υπόψη οι πιστοποιήσεις, οι σφραγίδες και τα σήματα [προστασίας των δεδομένων] για τον σκοπό της απόδειξης της συμμόρφωσης των πράξεων επεξεργασίας των υπεύθυνων επεξεργασίας και των εκτελούντων την επεξεργασία (άρθρο 42) με τον κανονισμό, καθώς και οι δεσμευτικοί εταιρικοί κανόνες .

Όλες οι συναφείς απαιτήσεις που περιέχει ο κανονισμός παρέχουν ένα ευρύ, γενικό πλαίσιο για τον σχεδιασμό και την υλοποίηση DPIA. Η πρακτική υλοποίηση μιας DPIA θα εξαρτηθεί από την πλήρωση των απαιτήσεων του κανονισμού, οι οποίες μπορεί να συμπληρωθούν με πιο αναλυτικές πρακτικές οδηγίες. Ως εκ τούτου, η υλοποίηση DPIA είναι κλιμακώσιμη. Τούτο σημαίνει, ότι ακόμη και ένας μικρής εμβέλειας υπεύθυνος επεξεργασίας, μπορεί να σχεδιάσει και να διενεργήσει DPIA πρόσφορη για τις πράξεις επεξεργασίας του.

Η αιτιολογική σκέψη 90 του κανονισμού παραθέτει μια σειρά στοιχείων της DPIA που αλληλεπικαλύπτονται με τα πλήρως καθορισμένα στοιχεία της διαχείρισης κινδύνων. Με όρους διαχείρισης κινδύνου, μια DPIA αποσκοπεί στη «διαχείριση των

κινδύνων» για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, με χρήση των ακόλουθων διαδικασιών, μέσω:

- του καθορισμού του πλαισίου: «λαμβάνοντας υπόψη τη φύση, την έκταση, το πλαίσιο και τους σκοπούς της επεξεργασίας και τις πηγές του κινδύνου»·
- της εκτίμησης των κινδύνων: «ώστε να εκτιμήσει την ιδιαίτερη πιθανότητα και τη σοβαρότητα του υψηλού κινδύνου»·
- της αντιμετώπισης των κινδύνων: «που μετριάζουν αυτόν τον κίνδυνο» και «διασφαλίζουν την προστασία των δεδομένων προσωπικού χαρακτήρα» και «αποδεικνύουν τη συμμόρφωση προς τον παρόντα κανονισμό».

Η DPIA κατά τον κανονισμό αποτελεί εργαλείο διαχείρισης των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων και, επομένως, υιοθετεί τη δική τους οπτική, όπως ισχύει σε ορισμένους τομείς (π.χ. κοινωνική ασφάλεια). Αντιθέτως, σε άλλους τομείς η διαχείριση των κινδύνων (π.χ. ασφάλεια πληροφοριών) επικεντρώνεται στην οργανωτική διάρθρωση.

Ο κανονισμός παρέχει ευελιξία στους υπεύθυνους επεξεργασίας για τον καθορισμό της ακριβούς δομής και της μορφής της DPIA, προκειμένου αυτή να εξυπηρετεί τις υφιστάμενες πρακτικές εργασίας. Υπάρχουν πολυάριθμες καθιερωμένες διαδικασίες, εντός της ΕΕ και παγκοσμίως, που λαμβάνουν υπόψη τα στοιχεία που περιγράφονται στην αιτιολογική σκέψη 90. Ωστόσο, ανεξαρτήτως της μορφής που θα λάβει, η DPIA θα πρέπει να αποτελεί μια πραγματική αξιολόγηση των κινδύνων, που θα παρέχει στους υπεύθυνους επεξεργασίας τη δυνατότητα να λάβουν μέτρα για την αντιμετώπισή τους. Διαφορετικές μεθοδολογίες, θα μπορούσαν, να χρησιμοποιηθούν για να συνδράμουν στην υλοποίηση των βασικών απαιτήσεων, που θέτει ο κανονισμός.

Έχουν προσδιοριστεί ορισμένα κοινά κριτήρια, ώστε να επιτρέπεται στους υπεύθυνους επεξεργασίας, να υιοθετούν διαφορετικές προσεγγίσεις, συμμορφούμενοι παράλληλα με τον κανονισμό. Τα εν λόγω κριτήρια αποσαφηνίζουν τις βασικές απαιτήσεις του κανονισμού και παρέχουν επαρκές έδαφος για τη χρήση διαφορετικών μορφών υλοποίησης. Τα εν λόγω κριτήρια μπορούν να χρησιμοποιηθούν για την απόδειξη ότι μια συγκεκριμένη μεθοδολογία DPIA πληροί τα απαιτούμενα πρότυπα που θέτει ο κανονισμός[54] .

[54] Κατευθυντήριες γραμμές για την εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) και καθορισμός του κατά πόσον η επεξεργασία «ενδέχεται να επιφέρει υψηλό κίνδυνο» για τους σκοπούς του κανονισμού 2016/679 http://ec.europa.eu/justice/data-protection/index_en.htm

3.2.6 Βήματα εκτέλεσης DPIA

Βήμα 1 - Προκαταρκτική αξιολόγηση και κριτήρια που καθορίζουν την ανάγκη διεξαγωγής μιας DPIA

Ο στόχος του πρώτου βήματος είναι να παρέχει καθοδήγηση στον ιδιοκτήτη του συστήματος ή της υπηρεσίας να διαπιστώσει εάν είναι απαραίτητη μια DPIA και ποιος θα πρέπει να διεξάγει αυτή την DPIA. Προτείνεται συνεπώς στον ιδιοκτήτη του συστήματος να πραγματοποιήσει μια αρχική ανάλυση της υπό εξέταση αίτησης και να αποφασίσει εάν θα προχωρήσει στα επόμενα βήματα της DPIA ή θα σταματήσει τη διαδικασία. Κατά τη διάρκεια αυτού του βήματος θα πρέπει να απαντηθούν βασικά ερωτήματα :

1) Γίνεται επεξεργασία προσωπικών δεδομένων;
2) Λειτουργεί ως εκτελών την επεξεργασία ή ως υπεύθυνος επεξεργασίας;
3) Υπάρχει αντίκτυπο στα δικαιώματα και τις ελευθέριες του ατόμου;
4) Σε ποιο στάδιο της ανάπτυξης θα πρέπει να διενεργηθεί η DPIA;
5) Ποιος είναι ο σκοπός της υπηρεσίας ή του συστήματος που επεξεργάζεται προσωπικά δεδομένα;

Οι θετικές απαντήσεις υποστηρίζουν την ανάγκη διεξαγωγής μιας DPIA. Δεν πρόκειται για ποσοτική άσκηση. Αυτό σημαίνει ότι μία μόνο θετική απάντηση θα μπορούσε να καταστήσει αναγκαία τη διεξαγωγή μιας DPIA.

Βήμα 2 - Αρχικοποίηση

Κατά την εκκίνηση μιας DPIA πρέπει να λαμβάνονται υπόψη διαφορετικά στοιχεία και να αποτυπώνονται :

1) Καταγραφή ομάδας έργου
2) Καταγραφή ρόλου ομάδας ή ατόμου
3) Καταγραφή αρμοδιοτήτων ομάδας έργου
4) Καταγραφή συνεντευξιαζόμενων και εγγράφων που παρέχονται

Βήμα 3 - Προσδιορισμός, χαρακτηρισμός και περιγραφή των συστημάτων / εφαρμογών που επεξεργάζονται δεδομένα προσωπικού χαρακτήρα

Σε αυτό το βήμα, ο ιδιοκτήτης του συστήματος, πρέπει να δώσει μια ολοκληρωμένη και πλήρη εικόνα της εφαρμογής, του περιβάλλοντος, των επεξεργασμένων δεδομένων και των ορίων του συστήματος. Πρέπει να περιγραφεί, ο σχεδιασμός της εφαρμογής, οι γειτονικές διεπαφές με άλλα συστήματα και οι ροές πληροφοριών. Τα διαγράμματα ροής δεδομένων, που δείχνουν επεξεργασία πρωτογενών και δευτερευόντων δεδομένων, συνιστώνται για την απεικόνιση της προέλευσης, της

θέσης και του προορισμού των δεδομένων. Οι δομές δεδομένων, πρέπει επίσης να τεκμηριώνονται, έτσι ώστε να μπορούν να αναλυθούν πιθανοί σύνδεσμοι.

Βήμα 4 - Προσδιορισμός των πιθανών κινδύνων

Ο στόχος αυτού του βήματος είναι να προσδιοριστούν οι συνθήκες και οι δυνητικοί κίνδυνοι που ενδέχεται να απειλήσουν ή να διακυβεύσουν τα προσωπικά δεδομένα του υποκειμένου των δεδομένων και να επηρεάσουν την ιδιωτική του ζωή με βάση κανονισμό. Μια διαδικασία εκτίμησης κινδύνου θα πρέπει συνήθως να εξετάζει τους κινδύνους από την άποψη της πιθανότητας εμφάνισης (likelihood) και τον αντίκτυπο των συνεπειών τους (impact). Αυτοί οι κίνδυνοι απορρήτου, αποτελούνται κυρίως από ένα ακραίο γεγονός και τις απειλές που θα μπορούσαν να πυροδοτήσουν αυτό το γεγονός (πολλές απειλές μπορούν να προκαλέσουν το ίδιο γεγονός). Ο υπεύθυνος προστασίας θα πρέπει να συμμετέχει στην ανάλυση αυτή, όπως έχει ήδη προταθεί.

Τα ακραία γεγονότα αντιπροσωπεύουν τις ακόλουθες καταστάσεις που πρέπει να αποφευχθούν:

1. Μη διαθεσιμότητα των νομικών διαδικασιών: δεν υπάρχουν ή δεν υπάρχουν πλέον ή δεν λειτουργούν
2. Αλλαγή της επεξεργασίας: αποκλίνει από αυτό που είχε αρχικά προγραμματιστεί (εκτροπή του σκοπού, υπερβολική ή αθέμιτη συλλογή ...).
3. Αθέμιτη πρόσβαση σε προσωπικά δεδομένα: αποκαλύπτονται σε μη εξουσιοδοτημένα άτομα.
4. Ανεπιθύμητη αλλαγή στα προσωπικά δεδομένα: τροποποιούνται ή αλλάζουν.
5. Εξαφάνιση προσωπικών δεδομένων: καταστρέφονται ή δεν είναι πλέον διαθέσιμα.
6. Γνωστοποίηση των προσωπικών δεδομένων σε άλλους: διανέμονται σε άτομα που δεν χρειάζονται.

