ΠΑΝΤΕΙΟΝ ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΟΙΝΩΝΙΚΩΝ ΚΑΙ ΠΟΛΙΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

PANTEION UNIVERSITY OF SOCIAL AND POLITICAL SCIENCES

ΣΧΟΛΗ ΕΠΙΣΤΗΜΩΝ ΟΙΚΟΝΟΜΙΑΣ ΚΑΙ ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ

ΤΜΗΜΑ ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

«ΝΟΜΙΚΗ ΚΑΙ ΔΙΟΙΚΗΤΙΚΗ ΕΠΙΣΤΗΜΗ»

ΚΑΤΕΥΘΥΝΣΗ: ΔΙΚΑΙΟ, ΤΕΧΝΟΛΟΓΙΑ ΚΑΙ ΟΙΚΟΝΟΜΙΑ

Η Διαβίβαση Δεδομένων στις ΗΠΑ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Κωνσταντίνος Δημήτριος Δανάλης

Αθήνα, 2023

Τριμελής Επιτροπή

Φερενίκη Παναγοπούλου - Κουτνατζή, Επίκουρη Καθηγήτρια Παντείου Πανεπιστημίου (Επιβλέπουσα)

Ισμήνη Κριάρη, Ομότιμη Καθηγήτρια Παντείου Πανεπιστημίου

Αντώνιος Χάνος, Αναπληρωτής Καθηγητής Παντείου Πανεπιστημίου

Συντομογραφίες

ΑΠΙΖ:	Ασπίδα Προστασίας Ιδιωτικής Ζωής
Βλ.:	βλέπε
ΓΚΠΔ:	Γενικός Κανονισμός για την Προστασία Δεδομένων
ΔΕΕ:	Δικαστήριο Ευρωπαϊκής Ένωσης
ΕΕ:	Ευρωπαϊκή Ένωση
ΕΟΧ:	Ευρωπαϊκός Οικονομικός Χώρος
ΕΣΠΔ:	Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων
ΗΠΑ:	Ηνωμένες Πολιτείες Αμερικής
κλπ.:	και λοιπά
ΣΕΕ:	Συνθήκη Ευρωπαϊκής Ένωσης
ΣΛΕΕ:	Συνθήκη για τη Λειτουργία της Ευρωπαϊκής Ένωσης
ΤΣΡ:	Τυποποιημένες Συμβατικές Ρήτρες
BCR:	Binding Corporate Rules
CJEU:	Court of Justice of the European Union
DoT:	Department of Transport
DPA:	Data Protection Agreement
DPC:	Data Protection Commission
EDPB:	European Data Protection Board
EO:	Executive Order
EU:	European Union
FISA:	Foreign Intelligence Surveillance Act
FTC:	Federal Trade Commission

Συντομογραφίες

GDPR:	General Data Protection Regulation
IOB:	Intelligence Oversight Board
ITA:	International Trade Administration
NSL:	National Security Letters
PCLOB:	Privacy & Civil Liberties Oversight Board
PIAB:	President's Intelligence Advisory Board
PPD:	Presidential Policy Directive
SCC:	Standard Contractual Clauses
US:	United States

Πίνακας Περιεχομένων

Περίληψη

Στην παρούσα εργασία, όπως γίνεται σαφές και από τον τίτλο της, θα αναφερθούμε στις μεθόδους διαβίβασης δεδομένων μεταξύ ΕΕ - ΗΠΑ όπως αναπτύχθηκαν τις τελευταίες δεκαετίες υπό το πρίσμα τόσο της οδηγίας 95/46/ΕΚ, όσο και του κανονισμού 2016/679/ΕΕ, αλλά και της αντίστοιχης νομολογίας του ΔΕΕ στις αποφάσεις Schrems I και Schrems II. Πιο αναλυτικά, στο πρώτο κεφάλαιο γίνεται αναφορά στις αποφάσεις επάρκειας 2000/520/ΕΚ (Αρχές Ασφαλούς Λιμένα) και 2016/1250/ΕΕ (Ασπίδα Προστασίας Ιδιωτικής Ζωής) της Ευρωπαϊκής Επιτροπής αλλά και στις αντίστοιχες αποφάσεις του ΔΕΕ (C-362/14: Schrems I, C-311/18: Schrems II) που ήρθαν να καταστήσουν ανίσχυρες τις παραπάνω αποφάσεις επάρκειας. Στο δεύτερο κεφάλαιο γίνεται αναφορά στις επιπτώσεις της απόφασης Schrems II στην διατλαντική διαβίβαση δεδομένων και στην συνέχεια γίνεται αναφορά στην απόφαση 2021/914/ΕΕ της Ευρωπαϊκής Επιτροπής, μέσω της οποίας υιοθετούνται οι νέες τυποποιημένες συμβατικές ρήτρες σύμφωνα με τον ΓΚΠΔ. Στο πλαίσιο των συμπερασμάτων αναλύεται το κατά πόσο μπορεί να αναπτυχθεί ένα νέο πλαίσιο διαβίβασης δεδομένων μεταξύ ΕΕ - ΗΠΑ με παράλληλη μνεία στα βήματα που έχουν γίνει στην προσπάθεια ανάπτυξης αυτού του πλαισίου (EU-US DPF).

Λέξεις-Κλειδιά:

Αρχές Ασφαλούς Λιμένα, Ασπίδα Προστασίας Ιδιωτικής Ζωής, ΓΚΠΔ, διατλαντική διαβίβαση δεδομένων, τυποποιημένες συμβατικές ρήτρες

“Data Transfer to the US”

Konstantinos Dimitrios Danalis

Abstract

In this thesis, as is clear from its title, we will refer to the methods of data transfer between the EU and the US as developed in recent decades in the light of both Directive 95/46/EC and Regulation 2016/679/EU, but also of the corresponding jurisprudence of the CJEU in the Schrems I and Schrems II decisions. In more detail, the first chapter refers to the adequacy decisions 2000/520/EC (Safe Harbor Principles) and 2016/1250/EU (Privacy Shield) of the European Commission as well as to the corresponding decisions of the CJEU (C-362/14: Schrems I, C-311/18: Schrems II) which came to invalidate the above adequacy decisions. In the second chapter, reference is made to the effects of the Schrems II decision on transatlantic data transfer and then reference is made to the decision 2021/914/EU of the European Commission, through which the new standard contractual clauses are adopted in accordance with the GDPR. In the context of the conclusions, it is analyzed whether a new EU-US data transfer framework can be developed, with a parallel reference to the steps that have been taken in the effort to develop this framework (EU-US DPF).

Keywords:

FISA, GDPR, Privacy Shield, Safe Harbor Principles, SCC, Schrems

Εισαγωγή

Το ζήτημα της διαβιβάσεως προσωπικών δεδομένων χαρακτηρίζεται από έντονο προβληματισμό. Καθοριστικοί παράγοντες όπως η παγκοσμιοποίηση της πληροφορίας, η απόδοση μεγάλης οικονομικής σημασίας στη διαβίβαση των δεδομένων σε χώρες εκτός ΕΕ σε συνδυασμό με το εξαιρετικά χαμηλότερο κόστος της επεξεργασίας δεδομένων στις χώρες αυτές, αλλά και η ανάγκη ουσιαστικής προστασίας των δεδομένων όλων όσοι ευρίσκονται εντός ΕΕ οδήγησε σε μια νέα θεώρηση της προστασίας. Και αυτό επειδή η διαβίβαση δεδομένων από μια ασφαλή χώρα της ΕΕ σε μια άλλη τρίτη μη ασφαλή χώρα θέτει υπό διακινδύνευση την προστασία δεδομένων σε ενωσιακό επίπεδο. Στο επίπεδο δημιουργίας ασφαλούς πλαισίου διαβίβασης δεδομένων προσωπικού χαρακτήρα, τα τελευταία χρόνια, λαμβάνουν χώρα συνεχείς εξελίξεις που έχουν ως αφετηρία κυρίως τις περιπτώσεις παραβιάσεως προσωπικών δεδομένων, οι οποίες εν τέλει καταλήγουν στο ΔΕΕ, ενώ οι αποφάσεις που προκύπτουν (Schrems I - Schrems II), διαπλάθουν και μεταλλάσσουν το αντίστοιχο πλαίσιο[1].

Για ποιο λόγο όμως πρέπει να δώσουμε ιδιαίτερη σημασία στη διασυνοριακή διαβίβαση δεδομένων και στην προστασία που θα παρέχεται στα δεδομένα[2];

Πρώτον, η διαρροή μέσω του διαδικτύου και των νέων τεχνολογικών εφαρμογών δεδομένων σε μια τρίτη μη ασφαλή χώρα αναιρεί την προβλεπόμενη στον ΓΚΠΔ προστασία δεδομένων προσωπικού χαρακτήρα. Επομένως, κρίνεται αδήριτη η ανάγκη της δημιουργίας προϋποθέσεων επεκτάσεως του προστατευτικού πεδίου εφαρμογής του ΓΚΠΔ και σε τρίτες χώρες, τις οποίες στοχεύει ο υπεύθυνος επεξεργασίας λόγω χαμηλότερου κόστους και στις οποίες η προστασία των προσωπικών δεδομένων είναι υποτυπώδης. Μέσω των μηχανισμών προστασίας κατά τη διασυνοριακή διαβίβαση δεδομένων εύλογα θα μπορούσε να υποστηριχθεί ότι επιτυγχάνεται μια διεύρυνση του πεδίου εφαρμογής του ΓΚΠΔ με κριτήριο όχι μόνο

---

[1] Βλ. Παναγοπούλου Φερενίκη - Παπακωνσταντίνου Σουζάνα, Διατλαντικές διαβιβάσεις δεδομένων προσωπικού χαρακτήρα: Η συμφωνία Ε.Ε. και Η.Π.Α. για το νέο Trans-Atlantic Data Privacy Framework, 19/04/2022, διαθέσιμο σε: https://www.syntagmawatch.gr/trending-issues/diatlantikes-diavivaseis-dedomenwn-proswpikou-xarakthra-h-symfwnia-ee-kai-hpa-gia-to-neo-trans-atlantic-data-privacy-framework/

[2] Βλ. Παναγοπούλου Φερενίκη, Συνταγματικές προεκτάσεις των μηχανισμών διευρύνσεως της προστασίας δεδομένων προσωπικού χαρακτήρα πέραν της ΕΕ: Εξωεφαφική εφαρμογή του ΓΚΠΔ και διασυνοριακή διαβίβαση δεδομένων, ΔίΜΕΕ τ. 4/2019, σελ. 510-511

την έδρα του υπευθύνου ή του υποκειμένου των δεδομένων, αλλά τα ίδια τα προστατευόμενα εντός ΕΕ δεδομένα. Συνεπώς, δεδομένα που βρίσκονται εντός της ΕΕ, όταν μεταφερθούν εκτός αυτής χαίρουν της προστασίας του ΓΚΠΔ. Υπό αυτή την έννοια, παρατηρείται μια έντονη επίδραση του ΓΚΠΔ σε αλλοδαπές έννομες τάξεις, με τελικό σκοπό να μην υπονομεύεται το υψηλό επίπεδο προστασίας των φυσικών προσώπων που εγγυάται ο ΓΚΠΔ (άρθρο 44). Και η προσπάθεια αυτή γίνεται εντονότερη μέσω της επαπειλήσεως δυσθεώρητων προστίμων σε περίπτωση παραβιάσεως των σχετικών διατάξεων περί διασυνοριακής διαβιβάσεως δεδομένων.

Δεύτερον, πολλές από τις διασυνοριακά διαβιβαζόμενες πληροφορίες συνθέτουν ένα άριστο «σκεπτογράφημα» πολλών ανθρώπων. Χαρακτηριστικό παράδειγμα αποτελούν τα στοιχεία επιβατών πτήσεων σε χώρες εκτός ΕΕ που δημιουργούν το προφίλ για τις ταξιδιωτικές συνήθειες, την οικονομική κατάσταση, τις διατροφικές συνήθειες και την υγεία των επιβατών. Άλλο εναργές παράδειγμα είναι οι εφαρμογές υγείας που στέλνουν τα δεδομένα τους σε υπολογιστικό νέφος εκτός ΕΕ. Συνεπώς, τα προσωπικά δεδομένα που διαβιβάζονται χρήζουν ιδιαίτερης προστασίας και για το λόγο αυτό δεν πρέπει να μένουν απροστάτευτα κατά τη διαβίβασή τους σε τρίτες χώρες.

Τρίτον, δεν θα μπορούσαμε να αγνοήσουμε το γεγονός ότι η διασυνοριακή διαβίβαση πληροφοριών αποτελεί πρωταρχική προϋπόθεση για το διεθνές εμπόριο και τη διεθνή συνεργασία (βλ. και αιτιολογική έκθεση 101 ΓΚΠΔ). Ως εκ τούτου, η διακίνηση των προσωπικών δεδομένων έχει αξία από μόνη της. Υπενθυμίζεται η βασική αρχή της οδηγίας 95/46/ΕΚ, η οποία θέτει επί ίσοις όροις ήδη στον τίτλο της την προστασία προσωπικών δεδομένων και την ελεύθερη διακίνηση των δεδομένων. Εν τοις πράγμασι, η οδηγία αποσκοπούσε στην απελευθέρωση της ροής δεδομένων εντός της Κοινότητας αποσκοπώντας στην άρση των περιορισμών κατά την άσκηση των τεσσάρων κοινοτικών ελευθεριών, θέτοντας ως όριο το θεμελιώδες δικαίωμα στην ιδιωτική ζωή. Απομακρυνόμαστε έτσι από την κατοχύρωση ενός απόλυτου - "απολυταρχικού" δικαιώματος με απώτερο στόχο την προστασία της ιδιωτικής ζωής. Επισημαίνεται επίσης ότι στη σχετική συζήτηση για την κατάρτιση της οδηγίας είχαν το προβάδισμα τα επιχειρήματα σχετικά με το οικονομικό σκέλος και την εσωτερική αγορά.

Τέταρτον, μέσω της διασυνοριακής διαβιβάσεως δεδομένων καθίσταται καταφανές ότι οι διάφορες έννομες τάξεις παρέχουν κυμαινόμενο επίπεδο προστασίας στα προσωπικά δεδομένα. Αυτή η διακύμανση οδηγεί σε προστασία πολλαπλών ταχυτήτων και για το λόγο αυτό έντονη καθίσταται η ανάγκη ενός ενιαίου κανονιστικού πλαισίου για τα δεδομένα που προστατεύονται υπό τη σκέπη του ΓΚΠΔ.

Συνειδητοποιώντας με τα παραπάνω τη σημασία ύπαρξης ενός ασφαλούς πλαισίου διαβίβασης δεδομένων προς τρίτες χώρες, θα εισέλθουμε στην ουσία της παρούσας εργασίας που είναι η εξέταση του πλαισίου διαβιβάσεως δεδομένων μεταξύ ΕΕ - ΗΠΑ από την περίοδο ισχύς των Αρχών Ασφαλούς Λιμένα στις αρχές της δεκαετίας του 2000, έως και σήμερα με τη διαβίβαση δεδομένων μέσω τυποποιημένων συμβατικών ρητρών και την προσπάθεια εγκαθίδρυσης ενός νέου πλαισίου διατλαντικών διαβιβάσεων.

Κεφάλαιο 1: Από το Safe Harbor Framework μέχρι την απόφαση Schrems II

1.1 Safe Harbor Framework

Σύμφωνα με την παράγραφο 1 του άρθρου 25 της οδηγίας 95/46/ΕΚ[3] η διαβίβαση από κράτος μέλος της ΕΕ σε τρίτη χώρα δεδομένων που έχουν υποστεί επεξεργασία ή πρόκειται να υποστούν επεξεργασία μετά τη διαβίβαση τους, επιτρέπεται μόνο στην περίπτωση που εκπληρούνται οι απαιτήσεις της εθνικής νομοθεσίας του εκάστοτε κράτους μέλους, όπως αυτές διαμορφώθηκαν από την παρούσα οδηγία, και υπό την προϋπόθεση η τρίτη χώρα να εξασφαλίζει ικανοποιητικό επίπεδο προστασίας. Έτσι η Ευρωπαϊκή Επιτροπή με την απόφαση 2000/520/ΕΚ[4], προχώρησε στην αναγνώριση της επάρκειας του συστήματος Safe Harbor (του πρώτου πλαισίου διατλαντικής διαβίβασης δεδομένων) στην διασφάλιση της προστασίας των προσωπικών δεδομένων σύμφωνα με την οικεία οδηγία. Τι είναι το σύστημα Ασφαλούς Λιμένα και ποιες αρχές περιλαμβάνονται σε αυτό; Οι ΗΠΑ αρχικά δεν παρείχαν ικανοποιητικό επίπεδο προστασίας προσωπικών δεδομένων, και κατ' επέκταση δεν μπορούσε να εκδοθεί η ανωτέρω αναφερόμενη απόφαση περί επαρκούς προστασίας από την Επιτροπή. Τόσο η ομάδα εργασίας του άρθρου 29 όσο και το Ευρωπαϊκό Κοινοβούλιο κατέληξαν το 2000 στο συμπέρασμα ότι η προστασία των προσωπικών δεδομένων στις ΗΠΑ δεν ανταποκρινόταν στα αντικειμενικά κριτήρια που είχε θέση η Ευρωπαϊκή Ένωση για τη χορήγηση απόφασης επάρκειας. Προκειμένου, να ξεπεραστεί αυτό το πρόβλημα και να συνεχιστούν απρόσκοπτα οι διαβιβάσεις προσωπικών δεδομένων, τον Μάιο του 2000 εγκρίθηκε ομοφώνως το καθεστώς Ασφαλούς Λιμένα ανάμεσα στην ΕΕ και τις ΗΠΑ. Το καθεστώς Ασφαλούς Λιμένα δεν είχε τον χαρακτήρα ούτε συνθήκης ούτε διεθνής συμφωνίας αλλά ενός πλαισίου εντός του οποίου η Ευρωπαϊκή Ένωση θέσπισε ορισμένες αρχές η τήρηση των οποίων ήταν επιβεβλημένη από τις ΗΠΑ και από την άλλη μεριά όσο οι ΗΠΑ

[3] Βλ. Οδηγία 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, διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:31995L0046&from=EL

[4] Βλ. Απόφαση 2000/520/ΕΚ της Επιτροπής της 26ης Ιουλίου 2000, βάσει της οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την επάρκεια της προστασίας που παρέχεται από τις αρχές ασφαλούς λιμένα για την προστασία της ιδιωτικής ζωής και τις συναφείς συχνές ερωτήσεις που εκδίδονται από το Υπουργείο Εμπορίου των ΗΠΑ, διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32000D0520&from=en

τηρούσαν τις εν λόγω αρχές η Ευρωπαϊκή Ένωση αποδεχόταν ότι υπήρχε επαρκής προστασία για τη διαβίβαση των προσωπικών δεδομένων από την Ευρώπη στις ΗΠΑ. Το πλαίσιο αυτό σαφώς μπορούσε να ανακληθεί από την Επιτροπή αν δεν λειτουργούσε όπως αναμενόταν. Η πρακτική εφαρμογή του καθεστώτος ασφαλούς λιμένα είναι ότι επέτρεπε στις αμερικανικές εταιρείες να εκπληρώνουν τις προϋποθέσεις περί της προστασίας προσωπικών δεδομένων που τίθενται από την νομοθεσία της ΕΕ για τις διαβιβάσεις προσωπικών δεδομένων σε τρίτες χώρες χωρίς ταυτόχρονα να υποχρεώνεται η ομοσπονδιακή κυβέρνηση των ΗΠΑ να αλλάξει ολόκληρη την προσέγγιση της στο ζήτημα της προστασίας των προσωπικών δεδομένων. Το καθεστώς ασφαλούς λιμένα περιελάμβανε βασικές αρχές οι οποίες εφαρμόζονταν υποχρεωτικά στα προσωπικά δεδομένα που λάμβαναν αμερικανικές εταιρείες από την Ευρώπη. Οι εταιρείες, όφειλαν να εναρμονίσουν τον εσωτερικό κανονισμό τους με τις αρχές του καθεστώτος Ασφαλούς Λιμένα. Η ένταξη αμερικανικών εταιρειών στο καθεστώς Ασφαλούς Λιμένα πραγματοποιήθηκε σταδιακά, για παράδειγμα 198 αμερικανικές εταιρείες είχαν ενταχθεί ως τον Ιούνιο του 2002, 388 ως τον Μάιο του 2003, λιγότερες από 700 ως το 2006, 2.500 το 2008 και 5.299 τον Ιούλιο του 2015[5]. Σύμφωνα με το Υπουργείο Εμπορίου των Ηνωμένων Πολιτειών στο Safe Harbor Framework περιλαμβάνονται 7 αρχές (κοινοποίηση, επιλογή, περαιτέρω διαβίβαση, ασφάλεια, ακεραιότητα των δεδομένων, πρόσβαση, εφαρμογή)[6]. Πιο αναλυτικά, βασιζόμενοι στο παράρτημα Ι της παραπάνω απόφασης (είτε στο αυτοτελές κείμενο της ΙΤΑ[7]) μπορούμε να ορίσουμε το περιεχόμενο κάθε μιας από τις παραπάνω αρχές ως εξής:

Κοινοποίηση: Κάθε εταιρεία έχει ως υποχρέωση την ενημέρωση των υποκειμένων των δεδομένων σχετικά με τους σκοπούς συλλογής και χρήσης των διαβιβαζόμενων δεδομένων που τα αφορούν, τον τρόπο επικοινωνίας με την εταιρεία για τυχόν αιτήσεις πληροφοριών ή παραπόνων, τους τρίτους στους οποίους γνωστοποιεί τα

[5] Βλ. Παύλου Αναστασία Η., Η διαβίβαση των προσωπικών δεδομένων από την Ευρώπη στις Ηνωμένες Πολιτείες Αμερικής (διπλωματική εργασία), Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών, σελ. 45

[6] Βλ. Federal Trade Commission Enforcement of the U.S.-EU and U.S.-Swiss Safe Harbor Frameworks, διαθέσιμο σε: https://www.ftc.gov/business-guidance/resources/federal-trade-commission-enforcement-us-eu-us-swiss-safe-harbor-frameworks

[7] Βλ. Department of Commerce - International Trade Administration, Issuance of Safe Harbor Principles and Transmission to European Commission, διαθέσιμο σε: https://www.govinfo.gov/content/pkg/FR-2000-07-24/pdf/00-18489.pdf

διαβιβαζόμενα δεδομένα, καθώς και τις επιλογές και τα μέσα που προσφέρει η εταιρεία στα υποκείμενα δεδομένων για τον περιορισμό της χρήσης και της γνωστοποίησης των πληροφοριών. Η κοινοποίηση αυτή θα πρέπει να παρέχεται σε σαφή και ευδιάκριτη γλώσσα κατά την πρώτη αίτηση παροχής πληροφοριών προσωπικού χαρακτήρα που απευθύνει στα υποκείμενα δεδομένων η εκάστοτε εταιρεία ή το συντομότερο δυνατό μετά ταύτα, αλλά οπωσδήποτε προτού προβεί η εταιρεία είτε στη χρήση των δεδομένων αυτών για σκοπό άλλο από εκείνο για τον οποίο συνελέγησαν αρχικά ή για τον οποίο υπέστησαν επεξεργασία από την διαβιβάζουσα εταιρεία, είτε στη γνωστοποίηση των προσωπικών δεδομένων σε τρίτο μέρος για πρώτη φορά.

Επιλογή: Κάθε εταιρεία υποχρεούται να παρέχει στα υποκείμενα δεδομένων την ευκαιρία να επιλέγουν (δικαίωμα εξαίρεσης από τα δεδομένα) εάν οι πληροφορίες προσωπικού χαρακτήρα που τα αφορούν πρόκειται α) να γνωστοποιηθούν σε ένα τρίτο μέρος ή β) να χρησιμοποιηθούν για ένα σκοπό ο οποίος δεν συνάδει με το σκοπό για τον οποίο συνελέγησαν αρχικά ή για τον οποίο εγκρίθηκαν στη συνέχεια από τα εν λόγω πρόσωπα. Πρέπει να παρέχονται στα υποκείμενα δεδομένων σαφείς, ευδιάκριτοι, άμεσα διαθέσιμοι και προσιτοί μηχανισμοί για την άσκηση της επιλογής.

Όσον αφορά το πεδίο των ευαίσθητων προσωπικών δεδομένων (δηλαδή δεδομένων που αναφέρονται λεπτομερώς σε ασθένειες ή την κατάσταση υγείας, τη φυλετική ή εθνική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, τη συμμετοχή σε συνδικαλιστικές οργανώσεις ή πληροφορίες σχετικά με τη σεξουαλική ζωή του προσώπου) πρέπει να παρέχεται καταφατική ή ρητή επιλογή (οικειοθελής συμμετοχή) κάθε φορά που τα δεδομένα αυτά πρόκειται να γνωστοποιηθούν σε τρίτο μέρος ή να χρησιμοποιηθούν για σκοπό άλλο από εκείνο για τον οποίο συνελέγησαν αρχικά ή τον οποίο ενέκρινε το ενδιαφερόμενο πρόσωπο μεταγενέστερα ασκώντας την επιλογή της οικειοθελούς συμμετοχής. Εν πάση περιπτώσει, κάθε εταιρεία οφείλει να μεταχειρίζεται ως ευαίσθητες οποιεσδήποτε πληροφορίες λαμβάνει από τρίτο μέρος, τις οποίες το εν λόγω τρίτο μέρος χαρακτηρίζει και μεταχειρίζεται ως ευαίσθητες.

