ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

**Πρόγραμμα Μεταπτυχιακών Σπουδών**

**«ΔΙΚΑΙΟ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ»**

Ακαδημαϊκό έτος 2021-2022

**ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ**
**της Ναταλίας Λουκαΐτη (Α.Μ. ΜΔΙ 2025)**

# ΔΙΑΒΙΒΑΣΗ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΟ ΠΕΡΙΒΑΛΛΟΝ ΤΟΥ ΥΠΟΛΟΓΙΣΤΙΚΟΥ ΝΕΦΟΥΣ

**Επιβλέπουσα:**

Λίλιαν Μήτρου

Πειραιάς, Μάιος 2022

**ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ**

**Περίληψη**

Αντικείμενο της παρούσας μελέτης αποτελούν τα θέματα της προστασίας προσωπικών δεδομένων που ανακύπτουν κατά τη διασυνοριακή διαβίβασή τους στο περιβάλλον του υπολογιστικού νέφους.

Αρχικά, στο πρώτο κεφάλαιο της παρούσας μελέτης περιγράφεται η αρχιτεκτονική του υπολογιστικού νέφους, δηλαδή τα χαρακτηριστικά του, οι τεχνικές εκδοχές, τα μοντέλα ανάπτυξης, το Ευρωπαϊκό κανονιστικό πλαίσιο ρύθμισής του, καθώς και τα πλεονεκτήματα και μειονεκτήματά του. Γίνεται σύντομη αναφορά επίσης στην ηθική δεοντολογία που πρέπει να διέπει τους παρόχους των υπηρεσιών υπολογιστικού νέφους και τους χρήστες αυτού.

Στη συνέχεια, στο δεύτερο κεφάλαιο αναλύεται το νομικό πλαίσιο των διαβιβάσεων προσωπικών δεδομένων, σύμφωνα με τον Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων 2016/679. Στη συνέχεια, γίνεται αναφορά στο καθεστώς διαβιβάσεων προς το Ηνωμένο Βασίλειο αλλά και προς τις ΗΠΑ. Η ενότητα αυτή καταλήγει με την ανάλυση της από 16.7.2020 απόφασης του Δικαστηρίου της Ευρωπαϊκής Ένωσης 'Schrems II', η οποία αποτελεί θεμέλιο λίθο για τον καθορισμό του πλαισίου των διαβιβάσεων, όταν ο πάροχος των υπηρεσιών «νέφους» είναι εγκατεστημένος εκτός της Ευρωπαϊκής Ένωσης.

Περαιτέρω, στο τρίτο κεφάλαιο εντοπίζονται τα νομικά ζητήματα που ανακύπτουν κατά τη διαβίβαση προσωπικών δεδομένων στο περιβάλλον του υπολογιστικού νέφους, αφού πρώτα εξειδικεύσουμε πότε η διακίνηση δεδομένων αποτελεί «διαβίβαση». Μελετώνται τα θέματα του εδαφικού πεδίου εφαρμογής του ως άνω κανονισμού, τα τεχνικά και οργανωτικά μέτρα που πρέπει να λαμβάνει ο πάροχος των υπηρεσιών αυτών κατά τη διαβίβαση, αλλά και η νόμιμη βάση επεξεργασίας των δεδομένων εντός του «νέφους».

Στο τέταρτο κεφάλαιο αναλύονται τα λοιπά νομικά θέματα που ανακύπτουν κατά τη χρήση των υπηρεσιών του υπολογιστικού νέφους, όπως κατά την επεξεργασία των προσωπικών δεδομένων, ή κατά τον προσδιορισμό του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία των δεδομένων. Άλλα τέτοια θέματα αποτελούν οι ουσιαστικές νομικές υποχρεώσεις του παρόχου των υπηρεσιών αυτών, η ανάκτηση του «απολεσθέντος» ελέγχου των δεδομένων αλλά και η υποχρέωση λογοδοσίας κατά τη διαβίβαση δεδομένων.

Καταλήγοντας, εξάγονται συμπεράσματα σχετικά με την εξωεδαφική εφαρμογή του ΓΚΠΔ καθώς και με το εάν η διαβίβαση προσωπικών δεδομένων στο περιβάλλον του υπολογιστικού νέφους διέπεται από τους κανόνες του Γενικού Κανονισμού Προστασίας Δεδομένων, ακόμη και αν ο πάροχος είναι εγκατεστημένος εκτός της Ευρωπαϊκής Ένωσης.

**1. Εισαγωγή**

Η πληροφορία κατέχει στον σύγχρονο ψηφιακό κόσμο θεμελιώδη ρόλο και έχει καταστεί αντικείμενο συναλλαγής. Τούτο ενισχύεται από την ανάπτυξη της αυτοματοποιημένης επεξεργασίας, η οποία δίνει τη δυνατότητα σε τεράστιες ποσότητες δεδομένων να διακινούνται μέσα σε λίγα δευτερόλεπτα διεθνώς[1]. Ιδιαίτερα μετά την πανδημία της νόσου COVID-19, παρατηρούνται μεγάλες αλλαγές στο τοπίο των διαβιβάσεων δεδομένων. Η πανδημία τις επιτάχυνε και τις αύξησε κατακόρυφα, καθώς η παγκόσμια οικονομία αναγκάστηκε αιφνιδίως να ψηφιοποιηθεί και να προσαρμοστεί στις απαιτήσεις των κυβερνήσεων και των υγειονομικών αρχών.

Το φαινόμενο της παγκόσμιας διακίνησης μεγαδεδομένων εγκυμονεί πολλαπλούς κινδύνους σχετικά με την παραβίαση της ιδιωτικότητας αλλά και την προστασία των προσωπικών δεδομένων των υποκειμένων των δεδομένων. Από την άλλη όμως, η όποια προσπάθεια περιορισμού της διακίνησης των δεδομένων, θα ενέχει τον κίνδυνο της παρεμπόδισης της ελεύθερης διασυνοριακής ροής των μεγαδεδομένων που συλλέγονται, αποθηκεύονται, διακινούνται και τυγχάνουν επεξεργασίας με ταχύτατους ρυθμούς παγκοσμίως. Τέτοιος περιορισμός θα είχε ως αρνητικό αντίκτυπο την πρόκληση δυσλειτουργίας σε πολλούς τομείς της αγοράς, του εμπορίου και της οικονομίας.

Η διακίνηση αυτών των δεδομένων πραγματοποιείται -μεταξύ άλλων- και εντός του υπολογιστικού νέφους, άλλως 'cloud'. Το υπολογιστικό νέφος αποτελεί ένα εικονικό περιβάλλον[2], το οποίο διευκολύνει τους χρήστες/πελάτες του να μην χρησιμοποιούν συσκευές αποθήκευσης και αποκλειστικούς διακομιστές για κάθε εφαρμογή, αφού όλες οι εφαρμογές μπορούν να βρίσκονται «σωσμένες» στο διαδίκτυο και με αυτόν τον τρόπο οι χρήστες του μπορούν να έχουν απομακρυσμένη πρόσβαση ανά πάσα στιγμή. Οι πελάτες του «νέφους» από την άλλη επιδιώκουν την προστασία του απορρήτου τους, των προσωπικών δεδομένων τους, αλλά και της ακεραιότητας και διαθεσιμότητας αυτών, γεγονός που δεν είναι πάντα εφικτό καθώς δεν γνωρίζουν ανά πάσα στιγμή που βρίσκονται αποθηκευμένα τα δεδομένα τους.

Η νεφοϋπολογιστική (cloud computing) αποτελεί την απόλυτη τεχνολογία αιχμής των τελευταίων ετών. Κάποιοι τη θεωρούν ως τη συνέχεια των τεχνολογιών που εξυπηρετούσαν τις υπηρεσίες υπολογιστικής κοινής ωφέλειας (utility computing), ενώ άλλοι την κατατάσσουν στις τεχνολογικές καινοτομίες του σήμερα[3].

Η Ευρωπαϊκή Επιτροπή[4] θέλοντας να δώσει έναν απλοποιημένο ορισμό για τη νεφοϋπολογιστική ορίζει ότι αυτή συνίσταται στην αποθήκευση, επεξεργασία και χρήση των δεδομένων σε απομακρυσμένους υπολογιστές[5], που είναι προσβάσιμοι μέσω του διαδικτύου. Εξηγεί ότι πρακτικά οι χρήστες του υπολογιστικού νέφους μπορούν να ζητούν ανά πάσα στιγμή απεριόριστη υπολογιστική δύναμη, ότι δεν απαιτείται να

---

[1] Κανέλλος Λ., The GDPR Handbook, Νομική Βιβλιοθήκη, 2020, σελ.157

[2] Κίτσος Π./ Παππά Π., *Η προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής στις υπηρεσίες του υπολογιστικού νέφους*, ΔΙΜΕΕ 2012, σελ. 166,

[3] Γνώμη 05/12 σχετικά με την νεφοϋπολογιστική (1.7.2012) της Ομάδας Εργασίας του Άρθρου 29 για την προστασία των δεδομένων

[4] *Unleashing the Potential of Cloud Computing in Europe*, COM(2012), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, διαθέσιμο σε https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF

[5] Ιγγλεζάκης Ι., *Δίκαιο Πληροφορικής*, Γ'έκδοση, Εκδόσεις Σάκκουλα, Αθήνα-Θεσσαλονίκη, 2018, σελ.176

προβαίνουν σε μεγάλες επενδύσεις κεφαλαίων προκειμένου να καλύψουν τις τρέχουσες ανάγκες τους και ότι μπορεί να έχουν πρόσβαση στα δεδομένα τους από οπουδήποτε στον κόσμο, αρκεί να είναι συνδεδεμένοι στο διαδίκτυο. Το υπολογιστικό νέφος λοιπόν καθιστά εφικτή την περικοπή των εξόδων των πελατών του για δαπάνες τεχνολογίας και ταυτόχρονα την ανάπτυξη νέων υπηρεσιών. Χρησιμοποιώντας το υπολογιστικό νέφος, ακόμη και οι μικρές επιχειρήσεις μπορούν να έχουν πρόσβαση σε μεγαλύτερες αγορές, ενώ οι κυβερνήσεις μπορούν να καταστήσουν τα προϊόντα τους πιο ελκυστικά και αποτελεσματικά, μειώνοντας τις δαπάνες τους.

Όλοι μας χρησιμοποιούμε υπηρεσίες νέφους, ακόμη και εν αγνοία μας. Ενδεικτικά αναφέρουμε τις δημοφιλέστερες, ήτοι τα κοινωνικά δίκτυα και το ηλεκτρονικό ταχυδρομείο[6]. Το λογισμικό του παρόχου του ηλεκτρονικού ταχυδρομείου βρίσκεται στο διαδικτυακό «σύννεφο» και ελέγχεται εξ ολοκλήρου από αυτόν, ενώ ο πελάτης του περιορίζεται στη χρήση που επιθυμεί να κάνει, προκειμένου να λαμβάνει για παράδειγμα την ηλεκτρονική αλληλογραφία του. Η ευκολία χρήσης των υπηρεσιών αυτών συνίσταται στο ότι δεν απαιτείται η εγκατάσταση κάποιας εφαρμογής στον προσωπικό μας υπολογιστή αλλά παρέχεται η δυνατότητα πρόσβασης στα προσωπικά μας αρχεία, μέσω οιασδήποτε συσκευής συνδεδεμένης στο διαδίκτυο.

Οι ταχύτητες αλλά και η ευελιξία του υπολογιστικού νέφους[7] ενισχύουν την αδιάλειπτη διαβίβαση δεδομένων, καθώς τα δεδομένα που είναι αποθηκευμένα εντός του «νέφους» βρίσκονται σε διακομιστές διάσπαρτους ανά τον κόσμο ή σε διαφορετικά κέντρα δεδομένων εντός ή εκτός ΕΕ. Οι πάροχοι υπηρεσιών υπολογιστικού νέφους λειτουργούν στην πλειοψηφία τους διασυνοριακά, ως επί το πλείστον εκτός της δικαιοδοσίας της ΕΕ. Για τις υπηρεσίες αυτές, η διαβίβαση δεδομένων αποτελεί τον κανόνα και όχι την εξαίρεση, καθώς είναι πολύ συχνό ένας οργανισμός να χρησιμοποιεί τις υπηρεσίες ενός κέντρου δεδομένων που είναι πολύ μακριά από την έδρα του. Για τον λόγο αυτό, είναι θεμελιώδους σημασίας η διαβίβαση δεδομένων προς χώρες εκτός ΕΕ και ΕΟΧ, η οποία αν περιοριστεί θα έχει αρνητικό αντίκτυπο στις υπηρεσίες της νεφοϋπολογιστικής.

Ως «διασυνοριακή διαβίβαση δεδομένων» καλείται η διαβίβαση ή η μεταφορά προσωπικών δεδομένων με σκοπό την επεξεργασία τους, πέρα από τα εθνικά σύνορα μιας χώρας[8]. Οι διασυνοριακές ροές προσωπικών δεδομένων αφορούν αφενός τη διακίνηση των δεδομένων από και προς χώρες της Ευρωπαϊκής Ένωσης (εφεξής 'ΕΕ') και του Ευρωπαϊκού Οικονομικού Χώρου (εφεξής ΄ΕΟΧ'- Ισλανδία, Νορβηγία, Λιχτενστάιν) και αφετέρου προς χώρες εκτός ΕΕ/ΕΟΧ (εφεξής 'τρίτες χώρες') και προς διεθνείς οργανισμούς. Οι ροές αυτές είναι απαραίτητες για την ενίσχυση του διεθνούς εμπορίου και της διεθνούς συνεργασίας[9]. Ωστόσο η αύξηση των ροών αυτών, δημιουργεί ζητήματα προστασίας προσωπικών δεδομένων.