Κάθε φορά που ένα τέτοιο γεγονός μπορεί να συμβεί, επιφέρει επιπτώσεις στην ιδιωτική ζωή των υποκειμένων των δεδομένων και οι εν λόγω επιπτώσεις θα πρέπει να αξιολογούνται δεόντως και συστηματικά και τελικά να μετριάζονται. Ατυχώς ή εσκεμμένα, αυτά τα γεγονότα μπορούν να δημιουργηθούν από μία ή περισσότερες πηγές κινδύνου :

Εσωτερική πηγή: πρόσωπα που ανήκουν στον οργανισμό, χρήστης, διαχειριστής συστήματος, διαχειριστής δικτύου, υπηρεσία χειριστής τηλεφωνικού κέντρου, υπάλληλο εμπορικής υπηρεσίας.

Εξωτερικοί συνεργάτες: άτομα εκτός του οργανισμού: αποδέκτης, πάροχος, ανταγωνιστής, εξουσιοδοτημένο τρίτο μέρος, κυβερνητική οργάνωση, ανθρώπινη δραστηριότητα που περιβάλλει, εξωτερική / υπεργολαβία.

Μη ανθρώπινες πηγές: προβληματικοί αισθητήρες, ιός υπολογιστών, φυσική καταστροφή όπως κεραυνός, ενεργειακή ανισορροπία, διακοπή ρεύματος, διακοπή λειτουργίας.

Βήμα 5 - Αξιολόγηση κινδύνου προστασίας δεδομένων

Σε αυτό το βήμα, τα προσδιορισμένα ακραία γεγονότα και οι σχετικές απειλές θα αξιολογούνται και θα μετρούνται με βάση τη σοβαρότητα των επιπτώσεων στα άτομα και την πιθανότητα εμφάνισης. Για να ταξινομηθούν οι επιπτώσεις και η πιθανότητα, μπορούν να χρησιμοποιηθούν αρκετά ευρέως διαθέσιμα μοντέλα. Είναι αποδεκτή η χρήση εναλλακτικών μεθοδολογιών είτε βιομηχανικών είτε εσωτερικών, εφόσον οι κίνδυνοι για την προστασία της ιδιωτικής ζωής που μπορούν να επηρεάσουν το υποκείμενο των δεδομένων προσδιορίζονται και ποσοτικοποιούνται κατάλληλα.

Βήμα 6 – Προσδιορισμός, σύσταση ελέγχων και υπολειπόμενοι κίνδυνοι

Στο στάδιο αυτό, ο στόχος είναι να εξεταστούν οι κίνδυνοι που εντοπίστηκαν και αξιολογήθηκαν στο προηγούμενο στάδιο και να παρουσιαστούν οι έλεγχοι που έχουν εφαρμοστεί ή πρόκειται να εφαρμοστούν προκειμένου να μειωθεί ο κίνδυνος σε κατάλληλα επίπεδα. Κάθε προσδιορισμένος κίνδυνος πρέπει να μετριαστεί κατάλληλα με έναν ή περισσότερους ελέγχους, λαμβάνοντας υπόψη την πιθανότητα και τον αντίκτυπό τους. Οι έλεγχοι που έχουν εγκριθεί ή έχουν ήδη σχεδιαστεί από τον ιδιοκτήτη του συστήματος πρέπει να καλύπτουν τις ακόλουθες διαστάσεις:

- Η υποδομή (δίκτυο επικοινωνιών, προστασία εξοπλισμού, κλπ.).
- Οι υπάλληλοι / προσωπικό που εμπλέκονται στη διαδικασία (μηχανισμοί πρόσβασης, ελέγχου κ.λπ.).
- Η οργάνωση και οι διαδικασίες.
- Οι τεχνολογίες (μέτρα προστασίας του συστήματος, συμπεριλαμβανομένου του ελέγχου ασφάλειας και της μεθοδολογίας ασφάλειας με βάση την τεχνολογία, κ.λπ.).

Η έκθεση DPIA πρέπει να εξηγεί λεπτομερώς τον τρόπο με τον οποίο οι επιλεγόμενοι (εφαρμοζόμενοι ή προγραμματισμένοι) έλεγχοι σχετίζονται με συγκεκριμένους κινδύνους και πρέπει να αποδεικνύουν, ότι οδηγούν σε αποδεκτά επίπεδα κινδύνου. Όταν ο κίνδυνος μοιράζεται με τρίτους, ο κάτοχος του συστήματος, θα πρέπει επίσης να διευκρινίσει ποιον έλεγχο έχει εφαρμόσει ή

σκοπεύει να εφαρμόσει αυτό το τρίτο μέρος προκειμένου να αντιμετωπίσει αυτόν τον κίνδυνο με αποδεκτό τρόπο. Συνιστάται επίσης, να σχεδιαστεί και να εφαρμοστεί μια εσωτερική διαδικασία, με σκοπό την τακτική επαλήθευση της ύπαρξης συγκεκριμένων ελέγχων (π.χ. διενέργεια ελέγχων σε τακτική βάση, ο οποίος αποτελεί τον τελικό έλεγχο.

Βήμα 7 - Τεκμηρίωση και σύνταξη της έκθεσης DPIA

Οι επιδόσεις της DPIA μετά τις φάσεις που προσδιορίστηκαν παραπάνω πρέπει να τεκμηριώνονται δεόντως και τα αποτελέσματά της να παρουσιάζονται στην τελική έκθεση DPIA. Η έκθεση DPIA μπορεί να δομηθεί γύρω από τις φάσεις της εργασίας που περιγράφονται σε αυτό το έγγραφο, παρουσιάζοντας τα αποτελέσματα κάθε φάσης στον αναγνώστη, επισυνάπτοντας οποιαδήποτε δικαιολογητικά ή υλικό που χρησιμοποιήθηκε στην αξιολόγηση. Ο στόχος της τεκμηρίωσης είναι διττός: α) να διευκολυνθεί η εφαρμογή της διαδικασίας και β) να εκπονηθεί τελική έκθεση η οποία θα μπορούσε να υποβληθεί στην ΑΠΔΠΧ εάν ζητηθεί. Ως εκ τούτου, η ανάλυση που πραγματοποιήθηκε και η τεκμηρίωσή της, ίσως χρειαστεί να εξασφαλιστούν κατάλληλα, σύμφωνα με το σύστημα ταξινόμησης πληροφοριών του οργανισμού. Η υπογεγραμμένη έκθεση DPIA, η οποία περιέχει εγκεκριμένη απόφαση, θα πρέπει να δίδεται στον υπεύθυνο προστασίας δεδομένων του εκάστοτε οργανισμού (εάν υπάρχει) σύμφωνα με τις εσωτερικές διαδικασίες του ιδιοκτήτη του συστήματος.

Βήμα 8 - Αναθεώρηση και συντήρηση

Σκοπός αυτής της φάσης είναι να διασφαλιστεί ότι η ανάληψη υποχρέωσης που απορρέει από την διεξαχθείσα DPIA διεξάγεται στο υπάρχον σύστημα ή στο έργο που υλοποιείται. Προτείνονται οι ακόλουθες εργασίες:

1.Επανεξέταση της εφαρμογής των ελέγχων μετριασμού και αποφυγής κινδύνου που εντοπίστηκαν στην DPIA.

2. Προετοιμασία έκθεσης ανασκόπησης.

3. Παρουσίαση της έκθεσης ανασκόπησης απορρήτου στα ανώτερα διευθυντικά στελέχη και τον DPO εφόσον υπάρχει.

4. Δημοσιοποίηση της έκθεσης απορρήτου.

5. Αξιολόγηση της ανάγκης για αναθεώρηση της DPIA μετά από ορισμένο χρονικό διάστημα ή μετά την ολοκλήρωση ενός νέου σταδίου στο έργο ή το πρόγραμμα. Η ανασκόπηση μπορεί να ενσωματωθεί στις τυπικές, περιοδικές ή περιστασιακές εσωτερικές διαδικασίες του οργανισμού.

3.2.7 Κριτήρια για μια αποδεκτή DPIA

Η ομάδα εργασίας του άρθρου 29 προτείνει τα ακόλουθα κριτήρια, τα οποία οι υπεύθυνοι επεξεργασίας, μπορούν να χρησιμοποιούν για να αξιολογούν, κατά πόσο μια ΕΑΠΔ ή μια μεθοδολογία διενέργειας DPIA είναι επαρκώς περιεκτική προκειμένου να συμμορφώνεται με τον κανονισμό:

1. παρέχεται συστηματική περιγραφή των πράξεων επεξεργασίας [άρθρο 35 παράγραφος 7 στοιχείο α)]:

α. λαμβάνονται υπόψη η φύση, η έκταση, το πλαίσιο και οι σκοποί της επεξεργασίας (αιτιολογική σκέψη 90)·

β. καταγράφονται τα δεδομένα προσωπικού χαρακτήρα, οι αποδέκτες και η περίοδος αποθήκευσης των δεδομένων προσωπικού χαρακτήρα·

γ. παρέχεται λειτουργική περιγραφή της πράξης επεξεργασίας·

δ. προσδιορίζονται τα στοιχεία του ενεργητικού στα οποία εναποτίθενται τα δεδομένα (λογισμικό, δίκτυα, πρόσωπα, έντυπα ή δίαυλοι διαβίβασης εντύπων)·

ε. λαμβάνεται υπόψη η συμμόρφωση με εγκεκριμένους κώδικες δεοντολογίας (άρθρο 35 παράγραφος 8)·

2. εκτιμώνται η αναγκαιότητα και η αναλογικότητα [άρθρο 35 παράγραφος 7 στοιχείο β)]·

α. καθορίζονται τα προβλεπόμενα μέτρα συμμόρφωσης με τον κανονισμό [άρθρο 35 παράγραφος 7 στοιχείο δ) και αιτιολογική σκέψη 90], λαμβάνοντας υπόψη:

i. τα μέτρα που κατατείνουν στην αναλογικότητα και την αναγκαιότητα της επεξεργασίας βάσει:

- καθορισμένων, ρητών και νόμιμων σκοπών [άρθρο 5 παράγραφος 1 στοιχείο β)]·
- της νομιμότητας της επεξεργασίας (άρθρο 6)·
- κατάλληλων, συναφών και περιορισμένων στα αναγκαία δεδομένων [άρθρο 5 παράγραφος 1 στοιχείο γ)]·
- της περιορισμένης διάρκειας αποθήκευσης [άρθρο 5 παράγραφος 1 στοιχείο ε)]·

ii. μέτρα που συμβάλλουν στη διαφύλαξη των δικαιωμάτων των υποκειμένων

- πληροφορίες που παρέχονται στο υποκείμενο των δεδομένων (άρθρα 12, 13 και 14)
- δικαίωμα πρόσβασης και δικαίωμα στη φορητότητα των δεδομένων (άρθρα 15 και 20)·
- δικαίωμα διόρθωσης και διαγραφής (άρθρα 16, 17 και 19)·
- δικαίωμα εναντίωσης και περιορισμού της επεξεργασίας (άρθρα 18, 19 και 21)·

- σχέσεις με τους εκτελούντες την επεξεργασία (άρθρο 28)·
- διασφαλίζονται οι περιστάσεις που περιβάλλουν τη διεθνή διαβίβαση ή τις διεθνείς διαβιβάσεις (Κεφάλαιο V)
- προηγούμενη διαβούλευση (άρθρο 36).