Περαιτέρω διαβίβαση: Για να γνωστοποιούν πληροφορίες σε τρίτο μέρος, οι εταιρείες πρέπει να εφαρμόζουν τις δύο προαναφερθείσες αρχές (αρχή της κοινοποίησης και της επιλογής). Όποτε μια εταιρεία που επιθυμεί να διαβιβάσει

δεδομένα σε ένα τρίτο μέρος το οποίο ενεργεί ως πράκτορας, μπορεί να το πράξει αφού εξακριβώσει πρώτα ότι τα τρίτα μέρη τηρούν τις αρχές του ασφαλούς λιμένα ή υπόκεινται στην οδηγία ή σε κάποιο μηχανισμό που να εξασφαλίζει την επάρκεια της προστασίας ή συνάπτει γραπτή συμφωνία με τα τρίτα μέρη που να απαιτεί από τα τελευταία να παρέχουν τουλάχιστον το ίδιο επίπεδο προστασίας της ιδιωτικής ζωής με εκείνο που επιβάλλουν οι συναφείς αρχές του ασφαλούς λιμένα. Εφόσον ο οργανισμός τηρεί τις προϋποθέσεις αυτές, δεν φέρει ευθύνη (εκτός αν ο οργανισμός αποφασίσει διαφορετικά) σε περίπτωση που το τρίτο μέρος στο οποίο διαβιβάζει δεδομένα, τα επεξεργάζεται κατά τρόπο που αντιβαίνει τους προβλεπόμενους περιορισμούς ή τις συμφωνημένες διατάξεις, εκτός και αν ο οργανισμός γνώριζε ή όφειλε να γνωρίζει ότι το τρίτο μέρος θα επεξεργαζόταν τα δεδομένα αυτά κατά τρόπο αντίθετο και δεν έλαβε εύλογα μέτρα προκειμένου να εμποδίσει ή να σταματήσει την επεξεργασία αυτή.

Ασφάλεια: Οι εταιρείες που δημιουργούν, διατηρούν, χρησιμοποιούν ή διαδίδουν πληροφορίες προσωπικού χαρακτήρα οφείλουν να λαμβάνουν τα απαραίτητα μέτρα για την προστασία των πληροφοριών αυτών από τυχόν απώλεια, κατάχρηση και μη εγκεκριμένη πρόσβαση, γνωστοποίηση, αλλαγή και καταστροφή.

Ακεραιότητα των δεδομένων: Σύμφωνα με τις αρχές, οι πληροφορίες προσωπικού χαρακτήρα πρέπει να παρουσιάζουν συνάφεια με τους σκοπούς για τους οποίους πρόκειται να χρησιμοποιηθούν. Μία εταιρεία δεν μπορεί να επεξεργαστεί πληροφορίες προσωπικού χαρακτήρα με τρόπο που θα αντιβαίνει τους σκοπούς για τους οποίους συνελέγησαν ή για τους οποίους εγκρίθηκαν από το υποκείμενο δεδομένων μεταγενέστερα. Στο μέτρο που είναι αναγκαίο για την εξυπηρέτηση των εν λόγω σκοπών, μια εταιρεία πρέπει να λαμβάνει τα απαραίτητα μέτρα για να εξασφαλίσει ότι τα δεδομένα είναι χρησιμοποιήσιμα, ακριβή, πλήρη και ενημερωμένα.

Πρόσβαση: Τα υποκείμενα δεδομένων πρέπει να έχουν πρόσβαση στα διαβιβαζόμενα δεδομένα που τα αφορούν, και τα οποία κατέχει μια εταιρεία, και συγχρόνως να έχουν τη δυνατότητα να διορθώνουν, τροποποιούν και εξαλείφουν τα δεδομένα αυτά όποτε είναι ανακριβείς, με εξαίρεση τις περιπτώσεις κατά τις οποίες η επιβάρυνση ή το κόστος που συνεπάγεται η παροχή πρόσβασης θα ήταν δυσανάλογη προς τους κινδύνους για την προστασία της ιδιωτικής ζωής του προσώπου εν

προκειμένω ή σε περίπτωση που παραβιάζονται τα δικαιώματα άλλων τρίτων προσώπων.

Εφαρμογή: Για να υπάρξει αποτελεσματική προστασία της ιδιωτικής ζωής πρέπει να υφίστανται μηχανισμοί οι οποίοι θα εξασφαλίζουν καταρχήν τη συμμόρφωση με τις αρχές, θα προβλέπουν μέσα προσφυγής για τα πρόσωπα περί των οποίων πρόκειται και τα οποία θίγονται από τη μη συμμόρφωση με τις αρχές, όπως επίσης θα προβλέπονται και συνέπειες για τις εταιρείες σε περίπτωση μη τήρησης των αρχών. Οι μηχανισμοί αυτοί πρέπει να περιλαμβάνουν τουλάχιστον α) άμεσα διαθέσιμους και προσιτούς ανεξάρτητους μηχανισμούς προσφυγής για τη διερεύνηση και τη διευθέτηση των καταγγελιών και των αμφισβητήσεων σύμφωνα με τις αρχές και για την αποζημίωση του κάθε προσώπου στις περιπτώσεις που προβλέπονται από το εφαρμοστέο δίκαιο ή τις πρωτοβουλίες του ιδιωτικού τομέα, β) διαδικασίες εποπτείας για την επαλήθευση τόσο της ακρίβειας των διαβεβαιώσεων και των ισχυρισμών των επιχειρήσεων όσον αφορά τις πρακτικές τους περί ιδιωτικής ζωής, όσο και της εφαρμογής των πρακτικών περί ιδιωτικής ζωής σύμφωνα με τη διατύπωσή τους, και γ) υποχρεώσεις επίλυσης των προβλημάτων που απορρέουν από την παράλειψη συμμόρφωσης με τις αρχές από εταιρείες που ισχυρίζονται ότι τις τηρούν και τις αντίστοιχες συνέπειες στις περιπτώσεις αυτές. Οι κυρώσεις πρέπει να είναι αρκετά αυστηρές ώστε να εξασφαλίζεται με αυτό τον τρόπο η συμμόρφωση εκ μέρους των εταιρειών.

Η εφαρμογή των αρχών αυτών από τις επιχειρήσεις συνεπικουρείται μέσω του τμήματος των συχνών ερωτήσεων - απαντήσεων που περιλαμβάνονται στο κείμενο, και παρέχει πιο λεπτομερής ανάλυση του τρόπου εφαρμογής των παραπάνω αρχών σε διαφορετικές περιπτώσεις. Τέλος, σύμφωνα με το άρθρο 3 της απόφασης 2000/520/ΕΚ της Επιτροπής, οι εθνικές αρχές των κρατών μελών επιφυλάσσονται της άσκησης αναστολής της ροής δεδομένων (προς επιχειρήσεις) σε δύο περιπτώσεις: α) όταν ο κρατικός φορέας των Ηνωμένων Πολιτειών (FTC ή Υπουργείο Μεταφορών) ή ένας ανεξάρτητος φορέας προσφυγής, κρίνει ότι μία εταιρεία παραβιάζει τις αρχές ασφαλούς λιμένα, όπως αυτές εφαρμόζονται σύμφωνα με τις συχνές ερωτήσεις, β) είτε, όταν υπάρχει σοβαρή πιθανότητα παραβίασης των αρχών ασφαλούς λιμένα, είτε, όταν υπάρχουν στοιχεία από τα οποία προκύπτει βασίμως ότι ο σχετικός φορέας εφαρμογής δεν λαμβάνει ή δεν προτίθεται να λάβει κατάλληλα και έγκαιρα μέτρα για τη διευθέτηση του προβλήματος, είτε, όταν η συνέχιση της διαβίβασης δεδομένων

δημιουργεί άμεσο κίνδυνο πρόκλησης σοβαρής ζημίας στα υποκείμενα των δεδομένων, και όταν οι αρμόδιες ελεγκτικές αρχές του κράτους μέλους κατέβαλαν, υπό τις συγκεκριμένες περιστάσεις, κάθε δυνατή προσπάθεια για να ενημερώσουν σχετικά την εταιρεία και να της δώσουν τη δυνατότητα να απαντήσει.

1.2 Απόφαση Schrems I[8]

1.2.1 Πραγματικά περιστατικά και προδικαστικά ερωτήματα

Από τις σκέψεις 26-35 της απόφασης μπορούμε να διαπιστώσουμε τα πραγματικά περιστατικά που οδήγησαν στην υπόθεση C-362/14. Ο M. Schrems, ο οποίος είναι πολίτης και κάτοικος της Αυστρίας χρησιμοποιεί από το 2008 το μέσο κοινωνικής δικτύωσης Facebook[9]. Κάθε πρόσωπο που επιθυμεί να χρησιμοποιήσει το εν λόγο μέσο κοινωνικής δικτύωσης και κατοικεί σε κράτος μέλος της ΕΕ, κατά την εγγραφή του οφείλει να υπογράψει σύμβαση με τη Facebook Ireland, θυγατρική της Facebook Inc., η οποία εδρεύει στις Ηνωμένες Πολιτείες. Τα προσωπικά δεδομένα των χρηστών του Facebook που κατοικούν στο έδαφος της Ευρωπαϊκής Ένωσης διαβιβάζονται, εν όλω ή εν μέρει, σε διακομιστές που ανήκουν στη Facebook Inc, οι οποίοι είναι εγκατεστημένοι στις Ηνωμένες Πολιτείες, όπου τα δεδομένα αυτά υπόκεινται σε επεξεργασία[10]. Στις 25 Ιουνίου 2013 ο M. Schrems μέσω καταγγελίας που υπέβαλε στον επίτροπο ζητούσε την απαγόρευση της διαβίβασης των δεδομένων που τον αφορούσαν από την Facebook Ireland στις Ηνωμένες Πολιτείες. Σύμφωνα με την καταγγελία του η νομοθεσία και η ισχύουσα πρακτική στις Ηνωμένες Πολιτείες δεν εγγυούνταν ικανοποιητική προστασία των δεδομένων που φυλάσσονταν στο έδαφος των ΗΠΑ έναντι των δραστηριοτήτων παρακολουθήσεως εκ μέρους των υπηρεσιών πληροφοριών. Καταλυτικός παράγοντας στις αιτιάσεις του M. Schrems ήταν αδιαμφισβήτητα οι αποκαλύψεις στις οποίες προχώρησε ο Edward Snowden σχετικά με τις δραστηριότητες των υπηρεσιών πληροφοριών των Ηνωμένων Πολιτειών, και ιδίως της NSA[11]. Ο επίτροπος έκρινε οτι δεν υποχρεούταν να διερευνήσει τα όσα

---

[8] Βλ. Δ.Ε.Ε., C-362/14 (Grand Chamber), Maximillian Schrems v. Data Protection Commissioner, 6/10/2015, διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:62014CJ0362&from=en

[9] Βλ. Δ.Ε.Ε., C-362/14, σκέψη 26

[10] Βλ. Δ.Ε.Ε., C-362/14, σκέψη 27

[11] Βλ. Δ.Ε.Ε., C-362/14, σκέψη 28

κατήγγειλε ο M. Schrems, υποστηρίζοντας οτι δεν υπήρχαν αποδείξεις οτι η NSA είχε πρόσβαση στα προσωπικά δεδομένα του και οτι οι αιτιάσεις που είχε προβάλει ο M. Schrems δεν μπορούσαν να προβληθούν λυσιτελώς. Ως συνέπεια των παραπάνω η καταγγελία απορρίφθηκε[12]. Στη συνέχεια ο M. Schrems άσκησε προσφυγή ενώπιον του ανωτάτου δικαστηρίου της Ιρλανδίας κατά της επίμαχης αποφάσεως. Το δικαστήριο μετά από εξέταση των αποδεικτικών στοιχείων που υποβλήθηκαν από τους διάδικους έφτασε στην διαπίστωση ότι η ηλεκτρονική παρακολούθηση και η υποκλοπή των διαβιβαζόμενων προσωπικών δεδομένων από την Ένωση στις ΗΠΑ εξυπηρετεί αναγκαίους και απαραίτητους για το δημόσιο συμφέρον σκοπούς. Προσέθεσε όμως στα παραπάνω, ότι οι αποκαλύψεις στις οποίες προέβη ο E. Snowden κατέδειξαν την ύπαρξη «σημαντικών υπερβάσεων» εκ μέρους της NSA και άλλων ομοσπονδιακών οργανισμών[13]. Το ανώτατο δικαστήριο επισήμανε επιπλέον ότι οι πολίτες της ΕΕ δεν διαθέτουν, όμως, πραγματικό δικαίωμα ακροάσεως. Πέραν αυτών η εποπτεία της δράσεως των υπηρεσιών πληροφοριών πραγματοποιείται στο πλαίσιο μυστικής και μονομερούς διαδικασίας. Όταν λοιπόν τα δεδομένα προσωπικού χαρακτήρα διαβιβαστούν στις Ηνωμένες Πολιτείες, η NSA καθώς και άλλοι ομοσπονδιακοί οργανισμοί, όπως το FBI, μπορούν να έχουν πρόσβαση σε αυτά στο πλαίσιο των μαζικών και άνευ διακρίσεων παρακολουθήσεων και υποκλοπών που πραγματοποιούν[14]. Το δικαστήριο επεσήμανε επίσης ότι το ιρλανδικό δίκαιο απαγορεύει τη διαβίβαση δεδομένων προσωπικού χαρακτήρα εκτός της εθνικής επικράτειας, εξαιρουμένων των τρίτων χωρών που εξασφαλίζουν ικανοποιητικό επίπεδο προστασίας της ιδιωτικής ζωής και των θεμελιωδών δικαιωμάτων και ελευθεριών. Η σημασία των δικαιωμάτων του σεβασμού της ιδιωτικής ζωής και του απαραβίαστου της κατοικίας, τα οποία κατοχυρώνονται στο ιρλανδικό Σύνταγμα, φαίνεται από την υποχρέωση κάθε ενέργειας που θίγει τα δικαιώματα αυτά να είναι σύμφωνη προς την αρχή της αναλογικότητας και τις απαιτήσεις του νόμου[15]. Άρα η μαζική και χωρίς διάκριση πρόσβαση σε δεδομένα προσωπικού χαρακτήρα έρχεται προδήλως σε αντίθεση προς την αρχή της αναλογικότητας και τις θεμελιώδεις αξίες που προστατεύει το ιρλανδικό Σύνταγμα. Προκειμένου, υποκλοπές ηλεκτρονικών

[12] Βλ. Δ.Ε.Ε., C-362/14, σκέψη 29

[13] Βλ. Δ.Ε.Ε., C-362/14, σκέψη 30

[14] Βλ. Δ.Ε.Ε., C-362/14, σκέψη 31

[15] Βλ. Δ.Ε.Ε., C-362/14, σκέψη 32

επικοινωνιών για να μπορούν να θεωρηθούν συνταγματικές, πρέπει να αποδεικνύεται ότι είναι στοχευμένες, ότι η παρακολούθηση ορισμένων προσώπων ή ορισμένων ομάδων προσώπων δικαιολογούνται αντικειμενικώς για λόγους εθνικής ασφάλειας ή της καταστολής της εγκληματικότητας και ότι υπάρχουν επαρκείς και ελέγξιμες εγγυήσεις. Έτσι, σύμφωνα με το Ιρλανδικό ανώτατο δικαστήριο, αν η υπόθεση της κύριας δίκης επρόκειτο να εξεταστεί αποκλειστικά βάσει του ιρλανδικού δικαίου, θα έπρεπε να κριθεί ότι, δεδομένων των σοβαρών αμφιβολιών ως προς το κατά πόσον οι Ηνωμένες Πολιτείες της Αμερικής διασφαλίζουν ικανοποιητικό επίπεδο προστασίας των δεδομένων προσωπικού χαρακτήρα, ο επίτροπος όφειλε να προβεί σε έρευνα σχετικά με όσα καταγγέλθηκαν από τον M. Schrems και ότι κακώς απέρριψε την καταγγελία του[16]. Ωστόσο, το δικαστήριο προχώρησε στην εκτίμηση ότι η παρούσα υπόθεση αφορά την εφαρμογή του ενωσιακού δικαίου, υπό την έννοια του άρθρου 51 του Χάρτη, με αποτέλεσμα η νομιμότητα της επίμαχης αποφάσεως να πρέπει να κριθεί βάσει του ευρωπαϊκού δικαίου. Κατά το ίδιο, η απόφαση 2000/520 δεν πληροί τις απαιτήσεις των άρθρων 7 και 8 του Χάρτη και τις αρχές που έχουν διατυπωθεί από το Δικαστήριο στην υπόθεση Digital Rights Ireland κλπ.. Το δικαίωμα στον σεβασμό της ιδιωτικής ζωής, σύμφωνα με το άρθρο 7 του Χάρτη και στις θεμελιώδεις αξίες που είναι κοινές στις παραδόσεις των κρατών μελών, θα καθίστατο κενό περιεχομένου, αν οι δημόσιες αρχές μπορούσαν να έχουν ελεύθερη πρόσβαση στις ηλεκτρονικές επικοινωνίες, με τυχαίο και γενικευμένο τρόπο, χωρίς καμία αντικειμενική δικαιολογία που να στηρίζεται σε λόγους εθνικής ασφάλειας ή προλήψεως της εγκληματικότητας, και η οποία να συνδέεται ειδικώς με τα οικεία άτομα, και με παράλληλη έλλειψη επαρκούς και επαληθεύσιμης εγγύησης[17]. Το ανώτατο δικαστήριο παρατηρεί, εξάλλου, ότι ο M. Schrems, στο πλαίσιο της προσφυγής του, αμφισβητεί στην πραγματικότητα το κύρος του καθεστώτος «ασφαλούς λιμένα» που θέσπισε η απόφαση 2000/250 και στο οποίο στηρίζεται η επίμαχη στην υπόθεση της κύριας δίκης απόφαση. Έτσι, παρότι ο M. Schrems δεν αμφισβήτησε τυπικά ούτε το κύρος της οδηγίας 95/46 ούτε της αποφάσεως 2000/250, κατά το ανωτέρω δικαστήριο τίθεται το ερώτημα αν, λόγω του άρθρου 25, παράγραφος 6, της εν λόγω οδηγίας, ο επίτροπος δεσμεύεται από τη διαπίστωση της Επιτροπής στην απόφαση 2000/520, κατά την οποία οι Ηνωμένες Πολιτείες της

[16] Βλ. Δ.Ε.Ε., C-362/14, σκέψη 33

[17] Βλ. Δ.Ε.Ε., C-362/14, σκέψη 34

Αμερικής εξασφαλίζουν ικανοποιητικό επίπεδο προστασίας ή αν το άρθρο 8 του Χάρτη δίνει τη δυνατότητα στον επίτροπο να αποστεί, εφόσον χρειάζεται, από τη διαπίστωση αυτή[18].

Τελικά το ανώτατο δικαστήριο της Ιρλανδίας, επέλεξε να αναστείλει την ενώπιον σε αυτό διαδικασία και να αποστείλει στο ΔΕΕ τα εξής δύο προδικαστικά ερωτήματα[19]:

Α) Σε περίπτωση κατάθεσης καταγγελίας, ενώπιον Αρχής, σύμφωνα με την οποία δεδομένα διαβιβάζονται σε τρίτη χώρα, όπου η νομοθεσία και η πρακτική δεν παρέχουν ικανοποιητικό επίπεδο προστασίας, η εν λόγω Αρχή δεσμεύεται από πιθανή απόφαση επάρκειας από την Επιτροπή που πιστοποιεί το αντίθετο;

Β) Η Αρχή αυτή μπορεί και/ή πρέπει να διεξαγάγει τη δική της έρευνα για κάθε ζήτημα υπό το φως των πραγματικών εξελίξεων που επήλθαν από τότε που δημοσιεύθηκε για πρώτη φορά η απόφαση επάρκειας της Επιτροπής;

1.2.2 Σκεπτικό ΔΕΕ[20]

Το Δικαστήριο ξεκίνησε την ανάλυσή του περιγράφοντας τις αρχές της ευρωπαϊκής οδηγίας για την προστασία των δεδομένων: οι διαβιβάσεις δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες πρέπει να πραγματοποιούνται μόνο εάν η τρίτη χώρα διασφαλίζει επαρκές επίπεδο προστασίας των δεδομένων. Οι εθνικές επιτροπές προστασίας δεδομένων ενδέχεται να διαπιστώσουν ότι υπάρχει επαρκές επίπεδο προστασίας λόγω του εθνικού δικαίου ή των διεθνών δεσμεύσεων. Κάθε κράτος μέλος ορίζει μία ή περισσότερες δημόσιες αρχές επιφορτισμένες με τον έλεγχο της εφαρμογής στο έδαφός του των εθνικών διατάξεων που θεσπίζονται βάσει της οδηγίας. Ωστόσο, το Δικαστήριο έκρινε, οτι η ύπαρξη απόφασης της Επιτροπής με την οποία διαπιστώνεται ότι μια χώρα διασφαλίζει επαρκή προστασία των δεδομένων προσωπικού χαρακτήρα δεν εξαλείφει ούτε μειώνει τις εξουσίες που διαθέτουν οι εθνικές αρχές ελέγχου βάσει του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και της οδηγίας. Τονίστηκε ότι η οδηγία επιδιώκει να

[18] Βλ. Δ.Ε.Ε., C-362/14, σκέψη 35

[19] Βλ. Δ.Ε.Ε., C-362/14, σκέψη 36

[20] Βλ. Global Freedom of Expression Columbia University, Schrems v. Data Protection Commissioner, διαθέσιμο σε: https://globalfreedomofexpression.columbia.edu/cases/schrems-v-data-protection-commissioner/

«διασφαλίσει όχι μόνο την αποτελεσματική και πλήρη προστασία των θεμελιωδών δικαιωμάτων και ελευθεριών των φυσικών προσώπων, ιδίως το θεμελιώδες δικαίωμα στον σεβασμό της ιδιωτικής ζωής όσον αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα, αλλά και υψηλό επίπεδο προστασίας των εν λόγω θεμελιωδών δικαιωμάτων και ελευθεριών».

Στη συνέχεια, το Δικαστήριο διερεύνησε εάν η απόφαση ασφαλούς λιμένα ήταν άκυρη. Το Δικαστήριο επισήμανε ότι δεν υπάρχει ορισμός της έννοιας του «επαρκούς επιπέδου προστασίας», αλλά επισήμανε ότι δεν απαιτεί επίπεδο προστασίας πανομοιότυπο με εκείνο που εγγυάται η έννομη τάξη της Ένωσης. Εντούτοις, απαιτούσε, λόγω του εσωτερικού του δικαίου ή των διεθνών δεσμεύσεών του, επίπεδο προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών κατ' ουσίαν ισοδύναμο με εκείνο που διασφαλίζεται εντός της Ένωσης. Κρίθηκε ότι το προσαπτόμενο σύστημα αυτοπιστοποιήσεως δεν αντέβαινε, αυτό καθεαυτό, στις απαιτήσεις περί επαρκούς επιπέδου προστασίας, αλλά ότι "η αξιοπιστία ενός τέτοιου συστήματος, υπό το πρίσμα της απαιτήσεως αυτής, στηρίζεται κατ' ουσίαν στη θέσπιση αποτελεσματικών μηχανισμών εντοπισμού και ελέγχου που καθιστούν δυνατό τον προσδιορισμό και την τιμωρία στην πράξη κάθε παράβασης των κανόνων που διασφαλίζουν την προστασία των θεμελιωδών δικαιωμάτων, ιδίως το δικαίωμα στον σεβασμό της ιδιωτικής ζωής και το δικαίωμα προστασίας των δεδομένων προσωπικού χαρακτήρα".

Το Δικαστήριο παρατήρησε ότι οι αρχές του ασφαλούς λιμένα εφαρμόζονταν μόνο σε αυτοπιστοποιούμενους οργανισμούς των ΗΠΑ που λαμβάνουν προσωπικά δεδομένα από την Ευρωπαϊκή Ένωση και οι δημόσιες αρχές των ΗΠΑ δεν ήταν υποχρεωμένες να συμμορφώνονται με αυτές[21]. Επιπλέον, κρίθηκε ότι η απόφαση περί ασφαλούς λιμένα δεν περιείχε επαρκείς διαπιστώσεις όσον αφορά τα μέτρα με τα οποία οι Ηνωμένες Πολιτείες διασφάλιζαν ικανοποιητικό επίπεδο προστασίας λόγω του εσωτερικού τους δικαίου ή των διεθνών δεσμεύσεών τους. Εξετάζοντας το επίπεδο προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών στην Ένωση, το δικαστήριο επισήμανε ότι κάθε επέμβαση απαιτούσε σαφείς και ακριβείς κανόνες που να διέπουν το πεδίο εφαρμογής και την εφαρμογή ενός μέτρου και να επιβάλλουν

[21] Βλ. Clark Kelli, The EU Safe Harbor Agreement Is Dead, Here's What To Do About It, 27/10/2015, διαθέσιμο σε: https://www.forbes.com/sites/riskmap/2015/10/27/the-eu-safe-harbor-agreement-is-dead-heres-what-to-do-about-it/?sh=34faa0723cea

ελάχιστες εγγυήσεις, οι οποίες ήταν αναγκαίες ακόμη περισσότερο όταν τα δεδομένα προσωπικού χαρακτήρα υποβάλλονταν σε αυτοματοποιημένη επεξεργασία και υπήρχε σημαντικός κίνδυνος παράνομης πρόσβασης στα δεδομένα αυτά. Επιπλέον, η προστασία του θεμελιώδους δικαιώματος στον σεβασμό της ιδιωτικής ζωής σε επίπεδο ΕΕ απαιτεί οι παρεκκλίσεις και οι περιορισμοί στην προστασία των δεδομένων προσωπικού χαρακτήρα να εφαρμόζονται μόνο όταν είναι απολύτως αναγκαίο. Αντιθέτως, το δικαστήριο επισήμανε ότι η απόφαση 2000/520 επέτρεπε να υπερισχύουν τυχόν απαιτήσεις εθνικής ασφάλειας, δημοσίου συμφέροντος και επιβολής του νόμου των Ηνωμένων Πολιτειών έναντι του συστήματος ασφαλούς λιμένα και ότι οι αμερικανικές οργανώσεις ήταν υποχρεωμένες να αγνοούν, χωρίς περιορισμό, τους προστατευτικούς κανόνες του συστήματος όταν συγκρούονταν με τις απαιτήσεις αυτές. Έτσι, το Δικαστήριο έκρινε οτι το σύστημα ασφαλούς λιμένα των ΗΠΑ επιτρέπει την παρέμβαση, από τις δημόσιες αρχές των ΗΠΑ, στα θεμελιώδη δικαιώματα των προσώπων. Η νομοθεσία που επιτρέπει στις δημόσιες αρχές να έχουν πρόσβαση σε δεδομένα προσωπικού χαρακτήρα, υπονόμευσε την ουσία του θεμελιώδους δικαιώματος στον σεβασμό της ιδιωτικής ζωής: «Για να αποδειχθεί η ύπαρξη παρέμβασης στο θεμελιώδες δικαίωμα του σεβασμού της ιδιωτικής ζωής, δεν έχει σημασία αν οι εν λόγω πληροφορίες που αφορούν την ιδιωτική ζωή είναι ευαίσθητες ή αν τα ενδιαφερόμενα πρόσωπα έχουν υποστεί αρνητικές συνέπειες λόγω αυτής της παρέμβασης».