Κύριο μέλημα των ευρωπαϊκών κρατών κατά τις διαβιβάσεις δεδομένων αποτελεί η διασφάλιση του επιπέδου προστασίας που ορίζει ο Γενικός Κανονισμός Προστασίας

---

[6] Κουσουνή- Πανταζοπούλου Α., *Νομικές διαστάσεις του Cloud Computing*, ΔΙΜΕΕ 2/2012, σελ.1

[7] Κουσουνή- Πανταζοπούλου Α, *Cloud Computing και Νομικά Ζητήματα*, Νομική Βιβλιοθήκη, 2022, σελ.160

[8] Ιγγλεζάκης Ι., *Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (Κανονισμός 2016/679) Εισαγωγή στο νέο νομικό πλαίσιο προστασίας προσωπικών δεδομένων*, Interactive Learning, 2018, 2η έκδοση

[9] Αιτιολογική σκέψη 101 του ΓΚΠΔ, σελ. 19

Προσωπικών Δεδομένων 2016/679 (εφεξής 'ΓΚΠΔ' ή 'Κανονισμός') ή 'General Data Protection Regulation' (αλλιώς 'GDPR'), που ψηφίστηκε στις 27.4.2016 και τέθηκε σε ισχύ στις 25.5.2018. Στην Ελλάδα ενσωματώθηκε με το νόμο 4624/2019. Ο ΓΚΠΔ επιτάσσει ότι η προστασία του συνοδεύει τα δεδομένα ανεξάρτητα από τον τόπο προορισμού τους, και ότι κατά συνέπεια οι κανόνες του εξακολουθούν να ισχύουν μέχρι τον τελικό τους προορισμό προς οιαδήποτε τρίτη χώρα. Ο ΓΚΠΔ παρέχει διαφορετικούς μηχανισμούς που καθορίζουν το πλαίσιο νομιμότητας των διασυνοριακών διαβιβάσεων δεδομένων[10], οι οποίοι θα αναλυθούν κατωτέρω.

Στην παρούσα εργασία θα αναφερθούμε στον ΓΚΠΔ και την εξωεδαφική του εφαρμογή, κυρίως όταν πραγματοποιούνται διαβιβάσεις προσωπικών δεδομένων στις οποίες ο πάροχος υπηρεσιών νεφοϋπολογιστικής βρίσκεται εκτός ΕΕ/ΕΟΧ.

Στο πρώτο κεφάλαιο της παρούσας εργασίας θα μελετήσουμε το φαινόμενο του υπολογιστικού νέφους και ειδικότερα την έννοια, τα χαρακτηριστικά, τις τεχνικές εκδοχές, τα μοντέλα ανάπτυξης, το κανονιστικό πλαίσιο που το ρυθμίζει, τα οφέλη και τα μειονεκτήματά του, και τέλος την ηθική δεοντολογία που πρέπει να διέπει αφενός τους παρόχους υπηρεσιών νεφοϋπολογιστικής και αφετέρου τους πελάτες αυτού.

Στο επόμενο κεφάλαιο θα αναφερθούμε στις διασυνοριακές διαβιβάσεις εντός του υπολογιστικού νέφους, ειδικότερα όταν ο πάροχος των υπηρεσιών αυτών βρίσκεται εκτός ΕΕ/ΕΟΧ. Θα μελετηθεί το προϊσχύσαν αλλά και το ισχύον νομικό πλαίσιο διαβιβάσεων. Περαιτέρω, θα αναλύσουμε τα άρθρα 44-50 του Κεφαλαίου V του ΓΚΠΔ. Το ως άνω κεφάλαιο εφαρμόζεται σε υπεύθυνους επεξεργασίας και σε εκτελούντες την επεξεργασία εντός ΕΕ/ΕΟΧ, οι οποίοι διαβιβάζουν προσωπικά δεδομένα εκτός του εδαφικού πεδίου εφαρμογής του ΓΚΠΔ[11]. Επιγραμματικά θα αναφέρουμε την γενική αρχή ότι οι διαβιβάσεις μεταξύ των χωρών ΕΕ/ΕΟΧ είναι ελεύθερες. Ωστόσο οι διαβιβάσεις σε τρίτες χώρες, είναι αποδεκτές μόνο εφόσον εφαρμόζονται συγκεκριμένοι μηχανισμοί διαβίβασης και εφόσον τηρούνται κάποιες προϋποθέσεις από τον υπεύθυνο επεξεργασίας και από τον εκτελούντα την επεξεργασία, με κοινό σκοπό τη διασφάλιση ενός ικανοποιητικού επιπέδου προστασίας των προσωπικών δεδομένων, όπως επιτάσσει ο ΓΚΠΔ.

Περαιτέρω, θα αναφερθούμε στο ισχύον καθεστώς διαβίβασης προς το Ηνωμένο Βασίλειο αλλά και προς τις ΗΠΑ. Θα γίνει ειδική μνεία στην από 16.7.2020 απόφαση του ΔΕΕ 'Schrems II'.

Τέλος, θα αναλύσουμε τα νομικά ζητήματα που ανακύπτουν κατά τη διαβίβαση προσωπικών δεδομένων στο περιβάλλον του υπολογιστικού νέφους, αλλά και άλλα ζητήματα που άπτονται της επεξεργασίας στο εν λόγω περιβάλλον.

Το μείζον ζήτημα που θα πραγματευτεί η παρούσα εργασία είναι το ζήτημα της εξωεδαφικότητας του ΓΚΠΔ και την κυριαρχία του σε άλλες νομοθεσίες. Χωρεί η εφαρμογή του σε επεξεργασία και διαβιβάσεις προσωπικών δεδομένων όταν ο πάροχος υπηρεσιών νεφοϋπολογιστικής βρίσκεται εκτός ΕΕ;

\

[10] Κανέλλος Λ. *The GDPR Handbook*, Νομική Βιβλιοθήκη, 2020, σελ.157

[11] Λωσταράκου Κ., *Διεθνείς διαβιβάσεις δεδομένων υπό τον νέο Κανονισμό*, δημοσιευμένο στο βιβλίο «Γενικός Κανονισμός για την προστασία των προσωπκών δεδομένων (GDPR) Νομική διάσταση και πρακτική εφαρμογή», 2η έκδοση, Νομική Βιβλιοθήκη, 2020, σελ.356

## 2. Το υπολογιστικό νέφος

### 2.1 Ορισμός και χαρακτηριστικά

Ο πιο πλήρης ορισμός του «υπολογιστικού νέφους» έχει διατυπωθεί από το Εθνικό Ίδρυμα Προτύπων και Τεχνολογίας των ΗΠΑ (U.S National Institute of Standard and Technology, NIST), και είναι ο εξής: «*Υπολογιστικό νέφος*[12] *είναι ένα μοντέλο, το οποίο παρέχει τη δυνατότητα ευχερούς, βασισμένης στη ζήτηση διαδικτυακής πρόσβασης σε ένα διαμοιραζόμενο χώρο (πχ. δίκτυα, εξυπηρετητές, αποθήκευση, εφαρμογές και υπηρεσίες) και το οποίο μπορεί να παρασχεθεί και να αποδεσμευτεί ταχέως με ελάχιστη διαχειριστική προσπάθεια ή αλληλεπίδραση με τον πάροχο της υπηρεσίας*».

Εκ των ανωτέρω συνάγουμε ότι τα βασικά χαρακτηριστικά του υπολογιστικού νέφους είναι τα εξής πέντε[13]:

α) η ευρεία διαδικτυακή πρόσβαση,

β) η υπολογιζόμενη και παρεχόμενη, βάσει της ζήτησης υπηρεσία (on demand), η οποία εξυπηρετεί την κοστολόγηση του χρήστη κατ'επιλογή, ανάλογα με τις εκάστοτε ανάγκες του, δίνοντάς του τη δυνατότητα της μη εγκατάστασης εφαρμογών τοπικά στον υπολογιστή του[14]

γ) η συγκέντρωση πόρων (resource pooling). Οι πόροι του παρόχου (π.χ αποθηκευτικός χώρος, μνήμη, δίκτυα) εξυπηρετούν ταυτόχρονα πολλούς χρήστες και έτσι διευκολύνεται η αξιοποίηση τεράστιου όγκου εξυπηρετητών με πολλούς χιλιάδες ηλεκτρονικούς υπολογιστές. Οι υλικοί και εικονικοί αυτοί πόροι εκχωρούνται ξανά και ξανά ανάλογα με τις ανάγκες των χρηστών.

δ) η ταχεία ελαστικότητα, που σημαίνει ότι δίνεται η δυνατότητα στον πελάτη να χρησιμοποιεί συγκεκριμένο όγκο π.χ αποθηκευτικού χώρου και να προσαρμόζει την έκταση της χρήσης των υπηρεσιών αυτών ανάλογα με τις ανάγκες του, απολαμβάνοντας ταυτόχρονα συγκεκριμένα οικονομικά οφέλη

ε) η ευέλικτη και ανεξάρτητη από την τοποθεσία του χρήστη πρόσβαση στους υπολογιστικούς αυτούς πόρους, που δύνανται να διαμοιράζονται προκειμένου να είναι προσβάσιμοι σε πολλαπλούς πελάτες ταυτόχρονα.

Ο όρος «cloud computing» δεν χαρακτηρίζει συγκεκριμένο είδος υπηρεσιών, αλλά τον τρόπο με τον οποίο αυτές δημιουργούνται, αφού οι υπηρεσίες και οι εφαρμογές διατίθενται αποκεντρωμένα μέσω του διαδικτύου, δηλαδή μέσα από το «σύννεφο»[15].

Το υπολογιστικό νέφος συνίσταται από μια σειρά από τεχνολογίες και υπηρεσίες που έχουν κοινό παρονομαστή τη χρήση του διαδικτύου και την παροχή εφαρμογών τεχνολογιών πληροφορικής και επικοινωνιών[16] (εφεξής 'ΤΠΕ'). Παρέχει τη δυνατότητα επεξεργασίας και αποθήκευσης δεδομένων, την παροχή μνήμης αλλά και τη δικτύωση. Συνδράμει επίσης στην ανάπτυξη υπολογιστικών πόρων (υλικό/λογισμικό) σε διάφορους τομείς της οικονομίας, αλλά και σε διαφορετικά γεωγραφικά πλάτη.

---

[12] P. Mell/ T.Grance, *The NIST Definition of Cloud Computing*, National Institute of Standards and Technology, 2009, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[13] Μήτρου Λ., *Προστασία προσωπικών δεδομένων και υπολογιστικό νέφος*, ΔΙΜΕ Ε, τ.4/2015, σελ.535

[14]Κουσουνή- Πανταζοπούλου Α., *Νομικές διαστάσεις του Cloud Computing*, ΔΙΜΕΕ 2/2012, σελ.1

[15] Κουσουνή- Πανταζοπούλου Α., *Νομικές διαστάσεις του Cloud Computing*, ΔΙΜΕΕ 2/2012, σελ.1

[16] Μήτρου Λ., *Προστασία προσωπικών δεδομένων και υπολογιστικό νέφος*, ΔΙΜΕΕ, τ.4/2015, σελ.534

Οι πάροχοι των υπηρεσιών νεφοϋπολογιστικής παρέχουν ευρεία γκάμα υπηρεσιών[17], οι οποίες συνίστανται σε συστήματα εικονικής επεξεργασίας, αλλά και σε υπηρεσίες που σχετίζονται με την ανάπτυξη εφαρμογών, τη δυνατότητα φιλοξενίας καθώς και διαδικτυακές λύσεις λογισμικού, οι οποίες ενίοτε αντικαθιστούν τις συμβατικές εφαρμογές που εγκαθίστανται στους προσωπικούς υπολογιστές των χρηστών. Τέτοιες είναι οι εφαρμογές επεξεργασίας κειμένων, οι ατζέντες και τα ημερολόγια, τα συστήματα αρχειοθέτησης και διαδικτυακής αποθήκευσης εγγράφων, αλλά και οι υπηρεσίες ηλεκτρονικού ταχυδρομείου που διατίθενται από τρίτους.

Στο υπολογιστικό νέφος γίνεται εκτεταμένη χρήση εικονικού υλικού (virtual hardware)[18], υπό την έννοια ότι ένας φυσικός εξυπηρετητής μπορεί να διαθέτει έναν ή και περισσότερους του ενός εικονικούς εξυπηρετητές (virtual servers), οι οποίοι διαμοιράζονται στους διαθέσιμους φυσικούς πόρους. Με τον τρόπο αυτόν διευκολύνεται η λελογισμένη χρήση των φυσικών πόρων και επιτρέπεται η μεταφορά του εικονικού εξυπηρετητή σε κάποιον φυσικό εξυπηρετητή σε περίπτωση φυσικής βλάβης. Έτσι διευκολύνονται η δημιουργία αντιγράφων και υποδομών μεγάλης διαθεσιμότητας, αλλά και η επεκτασιμότητα.

**2.2. Τεχνικές εκδοχές**

Οι πάροχοι των υπηρεσιών νέφους παρέχουν τις υπηρεσίες αυτές με διαφορετικούς τρόπους προκειμένου να καλύψουν τις διαφορετικές ανάγκες όλων των πελατών τους. Ως «υπηρεσία» στο περιβάλλον του «νέφους»[19] νοείται η δυνατότητα να επαναχρησιμοποιηθούν οι ίδιοι πόροι του δικτύου ενός παρόχου, και αυτό καλείται 'as a service'.