3. τελούν υπό διαχείριση οι κίνδυνοι για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων [άρθρο 35 παράγραφος 7 στοιχείο γ)]:

α. έχουν αξιολογηθεί η προέλευση, η φύση, η ιδιαιτερότητα και η σοβαρότητα των κινδύνων (πρβλ. αιτιολογική σκέψη 84) ή ειδικότερα κάθε κίνδυνος (αθέμιτη πρόσβαση, ανεπιθύμητη τροποποίηση, και εξαφάνιση δεδομένων) από την οπτική των υποκειμένων των δεδομένων·

i. έχουν ληφθεί υπόψη οι πηγές των κινδύνων (αιτιολογική σκέψη 90)·

ii. εξακριβώνονται οι δυνητικές επιπτώσεις στα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων σε περιπτώσεις συμβάντων που περιλαμβάνουν.

3.2.8 Κόστος εφαρμογής της DPIA

Η υποχρέωση των εκτελούντων της επεξεργασίας προσωπικών δεδομένων να διενεργούν εκτίμηση των επιπτώσεων σχετικά με την προστασία των δεδομένων (DPIA), όπου η επεξεργασία φαίνεται να παρουσιάζει κινδύνους για τα δικαιώματα και τις ελευθερίες των ατόμων, επιφέρει ένα επιπλέον κόστος για τον εκάστοτε οργανισμό, με την έννοια ότι χρειάζεται πόρους, για να εκτελέσει την εν λόγω εκτίμηση. Η εκτίμηση του πιθανού κόστους της DPIA, εξαρτάται από έναν σημαντικό αριθμό παραγόντων. Το μέγεθος και η αυστηρότητα της DPIA θα εξαρτηθούν κυρίως από το πώς, ο οργανισμός αντιλαμβάνεται τους κινδύνους αλλά και τη σοβαρότητα με την οποία τους αντιμετωπίζει. Η εκτίμηση του πιθανού κόστους της DPIA εξαρτάται από τους ενδεικτικά κάτωθι συναφείς παράγοντες:

- μέγεθος της εκτίμησης,
- αυστηρότητα της νομοθεσίας,
- συμμετοχή των εμπλεκόμενων μερών,
- πρόσληψη ειδικού στελέχους για την εκτέλεση της εκτίμησης.

Προσθέτοντας όλες τις παραπάνω πιθανές δαπάνες γίνεται κατανοητό πως η DPIA αποτελεί μια διαδικασία που κοστίζει αρκετά. Το ζήτημα που εγείρεται, είναι αν το όφελος από την DPIA, όντως καλύπτει το κόστος της, κάτι που μπορεί να εξακριβωθεί από μια ανάλυση κόστους-οφέλους, λαμβάνοντας όμως υπόψη και επιπλέον ποιοτικούς παράγοντες .

3.3 Ανάλυση αποκλίσεων (GAP Analysis)

Σκοπός της ανάλυσης αποκλίσεων (GAP analysis) είναι, να βοηθήσει την εταιρεία ή τον οργανισμό να καταλάβει που βρίσκεται σχετικά με την συμμόρφωση του ως προς το GDPR. Εκτός από βασική διεργασία που θα πρέπει να εκτελεστεί, ώστε να βοηθήσει στην αναγνώριση των κενών που προκύπτουν ως προς την συμμόρφωση, μπορεί να βοηθήσει και στην εξέλιξή της συμμόρφωσης ως μέτρο σύγκρισης και μέτρησης της προόδου που έχει γίνει. Επίσης η ανάλυση αποκλίσεων μπορεί να :

- Βοηθήσει την εταιρεία ώστε να επικεντρωθεί στις βασικές αρχές του GDPR
- Βοηθήσει την εταιρεία να δώσει την σωστή βαρύτητα στα δικαιώματα του ατόμου
- Βοηθήσει στην κατανόηση του βασικού σκοπού της εταιρείας
- Αναδείξει κενά ως προς νομικές υποχρεώσεις εκτός GDPR
- Δώσει μια γενική εικόνα των ελέγχων ιδιωτικότητας που εφαρμόζονται
- Δώσει μια γενική εικόνα των πολιτικών και των διαδικασιών που μπορούν να έχουν αντίκτυπο στην ιδιωτικότητα
- Αναδείξει κινδύνους για την προστασία δεδομένων

Η ανάλυση αποκλίσεων θα πρέπει να εκτελείται μέσω ερωτήσεων οι οποίες να καλύπτουν ξεκάθαρα τις ανάγκες των παρακάτω τομέων:

1. Ενημέρωση για θέματα προστασίας δεδομένων
2. Πληροφορίες και δεδομένα που διατηρούνται
3. Επικοινωνία σχετικά με θέματα προστασίας δεδομένων
4. Ατομικά δικαιώματα
5. Θέματα αιτήσεων πρόσβασης
6. Νομική βάση για την επεξεργασία δεδομένων προσωπικού χαρακτήρα
7. Παιδιά
8. Συγκατάθεση
9. Παραβιάσεις δεδομένων
10. Προστασία δεδομένων κατά τον σχεδιασμό - Εκτιμήσεις επιπτώσεων προστασίας
11. Υπεύθυνοι προστασίας δεδομένων
12. Διεθνές περιβάλλον

3.3.1 Μεθοδολογία εκτέλεσης ανάλυσης αποκλίσεων

Η μεθοδολογία εκτέλεσης της ανάλυσης αποκλίσεων θα πρέπει να περιλαμβάνει ένα σετ ερωτήσεων, με βάση το οποίο θα μπορεί να αποτυπώνεται η πραγματική εικόνα ως προς τη προστασία των δεδομένων αλλά και σε σχέση με της ανάγκες του

GDPR. Για αυτό το σκοπό είναι απαραίτητο το πλαίσιο να είναι οριοθετημένο με βάση τους τομείς που αναφέρθηκαν στην προηγούμενη ενότητα.

- Ενημέρωση για θέματα προστασίας δεδομένων: Οι υπεύθυνοι λήψης αποφάσεων και οι εργαζόμενοι στον οργανισμό γνωρίζουν και είναι ενημερωμένοι για το GDPR καθώς και να μπορούν να κατανοήσουν το αντίκτυπο.
- Πληροφορίες και δεδομένα που διατηρούνται: Θα πρέπει να τεκμηριωθεί ποια προσωπικά δεδομένα διατηρούνται, από πού προήλθαν και με ποιον μοιράζονται.
- Επικοινωνία σχετικά με θέματα προστασίας δεδομένων: Θα πρέπει να ελεγχθούν οι τρέχουσες ειδοποιήσεις απορρήτου και δημιουργηθεί ένα σχέδιο δράσης.
- Ατομικά δικαιώματα: Θα πρέπει να γίνει έλεγχος στις διαδικασίες για να βεβαιωθεί ότι καλύπτουν όλα τα δικαιώματα που πρέπει να έχουν τα άτομα.
- Θέματα αιτήσεων πρόσβασης: Θα πρέπει να ενημερωθούν οι διαδικασίες και να σχεδιαστεί τρόπος χειρισμού αιτημάτων εντός των νέων χρονοδιαγραμμάτων για την παροχή πληροφοριών προς τα υποκείμενα επεξεργασίας.
- Νομική βάση για την επεξεργασία δεδομένων προσωπικού χαρακτήρα: Θα πρέπει να προσδιοριστεί η νόμιμη βάση για την επεξεργασία.
- Παιδιά: Θα πρέπει να εξεταστεί αν μπορούν να τεθούν σε εφαρμογή συστήματα για την επαλήθευση της ηλικίας και να λάβουν τη συγκατάθεση των γονέων ή των κηδεμόνων οποιαδήποτε δραστηριότητα επεξεργασίας δεδομένων για παιδία.
- Συγκατάθεση: Θα πρέπει να ελεγχθεί ο τρόπος αναζήτησης, καταγραφής και διαχείρισης τη συγκατάθεσης.
- Παραβιάσεις δεδομένων: Πρέπει να εξεταστεί ότι υπάρχουν οι σωστές διαδικασίες για την ανιχνεύση παραβίασης δεδομένων.
- Προστασία δεδομένων κατά τον σχεδιασμό - εκτιμήσεις επιπτώσεων προστασίας: Θα πρέπει να υπάρχει εξοικείωση με τον κώδικα πρακτικής για την αξιολόγηση επιπτώσεων στην ιδιωτική ζωή καθώς και εναρμόνιση με τις τελευταίες κατευθυντήριες γραμμές του Άρθρου 29 της Ομάδας εργασίας.
- Υπεύθυνοι προστασίας δεδομένων : Θα πρέπει να οριστεί κάποιος που θα αναλάβει την ευθύνη για τη συμμόρφωση με την προστασία των δεδομένων και να εκτιμήσει.

- Διεθνές περιβάλλον: Εάν ο οργανισμός λειτουργεί σε περισσότερες από μία χώρες της ΕΕ (δηλαδή διεξάγονται διασυνοριακές συναλλαγές επεξεργασίας), θα πρέπει να καθοριστούν τα δεδομένα του οδηγού και να γνωστοποιηθούν στην εποπτικής αρχής προστασίας.