Τέλος, το Δικαστήριο έκρινε ότι η απόφαση περί ασφαλούς λιμένα στέρησε από τις εθνικές αρχές ελέγχου τις εξουσίες που τους παρέχει το άρθρο 25 της οδηγίας 95/46, όταν ένα πρόσωπο αμφισβητεί τη συμβατότητα μιας αποφάσεως με την προστασία της ιδιωτικής ζωής και των θεμελιωδών δικαιωμάτων και ελευθεριών των ατόμων.

Για όλους τους παραπάνω λόγους, το Δικαστήριο κήρυξε άκυρη την απόφαση ασφαλούς λιμένα, ενός πλαισίου δεκαπέντε ετών, κάτι που θα επηρέαζε περισσότερες από 4.400 αμερικανικές και ευρωπαϊκές εταιρείες που βασίζονταν στη συμφωνία για τη διατλαντική μεταφορά δεδομένων. Θα μπορούσε επίσης να έχει τεράστιες επιπτώσεις για τις αμερικανικές υπηρεσίες πληροφοριών, οι οποίες εξαρτώνται από

την ικανότητα να κοσκινίζουν μεγάλους όγκους δεδομένων αναζητώντας ενδείξεις για να αντιμετωπίσουν τρομοκρατικές ενέργειες[22].

1.3 EU-US Privacy Shield

Το 2016 μετά την απόφαση 2016/1250 της Επιτροπής, υιοθετήθηκε ο νέος μηχανισμός διατλαντικής διαβίβασης προσωπικών δεδομένων με την ονομασία Privacy Shield (EU-U.S. Privacy Shield). Εν τω μεταξύ, το 2017 ακολούθησε η ετήσια αναθεώρηση του νέου αυτού μηχανισμού που αν και θεωρήθηκε ότι ο μηχανισμός λειτουργούσε ικανοποιητικά, διατυπώθηκαν αρκετές ανησυχίες που πυροδοτήθηκαν από το πρόσφατο τότε σκάνδαλο Facebook/Cambridge Analytica[23].

Στο καινούριο πλαίσιο περιλαμβάνονται τόσο η απόφαση της Ευρωπαϊκής Επιτροπής περί επαρκούς προστασίας των προσωπικών δεδομένων, όσο και οι αρχές του Privacy Shield που υιοθετήθηκαν από το Αμερικανικό Υπουργείο Εμπορείου και η επίσημη δέσμευση της Αμερικανικής Κυβέρνησης ότι θα εφαρμόσει την συμφωνία. Όπως και στην περίπτωση του προϊσχύσαντος πλαισίου έτσι και υπό το καθεστώς του Privacy Shield, υπάρχει ένα σύστημα αυτοπιστοποίησης μέσω του οποίου οι αμερικανικοί οργανισμοί και εταιρείες εγγράφονται και προσαρμόζονται μέσω της υιοθέτησης από τον εσωτερικό τους κανονισμό των αρχών για την προστασία των προσωπικών δεδομένων. Το εν λόγω σύστημα πιστοποίησης βρίσκεται υπό τον έλεγχο του Υπουργείου Εμπορίου των ΗΠΑ. Η ουσιώδης διαφορά των δύο αυτών πλαισίων είναι ότι στην καινούρια αυτή συμφωνία ρυθμίζεται η πρόσβαση και η χρήση των προσωπικών δεδομένων που διαβιβάζονται, από τις δημόσιες αρχές των ΗΠΑ. Σύμφωνα με τα όσα αναφέρονται στο κείμενο της απόφασης «τα μέτρα παρακολούθησης θα εφαρμόζονται μόνο για την απόκτηση πληροφοριών από την αλλοδαπή και θα είναι όσο το δυνατόν περισσότερο εξατομικευμένα» γεγονός που σύμφωνα με την Επιτροπή οδηγεί σε συμμόρφωση με την απόφαση του Δικαστηρίου της ΕΕ στην απόφαση Schrems που τόνισε ότι οποιαδήποτε επέμβαση στα θεμελιώδη

[22] Βλ. Nakashima Ellen, Top E.U. court strikes down major data-sharing pact between U.S. and Europe,6/10/2015, διαθέσιμο σε: https://www.washingtonpost.com/world/national-security/eu-court-strikes-down-safe-harbor-data-transfer-deal-over-privacy-concerns/2015/10/06/2da2d9f6-6c2a-11e5-b31c-d80d62b53e28_story.html

[23] Βλ. Παναγοπούλου Φερενίκη - Παπακωνσταντίνου Σουζάνα, Διατλαντικές διαβιβάσεις δεδομένων προσωπικού χαρακτήρα: Η συμφωνία Ε.Ε. και Η.Π.Α. για το νέο Trans-Atlantic Data Privacy Framework, 19/04/2022, διαθέσιμο σε: https://www.syntagmawatch.gr/trending-issues/diatlantikes-diavivaseis-dedomenwn-proswpikou-xarakthra-h-symfwnia-ee-kai-hpa-gia-to-neo-trans-atlantic-data-privacy-framework/

δικαιώματα που προστατεύονται από τα άρθρα 7 και 8 του Χάρτη πρέπει να επιβάλει «ελάχιστο αριθμό απαιτήσεων». Η μεγαλύτερης σημασίας καινοτομία που εισήχθη με το νέο πλαίσιο διαβίβασης είναι ο μηχανισμός του διαμεσολαβητή, ο οποίος είναι ανώτερος υπάλληλος του Υπουργείου Εξωτερικών των ΗΠΑ και είναι ανεξάρτητος σε σχέση με τις υπηρεσίες πληροφοριών των ΗΠΑ. Ο ρόλος του νέου αυτού οργάνου είναι η διασφάλιση του ελέγχου των καταγγελιών καθώς και τον έλεγχο τήρησης της σχετικής νομοθεσίας από την πλευρά των ΗΠΑ ή σε περίπτωση διαπίστωσης παραβίασης την αποκατάσταση αυτής με διορθωτικά μέτρα. Παρότι η πρόβλεψη του διαμεσολαβητή αποτελεί ένα θετικό μέτρο ωστόσο, διαπιστώνεται έντονη αμφισβήτηση το εάν πράγματι η εν λόγω πρόβλεψη αρκεί για να καλύψει την απαιτούμενη προϋπόθεση του άρθρου 47 του Χάρτη Θεμελιωδών δικαιωμάτων, δηλαδή την παροχή επαρκούς δικαστικής προστασίας. Επιπλέον, η λειτουργία του νέου αυτού οργάνου χαρακτηρίζεται από την ύπαρξη αρκετών περιορισμών. Κατ' αρχάς, η διαδικασία πρόσβασης στο διαμεσολαβητή προϋποθέτει την υποβολή έγγραφου αιτήματος στην εποπτική αρχή του κράτους μέλους στο οποίο βρίσκεται το υποκείμενο της διαβίβασης και είναι υπεύθυνη για την εποπτεία των εθνικών υπηρεσιών ασφάλειας. Παρότι αναφέρεται ότι ο αιτών δεν υποχρεούται να αποδείξει ότι πράγματι τα δεδομένα του έτυχαν επεξεργασίας από τις υπηρεσίες πληροφοριών των ΗΠΑ, ωστόσο προτού υποβληθεί το αίτημα στον διαμεσολαβητή ελέγχεται ότι αφορά προσωπικά δεδομένα που διαβιβάστηκαν στις ΗΠΑ, και ότι το αίτημα δεν είναι επιπόλαιο, κακόβουλο ή καταχρηστικό. Εφόσον δε, το αίτημα διαβιβαστεί στον διαμεσολαβητή εκείνος ακολουθώντας τις προβλεπόμενες διαδικασίες θα απαντήσει επιβεβαιώνοντας ότι το αίτημα έχει αποτελέσει αντικείμενο δέουσας έρευνας και ότι έχει τηρηθεί η νομοθεσία των ΗΠΑ ή αν διαπιστώθηκε παραβίαση ότι έχει αποκατασταθεί ενώ διευκρινίζεται ότι δεν θα αποσαφηνίζεται αν ο αιτών αποτέλεσε πράγματι αντικείμενο παρακολούθησης από τις εθνικές υπηρεσίες πληροφοριών των ΗΠΑ. Πέραν των παραπάνω, ένα ουσιώδες ζήτημα που αναφέρθηκε και από την Ομάδα εργασίας του άρθρου 29[24] αφορά την διασφάλιση της ανεξαρτησίας του διαμεσολαβητή από τις κυβερνητικές επιδιώξεις καθώς όπως προαναφέρθηκε είναι ανώτερος υπάλληλος του Υπουργείου Εξωτερικών των ΗΠΑ.

[24] Βλ. Γνώμη 1/2016 της ομάδας εργασίας του άρθρου 29, υιοθετήθηκε στις 13 Απριλίου 2016

Περιληπτικά θα μπορούσαμε να αναφέρουμε οτι η "Ασπίδα Προστασίας" θεσπίζει αυστηρότερες υποχρεώσεις για τις αμερικανικές εταιρείες που εντάσσονται στον εν λόγω μηχανισμό καθώς και πιο εντατική εποπτεία από το Υπουργείο Εμπορίου των ΗΠΑ. Παράλληλα, προβλέπονται νέοι μηχανισμοί επιλύσεως διαφορών σε περίπτωση που τα υποκείμενα θεωρούν οτι έγινε κατάχρηση των δεδομένων τους. Πρώτον, προβλέπεται δυνατότητα των ιδιωτών να υποβάλλουν καταγγελία απευθείας στην εταιρεία που επεξεργάζεται δεδομένα τους. Δεύτερον, οι εταιρείες υποχρεούνται να διασφαλίζουν οτι τα υποκείμενα των δεδομένων μπορούν να προσφεύγουν, χωρίς χρέωση, σε "ανεξάρτητο μηχανισμό" για επίλυση των διαφορών με την εταιρεία. Τρίτον, προβλέπεται η δυνατότητα των πολιτών κρατών-μελών της ΕΕ να υποβάλλουν καταγγελίες στις Εθνικές Αρχές Προστασίας Δεδομένων, οι οποίες στη συνέχεια θα προωθήσουν τις καταγγελίες στο Υπουργείο Εμπορίου των ΗΠΑ. Μόνο μετά από την ενεργοποίηση και των τριών μηχανισμών οι ιδιώτες μπορούν να προσφύγουν στην ειδική διαδικασία διαιτησίας της Ασπίδας Προστασίας, τα αποτελέσματα της οποίας είναι δεσμευτικά. Τέλος, οι εταιρείες δύνανται να προχωρήσουν σε άμεση συνεργασία με τις Ευρωπαϊκές Αρχές Προστασίας Δεδομένων προς επίλυση των διαφορών. Για τη διασφάλιση οτι οι εταιρείες που συμμετέχουν στην Ασπίδα Προστασίας τηρούν όντως το θεσμικό πλαίσιο προβλέπονται τακτικοί έλεγχοι από το Υπουργείο Εμπορίου των ΗΠΑ, το οποίο θα διαγράφει από τον σχετικό κατάλογο τις εταιρείες που δεν συμμορφώνονται[25].

Από τα όσα αναφέρθηκαν μέχρι τώρα, προκύπτει ένας σοβαρός προβληματισμός για το κατά πόσο διαφοροποιείται ουσιωδώς το πλαίσιο της Ασπίδας Προστασίας από το καθεστώς Ασφαλούς Λιμένα, ώστε να καθίσταται σύμφωνο με την απόφαση Schrems I. Αυτό διότι το νέο πλαίσιο κινείται στο ίδιο μοτίβο με το προϊσχύσαν πλαίσιο μέσω της διαδικασίας αυτοπιστοποίησης και της υιοθέτησης των αρχών υπό την κρατική επίβλεψη. Εντούτοις, όπως θα δούμε και στην συνέχεια, είναι σαφές ότι ο ανωτέρω αναφερόμενος τρόπος προσέγγισης του ζητήματος εξασφάλισης επαρκούς προστασίας των προσωπικών δεδομένων που διαβιβάζονται από την Ευρώπη στις ΗΠΑ δεν καθιερώνει ένα ουσιαστικό καθεστώς προστασίας, διαφανές και προσιτό στα υποκείμενα επεξεργασίας των δεδομένων, καθώς όπως προαναφέρθηκε ακόμα

[25] Βλ. Παναγοπούλου Φερενίκη, Συνταγματικές προεκτάσεις των μηχανισμών διευρύνσεως της προστασίας δεδομένων προσωπικού χαρακτήρα πέραν της ΕΕ: Εξωεφαφική εφαρμογή του ΓΚΠΔ και διασυνοριακή διαβίβαση δεδομένων, ΔίΜΕΕ τ. 4/2019, σελ. 512

και όσοι προσφεύγουν στον διαμεσολαβητή δεν λαμβάνουν τελικά ουδεμία ουσιαστική ενημέρωση για την τυχούσα επεξεργασία των προσωπικών τους δεδομένων[26].

1.4 Απόφαση Schrems II[27]

1.4.1 Πραγματικά περιστατικά και προδικαστικά ερωτήματα

Μετά την ακύρωση του μηχανισμού ασφαλούς λιμένα, ο Max Schrems υπέβαλε εκ νέου την καταγγελία του στο ιρλανδικό DPC με το σκεπτικό ότι το Facebook συνέχισε να μεταφέρει προσωπικά δεδομένα από την ευρωπαϊκή έδρα του στην Ιρλανδία στις ΗΠΑ, βασιζόμενο τώρα σε SCC. Στις 12 Απριλίου 2018, το Ανώτατο Δικαστήριο της Ιρλανδίας παρέπεμψε την υπόθεση στο ΔΕΕ μαζί με έντεκα ερωτήματα που πρέπει να εξετάσει το δικαστήριο[28].

Τα προδικαστικά ερωτήματα όπως παρατίθενται στην απόφαση ήταν τα εξής[29]:

1) Στην περίπτωση που μια εταιρεία με έδρα κράτος μέλος της Ένωσης διαβιβάζει δεδομένα προσωπικού χαρακτήρα σε μια άλλη εταιρεία που βρίσκεται εγκατεστημένη σε τρίτη χώρα σύμφωνα με την απόφαση ΤΣΡ και τα δεδομένα αυτά υπόκεινται σε δυνητική επεξεργασία από τις αρχές αυτής της χώρας για λόγους εθνικής ασφάλειας, τυγχάνει εφαρμογής το δίκαιο της Ένωσης (περιλαμβανομένου του Χάρτη) ανεξαρτήτως των διατάξεων του άρθρου 4, παράγραφος 2, ΣΕΕ, που αφορά την εθνική ασφάλεια, και του άρθρου 3, παράγραφος 2, πρώτη περίπτωση, της οδηγίας 95/46, που αφορά τη δημόσια ασφάλεια, την εθνική άμυνα και την ασφάλεια του κράτους;

---

[26] Βλ. Παύλου Αναστασία Η., Η διαβίβαση των προσωπικών δεδομένων από την Ευρώπη στις Ηνωμένες Πολιτείες Αμερικής (διπλωματική εργασία), Εθνικόν και Καποδιστριακόν Πανεπιστήμιον Αθηνών, σελ. 50.

[27] Βλ. Δ.Ε.Ε., C-311/18 (Grand Chamber), Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems, 16/07/2020, διαθέσιμη σε: https://curia.europa.eu/juris/liste.jsf?oqp=&for=&mat=or&lgrec=el&jge=&td=%3BALL&jur=C%2CT%2CF&num=C-311%252F18&page=1&dates=&pcs=Oor&lg=&pro=&nat=or&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%252C%252C%252C%252C%252C%252C%252Ctrue%252Cfalse%252C

[28] Βλ. Data Guidance, The Definitive Guide to Schrems II, 25/03/2022, διαθέσιμο σε: https://www.dataguidance.com/resource/definitive-guide-schrems-ii

[29] Βλ. Δ.Ε.Ε., C-311/18, σκέψη 68

2) α) Ποιο πρέπει να θεωρείται ως σημείο αναφοράς, σύμφωνα με την φύση της οδηγίας 95/46, για να διαπιστώσουμε εάν λαμβάνει χώρα προσβολή των δικαιωμάτων των φυσικών προσώπων από την περαιτέρω επεξεργασία των δεδομένων τους από εθνικές αρχές τρίτης χώρας για λόγους εθνικής ασφάλειας;

i) ο Χάρτης, η ΣΕΕ, η ΣΛΕΕ, η οδηγία 95/46, η Ευρωπαϊκή Σύμβαση για την Προάσπιση των Δικαιωμάτων του Ανθρώπου και των Θεμελιωδών Ελευθεριών που υπογράφτηκε στη Ρώμη στις 4 Νοεμβρίου 1950, ή οποιαδήποτε άλλη διάταξη του δικαίου της Ένωσης, ή

ii) το εθνικό δίκαιο ενός ή περισσοτέρων κρατών μελών;

β) Αν θέσουμε ως μέτρο σύγκρισης το εθνικό δίκαιο ενός ή περισσοτέρων κρατών μελών της Ένωσης, πρέπει να συμπεριλάβουμε και τις ανάλογες πρακτικές που εφαρμόζονται στον τομέα της εθνικής ασφάλειας;

3) Κατά την διαδικασία αξιολόγησης του επιπέδου προστασίας των δεδομένων που διασφαλίζει μια τρίτη χώρα σύμφωνα με τις απαιτήσεις της ευρωπαϊκής νομοθεσίας για τις διαβιβάσεις δεδομένων, διενεργείται έλεγχος στα εξής:

α) τις εφαρμοστέες νομοθετικές διατάξεις της τρίτης χώρας, όπως απορρέουν από το εθνικό δίκαιο ή από τις διεθνείς δεσμεύσεις, και τις πρακτικές που έχουν σχεδιαστεί προκειμένου να διασφαλίζεται η συμμόρφωση με τους κανόνες αυτούς, περιλαμβανομένων των επαγγελματικών κανόνων και μέτρων ασφαλείας που τηρούνται στην τρίτη χώρα, ή

β) τις παραπάνω νομοθετικές διατάξεις, σε συνδυασμό με τυχόν διοικητικές και κανονιστικές πρακτικές καθώς και πρακτικές συμμόρφωσης, εγγυήσεις, διαδικασίες, πρωτόκολλα, εποπτικούς μηχανισμούς και εξωδικαστικά μέσα έννομης προστασίας που υφίστανται στην τρίτη χώρα;

4) Λαμβάνοντας υπόψη τα πραγματικά περιστατικά που διαπίστωσε το ανώτατο Ιρλανδικό δικαστήριο αναφορικά με το δίκαιο των Ηνωμένων Πολιτειών, υφίσταται προσβολή των δικαιωμάτων των φυσικών προσώπων κατά τα άρθρα 7 ή/και 8 του Χάρτη, σε περίπτωση που διαβιβάζονται δεδομένα προσωπικού χαρακτήρα από την Ένωση προς τις Ηνωμένες Πολιτείες δυνάμει της αποφάσεως ΤΣΡ;

5) Λαμβάνοντας υπόψη τα πραγματικά περιστατικά που διαπίστωσε το ανώτατο δικαστήριο της Ιρλανδίας αναφορικά με το δίκαιο των Ηνωμένων Πολιτειών, στην περίπτωση που τα δεδομένα διαβιβάζονται από την ΕΕ προς τις ΗΠΑ δυνάμει της αποφάσεως ΤΣΡ:

α) η νομοθεσία των ΗΠΑ σέβεται την ουσία του δικαιώματος προσφυγής των φυσικών προσώπων σε περίπτωση παραβίασης των δεδομένων τους και σύμφωνα με το άρθρο 47 του Χάρτη;

Σε περίπτωση καταφατικής απαντήσεως στο παραπάνω ερώτημα:

β) οι περιορισμοί που θέτονται από την αμερικανική νομοθεσία στο δικαίωμα δικαστικής προσφυγής ενός φυσικού προσώπου στο πλαίσιο που άπτεται της εθνικής ασφάλειας των Ηνωμένων Πολιτειών, μπορούν να θεωρηθούν ανάλογοι με την έννοια του άρθρου 52 του Χάρτη και μη υπερβαίνοντες το μέτρο του αναγκαίου για σκοπούς εθνικής ασφάλειας σε μια δημοκρατική κοινωνία;

6) α) Ποιο είναι το απαιτούμενο επίπεδο προστασίας που θα πρέπει να εξασφαλίζεται κατά την διαβίβαση προσωπικών δεδομένων μέσω ΤΣΡ που συνάπτονται σύμφωνα με απόφαση της Επιτροπής κατά την έννοια του άρθρου 26, παράγραφος 4, της οδηγίας 95/46, λαμβανομένων υπόψη των διατάξεων της οδηγίας 95/46, και ειδικότερα των άρθρων 25 και 26, υπό το πρίσμα του Χάρτη;

β) Κατά την διαδικασία αξιολόγησης του επιπέδου προστασίας που παρέχεται από την απόφαση ΤΣΡ σε σχέση με τις απαιτήσεις που προβλέπονται στην οδηγία 95/46 και στον Χάρτη, ποια στοιχεία θα πρέπει να λαμβάνουμε υπόψη;

7) Από την στιγμή που οι τυποποιημένες συμβατικές ρήτρες δεν είναι δεσμευτικές για τις εθνικές αρχές των τρίτων κρατών που μπορεί να έχουν πρόσβαση στα διαβιβαζόμενα δεδομένα εν δυνάμει της απόφασης ΤΣΡ, αποκλείεται να προκύπτουν από τις ρήτρες επαρκείς εγγυήσεις όπως προβλέπεται στην οδηγία 95/46;

8) Στην περίπτωση που εισαγωγέας δεδομένων από τρίτη χώρα υπόκειται σε νομικό πλαίσιο παρακολουθήσεων, το οποίο κατά την άποψη μιας εθνικής αρχής προστασίας δεδομένων συγκρούεται με τις τυποποιημένες συμβατικές ρήτρες ή με την οδηγία 95/46 ή/και με τον Χάρτη, είναι η αντίστοιχη εθνική αρχή προστασίας δεδομένων υποχρεωμένη να ασκήσει τις εξουσίες που προβλέπονται στην οδηγία

95/46 και να αναστείλει τις ροές δεδομένων, ή οι εξουσίες αυτές ασκούνται σε εξαιρετικές περιπτώσεις. Μπορεί η εκάστοτε εθνική αρχή προστασίας δεδομένων να στηριχθεί στη διακριτική της ευχέρεια και να μην αναστείλει τις ροές δεδομένων;

9) α) Η απόφαση ΑΠΙΖ συνιστά κανόνα γενικής ισχύος με δεσμευτικό χαρακτήρα τόσο για τις εθνικές αρχές προστασίας δεδομένων, όσο και για τα εθνικά δικαστήρια των κρατών μελών της Ένωσης;

β) Σε περίπτωση αρνητικής απάντησης στο παραπάνω ερώτημα, επηρεάζεται η διαδικασία αξιολόγησης του επιπέδου προστασίας που προσφέρουν οι νομοθετημένες εγγυήσεις που παρέχονται στους φορείς των δεδομένων στις διαβιβάσεις που γίνονται εν δυνάμει της απόφασης ΤΣΡ, από την απόφαση ΑΠΙΖ;

10) Λαμβάνοντας υπόψη τις διαπιστώσεις στις οποίες προχώρησε το Ιρλανδικό ανώτατο δικαστήριο σχετικά με το επίπεδο προστασίας που διασφαλίζει η αμερικανική νομοθεσία, σε συνδυασμό με την θέσπιση του μηχανισμού του Διαμεσολαβητή, μπορούμε να θεωρήσουμε οτι οι ΗΠΑ παρέχουν την αναγκαία σύμφωνα με το άρθρο 47 του Χάρτη έννομη προστασία στους ενδιαφερομένους των οποίων τα δεδομένα προσωπικού χαρακτήρα διαβιβάστηκαν προς τις Ηνωμένες Πολιτείες δυνάμει της αποφάσεως ΤΣΡ;

11) Αντιβαίνει η απόφαση περί τυποποιημένων συμβατικών ρητρών τα άρθρα 7, 8 και 47 του Χάρτη;

1.4.2 Σκεπτικό ΔΕΕ

Επί του πρώτου προδικαστικού ερωτήματος επισημάνθηκε οτι η διάταξη της ΣΕΕ που ορίζει την εθνική ασφάλεια εντός της ΕΕ ως ευθύνη των επιμέρους κρατών μελών, αφορά αποκλειστικώς τα εν λόγω κράτη μέλη της Ένωσης. Κατ' επέκταση η εν λόγω διάταξη δεν επηρεάζει την ερμηνεία του άρθρου 2, παράγραφος 1, και του άρθρου 2, παράγραφος 2, στοιχεία α΄, β΄ και δ΄, του ΓΚΠΔ[30]. Σύμφωνα με το άρθρο 2, παράγραφος 1, του ΓΚΠΔ, ο κανονισμός αυτός εφαρμόζεται στην περίπτωση της, εν όλω ή εν μέρει, αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα, καθώς και στη μη αυτοματοποιημένη επεξεργασία τέτοιων δεδομένων τα οποία περιλαμβάνονται ή πρόκειται να περιληφθούν σε σύστημα αρχειοθέτησης.

