ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών

«ΔΙΚΑΙΟ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ»

Ακαδημαϊκό έτος 2021-2022

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του Αιμίλιου - Αρτέμιου Στραγαλινού (Α.Μ.: ΜΔΙ2046)

ΤΟ ΙΣΧΥΟΝ ΠΛΑΙΣΙΟ ΓΙΑ ΤΙΣ ΔΙΑΒΙΒΑΣΕΙΣ ΔΕΔΟΜΕΝΩΝ ΣΕ ΤΡΙΤΕΣ ΧΩΡΕΣ ΥΠΟ ΤΟ ΦΩΣ ΤΩΝ ΑΠΟΦΑΣΕΩΝ ΤΟΥ ΔΙΚΑΣΤΗΡΙΟΥ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ ΣΤΗΝ ΥΠΟΘΕΣΗ SCHREMS

Επιβλέπουσα:

Ευαγγελία (Λίλιαν) Μήτρου

Πειραιάς, Μάιος 2022

ΑΦΙΕΡΩΣΗ

Η παρούσα διπλωματική εργασία αποτελεί καρπό ενός ακαδημαϊκού ταξιδιού που έχει ξεχωριστή σημασία για εμένα. Και τούτο διότι, χωρίς να είναι προμελετημένο, συνέπεσε με μια προσωπική μου δοκιμασία, για την οποία χρειάστηκε να παύσουν όλα γύρω μου για ορισμένο χρονικό διάστημα. Χάρη σε αυτό το μεταπτυχιακό, το πνεύμα μου δεν σταμάτησε να πλέει στα πελάγη της γνώσης και της δημιουργίας. Με τη μελέτη αυτή ολοκληρώνεται με τον καλύτερο δυνατό τρόπο το εν λόγω ταξίδι. Την αφιερώνω σε κάθε έναν ξεχωριστά από τους παραστάτες μου, για την αγάπη και τη στήριξή τους.

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΛΗΨΗ

Το καθεστώς για τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα, ως «ζωντανός οργανισμός», διαρκώς εξελίσσεται αλληλοεπιδρώντας με την τεχνολογική εξέλιξη, ώστε αφενός να διαφυλάξει το θεμελιώδες δικαίωμα του ανθρώπου στην προστασία των δεδομένων προσωπικού χαρακτήρα, και αφετέρου να ενισχύσει την οικουμενική ροή των εν λόγω δεδομένων, η οποία είναι απαραίτητη για την ανάπτυξη των διεθνών εμπορικών συναλλαγών. Η νομολογία του Δικαστηρίου της Ευρωπαϊκής Ένωσης παίζει καθοριστικό ρόλο στην εξέλιξη αυτή, με πρόμαχους τις αποφάσεις στην πολύκροτη υπόθεση *Schrems*, οι οποίες οδήγησαν πλήθος επιχειρήσεων σε αδιέξοδο αναφορικά με τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα προς τις Ηνωμένες Πολιτείες Αμερικής, και κατ' επέκταση σε άλλες τρίτες χώρες. Ωστόσο, τα θεσμικά όργανα της Ευρωπαϊκής Ένωσης, όπως και οι Αρχές Προστασίας Δεδομένων, δεν άργησαν να κινητοποιηθούν και να αναπτύξουν μηχανισμούς προς επίλυση του εν λόγω ζητήματος εφαρμόζοντας το νέο αυστηροποιημένο πλαίσιο που έθεσε το Δικαστήριο της Ευρωπαϊκής Ένωσης. Υπό το φως των προαναφερθέντων νομολογιακών και κανονιστικών ζυμώσεων σε ενωσιακό επίπεδο, η παρούσα μελέτη έχει ως στόχο να αναδείξει το υφιστάμενο καθεστώς για τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα από την Ευρωπαϊκή Ένωση σε τρίτες χώρες.

ABSTRACT

The regime for international data transfer, as a "living organism", is constantly evolving, interacting with technological developments in order to safeguard the fundamental human right to the protection of personal data and to enhance the international flow of personal data, which is essential for the development of international trade. The case law of the Court of Justice of the European Union is playing a decisive role in this development, led by its decisions in the controversial *Schrems* case, which led numerous companies to a deadlock regarding data transfers to the USA, and by extension to other third countries. However, the European Union's institutions, as well as the data protection authorities, reacted promptly and developed mechanisms to resolve this issue by implementing the new strict framework set by the Court of Justice of the European Union. In the light of the aforementioned legislative and regulatory developments at EU level, this master thesis aims to highlight the current framework for the transfer of personal data from the European Union to third countries.

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

ΑΠΔ	Αρχή(ες) Προστασίας Δεδομένων
ΓΚΠΔ	Γενικός Κανονισμός Προστασίας Δεδομένων
ΕΒΕ	Ευρωπαϊκές Βασικές Εγγυήσεις
ΕΔΑΔ	Ευρωπαϊκό Δικαστήριο Ανθρωπίνων Δικαιωμάτων
ΕΕ	Ευρωπαϊκή Ένωση
ΕΕΠΔ	Ευρωπαίος Επόπτης Προστασίας Δεδομένων
ΕΣΠΔ	Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων
ΔΕΕ	Δικαστήριο της Ευρωπαϊκής Ένωσης
ΔΕΚ	Δεσμευτικοί Εταιρικοί Κανόνες
ΗΠΑ	Ηνωμένες Πολιτείες Αμερικής
ΝΟΥΒ	None Of Your Business
ΤΣΡ	Τυποποιημένες Συμβατικές Ρήτρες
Χάρτης	Χάρτης Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης
IDTA	International Data Transfer Agreement
NSA	National Security Agency
FBI	Federal Bureau of Investigation
FISC	Foreign Intelligence Surveillance Court

ΕΙΣΑΓΩΓΗ

Στη σημερινή παγκοσμιοποιημένη ψηφιακή οικονομία, η διαβίβαση δεδομένων προσωπικού χαρακτήρα αποτελεί αναπόσπαστο κομμάτι της δραστηριότητας των περισσότερων επιχειρήσεων (όπως παρόχων υπηρεσιών υπολογιστικού νέφους, φορέων διαχείρισης κοινωνικών δικτύων και μηχανών αναζήτησης). Παράλληλα, είναι γνωστό ότι διενεργούνται διασυνοριακές διαβιβάσεις μεγάλου όγκου δεδομένων προσωπικού χαρακτήρα μεταξύ κρατών, διεθνών οργανισμών, ευρωπαϊκών θεσμικών οργάνων, διωκτικών αρχών και δημόσιων οργανισμών, πολλές φορές μάλιστα και εν κρυπτώ. Τα δεδομένα που κυκλοφορούν στις ηλεκτρονικές λεωφόρους της κοινωνίας της πληροφορίας αφορούν στοιχεία εργαζομένων, πελατών, ασθενών, στοιχεία διαδικτυακής κίνησης, καταγραφής καταναλωτικών προτιμήσεων κ.ο.κ., και αποθηκεύονται σε διακομιστές που βρίσκονται σε διαφορετικές χώρες ή στο υπολογιστικό νέφος, είτε εντός είτε εκτός της Ευρωπαϊκής Ένωσης (εφεξής «**ΕΕ**»)[1]. Σε ότι αφορά, μάλιστα, το υπολογιστικό νέφος, είναι δύσκολο να καθοριστεί, τουλάχιστον εκ των προτέρων, ο ακριβής τόπος αποθήκευσης των πληροφοριών, αφού, όπως χαρακτηριστικά έχει επισημάνει η Ομάδα του άρθρου 29[2], *«τα δεδομένα μπορεί να βρίσκονται στις 2 μ.μ. σε ένα κέντρο δεδομένων και στις 4 μ.μ. στην άλλη άκρη του κόσμου»*[3]. Αδιαμφισβήτητα, ο τομέας της διασυνοριακής διαβίβασης δεδομένων κατέστη πιο σημαντικός από ποτέ κατά τη διάρκεια της πανδημίας του κορονοϊού, αφού βρέθηκε στο επίκεντρο της καθημερινής μας ζωής, με χαρακτηριστικότερο παράδειγμα την εξ αποστάσεως εργασία.

Ο Γενικός Κανονισμός για την Προστασία Δεδομένων[4] (εφεξής «**ΓΚΠΔ**» ή «**Κανονισμός**») που τέθηκε σε εφαρμογή από τις 25 Μαΐου 2018, αντικαθιστώντας το πλαίσιο που είχε

[1] Κανέλλος Λ. (2020) *«The GDPR Handbook - Για DPOs, Επιχειρήσεις & Οργανισμούς»*. Αθήνα, Νομική Βιβλιοθήκη.

[2] Πρόκειται για την ανεξάρτητη ευρωπαϊκή ομάδα εργασίας που χειριζόταν θέματα σχετικά με την προστασία της ιδιωτικής ζωής και των δεδομένων προσωπικού χαρακτήρα έως την 25η Μαΐου 2018 (έναρξη ισχύος του Γενικού Κανονισμού για την Προστασία Δεδομένων), οπότε την σκυτάλη παρέλαβε το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων.

[3] Βλ. Μήτρου, Λ. (2015), «Προστασία Προσωπικών Δεδομένων και υπολογιστικό νέφος», *ΤΝΠ QUALEX, ΔiΜΕΕ*, 4/2015, σελ. 534 - 549.

[4] Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων). Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016R0679&from=EL

καθιερώσει η Οδηγία 95/46/ΕΚ[5] (εφεξής «**Οδηγία**»), θεσπίζει, ως θεματοφύλακας της ιδιωτικότητας, κανόνες σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα εντός της ΕΕ και κατ' αυτόν τον τρόπο επιτρέπει την ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα εντός της ΕΕ. Αναμφίβολα ένα από τα δυσκολότερα ζητήματα του Κανονισμού, που άπτονται των ορίων του ιδιωτικού διεθνούς δικαίου, αλλά και της διαδόσεως των ανθρωπίνων δικαιωμάτων και των βασικών θεμελιωδών ελευθεριών μέσω του διεθνούς εμπορικού δικαίου, αποτελεί η διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες[6]. Το πέμπτο κεφάλαιο του ΓΚΠΔ διέπει την προαναφερθείσα διαβίβαση δεδομένων θέτοντας ψηλά τον πήχη, καθώς η διαβίβαση δεν πρέπει να υπονομεύει το επίπεδο προστασίας που διασφαλίζει ο ΓΚΠΔ στην ΕΕ[7]. Επομένως, εφόσον η προστασία του ΓΚΠΔ συνοδεύει τα δεδομένα, οι κανόνες προστασίας αυτών εξακολουθούν να ισχύουν ανεξάρτητα από τον τελικό προορισμό τους. Προς τούτο, ο ΓΚΠΔ παρέχει μια σειρά από μηχανισμούς διαβίβασης που καθορίζουν τους όρους νομιμότητας της διαβίβασης δεδομένων σε τρίτες χώρες.

Οι διεθνείς αποκαλύψεις σχετικά με την πρακτική μαζικής επιτήρησης των υπηρεσιών ασφαλείας, και ιδίως των μυστικών υπηρεσιών, ορισμένων κρατών, όπως των Ηνωμένων Πολιτειών Αμερικής (εφεξής «**ΗΠΑ**»), με σημείο αναφοράς τις αποκαλύψεις του Edward Snowden[8], έδωσαν το έναυσμα να εκκινήσει μια παγκόσμια προσπάθεια τόσο για την ενημέρωση και ευαισθητοποίηση των πολιτών, όσο και για την πάταξη, ει δυνατόν, της εν λόγω πρακτικής. Σε επίπεδο ΕΕ, πρωτεργάτης της εν λόγω προσπάθειας είναι ο ακτιβιστής Maximillian Schrems[9] (εφεξής «**Max Schrems**»), ο οποίος προβαίνοντας σε καταγγελία

[5] 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 στο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:31995L0046&from=EL.

[6] Βλ. σχετικά Λεμπέση, Δ. (2018), «Γενικός Ευρωπαϊκός Κανονισμός για την προστασία προσωπικών δεδομένων (ΕΕ 2016/679) - Κατάργηση τής οδηγίας 95/46/ΕΚ - Συγκριτική μελέτη», *Δελτίον Εργατικής Νομοθεσίας*, τ. 74, τεύχ. 1733. Διαθέσιμο στο: http://www.den.gr/Login/?ReturnTo=/790/#main1.

[7] Άρθρο 44 του ΓΚΠΔ.

[8] Πρώην υπάλληλος (διαχειριστή συστημάτων) της Υπηρεσίας Εθνικής Ασφάλειας των ΗΠΑ, ο οποίος προέβη σε αποκαλύψεις σχετικά με τη μαζική και χωρίς διάκριση επεξεργασία από τις αμερικανικές μυστικές υπηρεσίες (ιδίως της Υπηρεσίας Εθνικής Ασφάλειας και του Ομοσπονδιακού Γραφείου Ερευνών) δεδομένων προσωπικού χαρακτήρα που αφορούν σε χρήστες των υπηρεσιών που παρέχουν οι κολοσσοί της Πληροφορικής (όπως Facebook, Google και Microsoft). Βλ. σχετικά Snowden E. (2019), *Το Μεγάλο Φακέλωμα*. Αθήνα: Ψυχογιός.

[9] Αυστριακός δικηγόρος και ιδρυτής της μη κερδοσκοπικής οργάνωσης ψηφιακών δικαιωμάτων «None Of Your Business» που εδρεύει στη Βιέννη, με στόχο την παραπομπή στο Δικαστήριο της ΕΕ νομικών

ενώπιον του Ιρλανδού Επιτρόπου Προστασίας Δεδομένων κατά της Facebook για τη διαβίβαση δεδομένων προσωπικών δεδομένων που τον αφορούν από την ΕΕ στις ΗΠΑ, κίνησε μια πολυετή δικαστική διαμάχη, που μέχρι σήμερα είχε ως αποτέλεσμα την έκδοση δυο αποφάσεων ορόσημο από το Δικαστήριο της Ευρωπαϊκής Ένωσης (εφεξής «**Δικαστήριο**» ή «**Δικαστήριο της ΕΕ**» ή «**ΔΕΕ**»), ευρέως γνωστών ως *Schrems I* και *Schrems II*.

Το γεγονός, μάλιστα, ότι το Δικαστήριο της ΕΕ προέβη στις δυο παραπάνω αποφάσεις σε διάστημα μόλις πέντε χρόνων, αδιαμφισβήτητα ταλάνισε τη δραστηριότητα πλήθους επιχειρήσεων παγκοσμίως. Πλέον έχει καταστεί περίπλοκη η διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες, και όχι μόνο προς τις ΗΠΑ, καθώς το Δικαστήριο με την απόφαση *Schrems II*, και με αφορμή τη διαβίβαση δεδομένων μεταξύ ΕΕ και ΗΠΑ, έθεσε συμπληρωματικές υποχρεώσεις, τις οποίες θα πρέπει να ακολουθούν τόσο οι εξαγωγείς όσο και οι εισαγωγείς δεδομένων σε όλο το φάσμα των διασυνοριακών διαβιβάσεων, και μάλιστα ανεξαρτήτως του μηχανισμού διαβίβασης που έχουν επιλέξει. Το ενισχυμένο αυτό πλαίσιο για την ασφάλεια των δεδομένων προσωπικού χαρακτήρα, πρόσθεσε μεγαλύτερο βάρος στην ήδη υπάρχουσα ευθύνη του εξαγωγέα δεδομένων βάσει του ΓΚΠΔ και της αρχής της λογοδοσίας[10]. Ταυτόχρονα, όμως, το ΔΕΕ αναγνώρισε την υποχρέωση του εισαγωγέα δεδομένων να συνδράμει των εξαγωγέα δεδομένων στην εκπλήρωση των διευρυμένων πλέον υποχρεώσεών του. Εντούτοις, ενώ το ΔΕΕ έθεσε νέες υποχρεώσεις για τους εξαγωγείς και εισαγωγείς δεδομένων στο πλαίσιο των διαβιβάσεων δεδομένων σε τρίτες χώρες, δεν προσδιόρισε τους τρόπους πρακτικής εκπλήρωσης αυτών, δημιουργώντας έτσι σύγχυση στον επιχειρηματικό κόσμο, ο οποίος βρέθηκε αιφνιδίως σε αχαρτογράφητα μονοπάτια.

Στο πλαίσιο αυτό, αρωγός των επιχειρήσεων στάθηκε το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (εφεξής «**ΕΣΠΔ**»), το οποίο μεσώ ειδικών συστάσεων, παρείχε στις επιχειρήσεις τις αναγκαίες εκείνες κατευθύνσεις, ώστε να κατορθώσουν να προσαρμόσουν σταδιακά τις δραστηριότητές τους στις νέες υποχρεώσεις που τις βαραίνουν βάσει της απόφασης *Schrems II*.

υποθέσεων σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα. Βλ. σχετικά: https://noyb.eu/en.

[10] Άρθρο 5, παράγραφος 2 σε συνδυασμό με τα άρθρα 24 και 32 του ΓΚΠΔ.

Η Ευρωπαϊκή Επιτροπή (εφεξής «**Επιτροπή**») με τη σειρά της υιοθέτησε νέες τυποποιημένες συμβατικές ρήτρες (εφεξής «**ΤΣΡ**»), οι οποίες ενσωματώνουν τις νέες υποχρεώσεις που έθεσε το ΔΕΕ, ενώ παρέχουν στις επιχειρήσεις μεγαλύτερη ευελιξία στο πλαίσιο των συμβατικών τους σχέσεων, καθώς απέχουν κατά πολύ από το κλασικό σενάριο που αφορά στη σχέση μεταξύ ενός υπευθύνου επεξεργασίας και ενός εκτελούντος την επεξεργασία. Παράλληλα, μέχρι και σήμερα έχουν εκδοθεί δυο αποφάσεις επάρκειας της Επιτροπής, που αφορούν στο Ηνωμένο Βασίλειο και τη Δημοκρατία της Κορέας, επί τη βάσει του νέου μηχανισμού που καθιέρωσε το ΔΕΕ μέσω της απόφασης *Schrems II* για την αξιολόγηση της νομοθεσίας μιας τρίτης χώρας.

Από την πλευρά τους οι Αρχές Προστασίας Δεδομένων (εφεξής «**ΑΠΔ**») δεν άργησαν να προσαρμοστούν στη νέα αυτή πραγματικότητα, εκδίδοντας αποφάσεις που αντικατοπτρίζουν τη νέα συνθήκη που καθιέρωσε η νομολογία του ΔΕΕ για τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες.

Σε πρώτο χρόνο, η παρούσα μελέτη έχει ως στόχο να αναδείξει το ενωσιακό πλαίσιο για τις διασυνοριακές διαβιβάσεις εκτός της ΕΕ, όπως αυτό αποτυπώθηκε αρχικά στην Οδηγία και εν συνεχεία στο ΓΚΠΔ (**Ενότητα Ι**). Σε δεύτερο χρόνο, θα επιχειρηθεί μια σύντομη αναδρομή στην πολύκροτη υπόθεση Schrems με επισκόπηση των σημαντικότερων πορισμάτων των αποφάσεων *Schrems I* και *Schrems II* (**Ενότητα ΙΙ**). Σε τρίτο χρόνο, η μελέτη επιχειρεί να αναδείξει το υφιστάμενο καθεστώς για τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες στον απόηχο της απόφασης *Schrems II*, υπό το φως των κατευθυντήριων γραμμών του ΕΣΠΔ, των νέων ΤΣΡ και των αποφάσεων επάρκειας της Επιτροπής, και των αποφάσεων των ΑΠΔ, ενώ τέλος επιχειρείται η παρουσίαση ορισμένων καίριων ζητημάτων για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα στη «μετά Schrems ΙΙ εποχή» (**Ενότητα ΙΙΙ**).

ΕΝΟΤΗΤΑ Ι - ΤΟ ΕΝΩΣΙΑΚΟ ΚΑΝΟΝΙΣΤΙΚΟ ΠΛΑΙΣΙΟ ΓΙΑ ΤΙΣ ΔΙΑΒΙΒΑΣΕΙΣ ΔΕΔΟΜΕΝΩΝ ΣΕ ΤΡΙΤΕΣ ΧΩΡΕΣ

Στην παρούσα ενότητα θα εξετάσουμε το σύγχρονο πλαίσιο για τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα (εφεξής «**δεδομένα προσωπικού χαρακτήρα**» και «**δεδομένα**») σε τρίτες χώρες, τα θεμέλια του οποίου τέθηκαν από την Οδηγία **(Α)**, και εν συνεχεία ισχυροποιήθηκαν από το ΓΚΠΔ **(Β)**, ο οποίος μεταξύ άλλων έφερε σημαντικές αλλαγές σε ότι αφορά την εξωεδαφική εφαρμογή του ενωσιακού πλαισίου για την επεξεργασία δεδομένων ισχυροποιώντας το λεγόμενο «Brussels Effect» **(Γ)**.

Α. ΟΙ ΔΙΑΒΙΒΑΣΕΙΣ ΔΕΔΟΜΕΝΩΝ ΠΡΙΝ ΤΗΝ ΥΙΟΘΕΤΗΣΗ ΤΟΥ ΓΚΠΔ

Η προσπάθεια ρύθμισης της διαβίβασης δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες δεν παρατηρείται για πρώτη φορά στο ΓΚΠΔ, αφού η Οδηγία είχε καθιερώσει συγκεκριμένο πλαίσιο για τη διενέργεια αυτής αναγνωρίζοντας ότι *«η διασυνοριακή ροή δεδομένων προσωπικού χαρακτήρα είναι απαραίτητη για την ανάπτυξη των διεθνών εμπορικών συναλλαγών»*[11].

Σύμφωνα με το προϊσχύσαν καθεστώς η διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες, τα οποία έχουν υποστεί επεξεργασία ή πρόκειται να υποστούν επεξεργασία μετά τη διαβίβασή τους, ήταν δυνατή μόνον εφόσον η τρίτη χώρα εξασφάλιζε ικανοποιητικό επίπεδο προστασίας των δεδομένων, εν όψει της εσωτερικής νομοθεσίας ή των διεθνών δεσμεύσεων που είχε αναλάβει.

Αρμόδιο όργανο για την αξιολόγηση της επάρκειας προστασίας των δεδομένων προσωπικού χαρακτήρα σε χώρα εκτός της ΕΕ ήταν (και εξακολουθεί να είναι) η Επιτροπή, η οποία λάμβανε υπόψη όλες τις περιστάσεις που επηρεάζουν τη διαβίβαση των δεδομένων, ειδικότερα, τη φύση των δεδομένων, τους σκοπούς και τη διάρκεια των προβλεπόμενων δραστηριοτήτων επεξεργασίας, τη χώρα προέλευσης και τελικού προορισμού, τους γενικούς ή τομεακούς κανόνες δικαίου, τους επαγγελματικούς κανόνες και τα μέτρα ασφαλείας που ισχύουν στην εν λόγω τρίτη χώρα[12]. Σε περίπτωση θετικής κατάληξης της αξιολόγησης,

[11] Αιτιολογική σκέψη 56 της Οδηγίας.

[12] Η Ομάδα Εργασίας του άρθρου 29 στο έγγραφο εργασίας 12 του 1998 καθόρισε ότι η ανάλυση της επάρκειας θα πρέπει να βασίζεται σε δύο κύριους παράγοντες, δηλαδή στο περιεχόμενο των κανόνων που εφαρμόζονται στα δεδομένα προσωπικού χαρακτήρα που διαβιβάζονται σε τρίτη χώρα και στο σύστημα διασφάλισης της αποτελεσματικότητας των κανόνων αυτών. Βλ. σχετικά D. Vrbljanac (2018),

επιτρεπόταν να διαβιβάζονται τα δεδομένα προσωπικού χαρακτήρα από τα κράτη-μέλη της ΕΕ, χωρίς να είναι απαραίτητη η λήψη πρόσθετων εγγυήσεων. Τα κράτη-μέλη της ΕΕ λάμβαναν τα αναγκαία μέτρα συμμόρφωσης προς την απόφαση της Επιτροπής. Χαρακτηριστικό παράδειγμα αποτελεί η απόφαση επάρκειας της Επιτροπής σύμφωνα με την οποία οι ΗΠΑ εξασφάλιζαν ικανοποιητικό επίπεδο προστασίας για τα δεδομένα προσωπικού χαρακτήρα (γνωστή ως Safe Harbour, εφεξής «**απόφαση Ασφαλούς Λιμένα**»)[13], η οποία αποτέλεσε την αφετηρία της πολυσήμαντης δικαστικής διαμάχης ονόματι Schrems που θα εξετάσουμε αναλυτικά στην επόμενη ενότητα της παρούσας μελέτης. Όταν η Επιτροπή διαπίστωνε ότι μία τρίτη χώρα δεν διέθετε επαρκές επίπεδο προστασίας, τα κράτη-μέλη της ΕΕ όφειλαν να λάβουν τα κατάλληλα μέτρα, ώστε να αποφευχθεί η διαβίβαση δεδομένων σε αυτή τη χώρα[14].

Κατ' εξαίρεση, η διαβίβαση δεδομένων προς τρίτη χώρα με μη ικανοποιητικό επίπεδο προστασίας μπορούσε να πραγματοποιηθεί επί τη βάσει των παρεκκλίσεων που προβλέπονταν στο άρθρο 26 της Οδηγίας, ήτοι τη συναίνεση του υποκειμένου των δεδομένων, την εκτέλεση σύμβασης, τη διασφάλιση σημαντικού δημόσιου συμφέροντος ή ζωτικού συμφέροντος του υποκειμένου των δεδομένων, ή τις νόμιμες αξιώσεις. Στο ίδιο άρθρο προβλεπόταν η διαβίβαση δεδομένων σε τρίτες χώρες βάσει επαρκών εγγυήσεων όσον αφορά την προστασία της ιδιωτικότητας και των θεμελιωδών δικαιωμάτων και ελευθεριών των φυσικών προσώπων και την άσκηση των αντίστοιχων δικαιωμάτων, που προέκυπταν ιδίως από τις «*κατάλληλες συμβατικές ρήτρες*». Η Επιτροπή ενέκρινε τέσσερις τυποποιημένες συμβατικές ρήτρες στο πλαίσιο της προϊσχύουσας Οδηγίας. Ειδικότερα, με την πρώτη κατά σειρά απόφαση 2001/497/ΕΚ[15], η Επιτροπή ενέκρινε την πρώτη δέσμη πρότυπων ρητρών που μπορούν να χρησιμοποιούνται όταν ο υπεύθυνος επεξεργασίας της ΕΕ διαβιβάζει δεδομένα προσωπικού χαρακτήρα σε υπεύθυνο επεξεργασίας εκτός της ΕΕ

«Personal Data Transfer to Third Countries - Disrupting the Even Flow?», *Athens Journal of Law*, σελ. 337 - 358. Διαθέσιμο στο: https://www.athensjournals.gr/law/2018-4-4-4-Vrbljanac.pdf.

[13] Απόφαση 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 στο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32000D0520&from=EL.

[14] Άρθρο 25, παράγραφος 4 της Οδηγίας.

[15] Απόφαση της Επιτροπής της 15ης Ιουνίου 2001 σχετικά με τις τυποποιημένες συμβατικές ρήτρες για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα προς τρίτες χώρες δυνάμει του άρθρου 26 παράγραφος 4 της οδηγίας 95/46/ΕΚ (2001/497/ΕΚ). Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32001D0497&from=en.

(Δέσμη Ι «Υπεύθυνος Επεξεργασίας - Υπεύθυνος Επεξεργασίας»). Η εν λόγω απόφαση τροποποιήθηκε από την απόφαση 2004/915/ΕΚ[16], με την οποία η Επιτροπή ενέκρινε μια νέα δέσμη πρότυπων ρητρών για την εν λόγω διαβίβαση δεδομένων προσωπικού χαρακτήρα (Δέσμη ΙΙ «Υπεύθυνος Επεξεργασίας - Υπεύθυνος Επεξεργασίας»). Οι άλλες δύο αποφάσεις της Επιτροπής ρυθμίζουν τη διαβίβαση δεδομένων προσωπικού χαρακτήρα από υπεύθυνο επεξεργασίας της ΕΕ σε εκτελούντα την επεξεργασία εκτός της ΕΕ. Πρόκειται για την απόφαση 2002/16/ΕΚ[17] (Δέσμη Ι «Υπεύθυνος Επεξεργασίας - Εκτελών την Επεξεργασία»), η οποία εν συνεχεία αντικαταστάθηκε από την απόφαση 2010/87/ΕΕ[18] (Δέσμη ΙΙ «Υπεύθυνος Επεξεργασίας - Εκτελών την Επεξεργασία»)[19].

Στον απόηχο της απόφασης *Schrems I* του ΔΕΕ, την οποία θα εξετάσουμε στην επόμενη ενότητα της παρούσας μελέτης, η Επιτροπή εξέδωσε την εκτελεστική απόφαση 2016/2297 για την τροποποίηση των αποφάσεων 2001/497/ΕΚ και 2010/87/ΕΕ σχετικά με τις ΤΣΡ για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες[20]. Οι αποφάσεις 2001/497/ΕΚ

[16] Απόφαση της Επιτροπής της 27ης Δεκεμβρίου 2004 για την τροποποίηση της απόφασης 2001/497/ΕΚ όσον αφορά την εισαγωγή μιας εναλλακτικής δέσμης τυποποιημένων συμβατικών ρητρών για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα προς τρίτες χώρες (2004/915/ΕΚ). Διαθέσιμο στο: https://op.europa.eu/en/publication-detail/-/publication/57a11830-3866-44bf-a03a-0384f7b3d3d6/language-el/format-PDF.

[17] Απόφαση της Επιτροπής της 27ης Δεκεμβρίου 2001, σχετικά με τις τυποποιημένες συμβατικές ρήτρες για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε εκτελούντες επεξεργασία εγκατεστημένους σε τρίτες χώρες, βάσει της οδηγίας 95/46/ΕΚ (2002/16/ΕΚ). Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32002D0016&from=en.

[18] Απόφαση της Επιτροπής της 5ης Φεβρουαρίου 2010 σχετικά με τις τυποποιημένες συμβατικές ρήτρες για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε εκτελούντες επεξεργασία εγκατεστημένους σε τρίτες χώρες βάσει της οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (2010/87/ΕΕ). Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32010D0087&from=EN.

[19] Ο λόγος για την κατάργηση της απόφασης 2002/16/ΕΚ ήταν η ανάγκη τροποποίησης των ΤΣΡ λαμβάνοντας υπόψη την επέκταση των δραστηριοτήτων επεξεργασίας και τα νέα επιχειρηματικά μοντέλα για τη διεθνή επεξεργασία δεδομένων προσωπικού χαρακτήρα. Ειδικότερα, αυτό περιλαμβάνει την υπεργολαβική ανάθεση της συμφωνημένης επεξεργασίας. Σύμφωνα με τις ρήτρες της Δέσμης ΙΙ «Υπεύθυνος Επεξεργασίας - Εκτελών την Επεξεργασία», ο εισαγωγέας δεδομένων μπορεί να αναθέσει υπεργολαβικά τις δραστηριότητες επεξεργασίας, εφόσον ο εξαγωγέας δεδομένων έδωσε τη συγκατάθεσή του, μέσω γραπτής συμφωνίας με τον υπεργολάβο επεξεργασίας, η οποία επιβάλλει τις ίδιες υποχρεώσεις με εκείνες που επιβάλλονται στον εισαγωγέα δεδομένων βάσει των ρητρών.

[20] Εκτελεστική Απόφαση (ΕΕ) 2016/2297 της Επιτροπής της 16ης Δεκεμβρίου 2016 για την τροποποίηση των αποφάσεων 2001/497/ΕΚ και 2010/87/ΕΕ σχετικά με τις τυποποιημένες συμβατικές ρήτρες για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα προς τρίτες χώρες και σε εκτελούντες επεξεργασία εγκατεστημένους σε τρίτες χώρες βάσει της οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου. Διαθέσιμη στο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016D2297.

και 2010/87/ΕΕ τροποποιήθηκαν, καθώς η κρίση του ΔΕΕ στην απόφαση *Schrems I*, ότι οι εθνικές ΑΠΔ παραμένουν αρμόδιες να επιβλέπουν τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτη χώρα, θα πρέπει να εφαρμόζεται κατ' αναλογία και στις αποφάσεις της Επιτροπής, για τις οποίες μέχρι τότε προβλεπόταν περιορισμένη εξουσία των εθνικών ΑΠΔ[21]. Το γεγονός, μάλιστα, ότι η Facebook άρχισε να επικαλείται την τροποποιημένη απόφαση 2010/87/ΕΕ για τη διαβίβαση των δεδομένων προσωπικού χαρακτήρα των χρηστών αυτής στις ΗΠΑ, πυροδότησε την αναδιατύπωση της καταγγελίας του Max Schrems κατά της Facebook ενώπιον του Ιρλανδού Επιτρόπου Προστασίας Δεδομένων, ο οποίος με τη σειρά του αποφάσισε, με μια απόφαση 152 σελίδων, να παραπέμψει το ζήτημα της εγκυρότητας των ΤΣΡ στο ΔΕΕ, με αποτέλεσμα την πολύκροτη απόφαση *Schrems II*, την οποία θα εξετάσουμε αναλυτικότερα στην επόμενη ενότητα της παρούσας μελέτης.

Η Οδηγία, σε αντίθεση με το ΓΚΠΔ, δεν ανέφερε ρητά τους δεσμευτικούς εταιρικούς κανόνες ως κατάλληλες εγγυήσεις για τη διαβίβαση δεδομένων σε τρίτες χώρες, αλλά αναπτύχθηκαν στην πράξη με την υποστήριξη της Ομάδα Εργασίας του άρθρου 29. Πιο συγκεκριμένα, το 2012 η Ομάδα Εργασίας του άρθρου 29 θέσπισε ένα πλαίσιο για την έγκριση δεσμευτικών εταιρικών κανόνων που θα εφαρμόζονται από ομίλους εταιρειών που ενεργούν ως εκτελούντες την επεξεργασία, ώστε να διασφαλίζεται ότι οι διαβιβάσεις δεδομένων προσωπικού χαρακτήρα εκτός της ΕΕ μεταξύ εταιριών που συμμετέχουν στον ίδιο όμιλο του εκτελούντος την επεξεργασία θα πραγματοποιούνται σύμφωνα με το ευρωπαϊκό πλαίσιο προστασίας δεδομένων[22].

Β. ΤΟ ΟΠΛΟΣΤΑΣΙΟ ΤΟΥ ΓΚΠΔ

Η διαβίβαση δεδομένων προσωπικού χαρακτήρα προς τρίτες χώρες ρυθμίζεται από το πέμπτο κεφάλαιο του ΓΚΠΔ και επιτρέπεται μόνο εάν η συγκεκριμένη τρίτη χώρα εξασφαλίζει επαρκές επίπεδο προστασίας των δεδομένων. Πιο συγκεκριμένα, στο πέμπτο κεφάλαιο του ΓΚΠΔ θεσμοθετείται η διαδικασία δυνάμει της οποίας είναι επιτρεπτή η διαβίβαση των δεδομένων προσωπικού χαρακτήρα προς τρίτες χώρες, συμπεριλαμβανομένης της διασυνοριακής διαβίβασης δεδομένων μεταξύ επιχειρήσεων που

[21] Βλ. D. Vrbljanac (2018), «Personal Data Transfer to Third Countries - Disrupting the Even Flow?», ο.π.
[22] Ομάδα εργασίας του άρθρου 29 (1998), «*Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules*». Βέλγιο: Ομάδα εργασίας του άρθρου 29. Διαθέσιμο στο: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp195_en.pdf.

ανήκουν στον ίδιο όμιλο ή επιδιώκουν κοινό οικονομικό σκοπό. Ο ΓΚΠΔ ρυθμίζει το ζήτημα της διαβίβασης δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες κατά τρόπο παρόμοιο με εκείνον της Οδηγίας, με σαφή επίδραση της νομολογίας του ΔΕΕ και κυρίως της απόφασης *Schrems I*.

Η διαβίβαση δεδομένων εκτός της ΕΕ αποτελεί πρακτικά μια διαδικασία δύο σταδίων: ο εξαγωγέας δεδομένων (υπεύθυνος επεξεργασίας ή εκτελών την επεξεργασία) πρέπει, σε πρώτο στάδιο, να διασφαλίσει ότι η διαβίβαση δεδομένων, ως μορφή επεξεργασίας, πληροί τις προϋποθέσεις των γενικών διατάξεων των άρθρων 5, 6 και 9 του ΓΚΠΔ[23], και σε δεύτερο στάδιο, ότι τηρούνται οι «ασφαλιστικές δικλείδες» του πέμπτου κεφαλαίου του Κανονισμού.

Οι «ασφαλιστικές δικλείδες» του ΓΚΠΔ ενσωματώνονται στους προβλεπόμενους μηχανισμούς διαβίβασης δεδομένων, οι οποίοι ιεραρχούνται σε τρία επίπεδα[24], και αποτελούν τις νομικές βάσεις για την ομαλή και ασφαλή διαβίβαση δεδομένων σε τρίτες χώρες[25]. Πιο συγκεκριμένα, η διαβίβαση δεδομένων σε τρίτες χώρες πρέπει να βασίζεται σε έναν από τους ακόλουθους μηχανισμούς διαβίβασης, κατά σειρά προτεραιότητας:

1. Απόφαση Επάρκειας (Επίπεδο 1)

Σε πρώτο επίπεδο εκείνο που θα πρέπει να εξετάσει ο εξαγωγέας δεδομένων (υπεύθυνος επεξεργασίας ή εκτελών την επεξεργασία) κατά τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτη χώρα είναι εάν υπάρχει απόφαση επάρκειας της Επιτροπής, με την οποία η τελευταία έχει αξιολογήσει ότι η τρίτη χώρα εξασφαλίζει επαρκές επίπεδο προστασίας για τα δεδομένα προσωπικού χαρακτήρα. Κατά την εκτίμηση της επάρκειας του επιπέδου προστασίας, η Επιτροπή λαμβάνει υπόψη ιδίως τους ακόλουθους παράγοντες: το κράτος δικαίου στην τρίτη χώρα, το σεβασμό των ανθρωπίνων δικαιωμάτων και των θεμελιωδών ελευθεριών, τη γενική και τομεακή νομοθεσία, ιδίως όσον αφορά στην δημόσια

[23] Άρθρο 5 (Αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα), 6 (Νομιμότητα της επεξεργασίας) και 9 (Επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα) του ΓΚΠΔ.

[24] «Three-tier hierarchy», βλ. Hallinan, D., Bernier, A., Cambon-Thomsen, A. Crawley F. P., Dimitrova, D. Bauzer Medeiros, C., Nilsonne, G., Parker, S., Pickering, B., and Rennes, S. (2021), «International transfers of personal data for health research following Schrems II: a problem in need of a solution», *European Journal of Human Genetics*. Διαθέσιμο στο: https://www.nature.com/articles/s41431-021-00893-y.

[25] Βλ. Ευρωπαίος Επόπτης Προστασίας Δεδομένων (2021), *Case Law Digest 2021: Transfers of personal data to third countries - From Lindqvist to Schrems II: case law of the CJEU on transfers of personal data to third countries*, Βέλγιο: Ευρωπαίος Επόπτης Προστασίας Δεδομένων. Διαθέσιμο στο: https://edps.europa.eu/data-protection/our-work/publications/court-cases/case-law-digest-2021-transfers-personal-data_en.

ασφάλεια, στην άμυνα, την εθνική ασφάλεια, το ποινικό δίκαιο, τη δυνατότητα πρόσβασης των δημοσίων αρχών σε δεδομένα προσωπικού χαρακτήρα, την ύπαρξη και ουσιαστική λειτουργία εθνικής ΑΠΔ, τις διεθνείς δεσμεύσεις που έχει αναλάβει η τρίτη χώρα, από τις οποίες απορρέουν νομικά δεσμευτικές υποχρεώσεις στον τομέα αυτόν, κτλ. Η Επιτροπή, αφού εκτιμήσει όλους τους προαναφερθέντες παράγοντες που προβλέπονται αναλυτικά στο άρθρο 45, παράγραφος 2 του ΓΚΠΔ, εκδίδει απόφαση επάρκειας, μέσω εκτελεστικής πράξης, η οποία βεβαιώνει ότι στην υπό κρίση τρίτη χώρα εξασφαλίζεται επαρκές επίπεδο προστασίας. Η εν λόγω απόφαση επάρκειας περιλαμβάνει τα εξής: α) την πρόταση της Επιτροπής, β) τη γνώμη του ΕΣΠΔ[26], γ) την έγκριση από εκπροσώπους των κρατών-μελών της ΕΕ και δ) την υιοθέτηση της απόφασης επάρκειας από την Επιτροπή[27].

Το αποτέλεσμα μιας τέτοιας απόφασης είναι ότι τα δεδομένα προσωπικού χαρακτήρα μπορούν να διαβιβάζονται στη συγκεκριμένη τρίτη χώρα χωρίς να είναι απαραίτητη η λήψη περαιτέρω εγγυήσεων. Με άλλα λόγια, η διαβίβαση δεδομένων αντιμετωπίζεται σαν να λαμβάνει χώρα εντός της ΕΕ. Ωστόσο, οι αποφάσεις επάρκειας δεν εμποδίζουν τα υποκείμενα των δεδομένων να υποβάλουν καταγγελίες ενώπιον των αρμόδιων ΑΠΔ, ούτε εμποδίζουν τις εθνικές ΑΠΔ να παραπέμψουν την υπόθεση ενώπιον εθνικού δικαστηρίου εάν έχουν αμφιβολίες σχετικά με την εγκυρότητα μιας απόφασης επάρκειας, ώστε το εθνικό δικαστήριο να υποβάλει αίτηση έκδοσης προδικαστικής απόφασης στο ΔΕΕ με σκοπό την εξέταση της εν λόγω εγκυρότητας[28].

Ανά πάσα στιγμή, το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο της ΕΕ μπορούν να ζητήσουν από την Επιτροπή να τροποποιήσει ή να ανακαλέσει μια απόφαση επάρκειας με την αιτιολογία ότι η πράξη της υπερβαίνει τις εκτελεστικές αρμοδιότητες που προβλέπονται

[26] Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων είναι ένας ανεξάρτητος ευρωπαϊκός οργανισμός, επιφορτισμένος με τη διασφάλιση της συνεκτικής εφαρμογής των κανόνων προστασίας δεδομένων σε όλη την ΕΕ, και την προαγωγή της συνεργασίας μεταξύ των ΑΠΔ της ΕΕ. Το ΕΣΠΔ απαρτίζεται από τους προϊσταμένους των ΑΠΔ των κρατών-μελών της ΕΕ και από τον Ευρωπαίο Επόπτη Προστασίας Δεδομένων, ή τους εκπροσώπους τους.

[27] Βλ. Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, «Διαβιβάσεις δεδομένων εκτός ΕΕ - Αποφάσεις Επάρκειας». Διαθέσιμο στο: https://www.dpa.gr/el/enimerwtiko/thematikes_enotites/diavivaseis_ee/apofaseis_eparkeias.

[28] ΔΕΕ, C-311/18, *Data Protection Commissioner κατά Facebook Ireland Limited και Maximillian Schrems* (εφεξής «*Schrems II*»), 16 Ιουλίου 2020. Διαθέσιμο στο: https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EL&mode=lst&dir=&occ=first&part=1&cid=3359385, παράγραφοι 118 - 120.

στο ΓΚΠΔ. Λόγω αυτού κρίνεται ιδιαίτερα σημαντικό οι εξαγωγείς δεδομένων να ελέγχουν ανά τακτά χρονικά διαστήματα εάν η απόφαση επάρκειας έχει ανακληθεί ή ακυρωθεί.

Οι αποφάσεις επάρκειας της Επιτροπής δημοσιεύονται στην Εφημερίδα της ΕΕ, και μέχρι σήμερα έχουν εκδοθεί αποφάσεις επάρκειας, μεταξύ άλλων, για τα ακόλουθα κράτη: Αργεντινή, Καναδά, Ισραήλ, Νέα Ζηλανδία, Ελβετία, Ιαπωνία, Ηνωμένο Βασίλειο και Δημοκρατία της Κορέας[29].

2. Μηχανισμοί Διαβίβασης (Επίπεδο 2)

Σε περίπτωση που δεν έχει εκδοθεί απόφαση επάρκειας από την Επιτροπή για την τρίτη χώρα όπου διαβιβάζονται τα δεδομένα, το άρθρο 46 του ΓΚΠΔ προβλέπει μια σειρά μηχανισμών διαβίβασης που παρέχουν κατάλληλες εγγυήσεις, τους οποίους οι εξαγωγείς δεδομένων μπορούν να χρησιμοποιήσουν, κατά περίπτωση, στο πλαίσιο διαβίβασης δεδομένων προσωπικού χαρακτήρα σε χώρες εκτός της ΕΕ. Οι κυριότεροι εξ αυτών των μηχανισμών είναι οι εξής:

(α) *Τυποποιημένες Συμβατικές Ρήτρες*

Πρόκειται για πρότυπες ρήτρες προστασίας των δεδομένων προσωπικού χαρακτήρα που έχουν εγκριθεί από την Επιτροπή και επιτρέπουν την ελεύθερη διακίνηση δεδομένων όταν ενσωματώνονται σε μια σύμβαση. Οι εν λόγω ρήτρες περιέχουν συμβατικές υποχρεώσεις για τον εξαγωγέα και τον εισαγωγέα δεδομένων, καθώς και δικαιώματα για τα φυσικά πρόσωπα, των οποίων τα δεδομένα προσωπικού χαρακτήρα διαβιβάζονται. Τα φυσικά πρόσωπα μπορούν να επιβάλλουν άμεσα τα εν λόγω δικαιώματα τόσο έναντι του εξαγωγέα όσο και του εισαγωγέα δεδομένων. Μέχρι πρότινος, η Επιτροπή παρείχε δύο δέσμες ΤΣΡ για τις διαβιβάσεις δεδομένων σε χώρες εκτός της ΕΕ: αφενός μεταξύ ενός υπευθύνου επεξεργασίας και ενός εκτελούντος την επεξεργασία, και αφετέρου μεταξύ δυο υπευθύνων επεξεργασίας [βλ. Ενότητα Ι(Α)]. Μάλιστα, με την εκτελεστική απόφαση 2016/2297 της Επιτροπής[30] τροποποιήθηκαν οι αποφάσεις της που αφορούσαν στις εν λόγω ΤΣΡ, με αποτέλεσμα να ενισχυθούν οι εξουσίες των εθνικών ΑΠΔ ως προς την εποπτεία της διασυνοριακής ροής δεδομένων, συμπεριλαμβανομένης της εξουσίας να απαγορεύσουν ή

[29] Η ενημερωμένη λίστα των τρίτων χωρών για τις οποίες έχουν εκδοθεί αποφάσεις επάρκειας της Επιτροπής είναι διαθέσιμη στον ακόλουθο σύνδεσμο: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

[30] Εκτελεστική Απόφαση (ΕΕ) 2016/2297 της Επιτροπής, ο.π.

να αναστείλουν τη διαβίβαση δεδομένων σε τρίτες χώρες εάν θεωρήσουν ότι η διαβίβαση διενεργείται κατά παράβαση της ευρωπαϊκής ή εθνικής νομοθεσίας για την προστασία των δεδομένων[31].

Ως ανταπόκριση στην απόφαση *Schrems II* του ΔΕΕ, η Επιτροπή υιοθέτησε ένα νέο σύνολο δεσμών ΤΣΡ, οι οποίες δεν περιορίζονται στην προηγηθείσα διάκριση, και προσφέρουν περισσότερες δυνατότητες στα συμβαλλόμενα μέρη, όπως θα εξετάσουμε παρακάτω. Βέβαια, η εν λόγω απόφαση του Δικαστηρίου της ΕΕ αναγνώρισε μεν τις ΤΣΡ ως μηχανισμό διαβίβασης, αλλά διευκρίνισε ότι τα μέρη που διενεργούν τη διαβίβαση δεδομένων χρειάζεται να προβαίνουν σε προηγούμενη αξιολόγηση του νομικού καθεστώτος της τρίτης χώρας όπου διαβιβάζονται τα δεδομένα προσωπικού χαρακτήρα, για να διαπιστωθεί εάν παρέχει ένα ουσιαστικά ισοδύναμο επίπεδο προστασίας των δεδομένων με εκείνο που εγγυάται ο ΓΚΠΔ στην ΕΕ.

Όμως, οι ΤΣΡ της Επιτροπής δεν είναι οι μόνες αποδεκτές ρήτρες για τις συμβάσεις διαβίβασης δεδομένων. Ο Κανονισμός παρέχει στις εθνικές ΑΠΔ την εξουσία να υιοθετούν τις δικές τους τυποποιημένες ρήτρες προστασίας δεδομένων[32]. Η διαδικασία προβλέπει ότι οι εθνικές ΑΠΔ πρέπει αρχικά να υποβάλλουν τις προτεινόμενες τυποποιημένες ρήτρες ενώπιον του ΕΣΠΔ για έγκριση[33]. Εφόσον εγκριθούν, οι επιχειρήσεις που υπόκεινται στη δικαιοδοσία των εν λόγω ΑΠΔ, μπορούν να επωφεληθούν χρησιμοποιώντας τις ρήτρες αυτές ως βάση για τις διαβιβάσεις δεδομένων σε τρίτες χώρες. Η εξέλιξη αυτή μπορεί να είναι προπομπός για την ανάπτυξη πρότυπων ρητρών που εξυπηρετούν ανάγκες σε συγκεκριμένους τομείς, όπως η νεφοϋπολογιστική. Μια περαιτέρω επιλογή για τους υπευθύνους επεξεργασίας αποτελεί και η σύνταξη συμβατικών ρητρών από τα ίδια τα μέρη της διαβίβασης (υπευθύνους επεξεργασίας ή εκτελούντες την επεξεργασία) και η υποβολή αυτών στην αρμόδια ΑΠΔ προς έγκριση, σύμφωνα με το μηχανισμό συνεκτικότητας του ΓΚΠΔ[34].

[31] Βλ. περισσότερα Λωσταράκου, Κ. (2021) «Διεθνείς Διαβιβάσεις Δεδομένων υπό τον Νέο Κανονισμό». Σε Κοτσαλής Λ., Μενουδάκος Κ. επιμ. *Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων (GDPR) (Νομική διάσταση και πρακτική εφαρμογή)*. Αθήνα: Νομική Βιβλιοθήκη, σελ. 355 - 364.

[32] Άρθρο 46, παράγραφος 2, εδάφιο δ' του ΓΚΠΔ.

[33] Άρθρο 28, παράγραφος 8 του ΓΚΠΔ.

[34] Άρθρο 46, παράγραφος 3, στοιχείο α' και παράγραφος 4, σε συνδυασμό με το άρθρο 63 του ΓΚΠΔ.

(β) ***Δεσμευτικοί Εταιρικοί Κανόνες***

Οι Δεσμευτικοί Εταιρικοί Κανόνες (εφεξής «**ΔΕΚ**») αποτελούν ένα νομικά δεσμευτικό εσωτερικό κώδικα δεοντολογίας που λειτουργεί εντός ενός πολυεθνικού ομίλου, ο οποίος εφαρμόζεται στις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα από τις οντότητες του ομίλου εντός της ΕΕ προς τις οντότητες αυτού εκτός της ΕΕ.

Πρόκειται για νομικά δεσμευτικούς κανόνες προστασίας δεδομένων, οι οποίοι εγκρίνονται από την αρμόδια ΑΠΔ. Υπάρχουν δύο τύποι ΔΕΚ που μπορούν να εγκριθούν: α) οι ΔΕΚ για τους υπευθύνους επεξεργασίας που χρησιμοποιούνται από την οντότητα του ομίλου για τη διαβίβαση δεδομένων για τα οποία έχει την ευθύνη, όπως τα δεδομένα των εργαζομένων ή των προμηθευτών, και β) οι ΔΕΚ για τους εκτελούντες την επεξεργασία που χρησιμοποιούνται από οντότητες που ενεργούν ως εκτελούντες την επεξεργασία για άλλους υπευθύνους επεξεργασίας, οι οποίοι συνήθως προστίθενται ως παράρτημα στη σύμβασή τους με τον εκάστοτε υπεύθυνο επεξεργασίας[35]. Τα σχετικά με τη χρήση των ΔΕΚ για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα ορίζονται στο άρθρο 47 του ΓΚΠΔ.

Οι ΔΕΚ εγκρίνονται από την αρμόδια ΑΠΔ, σύμφωνα με το μηχανισμό συνεκτικότητας του ΓΚΠΔ[36]. Η αρμόδια ΑΠΔ ανακοινώνει το σχέδιο απόφασής της στο ΕΣΠΔ, το οποίο στη συνέχεια εκδίδει γνωμοδότηση σχετικά με τις ΔΕΚ. Όταν οι υπό εξέταση ΔΕΚ έχουν ολοκληρωθεί σε συμφωνία με τη γνώμη του ΕΣΠΔ, η αρμόδια ΑΠΔ προχωρά στην έγκριση αυτών, ενώ δεν απαιτείται η έκδοση εθνικής άδειας από κάθε ενδιαφερόμενη ΑΠΔ[37].