3.4 Η κρυπτογράφηση και η ψευδωνυμοποίηση ως προτεινόμενα τεχνικά μέτρα στον ΓΚΠΔ

3.4.1 Ορισμοί

Στον ΓΚΠΔ δεν περιλαμβάνεται ένας ακριβής ορισμός της κρυπτογράφησης. Ωστόσο, ο όρος αυτός θα μπορούσε να περιγραφεί ως η εφαρμογή μιας διαδικασίας μετασχηματισμού μέσω κάποιου αλγορίθμου με τη χρήση «κλειδιών κρυπτογράφησης» (encryption keys), ενός συνόλου προσωπικών δεδομένων σε μία ακατανόητη (ακατάληπτη) μορφή ώστε να μην μπορούν να αναγνωσθούν από κανέναν εκτός του(ων) νόμιμου(ων) ιδιοκτήτη(τών) των κλειδιών κρυπτογράφησης.

Αντιθέτως, ο ΓΚΠΔ ορίζει επαρκώς την τεχνική της ψευδωνυμοποίησης. Σύμφωνα με το άρθρο 4 παρ. 5: «ψευδωνυμοποίηση είναι η επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τέτοιο τρόπο, ώστε τα δεδομένα να μην μπορούν πλέον, να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρωματικές πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλιστεί ότι δεν μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο». Ωστόσο, ένας όρος που συχνά συγχέεται με την ψευδωνυποποίηση στο πεδίο της ασφάλειας και της προστασίας των προσωπικών δεδομένων είναι η ανωνυμοποίηση. Ουσιαστικά πρόκειται για δύο διαφορετικές τεχνικές που θα πρέπει να διαχωρίζονται μεταξύ τους, πολύ περισσότερο μάλιστα στο πλαίσιο του ΓΚΠΔ, δεδομένου ότι τα «ανωνυμοποιημένα δεδομένα» και τα «ψευδωνυποιημένα δεδομένα» αντιμετωπίζονται ως δύο εντελώς διαφορετικές κατηγορίες.

Ως ανωνυμοποίηση ορίζεται η διαδικασία διαγραφής των αναγνωριστικών προσωπικού χαρακτήρα σε εγγραφές δεδομένων, έτσι ώστε να μην είναι πλέον εφικτό τα ανωνυμοποιημένα δεδομένα να συσχετιστούν με το υποκείμενο των δεδομένων[55].

Κατά συνέπεια από τους δύο αυτούς ορισμούς (δηλαδή αυτούς της ψευδωνυμοποίησης και της ανωνυμοποίησης) προκύπτει ότι, η χρήση της

[55] *Κ. Λαμπρινουδάκης, Σ. Γκρίτζαλης, Λ. Μήτρου, Σ. Κάτσικας,* Προστασία της Ιδιωτικότητας & Τεχνολογίες Πληροφορικής και Επικοινωνιών, 2010, σελ. 56

ανωνυμοποίησης έχει ως αποτέλεσμα την αδυναμία προσδιορισμού του υποκειμένου των δεδομένων, ενώ η ψευδωνυμοποίηση αντικαθιστά την ταυτότητα του υποκειμένου των δεδομένων με τέτοιο τρόπο, ώστε να απαιτούνται πρόσθετες πληροφορίες για την εκ νέου αναγνώριση του υποκειμένου των δεδομένων.

Βάσει του κανονισμού [Αιτ. Σκέψη υπ' αριθμ. (26)], οι βασικές αρχές της προστασίας δεδομένων δεν θα πρέπει να εφαρμόζονται σε ανώνυμες πληροφορίες, δηλαδή σε πληροφορίες που δεν μπορούν να συσχετιστούν με ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο, ή σε δεδομένα προσωπικού χαρακτήρα που έχουν καταστεί ανώνυμα κατά τρόπο ώστε η ταυτότητα του υποκειμένου των δεδομένων να μην μπορεί ή να μην μπορεί πλέον να εξακριβωθεί. Ως εκ τούτου, ο ΓΚΠΔ δεν αφορά την επεξεργασία τέτοιων ανώνυμων πληροφοριών. Αντιθέτως, τα δεδομένα προσωπικού χαρακτήρα, που έχουν υποστεί ψευδωνυμοποίηση, συνεχίζουν να θεωρούνται πληροφορίες σχετικά με ταυτοποιήσιμο φυσικό πρόσωπο και κατά συνέπεια συνεχίζουν να εμπίπτουν στις διατάξεις και στους περιορισμούς του ΓΚΠΔ.

3.4.2 Η υιοθέτηση των τεχνικών κρυπτογράφησης και ψευδωνυμοποίησης από μια εταιρεία

Η κρυπτογράφηση και η ψευδωνυμοποίηση μπορούν να μειώσουν σημαντικά τους κινδύνους που σχετίζονται με την επεξεργασία δεδομένων. Για τον λόγο αυτόν, ο ΓΚΠΔ παροτρύνει και δημιουργεί κίνητρα για τους υπεύθυνους επεξεργασίας να εφαρμόζουν τις τεχνικές αυτές στα προσωπικά δεδομένα που συλλέγουν, μέσω μάλιστα και της ελαστικοποίησης ορισμένων απαιτήσεων που τους αφορούν σε ορισμένα σημαντικά άρθρα του κανονισμού.

Ήδη από το άρθρο 6 («Νομιμότητα της επεξεργασίας»), όταν «η επεξεργασία για σκοπό άλλον από αυτόν για τον οποίο έχουν συλλεχθεί τα δεδομένα προσωπικού χαρακτήρα, δεν βασίζεται στη συγκατάθεση του υποκειμένου των δεδομένων ή στο δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, ο υπεύθυνος επεξεργασίας, προκειμένου να εξακριβωθεί κατά πόσο η επεξεργασία για άλλο σκοπό είναι συμβατή με τον σκοπό για τον οποίο συλλέγονται αρχικώς τα δεδομένα προσωπικού χαρακτήρα, λαμβάνει υπόψη, μεταξύ άλλων την ύπαρξη κατάλληλων εγγυήσεων, που μπορεί να περιλαμβάνουν κρυπτογράφηση ή ψευδωνυμοποίηση».

Η «Προστασία των Δεδομένων ήδη από τον Σχεδιασμό και εξ' Ορισμού» (data protection by design and by default), που περιγράφεται στο άρθρο 25, προβλέπει, ότι ο υπεύθυνος επεξεργασίας θα πρέπει να εφαρμόζει αποτελεσματικά, τόσο κατά τη στιγμή του καθορισμού των μέσων επεξεργασίας όσο και κατά τη στιγμή της επεξεργασίας, κατάλληλα τεχνικά και οργανωτικά μέτρα, όπως η ψευδωνυμοποίηση.

Το άρθρο 32 («Ασφάλεια Επεξεργασίας»), θεωρεί ότι η κρυπτογράφηση και η ψευδωνυμοποίηση δύνανται να διασφαλίσουν το κατάλληλο επίπεδο ασφάλειας στα δεδομένα προσωπικού χαρακτήρα έναντι των κινδύνων. Παράλληλα, στο άρθρο 34 («Ανακοίνωση Παραβίασης Δεδομένων Προσωπικού Χαρακτήρα στο Υποκείμενο των Δεδομένων») καθορίζεται ότι, δεν απαιτείται ενημέρωση του υποκειμένου των δεδομένων σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα που το αφορούν, εφόσον τα δεδομένα αυτά (μεταξύ και άλλων προϋποθέσεων) είναι κρυπτογραφημένα. Βάσει του άρθρου 40 («Κώδικες Δεοντολογίας»), ενώσεις και άλλοι φορείς που εκπροσωπούν κατηγορίες υπευθύνων επεξεργασίας παροτρύνονται να εκπονούν κώδικες δεοντολογίας, προκειμένου να προσδιορίσουν την εφαρμογή του κανονισμού ΓΚΠΔ όσον αφορά μεταξύ άλλων και την ψευδωνυμοποίηση των δεδομένων προσωπικού χαρακτήρα. Τέλος, στο άρθρο 89 («Διασφαλίσεις και παρεκκλίσεις σχετικά με την επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς») η ψευδωνυμοποίηση περιλαμβάνεται μεταξύ των εγγυήσεων ότι έχουν θεσπιστεί τα κατάλληλα τεχνικά και οργανωτικά μέτρα όταν τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε (περαιτέρω) επεξεργασία για λόγους αρχειοθέτησης για λόγους γενικού συμφέροντος, επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς.

Κεφάλαιο Δ'

Ζητήματα παραβίασης προσωπικών δεδομένων και ρήτρες εφαρμοστέου δικαίου/ διεθνούς δικαιοδοσίας στο ηλεκτρονικό εμπόριο

4. Εισαγωγικά

Ακριβώς επειδή σε μια ηλεκτρονική σύμβαση τα δύο αντισυμβαλλόμενα μέρη δεν βρίσκονται στον ίδιο φυσικό χώρο, αλλά δρουν δικαιοπρακτικά μέσω ενός Η/Υ, δημιουργείται γόνιμο έδαφος για την ολοκλήρωση συμφωνιών σε διασυνοριακό επίπεδο. Αποτελεί σύνηθες φαινόμενο στις μέρες μας, για παράδειγμα, ένας πολίτης-καταναλωτής κράτους μέλους της ΕΕ να προβαίνει συστηματικά σε αγορές προϊόντων τα οποία πωλεί μια επιχείρηση, η οποία έχει την έδρα της σε ένα άλλο κράτος μέλος της ΕΕ ή ακόμη και εκτός αυτής. Καθώς όμως μια ηλεκτρονική σύμβαση μπορεί να συνδέεται με περισσότερες από μία έννομες τάξεις, είναι σαφές ότι οι εθνικοί κανόνες δικαίου του εκάστοτε κράτους περιέχουν διαφορετικές μεταξύ τους ρυθμίσεις. Εγείρονται, λοιπόν, ερωτήματα σχετικά με τις διαφορές που μπορεί να προκύψουν από αυτή τη διασυνοριακή δραστηριότητα. Εξάλλου, ο διεθνής χαρακτήρας του ηλεκτρονικού εμπορίου έχει δώσει έναυσμα για επαναπροσδιορισμό των παραδοσιακών κανόνων του Ιδιωτικού Διεθνούς Δικαίου.