[30] Βλ. Δ.Ε.Ε., C-311/18, σκέψη 81

Παράλληλα, σύμφωνα με το άρθρο 4, σημείο 2, του ΓΚΠΔ η έννοια της «επεξεργασίας» ορίζεται ως «κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα» και παραθέτει, ως παραδείγματα, την «κοινολόγηση με διαβίβαση, τη διάδοση ή κάθε άλλη μορφή διάθεσης», χωρίς να διακρίνει ανάλογα με το αν οι πράξεις αυτές διενεργούνται στο εσωτερικό της Ένωσης ή συνδέονται με τρίτη χώρα. Πέραν αυτών, ο ΓΚΠΔ θεσπίζει ιδιαίτερους κανόνες για την διαβίβαση προσωπικών δεδομένων σε χώρες εκτός της ΕΕ ή σε διεθνείς οργανισμούς. Παράλληλα, σύμφωνα με το άρθρο 58 εξοπλίζει τις εθνικές εποπτικές αρχές με ειδικές εξουσίες[31]. Επομένως, η πράξη που συνίσταται στη διαβίβαση δεδομένων προσωπικού χαρακτήρα από κράτος μέλος της Ένωσης προς τρίτη χώρα συνιστά, αυτή καθεαυτήν, επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά την έννοια του άρθρου 4, σημείο 2, του ΓΚΠΔ, πραγματοποιούμενη σε κράτος μέλος, επί της οποίας ο ΓΚΠΔ έχει εφαρμογή δυνάμει του άρθρου 2, παράγραφος 1, του ίδιου αυτού κανονισμού[32]. Ως προς το ερώτημα όμως αν μια τέτοια πράξη μπορεί να εξαιρεθεί από το πεδίο εφαρμογής του ΓΚΠΔ, πρέπει να τονίσουμε οτι ο ίδιος ο κανονισμός προβλέπει εξαιρέσεις οι οποίες όμως πρέπει να ερμηνεύονται στενά[33]. Εν προκειμένω, επειδή η επίμαχη στην υπόθεση της κύριας δίκης διαβίβαση προσωπικών δεδομένων πραγματοποιείται από τη Facebook Ireland προς τη Facebook Inc., ήτοι μεταξύ δύο νομικών προσώπων, η διαβίβαση αυτή δεν εμπίπτει στον ΓΚΠΔ, καθώς δεν αποτελεί επεξεργασία προσωπικών δεδομένων που πραγματοποιείται από φυσικό πρόσωπο στο πλαίσιο αυστηρά προσωπικής ή οικιακής δραστηριότητας. Η επίμαχη διαβίβαση δεν καλύπτεται ούτε από τις εξαιρέσεις που προβλέπει ο ΓΚΠΔ, δεδομένου ότι οι δραστηριότητες οι οποίες αναφέρονται εκεί ως παραδείγματα είναι, σε όλες τις περιπτώσεις, δραστηριότητες που ασκούνται από κράτη ή από κρατικές αρχές και δεν άπτονται των τομέων δραστηριότητας των ιδιωτών[34]. Τέλος, μια διαβίβαση προσωπικών δεδομένων δεν πρέπει να εξαιρείται από το πεδίο εφαρμογής του ΓΚΠΔ επειδή τα επίμαχα δεδομένα μπορεί να αποτελέσουν αντικείμενο δυνητικής επεξεργασία, κατά τη διάρκεια ή κατόπιν της

[31] Βλ. Δ.Ε.Ε., C-311/18, σκέψη 82

[32] Βλ. Δ.Ε.Ε., C-311/18, σκέψη 83

[33] Βλ. Δ.Ε.Ε., C-311/18, σκέψη 84

[34] Βλ. Δ.Ε.Ε., C-311/18, σκέψη 85

διαβίβασης αυτής, από τις υπηρεσίες πληροφοριών της αντίστοιχης τρίτης χώρας για λόγους δημόσιας ασφάλειας, εθνικής άμυνας και ασφάλειας του κράτους[35]. Εκ των παραπάνω, σύμφωνα με τις παραγράφους 1 και 2 του άρθρου 2 του ΓΚΠΔ, στο πεδίο εφαρμογής του εν λόγου κανονισμού εμπίπτει κάθε διαβίβαση δεδομένων προσωπικού χαρακτήρα η οποία πραγματοποιείται για εμπορικούς σκοπούς από οικονομικό φορέα εγκατεστημένο σε κράτος μέλος προς άλλον οικονομικό φορέα εγκατεστημένο σε τρίτη χώρα, ανεξαρτήτως του ότι, κατά τη διάρκεια ή κατόπιν της διαβίβασης αυτής, τα δεδομένα ενδέχεται να υποστούν επεξεργασία από τις αρχές της αντίστοιχης τρίτης χώρας για λόγους δημόσιας ασφάλειας, εθνικής άμυνας και ασφάλειας του κράτους[36].

Επί του δεύτερου, τρίτου και έκτου προδικαστικού ερωτήματος πρέπει να δοθεί η απάντηση ότι οι παράγραφοι 1 και 2 του άρθρου 46 του κανονισμού ορίζουν οτι οι εγγυήσεις, τα εκτελεστά δικαιώματα και τα μέσα έννομης προστασίας, που αναφέρονται στις εν λόγω διατάξεις, θα πρέπει να συνθέτουν ένα ουσιαστικά ισοδύναμο επίπεδο προστασίας, στα δεδομένα προσωπικού χαρακτήρα που διαβιβάζονται σε τρίτη χώρα βάσει ΤΣΡ, σε σύγκριση με εκείνο που παρέχεται στην ΕΕ. Προς τούτο, κατά την διαδικασία αξιολόγησης του επιπέδου προστασίας που εξασφαλίζει μια διαβίβαση βασισμένη σε ΤΣΡ πρέπει, μεταξύ άλλων, να λαμβάνονται υπόψη τόσο οι συμβατικοί όροι που έχουν συμφωνηθεί μεταξύ των "προσώπων" που θα διενεργήσουν την διαβίβαση (υπεύθυνος/εκτελών την επεξεργασία - αποδέκτης δεδομένων) όσο και η ενδεχόμενη πρόσβαση στα διαβιβαζόμενα δεδομένα από τις δημόσιες αρχές της τρίτης χώρας. Φυσικά θα πρέπει να εξετάζονται και τα κρίσιμα στοιχεία του νομικού συστήματός της τρίτης χώρας, ιδίως εκείνα που αναφέρονται στην παράγραφο 2 του άρθρου 45 του ΓΚΠΔ[37].

Επί του όγδοου προδικαστικού ερωτήματος το δικαστήριο εκθέτει τις παρακάτω παρατηρήσεις. Σύμφωνα με την παράγραφο 3 του άρθρου 8 του Χάρτη, σε συνδυασμό με τα άρθρα 51 και 57 του κανονισμού, ο έλεγχος εφαρμογής και τήρησης αυτού, αποτελεί πρωταρχική αποστολή για τις εθνικές εποπτικές αρχές[38].

---

[35] Βλ. Δ.Ε.Ε., C-311/18, σκέψη 88

[36] Βλ. Δ.Ε.Ε., C-311/18, σκέψη 89

[37] Βλ. Δ.Ε.Ε., C-311/18, σκέψη 105

[38] Βλ. Δ.Ε.Ε., C-311/18, σκέψη 107

Επιπλέον, σύμφωνα με το άρθρο 57 του κανονισμού, κάθε εθνική εποπτική αρχή έχει την υποχρέωση αφενός, να εξετάζει τις καταγγελίες που υποβάλλονται σε αυτή από υποκείμενα δεδομένων σύμφωνα με την διάταξη του άρθρου 77 του ΓΚΠΔ και αφετέρου να ερευνά το αντικείμενό τους στο μέτρο του αναγκαίου[39]. Εν συνεχεία, στο άρθρο 78 του κανονισμού αναγνωρίζεται το δικαίωμα άσκησης αποτελεσματική δικαστική προσφυγή από το θιγόμενο πρόσωπο ακόμα και στην περίπτωση που η αρμόδια κατά τόπο εποπτική αρχή έχει παραλείψει να εξετάσει την καταγγελία του[40]. Ωστόσο δεν πρέπει να παραλείψουμε να αναφέρουμε οτι κάθε εποπτική αρχή θα πρέπει να ασκεί τις αρμοδιότητές της τηρώντας πλήρως πιθανές αποφάσεις επάρκειας της Επιτροπής που αναγνωρίζουν ικανοποιητικό επίπεδο προστασίας σε τρίτη χώρα[41]. Επιπλέον, η ύπαρξη απόφαση επάρκειας σε καμία περίπτωση δεν εμποδίζει τα υποκείμενα δεδομένων να υποβάλουν σύμφωνα με το άρθρο 77 του κανονισμού καταγγελία σε αρμόδια εποπτική αρχή. Ομοίως, η ύπαρξη μιας τέτοιας απόφασης δεν μπορεί ούτε να εξαλείψει, ούτε να περιορίσει τις εξουσίες που αναγνωρίζονται ρητώς στις εθνικές εποπτικές αρχές με το άρθρο 8 του Χάρτη αλλά και τα άρθρα 51 και 57 του ΓΚΠΔ[42]. Επομένως, ακόμη και στην περίπτωση ύπαρξης απόφασης επάρκειας, η εποπτική αρχή μπορεί να εξετάσει αν πληρούνται οι απαιτήσεις του ΓΚΠΔ κατά την διαβίβαση δεδομένων και να προσφύγει ενώπιον των εθνικών δικαστηρίων έτσι ώστε αυτά με την σειρά τους, αν συμμερίζονται τις αμφιβολίες της αρχής ελέγχου ως προς το κύρος της αποφάσεως επάρκειας, να υποβάλουν αίτηση προδικαστικής παραπομπής προς το ΔΕΕ για την εξέταση του κύρους[43]. Κατόπιν των ανωτέρω σκέψεων, στο όγδοο προδικαστικό ερώτημα πρέπει να δοθεί η παρακάτω απάντηση. Σύμφωνα με την παράγραφο 2 του άρθρου 58 του κανονισμού, όταν δεν έχει εκδοθεί κάποια απόφαση επάρκειας από την Επιτροπή, κάθε αρμόδια εποπτική αρχή έχει την υποχρέωση να αναστέλλει ή και να απαγορεύει κάθε διαβίβαση δεδομένων προς τρίτη χώρα, η οποία βασίζεται σε ΤΣΡ, υπό την προϋπόθεση ύπαρξης εκτίμησης από την Αρχή οτι οι εν λόγω ρήτρες δεν τηρούνται ή δεν μπορούν να τηρηθούν ορθά στην

[39] Βλ. Δ.Ε.Ε., C-311/18, σκέψη 109

[40] Βλ. Δ.Ε.Ε., C-311/18, σκέψη 110

[41] Βλ. Δ.Ε.Ε., C-311/18, σκέψη 116

[42] Βλ. Δ.Ε.Ε., C-311/18, σκέψη 119

[43] Βλ. Δ.Ε.Ε., C-311/18, σκέψη 120

τρίτη χώρα και παράλληλα δεν διασφαλίζεται ισοδύναμο επίπεδο προστασίας όπως κατοχυρώνεται στα άρθρα 45 και 46 του κανονισμού με άλλα μέσα[44].

Επί του έβδομου και ενδέκατου προδικαστικού ερωτήματος το δικαστήριο καταλήγει στις εξής παρατηρήσεις. Στην περίπτωση της διαβίβασης δεδομένων δια μέσω τυποποιημένων συμβατικών ρητρών σε τρίτη χώρα, είναι ευρέως κατανοητό οτι οι συμβατικοί όροι που εμπεριέχονται στις ρήτρες αυτές περιορίζουν αποκλειστικά αφενός τον υπεύθυνο επεξεργασίας, που βρίσκεται εγκατεστημένος εντός της ΕΕ, και αφετέρου τον εισαγωγέα των δεδομένων που βρίσκεται στην τρίτη χώρα. Άρα κατ' επέκταση οι ρήτρες αυτές δεν μπορούν να δεσμεύσουν τις Αρχές της τρίτης χώρας που μπορεί να προβούν σε επεξεργασία των διαβιβαζόμενων δεδομένων σύμφωνα με διατάξεις της εθνικής νομοθεσίας, καθώς δεν αποτελούν συμβαλλόμενα μέρη[45]. Για τον παραπάνω λόγο ενδέχεται οι ρήτρες αυτές να μην αποτελούν τελικά επαρκές μέσο για την διασφάλιση του αναγκαίου επιπέδου προστασίας που απαιτείται από τον ΓΚΠΔ για τις διαβιβάσεις δεδομένων σε τρίτες χώρες[46]. Στην περίπτωση αποφάσεως της Επιτροπής με την οποία θεσπίζονται τυποποιημένες συμβατικές ρήτρες για την προστασία των διαβιβαζόμενων δεδομένων, όπως είναι και η εξεταζόμενη από το ΔΕΕ απόφαση, στο μέτρο που μια τέτοια απόφαση δεν αφορά τρίτη χώρα, έδαφός της ή έναν ή περισσότερους συγκεκριμένους τομείς στο εσωτερικό της, δεν είναι δυνατόν να συναχθεί από το άρθρο 46, παράγραφος 1, και από το άρθρο 46, παράγραφος 2, στοιχείο γ΄, του ΓΚΠΔ ότι η Επιτροπή υποχρεούται να προβαίνει, πριν από την έκδοση τέτοιας απόφασης, σε αξιολόγηση της επάρκειας του επιπέδου προστασίας που εξασφαλίζουν οι τρίτες χώρες προς τις οποίες θα μπορούσαν να διαβιβαστούν δεδομένα προσωπικού χαρακτήρα βάσει τέτοιων ρητρών[47]. Υπενθυμίζεται συναφώς ότι, σύμφωνα με την παράγραφο 1 του άρθρου 46, στην περίπτωση που η Επιτροπή δεν έχει εκδώσει απόφαση επάρκειας που να θεσπίζει κατάλληλες εγγυήσεις, αυτό αποτελεί καθήκον είτε του υπεύθυνου επεξεργασίας είτε του εκτελούντος την επεξεργασία, οι οποίοι είναι αμφότεροι εγκατεστημένοι εντός της Ένωσης[48]. Στην

[44] Βλ. Δ.Ε.Ε., C-311/18, σκέψη 121

[45] Βλ. Δ.Ε.Ε., C-311/18, σκέψη 125

[46] Βλ. Δ.Ε.Ε., C-311/18, σκέψη 126

[47] Βλ. Δ.Ε.Ε., C-311/18, σκέψη 130

[48] Βλ. Δ.Ε.Ε., C-311/18, σκέψη 131

περίπτωση όμως που ούτε ο υπεύθυνος επεξεργασίας ούτε ο εκτελών την επεξεργασία, αμφότεροι εγκατεστημένοι εντός της ΕΕ, μπορούν να λάβουν επαρκή συμπληρωματικά μέτρα για τη διασφάλιση προσήκουσας προστασίας, τότε αυτοί ή, επικουρικώς, η αρμόδια αρχή ελέγχου υποχρεούνται να αναστείλουν ή να τερματίσουν τη διαβίβαση δεδομένων προσωπικού χαρακτήρα προς την οικεία τρίτη χώρα[49]. Το γεγονός λοιπόν οτι οι τυποποιημένες συμβατικές ρήτρες που εκδίδονται από την Επιτροπή σύμφωνα με την παράγραφο 2 του άρθρου 46 του κανονισμού, δεν γίνεται να δεσμεύουν τις δημόσιες αρχές τρίτης χώρας που μπορεί να έχουν πρόσβαση στα διαβιβαζόμενα δεδομένα δεν επηρεάζει καθόλου το κύρος της αντίστοιχης απόφασης[50]. Αντιθέτως, σημαντικός παράγοντας για την διασφάλιση του κύρους της απόφασης περί τυποποιημένων συμβατικών ρητρών αποτελεί η ύπαρξη ή όχι αποτελεσματικών μηχανισμών που θα εξασφαλίζουν την τήρηση του απαιτούμενου επιπέδου προστασίας στα διαβιβαζόμενα δεδομένα και ότι οι διαβιβάσεις δεδομένων προσωπικού χαρακτήρα βάσει τέτοιων ρητρών αναστέλλονται ή απαγορεύονται σε περίπτωση παράβασης των ρητρών αυτών ή αδυναμίας τήρησής τους[51]. Το δικαστήριο προέβη στον έλεγχο των μηχανισμών που προβλέπονταν στην απόφαση ΤΣΡ και αποφάνθηκε οτι η απόφαση όντως προβλέπει αποτελεσματικούς μηχανισμούς που διασφαλίζουν, επί της ουσίας, ότι η διαβίβαση δεδομένων προς τρίτες χώρες βάσει των τυποποιημένων συμβατικών ρητρών που περιλαμβάνονται στην απόφαση αυτή δύναται να αναστέλλεται ή απαγορεύεται όταν ο αποδέκτης της διαβίβασης είτε δεν τηρεί τις εν λόγω ρήτρες είτε αδυνατεί να τις τηρήσει[52]. Κατόπιν όλων των παραπάνω διατυπώσεων, στο έβδομο και στο ενδέκατο προδικαστικό ερώτημα πρέπει να δοθεί η απάντηση ότι από την εξέταση της αποφάσεως περί τυποποιημένων συμβατικών ρητρών υπό το πρίσμα των άρθρων 7, 8 και 47 του Χάρτη δεν προέκυψε κανένα στοιχείο ικανό να θίξει το κύρος της αποφάσεως αυτής[53].

[49] Βλ. Δ.Ε.Ε., C-311/18, σκέψη 135

[50] Βλ. Δ.Ε.Ε., C-311/18, σκέψη 136

[51] Βλ. Δ.Ε.Ε., C-311/18, σκέψη 137

[52] Βλ. Δ.Ε.Ε., C-311/18, σκέψη 148

[53] Βλ. Δ.Ε.Ε., C-311/18, σκέψη 149

Επί του τέταρτου, πέμπτου, ένατου και δέκατου προδικαστικού ερωτήματος το ΔΕΕ είχε την ευκαιρία να εξετάσει αν η απόφαση ΑΠΙΖ είναι σύμφωνη με τις απαιτήσεις οι οποίες απορρέουν από τον ΓΚΠΔ, όπως ερμηνεύεται σε συνδυασμό με τον Χάρτη. Κατά την διαδικασία έκδοσης απόφασης επάρκειας από την Επιτροπή σύμφωνα με τα αναφερόμενα στην παράγραφο 3 του άρθρου 45 του ΓΚΠΔ, πρέπει να διαπιστωθεί η ύπαρξη ενός ουσιαστικά ισοδύναμου επιπέδου προστασίας των δικαιωμάτων με αυτό που εξασφαλίζεται εντός της Ένωσης. Η διαπίστωση αυτή γίνεται μετά από την εξέταση της εσωτερικής νομοθεσίας και των διεθνών δεσμεύσεων για την προστασία των θεμελιωδών δικαιωμάτων που έχει αναλάβει η τρίτη χώρα[54]. Ωστόσο η εξεταζόμενη από το ΔΕΕ απόφαση επάρκειας αναγνωρίζει στο παράρτημα ΙΙ την δυνατότητα περιορισμού εφαρμογής των θεσπιζόμενων αρχών για λόγους εθνικής ασφάλειας, δημοσίου συμφέροντος ή επιβολής του νόμου. Κατά συνέπεια, όπως και το πλαίσιο των αρχών ασφαλούς λιμένα που εξετάστηκε στην υπόθεση Schrems I, έτσι και η απόφαση ΑΠΙΖ που εξετάζεται στα πλαίσια της υπόθεσης Schrems II καθιερώνει την υπεροχή των συγκεκριμένων απαιτήσεων έναντι των αρχών του πλαισίου της ασπίδας προστασίας ιδιωτικής ζωής, εξαιτίας αυτής της υπεροχής οι αυτοπιστοποιημένες αμερικανικές εταιρείες που λαμβάνουν δεδομένα προσωπικού χαρακτήρα από την ΕΕ οφείλουν να αποκλίνουν, χωρίς περιορισμό, από τις προαναφερθείσες αρχές όταν αυτές συγκρούονται με τις ανωτέρω απαιτήσεις και ως εκ τούτου παρίστανται ασύμβατες προς τις τελευταίες[55]. Συνέπεια των παραπάνω είναι να καθίστανται δυνατές επεμβάσεις στα προσωπικά δεδομένα που διαβιβάζονται ή θα μπορούσαν να διαβιβαστούν στις ΗΠΑ, έχοντας ως μοναδικό έρεισμα τις επιταγές περί εθνικής ασφάλειας και δημοσίου συμφέροντος της αμερικανικής νομοθεσίας. Το δικαστήριο στις σκέψεις 168-202 εξετάζει την επάρκεια του επιπέδου προστασίας που παρέχει η ΑΠΙΖ σύμφωνα με τις απαιτήσεις που απορρέουν από την παράγραφο 1 του άρθρου 45 του ΓΚΠΔ, όπως ερμηνεύεται σε συνδυασμό με τα άρθρα 7,8,47,52 του Χάρτη Θεμελιωδών Δικαιωμάτων. Τα άρθρα 7 και 8 του Χάρτη, συμβάλλουν στην επίτευξη του επιπέδου προστασίας που απαιτείται εντός της Ένωσης και γι’ αυτό τον λόγο η τήρησή τους θα πρέπει να διαπιστώνεται από την Επιτροπή πριν από την έκδοση της απόφασης επάρκειας σύμφωνα με την παράγραφο 1 του άρθρου 45 του κανονισμού. Πιο αναλυτικά

[54] Βλ. Δ.Ε.Ε., C-311/18, σκέψη 162

[55] Βλ. Δ.Ε.Ε., C-311/18, σκέψη 164

σύμφωνα με το άρθρο 7 κάθε φυσικό πρόσωπο απολαμβάνει το δικαίωμα σεβασμού στην ιδιωτική και οικογενειακή ζωή του, της κατοικίας του και των επικοινωνιών του. Το δε άρθρο 8, μέσω της παραγράφου 1 αναγνωρίζει ρητώς το δικαίωμα κάθε προσώπου στην προστασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν[56]. Το Δικαστήριο έχει κρίνει σε προηγούμενες αποφάσεις του ότι η πρόσβαση στα διαβιβαζόμενα δεδομένα από τρίτον, όπως είναι οι δημόσιες αρχές, συνιστά επέμβαση στα θεμελιώδη δικαιώματα τα οποία κατοχυρώνονται στα άρθρα 7 και 8 του Χάρτη, ανεξαρτήτως της μεταγενέστερης χρήσης των πληροφοριών που γνωστοποιήθηκαν. Το ίδιο ισχύει και στην περίπτωση διατήρησης δεδομένων προσωπικού χαρακτήρα καθώς και για την πρόσβαση στα δεδομένα αυτά με σκοπό τη χρήση τους από τις δημόσιες αρχές, ανεξαρτήτως του αν οι σχετικές με την ιδιωτική ζωή πληροφορίες έχουν ευαίσθητο χαρακτήρα ή του αν οι ενδιαφερόμενοι υπέστησαν τυχόν δυσμενείς συνέπειες λόγω της επέμβασης αυτής[57]. Όσον αφορά το άρθρο 47 του Χάρτη, αυτό κατοχυρώνει τόσο το δικαίωμα αποτελεσματικής προσφυγής σε κάθε πρόσωπο του οποίου θίγονται τα δικαιώματα και οι ελευθερίες που διασφαλίζει το ευρωπαϊκό δίκαιο, όσο και το δικαίωμα εκδίκασης της υπόθεσής του από ανεξάρτητο και αμερόληπτο δικαστήριο[58]. Τέλος, σύμφωνα με την παράγραφο 1 του άρθρου 52 του Χάρτη κάθε περιορισμός στην άσκηση των δικαιωμάτων και των ελευθεριών που αναγνωρίζονται με τον Χάρτη πρέπει να προβλέπεται από τον νόμο και να μη θίγει το ουσιαστικό περιεχόμενο των εν λόγω δικαιωμάτων. Σύμφωνα και με την αρχή της αναλογικότητας, περιορισμοί θα επιβάλλονται σε αυτά τα δικαιώματα μόνο εφόσον είναι αναγκαίοι και ανταποκρίνονται πραγματικά σε σκοπούς γενικού συμφέροντος τους οποίους αναγνωρίζει η Ένωση ή στην ανάγκη προστασίας των δικαιωμάτων και ελευθεριών των τρίτων[59]. Σχετικά με την νομοθεσία των ΗΠΑ, η πρόσβαση στα διαβιβαζόμενα δεδομένα από τις υπηρεσίες πληροφοριών των ΗΠΑ που στηρίζεται στο άρθρο 702 του νόμου FISA αλλά και στο εκτελεστικό διάταγμα 12333 (EO 12333), δεν υπόκειται στις απαιτήσεις της ευρωπαϊκής νομοθεσίας για την δημιουργία ενός ουσιαστικά ισοδύναμου επιπέδου προστασίας των δεδομένων, όπως αυτό

[56] Βλ. Δ.Ε.Ε., C-311/18, σκέψη 169

[57] Βλ. Δ.Ε.Ε., C-311/18, σκέψη 171

[58] Βλ. Δ.Ε.Ε., C-311/18, σκέψη 186

[59] Βλ. Δ.Ε.Ε., C-311/18, σκέψη 174

διαμορφώνεται στην παράγραφο 1 του άρθρου 52 του Χάρτη σε συνδυασμό με την αρχή της αναλογικότητας[60]. Επομένως δεν μπορούμε να συνάγουμε από το άρθρο 702 ούτε την ύπαρξη περιορισμών στην εξουσιοδότηση εφαρμογής τέτοιων προγραμμάτων παρακολούθησης, ούτε την ύπαρξη εγγυήσεων για τους μη Αμερικανούς πολίτες τους οποίους αφορούν εν δυνάμει τα σχετικά προγράμματα[61]. Επιπλέον μέσω της PPD 28 δεν παρέχονται στα υποκείμενα των δεδομένων εκτελεστά δικαιώματα τα οποία να μπορούν να προβληθούν έναντι των αμερικανικών αρχών ενώπιον των δικαστηρίων[62]. Επιπροσθέτως ο μηχανισμός διαμεσολάβησης τον οποίο θεσπίζει η απόφαση ΑΠΙΖ δεν παρέχει κανένα μέσο δικαστικής προστασίας ενώπιον οργάνου που να προσφέρει στα υποκείμενα των δεδομένων που διαβιβάζονται στις ΗΠΑ κατάλληλες εγγυήσεις, ουσιαστικά ισοδύναμες με εκείνες που επιβάλλει το άρθρο 47 του Χάρτη[63].

Το ΔΕΕ έχοντας κατά νου τα παραπάνω αποφάνθηκε τα εξής:

1) Η διαβίβαση προσωπικών δεδομένων για εμπορικούς σκοπούς μεταξύ οικονομικών φορέων όπου ο ένας είναι εγκατεστημένος στην Ένωση και ο δεύτερος σε τρίτη χώρα εμπίπτει στο πεδίο εφαρμογής του κανονισμού 2016/679 ακόμα και στην περίπτωση που τα διαβιβαζόμενα δεδομένα μπορεί να αποτελέσουν αντικείμενο επεξεργασίας από τις εθνικές αρχές της τρίτης χώρας για λόγους δημόσιας ασφάλειας ή εθνικής άμυνας.