Οι τεχνικές εκδοχές του cloud[20], δηλαδή η διάκρισή του με βάση το είδος της παρεχόμενης υπηρεσίας[21], είναι οι εξής τέσσερις:

i) Υποδομή ως υπηρεσία (infrastructure-as-a service- Iaas). Στο μοντέλο αυτό ο πάροχος εκμισθώνει στον πελάτη του μια υπολογιστική δομή εικονικών εξυπηρετητών. Μπορεί να του παρέχει υπολογιστική ισχύ, υπολογιστική αποθήκευση (hosting), χρήση εξυπηρετητή (server), χρήση κέντρου δεδομένων (data center) και υπολογιστικό δίκτυο (network)[22]. Στην περίπτωση αυτή ο πάροχος εξασφαλίζει τη συνεχή λειτουργία των συστημάτων, ενώ ο πελάτης ευθύνεται για την εγκατάσταση και ρύθμιση του λογισμικού, τη συντήρηση και παρακολούθησή του αλλά και τη δημιουργία αντιγράφων ασφαλείας. Τέτοια υπηρεσία είναι η Amazon Elastic Cloud Computing[23] και συνήθως

---

[17] Γνώμη 05/12 σχετικά με την νεφοϋπολογιστική (1.7.2012) της Ομάδας Εργασίας του Άρθρου 29 για την προστασία των δεδομένων, Εισαγωγή

[18] Παπαδόπουλος Μ., Ευγενίδης Π., *Νεφοϋπολογιστική (cloud computing) και προστασία προσωπικών δεδομένων*, ΔΙΜΕΕ 2/2016, σελ.1

[19] Κουσουνή-Πανταζοπούλου Α., *Cloud Computing & νομικά ζητήματα*, Νομική βιβλιοθήκη, 2022 σελ.10,

[20] Μήτρου Λ., Προστασία προσωπικών δεδομένων και υπολογιστικό νέφος, ΔΙΜΕΕ, τ.4/2015, σελ.535

[21] Παντελιάς Ι., Διπλωματική εργασία με θέμα «Νομικά ζητήματα συμφωνιών επιπέδου υπηρεσιών σε συμβάσεις αποθήκευσης ψηφιακών δεδομένων σε υπολογιστικό νέφος (cloud SLAs) στην Ευρώπη, Πανεπιστήμιο Πειραιώς,2018, σελ.10

[22]Παπαδόπουλος Μ., Ευγενίδης Π., Νεφοϋπολογιστική (cloud computing) και προστασία προσωπικών δεδομένων, ΔΙΜΕΕ 2/2016, σελ.1

[23] Κουσουνή- Πανταζοπούλου Α., *Νομικές διαστάσεις του Cloud Computing*, ΔΙΜΕΕ 2/2012, σελ.3

τέτοιες υπηρεσίες αφορούν κυρίως επιχειρήσεις, οι οποίες επιλέγουν το λειτουργικό τους σύστημα, αλλά και το περιβάλλον που διατίθεται.
ii) Πλατφόρμα ως υπηρεσία (platform-as-a-service- PaaS) ή άλλως γνωστή ως πλατφόρμα νέφους[24]. Στην περίπτωση αυτή ο πάροχος παρέχει μια πλατφόρμα υπολογιστικών εφαρμογών, δηλαδή εργαλεία για την κατασκευή και φιλοξενία εξατομικευμένων δικτυακών εφαρμογών και υπηρεσιών του πελάτη στο νέφος. Την ευθύνη για το λογισμικό την έχει ο πελάτης, ενώ ο πάροχος φροντίζει για την συνεχή και ορθή λειτουργία της πλατφόρμας, καθώς και τη συντήρηση αυτής. Στοιχεία αυτής της υπηρεσίας διαθέτει η Windows Azure Platform της Microsoft και η salesforce[25]. Οι υπηρεσίες αυτές αφορούν κυρίως παραγωγούς λογισμικών, οι οποίοι ελέγχουν τις εφαρμογές και το υπολογιστικό περιβάλλον τους, ενώ μέτρα ασφαλείας λαμβάνουν αμφότεροι οι πάροχοι και οι χρήστες του «νέφους».
iii) Λογισμικό ως υπηρεσία (software-as-a-service-SaaS). Πρόκειται για μοντέλο παροχής λογισμικού στον πελάτη, το οποίο ο πάροχος το μισθώνει σαν υπηρεσία και έτσι δεν χρειάζεται να το αγοράσει ο πελάτης και να το εγκαταστήσει στον υπολογιστή του. Σε αυτό το μοντέλο υπολογιστικού νέφους υπάγεται το ηλεκτρονικό ταχυδρομείο, ενώ στοιχεία αυτής της υπηρεσίας διαθέτουν οι Google (πχ. Google docs) ή το μοντέλο iWork.com της Apple[26].
iv) Δεδομένα ως υπηρεσία» (data-as-a-service)[27]. Πρόκειται για την πιο νέα εκδοχή του υπολογιστικού νέφους, η οποία προσομοιάζει με την SaaS και έχει ως στόχο τη συσχέτιση δεδομένων καταναλωτών που βρίσκονται διασκορπισμένα στο διαδίκτυο. Ο πελάτης δεν χρειάζεται να αγοράσει κάποια βάση δεδομένων καταναλωτών, και να επιβαρυνθεί με τα έξοδα δημιουργίας και διαχείρισής αυτής, αλλά στην ουσία ο πάροχος του εκμισθώνει τα ίδια τα δεδομένα. Έτσι, παρέχεται στον πελάτη μια υπηρεσία οικονομική και ευέλικτη, η οποία εστιάζει στην πώληση προϊόντων ή υπηρεσιών μέσω διαδικτύου, ίδιων με τα δικά του.

### 2.3. Μοντέλα ανάπτυξης

Το υπολογιστικό νέφος αναπτύσσεται και εφαρμόζεται με τους κάτωθι τρόπους:
i) Δημόσιο Νέφος: πρόκειται για το νέφος που έχει υποδομή διαθέσιμη στο ευρύ κοινό, είτε πρόκειται για παροχή υπηρεσιών σε εταιρίες, κυβερνήσεις είτε σε μεμονωμένους πελάτες/επιχειρήσεις[28]. Μπορεί, ενδεικτικά, να το διαχειρίζεται μέλος της ακαδημαϊκής κοινότητας[29], οργανισμός τοπικής αυτοδιοίκησης, νομικό πρόσωπο δημοσίου ή ιδιωτικού φορέα. Κάνει χρήση υπολογιστικών πόρων που υπάρχουν στον τόπο εγκατάστασης του παρόχου. Με αυτό το μοντέλο λειτουργούν οι google apps, amazon και windows azure[30].

---

[24] Κουσουνή- Πανταζοπούλου Α., *Νομικές διαστάσεις του Cloud Computing*, ΔΙΜΕΕ 2/2012, σελ.2
[25] Κουσουνή- Πανταζοπούλου Α., *Νομικές διαστάσεις του Cloud Computing*, ΔΙΜΕΕ 2/2012, σελ.2
[26] Κουσουνή- Πανταζοπούλου Α., *Νομικές διαστάσεις του Cloud Computing*, ΔΙΜΕΕ 2/2012, σελ.2
[27] Κουσουνή- Πανταζοπούλου Α., Cloud Computing & νομικά ζητήματα, Νομική Βιβλιοθήκη, 2022, σελ.17,
[28] Μήτρου Λ., *Προστασία προσωπικών δεδομένων και υπολογιστικό νέφος,* ΔΙΜΕΕ, τ.4/2015, σελ.535
[29] Παπαδόπουλος Μ., Ευγενίδης Π., *Νεφοϋπολογιστική (cloud computing) και προστασία προσωπικών δεδομένων*, ΔΙΜΕΕ 2/2016, σελ.7
[30] Κουσουνή- Πανταζοπούλου Α., *Νομικές διαστάσεις του Cloud Computing*, ΔΙΜΕΕ 2/2012, σελ.3

Χαρακτηριστικό του είναι ότι δεν λειτουργεί με συγκεκριμένες συμφωνίες επιπέδου υπηρεσιών και δεν αφήνει ικανοποιητικά ίχνη ελέγχου της δραστηριότητας του πελάτη[31].
ii) Ιδιωτικό Νέφος: πρόκειται για το νέφος που λειτουργεί μόνον για έναν φορέα, δηλαδή είναι δίκτυο ιδιόκτητο, το οποίο απευθύνεται σε συγκεκριμένο κύκλο προσώπων. Χαρακτηριστικό παράδειγμα ιδιωτικού νέφους αποτελεί το ebay[32]. Συνήθως το ιδιωτικό νέφος το διαχειρίζεται ο ίδιος ο οργανισμός ή τρίτο μέρος και υφίσταται (τοπικά) εντός του οργανισμού, οπότε ελέγχεται από αυτόν και τα δεδομένα παραμένουν συνεχώς στο «νέφος». Αυτό εξασφαλίζει μεγαλύτερη προστασία ασφάλειας και απορρήτου των επικοινωνιών αλλά δεν εξυπηρετεί τόσο σε επίπεδο αποτελεσματικότητας ή μείωσης κόστους.
iii) Νέφος κοινότητας: Πρόκειται για το νέφος το οποίο διαμοιράζεται ανάμεσα σε περισσότερους φορείς και αφορά μια συγκεκριμένη κοινότητα που διατηρεί κοινά ενδιαφέροντα. Μπορεί να διατηρείται είτε από τον οργανισμό ή από τρίτο, τοπικά ή και εκτός του οργανισμού.
iv) Υβριδικό Νέφος: Πρόκειται για τη μορφή νέφους που συνδυάζει στοιχεία δύο ή περισσότερων εκ των ως άνω ειδών νεφών, τα οποία ωστόσο παραμένουν ανεξάρτητα μεταξύ τους αλλά επιτρέπουν τη φορητότητα δεδομένων και εφαρμογών, χάρη στην τεχνολογία που εφαρμόζουν.

### 2.4. Κανονιστικό Πλαίσιο

Πλήθος κειμένων μαλακού δικαίου καλούνται να ρυθμίσουν το πλαίσιο λειτουργίας του υπολογιστικού νέφους. Τα παρακάτω κείμενα ρυθμίζουν, είτε σε διεθνές είτε σε ευρωπαϊκό επίπεδο, την αγορά του υπολογιστικού νέφους. Εξ αυτών, οι κώδικες δεοντολογίας αποτελούν ίσως την πιο κλασική μορφή αυτορρύθμισης[33]. Πρόκειται για «κανόνες» αυτοδέσμευσης των διαφόρων παρόχων υπηρεσιών νεφοϋπολογιστικής για ασφαλή χρήση των υπηρεσιών τους στο διαδίκτυο. Παρατηρείται λοιπόν πολυκεντρισμός του δικαίου. Οι νέοι αυτοί φορείς κανονιστικής δράσης συντονίζουν την δραστηριότητα του υπολογιστικού νέφους και διαχέουν τις ρυθμίσεις που παράγουν, στα κράτη τα οποία έχουν προσχωρήσει σε αυτές[34]. Είναι απαραίτητο να διευκρινιστεί ότι οι ως άνω συστάσεις δεν αποτελούν τυπικούς νόμους και ως εκ τούτου δεν αποτελούν δεσμευτικά κείμενα για τα συμβαλλόμενα κράτη μέλη, ωστόσο προτείνουν κοινές ρυθμίσεις, οι οποίες καθιστούν το ισχύον ρυθμιστικό πλαίσιο για τη λειτουργία του υπολογιστικού νέφους.
Ενδεικτικά, τέτοια κανονιστικά κείμενα είναι τα παρακάτω:

#### 2.4.1. Κώδικας Δεοντολογίας της ΕΕ για το Cloud (EU Cloud of Conduct)

Ο Κώδικας Δεοντολογίας της ΕΕ για το Cloud[35] θεσπίστηκε το Φεβρουάριο του 2017, μετά από τέσσερα χρόνια στενής συνεργασίας μεταξύ της Ευρωπαϊκής Επιτροπής

---

[31] Κουσουνή- Πανταζοπούλου Α., *Νομικές διαστάσεις του Cloud Computing*, ΔΙΜΕΕ 2/2012, σελ.3
[32] Κουσουνή- Πανταζοπούλου Α., *Νομικές διαστάσεις του Cloud Computing*, ΔΙΜΕΕ 2/2012, σελ.3
[33] Μήτρου Λ., *(Αυτορ)ρύθμιση στον κυβερνοχώρο;*, στο βιβλίο Αυτορρύθμιση, Θ.Κ.Παπαχρίστου, Χ.Βερναρδάκης, Γ.Θεοδόσης, Ιφ.Καμτσίδου, Κ.Μανωλάκου, Λ.Μήτρου, Β. Παπακωνσταντίνου, Ε.Ρεθυμιωτάκη, Κ.Στρατηλάτης, Γ. Τασόπουλος, σελ. 83, Εκδόσεις Σάκκουλα, 2005
[34] Ε. Ρεθυμιωτάκη, *Πηγές του δικαίου και νομικός πλουραλισμός στην ΕΕ*, Αθήνα-Θεσσαλονίκη, Εκδόσεις Σάκκουλα, 2012, σελ. 133
[35] https://eucoc.cloud/en/about/about-eu-cloud-coc/

και των μελών της κοινότητας του υπολογιστικού νέφους. Τον Μάιο του 2021 εγκρίθηκε από τη Βελγική Αρχή Προστασίας Δεδομένων[36], κατόπιν θετικής γνώμης του Ευρωπαϊκού Συμβουλίου Προστασίας Προσωπικών Δεδομένων (εφεξής ΈΣΠΔ'). Ήδη πριν την επίσημη ενσωμάτωσή του από τις εποπτικές αρχές των λοιπών ευρωπαϊκών χωρών, η Scope, η οποία αποτελεί το εποπτικό της συμμόρφωσης των παρόχων υπηρεσιών cloud του με τον ΓΚΠΔ, επέτρεψε στους παρόχους να προσχωρήσουν σε αυτόν, κατόπιν υποβολής τους σε προσωρινές διαδικασίες αυτοαξιολόγησης.