4.1 Δικαιοδοσία

Κατ' αρχήν σε μια ηλεκτρονική σύμβαση τα μέρη μπορούν ελεύθερα να συμφωνήσουν ποιας πολιτείας τα δικαστήρια θα είναι αρμόδια να επιλύσουν τις διαφορές που ενδέχεται να προκύψουν. Μάλιστα, στην ιστοσελίδα του προμηθευτή συχνά υπάρχει ένας ρητός όρος παρέκτασης της διεθνούς δικαιοδοσίας, ο οποίος για να έχει ισχύ (όπως και η σύμβαση) θα πρέπει φυσικά να γίνει αποδεκτός από το χρήστη με μια ηλεκτρονικά διαβιβαζόμενη δήλωση βούλησής του.

Στην περίπτωση, που τίθενται όροι στη σύμβαση, οι οποίοι αποκλείουν την υπαγωγή των διαφορών στο φυσικό τους δικαστή, προβλέποντας αποκλειστική αλλοδαπή δικαιοδοσία ή δωσιδικία, είναι καταχρηστικοί, σύμφωνα με το άρθ. 2 § 7 στ. λα' του ν. 2251/1994, αφού αποστερούν τον καταναλωτή από τη δυνατότητα να ζητήσει δικαστική προστασία αποφεύγοντας τα έξοδα, τις δυσκολίες και το ρίσκο εναγωγής του προμηθευτή σε αλλοδαπή χώρα. Η διάταξη αυτή του ν. 2251/1994 αποκτά ιδιαίτερη σημασία όταν ο προμηθευτής έχει την έδρα του εκτός της ΕΕ και η ρήτρα προβλέπει δικαιοδοσία του κράτους, όπου ο ίδιος βρίσκεται, οπότε δεν εφαρμόζεται η προστατευτική νομοθεσία του Κανονισμού «Βρυξέλλες Ι».

Σύμφωνα, λοιπόν, με το άρθ. 4 § 1 του νέου Κανονισμού Βρυξελλών 1215/2012, τα πρόσωπα που έχουν την κατοικία τους σε έδαφος κράτους μέλους της ΕΕ ενάγονται ενώπιον των δικαστηρίων αυτού του κράτους μέλους, ανεξάρτητα από την ιθαγένειά τους. Έτσι, οι αστικές ή εμπορικές διαφορές που προκύπτουν από μια διαδικτυακή συναλλαγή, πρέπει κατ' αρχήν να εισάγονται στο καθ' ύλην αρμόδιο δικαστήριο, στην περιφέρεια του οποίου βρίσκονται η κατοικία (εφόσον πρόκειται για φυσικό πρόσωπο) ή η έδρα (εφόσον πρόκειται για νομικό πρόσωπο) του εναγομένου.

Ωστόσο, η γενική δωσιδικία της κατοικίας παρουσιάζει προβλήματα, διότι πολλοί από τους χρήστες δεν εμφανίζονται με την πραγματική τους ταυτότητα στον εικονικό χώρο του ηλεκτρονικού εμπορίου, αλλά χρησιμοποιούν κωδικούς ή ψευδώνυμα, με αποτέλεσμα ο αντισυμβαλλόμενος να μην γνωρίζει κύρια στοιχεία τους, όπως τον τόπο κατοικίας ή συνήθους διαμονής τους και, συνεπώς, ο προσδιορισμός του κατά τόπον αρμόδιου δικαστηρίου να είναι δυσχερής.

Για να αντιμετωπιστεί αυτό το πρόβλημα ο κοινοτικός νομοθέτης, μέσω του άρθ. 5 § 1 στ. β' της Οδηγίας 2000/31/ΕΚ για το ηλεκτρονικό εμπόριο, υποχρέωσε τους φορείς παροχής υπηρεσιών της κοινωνίας της πληροφορίας να παρέχουν, μεταξύ άλλων, πληροφορίες για τη γεωγραφική διεύθυνση, όπου είναι εγκατεστημένοι.

Επίσης, στις διαφορές που προκύπτουν από τις ηλεκτρονικές συμβάσεις, όπως και σε κάθε εκ συμβάσεως διαφορά, καθιερώνεται συντρέχουσα δικαιοδοσία υπέρ των δικαστηρίων, στην περιφέρεια των οποίων εκπληρώθηκε ή οφείλεται να εκπληρωθεί

η παροχή, σύμφωνα με το άρθ. 7 § 1 στ. α' του Κανονισμού. Έτσι, ο ενάγων μπορεί να προτιμήσει να ενάγει τον αντισυμβαλλόμενό του σε αυτά τα δικαστήρια αντί εκείνου, στην περιφέρεια του οποίου ο τελευταίος έχει την κατοικία ή έδρα του.

Σύμφωνα με το άρθ. 6 § 1, εάν ο εναγόμενος δεν έχει την κατοικία του σε κράτος μέλος της ΕΕ, η διεθνής δικαιοδοσία ρυθμίζεται από το εσωτερικό δίκαιο του δικάζοντος δικαστή. Στην Ελλάδα, η διεθνής δικαιοδοσία των ελληνικών δικαστηρίων σε διαφορές από συμβάσεις ρυθμίζεται από τα άρθ. 3, 22 και 33 ΚΠολΔ και εξαρτάται από τη θεμελίωση τοπικής αρμοδιότητας.

Σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα από κατάστημα ηλεκτρονικού εμπορίου, το υποκείμενο των δεδομένων κινείται ενώπιον των δικαστηρίων του κράτους μέλους, στο οποίο ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία έχουν την εγκατάσταση. Εναλλακτικά, η εν λόγω διαδικασία μπορεί να κινηθεί ενώπιον των δικαστηρίων του κράτους μέλους στο οποίο το υποκείμενο των δεδομένων έχει τη συνήθη διαμονή του.

4.2 Εφαρμοστέο δίκαιο

Όπως και στον Κανονισμό «Βρυξέλλες Ι», επιφυλάσσεται ειδική ρύθμιση και στον Κανονισμό «Ρώμη Ι» για τις περιπτώσεις που ο ένας εκ των δύο συμβαλλομένων σε μια ηλεκτρονική σύμβαση είναι καταναλωτής και, άρα, τυγχάνει μεγαλύτερης προστασίας ως το ασθενέστερο μέρος της συμφωνίας, ενώ υιοθετείται και εδώ η στενή έννοια του «καταναλωτή». Έτσι, λοιπόν, σύμφωνα με το άρθ. 6 § 1 του Κανονισμού, για διαφορές που προκύπτουν από συμβάσεις μεταξύ καταναλωτή και επαγγελματία, εφαρμοστέο είναι το δίκαιο της χώρας όπου ο καταναλωτής έχει τη συνήθη διαμονή του, εφόσον ο επαγγελματίας ασκεί τις δραστηριότητές του στη χώρα αυτή ή τις κατευθύνει με οποιοδήποτε μέσο στη χώρα αυτή ή σε διάφορες χώρες μεταξύ των οποίων και η συγκεκριμένη, και η σύμβαση εμπίπτει στο πεδίο των εν λόγω δραστηριοτήτων.

Βέβαια, τα μέρη εξακολουθούν να έχουν τη δυνατότητα επιλογής του εφαρμοστέου δικαίου, κατά το προεκτεθέν άρθ. 3 § 1, ωστόσο οι αναγκαστικού χαρακτήρα κανόνες δικαίου της χώρας συνήθους διαμονής του καταναλωτή εφαρμόζονται άμεσα και σε κάθε περίπτωση, ακόμη δηλαδή και εάν τα μέρη είχαν επιλέξει ως εφαρμοστέο το δίκαιο άλλου κράτους μέλους (άρθ. 6 § 2).

Υπό την ισχύ της Οδηγίας σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα από ηλεκτρονικό κατάστημα, εφαρμοστέο τύγχανε το δίκαιο του κράτους μέλους, όπου ο υπεύθυνος επεξεργασίας είχε την εγκατάστασή του, νοούμενη ευρύτατα, είτε με τη μορφή θυγατρικής εταιρείας, είτε με τη μορφή υποκαταστήματος ή παραρτήματος. Μάλιστα σε περίπτωση πολλαπλών εγκαταστάσεων ο υπεύθυνος

επεξεργασίας είχε την υποχρέωση να τηρεί και να υπόκειται στην εποπτεία περισσότερων εθνικών αρχών (π.χ. μέσα από διαδικασίες γνωστοποίησης).

Ο Γενικός Κανονισμός, στο πλαίσιο της εξυπηρέτησης του σκοπού της ομοιόμορφης εφαρμογής του δικαίου της Ένωσης, εισάγει πλέον την έννοια της «κύριας εγκατάστασης» του υπευθύνου επεξεργασίας, αλλά και του εκτελούντος την επεξεργασία.

Σύμφωνα με το άρθρο 4 περ. 16 του Γενικού Κανονισμού, όταν πρόκειται για υπεύθυνο επεξεργασίας με εγκαταστάσεις σε περισσότερα του ενός κράτη μέλη, ως «κύρια εγκατάσταση», νοείται ο τόπος της κεντρικής του διοίκησης στην Ένωση, εκτός εάν οι αποφάσεις όσον αφορά στους σκοπούς και στα μέσα της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, λαμβάνονται σε άλλη εγκατάσταση του υπευθύνου επεξεργασίας στην Ένωση και η εγκατάσταση αυτή έχει την εξουσία εφαρμογής των αποφάσεων αυτών, οπότε ως «κύρια εγκατάσταση» θεωρείται η εγκατάσταση στην οποία έλαβε τις αποφάσεις αυτές.

Από την άλλη, όταν πρόκειται για εκτελούντα την επεξεργασία με εγκαταστάσεις σε περισσότερα του ενός κράτη μέλη, ως «κύρια εγκατάσταση» νοείται ο τόπος της κεντρικής του διοίκησης στην Ένωση ή, εάν ο εκτελών την επεξεργασία δεν έχει κεντρική διοίκηση στην Ένωση, η εγκατάσταση του εκτελούντος την επεξεργασία στην Ένωση, στην οποία εκτελούνται οι κύριες δραστηριότητες επεξεργασίας στο πλαίσιο των δραστηριοτήτων εγκατάστασης του εκτελούντος την επεξεργασία, στον βαθμό που ο εκτελών την επεξεργασία υπόκειται σε ειδικές υποχρεώσεις δυνάμει του Γενικού Κανονισμού.