2) Σύμφωνα με τον κανονισμό 2016/679, οι κατάλληλες εγγυήσεις, τα εκτελεστά δικαιώματα και τα αποτελεσματικά μέσα έννομης προστασίας που παρέχονται στα υποκείμενα δεδομένων βάσει τυποποιημένων συμβατικών ρητρών θα πρέπει να δημιουργούν ένα ουσιαστικά ισοδύναμο πλαίσιο προστασίας με αυτό της Ένωσης. Κατά την διαδικασία αξιολόγησης του επιπέδου προστασίας στο πλαίσιο μίας τέτοιας διαβίβασης θα πρέπει να λαμβάνονται υπόψη τόσο οι συμβατικοί όροι μεταξύ του εξαγωγέα και του εισαγωγέα των δεδομένων, όσο και η πιθανότητα πρόσβασης στα δεδομένα από τις εθνικές αρχές της τρίτης χώρας.

---

[60] Βλ. Δ.Ε.Ε., C-311/18, σκέψη 178

[61] Βλ. Δ.Ε.Ε., C-311/18, σκέψη 180

[62] Βλ. Δ.Ε.Ε., C-311/18, σκέψη 181

[63] Βλ. Δ.Ε.Ε., C-311/18, σκέψη 197

3) Κάθε εθνική αρχή προστασίας δεδομένων σε περίπτωση που κρίνει οτι οι τυποποιημένες συμβατικές ρήτρες δεν τηρούνται ή δεν μπορούν να τηρηθούν και κατ' επέκταση δεν μπορεί να διασφαλιστεί ισοδύναμο επίπεδο προστασίας με άλλα μέσα, υποχρεούται να αναστείλει ή να απαγορεύσει την ροή δεδομένων προς την τρίτη χώρα.

4) Από την εξέταση της αποφάσεως 2010/87 της Επιτροπής που θεσπίζει την διαβίβαση δεδομένων μέσω τυποποιημένων συμβατικών ρητών βάσει της οδηγίας 95/46 και μετέπειτα της απόφασης 2016/2297, δεν προέκυψε κανένα στοιχείο ικανό να θίξει το κύρος της.

5) Κηρύσσει ανίσχυρο τον μηχανισμό διαβίβασης δεδομένων (ΑΠΙΖ) μεταξύ ΕΕ - ΗΠΑ που θεσπίστηκε με την απόφαση επάρκειας 2016/1250 της Επιτροπής.

Εν κατακλείδι, προσπαθώντας να αποκωδικοποιήσουμε τα παραπάνω θα μπορούσαμε να πούμε τα εξής[64]:

Το ΔΕΕ εξετάζοντας το κύρος της απόφασης 2010/87 για τις διαβιβάσεις δεδομένων μέσω συμβατικών ρητρών, έκρινε οτι το κύρος της απόφασης δεν μπορεί να αμφισβητηθεί από το γεγονός οτι οι συμβατικές ρήτρες δεν δεσμεύουν την τρίτη χώρα, ωστόσο πρέπει να εξετάζεται εάν περιλαμβάνονται αποτελεσματικοί μηχανισμοί που εξασφαλίζουν ένα ισοδύναμο επίπεδο προστασίας όπως και η ύπαρξη της επιλογής της αναστολής της διαβίβασης δεδομένων σε περίπτωση παραβίασης ή μη εκπλήρωσης των συμβατικών υποχρεώσεων που απορρέουν από τις ρήτρες. Από την στιγμή που η εξεταζόμενη απόφαση επιβάλλει στον εξαγωγέα των δεδομένων και στον αποδέκτη των δεδομένων («εισαγωγέας δεδομένων») την υποχρέωση να ελέγχουν, πριν από κάθε διαβίβαση αν το συγκεκριμένο επίπεδο προστασίας τηρείται στην οικεία τρίτη χώρα, όπως επίσης και την υποχρέωση που έχει ο εισαγωγέας δεδομένων να ενημερώνει τον εξαγωγέα δεδομένων για κάθε αδυναμία συμμόρφωσης με τις τυποποιημένες ρήτρες προστασίας δεδομένων και, εν ανάγκη, με τυχόν πρόσθετα μέτρα εκτός εκείνων που παρέχει η εν λόγω ρήτρα, ο οποίος, με τη σειρά του, υποχρεούται να αναστείλει τη διαβίβαση των δεδομένων ή/και να

[64] Βλ. Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων, Συχνές ερωτήσεις σχετικά με την απόφαση του Δικαστηρίου της Ευρωπαϊκής Ένωσης στην υπόθεση C-311/18 - Επίτροπος προστασίας δεδομένων κατά Facebook Ireland Ltd και Maximillian Schrems, 23/07/2020, διαθέσιμο σε: https://edpb.europa.eu/sites/default/files/files/file1/20200724_edpb_faqoncjeuc31118_el.pdf

καταγγείλει τη σύμβαση με τον εισαγωγέα των δεδομένων, το δικαστήριο έκρινε ως έγκυρο το πλαίσιο διαβιβάσεων μέσω συμβατικών ρητρών.

Στην εξέταση του επιπέδου επάρκειας που διασφαλίζει ο μηχανισμός ΑΠΙΖ το ΔΕΕ έκρινε οτι η πρόσβαση στα διαβιβαζόμενα δεδομένα από τις υπηρεσίες πληροφοριών των ΗΠΑ, σύμφωνα με τις απαιτήσεις της αμερικανικής νομοθεσίας για λόγους εθνικής ασφάλειας, οδηγεί σε περιορισμό της προστασίας των δεδομένων. Επιπλέον δεν προβλέπονται εκτελεστά δικαιώματα που θα μπορούσαν να προβάλουν τα υποκείμενα των δεδομένων ενώπιον των αμερικανικών δικαστηρίων. Κατ' επέκταση των παραπάνω δεν δημιουργείται ένα ουσιαστικά ισοδύναμο πλαίσιο προστασίας και ως συνέπεια αυτού του βαθμού παρέμβασης στα θεμελιώδη δικαιώματα των προσώπων των οποίων τα δεδομένα διαβιβάζονται στις Ηνωμένες Πολιτείες Αμερικής, το ΔΕΕ κήρυξε την απόφαση επάρκειας 2016/1250 της Επιτροπής για την ασπίδα προστασίας της ιδιωτικής ζωής άκυρη.

Κεφάλαιο 2: Η διαβίβαση δεδομένων μετά την απόφαση Schrems II και οι SCC

2.1 Συνέπειες απόφασης Schrems II

Ενώ η απόφαση Schrems II ακύρωσε το Privacy Shield, εξακολουθούσε να αφήνει περιθώρια για διαβιβάσεις δεδομένων στις Ηνωμένες Πολιτείες με βάση SCC ή άλλους μηχανισμούς σύμφωνα με το άρθρο 46 του ΓΚΠΔ. Ακόμη και όταν η διαβίβαση δεδομένων βασιζόταν σε αυτούς τους μηχανισμούς, το ΔΕΕ εξήγησε ότι οι εξαγωγείς δεδομένων πρέπει να αναλύσουν το δίκαιο της χώρας εκτός ΕΕ και να υιοθετήσουν οποιαδήποτε «συμπληρωματικά μέτρα» είναι απαραίτητα για να διασφαλιστεί η επαρκής προστασία που απαιτείται από το δίκαιο της ΕΕ. Αν και η Schrems II δεν διευκρίνισε τι μορφές μπορούν να λάβουν τα «συμπληρωματικά μέτρα», στις 11 Νοεμβρίου 2020, το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων («EDPB») δημοσίευσε συστάσεις που απαριθμούν παραδείγματα μέτρων.

Αυτά περιλαμβάνουν κατά κύριο λόγο «τεχνικά μέτρα», όπως (1) ψευδωνυμοποίηση των δεδομένων, έτσι ώστε «να μην μπορούν πλέον να αποδοθούν σε ένα συγκεκριμένο θέμα», (2) η κρυπτογράφηση των δεδομένων με τέτοιο τρόπο ώστε ούτε ο παραλήπτης ούτε οι σχετικές δημόσιες αρχές να μπορούν να τα αποκρυπτογραφήσουν ή (3) να διαχωρίσουν τα δεδομένα μεταξύ δύο ή περισσότερων ανεξάρτητων υπευθύνων επεξεργασίας με διαφορετικές δικαιοδοσίες, έτσι ώστε κανένας μεμονωμένος εκτελών την επεξεργασία να μην μπορεί να «ανακατασκευάσει τα προσωπικά δεδομένα εν όλω ή εν μέρει».

Ωστόσο, σύμφωνα με το EDPB, υπάρχουν ορισμένα σενάρια όπου δεν μπορούν να βρεθούν «αποτελεσματικά» συμπληρωματικά μέτρα. Ειδικότερα, το EDPB επεσήμανε περιπτώσεις κατά τις οποίες ένας εξαγωγέας μεταφέρει δεδομένα σε «υπηρεσία cloud ή άλλον εκτελών την επεξεργασία» σε τρίτη χώρα που χρειάζεται πρόσβαση «σε καθαρά» δεδομένα (δηλαδή, μη κρυπτογραφημένα ή αμετάβλητα) για να εκτελέσει το έργο που του έχει ανατεθεί. Σε τέτοιες περιπτώσεις, το EDPB δήλωσε ότι «είναι ανίκανο να οραματιστεί ένα αποτελεσματικό τεχνικό μέτρο για να αποτρέψει την παραβίαση των δικαιωμάτων των υποκειμένων των δεδομένων από αυτού του είδους την πρόσβαση σε αυτά», δεδομένης της τρέχουσας κατάστασης της τεχνολογίας. Ωστόσο, δεν «απέκλεισε ότι η περαιτέρω τεχνολογική ανάπτυξη μπορεί

να προσφέρει μέτρα που επιτυγχάνουν τους επιδιωκόμενους επιχειρηματικούς σκοπούς, χωρίς να απαιτείται πρόσβαση σε «καθαρά» δεδομένα.

Ένα σημείο συζήτησης μετά την απόφαση Schrems II είναι εάν απαιτούνται πάντα συμπληρωματικά μέτρα πριν από τη μεταφορά δεδομένων που ενδέχεται να αποτελούν αντικείμενο επεξεργασίας από τις αμερικανικές υπηρεσίες πληροφοριών. Από την μια πλευρά, οι συστάσεις του EDPB υποδεικνύουν ότι σε τέτοιες περιπτώσεις απαιτούνται πάντα συμπληρωματικά μέτρα. Συγκεκριμένα, το EDPB αναφέρεται στην απόφαση Schrems II και στο γεγονός ότι «το επίπεδο προστασίας των προγραμμάτων που έχουν εγκριθεί από το νόμο FISA δεν είναι ουσιαστικά ισοδύναμο με τις διασφαλίσεις που απαιτούνται από τη νομοθεσία της ΕΕ». Κατά συνέπεια, «εάν τα δεδομένα εμπίπτουν στο νόμο FISA», τότε μπορεί να μεταφερθούν στις Ηνωμένες Πολιτείες μόνο εάν «πρόσθετα συμπληρωματικά τεχνικά μέτρα καθιστούν αδύνατη ή αναποτελεσματική την πρόσβαση στα δεδομένα που διαβιβάζονται». Αν και οι Συστάσεις του EDPB αναφέρουν μόνο το νόμο FISA, η λογική του ισχύει αναμφισβήτητα και για δεδομένα που υπόκεινται σε επιτήρηση στο πλαίσιο του ΕΟ 12333, το οποίο το ΔΕΕ θεώρησε επίσης προβληματικό. Από την άλλη πλευρά, η κυβέρνηση των ΗΠΑ δημοσίευσε μια Λευκή Βίβλο[65] μετά την απόφαση Schrems II που υιοθέτησε λιγότερο κατηγορηματική προσέγγιση από το EDPB. Η Λευκή Βίβλος υποστηρίζει ότι η Schrems II «δεν ήταν απόφαση σχετικά με το εάν η προστασία της ιδιωτικής ζωής στο αμερικανικό δίκαιο καθεαυτή είναι συνεπείς με το δίκαιο της ΕΕ». Αντίθετα, σύμφωνα με τη Λευκή Βίβλο, το ΔΕΕ «αποφάνθηκε μόνο για την εγκυρότητα» της απόφασης της Ασπίδας Προστασίας Ιδιωτικής Ζωής και η «αξιολόγηση της νομοθεσίας των ΗΠΑ κατά συνέπεια βασίστηκε κυρίως στα περιορισμένα ευρήματα σχετικά με τη νομοθεσία των ΗΠΑ που καταγράφηκαν από την Ευρωπαϊκή Επιτροπή το 2016 στο πλαίσιο της απόφασης επάρκειας για την διατλαντική μεταφορά δεδομένων. Στη συνέχεια, η Λευκή Βίβλος σκιαγραφεί πρόσθετες διασφαλίσεις και επιλογές επανόρθωσης στη νομοθεσία των ΗΠΑ που δεν περιλαμβάνονται στην απόφαση Schrems II, προκειμένου να βοηθηθούν οι εταιρείες να «προσδιορίσουν εάν η νομοθεσία των Ηνωμένων

[65] Βλ. Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II, White Paper, U.S. Department of Commerce, U.S. Department of Justice, Office of the Director of National Intelligence , Σεπτέμβριος 2020, διαθέσιμο σε: https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF

Πολιτειών διασφαλίζει επαρκή προστασία, όπως προβλέπεται από τη νομοθεσία της ΕΕ»[66].

2.2 Τυποποιημένες Συμβατικές Ρήτρες (SCC)

Όπως είδαμε παραπάνω η απόφαση Schrems II κατήργησε την ΑΠΙΖ, καθιστώντας επιτακτική πλέον την διαβίβαση δεδομένων προς τις ΗΠΑ με κάποιον από τους υπόλοιπους μηχανισμούς διαβίβασης που προβλέπονται στον ΓΚΠΔ, όπως είναι η διαβίβαση βάσει κατάλληλων εγγυήσεων, οι διαβιβάσεις μεταξύ δημόσιων αρχών, οι εγγυήσεις με μορφή συμβατικών ρητών, οι εγκεκριμένοι κώδικες δεοντολογίας, οι δεσμευτικοί εταιρικοί κανόνες κλπ.

Στην παρούσα εργασία θα αναφερθούμε μόνο στην διαβίβαση δεδομένων βάσει εγγυήσεων με την μορφή συμβατικών ρητρών, τις γνωστές Τυποποιημένες Συμβατικές Ρήτρες. Οι SCC δεν αποτελούν ένα νέο εργαλείο του ΓΚΠΔ για την διαβίβαση δεδομένων προς τρίτες χώρες, αλλά προϋπήρχαν και υπό την οδηγία 95/46/ΕΚ με τις αποφάσεις 2001/479/ΕΚ, 2004/915/ΕΚ και 2010/87/ΕΕ της Επιτροπής.

Προτού προχωρήσουμε όμως στην εκτελεστική απόφαση 2021/914 της Επιτροπής ("σχετικά με τις τυποποιημένες συμβατικές ρήτρες για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα προς τρίτες χώρες σύμφωνα με τον κανονισμό (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου") ας δούμε τί είναι οι SCC και ποια τα πλεονεκτήματα από την υιοθέτησή τους.

Οι τυποποιημένες συμβατικές ρήτρες ή άλλως πρότυπες συμβατικές ρήτρες (SCC) είναι τυποποιημένες και προεγκεκριμένες πρότυπες ρήτρες προστασίας δεδομένων που αποτελούν στην ουσία το παράρτημα σε μια σύμβαση DPA (Data Protection Agreement)[67] και δίνουν την δυνατότητα στους υπεύθυνους επεξεργασίας και τους εκτελούντες την επεξεργασία να συμμορφώνονται με τις υποχρεώσεις τους βάσει της νομοθεσίας της Ένωσης για την προστασία δεδομένων. Μπορούν να ενσωματωθούν από τους υπεύθυνους επεξεργασίας και τους εκτελούντες την επεξεργασία στις

[66] Βλ. Linebaugh Chris - Liu Edward, EU Data Transfer Requirements and U.S. Intelligence Laws: Understanding Schrems II and Its Impact on the EU-U.S. Privacy Shield, Congressional Research Service, σελ. 6

[67] Βλ. Λουκαΐτη Ναταλία, Διαβίβαση Προσωπικών Δεδομένων στο Περιβάλλον του Υπολογιστικού Νέφους (διπλωματική εργασία), Πανεπιστήμιο Πειραιώς, σελ. 21

συμβατικές τους ρυθμίσεις με άλλα μέρη, για παράδειγμα εμπορικούς εταίρους. Η χρήση των SCC δεν είναι υποχρεωτική και κατ' επέκταση οι ρήτρες μπορούν να χρησιμοποιηθούν σε εθελοντική βάση για να αποδειχθεί η συμμόρφωση με τις απαιτήσεις προστασίας δεδομένων, οπότε απαιτούν συμβατική δέσμευση για την τήρησή τους. Η Ευρωπαϊκή Επιτροπή έχει την εξουσία να εγκρίνει SCC για τη σχέση μεταξύ υπευθύνων και εκτελούντων την επεξεργασία και για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε χώρες εκτός του ΕΟΧ. Μέσω της τυποποίησης και της προέγκρισής τους, οι SCC είναι ένα «έτοιμο» και εύκολο στην εφαρμογή εργαλείο. Αυτό είναι ιδιαίτερα σημαντικό για τις μικρομεσαίες επιχειρήσεις ή άλλες εταιρείες που μπορεί να μην έχουν τους πόρους να διαπραγματεύονται μεμονωμένες συμβάσεις με κάθε έναν από τους εμπορικούς τους εταίρους, χωρίς αυτό να σημαίνει οτι εταιρικοί κολοσσοί όπως η Google, η Facebook, η Apple και η Microsoft δεν κάνουν χρήση αυτών[68]. Διακρίνονται επίσης οι SCC από άλλους μηχανισμούς συμμόρφωσης που απαιτούν προηγούμενη έγκριση από μια εθνική αρχή προστασία δεδομένων (π.χ. ad hoc συμβάσεις για μεταφορά δεδομένων) ή είναι συνήθως πιο δαπανηρή η εφαρμογή τους (π.χ συστήματα πιστοποίησης). Όσον αφορά τις SCC για τις διαβιβάσεις δεδομένων, η ανατροφοδότηση από τα ενδιαφερόμενα μέρη δείχνει ότι είναι κατά πολύ πιο χρησιμοποιούμενο μέσο μεταφοράς δεδομένων για ευρωπαϊκές εταιρείες. Για παράδειγμα, σύμφωνα με την IAPP - EY Annual Privacy Governance Report 2019, «τα πιο δημοφιλή από αυτά τα εργαλεία [μεταφοράς] – χρόνο με το χρόνο – είναι συντριπτικά οι τυποποιημένες συμβατικές συμβάσεις: το 88% των ερωτηθέντων στη φετινή έρευνα ανέφερε τις SCC ως την κορυφαία μέθοδο τους για εξωεδαφικές διαβιβάσεις δεδομένων[69]».

Στις 4 Ιουνίου 2021, δημοσιεύτηκε από την Επιτροπή το πολυαναμενόμενο νέο πακέτο τυποποιημένων συμβατικών ρητρών, γνωστών ως «SCCs». Μέσω του επικαιροποιημένου αυτού μηχανισμού διαβίβασης δεδομένων επιτρέπεται η διαβίβαση δεδομένων προσωπικού χαρακτήρα εκτός του Ευρωπαϊκού Οικονομικού

---

[68] Βλ. Παλιού Ε. Οι νέες τυποποιημένες συμβατικές ρήτρες της Ευρωπαϊκής Επιτροπής- Η διασυνοριακή διαβίβαση προσωπικών δεδομένων στον απόηχο της νομολογίας Schrems (αποφάσεις του ΔΕΕ υπ'αριθμ. C362/14 και C-311/18), ΔίΜΕΕ τ. 4/2021, σελ. 535

[69] Βλ. European Commission, New Standard Contractual Clauses - Questions and Answers overview, διαθέσιμο σε: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions-and-answers-overview_en

Χώρου (ΕΟΧ) και αντικαθιστά τις μέχρι σήμερα ισχύουσες Τυποποιημένες Συμβατικές Ρήτρες. Οι νέες ρήτρες λαμβάνουν υπόψη την απόφαση Schrems II του ΔΕΕ που ακύρωσε την ΑΠΙΖ για τη διαβίβαση δεδομένων μεταξύ ΕΕ. και ΗΠΑ και απαιτούν από τους «εξαγωγείς» και «εισαγωγείς» προσωπικών δεδομένων να λαμβάνουν μέτρα για να διασφαλίζουν την αποτελεσματική συμμόρφωση με τις απαιτήσεις προστασίας των προσωπικών δεδομένων, όπως αποτυπώνονται σε αυτές. Είναι σημαντικό ότι οι νέες ρήτρες επιτρέπουν μια προσέγγιση με βάση τον κίνδυνο στις εκτιμήσεις επιπτώσεων της μεταφοράς δεδομένων κατά την αξιολόγηση του επιπέδου προστασίας που θα παρέχεται στα μεταφερόμενα δεδομένα. Επιπλέον, με τις νέες τυποποιημένες συμβατικές ρήτρες γίνεται προσπάθεια αντιμετώπισης προβλημάτων που διαπιστώθηκαν κατά την τελευταία δεκαετία, όπως η ανάγκη κάλυψης περισσότερων περιπτώσεων διαβίβασης δεδομένων (από Εκτελούντα σε Εκτελούντα, από Εκτελούντα εντός ΕΟΧ σε Υπεύθυνο εκτός ΕΟΧ) στο πλαίσιο του ίδιου συνόλου ρητρών και μεγαλύτερης ευελιξίας όσον αφορά την προσθήκη ή την απόσυρση συμβαλλομένων μερών σε υφιστάμενες συμφωνίες[70].

Οι νεωτερισμοί των ανανεωμένων SCC θα μπορούσαν να συνοψιστούν στους εξής[71]:

Πρώτον, η "αρχιτεκτονική" των SCC έχει ενημερωθεί, για παράδειγμα:

Οι τυποποιημένες συμβατικές ρήτρες καλύπτουν πρόσθετα σενάρια διαβίβασης: ενώ το πεδίο εφαρμογής των προηγούμενων τυποποιημένων συμβατικών ρητρών περιοριζόταν στις διαβιβάσεις δεδομένων από τους υπευθύνους επεξεργασίας στους υπευθύνους επεξεργασίας και από τους υπευθύνους επεξεργασίας στους εκτελούντες την επεξεργασία, οι εκσυγχρονισμένες μπορούν να χρησιμοποιηθούν σε όλες από τις πιο σχετικές περιπτώσεις: από υπεύθυνο επεξεργασίας σε υπεύθυνο επεξεργασίας, από υπεύθυνο επεξεργασίας σε εκτελούντα την επεξεργασία, από εκτελούντα την επεξεργασία σε εκτελούντα την επεξεργασία, και εκτελών την επεξεργασία σε υπεύθυνο επεξεργασίας.

---

[70] Βλ. Κωνσταντίνου Στέργιος, Τυποποιημένες Συμβατικές Ρήτρες (SCCs) και επόμενα βήματα, 14/06/2021, διαθέσιμο σε: https://www.lawspot.gr/nomika-blogs/stergios_konstantinoy/typopoiimenes-symvatikes-ritres-sccs-kai-epomena-vimata

[71] Βλ. European Commission, New Standard Contractual Clauses - Questions and Answers overview, διαθέσιμο σε: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions-and-answers-overview_en

Τρία ξεχωριστά σύνολα SCC που κάλυπταν δύο σενάρια μεταφοράς έχουν αντικατασταθεί από ένα σύνολο SCC με αρθρωτή δομή (που καλύπτει τέσσερα σενάρια μεταφοράς). Τα μέρη πρέπει να συνδυάζουν γενικές ρήτρες (που ισχύουν ανεξάρτητα από το συγκεκριμένο σενάριο μεταφοράς) με την ενότητα ή τις ενότητες που ισχύουν για την περίπτωσή τους.

Μια ρήτρα σύνδεσης επιτρέπει πλέον στα νέα μέρη να συμμετέχουν στις SCC καθ' όλη τη διάρκεια του κύκλου ζωής της σύμβασης.

Οι τυποποιημένες συμβατικές ρήτρες συμπληρώνονται από παραρτήματα στα οποία πρέπει να παρέχονται συγκεκριμένες πληροφορίες σχετικά με τις συγκεκριμένες διαβιβάσεις, για παράδειγμα κατάλογος των μερών και των αντίστοιχων ρόλων τους, περιγραφή των σκοπών κάθε μεμονωμένης διαβίβασης που πρόκειται να πραγματοποιηθεί στο πλαίσιο της συμφωνίας, κατάλογος των μέτρων ασφαλείας που εφαρμόζονται, των διασφαλίσεων που εφαρμόζονται για την προστασία των ευαίσθητων δεδομένων, κλπ.

Δεύτερον, εισήχθησαν ορισμένες ουσιαστικές αλλαγές, για παράδειγμα:

Οι τυποποιημένες συμβατικές ρήτρες αντικατοπτρίζουν τις νέες απαιτήσεις του ΓΚΠΔ, συμπεριλαμβανομένων ενισχυμένων υποχρεώσεων διαφάνειας και λεπτομερέστερων ρητρών σχετικά με τα δικαιώματα των υποκειμένων των δεδομένων, την κοινοποίηση παραβίασης δεδομένων και τους κανόνες για περαιτέρω διαβιβάσεις.

Για μεταφορές δεδομένων από υπεύθυνους επεξεργασίας σε εκτελούντες την επεξεργασία ή εκτελούντες την επεξεργασία σε υπεργολάβους επεξεργασίας, οι απαιτήσεις του άρθρου 28 του ΓΚΠΔ έχουν ενσωματωθεί στις SCC. Ως εκ τούτου, οι εταιρείες δεν χρειάζεται να υπογράψουν ξεχωριστή σύμβαση για να συμμορφωθούν με το άρθρο 28 του GDPR.

Ρήτρες εφαρμογής της απόφασης Schrems II του Δικαστηρίου της ΕΕ: τα μέρη των SCC πρέπει τώρα να διενεργούν «εκτίμηση επιπτώσεων διαβίβασης» που να τεκμηριώνει τις ειδικές συνθήκες της διαβίβασής τους, τη νομοθεσία της χώρας προορισμού και τις πρόσθετες διασφαλίσεις που εφαρμόζουν για την προστασία των δεδομένων προσωπικού χαρακτήρα.

Νέες υποχρεώσεις σε περίπτωση πρόσβασης των δημόσιων αρχών στα διαβιβαζόμενα δεδομένα, π.χ. υποχρέωση παροχής πληροφοριών στους εξαγωγείς δεδομένων και αμφισβήτησης παράνομων αιτημάτων.