Ενδεικτικά και όχι περιοριστικά, οι ΔΕΚ θα πρέπει να διευκρινίζουν τη δομή του ομίλου, τις διαβιβάσεις και τις κατηγορίες δεδομένων που διαβιβάζονται, τη νομικά δεσμευτική φύση τους, την εφαρμογή των γενικών αρχών προστασίας, ιδίως τον περιορισμό του σκοπού, την ελαχιστοποίηση, τις περιορισμένες περιόδους αποθήκευσης, την ποιότητα των δεδομένων, την προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού, τον τρόπο επεξεργασίας των ειδικών κατηγοριών δεδομένων, τα μέτρα διασφάλισης, τα δικαιώματα

[35] Data Protection Commission (DPC) Ιρλανδίας, «*Transfers of Personal Data to Third Countries or International Organisations*», Διαθέσιμο στο: https://www.dataprotection.ie/en/organisations/international-transfers/transfers-personal-data-third-countries-or-international-organisations#_msocom_1.

[36] Άρθρα 47 και 63 του ΓΚΠΔ.

[37] Βλ. σχετικά Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, «*Διαβιβάσεις δεδομένων εκτός ΕΕ - Δεσμευτικοί Εταιρικοί Κανόνες (BCR)*». Διαθέσιμο στο: https://www.dpa.gr/el/enimerwtiko/thematikes_enotites/diavivaseis_ee/bcr.

των υποκειμένων των δεδομένων, την αποδοχή ευθύνης για τυχόν παραβιάσεις, τον τρόπο παροχής ενημέρωσης σχετικά με τους ΔΕΚ, τα καθήκοντα κάθε υπευθύνου προστασίας δεδομένων, τις διαδικασίες καταγγελίας, τους μηχανισμούς για τον έλεγχο της συμμόρφωσης, τους μηχανισμούς συνεργασίας και αναφοράς με τις ΑΠΔ, την κατάλληλη εκπαίδευση του προσωπικού και γενικά, ένα πλαίσιο ρυθμίσεων, που αντανακλούν όλο το περιεχόμενο, τη λογική και τους μηχανισμούς του ΓΚΠΔ[38].

(γ) *Κώδικες Δεοντολογίας*

Η χρήση των κωδίκων δεοντολογίας ως μηχανισμού διαβίβασης, υπό συγκεκριμένες συνθήκες, προβλέπεται στο άρθρο 40, παράγραφος 3 του ΓΚΠΔ. Οι κώδικες δεοντολογίας είναι προαιρετικοί και καθορίζουν συγκεκριμένους κανόνες προστασίας δεδομένων για ορισμένες κατηγορίες υπευθύνων επεξεργασίας και εκτελούντων την επεξεργασία. Μπορούν να αποτελέσουν ένα χρήσιμο και αποτελεσματικό εργαλείο λογοδοσίας, παρέχοντας λεπτομερή περιγραφή της πλέον ενδεδειγμένης, νόμιμης και ηθικής συμπεριφοράς σε έναν συγκεκριμένο τομέα.

Οι κώδικες δεοντολογίας προσομοιάζουν σε προγράμματα «αυτορρύθμισης» που χρησιμοποιούνται για να αποδεικνύουν στις αρμόδιες ΑΠΔ, αλλά και στο κοινό, ότι μια επιχείρηση τηρεί ορισμένους κανόνες προστασίας της ιδιωτικής ζωής και των δεδομένων προσωπικού χαρακτήρα[39]. Σύμφωνα με τον Κανονισμό τέτοιοι κώδικες μπορούν να εκπονούνται από ενώσεις ή άλλους φορείς που εκπροσωπούν υπευθύνους επεξεργασίας και εκτελούντες την επεξεργασία για τον προσδιορισμό της εφαρμογής του Κανονισμού όσον αφορά, μεταξύ άλλων, τη διαβιβάσεων δεδομένων σε τρίτες χώρες[40].

Οι εγκεκριμένοι κώδικες δεοντολογίας μπορούν να τηρούνται και από υπευθύνους επεξεργασίας ή εκτελούντες την επεξεργασία μη υπαγόμενους στον Κανονισμό, προκειμένου να παρέχονται οι κατάλληλες εγγυήσεις στο πλαίσιο των διαβιβάσεων δεδομένων σε τρίτες χώρες[41]. Για να θεωρηθούν δε ως επαρκείς διασφαλίσεις που επιτρέπουν διαβιβάσεις δεδομένων στο πλαίσιο του Κανονισμού, πρέπει να συνοδεύονται

[38] Άρθρο 45, παράγραφος 2 του ΓΚΠΔ.
[39] Βλ. Λωσταράκου, Κ. (2021) «Διεθνείς Διαβιβάσεις Δεδομένων υπό τον Νέο Κανονισμό». Σε Κοτσαλής Λ., Μενουδάκος Κ. επιμ. *Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων (GDPR) (Νομική διάσταση και πρακτική εφαρμογή)*, ο.π., σελ. 363.
[40] Άρθρο 40, παράγραφος 2 του ΓΚΠΔ.
[41] Άρθρο 40, παράγραφος 3 του ΓΚΠΔ.

από μηχανισμό με τον οποίο καθίστανται νομικά δεσμευτικοί για τους τρίτους, για παράδειγμα με την κατάρτιση σύμβασης μεταξύ ενός υπευθύνου επεξεργασίας στην ΕΕ και ενός εκτελούντος την επεξεργασία στις ΗΠΑ, ο οποίος συμφωνεί να εφαρμόσει τον εγκεκριμένο κώδικα δεοντολογίας. Οι προτεινόμενοι κώδικες δεοντολογίας πρέπει να υποβάλλονται προς έγκριση στην αρμόδια ΑΠΔ, ή στο ΕΣΠΔ όταν ο κώδικας δεοντολογίας αναφέρεται σε δραστηριότητες επεξεργασίας σε διάφορα κράτη-μέλη της ΕΕ[42].

(δ) ***Μηχανισμοί Πιστοποίησης***

Η πιστοποίηση ορίζεται από το Διεθνή Οργανισμό Τυποποίησης (International Organization for Standardization - ISO) ως *«η παροχή γραπτής διαβεβαίωσης (πιστοποιητικό) από ανεξάρτητο φορέα ότι ένα προϊόν, υπηρεσία ή σύστημα πληροί συγκεκριμένες απαιτήσεις ενός προτύπου»*[43]. Ως εκ τούτου, όπως προβλέπεται στο άρθρο 42, παράγραφος 2 του ΓΚΠΔ, μπορούν να αναπτυχθούν μηχανισμοί πιστοποίησης για την απόδειξη ύπαρξης κατάλληλων εγγυήσεων που παρέχονται από υπευθύνους επεξεργασίας και εκτελούντες την επεξεργασία σε τρίτες χώρες. Ταυτόχρονα, οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία θα αναλαμβάνουν δεσμεύσεις για την εφαρμογή των εγγυήσεων, συμπεριλαμβανομένων των διατάξεων για τα δικαιώματα των υποκειμένων των δεδομένων. Μάλιστα, όπως θα δούμε παρακάτω, ο αντίκτυπος της απόφασης *Schrems II* του ΔΕΕ επεκτείνεται και στην εφαρμογή αυτού του μηχανισμού διαβίβασης, με αποτέλεσμα τα μέρη της διαβίβασης να πρέπει να διασφαλίζουν από κοινού ότι τα διαβιβαζόμενα δεδομένα προσωπικού χαρακτήρα θα προστατεύονται από ένα ουσιαστικά ισοδύναμο επίπεδο προστασίας.

3. Παρεκκλίσεις (Επίπεδο 3)

Κατ' εξαίρεση, σε περίπτωση που δεν υφίσταται απόφαση επάρκειας της Επιτροπής, και δεν μπορεί να τύχει εφαρμογής κάποιος από τους μηχανισμούς διαβίβασης του άρθρου 46 του ΓΚΠΔ, οι παρεκκλίσεις του άρθρου 49 του Κανονισμού εφαρμόζονται ως έσχατη λύση όταν η διαβίβαση κρίνεται από τις καταστάσεις απολύτως απαραίτητη. Με την επιφύλαξη, λοιπόν, συγκεκριμένων προϋποθέσεων, τα ενδιαφερόμενα μέρη μπορούν να διαβιβάσουν δεδομένα προσωπικού χαρακτήρα βάσει ορισμένης παρέκκλισης και μόνο για

[42] Άρθρο 40, παράγραφος 5 και 6 του ΓΚΠΔ.
[43] Βλ. ISO, «FREQUENTLY ASKED QUESTIONS (FAQS) - GLOSSARY». Διαθέσιμο στο: https://www.iso.org/glossary.html.

συγκεκριμένες περιπτώσεις. Εντούτοις, οι παρεκκλίσεις της εν λόγω διάταξης πρέπει να ερμηνεύονται συσταλτικά και να αφορούν κυρίως δραστηριότητες επεξεργασίας που είναι περιστασιακού ή μη επαναλαμβανόμενου χαρακτήρα, καθώς αποτελούν εξαιρέσεις από τον γενικό κανόνα απαίτησης επαρκούς επιπέδου προστασίας ή επαρκών εγγυήσεων και αποτελεσματικών δικαιωμάτων. Οι παρεκκλίσεις επιτρέπουν τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε συγκεκριμένες περιπτώσεις, όπως βάσει ρητής συγκατάθεσης του υποκειμένου των δεδομένων, για την εκτέλεση ή τη σύναψη σύμβασης, για την άσκηση νομικών αξιώσεων ή για σημαντικούς λόγους δημοσίου συμφέροντος. Συνάγεται ότι για να μπορέσει κάποιος να στηρίξει τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε μια από τις παρεκκλίσεις του άρθρου 49 του ΓΚΠΔ, πρέπει να ελέγξει καταρχήν εάν η διαβίβαση πληροί τις αυστηρές προϋποθέσεις που ορίζει η εν λόγω διάταξη για καθεμία από αυτές. Μάλιστα, προς διευκόλυνση εκτίμησης πλήρωσης των εν λόγω προϋποθέσεων, το ΕΣΠΔ έχει εκδώσει σχετικές κατευθυντήριες γραμμές[44].

Γ. ΕΞΩΕΔΑΦΙΚΗ ΕΦΑΡΜΟΓΗ ΤΟΥ ΓΚΠΔ

Πέρα από την ισχυροποίηση του πλαισίου για τις διαβιβάσεις δεδομένων σε τρίτες χώρες, ο ΓΚΠΔ έφερε σημαντικές αλλαγές σε ότι αφορά την εξωεδαφική εφαρμογή του ενωσιακού πλαισίου για την προστασία των δεδομένων προσωπικού χαρακτήρα από μέρη που είναι εγκατεστημένα εκτός της ΕΕ **(1)**. Παρόλα αυτά, δεν κατάφερε να δώσει ορισμένη λύση στην «αθόρυβη σύγκρουση» μεταξύ των κανόνων που οριοθετούν το εδαφικό πεδίο εφαρμογής του Κανονισμού, και εκείνων που αφορούν στη διαβίβαση δεδομένων σε τρίτες χώρες **(2)**. Πρόκειται για ένα πρακτικό ζήτημα ιδιαίτερης σημασίας που χρήζει διευθέτησης, δεδομένης της επιδραστικής δύναμης της ΕΕ στο πλαίσιο του λεγόμενου «Brussels Effect» **(3)**.

1. Η καινοτομία του ΓΚΠΔ επί των γεωγραφικών ορίων της προστασίας

Οι κανόνες της Οδηγίας σχετικά με το εδαφικό πεδίο εφαρμογής της ενωσιακής νομοθεσίας περί δεδομένων προσωπικού χαρακτήρα περιλαμβάνονταν στο άρθρο 4 αυτής. Πιο συγκεκριμένα, η Οδηγία τύγχανε εφαρμογής στην επεξεργασία δεδομένων που πραγματοποιείται στο πλαίσιο των δραστηριοτήτων ενός υπευθύνου επεξεργασίας στο

[44] Βλ. Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (2018), *Κατευθυντήριες γραμμές 2/2018 αναφορικά με τις παρεκκλίσεις που προβλέπονται στο άρθρο 49 του Κανονισμού 2016/679*. Βέλγιο: Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. Διαθέσιμο στο: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_el.pdf.

έδαφος ενός κράτους-μέλους της ΕΕ[45], καθώς και στους υπευθύνους επεξεργασίας που δεν ήταν εγκατεστημένοι στο έδαφος της ΕΕ, αλλά χρησιμοποιούσαν εξοπλισμό, αυτοματοποιημένο ή μη, που βρίσκεται στο έδαφος ενός κράτους-μέλους της ΕΕ για την επεξεργασία δεδομένων προσωπικού χαρακτήρα[46].

Ο ΓΚΠΔ εγκατέλειψε το «κυνήγι του εξοπλισμού»[47] και έφερε αλλαγές στους κανόνες που αφορούν στην εφαρμογή της ενωσιακής νομοθεσίας στην επεξεργασία δεδομένων από μέρη εγκατεστημένα εκτός της ΕΕ, σηματοδοτώντας μια σημαντική εξέλιξη της νομοθεσίας της ΕΕ για την προστασία των δεδομένων. Ειδικότερα, σύμφωνα με το λεγόμενο κριτήριο της «στόχευσης»[48] του άρθρου 3, παράγραφος 2 του ΓΚΠΔ, ο Κανονισμός εφαρμόζεται α) στην επεξεργασία δεδομένων από υπευθύνους επεξεργασίας ή εκτελούντες την επεξεργασία που δεν είναι εγκατεστημένοι στην ΕΕ, όταν αυτή σχετίζεται με την προσφορά αγαθών ή υπηρεσιών σε υποκείμενα των δεδομένων που βρίσκονται στην ΕΕ, ανεξάρτητα από το εάν απαιτείται πληρωμή από αυτά, και β) στις δραστηριότητες επεξεργασίας από υπευθύνους επεξεργασίας και εκτελούντες την επεξεργασία χωρίς εγκατάσταση στην ΕΕ όσον αφορά την παρακολούθηση της συμπεριφοράς υποκειμένων των δεδομένων στην ΕΕ, εφόσον η εν λόγω συμπεριφορά λαμβάνει χώρα εντός της ΕΕ. Είναι χαρακτηριστικό ότι η εν λόγω διάταξη απαιτεί τα υποκείμενα των δεδομένων να βρίσκονται στην ΕΕ όταν λαμβάνει χώρα η σχετική δραστηριότητα (δηλαδή η προσφορά αγαθών ή υπηρεσιών ή η παρακολούθηση της συμπεριφοράς)[49].

Στο άρθρο 3 του ΓΚΠΔ αποτυπώνεται η πρόθεση του νομοθέτη να διασφαλίσει την πλήρη προστασία των δικαιωμάτων των υποκειμένων των δεδομένων στην ΕΕ και να

[45] Άρθρο 4, παράγραφος 1, στοιχείο α' της Οδηγίας.
[46] Άρθρο 4, παράγραφος 1, στοιχείο γ' της Οδηγίας.
[47] Κατ' αναλογία προς το «κυνήγι του εξυπηρετητή», βλ. Μήτρου, Λ. (2015), «Προστασία Προσωπικών Δεδομένων και υπολογιστικό νέφος», ο.π., σελ. 534 - 549.
[48] Βλ. Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (2019), *Κατευθυντήριες γραμμές 3/2018 σχετικά με το εδαφικό πεδίο εφαρμογής του ΓΚΠΔ (άρθρο 3).* Βέλγιο: Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. Διαθέσιμο στο: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_consultation_el.pdf, σελ. 16 - 27.
[49] Ο ΓΚΠΔ δεν προϋποθέτει κάποιο νομικό δεσμό του υποκειμένου των δεδομένων με την ΕΕ, όπως ιθαγένεια ή συνήθη διαμονή, ώστε να εφαρμόζονται οι διατάξεις του, σύμφωνα με το άρθρο 3, παράγραφος 2. Αρκεί το υποκείμενο των δεδομένων να βρίσκεται εντός της ΕΕ για οποιονδήποτε λόγο. Βλ. σχετικά Παναγοπούλου-Κουτνατζή, Φ. (2019), «Συνταγματικές προεκτάσεις των μηχανισμών διευρύνσεως της προστασίας δεδομένων προσωπικού χαρακτήρα πέραν της ΕΕ: Εξωεδαφική εφαρμογή του ΓΚΠΔ και διασυνοριακή διαβίβαση δεδομένων», *ΤΝΠ QUALEX, ΔiΜΕΕ*, 4/2019, σελ. 504 - 520.

δημιουργήσει, από πλευράς απαιτήσεων προστασίας των δεδομένων, ισότιμους όρους ανταγωνισμού για τις επιχειρήσεις που δραστηριοποιούνται στις αγορές της ΕΕ, σε ένα πλαίσιο παγκόσμιας κυκλοφορίας δεδομένων. Προς τούτο, το ΕΣΠΔ δημοσίευσε σχετικές κατευθυντήριες γραμμές[50], όπου μεταξύ άλλων, αποσαφήνισε ότι σκοπός της εφαρμογής του άρθρου 3 είναι να προσδιορίζεται εάν μια συγκεκριμένη δραστηριότητα επεξεργασίας, και όχι ένα πρόσωπο (νομικό ή φυσικό), εμπίπτει στο πεδίο εφαρμογής του ΓΚΠΔ. Ως εκ τούτου, μια συγκεκριμένη δραστηριότητα επεξεργασίας δεδομένων προσωπικού χαρακτήρα από υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία μπορεί να εμπίπτει στο πεδίο εφαρμογής του Κανονισμού, χωρίς να ισχύει το ίδιο και για τις υπόλοιπες δραστηριότητες επεξεργασίας αυτού.

2. Η «αθόρυβη σύγκρουση» της εξωεδαφικότητας με τους κανόνες διαβίβασης δεδομένων σε τρίτες χώρες

Όπως είδαμε στην υποενότητα Β της παρούσας ενότητας, οι κανόνες για τη διαβίβαση δεδομένων σε χώρες εκτός της ΕΕ περιλαμβάνονται στο πέμπτο κεφάλαιο του ΓΚΠΔ. Στόχος αυτού του κεφαλαίου είναι να διασφαλίσει ότι τα διαβιβαζόμενα σε τρίτη χώρα δεδομένα προσωπικού χαρακτήρα εξακολουθούν να χαίρουν ενός επιπέδου προστασίας ουσιαστικά ισοδύναμου με εκείνο που παρέχεται στην ΕΕ. Προς τούτο, τα μέρη υποχρεούνται να θέσουν σε εφαρμογή τον κατάλληλο, κατά περίπτωση, μηχανισμό διαβίβασης. Εφόσον ο πρώτος κατά σειρά μηχανισμός, ήτοι η απόφαση επάρκειας της Επιτροπής, δεν είναι διαθέσιμος, τα μέρη μπορούν να βασιστούν σε έναν από τους μηχανισμούς διαβίβασης του άρθρου 46 του ΓΚΠΔ, όπως για παράδειγμα τις ΤΣΡ ή τους ΔΕΚ. Εναλλακτικά, και σε εξαιρετικές μόνο περιστάσεις, τα μέρη μπορούν να επικαλεστούν μία από τις παρεκκλίσεις του άρθρου 49 του ΓΚΠΔ.

Ήδη, όμως, από την ψήφιση της Οδηγίας επικρατούσε σύγχυση ως προς τη σχέση μεταξύ των κανόνων που οριοθετούν το εδαφικό πεδίο εφαρμογής του ενωσιακού πλαισίου στην επεξεργασία δεδομένων από μέρη που είναι εγκατεστημένα εκτός της ΕΕ (επί του παρόντος διέπονται από το άρθρο 3 παράγραφος 2 του ΓΚΠΔ), και εκείνων που αφορούν στη διαβίβαση δεδομένων σε τρίτες χώρες (επί του παρόντος διέπονται από το πέμπτο κεφάλαιο του ΓΚΠΔ). Και τούτο διότι ο ΓΚΠΔ δεν περιέχει καμία διάταξη που να ρυθμίζει την αλληλεπίδραση

[50] Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (2019), «*Κατευθυντήριες γραμμές 3/2018 σχετικά με το εδαφικό πεδίο εφαρμογής του ΓΚΠΔ (άρθρο 3)*», ο.π.

μεταξύ του εδαφικού πεδίου εφαρμογής και των κανόνων διαβίβασης δεδομένων σε τρίτες χώρες, είτε ρητά είτε σιωπηρά. Αυτό έχει ως αποτέλεσμα και τα δύο σύνολα κανόνων να εφαρμόζονται όταν ενεργοποιούνται οι προϋποθέσεις για την εφαρμογή τους, πράγμα που σημαίνει ότι μπορεί να εφαρμόζονται και ταυτόχρονα σε ορισμένες περιπτώσεις. Η «αθόρυβη» αυτή σύγκρουση κατέστη μάλιστα «ηχηρή» με την πρόσφατη νομολογία του ΔΕΕ, η οποία έθεσε αυστηρότερες υποχρεώσεις σε ότι αφορά τη διαβίβαση των δεδομένων σε τρίτες χώρες.

Στις 18 Νοεμβρίου 2021 το ΕΣΠΔ εξέδωσε τις υπ'αριθμ. 05/2021 κατευθυντήριες γραμμές που σηματοδοτούν την πρώτη απόπειρα εποπτικής αρχής να γνωμοδοτήσει με σκοπό να αποσαφηνιστεί η αλληλεπίδραση μεταξύ του εδαφικού πεδίου εφαρμογής του ΓΚΠΔ και των κανόνων διαβίβασης δεδομένων σε τρίτες χώρες[51]. Οι εν λόγω κατευθυντήριες γραμμές συντάχθηκαν για να βοηθήσουν τους υπευθύνους επεξεργασίας και τους εκτελούντες την επεξεργασία στην ΕΕ να προσδιορίσουν εάν οι δραστηριότητες επεξεργασίας δεδομένων που διενεργούν, συνιστούν διαβίβαση σε τρίτη χώρα και, εν συνεχεία, εάν απαιτούνται συμπληρωματικά μέτρα για να πραγματοποιηθεί νόμιμα η διαβίβαση.

Καθώς ο ΓΚΠΔ δεν παρέχει ορισμό της διαβίβασης δεδομένων προσωπικού χαρακτήρα σε τρίτη χώρα, το ΕΣΠΔ προέβη στην αποτύπωση των ακόλουθων κριτηρίων, τα οποία θα πρέπει να συντρέχουν σωρευτικά για να θεωρηθεί μια επεξεργασία δεδομένων προσωπικού χαρακτήρα ως «διαβίβαση»: (1) ο εξαγωγέας δεδομένων (υπεύθυνος επεξεργασίας ή εκτελών την επεξεργασία) υπόκειται στο ΓΚΠΔ για τη συγκεκριμένη επεξεργασία, (2) ο εξαγωγέας δεδομένων διαβιβάζει ή καθιστά διαθέσιμα τα δεδομένα προσωπικού χαρακτήρα στον εισαγωγέα δεδομένων (άλλος υπεύθυνος επεξεργασίας ή εκτελών την επεξεργασία), και (3) ο εισαγωγέας δεδομένων βρίσκεται σε τρίτη χώρα[52]. Η άποψη του ΕΣΠΔ είναι ότι όλες οι διαβιβάσεις δεδομένων προσωπικού χαρακτήρα σε εισαγωγείς δεδομένων εκτός της ΕΕ πρέπει να συμμορφώνονται με το πέμπτο κεφάλαιο του ΓΚΠΔ και

[51] Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (2021), *Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR*. Βέλγιο: Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. Διαθέσιμο στο: https://edpb.europa.eu/system/files/2021-11/edpb_guidelinesinterplaychapterv_article3_adopted_en.pdf.

[52] Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (2021), *Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR*, ο.π., σελ. 4.

να χρησιμοποιούν ένα μηχανισμό διαβίβασης, ακόμη και εάν ο εισαγωγέας δεδομένων υπόκειται ήδη στο ΓΚΠΔ σύμφωνα με το άρθρο 3 του ΓΚΠΔ[53].

Αξίζει, ωστόσο, να σημειωθεί ότι σε αδημοσίευτο σχέδιο των υπ'αριθμ. 3/2018 κατευθυντήριων γραμμών του, το ΕΣΠΔ διατύπωνε τη θέση ότι το πέμπτο κεφάλαιο δεν θα πρέπει να εφαρμόζεται σε περιπτώσεις όπου ο ΓΚΠΔ εφαρμόζεται απευθείας βάσει του άρθρου 3. Πιο συγκεκριμένα, το σχέδιο ανέφερε τα εξής: «*… Η σχέση μεταξύ του εδαφικού πεδίου εφαρμογής του ΓΚΠΔ, όπως ορίζεται στο άρθρο 3, και των διατάξεων του κεφαλαίου V μπορεί συνεπώς να περιγραφεί ως συμπληρωματική ή αντισταθμιστική… Κατά συνέπεια, όταν η επεξεργασία δεδομένων προσωπικού χαρακτήρα που πραγματοποιείται από τον αποδέκτη (υπεύθυνος επεξεργασίας ή εκτελών την επεξεργασία) σε τρίτη χώρα καλύπτεται από το πεδίο εφαρμογής του ΓΚΠΔ σύμφωνα με το άρθρο 3, δεν υπάρχει έλλειψη προστασίας και το κεφάλαιο V δεν εφαρμόζεται στη διαβίβαση των δεδομένων στον αποδέκτη των δεδομένων. Αντιθέτως, όταν η επεξεργασία δεδομένων προσωπικού χαρακτήρα που πραγματοποιείται από τον αποδέκτη των δεδομένων (υπεύθυνος επεξεργασίας ή εκτελών την επεξεργασία) σε τρίτη χώρα δεν εμπίπτει στο άρθρο 3 του ΓΚΠΔ και, ως εκ τούτου, δεν επωφελείται από την προστασία του ΓΚΠΔ, η διαβίβαση των δεδομένων πρέπει να υπόκειται στους όρους του κεφαλαίου V*»[54]. Όμως, το απόσπασμα αυτό δεν συμπεριλήφθηκε στην τελική έκδοση των εν λόγω κατευθυντήριων γραμμών, οι οποίες περιλαμβάνουν μόνο μερικές σύντομες αναφορές στο πέμπτο κεφάλαιο του ΓΚΠΔ, χωρίς καμία αναφορά στη σχέση μεταξύ του εδαφικού πεδίου εφαρμογής και των κανόνων διαβίβασης δεδομένων σε τρίτες χώρες, με μόνη εξαίρεση την ακόλουθη δήλωση: «*Το ΕΣΠΔ θα εξετάσει επίσης περαιτέρω την αλληλεπίδραση μεταξύ της εφαρμογής του εδαφικού πεδίου εφαρμογής του ΓΚΠΔ, κατά τα οριζόμενα στο άρθρο 3, και των διατάξεων σχετικά με τις διεθνείς διαβιβάσεις δεδομένων σύμφωνα με το κεφάλαιο V. Εάν κριθεί αναγκαίο, μπορεί να εκδοθεί πρόσθετη καθοδήγηση επί του θέματος αυτού*»[55].

[53] Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (2021), *Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR*, ο.π., σελ. 8.
[54] Βλ. Kuner, C. (2021), «Territorial Scope and Data Transfer Rules in the GDPR: Realising the EU's Ambition of Borderless Data Protection», *University of Cambridge Faculty of Law Research Paper No. 20/2021*. Διαθέσιμο στο: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3827850.
[55] Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (2019), *Κατευθυντήριες γραμμές 3/2018 σχετικά με το εδαφικό πεδίο εφαρμογής του ΓΚΠΔ (άρθρο 3)*, ο.π., σελ. 28.

Όπως θα δούμε στην τρίτη ενότητα της παρούσας μελέτης, τον Ιούνιο του 2021, η Επιτροπή εισήγαγε, υπό το φως της απόφασης *Schrems II* του ΔΕΕ, ένα νέο σύνολο δεσμών ΤΣΡ, οι οποίες αποτελούν έναν από τους προτεινόμενους μηχανισμούς διαβίβασης σύμφωνα με το πέμπτο κεφάλαιο του ΓΚΠΔ. Στην αιτιολογική σκέψη 7 της εκτελεστικής απόφασης της Επιτροπής[56] διευκρινίζεται ότι οι νέες ΤΣΡ προορίζονται για χρήση «*με την επιφύλαξη της ερμηνείας της έννοιας της διεθνούς μεταφοράς στον κανονισμό (ΕΕ) 2016/679. Οι τυποποιημένες συμβατικές ρήτρες μπορούν να χρησιμοποιούνται για τις εν λόγω διαβιβάσεις μόνο στο βαθμό που η επεξεργασία από τον εισαγωγέα δεν εμπίπτει στο πεδίο εφαρμογής του κανονισμού (ΕΕ) 2016/679*». Πρακτικά αυτό σημαίνει ότι στο βαθμό που ο εισαγωγέας δεδομένων εκτός της ΕΕ εμπίπτει στο εδαφικό πεδίο εφαρμογής του ΓΚΠΔ, οι νέες ΤΣΡ δεν μπορούν να χρησιμοποιηθούν για τη νομιμοποίηση της διαβίβασης δεδομένων προς αυτόν. Αυτό, όμως, έρχεται σε αντίθεση με τα κριτήρια που έθεσε το ΕΣΠΔ στις υπ'αριθμ. 05/2021 κατευθυντήριες γραμμές, σύμφωνα με τα οποία ο εισαγωγέας δεδομένων πρέπει να βρίσκεται σε τρίτη χώρα, ανεξάρτητα από το εάν καλύπτεται από το ΓΚΠΔ σε ότι αφορά την υπό κρίση επεξεργασία με βάση το άρθρο 3 του ΓΚΠΔ. Όπως είναι αναμενόμενο, αυτό μπορεί να οδηγήσει σε σύγχυση ως προς το εάν η χρήση κατάλληλων εγγυήσεων για τη διαβίβαση δεδομένων βάσει του άρθρου 46 ΓΚΠΔ, όπως οι ΤΣΡ, είναι δυνατή σε περιπτώσεις που το μέρος που λαμβάνει τα δεδομένα υπόκειται επίσης στο ΓΚΠΔ. Μάλιστα, η διατύπωση «*με επιφύλαξη*» που επιλέγει η Επιτροπή στην εν λόγω εκτελεστική απόφαση, καθιστά σαφές ότι η Επιτροπή άφησε την ερμηνεία των διαβιβάσεων στο ΕΣΠΔ ή κατ' επέκταση στο Δικαστήριο της ΕΕ[57]. Επομένως, κατά τη γνώμη του γράφοντος, μέχρι την έκδοση τυχόν συμπληρωματικών οδηγιών από το ΕΣΠΔ ή σχετικής νομολογίας του ΔΕΕ, το βάρος αξιολόγησης και επιλογής πέφτει στους ώμους του εξαγωγέα δεδομένων, ο οποίος σε

[56] Ευρωπαϊκή Επιτροπή (2021), *Εκτελεστική Απόφαση (ΕΕ) 2021/914 της Επιτροπής της 4ης Ιουνίου 2021 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*. Βέλγιο: Ευρωπαϊκή Επιτροπή. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32021D0914.

[57] Βλ. Ilan, D., Kristensen, G., Ka Chun, L., Gerlach, N. και Mammì Borruto, F. (2021), «New Standard Contractual Clauses for Data Transfers under the GDPR - New Changes, New Questions?», *Cleary Gottlieb*. Διαθέσιμο στο: https://www.clearygottlieb.com/-/media/files/alert-memos-2021/the-new-commission-sccs-for-data-transfers-under-gdpr-more-questions-than-answers.pdf.

περίπτωση αμφιβολίας, όπως είναι αναμενόμενο, θα προβεί σε ταυτόχρονη εφαρμογή αμφότερων κανόνων[58].

3. Ο ενωσιακός «ιμπεριαλισμός» της πληροφοριακής ιδιωτικότητας

Το ρυθμιστικό πλαίσιο που καθιερώθηκε για τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες, αρχικά από την Οδηγία και εν συνεχεία από τον Κανονισμό, αποτυπώνει την προσπάθεια της ΕΕ να ασκήσει επιρροή στη νομοθεσία τρίτων χωρών, μέσω της επιβολής των ενωσιακών κανόνων, ώστε να δημιουργηθεί ένα ενιαίο και ασφαλές πεδίο ροής δεδομένων παγκοσμίως. Πρόκειται για το λεγόμενο «ιμπεριαλισμό της πληροφοριακής ιδιωτικότητας»[59] ή «Brussels Effect»[60] που καθιστά την ΕΕ μια επιδραστική υπερδύναμη που διαμορφώνει τον κόσμο κατ' εικόνα και ομοίωσή της, για την ανάπτυξη του οποίου, πέρα από τις νομοθετικές πράξεις της ΕΕ, καθοριστικό ρόλο έπαιξε και η νομολογία του ΔΕΕ.

Είναι χαρακτηριστικό ότι ακόμη και πριν από την έναρξη ισχύος του ΓΚΠΔ, το ΔΕΕ είχε ήδη εκδώσει ορισμένες αποφάσεις με μεγάλη επιρροή στον τομέα της προστασίας των δεδομένων, όπως η απόφαση *Google Spain*[61], η οποία έκρινε ότι τα φυσικά πρόσωπα δύνανται να υποχρεώσουν τις μηχανές αναζήτησης να αφαιρέσουν συνδέσμους που αφορούν σε

---

[58] Άλλωστε, σύμφωνα με το ΕΣΠΔ, σε περίπτωση που ένας εξαγωγέας δεδομένων επιθυμεί να χρησιμοποιήσει τις ΤΣΡ ως μηχανισμό διαβίβασης, ενώ ο εισαγωγέας δεδομένων εμπίπτει ήδη στο εδαφικό πεδίο εφαρμογής του άρθρου 3, παράγραφος 2 του ΓΚΠΔ, απαιτείται πιθανότατα ένα νέο σύνολο ΤΣΡ, για το οποίο θα πρέπει να ληφθεί υπόψη η συνθήκη του άρθρου 3, παράγραφος 2 του ΓΚΠΔ προκειμένου να μην επικαλύπτονται οι υποχρεώσεις του ΓΚΠΔ, αλλά μάλλον να συμπληρωθούν τα στοιχεία και οι αρχές που «λείπουν», ώστε να καλυφθούν τα κενά που σχετίζονται με τη νομοθεσία της τρίτης χώρας όπου βρίσκεται ο εισαγωγέας δεδομένων. Βλ. Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (2021), *Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR*, ο.π, σελ. 9.

[59] Βλ. Svantesson, D. J. B. (2013), «A "layered approach" to the extraterritoriality of data privacy laws», *International Data Privacy Law*. Διαθέσιμο στο: https://www.researchgate.net/publication/275003577_A_layered_approach_to_the_extraterritoriality_of_data_privacy_laws, και Μήτρου, Λ. (2017), *Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων*. Αθήνα: Σάκκουλας, σελ. 51 - 54.

[60] Βλ. Bygrave, L. A. (2021), «The 'Strasbourg Effect' on data protection in light of the 'Brussels Effect': Logic, mechanics and prospects», *Computer Law & Security Review*, Volume 40. Διαθέσιμο στο: https://www.sciencedirect.com/science/article/pii/S0267364920300650?via%3DihubT, και Christakis, T. (2020), «'European Digital Sovereignty': Successfully Navigating Between the 'Brussels Effect' and Europe's Quest for Strategic Autonomy». Διαθέσιμο στο: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3748098. Ο όρος «Brussels Effect» επινοήθηκε από τη νομικό Anu Bradford στο πολυσυζητημένο βιβλίο «*The Brussels Effect: How the European Union Rules the World*» από τις εκδόσεις Oxford University Press*:*

[61] ΔΕΕ, C-131/12, *Google Spain SL και Google Inc. κατά Agencia Española de Protección de Datos (AEPD) και Mario Costeja González*, 13 Μαΐου 2014. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A62012CJ0131&msclkid=dfab6b55c4c311ecae40f26a8ea11235.

προσωπικές τους πληροφορίες που δεν εμπίπτουν στο δημόσιο συμφέρον, γεννώντας το αποκαλούμενο «δικαίωμα στη λήθη».

Η απόφαση *Schrems II* του ΔΕΕ, την οποία θα εξετάσουμε αναλυτικά παρακάτω, πέρα από την ακύρωση της απόφασης επάρκειας της Επιτροπής για την ασπίδα προστασίας της ιδιωτικής ζωής ΕΕ - ΗΠΑ[62] (εφεξής «**απόφαση για την Ασπίδα Προστασίας της Ιδιωτικής Ζωής**»), που επηρέασε καθοριστικά τις μελλοντικές διαβιβάσεις δεδομένων από την ΕΕ στις ΗΠΑ, είχε επίσης ως συνέπεια οι εθνικές ΑΠΔ τρίτων χωρών να αμφισβητήσουν τις δικές τους συμφωνίες για τη διαβίβαση δεδομένων στις ΗΠΑ. Για παράδειγμα, στις 8 Σεπτεμβρίου 2020, ο Ομοσπονδιακός Επίτροπος Προστασίας Δεδομένων και Πληροφοριών της Ελβετίας δήλωσε ότι η απόφαση επάρκειας για τη διαβίβαση δεδομένων μεταξύ Ελβετίας και ΗΠΑ (ασπίδα προστασίας της ιδιωτικής ζωής Ελβετία - ΗΠΑ)[63] δεν προστατεύει κατάλληλα τις πληροφορίες των πολιτών όταν αυτές διαβιβάζονται στις ΗΠΑ. Ειδικότερα, ο Ομοσπονδιακός Επίτροπος Προστασίας Δεδομένων και Πληροφοριών της Ελβετίας διαπίστωσε ότι η προαναφερθείσα απόφαση επάρκειας δεν ανταποκρίνεται στα πρότυπα της ομοσπονδιακής νομοθεσίας της χώρας για την προστασία των δεδομένων μετά από αξιολόγηση της ασπίδας προστασίας της ιδιωτικής ζωής Ελβετία - ΗΠΑ επί τη βάσει της πρόσφατης κρίσης του Δικαστηρίου της ΕΕ κατά της απόφασης για την Ασπίδα Προστασίας της Ιδιωτικής Ζωής[64].

Βέβαια, η ιμπεριαλιστική αυτή τάση της ΕΕ ενέχει μια σημαντική αντίφαση στον πυρήνα της, δεδομένου ότι το αυστηρό πλαίσιο προστασίας των δεδομένων προσωπικού χαρακτήρα, πολλώ δε μάλλον η υποχρεωτική αξιολόγηση του επιπέδου παρακολούθησης των δεδομένων προσωπικού χαρακτήρα από τις κυβερνητικές αρχές της τρίτης χώρας, δεν εφαρμόζεται στο εσωτερικό της ΕΕ, αφού σύμφωνα με τη Συνθήκη για τη λειτουργία της

[62] Ευρωπαϊκή Επιτροπή (2016), *Εκτελεστική Απόφαση (ΕΕ) 2016/1250 της Επιτροπής της 12ης Ιουλίου 2016 βάσει της οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την επάρκεια της προστασίας που παρέχεται από την ασπίδα προστασίας της ιδιωτικής ζωής ΕΕ - ΗΠΑ. Βέλγιο: Ευρωπαϊκή Επιτροπή.* Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016D1250&from=NL.

[63] Ευρωπαϊκή Επιτροπή (2020), *Απόφαση της Επιτροπής, της 26ης Ιουλίου 2000, δυνάμει της οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την επάρκεια της προστασίας των δεδομένων προσωπικού χαρακτήρα που παρέχεται στην Ελβετία.* Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32000D0518&from=EL.

[64] Ομοσπονδιακός Επίτροπος Προστασίας Δεδομένων και Πληροφοριών της Ελβετίας (2020), *FDPIC considers CH-US Privacy Shield does not provide adequate level of data protection*. Ελβετία: Ομοσπονδιακός Επίτροπος Προστασίας Δεδομένων και Πληροφοριών της Ελβετίας. Διαθέσιμο στο: https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-80318.html.

Ευρωπαϊκής Ένωσης (εφεξής «**Συνθήκη της ΕΕ**») η εθνική ασφάλεια ανήκει στην αποκλειστική αρμοδιότητα των κρατών-μελών της ΕΕ[65]. Το γεγονός αυτό ευλόγως γεννά ερωτηματικά ως προς την φερεγγυότητα και σκοπιμότητα του «Brussels Effect». Μάλιστα, η εν λόγω αντίφαση επισημαίνεται, όπως θα δούμε παρακάτω, στη Λευκή Βίβλο του Υπουργείου Εμπορίου των ΗΠΑ[66], ως απάντηση επί των ισχυρισμών του ΔΕΕ στην απόφαση *Schrems II*. Κατά πόσο είναι εφικτό μια τρίτη χώρα να δεχτεί άκριτα τους αυστηρούς όρους της ΕΕ, κυρίως δε τους επιβεβλημένους περιορισμούς στο εσωτερικό της σύστημα ασφαλείας, όταν οι όροι αυτοί δεν εφαρμόζονται πρώτιστα στα ίδια τα κράτη-μέλη της ΕΕ; Πρόκειται για ένα ερώτημα που, κατά τη γνώμη του γράφοντος, αποτελεί τη χρυσή τομή στην ενωσιακή προσπάθεια ανάπτυξης ενός ενιαίου και ασφαλούς οικουμενικού ιστού για τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα.

[65] Άρθρο 4, παράγραφος 2 της Συνθήκης για τη Λειτουργία της Ευρωπαϊκής Ένωσης: «*Η Ένωση σέβεται την ισότητα των κρατών μελών ενώπιον των Συνθηκών καθώς και την εθνική τους ταυτότητα που είναι συμφυής με τη θεμελιώδη πολιτική και συνταγματική τους δομή, στην οποία συμπεριλαμβάνεται η περιφερειακή και τοπική αυτοδιοίκηση. Σέβεται τις ουσιώδεις λειτουργίες του κράτους, ιδίως δε τις λειτουργίες που αποβλέπουν στη διασφάλιση της εδαφικής ακεραιότητας, τη διατήρηση της δημόσιας τάξης και την προστασία της εθνικής ασφάλειας. Ειδικότερα, η εθνική ασφάλεια παραμένει στην ευθύνη κάθε κράτους μέλους*». Διαθέσιμο στο: https://op.europa.eu/el/publication-detail/-/publication/9e8d52e1-2c70-11e6-b497-01aa75ed71a1?msclkid=2f1215adc58611ec9ffeb2d1d687b9d6.

[66] United States Department of Commerce (2020), *Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II*. Ουάσιγκτον, ΗΠΑ: United States Department of Commerce. Διαθέσιμο στο: https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF.

ΕΝΟΤΗΤΑ ΙΙ - Η ΕΝΩΣΙΑΚΗ ΠΡΟΣΠΑΘΕΙΑ ΕΛΕΓΧΟΥ ΤΟΥ ΟΙΚΟΥΜΕΝΙΚΟΥ ΙΣΤΟΥ ΔΙΑΒΙΒΑΣΕΩΝ

Έχοντας κατανοήσει το μηχανισμό και τη λειτουργία του ενωσιακού πλαισίου για τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες, στην παρούσα ενότητα θα ανατρέξουμε το ιστορικό της πολυετούς δικαστικής διαμάχης *Schrems* **(Α)** αναδεικνύοντας τα σημαντικότερα πορίσματα της απόφασης *Schrems I*, η οποία κήρυξε ανίσχυρη την απόφαση Ασφαλούς Λιμένα **(Β),** και εν συνεχεία εξετάζοντας συνοπτικά το σκεπτικό της πρόσφατης ρηξικέλευθης απόφασης *Schrems II* που αφαίρεσε από τη φαρέτρα των μηχανισμών για τις διατλαντικές διαβιβάσεις δεδομένων την απόφαση επάρκειας για την Ασπίδα Προστασίας της Ιδιωτικής Ζωής **(Γ)**.

Α. ΤΟ ΙΣΤΟΡΙΚΟ ΤΗΣ ΠΟΛΥΚΡΟΤΗΣ ΥΠΟΘΕΣΗΣ SCHREMS

Η πολυετής δικαστική διαμάχη *Schrems* έχει ως αφετηρία την καταγγελία του ακτιβιστή Max Schrems[67], Αυστριακού χρήστη του facebook, προς τον Ιρλανδό Επίτροπο Προστασίας Δεδομένων (εφεξής **«Ιρλανδός Επίτροπος»**), το 2013, που αφορούσε στη διαβίβαση δεδομένων προσωπικού χαρακτήρα που τον αφορούν από την Facebook Ireland Ltd σε διακομιστές που ανήκουν στη μητρική της εταιρεία, Facebook Inc., οι οποίοι είναι εγκατεστημένοι στις ΗΠΑ, όπου τα δεδομένα αυτά αποτελούν αντικείμενο επεξεργασίας. Ο Max Schrems υποστήριξε, μεταξύ άλλων, ότι το δίκαιο και οι πρακτικές των ΗΠΑ δεν προσφέρουν επαρκή προστασία έναντι της πρόσβασης των αμερικανικών δημοσίων αρχών στα δεδομένα που διαβιβάζονται και αποθηκεύονται εκεί, παραβιάζοντας έτσι τον ΓΚΠΔ και, γενικότερα, το δίκαιο της ΕΕ[68]. Λόγω αυτού, ο Max Schrems ζητούσε από τον Ιρλανδό

[67] Το παρασκήνιο της καταγγελίας: Ο Max Schrems ευρισκόμενος στις ΗΠΑ με πρόγραμμα ανταλλαγής σπουδαστών παρακολούθησε την ομιλία ενός δικηγόρου της Facebook που αφορούσε στο πώς και γιατί σύμφωνα με τους νόμους των ΗΠΑ, η εταιρεία συλλέγει κάθε πληροφορία για τους χρήστες της. Η εν λόγω ανάλυση απασχόλησε ιδιαίτερα τον Max Schrems, ο οποίος αποφάσισε να κάνει μία εργασία για το επίπεδο προστασίας των δεδομένων προσωπικού χαρακτήρα των πολιτών της ΕΕ που διαβιβάζονται στις ΗΠΑ «κάτω από τον μανδύα» της απόφασης Ασφαλούς Λιμένα. Επιστρέφοντας στην ΕΕ και βασιζόμενος στο δικαίωμα πρόσβασης, ζήτησε και έλαβε όλα τα δεδομένα που είχε η Facebook και τον αφορούσαν. Το αποτέλεσμα ήταν 1.200 σελίδες με δεδομένα που περιείχαν κάθε του κίνηση στο ή μέσω του facebook, κι έτσι αποφάσισε να κινηθεί νομικά εναντίον της Facebook με το σκεπτικό ότι παραβίαζε την ενωσιακή νομοθεσία για την προστασία των δεδομένων προσωπικού χαρακτήρα και συνακόλουθα τα θεμελιώδη ανθρώπινα δικαιώματα. Πηγή: Τάσσης Σ. (2015), «Σημείωμα στην ΔΕΕ υπόθ. C-362/14, απόφ. της 6.10.2015 - ΟΙ ΗΠΑ δεν αποτελούν πλέον «ασφαλές λιμάνι» για τα προσωπικά δεδομένα των πολιτών της ΕΕ», *ΤΝΠ QUALEX, ΔiΜΕΕ*, 3/2015, σελ. 508 - 512.

[68] Βλ. σχετικά Rotenberg, M. (2020) «Schrems II, from Snowden to China: Toward a new alignment on transatlantic data protection», *European Law Journal*, Volume 26, Issue 1-2, σελ. 141-152. Διαθέσιμο στο: https://doi.org/10.1111/eulj.12370.

Επίτροπο να ασκήσει τις αρμοδιότητες που έχει εκ του νόμου, απαγορεύοντας στη Facebook Ireland Ltd να διαβιβάζει στις ΗΠΑ τα δεδομένα προσωπικού χαρακτήρα που τον αφορούν. Αφορμή των ισχυρισμών του Max Schrems αποτέλεσε αναμφίβολα ο χείμαρρος αποκαλύψεων που είχε προηγηθεί εκείνη την περίοδο από τον Edward Snowden, πρώην υπάλληλο (διαχειριστή συστημάτων) της Υπηρεσίας Εθνικής Ασφάλειας των ΗΠΑ (National Security Agency, εφεξής «**NSA**»), σχετικά με τη μαζική και χωρίς διάκριση επεξεργασία από τις αμερικανικές μυστικές υπηρεσίες (ιδίως της NSA και του Ομοσπονδιακού Γραφείου Ερευνών - Federal Bureau of Investigation - εφεξής «**FBI**») δεδομένων προσωπικού χαρακτήρα που αφορούν σε χρήστες των υπηρεσιών που παρέχουν οι κολοσσοί της πληροφορικής (όπως Facebook, Google και Microsoft)[69]. Ο Max Schrems αναφέρθηκε σε έγγραφα της NSA, δημοσιευμένα στη βρετανική εφημερίδα *The Guardian*[70], που δεν διαψεύστηκαν από την αμερικανική κυβέρνηση, κατά τα οποία η NSA έχει μαζική πρόσβαση στα δεδομένα χρηστών της Facebook Inc. (καθώς και άλλων εταιριών, όπως η Google) από το 2009 μέσω του προγράμματος PRISM[71], στο πλαίσιο εθελοντικής συνεργασίας[72]. Το αίτημα του Max Schrems συνίστατο στη διερεύνηση της καταγγελίας του από τον Ιρλανδό Επίτροπο και, εφόσον κρινόταν αναγκαίο, στην απαγόρευση της διαβίβασης δεδομένων προς τις ΗΠΑ, «*σε περίπτωση που η Facebook Ireland Ltd δεν μπορέσει να αποδείξει ότι δεν λαμβάνει χώρα η αναφερόμενη διαβίβαση δεδομένων προς την NSA*»[73].

Ο Ιρλανδός Επίτροπος απέρριψε την παραπάνω καταγγελία με την αιτιολογία αφενός ότι δεν υπήρχαν αποδείξεις ότι η NSA είχε προσπελάσει τα δεδομένα προσωπικού χαρακτήρα του αιτούντος, και αφετέρου ότι δεσμεύεται από την απόφαση Ασφαλούς Λιμένα της ΕΕ, με την οποία η ΕΕ διαπίστωνε ότι οι ΗΠΑ εξασφαλίζουν επαρκές επίπεδο προστασίας για τα

[69] Snowden E. (2019), *Το Μεγάλο Φακέλωμα*. Αθήνα: Ψυχογιός.

[70] Βλ. Greenwald, G. and MacAskill, E. (2013), «NSA Prism program taps in to user data of Apple, Google and others», *The Guardian*. Διαθέσιμο στο: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data, και Ball, J. (2013), «NSA's Prism surveillance program: how it works and what it can do», *The Guardian*. Διαθέσιμο στο: https://www.theguardian.com/world/2013/jun/08/nsa-prism-server-collection-facebook-google.

[71] Αμερικανικό πρόγραμμα συλλογής πληροφοριών σε μεγάλη κλίμακα.

[72] Αλεξανδροπούλου - Αιγυπτιάδου, Ε. (2016), «Διασυνοριακή ροή προσωπικών δεδομένων από την ΕΕ στις ΗΠΑ: Η πρόσφατη απόφαση του ΔΕΕ ενόψει της σχετικής δραστηριότητας του Facebook (C-362/2014, M. Schrems κατά Ιρλανδού Επιτρόπου Προστασίας Προσωπικών Δεδομένων), *ΤΝΠ QUALEX*, *ΔiΜΕΕ*, 1/2016, σελ. 12 - 24, και Ball, J. (2013), «NSA's Prism surveillance program: how it works and what it can do», ο.π.

[73] «*I am therefore asking the DPC to investigate this complaint and if necessary stop the transfer of data to "Facebook Inc", if "Facebook Ireland Ltd" cannot prove that the reported forwarding of data to the NSA is not taking place*», βλ. Καταγγελία του Maximilian Schrems κατά της Facebook Ireland Ltd, 25 Ιουνίου 2013. Διαθέσιμη στο: http://www.europe-v-facebook.org/prism/facebook.pdf.