Προφανώς η κύρια εγκατάσταση του εκτελούντος την επεξεργασία καθίσταται ιδιαιτέρως κρίσιμη, όταν ο υπεύθυνος επεξεργασίας είναι εγκατεστημένος εκτός της Ένωσης, περίπτωση στην οποία και πάλι εφαρμόζεται ο Γενικός Κανονισμός λόγω της γεωγραφικής σύνδεσης του εκτελούντος την επεξεργασία με την Ένωση. Αν ο υπεύθυνος επεξεργασίας είναι εγκατεστημένος εντός της Ένωσης η «κύρια εγκατάσταση» του εκτελούντος την επεξεργασία νομικά εξακολουθεί να ενδιαφέρει, καθώς προσδιορίζει την «ενδιαφερόμενη εποπτική αρχή», η οποία θα πρέπει να συμμετέχει στη «διαδικασία συνεργασίας» του Γενικού Κανονισμού. Η εθνική αρχή του τόπου της κύριας εγκατάστασης του υπευθύνου επεξεργασίας είναι η «επικεφαλής εποπτική αρχή», η οποία κατ' άρθρον 56 εποπτεύει τις διασυνοριακές ενέργειες του υπευθύνου επεξεργασίας σύμφωνα με τη διαδικασία της συνεργασίας του άρθρου 60.

Σε πολύ πρόσφατη απόφασή[56] του, το ΔΕΕ εξέτασε ένα ενδιαφέρον ζήτημα που σχετίζεται με την επιλογή του εφαρμοστέου δικαίου αναφορικά με τις διαδικτυακές συναλλαγές εντός του κοινοτικού χώρου. Το Δικαστήριο κλήθηκε να αποφανθεί για την σχέση των δύο κανονισμών (Ρώμη Ι και Ρώμη ΙΙ) και των τριών οδηγιών (Οδηγία 2009/22, περί των αγωγών παραλείψεως στον τομέα προστασίας των συμφερόντων των καταναλωτών, Οδηγία 93/13 για τις καταχρηστικές ρήτρες και Οδηγία 95/46 για την προστασία προσωπικών δεδομένων) στο πεδίο της σύγκρουσης νόμων.

Για το άρθρο 4, παράγραφο 1, στοιχείο α' της οδηγίας 95/46/ΕΚ το δικαστήριο απεφάνθη ότι, η επεξεργασία δεδομένων προσωπικού χαρακτήρα από επιχείρηση ηλεκτρονικού εμπορίου, διέπεται από το δίκαιο του κράτους μέλους, προς το οποίο η επιχείρηση αυτή κατευθύνει τις δραστηριότητές της, εφόσον αποδεικνύεται, ότι η εν λόγω επιχείρηση, προβαίνει σε επεξεργασία των επίμαχων δεδομένων στο πλαίσιο των δραστηριοτήτων εγκαταστάσεως ευρισκόμενης στο συγκεκριμένο κράτος μέλος. Στο εθνικό δικαστήριο εναπόκειται να εκτιμήσει αν συντρέχει τέτοια περίπτωση.

4.3 Η διεύρυνση του γεωγραφικού πεδίου εφαρμογής των κανόνων προστασίας εκτός της Ένωσης

Με την εφαρμογή του ΓΚΠΔ, το Ενωσιακό δίκαιο προστασίας δεδομένων αποκτά ρητά και ξεκάθαρα διευρυμένο πεδίο εφαρμογής και σε κράτη που δεν είναι μέλη της Ε.Ε.. Συγκεκριμένα, το άρθρο 3 του ΓΚΠΔ (εδαφικό πεδίο εφαρμογής) ορίζει, πως ο Κανονισμός εφαρμόζεται, τόσο σε περίπτωση που ο υπεύθυνος ή ο εκτελών την επεξεργασία βρίσκεται εντός της Ένωσης ακόμα και εάν η επεξεργασία τελείται εκτός της Ένωσης, όσο και στην περίπτωση που ακόμα και αν ο υπεύθυνος ή ο εκτελών την επεξεργασία βρίσκονται εκτός της Ένωσης το υποκείμενο των δεδομένων, ωστόσο, βρίσκεται στην Ένωση και για συγκεκριμένες περιπτώσεις (προσφορά αγαθών ή υπηρεσιών και παρακολούθηση συμπεριφοράς).

Το άρθρο αυτό αποτελεί τη νομοθετική μετουσίωση της νομολογίας της Weltimmo[57]. Με αυτή την καινοτόμα ρύθμιση επιχειρήσεις μη εγκαταστημένες στην

[56] C-191/2015 Verein für Konsumenteninformation/Amazon EU Sarl

[57] Πρόκειται για την υπόθεση C-230/14 , το διατακτικό της οποίας ανέφερε: Το άρθρο 4 παρ. 1 , στοιχείο α', 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, έχει την έννοια ότι παρέχει τη δυνατότητα εφαρμογής της νομοθεσίας περί προστασίας των δεδομένων προσωπικού χαρακτήρα κράτους μέλους διαφορετικού από αυτό εντός του οποίου είναι εγκαταστημένος ο υπεύθυνος για την επεξεργασία των δεδομένων αυτών, υπό την προϋπόθεση ωστόσο ότι αυτός ασκεί, μέσω μόνιμης εγκαταστάσεως στο

Ένωση, οι οποίες παρέχουν υπηρεσίες ή πωλούν προϊόντα μέσω διαδικτύου (e-shop), αλλά και επιχειρήσεις που διενεργούν αναζήτηση και δημιουργία προφίλ χρηστών του διαδικτύου, είτε διαφημιστικές, είτε απλώς εταιρίες που παρέχουν την τεχνική υποδομή για τη σχετική αναζήτηση (π.χ. data mining) θα υποχρεούνται στην τήρηση των ουσιαστικών και διαδικαστικών προϋποθέσεων της χώρας εγκατάστασης του κοινού, στο οποίο απευθύνονται. Πρόκειται για μια ρύθμιση που ήταν αναγκαία στο φως των τεχνολογικών εξελίξεων και η οποία αποκαθιστά τη δίκαιη ισορροπία υπέρ του υποκειμένου των δεδομένων. Με αυτόν τον τρόπο, ο Γενικός Κανονισμός πετυχαίνει να εξασφαλίσει το δικαίωμα στην προστασία από την επεξεργασία δεδομένων, για όλα τα φυσικά πρόσωπα που διαμένουν, εντός της Ευρωπαϊκής Ένωσης. Μάλιστα το προοίμιο του Γενικού Κανονισμού περιέχει σημαντικές κατευθύνσεις για την ερμηνεία της παραπάνω διάταξης. Έτσι αναφορικά με την περ. α' ανωτέρω της παρ. 2 του άρθρου 3 αναφέρεται ότι «ενώ η απλή προσβασιμότητα στην ιστοσελίδα του υπεύθυνου επεξεργασίας, του εκτελούντος την επεξεργασία ή ενός μεσάζοντος στην Ένωση ή στην διεύθυνση του ηλεκτρονικού ταχυδρομείου και σε άλλα στοιχεία επικοινωνίας ή η χρήση γλώσσας που χρησιμοποιείται συνήθως στην τρίτη χώρα, όπου ο υπεύθυνος επεξεργασίας είναι εγκαταστημένος, δεν αρκεί για να τεκμηριωθεί τέτοια πρόθεση [προσφοράς αγαθών ή υπηρεσιών στην Ένωση], παράγοντες όπως η χρήση γλώσσας ή νομίσματος που χρησιμοποιούνται συνήθως σε ένα ή περισσότερα κράτη μέλη, με δυνατότητα παραγγελίας προϊόντων και υπηρεσιών σε αυτή την άλλη γλώσσα, ή η αναφορά σε πελάτες ή χρήστες που βρίσκονται στην Ένωση, μπορούν να καταστήσουν πρόδηλο ότι, ο υπεύθυνος επεξεργασίας προτίθεται να προσφέρει αγαθά ή υπηρεσίες σε υποκείμενα των δεδομένων στην Ένωση».

έδαφος του κράτους μέλους αυτού, πραγματική και ουσιαστικού χαρακτήρα δραστηριότητα, έστω και περιορισμένη, στο πλαίσιο της οποίας πραγματοποιείται η επεξεργασία αυτή. Προκειμένου δε να προσδιορίσει υπό περιστάσεις όπως αυτές της κύριας δίκης, αν συμβαίνει κάτι τέτοιο, το αιτούν δικαστήριο μπορεί να λάβει υπόψη, ιδίως, το γεγονός, αφενός , ότι η δραστηριότητα του υπεύθυνου της εν λόγω επεξεργασίας, στο πλαίσιο της οποίας αυτή πραγματοποιείται, συνίσταται στη διαχείριση ιστοσελίδων αγγελιών ακινήτων σχετικά με ακίνητα που βρίσκονται στο έδαφος του κράτους μέλους αυτού, ιστοσελίδων συντεταγμένων στην γλώσσα του εν λόγω κράτους, και ότι η ανωτέρω δραστηριότητα συνδέεται κατά συνέπεια, κυρίως, ή και ακόμα και αποκλειστικώς, με το εν λόγω κράτος μέλος , και αφετέρου, ότι ο υπεύθυνος αυτός έχει ορίσει εκπρόσωπο εντός του εν λόγω κράτους μέλους, επιφορτισμένο με την είσπραξη των απαιτήσεων κατά την δραστηριότητα αυτή, καθώς και με την εκπροσώπησή του σε διοικητικές και δικαστικές διαδικασίες σχετικές με την επεξεργασία των οικείων δεδομένων.

Σχετικά δε με την περ. β ανωτέρω της ίδιας ως άνω διάταξης, αναφέρεται ότι «για τον καθορισμό του κατά πόσον μια δραστηριότητα επεξεργασίας, μπορεί να θεωρηθεί, ότι παρακολουθεί τη συμπεριφορά υποκειμένου των δεδομένων, θα πρέπει να εξακριβωθεί κατά πόσον φυσικά πρόσωπα, παρακολουθούνται στο Διαδίκτυο, συμπεριλαμβανομένης της δυνητικής, μετέπειτα χρήσης τεχνικών επεξεργασίας δεδομένων προσωπικού χαρακτήρα, οι οποίες συνίστανται στη διαμόρφωση του «προφίλ» ενός φυσικού προσώπου, ιδίως με σκοπό να ληφθούν αποφάσεις, που το αφορούν ή να αναλυθούν ή να προβλεφθούν οι προσωπικές προτιμήσεις, οι συμπεριφορές και οι νοοτροπίες του». Σε περίπτωση δε που ο υπεύθυνος της επεξεργασίας ή ο εκτελών την επεξεργασία δεν είναι εγκαταστημένοι στην Ένωση, αλλά ασκούν τις παραπάνω δραστηριότητες εντός της Ένωσης απευθυνόμενοι στο κοινό, θα πρέπει να ορίζεται ένας εκπρόσωπος εντός της Ένωσης κατά τους ορισμούς του άρθρου 27 του Γενικού Κανονισμού.