Ωστόσο δεν έλειψε και ο αντίλογος ως προς τις παραπάνω καινοτομίες των νέων ΤΣΡ, καθώς στο περιεχόμενο αυτών εντοπίζονται ορισμένες αντιφάσεις[72].

Αρχικά, όσον αφορά τον εισαγωγέα δεδομένων, όπως προβλέπεται στην παράγραφο 1 του άρθρου 1, όπως και στην Αιτιολογική Σκέψη 7 της εκτελεστικής απόφασης της Επιτροπής για τις τυποποιημένες συμβατικές ρήτρες, οι νέες ρήτρες θεωρούνται κατάλληλες εγγυήσεις, σύμφωνα με τον ΓΚΠΔ, μόνο στην περίπτωση που λαμβάνει χώρα διαβίβαση δεδομένων σε εισαγωγέα εγκατεστημένο εκτός της Ένωσης που δεν εμπίπτει στο εδαφικό πεδίο εφαρμογής του Κανονισμού σύμφωνα με το άρθρο 3. Άρα στην περίπτωση που ο εισαγωγέας δεδομένων με εγκατάσταση εκτός της Ένωσης εμπίπτει στο εδαφικό πεδίο εφαρμογής του Κανονισμού, οι νέες τυποποιημένες συμβατικές ρήτρες δεν μπορούν να νομιμοποιήσουν την διαβίβαση δεδομένων προς αυτόν. Ωστόσο το παραπάνω έρχεται σε αντίθεση με την θέση του ΕΣΠΔ, σύμφωνα με την οποία το ουσιαστικό ζήτημα είναι η εγκατάσταση του εισαγωγέα δεδομένων σε τρίτη χώρα ανεξαρτήτως της κάλυψης ή μη αυτού από τον ΓΚΠΔ.

Επιπροσθέτως στην απόφαση της Επιτροπής για τις νέες τυποποιημένες συμβατικές ρήτρες δεν γίνεται κάποια αναφορά στα μέτρα που θα πρέπει να λαμβάνονται από την πλευρά των εξαγωγέων και των εισαγωγέων των δεδομένων έτσι ώστε να εξασφαλίζεται ένα ουσιαστικά ισοδύναμο επίπεδο προστασίας. Γίνεται αναφορά μόνο στο οτι τα μέρη θα πρέπει να εξετάζουν το ενδεχόμενο προσφυγής σε μέσα όπως η κρυπτογράφηση ή ψευδωνυμοποίηση όταν αυτό είναι δυνατό και δεν κωλύει την επίτευξη του σκοπού της επεξεργασίας. Εξαιτίας των παραπάνω, οι απόφαση για τις ΤΣΡ θα πρέπει να διαβάζεται και να εφαρμόζεται σε συνδυασμό με τις Συστάσεις 01/2020 και 02/2020 του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων (ΕΣΠΔ) για περαιτέρω σαφήνεια. Και αυτό επειδή, οι συγκεκριμένες συστάσεις του ΕΣΠΔ προσφέρουν έναν μη εξαντλητικό κατάλογο παραγόντων για τον προσδιορισμό των

[72] Βλ. Στραγαλινός Αιμίλιος - Αρτέμιος, Το ισχύον πλαίσιο για τις διαβιβάσεις δεδομένων σε τρίτες χώρες υπό το φως των αποφάσεων του Δικαστηρίου της Ευρωπαϊκής Ένωσης στην υπόθεση Schrems (διπλωματική εργασία), Πανεπιστήμιο Πειραιώς, σελ. 76 επ.

μέτρων που θα ήταν πιο αποτελεσματικά για την προστασία των διαβιβαζόμενων δεδομένων από τις αιτήσεις πρόσβασης των δημόσιων αρχών, συμπεριλαμβανομένου του μορφότυπου των προς διαβίβαση δεδομένων (δηλαδή σε απλό κείμενο, ψευδωνυμοποιημένα ή κρυπτογραφημένα), της φύσης των δεδομένων, της διάρκειας και της πολυπλοκότητας της διαβίβασης, του αριθμού των φορέων που εμπλέκονται στην επεξεργασία και της μεταξύ τους σχέσης, των παραμέτρων της πρακτικής εφαρμογής του δικαίου της τρίτης χώρας και της πιθανότητας τα δεδομένα να αποτελέσουν αντικείμενο περαιτέρω διαβίβασης.

Εν τέλει, φτάνουμε στο συμπέρασμα οτι η πολυπλοκότητα και το υψηλό κόστος της διαδικασίας αξιολόγησης του επιπέδου προστασίας που προσφέρει η νομοθεσία μιας τρίτης χώρας στα διαβιβαζόμενα δεδομένα, μπορεί δυνητικά να λειτουργήσει ως τροχοπέδη για τις μικρομεσαίες επιχειρήσεις, οι οποίες δεν έχουν την ικανότητα να ανταπεξέλθουν τόσο οικονομικά, όσο και πρακτικά, σε σύγκριση με τις μεγάλες επιχειρήσεις, κάτι που μπορεί να τις απωθήσει από την υιοθέτηση τυποποιημένων συμβατικών ρητών.

Συμπεράσματα

Α) Σχετικά με την δυνατότητα ανάπτυξης πλαισίου διατλαντικής διαβίβασης δεδομένων[73]

Κατανοώντας όσα ελέχθησαν στα προηγούμενα κεφάλαια μπορούμε να πούμε οτι οποιαδήποτε ομοσπονδιακή ή πολιτειακή νομοθεσία των ΗΠΑ είναι απίθανο να παρέχει «ουσιαστικά ισοδύναμη » προστασία σε σύγκριση με τον GDPR της ΕΕ στο άμεσο μέλλον. Πράγματι, υπάρχουν σοβαρά και στην πράξη ανυπέρβλητα συνταγματικά και θεσμικά καθώς και πολιτικά εμπόδια για την υιοθέτηση τέτοιων νόμων.

Ωστόσο, τα παραπάνω εμπόδια θα μπορούσαν να ξεπεραστούν εάν (i) οι ΗΠΑ και η ΕΕ επρόκειτο να λάβουν νομοθετικά μέτρα σχετικά με την ουσία, την επιβολή και τα ατομικά δικαιώματα και εάν (ii) οι ΗΠΑ επρόκειτο να μεταρρυθμίσουν τους νόμους και τις πρακτικές παρακολουθήσεων. Στη συνέχεια θα μπορούσε να επιτευχθεί νέα συμφωνία ΕΕ - ΗΠΑ για αυτοπιστοποίηση από οντότητες των ΗΠΑ, βάσει της οποίας η ΕΕ θα μπορούσε να εκδώσει μια νέα θετική απόφαση επάρκειας για τις ΗΠΑ, περιορισμένη στα προσωπικά δεδομένα που διαβιβάζονται από την ΕΕ σε οντότητες που είχαν αυτοπιστοποιήσει την εκούσια συμμόρφωσή τους με τα ουσιαστικά πρότυπα της ΕΕ, όπως αναφέρονται στον GDPR.

Δεν μιλάμε για αναβίωση του καταστροφικού και αβάσιμου Safe Harbour/Privacy Shield, αλλά για ένα θεμελιωδώς διαφορετικό, βελτιωμένο σύστημα αυτοπιστοποίησης, με την ίδια την αυτοπιστοποίηση να σχετίζεται με το σύνολο του GDPR (αντί για μια αποδυναμωμένη αντανάκλαση του κανονισμού σε αδιαπέραστες συλλογές εγγράφων) και πολύ ισχυρότερη επιβολή από την FTC (η οποία θα πρέπει να λάβει πολύ ευρύτερες εξουσίες για τον σκοπό αυτό).

Επιπλέον, ακόμη και το καλύτερο σύστημα που βασίζεται στην αυτοπιστοποίηση δεν μπορεί να ξεπεράσει τις ελλείψεις στα νομικά καθεστώτα των ΗΠΑ για την

---

[73] Βλ. Brown Ian - Korff Douwe, Exchanges of personal data after the Schrems II judgment, σελ. 113 επ., διαθέσιμο σε: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/694678/IPOL_STU(2021)694678_EN.pdf

πρόσβαση σε δεδομένα που μεταφέρονται από την ΕΕ στις ΗΠΑ (ή στα οποία έχουν άμεση πρόσβαση οι υπηρεσίες πληροφοριών των ΗΠΑ). Οποιαδήποτε λύση πρέπει να περιλαμβάνει και τα δύο στοιχεία: παροχή «επάρκειας»/«ουσιαστικής ισοδυναμίας» (μέσω ενός συστήματος ενισχυμένης αυτοπιστοποίησης με ενισχυμένη επιβολή) και θεμελιώδεις μεταρρυθμίσεις στους νόμους περί επιτήρησης των ΗΠΑ.

Πιο αναλυτικά θα μπορούσαμε να αναφέρουμε τους παρακάτω τρόπους για την άμβλυνση των διαφορών που έχουν προκύψει[74]:

1) Επίτευξη γενικού ρυθμού επάρκειας στο θέμα της αδικαιολόγητης πρόσβασης: Η ΕΕ και οι ΗΠΑ θα πρέπει να ξεκινήσουν συζητήσεις για τη δημιουργία ενός πολύ διευρυμένου και ενισχυμένου συστήματος αυτοπιστοποίησης για τις αμερικανικές εταιρείες. Ωστόσο, οποιοδήποτε τέτοιο νέο σύστημα αυτοπιστοποίησης θα πρέπει να ισχύει για όλες τις ουσιαστικές απαιτήσεις του GDPR της ΕΕ. Η FTC θα πρέπει να λάβει ευρύτερες και ισχυρότερες εξουσίες και στα υποκείμενα των δεδομένων της ΕΕ θα πρέπει να παραχωρούνται δικαιώματα (μέσω ένδικων μέσων) σε περίπτωση που προκύπτουν παραβάσεις του συστήματος.

2) Για την αντιμετώπιση του ζητήματος της αδικαιολόγητης πρόσβασης σε δεδομένα από τις υπηρεσίες πληροφοριών των ΗΠΑ: Οι ΗΠΑ θα πρέπει να κληθούν να μεταρρυθμίσουν επειγόντως την ομοσπονδιακή νομοθεσία επιτήρησης. Αυτό θα πρέπει να περιλαμβάνει τον περιορισμό της μαζικής συλλογής. Περιορισμός του ορισμού των πληροφοριών ξένων μυστικών υπηρεσιών και καθορισμός ισχυρότερων προτύπων για την αιτιολόγηση των στόχων επιτήρησης, μείωση της προεπιλεγμένης περιόδου διατήρησης των συλλεγόμενων πληροφοριών από πέντε χρόνια σε τρία, αύξηση της διαφάνειας σχετικά με τις δραστηριότητες επιτήρησης και παροχή στα υποκείμενα των δεδομένων της ΕΕ «ενός αποτελεσματικού ένδικου μέσου ενώπιον ενός ανεξάρτητου και αμερόληπτου δικαστηρίου».

3) Η εποπτεία εν γένει υπό το κράτος δικαίου: Τα θεσμικά όργανα της ΕΕ και ειδικότερα το Ευρωπαϊκό Κοινοβούλιο θα πρέπει να υπερασπιστούν το κράτος δικαίου και να απαιτήσουν τόσο από τα κράτη μέλη όσο και από τρίτες χώρες να ευθυγραμμίσουν πλήρως τις πρακτικές πληροφοριών και τα εθνικά νομοθετικά τους πλαίσια με το διεθνές δίκαιο των ανθρωπίνων δικαιωμάτων.

---

[74] Βλ. Brown Ian - Korff Douwe, όπ. ανωτ. (υποσ. 74)

4) Ενίσχυση αντιπροσωπευτικών/συλλογικών αγωγών στην ΕΕ: Η ΕΕ θα πρέπει να δώσει στις ΗΠΑ την δυνατότητα εισαγωγή μιας ομαδικής προσφυγής για οποιονδήποτε υπέστη υλική ή ηθική βλάβη ως αποτέλεσμα παραβίασης (όποια και αν είναι η εθνικότητα, το καθεστώς ή ο τόπος διαμονής τους).

Συνολικά, καταλήγουμε στο συμπέρασμα ότι εάν εφαρμοστούν οι παραπάνω τέσσερις συστάσεις, οι διαβιβάσεις προσωπικών δεδομένων από την ΕΕ στις ΗΠΑ θα μπορούσαν και πάλι να διευκολυνθούν στο πλαίσιο του νέου συστήματος αυτοπιστοποίησης, με μια νέα απόφαση επάρκειας που θα εκδοθεί από την Επιτροπή της ΕΕ και που δεν θα ακυρωθεί από το ΔΕΕ.

Μέχρι να επιτευχθεί αυτό, οι διαβιβάσεις προσωπικών δεδομένων από την ΕΕ στις ΗΠΑ πρέπει να βασίζονται σε «κατάλληλες διασφαλίσεις», συμπεριλαμβανομένων των τυπικών συμβατικών ρητρών (SCC) και των Δεσμευτικών Εταιρικών Κανόνων (BCR), ή σε εύθετο χρόνο εγκεκριμένους κώδικες συμπεριφοράς ή πιστοποιήσεις κλπ σε συνδυασμό με «συμπληρωματικά μέτρα», όπως ισχυρή κρυπτογράφηση για την προστασία των μεταφερόμενων δεδομένων από αδικαιολόγητη πρόσβαση από τις υπηρεσίες πληροφοριών των ΗΠΑ. Και δεν έχουν ακόμη εντοπιστεί αποτελεσματικά συμπληρωματικά μέτρα που θα μπορούσαν να προστατεύσουν από μια τέτοια αδικαιολόγητη πρόσβαση, εάν τα δεδομένα πρέπει να είναι ξεκάθαρα προσβάσιμα στον εισαγωγέα δεδομένων στις ΗΠΑ. Ορισμένα μέτρα, όπως έλεγχοι, αρχεία καταγραφής και μηχανισμοί αναφοράς θα μπορούσαν ενδεχομένως να χρησιμοποιηθούν σε ορισμένα τέτοια πλαίσια (ιδίως, όπου τα δεδομένα δεν είναι σαφώς καθόλου ευαίσθητα και απίθανο να ενδιαφέρουν τις υπηρεσίες πληροφοριών των ΗΠΑ) . Αλλά για ευαίσθητα δεδομένα με την ευρεία έννοια (ευαίσθητα δεδομένα με την επίσημη έννοια του GDPR και άλλα, γενικότερα ευαίσθητα δεδομένα, όπως δεδομένα επικοινωνιών, οικονομικά δεδομένα και δεδομένα ταξιδιού), αυτά γενικά δεν αρκούν.

Β) EU-US Data Privacy Framework

1 Τα πρώτα βήματα για την δημιουργία του νέου πλαισίου και η υπογραφή του Εκτελεστικού Διατάγματος

Στις 25 Μαρτίου 2022 η Ευρωπαϊκή Επιτροπή και οι Ηνωμένες Πολιτείες ανακοίνωσαν ότι συμφώνησαν επί της αρχής στο νέο πλαίσιο διατλαντικής

διαβίβασης δεδομένων, το οποίο θα ενισχύσει τις ροές δεδομένων και θα αντιμετωπίσει τις ανησυχίες που εξέφρασε το Δικαστήριο της Ευρωπαϊκής Ένωσης στην απόφαση Schrems II του Ιουλίου 2020. Σύμφωνα με το Trans-Atlantic Data Privacy Framework, οι Ηνωμένες Πολιτείες πρόκειται να θέσουν σε εφαρμογή νέες διασφαλίσεις για να διασφαλιστεί ότι οι δραστηριότητες επιτήρησης είναι απαραίτητες και αναλογικές στην επιδίωξη καθορισμένων στόχων εθνικής ασφάλειας, δημιουργία ενός ανεξάρτητου μηχανισμού προσφυγής σε δύο επίπεδα με δεσμευτική εξουσία να κατευθύνει διορθωτικά μέτρα και να ενισχύσει την αυστηρή και πολυεπίπεδη εποπτεία. Το νέο πλαίσιο θα προωθήσει μια ψηφιακή οικονομία χωρίς αποκλεισμούς στην οποία μπορούν να συμμετέχουν όλοι οι άνθρωποι και στην οποία εταιρείες όλων των μεγεθών από όλες τις χώρες θα μπορούν να ευδοκιμήσουν[75].

Σύμφωνα με τις βασικές αρχές της συμφωνίας, διασφαλίζεται η ελεύθερη και ασφαλής κυκλοφορία των προσωπικών δεδομένων ανάμεσα στην ΕΕ και στις συμμετέχουσες στη συμφωνία αμερικανικές εταιρείες. Ο στόχος της περιορισμένης πρόσβασης στα δεδομένα προσωπικού χαρακτήρα που έχουν διαβιβαστεί στις ΗΠΑ από τις υπηρεσίες πληροφοριών εκπληρώνεται μέσω μίας νέας δέσμης μέτρων και δεσμευτικών εγγυήσεων. Ωστόσο, ο περιορισμός στην πρόσβαση ισχύει μόνο στο βαθμό που η πρόσβαση είναι αναγκαία και πρόσφορη για την προστασία της εθνικής ασφάλειας. Οι υπηρεσίες πληροφοριών θα εξαναγκαστούν να υιοθετήσουν διαδικασίες οι οποίες θα συμμορφώνονται με τα ευρωπαϊκά πρότυπα προστασίας της ιδιωτικότητας και των ατομικών ελευθεριών. Περαιτέρω, ιδρύεται ένας νέος μηχανισμός επανόρθωσης δύο επιπέδων, με επιστέγασμα τη σύσταση νέας ειδικής ανεξάρτητης αρχής, η οποία θα προσομοιάζει σε Δικαστήριο Προσωπικών Δεδομένων, ώστε να μπορούν να προσφεύγουν σε αυτό τα υποκείμενα των δεδομένων, εφόσον θεωρούν ότι τα δεδομένα τους υφίστανται παράνομες δραστηριότητες επεξεργασίας από τις μυστικές υπηρεσίες των ΗΠΑ. Θεσπίζονται σημαντικές υποχρεώσεις για τις εταιρείες που επεξεργάζονται εισαγόμενα δεδομένα που διαβιβάζονται από την ΕΕ, και συνεχίζει να ισχύει η υποχρέωση

[75] Βλ. European Commission - Press release, European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework, 25/03/2022, διαθέσιμο σε: https://ec.europa.eu/commission/presscorner/detail/nl/ip_22_2087

αυτοπιστοποίησης, πάντα φυσικά σε συμμόρφωση με τις επιταγές του Υπουργείου Εμπορίου. Προβλέπεται επίσης μηχανισμός ελέγχου και αναθεώρησης[76].

Σε συνέχεια της πολιτικής συμφωνίας της 25ης Μαρτίου 2022, ο Πρόεδρος Biden υπέγραψε στις 7 Οκτωβρίου 2022 εκτελεστικό διάταγμα αναφορικά με την ενίσχυση των διασφαλίσεων για τις δραστηριότητες των ΗΠΑ σχετικά με την συλλογή πληροφοριών μέσω σημάτων. Το εκτελεστικό διάταγμα απαιτεί από τις αρχές πληροφοριών των ΗΠΑ να αναθεωρήσουν τις πολιτικές και τις πρακτικές τους έτσι ώστε να υλοποιούν τις παρακάτω διασφαλίσεις[77]:

Η πρόσβαση σε προσωπικά δεδομένα από τις υπηρεσίες πληροφοριών των ΗΠΑ θα διεξάγονται μόνο όταν είναι απαραίτητο για την προώθηση μιας επιβεβαιωμένης προτεραιότητας και μόνο στο βαθμό και με τρόπο ανάλογο με αυτήν την προτεραιότητα. Περαιτέρω, ακόμη και στην περίπτωση πρόσβασης σε δεδομένα για την επιδίωξη καθορισμένων στόχων εθνικής ασφάλειας θα πρέπει να λαμβάνεται υπόψη τόσο η ιδιωτική ζωή, όσο και οι πολιτικές ελευθερίες όλων των προσώπων ανεξαρτήτως εθνικότητας και χώρας διαμονής.

Οι υπηρεσιών πληροφοριών των ΗΠΑ υποχρεούνται να ενημερώσουν τις πολιτικές και τις διαδικασίες τους ώστε να αντικατοπτρίζουν τις νέες διασφαλίσεις για το απόρρητο και τις πολιτικές ελευθερίες

Δημιουργείται ένας πολυεπίπεδος μηχανισμός για άτομα από πολιτείες που πληρούν τις προϋποθέσεις και περιφερειακούς οργανισμούς, προκειμένου να έχουν πρόσβαση σε ανεξάρτητη εξέταση και αποκατάσταση των ισχυρισμών τους σε περιπτώσεις που τα προσωπικά τους στοιχεία συλλέχθηκαν κατά παραβίαση της ισχύουσας νομοθεσίας των ΗΠΑ.

---

[76] Βλ. Λουκαΐτη Ναταλία, Διαβίβαση Προσωπικών Δεδομένων στο Περιβάλλον του Υπολογιστικού Νέφους (διπλωματική εργασία), Πανεπιστήμιο Πειραιώς, σελ. 34

[77] Βλ. Lawspot, Διαβίβαση δεδομένων μεταξύ ΕΕ και ΗΠΑ: Υπεγράφη το Διάταγμα για την εφαρμογή του νέου πλαισίου από τον Πρόεδρο Μπάιντεν, 7/10/2022, διαθέσιμο σε: https://www.lawspot.gr/nomika-nea/diavivasidedomenon-metaxy-ee-kai-ipa-ypegrafi-diatagma-gia-tin-efarmogi-toy neoy?fbclid=IwAR2ii1ww64MnUZJ23QHLLXiR2mSu44Ul7SAcL7NXd7kBvAqyTCzDJojL4rs

Ο νέος μηχανισμός αντιμετώπισης καταγγελιών διαρθρώνεται σε δύο επίπεδα[78]. Στο πρώτο επίπεδο, οι πολίτες της ΕΕ θα μπορούν να υποβάλουν καταγγελία στο λεγόμενο «Πολιτικό Υπεύθυνο Προστασίας των Ελευθεριών» της κοινότητας πληροφοριών των ΗΠΑ. Αυτό το άτομο είναι υπεύθυνο για τη διασφάλιση συμμόρφωση των υπηρεσιών πληροφοριών των ΗΠΑ με το απόρρητο και τα θεμελιώδη δικαιώματα. Στο δεύτερο επίπεδο, τα άτομα θα έχουν τη δυνατότητα να ασκήσουν έφεση κατά της απόφασης του «Πολιτικού Υπεύθυνου Προστασίας των Ελευθεριών» ενώπιον του νεοσύστατου Δικαστηρίου Αναθεώρησης Προστασίας Δεδομένων. Το Δικαστήριο θα αποτελείται από μέλη που επιλέγονται εκτός της κυβέρνησης των ΗΠΑ, που διορίζονται βάσει ειδικών προσόντων, μπορούν να απολυθούν μόνο για σοβαρούς λόγους (όπως η καταδίκη για έγκλημα ή κρίνεται διανοητικά ή σωματικά ανίκανος να εκτελέσει τις εργασίες) και δεν μπορούν να λάβουν οδηγίες από τη κυβέρνηση. Το Δικαστήριο Αναθεώρησης Προστασίας Δεδομένων θα έχει εξουσίες να διερευνά καταγγελίες από πολίτες της ΕΕ, συμπεριλαμβανομένης της λήψης σχετικών πληροφοριών από τις υπηρεσίες πληροφοριών, και θα μπορεί να λαμβάνει δεσμευτικές διορθωτικές αποφάσεις. Για παράδειγμα, εάν το δικαστήριο διαπιστώσει ότι τα δεδομένα συλλέχθηκαν σε παραβίαση των διασφαλίσεων που προβλέπονται στο εκτελεστικό διάταγμα, θα μπορεί να διατάξει τη διαγραφή των δεδομένων.

Για περαιτέρω ενίσχυση του ελέγχου του δικαστηρίου, σε κάθε περίπτωση, το δικαστήριο θα επιλέγει έναν ειδικό δικηγόρο με σχετική πείρα για την υποστήριξη του δικαστηρίου, το οποίο θα διασφαλίσει ότι τα συμφέροντα του καταγγέλλοντα εκπροσωπούνται ενώπιον του δικαστηρίου και ότι το δικαστήριο είναι καλά ενημερωμένο για τις πραγματικές και νομικές πτυχές της υπόθεσης. Αυτό θα διασφαλίσει την εκπροσώπηση και των δύο πλευρών και θα εισαγάγει περισσότερες εγγυήσεις όσον αφορά τους όρους δίκαιης δίκης, επανόρθωσης και δίκαιης διαδικασίας.