διαβιβαζόμενα δεδομένα προσωπικού χαρακτήρα. Εν συνεχεία, ο Max Schrems άσκησε προσφυγή ενώπιον του Ανώτατου Ακυρωτικού Δικαστηρίου της Ιρλανδίας κατά της αποφάσεως του Ιρλανδού Επιτρόπου. Το Ανώτατο Ακυρωτικό Δικαστήριο της Ιρλανδίας, αφού διαπίστωσε σημαντικές υπερβάσεις του δημόσιου συμφέροντος - το οποίο εάν συνέτρεχε θα δικαιολογούσε την ηλεκτρονική επεξεργασία των δεδομένων προσωπικού χαρακτήρα που διαβιβάζονται από την ΕΕ στις ΗΠΑ[74] -, την κατ' ουσία στέρηση του δικαιώματος ακροάσεως των υποκειμένων των δεδομένων και την παραβίαση της αρχής της αναλογικότητας[75] λόγω της μαζικής και χωρίς διάκριση επεξεργασίας, θεωρώντας ότι η υπόθεση αφορά σε εφαρμογή του ενωσιακού δικαίου, ανέστειλε την ενώπιόν του διαδικασία και υπέβαλε προς το Δικαστήριο της ΕΕ προδικαστικά ερωτήματα. Πιο συγκεκριμένα, έθεσε ερωτήματα σχετικά με το εάν ο Ιρλανδός Επίτροπος, ως ανεξάρτητος επίτροπος, δεσμεύεται πλήρως από τη διαπίστωση της Επιτροπής περί παροχής ικανοποιητικού επιπέδου προστασίας για τα υποκείμενα των δεδομένων από τη νομοθεσία και την πρακτική των ΗΠΑ, όπως εκτίθεται στην απόφαση Ασφαλούς Λιμένα, λαμβανομένων υπόψη των άρθρων 7, 8 και 47 του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (εφεξής «**Χάρτης**»), και υπό την επιφύλαξη των διατάξεων της Οδηγίας, ή εάν ως ανεξάρτητος επίτροπος μπορεί ή πρέπει να διεξαγάγει τη δική του έρευνα ως προς το εν λόγω ζήτημα υπό το φως των πραγματικών εξελίξεων που επήλθαν από τότε που δημοσιεύθηκε η προαναφερθείσα απόφαση της Επιτροπής.

Β. Η ΑΚΥΡΩΣΗ ΤΗΣ ΑΠΟΦΑΣΗΣ ΑΣΦΑΛΟΥΣ ΛΙΜΕΝΑ (SCHREMS I)

Το ΔΕΕ εκκίνησε τον έλεγχό του από το ρόλο των εθνικών ΑΠΔ, επί του οποίου το ΔΕΕ υπογράμμισε ότι κάθε εθνική ΑΠΔ οφείλει να εξετάζει με τη δέουσα επιμέλεια την αίτηση ενός φυσικού προσώπου, του οποίου τα δεδομένα διαβιβάστηκαν ή θα μπορούσαν να διαβιβαστούν προς τρίτη χώρα, για την οποία έχει εκδοθεί απόφαση επάρκειας της Επιτροπής, με την οποία αμφισβητείται το σύννομο της απόφασης αυτής[76]. Το ΔΕΕ, μάλιστα, προβαίνει σε ακριβή εξειδίκευση των αρμοδιοτήτων που έχουν οι εθνικές ΑΠΔ. Στην περίπτωση που η εθνική ΑΠΔ καταλήξει ότι η υπό εξέταση αίτηση είναι αβάσιμη, ο αιτών πρέπει να έχει τη δυνατότητα να προσβάλει την απόφαση της ΑΠΔ ενώπιον εθνικού δικαστηρίου, το οποίο, με τη σειρά του, οφείλει να αναστείλει την ενώπιόν του διαδικασία

[74] ΔΕΕ, C-362/14, *Schrems I*, ο.π., παράγραφος 33.
[75] ΔΕΕ, C-362/14, *Schrems I*, ο.π., παράγραφος 32.
[76] ΔΕΕ, C-362/14, *Schrems I*, ο.π., παράγραφος 63.

και να υποβάλει στο ΔΕΕ προδικαστικό ερώτημα, όταν κρίνει ότι είναι βάσιμος ένας ή περισσότεροι λόγοι ακυρότητας που προβλήθηκαν από τα μέρη ή ενδεχομένως εξετάστηκαν αυτεπαγγέλτως[77]. Στην αντίθετη περίπτωση που η εθνική ΑΠΔ κρίνει ότι η αίτηση που έχει λάβει είναι βάσιμη, πρέπει να έχει τη δυνατότητα να προσφύγει σε εθνικό δικαστήριο, το οποίο σε περίπτωση που συμφωνεί ότι υπάρχουν αμφιβολίες ως προς το κύρος της απόφασης της Επιτροπής θα ενεργήσει, υποβάλλοντας προδικαστικό ερώτημα ενώπιον του ΔΕΕ προς έλεγχο του κύρους της συγκεκριμένης απόφασης[78].

Εν συνεχεία, και πριν προβεί στην αξιολόγηση της απόφασης Ασφαλούς Λιμένα, το ΔΕΕ επιχείρησε να ερμηνεύσει την έννοια του «*ικανοποιητικού επίπεδου προστασίας*», η οποία προβλεπόταν στο άρθρο 25, παράγραφος 6 της Οδηγίας. Σύμφωνα με το ΔΕΕ, το οποίο υιοθέτησε τις προτάσεις του Γενικού Εισαγγελέα, Yves Brot[79], η έκφραση «*ικανοποιητικό επίπεδο προστασίας*» δεν συνεπάγεται απαίτηση προς την τρίτη χώρα να εξασφαλίζει το ίδιο ακριβώς επίπεδο προστασίας με αυτό που παρέχει η έννομη τάξη της ΕΕ. Η έκφραση «*ικανοποιητικό επίπεδο προστασίας*» πρέπει να ερμηνευθεί υπό την έννοια ότι απαιτείται η τρίτη αυτή χώρα να διασφαλίζει, λόγω της εσωτερικής της νομοθεσίας ή των διεθνών δεσμεύσεων που έχει αναλάβει, επίπεδο προστασίας ουσιαστικά ισοδύναμο με αυτό που εξασφαλίζεται εντός της ΕΕ[80], ακόμη και εάν είναι διαφορετικά τα μέσα που χρησιμοποιεί η τρίτη αυτή χώρα για να εξασφαλίσει αυτό το επίπεδο, αρκεί να αποδεικνύονται στην πράξη αποτελεσματικά ώστε να εξασφαλίζουν προστασία ουσιαστικά ισοδύναμη με αυτή που παρέχεται στην ΕΕ[81].

Επί τη βάσει της προαναφερθείσας ερμηνείας των κανόνων και της διαδικασίας, το ΔΕΕ προέβη στον έλεγχο της εγκυρότητας της απόφασης Ασφαλούς Λιμένα, εκκινώντας από τον έλεγχο του άρθρου 1 της εν λόγω απόφασης, το οποίο αφορά στις αρχές του ασφαλούς λιμένα, όπως αυτές εκδόθηκαν από το Υπουργείο Εμπορίου των ΗΠΑ. Το Δικαστήριο έκρινε ότι ο προβλεπόμενος στην απόφαση Ασφαλούς Λιμένα μηχανισμός, με τον οποίο μια εταιρεία δηλώνει ότι θα υιοθετεί και τηρεί τις αρχές προστασίας των δεδομένων, θα

[77] ΔΕΕ, C-362/14, *Schrems I*, ο.π., παράγραφος 64.
[78] ΔΕΕ, C-362/14, *Schrems I*, ο.π., παράγραφος 65.
[79] Προτάσεις του Γενικού Εισαγγελέα, Yves Bot, C-362/14, *Maximillian Schrems κατά Data Protection Commissioner*, 23 Σεπτεμβρίου 2015. Διαθέσιμο στο: https://curia.europa.eu/juris/document/document.jsf?text=&docid=168421&pageIndex=0&doclang=el&mode=lst&dir=&occ=first&part=1&cid=897177.
[80] ΔΕΕ, C-362/14, *Schrems I*, ο.π., παράγραφος 73.
[81] ΔΕΕ, C-362/14, *Schrems I*, ο.π., παράγραφος 74.

μπορούσε να αποτελέσει αξιόπιστο μέτρο επάρκειας, μόνο εφόσον υποστηρίζεται από μηχανισμούς ελέγχου που επιτρέπουν να εντοπίζονται και να τιμωρούνται στην πράξη οι εταιρείες που δεν τηρούν τις αρχές της εν λόγω απόφασης[82]. Εν προκειμένω, όμως, το Δικαστήριο διαπίστωσε ότι η ρύθμιση του ασφαλούς λιμένα δεν διαθέτει τέτοιου είδους μηχανισμούς, και ότι οι κανόνες θα μπορούσαν να παρακαμφθούν επί τη βάσει των εθνικών απαιτήσεων ασφαλείας που ορίζονται στο αμερικανικό δίκαιο[83].

Επιπλέον, το Δικαστήριο διαπίστωσε ότι στο πλαίσιο κρατικής παρακολούθησης, σε αντίθεση με το δίκαιο της ΕΕ, το οποίο ερμηνευόμενο υπό το πρίσμα του Χάρτη, περιορίζει την κρατική παρέμβαση στο απολύτως αναγκαίο, η απόφαση Ασφαλούς Λιμένα επιτρέπει στις αμερικανικές δημόσιες αρχές να διατηρούν τα δεδομένα προσωπικού χαρακτήρα όλων των προσώπων, των οποίων τα δεδομένα διαβιβάστηκαν από την ΕΕ στις ΗΠΑ, χωρίς καμία διαφοροποίηση, περιορισμό ή εξαίρεση σε σχέση με τον επιδιωκόμενο σκοπό, και χωρίς να προβλέπεται αντικειμενικό κριτήριο που θα μπορούσε να οριοθετήσει την πρόσβαση των αμερικανικών δημόσιων αρχών στα δεδομένα και τη μεταγενέστερη χρήση τους για συγκεκριμένους σκοπούς, αυστηρά περιορισμένους, που μπορούν να δικαιολογήσουν την προσβολή που συνεπάγεται τόσο η πρόσβαση όσο και η χρήση των δεδομένων αυτών[84]. Επιπροσθέτως, η απόφαση Ασφαλούς Λιμένα δεν προέβλεπε ένδικα βοηθήματα προκειμένου ο εκάστοτε ενδιαφερόμενος να έχει πρόσβαση στα δεδομένα προσωπικού χαρακτήρα που τον αφορούν ή να επιτύχει την τροποποίηση ή τη διαγραφή τέτοιων δεδομένων, γεγονός που δεν σέβεται το ουσιαστικό περιεχόμενο του θεμελιώδους δικαιώματος αποτελεσματικής δικαστικής προστασίας, όπως αυτό κατοχυρώνεται στο άρθρο 47 του Χάρτη.

Προς ενίσχυση των παραπάνω διαπιστώσεών του, το ΔΕΕ μνημόνευσε την υπ'αριθμ. COM(2013) 846 ανακοίνωση της Επιτροπής με τίτλο «Αποκατάσταση της εμπιστοσύνης στις ροές δεδομένων μεταξύ της Ευρωπαϊκής Ένωσης και των Ηνωμένων Πολιτειών της Αμερικής», με την οποία είχε διαπιστωθεί ότι η απόφαση Ασφαλούς Λιμένα περιλαμβάνει ασθενείς εγγυήσεις μηχανισμών ελέγχου και κυρώσεων για την τήρηση των αρχών του ασφαλούς λιμένα. Η ανακοίνωση ανέφερε συγκεκριμένα ότι «*τα δεδομένα προσωπικού χαρακτήρα των πολιτών ΕΕ που αποστέλλονται στις Ηνωμένες Πολιτείες στο πλαίσιο της*

[82] ΔΕΕ, C-362/14, *Schrems I*, ο.π., παράγραφος 81.
[83] ΔΕΕ, C-362/14, *Schrems I*, ο.π., παράγραφος 82.
[84] ΔΕΕ, C-362/14, *Schrems I*, ο.π., παράγραφος 93.

συμφωνίας ασφαλούς λιμένα τίθενται, ενδεχομένως, στη διάθεση των αμερικανικών αρχών και αποτελούν το αντικείμενο περαιτέρω επεξεργασίας κατά τρόπο ασυμβίβαστο με τους λόγους για τους οποίους συγκεντρώθηκαν αρχικά στην ΕΕ και με τους σκοπούς της διαβίβασής τους στις Ηνωμένες Πολιτείες» καθ' υπέρβαση των ορίων του απολύτως αναγκαίου και του αναλογικού για την προστασία της εθνικής ασφάλειας[85].

Το Δικαστήριο κατέληξε επισημαίνοντας ότι στο άρθρο 1 της απόφασης Ασφαλούς Λιμένα δεν διαπιστώνεται επαρκώς και αιτιολογημένα ότι πληρούνται οι προϋποθέσεις του άρθρου 25, παράγραφος 6 της Οδηγίας, δυνάμει του οποίου εκδόθηκε η απόφαση Ασφαλούς Λιμένα, ότι δηλαδή οι ΗΠΑ εξασφαλίζουν ικανοποιητικό επίπεδο προστασίας των προσωπικών δεδομένων, ουσιαστικά ισοδύναμο με αυτό της ΕΕ, λόγω της εσωτερικής τους νομοθεσίας ή των διεθνών δεσμεύσεων που έχουν αναλάβει. Μάλιστα, κατά το ΔΕΕ, και μόνο αυτή η πλημμέλεια καθιστά άκυρο το άρθρο 1 της απόφασης Ασφαλούς Λιμένα, χωρίς να χρειάζεται να εξετασθούν οι αρχές του ασφαλούς λιμένα ως προς το περιεχόμενό τους[86].

Αναφορικά με το άρθρο 3 της απόφασης Ασφαλούς Λιμένα, το οποίο προβλέπει ειδική ρύθμιση σχετικά με τις εξουσίες που διαθέτουν οι ΑΠΔ σε σχέση με τη διαπίστωση που έχει πραγματοποιήσει η Επιτροπή ως προς το ικανοποιητικό επίπεδο προστασίας, το ΔΕΕ αποφάνθηκε ότι, με τη θέσπιση του εν λόγω άρθρου, η Επιτροπή υπερέβη τις αρμοδιότητες που της απένειμε το άρθρο 25, παράγραφος 6 της Οδηγίας, στο μέτρο που η εν λόγω διάταξη στερεί από τις ΑΠΔ τις εξουσίες που αντλούν από το άρθρο 28 της Οδηγίας, σε περίπτωση που κάποιο πρόσωπο προβάλλει, στο πλαίσιο υποβολής αίτησης δυνάμει της εν λόγω διάταξης, στοιχεία δυνάμενα να κλονίσουν τη συμβατότητα με την προστασία της ιδιωτικής ζωής και των θεμελιωδών δικαιωμάτων και ελευθεριών των προσώπων αποφάσεως, με την οποία η Επιτροπή έχει διαπιστώσει ότι τρίτη χώρα εξασφαλίζει ικανοποιητικό επίπεδο προστασίας[87].

Στην απόφαση *Schrems I* το ΔΕΕ διαπίστωσε την «ασυμβατότητα» της απόφασης Ασφαλούς Λιμένα με τον Χάρτη, και συγκεκριμένα τα άρθρα 7, 8 και 47 που κατοχυρώνουν το δικαίωμα

[85] Βλ. Ευρωπαϊκή Επιτροπή (2013), *Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο - Αποκατάσταση της εμπιστοσύνης στις ροές δεδομένων μεταξύ της Ευρωπαϊκής Ένωσης και των Ηνωμένων Πολιτειών της Αμερικής*. Βέλγιο: Ευρωπαϊκή Επιτροπή. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52013DC0846&from=GA, και ΔΕΕ, C-362/14, *Schrems I*, ο.π., παράγραφος 14.

[86] ΔΕΕ, C-362/14, *Schrems I*, ο.π., παράγραφοι 96 - 98.

[87] ΔΕΕ, C-362/14, *Schrems I*, ο.π., παράγραφος 102.

στο σεβασμό της ιδιωτικής ζωής, το δικαίωμα προστασίας των δεδομένων προσωπικού χαρακτήρα και το δικαίωμα πραγματικής δικαστικής προσφυγής και αμερόληπτου δικαστή αντίστοιχα. Η εν λόγω ασυμβατότητα συνοψίζεται στις ακόλουθες διαπιστώσεις του ΔΕΕ:

α) Παραβίαση της αρχής της αναλογικότητας λόγω της μαζικής διαβίβασης δεδομένων και της μαζικής παρακολούθησης από τις αμερικανικές μυστικές υπηρεσίες που αφορούν σε όλα τα μέσα ηλεκτρονικής επικοινωνίας, χωρίς καμία διάκριση, περιορισμό ή εξαίρεση[88].

β) Μη δέσμευση των αμερικανικών δημόσιων αρχών, παρά μόνο των αμερικανικών επιχειρήσεων που έχουν προσχωρήσει στο πλαίσιο του ασφαλούς λιμένα.[89].

γ) Απουσία κρατικών κανόνων για τον περιορισμό τυχόν επεμβάσεων στα θεμελιώδη δικαιώματα των προσώπων, των οποίων τα δεδομένα διαβιβάζονται από την ΕΕ στις ΗΠΑ, επεμβάσεις στις οποίες επιτρέπεται να προβαίνουν κρατικοί φορείς των ΗΠΑ για λόγους εθνικής ασφάλειας και δημοσίου συμφέροντος[90].

δ) Υπεροχή των απαιτήσεων εθνικής ασφάλειας, δημόσιου συμφέροντος και εφαρμογής του δικαίου των ΗΠΑ έναντι των αρχών του ασφαλούς λιμένα, με αποτέλεσμα οι αμερικανικές επιχειρήσεις να οφείλουν να αποκλίνουν χωρίς περιορισμό από τις αρχές αυτές[91].

ε) Απουσία πρόβλεψης αποτελεσματικής δικαστικής προστασίας κατά των επεμβάσεων των αμερικανικών δημοσίων αρχών[92].

Επί τη βάσει των παραπάνω διαπιστώσεων, το ΔΕΕ κήρυξε την απόφαση Ασφαλούς Λιμένα ανίσχυρη, αναδεικνύοντας με ηχηρό τρόπο τη βαθιά διάσταση ανάμεσα στην ευρωπαϊκή και αμερικανική αντίληψη για το δίκαιο προστασίας από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, η οποία έγκειται κυρίως στη θεσμική διάσταση της προστασίας. Και τούτο διότι, από τη μια οι ευρωπαϊκές χώρες δίνουν μεγάλη έμφαση στους μηχανισμούς

[88] ΔΕΕ, C-362/14, *Schrems I*, ο.π., παράγραφοι 33, 93 και 94.
[89] ΔΕΕ, C-362/14, *Schrems I*, ο.π., παράγραφος 82.
[90] ΔΕΕ, C-362/14, *Schrems I*, ο.π., παράγραφος 88.
[91] ΔΕΕ, C-362/14, *Schrems I*, ο.π., παράγραφοι 86 και 90 σε συνδυασμό με Ευρωπαϊκή Επιτροπή (2013), *Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο όσον αφορά τη λειτουργία του ασφαλούς λιμένα από τη σκοπιά των πολιτών της Ένωσης και των εταιρειών που είναι εγκατεστημένες στην ΕΕ*, ενότητες 7.1, 7.2 και 8, Βέλγιο: Ευρωπαϊκή Επιτροπή. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52013DC0847&from=EN, καθώς και Ευρωπαϊκή Επιτροπή (2013), *Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο - Αποκατάσταση της εμπιστοσύνης στις ροές δεδομένων μεταξύ της Ευρωπαϊκής Ένωσης και των Ηνωμένων Πολιτειών της Αμερικής*, ο.π., ενότητες 2 και 3.2.
[92] ΔΕΕ, C-362/14, *Schrems I*, ο.π., παράγραφος 89.

εξασφάλισης του δικαιώματος, ιδρύοντας αρχές με χαρακτηριστικά ανεξαρτησίας ή ορίζοντας διαμεσολαβητές ως αντικειμενικούς παρατηρητές ανάμεσα στη διοίκηση και στην κοινωνία των πολιτών, ενώ από την άλλη οι ΗΠΑ βασίζονταν κυρίως στην αυτορρύθμιση και στην αυτοδέσμευση των ιδιωτών[93].

Μετά την απόφαση *Schrems I*, το Ανώτατο Ακυρωτικό Δικαστήριο της Ιρλανδίας ακύρωσε την απόφαση με την οποία ο Ιρλανδός Επίτροπος απέρριψε την καταγγελία του Max Schrems, και παρέπεμψε την απόφαση αυτή στον Ιρλανδό Επίτροπο για επαναξιολόγηση. Ο Ιρλανδός Επίτροπος ξεκίνησε εκ νέου έρευνα και ζήτησε από τον Max Schrems να αναδιατυπώσει την καταγγελία του υπό το πρίσμα της ακύρωσης της απόφασης Ασφαλούς Λιμένα από το ΔΕΕ.

Στο πλαίσιο αυτό, ο Max Schrems ζήτησε από την Facebook Ireland Ltd να προσδιορίσει τη νομική βάση για τη διαβίβαση των δεδομένων προσωπικού χαρακτήρα των χρηστών του facebook από την ΕΕ στις ΗΠΑ. Η Facebook Ireland Ltd παρέπεμψε στη συμφωνία επεξεργασίας για τη διαβίβαση δεδομένων με την Facebook Inc, η οποία ίσχυε από το 2015, και επικαλέστηκε την απόφαση 2010/87/ΕΕ της Επιτροπής για τις ΤΣΡ [βλ. Ενότητα I (Α) και (Β)(2)(α)][94]. Στην αναδιατυπωμένη καταγγελία του, ο Max Schrems υποστήριξε ότι οι ΗΠΑ δεν προσφέρουν επαρκή προστασία για τα διαβιβαζόμενα δεδομένα προσωπικού χαρακτήρα, και ζήτησε την ακύρωση της απόφασης για την Ασπίδα Προστασίας της Ιδιωτικής Ζωής. Ο Max Schrems ζήτησε επίσης την αναστολή ή την απαγόρευση των μελλοντικών διαβιβάσεων δεδομένων προσωπικού χαρακτήρα από την ΕΕ προς τις ΗΠΑ, τις οποίες πραγματοποιούσε η Facebook Ireland Ltd επί τη βάσει των ΤΣΡ. Ωστόσο, ο Max Schrems δεν αμφισβήτησε τη νομική εγκυρότητα της απόφασης 2010/87/ΕΕ της Επιτροπής για τις ΤΣΡ.

Ο Ιρλανδός Επίτροπος διεξήγαγε έρευνα για να διαπιστώσει εάν οι ΗΠΑ εξασφάλιζαν επαρκή προστασία των δεδομένων προσωπικού χαρακτήρα των πολιτών της ΕΕ και, εάν όχι, κατά πόσο η χρήση των ΤΣΡ προσέφερε επαρκείς εγγυήσεις για την προστασία των ελευθεριών και των θεμελιωδών δικαιωμάτων των εν λόγω πολιτών. Θεωρώντας ότι η εκδίκαση της καταγγελίας του Max Schrems εξαρτάται, ιδίως, από τη νομική εγκυρότητα της

[93] Βλ. Χρήστου, Β. (2017), *Το δικαίωμα στην προστασία από την επεξεργασία δεδομένων*. Αθήνα: Σάκκουλας, σελ. 75 - 80.

[94] Απόφαση της Επιτροπής της 5ης Φεβρουαρίου 2010 σχετικά με τις τυποποιημένες συμβατικές ρήτρες για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε εκτελούντες επεξεργασία εγκατεστημένους σε τρίτες χώρες βάσει της οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (2010/87/ΕΕ), ο.π.

απόφασης 2010/87/ΕΕ, ο Ιρλανδός Επίτροπος άσκησε προσφυγή ενώπιον του Ανώτατου Ακυρωτικού Δικαστηρίου της Ιρλανδίας και αιτήθηκε να υποβληθεί από αυτό σχετικό προδικαστικό ερώτημα στο ΔΕΕ, σύμφωνα με το άρθρο 267 της Συνθήκης της ΕΕ.

Στο πλαίσιο εκκίνησης της εν λόγω διαδικασίας, η Επιτροπή εξέδωσε την απόφαση για την Ασπίδα Προστασίας της Ιδιωτικής Ζωής[95]. Στην απόφαση αυτή, η Επιτροπή διαπίστωσε ότι οι ΗΠΑ εξασφάλιζαν επαρκές επίπεδο προστασίας των δεδομένων προσωπικού χαρακτήρα που διαβιβάζονται από την ΕΕ στο πλαίσιο του συστήματος που θεσπίστηκε με την ασπίδα προστασίας της ιδιωτικής ζωής ΕΕ - ΗΠΑ, λαμβάνοντας υπόψη, μεταξύ άλλων, τις εγγυήσεις που περιβάλλουν την πρόσβαση των αμερικανικών αρχών πληροφοριών στα διαβιβαζόμενα δεδομένα προσωπικού χαρακτήρα και τη δικαστική προστασία που παρέχεται στα υποκείμενα των δεδομένων. Σε σύγκριση με την απόφαση Ασφαλούς Λιμένα, η απόφαση για την Ασπίδα Προστασίας της Ιδιωτικής Ζωής πρόσφερε οριακή μόνο βελτίωση, δεδομένου ότι το σχετικό νομικό σύστημα των ΗΠΑ δεν είχε τροποποιηθεί μεταξύ της απόφασης του ΔΕΕ *Schrems I* και της απόφασης για την Ασπίδα Προστασίας της Ιδιωτικής Ζωής, καθώς η τελευταία δεν τροποποίησε την πρακτική των ΗΠΑ περί μαζικής παρακολούθησης χωρίς αιτία, ενώ δεν ενίσχυσε τα δικαιώματα των θιγόμενων υποκειμένων των δεδομένων[96].

Το 2017, με μια απόφαση 152 σελίδων, το Ανώτατο Ακυρωτικό Δικαστήριο της Ιρλανδίας έκρινε αναγκαία την υποβολή προδικαστικών ερωτημάτων ενώπιον του ΔΕΕ[97]. Το αιτούν δικαστήριο υπέβαλε, μεταξύ άλλων, ερωτήματα σχετικά με: α) εάν ο ΓΚΠΔ τυγχάνει εφαρμογής σε περίπτωση που δεδομένα προσωπικού χαρακτήρα διαβιβάζονται από ιδιωτική εταιρία εγκατεστημένη σε κράτος-μέλος της ΕΕ προς άλλη ιδιωτική εταιρία σε τρίτη χώρα για εμπορικούς σκοπούς, δυνάμει της αποφάσεως 2010/87/ΕΕ για τις ΤΣΡ, και υπόκεινται ενδεχομένως σε περαιτέρω επεξεργασία από τις αρχές της τρίτης χώρας για

[95] Ευρωπαϊκή Επιτροπή (2016), Εκτελεστική Απόφαση (ΕΕ) 2016/1250 της Επιτροπής της 12ης Ιουλίου 2016 βάσει της οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την επάρκεια της προστασίας που παρέχεται από την ασπίδα προστασίας της ιδιωτικής ζωής ΕΕ - ΗΠΑ, ο.π. Η εν λόγω εκτελεστική απόφαση εκδόθηκε κατόπιν της δημοσίευσης της απόφασης του ΔΕΕ *Schrems I*.

[96] Βλ. Tracol, X. (2016) «EU U.S. Privacy Shield: The saga continues», *Computer Law & Security Review*, Volume 2, Issue 5, σελ. 777. Διαθέσιμο στο: https://www.sciencedirect.com/science/article/abs/pii/S0267364916301273.

[97] The High Court Commercial, *Data Protection Commissioner and Facebook Ireland Limited and Maximillian Schrems*, υπ'αριθμ. 2016 No. 4809 P. Διαθέσιμο στο: https://www.dataprotection.ie/sites/default/files/uploads/2018-12/High%20Court%20Judgment_03_10_2017.pdf.

σκοπούς εθνικής ασφάλειας, β) ποιο επίπεδο προστασίας απαιτεί ο ΓΚΠΔ σε σχέση με τις διαβιβάσεις αυτές και γ) ποιες υποχρεώσεις βαρύνουν την αρμόδια ΑΠΔ σε αυτές τις περιπτώσεις. Το Ανώτατο Ακυρωτικό Δικαστήριο της Ιρλανδίας έθεσε επίσης το ερώτημα της νομικής εγκυρότητας τόσο της απόφασης 2010/87/ΕΕ για τις ΤΣΡ, όσο και της απόφασης για την Ασπίδα Προστασίας της Ιδιωτικής Ζωής.

Γ. Η ΡΗΞΙΚΕΛΕΥΘΗ ΑΠΟΦΑΣΗ SCHREMS II

Στη δεύτερη κατά σειρά απόφασή του, το Δικαστήριο της ΕΕ έκρινε, κατ' αρχάς, ότι το δίκαιο της ΕΕ, και ειδικότερα ο ΓΚΠΔ, έχει εφαρμογή στην περίπτωση διαβίβασης δεδομένων προσωπικού χαρακτήρα, η οποία πραγματοποιείται για εμπορικούς σκοπούς από οικονομικό φορέα εγκατεστημένο σε κράτος-μέλος της ΕΕ προς άλλον οικονομικό φορέα εγκατεστημένο σε τρίτη χώρα, ακόμη και εάν, είτε κατά τη διάρκεια είτε κατόπιν της διαβίβασης αυτής, τα δεδομένα ενδέχεται να υποστούν επεξεργασία από τις δημόσιες αρχές της αντίστοιχης τρίτης χώρας για λόγους δημόσιας ασφάλειας, εθνικής άμυνας και ασφάλειας του κράτους[98]. Πρόσθεσε δε ότι αυτού του είδους η επεξεργασία από τις δημόσιες αρχές τρίτης χώρας δεν συνεπάγεται ότι η διαβίβαση πρέπει να εξαιρείται από το πεδίο εφαρμογής του ΓΚΠΔ[99].

Σε αντίθεση με τις προτάσεις του Γενικού Εισαγγελέα, Henrik Saugmandsgaard Øe[100], το ΔΕΕ δεν προέβη σε διάκριση μεταξύ της «*επεξεργασίας που συνίσταται στην ίδια τη διαβίβαση*» και της περαιτέρω επεξεργασίας. Εντούτοις, το Δικαστήριο συμφώνησε με τη γνώμη του Γενικού Εισαγγελέα ότι το πρότυπο του ουσιαστικά ισοδύναμου επιπέδου προστασίας με το δίκαιο της ΕΕ βάσει του άρθρου 45 του ΓΚΠΔ ισχύει και για τις ΤΣΡ βάσει του άρθρου 46 του

[98] ΔΕΕ, C-311/18, *Schrems II*, ο.π., παράγραφοι 86 και 89.
[99] ΔΕΕ, C-311/18, *Schrems II*, ο.π., παράγραφος 88.
[100] Προτάσεις του Γενικού Εισαγγελέα, Henrik Saugmandsgaard Øe, C-311/18, *Maximillian Schrems κατά Data Protection Commissioner*, 19 Δεκεμβρίου 2019, παράγραφος 104. Διαθέσιμο στο: https://curia.europa.eu/juris/document/document.jsf;jsessionid=1A97A2D89262C458AB209A52CAAF1869?text=&docid=221826&pageIndex=0&doclang=EL&mode=req&dir=&occ=first&part=1&cid=742986.

ΓΚΠΔ[101]. Έκρινε δε ότι το πρότυπο αυτό πρέπει να βασίζεται στο δίκαιο της ΕΕ γενικά και στο Χάρτη ειδικότερα[102], και όχι στο εσωτερικό δίκαιο των κρατών-μελών της ΕΕ[103].

Όσον αφορά το απαιτούμενο επίπεδο προστασίας στο πλαίσιο μιας τέτοιας διαβίβασης δεδομένων, το Δικαστήριο απεφάνθη ότι οι απαιτήσεις που προβλέπονται από τις διατάξεις του ΓΚΠΔ και συνίστανται στην ύπαρξη κατάλληλων εγγυήσεων, εκτελεστών δικαιωμάτων και αποτελεσματικών μέσων έννομης προστασίας, έχουν την έννοια ότι τα πρόσωπα, των οποίων τα δεδομένα προσωπικού χαρακτήρα διαβιβάζονται προς τρίτη χώρα βάσει ΤΣΡ, πρέπει να απολαύουν επιπέδου προστασίας ουσιαστικά ισοδύναμου με εκείνο που εγγυάται εντός της ΕΕ ο ΓΚΠΔ, σε συνδυασμό με το Χάρτη. Στο πλαίσιο αυτό, το ΔΕΕ διευκρίνισε ότι κατά την αξιολόγηση αυτού του επιπέδου προστασίας πρέπει να λαμβάνονται υπόψη τόσο οι συμβατικοί όροι που έχουν συμφωνηθεί μεταξύ του εγκατεστημένου στην ΕΕ υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία, και του εγκατεστημένου στην τρίτη χώρα αποδέκτη της διαβίβασης, όσο και τα κρίσιμα στοιχεία του νομικού συστήματος της συγκεκριμένης τρίτης χώρας σε σχέση με την ενδεχόμενη πρόσβαση των δημοσίων αρχών αυτής στα διαβιβαζόμενα δεδομένα[104].

Σε απόλυτη συμφωνία με την απόφαση *Schrems I* το ΔΕΕ επεσήμανε ότι η έκφραση «*ικανοποιητικό επίπεδο προστασίας*» πρέπει να γίνεται αντιληπτή, όπως πλέον επιβεβαιώνει η αιτιολογική σκέψη 104 του ΓΚΠΔ, υπό την έννοια ότι απαιτείται από την τρίτη χώρα να εξασφαλίζει πράγματι, μέσω της εσωτερικής νομοθεσίας της ή των διεθνών δεσμεύσεων που έχει αναλάβει, επίπεδο προστασίας των θεμελιωδών ελευθεριών και δικαιωμάτων ουσιαστικά ισοδύναμο με εκείνο το οποίο διασφαλίζεται εντός της ΕΕ δυνάμει του Κανονισμού, όπως ερμηνεύεται σε συνδυασμό με το Χάρτη[105].

---

[101] ΔΕΕ, C-311/18, *Schrems II*, ο.π., παράγραφος 96.

[102] Στην απόφαση *Schrems II*, το ΔΕΕ υπογράμμισε ότι η ερμηνεία του δικαίου της ΕΕ καθώς και η εξέταση του κύρους των πράξεων της ΕΕ πρέπει να διεξάγονται υπό το πρίσμα των θεμελιωδών δικαιωμάτων που κατοχυρώνονται στον Χάρτη και όχι στην Ευρωπαϊκή Σύμβαση για την Προάσπιση των Δικαιωμάτων του Ανθρώπου και των Θεμελιωδών Ελευθεριών (ΕΣΔΑ), καθώς «*…η ΕΣΔΑ δεν συνιστά, ενόσω η Ένωση δεν έχει προσχωρήσει σε αυτήν, νομική πράξη τυπικώς ενταγμένη στην έννομη τάξη της Ένωσης*», βλ. ΔΕΕ, C-311/18, *Schrems II*, ο.π., παράγραφοι 97 - 99. Μάλιστα, μερίδα του νομικού κόσμου θεωρεί ότι η ΕΣΔΑ είναι «λιγότερο απαιτητική» στο θέμα της προστασίας της ιδιωτικής ζωής, βλ. σχετικά Bignami, F. (2020) «Schrems II: The Right to Privacy and the New Illiberalism», *Media Laws*. Διαθέσιμο στο: https://verfassungsblog.de/schrems-ii-the-right-to-privacy-and-the-new-illiberalism/.

[103] ΔΕΕ, C-311/18, *Schrems II*, ο.π., παράγραφοι 99 και 100.

[104] ΔΕΕ, C-311/18, *Schrems II*, ο.π., παράγραφος 105.

[105] ΔΕΕ, C-311/18, *Schrems II*, ο.π., παράγραφος 94.

Στο βασικό της κορμό η απόφαση *Schrems II* αμφισβητεί τους μηχανισμούς διαβίβασης δεδομένων μεταξύ της ΕΕ και των ΗΠΑ επί τη βάσει της αδυναμίας του αμερικανικού δικαίου να διασφαλίσει ένα επίπεδο προστασίας «ουσιαστικά ισοδύναμο» με εκείνο που εγγυάται το δίκαιο της ΕΕ. Το ΔΕΕ διαπίστωσε ότι σε περίπτωση που υπάρχουν επαρκείς εγγυήσεις στην τρίτη χώρα ή οι συμβατικοί όροι παρέχουν την απαιτούμενη «ουσιαστικά ισοδύναμη» προστασία με το δίκαιο της ΕΕ, η χρήση των ΤΣΡ είναι έγκυρη **(1)**. Εν συνεχεία, το Δικαστήριο αξιολόγησε την εγκυρότητα των διαβιβάσεων δεδομένων μεταξύ ΕΕ και ΗΠΑ στο πλαίσιο της ασπίδας προστασίας της ιδιωτικής ζωής ΕΕ - ΗΠΑ, κρίνοντας ανίσχυρη την απόφαση για την Ασπίδα Προστασίας της Ιδιωτικής Ζωής λόγω ανεπάρκειας των εγγυήσεων που παρέχει το αμερικανικό δίκαιο **(2)**.

1. Η υπό όρους αποδοχή των Τυποποιημένων Συμβατικών Ρητρών

Το ΔΕΕ αρχικά επικεντρώνεται στον έλεγχο εγκυρότητας της απόφασης της Επιτροπής που αφορά στο μηχανισμό διαβίβασης των ΤΣΡ. Κατά το ΔΕΕ, το κύρος της αποφάσεως 2010/87/ΕΕ της Επιτροπής δεν θίγεται απλώς και μόνο επειδή οι εκεί περιεχόμενες ΤΣΡ δεν δεσμεύουν, λόγω του συμβατικού τους χαρακτήρα, τις δημόσιες αρχές της τρίτης χώρας προς την οποία θα μπορούσαν να διαβιβαστούν τα δεδομένα προσωπικού χαρακτήρα[106]. Αντιθέτως, το Δικαστήριο κατέστησε σαφές ότι το κύρος της εν λόγω απόφασης εξαρτάται από το εάν αυτή περιλαμβάνει αποτελεσματικούς μηχανισμούς που: α) καθιστούν δυνατή τη διασφάλιση της συμμόρφωσης με επίπεδο προστασίας ουσιαστικά ισοδύναμο με το επίπεδο που εγγυάται ο ΓΚΠΔ εντός της ΕΕ, και β) διασφαλίζουν, στην πράξη, ότι τηρείται το απαιτούμενο από το δίκαιο της ΕΕ επίπεδο προστασίας και ότι οι διαβιβάσεις δεδομένων προσωπικού χαρακτήρα βάσει τέτοιων ρητρών αναστέλλονται ή απαγορεύονται σε περίπτωση παράβασης των ΤΣΡ ή αδυναμίας εκπλήρωσής τους. Το ΔΕΕ κατέληξε ότι η απόφαση 2010/87/ΕΕ της Επιτροπής προβλέπει τέτοιους μηχανισμούς και, ως εκ τούτου, είναι έγκυρη[107].

Ωστόσο, το Δικαστήριο επεσήμανε την πρωταρχική υποχρέωση τόσο του εξαγωγέα όσο και του εισαγωγέα δεδομένων να αξιολογούν κατά περίπτωση, πριν από κάθε διαβίβαση δεδομένων προσωπικού χαρακτήρα, το δίκαιο της χώρας προορισμού για να προσδιορίσουν εάν το εν λόγω εθνικό δίκαιο επιτρέπει στον εισαγωγέα δεδομένων να συμμορφώνεται στην

[106] ΔΕΕ, C-311/18, *Schrems II*, ο.π., παράγραφοι 125 και 132.
[107] ΔΕΕ, C-311/18, *Schrems II*, ο.π., παράγραφος 149.

πράξη με τον επιλεγμένο συμβατικά μηχανισμό διαβίβασης δεδομένων, λαμβάνοντας υπόψη όλες τις περιστάσεις της διαβίβασης δεδομένων. Στο πλαίσιο αυτού του ελέγχου μπορεί να συναχθεί ότι απαιτείται η εφαρμογή από τον εξαγωγέα και των εισαγωγέα δεδομένων πρόσθετων μέτρων, τα οποία, όταν προστίθενται στις εγγυήσεις που περιέχονται στον επιλεγμένο συμβατικά μηχανισμό διαβίβασης, θα διασφαλίσουν ότι τα διαβιβαζόμενα δεδομένα τυγχάνουν ενός επιπέδου προστασίας στην τρίτη χώρα, το οποίο είναι ουσιαστικά ισοδύναμο με αυτό που διασφαλίζεται στο εσωτερικό της ΕΕ[108].

Όμως, το ΔΕΕ δεν συγκεκριμενοποίησε ποια θα μπορούσαν να είναι τα πρόσθετα αυτά μέτρα, γεγονός που κατέστησε (και εξακολουθεί να καθιστά όπως θα δούμε παρακάτω) ιδιαίτερα δυσχερή την εμπέδωση και την εφαρμογή της νέας αυτής υποχρέωσης, τόσο για τον εξαγωγέα όσο και για τον εισαγωγέα δεδομένων. Εντούτοις, με την εν λόγω κρίση του το Δικαστήριο δεν απαίτησε τα πρόσθετα μέτρα να παρέχουν 100% εγγύηση ότι η πρόσβαση σε διαβιβαζόμενα δεδομένα από τρίτους δεν μπορεί ποτέ να συμβεί, αλλά ότι αποτελούν αποτελεσματικούς μηχανισμούς που διασφαλίζουν, στην πράξη, ότι τηρείται το απαιτούμενο από το δίκαιο της ΕΕ επίπεδο προστασίας.

Όταν οι ΤΣΡ δεν μπορούν να παρέχουν ένα ουσιαστικά ισοδύναμο επίπεδο προστασίας με το δίκαιο της ΕΕ και ο εξαγωγέας δεδομένων δεν έχει ενεργήσει καταλλήλως, το ΔΕΕ έκρινε ότι οι αρμόδιες ΑΠΔ πρέπει να αναστέλλουν, να περιορίζουν ή ακόμη και να απαγορεύουν τη διαβίβαση δεδομένων[109]. Εντούτοις, το ΔΕΕ έκρινε ότι οι ΑΠΔ δεν μπορούν να αναστείλουν, να περιορίσουν ή να απαγορεύσουν τη διαβίβαση δεδομένων σε τρίτη χώρα όταν υπάρχει απόφαση επάρκειας της Επιτροπής, όπως η απόφαση για την Ασπίδα Προστασίας της Ιδιωτικής Ζωής. Πιο συγκεκριμένα, το Δικαστήριο διαβεβαίωσε ότι οι ΑΠΔ *«δεν μπορούν να λαμβάνουν μέτρα αντίθετα προς την απόφαση αυτή, όπως είναι οι πράξεις που διαπιστώνουν δεσμευτικά ότι η τρίτη χώρα την οποία αφορά η απόφαση επάρκειας δεν εξασφαλίζει ικανοποιητικό επίπεδο προστασίας»*[110]. Όμως, το ΔΕΕ διευκρίνισε ότι οι ΑΠΔ πρέπει να εξετάζουν τις καταγγελίες που λαμβάνουν, με πλήρη ανεξαρτησία, και, σε περίπτωση που γεννηθούν προβληματισμοί για την ισοδυναμία της προστασίας βάσει απόφασης επάρκειας, να προσφεύγουν ενώπιον των εθνικών δικαστηρίων αμφισβητώντας την εν λόγω επάρκεια. Εάν το εθνικό δικαστήριο συμφωνεί με τους ισχυρισμούς της

[108] ΔΕΕ, C-311/18, *Schrems II*, ο.π., παράγραφος 96.
[109] ΔΕΕ, C-311/18, *Schrems II*, ο.π., παράγραφος 121.
[110] ΔΕΕ, C-311/18, *Schrems II*, ο.π., παράγραφος 118.

προσφυγής, μπορεί να υποβάλει αίτηση ενώπιον του ΔΕΕ για την έκδοση προδικαστικής απόφασης σχετικά με την εγκυρότητα της αμφισβητούμενης απόφασης επάρκειας[111].

2. Η ακύρωση της απόφασης για την Ασπίδα Προστασίας της Ιδιωτικής Ζωής

Στο πλαίσιο της απόφασης *Schrems II*, το Δικαστήριο εξέτασε επίσης το κύρος της απόφασης για την Ασπίδα Προστασίας της Ιδιωτικής Ζωής, καθώς οι επίμαχες διαβιβάσεις δεδομένων, στο πλαίσιο της εθνικής δικαστικής διαμάχης που οδήγησε στην αίτηση έκδοσης προδικαστικής απόφασης, έλαβαν χώρα μεταξύ της ΕΕ και των ΗΠΑ. Η εν λόγω αξιολόγηση πραγματοποιήθηκε υπό το πρίσμα των απαιτήσεων που απορρέουν από το ΓΚΠΔ, σε συνδυασμό με τις διατάξεις του Χάρτη, οι οποίες εγγυώνται το σεβασμό της ιδιωτικής και οικογενειακής ζωής (Άρθρο 7), την προστασία των δεδομένων προσωπικού χαρακτήρα (Άρθρο 8) και το δικαίωμα αποτελεσματικής δικαστικής προστασίας (Άρθρο 47).

Ως προς το ζήτημα αυτό, το ΔΕΕ επεσήμανε ότι η ως άνω απόφαση, όπως και η απόφαση Ασφαλούς Λιμένα (η οποία ακυρώθηκε με την προεκτεθείσα απόφαση *Schrems I*), καθιερώνει την υπεροχή των απαιτήσεων που συνδέονται με την εθνική ασφάλεια, το δημόσιο συμφέρον και την τήρηση της αμερικανικής νομοθεσίας, καθιστώντας έτσι δυνατές τις επεμβάσεις στα θεμελιώδη δικαιώματα των προσώπων, των οποίων τα δεδομένα διαβιβάζονται προς τη συγκεκριμένη τρίτη χώρα[112].

Το ΔΕΕ αφού τόνισε ότι η ΕΕ μπορεί να εκδώσει μια απόφαση επάρκειας βάσει του άρθρου 45, παράγραφος 3 του ΓΚΠΔ μόνο εάν η νομοθεσία της τρίτης χώρας περιλαμβάνει όλες τις απαραίτητες εγγυήσεις για τη διασφάλιση ικανοποιητικού επίπεδο προστασίας, προέβη σε αξιολόγηση του επιπέδου προστασίας που παρέχουν οι ΗΠΑ. Στο πλαίσιο της αξιολόγησης του, το Δικαστήριο επεσήμανε τις εκτεταμένες δυνατότητες παρακολούθησης που υπάρχουν βάσει των νόμων περί εθνικής ασφάλειας των ΗΠΑ - επικεντρώνοντας την προσοχή του στο άρθρο 702 του νόμου FISA (Foreign Intelligence Surveillance Act)[113] και στο εκτελεστικό διάταγμα ΕΟ 12333[114] σε συνδυασμό με την Προεδρική Οδηγία Πολιτικής

[111] ΔΕΕ, C-311/18, *Schrems II*, ο.π., παράγραφος 120.
[112] ΔΕΕ, C-311/18, *Schrems II*, ο.π., παράγραφος 164.
[113] Το συγκεκριμένο άρθρο επιτρέπει στην κυβέρνηση των ΗΠΑ να διεξάγει στοχευμένη παρακολούθηση αλλοδαπών προσώπων που βρίσκονται εκτός των ΗΠΑ, με την υποχρεωτική συνδρομή των παρόχων υπηρεσιών ηλεκτρονικών επικοινωνιών για την συγκέντρωση πληροφοριών από την αλλοδαπή.
[114] Το εκτελεστικό αυτό διάταγμα αποτελεί μια γενική οδηγία, βάσει της οποίας διεξάγονται ποικίλες δραστηριότητες των μυστικών υπηρεσιών των ΗΠΑ, συμπεριλαμβανομένων ορισμένων δραστηριοτήτων ηλεκτρονικής παρακολούθησης.

(Presidential Policy Directive - PPD) 28[115]. Το εν λόγω κανονιστικό πλαίσιο ρυθμίζει την πρόσβαση και τη χρήση από τις αμερικανικές δημόσιες αρχές των δεδομένων προσωπικού χαρακτήρα που εισάγονται από την ΕΕ στις ΗΠΑ, και δεν διαθέτει τους αναγκαίους ελέγχους για την επαρκή προστασία των υποκειμένων των δεδομένων της ΕΕ που ενδέχεται να γίνουν στόχος ερευνών για λόγους εθνικής ασφάλειας.

Πιο συγκεκριμένα, κατά το ΔΕΕ, οι περιορισμοί στην προστασία των δεδομένων προσωπικού χαρακτήρα, οι οποίοι απορρέουν από την εσωτερική κανονιστική ρύθμιση των ΗΠΑ σχετικά με την πρόσβαση των αμερικανικών δημοσίων αρχών σε διαβιβαζόμενα δεδομένα από την ΕΕ προς τις ΗΠΑ, και με την εκ μέρους τους χρήση τέτοιων δεδομένων - περιορισμοί που αξιολογήθηκαν από την Επιτροπή στην απόφαση για την Ασπίδα Προστασίας της Ιδιωτικής Ζωής - δεν οριοθετούνται με τέτοιον τρόπο ώστε να ανταποκρίνονται σε απαιτήσεις ουσιαστικά ισοδύναμες με εκείνες που επιβάλλει το δίκαιο της ΕΕ. Ειδικότερα, έκρινε πως *«ούτε το άρθρο 702 του FISA ούτε το Ε.Ο. 12333, σε συνδυασμό με την PPD 28, ανταποκρίνονται στις ελάχιστες απαιτήσεις που συνδέονται, κατά το δίκαιο της Ένωσης, με την αρχή της αναλογικότητας, οπότε δεν μπορεί να γίνει δεκτό ότι τα προγράμματα παρακολούθησης τα οποία στηρίζονται στις διατάξεις αυτές περιορίζονται στο απολύτως αναγκαίο»*[116].

[115] Η Προεδρική Οδηγία Πολιτικής 28, που εκδόθηκε στις 17 Ιανουαρίου 2014, διατυπώνει αρχές και επιβάλλει ορισμένους περιορισμούς για τις σχετικές με τις «πληροφορίες σημάτων» πράξεις για σκοπούς εξωτερικής αντικατασκοπείας. Συγκεκριμένα, η ενότητα 4 της Προεδρικής Οδηγίας Πολιτικής 28 καθορίζει αρχές για τη διασφάλιση των προσωπικών πληροφοριών που συλλέγονται από δραστηριότητες που σχετίζονται με τη συλλογή πληροφοριών σημάτων, και απαιτεί από τις μονάδες της κοινότητα των υπηρεσιών πληροφοριών να θεσπίσουν πολιτικές και διαδικασίες για την εφαρμογή των αρχών αυτών, σύμφωνα με τις τεχνικές δυνατότητες και τις επιχειρησιακές ανάγκες. Η Προεδρική Οδηγία Πολιτικής 28 είναι ιδιαίτερα σημαντική για πρόσωπα που δεν είναι πολίτες των ΗΠΑ, συμπεριλαμβανομένων των προσώπων από την ΕΕ στα οποία αναφέρονται τα δεδομένα. Βλ. σχετικά Ευρωπαϊκή Επιτροπή (2016), *Εκτελεστική Απόφαση (ΕΕ) 2016/1250 της Επιτροπής της 12ης Ιουλίου 2016 βάσει της οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την επάρκεια της προστασίας που παρέχεται από την ασπίδα προστασίας της ιδιωτικής ζωής ΕΕ–ΗΠΑ*, ο.π., Αιτιολογικές Σκέψεις 69 και 70, και Παράρτημα VI, σε συνδυασμό με Ομοσπονδιακό Γραφείο των ΗΠΑ (Federal Bureau of Investigation - FBI), *«FBI Policies and Procedures for Safeguarding Personal Information as Required by PPD-28 (Signals Intelligence Activities)»*. Διαθέσιμο στο: https://www.fbi.gov/file-repository/ppd-28-policies-procedures-signed.pdf/view. Η Προεδρική Οδηγία Πολιτικής 28 συνιστά την απάντηση της αμερικανικής κυβέρνησης (επί της προεδρίας του Barack Obama) στις αποκαλύψεις του Edward Snowden, η οποία επιχειρεί να περιορίσει τη μαζική παρακολούθηση, βλ. Churches, G. and Zalnieriute, M. (2020), «Contracting Out" Human Rights in International Law: Schrems II and the Fundamental Flaws of U.S. Surveillance Law», *Harvard International Law Journal*. Διαθέσιμο στο: https://harvardilj.org/2020/08/contracting-out-human-rights-in-international-law-schrems-ii-and-the-fundamental-flaws-of-u-s-surveillance-law/.

[116] ΔΕΕ, C-311/18, *Schrems II*, ο.π., παράγραφοι 184 και 185.

Βασιζόμενο στις διαπιστώσεις που περιέχονται στην απόφαση για την Ασπίδα Προστασίας της Ιδιωτικής Ζωής, το Δικαστήριο της ΕΕ τόνισε ότι, σε σχέση με ορισμένα προγράμματα παρακολούθησης (όπως το PRISM ή το UPSTREAM), ουδόλως προκύπτει από την εν λόγω κανονιστική ρύθμιση η ύπαρξη περιορισμών στην εξουσιοδότηση που παρέχεται για την εφαρμογή των προγραμμάτων αυτών, όπως δεν προκύπτει και η ύπαρξη εγγυήσεων για τους μη Αμερικανούς πολίτες, τους οποίους αφορούν εν δυνάμει τα σχετικά προγράμματα[117]. Το Δικαστήριο επεσήμανε ότι η προαναφερθείσα κανονιστική ρύθμιση θέτει μεν απαιτήσεις, τις οποίες οι αμερικανικές δημόσιες αρχές οφείλουν να τηρούν κατά την εφαρμογή των οικείων προγραμμάτων παρακολούθησης, πλην όμως δεν παρέχει στα υποκείμενα των δεδομένων εκτελεστά δικαιώματα δυνάμενα να προβληθούν εναντίον των αμερικανικών δημοσίων αρχών ενώπιον δικαστηρίων[118], παραβιάζοντας, κατά συνέπεια, στην ουσία του το θεμελιώδες δικαίωμα των πολιτών στην αποτελεσματική δικαστική προστασία[119].