Ι. Παράρτημα

Υπόδειγμα Πολιτικής Προστασίας Προσωπικών δεδομένων ηλεκτρονικού καταστήματος.

Η παρούσα Πολιτική Προστασίας Προσωπικών Δεδομένων (εφεξής «Πολιτική») αφορά την επεξεργασία των προσωπικών σας στοιχείων από την «.....», και διακριτικό τίτλο: «.....» (στο εξής «Εταιρεία» ή «εμείς» ή «μας»), ως Υπεύθυνη Επεξεργασίας, με έδρα τ....., τηλ. ....., e-mail: ....., website: .....

Για την επίλυση οποιασδήποτε απορίας σας σχετικά με την παρούσα Πολιτική μπορείτε να επικοινωνήσετε μαζί μας στα ανωτέρω στοιχεία επικοινωνίας.

1. Τι είναι τα προσωπικά Δεδομένα; Ο όρος «προσωπικά Δεδομένα», αναφέρεται σε πληροφορίες φυσικών προσώπων, όπως ονοματεπώνυμο, ταχυδρομική διεύθυνση, ηλεκτρονική διεύθυνση, τηλέφωνο επικοινωνίας κ.ά., οι οποίες προσδιορίζουν ή μπορούν να προσδιορίσουν την ταυτότητα σας, εφεξής «Προσωπικά Δεδομένα» ή «Δεδομένα».

2. Τι είναι η Επεξεργασία Προσωπικών Δεδομένων; Κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε Δεδομένα προσωπικού χαρακτήρα ή σε σύνολα Δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή.

3. Ποια Δεδομένα σας συλλέγουμε;

Φροντίζουμε να συλλέγουμε μόνο τα απολύτως απαραίτητα Δεδομένα σας, τα οποία είναι κατάλληλα και σαφή για τον σκοπό που προορίζονται. Με εξαίρεση τυχόν Δεδομένων που συλλέγονται από τα Cookies (βλ. περισσότερα Πολιτική Cookies) και βιογραφικών στοιχείων που καταχωρείτε σε ιστοτόπους ή εφαρμογές εύρεσης εργασίας για κάλυψη θέσης εργασίας στην Εταιρεία, τα Δεδομένα περιορίζονται σε όσα συμπληρώνετε σε φόρμες που βρίσκονται στον ιστότοπο μας ..... Αυτά ενδέχεται να αφορούν:

- Πληροφορίες αναγνώρισης (όνομα, επώνυμο, φύλο, γενέθλια).
- Οικονομικά Δεδομένα (αριθμός χρεωστικής/πιστωτικής κάρτας, τραπεζικό λογαριασμό).
- Πληροφορίες επικοινωνίας (τηλέφωνο, email).
- Δεδομένα αποστολής προϊόντων (ταχυδρομική διεύθυνση)

4. Πώς χρησιμοποιούμε τα Δεδομένα σας;

Η επεξεργασία των Δεδομένων σας διεξάγεται είτε από το προσωπικό της Εταιρείας, είτε μέσω συστημάτων πληροφορικής και ηλεκτρονικών συσκευών από την Εταιρεία και κατ' εξαίρεση από τρίτους, οι οποίοι διεξάγουν εργασίες που είναι απαραίτητες για την επίτευξη των σκοπών που συνδέονται αυστηρά με τη χρήση του ιστότοπου και την πώληση προϊόντων μέσω του ιστότοπου (βλέπετε παρακάτω «Ποιοι είναι οι αποδέκτες των Δεδομένων σας;»). Γενικότερα, τα Δεδομένα σας υποβάλλονται σε επεξεργασία προκειμένου να σας παρασχεθούν οι ακόλουθες υπηρεσίες:

- Παραγγελίες προϊόντων: Η Εταιρεία επεξεργάζεται Δεδομένα σας προκειμένου να εκπληρώσει τη συμβατική της σχέση, να διεκπεραιώσει την παραγγελία προϊόντων, να παρέχει υπηρεσίες εξυπηρέτησης πελατών, να συμμορφωθεί με νομικές υποχρεώσεις, να αντικρούσει, εγείρει ή ασκήσει νομικές απαιτήσεις.
- Δημιουργία Λογαριασμού Χρήστη: Η Εταιρεία επεξεργάζεται τα Δεδομένα σας προκειμένου να απολαμβάνετε ως καταναλωτές υπηρεσίες αγοράς, αποστολής προϊόντων, καταγραφής ιστορικού παραγγελιών και άλλων ειδικών προνομίων.
- Κάρτα Προνομίων: Η Εταιρεία επεξεργάζεται τα Δεδομένα σας για τις ανάγκες της συμμετοχής σας στο πρόγραμμα Προνομίων δηλαδή τόσο της εξέτασης της αίτησης συμμετοχής σας, όσο και της συγκέντρωσης και εξαργύρωσης πόντων και γενικότερα της απόλαυσης προνομίων πελάτη, όπως αυτά αναλύονται στους όρους συμμετοχής του προγράμματος επιβράβευσης.
- Αποστολή ενημερωτικού δελτίου (newsletter): Η Εταιρεία σας παρέχει τη δυνατότητα να ενημερώνεστε στην ηλεκτρονική σας διεύθυνση σχετικά με προωθητικές/ διαφημιστικές ενέργειες που διεξάγει η Εταιρεία (π.χ. για νέα προϊόντα στην αγορά, τυχόν προσφορές, διαγωνισμούς κ.λπ.).
- Επικοινωνία: Η Εταιρεία χρησιμοποιεί τα Δεδομένα σας για να απαντήσει στα αιτήματα/ερωτήματα που υποβάλλετε μέσω της φόρμας επικοινωνίας.
- Εύρεση εργασίας: Η Εταιρεία χρησιμοποιεί τα δεδομένα σας που έχετε παράσχει σε τρίτους με σκοπό την εύρεση εργασίας για να εξετάσει την πιθανότητα πρόσληψης σας.

5. Για ποιο σκοπό επεξεργαζόμαστε τα στοιχεία σας;

Συλλέγουμε τα Δεδομένα σας για τον σκοπό παροχής προϊόντων ή/και υπηρεσιών της Εταιρείας, μέσω της ιστοσελίδας ..... . και ιδίως για:

- τη διαχείριση της πώλησης των προϊόντων ή/και των υπηρεσιών μας, π.χ. την επικοινωνία και ενημέρωση σας σχετικά με τη διαθεσιμότητά τους και την εξέλιξη παραγγελίας σας, την εκτέλεση της παραγγελίας σας, την αποστολή των προϊόντων, τη διαχείριση των οφειλών σας προς την Εταιρεία και την πραγματοποίηση επιστροφών.

- την προώθηση προϊόντων μας, την αποστολή ενημερωτικών δελτίων για προϊόντα ή/και υπηρεσίες μας

- τον έλεγχο, βελτίωση και προσαρμογή σε προτιμήσεις και επιλογές σας σχετικά με προϊόντα ή/ και υπηρεσίες μας.

- τη συμμόρφωση με τις υποχρεώσεις που επιβάλλονται από την εκάστοτε ισχύουσα νομοθεσία π.χ. φορολογική νομοθεσία, οδηγία για το ηλεκτρονικό εμπόριο.

6. Ποια είναι η νόμιμη βάση επεξεργασίας των Δεδομένων σας από την Εταιρεία;

Η επεξεργασία των Δεδομένων σας διενεργείται σύμφωνα με:

- τους όρους της συμβατικής μας σχέσης, ήτοι της πώλησης προϊόντων,

- τη συναίνεσή σας, όπου απαιτείται,

- τις υποχρεώσεις μας που πηγάζουν από το νόμο (π.χ. φορολογική νομοθεσία, νομοθεσία για το ηλεκτρονικό εμπόριο κ.ά.),

- το έννομο συμφέρον της Εταιρείας μας.

7. Ποιοι είναι οι αποδέκτες των Δεδομένων σας;

Πρόσβαση στα Δεδομένα σας ενδέχεται να έχουν τρίτοι, οι οποίοι επεξεργάζονται τα Δεδομένα σας για λογαριασμό μας, ως Εκτελούντες την Επεξεργασία, οι οποίοι παρέχουν υπηρεσίες προώθησης και διαφήμισης, τεχνικής υποστήριξης και παροχής λογισμικού, ταχυμεταφορών, έρευνας και ανάλυσης, εύρεσης προσωπικού και λογιστικών/ οικονομικών υπηρεσιών.

8.Πώς εξασφαλίζουμε ότι οι Εκτελούντες την Επεξεργασία σέβονται τα Προσωπικά σας Δεδομένα;

Οι Εκτελούντες την Επεξεργασία, που χρησιμοποιούμε συμφωνούν και δεσμεύονται:

- να τηρούν εχεμύθεια,

- να μη στέλνουν σε τρίτους Δεδομένα χωρίς την άδεια της Εταιρείας,

- να λαμβάνουν κατάλληλα μέτρα ασφαλείας,

- να συμμορφώνονται με το νομικό πλαίσιο για την προστασία των προσωπικών Δεδομένων και ιδίως τον Κανονισμό 679/2016/ΕΕ (άλλως GDPR).

9.Στέλνουμε τα Δεδομένα σας εκτός Ε.Ε.;

Τα Προσωπικά σας Δεδομένα αποτελούν αντικείμενο αποθήκευσης και επεξεργασίας μόνο εντός Ε.Ε. Κατ' εξαίρεση, ενδέχεται να στείλουμε τα Δεδομένα σας εκτός Ε.Ε. πάντοτε τηρουμένων κατάλληλων εγγυήσεων για τη διαβίβαση των Δεδομένων, όπως αυτές υπαγορεύονται από τον Κανονισμό 679/2016/Ε.Ε. (GDPR).