Οι Κώδικες Δεοντολογίας προβλέπονται για τον έλεγχο της συμμόρφωσης κάποιου φορέα με τον ΓΚΠΔ (άρθρο 40 ΓΚΠΔ). Η πιστοποίηση των μελών που έχουν αποδεχτεί τους κώδικες δεοντολογίας είναι εθελοντική. Ο συγκεκριμένος κώδικας θεσπίστηκε προκειμένου να καλλιεργηθεί ένα περιβάλλον εμπιστοσύνης και διαφάνειας στην αγορά του υπολογιστικού νέφους, έτσι ώστε να απλοποιηθεί η διαδικασία εκτίμησης ρίσκου των πελατών του έναντι των παρόχων τους. Ωστόσο, σε καμία περίπτωση αυτός ο κώδικας δεν υποκαθιστά τη σύμβαση παροχής υπηρεσιών νέφους (cloud services agreement) που πρέπει να υπογραφεί μεταξύ του παρόχου των υπηρεσιών αυτών και του καταναλωτή, η οποία πρέπει να αναφέρει αναλυτικά τη συμφωνία των μερών, την επεξεργασία που θα λάβει χώρα, τη φύση και τον σκοπό αυτής, το είδος των προσωπικών δεδομένων που θα υποστούν επεξεργασία, την ταυτότητα των υποκειμένων των δεδομένων και τέλος τις υποχρεώσεις και τα δικαιώματα του εκτελούντος την επεξεργασία.

Ο ως άνω Κώδικας αποτελεί τον πρώτο διακρατικό κώδικα δεοντολογίας από την εφαρμογή του ΓΚΠΔ. Παρέχει καθοδήγηση σχετικά με τις απαιτήσεις τις οποίες πρέπει να πληρούν οι εκτελούντες την επεξεργασία. Το πεδίο εφαρμογής του είναι σχετικά περιορισμένο καθώς απευθύνεται μόνο σε εκτελούντες επεξεργασία. Άρα δεν αφορά δραστηριότητες επιχειρήσεων προς καταναλωτές (B2C -Business to Consumer) ή επεξεργασία, κατά την οποία ο πάροχος υπηρεσιών νέφους δρα ως υπεύθυνος επεξεργασίας. Επιπρόσθετα, δεν επιτρέπει διεθνείς διαβιβάσεις δεδομένων σύμφωνα με το άρθρο 46(2) του ΓΚΠΔ. Εξασφαλίζει στους πελάτες του ότι οι πάροχοι των υπηρεσιών νέφους τηρούν τις απαιτήσεις του ΓΚΠΔ και ότι εφαρμόζουν ως εκτελούντες την επεξεργασία τα τεχνικά και οργανωτικά μέτρα που αυτός ορίζει. Καλύπτει όλες ανεξαιρέτως τις υπηρεσίες υπολογιστικού νέφους (SaaS, IaaS, PaaS). Προβλέπει ανεξάρτητο σύστημα διαχείρισης των θεμάτων συμμόρφωσης με τον ΓΚΠΔ, και ως όργανο παρακολούθησης το 'Scope Europe', το οποίο επιτηρεί αφενός εάν είναι προσήκουσα η παροχή των υπηρεσιών cloud από τους παρόχους που τον έχουν προσυπογράψει, και αφετέρου τη λειτουργία των υπηρεσιών που αναφέρονται σε αυτόν.

Συνοψίζοντας, ο βασικός στόχος του συγκεκριμένου Κώδικα είναι να συγκεκριμενοποιήσει τις απαιτήσεις του άρθρου 28 του ΓΚΠΔ. Παρέχει πρακτική καθοδήγηση και μια σειρά από δεσμευτικές απαιτήσεις (όπως συστάσεις για τους εκτελούντες επεξεργασία, το δικαίωμα ελέγχου, συμμόρφωση ως προς τα δικαιώματα του υποκειμένου, διαφάνεια και λογοδοσία), καθώς και στόχευση προκειμένου να διευκολυνθούν οι πάροχοι να συμμορφωθούν με το άρθρο 28 του ΓΚΠΔ.

[36] https://eucoc.cloud/en/about/about-eu-cloud-coc/

### 2.4.2. Κώδικας Συμπεριφοράς Προστασίας Δεδομένων της CISPE (CISPE Code)[37]

Ο ως άνω κώδικας εγκρίθηκε από το ΕΣΠΔ και την Γαλλική Αρχή Προστασίας Δεδομένων (CNIL), δυνάμει των άρθρων 40 και 41 του ΓΚΠΔ. Απευθύνεται ειδικά στους παρόχους υπηρεσιών υπολογιστικού νέφους στην Ευρώπη και συγκεκριμένα στους παρόχους υπηρεσιών IaaS. Έχει εφαρμογή μόνο στην παροχή υπηρεσιών Cloud από επιχειρήσεις σε επιχειρήσεις (B2B- Business to business), κατά τις οποίες ο πάροχος υπηρεσιών νέφους ενεργεί ως εκτελών επεξεργασία, σύμφωνα με το άρθρο 28 του ΓΚΠΔ.

Σκοπός του παρόντος κώδικα είναι να παρέχει ένα αυτορρυθμιστικό μοντέλο για τους παρόχους υπηρεσιών IaaS, που να είναι συμβατό με το ευρωπαϊκό πλαίσιο προστασίας προσωπικών δεδομένων. Με την αποδοχή του από τους ως άνω παρόχους υπηρεσιών νεφοϋπολογιστικής, αυτοί δεσμεύονται ότι θα χρησιμοποιούν τα προσωπικά δεδομένα των πελατών τους με συμβατικό τρόπο, και ότι θα τα αποθηκεύουν και θα τα επεξεργάζονται εντός της ΕΕ.

### 2.4.3. Κατευθυντήριες αρχές ΟΟΣΑ

Οι κατευθυντήριες γραμμές του Οργανισμού Οικονομικής Συνεργασίας και Ανάπτυξης (εφεξής 'ΟΟΣΑ') για την προστασία της ιδιωτικότητας και των προσωπικών δεδομένων, οι οποίες διατυπώθηκαν το 1980 και αναθεωρήθηκαν το 2013[38], σκιαγραφούν εννέα βασικές αρχές που πρέπει να τηρούνται κατά τη συλλογή και την επεξεργασία προσωπικών δεδομένων στο περιβάλλον της νεφοϋπολογιστικής.

Οι αρχές αυτές είναι οι εξής: α) η αρχή του σκοπού, β) ο προσδιορισμός του σκοπού της συλλογής των δεδομένων κατά τον χρόνο της συλλογής τους, γ) η χρήση των δεδομένων να γίνεται για τον σκοπό για τον οποίο συλλέχθηκαν, δ) να είναι κατάλληλα, αληθή, πλήρη και επικαιροποιημένα, ε) να χαίρουν προστασίας μέσω της υιοθέτησης κατάλληλων μέτρων προστασίας έναντι κινδύνων απώλειας, μη εξουσιοδοτημένης χρήσης ή πρόσβασης, κοινοποίησης σε τρίτους, καταστροφής ή αλλοίωσής τους, στ) να υπάρχει πολιτική διαφάνειας ως προς τη διαχείρισή τους, ζ) να δίνεται η δυνατότητα στο υποκείμενο των δεδομένων να έχει πρόσβαση σε αυτά, και να ασκεί τυχόν δικαιώματά του που απορρέουν από αυτά, η) να επιβάλλεται υποχρέωση λογοδοσίας στους υπεύθυνους επεξεργασίας έναντι των υποκειμένων των δεδομένων και θ) να αποκλείεται η διαβίβαση των δεδομένων από μια δικαιοδοσία σε άλλη, εφόσον η δεύτερη δεν παρέχει ισόβαθμο πλέγμα προστασίας τους.

### 2.4.4 Συστάσεις από την Γαλλική Αρχή Προστασίας Δεδομένων

Η Γαλλική Αρχή Προστασίας Δεδομένων (CNIL) εξέδωσε το 2012 συστάσεις[39] για τις γαλλικές εταιρίες που πρόκειται να χρησιμοποιήσουν υπηρεσίες νέφους, καθώς θεωρεί ότι η χρήση αυτών των υπηρεσιών εγκυμονεί κινδύνους ως προς τη συμμόρφωση με τον ΓΚΠΔ, ειδικά όταν μιλάμε για το δημόσιο σύννεφο. Οι δυσκολίες αυτές οξύνονται στην περίπτωση των τυποποιημένων συμβάσεων, οι οποίες δεν παρέχουν στους πελάτες

---

[37] https://www.codeofconduct.cloud/wp-content/uploads/2022/01/CISPE-Cloud-Data-Protection-Code-of-Conduct-DIGITAL.pdf

[38] Revised guidelines on the protection of privacy and transborder flows of personal data, διαθέσιμο σε https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[39] https://www.cnil.fr/sites/default/files/typo/document/Recommendations_for_companies_planning_to_use_Cloud_computing_services.pdf

περιθώριο διαπραγμάτευσης. Έχει διαπιστωθεί ότι οι συμβάσεις αυτές στερούνται διαφάνειας εκ μέρους των παρόχων υπηρεσιών νέφους ως προς τις υπηρεσίες που παρέχονται, συγκεκριμένα σε επίπεδο ασφάλειας και διαβίβασης των δεδομένων των πελατών σε τρίτες χώρες.

Κατά συνέπεια, η CNIL θεωρεί απαραίτητο για κάθε γαλλική εταιρία που πρόκειται να χρησιμοποιήσει υπηρεσίες νέφους να προβεί προηγουμένως σε εκτίμηση ρίσκου και να κάνει αυστηρή επιλογή παρόχου νέφους. Θα πρέπει να λάβει υπόψη της τις εγγυήσεις που της παρέχει ο κάθε πάροχος σχετικά με την προστασία των προσωπικών δεδομένων και να διασφαλίζει ότι αυτός θα της παρέχει όλα τα εχέγγυα για να εκπληρώνει τις υποχρεώσεις της, συγκεκριμένα σε επίπεδο ενημέρωσης των υποκειμένων των δεδομένων, ρύθμισης των διασυνοριακών διαβιβάσεων και ασφάλειας των δεδομένων.

Η CNIL κρίνει απαραίτητες τις κάτωθι πέντε συστάσεις όταν γίνεται χρήση υπηρεσιών υπολογιστικού νέφους, δηλαδή: 1) την ταυτοποίηση των προσωπικών δεδομένων που θα υποστούν επεξεργασία, καθώς και των διαδικασιών επεξεργασίας που θα γίνουν στο «νέφος», 2) τον σαφή ορισμό των απαιτήσεων του πελάτη ως προς τα τεχνικά μέτρα ασφάλειας που θα ληφθούν και τη νομική προστασία του, 3) τη διεξαγωγή ανάλυσης ρίσκου προκειμένου να διαπιστωθούν τα απαραίτητα μέτρα ασφάλειας για τον πελάτη, 4) την επιλογή μεταξύ των κατάλληλων υπηρεσιών νέφους που παρέχονται για κάθε επεξεργασία και 5) την επιλογή παρόχου υπηρεσιών νέφους, ο οποίος θα προσφέρει επαρκείς εγγυήσεις.

**2.5. Οφέλη και μειονεκτήματα**

Τα οφέλη του υπολογιστικού νέφους είναι πολλαπλά και πρωτίστως οικονομικά. Οι υπηρεσίες υπολογιστικού νέφους διευκολύνουν τη δημιουργία οικονομιών κλίμακος[40], δηλαδή οικονομικά μοντέλα που επιτυγχάνουν μείωση του συνολικού κόστους και ταυτόχρονα αύξηση της παραγωγής. Μπορούν να καταστούν χρήσιμες και για τις μικρομεσαίες επιχειρήσεις, αφού τους δίνεται η δυνατότητα να εξασφαλίσουν μικρό κόστος πρόσβασης σε τεχνολογικούς πόρους στο διαδίκτυο, οι οποίοι θα ήταν απροσπέλαστοι διαφορετικά.

Το υπολογιστικό νέφος μειώνει το λειτουργικό κόστος μιας επιχείρησης ή ενός δημόσιου ή ιδιωτικού φορέα, όσον αφορά τη χρήση των πληροφοριακών συστημάτων και υποδομών. Παρέχει τη δυνατότητα διαμόρφωσης των πληροφοριακών πόρων του κάθε οργανισμού, με γνώμονα τις εκάστοτε ανάγκες του, με συνέπεια να χρεώνεται με βάση την εκάστοτε κατανάλωσή του. Χάρη στις υπηρεσίες νέφους, οι χρήστες/επιχειρήσεις δεν χρειάζεται να αγοράζουν λογισμικά ή να συντηρούν ακριβούς εξυπηρετητές και εγκαταστάσεις αποθήκευσης δεδομένων, ούτε να συντηρούν γραφεία ή προσωπικό για να υποστηρίξουν τις υπηρεσίες αυτές πληροφορικής.