Αναφορικά δε με την απαίτηση δικαστικής προστασίας, το Δικαστήριο απεφάνθη ότι, σε αντίθεση με την κρίση της Επιτροπής στην απόφαση για την Ασπίδα Προστασίας της Ιδιωτικής Ζωής, ο προβλεπόμενος στην εν λόγω απόφαση μηχανισμός διαμεσολάβησης («*Ombudsperson Mechanism*») δεν παρέχει στα υποκείμενα των δεδομένων ένα μέσο δικαστικής προστασίας ενώπιον οργάνου που να προσφέρει εγγυήσεις ουσιαστικά ισοδύναμες με εκείνες που επιβάλλει το δίκαιο της ΕΕ, ώστε να διασφαλίζεται τόσο η ανεξαρτησία του διαμεσολαβητή στο πλαίσιο του επίμαχου μηχανισμού, όσο και η ύπαρξη κανόνων, οι οποίοι να εξουσιοδοτούν το διαμεσολαβητή να εκδίδει αποφάσεις δεσμευτικές για τις αμερικανικές υπηρεσίες πληροφοριών[120].

Όλα τα παραπάνω καταδεικνύουν το βαθμό παρέμβασης στα θεμελιώδη δικαιώματα των προσώπων, των οποίων τα δεδομένα διαβιβάζονται στις ΗΠΑ, γεγονός που οδήγησε το Δικαστήριο στο συμπέρασμα ότι η απόφαση για την Ασπίδα Προστασίας της Ιδιωτικής Ζωής δεν μπορούσε να παράσχει ουσιαστικά ισοδύναμες εγγυήσεις για τα θεμελιώδη δικαιώματα, με εκείνες που κατοχυρώνονται βάσει της έννομης τάξης της ΕΕ και, ως εκ τούτου, την κήρυξε ανίσχυρη[121], με αποτέλεσμα να τεθεί εκτός ισχύος το σύστημα διαβίβασης δεδομένων

[117] ΔΕΕ, C-311/18, *Schrems II*, ο.π., παράγραφος 180.
[118] ΔΕΕ, C-311/18, *Schrems II*, ο.π., παράγραφος 192.
[119] Βλ. Κόμνιου Κ. (2020), «Η διαβίβαση προσωπικών δεδομένων σε τρίτες χώρες μετά την απόφαση Schrems II -"Now what?», *Capital. Gr*. Διαθέσιμο στο: https://www.capital.gr/me-apopsi/3485424/i-diabibasi-prosopikon-dedomenon-se-trites-xores-meta-tin-apofasi-schrems-ii-now-what.
[120] ΔΕΕ, C-311/18, *Schrems II*, ο.π., παράγραφοι 191, 195, 196 και 197.
[121] ΔΕΕ, C-311/18, *Schrems II*, ο.π., παράγραφος 201.

προσωπικού χαρακτήρα προς τις ΗΠΑ που στηριζόταν στην ασπίδα προστασίας της ιδιωτικής ζωής ΕΕ - ΗΠΑ.

ΕΝΟΤΗΤΑ ΙΙΙ - Η «ΜΕΤΑ SCHREMS II» ΕΠΟΧΗ

Η απόφαση *Schrems II* του Δικαστηρίου της ΕΕ δικαίωσε για δεύτερη φορά τον Max Schrems στην προσπάθεια διαφύλαξης του θεμελιώδους δικαιώματος του ανθρώπου στην προστασία των δεδομένων προσωπικού χαρακτήρα που τον αφορούν. Όπως ο ίδιος δήλωσε χαρακτηριστικά: «*Είμαι πολύ χαρούμενος για την απόφαση... Πρόκειται για ένα ολοκληρωτικό πλήγμα για την ιρλανδική ΑΠΔ και την Facebook. Είναι σαφές ότι οι ΗΠΑ θα πρέπει να αλλάξουν τους νόμους περί παρακολούθησης, εάν οι αμερικανικές εταιρείες θέλουν να συνεχίσουν να διαδραματίζουν σημαντικό ρόλο στην αγορά της ΕΕ*»[122].

Σε θεωρητικό επίπεδο, η απόφαση *Schrems II* εμφανίζεται ως μια ισχυρή συνταγματική επιβεβαίωση της σημασίας που έχει η οικοδόμηση ενός σταθερού, ολοκληρωμένου και συνεκτικού καθεστώτος προστασίας των ευρωπαϊκών διαβιβάσεων δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων και έναντι της κυβερνητικής πρόσβασης στα δεδομένα αυτά. Ωστόσο, στην πράξη η απόφαση δημιούργησε πολλές αβεβαιότητες σχετικά με τη νομική βάση για τις μελλοντικές διαβιβάσεις δεδομένων από την ΕΕ προς τις ΗΠΑ και τον υπόλοιπο κόσμο. Η μεγαλύτερη, επομένως, πρόκληση μετά την απόφαση *Schrems II* είναι να καθοριστεί ο τρόπος «συμφιλίωσης» της θεωρίας με την πράξη[123].

Από την άλλη πλευρά του Ατλαντικού, εδώ και καιρό διαμαρτύρονται για την προσπάθεια επιβολής παγκοσμιοποιημένων ρυθμιστικών κανόνων («unilateral regulatory globalization») από την ΕΕ, το οποίο μεταφράζεται σε επιβολή από ένα μεγάλο παίκτη της παγκόσμιας αγοράς των δικών του ρυθμιστικών όρων. Στην προκειμένη περίπτωση, η ΕΕ κατηγορείται ότι, αφού δημιούργησε μια σειρά κανόνων πολύ αυστηρότερων από τις άλλες δικαιοδοσίες, οδήγησε στην επιβολή εξαιρετικά περιοριστικών μέτρων για την επίβλεψη των δεσμευτικών κανόνων, τόσο από ιδιώτες όσο και από δημόσιους φορείς. Ωστόσο, αυτοί που πλήττονται περισσότερο από αυτή την αυστηροποίηση είναι οι αμερικανικοί κολοσσοί της πληροφορικής και του διαδικτύου, αλλά και οι υπηρεσίες ασφάλειας των ΗΠΑ[124].

---

[122] Βλ. NOYB (2020), «CJEU Judgment - First Statement», *noyb.eu*. Διαθέσιμο στο: https://noyb.eu/en/cjeu.

[123] Βλ. σχετικά Christakis, T. (2020), «After Schrems II : Uncertainties on the Legal Basis for Data Transfers and Constitutional Implications for Europe», *European Law Blog*. Διαθέσιμο στο: https://europeanlawblog.eu/2020/07/21/after-schrems-ii-uncertainties-on-the-legal-basis-for-data-transfers-and-constitutional-implications-for-europe/.

[124] Τάσσης Σ. (2020), «Schrems II - και τώρα τι;», *Lawyer - The Business Magazine*. Διαθέσιμο στο:: https://lawyermagazine.gr/schrems-ii-kai-twra-ti/.

Στο τρίτο μέρος της παρούσας μελέτης θα αποτυπωθεί αρχικά ο αντίκτυπος της απόφασης *Schrems II* στο σύνολο των μηχανισμών διαβίβασης του ΓΚΠΔ, καθώς και η θέση που έλαβαν οι ΗΠΑ απέναντι στου αυστηρούς ρυθμιστικούς όρους που έθεσε η ευρωπαϊκή νομολογία **(Α)**. Εν συνεχεία, θα αναδειχθεί η καθοριστική συμβολή του ΕΣΠΔ τόσο στην ερμηνεία των νέων υποχρεώσεων που «σφυρηλάτησε» το ΔΕΕ, όσο και στον τρόπο εφαρμογής αυτών (**Β)**. Τέλος, αφού γίνει μια συνοπτική παρουσίαση και προσέγγιση των νεών ΤΣΡ που υιοθέτησε η Επιτροπή **(Γ)**, θα εξετάσουμε ορισμένα ζητήματα που έχουν ανακύψει στη «μετά Schrems II» εποχή, καθώς και τις πρώτες προσπάθειες τόσο της Επιτροπής όσο και των ΑΠΔ να εφαρμόσουν τα νέα αυστηρά κριτήρια που έθεσε το ΔΕΕ **(Δ)**.

Α. Η ΑΠΟΔΟΜΗΣΗ ΤΩΝ ΜΗΧΑΝΙΣΜΩΝ ΔΙΑΒΙΒΑΣΗΣ ΚΑΙ Η ΘΕΣΗ ΤΩΝ ΗΠΑ

Μπορεί το Δικαστήριο της ΕΕ να περιόρισε την κρίση του στην απόφαση για την Ασπίδα Προστασίας της Ιδιωτικής Ζωής και τις ΤΣΡ σε ότι αφορά τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα στις ΗΠΑ, όμως το σκεπτικό της απόφασης *Schrems II* τυγχάνει εφαρμογής στο σύνολο των κατάλληλων εγγυήσεων του άρθρου 46 του ΓΚΠΔ, όπως τους ΔΕΚ **(1)**, αλλά και στις παρεκκλίσεις του άρθρου 49 του Κανονισμού **(2)**. Οι ΗΠΑ από την πλευρά τους δεν άργησα να πάρουν θέση απέναντι στους αυστηρούς περιορισμούς που έθεσε η ευρωπαϊκή νομολογία δημοσιεύοντας μια Λευκή Βίβλο επί των αμερικανικών εγγυήσεων που αφορούν στις ΤΣΡ και τις άλλες νομικές βάσεις για τη διαβίβαση δεδομένων από την ΕΕ στις ΗΠΑ **(3)**. Ταυτόχρονα, οι ΗΠΑ έσπευσαν να εντοπίσουν από κοινού με τα θεσμικά όργανα της ΕΕ τη λύση που θα μπορούσε να διασφαλίσει αποτελεσματικά την διατλαντική ροή δεδομένων **(4)**.

1. Η έμμεση κρίση για τους Δεσμευτικούς Εταιρικούς Κανόνες

Κατά το ΕΣΠΔ, δεδομένης της απόφασης του Δικαστηρίου, με την οποία κηρύχθηκε άκυρη η απόφαση για την Ασπίδα Προστασίας της Ιδιωτικής Ζωής λόγω του βαθμού επέμβασης που δημιουργεί η νομοθεσία των ΗΠΑ στα θεμελιώδη δικαιώματα των προσώπων, των οποίων τα δεδομένα διαβιβάζονται στην εν λόγω τρίτη χώρα, και του γεγονότος ότι το πλαίσιο της ασπίδας προστασίας της ιδιωτικής ζωής ΕΕ - ΗΠΑ είχε επίσης σκοπό να παρέχει εγγυήσεις στα δεδομένα που διαβιβάζονται με άλλους μηχανισμούς, η κρίση του

Δικαστηρίου της ΕΕ επιδρά και στην εφαρμογή των ΔΕΚ, εφόσον η νομοθεσία των ΗΠΑ υπερισχύει και έναντι αυτού του μηχανισμού διαβίβασης[125].

Όπως είδαμε παραπάνω, οι εθνικές ΑΠΔ εγκρίνουν τους ΔΕΚ, αφού προηγουμένως διενεργηθεί έλεγχος αυτών για να διασφαλιστεί ότι οι κανόνες πληρούν τις απαιτήσεις του ΓΚΠΔ [βλ. Ενότητα Ι (Β)(2)(β)]. Η έγκριση, όμως, από μια εθνική ΑΠΔ δεν σημαίνει ότι όλες οι διαβιβάσεις εγκρίνονται αυτόματα, καθώς η εθνική ΑΠΔ δεν προβαίνει σε ανάλυση και αξιολόγηση της νομοθεσίας της χώρας προορισμού για να βεβαιώσει τη συμμόρφωση αυτής με τις απαιτήσεις του ΓΚΠΔ. Αντίθετα, εναπόκειται στον όμιλο εταιρειών να διασφαλίσει ότι η εθνική νομοθεσία των χωρών προορισμού σέβεται το ΓΚΠΔ. Επομένως, το κατά πόσο θα είναι εφικτή η διαβίβαση δεδομένων προσωπικού χαρακτήρα με βάση τους ΔΕΚ θα εξαρτηθεί από το αποτέλεσμα της κατά περίπτωση αξιολόγησης του εξαγωγέα δεδομένων (σε συνεργασία με τον εισαγωγέα δεδομένων) και των περιστάσεων της διαβίβασης, καθώς και των πρόσθετων μέτρων που τυχόν θα χρειαστεί να εφαρμοστούν ώστε να διασφαλιστεί ένα ουσιαστικά ισοδύναμο επίπεδο προστασίας με εκείνο που διασφαλίζεται εντός της ΕΕ.

Σε πρακτικό επίπεδο, τα πρόσθετα μέτρα, σε συνδυασμό με τους ΔΕΚ, μετά την ανάλυση των περιστάσεων που αφορούν στη διαβίβαση δεδομένων, θα πρέπει να διασφαλίζουν ότι η νομοθεσία της τρίτης χώρας δεν θίγει το επαρκές επίπεδο προστασίας που αυτά εγγυώνται. Μάλιστα, οι πιθανότητες να επιτευχθεί εν προκειμένω η δέουσα συνεργασία στο πλαίσιο της προαναφερθείσας αξιολόγησης είναι περισσότερες, καθώς η διαβίβαση δεδομένων μεταξύ υπευθύνων επεξεργασίας ή εκτελούντων την επεξεργασία στην περίπτωση των ΔΕΚ βασίζεται στην καθιερωμένη σχέση εμπιστοσύνης μεταξύ των μερών λόγω της συμμέτοχής τους στον ίδιο όμιλο εταιρειών και της άσκησης κοινής οικονομικής δραστηριότητας[126].

Όπως και στην περίπτωση των νέων ΤΣΡ, εάν ο εξαγωγέας δεδομένων καταλήξει στο συμπέρασμα ότι δεν μπορούν να διασφαλιστούν κατάλληλες εγγυήσεις, αφού έλαβε υπόψη του τις περιστάσεις της διαβίβασης και τα πιθανά πρόσθετα μέτρα, είναι υποχρεωμένος να αναστείλει ή να τερματίσει τη διαβίβαση των δεδομένων προσωπικού χαρακτήρα. Ωστόσο,

[125] Βλ. Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (2020), *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*. Βέλγιο: Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. Διαθέσιμο στο: https://edpb.europa.eu/sites/default/files/files/file1/edpb_faqs_schrems_ii_202007_adopted_el.pdf.

[126] Βλ. Kosta, E., Leenes, R. and Irene Kamara (2022), *Research Handbook on EU Data Protection Law*. Ηνωμένο Βασίλειο: Edward Elgar Publishing, σελ. 24.

εάν επιθυμεί να συνεχίσει τη διαβίβαση δεδομένων παρά το συμπέρασμα αυτό, θα πρέπει να ειδοποιήσει την αρμόδια ΑΠΔ.

2. Η διέξοδος των παρεκκλίσεων

Προκειμένου να αποφευχθεί «η δημιουργία νομικού κενού», το ίδιο το ΔΕΕ στην καταληκτική του κρίση στην απόφαση *Schrems II* επεσήμανε ότι εξακολουθεί να είναι δυνατή η διαβίβαση δεδομένων από την ΕΕ στις ΗΠΑ (και συνακόλουθα σε όλες τις τρίτες χώρες) βάσει των παρεκκλίσεων που προβλέπονται στο άρθρο 49 του ΓΚΠΔ, υπό τον όρο ότι ισχύουν οι προϋποθέσεις που ορίζονται στο συγκεκριμένο άρθρο [βλ. Ενότητα 1(Β)(3)][127]. Μάλιστα, στο πλαίσιο χρήσης του συγκεκριμένου μηχανισμού διαβίβασης μπορούν να ληφθούν υπόψη οι κατευθυντήριες γραμμές του ΕΣΠΔ που έχουν καταρτίσει ειδικά για τη συγκεκριμένη διάταξη[128].

Εντούτοις, η εν λόγω κρίση του ΔΕΕ δεν είναι βάσιμη, καθώς η απόφαση *Schrems II* δημιούργησε νομικό κενό, δεδομένου ότι οι διαβιβάσεις δεδομένων προσωπικού χαρακτήρα από την ΕΕ στις ΗΠΑ βάσει της απόφασης για την Ασπίδα Προστασίας της Ιδιωτικής Ζωής, οι οποίες ήταν νόμιμες πριν από την απόφαση του ΔΕΕ, κατέστησαν παράνομες από την ημερομηνία έκδοσης της εν λόγω απόφασης[129].

Επιπροσθέτως, δεν είναι σαφές το κατά πόσο οι παρεκκλίσεις θα αποτελέσουν τον κατάλληλο εναλλακτικό μηχανισμό διαβίβασης, αφού, όπως έχει επισημανθεί ανωτέρω, ο εν λόγω μηχανισμός διαβίβασης δεν παρέχει από μόνος του προστασία για τη διαβίβαση δεδομένων, δεδομένου ότι προορίζεται να καλύψει καταστάσεις στις οποίες δεν υπάρχει επαρκής προστασία στη χώρα προορισμού, αλλά οι κίνδυνοι για το υποκείμενο των δεδομένων είναι σχετικά μικροί ή άλλα συμφέροντα (δημόσια συμφέροντα ή συμφέροντα του ίδιου του υποκειμένου των δεδομένων) υπερισχύουν του δικαιώματος του υποκειμένου των δεδομένων στην ιδιωτική ζωή[130]. Εξ αυτού του λόγου, οι παρεκκλίσεις πρέπει να

[127] ΔΕΕ, C-311/18, *Schrems II*, ο.π., παράγραφος 202.

[128] Βλ. Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (2018), *Κατευθυντήριες γραμμές 2/2018 αναφορικά με τις παρεκκλίσεις που προβλέπονται στο άρθρο 49 του Κανονισμού 2016/679*, ο.π., σελ. 3.

[129] Βλ. σχετικά Tracol, X. (2020), «"Schrems II": The return of the Privacy Shield», *Computer Law & Security Review*, Volume 39. Διαθέσιμο στο: https://www.sciencedirect.com/science/article/pii/S0267364920300893?via%3Dihub.

[130] Κατά αναλογία με τις διατάξεις της προισχύσας Οδηγίας, βλ. Ομάδα εργασίας του άρθρου 29 (1998), *Transfers of personal data to third countries : Applying Articles 25 and 26 of the EU data protection directive*, σελ. 24. Βέλγιο: Ομάδα εργασίας του άρθρου 29. Διαθέσιμο στο: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1998/wp12_en.pdf.

ερμηνεύονται περιοριστικά[131], και να χρησιμοποιούνται με φειδώ, επί τη βάσει των κατευθυντήριων γραμμών του ΕΣΠΔ[132].

Για παράδειγμα, σε ότι αφορά την παρέκκλιση της συγκατάθεσης του υποκειμένου των δεδομένων[133], η συγκατάθεση θα πρέπει να είναι ρητή για τη συγκεκριμένη διαβίβαση δεδομένων ή σειρά διαβιβάσεων (ήτοι ο εξαγωγέας δεδομένων να λάβει ειδική συγκατάθεση πριν από τη διαβίβαση, ακόμη και εάν αυτή πραγματοποιείται μετά τη συλλογή των δεδομένων), και να έχει προηγηθεί ενημέρωση του υποκειμένου των δεδομένων, ιδίως για τους πιθανούς κινδύνους που απορρέουν, αφενός, από το γεγονός ότι τα δεδομένα του θα διαβιβαστούν σε μια τρίτη χώρα που δεν προσφέρει κατάλληλη προστασία και, αφετέρου, από τη μη εφαρμογή κατάλληλων διασφαλίσεων για την προστασία των δεδομένων[134].

3. Η θέση των ΗΠΑ

Από την πλευρά της η αμερικανική κυβέρνηση δεν έμεινε αδρανής μπροστά στην απόφαση *Schrems II*, η οποία επιφόρτισε τις ιδιωτικές επιχειρήσεις που διαβιβάζουν δεδομένα στις ΗΠΑ επί τη βάσει του μηχανισμού των ΤΣΡ με την υποχρέωση να διεξάγουν προηγούμενη αξιολόγηση της ισχύουσας νομοθεσίας των ΗΠΑ σχετικά με την πρόσβαση των μυστικών υπηρεσιών στα δεδομένα προσωπικού χαρακτήρα. Έτσι, στις 20 Σεπτεμβρίου του 2020 η αμερικανική κυβέρνηση, και συγκεκριμένα το Υπουργείο Εμπορίου των ΗΠΑ σε συνεργασία με το Υπουργείο Δικαιοσύνης και το Γραφείο του Διευθυντή της Εθνικής Υπηρεσίας Πληροφοριών (Department of Justice and the Office of the Director of National Intelligence) δημοσιοποίησε Λευκή Βίβλο (White Paper)[135], στην οποία αποτύπωσε τη δική του θέση απέναντι στην κρίση του Δικαστηρίου της ΕΕ.

---

[131] ΔΕΕ, C-362/14, *Schrems I*, ο.π., παράγραφος 92, και ΔΕΕ, συνεκδικαζόμενες υποθέσεις C-293/12 και C-594/12, *Digital Rights Ireland Ltd κατά Minister for Communications, Marine and Natural Resources κ.λπ. και Kärntner Landesregierung κ.λπ.*, 8 Απριλίου 2014, παράγραφος 52 και εκεί παρατιθέμενη νομολογία, ηλεκτρονικά διαθέσιμη στον ακόλουθο σύνδεσμο: https://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=EL&mode=lst&dir=&occ=first&part=1&cid=3284789. Σε συνδυασμό με Kuner, C. (2021), «Territorial Scope and Data Transfer Rules in the GDPR: Realising the EU's Ambition of Borderless Data Protection», ο.π.

[132] Βλ. Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (2018), *Κατευθυντήριες γραμμές 2/2018 αναφορικά με τις παρεκκλίσεις που προβλέπονται στο άρθρο 49 του Κανονισμού 2016/679*, ο.π., σελ. 3.

[133] Άρθρο 49, παράγραφος 1, στοιχείο α' του ΓΚΠΔ.

[134] Βλ. Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (2020), *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*, ο.π., ερώτημα 8.

[135] United States Department of Commerce (2020), *Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II*, ο.π.

Η εν λόγω Λευκή Βίβλος παρουσιάζει λεπτομερώς το ευρύ φάσμα πληροφοριών σχετικά με την προστασία της ιδιωτικής ζωής στην ισχύουσα αμερικανική νομοθεσία και πρακτική που αφορά στην κυβερνητική πρόσβαση σε δεδομένα προσωπικού χαρακτήρα για σκοπούς εθνικής ασφάλειας, εστιάζοντας ιδίως στα θέματα που απασχόλησαν το ΔΕΕ στην απόφαση *Schrems II*. Απώτερος σκοπός της Λευκής Βίβλου είναι οι πληροφορίες αυτές να ληφθούν υπόψη από τις ιδιωτικές επιχειρήσεις που διαβιβάζουν δεδομένα προσωπικού χαρακτήρα από την ΕΕ στις ΗΠΑ, στο πλαίσιο της υποχρεωτικής αξιολόγησης που διενεργούν για την εθνική νομοθεσία της χώρας προορισμού.

Σύμφωνα με τη συνοδευτική επιστολή της Λευκής Βίβλου[136], η τελευταία «*περιγράφει τα ισχυρά όρια και τις εγγυήσεις στις Ηνωμένες Πολιτείες που αφορούν την κυβερνητική πρόσβαση στα δεδομένα*», στο πλαίσιο «*μιας προσπάθειας να βοηθηθούν οι οργανισμοί να αξιολογήσουν κατά πόσον οι διαβιβάσεις τους προσφέρουν κατάλληλη προστασία των δεδομένων σύμφωνα με την απόφαση του ΔΕΕ*». Λόγω, μάλιστα, της σημασίας της «*διατλαντικής οικονομικής σχέσης ύψους 7,1 τρισεκατομμυρίων δολαρίων*», «*η* [τότε] *κυβέρνηση Τραμπ διερευνά όλες τις επιλογές που έχει στη διάθεσή της και παραμένει δεσμευμένη να συνεργαστεί με την Ευρωπαϊκή Επιτροπή για τη διαπραγμάτευση μιας λύσης που να ικανοποιεί τις απαιτήσεις του ΔΕΕ και ταυτόχρονα να προστατεύει τα συμφέροντα των Ηνωμένων Πολιτειών*».

Τα σημαντικότερα σημεία που ανέδειξε η Λευκή Βίβλος αναφορικά με τις εγγυήσεις που ισχύουν βάσει της αμερικανικής νομοθεσίας για τον περιορισμό της συλλογής δεδομένων προσωπικού χαρακτήρα από τις αμερικανικές υπηρεσίες πληροφοριών, είναι τα ακόλουθα:

(α) Τα ζητήματα πρόσβασης σε δεδομένα προσωπικού χαρακτήρα λόγω εθνικής ασφάλειας που απασχόλησαν το ΔΕΕ δεν αφορούν τις περισσότερες ιδιωτικές επιχειρήσεις, καθώς τα δεδομένα που διαχειρίζονται δεν ενδιαφέρουν την κοινότητα των αμερικανικών μυστικών υπηρεσιών. Οι περισσότερες ιδιωτικές επιχειρήσεις που δραστηριοποιούνται στην ΕΕ δεν διαχειρίζονται, και δεν έχουν λόγους να πιστεύουν ότι διαχειρίζονται, δεδομένα που ενδιαφέρουν τις αμερικανικές υπηρεσίες πληροφοριών. Μάλιστα, σύμφωνα με τη Λευκή Βίβλο το υποθετικό σενάριο μονομερούς πρόσβασης μιας αμερικάνικης υπηρεσίας πληροφοριών σε δεδομένα

[136] United States Department of Commerce (2020*), Letter from Deputy Assistant Secretary James Sullivan on the Schrems II Decision*. Ουάσιγκτον, ΗΠΑ: United States Department of Commerce. Διαθέσιμο στο: https://www.commerce.gov/about/letter-deputy-assistant-secretary-james-sullivan-schrems-ii-decision.

που διαβιβάζονται από την ΕΕ, χωρίς να το γνωρίζει η επιχείρηση, δεν διαφέρει από το υποθετικό σενάριο οι υπηρεσίες πληροφοριών άλλων κυβερνήσεων, συμπεριλαμβανομένων εκείνων των κρατών-μελών της ΕΕ, να αποκτήσουν πρόσβαση σε δεδομένα προσωπικού χαρακτήρα.

(β) Σε περίπτωση που ζητηθεί η πρόσβαση από τις αμερικανικές δημόσιες αρχές, οι ιδιωτικές επιχειρήσεις που διαβιβάζουν δεδομένα προσωπικού χαρακτήρα από την ΕΕ μπορούν χρησιμοποιήσουν ως νομική βάση για τη διαβίβαση την παρέκκλιση του δημοσίου συμφέροντος που προβλέπεται στο άρθρο 49 του ΓΚΠΔ. Προς αυτή την κατεύθυνση, άλλωστε, συνηγορεί και η καταληκτική κρίση του ΔΕΕ στην απόφαση *Schrems II*, σύμφωνα με την οποία ο μηχανισμός των παρεκκλίσεων εξακολουθεί να είναι διαθέσιμος για τη διαβίβαση των δεδομένων στις ΗΠΑ, παρά το γεγονός ότι η απόφαση για την Ασπίδα Προστασίας της Ιδιωτικής Ζωής δεν είναι πλέον ισχυρή[137]. Παράλληλα, και το ίδιο το ΕΣΠΔ είχε αναγνωρίσει ότι η κοινή χρήση δεδομένων στο πνεύμα αμοιβαιότητας για τη διεθνή συνεργασία θεωρείται «*σημαντικό δημόσιο συμφέρον*» σύμφωνα με την παράγραφο 3 του άρθρου 49 του ΓΚΠΔ[138]. Ο εν λόγω διαμοιρασμός δεδομένων είναι ζωτικής σημασίας για τη συλλογική ασφάλεια και την αντιμετώπιση ποικίλων απειλών, όπως της διεθνούς τρομοκρατίας και της διάδοσης όπλων μαζικής καταστροφής. Προς υποστήριξη αυτής της θέσης, η Λευκή Βίβλος περιγράφει τη συχνή ανταλλαγή πληροφοριών μεταξύ της κυβέρνησης των ΗΠΑ και των κυβερνήσεων των κρατών-μελών της ΕΕ για την αντιμετώπιση των προαναφερθέντων απειλών, η οποία αναμφίβολα εξυπηρετεί σημαντικά δημόσια συμφέροντα της ΕΕ προστατεύοντας τις κυβερνήσεις και τους πολίτες των κρατών-μελών.

(γ) Για τις ιδιωτικές επιχειρήσεις, οι οποίες επιλέγουν ως μηχανισμό διαβίβασης των δεδομένων τις ΤΣΡ, και άρα θα πρέπει να προβούν σε αξιολόγηση του νομοθετικού πλαισίου των ΗΠΑ, η Λευκή Βίβλος θέτει στη διάθεσή τους πληροφορίες επί του αμερικανικού κανονιστικού πλαισίου, τις οποίες δεν έλαβε υπόψη του το ΔΕΕ στην απόφαση *Schrems II*, καθώς δεν υφίσταντο όταν δημοσιεύθηκε η απόφαση για την

[137] ΔΕΕ, C-311/18, *Schrems II*, ο.π., παράγραφος 202.

[138] Ευρωπαϊκή Επιτροπή (2018), *Κατευθυντήριες γραμμές 2/2018 του ΕΣΠΔ αναφορικά με τις παρεκκλίσεις που προβλέπονται στο άρθρο 49 του κανονισμού 2016/679*, ο.π., σημείο 2.4.

Ασπίδα Προστασίας της Ιδιωτικής Ζωής. Μάλιστα, παρέχει παραπομπές σε έγγραφα και πηγές που προσφέρουν πρόσθετες σχετικές πληροφορίες[139].

Αξιοσημείωτο είναι ότι μέσω της Λευκής Βίβλου αποσαφηνίστηκαν οι πτυχές εκείνες του αμερικανικού δικαίου που, παρά το γεγονός ότι το ΔΕΕ παρέλειψε να τις λάβει υπόψη του, θα φανούν χρήσιμες στο έργο αξιολόγησης της νομοθεσίας της χώρας προορισμού από τους εξαγωγείς και εισαγωγείς δεδομένων. Πιο συγκεκριμένα, η Λευκή Βίβλος περιορίστηκε στα νομοθετήματα που έλαβε υπόψη κατά την κρίση του το ΔΕΕ, και επεσήμανε συνοπτικά τα εξής:

(α) Σε ότι αφορά το άρθρο 702 του νόμου FISA, στη Λευκή Βίβλο αφενός επεξηγείται ο ενεργός ρόλος του United States Foreign Intelligence Surveillance Court (Δικαστήριο δυνάμει του νόμου FISA, εφεξής «**FISC**»)[140] ως προς τα μέτρα παρακολούθησης σε ατομική βάση - τον οποίο είχε αμφισβητήσει με κατηγορηματικό τρόπο το ΔΕΕ στην απόφαση *Schrems II*[141] - και αφετέρου απαριθμούνται τα ένδικά μέσα που έχει στην διάθεσή του το υποκείμενο των δεδομένων σε περίπτωση που θεωρήσει ότι τα δικαιώματά του επί των δεδομένων προσωπικού χαρακτήρα παραβιάζονται, καθώς και τις πρόσθετες εγγυήσεις προστασίας της ιδιωτικής ζωής που προστέθηκαν στο άρθρο 702 του νόμου FISA από την έκδοση της απόφασης για την Ασπίδα Προστασίας της Ιδιωτικής Ζωής, ήτοι από το 2017 και μετά, τα οποία δεν έλαβε υπόψη του συνολικά το ΔΕΕ. Στο πλαίσιο αυτό, παρουσιάζει ιδιαίτερο ενδιαφέρον η δήλωση, στην οποία προέβη η αμερικανική κυβέρνηση μέσω της Λευκής Βίβλου σχετικά με το εάν η προστασία της ιδιωτικής ζωής βάσει του άρθρο 702 του νόμου FISA ανταποκρίνεται στα νομικά πρότυπα της ΕΕ, παρέχοντας προστασία ουσιωδώς ισοδύναμη με την προστασία που παρέχεται στην ΕΕ. Σύμφωνα με την αμερικανική κυβέρνηση, τα δεδομένα που διαβιβάζονται στις ΗΠΑ απολαμβάνουν μεγαλύτερη προστασία όσον αφορά την παρακολούθηση πληροφοριών σε σύγκριση με τα δεδομένα που βρίσκονται εντός της ΕΕ, και τούτο διότι αφενός η ΕΕ δεν έχει καμία αρμοδιότητα επί θεμάτων εθνικής ασφάλειας, τα οποία αποτελούν αποκλειστική

[139] Office of the Director of National Intelligence (ODNI), «IC ON THE RECORD». Διαθέσιμο στο: https://icontherecord.tumblr.com/.

[140] Ομοσπονδιακό Δικαστήριο που στελεχώνεται από ανεξάρτητους, ισόβιους δικαστές, τους οποίους το καθεστώς FISA εξουσιοδοτεί να εγκρίνουν και να εποπτεύουν τη μυστική παρακολούθηση πληροφοριών από την αλλοδαπή.

[141] ΔΕΕ, C-311/18, *Schrems II*, ο.π., παράγραφος 179.

αρμοδιότητα των κρατών-μελών της ΕΕ, ενώ το Ευρωπαϊκό Δικαστήριο Ανθρωπίνων Δικαιωμάτων (εφεξής «**ΕΔΑΔ**»), το οποίο τακτικά αξιολογεί τα εγχώρια προγράμματα παρακολούθησης πληροφοριών των κρατών-μελών της ΕΕ, έχει επικυρώσει προγράμματα που είναι παρόμοια ή πιο εκτεταμένα από εκείνο του άρθρου 702 του νόμου FISA[142].

(β) Όσον αφορά το εκτελεστικό διάταγμα ΕΟ 12333, η Λευκή Βίβλος υπογραμμίζει ότι η κυβέρνηση των ΗΠΑ δεν μπορεί να απαιτήσει από νομικό ή φυσικό πρόσωπο την αποκάλυψη δεδομένων προσωπικού χαρακτήρα, ενώ η μαζική συλλογή δεδομένων απαγορεύεται ρητά. Εν συνεχεία, περιγράφονται λεπτομερώς οι διάφοροι κανονιστικοί περιορισμοί που επιβάλλονται για τη συλλογή και επεξεργασία δεδομένων προσωπικού χαρακτήρα που διενεργείται με βάση το εκτελεστικό διάταγμα ΕΟ 12333[143] που δεν εξετάστηκαν από το ΔΕΕ στην απόφαση *Schrems II*, παρά το γεγονός ότι οι πήγες των εν λόγω περιορισμών ήταν και είναι διαθέσιμες στο ευρύ κοινό.

4. Ο διάδοχος του Ασφαλούς Λιμένα και της Ασπίδας Προστασίας της Ιδιωτικής Ζωής

Στις 10 Αυγούστου 2020, το Υπουργείο Εμπορίου των ΗΠΑ και η Επιτροπή ανακοίνωσαν την έναρξη διαπραγματεύσεων για την αξιολόγηση των δυνατοτήτων ενός ενισχυμένου πλαισίου ασπίδας προστασίας της ιδιωτικής ζωής ΕΕ - ΗΠΑ για τη συμμόρφωση με την απόφαση *Schrems II*[144]. Όπως χαρακτηριστικά αναφέρει το Δελτίο Τύπου της Επιτροπής: «*Η Ευρωπαϊκή Ένωση και οι Ηνωμένες Πολιτείες αναγνωρίζουν τη ζωτική σημασία της προστασίας των δεδομένων και τη σημασία των διασυνοριακών διαβιβάσεων δεδομένων για τους πολίτες και τις οικονομίες μας… Καθώς αντιμετωπίζουμε από κοινού νέες προκλήσεις,*

[142] Βλ. United States Department of Commerce (2020), *Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II*, ο.π., σελ. 15 και η εκεί παρατιθέμενη νομολογία του ΕΔΑΔ.

[143] Για παράδειγμα, η Προεδρική Οδηγία Πολιτικής (Presidential Policy Directive - PPD) 28 - την οποία συμπεριέλαβε στην κρίση του το ΔΕΕ - οριοθετεί τη χρήση των σημάτων που συλλέγονται μαζικά για τον εντοπισμό και την αντιμετώπιση των ακόλουθων απειλών: (1) κατασκοπεία, (2) τρομοκρατία, (3) απειλές από όπλα μαζικής καταστροφής, (4) απειλές για την ασφάλεια στον κυβερνοχώρο, (5) απειλές κατά των δυνάμεων των ΗΠΑ ή των συμμάχων τους και (6) απειλές από το διεθνές έγκλημα. Για τους υπόλοιπους κανονιστικούς περιορισμούς βλ. United States Department of Commerce (2020), *Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II*, ο.π., σελ. 19 - 21.

[144] Ευρωπαϊκή Επιτροπή (2020), *Joint Press Statement by European Commissioner for Justice Didier Reynders and U.S. Secretary of Commerce Wilbur Ross*. Βέλγιο: Ευρωπαϊκή Επιτροπή. Διαθέσιμο στο: https://ec.europa.eu/info/news/joint-press-statement-european-commissioner-justice-didier-reynders-and-us-secretary-commerce-wilbur-ross-7-august-2020-2020-aug-07_en.

συμπεριλαμβανομένης της ανάκαμψης της παγκόσμιας οικονομίας μετά την πανδημία COVID-19, η συνεργασία μας θα ενισχύσει την προστασία των δεδομένων και θα προωθήσει μεγαλύτερη ενημερία για τα σχεδόν 800 εκατομμύρια πολιτών μας και στις δύο πλευρές του Ατλαντικού». Μάλιστα, οι εν λόγω διαπραγματεύσεις εντατικοποιήθηκαν κοινή συναινέσει καθιστώντας σαφή την κοινή δέσμευση της ΕΕ και των ΗΠΑ για την προστασία της ιδιωτικής ζωής, την προστασία των δεδομένων και του κράτους δικαίου, και την αμοιβαία αναγνώριση της σημασίας της διατλαντικής ροής δεδομένων[145].

Μέχρι πρότινος, βέβαια, οι ΗΠΑ δεν έδειχναν πρόθυμες να προβούν σε τροποποιήσεις του εσωτερικού τους καθεστώτος, καθώς αφενός μια τέτοια τροποποίηση του αμερικανικού δικαίου δεν θα ήταν εύκολο να πραγματοποιηθεί, και αφετέρου σύμφωνα με τα όσα εκτίθενται στην προαναφερθείσα Λευκή Βίβλο του Υπουργείου Εμπορίου, οι ΗΠΑ παρέχουν ήδη ένα ουσιαστικά ισοδύναμο νομοθετικό πλαίσιο για την προστασία των δεδομένων προσωπικού χαρακτήρα. Μάλιστα, ορισμένοι σχολιαστές αμφισβητούσαν (και, ίσως, εξακολουθούν να αμφισβητούν) εάν θα έπρεπε να πραγματοποιηθεί μια τέτοια τροποποίηση, με χαρακτηριστικό παράδειγμα τον πρώην Γενικό Σύμβουλο της Εθνικής Υπηρεσίας Ασφαλείας των ΗΠΑ, Stewart Baker[146], ο οποίος υποστήριξε ότι οι ΗΠΑ θα πρέπει να υπενθυμίσουν στην ΕΕ ότι έχουν το δικαίωμα να θεσμοθετούν χωρίς να παίρνουν άδεια από τις ευρωπαϊκές κυβερνήσεις[147].

Ωστόσο, στις 25 Μαρτίου 2022, η Επιτροπή και οι ΗΠΑ ανακοίνωσαν από κοινού τη συμφωνία για την υιοθέτηση ενός νέου Διατλαντικού Πλαισίου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (εφεξής «**Διατλαντικό Πλαίσιο**»)[148], το οποίο θα προωθήσει τη

---

[145] Δελτίο Τύπου Ευρωπαϊκής Επιτροπής (2021), *Intensifying Negotiations on transatlantic Data Privacy Flows: A Joint Press Statement by European Commissioner for Justice Didier Reynders and U.S. Secretary of Commerce Gina Raimondo*. Βέλγιο: Ευρωπαϊκή Επιτροπή. Διαθέσιμο στο: https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_21_1443.

[146] Υπηρέτησε ως Γενικός Σύμβουλος της Υπηρεσίας Εθνικής Ασφάλειας των ΗΠΑ για το χρονικό διάστημα 1992 - 1994.

[147] Baker, S. (2020), «How Can the U.S. Respond to Schrems II?», *Lawfare*. Διαθέσιμο στο: https://www.lawfareblog.com/how-can-us-respond-schrems-ii#, ο οποίος χαρακτηριστικά αναφέρει: «*… But now is the time to show Europe that the U.S. is serious about keeping in place effective counterterrorism measures - and keeping the right to write U.S. laws without getting permission from European governments*».

[148] Λευκός Οίκος (2022), *FACT SHEET: United States and European Commission Announce Trans-Atlantic Data Privacy Framework*. ΗΠΑ: Λευκός Οίκος. Διαθέσιμο στο: https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/.

διατλαντική ροή δεδομένων και θα εξαλείψει τις ανησυχίες που εξέφρασε το Δικαστήριο της ΕΕ στην απόφαση *Schrems II*.

Το εν λόγω Διατλαντικό Πλαίσιο αποτελεί αποτέλεσμα των διαπραγματεύσεων μεταξύ της ΕΕ και των ΗΠΑ εδώ και ένα χρόνο με επικεφαλής την Υπουργό Εμπορίου των ΗΠΑ, Gina Raimondo, και τον Επίτροπο Δικαιοσύνης της ΕΕ, Didier Reynders. Θα παράσχει μια διαρκή και αξιόπιστη νομική βάση για τη διατλαντική ροή δεδομένων, η οποία είναι ζωτικής σημασίας για την προστασία των δικαιωμάτων των πολιτών και τη δυνατότητα διατλαντικού εμπορίου σε όλους τους τομείς της οικονομίας, συμπεριλαμβανομένων των μικρών και μεσαίων επιχειρήσεων. Τοιουτοτρόπως, θα στηρίξει μια χωρίς αποκλεισμούς και ανταγωνιστική ψηφιακή οικονομία, ενώ θα τεθούν τα θεμέλια για περαιτέρω οικονομική συνεργασία μεταξύ των ΗΠΑ και της ΕΕ[149]. Άλλωστε, η ύπαρξη ενός σαφούς, ασφαλούς και ομοιόμορφου ρυθμιστικού πλαισίου για τις διατλαντικές διαβιβάσεις δεδομένων αποτελεί *conditio sine qua non* για τη συνέχιση και προαγωγή της παγκόσμιας οικονομικής δραστηριότητας[150].

Το νέο πλαίσιο σηματοδοτεί μια άνευ προηγουμένου δέσμευση των ΗΠΑ για την εφαρμογή μεταρρυθμίσεων που θα ενισχύσουν την προστασία της ιδιωτικής ζωής και των ατομικών ελευθεριών στο πεδίο δραστηριότητας των αμερικανικών υπηρεσιών πληροφοριών. Σύμφωνα με το Διατλαντικό Πλαίσιο, οι ΗΠΑ θα θέσουν σε εφαρμογή νέες εγγυήσεις για να διασφαλίσουν ότι οι δραστηριότητες παρακολούθησης σημάτων είναι αναγκαίες και αναλογικές για την επίτευξη καθορισμένων στόχων εθνικής ασφάλειας, θα δημιουργήσουν έναν ανεξάρτητο μηχανισμό προσφυγής δύο επιπέδων με δεσμευτική εξουσία, και θα ενισχύσουν την αυστηρή και πολυεπίπεδη εποπτεία των εν λόγω δραστηριοτήτων για να διασφαλίσουν τη συμμόρφωση με τους περιορισμούς στις δραστηριότητες παρακολούθησης[151].

---

[149] Λευκός Οίκος (2022), *FACT SHEET: United States and European Commission Announce Trans-Atlantic Data Privacy Framework*, ο.π., όπου χαρακτηριστικά αναφέρεται το εξής: «*στην πραγματικότητα, μεταξύ των Ηνωμένων Πολιτειών και της Ευρώπης διακινούνται περισσότερα δεδομένα από οπουδήποτε αλλού στον κόσμο, επιτρέποντας μια οικονομική σχέση ΗΠΑ-ΕΕ ύψους 7,1 τρισεκατομμυρίων δολαρίων*».

[150] Αλεξανδροπούλου - Αιγυπτιάδου, Ε. (2016), «Διασυνοριακή ροή προσωπικών δεδομένων από την ΕΕ στις ΗΠΑ: Η πρόσφατη απόφαση του ΔΕΕ ενόψει της σχετικής δραστηριότητας του Facebook (C-362/2014, M. Schrems κατά Ιρλανδού Επιτρόπου Προστασίας Προσωπικών Δεδομένων), *ΤΝΠ QUALEX, ΔiΜΕΕ*, 1/2016, σελ. 12 - 24.

[151] Ευρωπαϊκή Επιτροπή (2022), *European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework.* Βέλγιο: Ευρωπαϊκή Επιτροπή. Διαθέσιμο στο: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087.

Το επόμενο βήμα είναι οι ομάδες της αμερικανικής κυβέρνησης και της Επιτροπής να αποτυπώσουν και εγγράφως τα στοιχεία της παραπάνω συμφωνίας, ώστε να τεθεί σε εφαρμογή το Διατλαντικό Πλαίσιο, αφού προηγουμένως λάβει την έγκριση και από τις δύο πλευρές. Για τον σκοπό αυτό, οι παραπάνω δεσμεύσεις των ΗΠΑ θα συμπεριληφθούν σε εκτελεστικό διάταγμα, το οποίο εν συνεχεία θα αποτελέσει τη βάση της αξιολόγησης της Επιτροπής για την πολυαναμενόμενη νέα απόφαση επάρκειας.

Κατά τη γνώμη του γράφοντος, η τύχη της επερχόμενης τρίτης απόφασης επάρκειας για τις ΗΠΑ κρίνεται μεγαλύτερη σε περίπτωση που τεθεί υπό την κρίση του ΔΕΕ, αφού κατά την εκ νέου αξιολόγηση του αμερικανικού καθεστώτος, η Επιτροπή θα λάβει υπόψη της τις ως άνω αναφερόμενες συμφωνημένες τροποποιήσεις, καθώς και τα στοιχεία της αμερικανικής νομοθεσίας που υποδεικνύονται στη Λευκή Βίβλο του Υπουργείου Εμπορίου των ΗΠΑ. Εκείνο που μένει, είναι να δούμε ποια θα είναι η ονομασία που θα επιλεγεί για το νέο πλαίσιο διαβιβάσεων μεταξύ ΕΕ και ΗΠΑ, μετά τον «ασφαλή λιμένα» και την «ασπίδα προστασίας της ιδιωτικής ζωής».

Β. Η ΣΥΝΔΡΟΜΗ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΣΥΜΒΟΥΛΙΟΥ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

Έχει καταστεί σαφές ότι η απόφαση *Schrems II* κλόνισε το μέχρι τότε νομικό καθεστώς για τις διαβιβάσεις δεδομένων σε τρίτες χώρες, «αποκαθηλώνοντας» τον πιο διαδεδομένο μηχανισμό διαβίβασης, τις αποφάσεις επάρκειας. Ο νομικός και επιχειρηματικός κόσμος ανέμενε από την Επιτροπή να ρίξει φως στο αδιέξοδο που δημιουργήθηκε για πλήθος ιδιωτικών επιχειρήσεων σε ότι αφορά τις διαβιβάσεις δεδομένων. Όμως, το ΕΣΠΔ είναι ο ενωσιακός θεσμός, και δη εποπτικός, που έκανε το πρώτο βήμα στη ρύθμιση της νέας πραγματικότητας για τις διαβιβάσεις δεδομένων σε τρίτες χώρες[152]. Πράγματι, στον απόηχο της απόφασης *Schrems II*, το ΕΣΠΔ εξέδωσε δυο δέσμες συστάσεων (εφεξής «**Συστάσεις**») ως απάντηση στα νομικά ζητήματα που προέκυψαν από την εν λόγω απόφαση, σε μια προσπάθεια αφενός να παράσχει μεγαλύτερη σαφήνεια και καθοδήγηση σχετικά με τη χρήση των μηχανισμών για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες, και αφετέρου προκειμένου να συνδράμει τους εξαγωγείς (είτε πρόκειται για

[152] Βλ. Ikeda, S. (2020), «EDPB Issues Recommendations on International Data Transfers in Response to Schrems II Decision; Is It a Lasting Solution?», *CPO Magazine*. Διαθέσιμο στο: https://www.cpomagazine.com/data-privacy/edpb-issues-recommendations-on-international-data-transfers-in-response-to-schrems-ii-decision-is-it-a-lasting-solution/.

υπεύθυνους επεξεργασίας ή εκτελούντες την επεξεργασία) στο περίπλοκο έργο της αξιολόγησης του νομικού καθεστώτος τρίτων χωρών και του προσδιορισμού κατάλληλων πρόσθετων μέτρων, όπου απαιτείται. Η πρώτη δέσμη Συστάσεων αφορά την αξιολόγηση που πρέπει να διενεργεί ο εκάστοτε εξαγωγέας δεδομένων, σε συνεργασία με τον εισαγωγέα δεδομένων, καθώς και τα πιθανά πρόσθετα μέτρα που θα πρέπει να εφαρμόσουν προς εξασφάλιση ενός ουσιαστικά ισοδύναμου επιπέδου προστασίας των δεδομένων που διαβιβάζονται σε τρίτες χώρες **(1)**[153], ενώ η δεύτερη δέσμη Συστάσεων παρέχει καθοδήγηση σχετικά με το κατά πόσο τα μέτρα παρακολούθησης από τις υπηρεσίες εθνικής ασφάλειας ή τις αρχές επιβολής του νόμου σε τρίτες χώρες μπορούν να θεωρηθούν ως δικαιολογημένη παρέμβαση ή όχι **(2)**[154].

1. Συστάσεις 01/2020

Η πρώτη δέσμη Συστάσεων, την οποία ενέκρινε το ΕΣΠΔ στις 18 Ιουνίου 2021, μετά από δημόσια διαβούλευση της αρχικής δημοσίευσής της στις 12 Νοεμβρίου 2020, σκοπό έχει να συνδράμει τους εξαγωγείς δεδομένων στο περίπλοκο έργο της αξιολόγησης του επιπέδου προστασίας των δεδομένων σε τρίτες χώρες και, όπου είναι απαραίτητο, στη λήψη πρόσθετων μέτρων για τη διασφάλιση της διασυνοριακής διαβίβασης δεδομένων προσωπικού χαρακτήρα. Η πρώτη αυτή δέσμη περιγράφει τα βήματα που πρέπει να ακολουθηθούν, τις πηγές πληροφοριών που πρέπει να χρησιμοποιηθούν, καθώς και ορισμένα ενδεικτικά πρόσθετα μέτρα που μπορούν να ληφθούν. Πιο συγκεκριμένα, οι Συστάσεις 01/2020 του ΕΣΠΔ περιλαμβάνουν έναν «οδικό χάρτη» με τα ακόλουθα βήματα:

Πρώτο Βήμα - Καταγραφή των διασυνοριακών διαβιβάσεων: Οι εξαγωγείς δεδομένων θα πρέπει να χαρτογραφούν όλες τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες, συμπεριλαμβανομένων τυχόν διαβιβάσεων σε εκτελούντες την επεξεργασία δεδομένων ή υπεργολάβους επεξεργασίας. Το ΕΣΠΔ, μάλιστα, επιβεβαιώνει την άποψη ότι η απομακρυσμένη πρόσβαση από τρίτη χώρα και η αποθήκευση σε περιβάλλον

[153] Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (2021), *Συστάσεις 01/2020 σχετικά με τα μέτρα που συμπληρώνουν τα εργαλεία διαβίβασης για τη διασφάλιση της συμμόρφωσης με το επίπεδο προστασίας δεδομένων προσωπικού χαρακτήρα στην ΕΕ*. Βέλγιο: Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. Διαθέσιμο στο: https://edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_el.pdf.

[154] Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (2020), *Συστάσεις 02/2020 σχετικά με τις Ευρωπαϊκές Βασικές Εγγυήσεις για τα μέτρα παρακολούθησης*. Βέλγιο: Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. Διαθέσιμο στο: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_el.

υπολογιστικού νέφους που παρέχει τρίτος πάροχος υπηρεσιών εκτός της ΕΕ, θεωρούνται επίσης διαβίβαση σε τρίτη χώρα.