10. Για πόσο τηρούμε τα Δεδομένα σας και πότε τα διαγράφουμε;

Διατηρούμε τα Δεδομένα σας για όσο είναι απαραίτητο προκειμένου να σας παρέχουμε τα προϊόντα/ή και τις υπηρεσίες που μας ζητάτε, εκτός αν απαιτείται παράταση του χρόνου αυτού λόγω νομικών αξιώσεων ή εννόμων υποχρεώσεων της Εταιρείας. Η δήλωση συγκατάθεσης σας για αποστολή ενημερωτικού δελτίου

(newsletter) τηρείται για όσο χρόνο σας αποστέλλεται newsletter από την Εταιρεία και πάντως όχι περισσότερο από έξι μήνες από τη διακοπή αποστολής του. Τα Δεδομένα που συλλέγουν τα Cookies, τα διαγράφουμε σύμφωνα με την Πολιτική Cookies .

11. Είναι ασφαλή τα Δεδομένα σας;

Δεσμευόμαστε να διαφυλάσσουμε τα Προσωπικά σας Δεδομένα. Η με οποιοδήποτε τρόπο επεξεργασία των Δεδομένων σας επιτρέπεται μόνο σε εξουσιοδοτημένα από εμάς πρόσωπα, εργαζόμενους και συνεργάτες μας αποκλειστικά για τους ως άνω αναφερόμενους σκοπούς. Έχουμε λάβει τα απαραίτητα και κατάλληλα οργανωτικά και τεχνικά μέτρα για την ασφάλεια και την προστασία των Δεδομένων σας από κάθε μορφής τυχαία ή αθέμιτη επεξεργασία τόσο σε φυσικό επίπεδο όσο και σε επίπεδο λογικής ασφάλειας. Τα εν λόγω μέτρα επανεξετάζονται και τροποποιούνται όταν κρίνεται απαραίτητο.

12. Ποια είναι τα δικαιώματα σας;

- Έχετε δικαίωμα πρόσβασης στα προσωπικά σας Δεδομένα. Αυτό σημαίνει ότι έχετε το δικαίωμα να ενημερωθείτε από εμάς πώς και ποια Δεδομένα σας επεξεργαζόμαστε. Μπορείτε να ζητήσετε να ενημερωθείτε για τον σκοπό της επεξεργασίας, το είδος των Δεδομένων σας που τηρούμε, σε ποιους τα δίνουμε, πόσο διάστημα τα αποθηκεύουμε, αν γίνεται αυτοματοποιημένη λήψη αποφάσεων.
- Έχετε δικαίωμα διόρθωσης ανακριβών Δεδομένων προσωπικού χαρακτήρα. Αν διαπιστώσετε ότι υφίσταται λάθος στα Δεδομένα σας μπορείτε να μας υποβάλλετε αίτηση για να τα διορθώσουμε (π.χ. διόρθωση ονόματος ή ενημέρωση αλλαγής διεύθυνσης).
- Έχετε δικαίωμα διαγραφής. Μπορείτε να μας ζητήσετε να διαγράψουμε τα Δεδομένα σας αν δεν είναι απαραίτητα πλέον για τους ως άνω αναφερόμενους σκοπούς επεξεργασίας.
- Έχετε δικαίωμα φορητότητας των Δεδομένων σας. Μπορείτε να μας ζητήσετε να λάβετε σε αναγνώσιμη μορφή τα Δεδομένα που έχετε παράσχει ή να μας ζητήσετε να τα διαβιβάσουμε σε άλλο υπεύθυνο επεξεργασίας.
- Έχετε δικαίωμα περιορισμού της επεξεργασίας. Μπορείτε να μας ζητήσετε να περιορίσουμε την επεξεργασία των Δεδομένων σας για όσο χρόνο εκκρεμεί η εξέταση των αντιρρήσεων σας ως προς την επεξεργασία.
- Έχετε δικαίωμα ανάκλησης/εναντίωσης στην επεξεργασία των Δεδομένων σας. Μπορείτε να αντιταχθείτε στην επεξεργασία των Δεδομένων σας ή να άρετε τη συγκατάθεση σας, όπου έχει απαιτηθεί και εμείς θα σταματήσουμε την επεξεργασία των Δεδομένων σας, αν δεν υφίστανται άλλοι επιτακτικοί και νόμιμοι λόγοι που

υπερισχύουν έναντι του δικαιώματος σας ή αν δεν είναι απαραίτητα πλέον για τους ως άνω αναφερόμενους σκοπούς επεξεργασίας.

13. Πώς μπορείτε να ασκήσετε τα δικαιώματα σας;

Για να ασκήσετε τα δικαιώματα σας μπορείτε να μας αποστείλετε σχετικό αίτημα είτε στην έδρα της Εταιρείας ....., είτε στο e-mail ..... Επίσης, μπορείτε ανά πάσα στιγμή να συνδεθείτε στον λογαριασμό σας και να αλλάξετε τις προτιμήσεις σας.

14. Πότε απαντάμε στα Αιτήματα σας;

Απαντάμε στα Αιτήματά σας δωρεάν χωρίς καθυστέρηση, και σε κάθε περίπτωση εντός (1) ενός μηνός από τότε που θα λάβουμε το αίτημα σας. Αν, όμως, το Αίτημα σας είναι πολύπλοκο ή υπάρχει μεγάλος αριθμός Αιτημάτων σας θα σας ενημερώσουμε εντός του μήνα αν χρειαστεί να λάβουμε παράταση άλλων (2) δύο μηνών εντός των οποίων θα σας απαντήσουμε. Αν τα Αιτήματα σας είναι προδήλως αβάσιμα ή υπερβολικά ιδίως λόγω του επαναλαμβανόμενου χαρακτήρα τους, η Εταιρεία μπορεί να επιβάλει την καταβολή εύλογου τέλους, λαμβάνοντας υπόψη τα διοικητικά έξοδα για την παροχή της ενημέρωσης ή την εκτέλεση της ζητούμενης ενέργειας ή να αρνηθεί να δώσει συνέχεια στο Αίτημα αιτιολογώντας στην απάντησή προς εσάς. Σε περίπτωση που δεν λάβετε απάντηση εντός της ανωτέρω προβλεπόμενης προθεσμίας ή η απάντηση που λάβατε δεν ήταν ικανοποιητική ή το ζήτημα σας δεν έχει επιλυθεί, μπορείτε να απευθυνθείτε στην Αρχή Προστασίας Προσωπικών Δεδομένων (www.dpa.gr).

15. Κάνουμε χρήση αυτοματοποιημένης λήψης αποφάσεων/ περιλαμβανομένης της κατάρτισης προφίλ κατά την επεξεργασία των Δεδομένων σας; Η Εταιρεία μας, δεν λαμβάνει αποφάσεις βάσει αυτοματοποιημένης επεξεργασίας των Δεδομένων σας, εκτός από την περίπτωση χρήσης «cookies» στην ιστοσελίδα μας, και κατάρτισης προφίλ με σκοπό την αποστολή προσωποποιημένων διαφημίσεων/ προσφορών, οι οποίες δεν έχουν για εσάς καμία νομική συνέπεια και δέσμευση.

16. Ποιο είναι το εφαρμοστέο δίκαιο κατά την επεξεργασία των Δεδομένων σας από εμάς; Εφαρμοστέο Δίκαιο είναι το Ελληνικό Δίκαιο, όπως διαμορφώνεται σύμφωνα με το Γενικό Κανονισμό για την Προστασία των Προσωπικών Δεδομένων 2016/679/ΕΕ, και εν γένει το ισχύον εθνικό και ευρωπαϊκό νομοθετικό και κανονιστικό πλαίσιο για την προστασία προσωπικών Δεδομένων. Αρμόδια δικαστήρια για τυχόν διαφορές που αφορούν τα Δεδομένα είναι τα Δικαστήρια ……..

17. Πώς θα ενημερωθείτε για τυχόν τροποποιήσεις της παρούσας Πολιτικής; Ενημερώνουμε την παρούσα Πολιτική όποτε αυτό είναι αναγκαίο. Εάν υπάρχουν σημαντικές αλλαγές στην Πολιτική ή στον τρόπο με τον οποίο χρησιμοποιούμε τα Προσωπικά Δεδομένα σας, θα δημοσιεύουμε στην ιστοσελίδα μας την επικαιροποίηση της παρούσας, προτού οι αλλαγές τεθούν σε ισχύ και θα σας

ειδοποιούμε με κάθε πρόσφορο τρόπο. Σας ενθαρρύνουμε να διαβάζετε ανά τακτά διαστήματα την παρούσα Πολιτική για να γνωρίζετε πώς προστατεύονται τα Δεδομένα σας.

Βιβλιογραφία

- Αλεξανδρίδου Ε., Το δίκαιο του ηλεκτρονικού εμπορίου, 2004
- Γεωργιάδης Απ., Γενικές αρχές αστικού δικαίου, 2012
- Γιαννακάκης Ι., Ο ρόλος και οι ευθύνες του Data Protection Officer
- Δελούκα – Ιγγλέση Κ., Δίκαιο του καταναλωτή (ενωσιακό και ελληνικό), 2014
- Δέλλιος Γ., σε Αλεξανδρίδου Ελίζα, Δίκαιο προστασίας καταναλωτή, ελληνικό – ενωσιακό, κατ' άρθρο ερμηνεία του Ν. 2251/1994 και άλλων σχετικών νομοθετημάτων, 2015
- Ιγγλεζάκης Ι., Δίκαιο πληροφορικής, 2018
- Καράκωστας Ι., Προστασία του καταναλωτή (ν. 2251/1994), 2016
- Καράκωστας Ι., Δίκαιο & Internet, Νομικά ζητήματα του Διαδικτύου, 2003
- Λαμπρινουδάκης Κ., Γκρίτζαλης Σ., Μήτρου Λ., Κάτσικας Σ., Προστασία της Ιδιωτικότητας & Τεχνολογίες Πληροφορικής και Επικοινωνιών, 2010
- Μήτρου Λ., Ο γενικός κανονισμός προστασίας προσωπικών δεδομένων, 2017
- Παναγοπούλου – Κουτνατζή Φ., Βιομετρικές μέθοδοι και προστασία ιδιωτικότητας: Σκέψεις με αφορμή την απόφαση του ΔΕΕ Michael Schwarz κατά Κρατιδίου του Bochum (C-291/2012), ΔίΜΜΕ, 2013
- Τζίβα Ε., Το ηλεκτρονικό εμπόριο και η προστασία των καταναλωτών απέναντι σε γενικούς όρους συναλλαγών, ΔΕΕ 10/2003
- Philippe Jougleux, Ευρωπαϊκό δίκαιο του διαδικτύου, 2016