[78] Βλ. European Commission, Questions & Answers: EU-US Data Privacy Framework, 7/10/2022, διαθέσιμο σε: https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_6045

2 Η δημοσίευση του προσχεδίου απόφασης επάρκειας από την Επιτροπή

Στις 13 Δεκεμβρίου 2022 η Επιτροπή εξέδωσε ανακοίνωση με την οποία γνωστοποιούσε την δημοσίευση του προσχεδίου[79] της επερχόμενης απόφασης επάρκειας για την διαβίβαση δεδομένων μεταξύ ΕΕ και ΗΠΑ. Σύμφωνα με την παραπάνω ανακοίνωση[80] οι αμερικανικές εταιρείες θα μπορούν να ενταχθούν στο νέο πλαίσιο διαβίβασης δεδομένων με τη δέσμευση για συμμόρφωση με ένα λεπτομερές σύνολο υποχρεώσεων απορρήτου, για παράδειγμα, την απαίτηση διαγραφής προσωπικών δεδομένων όταν δεν είναι πλέον απαραίτητα για τον σκοπό για τον οποίο συλλέχθηκαν και για τη διασφάλιση της συνέχειας της προστασίας όταν κοινοποιούνται προσωπικά δεδομένα σε τρίτους. Οι πολίτες της ΕΕ θα επωφεληθούν από διάφορες οδούς προσφυγής εάν τα προσωπικά τους δεδομένα υποβάλλονται σε επεξεργασία κατά παράβαση του Πλαισίου, μεταξύ άλλων δωρεάν ενώπιον ανεξάρτητων μηχανισμών επίλυσης διαφορών και ειδικής ομάδας διαιτησίας. Επιπλέον, το νομικό πλαίσιο των ΗΠΑ προβλέπει ορισμένους περιορισμούς και διασφαλίσεις σχετικά με την πρόσβαση σε δεδομένα από τις δημόσιες αρχές των ΗΠΑ, ιδίως για σκοπούς επιβολής του ποινικού νόμου και εθνικής ασφάλειας. Αυτό περιλαμβάνει τους νέους κανόνες που εισήγαγε το εκτελεστικό διάταγμα των ΗΠΑ, το οποίο αντιμετώπιζε τα ζητήματα που έθεσε το Δικαστήριο της ΕΕ στην απόφαση Schrems II:

> Η πρόσβαση σε ευρωπαϊκά δεδομένα από τις υπηρεσίες πληροφοριών των ΗΠΑ θα περιοριστεί σε ό,τι είναι απαραίτητο και αναλογικό για την προστασία της εθνικής ασφάλειας.
>
> Τα άτομα της ΕΕ θα έχουν τη δυνατότητα να ζητήσουν ένδικα μέσα σχετικά με τη συλλογή και τη χρήση των δεδομένων τους από τις υπηρεσίες πληροφοριών των ΗΠΑ ενώπιον ενός ανεξάρτητου και αμερόληπτου μηχανισμού προσφυγής, ο οποίος περιλαμβάνει ένα νεοσύστατο Δικαστήριο Αναθεώρησης Προστασίας

[79] Βλ. Ευρωπαϊκή Επιτροπή, Προσχέδιο εκτελεστικής απόφασης σύμφωνα με τον κανονισμό (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το επαρκές επίπεδο προστασίας των προσωπικών δεδομένων βάσει του EU-US Data Privacy Framework, διαθέσιμο σε: https://commission.europa.eu/system/files/2022-12/Draft_adequacy_decision_on_EU-US_Data_Privacy_Framework_0.pdf

[80] Βλ. European Commission - Press release, Data protection: Commission starts process to adopt adequacy decision for safe data flows with the US, 13/12/2022, διαθέσιμο σε: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7631

Δεδομένων. Το Δικαστήριο θα ερευνά και θα επιλύει ανεξάρτητα καταγγελίες από Ευρωπαίους, με την υιοθέτηση δεσμευτικών διορθωτικών μέτρων.

Τέλος, οι ευρωπαϊκές εταιρείες θα μπορούν να βασίζονται σε αυτές τις διασφαλίσεις για τις διατλαντικές μεταφορές δεδομένων, ακόμα και όταν χρησιμοποιούν άλλους μηχανισμούς μεταφοράς, όπως τυπικές συμβατικές ρήτρες και δεσμευτικούς εταιρικούς κανόνες.

3 Οι αρχές του νέου πλαισίου διατλαντικών διαβιβάσεων[81]

Ειδοποίηση: Κάθε εταιρεία θα πρέπει να ενημερώνει τα άτομα σχετικά με: α) τη συμμετοχή του στο νέο πλαίσιο και να παρέχει σύνδεσμο προς ή τη διεύθυνση ιστού για τη λίστα του Υπουργείου Εμπορίου, β) τα είδη των προσωπικών δεδομένων που συλλέγονται και τις οντότητες ή τις θυγατρικές του οργανισμού που τηρεί επίσης τις Αρχές, γ) τη δέσμευσή της να υπόκειται στις Αρχές όλα τα προσωπικά δεδομένα που λαμβάνονται από την ΕΕ, δ) τους σκοπούς για τους οποίους συλλέγει και χρησιμοποιεί προσωπικές πληροφορίες, ε) πώς να επικοινωνήσετε με την εταιρεία για τυχόν απορίες ή παράπονα, συμπεριλαμβανομένης οποιασδήποτε σχετικής εγκατάστασης στην ΕΕ που μπορεί να απαντήσει σε τέτοιες έρευνες ή παράπονα, στ) το είδος ή την ταυτότητα τρίτων στους οποίους αποκαλύπτει προσωπικές πληροφορίες και τους σκοπούς για τους οποίους το κάνει, ζ) το δικαίωμα των ατόμων να έχουν πρόσβαση στα προσωπικά τους δεδομένα, η) τις επιλογές και τα μέσα που προσφέρει η εταιρεία στα άτομα για τον περιορισμό της χρήσης και της αποκάλυψης των προσωπικών δεδομένων τους, θ) το ανεξάρτητο όργανο επίλυσης διαφορών που έχει οριστεί για την αντιμετώπιση καταγγελιών και την παροχή των κατάλληλων προσφυγών δωρεάν στο άτομο, και αν είναι: (1) η επιτροπή που έχει συσταθεί από τις ΑΠΔ, (2) ένας εναλλακτικός πάροχος επίλυσης διαφορών με έδρα την ΕΕ ή (3) ένας εναλλακτικός πάροχος επίλυσης διαφορών με έδρα τις Ηνωμένες Πολιτείες, ι) υπόκεινται σε αρμοδιότητες έρευνας και επιβολής της Επιτροπής Εμπορίου, του Υπουργείου Μεταφορών ή οποιασδήποτε άλλης αρχής, κ) η δυνατότητα, υπό προϋποθέσεις, για το άτομο να επικαλεστεί δεσμευτική διαιτησία, λ) την απαίτηση αποκάλυψης προσωπικών πληροφοριών σε ανταπόκριση σε νόμιμα αιτήματα

[81] Βλ. Παράρτημα 1 - Μέρος ΙΙ Προσχεδίου Απόφασης Επάρκειας

δημοσίων αρχών, συμπεριλαμβανομένων της εθνικής ασφάλειας, μ) την ευθύνη σε περιπτώσεις περαιτέρω μεταβιβάσεων σε τρίτους.

Η ειδοποίηση πρέπει να παρέχεται σε σαφή και καταφανή γλώσσα όταν τα άτομα καλούνται πρώτη φορά να παράσχουν προσωπικές πληροφορίες στην εκάστοτε εταιρεία ή το συντομότερο εφικτό, αλλά σε κάθε περίπτωση προτού η εταιρεία χρησιμοποιήσει αυτές τις πληροφορίες για άλλο σκοπό εκτός από αυτό για τον οποίο είχαν αρχικά συλλεχθεί ή υποβληθεί σε επεξεργασία.

Επιλογή: Κάθε εταιρεία θα πρέπει να προσφέρει στα άτομα την ευκαιρία να επιλέξουν εάν τα προσωπικά τους στοιχεία α) πρόκειται να γνωστοποιηθούν σε τρίτο μέρος ή β) να χρησιμοποιηθούν για ουσιωδώς διαφορετικό σκοπό από τον σκοπό για τον οποίο συλλέχθηκαν αρχικά ή στη συνέχεια εξουσιοδοτήθηκαν από τα άτομα. Τα άτομα πρέπει να έχουν πρόσβαση σε σαφείς, εμφανείς και άμεσα διαθέσιμους μηχανισμούς για να ασκήσουν την επιλογή τους.

Λογοδοσία για μελλοντική μεταφορά: Για να μεταφερθούν προσωπικά δεδομένα σε τρίτο μέρος που ενεργεί ως αντιπρόσωπος, κάθε εταιρεία θα πρέπει: α) να μεταφέρει δεδομένα μόνο για περιορισμένους και καθορισμένους σκοπούς, β) εξακριβώσει ότι ο πράκτορας είναι υποχρεωμένος να παρέχει τουλάχιστον το ίδιο επίπεδο προστασίας που απαιτείται από τις Αρχές, γ) να λάβει εύλογα και κατάλληλα μέτρα για να εξασφαλίσει ότι ο αντιπρόσωπος επεξεργάζεται αποτελεσματικά τις προσωπικές πληροφορίες που μεταφέρονται με τρόπο συνεπή με τις υποχρεώσεις της εταιρείας σύμφωνα με τις Αρχές, δ) απαιτεί από τον πράκτορα να ειδοποιήσει την εταιρεία εάν λάβει απόφαση ότι δεν μπορεί πλέον να ανταποκριθεί στην υποχρέωσή του να παρέχει το ίδιο επίπεδο προστασία όπως απαιτείται από τις Αρχές, ε) κατόπιν ειδοποίησης να λάβει εύλογα και κατάλληλα μέτρα για να σταματήσει και να αποκαταστήσει μη εξουσιοδοτημένη επεξεργασία και στ) παρέχει μια περίληψη ή αντιπροσωπευτικό αντίγραφο των σχετικών διατάξεων περί απορρήτου της σύμβασής του με αυτόν τον πράκτορα στο Υπουργείο κατόπιν αιτήματος.

Ασφάλεια: Οι εταιρείες που δημιουργούν, διατηρούν, χρησιμοποιούν ή διαδίδουν προσωπικές πληροφορίες πρέπει να λαμβάνουν εύλογα και κατάλληλα μέτρα για την προστασία από απώλεια, κακή χρήση και μη εξουσιοδοτημένη πρόσβαση, αποκάλυψη, τροποποίηση και καταστροφή, λαμβάνοντας δεόντως υπόψη τους κινδύνους που ενέχονται στην επεξεργασία και τη φύση των προσωπικών δεδομένων.

Ακεραιότητα δεδομένων και περιορισμός σκοπού: Σύμφωνα με τις Αρχές, τα προσωπικά στοιχεία πρέπει να περιορίζονται στις πληροφορίες που είναι σχετικές για τους σκοπούς της επεξεργασίας. Κάθε εταιρεία μπορεί να μην επεξεργάζεται προσωπικές πληροφορίες με τρόπο τέτοιο που είναι ασυμβίβαστος με τους σκοπούς για τους οποίους είχαν συλλεχθεί ή εξουσιοδοτηθεί στη συνέχεια από το άτομο. Στο βαθμό που απαιτείται για αυτούς τους λόγους, κάθε εταιρεία πρέπει να λάβει εύλογα μέτρα για να εξασφαλίσει ότι τα προσωπικά δεδομένα είναι αξιόπιστα για τη χρήση για την οποία προορίζονται, ακριβή, πλήρη, και τρέχοντα. Κάθε εταιρεία πρέπει να τηρεί τις Αρχές για όσο διάστημα διατηρεί τέτοιες πληροφορίες.

Οι πληροφορίες μπορούν να διατηρηθούν σε μορφή που ταυτοποιεί ή καθιστά ταυτοποιήσιμο το άτομο μόνο για όσο διάστημα εξυπηρετεί έναν σκοπό επεξεργασίας μέσα στην έννοια της προηγούμενης παραγράφου. Αυτή η υποχρέωση δεν εμποδίζει τις εταιρείες να επεξεργάζονται προσωπικές πληροφορίες για μεγαλύτερα χρονικά διαστήματα για το χρόνο και στο βαθμό που αυτή η επεξεργασία εξυπηρετεί εύλογα τους σκοπούς της αρχειοθέτησης για το δημόσιο συμφέρον, δημοσιογραφία, λογοτεχνία και τέχνη, επιστημονική ή ιστορική έρευνα και στατιστική ανάλυση. Σε αυτές τις περιπτώσεις, η επεξεργασία αυτή θα γίνεται με την επιφύλαξη των λοιπών αρχών και διατάξεων του νέου πλαισίου.

Πρόσβαση: Τα άτομα πρέπει να έχουν πρόσβαση σε δικές τους προσωπικές πληροφορίες που μια εταιρεία διατηρεί και να μπορούν να τις διορθώσουν, να τις τροποποιήσουν ή να τις διαγράψουν εάν είναι ανακριβείς ή έχουν υποστεί επεξεργασία κατά παράβαση των Αρχών, εκτός εάν το βάρος ή το κόστος παροχής πρόσβαση θα ήταν δυσανάλογο σε σχέση με τους κινδύνους για την προστασία της ιδιωτικής ζωής του ατόμου στην εν λόγω περίπτωση ή όταν τα δικαιώματα άλλων προσώπων πέραν του ατόμου θα παραβιάζονταν.

Προσφυγή, επιβολή, ευθύνη: Η αποτελεσματική προστασία της ιδιωτικής ζωής πρέπει να περιλαμβάνει ισχυρούς μηχανισμούς που θα διασφαλίζουν τη συμμόρφωση με τις Αρχές, την προσφυγή για άτομα που επηρεάζονται από τη μη συμμόρφωση με τις Αρχές και τις συνέπειες για τον οργανισμό όταν δεν τηρούνται οι Αρχές.

Όταν μια εταιρεία υπόκειται σε δικαστική απόφαση που βασίζεται σε μη συμμόρφωση ή εντολή από θεσμικό φορέα των ΗΠΑ που βασίζεται και πάλι σε μη συμμόρφωση, η εταιρεία θα πρέπει να δημοσιοποιεί οποιαδήποτε έκθεσης

συμμόρφωσης ή αξιολόγησης αναφορικά με το νέο πλαίσιο που υποβάλλεται στο δικαστήριο ή στον ανάλογο θεσμικό φορέα στο βαθμό που συνάδει με τις απαιτήσεις εμπιστευτικότητας.

4 Ο τρόπος λειτουργίας του νέου πλαισίου

Όπως διαπιστώσαμε και παραπάνω, το νέο πλαίσιο βασίζεται σε ένα σύστημα πιστοποίησης με το οποίο οι αμερικανικές εταιρείες δεσμεύονται σε ένα σύνολο αρχών απορρήτου, συμπεριλαμβανομένων των Συμπληρωματικών Αρχών που εκδόθηκαν από το Υπουργείο Εμπορίου των ΗΠΑ. Για να είναι επιλέξιμη μια εταιρεία για πιστοποίηση θα πρέπει να υπόκειται στις εξουσίες διερεύνησης και επιβολής της Ομοσπονδιακής Επιτροπής Εμπορίου (FTC) ή του Υπουργείου Μεταφορών των ΗΠΑ (DoT). Οι αρχές ισχύουν αμέσως μετά την πιστοποίηση και οι εταιρείες υποχρεούνται να πιστοποιούνται εκ νέου σε ετήσια βάση[82].

Πιο αναλυτικά, για να πιστοποιηθεί μια εταιρεία θα πρέπει δημοσίως να δηλώσει την δέσμευσή της στην τήρηση των Αρχών, να κάνει διαθέσιμες τις πολιτικές απορρήτου που χρησιμοποιεί και να τις εφαρμόσει πλήρως[83]. Σε αυτή την διαδικασία το Υπουργείο Εμπορίου θα ελέγχει εάν οι εταιρείες πληρούν τα κριτήρια πιστοποίησης[84] και θα τις ενημερώνει οτι θα πρέπει να επιλύουν τυχών ζητήματα που προκύπτουν κατά τον έλεγχο[85]. Οι εταιρείες στην συνέχεια θα μπορούν να λαμβάνουν προσωπικά δεδομένα βασισμένες στο νέο πλαίσιο από την ημέρα που θα αναγράφονται στην αντίστοιχη λίστα του Υπουργείου Εμπορίου[86].

Επιπλέον το Υπουργείο Εμπορίου θα παρακολουθεί σε συνεχή βάση την αποτελεσματική εφαρμογή των αρχών από τις πιστοποιημένες εταιρείες δια μέσω διαφόρων μηχανισμών[87], όπως επίσης θα παρακολουθεί για τυχόν ψευδείς

[82] Βλ. Αιτιολογική Σκέψη 9 Προσχεδίου Απόφασης Επάρκειας

[83] Βλ. Αιτιολογική Σκέψη 48 Προσχεδίου Απόφασης Επάρκειας

[84] Βλ. Αιτιολογική Σκέψη 50 Προσχεδίου Απόφασης Επάρκειας

[85] Βλ. Αιτιολογική Σκέψη 51 Προσχεδίου Απόφασης Επάρκειας

[86] Βλ. Αιτιολογική Σκέψη 49 Προσχεδίου Απόφασης Επάρκειας

[87] Βλ. Αιτιολογική Σκέψη 53 Προσχεδίου Απόφασης Επάρκειας

ισχυρισμούς συμμετοχής ή λάθος χρήσης του σήματος πιστοποίησης είτε αυτεπαγγέλτως, είτε μετά από καταγγελία[88].

Ωστόσο τον μεγαλύτερο ρόλο στον τομέα επίβλεψης της ορθής εφαρμογής του πλαισίου διαβίβασης δεδομένων κατέχει η Ομοσπονδιακή Επιτροπή Εμπορίου μαζί με το Υπουργείο Μεταφορών.

Η Ομοσπονδιακή Επιτροπή Εμπορίου μπορεί να διερευνήσει τη συμμόρφωση με τις Αρχές, καθώς και ψευδείς ισχυρισμούς τήρησης των Αρχών ή συμμετοχή στο νέο πλαίσιο από εταιρείες που είτε δεν βρίσκονται πλέον στη λίστα του Υπουργείου Εμπορίου είτε δεν έχουν πιστοποιηθεί ποτέ. Η επιτροπή μπορεί να επιβάλλει τη συμμόρφωση ζητώντας διοικητικές ή ομοσπονδιακές δικαστικές αποφάσεις (συμπεριλαμβανομένων «εντολών συναίνεσης» που επιτυγχάνονται μέσω διακανονισμών) για προκαταρκτικές ή μόνιμες διαταγές ή άλλα ένδικα μέσα και θα παρακολουθεί συστηματικά τη συμμόρφωση με τέτοιες εντολές. Σε περίπτωση που οι εταιρείες δεν συμμορφωθούν με τέτοιες εντολές, η επιτροπή μπορεί να ζητήσει αστικές κυρώσεις και άλλα ένδικα μέσα. Τέλος, η επιτροπή θα διατηρεί μια ηλεκτρονική λίστα εταιρειών που υπόκεινται σε διαταγές από την ίδια ή από δικαστήριο[89].

Το Υπουργείο Μεταφορών από την άλλη πλευρά έχει την αποκλειστική εξουσία να ρυθμίζει τις πρακτικές απορρήτου των αεροπορικών εταιρειών και έχει κοινή δικαιοδοσία με την Ομοσπονδιακή Επιτροπή Εμπορίου όσον αφορά τις πρακτικές απορρήτου των πρακτόρων εισιτηρίων στην πώληση αεροπορικών μεταφορών. Οι αξιωματούχοι του Υπουργείου στοχεύουν πρώτα στην επίτευξη συμφωνίας και, εάν αυτό δεν είναι δυνατό, μπορεί να εκκινήσουν εκτελεστικές διαδικασίες που περιλαμβάνουν ακρόαση ενώπιον δικαστή διοικητικού δικαίου του Υπουργείου που έχει την εξουσία να εκδίδει παύση και να σταματήσει τις εντολές και τις αστικές κυρώσεις. Το υπουργείο δεσμεύεται να παρακολουθεί τις εκτελεστές αποφάσεις και να διασφαλίζει ότι οι εντολές που προκύπτουν είναι διαθέσιμες στην ιστοσελίδα του[90].

---

[88] Βλ. Αιτιολογική Σκέψη 56 Προσχεδίου Απόφασης Επάρκειας

[89] Βλ. Αιτιολογική Σκέψη 61 Προσχεδίου Απόφασης Επάρκειας

[90] Βλ. Αιτιολογική Σκέψη 63 Προσχεδίου Απόφασης Επάρκειας

Ως προς την προστασία των υποκειμένων των δεδομένων,

α) Τα υποκείμενα των δεδομένων θα μπορούν να καταγγέλλουν υποθέσεις μη εφαρμογής των αρχών μέσω απευθείας επικοινωνίας με την αντίστοιχη εταιρεία[91],

β) τα άτομα μπορούν επίσης να υποβάλουν καταγγελία απευθείας σε ανεξάρτητο φορέα επίλυσης διαφορών (είτε στις Ηνωμένες Πολιτείες είτε στην Ένωση) που ορίζεται από έναν οργανισμός για τη διερεύνηση και την επίλυση μεμονωμένων καταγγελιών (εκτός εάν είναι προφανώς αβάσιμες ή επιπόλαιες) και να παρέχει την κατάλληλη προσφυγή δωρεάν[92],

γ) τα άτομα μπορούν να καταθέτουν τις καταγγελίες τους σε μια εθνική αρχή προστασίας δεδομένων[93],

δ) Το Υπουργείο Εμπορίου έχει δεσμευτεί να λάβει, να επανεξετάσει και να καταβάλει κάθε δυνατή προσπάθεια επίλυσης παραπόνων σχετικά με τη μη συμμόρφωση μίας εταιρείας με τις αρχές[94],

ε) κάθε εταιρεία πρέπει να υπόκειται στη δικαιοδοσία των αμερικανικών αρχών, ιδίως της Ομοσπονδιακής Επιτροπής Εμπορίου[95],

στ) ως μηχανισμός προσφυγής «έσχατης ανάγκης» σε περίπτωση που δεν έχει επιλυθεί ικανοποιητικά από τα άλλα διαθέσιμα εργαλεία καταγγελία ενός ατόμου, το υποκείμενο των δεδομένων μπορεί να επικαλεστεί δεσμευτική διαιτησία[96],

ζ) όταν μια εταιρεία δεν συμμορφώνεται με τη δέσμευσή του να σέβεται τις αρχές και τη δημοσιευμένη πολιτική απορρήτου, πρόσθετες οδοί για δικαστική αποκατάσταση είναι διαθέσιμοι βάσει της νομοθεσίας των ΗΠΑ, συμπεριλαμβανομένης της λήψης αποζημίωσης για ζημίες[97].

---

[91] Βλ. Αιτιολογική Σκέψη 68 Προσχεδίου Απόφασης Επάρκειας

[92] Βλ. Αιτιολογική Σκέψη 69 Προσχεδίου Απόφασης Επάρκειας

[93] Βλ. Αιτιολογική Σκέψη 72 Προσχεδίου Απόφασης Επάρκειας

[94] Βλ. Αιτιολογική Σκέψη 77 Προσχεδίου Απόφασης Επάρκειας

[95] Βλ. Αιτιολογική Σκέψη 79 Προσχεδίου Απόφασης Επάρκειας

[96] Βλ. Αιτιολογική Σκέψη 80 Προσχεδίου Απόφασης Επάρκειας

[97] Βλ. Αιτιολογική Σκέψη 85 Προσχεδίου Απόφασης Επάρκειας

5 Η συμμόρφωση του νέου πλαισίου με τις αποφάσεις Schrem και η πρόσβαση στα δεδομένα από τις υπηρεσίες πληροφοριών των ΗΠΑ

5.1 Πρόσβαση στα δεδομένα για λόγους ποινικού δικαίου

Η πρόσβαση σε δεδομένα υποκειμένων που έχουν μεταβιβαστεί στις ΗΠΑ για λόγους ποινικού δικαίου μπορεί να γίνει: α) κατόπιν αιτήματος ομοσπονδιακού αξιωματικού επιβολής του νόμου ή δικηγόρου για τη κυβέρνηση ή ενός δικαστής που μπορεί να εκδώσει ένταλμα για έρευνα ή κατάσχεση (συμπεριλαμβανομένων των ηλεκτρονικά αποθηκευμένων πληροφοριών). Ένα τέτοιο ένταλμα μπορεί να εκδοθεί μόνο εάν υπάρχει «πιθανή αιτία» ότι «κατασχεθέντα αντικείμενα» (στοιχεία εγκλήματος, κατεχόμενα παράνομα αντικείμενα ή περιουσιακά στοιχεία που έχουν σχεδιαστεί ή προορίζονται για χρήση ή που χρησιμοποιούνται για τη διάπραξη εγκλήματος) είναι πιθανόν να βρεθούν στον τόπο που καθορίζεται από το ένταλμα. Το ένταλμα πρέπει να προσδιορίζει τη περιουσία ή τα αντικείμενα προς κατάσχεση και να ορίζει τον δικαστή στον οποίο πρέπει να αποδοθεί το ένταλμα. Ένα άτομο που υποβάλλεται σε έρευνα ή του οποίου η περιουσία υπόκειται σε έρευνα μπορεί να ζητήσει την καταστολή αποδεικτικών στοιχείων που αποκτήθηκαν ή προέρχονται από παράνομη έρευνα, εάν αυτά προσκομίζονται αποδεικτικά στοιχεία εναντίον αυτού του ατόμου κατά τη διάρκεια ποινικής δίκης. Όταν ένας κάτοχος δεδομένων (π.χ. μια εταιρεία) υποχρεούται να αποκαλύψει δεδομένα σύμφωνα με ένα ένταλμα, μπορεί παραλείπει την απαίτηση γνωστοποίησης ως αδικαιολόγητα επαχθής[98]. β) μια κλήτευση μπορεί να εκδοθεί από το σώμα ενόρκων στο πλαίσιο ερευνών για ορισμένα σοβαρά εγκλήματα, συνήθως κατόπιν αιτήματος ομοσπονδιακού εισαγγελέα, να απαιτηθεί από κάποιον να προσκομίσει ή να καταστήσει διαθέσιμα επαγγελματικά αρχεία, ηλεκτρονικά αποθηκευμένες πληροφορίες ή άλλα απτά στοιχεία. Επιπλέον, διαφορετικά καταστατικά επιτρέπουν τη χρήση διοικητικών κλητεύσεων για να καθιστούν διαθέσιμα επαγγελματικά αρχεία, ηλεκτρονικά αποθηκευμένες πληροφορίες ή άλλα απτά στοιχεία σε έρευνες που αφορούν απάτες υγειονομικής περίθαλψης, κακοποίηση παιδιών, μυστικές υπηρεσίες προστασίας, υποθέσεις ελεγχόμενων ουσιών και έρευνες Γενικού Επιθεωρητή. Και στις δύο υποθέσεις, οι πληροφορίες πρέπει να είναι σχετικές με την έρευνα και η κλήτευση δεν μπορεί να

[98] Βλ. Αιτιολογική Σκέψη 90 Προσχεδίου Απόφασης Επάρκειας

είναι παράλογη, δηλ. υπερβολική, καταπιεστική ή επαχθής[99]. γ) πολλές νομικές βάσεις επιτρέπουν στις αρχές επιβολής του ποινικού νόμου να αποκτήσουν πρόσβαση σε δεδομένα επικοινωνιών. Το δικαστήριο μπορεί να εκδώσει διάταγμα που επιτρέπει την συλλογή σε πραγματικό χρόνο πληροφοριών (για κλήσεις, δρομολόγηση, διεύθυνση και σηματοδότηση ενός αριθμού τηλεφώνου ή ηλεκτρονικού ταχυδρομείου), εάν διαπιστώσει ότι η αρχή έχει πιστοποιήσει ότι οι πληροφορίες που ενδέχεται να ληφθούν είναι σχετικές με εκκρεμή ποινική έρευνα. Η παραγγελία πρέπει, μεταξύ άλλων, να προσδιορίζει τη ταυτότητα, εάν είναι γνωστή, του υπόπτου, τα χαρακτηριστικά των επικοινωνιών στις οποίες ισχύει και δήλωση του αδικήματος στο οποίο σχετίζονται οι πληροφορίες που θα συλλεχθούν. Η χρήση καταγραφέα στυλό ή συσκευής παγίδευσης και ανίχνευσης μπορεί να επιτρέπεται για μέγιστη περίοδο εξήντα ημερών, η οποία μπορεί να παραταθεί μόνο με νέα δικαστική απόφαση[100]. δ) τέλος μπορεί να ζητηθεί πρόσβαση σε πληροφορίες συνδρομητών, δεδομένα κίνησης και αποθηκευμένο περιεχόμενο επικοινωνιών που κατέχονται από παρόχους υπηρεσιών διαδικτύου, τηλεφωνικές εταιρείες και άλλους τρίτους παρόχους υπηρεσιών βάση του νόμου περί αποθηκευμένων επικοινωνιών[101]. Σε αυτή την περίπτωση οι πάροχοι που λαμβάνουν το αίτημα μπορούν οικειοθελώς να ειδοποιήσουν τον πελάτη ή συνδρομητή του οποίου οι πληροφορίες ζητούνται, εκτός και εάν έχει απαγορευτεί η γνωστοποίηση από την αρχή επιβολής του νόμου[102].