Δεύτερο Βήμα - Αξιολόγηση της καταλληλότητας του μηχανισμού διαβίβασης: Οι εξαγωγείς δεδομένων θα πρέπει να χρησιμοποιούν έναν από τους μηχανισμούς διαβίβασης, που προβλέπονται στο ΓΚΠΔ, όπως τις ΤΣΡ, τις ΔΕΚ, τους κώδικες δεοντολογίας ή τους μηχανισμούς πιστοποίησης. Ο μηχανισμός διαβίβασης πρέπει στο πλαίσιο εφαρμογής του να παρέχει ένα ουσιαστικά ισοδύναμο επίπεδο προστασίας με το ΓΚΠΔ. Ο εξαγωγέας δεδομένων δύναται να επικαλεστεί και τις παρεκκλίσεις του άρθρου 49 του ΓΚΠΔ, αλλά μόνο σε περιστασιακές και μη επαναλαμβανόμενες καταστάσεις, ενώ θα πρέπει να ερμηνεύονται κατά τρόπο που να μην έρχεται σε αντίθεση με την ίδια τη φύση των παρεκκλίσεων ως εξαιρέσεων από τον κανόνα ότι τα δεδομένα προσωπικού χαρακτήρα δεν μπορούν να διαβιβαστούν σε τρίτη χώρα, εκτός εάν η χώρα αυτή προβλέπει επαρκές επίπεδο προστασίας των δεδομένων ή, εναλλακτικά, κατάλληλες εγγυήσεις. Εάν ένας εξαγωγέας δεδομένων βασίζεται σε απόφαση επάρκειας της Επιτροπής για τη χώρα προορισμού, δεν απαιτούνται περαιτέρω μέτρα, εντούτοις ο εξαγωγέας δεδομένων θα πρέπει να επιβεβαιώνει ανά τακτά χρονικά διαστήματα ότι η απόφαση επάρκειας παραμένει εν ισχύ. Παράλληλα, οι αποφάσεις επάρκειας δεν εμποδίζουν τα υποκείμενα των δεδομένων να υποβάλουν καταγγελία ενώπιον των εθνικών ΑΠΔ. Ούτε εμποδίζουν τις εθνικές ΑΠΔ να προσφύγουν σε εθνικό δικαστήριο εάν έχουν αμφιβολίες σχετικά με την εγκυρότητα μιας απόφασης επάρκειας, ώστε το εθνικό δικαστήριο να υποβάλει προδικαστικά ερωτήματα ενώπιον του ΔΕΕ με σκοπό την εξέταση της εγκυρότητας αυτής.

Τρίτο Βήμα - Αξιολόγηση της νομοθεσίας τρίτων χωρών: Οι εξαγωγείς δεδομένων θα πρέπει να αξιολογούν κάθε διαβίβαση για να εκτιμήσουν κατά πόσο οι νόμοι της τρίτης χώρας ισχύουν για τα διαβιβαζόμενα δεδομένα, ενδεχομένως με τη συνδρομή του εισαγωγέα δεδομένων - ο οποίος θα είναι πιο εξοικειωμένος με τους σχετικούς νόμους - και κατά πόσο οι νόμοι αυτοί επηρεάζουν την αποτελεσματικότητα του μηχανισμού διαβίβασης που εφαρμόζεται. Ειδικότερα, η αξιολόγηση αυτή θα πρέπει, μεταξύ άλλων, να εστιάζει σε νόμους που ορίζουν απαιτήσεις για την κοινοποίηση δεδομένων προσωπικού χαρακτήρα σε δημόσιες αρχές (για παράδειγμα, για σκοπούς επιβολής της ποινικής νομοθεσίας και για λόγους εθνικής ασφάλειας), και σε λοιπές πηγές πληροφοριών που είναι σχετικές,

αντικειμενικές, αξιόπιστες, επαληθεύσιμες και διαθέσιμες στο κοινό ή με άλλο τρόπο προσβάσιμες[155].

Προς διευκόλυνση των εξαγωγέων δεδομένων στην αξιολόγησή τους ως προς το κατά πόσο οι νόμοι μιας τρίτης χώρας μπορούν να θεωρηθούν ως δικαιολογημένη παρέμβαση που δεν θίγει τις εγγυήσεις διαβίβασης, το ΕΣΠΔ δημοσίευσε τις Συστάσεις 02/2020 σχετικά με τις Ευρωπαϊκές Βασικές Εγγυήσεις (εφεξής «**ΕΒΕ**») για τα μέτρα επιτήρησης, την ίδια ημέρα με τη δημοσίευση της πρώτης έκδοσης των Συστάσεων 1/2020 που είχε τεθεί σε δημόσια διαβούλευση. Τα εν λόγω πρότυπα απορρέουν από το δίκαιο της ΕΕ και τη νομολογία του ΔΕΕ και του ΕΔΑΔ, η οποία είναι δεσμευτική για τα κράτη-μέλη της ΕΕ[156].

Σε περίπτωση που η αξιολόγηση αποκαλύψει ότι η σχετική νομοθεσία στην τρίτη χώρα είναι ή μπορεί να είναι προβληματική[157], και ότι τα διαβιβαζόμενα δεδομένα ή/και ο εν λόγω εισαγωγέας εμπίπτουν ή ενδέχεται να εμπίπτουν στο πεδίο εφαρμογής αυτής της προβληματικής νομοθεσίας, το ΕΣΠΔ προσφέρει τρεις πιθανές λύσεις για τον εξαγωγέα των δεδομένων: α) να αναστείλει η διαβίβαση των δεδομένων, ή β) να εφαρμόσει συμπληρωματικές εγγυήσεις για να αποτρέψει τον κίνδυνο ενδεχόμενης εφαρμογής στον εισαγωγέα ή/και στα διαβιβαζόμενα δεδομένα νόμων ή/και πρακτικών της τρίτης χώρας, οι οποίοι μπορούν να επηρεάσουν τις συμβατικές εγγυήσεις του μηχανισμού διαβίβασης που έχει επιλεγεί[158], είτε γ) να προχωρήσει στη διαβίβαση χωρίς την εφαρμογή συμπληρωματικών εγγυήσεων, εφόσον κρίνει ότι στην πράξη η προβληματική νομοθεσία δεν θα τύχει εφαρμογής στα διαβιβαζόμενα δεδομένα και/ή τον εισαγωγέα δεδομένων. Όπως πολύ εύστοχα έχει επισημανθεί, ο μηχανισμός αξιολόγησης που προτείνει το ΕΣΠΔ

[155] Συστάσεις 01/2020, ο.π., παράγραφος 46 και Παράρτημα 3.

[156] Συστάσεις 01/2020, ο.π., παράγραφος 42.

[157] Ως «προβληματική νομοθεσία» το ΕΣΠΔ ορίζει τη νομοθεσία, η οποία αφενός επιβάλλει στον αποδέκτη δεδομένων προσωπικού χαρακτήρα από την ΕΕ υποχρεώσεις ή/και επηρεάζει τα διαβιβαζόμενα δεδομένα κατά τρόπο που μπορεί να επηρεάσει τις συμβατικές εγγυήσεις του μηχανισμού διαβίβασης για ένα ουσιαστικά ισοδύναμο επίπεδο προστασίας, και αφετέρου δεν σέβεται την ουσία των θεμελιωδών δικαιωμάτων και ελευθεριών που αναγνωρίζονται από τον Χάρτη ή υπερβαίνει αυτό που είναι αναγκαίο και αναλογικό σε μια δημοκρατική κοινωνία για τη διασφάλιση ενός από τους σημαντικούς στόχους, οι οποίοι αναγνωρίζονται στο δίκαιο της ΕΕ ή των κρατών-μελών της ΕΕ, όπως αυτοί που απαριθμούνται στο άρθρο 23, παράγραφος 1 του ΓΚΠΔ.

[158] Μάλιστα, το ΕΣΠΔ στις Συστάσεις 01/2020 υπογραμμίζει ότι η αποτελεσματικότητα του μηχανισμού διαβίβασης δεδομένων μπορεί να επηρεαστεί από τη νομοθεσία της χώρας προορισμού που επιτρέπει στις δημόσιες αρχές της να έχουν πρόσβαση στα διαβιβαζόμενα δεδομένα, ακόμη και χωρίς την παρέμβαση του εισαγωγέα δεδομένων. Βλ. Συστάσεις 01/2020, ο.π., παράγραφος 43.3, υποσημείωση 55.

στο τελικό κείμενο των Συστάσεων 01/2020[159] ομοιάζει με το μηχανισμό διενέργειας εκτίμησης αντικτύπου για την προστασία δεδομένων προσωπικού χαρακτήρα (γνωστή ως «DPIA») του άρθρου 35 του ΓΚΠΔ, καθώς ακολουθεί μια προσέγγιση με βάση τον κίνδυνο, ενώ πρόκειται για μια συνεχή διαδικασία, όπου η αξιολόγηση θα πρέπει να επικαιροποιείται, καθώς μπορεί να οδηγήσει σε διαφορετικό αποτέλεσμα, εάν τα δεδομένα της κατάστασης αλλάξουν[160].

Οι Συστάσεις 01/2020 περιλαμβάνουν ένα λεπτομερές παράδειγμα για τον τρόπο αξιολόγησης του κινδύνου που ενέχει το άρθρο 702 του νόμου FISA για τα δεδομένα που διαβιβάζονται στις ΗΠΑ. Το περιεχόμενο του συγκεκριμένου παραδείγματος είναι ιδιαίτερα χρήσιμο για τους εισαγωγείς δεδομένων στις ΗΠΑ (όπως τους παρόχους υπηρεσιών υπολογιστικού νέφους με έδρα τις ΗΠΑ) καθώς παρουσιάζει το συλλογισμό που απαιτείται να ακολουθήσουν τόσο οι εξαγωγείς όσο και οι εισαγωγείς δεδομένων κατά την αξιολόγησή τους, ήτοι να εστιάζουν στην πρακτική εφαρμογή του άρθρου 702 του νόμου FISA στη συγκεκριμένη κάθε φορά διαβίβαση.

Το παράδειγμα προβλέπει την τεκμηρίωση που θα πρέπει να συνοδεύει τόσο τη θετική όσο και την αρνητική κατάληξη της αξιολόγησης[161]. Πιο συγκεκριμένα, η θετική απάντηση θα στηρίζεται στη διαπίστωση βάσει των διαθέσιμων στο κοινό πληροφοριών[162] ότι το άρθρο 702 του νόμου FISA εφαρμόζεται στην υπό εξέταση διαβίβαση και, ως εκ τούτου, προσκρούει

---

[159] Στο αρχικό κείμενο των Συστάσεων 01/2020, το ΕΣΠΔ δεν επέτρεπε στους εξαγωγείς δεδομένων να βασιστούν σε υποκειμενικούς παράγοντες, όπως η πιθανότητα πρόσβασης των δημοσίων αρχών στα δεδομένα, στο πλαίσιο της αξιολόγησης της νομιμότητας μιας διαβίβασης: «*Η αξιολόγησή σας πρέπει να βασίζεται πρωτίστως στη νομοθεσία που είναι δημόσια διαθέσιμη. Ωστόσο , σε ορισμένες περιπτώσεις αυτό δεν θα αρκεί, διότι η νομοθεσία στις τρίτες χώρες ενδέχεται να είναι ελλιπής. Σε αυτήν την περίπτωση, εάν εξακολουθείτε να επιθυμείτε να προβλέψετε τη διαβίβαση, θα πρέπει να εξετάσετε άλλους σχετικούς και αντικειμενικούς παράγοντες, και να μην βασίζεστε σε υποκειμενικούς παράγοντες όπως η πιθανότητα πρόσβασης των δημοσίων αρχών στα δεδομένα σας με τρόπο που δεν συνάδει με τα πρότυπα της ΕΕ*». Το αρχικό κείμενο των Συστάσεων 01/2020 είναι διαθέσιμο στο: *https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf*

[160] Βλ. σχετικά Breitbarth, P. (2021), «A Risk-Based Approach to International Data Transfers», *European Data Protection Law Review*, Volume 7, Issue 4 (2021). Διαθέσιμο στο: https://edpl.lexxion.eu/article/EDPL/2021/4/9 και Tielemans, J., Cooper, D. and Maldoff, G. (2021), «EDPB's data transfer recommendations adopt a risk-based approach with teeth», *International Association of Privacy Professionals - The Privacy Advisor*, Διαθέσιμο στο: https://iapp.org/news/a/edpbs-data-transfer-recommendations-adopt-a-risk-based-approach-with-teeth/.

[161] Συστάσεις 01/2020, ο.π., παράδειγμα σελίδας 20.

[162] Το ΕΣΠΔ απαριθμεί τις αξιόπιστες πηγές πληροφοριών για τον προσδιορισμό της πρακτικής εφαρμογής του άρθρου 702 του νόμου FISA, όπως τον εσωτερικό κανονισμό, τις γνωμοδοτήσεις και τις αποφάσεις του FISC, καθώς και τη νομολογία των αμερικανικών Δικαστηρίων. Βλ. Συστάσεις 01/2020, ο.π., παράδειγμα σελίδας 20.

στην αποτελεσματικότητα του μηχανισμού διαβίβασης του άρθρου 46 του ΓΚΠΔ που έχει επιλεγεί[163], οπότε, κατά συνέπεια, η υπό αξιολόγηση διαβίβαση θα μπορέσει να διενεργηθεί ύστερα από την υιοθέτηση πρόσθετων μέτρων (τα οποία θα ληφθούν σε συνεργασία με τον εισαγωγέα δεδομένων) προς εξασφάλιση ενός ουσιαστικά ισοδύναμου επίπεδου προστασίας των διαβιβαζόμενων δεδομένων με εκείνο που εγγυάται η ΕΕ. Αντιθέτως, η αρνητική απάντηση θα βασίζεται στη διαπίστωση ότι το άρθρο 702 του νόμου FISA δεν εφαρμόζεται στην υπό εξέταση διαβίβαση και, ως εκ τούτου, δεν επηρεάζει την αποτελεσματικότητα του μηχανισμού διαβίβασης που έχει επιλεγεί[164].

Τέταρτο Βήμα - Προσδιορισμός και εφαρμογή πρόσθετων μέτρων: Εάν από το τρίτο βήμα προκύπτει ότι η νομοθεσία της τρίτης χώρας επηρεάζει την αποτελεσματικότητα του μηχανισμού διαβίβασης που έχει επιλεγεί, απαιτείται ένα τέταρτο βήμα, και τούτο διότι οι ΤΣΡ και οι υπόλοιποι μηχανισμοί διαβίβασης που αναφέρονται στο άρθρο 46 του ΓΚΠΔ δεν λειτουργούν σε συνθήκες νομικού κενού[165]. Το εν λόγω τέταρτο βήμα συνίσταται στον προσδιορισμό και την εφαρμογή πρόσθετων μέτρων που είναι αναγκαία για τη διασφάλιση ουσιαστικά ισοδύναμου επιπέδου προστασίας των δεδομένων προσωπικού χαρακτήρα με εκείνο που προβλέπεται από το ΓΚΠΔ. Το Παράρτημα 2 των Συστάσεων 01/2020 περιέχει έναν μη εξαντλητικό κατάλογο παραδειγμάτων πρόσθετων μέτρων, όπως η χρήση κρυπτογράφησης ή/και ψευδωνυμοποίησης. Το ΕΣΠΔ διακρίνει μεταξύ συμβατικών, τεχνικών και οργανωτικών μέτρων, τα οποία μπορούν να συνδυαστούν, όπου είναι απαραίτητο. Σύμφωνα με το ΕΣΠΔ, για να εκτιμηθεί ποια πρόσθετα μέτρα είναι αποτελεσματικά, πρέπει να λαμβάνονται υπόψη, μεταξύ άλλων, ο μορφότυπος με τον οποίο διαβιβάζονται τα δεδομένα προσωπικού χαρακτήρα, η φύση των δεδομένων προσωπικού χαρακτήρα, η διάρκεια και η πολυπλοκότητα της διαβίβασης και τα μέρη που εμπλέκονται στη διαβίβαση.

Πέμπτο Βήμα - Διαδικαστικά βήματα: Ανάλογα με το μηχανισμό διαβίβασης που χρησιμοποιεί ή προτίθεται να χρησιμοποιήσει ο εξαγωγές δεδομένων, ενδέχεται να χρειαστεί να προβεί σε περαιτέρω διαδικαστικά βήματα, όπως να επικοινωνήσει με την αρμόδια ΑΠΔ για έγκριση. Το ΕΣΠΔ διευκρίνισε ότι δεν χρειάζεται έγκριση από την ΑΠΔ

[163] Επί παραδείγματι, η διαπίστωση ότι υπάρχει νομική απαγόρευση για την ενημέρωση του εξαγωγέα δεδομένων σχετικά με συγκεκριμένο αίτημα πρόσβασης σε διαβιβαζόμενα δεδομένα.
[164] Επί παραδείγματι, η διαπίστωση ότι υπάρχουν περιορισμοί στην παροχή γενικών πληροφοριών σχετικά με αιτήματα πρόσβασης σε διαβιβαζόμενα δεδομένα ή απουσία τέτοιων αιτημάτων.
[165] Συστάσεις 01/2020, ο.π., σελ. 2 (Συνοπτική παρουσίαση) και παράγραφος 66.

όταν εφαρμόζονται πρόσθετα μέτρα πέραν των ΤΣΡ, εφόσον δεν έρχονται σε αντίθεση, άμεσα ή έμμεσα, με τις ΤΣΡ και επαρκούν για να διασφαλιστεί ότι δεν υπονομεύεται το επίπεδο προστασίας που εγγυάται ο ΓΚΠΔ[166].

Έκτο Βήμα - Επανεκτίμηση του επιπέδου προστασίας των δεδομένων ανά τακτά χρονικά διαστήματα: Οι εξαγωγείς δεδομένων θα πρέπει να παρακολουθούν, σε συνεχή βάση και, κατά περίπτωση, σε συνεργασία με τους εισαγωγείς δεδομένων, τις εξελίξεις στην τρίτη χώρα, στην οποία έχουν διαβιβάσει δεδομένα προσωπικού χαρακτήρα, οι οποίες θα μπορούσαν να επηρεάσουν την αρχική τους αξιολόγηση σχετικά με το επίπεδο προστασίας. Οι εν λόγω προσπάθειες θα πρέπει να τεκμηριώνονται επί τη βάσει της αρχής της λογοδοσίας[167].

Χαρακτηριστικό παράδειγμα πρακτικής εφαρμογής των Συστάσεων 01/2020 συναντάμε στη Λευκή Βίβλο της Microsoft[168], με την οποία η εταιρεία καταδεικνύει προς τους πελάτες της τη συμμόρφωση των διαδικτυακών υπηρεσιών που παρέχει μέσω του περιβάλλοντος υπολογιστικού νέφους, με τις νέες αυστηρές απαιτήσεις για την προστασία των δεδομένων προσωπικού χαρακτήρα ύστερα από την απόφαση *Schrems II*, ακολουθώντας «βήμα βήμα» τις Συστάσεις 01/2020 του ΕΣΠΔ.

Πιο συγκεκριμένα, η Microsoft λαμβάνοντας υπόψη την απόφαση *Schrems II* έπαυσε να βασίζεται στην απόφαση για την Ασπίδα Προστασίας της Ιδιωτικής Ζωής και συνέχισε να χρησιμοποιεί τις ΤΣΡ ως νομική βάση για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα στις ΗΠΑ, γεγονός που επέτρεψε στους χρήστες να εξακολουθήσουν τη χρήση των υπηρεσιών της. Παράλληλα, όμως, έχει λάβει όλα τα αναγκαία μέτρα ώστε να πληροί τις νέες αυστηρές προϋποθέσεις για τις ΤΣΡ[169].

Στο πλαίσιο αυτό, η Microsoft κυκλοφόρησε στις 15 Σεπτεμβρίου 2021 μια αναθεωρημένη έκδοση του Παραρτήματος Προστασίας Δεδομένων Προσωπικού Χαρακτήρα Προϊόντων και

[166] Συστάσεις 01/2020, ο.π., παράγραφος 56.
[167] Άρθρο 5, παράγραφος 2 του ΓΚΠΔ.
[168] Microsoft (2021), «*Compliance with EU transfer requirements for personal data in the Microsoft cloud*». Διαθέσιμο στο: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWRql1?culture=en-us&country=US.
[169] Microsoft (2021), «*Compliance with EU transfer requirements for personal data in the Microsoft cloud*», ο.π., σελ. 4.

Υπηρεσιών της Microsoft, με το οποίο εφαρμόζονται οι νέες ΤΣΡ[170]. Σύμφωνα με το εν λόγω Παράρτημα η Microsoft εφαρμόζει την τρίτη δέσμη των νέων ΤΣΡ (Εκτελών την Επεξεργασία - Εκτελών την Επεξεργασία) στη συμβατική σχέση μεταξύ της Ιρλανδικής Microsoft (ως εξαγωγέα δεδομένων) και της αμερικανικής Microsoft Corporation (ως εισαγωγέα δεδομένων)[171].

Πέρα, όμως, από τον καθορισμό της κατάλληλης δέσμης ΤΣΡ μεταξύ των μερών, η Microsoft προέβη και στην εκπλήρωση των υπόλοιπων βημάτων που έθεσε η ΕΣΠΔ. Ειδικότερα, και σε ότι αφορά το τρίτο βήμα, ήτοι την αξιολόγηση του νομοθετικού πλαισίου της χώρας προορισμού, η Microsoft αξιολογεί τη δημόσια διαθέσιμη πληροφορία που αφορά στο νομοθετικό πλαίσιο και την πρακτική της χώρας προορισμού σε συνδυασμό με τα μέτρα ασφαλείας που έχει λάβει η ίδια[172]. Καθώς το επίκεντρο των διαβιβάσεων βρίσκεται στις ΗΠΑ, η Microsoft προέβη σε αξιολόγηση του αμερικάνικου δικαίου, και συγκεκριμένα του άρθρου 702 του νόμου FISA και του εκτελεστικού διατάγματος ΕΟ 12333, για να καταλήξει στο συμπέρασμα ότι το αμερικανικό πλαίσιο δεν την εμποδίζει από το να συμμορφωθεί με τις υποχρεώσεις που απορρέουν από το μηχανισμό διαβίβασης των ΤΣΡ[173].

Ακολουθώντας το τέταρτο βήμα, και ειδικότερα στο πλαίσιο εφαρμογής κατάλληλων συμβατικών μέτρων, ενδιαφέρον παρουσιάζει η πρόβλεψη ότι σε περίπτωση που η Microsoft λάβει αίτημα από αρχές επιβολής του νόμου για απόκτηση πρόσβασης στα δεδομένα ορισμένου πελάτη (χρήστη), η Microsoft θα προσπαθήσει να ανακατευθύνει την αρχή επιβολής του νόμου στα να αιτηθεί την εν λόγω πρόσβαση απευθείας από τον πελάτη (χρήστη). Μάλιστα, σε περίπτωση που κάποιος υπεργολάβος επεξεργασίας της Microsoft - τη λίστα των οποίων φροντίζει να επικαιροποιεί ανά τακτά χρονικά διαστήματα[174] - λάβει

---

[170] Microsoft (2021*), «Παράρτημα Προστασίας Δεδομένων Προσωπικού Χαρακτήρα Προϊόντων και Υπηρεσιών της Microsoft*». Διαθέσιμο στο: https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA.

[171] Microsoft (2021), *«Παράρτημα Προστασίας Δεδομένων Προσωπικού Χαρακτήρα Προϊόντων και Υπηρεσιών της Microsoft»*, ο.π., σελ. 5.

[172] Αξιοσημείωτο είναι ότι η Microsoft πριν το άνοιγμα μιας νέας βάσης δεδομένων σε χώρα εκτός της ΕΕ, διενεργεί αξιολόγηση του τοπικού δικαίου για να επιβεβαιώσει ότι τα δεδομένα θα τηρηθούν στην τρίτη χώρα με τρόπο που είναι συμβατός με τις υποχρεώσεις της Microsoft προς τους πελάτες της. Βλ. Microsoft (2021), *«Compliance with EU transfer requirements for personal data in the Microsoft cloud»*, ο.π. Παράρτημα 1, σελ. 10.

[173] Microsoft (2021), *«Compliance with EU transfer requirements for personal data in the Microsoft cloud»*, ο.π. Παράρτημα 1, σελ. 18 - 20.

[174] Microsoft (2021), *«Microsoft Online Services Subprocessors List»*. Διαθέσιμο στο: https://servicetrust.microsoft.com/ViewPage/TrustDocumentsV3?command=Download&downloadType=

αίτημα που αφορά σε δεδομένα πελατών (χρηστών), είναι υποχρεωμένος συμβατικά να το διαβιβάσει στην Microsoft[175].

Αξιοσημείωτο, τέλος, είναι ότι η Microsoft δεν περιορίστηκε μόνο στην απόδειξη συμμόρφωσής της με το μηχανισμό του ΕΣΠΔ, αλλά θέλησε παράλληλα «να νίψει τας χείρας της» για τις όποιες παρεκτροπές, αποτυπώνοντας στη Λευκή της Βίβλο τη διαφωνία της ως προς τους περιορισμούς που επιβάλλει η νομοθεσία την ΗΠΑ, ήτοι ότι οι πάροχοι δεν μπορούν να επιβεβαιώσουν ούτε να αρνηθούν ότι έχουν λάβει συγκεκριμένο αίτημα πρόσβασης που υπόκειται σε υποχρέωση τήρησης απορρήτου[176]. Προς τούτο, η Microsoft δηλώνει ότι υποστηρίζει σθεναρά την προσπάθεια για αλλαγές στο υφιστάμενο νομοθετικό σύστημα των ΗΠΑ, με σκοπό να παρέχεται στους πελάτες η δέουσα διαφάνεια. Απτή απόδειξη της πρόθεσής της είναι και η δημοσιοποίηση από πλευράς της μιας αναφοράς[177], η οποία δίνει μια εικόνα των αιτημάτων πρόσβασης που λαμβάνει από την αμερικανική κυβέρνηση και αφορούν στην εθνική ασφάλεια, όσο βέβαια της το επιτρέπει η υφιστάμενη αμερικανική νομοθεσία. Κατά τη γνώμη του γράφοντος, παρά το γεγονός ότι κρίνεται απίθανη η τροποποίηση του αμερικανικού δικαίου κατ'εντολήν της ΕΕ, οι διατυπώσεις της Microsoft καθιστούν σαφή τη θέση μερίδας των ισχυρών παρόχων διαδικτυακών υπηρεσιών, οι οποίοι είναι έτοιμοι εφόσον πάρουν το «πράσινο φως» από την αμερικανική κυβέρνηση, να πορευτούν με τη μέγιστη δυνατή διαφάνεια απέναντι στους πελάτες τους, με σκοπό την εύρυθμη και ασφαλή λειτουργία της διατλαντικής ροής δεδομένων.

2. Συστάσεις 02/2020

Εκτός από τις Συστάσεις 01/2020, το ΕΣΠΔ υιοθέτησε ταυτόχρονα μια επικαιροποιημένη εκδοχή των συστάσεων για τις Ευρωπαϊκές Βασικές Εγγυήσεις (European Essential Guarantees) που είχαν αρχικώς καταρτιστεί από την Ομάδα Εργασίας 29 ως απάντηση στην απόφαση *Schrems I*[178], μέσω της ενσωμάτωσης των διευκρινίσεων που έχει παράσχει το ΔΕΕ

Document&downloadId=ede6342e-d641-4a9b-9162-7d66025003b0&tab=7f51cb60-3d6c-11e9-b2af-7bb9f5d2d913&docTab=7f51cb60-3d6c-11e9-b2af-7bb9f5d2d913_Subprocessor_List.

[175] Microsoft (2021), «*Compliance with EU transfer requirements for personal data in the Microsoft cloud*», ο.π., σελ. 14.

[176] Microsoft (2021), «*Compliance with EU transfer requirements for personal data in the Microsoft cloud*». ο.π., σελ. 4 και 10.

[177] Microsoft, «*US National Security Orders Report*». Διαθέσιμο στο: https://www.microsoft.com/en-us/corporate-responsibility/us-national-security-orders-report?activetab=pivot_1:primaryr2

[178] Ομάδα Εργασίας του Άρθρου 29 για την προστασία των δεδομένων (2016), *Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees)*. Βέλγιο: Ομάδα Εργασίας του

και το ΕΔΑΔ από την πρώτη δημοσίευση του εγγράφου, ιδίως στο πλαίσιο της απόφασης *Schrems II*[179].

Οι ΕΒΕ είναι πρότυπα αναφοράς που προσδιορίστηκαν επ' αφορμή της απόφασης *Schrems I*, και θεσπίστηκαν με σκοπό να παράσχουν καθοδήγηση σχετικά με το κατά πόσο τα εποπτικά μέτρα που επιτρέπουν την πρόσβαση σε δεδομένα προσωπικού χαρακτήρα από δημόσιες αρχές σε τρίτη χώρα μπορούν να θεωρηθούν ως δικαιολογημένη παρέμβαση υπό το πρίσμα του Χάρτη. Πιο συγκεκριμένα, και βάσει ανάλυσης της ισχύουσας νομολογίας του ΔΕΕ και ΕΔΑΔ, το ΕΣΠΔ είναι της γνώμης ότι μια τέτοια παρέμβαση δύναται να δικαιολογηθεί μόνο βάσει των ακόλουθων τεσσάρων ΕΒΕ[180]:

1. Η επεξεργασία θα πρέπει να βασίζεται σε σαφείς, ακριβείς και προσιτούς κανόνες: Η κυβερνητική παρέμβαση στις ελευθερίες των πολιτών πρέπει να έχει νομική βάση στο δίκαιο της τρίτης χώρας. Αυτή η νομική βάση πρέπει να περιέχει σαφείς και ακριβείς κανόνες σχετικά με το πεδίο εφαρμογής και να περιλαμβάνει ελάχιστες εγγυήσεις.
2. Πρέπει να αποδεικνύεται η αναγκαιότητα και η αναλογικότητα ως προς τους θεμιτούς επιδιωκόμενους στόχους: Σύμφωνα με το Χάρτη, κάθε περιορισμός στην άσκηση των δικαιωμάτων και ελευθεριών που αναγνωρίζονται από το Χάρτη πρέπει να σέβεται την ουσία των εν λόγω δικαιωμάτων και ελευθεριών. Επιπλέον, με την επιφύλαξη της αρχής της αναλογικότητας, τα εν λόγω δικαιώματα και ελευθερίες μπορούν να υπόκεινται σε περιορισμούς μόνον εφόσον είναι αναγκαίοι και ανταποκρίνονται πραγματικά σε στόχους γενικού ενδιαφέροντος που αναγνωρίζονται από την ΕΕ ή στην ανάγκη προστασίας των δικαιωμάτων και ελευθεριών άλλων[181].
3. Θα πρέπει να υφίσταται ένας ανεξάρτητος μηχανισμός εποπτείας: Οποιαδήποτε παρέμβαση στο δικαίωμα στην ιδιωτική ζωή και στην προστασία των δεδομένων προσωπικού χαρακτήρα πρέπει να υπόκειται σε ένα αποτελεσματικό, ανεξάρτητο και

Άρθρου 29 για την προστασία των δεδομένων. Διαθέσιμο στο: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp237_en.pdf. Τόσο το ΔΕΕ όσο και το ΕΔΑΔ έχουν πολλάκις αποφανθεί σχετικά με το τι συνιστά δικαιολογημένη παρέμβαση στα θεμελιώδη δικαιώματα της ιδιωτικής ζωής και της προστασίας των δεδομένων όταν πρόκειται για εθνική ασφάλεια. Η ανάλυση αυτών των υποθέσεων είναι εκείνη που βοήθησε την Ομάδα Εργασίας του άρθρου 29 να αναπτύξει τις τέσσερις Ευρωπαϊκές Βασικές Εγγυήσεις. Βλ. Breitbarth P. (2021), «A Risk-Based Approach to International Data Transfers», ο.π.

[179] Συστάσεις 02/2020, ο.π., παράγραφοι 1 - 3.

[180] Συστάσεις 02/2020, ο.π., παράγραφος 24.

[181] Άρθρο 52, παράγραφος 1 του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης.

αμερόληπτο σύστημα εποπτείας, το οποίο θεσπίζεται από δικαστή ή από άλλο ανεξάρτητο όργανο (για παράδειγμα διοικητική αρχή ή κοινοβουλευτικό όργανο).

4. Πρέπει να είναι διαθέσιμα αποτελεσματικά μέσα προσφυγής: Το υποκείμενο των δεδομένων πρέπει να διαθέτει αποτελεσματικό μέσο προσφυγής για τη συμμόρφωση με τα δικαιώματά του, σε περίπτωση που κρίνει ότι αυτά δεν γίνονται ή δεν έγιναν σεβαστά. Για παράδειγμα, εάν ο νόμος δεν παρέχει σε ένα φυσικό πρόσωπο ένδικα μέσα για να αποκτήσει πρόσβαση στα δεδομένα προσωπικού χαρακτήρα που τον αφορούν, δεν υπάρχει αποτελεσματική δικαστική προστασία[182].

Στις Συστάσεις 02/2020, το ΕΣΠΔ τόνισε ότι οι ΕΒΕ αποτελούν μέρος της αξιολόγησης για τον προσδιορισμό του εάν μια τρίτη χώρα προσφέρει επίπεδο προστασίας ουσιωδώς ισοδύναμο με εκείνο που διασφαλίζεται εντός της ΕΕ, όμως δεν αποσκοπούν αυτές καθαυτές στον προσδιορισμό του συνόλου των στοιχείων που απαιτούνται για να θεωρηθεί ότι μια τρίτη χώρα προσφέρει ένα τέτοιο επίπεδο προστασίας σύμφωνα με το άρθρο 45 του ΓΚΠΔ. Ομοίως, οι εν λόγω εγγυήσεις δεν έχουν ως στόχο να προσδιορίσουν το σύνολο των στοιχείων που πρέπει να ληφθούν υπόψη κατά την αξιολόγηση του κατά πόσο το νομικό καθεστώς μιας τρίτης χώρας δεν επιτρέπει στους εξαγωγείς και εισαγωγείς δεδομένων να εφαρμόσουν αποτελεσματικά το μηχανισμό διαβίβασης που έχει επιλεγεί σύμφωνα με το άρθρο 46 του ΓΚΠΔ[183].

Στόχος των τεσσάρων ΕΒΕ, είναι να εξειδικεύσουν περαιτέρω τους τρόπους αξιολόγησης του επιπέδου παρέμβασης στα θεμελιώδη δικαιώματα της ιδιωτικής ζωής και της προστασίας δεδομένων προσωπικού χαρακτήρα στο πλαίσιο μέτρων παρακολούθησης από δημόσιες αρχές σε μια τρίτη χώρα, κατά τη διαβίβαση δεδομένων προσωπικού χαρακτήρα, και των νομικών προϋποθέσεων που πρέπει, κατά συνέπεια, να ισχύουν για την αξιολόγηση του εάν οι εν λόγω παρεμβάσεις θα μπορούσαν να είναι αποδεκτές στο πλαίσιο του Χάρτη[184].

Οι παραπάνω εκτεθείσες Συστάσεις 02/2020 αποτελούν αναμφίβολα ένα σημαντικό αρωγό στο δύσκολο έργο που έχουν πλέον αναλάβει τόσο οι εξαγωγείς όσο και οι εισαγωγείς των δεδομένων. Εντούτοις, η ουσία της κατά περίπτωση αξιολόγησης επαφίεται στο έργο αξιολόγησης και την τελική κρίση του εξαγωγέα δεδομένων. Όπως, άλλωστε, είχε εξ αρχής τονίσει το ίδιο το ΕΣΠΔ στο Δελτίο Τύπου που συνόδευσε τις Συστάσεις: «*...τελικά οι*

[182] ΔΕΕ, C-362/14, *Schrems I*, ο.π.. παράγραφος 95.
[183] Συστάσεις 2/2020, ο.π., παράγραφος 8.
[184] Συστάσεις 2/2020, ο.π., παράγραφος 23.

εξαγωγείς δεδομένων είναι υπεύθυνοι για τη συγκεκριμένη αξιολόγηση στο πλαίσιο της διαβίβασης, του δικαίου της τρίτης χώρας και του μηχανισμού διαβίβασης στον οποίο βασίζονται»[185]. Στο πλαίσιο αυτό, οι εξαγωγείς δεδομένων πρέπει να ενεργούν με τη δέουσα επιμέλεια και να τεκμηριώνουν ενδελεχώς τη διαδικασία που ακολουθούν, καθώς έχουν υποχρέωση να λογοδοτούν για τις αποφάσεις που λαμβάνουν, σύμφωνα με την αρχή λογοδοσίας του ΓΚΠΔ.

Εκείνο, τέλος, που αδιαμφισβήτητα καθίσταται σαφές μέσω των Συστάσεων 02/2020 είναι ότι το πραγματικό ερώτημα δεν είναι εάν οι διαβιβάσεις δεδομένων υπονομεύουν το επίπεδο προστασίας που λαμβάνουν τα φυσικά πρόσωπα βάσει του ΓΚΠΔ, αλλά σε ποιο βαθμό η νομοθεσία για την προστασία των δεδομένων προσωπικού χαρακτήρα είναι επαρκώς κατάλληλη για την προστασία των δεδομένων από την κυβερνητική πρόσβαση οπουδήποτε παγκοσμίως. Φυσικά, αυτό είναι ένα ερώτημα που αφορά αποκλειστικά τη νομοθεσία τρίτων χωρών και όχι τη νομοθεσία των κρατών-μελών της ΕΕ, αφού η εθνική ασφάλεια ανήκει στην αποκλειστική αρμοδιότητα των κρατών-μελών σύμφωνα με τη Συνθήκη της ΕΕ.

Γ. ΟΙ ΝΕΕΣ ΤΥΠΟΠΟΙΗΜΕΝΕΣ ΣΥΜΒΑΤΙΚΕΣ ΡΗΤΡΕΣ

Μετά την απόφαση του ΔΕΕ *Schrems I*, με την οποία ακυρώθηκε η απόφαση Ασφαλούς Λιμένα [βλ. Ενότητα II(Β)], πολλές επιχειρήσεις και οργανισμοί προχώρησαν στην υπογραφή των ΤΣΡ για να πλαισιώσουν τις διαβιβάσεις δεδομένων που διενεργούν σε τρίτες χώρες. Η αυξανόμενη πολυπλοκότητα της διασυνοριακής διαβίβασης και επεξεργασίας δεδομένων κατέστησε εμφανείς ορισμένες από τις προκλήσεις των προηγούμενων ΤΣΡ και εκτός από την πρόδηλη ανάγκη προσαρμογής αυτών στις νέες πτυχές του ΓΚΠΔ, η ανάγκη για επικαιροποίηση τους οξύνθηκε περισσότερο όταν το ΔΕΕ εξέδωσε την απόφαση *Schrems II*[186]. Ο νομικός και επιχειρηματικός κόσμος ανέμενε ούτως ή άλλως τις νέες ΤΣΡ από τότε που τέθηκε σε ισχύ ο ΓΚΠΔ, αλλά υπήρξε επιτακτική ανάγκη για τη συμπλήρωση αυτών των προτύπων μετά την απόφαση *Schrems II*, καθώς η εν λόγω απόφαση επέφερε μεγάλη αβεβαιότητα για τις επιχειρήσεις που διενεργούν διαβιβάσεις δεδομένων σε τρίτες χώρες.

[185] Δελτίο Τύπου Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων (2020*), European Data Protection Board - 41st Plenary session: EDPB adopts recommendations on supplementary measures following Schrems II*. Βέλγιο: Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. Διαθέσιμο στο: https://edpb.europa.eu/news/news/2020/european-data-protection-board-41st-plenary-session-edpb-adopts-recommendations_en.

[186] Βλ. Ilan, D., Kristensen, G., Ka Chun, L., Gerlach, N. και Mammì Borruto, F. (2021), «New Standard Contractual Clauses for Data Transfers under the GDPR - New Changes, New Questions?», ο.π.

Στις 4 Ιουνίου 2021, η Επιτροπή δημοσίευσε δυο εκτελεστικές αποφάσεις που υιοθετούν τις νέες ΤΣΡ, ύστερα από σχετική κοινοποίηση του σχεδίου αυτών για δημόσια διαβούλευση στις 12 Νοεμβρίου 2020. Πιο συγκεκριμένα, η Επιτροπή δημοσίευσε δύο δέσμες νέων ΤΣΡ, οι οποίες σηματοδοτούν τις πρώτες επικαιροποιήσεις των ΤΣΡ εδώ και περισσότερο από μια δεκαετία[187]. Οι εν λόγω εκτελεστικές αποφάσεις κατήργησαν τις αποφάσεις της Επιτροπής για την εφαρμογή των προηγούμενων ΤΣΡ, με ισχύ από τις 27 Σεπτεμβρίου 2021.

1. Το ευρύ φάσμα «σεναρίων» διαβίβασης

Η πρώτη δέσμη των προαναφερθέντων ΤΣΡ αντικαθιστά τις προηγούμενες ΤΣΡ για τις διαβιβάσεις δεδομένων σε τρίτες χώρες εκτός της ΕΕ (ήτοι τις αποφάσεις 2001/497/ΕΚ και 2010/87/ΕΕ)[188] (εφεξής «**Δέσμη Α**»), ενώ η δεύτερη δέσμη προορίζεται για χρήση μεταξύ υπευθύνων επεξεργασίας και εκτελούντων την επεξεργασία (εφεξής «**Δέσμη Β**»)[189]. Η υιοθέτηση των δυο αυτών δεσμών θα επιφέρει ομοιομορφία στις συμβατικές σχέσεις, καθώς μέχρι πρότινος οι εξαγωγείς δεδομένων διαμόρφωναν τους δικούς τους συμβατικούς όρους για την εκπλήρωση των υποχρεώσεων υπευθύνου επεξεργασίας - εκτελούντος την επεξεργασία βάσει του ΓΚΠΔ.

Οι νέες ΤΣΡ αντικατοπτρίζουν καλύτερα τις απαιτήσεις τόσο του ΓΚΠΔ όσο και της πρόσφατης κρίσης του ΔΕΕ στην απόφαση *Schrems II*, το σκεπτικό της οποίας επηρέασε, όπως είδαμε παραπάνω, και τις διαβιβάσεις που βασίζονται στο μηχανισμό των ΤΣΡ. Σε γενικές γραμμές, οι νέες ΤΣΡ βελτιστοποιούν τα προηγούμενα πρότυπα, καθώς παρέχουν μεγαλύτερη ευελιξία για μεγάλες και πολύπλοκες αλυσίδες επεξεργασίας και ένα ενιαίο σημείο εισόδου που καλύπτει ένα ευρύ φάσμα «σεναρίων» διαβίβασης[190].

---

[187] Francis, M. and Serafino M., (2021) «EU Releases New Standard Contractual Clauses for Cross-Border Data Transfers», *Holland & Knight Alert*. Διαθέσιμο στο: https://www.hklaw.com/en/insights/publications/2021/06/eu-releases-new-standard-contractual-clauses-for-crossborder.

[188] Ευρωπαϊκή Επιτροπή (2021), *Εκτελεστική Απόφαση (ΕΕ) 2021/914 της Επιτροπής της 4ης Ιουνίου 2021 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*, ο.π.

[189] Ευρωπαϊκή Επιτροπή (2021), *COMMISSION IMPLEMENTING DECISION on standard contractual clauses between controllers and processors under Article 28 (7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29 (7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council*. Βέλγιο: Ευρωπαϊκή Επιτροπή. Διαθέσιμο στο: https://ec.europa.eu/info/law/law-topic/data-protection/publications/standard-contractual-clauses-controllers-and-processors_en.

[190] Βλ. Δελτίο Τύπου Ευρωπαϊκής Επιτροπής (2021), *European Commission adopts new tools for safe exchanges of personal data*. Βέλγιο: Ευρωπαϊκή Επιτροπή. Διαθέσιμο στο: https://ec.europa.eu/commission/presscorner/detail/el/ip_21_2847.

Όπως χαρακτηριστικά δήλωσε η Αντιπρόεδρος της Ευρωπαϊκής Επιτροπής Αξιών και Διαφάνειας, Vera Jourová, στο Δελτίο Τύπου που συνόδευσε τις νέες ΤΣΡ: *«Στην Ευρώπη, θέλουμε να παραμείνουμε ανοικτοί και να επιτρέψουμε τη ροή των δεδομένων, υπό την προϋπόθεση ότι η προστασία θα είναι σύμφωνη με αυτά. Οι εκσυγχρονισμένες τυποποιημένες συμβατικές ρήτρες θα συμβάλουν στην επίτευξη αυτού του στόχου καθώς προσφέρουν στις επιχειρήσεις ένα χρήσιμο εργαλείο για να διασφαλίσουν ότι συμμορφώνονται με τους νόμους περί προστασίας δεδομένων, τόσο για τις δραστηριότητές τους εντός της Ευρωπαϊκής Ένωσης όσο και για τις διεθνείς διαβιβάσεις. Πρόκειται για μια αναγκαία λύση στο διασυνδεδεμένο ψηφιακό κόσμο, όπου η διαβίβαση δεδομένων γίνεται με ένα ή δύο κλικ»*[191].

Οι νέες ΤΣΡ θα πρέπει να διαβαστούν σε συνδυασμό με τις Συστάσεις 1/2020 του ΕΣΠΔ σχετικά με τα μέτρα που συμπληρώνουν τους μηχανισμούς διαβίβασης για τη διασφάλιση της συμμόρφωσης με το επίπεδο προστασίας των δεδομένων προσωπικού χαρακτήρα της ΕΕ, οι οποίες παρέχουν παραδείγματα αποδεκτών πρόσθετων μέτρων.

α) ΤΣΡ για τις διαβιβάσεις δεδομένων σε τρίτες χώρες (Δέσμη Α)

Η πρώτη δέσμη μπορεί να χρησιμοποιηθεί για διαβιβάσεις δεδομένων από την ΕΕ σε τρίτες χώρες, ως παραλήπτες, που η Επιτροπή δεν θεωρεί ότι παρέχουν επαρκή προστασία των δεδομένων προσωπικού χαρακτήρα. Σε αντίθεση με τις προηγούμενες ΤΣΡ, οι οποίες κάλυπταν αφενός τις διαβιβάσεις μεταξύ δυο υπεύθυνων επεξεργασίας και αφετέρου τις διαβιβάσεις μεταξύ ενός υπευθύνου επεξεργασίας και ενός εκτελούντος την επεξεργασία, η πρώτη δέσμη έχει σχεδιαστεί για να είναι πιο ευέλικτη, ακολουθώντας μια προσέγγιση βάσει ενοτήτων («*modular approach*») που θα χρησιμοποιούν οι εξαγωγείς δεδομένων με βάση τη διανομή των αρμοδιοτήτων τους σε σχέση με την κατά περίπτωση διαβίβαση δεδομένων. Πιο συγκεκριμένα, προβλέπονται οι εξής ενότητες:

- Πρώτη Ενότητα: Διαβιβάσεις μεταξύ υπευθύνων επεξεργασίας (*«Controller-to-Controller»*)
- Δεύτερη Ενότητα: Διαβιβάσεις μεταξύ υπευθύνου επεξεργασίας και εκτελούντος την επεξεργασία (*«Controller-to-Processor»*)
- Τρίτη Ενότητα: Διαβιβάσεις μεταξύ εκτελούντων την επεξεργασία (*«Processor-to-Processor»*)

[191] Βλ. Δελτίο Τύπου Ευρωπαϊκής Επιτροπής (2021), *European Commission adopts new tools for safe exchanges of personal data*, ο.π.

- Τέταρτη Ενότητα: Διαβιβάσεις μεταξύ εκτελούντος την επεξεργασία και υπευθύνου επεξεργασίας («*Processor-to-Controller*»)

Αξίζει να σημειωθεί ότι οι προηγούμενες ΤΣΡ δεν προέβλεπαν την περίπτωση διαβιβάσεων μεταξύ εκτελούντων την επεξεργασία ή μεταξύ ενός εκτελούντος την επεξεργασία προς έναν υπεύθυνο επεξεργασίας. Επομένως, όταν προέκυπταν τέτοιες περιστάσεις κατά τη σύναψη συμβάσεων, υπήρχε ένα κενό στις νόμιμες διαβιβάσεις δεδομένων σε τρίτες χώρες. Επιπλέον, οι επικαιροποιήσεις αναγνωρίζουν - για πρώτη φορά - ότι ο εξαγωγέας δεδομένων μπορεί να είναι οντότητα εκτός της ΕΕ, γεγονός που είναι χρήσιμο όταν, για παράδειγμα, ένας εξαγωγέας δεδομένων εκτός της ΕΕ υπόκειται στο ΓΚΠΔ και θέλει να διαβιβάσει δεδομένα σε τρίτη χώρα εκτός της ΕΕ.

β) ΤΣΡ μεταξύ υπευθύνου επεξεργασίας και εκτελούντος την επεξεργασία (Δέσμη Β)

Η δεύτερη δέσμη ΤΣΡ προβλέπει μια τυποποιημένη συμφωνία προστασίας δεδομένων που ενέκρινε η Επιτροπή[192], όσον αφορά τον ορισμό των εκτελούντων την επεξεργασία εντός της ΕΕ σύμφωνα με το άρθρο 28 του ΓΚΠΔ. Η εν λόγω τυποποιημένη συμφωνία χρησιμοποιείται κυρίως μεταξύ εκτελούντων την επεξεργασία και υπευθύνων επεξεργασίας που είναι εγκατεστημένοι στην ΕΕ. Παρά το γεγονός ότι μέχρι και σήμερα οι εν λόγω εξαγωγείς δεδομένων στηρίζονταν σε δικές τους έντυπες ΤΣΡ στο πλαίσιο των διαβιβάσεων μεταξύ των κρατών-μελών της ΕΕ, πλέον η Δέσμη Β χορηγεί ένα πλήρες πρότυπο προς τις επιχειρήσεις, και δη στις μικρομεσαίες επιχειρήσεις, με το οποίο θα εξασφαλίζουν με βεβαιότητα - την όποια βεβαιότητα μπορεί κανείς να εγγυηθεί δεδομένης της ταχύτητας των εναλλαγών στο πεδίο των διαβιβάσεων - την πολυπόθητη συμμόρφωση με το ΓΚΠΔ.

2. Καινοτομίες και αντιφάσεις των ΤΣΡ για τις διαβιβάσεις δεδομένων

Οι νέες ΤΣΡ της Δέσμης Α, όπως ήταν αναμενόμενο και θεμιτό, επέφεραν πλήθος καινοτομιών στο πεδίο των διαβιβάσεων δεδομένων σε τρίτες χώρες, μεταξύ των οποίων θα μπορούσαμε να ξεχωρίσουμε τις ακόλουθες:

(α) Κατέστησαν δυνατή την προσχώρηση περισσότερων μερών στους συμβατικούς όρους, μέσω της πρόβλεψης ότι επιτρέπεται σε πρόσθετους υπευθύνους επεξεργασίας και εκτελούντες την επεξεργασία να προσχωρούν στις ΤΣΡ, ως

[192] Επί τη βάσει του άρθρου 28, παράγραφος 7 του ΓΚΠΔ: «*Η Επιτροπή μπορεί να θεσπίσει τυποποιημένες συμβατικές ρήτρες για τα θέματα που αναφέρονται στις παραγράφους 3 και 4 του παρόντος άρθρου και σύμφωνα με τη διαδικασία εξέτασης που αναφέρεται στο άρθρο 93 παράγραφος 2*».

εξαγωγείς ή εισαγωγείς δεδομένων, καθ' όλη τη διάρκεια του κύκλου ζωής της σύμβασης[193]. Ωστόσο, η Δέσμη Α δεν προσδιορίζει τον τρόπο με τον οποίο τα υφιστάμενα μέρη θα πρέπει να παρέχουν τη συγκατάθεσή τους για την προσχώρηση έκαστου νέου μέρους στις ΤΣΡ, γεγονός που μπορεί να οδηγήσει σε διαφορετικές ερμηνείες, και κατ' επέκταση πρακτικές, μεταξύ των επιχειρήσεων, και άρα να καταστήσει το σύνθετο αυτό συμβατικό «οικοσύστημα» γρήγορα δυσλειτουργικό και να υπονομεύσει την ευελιξία που αυτό εισήγαγε.

(β) Οι νέες ΤΣΡ επιτρέπουν στους εισαγωγείς δεδομένων να διαβιβάζουν δεδομένα προσωπικού χαρακτήρα σε τρίτες χώρες χωρίς τη σύναψη ΤΣΡ ή παρόμοιων δεσμευτικών μέσων, όταν η περαιτέρω διαβίβαση είναι απαραίτητη για τη θεμελίωση, άσκηση ή υπεράσπιση νομικών αξιώσεων ή είναι απαραίτητη για την προστασία των ζωτικών συμφερόντων του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου[194].