Το υπολογιστικό νέφος παρέχει και ελαστικότητα, υπό την έννοια ότι η εκάστοτε επιχείρηση δεν επενδύει μεν χρήματα και ανθρώπινο δυναμικό για την απόκτηση, εγκατάσταση και λειτουργία λογισμικών και εν γένει συστημάτων πληροφορικής, τα οποία της προσφέρονται μέσα από το «σύννεφο», αλλά παράλληλα απολαμβάνει ποιότητα και ευχερή πρόσβαση στα δεδομένα της[41]. Και σε επίπεδο αποδοτικότητας έχει

[40]Παπαδόπουλος Μ., Ευγενίδης Π.,, *Νεφοϋπολογιστική (cloud computing) και προστασία προσωπικών δεδομένων*, ΔΙΜΕΕ 2/2016, σελ.7

[41] Κουσουνή- Πανταζοπούλου Α., *Νομικές διαστάσεις του Cloud Computing*, ΔΙΜΕΕ 2/2012, σελ.2

ευεργετικά αποτελέσματα το υπολογιστικό νέφος καθώς οι επιχειρήσεις μπορούν να δαπανήσουν τα κεφάλαια που έχουν εξοικονομήσει από τη χρήση του σε άλλους τομείς και σε άλλες δράσεις[42]. Ακόμη και σε επίπεδο κατανάλωσης ενέργειας μπορεί να έχει θετική επίδραση το υπολογιστικό νέφος, καθώς οι επιχειρήσεις μπορούν κατά περίπτωση να μειώνουν ή να αυξάνουν την υπολογιστική αλλά και την αποθηκευτική δύναμη που χρειάζονται, και κατ'επέκταση να εξοικονομείται έτσι ενέργεια[43]. Επίσης, μπορεί να αποτελέσει το εργαλείο ώστε να διευρύνει μια επιχείρηση τη δραστηριότητά της και να επεκταθεί και σε νέους τομείς και να προσαρμοστεί στις νέες προκλήσεις της αγοράς.

Από την άλλη πλευρά το υπολογιστικό νέφος εμφανίζει και σοβαρά μειονεκτήματα, ως προς την ασφάλεια των δεδομένων, την αποθήκευση και διαβίβασή τους, την παραμονή τους στο περιβάλλον του διαδικτύου που είναι εν πολλοίς αρρύθμιστο, την έλλειψη ελέγχου των δεδομένων από τα ίδια τα υποκείμενα των δεδομένων αλλά και σε επίπεδο ιδιωτικότητας και προστασίας προσωπικών δεδομένων.

Δεδομένου ότι στο νέφος συλλέγονται μεγάλες ποσότητες δεδομένων, και δη προσωπικών δεδομένων, ελλοχεύει διαρκής κίνδυνος για τα δικαιώματα των υποκειμένων των δεδομένων. Επιπρόσθετα, μέσω της συσσώρευσης των δεδομένων που λαμβάνει χώρα στο «νέφος», αυτά τα δεδομένα μπορεί να εμπορευματοποιηθούν και να καταστούν περαιτέρω αντικείμενο συναλλαγής, εν αγνοία των υποκειμένων των δεδομένων. Επίσης, καθώς τα δεδομένα αυτά κατακερματίζονται σε κατανεμημένες υποδομές, ενδέχεται να χάσουν οι χρήστες τον έλεγχο αυτών και να μην μπορούν να έχουν πρόσβαση σε αυτά χωρίς τη συνδρομή του παρόχου των υπηρεσιών νέφους. Περαιτέρω, ακόμη και λόγω των πολλαπλών θέσεων των κέντρων των δεδομένων δημιουργούνται ζητήματα νομικά ως προς τη διασυνοριακή διαβίβαση αυτών των δεδομένων και ειδικότερα ως προς την αναζήτηση του εφαρμοστέου δίκαιου.

Επιφυλάξεις ως προς την προστασία των προσωπικών δεδομένων στο περιβάλλον του υπολογιστικού νέφους, ανακύπτουν ως προς το ζήτημα της εμπιστοσύνης στους παρόχους. Η έλλειψη εμπιστοσύνης αποτελεί έναν σημαντικό παράγοντα που αποτρέπει τους καταναλωτές να χρησιμοποιήσουν τις υπηρεσίες νέφους, ειδικότερα στον χώρο του ηλεκτρονικού εμπορίου. Προκειμένου να ενισχύσουν οι πάροχοι αυτή την εμπιστοσύνη θα πρέπει να ενισχύσουν την ασφάλεια των πληροφοριών και τη συμμόρφωση με τους κανόνες προστασίας των προσωπικών δεδομένων. Από την άλλη όμως, θα πρέπει να διευκρινιστεί ότι τελικά κάποιοι πάροχοι παρέχουν πολύ πιο αξιόπιστο επίπεδο ασφάλειας από αυτό που θα επετύγχαναν οι ίδιοι οι χρήστες μεμονωμένα.

Συνοψίζοντας, οι πάροχοι υπηρεσιών νέφους υποχρεούνται στη λήψη κατάλληλων και επαρκών μέτρων ασφάλειας, ως μέτρο συμμόρφωσης στις δεσμευτικές νομικές απαιτήσεις του ΓΚΠΔ. Αυτό μπορεί να επιτευχθεί με την ύπαρξη σαφών ρυθμίσεων, την παροχή ασφάλειας δικαίου όσον αφορά το εκάστοτε ισχύον δίκαιο, την σαφή οριοθέτηση ρόλων και αρμοδιοτήτων, την υιοθέτηση μέτρων ασφάλειας αλλά και την τήρηση των νομικών κανόνων για τις διασυνοριακές διαβιβάσεις δεδομένων.

[42] Μήτρου Λ., *Προστασία προσωπικών δεδομένων και υπολογιστικό νέφος*, ΔΙΜΕΕ, τ.4/2015, σελ.535
[43]Μήτρου Λ., *Προστασία προσωπικών δεδομένων και υπολογιστικό νέφος*, ΔΙΜΕΕ, τ.4/2015, σελ.535

**2.6. Ηθική δεοντολογία και προσωπικά δεδομένα**

Για την κατανόηση της ηθικής δεοντολογίας (ethical approach) του υπολογιστικού νέφους, πρέπει να κάνουμε διάκριση μεταξύ αφενός των παικτών (actors)[44] της βιομηχανίας αυτής, και αφετέρου των εμπλεκόμενων μερών (stakeholders).

Στο επίπεδο των παικτών, εντοπίζουμε πρώτα τους παρόχους φιλοξενίας (hosting companies), οι οποίοι είναι οι ιδιοκτήτες και διαχειριστές των κέντρων δεδομένων (data centers), των εξυπηρετητών, των σκληρών δίσκων στους οποίους αποθηκεύονται τα δεδομένα, καθώς και των απαραίτητων επεξεργαστών. Δεύτεροι είναι οι πάροχοι υπηρεσιών νέφους, οι οποίοι προσφέρουν τις συγκεκριμένες αυτές υπηρεσίες μέσω διαδικτύου. Τέλος, υπάρχουν και οι χρήστες (clouders), οι οποίοι μπορεί να είναι μεμονωμένοι ή επαγγελματικοί πελάτες των παρόχων υπηρεσιών νέφους, οι οποίοι χρησιμοποιούν την υπηρεσία του υπολογιστικού νέφους ως λογισμικό (SaaS) για οικιακή ή επαγγελματική χρήση.

Εμπλεκόμενα μέρη στην παροχή των υπηρεσιών νέφους μπορεί να είναι είτε μεμονωμένα φυσικά πρόσωπα είτε ομάδες, στα συμφέροντα ή τα δικαιώματα των οποίων οι εταιρικές δραστηριότητες έχουν αντίκτυπο. Αυτοί μπορεί να είναι ιδιοκτήτες, επενδυτές, εργαζόμενοι, πελάτες, προμηθευτές, ανταγωνιστές, κυβερνήσεις ή ακόμη και το περιβάλλον.

Παρατηρείται σήμερα αλλαγή στην στάση των πελατών απέναντι στην ιδιοκτησία και την ελευθερία στο περιβάλλον του υπολογιστικού νέφους. Οι χρήστες των τεχνολογιών της πληροφορίας σταδιακά υιοθετούν μια αποδυναμωμένη οπτική της αξίας της ιδιοκτησίας, υπό την έννοια ότι δεν θεωρούν απαραίτητο να είναι οι ίδιοι ιδιοκτήτες των υπολογιστικών πόρων που χρησιμοποιούν και αυτό εμπεριέχει ενισχυμένη αίσθηση ελευθερίας. Αναπόφευκτα δηλαδή μεταφερόμαστε από τον ιδιοκτήτη στον χρήστη, που δεν τον ενδιαφέρει τόσο η επεξεργασία μιας φωτογραφίας, όσο το γεγονός ότι μπορεί να δει φωτογραφίες, να τις δείξει στους φίλους του, να τις συμπεριλάβει στην ιστοσελίδα του και στο προφίλ του σε κάποιο κοινωνικό δίκτυο, ή να τις τροποποιήσει μέσω του προγράμματος Photoshop.

Η αλληλεπίδραση του καταναλωτή με τον πάροχο υπηρεσιών νέφους είναι σημαντική και πρέπει να οδηγεί στην εγκαθίδρυση μιας κοινής γνώσης, με πρωταρχικό στόχο την επιτυχή επικοινωνία μεταξύ των μερών και την προστασία των προσωπικών δεδομένων τους. Πολλές φορές το πλαίσιο της ενημέρωσης και της συγκατάθεσης που θέτουν οι πάροχοι στους καταναλωτές δεν είναι σαφές και έτσι η συγκατάθεση του χρήστη δεν είναι ελεύθερη, συγκεκριμένη, ρητή, ούτε εν πλήρει επιγνώσει, όπως επιτάσσει ο ΓΚΠΔ. Οι πάροχοι πρέπει να καθιστούν σαφές στον καταναλωτή ποιο ακριβώς προϊόν αγοράζει. Σε κάθε περίπτωση όμως, τυχόν αυστηρή ρύθμιση των παρόχων φιλοξενίας και των παρόχων υπηρεσιών νέφους θα πρέπει να αποφεύγεται, γιατί αλλιώς μπορεί να παρεμποδίσει την ενίσχυση της καινοτομίας. Από την άλλη πλευρά, κρίνεται επιθυμητή και επιτακτική η ρύθμιση των επαγγελματικών πελατών του νέφους. Η ως άνω προσέγγιση είναι συμβατή με τις επιταγές της τεχνολογίας περί ουδετερότητας.

---

[44] Boudewijn de Bruin, Luciano Floridi, *The Ethics of Cloud Computing*, διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3835151

## 3. Διασυνοριακή Διαβίβαση προσωπικών δεδομένων

### 3.1. Προϊσχύσαν νομοθετικό πλαίσιο

#### 3.1.1. Οδηγία 95/46/ΕΕ[45]

Πριν την έναρξη ισχύος του ΓΚΠΔ, δηλαδή πριν την 25.5.2018, τα θέματα της διασυνοριακής διαβίβασης δεδομένων εντός ΕΕ αλλά και σε τρίτες χώρες ρυθμίζονταν από τα άρθρα 25 και 26 της προϊσχύσασας Οδηγίας 95/46/ΕΚ[46], η οποία προέβλεπε ότι οι διασυνοριακές διαβιβάσεις εντός ΕΕ/ΕΟΧ είναι επιτρεπτές. Ωστόσο η διασυνοριακή διαβίβαση προσωπικών δεδομένων σε τρίτες χώρες ή διεθνή οργανισμό για να είναι σύννομη έπρεπε η τρίτη χώρα να εξασφαλίζει ικανοποιητικό επίπεδο προστασίας[47]. Όταν διαπιστωνόταν από την Επιτροπή ότι η τρίτη χώρα δεν διέθετε επαρκές επίπεδο προστασίας, τα κράτη μέλη όφειλαν να λάβουν τα κατάλληλα μέτρα ώστε να αποφευχθεί η διαβίβαση αυτή. Στο άρθρο 26 της εν λόγω Οδηγίας προβλέπονταν οι παρεκκλίσεις δυνάμει των οποίων, κατ'εξαίρεση, επιτρεπόταν η διασυνοριακή διαβίβαση, παρά το γεγονός ότι η χώρα αυτή δεν διέθετε επαρκές επίπεδο προστασίας. Τέτοιες παρεκκλίσεις ήταν η συναίνεση του υποκειμένου των δεδομένων, η αναγκαιότητα για εκτέλεση σύμβασης, η διασφάλιση του δημοσίου συμφέροντος ή ζωτικού συμφέροντος του υποκειμένου, κατάλληλες συμβατικές ρήτρες κ.λ.π

#### 3.1.2. Νόμος 2472/1997[48]

Ο νόμος 2472/1997 ενσωμάτωσε την Οδηγία 95/46/ΕΚ στην ελληνική έννομη τάξη. Σχετικά με τις διεθνείς διαβιβάσεις, ο ως άνω νόμος προέβλεπε στο άρθρο 9 ότι προϋπόθεση για κάθε διεθνή διαβίβαση προς χώρα εκτός ΕΕ ήταν η προηγούμενη άδεια της Αρχής Προστασίας Προσωπικών Δεδομένων, εφόσον κρινόταν ότι η εν λόγω χώρα εξασφάλιζε επαρκές επίπεδο προστασίας των δεδομένων. Εξαίρεση στα ανωτέρω αποτελούσε η τυχόν ύπαρξη άδειας επάρκειας για κάποια χώρα, εκδοθείσας από την Ευρωπαϊκή Επιτροπή, η οποία αποτελούσε τεκμήριο ότι η ως άνω χώρα πληρούσε ικανοποιητικό επίπεδο προστασίας των δεδομένων.