Φυσικά οι παραπάνω δραστηριότητες βρίσκονται υπό την εποπτεία διαφορετικών οργάνων (υπεύθυνοι προστασίας ιδιωτικότητας και ελευθεριών, Γενικός Επιθεωρητής, επιτροπές του Κογκρέσου).

Οι υπεύθυνοι προστασίας ιδιωτικότητας και ελευθεριών υπάρχουν σε διάφορα τμήματα με ευθύνη επιβολής του ποινικού νόμου. Ενώ οι αρμοδιότητες αυτών των υπαλλήλων μπορεί να διαφέρουν κάπως ανάλογα με το καταστατικό εξουσιοδότησης, συνήθως περιλαμβάνουν την εποπτεία των διαδικασιών για να διασφαλιστεί οτι το αντίστοιχο τμήμα/υπηρεσία εξετάζει επαρκώς τα ζητήματα που αφορούν το απόρρητο και τις ελευθερίες και έχει θέσει σε εφαρμογή επαρκείς διαδικασίες για την

[99] Βλ. Αιτιολογική Σκέψη 91 Προσχεδίου Απόφασης Επάρκειας

[100] Βλ. Αιτιολογική Σκέψη 92 Προσχεδίου Απόφασης Επάρκειας

[101] Βλ. Αιτιολογική Σκέψη 93 Προσχεδίου Απόφασης Επάρκειας

[102] Βλ. Αιτιολογική Σκέψη 94 Προσχεδίου Απόφασης Επάρκειας

αντιμετώπιση καταγγελιών από άτομα που θεωρούν ότι έχει παραβιαστεί το απόρρητο ή οι ελευθερίες τους. Οι επικεφαλής κάθε υπουργείου ή υπηρεσίας πρέπει να διασφαλίζουν ότι οι υπεύθυνοι προστασίας ιδιωτικότητας και ελευθεριών έχουν τα υλικά και τους πόρους για την εκπλήρωση της εντολής τους, έχουν πρόσβαση σε οποιοδήποτε υλικό και προσωπικό που είναι απαραίτητο για την εκτέλεση των καθηκόντων τους[103].

Ένας ανεξάρτητος Γενικός Επιθεωρητής επιβλέπει τις δραστηριότητες του Υπουργείο Δικαιοσύνης, συμπεριλαμβανομένου του FBI. Οι Γενικοί Επιθεωρητές είναι εκ του νόμου ανεξάρτητοι και υπεύθυνοι για τη διεξαγωγή ανεξάρτητων ερευνών, ελέγχων και επιθεωρήσεων των προγραμμάτων και των λειτουργιών του υπουργείου. Έχουν πρόσβαση σε όλα τα αρχεία, εκθέσεις, ελέγχους, επισκοπήσεις, έγγραφα, συστάσεις ή άλλο σχετικό υλικό, εάν χρειαστεί με κλήτευση, και μπορεί να λάβουν μαρτυρία. Ενώ οι Γενικοί Επιθεωρητές εκδίδουν μη δεσμευτικές συστάσεις για διορθωτικές ενέργειες, οι εκθέσεις τους, συμπεριλαμβανομένων των δράσεων παρακολούθησης γενικά δημοσιοποιούνται και αποστέλλονται στο Κογκρέσο, το οποίο μπορεί σε αυτή τη βάση να ασκήσει την εποπτική του λειτουργία[104].

5.2 Πρόσβαση στα δεδομένα για λόγους εθνικής ασφάλειας

Οι υπηρεσίες πληροφοριών των ΗΠΑ ενδέχεται να ζητήσουν πρόσβαση σε προσωπικά δεδομένα τα οποία έχουν διαβιβαστεί σε εταιρείες που βρίσκονται στις Ηνωμένες Πολιτείες μόνο για λόγους εθνικής ασφάλειας με εξουσιοδότηση υπό τον νόμο FISA ή και με νομοθετικές διατάξεις που επιτρέπουν την πρόσβαση μέσω Εθνικών Γραμμάτων Ασφαλείας (NSL)[105].

Οι υπηρεσίες πληροφοριών των ΗΠΑ έχουν επίσης δυνατότητα συλλογής προσωπικών δεδομένων εκτός των Ηνωμένων Πολιτειών, οι οποία ενδέχεται να περιλαμβάνει δεδομένα προσωπικού χαρακτήρα κατά τη διαβίβασή τους μεταξύ ΕΕ - ΗΠΑ. Η συλλογή αυτή βασίζεται στο ΕΟ 12333[106].

---

[103] Βλ. Αιτιολογική Σκέψη 104 Προσχεδίου Απόφασης Επάρκειας

[104] Βλ. Αιτιολογική Σκέψη 105 Προσχεδίου Απόφασης Επάρκειας

[105] Βλ. Αιτιολογική Σκέψη 115 Προσχεδίου Απόφασης Επάρκειας

[106] Βλ. Αιτιολογική Σκέψη 117 Προσχεδίου Απόφασης Επάρκειας

Φυσικά ο χαρακτήρας των παραπάνω δραστηριοτήτων και η απαίτηση συμμόρφωσης με τους κανόνες της ΕΕ για την προστασία δεδομένων, οδήγησαν στην πρόβλεψη ορισμένων περιορισμών και ασφαλιστικών δικλίδων. Πρώτον, τέτοιες δραστηριότητες πρέπει να βασίζονται σε νόμο ή προεδρική εξουσιοδότηση και διενεργούνται σύμφωνα με τη νομοθεσία των ΗΠΑ, συμπεριλαμβανομένου του Συντάγματος[107]. Δεύτερον, πρέπει να υπάρχουν κατάλληλες διασφαλίσεις για να διασφαλιστεί ότι το απόρρητο και οι ελευθερίες αποτελούν αναπόσπαστο στοιχείο στο σχεδιασμό τέτοιων δραστηριοτήτων[108]. Ειδικότερα, οποιαδήποτε δραστηριότητα συλλογής πληροφοριών μπορεί να πραγματοποιηθεί μόνο «μετά από προσδιορισμό, με βάση μια λογική εκτίμηση όλων των σχετικών παραγόντων, ότι οι δραστηριότητες είναι απαραίτητες για την προώθηση μιας επικυρωμένης προτεραιότητας πληροφοριών»[109]. Επιπλέον, τέτοιες δραστηριότητες μπορούν να διεξάγονται μόνο «στο βαθμό και με τρόπο που είναι ανάλογες με την επικυρωμένη προτεραιότητα πληροφοριών για την οποία έχει υπάρξει εξουσιοδότηση". Με άλλα λόγια, πρέπει να επιτευχθεί μια σωστή ισορροπία «μεταξύ της σημασίας της επιδιωκόμενης προτεραιότητας πληροφοριών και τον αντίκτυπο στην ιδιωτική ζωή και τις ελευθερίες των θιγόμενων ατόμων, ανεξάρτητα από την εθνικότητά τους ή τον τόπο κατοικία τους"[110]. Τέλος, για να διασφαλιστεί η συμμόρφωση με αυτές τις γενικές απαιτήσεις, οι οποίες αντικατοπτρίζουν τις αρχές της νομιμότητας, της αναγκαιότητας και της αναλογικότητας, οι παραπάνω δραστηριότητες υπόκεινται σε επίβλεψη[111].

Όπως και στην περίπτωση πρόσβασης σε δεδομένα για λόγους εφαρμογής του ποινικού δικαίου, έτσι και στην περίπτωση πρόσβασης για λόγους εθνικής ασφάλειας οι υπηρεσίες πληροφοριών εποπτεύονται μέσω των υπεύθυνων προστασίας ιδιωτικότητας και ελευθεριών, του Γενικού Επιθεωρητή και διαφόρων επιτροπών του Κογκρέσου.

Πέραν των παραπάνω έχουμε το Συμβούλιο Εποπτείας Πληροφοριών (IOB) που εντάσσεται στο Συμβουλευτικό Συμβούλιο Πληροφοριών του Προέδρου (PIAB), και

[107] Βλ. Αιτιολογική Σκέψη 122 Προσχεδίου Απόφασης Επάρκειας

[108] Βλ. Αιτιολογική Σκέψη 123 Προσχεδίου Απόφασης Επάρκειας

[109] Βλ. Αιτιολογική Σκέψη 124 Προσχεδίου Απόφασης Επάρκειας

[110] Βλ. Αιτιολογική Σκέψη 125 Προσχεδίου Απόφασης Επάρκειας

[111] Βλ. Αιτιολογική Σκέψη 126 Προσχεδίου Απόφασης Επάρκειας

εποπτεύει την συμμόρφωση των αμερικανικών υπηρεσιών πληροφοριών με το Σύνταγμα και όλους τους εφαρμοζόμενους νόμους. Το συμβούλιο υποχρεούται να ενημερώνει τον Πρόεδρο σχετικά με δραστηριότητες συλλογής πληροφοριών στις οποίες πιστεύει ότι μπορεί να υπάρχει παραβίαση του νόμου και δεν γίνονται επαρκώς από τον Υπουργό Δικαιοσύνης, τον Διευθυντή Εθνικών Πληροφοριών ή τον επικεφαλής μιας υπηρεσίας πληροφοριών[112].

Επιπλέον, οι υπηρεσίες πληροφοριών υπόκεινται σε εποπτεία από το Συμβούλιο Εποπτείας Απορρήτου και Ελευθεριών (PCLOB), μια ανεξάρτητη υπηρεσία εντός της εκτελεστικής εξουσίας που αποτελείται από ένα δικομματικό, πενταμελές συμβούλιο που διορίζεται από τον Πρόεδρο για ορισμένη εξαετή θητεία με έγκριση της Γερουσίας. Σύμφωνα με το ιδρυτικό καταστατικό, του ανατίθενται αρμοδιότητες στο πλαίσιο αντιτρομοκρατικών πολιτικών και την εφαρμογή τους, με σκοπό την προστασία της ιδιωτική ζωή και τις ελευθερίες. Κατά την επισκόπηση των ενεργειών των υπηρεσιών πληροφοριών, μπορεί να έχει πρόσβαση σε όλα τα αρχεία, τις εκθέσεις, τους ελέγχους, τις επιθεωρήσεις, τα έγγραφα, και τις συστάσεις (συμπεριλαμβανομένων απορρήτων πληροφοριών) διεξαγωγή συνεντεύξεων και ακρόαση μαρτύρων. Λαμβάνει αναφορές από τους Υπευθύνους Προστασίας Ιδιωτικότητας και Ελευθεριών αρκετών ομοσπονδιακών υπηρεσιών, ενδέχεται να εκδίδει συστάσεις προς την κυβέρνηση και τις υπηρεσίες πληροφοριών και υποβάλλει τακτικά αναφορές σε επιτροπές του Κογκρέσου και τον Πρόεδρο[113].

Γ) Αντί Επιλόγου

Έχοντας πλήρη γνώση του έντονου προβληματισμού γύρω από το ζήτημα της διαβίβασης προσωπικών δεδομένων ιδίως μετά τις αποφάσεις Schrems παράλληλα με την εποχή παγκοσμιοποίησης της πληροφορίας που διανύουμε και στο πλαίσιο της σύνταξης της διπλωματικής μου εργασίας, είχα την ευκαιρία να διενεργήσω την παραπάνω βιβλιογραφική έρευνα έχοντας ως στόχο να αναδείξω στους δυνητικούς αναγνώστες τις μεθόδους διαβίβασης προσωπικών δεδομένων από την ΕΕ προς τις ΗΠΑ τόσο πριν, όσο και μετά από την εφαρμογή του GDPR, με την παράλληλη ανάδειξη των ζητημάτων που προέκυψαν από τις αποφάσεις Schrems I και Schrems

[112] Βλ. Αιτιολογική Σκέψη 158 Προσχεδίου Απόφασης Επάρκειας

[113] Βλ. Αιτιολογική Σκέψη 159 Προσχεδίου Απόφασης Επάρκειας

II. Τα σημαντικότερα εξ αυτών ήταν α) η πρόσβαση που είχαν στα δεδομένα των ευρωπαίων πολιτών οι υπηρεσίες μυστικών πληροφοριών των ΗΠΑ και β) η μη ύπαρξη ενός πλαισίου ενημέρωσης και προστασίας των υποκειμένων των δεδομένων.

Τόσο υπό το καθεστώς του Ασφαλούς Λιμένα, όσο και υπό το καθεστώς της Ασπίδας Προστασίας Ιδιωτικής Ζωής, γινόταν δεκτό οτι μόνο οι αυτοπιστοποιούμενοι οργανισμοί των ΗΠΑ υπόκεινται στην υποχρεωτική εφαρμογή των Αρχών που θεσπίζονταν, παρά το γεγονός οτι αναγνωριζόταν η δυνατότητα υπερίσχυσης τυχόν απαιτήσεων εθνικής ασφάλειας, δημοσίου συμφέροντος και επιβολής του νόμου εις βάρος των Αρχών. Η δυνατότητα αυτή των μυστικών υπηρεσιών των ΗΠΑ να έχουν πρόσβαση σε προσωπικά δεδομένα πολιτών της ΕΕ χωρίς να είναι υποχρεωμένες να τηρούν τις ανάλογες Αρχές που θεσπίζονταν ή υπό το καθεστώς ενισχυμένης εποπτείας σε ένα πλαίσιο κανόνων υπονομεύει την ουσία του θεμελιώδους δικαιώματος στο σεβασμό της ιδιωτικής ζωής.

Πλέον η Ευρωπαϊκή Επιτροπή από κοινού με την Ηγεσία των ΗΠΑ βρίσκεται στο τελικό στάδιο εγκαθίδρυσης ενός πλαισίου διατλαντικής διαβίβασης δεδομένων που προσπαθεί να “θεραπεύσει” τις παραπάνω παθογένειες. Κατά την γνώμη μου η πιο ορθή αντιμετώπιση του προβλήματος, θα ήταν η προσπάθεια ανάπτυξης μιας κοινής νομοθεσίας για την προστασία προσωπικών δεδομένων μεταξύ ΕΕ - ΗΠΑ. Πως θα μπορούσε όμως να γίνει αυτό; Από την στιγμή που η ΕΕ έχει θεσπίσει τον GDPR, θα μπορούσε να θεωρηθεί ορθή μια προσπάθεια συνολικής υιοθέτησης της εν λόγω νομοθεσίας και από τα δύο μέρη (ΕΕ - ΗΠΑ) μέσω διαπραγματεύσεων. Κατ΄ αυτόν τον τρόπο θα δημιουργούταν ένα επαρκές επίπεδο προστασίας με την ουσιαστική σημασία του όρου. Ωστόσο επειδή από την μία πλευρά μία τέτοια κίνηση θα δημιουργούσε ζητήματα θεσμικής αυτοτέλειας και από την άλλη το ίδιο το ΔΕΕ με την νομολογία του (Schrems I) δεν απαιτεί πανομοιότυπο πλαίσιο αλλά κατ΄ ουσίαν ισοδύναμο πλαίσιο προστασίας, η ανάπτυξη ενός πλαισίου διαβίβασης δεδομένων που αντιμετωπίζει τις παραπάνω παθογένειες θεωρείται ως η πιο πρόσφορη λύση. Κατ΄ επέκταση των παραπάνω οι ΗΠΑ αναδιαμόρφωσαν την νομοθεσία τους συμπεριλαμβάνοντας προϋποθέσεις για την πρόσβαση των μυστικών υπηρεσιών σε δεδομένα που έχουν διαβιβαστεί από την ΕΕ, ορίζονται μηχανισμοί εποπτείας και επίλυσης διαφορών. Η Επιτροπή με την δημοσίευση του προσχεδίου επάρκειας αναγνωρίζει την συμμόρφωση με τις απαιτήσεις του GDPR και την νομολογίας του

ΔΕΕ. Πλέον αναμένεται η γνωμοδότηση του ΕΣΠΔ και εν τέλει ο χρόνος θα δείξει την επιτυχία ή όχι του νέου πλαισίου, που εκ πρώτης όψεως φαίνεται να είναι ορθό.

Βιβλιογραφία

Λουκαΐτη Ναταλία, Διαβίβαση Προσωπικών Δεδομένων στο Περιβάλλον του Υπολογιστικού Νέφους (διπλωματική εργασία), Πανεπιστήμιο Πειραιώς

Παύλου Αναστασία Η., Η διαβίβαση των προσωπικών δεδομένων από την Ευρώπη στις Ηνωμένες Πολιτείες Αμερικής (διπλωματική εργασία), Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών

Στραγαλινός Αιμίλιος - Αρτέμιος, Το ισχύον πλαίσιο για τις διαβιβάσεις δεδομένων σε τρίτες χώρες υπό το φως των αποφάσεων του Δικαστηρίου της Ευρωπαϊκής Ενωσης στην υπόθεση Schrems (διπλωματική εργασία), Πανεπιστήμιο Πειραιώς

Άρθρα - Μελέτες

Διαβίβαση δεδομένων μεταξύ ΕΕ και ΗΠΑ: Υπεγράφη το Διάταγμα για την εφαρμογή του νέου πλαισίου από τον Πρόεδρο Μπάιντεν, 7/10/2022, διαθέσιμο σε: https://www.lawspot.gr/nomika-nea/diavivasidedomenon-metaxy-ee-kai-ipa-ypegrafi-diatagma-gia-tin-efarmogi-toy neoy?fbclid=IwAR2ii1ww64MnUZJ23QHLLXiR2mSu44Ul7SAcL7NXd7kBvAqyTCzDJojL4rs (τελευταία πρόσβαση 14/01/2023)

Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων, Συχνές ερωτήσεις σχετικά με την απόφαση του Δικαστηρίου της Ευρωπαϊκής Ένωσης στην υπόθεση C-311/18 - Επίτροπος προστασίας δεδομένων κατά Facebook Ireland Ltd και Maximillian Schrems, 23/07/2020, διαθέσιμο σε: https://edpb.europa.eu/sites/default/files/files/file1/20200724_edpb_faqoncjeuc31118_el.pdf (τελευταία πρόσβαση 14/01/2023)

Κωνσταντίνου Στέργιος, Τυποποιημένες Συμβατικές Ρήτρες (SCCs) και επόμενα βήματα, 14/06/2021, διαθέσιμο σε: https://www.lawspot.gr/nomika-blogs/stergios_konstantinoy/typopoiimenes-symvatikes-ritres-sccs-kai-epomena-vimata (τελευταία πρόσβαση 14/01/2023)

Παλιού Ε. Οι νέες τυποποιημένες συμβατικές ρήτρες της Ευρωπαϊκής Επιτροπής- Η διασυνοριακή διαβίβαση προσωπικών δεδομένων στον απόηχο της νομολογίας Schrems (αποφάσεις του ΔΕΕ υπ'αριθμ. C362/14 και C-311/18), ΔίΜΕΕ τ. 4/2021

Παναγοπούλου Φερενίκη - Παπακωνσταντίνου Σουζάνα, Διατλαντικές διαβιβάσεις δεδομένων προσωπικού χαρακτήρα: Η συμφωνία Ε.Ε. και Η.Π.Α. για το νέο Trans-Atlantic Data Privacy Framework, 19/04/2022, διαθέσιμο σε: https://www.syntagmawatch.gr/trending-issues/diatlantikes-diavivaseis-dedomenwn-proswpikou-xarakthra-h-symfwnia-ee-kai-hpa-gia-to-neo-trans-atlantic-data-privacy-framework/ (τελευταία πρόσβαση 14/01/2023)

Παναγοπούλου Φερενίκη, Συνταγματικές προεκτάσεις των μηχανισμών διευρύνσεως της προστασίας δεδομένων προσωπικού χαρακτήρα πέραν της ΕΕ: Εξωεφαφική εφαρμογή του ΓΚΠΔ και διασυνοριακή διαβίβαση δεδομένων, ΔίΜΕΕ τ. 4/2019

Brown Ian - Korff Douwe, Exchanges of personal data after the Schrems II judgment, διαθέσιμο σε: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/694678/IPOL_STU(2021)694678_EN.pdf (τελευταία πρόσβαση 14/01/2023)

Clark Kelli, The EU Safe Harbor Agreement Is Dead, Here's What To Do About It, 27/10/2015, διαθέσιμο σε: https://www.forbes.com/sites/riskmap/2015/10/27/the-eu-safe-harbor-agreement-is-dead-heres-what-to-do-about-it/?sh=34faa0723cea (τελευταία πρόσβαση 14/01/2023)

Data Guidance, The Definitive Guide to Schrems II, 25/03/2022, διαθέσιμο σε: https://www.dataguidance.com/resource/definitive-guide-schrems-ii (τελευταία πρόσβαση 14/01/2023)

European Commission, New Standard Contractual Clauses - Questions and Answers overview, διαθέσιμο σε: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions-and-answers-overview_en (τελευταία πρόσβαση 14/01/2023)

European Commission - Press release, Data protection: Commission starts process to adopt adequacy decision for safe data flows with the US, 13/12/2022, διαθέσιμο σε: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7631 (τελευταία πρόσβαση 14/01/2023)

European Commission - Press release, European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework, 25/03/2022, διαθέσιμο σε: https://ec.europa.eu/commission/presscorner/detail/nl/ip_22_2087 (τελευταία πρόσβαση 14/01/2023)

European Commission, Questions & Answers: EU-US Data Privacy Framework, 7/10/2022, διαθέσιμο σε: https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_6045 (τελευταία πρόσβαση 14/01/2023)

Federal Trade Commission Enforcement of the U.S.-EU and U.S.-Swiss Safe Harbor Frameworks, διαθέσιμο σε: https://www.ftc.gov/business-guidance/resources/federal-trade-commission-enforcement-us-eu-us-swiss-safe-harbor-frameworks (τελευταία πρόσβαση 14/01/2023)

Global Freedom of Expression Columbia University, Schrems v. Data Protection Commissioner, διαθέσιμο σε: https://globalfreedomofexpression.columbia.edu/cases/schrems-v-data-protection-commissioner/ (τελευταία πρόσβαση 14/01/2023)

Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II, White Paper, U.S. Department of Commerce, U.S. Department of Justice, Office of the Director of National Intelligence , Σεπτέμβριος 2020, διαθέσιμο σε: https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF (τελευταία πρόσβαση 14/01/2023)

Linebaugh Chris - Liu Edward, EU Data Transfer Requirements and U.S. Intelligence Laws: Understanding Schrems II and Its Impact on the EU-U.S. Privacy Shield, Congressional Research Service

Nakashima Ellen, Top E.U. court strikes down major data-sharing pact between U.S. and Europe, 6/10/2015, διαθέσιμο σε: https://www.washingtonpost.com/world/national-security/eu-court-strikes-down-safe-harbor-data-transfer-deal-over-privacy-concerns/2015/10/06/2da2d9f6-6c2a-11e5-b31c-d80d62b53e28_story.html (τελευταία πρόσβαση 14/01/2023)

Νομοθεσία - Νομολογία

Απόφαση 2000/520/ΕΚ της Επιτροπής της 26ης Ιουλίου 2000, βάσει της οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την επάρκεια της προστασίας που παρέχεται από τις αρχές ασφαλούς λιμένα για την προστασία της ιδιωτικής ζωής και τις συναφείς συχνές ερωτήσεις που εκδίδονται από το Υπουργείο Εμπορίου των ΗΠΑ, διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32000D0520&from=en (τελευταία πρόσβαση 14/01/2023)

Γνώμη 1/2016 της ομάδας εργασίας του άρθρου 29, υιοθετήθηκε στις 13 Απριλίου 2016

Δ.Ε.Ε., C-311/18 (Grand Chamber), Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems, 16/07/2020, διαθέσιμη σε: https://curia.europa.eu/juris/liste.jsf?oqp=&for=&mat=or&lgrec=el&jge=&td=%3BALL&jur=C%2CT%2CF&num=C-311%252F18&page=1&dates=&pcs=Oor&lg=&pro=&nat=or&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%252C%252C%252C%252C%252C%252C%252Ctrue%252Cfalse%252C (τελευταία πρόσβαση 14/01/2023)

Δ.Ε.Ε., C-362/14 (Grand Chamber), Maximillian Schrems v. Data Protection Commissioner, 6/10/2015, διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:62014CJ0362&from=en (τελευταία πρόσβαση 14/01/2023)

Ευρωπαϊκή Επιτροπή, Προσχέδιο εκτελεστικής απόφασης σύμφωνα με τον κανονισμό (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το επαρκές επίπεδο προστασίας των προσωπικών δεδομένων βάσει του EU-US Data Privacy Framework, διαθέσιμο σε: https://commission.europa.eu/system/files/2022-12/Draft_adequacy_decision_on_EU-US_Data_Privacy_Framework_0.pdf (τελευταία πρόσβαση 14/01/2023)

Οδηγία 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, διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:31995L0046&from=EL (τελευταία πρόσβαση 14/01/2023)

Department of Commerce - International Trade Administration, Issuance of Safe Harbor Principles and Transmission to European Commission, διαθέσιμο σε: https://www.govinfo.gov/content/pkg/FR-2000-07-24/pdf/00-18489.pdf (τελευταία πρόσβαση 14/01/2023)