(γ) Σύμφωνα με τις προηγούμενες ΤΣΡ, ο εξαγωγέας δεδομένων έπρεπε να είναι εγκατεστημένος στην ΕΕ, καθιστώντας τον εν λόγω μηχανισμό διαβίβασης μη διαθέσιμο για έναν εξαγωγέα δεδομένων που είναι εγκατεστημένος εκτός της ΕΕ, που όμως εξακολουθεί να υπόκειται στο ΓΚΠΔ δυνάμει του άρθρου 3 παράγραφος 2 του ΓΚΠΔ. Αντίθετα, οι νέες ΤΣΡ δεν περιέχουν κανένα ρητό περιορισμό όσον αφορά τον τόπο εγκατάστασης του εξαγωγέα δεδομένων. Συγκεκριμένα, η εκτελεστική απόφαση για τις νέες ΤΣΡ της Δέσμης Α ορίζει ότι: «*Οι τυποποιημένες συμβατικές ρήτρες… θεωρείται ότι παρέχουν κατάλληλες εγγυήσεις… για τη διαβίβαση, από υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία, δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία σύμφωνα με τις διατάξεις του εν λόγω κανονισμού (εξαγωγέας των δεδομένων) προς υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία (υπεργολάβο επεξεργασίας) ο οποίος εκτελεί επεξεργασία που δεν υπόκειται στις διατάξεις του εν λόγω κανονισμού (εισαγωγέας των δεδομένων)*»[195].

(δ) Ειδικότερα, σε ότι αφορά την σχέση υπευθύνου επεξεργασίας και εκτελούντος την επεξεργασία οι νέες ΤΣΡ προβλέπουν τις εξής υποχρεώσεις:

[193] Ρήτρα 7 της Εκτελεστικής Απόφασης (ΕΕ) 2021/914 της Ευρωπαϊκής Επιτροπής, ο.π.

[194] Ρήτρα 8.7 (Ενότητα 1) και Ρήτρα 8.8 (Ενότητες 2 και 3) της Εκτελεστικής Απόφασης (ΕΕ) 2021/914 της Ευρωπαϊκής Επιτροπής, ο.π.

[195] Άρθρο 1 της Εκτελεστικής Απόφασης (ΕΕ) 2021/914 της Ευρωπαϊκής Επιτροπής, ο.π.

1. Ο εξαγωγέας δεδομένων με τη συνδρομή του εισαγωγέα δεδομένων να εξετάζει το επίπεδο προστασίας των δεδομένων προσωπικού χαρακτήρα στη χώρα προορισμού εκτός της ΕΕ,

2. Ο εισαγωγέας δεδομένων να ενημερώνει τον εξαγωγέα δεδομένων για τυχόν αδυναμία συμμόρφωσης με τις νέες ΤΣΡ, ώστε ο εξαγωγέας δεδομένων είτε να αναστέλλει τη διαβίβαση δεδομένων είτε να τερματίζει τη συμφωνία.

3. Ο εισαγωγέας δεδομένων να ενημερώνει αμέσως τον εξαγωγέα δεδομένων και, εφόσον είναι δυνατόν, το υποκείμενο των δεδομένων σε περίπτωση που[196]:

- λαμβάνει νομικά δεσμευτικό αίτημα από δημόσια αρχή, συμπεριλαμβανομένων των δικαστικών αρχών, για τη γνωστοποίηση των διαβιβαζόμενων δεδομένων προσωπικού χαρακτήρα, ή εάν
- λάβει γνώση οποιασδήποτε άμεσης πρόσβασης δημόσιων αρχών στα διαβιβαζόμενα δεδομένα προσωπικού χαρακτήρα.

Στις περιπτώσεις, μάλιστα, όπου ο εισαγωγέας δεδομένων απαγορεύεται να ενημερώσει τον εξαγωγέα δεδομένων ή/και το υποκείμενο των δεδομένων σύμφωνα με τη νομοθεσία της χώρας προορισμού, οι νέες ΤΣΡ προβλέπουν ότι ο εισαγωγέας δεδομένων πρέπει να καταβάλει κάθε δυνατή προσπάθεια για να επιτύχει την άρση της απαγόρευσης, με σκοπό την κοινοποίηση όσο το δυνατόν περισσότερων πληροφοριών και το συντομότερο δυνατόν[197].

Εντούτοις, υπάρχει και ο αντίλογος ως προς τις παραπάνω καινοτομίες των νέων ΤΣΡ, καθώς στο περιεχόμενο αυτών εντοπίζονται ορισμένες αντιφάσεις.

Ειδικότερα, αναφορικά με τον εισαγωγέα δεδομένων, τόσο το άρθρο 1, παράγραφος 1 όσο και η Αιτιολογική Σκέψη 7 της εκτελεστικής απόφασης για τις νέες ΤΣΡ της Δέσμης Α προβλέπουν ρητά ότι οι νέες ΤΣΡ θεωρούνται κατάλληλες εγγυήσεις κατά την έννοια του ΓΚΠΔ μόνο σε περίπτωση διαβίβασης δεδομένων σε εισαγωγέα δεδομένων εκτός της ΕΕ που δεν εμπίπτει στο εδαφικό πεδίο εφαρμογής του ΓΚΠΔ σύμφωνα με το άρθρο 3. Τούτου λεχθέντος, εφόσον ο εισαγωγέας δεδομένων εκτός της ΕΕ εμπίπτει στο εδαφικό πεδίο εφαρμογής του ΓΚΠΔ, οι νέες ΤΣΡ δεν μπορούν να εφαρμοστούν για τη νομιμοποίηση της

[196] Αιτιολογική Σκέψη 22 της Εκτελεστικής Απόφασης (ΕΕ) 2021/914 της Ευρωπαϊκής Επιτροπής, ο.π.
[197] Ρήτρα 15, παράγραφος 15.1, στοιχείο β' της Εκτελεστικής Απόφασης (ΕΕ) 2021/914 της Ευρωπαϊκής Επιτροπής, ο.π.

διαβίβασης δεδομένων προς αυτόν[198]. Η εν λόγω, βέβαια, διατύπωση και προσέγγιση έρχεται σε αντίθεση με τη θέση που έχει λάβει το ΕΣΠΔ [βλ. Ενότητα Ι(Γ)(2)], το οποίο στα σωρευτικά κριτήρια των προαναφερόμενων κατευθυντήριων γραμμών του, αναφέρει ότι ο εισαγωγέας δεδομένων πρέπει να βρίσκεται σε τρίτη χώρα, ανεξάρτητα από το εάν καλύπτεται από το ΓΚΠΔ σε ότι αφορά την υπό κρίση επεξεργασία με βάση το άρθρο 3 του ΓΚΠΔ.

Επιπλέον, οι νέες ΤΣΡ δεν διευκρινίζουν ποια αποτελεσματικά μέτρα πρέπει να λαμβάνουν οι εξαγωγείς και οι εισαγωγείς δεδομένων προκειμένου να εξασφαλίζουν ένα ουσιαστικά ισοδύναμο επίπεδο προστασίας των δεδομένων προσωπικού χαρακτήρα. Αναφέρουν μόνο ότι τα μέρη θα πρέπει να εξετάζουν το ενδεχόμενο να προσφεύγουν σε κρυπτογράφηση ή ψευδωνυμοποίηση, όταν ο σκοπός της επεξεργασίας μπορεί να εκπληρωθεί με αυτόν τον τρόπο. Λόγω αυτού, οι ΤΣΡ θα πρέπει να διαβαστούν, όπως εισαγωγικά αναφέρθηκε, σε συνδυασμό με τις προαναφερθείσες Συστάσεις 01/2020 του ΕΣΠΔ για περαιτέρω σαφήνεια. Και τούτο διότι, οι συγκεκριμένες συστάσεις του ΕΣΠΔ προσφέρουν έναν μη εξαντλητικό κατάλογο παραγόντων για τον προσδιορισμό των 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.

Όπως είναι αναμενόμενο, η πολυπλοκότητα της νέας διαδικασίας μπορεί να οδηγήσει τις επιχειρήσεις, ιδίως τις μικρομεσαίες, να αποφύγουν τη «διέξοδο» των ΤΣΡ. Και τούτο διότι, ενώ οι μεγάλες επιχειρήσεις μπορούν να ανταπεξέλθουν οικονομικά στις δαπανηρές διαδικασίες για την αξιολόγηση της νομοθεσίας μιας τρίτης χώρας ως προς τη συμβατότητά

[198] Ionescu, R. and Bucur, M. (2021) «First thoughts on the new SCCs for international transfers of personal data», *Privacy Out Loud - Nestor Nestor Diculescu Kingston Petersen*. Διαθέσιμο στο: https://privacyoutloud.ro/articles/first-thoughts-on-the-new-sccs-for-international-transfers-of-personal-data-2/.

της με το δίκαιο της ΕΕ, οι μικρομεσαίες επιχειρήσεις δεν έχουν αυτή την οικονομική και πρακτική δυνατότητα[199].

3. Στη σκιά της απόφασης Schrems II

Όπως είδαμε παραπάνω, το Δικαστήριο της ΕΕ διακήρυξε στην απόφαση *Schrems II* ότι οι προηγούμενες ΤΣΡ παραμένουν ένας έγκυρος μηχανισμός για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες από εξαγωγείς δεδομένων που εδρεύουν στην ΕΕ σε εισαγωγείς δεδομένων εκτός της ΕΕ.

Ωστόσο, το ΔΕΕ (και εν συνεχεία το ΕΣΠΔ μέσω των Συστάσεών του) διευκρίνισε ότι θα πρέπει να αξιολογείται κατά περίπτωση: α) εάν οι ΤΣΡ επαρκούν για τη διασφάλιση των δεδομένων προσωπικού χαρακτήρα και β) εάν τυχόν θα πρέπει να εφαρμοστούν κατάλληλες πρόσθετες εγγυήσεις.

Η Δέσμη Α περιέχει διατάξεις που επιδιώκουν να αντιμετωπίσουν τυχόν επιπτώσεις που μπορεί να έχουν οι νόμοι της χώρας προορισμού στη συμμόρφωση του εισαγωγέα δεδομένων με τις υποχρεώσεις του βάσει αυτής της δέσμης. Αυτό περιλαμβάνει διατάξεις που διέπουν τον τρόπο αντιμετώπισης δεσμευτικών αιτημάτων από δημόσιες αρχές της χώρας προορισμού, καθώς και εγγυήσεις που αφορούν στην ακρίβεια της εκτίμησης των μερών σχετικά με τη νομοθεσία της χώρας προορισμού και την προστασία που παρέχει στα δεδομένα προσωπικού χαρακτήρα.

Εντούτοις, ενώ η Δέσμη Α περιλαμβάνει συμβατικές εγγυήσεις για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες, δεν αίρει εντελώς τις ανησυχίες που επισημάνθηκαν από το ΔΕΕ στην απόφαση *Schrems II*. Οι εξαγωγείς δεδομένων που διαβιβάζουν δεδομένα προσωπικού χαρακτήρα εκτός της ΕΕ εξακολουθούν να υποχρεούνται στη διενέργεια της σχετικής αξιολόγησης κινδύνου και, κατά περίπτωση, να εφαρμόζουν τεχνικές και οργανωτικές εγγυήσεις που συμπληρώνουν τις συμβατικές διατάξεις που περιέχονται στη Δέσμη Α. Σημαντικό αρωγό στην εν λόγω υποχρέωση των εξαγωγέων δεδομένων συνιστούν οι Συστάσεις του ΕΣΠΔ, που εξετάσαμε ανωτέρω.

Στο πλαίσιο αυτό, οι νέες ΤΣΡ της Δέσμης Α ενσωματώνουν πρόβλεψη για τη διενέργεια εκτίμησης αντικτύπου της διαβίβασης (Transfer Impact Assessment ή «TIA») από τον

[199] Βλ. Chander, A. (2020), «Is Data Localization a Solution for Schrems II?», *Journal of International Economic Law*, 2020, 23, 771-784. Διαθέσιμο στο: https://academic.oup.com/jiel/article-abstract/23/3/771/5909035?redirectedFrom=fulltext.

εξαγωγέα δεδομένων (σε συνεργασία με την εισαγωγέα δεδομένων), και τη διάθεση της τεκμηριωμένης αυτής αξιολόγησης στην αρμόδια ΑΠΔ κατόπιν αιτήματος αυτής[200]. Οι ρήτρες καθορίζουν τους παράγοντες που πρέπει να εξετάζει ο εξαγωγέας δεδομένων (με τη συνδρομή του εισαγωγέα δεδομένων) σε μια εκτίμηση αντικτύπου διαβίβασης. Εκτός από την εξέταση της νομοθεσίας και της πρακτικής στην τρίτη χώρα, οι ρήτρες των νέων ΤΣΡ αναφέρονται επίσης και σε άλλα χρήσιμα στοιχεία, ήτοι τις ειδικές περιστάσεις της διαβίβασης, συμπεριλαμβανομένου του μήκους της αλυσίδας επεξεργασίας, του αριθμού των εμπλεκόμενων παραγόντων και των διαύλων διαβίβασης που χρησιμοποιήθηκαν, τις σκοπούμενες περαιτέρω διαβιβάσεις, τον τύπο του αποδέκτη, τον σκοπό της επεξεργασίας, τις κατηγορίες και το μορφότυπο των διαβιβαζόμενων δεδομένων προσωπικού χαρακτήρα, τον οικονομικό τομέα στον οποίο πραγματοποιείται η διαβίβαση, και τη θέση αποθήκευσης των διαβιβαζόμενων δεδομένων.

Η παραπάνω αξιολόγηση (των νόμων και των πρακτικών) θα πρέπει να περιλαμβάνει αξιόπιστες πληροφορίες σχετικά με την εφαρμογή του νόμου στην πράξη (όπως νομολογία και εκθέσεις ανεξάρτητων εποπτικών φορέων), την ύπαρξη ή την απουσία αιτημάτων στον ίδιο τομέα και, υπό αυστηρές προϋποθέσεις, την τεκμηριωμένη πρακτική εμπειρία του εξαγωγέα ή/και του εισαγωγέα δεδομένων με προηγούμενες περιπτώσεις αιτημάτων πρόσβασης από δημόσιες αρχές ή την απουσία τέτοιων αιτημάτων, που καλύπτουν ένα επαρκώς αντιπροσωπευτικό χρονικό διάστημα[201]. Ωστόσο, εάν τα μέρη επιθυμούν να επικαλεστούν την πρακτική εμπειρία τους από την πρόσβαση των δημόσιων αρχών στα δεδομένα, θα πρέπει να υποστηρίζεται από άλλα σχετικά, αντικειμενικά στοιχεία. Ειδικότερα, τα μέρη πρέπει να λάβουν υπόψη τους κατά πόσο η εμπειρία τους επιβεβαιώνεται και δεν αντικρούεται από δημοσίως διαθέσιμες ή με άλλον τρόπο προσβάσιμες, αξιόπιστες πληροφορίες σχετικά με την ύπαρξη ή την απουσία αιτημάτων στον ίδιο τομέα και/ή την εφαρμογή της νομοθεσίας στην πράξη, όπως η νομολογία και οι εκθέσεις ανεξάρτητων εποπτικών φορέων[202].

4. Το χρονικό πλαίσιο εφαρμογής

[200] Ρήτρα 14 της Εκτελεστικής Απόφασης (ΕΕ) 2021/914 της Ευρωπαϊκής Επιτροπής, ο.π.

[201] Βλ. Ilan, D., Kristensen, G., Ka Chun, L., Gerlach, N. και Mammì Borruto, F. (2021), «New Standard Contractual Clauses for Data Transfers under the GDPR - New Changes, New Questions?», ο.π.

[202] Βλ. υποσημείωση 12, αφορώσα στη Ρήτρα 14, της Εκτελεστικής Απόφασης (ΕΕ) 2021/914 της Ευρωπαϊκής Επιτροπής, ο.π.

Οι νέες ΤΣΡ τέθηκαν σε ισχύ την εικοστή ημέρα από τη δημοσίευσή τους στην Επίσημη Εφημερίδα της ΕΕ, ήτοι στις 27 Ιουνίου 2021. Επομένως, από εκείνη την ημερομηνία, οι εξαγωγείς δεδομένων μπορούσαν να τις χρησιμοποιούν για τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα.

Οι προηγούμενες ΤΣΡ καταργήθηκαν τρεις μήνες μετά τη δημοσίευση των νέων ΤΣΡ, ήτοι στις 27 Σεπτεμβρίου 2021. Αξιοσημείωτο είναι ότι η Επιτροπή παρέχει στις επιχειρήσεις περίοδο χάριτος δεκαπέντε μηνών για να συνεχίσουν να χρησιμοποιούν τις προηγούμενες ΤΣΡ σε συμφωνίες που έχουν συναφθεί πριν από την κατάργηση των προηγούμενων προτύπων. Ωστόσο, αυτό ισχύει μόνο υπό την προϋπόθεση ότι οι πράξεις επεξεργασίας που αποτελούν αντικείμενο της σύμβασης παραμένουν αμετάβλητες και *«ότι η επίκληση των ρητρών διασφαλίζει ότι η διαβίβαση δεδομένων προσωπικού χαρακτήρα υπόκειται σε κατάλληλες εγγυήσεις»*[203]. Το τελευταίο συνεπάγεται ότι η αξιολόγηση κινδύνου που απαιτείται από την απόφαση *Schrems II*, θα πρέπει να διενεργηθεί.

Αντίθετα, σε περίπτωση που οι πράξεις επεξεργασίας μεταβληθούν, οι επιχειρήσεις υποχρεούνται να θέσουν απευθείας σε εφαρμογή τις νέες ΤΣΡ ή άλλους μηχανισμούς διαβίβασης σύμφωνα με το ΓΚΠΔ, προκειμένου να νομιμοποιήσουν τις διαβιβάσεις δεδομένων που διενεργούν. Στο πλαίσιο αυτό, παρά το γεγονός ότι η Δέσμη Α δεν παρέχει συγκεκριμένο κατάλογο με τις μεταβολές που μπορούν ενεργοποιούσαν την εν λόγω υποχρέωση, η Αιτιολογική Σκέψη 24 της Δέσμης Α αναφέρει ρητά ότι η υποχρέωση αυτή θα υφίσταται σε περίπτωση ανάθεσης σε υπεργολάβους επεξεργασίας μέρους ή συνόλου των πράξεων επεξεργασίας που καλύπτονται από τη σύμβαση του εκτελούντα την επεξεργασία (αναδόχου) με τον υπεύθυνο επεξεργασίας.

Στο σύνολό τους, οι προηγούμενες ΤΣΡ θα πρέπει να αντικατασταθούν με τη Δέσμη Α το αργότερο μέχρι τις 27 Δεκεμβρίου 2022, υπό την προϋπόθεση βέβαια ότι οι εξαγωγείς και εισαγωγείς δεδομένων θα συνεχίσουν να βασίζονται στις ΤΣΡ ως μηχανισμό για τη διενέργεια των διαβιβάσεων εκτός της ΕΕ.

Όσον αφορά τη Δέσμη Β, δεν τίθεται ορισμένο χρονικό πλαίσιο εφαρμογής αυτής, αφού δεν αντικαθιστά υφιστάμενους όρους ή πρότυπα. Επομένως, μπορεί να χρησιμοποιηθεί ως

[203] Αιτιολογική Σκέψη 24 και Άρθρο 4 της Εκτελεστικής Απόφασης (ΕΕ) 2021/914 της Ευρωπαϊκής Επιτροπής, ο.π.

υπόδειγμα για μελλοντικές συμφωνίες επεξεργασίας δεδομένων μεταξύ ενός υπευθύνου επεξεργασίας και ενός εκτελούντος την επεξεργασία εντός της ΕΕ ανά πάσα στιγμή.

Είναι βέβαιο ότι οι νέες ΤΣΡ θα αποτελέσουν εφεξής σημαντικό αρωγό για τις διαβιβάσεις δεδομένων, καθώς ενσωματώνουν την κρίση του ΔΕΕ με τη μορφή υποχρεώσεων για κάθε εμπλεκόμενο «ρόλο ιδιωτικότητας», γεγονός που ήδη έχει ξεκινήσει να μεταλαμπαδεύει ταχύτατα το νέο καθεστώς σε όλα τα μήκη και πλάτη του σύγχρονου ψηφιακού κόσμου. Όπως χαρακτηριστικά δήλωσε ο Επίτροπος Δικαιοσύνης της ΕΕ, Didier Reynders: *«Στο σύγχρονο ψηφιακό κόσμο, είναι σημαντικό να μπορούμε να μοιραζόμαστε τα δεδομένα έχοντας την απαραίτητη προστασία, τόσο εντός και όσο και εκτός της ΕΕ. Με αυτές τις ενισχυμένες ρήτρες, παρέχουμε μεγαλύτερη προστασία και ασφάλεια δικαίου στις εταιρείες για τη διαβίβαση δεδομένων. Μετά την έκδοση της απόφασης Schrems II, ήταν καθήκον και προτεραιότητά μας να επινοήσουμε εργαλεία φιλικά προς τον χρήστη, στα οποία οι επιχειρήσεις θα μπορούν να έχουν απόλυτη εμπιστοσύνη...»*[204].

Δ. ΕΙΔΙΚΑ ΖΗΤΗΜΑΤΑ

Όπως ήταν αναμενόμενο, οι παραπάνω εξελίξεις σε ενωσιακό επίπεδο δημιούργησαν πρακτικά προβλήματα αναφορικά με τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες, και ώθησαν σε άμεση κινητοποίηση τόσο την Επιτροπή, όσο και τις ΑΠΔ. Πιο συγκεκριμένα, στην παρούσα υποενότητα θα προσπαθήσουμε αρχικά να δώσουμε απάντηση σε ορισμένα καίρια ερωτήματα που έχουν ανακύψει αναφορικά με το νέο πεδίο δράσης τόσο για τους εξαγωγείς όσο και για τους εισαγωγείς δεδομένων **(1)**. Στη συνεχεία, θα εξετάσουμε το νέο καθεστώς διαβιβάσεων που ισχύει για το Ηνωμένο Βασίλειο μετά το Brexit **(2)**, καθώς και την πρώτη απόφαση επάρκειας που δημοσίευσε η Επιτροπή μετά την απόφαση *Schrems II* **(3)**. Τέλος, θα μελετήσουμε τις πρώτες αποφάσεις των ΑΠΔ που αντικατοπτρίζουν τη νέα συνθήκη που καθιέρωσε η νομολογία του ΔΕΕ για τις διαβίβασης δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες **(4)**.

1. Το νέο πεδίο δράσης για τους «ρόλους ιδιωτικότητας»

Οι παραπάνω ενωσιακές εξελίξεις ευλόγως γέννησαν τα ακόλουθα ερωτήματα: α) πως πρέπει να ενεργούν πλέον οι εξαγωγείς και εισαγωγείς δεδομένων; ειδικότερα β) τι πρέπει να προσέχει ένας υπεύθυνος επεξεργασίας σε περίπτωση που χρησιμοποιεί έναν εκτελών

[204] Βλ. Δελτίο Τύπου Ευρωπαϊκής Επιτροπής (2021), *European Commission adopts new tools for safe exchanges of personal data*, ο.π.

την επεξεργασίας, ο οποίος διαβιβάζει δεδομένα στις ΗΠΑ ή σε άλλη τρίτη χώρα; και γ) ποιος ο υφιστάμενος ρόλος των εθνικών ΑΠΔ; Στην παρούσα υποενότητα θα προσπαθήσουμε να δώσουμε σύντομες απαντήσεις επί των εν λόγω ερωτημάτων, σύμφωνα με το υφιστάμενο πλαίσιο.

α) Πως πρέπει να ενεργούν πλέον οι εξαγωγείς και εισαγωγείς δεδομένων;

Το ΔΕΕ στην απόφασή του *Schrems II* επισήμανε ότι αποτελεί πρωταρχική υποχρέωση τόσο του εξαγωγέα όσο και του εισαγωγέα δεδομένων να αξιολογούν κατά περίπτωση, πριν από κάθε διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτη χώρα, το δίκαιο της χώρας προορισμού για να προσδιορίσουν εάν το εν λόγω εθνικό δίκαιο επιτρέπει στον εισαγωγέα δεδομένων να συμμορφώνεται στην πράξη με το μηχανισμό διαβίβασης που έχει επιλεγεί συμβατικά, λαμβάνοντας υπόψη όλες τις περιστάσεις της διαβίβασης, και τα πιθανά πρόσθετα μέτρα που θα μπορούσαν να εφαρμόσουν τα συμβαλλόμενα μέρη μέσω συμβατικών δεσμεύσεων. Πιο συγκεκριμένα, θα πρέπει να ελέγχουν, πριν από την πρώτη διαβίβαση δεδομένων, εάν υπάρχει δυνατότητα για τις δημόσιες αρχές της τρίτης χώρας να έχουν πρόσβαση στα διαβιβαζόμενα δεδομένα, κατά τρόπο που υπερβαίνει τα επιτρεπόμενα από το δίκαιο της ΕΕ. Παράλληλα, θα πρέπει να ελέγξουν εάν το επίπεδο προστασίας των δεδομένων που απαιτείται από το δίκαιο της ΕΕ τηρείται εντός της τρίτης χώρας. Στο πλαίσιο αυτού του ελέγχου μπορεί να συναχθεί ότι απαιτείται η εφαρμογή από τον εξαγωγέα και των εισαγωγέα δεδομένων πρόσθετων μέτρων[205], τα οποία, όταν προστίθενται στις εγγυήσεις που περιέχονται στο μηχανισμό διαβίβασης, θα διασφαλίσουν ότι τα δεδομένα που διαβιβάζονται τυγχάνουν ενός επιπέδου προστασίας στην τρίτη χώρα, το οποίο είναι ουσιαστικά ισοδύναμο με εκείνο που διασφαλίζεται στο εσωτερικό της ΕΕ[206]. Μετά από αυτή την αξιολόγηση, εάν ο εξαγωγέας δεδομένων που διαβιβάζει δεδομένα προσωπικού χαρακτήρα, καταλήξει στο συμπέρασμα ότι δεν έχουν διασφαλιστεί οι κατάλληλες εγγυήσεις, και ότι κανένα πρόσθετο μέτρο δεν μπορεί να διασφαλίσει ένα ουσιαστικά ισοδύναμο επίπεδο προστασίας για τη διαβίβαση, τότε πρέπει να αναστείλει ή να διακόψει τη διαβίβαση των δεδομένων στον εισαγωγέα δεδομένων, ενώ τα δεδομένα που έχουν ήδη διαβιβαστεί στην τρίτη χώρα και τα αντίγραφα αυτών θα πρέπει να επιστραφούν ή να καταστραφούν στο σύνολό τους. Εάν, ωστόσο, ο εξαγωγέας δεδομένων σκοπεύει να

[205] Τα πρόσθετα μέτρα είναι εξ ορισμού συμπληρωματικά των εγγυήσεων που παρέχει ήδη ο μηχανισμός διαβίβασης του άρθρου 46 του ΓΚΠΔ, βλ. Αιτιολογική σκέψη 109 του ΓΚΠΔ και ΔΕΕ, C-311/18, *Schrems II*, ο.π., παράγραφος 133.

[206] ΔΕΕ, C-311/18, *Schrems II*, ο.π., παράγραφος 96.

συνεχίσει τη διαβίβαση δεδομένων προσωπικού χαρακτήρα παρά το προαναφερθέν συμπέρασμα, τότε πρέπει να ενημερώσει την αρμόδια ΑΠΔ, η οποία σε αυτή την περίπτωση δύναται είτε να αναστείλει είτε να απαγορεύσει τη συγκεκριμένη διασυνοριακή διαβίβαση[207].

Για το συμβαλλόμενο μέρος που ενεργεί ως εισαγωγέας των δεδομένων, το ΔΕΕ προβλέπει την υποχρέωση να ενημερώνει τον εξαγωγέα των δεδομένων σε περίπτωση τυχόν αδυναμίας του να συμμορφωθεί με τις ΤΣΡ, οπότε ο εξαγωγέας δεδομένων οφείλει να αναστείλει τη διαβίβαση δεδομένων ή να καταγγείλει τη σύμβαση την οποία έχει συνάψει με τον εισαγωγέα των δεδομένων[208].

Σε ότι αφορά τους υπευθύνους επεξεργασίας δεν προξενεί έκπληξη η προαναφερθείσα μετακύλιση του βάρους απόφασης από τις ΑΠΔ στους πρώτους, καθώς αυτό αντανακλά το γενικότερο πνεύμα του ΓΚΠΔ, ο οποίος επιφορτίζει τους υπεύθυνους επεξεργασίας με πλήθος αρμοδιοτήτων, όπως ενδεικτικά στις διατάξεις που αφορούν στην υποχρέωση διεξαγωγής εκτίμησης αντικτύπου, η οποία, μαζί με την υποχρέωση τήρησης αρχείων καταγραφής δραστηριοτήτων, έρχεται να αντικαταστήσει την προισχύσασα γενική υποχρέωση γνωστοποίησης στην αρμόδια ΑΠΔ που θέσπιζε η Οδηγία.

Όπως γίνεται αντιληπτό, η νέα αυστηροποιημένη συνθήκη για τις διαβιβάσεις δεδομένων σε τρίτες χώρες, απαιτεί από τους εξαγωγείς δεδομένων (είτε υπευθύνους επεξεργασίας είτε εκτελούντες την επεξεργασία) να γίνουν εμπειρογνώμονες στο δίκαιο των τρίτων χωρών, κατά τρόπο που πιθανώς υπερβαίνει τις δυνατότητες αυτών, και εγείρει ερωτήματα ιδίως σχετικά με τη διαβίβαση δεδομένων σε τρίτες χώρες που δεν είναι δημοκρατικές ή στις οποίες δεν ισχύει το κράτος δικαίου[209]. Για παράδειγμα, εύλογα μπορεί κανείς να αναρωτηθεί, κατά πόσο οι ιδιωτικές επιχειρήσεις που επεξεργάζονται δεδομένα προσωπικού χαρακτήρα μπορούν να εξειδικεύσουν τις δυσνόητες και αόριστες νομικές έννοιες που άπτονται στο δίκαιο προστασίας δεδομένων προσωπικού χαρακτήρα, και να

[207] ΔΕΕ, C-311/18, *Schrems II*, ο.π., παράγραφος 145. Επίσης, Συστάσεις 01/2020, ο.π., παράγραφος 53.
[208] ΔΕΕ, C-311/18, *Schrems II*, ο.π., παράγραφοι 142.
[209] Kuner, C. (2020), «The Schrems II judgment of the Court of Justice and the future of data transfer regulation», *European Law Blog*. Διαθέσιμο στο: https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation/#:~:text=In%20Schrems%20II%20the%20Court,Privacy%20Shield%2C%20which%20was%20the.

παρέχουν εχέγγυα για μια ορθή κρίση[210]. Επίσης, η αξιολόγηση των κινδύνων διαβίβασης δεδομένων προσωπικού χαρακτήρα από μια ιδιωτική επιχείρηση θα πρέπει να συνιστά μια συνεχή διαδικασία και να μην διενεργείται μόνο όταν η διαβίβαση υπόκειται σε κυβερνητικά μέτρα επιτήρησης, ενώ θα πρέπει να επικαιροποιείται ανά τακτά χρονικά διαστήματα, καθώς ενδέχεται να έχει διαφορετικό αποτελέσματα, εάν οι συνθήκες της κατάστασης αλλάξουν[211].

Όμως, το Δικαστήριο δεν απαιτεί τα πρόσθετα μέτρα να παρέχουν 100% εγγύηση ότι η πρόσβαση σε δεδομένα από τρίτους δεν μπορεί ποτέ να συμβεί, αλλά ότι αποτελούν «*αποτελεσματικούς μηχανισμούς που να διασφαλίζουν, στην πράξη, ότι τηρείται το απαιτούμενο από το δίκαιο της Ένωσης επίπεδο προστασίας*»[212]. Συνεπώς, τα πρόσθετα μέτρα θα πρέπει να αξιολογούνται με βάση το κριτήριο της αναλογικότητας και όχι της τελειότητας[213]. Παρόλα αυτά, ενόψει των υψηλών κυρώσεων για τον υπεύθυνο επεξεργασίας σε περίπτωση εσφαλμένης κρίσης του[214], το πιο πιθανό είναι ο υπεύθυνος επεξεργασίας να απέχει από οποιαδήποτε ενέργεια που ενέχει τον παραμικρό κίνδυνο, εις βάρος της ελεύθερης κυκλοφορίας των πληροφοριών που αποτελεί στόχο του δικαίου προστασίας δεδομένων προσωπικού χαρακτήρα.

Τέλος, αξίζει να σημειώσουμε ότι το έργο που έχει αναθέσει το ΔΕΕ στους εξαγωγείς δεδομένων, ήτοι να επαληθεύσουν, σε σύμπραξη με τους εκάστοτε εισαγωγείς δεδομένων, ότι υπάρχει επαρκές επίπεδο προστασίας στη χώρα προορισμού - έργο που σύμφωνα με το άρθρο 45 του ΓΚΠΔ ανατίθεται στην Επιτροπή - δημιουργεί (εύλογα ή μη) την εντύπωση στο νομικό κόσμο ότι η χρήση των ΤΣΡ καθίσταται πλέον μια μικρογραφία της αξιολόγησης για την έκδοση μιας απόφασης επάρκειας[215].

β) Τι πρέπει να προσέχει ο υπεύθυνος επεξεργασίας σε περίπτωση που συμβάλλεται με έναν εκτελών την επεξεργασία, ο οποίος διαβιβάζει δεδομένα στις ΗΠΑ ή σε άλλη τρίτη χώρα;

---

[210] Κέντρο Διεθνούς και Ευρωπαϊκού Οικονομικού Δικαίου (2018), *Προστασία των δεδομένων προσωπικού χαρακτήρα*. Αθήνα: Σάκκουλας, σελ. 27-33.

[211] Breitbarth, P. (2021), «A Risk-Based Approach to International Data Transfers», ο.π.

[212] ΔΕΕ, C-311/18, *Schrems II*, ο.π., παράγραφος 137.

[213] Kuner, C. (2020), «Schrems II Re-Examined», *Verfassungsblog*. Διαθέσιμο στο: https://verfassungsblog.de/schrems-ii-re-examined/.

[214] Προβλέπεται πρόστιμο μέχρι και είκοσι εκατομμύρια ευρώ ή μέχρι το 4% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους, βλ. Άρθρο 83 του ΓΚΠΔ.

[215] Kuner, C. (2020), «The Schrems II judgment of the Court of Justice and the future of data transfer regulation», ο.π.

Σε περίπτωση που ο υπεύθυνος επεξεργασίας συμβάλλεται με έναν εκτελών την επεξεργασία με σκοπό τη διαβίβαση δεδομένων στις ΗΠΑ ή σε άλλη τρίτη χώρα, θα πρέπει να διασφαλίσει τα εξής:

- Η σύμβαση που έχει συνάψει με τον εκτελών την επεξεργασία σύμφωνα με το άρθρο 28, παράγραφος 3 του ΓΚΠΔ να προβλέπει κατά πόσο επιτρέπονται ή όχι οι διαβιβάσεις δεδομένων σε τρίτες χώρες. Στο πλαίσιο αυτό, θα πρέπει να λαμβάνει υπόψη του ότι ακόμα και η παροχή πρόσβασης σε δεδομένα από τρίτη χώρα, λόγου χάρη για διοικητικούς σκοπούς, ισοδυναμεί με διαβίβαση.
- Να παρέχει άδεια προκειμένου ο εκτελών την επεξεργασία να αναθέτει σε υπεργολάβους επεξεργασίας τη διαβίβαση δεδομένων σε τρίτες χώρες. Στο πλαίσιο αυτό χρειάζεται ιδιαίτερη προσοχή δεδομένου ότι ένα ευρύ φάσμα υπολογιστικών λύσεων ενδέχεται να συνεπάγεται τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτη χώρα (όπως για σκοπούς αποθήκευσης ή συντήρησης).

Παράλληλα, σε περίπτωση που σύμβαση υποδεικνύει ότι τα δεδομένα ενδέχεται να διαβιβάζονται στις ΗΠΑ ή σε άλλη τρίτη χώρα, ο υπεύθυνος επεξεργασίας έχεις τις ακόλουθες εναλλακτικές ώστε να συνεχίσει να χρησιμοποιεί τις υπηρεσίες του οικείου εκτελούντος την επεξεργασία:

- Εάν τα δεδομένα ενδέχεται να διαβιβάζονται στις ΗΠΑ και δεν είναι δυνατή η λήψη πρόσθετων μέτρων προκειμένου να διασφαλιστεί ότι η νομοθεσία των ΗΠΑ δεν θίγει το ουσιωδώς ισοδύναμο επίπεδο προστασίας που παρέχεται εντός της ΕΕ από τους μηχανισμούς διαβίβασης, ούτε ισχύουν παρεκκλίσεις βάσει του άρθρου 49 του ΓΚΠΔ, η μόνη λύση είναι η διαπραγμάτευση μιας τροποποίησης ή μιας συμπληρωματικής ρήτρας στη σύμβαση για την απαγόρευση των διαβιβάσεων στις ΗΠΑ. Επιπλέον, τόσο η αποθήκευση όσο και η διαχείριση των δεδομένων θα πρέπει να λαμβάνει χώρα εκτός των ΗΠΑ.
- Εάν τα δεδομένα ενδέχεται να διαβιβάζονται σε άλλη τρίτη χώρα, ο υπεύθυνος επεξεργασίας θα πρέπει να επαληθεύσει τη νομοθεσία της εν λόγω τρίτης χώρας για να ελέγξει κατά πόσο συμμορφώνεται με τις απαιτήσεις του ΔΕΕ και με το αναμενόμενο επίπεδο προστασίας δεδομένων προσωπικού χαρακτήρα. Εάν δεν υφίσταται καμία κατάλληλη βάση για τις διαβιβάσεις σε τρίτη χώρα, τα δεδομένα προσωπικού χαρακτήρα δεν θα πρέπει να διαβιβάζονται εκτός της επικράτειας της ΕΕ και όλες οι δραστηριότητες επεξεργασίας θα πρέπει να λαμβάνουν χώρα εντός της ΕΕ.

(γ) Ποιος ο ρόλος των εθνικών Αρχών Προστασίας Δεδομένων;

Στην απόφαση *Schrems II* το Δικαστήριο της ΕΕ δεν επικεντρώθηκε μόνο στον προσδιορισμό των υποχρεώσεων που έχουν οι εξαγωγείς και εισαγωγείς δεδομένων, αλλά ανέδειξε τον καίριο ρόλο που διαδραματίζουν οι εθνικές ΑΠΔ κατά την επιβολή του ΓΚΠΔ και την έκδοση αποφάσεων σχετικά με διαβιβάσεις δεδομένων σε τρίτες χώρες. Πιο συγκεκριμένα, έκρινε ότι, ελλείψει απόφασης επάρκειας της Επιτροπής, οι εθνικές ΑΠΔ υποχρεούνται να αναστείλουν ή να απαγορεύσουν τη διαβίβαση δεδομένων προσωπικού χαρακτήρα από την ΕΕ σε τρίτη χώρα, σε περίπτωση που εκτιμούν, λαμβάνοντας υπόψη όλες τις περιστάσεις της διαβίβασης, ότι οι ΤΣΡ δεν τηρούνται ή δεν είναι δυνατόν να τηρηθούν στην επίμαχη τρίτη χώρα, και ότι η απαιτούμενη από το δίκαιο της ΕΕ προστασία των διαβιβαζόμενων δεδομένων δεν μπορεί να διασφαλιστεί με άλλα μέσα, όταν ο εγκατεστημένος στην ΕΕ εξαγωγέας δεδομένων δεν έχει αναστείλει ή τερματίσει ο ίδιος την εν λόγω διαβίβαση[216]. Μάλιστα, όπως υποστηρίζεται στο νομικό κόσμο, οι εν λόγω σημαντικές διαπιστώσεις του ΔΕΕ σχετικά με το ρόλο των εθνικών ΑΠΔ σε σχέση με τις ΤΣΡ, μπορούν να τύχουν εφαρμογής και επί των λοιπών κατάλληλων εγγυήσεων που προβλέπονται στο άρθρο 46 του ΓΚΠΔ[217].

Ειδικότερα, οι εθνικές ΑΠΔ μπορούν να αναστείλουν, περιορίσουν ή απαγορεύσουν μια διαβίβαση δεδομένων, σε περίπτωση που οι ΤΣΡ δεν παρέχουν ένα ουσιαστικά ισοδύναμο πλαίσιο με εκείνο που επιβάλλει το δίκαιο της ΕΕ, και ο εξαγωγέας δεδομένων δεν έχει ενεργήσει καταλλήλως [όπως αναφέραμε στο ερώτημα (α)]. Για παράδειγμα, όταν λόγω του εθνικού δικαίου δεν είναι εφικτό για τον εισαγωγέα δεδομένων να συμμορφωθεί με κάποιες από τις ΤΣΡ που είχαν αρχικώς συμφωνηθεί[218]. Σε περίπτωση δε που προκύπτουν περιστάσεις στο πλαίσιο των ΤΣΡ όπου οι ΑΠΔ των κρατών-μελών της ΕΕ έχουν αποκλίνουσες γνώμες σχετικά με την επάρκεια των εγγυήσεων σε τρίτες χώρες, το ΔΕΕ έκρινε ότι το θέμα θα πρέπει να παραπέμπεται στο ΕΣΠΔ για γνωμοδότηση[219].

Αντίθετα, σε ότι αφορά τις αποφάσεις επάρκειας, η υποχρέωση των εθνικών ΑΠΔ να αναστείλουν, περιορίσουν ή να απαγορεύσουν τις διαβιβάσεις, περιορίζεται. Ωστόσο, ακόμη

[216] ΔΕΕ, C-311/18, *Schrems II*, ο.π., παράγραφος 146.
[217] Βλ. Kuner, C. (2020), «The Schrems II judgment of the Court of Justice and the future of data transfer regulation», ο.π.
[218] Βλ. Zalnieriute M. (2021), «Data Transfers after Schrems II: The EU-US Disagreements Over Data Privacy and National», *Vanderbilt Journal of Transnational Law*. Διαθέσιμο στο: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3826878.
[219] ΔΕΕ, C-311/18, *Schrems II*, ο.π., παράγραφος 147.

και σε αυτή την περίπτωση οι εθνικές ΑΠΔ παίζουν ουσιαστικό ρόλο - όπως άλλωστε καταδεικνύει η στάση της ιρλανδικής ΑΠΔ στην υπόθεση *Schrems II* σε σχέση με την απόφαση για την Ασπίδα Προστασίας της Ιδιωτικής Ζωής - καθώς οι εθνικές ΑΠΔ υποχρεούνται να παραπέμπουν τυχόν αμφιβολίες τους σχετικά με το εάν μια τρίτη χώρα διαθέτει επαρκές πλαίσιο προστασία της ιδιωτικής ζωής στα εθνικά δικαστήρια, τα οποία με τη σειρά τους δύνανται να παραπέμψουν το ζήτημα ενώπιον του Δικαστηρίου της ΕΕ μέσω της υποβολής προδικαστικών ερωτημάτων[220].

Γεννά, όμως, προβληματισμούς το κατά πόσο μια εθνική ΑΠΔ, με τους περιορισμένους πόρους της, ή ένα εθνικό δικαστήριο, το οποίο επικεντρώνεται στο εθνικό και/ή ενωσιακό δίκαιο, δύναται να προβεί σε ουσιαστική σύγκριση μεταξύ του δικαίου τρίτων κρατών και του δικαίου της ΕΕ για την προστασία των δεδομένων προσωπικού χαρακτήρα. Λαμβάνοντας υπόψη δε ότι, σε περίπτωση προδικαστικής παραπομπής, οι αποφάσεις των εθνικών δικαστηρίων θα γίνονται δεκτές από το ΔΕΕ χωρίς περαιτέρω έρευνα, ενδεχομένως η απόφαση επί της συνδρομής ουσιαστικής ισοδυναμίας να ληφθεί βάσει μιας ανεπαρκούς αξιολόγησης του αλλοδαπού δικαίου, όπως π.χ. όταν τα αποδεικτικά στοιχεία που αφορούν στο αλλοδαπό δίκαιο παρέχονται μόνο από ένα διάδικο και δεν αμφισβητούνται. Μάλιστα, στο πεδίο του ιδιωτικού διεθνούς δίκαιου, η χωρίς αντίκρουση παρουσίαση των αποδεικτικών στοιχείων του αλλοδαπού δικαίου μόνο από το ένα μέρος, έχει κριθεί ως *«εσφαλμένη εφαρμογή του αλλοδαπού δικαίου»*[221].

Επομένως, η τύχη των αποφάσεων επάρκειας θα εξαρτηθεί σε μεγάλο βαθμό και από τις εθνικές υποθέσεις που τίθενται ενώπιον του ΔΕΕ μέσω του ενωσιακού μηχανισμού προδικαστικής παραπομπής. Λόγω αυτού, καθίσταται σημαντικό για τις τρίτες χώρες να παρακολουθούν τις διαδικασίες στα εθνικά δικαστήρια των κρατών-μελών της ΕΕ όσον αφορά την εγκυρότητα των αποφάσεων επάρκειας που τις αφορούν, και να προσπαθούν να παρεμβαίνουν στις διαδικασίες αυτές, όταν αυτό είναι δυνατόν, καθώς μόνο κατά αυτόν τον τρόπο θα μπορέσουν να συμμετάσχουν, ως διάδικοι της κύριας δίκης σε εθνικό επίπεδο, στη διαδικασία ενώπιον του ΔΕΕ[222], όπως άλλωστε συνέβη και ενώπιον του Ανώτατου

[220] ΔΕΕ, C-311/18, *Schrems II*, ο.π., παράγραφοι 119 και 120. Επίσης, Bignami, F. (2020), «Schrems II: The Right to Privacy and the New Illiberalism», ο.π.

[221] Βλ. Kuner, C. (2017), «Reality and Illusion in EU Data Transfer Regulation Post Schrems», *German Law Journal*, σελ. 901 και εκεί παραπομπές. Διαθέσιμο στο: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2732346.

[222] Βλ. άρθρο 93 του Κανονισμού Διαδικασίας του Δικαστηρίου της ΕΕ, διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32012Q0929(01)&from=EN, σε συνδυασμό με την

Δικαστηρίου της Ιρλανδίας, όπου επετράπη η παρέμβαση της κυβέρνησης των ΗΠΑ και λοιπών άλλων ενδιαφερόμενων μερών[223]. Σε διαφορετική περίπτωση, η παρέμβαση ενώπιον του ΔΕΕ για την έκδοση προδικαστικής απόφασης δεν θα είναι εφικτή, με αποτέλεσμα να μην υπάρχει η δυνατότητα για τρίτα μέρη (όπως αλλοδαπές κυβερνήσεις ή ακαδημαϊκούς εμπειρογνώμονες) να παράσχουν περαιτέρω διευκρινίσεις σχετικά με τα πρότυπα προστασίας των δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες.

2. Το νέο καθεστώς του Ηνωμένου Βασιλείου για τις διαβιβάσεις δεδομένων

Η διαβίβαση δεδομένων ως καθεστώς συνδέεται για τους περισσότερους με τις διαβιβάσεις που διενεργούνται προς τρίτες χώρες, και δη άλλων ηπείρων. Όμως, το εν λόγω πλαίσιο τυγχάνει εφαρμογής και σε χώρες που βρίσκονται εντός της Ευρώπης. Χαρακτηριστικό παράδειγμα αποτελεί το Ηνωμένο Βασίλειο, το οποίο μετά την έξοδό του από την ΕΕ (γνωστή διεθνώς ως Brexit - συντομογραφία του British exit), απώλεσε την ιδιότητα του κράτους-μέλους της ΕΕ, και απέκτησε αυτόματα καθεστώς τρίτης χώρας, το οποίο εμπίπτει στο πεδίο εφαρμογής του πέμπτου κεφαλαίου του ΓΚΠΔ. Επομένως, ο αντίκτυπος της απόφασης *Schrems II* είναι εξίσου σημαντικός και για το Ηνωμένο Βασίλειο, πολλώ δε μάλλον από τη στιγμή που είναι ευρέως γνωστό ότι εφαρμόζει εκτεταμένες πρακτικές επιτήρησης ως μέλος της συμμαχίας ανταλλαγής πληροφοριών «Five Eyes Alliance»[224][225], για λόγους εθνικής ασφάλειας, οι οποίες δεν έχουν εξεταστεί από το ΔΕΕ, καθώς η εθνική ασφάλεια αποτελεί αποκλειστική ευθύνη κάθε κράτους-μέλους της ΕΕ και δεν εμπίπτει στην αρμοδιότητα της ΕΕ[226][227]. Στην παρούσα υποενότητα θα εξετάσουμε το ισχύον

παρουσίαση των αρμοδιοτήτων του ΔΕΕ στην επίσημη ιστοσελίδα του Δικαστηρίου: https://curia.europa.eu/jcms/jcms/Jo2_7024/el/.

[223] Βλ. Ανώτατο Δικαστήριο της Ιρλανδίας, 2016/4809 P, *Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems - Judgment of Mr. Justice Brian J. McGovern*, 19 Ιουλίου 2016. Διαθέσιμο στο: https://regmedia.co.uk/2016/07/19/facebook_eff_schrems.pdf.

[224] Βλ. Office of The Director of National Intelligence, *«Five Eyes Intelligence Oversight and Review Council (Fiorc)»*. Διαθέσιμο στο: https://www.dni.gov/index.php/ncsc-how-we-work/217-about/organization/icig-pages/2660-icig-fiorc.

[225] Η Five Eyes Alliance αποτελεί μία συμμαχία ανταλλαγής πληροφοριών μεταξύ πέντε αγγλόφωνων δημοκρατιών: των ΗΠΑ, του Ηνωμένου Βασιλείου, του Καναδά, της Αυστραλίας και της Νέας Ζηλανδίας. Τέθηκε σε ισχύ με τη Συμφωνία της UKUSA (Συμφωνία Ηνωμένου Βασιλείου - ΗΠΑ) το 1946 και εξελίχθηκε κατά τη διάρκεια του Ψυχρού Πολέμου ως μηχανισμός παρακολούθησης κινήσεων της Σοβιετικής Ένωσης και ανταλλαγής απόρρητων πληροφοριών. Βλ. σχετικά Cotton, B. (2019), «Five Eyes Alliance: Everything You Need To Know», Business Leader Magazine. Διαθέσιμο στο: https://www.businessleader.co.uk/about/.

[226] Άρθρο 4, παράγραφος 2 της Συνθήκης για τη Λειτουργία της Ευρωπαϊκής Ένωσης, ο.π.

[227] Για σκοπούς επιβολής του νόμου, υπάρχει επίσης η συμφωνία Cloud Act μεταξύ Ηνωμένου Βασιλείου και ΗΠΑ για την πρόσβαση των αστυνομικών αρχών σε αποθηκευμένες επικοινωνίες, καθώς και για υποκλοπές ενσύρματων και ηλεκτρονικών επικοινωνιών σε πραγματικό χρόνο. Η

καθεστώς για τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα, τόσο μεταξύ της ΕΕ και του Ηνωμένου Βασιλείου **(α)**, αλλά και μεταξύ του Ηνωμένου Βασιλείου και τρίτων χωρών **(β)**.

α) Διαβιβάσεις δεδομένων από την ΕΕ στο Ηνωμένο Βασίλειο

Από τη λήξη της μεταβατικής περιόδου που είχε τεθεί για το Ηνωμένο Βασίλειο στο πλαίσιο εξόδου αυτού από την ΕΕ, και πιο συγκεκριμένα από 1η Ιανουαρίου 2021, οι διαβιβάσεις δεδομένων προσωπικού χαρακτήρα από την ΕΕ στο Ηνωμένο Βασίλειο διέπονται από το πέμπτο κεφάλαιο του ΓΚΠΔ, και επομένως τους ίδιους κανόνες και πρότυπα που ισχύουν για τις ΗΠΑ και άλλες τρίτες χώρες. Ως τρίτη πλέον χώρα, το Ηνωμένο Βασίλειο θα πρέπει να διασφαλίζει για τα δεδομένα προσωπικού χαρακτήρα ένα επίπεδο προστασίας ουσιαστικά ισοδύναμο με εκείνο που διασφαλίζεται εντός της ΕΕ.

Στο πλαίσιο αυτό, η Επιτροπή εξέδωσε στις 28 Ιουνίου 2021 δύο αποφάσεις επάρκειας για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα στο Ηνωμένο Βασίλειο, στο πλαίσιο του ΓΚΠΔ[228] και της Οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου (ευρέως γνωστής ως Law Enforcement Directive ή LED, εφεξής «**Οδηγία LED**»)[229]. Οι εν λόγω μονομερείς και αυτόνομες αποφάσεις επάρκειας διασφάλισαν την ορθή εφαρμογή της Συμφωνίας Εμπορίου και Συνεργασίας μεταξύ της Ευρωπαϊκής Ένωσης και της Ευρωπαϊκής Κοινότητας Ατομικής Ενέργειας, αφενός, και του Ηνωμένου Βασιλείου και της Βόρειας Ιρλανδίας αφετέρου (εφεξής **«Συμφωνία Εμπορίου και Συνεργασίας ΕΕ-**

συμφωνία αυτή προβλέπει ειδικά την πρόσβαση των ΗΠΑ στις επικοινωνίες υπηκόων τρίτων χωρών που διαχειρίζονται οι πάροχοι του Ηνωμένου Βασιλείου, για παράδειγμα υπηκόους της ΕΕ, βλ. σχετικά Bignami, F. (2020), «Schrems II: The Right to Privacy and the New Illiberalism», ο.π.