#### 3.1.3. Συγκριτική επισκόπηση Οδηγίας 95/46/ΕΕ & ΓΚΠΔ 2016/679 (ΓΚΠΔ)[49]

Από 25.5.2018 που τέθηκε σε ισχύ ο ΓΚΠΔ, τα θέματα των διασυνοριακών διαβιβάσεων προσωπικών δεδομένων εκτός χωρών του Ευρωπαϊκού Οικονομικού Χώρου ή σε διεθνείς οργανισμούς ρυθμίζονται από το κεφάλαιο V του ΓΚΠΔ, και συγκεκριμένα από τα άρθρα 44 επ. Τα ως άνω άρθρα πραγματεύονται το ζήτημα των διαβιβάσεων δεδομένων και έχουν εφαρμογή σε υπεύθυνους επεξεργασίας και εκτελούντες

[45] https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A31995L0046

[46] Μήτρου Λ., *Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων*, Σάκκουλας Α.Ε, 2017

[47] Παναγοπούλου-Κουντατζή Φ., *Συνταγματικές προεκτάσεις των μηχανισμών διευρύνσεως της προστασίας δεδομένων προσωπικού χαρακτήρα πέραν της ΕΕ: Εξωεδαφική εφαρμογή του ΓΚΠΔ και διασυνοριακή διαβίβαση δεδομένων*, ΔΙΤΕ (π. ΔΙΜΕΕ 4/2019)

[48] https://www.e-nomothesia.gr/kat-dedomena-prosopikou-kharaktera/n-2472-1997.html

[49] https://eur-lex.europa.eu/legal-content/EL/ALL/?uri=CELEX%3A32016R0679

επεξεργασία που βρίσκονται εντός του ΕΟΧ, και διαβιβάζουν προσωπικά δεδομένα σε τρίτες χώρες/διεθνείς οργανισμούς, δηλαδή εκτός της προστασίας του ΓΚΠΔ[50].

Ο ΓΚΠΔ κινείται στην ίδια λογική με την Οδηγία 95/46/ΕΚ ορίζοντας ότι οι διαβιβάσεις προσωπικών δεδομένων προς χώρες της ΕΕ είναι ελεύθερες, ενώ προς τρίτες χώρες ή διεθνείς οργανισμούς απαγορεύονται γενικά, εκτός εάν εξασφαλίζουν επαρκές επίπεδο προστασίας. Αντίθετα, οι διαβιβάσεις δεδομένων μη προσωπικού χαρακτήρα είναι ελεύθερες[51].

Ο ΓΚΠΔ πολλαπλασιάζει μεν τους μηχανισμούς διαβίβασης δεδομένων, αλλά καταργεί την προβλεπόμενη από την Οδηγία 95/46/ΕΕ απόφαση της αρμόδιας εποπτικής αρχής σχετικά με την πιστοποίηση του ικανοποιητικού επιπέδου προστασίας των δεδομένων της τρίτης χώρας[52]. Περιορίζει επίσης την αρμοδιότητα της εποπτικής αρχής να εγκρίνει κάποια διασυνοριακή διαβίβαση δεδομένων, καθώς δημιουργεί καθεστώς οιονεί αυτορρύθμισης, δηλαδή μετακυλίει την ευθύνη της επεξεργασίας στον υπεύθυνο επεξεργασίας αλλά και στον εκτελούντα, σύμφωνα με την αρχή της λογοδοσίας. Απαλλάσσει δηλαδή τις εποπτικές αρχές από τη λήψη αποφάσεων και μεταθέτει την ευθύνη στον υπεύθυνο επεξεργασίας και στον εκτελούντα την επεξεργασία, με κίνδυνο να μην μπορούν οι δημόσιοι και οι ιδιωτικοί φορείς να ασκήσουν τέτοιο έλεγχο με επάρκεια.

Όπως προαναφέραμε, επιπλέον των μηχανισμών διαβίβασης που όριζε η ανωτέρω Οδηγία, ο ΓΚΠΔ, θέσπισε νέους, όπως τους εγκεκριμένους μηχανισμούς πιστοποίησης και τους εγκεκριμένους κώδικες δεοντολογίας. Καθιερώνει επίσης τους δεσμευτικούς εταιρικούς κανόνες επίσημα ως μηχανισμό διαβίβασης και παύει την υποχρέωση προηγούμενης γνωστοποίησης και αδειοδότησης από τις εθνικές εποπτικές αρχές.

### 3.2. Το ισχύον νομικό πλαίσιο διαβιβάσεων (άρθρα 44-49 ΓΚΠΔ)- Μηχανισμοί διαβίβασης

#### 3.2.1. Αποφάσεις Επάρκειας (adequacy decisions)

Ο Κανονισμός κατά κανόνα επιτρέπει διαβιβάσεις σε χώρες εντός ΕΕ/ΕΟΧ. Κατ'εξαίρεση, επιτρέπονται και σε τρίτες χώρες, καθώς και σε έδαφος ή σε συγκεκριμένο τομέα ή σε διεθνή οργανισμό, αρκεί να πληρούνται οι προϋποθέσεις των άρθρων 44επ. του ΓΚΠΔ.

Ο Κανονισμός θέτει σαφή ιεράρχηση ως προς τους μηχανισμούς διαβίβασης. Ο επικρατέστερος μηχανισμός είναι οι αποφάσεις επάρκειας, που εκδίδονται από την Ευρωπαϊκή Επιτροπή (α.45 ΓΚΠΔ), εφόσον η τελευταία αποφασίσει ότι η τρίτη χώρα διασφαλίζει επαρκές επίπεδο προστασίας των προσωπικών δεδομένων.

---

[50] Λωσταράκου Κ., *Διεθνείς διαβιβάσεις δεδομένων υπό τον νέο Κανονισμό*, δημοσιευμένο σε Κοτσαλή Λ./ Μενουδάκο Κ. «Γενικός Κανονισμός για την προστασία των προσωπικών δεδομένων (GDPR) Νομική διάσταση και πρακτική εφαρμογή», σελ.356, Νομική Βιβλιοθήκη, 2020

[51] Παλιού Ελ., *Οι νέες τυποποιημένες συμβατικές ρήτρες της ΕΕ: η διασυνοριακή διαβίβαση προσωπικών δεδομένων στον απόηχο της νομολογίας Schrems* , ΔΙΜΕΕ 4/2021, σελ. 536

[52] Παναγοπούλου-Κουντατζή Φ. *Συνταγματικές προεκτάσεις των μηχανισμών διευρύνσεως της προστασίας δεδομένων προσωπικού χαρακτήρα πέραν της ΕΕ: Εξωεδαφική εφαρμογή του ΓΚΠΔ και διασυνοριακή διαβίβαση δεδομένων*, ΔΙΤΕ 4/2019

Τα κριτήρια βάσει των οποίων γίνεται η εκτίμηση της επάρκειας του επιπέδου προστασίας της τρίτης χώρας, σύμφωνα με το άρθρο 45 παρ.2 του ΓΚΠΔ, είναι τα εξής[53]: α) το κράτος δικαίου, ο σεβασμός των ανθρωπίνων δικαιωμάτων και των θεμελιωδών ελευθεριών, η σχετική νομοθεσία της τρίτης χώρας και η εφαρμογή αυτής, οι κανόνες περί προστασίας δεδομένων, οι επαγγελματικοί κανόνες και τα μέτρα ασφάλειας, η νομολογία, τα ουσιαστικά και εκτελεστά δικαιώματα των υποκειμένων των δεδομένων και τα αποτελεσματικά διοικητικά και δικαστικά μέσα προσφυγής, β) η ύπαρξη και αποτελεσματική λειτουργία των εποπτικών αρχών και γ) οι διεθνείς δεσμεύσεις που έχει αναλάβει η τρίτη χώρα ή ο διεθνής οργανισμός ή άλλες υποχρεώσεις που απορρέουν από νομικά δεσμευτικές πράξεις ως προς την προστασία προσωπικών δεδομένων. Η απόφαση Schrems II με τη σειρά της εξειδικεύει ότι μιωψ α απόφαση επάρκειας είναι ισχυρή μόνο εφόσον ο νόμος προστασίας των δεδομένων στην χώρα προορισμού είναι «ουσιαστικά ισοδύναμος» με το δίκαιο της ΕΕ[54].

Σε συνέχεια των ανωτέρω, η Επιτροπή με την με αριθμό 2016/229 εκτελεστική απόφασή της, θέτει ως υποχρέωση αυτής αλλά και των εθνικών εποπτικών αρχών να επιτηρούν τις εξελίξεις στις τρίτες χώρες. Ειδικότερα, να παρακολουθούν για τυχόν αδικαιολόγητη επέμβαση των -επιφορτισμένων με την εθνική ασφάλεια - κρατικών αρχών των τρίτων χωρών στα δικαιώματα των υποκειμένων των δεδομένων, δηλαδή να εποπτεύουν την τήρηση της αρχής της αναλογικότητας, αλλά και εάν τα υποκείμενα χαίρουν επαρκούς και αποτελεσματικής προστασίας. Δίδεται επίσης η αρμοδιότητα στις εθνικές εποπτικές αρχές να εξετάζουν προσφυγές των υποκειμένων των δεδομένων για την εγκυρότητα μιας απόφασης επάρκειας και εφόσον αυτές κριθούν βάσιμες να μπορούν να αχθούν ενώπιον των εθνικών δικαστηρίων, τα οποία με τη σειρά τους θα νομιμοποιούνται να θέσουν προδικαστικό ερώτημα στο ΔΕΕ[55].

Αποφάσεις επάρκειας κατέχουν κατά την παρούσα περίοδο οι κάτωθι χώρες[56]: Λαϊκή Δημοκρατία της Κορέας, Ανδόρρα, Αργεντινή, Καναδάς, Νησιά Φαρόε, Guernsey, Ισραήλ, Isle of Man, Jersey, Νέα Ζηλανδία, Ελβετία, Ουρουγουάη και Ηνωμένο Βασίλειο. Η Ιαπωνία αποτελεί την πρώτη χώρα που έλαβε απόφαση επάρκειας μετά την έναρξη ισχύος του ΓΚΠΔ, συγκεκριμένα τον Ιανουάριο του 2019, η οποία συνοδεύεται από πρόσθετες εγγυήσεις για την προστασία των προσωπικών δεδομένων που διαβιβάζονται στην Ιαπωνία[57].

Το άρθρο 45 παρ. 9 του ΓΚΠΔ ορίζει ότι αποφάσεις που έχουν εκδοθεί με βάση το άρθρο 25 παρ. 6 της Οδηγίας 95/46/ΕΚ παραμένουν σε ισχύ μέχρι να τροποποιηθούν, αντικατασταθούν ή καταργηθούν με σχετική απόφαση της Επιτροπής. Σε κάθε περίπτωση στο άρθρο 45 παρ.3 του ΓΚΠΔ προβλέπεται μηχανισμός περιοδικής

---

[53] Murray Andrew, *Information Technology Law*, σελ.624, 4th edition, Oxford University Press, 2019

[54] Λωσταράκου Κ., *Διεθνείς διαβιβάσεις δεδομένων υπό τον νέο Κανονισμό*, δημοσιευμένο σε Κοτσαλή Λ./ Μενουδάκο Κ. «Γενικός Κανονισμός για την προστασία των προσωπικών δεδομένων (GDPR) Νομική διάσταση και πρακτική εφαρμογή», Νομική Βιβλιοθήκη, 2020, σελ.358

[55] Λωσταράκου Κ., *Διεθνείς διαβιβάσεις δεδομένων υπό τον νέο Κανονισμό*, δημοσιευμένο σε Κοτσαλή Λ./ Μενουδάκο Κ. «Γενικός Κανονισμός για την προστασία των προσωπικών δεδομένων (GDPR) Νομική διάσταση και πρακτική εφαρμογή», Νομική Βιβλιοθήκη, 2020, σελ.358

[56] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[57] Λωσταράκου Κ., *Διεθνείς διαβιβάσεις δεδομένων υπό τον νέο Κανονισμό*, δημοσιευμένο σε Κοτσαλή Λ./ Μενουδάκο Κ. «Γενικός Κανονισμός για την προστασία των προσωπικών δεδομένων (GDPR) Νομική διάσταση και πρακτική εφαρμογή», Νομική Βιβλιοθήκη, 2020, σελ.357

επανεξέτασης κάθε απόφασης επάρκειας, τουλάχιστον ανά τετραετία, στην οποία συνεκτιμώνται όλες οι σχετικές εξελίξεις στην τρίτη χώρα ή τον διεθνή οργανισμό.

### 3.2.2. Διαβιβάσεις μέσω κατάλληλων εγγυήσεων

Το άρθρο 46 του ΓΚΠΔ ορίζει ως δεύτερο μηχανισμό διαβίβασης, ελλείψει απόφασης επάρκειας, την παροχή κατάλληλων εγγυήσεων. Για τη συγκεκριμένη διαβίβαση, ο υπεύθυνος ή ο εκτελών την επεξεργασία, που εξάγει τα δεδομένα, πρέπει να παρέχει κατάλληλες εγγυήσεις στον αποδέκτη στην τρίτη χώρα, ως πιθανά μέσα εξασφάλισης επαρκούς επιπέδου προστασίας για τον τελευταίο και πάντα υπό την προϋπόθεση ότι υφίστανται εκτελεστά δικαιώματα και αποτελεσματικά ένδικα μέσα για τα υποκείμενα των δεδομένων[58]

Η επιλογή ενός εργαλείου διαβίβασης του παρόντος άρθρου ενδέχεται να μην είναι επαρκής. Το εκάστοτε εργαλείο πρέπει να εξασφαλίζει ότι το επίπεδο προστασίας που εγγυάται ο ΓΚΠΔ δεν υπονομεύεται από τη διαβίβαση, δηλαδή πρέπει να είναι αποτελεσματικό. Πρακτικά αυτό σημαίνει ότι τα διαβιβαζόμενα προσωπικά δεδομένα πρέπει να τυγχάνουν ενός επιπέδου προστασίας στην τρίτη χώρα που είναι ουσιαστικά ισοδύναμο με εκείνο που εξασφαλίζεται εντός του ΕΟΧ. Αυτό δεν θα ισχύει εάν ο εισαγωγέας των δεδομένων κωλύεται να συμμορφωθεί με τις απορρέουσες από το συγκεκριμένο εργαλείο υποχρεώσεις, λόγω της νομοθεσίας και των πρακτικών της τρίτης χώρας που εφαρμόζονται κατά τη διαβίβαση.

Εάν διαπιστωθεί ότι το επιλεγέν εργαλείο δεν παρέχει επαρκή προστασία, θα πρέπει να υιοθετηθούν πρόσθετα μέτρα[59], τα οποία θα είναι συμπληρωματικά των ως άνω εγγυήσεων. Τέτοια μέτρα μπορεί να είναι α) τεχνικά μέτρα (πχ. αποθήκευση δεδομένων για σκοπούς δημιουργίας αντιγράφων ασφαλείας και για άλλους σκοπούς που δεν απαιτούν αποκωδικοποιημένη πρόσβαση σε δεδομένα, διαβίβαση ψευδωνυμοποιημένων δεδομένων, κρυπτογράφηση δεδομένων που διέρχονται απλώς από τρίτες χώρες, διαβίβαση σε προστατευόμενο παραλήπτη, πολυσυμμετοχικός διαχωρισμός ή επεξεργασία των δεδομένων κλπ) ή β) πρόσθετα συμβατικά μέτρα, τα οποία αποτελούνται από μονομερείς, διμερείς ή πολυμερείς συμβατικές δεσμεύσεις, γ) πρόβλεψη για συμβατική υποχρέωση χρήσης ειδικών τεχνικών μέτρων, δ) υποχρεώσεις διαφάνειας, καθώς και ε) οργανωτικά μέτρα (πχ. εσωτερικές πολιτικές, οργανωτικές μεθόδους και πρότυπα), στ) μέτρα διαφάνειας και λογοδοσίας, και ζ) μέθοδοι οργάνωσης και μέτρα ελαχιστοποίησης δεδομένων.

Τέτοιες κατάλληλες εγγυήσεις μπορεί να περιλαμβάνουν τους παρακάτω μηχανισμούς:

#### 3.2.2.1 Νομικά δεσμευτικά και εκτελεστά μέσα μεταξύ δημοσίων αρχών ή φορέων

Αυτό πρακτικά σημαίνει ότι μπορούν οι δημόσιες αρχές, στο πλαίσιο μεταξύ τους συμφωνίας που διέπεται από τις απαιτήσεις του ΓΚΠΔ, να πραγματοποιούν διαβιβάσεις

---

[58] *Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων*, Οργανισμός Θεμελιωδών δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ευρώπης, έκδοση 2018, σελ.325

[59] *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*, διαθέσιμες σε https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_el.pdf

και να εξασφαλίζουν εκτελεστά και ουσιαστικά δικαιώματα των υποκειμένων. Δεν προϋποθέτει η διαβίβαση αυτή άδεια της εθνικής εποπτικής αρχής, εκτός και εάν οι εγγυήσεις αυτές προβλέπονται σε νομικά μη δεσμευτικές διοικητικές ρυθμίσεις (πχ. μνημόνιο συνεργασίας), περίπτωση κατά την οποία θα πρέπει να εφαρμόζεται ο μηχανισμός συνεκτικότητας του α.63 ΓΚΠΔ (α.46 παρ.3 & 4 ΓΚΠΔ).

**3.2.2.2 Δεσμευτικοί εταιρικοί κανόνες (Binding Corporate Rules-BCR)**

Πρόκειται για έναν εσωτερικό κώδικα δεοντολογίας[60], που λειτουργεί μεταξύ των μελών ενός ομίλου επιχειρήσεων ή ομίλου εταιριών, που ασκούν κοινή οικονομική δραστηριότητα, συμπεριλαμβανομένων των υπαλλήλων τους. Είναι νομικά δεσμευτικοί κανόνες, οι οποίοι ισχύουν για διαβιβάσεις από οντότητες του ομίλου εταιριών εντός ΕΟΧ σε οντότητες εκτός ΕΟΧ. Οι κανόνες αυτοί πρέπει να απονέμουν ρητά εκτελεστά δικαιώματα στα υποκείμενα των δεδομένων όσον αφορά την επεξεργασία των προσωπικών δεδομένων τους και επίσης να πληρούνται οι παρακάτω προϋποθέσεις της παραγράφου 2 του άρθρου 47.

Το βασικό πλεονέκτημα των δεσμευτικών εταιρικών κανόνων είναι ότι δεν έχουν προκαθορισμένο περιεχόμενο, όπως οι τυποποιημένες συμβατικές ρήτρες[61], με αποτέλεσμα το περιεχόμενό τους να μπορεί να διαμορφωθεί ελεύθερα, ανάλογα με τις εκάστοτε ανάγκες ενός οργανισμού. Το μειονέκτημά τους ωστόσο είναι ότι είναι αρκετά χρονοβόρα η διαδικασία έγκρισής τους. Κατά συνέπεια, παρόλο που πολλές επιχειρήσεις έχουν καταρτίσει εταιρικούς δεσμευτικούς κανόνες, λίγες έχουν καταφέρει να λάβουν έγκριση από το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων, ώστε στη συνέχεια να λάβουν την τελική έγκριση και από την επικεφαλής εθνική αρχή.

Οι όμιλοι επιχειρήσεων που χρησιμοποιούσαν δεσμευτικούς εταιρικούς κανόνες με βάση την Οδηγία 95/46/ΕΕ, πρέπει να τους τροποποιήσουν με βάση τα παρακάτω κριτήρια που επιβάλλει ο ΓΚΠΔ[62]. Επιγραμματικά αναφέρουμε ότι στους δεσμευτικούς εταιρικούς κανόνες πρέπει αναλυτικά να γίνεται καταγραφή της δομής και των στοιχείων επικοινωνίας του ομίλου επιχειρήσεων και των μελών του, των διαβιβάσεων που εκτελούνται, τον τύπο της επεξεργασίας που τελούν, τους σκοπούς αυτής, τη νομικά δεσμευτική φύση τους, την εφαρμογή των γενικών αρχών προστασίας δεδομένων, τα δικαιώματα των υποκειμένων των δεδομένων όσον αφορά την επεξεργασία και τα μέσα άσκησης αυτών, την αποδοχή ευθύνης του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, που είναι εγκαταστημένος στο κράτος μέλος σχετικά με τυχόν παραβιάσεις, τον τρόπο ενημέρωσης των υποκειμένων των δεδομένων σχετικά με τους εν λόγω κανόνες, τα καθήκοντα του υπευθύνου προστασίας δεδομένων, τις διαδικασίες καταγγελίας, τους μηχανισμούς εντός του ομίλου για τον έλεγχο της συμμόρφωσης προς

---

[60] Λωσταράκου Κ., *Διεθνείς διαβιβάσεις δεδομένων υπό τον νέο Κανονισμό*, δημοσιευμένο σε Κοτσαλή Λ./ Μενουδάκο Κ. «Γενικός Κανονισμός για την προστασία των προσωπικών δεδομένων (GDPR) Νομική διάσταση και πρακτική εφαρμογή», Νομική Βιβλιοθήκη, 2020, σελ.360

[61] Παλιού Ε. *Οι νέες τυποποιημένες συμβατικές ρήτρες της Ευρωπαϊκής Επιτροπής- Η διασυνοριακή διαβίβαση προσωπικών δεδομένων στον απόηχο της νομολογίας Schrems (αποφάσεις του ΔΕΕ υπ'αριθμ. C362/14 και C-311/18),* ΔΙΜΕΕ 4/2021, σελ. 537

[62] Λωσταράκου Κ., *Διεθνείς διαβιβάσεις δεδομένων υπό τον νέο Κανονισμό*, δημοσιευμένο σε Κοτσαλή Λ./ Μενουδάκο Κ. «Γενικός Κανονισμός για την προστασία των προσωπικών δεδομένων (GDPR) Νομική διάσταση και πρακτική εφαρμογή», Νομική Βιβλιοθήκη, 2020, σελ.360

τους κανόνες αυτούς, τους μηχανισμούς αναφοράς και καταχώρισης αλλαγών στους κανόνες και αναφορά τους στην εποπτική αρχή, τον μηχανισμό συνεργασίας με την εποπτική αρχή, τους μηχανισμούς αναφοράς στην αρμόδια εποπτική αρχή κάθε νομικής απαίτησης στην οποία εμπλέκεται μέλος του ομίλου, και τέλος την κατάλληλη εκπαίδευση του προσωπικού του ομίλου σχετικά με την προστασία δεδομένων.

Οι δεσμευτικοί εταιρικοί κανόνες εγκρίνονται σε ευρωπαϊκό επίπεδο χωρίς την απαίτηση εθνικής άδειας. Όταν στοχεύουν στην κάλυψη διαβιβάσεων δεδομένων περισσότερων κρατών μελών, εφαρμόζεται ο Μηχανισμός Συνεκτικότητας (α.63 επ. ΓΚΠΔ) και η αρμόδια εποπτική αρχή εγκρίνει τους δεσμευτικούς εταιρικούς κανόνες ως τον κατάλληλο μηχανισμό διασυνοριακής διαβίβασης μεταξύ εταιριών ενός ομίλου, μόνο εφόσον πληρούνται τα απαιτούμενα από τον ΓΚΠΔ κριτήρια.

**3.2.2.3. Τυποποιημένες Συμβατικές Ρήτρες (Standard Contractual Clauses- SCCs)**

Οι τυποποιημένες συμβατικές ρήτρες (εφεξής 'ΤΣΡ') ή άλλως πρότυπες συμβατικές ρήτρες καταρτίζονται από την Ευρωπαϊκή Επιτροπή και αποτελούν το πλέον δημοφιλές μέσο διαβίβασης σε τρίτες χώρες, μετά την απόφαση Schrems II.

Οι ΤΣΡ περιέχουν συμβατικές υποχρεώσεις του εξαγωγέα και του εισαγωγέα των δεδομένων, στην ουσία δήλωση αυτοδέσμευσής τους, ότι θα τηρήσουν τις απαιτήσεις των ρητρών αυτών κατά τη διαβίβαση προσωπικών δεδομένων των υποκειμένων σε τρίτη χώρα, καθώς και δεσμεύσεις ως προς τα δικαιώματα των υποκειμένων, τα οποία μπορούν να ασκηθούν απευθείας έναντι του εξαγωγέα και του εισαγωγέα των δεδομένων. Οι ΤΣΡ αποτελούν στην ουσία το παράρτημα σε μια σύμβαση DPA (Data Protection Agreement). Ενδεικτικά αναφέρουμε ότι οι ΤΣΡ χρησιμοποιούνται από την Google, την Facebook, την Apple και τη Microsoft[63].

Υπό την προϊσχύσασα Οδηγία 95/46/ΕΕ η Επιτροπή είχε υιοθετήσει δύο είδη ΤΣΡ, ήτοι ένα για διαβιβάσεις μεταξύ υπευθύνων επεξεργασίας (απόφαση 2001/497/ΕΚ[64]) και ένα μεταξύ εκτελούντων την επεξεργασία (απόφαση 2010/87/ΕΕ[65]). Το 2016 η Επιτροπή εξέδωσε την εκτελεστική απόφαση 2016/2297[66], η οποία τροποποίησε τις ως άνω δύο αποφάσεις προκειμένου να εναρμονιστεί με την απόφαση Schrems I.

Με την υπ'αριθμ. 2021/914 απόφασή της, η Επιτροπή κατάργησε τις αποφάσεις 2001/497/ΕΚ και 2010/87/ΕΕ. Στη συνέχεια, εξέδωσε την υπ'αριθμ. 2021/915[67] απόφαση στο πλαίσιο του Κανονισμού 2018/1725 για την επεξεργασία προσωπικών δεδομένων από θεσμικά όργανα και οργανισμούς της ΕΕ[68].

Οι νέες ΤΣΡ έχουν ως νομική βάση τον ΓΚΔΠ, ενώ οι παλιές είχαν την Οδηγία 95/46/ΕΚ. Οι νέες ρήτρες εναρμονίζονται με την απόφαση Schrems II, και παρέχουν ευελιξία, μέσω της συνδυαστικής εφαρμογής γενικών ρητρών, με μια προσέγγιση βάσει

---

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

[64] https://eur-lex.europa.eu/legal-content/EL/ALL/?uri=celex:32001D0497

[65] https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32010D0087

[66] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016D2297

[67] https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32021D0915

[68] Παλιού Ε. *Οι νέες τυποποιημένες συμβατικές ρήτρες της Ευρωπαϊκής Επιτροπής- Η διασυνοριακή διαβίβαση προσωπικών δεδομένων στον απόηχο της νομολογίας Schrems (αποφάσεις του ΔΕΕ υπ'αριθμ. C362/14 και C-311/18),* ΔΙΜΕΕ 4/2021, σελ. 538

των ενοτήτων κατωτέρω, λαμβάνοντας υπόψη τα διαφορετικά σχήματα διαβίβασης και την πολύπλοκη και πολυπρόσωπη εμπλοκή των φορέων στη σύγχρονη αλυσίδα επεξεργασίας[69].