[228] Ευρωπαϊκή Επιτροπή (2021), *Commission Implementing Decision of 28.6.2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom*. Βέλγιο: Ευρωπαϊκή Επιτροπή. Διαθέσιμο στο: https://ec.europa.eu/info/sites/default/files/decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_-_general_data_protection_regulation_en.pdf.

[229] Ευρωπαϊκή Επιτροπή (2021), *Commission Implementing Decision of 28.6.2021 pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom*. Βέλγιο: Ευρωπαϊκή Επιτροπή. Διαθέσιμο στο: https://ec.europa.eu/info/sites/default/files/decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_law_enforcement_directive_en.pdf.

Ηνωμένου Βασιλείου»)[230][231], η οποία συνήφθη λόγω της αποχώρησης του Ηνωμένου Βασιλείου από την ΕΕ[232]. Η εν λόγω Συμφωνία, μεταξύ άλλων, περιλαμβάνει δέσμευση της ΕΕ και του Ηνωμένου Βασιλείου να διατηρήσουν υψηλά επίπεδα προτύπων προστασίας κατά την ανταλλαγή δεδομένων προσωπικού χαρακτήρα, όπως για παράδειγμα στο πλαίσιο συνεργασίας στον τομέα της πρόληψης και της καταπολέμησης της σοβαρής εγκληματικότητας και της τρομοκρατίας[233]. Μάλιστα, η Συμφωνία Εμπορίου και Συνεργασίας ΕΕ-Ηνωμένου Βασιλείου προβλέπει ότι κάθε διαβίβαση δεδομένων που θα πραγματοποιηθεί στο πλαίσιο της εφαρμογής της, θα πρέπει να συμμορφώνεται με τις απαιτήσεις προστασίας δεδομένων του μέρους που διαβιβάζει τα δεδομένα (για την ΕΕ, τις απαιτήσεις του ΓΚΠΔ και της Οδηγίας LED).

Η εκτενής απόφαση επάρκειας της Επιτροπής για τον ΓΚΠΔ του Ηνωμένου Βασιλείου[234] αξιολογεί λεπτομερώς το νομοθετικό πλαίσιο του Ηνωμένου Βασιλείου για την προστασία των δεδομένων προσωπικού χαρακτήρα, και επισημαίνει ότι: «*Καθώς ο ΓΚΠΔ του Ηνωμένου Βασιλείου βασίζεται στη νομοθεσία της Ευρωπαϊκής Ένωσης, οι κανόνες προστασίας δεδομένων στο Ηνωμένο Βασίλειο σε πολλές πτυχές αντικατοπτρίζουν στενά τους αντίστοιχους κανόνες που ισχύουν στην Ευρωπαϊκή Ένωση*»[235]. Η Επιτροπή καταλήγει στο συμπέρασμα ότι «*… ο ΓΚΠΔ του Ηνωμένου Βασιλείου και ο DPA 2018* (Νόμος για την προστασία των δεδομένων στο Ηνωμένο Βασίλειο) *εξασφαλίζουν επίπεδο προστασίας για τα δεδομένα προσωπικού χαρακτήρα που διαβιβάζονται από την Ευρωπαϊκή Ένωση, το οποίο είναι ουσιαστικά ισοδύναμο*

---

[230] Συμφωνία Εμπορίου και Συνεργασίας μεταξύ της Ευρωπαϊκής Ένωσης και της Ευρωπαϊκής Κοινότητας Ατομικής Ενέργειας, αφενός, και του Ηνωμένου Βασιλείου της Μεγάλης Βρετανίας και της Βόρειας Ιρλανδίας, αφετέρου. Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:22021A0430(01)&from=EN.

[231] Δελτίο Τύπου Ευρωπαϊκής Επιτροπής (2021), «*Data protection: European Commission launches process on personal data flows to UK*». Βέλγιο: Ευρωπαϊκή Επιτροπή. Διαθέσιμο στο: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_661.

[232] Οι εν λόγω αποφάσεις επάρκειας εκδόθηκαν λίγο πριν από τη λήξη του προσωρινού καθεστώτος για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα που προέβλεπε η Συμφωνία Εμπορίου και Συνεργασίας ΕΕ-Ηνωμένου Βασιλείου (ήτοι 30 Ιουνίου 2021), βλ. Δελτίο Τύπου Ευρωπαϊκής Επιτροπής (2021), «*Data protection: European Commission launches process on personal data flows to UK*», ο.π.

[233] Βλ. Συμφωνία Εμπορίου και Συνεργασίας ΕΕ - Ηνωμένου, ο.π., ΤΙΤΛΟΣ V - Συνεργασία με την Ευρωπόλ.

[234] Η διατύπωση «UK GDPR» χρησιμοποιείται στον επίσημο ιστότοπο του Γραφείου του Επιτρόπου Πληροφοριών του Ηνωμένου Βασιλείου (ICO), όπου, μεταξύ άλλων, διευκρινίζεται το εξής: «*The GDPR is retained in domestic law as the UK GDPR, but the UK has the independence to keep the framework under review. The 'UK GDPR' sits alongside an amended version of the DPA 2018*». Βλ. Γραφείο του Επιτρόπου Πληροφοριών του Ηνωμένου Βασιλείου (ICO), *The UK GDPR*. Διαθέσιμο στο: https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-and-the-eu-in-detail/the-uk-gdpr/.

[235] Ευρωπαϊκή Επιτροπή (2021), *Commission Implementing Decision of 28.6.2021 pursuant to Regulation (EU) 2016/679*, ο.π., παράγραφος 16.

με αυτό που εγγυάται ο κανονισμός (ΕΕ) 2016/679»[236]. Ως εκ τούτου, τα δεδομένα προσωπικού χαρακτήρα μπορούν να συνεχίσουν να διακινούνται ελεύθερα από την ΕΕ προς το Ηνωμένο Βασίλειο και δεν απαιτούνται ΤΣΡ.

Η Επιτροπή διαπίστωσε ότι το σύστημα προστασίας δεδομένων προσωπικού χαρακτήρα του Ηνωμένου Βασιλείου συνέχισε να τηρεί τους ίδιους κανόνες που ίσχυαν όταν ήταν κράτος-μέλος της ΕΕ, καθώς μετά το Brexit το Ηνωμένο Βασίλειο ενσωμάτωσε πλήρως στο νομικό του σύστημα τις αρχές, τα δικαιώματα και τις υποχρεώσεις του ΓΚΠΔ και της Οδηγίας LED[237]. Επιπλέον, η Επιτροπή διαπίστωσε ότι το σύστημα του Ηνωμένου Βασιλείου παρέχει ισχυρές εγγυήσεις όσον αφορά τον τρόπο με τον οποίο χειρίζεται την πρόσβαση σε δεδομένα προσωπικού χαρακτήρα από δημόσιες αρχές, ιδίως για θέματα εθνικής ασφάλειας[238]. Ειδικότερα, η συλλογή δεδομένων από τις αρχές πληροφοριών υπόκειται σε προηγούμενη έγκριση από ανεξάρτητο δικαστικό όργανο[239]. Κάθε μέτρο πρέπει να είναι αναγκαίο και ανάλογο προς αυτό που επιδιώκει να επιτύχει[240], ενώ κάθε φυσικό πρόσωπο που πιστεύει ότι έχει γίνει αντικείμενο παράνομης παρακολούθησης μπορεί να προσφύγει στο Δικαστήριο Ερευνών («*Investigatory Powers Tribunal*»)[241]. Μάλιστα, καθοριστικό ρόλο στην αξιολόγηση της Επιτροπής έπαιξαν και οι διεθνείς δεσμεύσεις του Ηνωμένου Βασιλείου, καθώς το εν λόγω κράτος παραμένει μέλος της ευρωπαϊκής «οικογένειας ιδιωτικότητας»[242] και συνεχίζει να συμμορφώνεται με την Ευρωπαϊκή Σύμβαση Ανθρωπίνων Δικαιωμάτων και με τη «Σύμβαση 108» του Συμβουλίου της Ευρώπης, τη μόνη δεσμευτική διεθνή συνθήκη στον τομέα της προστασίας των δεδομένων προσωπικού χαρακτήρα[243], ενώ υπόκειται και στη

[236] Ευρωπαϊκή Επιτροπή (2021), *Commission Implementing Decision of 28.6.2021 pursuant to Regulation (EU) 2016/679*, ο.π., παράγραφος 272.
[237] Ευρωπαϊκή Επιτροπή (2021), *Commission Implementing Decision of 28.6.2021 pursuant to Regulation (EU) 2016/679*, ο.π., παράγραφος 13. Επίσης, βλ. σχετικά Chiavetta R. (2021) «European Commission adopts UK adequacy decisions», *The Privacy Advisor - IAPP*, ηλεκτρονικά διαθέσιμο στον ακόλουθο σύνδεσμο: https://iapp.org/news/a/european-commission-adopts-uk-adequacy-decisions/
[238] Ευρωπαϊκή Επιτροπή (2021), *Commission Implementing Decision of 28.6.2021 pursuant to Regulation (EU) 2016/679*, ο.π., παράγραφος 156.
[239] Ευρωπαϊκή Επιτροπή (2021), *Commission Implementing Decision of 28.6.2021 pursuant to Regulation (EU) 2016/679*, ο.π., παράγραφοι 203, 204 και 271.
[240] Ευρωπαϊκή Επιτροπή (2021), *Commission Implementing Decision of 28.6.2021 pursuant to Regulation (EU) 2016/679*, ο.π., παράγραφοι 133, 143, 239 - 242, 248 και 271.
[241] Ευρωπαϊκή Επιτροπή (2021), *Commission Implementing Decision of 28.6.2021 pursuant to Regulation (EU) 2016/679*, ο.π., παράγραφοι 266 - 269.
[242] Δελτίο Τύπου Ευρωπαϊκής Επιτροπής (2021), «*Data protection: European Commission launches process on personal data flows to UK*», ο.π.
[243] Όπως χαρακτηριστικά αναφέρει η Επιτροπή στην απόφασή της: «*In its structure and main components, the UK legal framework applying to data transferred under this Decision is thus very similar to the one applying in the European Union. This includes the fact that such framework does not only rely on obligations laid down in*

δικαιοδοσία του ΕΔΑΔ, γεγονός που έχει ιδιαίτερη σημασία για τη σταθερότητα των ευρημάτων επάρκειας[244].

Σε πρακτικό επίπεδο, οι εν λόγω αποφάσεις επάρκειας της Επιτροπής σημαίνουν ότι οι ιδιωτικές επιχειρήσεις του Ηνωμένου Βασιλείου μπορούν να συνεχίσουν να λαμβάνουν δεδομένα προσωπικού χαρακτήρα από την ΕΕ χωρίς να χρειάζεται να θέσουν πρόσθετες ρυθμίσεις με τους ευρωπαίους ομολόγους τους. Όπως χαρακτηριστικά επεσήμανε σε ανακοίνωσή του το Υπουργείο Ψηφιακής Πολιτικής, Πολιτισμού, Μέσων Μαζικής Ενημέρωσης και Αθλητισμού του Ηνωμένου Βασιλείου « *… αυτή η ελεύθερη ροή προσωπικών δεδομένων υποστηρίζει το εμπόριο, την καινοτομία και τις επενδύσεις, βοηθά τις υπηρεσίες επιβολής του νόμου στην αντιμετώπιση του εγκλήματος και υποστηρίζει την παροχή κρίσιμων δημόσιων υπηρεσιών που μοιράζονται προσωπικά δεδομένα, καθώς και τη διευκόλυνση της υγείας και της επιστημονικής έρευνας*[245]».

Αξίζει να σημειωθεί ότι για πρώτη φορά μια απόφαση επάρκειας έχει ορισμένη χρονική διάρκεια εφαρμογής. Ειδικότερα, η Επιτροπή συμπεριέλαβε και στις δυο αποφάσεις επάρκειας μια ρήτρα λήξης ισχύος («*sunset clause*») για την επάρκεια του Ηνωμένου Βασιλείου. Πιο συγκεκριμένα, έκαστη απόφαση θα διαρκέσει για τέσσερα χρόνια μετά την έναρξη ισχύος της, δηλαδή μέχρι το 2025. Κατά τη διάρκεια των τεσσάρων αυτών ετών, η Επιτροπή θα παρακολουθεί τις νομικές εξελίξεις στο Ηνωμένο Βασίλειο και θα δύναται να παρέμβει ανά πάσα στιγμή, σε περίπτωση που το Ηνωμένο Βασίλειο αποκλίνει από το ισχύον επίπεδο προστασίας των δεδομένων. Μετά το πέρας αυτής της περιόδου, τα πορίσματα περί επάρκειας μπορούν να επανεξεταστούν και να επικαιροποιηθούν, εφόσον το Ηνωμένο Βασίλειο εξακολουθεί να διασφαλίζει ένα ουσιαστικά ισοδύναμο επίπεδο προστασίας των δεδομένων με εκείνο της ΕΕ[246].

---

domestic law, that have been shaped by EU law, but also on obligations enshrined in international law, in particular through the United Kingdom's adherence to the ECHR and Convention 108, as well as its submission to the jurisdiction of the European Court of Human Rights». Βλ. Ευρωπαϊκή Επιτροπή (2021), *Commission Implementing Decision of 28.6.2021 pursuant to Regulation (EU) 2016/679*, ο.π., παράγραφος 19.

[244] Δελτίο Τύπου Ευρωπαϊκής Επιτροπής (2021), *Data protection: European Commission launches process on personal data flows to UK*, ο.π.

[245] Department for Digital, Culture, Media & Sport (2021), «*EU adopts 'adequacy' decisions allowing data to continue flowing freely to the UK*». Διαθέσιμο στο: https://www.gov.uk/government/news/eu-adopts-adequacy-decisions-allowing-data-to-continue-flowing-freely-to-the-uk.

[246] Βλ. σχετικά O'Donoghue, C. and O'Brien, S. (202) «UK adequacy decision for European data transfers», *Technology Law Dispatch*, Reed Smith LLP. Διαθέσιμο στο: https://www.technologylawdispatch.com/2021/07/privacy-data-protection/uk-adequacy-decision-for-

Τέλος, σε ότι αφορά τις ροές δεδομένων προς την αντίθετη κατεύθυνση, ήτοι από το Ηνωμένο Βασίλειο προς την ΕΕ, αυτές ρυθμίζονται από τη νομοθεσία του Ηνωμένου Βασιλείου, η οποία εφαρμόζεται από την 1η Ιανουαρίου 2021. Στο πλαίσιο αυτό, και μέσω του εθνικού μηχανισμού κανονισμών επάρκειας («*adequacy regulations*») - κλώνο θα λέγαμε του μηχανισμού αποφάσεων επάρκειας του ενωσιακού ΓΚΠΔ - το Ηνωμένο Βασίλειο έκρινε ότι η ΕΕ διασφαλίζει επαρκές επίπεδο προστασίας και ότι, ως εκ τούτου, τα δεδομένα μπορούν να διαβιβάζονται ελεύθερα από το Ηνωμένο Βασίλειο προς την ΕΕ[247].

β) Διαβιβάσεις δεδομένων από το Ηνωμένο Βασίλειο σε τρίτη χώρα

Από τη λήξη της προαναφερθείσας μεταβατικής περιόδου για το Ηνωμένο Βασίλειο, ήτοι από 31 Δεκεμβρίου 2020, το δίκαιο της ΕΕ (συμπεριλαμβανομένων των αποφάσεων της Επιτροπής) δεν ισχύει σε ότι αφορά τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα από το Ηνωμένο Βασίλειο σε τρίτη χώρα. Ως εκ τούτου, οι νέες ΤΣΡ δεν μπορούν να τύχουν εφαρμογής για τις εν λόγω διαβιβάσεις δεδομένων. Σύμφωνα, όμως, με το ΓΚΠΔ του Ηνωμένου Βασιλείου, οι προηγούμενες (ενωσιακές) ΤΣΡ εξακολουθούν να ισχύουν έως ότου το Γραφείο του Επιτρόπου Πληροφοριών του Ηνωμένου Βασιλείου (ICO) δημοσιεύσει τις δικές του ΤΣΡ[248].

Στις 2 Φεβρουαρίου 2022, ο Υπουργός Εξωτερικών του Ηνωμένου Βασιλείου κατέθεσε στο Κοινοβούλιο του Ηνωμένου Βασιλείου τη σύμβαση διεθνούς διαβίβασης δεδομένων (International Data Transfer Agreement, εφεξής «**IDTA**»)[249], και το Παράρτημα διεθνούς διαβίβασης δεδομένων για τις ΤΣΡ της Ευρωπαϊκής Επιτροπής (International Data Transfer

european-data-transfers/, και Chiavetta R. (2021) «European Commission adopts UK adequacy decisions», ο.π.

[247] Βλ. κεφάλαιο «International transfers after the UK exit from the EU Implementation Period» από Information Commissioner's Office (2021), *Guide to the General Data Protection Regulation (GDPR)*. Ηνωμένο Βασίλειο: Information Commissioner's Office. Διαθέσιμο στο: https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdfv, και Δελτίο Τύπου Ευρωπαϊκής Επιτροπής (2021), Data protection: European Commission launches process on personal data flows to UK, ο.π.

[248] Βλ. Ilan, D., Kristensen, G., Ka Chun, L., Gerlach, N. και Mammì Borruto, F. (2021), «New Standard Contractual Clauses for Data Transfers under the GDPR – New Changes, New Questions?», ο.π.

[249] Η IDTA μπορεί να χρησιμοποιηθεί για να επιτραπεί η διαβίβαση δεδομένων προσωπικού χαρακτήρα από το Ηνωμένο Βασίλειο σε οποιαδήποτε τρίτη χώρα που δεν διαθέτει επαρκή προστασία δεδομένων. Είναι ουσιαστικά παρόμοιο εργαλείο διαβίβασης με τις νέες ΤΣΡ της Επιτροπής. Διαθέσιμο στο: https://ico.org.uk/media/for-organisations/documents/4019538/international-data-transfer-agreement.pdf.

Addendum to the EU Commission Standard Contractual Clauses, εφεξής «**Παράρτημα**»)[250], τα οποία λαμβάνουν υπόψη τη δεσμευτική απόφαση του ΔΕΕ στην υπόθεση *Schrems II*. Εάν δεν διατυπωθούν αντιρρήσεις από το Κοινοβούλιο του Ηνωμένου Βασιλείου, τα εν λόγω έγγραφα θα τεθούν σε ισχύ την 21η Μαρτίου 2022, οπότε και οι εξαγωγείς δεδομένων θα μπορούν να χρησιμοποιούν το IDTA ή το Παράρτημα ως εργαλείο διαβίβασης για να συμμορφώνονται με το ΓΚΠΔ του Ηνωμένου Βασιλείου.

Μάλιστα, σύμφωνα με το Γραφείο του Επιτρόπου Πληροφοριών του Ηνωμένου Βασιλείου, οι εξαγωγείς δεδομένων θα μπορούν να συνεχίσουν να συνάπτουν νέες συμβάσεις με βάση τις προηγούμενες ΤΣΡ της ΕΕ έως και την 21η Σεπτεμβρίου 2022. Όλες δε οι συμβάσεις με βάση τις προηγούμενες ΤΣΡ της ΕΕ θα εξακολουθήσουν να παρέχουν κατάλληλες εγγυήσεις για τους σκοπούς του ΓΚΠΔ του Ηνωμένου Βασιλείου, έως την 21η Μαρτίου 2024. Από την ημερομηνία αυτή και μετά, εάν η διαβίβαση συνεχίζεται, θα πρέπει ο εξαγωγέας δεδομένων να συνάψει σύμβαση είτε με τη χρήση της IDTA ή του Παραρτήματος ώστε να διενεργηθεί η διαβίβαση σύμφωνα με το ΓΚΠΔ του Ηνωμένου Βασιλείου[251]. Και στις δυο περιπτώσεις, ο εξαγωγέας δεδομένων εξακολουθεί να φέρει την υποχρέωση διενέργειας αξιολόγησης κινδύνου, ώστε να βεβαιωθεί ότι η προστασία που παρέχεται από την IDTA ή το Παράρτημα, επί τη βάσει των πραγματικών περιστάσεων της διαβίβασης, είναι σύμφωνη με τις αρχές που διέπουν τη νομοθεσία περί προστασίας δεδομένων του Ηνωμένου Βασιλείου.

3. Η απόφαση επάρκειας για τη Δημοκρατία της Κορέας

Στις 17 Δεκεμβρίου 2021, η Επιτροπή ανακοίνωσε σε κοινή δήλωση με την Επιτροπή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα της Δημοκρατίας της Κορέας (Personal Information Protection Commission - PIPC)[252] την υιοθέτηση απόφασης σχετικά με την

[250] Το Παράρτημα μπορεί να χρησιμοποιηθεί για την προσαρμογή των νέων ΤΣΡ της Επιτροπής, επιτρέποντας τη χρήση τους για τις διαβιβάσεις δεδομένων από το Ηνωμένο Βασίλειο σε οποιαδήποτε τρίτη χώρα. Ουσιαστικά έχουν διενεργηθεί οι απαιτούμενες αλλαγές για να διασφαλιστεί ότι οι νέες ΤΣΡ της Επιτροπής πληρούν τις απαιτήσεις του Ηνωμένου Βασιλείου. Αυτό θα επιτρέψει στις επιχειρήσεις που υπόκεινται τόσο στο καθεστώς προστασίας δεδομένων της ΕΕ όσο και στο αντίστοιχο καθεστώς του Ηνωμένου Βασιλείου, να χρησιμοποιούν μία ενιαία ρύθμιση για τη διαβίβαση δεδομένων ώστε να συμμορφώνονται ταυτόχρονα και με τις δύο ομάδες απαιτήσεων. Διαθέσιμο στο: https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf.

[251] Βλ. κεφάλαιο «International transfers after the UK exit from the EU Implementation Period» από Information Commissioner's Office (2021), *Guide to the General Data Protection Regulation (GDPR)*, ο.π.

[252] Δελτίο Τύπου Ευρωπαϊκής Επιτροπής (2021), *Joint Press Statement by Didier Reynders, Commissioner for Justice of the European Commission, and Yoon Jong In, Chairperson of the Personal Information Protection*

επάρκεια της προστασίας που παρέχεται από τη Δημοκρατία της Κορέας (ευρέως γνωστή ως Νότια Κορέα) στο πλαίσιο του εθνικού Νόμου περί προστασίας προσωπικών πληροφοριών (Personal Information Protection Act - PIPA)[253][254]. Κατά τα λεγόμενα της Επιτροπής, η εν λόγω απόφαση «*βασίζεται στην ισχυρή προστασία των Ευρωπαίων βάσει της κορεατικής νομοθεσίας κατά τη διαβίβαση των δεδομένων τους*»[255].

Πρόκειται για τη δεύτερη χρονικά απόφαση επάρκειας που εκδόθηκε από την Επιτροπή στον απόηχο της απόφασης *Schrems II*, ύστερα από την απόφαση επάρκειας για το Ηνωμένο Βασίλειο. Δεδομένου, όμως, ότι το νομοθετικό πλαίσιο του Ηνωμένου Βασιλείου για την προστασία των δεδομένων προσωπικού χαρακτήρα είχε ήδη παρεμφερές περιεχόμενο με το ΓΚΠΔ - και άρα το Ηνωμένο Βασίλειο απλά μεταπήδησε από την απόλυτη και ευθεία εφαρμογή του ΓΚΠΔ, στη συμμόρφωσή του με μια απόφαση επάρκειας - η απόφαση της Επιτροπής για τη Δημοκρατία της Κορέας θα μπορούσε να θεωρηθεί ως η πρώτη ουσιαστικά απόφαση επάρκειας, αφού εν προκειμένω η Επιτροπή προέβη σε μια εκ του μηδενός αξιολόγηση του εθνικού νομοθετικού πλαισίου για την προστασία των δεδομένων προσωπικού χαρακτήρα, επί τη βάσει του αναθεωρημένου μηχανισμού αξιολόγησης που ακολουθεί τις επιταγές της απόφασης *Schrems II*. Μάλιστα, λόγω αυτού, ενισχύεται η εντύπωση ότι «*η Λατινική Αμερική και η περιοχή Ασίας-Ειρηνικού αποτελούν σήμερα τα πραγματικά εργαστήρια για τους νέους κανόνες, τις πρωτοβουλίες και τις λύσεις για την προστασία των δεδομένων. Αυτό δημιουργεί νέες ευκαιρίες για τη διευκόλυνση της ροής*

Commission of the Republic of Korea. Βέλγιο: Ευρωπαϊκή Επιτροπή. Διαθέσιμο στο: https://ec.europa.eu/commission/presscorner/detail/en/statement_21_6915

[253] Ευρωπαϊκή Επιτροπή (2021), *Commission Implementing Decision of 17.12.2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the Republic of Korea under the Personal Information Protection Act*, Βέλγιο: Ευρωπαϊκή Επιτροπή. Διαθέσιμο στο: https://ec.europa.eu/info/files/decision-adequate-protection-personal-data-republic-korea-annexes_en.

[254] Σημαντικό βήμα στις διαπραγματεύσεις για την επάρκεια αποτέλεσε η μεταρρύθμιση του νόμου PIPA, ο οποίος τέθηκε σε ισχύ τον Αύγουστο του 2020 και ενίσχυσε τις εξουσίες έρευνας και επιβολής της Επιτροπής PIPC, της ανεξάρτητης αρχής προστασίας δεδομένων της Δημοκρατίας της Κορέας. Επίσης, στο πλαίσιο των διαπραγματεύσεων για την επάρκεια, οι δύο πλευρές συμφώνησαν σε διάφορες πρόσθετες εγγυήσεις που θα βελτιώσουν την προστασία των δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία στη Δημοκρατία της Κορέας, όπως η διαφάνεια. Βλ. σχετικά Ευρωπαϊκή Επιτροπή (2021), *Commission Implementing Decision of 17.12.2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the Republic of Korea under the Personal Information Protection Act*, ο.π., παράγραφοι 128 και 171.

[255] Δελτίο Τύπου Ευρωπαϊκής Επιτροπής (2021), *Joint Press Statement by Didier Reynders, Commissioner for Justice of the European Commission, and Yoon Jong In, Chairperson of the Personal Information Protection Commission of the Republic of Korea*, ο.π.

δεδομένων με τις περιοχές αυτές, αλλά και μεταξύ των περιοχών αυτών και του υπόλοιπου κόσμου»[256].

Η προαναφερθείσα απόφαση της Επιτροπής αναγνωρίζει ότι η Δημοκρατία της Κορέας διαθέτει ένα ουσιαστικά ισοδύναμο επίπεδο προστασίας των δεδομένων προσωπικού χαρακτήρα, και οι διαβιβάσεις δεδομένων προς αυτή μπορούν να πραγματοποιούνται σαν να επρόκειτο για διαβιβάσεις προς άλλο κράτος-μέλος της ΕΕ, χωρίς να απαιτούνται πρόσθετα μέτρα ή προϋποθέσεις διαβίβασης (όπως οι ΤΣΡ) ή εγκρίσεις από τις ΑΠΔ στην ΕΕ. Συμπληρώνει δε τη Συμφωνία Ελεύθερων Συναλλαγών (ΣΕΣ) μεταξύ της ΕΕ και της Δημοκρατίας της Κορέας, η οποία τέθηκε σε ισχύ τον Ιούλιο του 2011[257], και οδήγησε σε σημαντική αύξηση του διμερούς εμπορίου αγαθών και υπηρεσιών και, αναπόφευκτα, στην ανταλλαγή δεδομένων προσωπικού χαρακτήρα.

Ειδικότερα, η εν λόγω απόφαση επάρκειας καλύπτει τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα από την ΕΕ στη Δημοκρατία της Κορέας, με εξαίρεση τις διαβιβάσεις σε παραλήπτες που εμπίπτουν σε μία από τις ακόλουθες κατηγορίες[258]: α) σε θρησκευτικές οργανώσεις στο βαθμό που επεξεργάζονται δεδομένα προσωπικού χαρακτήρα για τις ιεραποστολικές τους δραστηριότητες, β) σε πολιτικά κόμματα στο βαθμό που επεξεργάζονται δεδομένα προσωπικού χαρακτήρα στο πλαίσιο της ανάδειξης υποψηφίων, ή γ) σε υπεύθυνους επεξεργασίας που υπόκεινται στην εποπτεία της Επιτροπής Χρηματοοικονομικών Υπηρεσιών (Financial Services Commission) για την επεξεργασία προσωπικών πιστωτικών πληροφοριών σύμφωνα με το Νόμο περί πληροφοριών

[256] Δήλωση του Bruno Gencarelli, επικεφαλή του Τμήματος «Διεθνείς Ροές Δεδομένων και Προστασία Δεδομένων» της Επιτροπής, στο πλαίσιο του 43ου Συνέδριου της Παγκόσμιας Συνέλευσης Προστασίας Προσωπικών Δεδομένων, που διοργανώθηκε εξ αποστάσεως από την ΑΠΔ του Μεξικού (Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales - INAI) στις 18 και 19 Οκτωβρίου 2021. Βλ. Zanfir-Fortuna, G. (2021), «Dispatch from the Global Privacy Assembly: The brave new world of International Data Transfers», *Future of Privacy Forum*, Διαθέσιμο στο: https://fpf.org/blog/dispatch-from-the-global-privacy-assembly-the-brave-new-world-of-international-data-transfers/. Περισσότερες πληροφορίες σχετικά με το εν λόγω συνέδριο είναι διαθέσιμες στον επίσημο ιστότοπο του Ευρωπαίου Επόπτη για την Προστασία των Δεδομένων: https://edps.europa.eu/data-protection/our-work/publications/international-conferences/global-privacy-assembly-2021-mexico_en.

[257] Συμφωνία ελεύθερων συναλλαγών μεταξύ της Ευρωπαϊκής Ένωσης και των κρατών μελών της, αφενός, και της Δημοκρατίας της Κορέας, αφετέρου. Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=OJ:L:2011:127:FULL&from=EN.

[258] Ευρωπαϊκή Επιτροπή (2021), *Commission Implementing Decision of 17.12.2021 pursuant to Regulation (EU) 2016/679*, ο. π., παράγραφοι 30, 32 και Ενότητα 8 (*Final considerations*), άρθρο 1. Επίσης, βλ. Tielemans, J. (2021) «EU adequacy decision for South Korea», *International Association of Privacy Professionals - The Privacy Advisor*, Διαθέσιμο στο: https://iapp.org/news/a/eu-adequacy-decision-for-south-korea/.

καταναλωτικής πίστης (Credit Information Act), στο βαθμό που επεξεργάζονται τέτοιες πληροφορίες. Στις τρεις αυτές περιπτώσεις θα ισχύει το γενικό καθεστώς που προβλέπεται στο ΓΚΠΔ για τη διαβίβαση δεδομένων σε τρίτες χώρες που δεν διαθέτουν επαρκές επίπεδο προστασίας των δεδομένων.

Στο πλαίσιο αξιολόγησης του κατά πόσο οι όροι υπό τους οποίους οι δημόσιες αρχές της Δημοκρατίας της Κορέας έχουν πρόσβαση σε δεδομένα που διαβιβάζονται από την ΕΕ, τόσο για την επιβολή του νόμου όσο και για σκοπούς εθνικής ασφάλειας, πληρούν το κριτήριο της «ουσιώδους ισοδυναμίας» σύμφωνα με το άρθρο 45, παράγραφος 1 του ΓΚΠΔ, όπως ερμηνεύεται από το ΔΕΕ στις αποφάσεις *Schrems* υπό το πρίσμα του Χάρτη, η Επιτροπή έλαβε υπόψη της ιδίως τα ακόλουθα κριτήρια:

1) Κάθε περιορισμός του δικαιώματος προστασίας των δεδομένων προσωπικού χαρακτήρα πρέπει να προβλέπεται από το νόμο, και η νομική βάση που επιτρέπει την παρέμβαση στο δικαίωμα αυτό να καθορίζει η ίδια το πεδίο εφαρμογής του περιορισμού της άσκησης αυτού.
2) Η νομοθεσία της τρίτης χώρας πρέπει να προβλέπει σαφείς και ακριβείς κανόνες που διέπουν το πεδίο εφαρμογής και την εφαρμογή των υπό κρίση μέτρων και να επιβάλλει ελάχιστες εγγυήσεις ώστε τα πρόσωπα, των οποίων τα δεδομένα διαβιβάστηκαν, να έχουν επαρκείς εγγυήσεις για την αποτελεσματική προστασία των δεδομένων που τους αφορούν από τον κίνδυνο κατάχρησης. Η νομοθεσία πρέπει, ιδίως, να αναφέρει σε ποιες περιπτώσεις, και υπό ποιες προϋποθέσεις, μπορεί να ληφθεί μέτρο που προβλέπει την επεξεργασία των δεδομένων αυτών, καθώς και να θέτει την εκπλήρωση των απαιτήσεων αυτών σε ανεξάρτητη εποπτεία.
3) Η υπό κρίση νομοθεσία και οι απαιτήσεις αυτής πρέπει να είναι νομικά δεσμευτικές για τις δημόσιες αρχές της τρίτης χώρας, αλλά και εκτελεστές ενώπιον των εθνικών δικαστηρίων. Ειδικότερα, τα υποκείμενα των δεδομένων πρέπει να έχουν τη δυνατότητα να προσφύγουν ενώπιον ενός ανεξάρτητου και αμερόληπτου δικαστηρίου προκειμένου να έχουν πρόσβαση στα δεδομένα προσωπικού χαρακτήρα που τους αφορούν ή να επιτύχουν τη διόρθωση ή διαγραφή αυτών.

Εν προκειμένω, η Επιτροπή έκρινε ότι το νομοθετικό πλαίσιο πρόσβασης των δημοσίων αρχών της Δημοκρατίας της Κορέας σε δεδομένα προσωπικού χαρακτήρα που διαβιβάζονται από την ΕΕ, τόσο στο πλαίσιο επιβολής του ποινικού νόμου όσο και για σκοπούς εθνικής ασφάλειας, καλύπτει τα παραπάνω κριτήρια καθώς:

1) Το υφιστάμενο νομοθετικό πλαίσιο της Δημοκρατίας της Κορέας [και συγκεκριμένα, α) ο Νόμος Ποινικής Δικονομίας (Criminal Procedure Act - CPA) για έρευνες και κατασχέσεις, β) ο Νόμος περί προστασίας του απορρήτου των επικοινωνιών (Communication Privacy Protection Act - CPPA) για την πρόσβαση στις επικοινωνίες, γ) ο Νόμος για τις τηλεπικοινωνίες (Telecommunications Business Act - TBA) που αφορά σε αιτήματα για οικειοθελή κοινοποίηση δεδομένων συνδρομητών, σε συνδυασμό με τις διατάξεις του Συντάγματος της Δημοκρατίας της Κορέας, δ) ο Νόμος περί προστασίας προσωπικών πληροφοριών (Personal Information Protection Act - PIPA), ε) η Ενημέρωση 2021-5 (Notification 2021-5) που υιοθετήθηκε από την Επιτροπή Προστασίας Προσωπικών Πληροφοριών (Personal Information Protection Commission - PIPC), και ζ) ο Νόμος κατά της τρομοκρατίας (Anti-Terrorism Act)] παρέχει την αναγκαία νομική βάση για την παρέμβαση στο δικαίωμα προστασίας των δεδομένων προσωπικού χαρακτήρα, καθορίζοντας παράλληλα την έκταση του περιορισμού άσκησης του εν λόγω δικαιώματος[259].
2) Οποιαδήποτε παρέμβαση για λόγους δημοσίου συμφέροντος, ιδίως για σκοπούς επιβολής του ποινικού δικαίου και για λόγους εθνικής ασφάλειας, από τις δημόσιες αρχές στα θεμελιώδη δικαιώματα των προσώπων, των οποίων τα δεδομένα διαβιβάζονται από την ΕΕ στη Δημοκρατία της Κορέας, περιορίζεται στο απολύτως αναγκαίο για την επίτευξη του νόμιμου σκοπού, ενώ υπάρχει αποτελεσματική νομική προστασία κατά της παρέμβασης αυτής. Και τούτο διότι το νομοθετικό πλαίσιο της Δημοκρατίας της Κορέας θεσπίζει σαφείς και ακριβείς κανόνες σχετικά με το πεδίο εφαρμογής και την εφαρμογή αυτών των παρεμβάσεων, εκ των προτέρων («*ex ante*») όσο και εκ των υστέρων («*ex post*»), διασφαλίζοντας έτσι ότι η παρέμβαση στα δικαιώματα των προσώπων θα είναι περιορισμένη σε ότι είναι απαραίτητο και ανάλογο προς τον επιδιωκόμενο σκοπό, ώστε τα πρόσωπα, των οποίων τα δεδομένα διαβιβάστηκαν, να έχουν επαρκείς εγγυήσεις για την αποτελεσματική προστασία των δεδομένων που τους αφορούν από τον κίνδυνο κατάχρησης[260].

[259] Ευρωπαϊκή Επιτροπή (2021), *Commission Implementing Decision of 17.12.2021 pursuant to Regulation (EU) 2016/679*, ο. π., παράγραφοι 153, 162, 163, 166, 189.
[260] Ευρωπαϊκή Επιτροπή (2021), *Commission Implementing Decision of 17.12.2021 pursuant to Regulation (EU) 2016/679*, ο. π., παράγραφοι 153, 162, 163, 166.

3) Οι μηχανισμοί εποπτείας[261] και τα μέσα προσφυγής που προβλέπονται στο δίκαιο της Δημοκρατίας της Κορέας επιτρέπουν τον εντοπισμό των παραβιάσεων των κανόνων προστασίας δεδομένων από υπεύθυνους επεξεργασίας, την αντιμετώπιση αυτών στην πράξη, ενώ προσφέρουν ένδικα μέσα στο υποκείμενο των δεδομένων ενώπιον ανεξάρτητων και αμερόληπτων διοικητικών και δικαστικών αρχών για την απόκτηση πρόσβασης στα δεδομένα προσωπικού χαρακτήρα που το αφορούν και, τελικά, την διόρθωση ή διαγραφή αυτών[262].

Η απόφαση επάρκειας για τη Δημοκρατία της Κορέας καταδεικνύει την επίδραση της απόφασης *Schrems II* στον τρόπο αξιολόγησης της επάρκειας του νομικού συστήματος μιας τρίτης χώρας. Η σε βάθος εξέταση του εκάστοτε νομικού πλαισίου, με το ενδιαφέρον να επικεντρώνεται κατά κύριο λόγο στη νομιμότητα της επιβολής περιορισμών, τα μέτρα ασφαλείας που λαμβάνονται, την προηγούμενη ενημέρωση του υποκειμένου των δεδομένων και τα ένδικα μέσα που έχει στη διάθεσή του, ως στόχο έχουν να αναδείξουν το ποσοστό ισοδυναμίας του νομικού πλαισίου της τρίτης χώρας με το αντίστοιχο της ΕΕ. Ενδεχομένως η νέα απόφαση επάρκειας για τις ΗΠΑ να ακολουθήσει την ίδια κατεύθυνση, επί τη βάσει των εθνικών νομοθετικών ρυθμίσεων που ανέδειξε η Λευκή Βίβλος του Υπουργείου Εμπορίου των ΗΠΑ [βλ. Ενότητα ΙΙΙ (Α)(3)]. Είναι σαφές ότι η Επιτροπή έχει επικαιροποιήσει τη μέθοδό της, και εκείνο που μένει να δούμε είναι πως θα την εφαρμόσει στην περίπτωση των ΗΠΑ.

4. Οι πρώτες αποφάσεις των Αρχών Προστασίας Δεδομένων

Πέρα από τις παραπάνω αποφάσεις επάρκειας της Επιτροπής, ο αντίκτυπος της απόφασης *Schrems II* δεν άργησε να αποτυπωθεί και στις αποφάσεις των ΑΠΔ. Το δρόμο άνοιξε ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων (εφεξής «**ΕΕΠΔ**») με απόφασή του επί της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από το Ευρωπαϊκό Κοινοβούλιο **(α)**. Λίγες ημέρες αργότερα, η ΑΠΔ της Αυστρίας δημοσίευσε μια δικαστική απόφαση ορόσημο κατά της χρήσης της υπηρεσίας Google Analytics **(β)**.

α) Το Ευρωπαϊκό Κοινοβούλιο στην κρίση του Ευρωπαίου Επόπτη Προστασίας Δεδομένων

[261] Ευρωπαϊκή Επιτροπή (2021), *Commission Implementing Decision of 17.12.2021 pursuant to Regulation (EU) 2016/679*, ο. π., παράγραφοι 169 - 174 και 197 - 202.
[262] Ευρωπαϊκή Επιτροπή (2021), *Commission Implementing Decision of 17.12.2021 pursuant to Regulation (EU) 2016/679*, ο. π., παράγραφοι 175 - 184 και 203 - 208.

Στις 5 Ιανουαρίου 2021, η μη κερδοσκοπική οργάνωση «None Of Your Business»[263] (εφεξής «**NOYB**») κατέθεσε καταγγελία κατά του Ευρωπαϊκού Κοινοβουλίου εξ ονόματος έξι μελών αυτού σχετικά με έναν εσωτερικό ιστότοπο ελέγχου για τον κορονοϊό. Τα ζητήματα που τέθηκαν αφορούσαν τα εξής: α) παραπλανητικές προειδοποιήσεις για τους ιχνηλάτες («*cookie banners*»), β) ασαφείς ενημερώσεις προστασίας δεδομένων και γ) παράνομη διαβίβαση δεδομένων στις ΗΠΑ μέσω των ιχνηλατών («*cookies*») της υπηρεσίας Google Analytics και του παρόχου πληρωμών Stripe. Ο ΕΕΠΔ διερεύνησε τα προαναφερθέντα και απηύθυνε επίπληξη στο Ευρωπαϊκό Κοινοβούλιο βάσει του άρθρου 58, παράγραφος 2, στοιχείο β' του ΓΚΠΔ για παραβίαση του Κανονισμού 2018/1725 που ισχύει για τα θεσμικά όργανα της ΕΕ[264][265].

Ο ΕΕΠΔ διαπίστωσε ότι ο ιστότοπος του Ευρωπαϊκού Κοινοβουλίου χρησιμοποιούσε ιχνηλάτες, μέσω των οποίων διαβιβάζονταν δεδομένα προσωπικού χαρακτήρα στις ΗΠΑ, όπου έχουν την έδρα τους τόσο η Stripe όσο και η Google. Παράλληλα, διαπίστωσε ότι το Ευρωπαϊκό Κοινοβούλιο δεν είχε παράσχει τεκμηρίωση[266], αποδεικτικά στοιχεία ή άλλες πληροφορίες σχετικά με τα συμβατικά, τεχνικά ή οργανωτικά μέτρα που εφαρμόζει για να εξασφαλίσει ένα ουσιαστικά ισοδύναμο επίπεδο προστασίας των δεδομένων προσωπικού χαρακτήρα που διαβιβάζονται στις ΗΠΑ στο πλαίσιο χρήσης των προαναφερθέντων ιχνηλατών στον εν λόγω ιστότοπο.

Ως εκ τούτου, ο ΕΕΠΔ έκρινε ότι το Ευρωπαϊκό Κοινοβούλιο δεν είχε εκπληρώσει τις απαιτήσεις των ενωσιακών κανόνων προστασίας δεδομένων (στην προκειμένη περίπτωση του Κανονισμού 2018/1725) και δεν είχε διασφαλίσει επαρκές επίπεδο προστασίας των

[263] Πρόκειται για τη μη κερδοσκοπική οργάνωση ψηφιακών δικαιωμάτων, την οποία ίδρυσε ο Max Schrems, που εδρεύει στη Βιέννη, με στόχο την παραπομπή στο Δικαστήριο της ΕΕ νομικών υποθέσεων σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα.

[264] Ευρωπαίος Επόπτης Προστασίας Δεδομένων, Case 2020-1013, *Decision of the European Data Protection Supervisor in complaint case 2020-1013 submitted by Members of the Parliament against the European Parliament*, 5 Ιανουαρίου 2022. Διαθέσιμο στο: https://noyb.eu/sites/default/files/2022-01/Case%202020-1013%20-%20EDPS%20Decision_bk.pdf.

[265] Κανονισμός (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Οκτωβρίου 2018, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης και την ελεύθερη κυκλοφορία των δεδομένων αυτών, και για την κατάργηση του κανονισμού (ΕΚ) αριθ. 45/2001 και της απόφασης αριθ. 1247/2002/ΕΚ. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32018R1725&from=EL.

[266] Για παράδειγμα, στον ιστότοπο του Ευρωπαϊκού Κοινοβουλίου η διαθέσιμη πολιτική για τους ιχνηλάτες δεν παρείχε τις κατάλληλες πληροφορίες σχετικά με τους ιχνηλάτες που συλλέγονται και τυγχάνουν διασυνοριακής διαβίβασης και επεξεργασίας.

δεδομένων προσωπικού χαρακτήρα για την περίοδο μεταξύ 30 Σεπτεμβρίου και 4 Νοεμβρίου 2020, κατά την οποία οι προαναφερθέντες ιχνηλάτες υπήρχαν στον ιστότοπο του Ευρωπαϊκού Κοινοβουλίου.

Ωστόσο, ο ΕΕΠΔ δεν επέβαλε πρόστιμο, αλλά απηύθυνε επίπληξη στο Ευρωπαϊκό Κοινοβούλιο, καθώς σε αντίθεση με τις εθνικές ΑΠΔ βάσει του ΓΚΠΔ, ο ΕΕΠΔ μπορεί να επιβάλει πρόστιμο μόνο σε περιορισμένες περιπτώσεις[267], οι οποίες δεν συντρέχουν στην προκειμένη περίπτωση. Επιπλέον, ο ΕΕΠΔ έδωσε στο Ευρωπαϊκό Κοινοβούλιο προθεσμία ενός μήνα για να επικαιροποιήσει την ενημέρωση προστασίας δεδομένων και να διευθετήσει τα εναπομείναντα ζητήματα σχετικά με τη διαφάνεια.

Σύμφωνα με τον οργανισμό NOYB, πρόκειται για την πρώτη απόφαση μιας ΑΠΔ που βασίστηκε στο σκεπτικό της απόφασης *Schrems II*, γεγονός που προαναγγέλλει ένα κύμα ευθυγραμμισμένων αποφάσεων από τις ΑΠΔ της ΕΕ, δεδομένων των δεκάδων παρόμοιων καταγγελιών που υποβλήθηκαν από τον οργανισμό NOYB τον Αύγουστο του 2020. Όπως χαρακτηριστικά δήλωσε ο Max Schrems: «*Ο ΕΕΠΔ κατέστησε σαφές ότι ακόμη και η τοποθέτηση ενός ιχνηλάτη από έναν αμερικανικό πάροχο παραβιάζει τη νομοθεσία της ΕΕ για την προστασία της ιδιωτικής ζωής. Δεν υπήρχε καμία κατάλληλη προστασία έναντι της παρακολούθησης από τις ΗΠΑ, παρά το γεγονός ότι οι Ευρωπαίοι πολιτικοί αποτελούν γνωστό στόχο παρακολούθησης*»[268].

Αξίζει, τέλος, να σημειωθεί ότι στις 27 Μαΐου 2021, ο ΕΕΠΔ ανακοίνωσε ότι έχει εκκινήσει τη διεξαγωγή δύο άλλων ερευνών. Η πρώτη αφορά στη χρήση των υπηρεσιών υπολογιστικού νέφους της Amazon Web Services και της Microsoft από τα θεσμικά όργανα και τους οργανισμούς της ΕΕ στο πλαίσιο των λεγόμενων «συμβάσεων Cloud II», ενώ η δεύτερη στη χρήση του Microsoft Office 365 από την Επιτροπή[269]. Οι εν λόγω έρευνες αποτελούν μέρος της στρατηγικής του ΕΕΠΔ για τη συμμόρφωση των θεσμικών οργάνων της ΕΕ με την απόφαση *Schrems II* σε σχέση με τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες,

[267] Βάσει των κριτηρίων που απαριθμούνται στο άρθρο 83, παράγραφος 2 του ΓΚΠΔ.
[268] NOYB (2022), «EDPS sanctions Parliament over EU-US Data Transfers to Google and Stripe», *noyb.eu*. Διαθέσιμο στο: https://noyb.eu/en/edps-sanctions-parliament-over-eu-us-data-transfers-google-and-stripe.
[269] Ευρωπαίος Επόπτης Προστασίας Δεδομένων (2021), *The EDPS opens two investigations following the "Schrems II" Judgement*. Βέλγιο: Ευρωπαίος Επόπτης Προστασίας Δεδομένων. Διαθέσιμο στο: https://edps.europa.eu/system/files/2021-05/EDPS-2021-11-The_EDPS_opens_two_investigations_following_the_Schrems%20II_Judgement_EN.pdf.

και ιδίως στις ΗΠΑ[270]. Μέχρι και σήμερα, ο ΕΕΠΔ δεν έχει δημοσιοποιήσει περισσότερες πληροφορίες αναφορικά με την πορεία των εν λόγω ερευνών. Είναι, όμως, βέβαιο ότι τα αποτελέσματα αυτών των ερευνών θα ρίξουν ακόμη περισσότερο φως στο δύσβατο πλέον μονοπάτι των διασυνοριακών διαβιβάσεων, στο οποίο πορεύονται τα θεσμικά όργανα της ΕΕ, αλλά κατ' επέκταση και οι ιδιωτικές επιχειρήσεις.

β) Η ΑΠΔ της Αυστρίας για τη χρήση της υπηρεσίας Google Analytics

Λίγες ημέρες αργότερα, στις 12 Ιανουαρίου 2022, η ΑΠΔ της Αυστρίας, Österreichische Datenschutzbehörde, δημοσίευσε μια δικαστική απόφαση ορόσημο, με την οποία διαπιστώθηκε ότι ένας ιδιωτικός φορέας εκμετάλλευσης ιστότοπου της ΕΕ παραβίασε το άρθρο 44 του ΓΚΠΔ για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε εισαγωγέα δεδομένων στις ΗΠΑ, την Google, μέσω της συνεχιζόμενης χρήσης της υπηρεσίας Google Analytics, χωρίς να διασφαλίζεται επαρκές επίπεδο προστασίας, όπως απαιτείται σύμφωνα με το πέμπτο κεφάλαιο του ΓΚΠΔ. Αφορμή της εν λόγω απόφασης αποτέλεσε καταγγελία που κατατέθηκε τον Αύγουστο του 2020 ενώπιον της ΑΠΔ της Αυστρίας από τον οργανισμό NOYB για λογαριασμό του προσβαλλόμενου υποκειμένου των δεδομένων.

Πιο συγκεκριμένα, στις 14 Αυγούστου 2020, ένας χρήστης με λογαριασμό Google επισκέφτηκε έναν αυστριακό ιστότοπο σχετικό με θέματα υγείας. Ο ιστότοπος χρησιμοποιούσε την υπηρεσία Google Analytics και τα δεδομένα του χρήστη διαβιβάζονταν με αυτό τον τρόπο στην Google στις ΗΠΑ. Βάσει αυτών των δεδομένων, η Google ήταν σε θέση να γνωρίζει την ταυτότητα του χρήστη. Στις 18 Αυγούστου 2020, ο ίδιος ο χρήστης κατέθεσε καταγγελία ενώπιον της ΑΠΔ της Αυστρίας με τη συνδρομή του οργανισμού NOYB. Η εν λόγω καταγγελία αποτελεί μια από τις περίφημες 101 καταγγελίες που κατατέθηκαν από τον οργανισμό NOYB ενώπιον 30 ΑΠΔ της ΕΕ, οι οποίες θέτουν το ζήτημα της νομιμότητας των διαβιβάσεων δεδομένων προσωπικού χαρακτήρα που προκύπτουν από τη χρήση ιχνηλατών προς την Google και την Facebook στις ΗΠΑ, ύστερα από την απόφαση *Schrems II*[271]. Μάλιστα, το ΕΣΠΔ δημιούργησε μια ομάδα εργασίας για να συντονίσει τις

[270] Ευρωπαίος Επόπτης Προστασίας Δεδομένων (2020), *Strategy for EU institutions to comply with "Schrems II" Ruling*. Βέλγιο: Ευρωπαίος Επόπτης Προστασίας Δεδομένων. Διαθέσιμο στο: https://edps.europa.eu/sites/default/files/edpsweb_press_releases/edps-2020-11_strategy_shremsii_judgement_en.pdf. Είναι χαρακτηριστικό ότι ο ΕΕΠΔ ενθάρρυνε έντονα, ήδη από τότε, τα θεσμικά όργανα της ΕΕ να αποφεύγουν τη διαβίβαση δεδομένων προσωπικού χαρακτήρα προς τις ΗΠΑ για νέες πράξεις επεξεργασίας ή νέες συμβάσεις με παρόχους υπηρεσιών.

[271] Βλ. NOYB (2020), «101 Complaints on EU-US transfers filed», *noyb.eu*. Διαθέσιμο στο: https://noyb.eu/en/101-complaints-eu-us-transfers-filed. Σε συνδυασμό με NOYB, «EU-US Transfers

απαντήσεις επί των καταγγελιών που υποβλήθηκαν από τον οργανισμό NOYB. Η εν λόγω απόφαση της ΑΠΔ της Αυστρίας αποτελεί ορόσημο για τη νέα πραγματικότητα των διαβιβάσεων δεδομένων σε τρίτες χώρες, ως η πρώτη απόφαση που εκδίδεται σε σχέση με τις προαναφερθείσες 101 καταγγελίες, και εύλογα θεωρείται ότι χαράζει το δρόμο για τις υπόλοιπες ΑΠΔ.

Στην απόφασή της, η αυστριακή ΑΠΔ διαπίστωσε ότι η χρήση των ιχνηλατών της υπηρεσίας Google Analytics από έναν αυστριακό ιστότοπο συνεπάγεται τη συλλογή και διαβίβαση δεδομένων προσωπικού χαρακτήρα στην Google στις ΗΠΑ, συμπεριλαμβανομένων μοναδικών αριθμών αναγνώρισης χρήστη και διευθύνσεων IP. Στο πλαίσιο αυτό, η αυστριακή ΑΠΔ διαπίστωσε ότι οι ΤΣΡ που συνήφθησαν μεταξύ του διαχειριστή του ιστοτόπου και της Google δεν παρείχαν επαρκές επίπεδο προστασίας σύμφωνα με τον ΓΚΠΔ, για τους εξής λόγους:

1) Η Google χαρακτηρίζεται ως πάροχος υπηρεσιών ηλεκτρονικών επικοινωνιών και ως εκ τούτου υπόκειται σε παρακολούθηση από τις υπηρεσίες πληροφοριών των ΗΠΑ στο πλαίσιο του αμερικανικού νόμου FISA 702,
2) Τα πρόσθετα μέτρα ασφαλείας της Google δεν ήταν αποτελεσματικά στο να καλύψουν τα κενά νομικής προστασίας που εντοπίστηκαν στην απόφαση *Schrems II*. Πιο συγκεκριμένα, η αυστριακή ΑΠΔ διαπίστωσε ότι τα τεχνικά μέτρα που εφάρμοσε η Google, εκτός από τις ΤΣΡ, δεν είναι αποτελεσματικά, διότι δεν εξαλείφουν την πιθανότητα παρακολούθησης και πρόσβασης στα δεδομένα προσωπικού χαρακτήρα από τις υπηρεσίες πληροφοριών των ΗΠΑ. Επιπλέον, η αυστριακή ΑΠΔ τόνισε ότι τα οργανωτικά και συμβατικά μέτρα που εφαρμόζει η Google (συμπεριλαμβανομένης της υποχρέωσης α) να ενημερώνει τα υποκείμενα των δεδομένων σχετικά με τα αιτήματα πρόσβασης των κυβερνητικών αρχών, β) να δημοσιεύει εκθέσεις διαφάνειας, γ) να διατηρεί πολιτική για το χειρισμό των αιτημάτων των κυβερνητικών αρχών και δ) να αξιολογεί προσεκτικά κάθε αίτημα των κυβερνητικών αρχών) είναι γενικά ανεπαρκή και αναποτελεσματικά για την εξασφάλιση επαρκούς επιπέδου προστασίας των δεδομένων που διαβιβάζονται στις ΗΠΑ[272].

Complaint Overview» (η λίστα των 101 καταγγελιών), *noyb.eu*. Διαθέσιμο στο: : https://noyb.eu/en/eu-us-transfers-complaint-overview.

[272] ΑΠΔ της Αυστρίας (Österreichische Datenschutzbehörde), Google Analytics case, 12 Ιανουαρίου 2022. Διαθέσιμο στο: https://noyb.eu/sites/default/files/2022-01/E-DSB%20-%20Google%20Analytics_EN_bk.pdf, σελ. 37.

3) Η αυστριακή ΑΠΔ απέρριψε το επιχείρημα ότι τα δεδομένα προσωπικού χαρακτήρα που συλλέχθηκαν μέσω ιχνηλατών και στη συνέχεια διαβιβάστηκαν στις ΗΠΑ δεν αφορούσαν ή δεν ταυτοποιούσαν άμεσα συγκεκριμένα πρόσωπα.[273] Ειδικότερα, η ΑΠΔ της Αυστρίας διαπίστωσε ότι οι διευθύνσεις IP και τα επιγραμμικά αναγνωριστικά χαρακτηρίζονται ως δεδομένα προσωπικού χαρακτήρα, διότι επιτρέπουν την ταυτοποίηση προσώπων.
4) Στην εν λόγω απόφαση γίνεται για πρώτη φορά εφαρμογή των κριτηρίων που έθεσε το ΕΣΠΔ για την υπαγωγή μιας διαβίβασης στο πεδίο εφαρμογής του πέμπτου κεφαλαίου του ΓΚΠΔ. Πιο συγκεκριμένα, σύμφωνα με την αυστριακή ΑΠΔ οι κανόνες του πέμπτου κεφαλαίου του ΓΚΠΔ σχετικά με τις διαβιβάσεις δεδομένων σε τρίτες χώρες ισχύουν μόνο για τους εξαγωγείς δεδομένων της ΕΕ και όχι για τους εισαγωγείς δεδομένων στις ΗΠΑ. Ως εκ τούτου, η αυστριακή ΑΠΔ διαπίστωσε ότι η εν λόγω παραβίαση οφειλόταν στον διαχειριστή του ιστοτόπου και όχι στην Google.

Η αυστριακή ΑΠΔ κατέληξε στο συμπέρασμα ότι επειδή δεν υπήρχε άλλος διαθέσιμος μηχανισμός διαβίβασης σύμφωνα με το πέμπτο κεφάλαιο του ΓΚΠΔ που θα μπορούσε να χρησιμοποιηθεί από τον διαχειριστή του ιστότοπου για τη διαβίβαση δεδομένων στην Google στις ΗΠΑ, δεν υπήρχε επαρκές επίπεδο προστασίας των δεδομένων προσωπικού χαρακτήρα που συλλέχθηκαν μέσω των ιχνηλατών της υπηρεσίας Google Analytics, συνιστώντας παραβίαση του άρθρου 44 του ΓΚΠΔ[274].

Όπως είναι αναμενόμενο, η εν λόγω απόφαση ενδέχεται να έχει εκτεταμένη επίδραση στην κρίση των ΑΠΔ των άλλων κρατών-μελών της ΕΕ, γεγονός που θα μπορούσε δυνητικά να οδηγήσει στον αποκλεισμό της χρήσης της υπηρεσίας Google Analytics σε ολόκληρη την ΕΕ, όπως και εν γένει των διαβιβάσεων δεδομένων προσωπικού χαρακτήρα στις ΗΠΑ. Στο ρεύμα αυτό, χαρακτηριστικό παράδειγμα αποτελεί η ΑΠΔ της Ολλανδίας, Autoriteit Persoonsgegevens, η οποία πρόσφατα δημοσίευσε στο δημόσια διαθέσιμο οδηγό της μια ενημέρωση σχετικά με τον τρόπο ρύθμισης της λειτουργίας των ιχνηλατών της υπηρεσίας Google Analytics. Στην εν λόγω ενημέρωση, η ΑΠΔ της Ολλανδίας μνημονεύει την απόφαση

[273] ΑΠΔ της Αυστρίας (Österreichische Datenschutzbehörde), Google Analytics case, ο.π., σελ. 28.

[274] Αξίζει να σημειωθεί ότι η αυστριακή ΑΠΔ δεν επέβαλε κυρώσεις ή διορθωτικά μέτρα, επισημαίνοντας ότι ο διαχειριστής του ιστότοπου συγχωνεύθηκε με εταιρεία που εδρεύει στο Μόναχο και, ως εκ τούτου, το ενδεχόμενο απαγόρευσης των διαβιβάσεων προς την Google θα πρέπει να αξιολογηθεί από την αρμόδια ΑΠΔ της Γερμανίας. Βλ. ΑΠΔ της Αυστρίας (Österreichische Datenschutzbehörde), Google Analytics case, ο.π., σελ. 40.

της ΑΠΔ της Αυστρίας και ανακοινώνει ότι διερευνά επί του παρόντος δύο παρόμοιες καταγγελίες σχετικά με τη χρήση της υπηρεσίας Google Analytics στην Ολλανδία, ώστε να αποφανθεί και η ίδια επί της νομιμότητας χρήσης αυτής. Οι εν λόγω έρευνες αναμένεται να ολοκληρωθούν εντός του 2022[275].

Πλέον οι οργανισμοί και οι επιχειρήσεις στην ΕΕ θα πρέπει να αναρωτηθούν εάν θα πρέπει να αφαιρέσουν την υπηρεσία Google Analytics από τους ιστοτόπους τους ή να ρισκάρουν την επιβολή προστίμου από την αρμόδια ΑΠΔ για παραβίαση του ΓΚΠΔ. Η περίπτωση της Google φυσικά είναι μόνο η αρχή, και θα ακολουθήσει ο περιορισμός και άλλων πάροχων που βρίσκονται στις ΗΠΑ, με μόνη διέξοδο είτε οι ΗΠΑ να αλλάξουν τη νομοθεσία περί μαζικής παρακολούθησης ώστε να ισχυροποιήσουν τη δραστηριότητα των ιδιωτικών επιχειρήσεων, είτε οι πάροχοι υπηρεσιών με έδρα στις ΗΠΑ να ξεκινήσουν να φιλοξενούν τα δεδομένα προσωπικού χαρακτήρα των ευρωπαίων πολιτών εντός της ΕΕ. Μόνο εντύπωση δεν θα προκαλέσει εάν στο εγγύς μέλλον τη θέση των ΗΠΑ λάβουν άλλες τρίτες χώρες, όπου κολοσσοί της τεχνολογίας και της πληροφορικής έχουν την έδρα τους.

[275] Bryant, J. (2022), «Austrian DPA's Google Analytics decision could have 'far-reaching implications», *International Association of Privacy Professionals - The Privacy Advisor*. Διαθέσιμο στο: https://iapp.org/news/a/far-reaching-implications-anticipated-with-austrian-dpas-google-analytics-decision/. Σε συνδυασμό με την ενότητα *Cookies* από τον επίσημο ιστότοπο της ΑΠΔ της Ολλανδίας, Autoriteit Persoonsgegevens. Διαθέσιμο στο: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internet-telefoon-tv-en-post/cookies#hoe-kan-ik-bij-google-analytics-de-privacy-van-mijn-websitebezoekers-beschermen-4898.

ΕΠΙΛΟΓΟΣ

Με την παρούσα μελέτη κατέστη σαφές ότι οι αποφάσεις του ΔΕΕ για την υπόθεση Schrems άλλαξαν σημαντικά και αισθητά το τοπίο για τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα, όχι μόνο προς τις ΗΠΑ, αλλά προς κάθε χώρα εκτός της ΕΕ. Αυτό βέβαια, δεν σημαίνει ότι εφεξής παύουν οι διαβιβάσεις δεδομένων σε τρίτες χώρες, καθώς ο ΓΚΠΔ παρέχει στους εξαγωγείς δεδομένων και άλλους μηχανισμούς διαβίβασης πέρα από τις αποφάσεις επάρκειας και τις ΤΣΡ. Η απόφαση *Schrems II* κήρυξε ανίσχυρη αφενός την απόφαση για την Ασπίδα Προστασίας της Ιδιωτικής Ζωής, και αναγνώρισε αφετέρου τις ΤΣΡ ως έγκυρο μηχανισμό διαβίβασης, προβαίνοντας ωστόσο στην προσθήκη συμπληρωματικών υποχρεώσεων για τους εξαγωγείς και εισαγωγείς δεδομένων, με σκοπό τη διασφάλιση κάθε φορά ενός ουσιαστικά ισοδύναμου επιπέδου προστασίας με εκείνο της ΕΕ. Το ΕΣΠΔ έχει ήδη εξοπλίσει τους εξαγωγείς δεδομένων με δυο εξειδικευμένες Συστάσεις, οι οποίες τους συνδράμουν στο νέο και δύσκολο έργο τους. Παράλληλα, η Επιτροπή επικαιροποίησε τις ΤΣΡ, ώστε οι εξαγωγείς δεδομένων να μην έχουν πλέον καμία δικαιολογία ως προς την πρακτική εφαρμογή των νέων υποχρεώσεων που έθεσε το ΔΕΕ, και εξέδωσε δυο αποφάσεις επάρκειας, γεγονός που αποδεικνύει ότι παρόλες τις νομολογικές και πολιτικές εξελίξεις, γίνεται προσπάθεια εξεύρεσης της χρυσής εκείνης τομής, ώστε να μην σταματήσει η ροή των δεδομένων προσωπικού χαρακτήρα στο σύγχρονο ψηφιακό κόσμο. Μάλιστα, η επερχόμενη τρίτη απόφαση επάρκειας της Επιτροπής για τις ΗΠΑ θα αποτελέσει σημαντικό παράγοντα στην ευρύτερη ενωσιακή προσπάθεια δημιουργίας ενός ενιαίου και ασφαλούς οικουμενικού ιστού για την προστασία της ιδιωτικής ζωής και των δεδομένων προσωπικού χαρακτήρα.

Στο νέο αυτό καθεστώς για τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες, τόσο οι εξαγωγείς όσο και οι εισαγωγείς δεδομένων καθίστανται θεματοφύλακες των αρχών προστασίας των δεδομένων, αφού θα πρέπει να συμμορφώνονται με τις νέες υποχρεώσεις, και να συνδράμουν ο ένας τον άλλον, με απώτερο πάντα σκοπό τη διασφάλιση του θεμελιώδους δικαιώματος του ανθρώπου για την προστασία των δεδομένων που τον αφορούν. Σε θεσμικό επίπεδο, η διαρκής επαγρύπνηση για την ομοιόμορφη και νόμιμη διαβίβαση δεδομένων βαρύνει συλλογικά, τόσο τα όργανα της ΕΕ, που θα πρέπει να ελέγχουν ανά τακτά χρονικά διαστήματα τη νομιμότητα και τις πρακτικές εφαρμογής των αποφάσεων επάρκειας - ακόμη και αναστέλλοντας την ισχύ τους - όσο και τις εθνικές ΑΠΔ, οι οποίες θα πρέπει να διασφαλίσουν την προσήκουσα ισορροπία μεταξύ, αφενός, του

σεβασμού του θεμελιώδους δικαιώματος στην ιδιωτική ζωή και, αφετέρου, των συμφερόντων που επιβάλλουν την ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα. Εκείνοι, όμως, που οφείλουν αδιαμφισβήτητα να επαγρυπνούν είναι οι ίδιοι οι πολίτες του σύγχρονου ψηφιακού κόσμου, γιατί, όπως απέδειξε η πολύκροτη υπόθεση Schrems, εκείνοι είναι που, με την επιμονή και τη μαχητικότητά τους, έχουν τελικά τη δύναμη να επιβάλουν την αποκατάσταση της διαταραχθείσας νομιμότητας[276]. Αυτό άλλωστε επιτάσσει και η λεγόμενη «*ψηφιακή κυριαρχία* του χρήστη»[277], μια ιδέα που έχει διατυπωθεί και από το δημιουργό του παγκόσμιου ιστού, Tim Berners-Lee, κατά τα λεγόμενα του οποίου πρέπει να φανταστούμε έναν ψηφιακό κόσμο, στον οποίο κάθε δεδομένο που δημιουργεί ένας χρήστης (πολίτης) θα βρίσκεται υπό τον έλεγχό του[278].

[276] Τζέμος, Β. Γ. (2016), *Το Δημόσιο Δίκαιο μέσα από τις αποφάσεις των Δικαστηρίων*. Αθήνα: Νομική Βιβλιοθήκη, σελ. 177 - 178.

[277] Βλ. σχετικά T. Christakis (2021), «'European Digital Sovereignty': Successfully Navigating Between the 'Brussels Effect' and Europe's Quest for Strategic Autonomy», ο.π., σελ. 17 - 19.

[278] «*… we have to imagine a world in which any data you create is under your control*». Βλ. J. Thornhill (2019), «The people, not governments, should exercise digital sovereignty», *Financial Times*. Διαθέσιμο στο: https://www.ft.com/content/9ca5b0b2-0f64-11ea-a7e6-62bf4f9e548a.

ΒΙΒΛΙΟΓΡΑΦΙΑ

I. ΣΥΓΓΡΑΜΑΤΑ

1. Kosta, E., Leenes, R. and Irene Kamara (2022), *Research Handbook on EU Data Protection Law*. Ηνωμένο Βασίλειο: Edward Elgar Publishing.
2. Κοτσαλής Λ., Μενουδάκος Κ. (2021), *Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων (GDPR) (Νομική διάσταση και πρακτική εφαρμογή)*. Αθήνα: Νομική Βιβλιοθήκη.
3. Κανέλλος Λ. (2020), *The GDPR Handbook - Για DPOs, Επιχειρήσεις & Οργανισμούς*. Αθήνα, Νομική Βιβλιοθήκη.
4. Snowden E. (2019), *Το Μεγάλο Φακέλωμα*. Αθήνα: Ψυχογιός.
5. Κέντρο Διεθνούς και Ευρωπαϊκού Οικονομικού Δικαίου (2018), *Προστασία των δεδομένων προσωπικού χαρακτήρα*. Αθήνα: Σάκκουλας.
6. Μήτρου, Λ. (2017), *Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων*. Αθήνα: Σάκκουλας.
7. Χρήστου, Β. (2017), *Το δικαίωμα στην προστασία από την επεξεργασία δεδομένων*. Αθήνα: Σάκκουλας.
8. Τζέμος, Β. Γ. (2016), *Το Δημόσιο Δίκαιο μέσα από τις αποφάσεις των Δικαστηρίων*. Αθήνα: Νομική Βιβλιοθήκη.

II. ΑΡΘΡΑ/ΜΕΛΕΤΕΣ

1. Bryant, J. (2022), «Austrian DPA's Google Analytics decision could have 'far-reaching implications», *International Association of Privacy Professionals - The Privacy Advisor*. Διαθέσιμο στο: https://iapp.org/news/a/far-reaching-implications-anticipated-with-austrian-dpas-google-analytics-decision/.
2. NOYB (2022), «EDPS sanctions Parliament over EU-US Data Transfers to Google and Stripe», *noyb.eu*. Διαθέσιμο στο: https://noyb.eu/en/edps-sanctions-parliament-over-eu-us-data-transfers-google-and-stripe.
3. Zanfir-Fortuna, G. (2021), «Dispatch from the Global Privacy Assembly: The brave new world of International Data Transfers», *Future of Privacy Forum*. Διαθέσιμο στο: https://fpf.org/blog/dispatch-from-the-global-privacy-assembly-the-brave-new-world-of-international-data-transfers/.
4. Ilan, D., Kristensen, G., Ka Chun, L., Gerlach, N. και Mammì Borruto, F. (2021), «New Standard Contractual Clauses for Data Transfers under the GDPR - New Changes, New Questions?», *Cleary Gottlieb*. Διαθέσιμο στο: https://www.clearygottlieb.com/-/media/files/alert-memos-2021/the-new-commission-sccs-for-data-transfers-under-gdpr-more-questions-than-answers.pdf.
5. Ionescu, R. and Bucur, M. (2021) «First thoughts on the new SCCs for international transfers of personal data», *Privacy Out Loud - Nestor Nestor Diculescu Kingston Petersen.* Διαθέσιμο στο: https://privacyoutloud.ro/articles/first-thoughts-on-the-new-sccs-for-international-transfers-of-personal-data-2/.
6. Hallinan, D., Bernier, A., Cambon-Thomsen, A. Crawley F. P., Dimitrova, D. Bauzer Medeiros, C., Nilsonne, G., Parker, S., Pickering, B., and Rennes, S. (2021), «International transfers of personal data for health researchfollowing Schrems II: a problem in need of a solution», *European Journal of Human Genetics.* Διαθέσιμο στο: https://www.nature.com/articles/s41431-021-00893-y.
7. Breitbarth, P. (2021), «A Risk-Based Approach to International Data Transfers», *European Data Protection Law Review*, Volume 7, Issue 4 (2021). Διαθέσιμο στο: https://edpl.lexxion.eu/article/EDPL/2021/4/9.
8. Tielemans, J., Cooper, D. and Maldoff, G. (2021), «EDPB's data transfer recommendations adopt a risk-based approach with teeth», *International Association of Privacy Professionals - The Privacy Advisor*. Διαθέσιμο στο: https://iapp.org/news/a/edpbs-data-transfer-recommendations-adopt-a-risk-based-approach-with-teeth/.

9. Tielemans, J. (2021) «EU adequacy decision for South Korea», *International Association of Privacy Professionals - The Privacy Advisor*. Διαθέσιμο στο: https://iapp.org/news/a/eu-adequacy-decision-for-south-korea/.
10. Zalnieriute M. (2021), «Data Transfers after Schrems II: The EU-US Disagreements Over Data Privacy and National», *Vanderbilt Journal of Transnational Law*, (2022) 55(1) forthcoming. Διαθέσιμο στο: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3826878.
11. Chiavetta R. (2021) «European Commission adopts UK adequacy decisions», *The Privacy Advisor - IAPP*. Διαθέσιμο στο: https://iapp.org/news/a/european-commission-adopts-uk-adequacy-decisions/.
12. Francis, M. and Serafino M., (2021) «EU Releases New Standard Contractual Clauses for Cross-Border Data Transfers», *Holland & Knight Alert*. Διαθέσιμο στο: https://www.hklaw.com/en/insights/publications/2021/06/eu-releases-new-standard-contractual-clauses-for-crossborder.
13. Kuner, C. (2021), «Territorial Scope and Data Transfer Rules in the GDPR: Realising the EU's Ambition of Borderless Data Protection», *University of Cambridge Faculty of Law Research Paper No. 20/2021*. Διαθέσιμο στο: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3827850.
14. Bygrave, L. A. (2020), «The 'Strasbourg Effect' on data protection in light of the 'Brussels Effect': Logic, mechanics and prospects», *Computer Law & Security Review*, Volume 40. Διαθέσιμο στο: https://www.sciencedirect.com/science/article/pii/S0267364920300650?via%3Dihub.
15. O'Donoghue, C. and O'Brien, S. (2021) «UK adequacy decision for European data transfers», *Technology Law Dispatch*, Reed Smith LLP. Διαθέσιμο στο: https://www.technologylawdispatch.com/2021/07/privacy-data-protection/uk-adequacy-decision-for-european-data-transfers/.
16. Christakis, T. (2020), «'European Digital Sovereignty': Successfully Navigating Between the 'Brussels Effect' and Europe's Quest for Strategic Autonomy». Διαθέσιμο στο: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3748098.
17. Chander, A. (2020), «Is Data Localization a Solution for Schrems II?», *Journal of International Economic Law*, Volume 23, Issue 3, 771 - 784. Διαθέσιμο στο: https://academic.oup.com/jiel/article-abstract/23/3/771/5909035?redirectedFrom=fulltext.
18. Kuner, C. (2020), «Schrems II Re-Examined», *Verfassungsblog*. Διαθέσιμο στο: https://verfassungsblog.de/schrems-ii-re-examined/.
19. Ikeda, S. (2020), «EDPB Issues Recommendations on International Data Transfers in Response to Schrems II Decision; Is It a Lasting Solution?», *CPO Magazine*. Διαθέσιμο στο: https://www.cpomagazine.com/data-privacy/edpb-issues-recommendations-on-international-data-transfers-in-response-to-schrems-ii-decision-is-it-a-lasting-solution/.
20. Kuner, C. (2020), «The Schrems II judgment of the Court of Justice and the future of data transfer regulation», *European Law Blog*. Διαθέσιμο στο: https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation/#:~:text=In%20Schrems%20II%20the%20Court,Privacy%20Shield%2C%20which%20was%20the.
21. Τάσσης Σ. (2020), «Schrems II - και τώρα τι;», *Lawyer - The Business Magazine*. Διαθέσιμο στο: https://lawyermagazine.gr/schrems-ii-kai-twra-ti/.
22. Κόμνιου Κ. (2020), «Η διαβίβαση προσωπικών δεδομένων σε τρίτες χώρες μετά την απόφαση Schrems II -"Now what?», *capital. gr*. Διαθέσιμο στο: https://www.capital.gr/me-apopsi/3485424/i-diabibasi-prosopikon-dedomenon-se-trites-xores-meta-tin-apofasi-schrems-ii-now-what.
23. Rotenberg, M. (2020), «Schrems II, from Snowden to China: Toward a new alignment on transatlantic data protection" *European Law Journal*, Volume 26, Issue 1-2, Pages 141-152. Διαθέσιμο στο: https://doi.org/10.1111/eulj.12370.
24. Bignami, F. (2020), «Schrems II: The Right to Privacy and the New Illiberalis», *Media Laws*. Διαθέσιμο στο: https://verfassungsblog.de/schrems-ii-the-right-to-privacy-and-the-new-illiberalism/.
25. Christakis, T. (2020), «After Schrems II : Uncertainties on the Legal Basis for Data Transfers and Constitutional Implications for Europe», *European Law Blog*. Διαθέσιμο στο: https://europeanlawblog.eu/2020/07/21/after-schrems-ii-uncertainties-on-the-legal-basis-for-data-transfers-and-constitutional-implications-for-europe/.

26. NOYB (2020), «CJEU Judgment - First Statement», *noyb.eu*. Διαθέσιμο στο: https://noyb.eu/en/cjeu.

27. Churches, G. and Zalnieriute, M. (2020), «Contracting Out" Human Rights in International Law: Schrems II and the Fundamental Flaws of U.S. Surveillance Law», *Harvard International Law Journal*. Διαθέσιμο στο: https://harvardilj.org/2020/08/contracting-out-human-rights-in-international-law-schrems-ii-and-the-fundamental-flaws-of-u-s-surveillance-law/.

28. NOYB (2020), «101 Complaints on EU-US transfers filed», *noyb.eu*. Διαθέσιμο στο: https://noyb.eu/en/101-complaints-eu-us-transfers-filed.

29. Tracol, X. (2020), «"Schrems II": The return of the Privacy Shield», *Computer Law & Security Review*, Volume 39. Διαθέσιμο στο: https://www.sciencedirect.com/science/article/pii/S0267364920300893?via%3Dihub.

30. Baker, S. (2020), «How Can the U.S. Respond to Schrems II?», *Lawfare*. Διαθέσιμο στο: https://www.lawfareblog.com/how-can-us-respond-schrems-ii#.

31. Cotton, B. (2019), «Five Eyes Alliance: Everything You Need To Know», *Business Leader Magazine*. Διαθέσιμο στο: https://www.businessleader.co.uk/about/.

32. Παναγοπούλου-Κουτνατζή, Φ. (2019), «Συνταγματικές προεκτάσεις των μηχανισμών διευρύνσεως της προστασίας δεδομένων προσωπικού χαρακτήρα πέραν της ΕΕ: Εξωεδαφική εφαρμογή του ΓΚΠΔ και διασυνοριακή διαβίβαση δεδομένων», *ΤΝΠ QUALEX, ΔiMEE*, 4/2019, σελ. 504 - 520.

33. Thornhill, J. (2019), «The people, not governments, should exercise digital sovereignty», *Financial Times*. Διαθέσιμο στο: https://www.ft.com/content/9ca5b0b2-0f64-11ea-a7e6-62bf4f9e548a.

34. Vrbljanac, D. (2018), «Personal Data Transfer to Third Countries - Disrupting the Even Flow?», *Athens Journal of Law*, σελ. 337 - 358. Διαθέσιμο στο: https://www.athensjournals.gr/law/2018-4-4-4-Vrbljanac.pdf.

35. Λεμπέση, Δ. (2018), «Γενικός Ευρωπαϊκός Κανονισμός για την προστασία προσωπικών δεδομένων (ΕΕ 2016/679) - Κατάργηση τής οδηγίας 95/46/ΕΚ - Συγκριτική μελέτη», *Δελτίον Εργατικής Νομοθεσίας*, τ. 74, τεύχ. 1733. Διαθέσιμο στο: http://www.den.gr/Login/?ReturnTo=/790/#main1.

36. Kuner, C. (2017), «Reality and Illusion in EU Data Transfer Regulation Post Schrems», *German Law Journal*. Διαθέσιμο στο: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2732346.

37. Αλεξανδροπούλου - Αιγυπτιάδου, Ε. (2016), «Διασυνοριακή ροή προσωπικών δεδομένων από την ΕΕ στις ΗΠΑ: Η πρόσφατη απόφαση του ΔΕΕ ενόψει της σχετικής δραστηριότητας του Facebook (C-362/2014, M. Schrems κατά Ιρλανδού Επιτρόπου Προστασίας Προσωπικών Δεδομένων), *ΤΝΠ QUALEX, ΔiMEE*, 1/2016, σελ. 12 - 24.

38. Tracol, X. (2016) «EU U.S. Privacy Shield: The saga continues», *Computer Law & Security Review*, Volume 2, Issue 5. Διαθέσιμο στο: https://www.sciencedirect.com/science/article/abs/pii/S0267364916301273.

39. Μήτρου, Λ. (2015), «Προστασία Προσωπικών Δεδομένων και υπολογιστικό νέφος», *ΤΝΠ QUALEX, ΔiMEE*, 4/2015, σελ. 534 - 549.

40. Τάσσης Σ. (2015), «Σημείωμα στην ΔΕΕ υπόθ. C-362/14, απόφ. της 6.10.2015 - ΟΙ ΗΠΑ δεν αποτελούν πλέον «ασφαλές λιμάνι» για τα προσωπικά δεδομένα των πολιτών της ΕΕ», *ΤΝΠ QUALEX, ΔiMEE*, 3/2015, σελ. 508 - 512.

41. Greenwald, G. and MacAskill, E. (2013), «NSA Prism program taps in to user data of Apple, Google and others», *The Guardian*. Διαθέσιμο στο: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

42. Ball, J. (2013), «NSA's Prism surveillance program: how it works and what it can do», *The Guardian*. Διαθέσιμο στο: https://www.theguardian.com/world/2013/jun/08/nsa-prism-server-collection-facebook-google.

43. Svantesson, D. J. B. (2013), «A "layered approach" to the extraterritoriality of data privacy laws», *International Data Privacy Law*. Διαθέσιμο στο: https://www.researchgate.net/publication/275003577_A_layered_approach_to_the_extraterritoriality_of_data_privacy_laws.

III. ΝΟΜΟΛΟΓΙΑ

1. ΔΕΕ, C-311/18, *Data Protection Commissioner κατά Facebook Ireland Limited και Maximillian Schrems* (Schrems II), 16 Ιουλίου 2020. Διαθέσιμο στο: https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EL&mode=lst&dir=&occ=first&part=1&cid=3359385.
2. ΔΕΕ, C-362/14, *Maximillian Schrems κατά Data Protection Commissioner* (Schrems I), 6 Οκτωβρίου 2015. Διαθέσιμο στο: https://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=el&mode=lst&dir=&occ=first&part=1&cid=749866.
3. Προτάσεις του Γενικού Εισαγγελέα, Yves Bot, C-362/14, *Maximillian Schrems κατά Data Protection Commissioner*, 23 Σεπτεμβρίου 2015. Διαθέσιμο στο: https://curia.europa.eu/juris/document/document.jsf?text=&docid=168421&pageIndex=0&doclang=el&mode=lst&dir=&occ=first&part=1&cid=897177.
4. Προτάσεις του Γενικού Εισαγγελέα, Henrik Saugmandsgaard Øe, C-311/18, *Maximillian Schrems κατά Data Protection Commissioner*, 19 Δεκεμβρίου 2019. Διαθέσιμο στο: https://curia.europa.eu/juris/document/document.jsf;jsessionid=1A97A2D89262C458AB209A52CAAF1869?text=&docid=221826&pageIndex=0&doclang=EL&mode=req&dir=&occ=first&part=1&cid=742986.
5. Ανώτατο Δικαστήριο της Ιρλανδίας, 2016/4809 P, *Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems - Judgment of Mr. Justice Brian J. McGovern*, 19 Ιουλίου 2016. Διαθέσιμο στο: https://regmedia.co.uk/2016/07/19/facebook_eff_schrems.pdf.
6. ΔΕΕ, C-131/12, *Google Spain SL και Google Inc. κατά Agencia Española de Protección de Datos (AEPD) και Mario Costeja González*, 13 Μαΐου 2014. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A62012CJ0131&msclkid=dfab6b55c4c311ecae40f26a8ea11235.
7. ΔΕΕ, συνεκδικαζόμενες υποθέσεις C 293/12 και C 594/12, *Digital Rights Ireland Ltd κατά Minister for Communications, Marine and Natural Resources κ.λπ. και Kärntner Landesregierung κ.λπ.*, 8 Απριλίου 2014. Διαθέσιμο στο: https://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=EL&mode=lst&dir=&occ=first&part=1&cid=3284789.

IV. ΑΠΟΦΑΣΕΙΣ ΕΥΡΩΠΑΙΚΗΣ ΕΠΙΤΡΟΠΗΣ

1. Ευρωπαϊκή Επιτροπή (2021), *COMMISSION IMPLEMENTING DECISION on standard contractual clauses between controllers and processors under Article 28 (7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29 (7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council*. Βέλγιο: Ευρωπαϊκή Επιτροπή. Διαθέσιμο στο: https://ec.europa.eu/info/law/law-topic/data-protection/publications/standard-contractual-clauses-controllers-and-processors_en.
2. Ευρωπαϊκή Επιτροπή (2021), *Εκτελεστική Απόφαση (ΕΕ) 2021/914 της Επιτροπής της 4ης Ιουνίου 2021 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*. Βέλγιο: Ευρωπαϊκή Επιτροπή. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32021D0914.
3. Ευρωπαϊκή Επιτροπή (2021), *Commission Implementing Decision of 17.12.2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the Republic of Korea under the Personal Information Protection Act*, Βέλγιο: Ευρωπαϊκή Επιτροπή. Διαθέσιμο στο: https://ec.europa.eu/info/files/decision-adequate-protection-personal-data-republic-korea-annexes_en.
4. Ευρωπαϊκή Επιτροπή (2021), *Commission Implementing Decision of 28.6.2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom*. Βέλγιο: Ευρωπαϊκή Επιτροπή. Διαθέσιμο στο: https://ec.europa.eu/info/sites/default/files/decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_-_general_data_protection_regulation_en.pdf.

5. Ευρωπαϊκή Επιτροπή (2021), *Commission Implementing Decision of 28.6.2021 pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom.* Βέλγιο: Ευρωπαϊκή Επιτροπή. Διαθέσιμο στο: https://ec.europa.eu/info/sites/default/files/decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_law_enforcement_directive_en.pdf.
6. Ευρωπαϊκή Επιτροπή (2016), *Εκτελεστική Απόφαση (ΕΕ) 2016/1250 της Επιτροπής της 12ης Ιουλίου 2016 βάσει της οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την επάρκεια της προστασίας που παρέχεται από την ασπίδα προστασίας της ιδιωτικής ζωής ΕΕ–ΗΠΑ*. Βέλγιο: Ευρωπαϊκή Επιτροπή. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016D1250&from=NL.
7. Ευρωπαϊκή Επιτροπή (2016), *Εκτελεστική Απόφαση (ΕΕ) 2016/2297 της Επιτροπής της 16ης Δεκεμβρίου 2016 για την τροποποίηση των αποφάσεων 2001/497/ΕΚ και 2010/87/ΕΕ σχετικά με τις τυποποιημένες συμβατικές ρήτρες για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα προς τρίτες χώρες και σε εκτελούντες επεξεργασία εγκατεστημένους σε τρίτες χώρες βάσει της οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου*. Βέλγιο: Ευρωπαϊκή Επιτροπή. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016D2297
8. Απόφαση της Επιτροπής της 5ης Φεβρουαρίου 2010 σχετικά με τις τυποποιημένες συμβατικές ρήτρες για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε εκτελούντες επεξεργασία εγκατεστημένους σε τρίτες χώρες βάσει της οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (2010/87/ΕΕ). Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32010D0087&from=EN.
9. Απόφαση της Επιτροπής της 27ης Δεκεμβρίου 2004 για την τροποποίηση της απόφασης 2001/497/ΕΚ όσον αφορά την εισαγωγή μιας εναλλακτικής δέσμης τυποποιημένων συμβατικών ρητρών για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα προς τρίτες χώρες (2004/915/ΕΚ). Διαθέσιμο στο: https://op.europa.eu/en/publication-detail/-/publication/57a11830-3866-44bf-a03a-0384f7b3d3d6/language-el/format-PDF.
10. Απόφαση της Επιτροπής της 15ης Ιουνίου 2001 σχετικά με τις τυποποιημένες συμβατικές ρήτρες για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα προς τρίτες χώρες δυνάμει του άρθρου 26 παράγραφος 4 της οδηγίας 95/46/ΕΚ (2001/497/ΕΚ). Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32001D0497&from=en.
11. Απόφαση της Επιτροπής της 27ης Δεκεμβρίου 2001, σχετικά με τις τυποποιημένες συμβατικές ρήτρες για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε εκτελούντες επεξεργασία εγκατεστημένους σε τρίτες χώρες, βάσει της οδηγίας 95/46/ΕΚ (2002/16/ΕΚ). Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32002D0016&from=en.
12. Απόφαση 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 στο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32000D0520&from=EL.
13. Ευρωπαϊκή Επιτροπή (2000), Απόφαση της Επιτροπής, της 26ης Ιουλίου 2000, δυνάμει της οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την επάρκεια της προστασίας των δεδομένων προσωπικού χαρακτήρα που παρέχεται στην Ελβετία. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32000D0518&from=EL.

V. ΑΠΟΦΑΣΕΙΣ ΑΡΧΩΝ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

1. Αρχή Προστασίας Δεδομένων της Αυστρίας (Österreichische Datenschutzbehörde), Google Analytics case, 12 Ιανουαρίου 2022. Διαθέσιμο στο: https://noyb.eu/sites/default/files/2022-01/E-DSB%20-%20Google%20Analytics_EN_bk.pdf
2. Ευρωπαίος Επόπτης Προστασίας Δεδομένων, Case 2020-1013, *Decision of the European Data Protection Supervisor in complaint case 2020-1013 submitted by Members of the Parliament against the European*

Parliament, 5 Ιανουαρίου 2022. Διαθέσιμο στο: https://noyb.eu/sites/default/files/2022-01/Case%202020-1013%20-%20EDPS%20Decision_bk.pdf.

3. The High Court Commercial, *Data Protection Commissioner and Facebook Ireland Limited and Maximillian Schrems*, υπ'αριθμ. 2016 No. 4809 P. Διαθέσιμο στο: https://www.dataprotection.ie/sites/default/files/uploads/2018-12/High%20Court%20Judgment_03_10_2017.pdf.

VI. ΝΟΜΟΘΕΣΙΑ

1. Κανονισμός (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Οκτωβρίου 2018, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης και την ελεύθερη κυκλοφορία των δεδομένων αυτών, και για την κατάργηση του κανονισμού (ΕΚ) αριθ. 45/2001 και της απόφασης αριθ. 1247/2002/ΕΚ. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32018R1725&from=EL.
2. Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων). Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016R0679&from=EL.
3. 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 στο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:31995L0046&from=EL.
4. Κανονισμός Διαδικασίας του Δικαστηρίου της ΕΕ. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=OJ:L:2012:265:FULL&from=EL.
5. Συνθήκης για τη Λειτουργία της Ευρωπαϊκής Ένωσης. Διαθέσιμο στο: https://op.europa.eu/el/publication-detail/-/publication/9e8d52e1-2c70-11e6-b497-01aa75ed71a1?msclkid=2f1215adc58611ec9ffeb2d1d687b9d6.
6. Χάρτης των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A12016P%2FTXT.

VII. ΛΟΙΠΕΣ ΠΗΓΕΣ

1. Ευρωπαϊκή Επιτροπή (2022), *European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework*. Βέλγιο: Ευρωπαϊκή Επιτροπή. Διαθέσιμο στο: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087.
2. Λευκός Οίκος (2022), *FACT SHEET: United States and European Commission Announce Trans-Atlantic Data Privacy Framework*. ΗΠΑ: Λευκός Οίκος. Διαθέσιμο στο: https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/.
3. Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (2021), *Συστάσεις 01/2020 σχετικά με τα μέτρα που συμπληρώνουν τα εργαλεία διαβίβασης για τη διασφάλιση της συμμόρφωσης με το επίπεδο προστασίας δεδομένων προσωπικού χαρακτήρα στην ΕΕ*. Βέλγιο: Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. Διαθέσιμο στο: https://edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_el.pdf.
4. Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (2021), *Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR*. Βέλγιο: Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. Διαθέσιμο στο: https://edpb.europa.eu/system/files/2021-11/edpb_guidelinesinterplaychapterv_article3_adopted_en.pdf.
5. Ευρωπαίος Επόπτης Προστασίας Δεδομένων (2021), *Case Law Digest 2021: Transfers of personal data to third countries - From Lindqvist to Schrems II: case law of the CJEU on transfers of personal data to third*

countries. Βέλγιο: Ευρωπαίος Επόπτης Προστασίας Δεδομένων. Διαθέσιμο στο: https://edps.europa.eu/data-protection/our-work/publications/court-cases/case-law-digest-2021-transfers-personal-data_en.

6. Δελτίο Τύπου Ευρωπαϊκής Επιτροπής (2021), *European Commission adopts new tools for safe exchanges of personal data*. Βέλγιο: Ευρωπαϊκή Επιτροπή. Διαθέσιμο στο: https://ec.europa.eu/commission/presscorner/detail/el/ip_21_2847.
7. Department for Digital, Culture, Media & Sport (2021), *EU adopts 'adequacy' decisions allowing data to continue flowing freely to the UK*. Διαθέσιμο στο: https://www.gov.uk/government/news/eu-adopts-adequacy-decisions-allowing-data-to-continue-flowing-freely-to-the-uk.
8. Δελτίο Τύπου Ευρωπαϊκής Επιτροπής (2021), *Intensifying Negotiations on transatlantic Data Privacy Flows: A Joint Press Statement by European Commissioner for Justice Didier Reynders and U.S. Secretary of Commerce Gina Raimondo*. Βέλγιο: Ευρωπαϊκή Επιτροπή. Διαθέσιμο στο: https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_21_1443.
9. Ευρωπαίος Επόπτης Προστασίας Δεδομένων (2021), *The EDPS opens two investigations following the "Schrems II" Judgement*. Βέλγιο: Ευρωπαίος Επόπτης Προστασίας Δεδομένων. Διαθέσιμο στο: https://edps.europa.eu/system/files/2021-05/EDPS-2021-11-The_EDPS_opens_two_investigations_following_the_Schrems%20II_Judgement_EN.pdf.
10. Δελτίο Τύπου Ευρωπαϊκής Επιτροπής (2021), *Joint Press Statement by Didier Reynders, Commissioner for Justice of the European Commission, and Yoon Jong In, Chairperson of the Personal Information Protection Commission of the Republic of Korea*. Βέλγιο: Ευρωπαϊκή Επιτροπή. Διαθέσιμο στο: https://ec.europa.eu/commission/presscorner/detail/en/statement_21_6915.
11. Information Commissioner's Office (2021), «*Guide to the General Data Protection Regulation (GDPR)*». Ηνωμένο Βασίλειο: Information Commissioner's Office. Διαθέσιμο στο: https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdfv.
12. Δελτίο Τύπου Ευρωπαϊκής Επιτροπής (2021), *Data protection: European Commission launches process on personal data flows to UK*. Βέλγιο: Ευρωπαϊκή Επιτροπή. Διαθέσιμο στο: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_661.
13. Microsoft (2021), «*Compliance with EU transfer requirements for personal data in the Microsoft cloud*». Διαθέσιμο στο: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWRql1?culture=en-us&country=US.
14. Microsoft (2021), «*Παράρτημα Προστασίας Δεδομένων Προσωπικού Χαρακτήρα Προϊόντων και Υπηρεσιών της Microsoft*». Διαθέσιμο στο: https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA.
15. Microsoft (2021), «*Microsoft Online Services Subprocessors List*». Διαθέσιμο στο: https://servicetrust.microsoft.com/ViewPage/TrustDocumentsV3?command=Download&downloadType=Document&downloadId=ede6342e-d641-4a9b-9162-7d66025003b0&tab=7f51cb60-3d6c-11e9-b2af-7bb9f5d2d913&docTab=7f51cb60-3d6c-11e9-b2af-7bb9f5d2d913_Subprocessor_List.
16. Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (2020), *Συστάσεις 02/2020 σχετικά με τις Ευρωπαϊκές Βασικές Εγγυήσεις για τα μέτρα παρακολούθησης*. Βέλγιο: Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. Διαθέσιμο στο: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_el.
17. United States Department of Commerce (2020), *Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II*. Ουάσιγκτον, ΗΠΑ: United States Department of Commerce. Διαθέσιμο στο: https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF.
18. Ευρωπαϊκή Επιτροπή (2020), *Joint Press Statement by European Commissioner for Justice Didier Reynders and U.S. Secretary of Commerce Wilbur Ross.* Βέλγιο: Ευρωπαϊκή Επιτροπή. Διαθέσιμο στο: https://ec.europa.eu/info/news/joint-press-statement-european-commissioner-justice-didier-reynders-and-us-secretary-commerce-wilbur-ross-7-august-2020-2020-aug-07_en.
19. United States Department of Commerce (2020), *Letter from Deputy Assistant Secretary James Sullivan on the Schrems II Decision.* Ουάσιγκτον, ΗΠΑ: United States Department of Commerce. Διαθέσιμο στο:

https://www.commerce.gov/about/letter-deputy-assistant-secretary-james-sullivan-schrems-ii-decision.
20. Ευρωπαίος Επόπτης Προστασίας Δεδομένων (2020), *Strategy for EU institutions to comply with "Schrems II" Ruling*. Βέλγιο: Ευρωπαίος Επόπτης Προστασίας Δεδομένων. Διαθέσιμο στο: https://edps.europa.eu/sites/default/files/edpsweb_press_releases/edps-2020-11_strategy_shremsii_judgement_en.pdf.
21. Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (2020), *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*. Βέλγιο: Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. Διαθέσιμο στο: https://edpb.europa.eu/sites/default/files/files/file1/edpb_faqs_schrems_ii_202007_adopted_el.pdf.
22. Δελτίο Τύπου Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων (2020), *European Data Protection Board - 41st Plenary session: EDPB adopts recommendations on supplementary measures following Schrems II.* Βέλγιο: Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. Διαθέσιμο στο: https://edpb.europa.eu/news/news/2020/european-data-protection-board-41st-plenary-session-edpb-adopts-recommendations_en.
23. Ομοσπονδιακός Επίτροπος Προστασίας Δεδομένων και Πληροφοριών της Ελβετίας (2020), *FDPIC considers CH-US Privacy Shield does not provide adequate level of data protection*. Ελβετία: Ομοσπονδιακός Επίτροπος Προστασίας Δεδομένων και Πληροφοριών της Ελβετίας. Διαθέσιμο στο: https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-80318.html.
24. Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (2019), *Κατευθυντήριες γραμμές 3/2018 σχετικά με το εδαφικό πεδίο εφαρμογής του ΓΚΠΔ (άρθρο 3)*. Βέλγιο: Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. Διαθέσιμο στο: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_consultation_el.pdf.
25. Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (2018), *Κατευθυντήριες γραμμές 2/2018 αναφορικά με τις παρεκκλίσεις που προβλέπονται στο άρθρο 49 του Κανονισμού 2016/679*. Βέλγιο: Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. Διαθέσιμο στο: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_el.pdf.
26. Ομάδα Εργασίας του Άρθρου 29 για την προστασία των δεδομένων (2016), *Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees).* Βέλγιο: Ομάδα Εργασίας του Άρθρου 29 για την προστασία των δεδομένων. Διαθέσιμο στο: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp237_en.pdf.
27. Ευρωπαϊκή Επιτροπή (2013), *Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο όσον αφορά τη λειτουργία του ασφαλούς λιμένα από τη σκοπιά των πολιτών της Ένωσης και των εταιρειών που είναι εγκατεστημένες στην ΕΕ.* Βέλγιο: Ευρωπαϊκή Επιτροπή. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52013DC0847&from=EN.
28. Ευρωπαϊκή Επιτροπή (2013), *Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο - Αποκατάσταση της εμπιστοσύνης στις ροές δεδομένων μεταξύ της Ευρωπαϊκής Ένωσης και των Ηνωμένων Πολιτειών της Αμερικής.* Βέλγιο: Ευρωπαϊκή Επιτροπή. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52013DC0846&from=GA.
29. Ομάδα εργασίας του άρθρου 29 (1998), *Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules*. Βέλγιο: Ομάδα εργασίας του άρθρου 29. Διαθέσιμο στο: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp195_en.pdf.
30. Ομάδα εργασίας του άρθρου 29 (1998), *Transfers of personal data to third countries : Applying Articles 25 and 26 of the EU data protection directive*. Βέλγιο: Ομάδα εργασίας του άρθρου 29. Διαθέσιμο στο**:** https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1998/wp12_en.pdf.
31. Data Protection Commission (DPC) Ιρλανδίας, «*Transfers of Personal Data to Third Countries or International Organisations*», Διαθέσιμο στο:

https://www.dataprotection.ie/en/organisations/international-transfers/transfers-personal-data-third-countries-or-international-organisations#_msocom_1.
32. Καταγγελία του Maximilian Schrems κατά της Facebook Ireland Ltd. Διαθέσιμη στο: http://www.europe-v-facebook.org/prism/facebook.pdf.
33. Ομοσπονδιακό Γραφείο των ΗΠΑ (Federal Bureau of Investigation - FBI), «*FBI Policies and Procedures for Safeguarding Personal Information as Required by PPD-28 (Signals Intelligence Activities)*». Διαθέσιμο στο: https://www.fbi.gov/file-repository/ppd-28-policies-procedures-signed.pdf/view.
34. Office of The Director of National Intelligence, «Five Eyes Intelligence Oversight and Review Council (Fiorc)». Διαθέσιμο στο: https://www.dni.gov/index.php/ncsc-how-we-work/217-about/organization/icig-pages/2660-icig-fiorc.
35. Συμφωνία ελεύθερων συναλλαγών μεταξύ της Ευρωπαϊκής Ένωσης και των κρατών μελών της, αφενός, και της Δημοκρατίας της Κορέας, αφετέρου, Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=OJ:L:2011:127:FULL&from=EN.
36. Συμφωνία Εμπορίου και Συνεργασίας μεταξύ της Ευρωπαϊκής Ένωσης και της Ευρωπαϊκής Κοινότητας Ατομικής Ενέργειας, αφενός, και του Ηνωμένου Βασιλείου της Μεγάλης Βρετανίας και της Βόρειας Ιρλανδίας, αφετέρου. Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:22021A0430(01)&from=EN.
37. Office of the Director of National Intelligence (ODNI), «IC ON THE RECORD». Διαθέσιμο στο: https://icontherecord.tumblr.com/.
38. Microsoft, «*US National Security Orders Report*». Διαθέσιμο στο: https://www.microsoft.com/en-us/corporate-responsibility/us-national-security-orders-report?activetab=pivot_1:primaryr2.
39. Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, «Διαβιβάσεις δεδομένων εκτός ΕΕ - Αποφάσεις Επάρκειας». Διαθέσιμο στο: https://www.dpa.gr/el/enimerwtiko/thematikes_enotites/diavivaseis_ee/apofaseis_eparkeias.
40. Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, «Διαβιβάσεις δεδομένων εκτός ΕΕ - Δεσμευτικοί Εταιρικοί Κανόνες (BCR)». Διαθέσιμο στο: https://www.dpa.gr/el/enimerwtiko/thematikes_enotites/diavivaseis_ee/bcr.
41. Επίσημη λίστα τρίτων χωρών για τις οποίες έχουν εκδοθεί αποφάσεις επάρκειας της Ευρωπαϊκής Επιτροπής: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.
42. ISO, «FREQUENTLY ASKED QUESTIONS (FAQS) - GLOSSARY». Διαθέσιμο στο: https://www.iso.org/glossary.html.
43. Γραφείου του Επιτρόπου Πληροφοριών του Ηνωμένου Βασιλείου (ICO), *The UK GDPR*. Ηνωμένο Βασίλειο: Information Commissioner's Office. Διαθέσιμο στο: https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-and-the-eu-in-detail/the-uk-gdpr/.
44. Γραφείου του Επιτρόπου Πληροφοριών του Ηνωμένου Βασιλείου (ICO), *International Data Transfer Agreement (IDTA)*. Ηνωμένο Βασίλειο: Information Commissioner's Office. Διαθέσιμο στο: https://ico.org.uk/media/for-organisations/documents/4019538/international-data-transfer-agreement.pdf.
45. Γραφείου του Επιτρόπου Πληροφοριών του Ηνωμένου Βασιλείου (ICO), *International Data Transfer Addendum to the EU Commission Standard Contractual Clauses Addendum)*. Ηνωμένο Βασίλειο: Information Commissioner's Office. Διαθέσιμο στο: https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf.
46. NOYB, «EU-US Transfers Complaint Overview» (η λίστα των 101 καταγγελιών), *noyb.eu*. Διαθέσιμο στο: https://noyb.eu/en/eu-us-transfers-complaint-overview.