Με την υπ'αριθμ. 2021/914[70] εκτελεστική απόφασή της, η Επιτροπή έκανε τη διάκριση των ΤΣΡ στις παρακάτω τέσσερις ενότητες, προκειμένου να ρυθμίσει τις διαβιβάσεις ανάλογα με τα μέρη που εμπλέκονται, και ειδικότερα[71]:

- Από υπεύθυνο επεξεργασίας σε υπεύθυνο επεξεργασίας (1η ενότητα)
- Από υπεύθυνο επεξεργασίας σε εκτελούντα την επεξεργασία (2η ενότητα)
- Από εκτελούντα την επεξεργασία σε εκτελούντα την επεξεργασία (3η ενότητα)
- Από εκτελούντα την επεξεργασία σε υπεύθυνο επεξεργασίας (4η ενότητα).

Ανάλογα λοιπόν με το είδος της διαβίβασης, ο εκάστοτε οργανισμός καλείται να επιλέξει ποια ΤΣΡ θα χρησιμοποιήσει, πάντα σε συνάρτηση με τις διαβιβάσεις που εκτελεί. Η ως άνω διάκριση διευκολύνει τη σύνθετη μορφή που λαμβάνει η επεξεργασία σήμερα[72]. Οι ως άνω ενότητες περιέχουν κάποιους γενικούς κανόνες που εφαρμόζονται σε κάθε ενότητα, και κάποιους ειδικούς που αφορούν σε κάθε επιμέρους ενότητα.

Ενώ με τις παλιές ΤΣΡ την ευθύνη για την διαβίβαση την είχε αποκλειστικά ο εξαγωγέας των δεδομένων, με τις νέες ΤΣΡ επιβεβαιώθηκε από το ΔΕΕ στην απόφαση Schrems II ότι ο εξαγωγέας έχει μεν πρωταρχική ευθύνη, αλλά ότι επικουρικά ευθύνεται και η αρμόδια εποπτική αρχή. Ο εξαγωγέας δηλαδή φέρει το κύριο βάρος του ελέγχου του δικαίου της χώρας προορισμού των δεδομένων και του κατά πόσο αυτή εξασφαλίζει προστασία των προσωπικών δεδομένων που διαβιβάζονται, παρέχοντας στην ανάγκη εγγυήσεις πλέον αυτών που προσφέρουν οι ΤΣΡ.

Με τη ρήτρα 8 της απόφασης 2021/914 διατυπώθηκε ότι ο εξαγωγέας των δεδομένων φέρει το βάρος της ευθύνης για τη διαβίβαση, και ταυτόχρονα την οριοθετεί σχετικά με το εάν αυτός έχει καταβάλει εύλογες προσπάθειες για να εξακριβώσει ότι ο εισαγωγέας θα συμμορφωθεί με τις ΤΣΡ. Συνδυαστικά με τη ρήτρα 12 της ως άνω απόφασης, αναφέρεται η περίπτωση της διαβίβασης από υπευθύνους επεξεργασίας και γίνεται μνεία στο δικαίωμα αποζημίωσης του υποκειμένου των δεδομένων στην περίπτωση που έχει υποστεί ζημία κατά την διαβίβαση των δεδομένων του. Ο εξαγωγέας και ο εισαγωγέας των δεδομένων ευθύνονται αλληλεγγύως και εις ολόκληρον έναντι του υποκειμένου και το τελευταίο καλείται να εντοπίσει ποιος εκ των ως άνω δύο του προκάλεσε την ζημία και ποιος κατ'επέκταση θα κληθεί να τον αποζημιώσει.

Πρέπει να σημειωθεί ότι οι νέες ρήτρες τέθηκαν σε ισχύ στις 27.6.2021, όμως προβλέπουν μεταβατική περίοδο δεκαοκτώ (18) μηνών για την αντικατάσταση των προηγούμενων ΤΣΡ, ήτοι μέχρι 27.12.2022. Οι εξαγωγείς νομιμοποιούνταν να συνεχίσουν

---

69 https://www.dpa.gr/index.php/el/enimerwtiko/thematikes_enotites/diavivaseis_ee/simvatikes_ritres

70 https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32021D0914

71 https://www.dpa.gr/index.php/el/enimerwtiko/thematikes_enotites/diavivaseis_ee/simvatikes_ritres

72 *Personal Data Protection Digest* by Personal Data Protection Commission Singapore, 2021, διαθέσιμο σε https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Commissions-Decisions/2021-Personal-Data-Protection-Digest.ashx

να εφαρμόζουν τις προηγούμενες συμβατικές ρήτρες για τρεις (3) μήνες από την έναρξη ισχύος τους, δηλαδή μέχρι τις 27.9.2021[73].

### 3.2.2.4. Τυποποιημένες Ρήτρες Προστασίας Δεδομένων

Άλλο εναλλακτικό εργαλείο που προβλέπεται από τον ΓΚΠΔ είναι οι τυποποιημένες ρήτρες προστασίας των δεδομένων που θεσπίζονται από εθνική εποπτική αρχή ή οι συμβατικές ρήτρες που εγκρίνονται από εθνική αρχή ελέγχου[74]. Οι εν λόγω ρήτρες δεν χρησιμοποιούνται ευρέως.

Οι αρμόδιες εποπτικές αρχές πρέπει αρχικά να υποβάλουν τις ρήτρες στο ΕΣΠΔ για έγκριση. Κατόπιν της έγκρισης αυτής, οι εταιρίες μπορούν να τις χρησιμοποιούν ως ευρύτερο εργαλείο ή ως συνολικό εργαλείο για τις διεθνείς διαβιβάσεις. Αυτή η εξέλιξη μπορεί να αποτελέσει το βήμα ώστε να εγκρίνονται πρότυπες ρήτρες που εξυπηρετούν συγκεκριμένο τομέα, όπως η νεφοϋπολογιστική ή ο τουριστικός τομέας[75].

Στους υπεύθυνους επεξεργασίας δίνεται επίσης η δυνατότητα σύνταξης συμβατικών ρητρών από τα δύο μέρη που εμπλέκονται στη διαβίβαση (υπεύθυνους ή εκτελούντες) και η υποβολή τους στην αρμόδια εθνική εποπτική αρχή, σύμφωνα με τον μηχανισμό συνεκτικότητας.

Ο Κανονισμός ενθαρρύνει τις εταιρίες να θεσπίσουν πρόσθετες εγγυήσεις για την προστασία των δεδομένων μέσω συμβατικών υποχρεώσεων, επιπλέον δηλαδή των ως άνω πρόσθετων ρητρών. Μόνη προϋπόθεση για τη θέσπισή τους είναι να μην αντίκεινται στις υποχρεωτικές πρότυπες ρήτρες και να μην θίγουν την ιδιωτικότητα των υποκειμένων των δεδομένων[76].

### 3.2.2.5. Κώδικες Δεοντολογίας

Αποτελούν στην ουσία εργαλεία αυτορρύθμισης[77], που χρησιμοποιούνται από τους διάφορους φορείς προκειμένου να αποδεικνύουν στις εθνικές εποπτικές αρχές και στους καταναλωτές ότι μια εταιρία συμμορφώνεται με τους κανόνες προστασίας της ιδιωτικής ζωής.

Όσον αφορά τις διαβιβάσεις, το άρθρο 40 παρ.2 του ΓΚΠΔ ορίζει ότι «*ενώσεις και άλλοι φορείς που εκπροσωπούν κατηγορίες υπευθύνων επεξεργασίας ή εκτελούντων την επεξεργασία μπορούν να εκπονούν κώδικες δεοντολογίας ή να τροποποιούν ή να επεκτείνουν υφιστάμενους κώδικες δεοντολογίας, προκειμένου να προσδιορίσουν την*

---

[73] https://www.dpa.gr/index.php/el/enimerwtiko/thematikes_enotites/diavivaseis_ee/simvatikes_ritres

[74] Παλιού Ε. *Οι νέες τυποποιημένες συμβατικές ρήτρες της Ευρωπαϊκής Επιτροπής- Η διασυνοριακή διαβίβαση προσωπικών δεδομένων στον απόηχο της νομολογίας Schrems (αποφάσεις του ΔΕΕ υπ'αριθμ. C362/14 και C-311/18),* ΔΙΜΕΕ 4/2021, σελ. 536

[75] Λωσταράκου Κ., *Διεθνείς διαβιβάσεις δεδομένων υπό τον νέο Κανονισμό*, δημοσιευμένο σε Κοτσαλή Λ./ Μενουδάκο Κ. «Γενικός Κανονισμός για την προστασία των προσωπικών δεδομένων (GDPR) Νομική διάσταση και πρακτική εφαρμογή», Νομική Βιβλιοθήκη, 2020, σελ.362

[76] Λωσταράκου Κ., *Διεθνείς διαβιβάσεις δεδομένων υπό τον νέο Κανονισμό*, δημοσιευμένο σε Κοτσαλή Λ./ Μενουδάκο Κ. «Γενικός Κανονισμός για την προστασία των προσωπικών δεδομένων (GDPR) Νομική διάσταση και πρακτική εφαρμογή», Νομική Βιβλιοθήκη, 2020, σελ.363

[77] Λωσταράκου Κ., *Διεθνείς διαβιβάσεις δεδομένων υπό τον νέο Κανονισμό*, δημοσιευμένο σε Κοτσαλή Λ./ Μενουδάκο Κ. «Γενικός Κανονισμός για την προστασία των προσωπικών δεδομένων (GDPR) Νομική διάσταση και πρακτική εφαρμογή», Νομική Βιβλιοθήκη, 2020, σελ.363

*εφαρμογή του Κανονισμού, όπως όσον αφορά…….ι) τη διαβίβαση δεδομένων σε τρίτες χώρες ή διεθνείς οργανισμούς……».*

Οι κώδικες δεοντολογίας, πέρα από την τήρησή τους από υπευθύνους επεξεργασίας ή εκτελούντες την επεξεργασία υπαγόμενους στον Κανονισμό, μπορούν να τηρούνται και από υπεύθυνους επεξεργασίας που δεν υπάγονται στον Κανονισμό (α.40 παρ.3 ΓΚΠΔ). Παρέχουν συνδυαστικά με δεσμευτικές και εκτελεστές υποχρεώσεις του υπευθύνου ή του εκτελούντος την επεξεργασία τις κατάλληλες εγγυήσεις για διαβίβαση δεδομένων σε τρίτες χώρες[78]

Αρκεί οι ενώσεις και οι φορείς να υποβάλλουν το σχέδιο κώδικα στην αρμόδια εποπτική αρχή, η οποία καλείται να γνωμοδοτήσει ως προς τη συμμόρφωση του σχεδίου κώδικα, και να το εγκρίνει. Εάν αυτό αναφέρεται σε δραστηριότητες επεξεργασίας σε διάφορα κράτη μέλη, η αρμόδια εποπτική αρχή το υποβάλλει στη διαδικασία του άρθρου 63 ΓΚΠΔ στο Συμβούλιο Προστασίας Δεδομένων, το οποίο γνωμοδοτεί ως προς τη συμμόρφωση (άρθρο 40 παρ.5 ΓΚΠΔ).

Η Επιτροπή με εκτελεστική της πράξη μπορεί να αποφασίζει ότι οι εγκεκριμένοι κώδικες δεοντολογίας έχουν γενική ισχύ εντός της Ένωσης (α.40 παρ.9 ΓΚΠΔ). Για να θεωρηθούν οι κώδικες αυτοί ότι επιτρέπουν επαρκή διασφάλιση για διεθνείς διαβιβάσεις στο πλαίσιο του ΓΚΠΔ, πρέπει να καθίστανται νομικά δεσμευτικοί για τους τρίτους, για παράδειγμα μέσω σύμβασης μεταξύ του υπευθύνου επεξεργασίας και του εκτελούντα την επεξεργασία στις ΗΠΑ, που συμφωνεί να τον εφαρμόσει.[79]

Το ΕΣΠΔ έχει εκδώσει τις Κατευθυντήριες Γραμμές 1/2019[80] της 4ης Ιουνίου 2019 σχετικά με τους Κώδικες Δεοντολογίας και τους Φορείς Παρακολούθησης στο πλαίσιο του Κανονισμού 2016/679, με τις οποίες επιδιώκεται η παροχή πρακτικής καθοδήγησης και ερμηνευτικής συνδρομής σχετικά με την εφαρμογή των άρθρων 40-41 ΓΚΠΔ.

**3.2.2.6 Εγκεκριμένοι Μηχανισμοί Πιστοποίησης**

Στα άρθρα 42-43 του ΓΚΠΔ γίνεται αναφορά στους μηχανισμούς και στους φορείς πιστοποίησης. Η θέσπισή τους αποδεικνύει την ύπαρξη κατάλληλων εγγυήσεων στο πλαίσιο της διαβίβασης δεδομένων σε τρίτες χώρες ή διεθνείς οργανισμούς από υπευθύνους επεξεργασίας ή εκτελούντες που δεν υπόκεινται στον ΓΚΠΔ.

Μπορεί μια εταιρία σε τρίτη χώρα να υποβάλει αίτηση και να λάβει πιστοποίηση, παρέχοντας παράλληλα τη διαβεβαίωση ότι προσφέρει επαρκή προστασία στα προσωπικά δεδομένα που προέρχονται από την Ε.Ε. Εάν δε, συνδυάσει την πιστοποίηση με μια νομική δέσμευση περί εφαρμογής των προτύπων πιστοποίησης, μπορεί να θεωρηθεί ότι παρέχει επαρκείς εγγυήσεις και συνεπώς να καθίσταται αξιόπιστη για να λαμβάνει προσωπικά δεδομένα από την Ε.Ε.

---

[78] Γιαννόπουλος Γιώργος, Εισαγωγή στη Νομική Πληροφορική, Νομική Βιβλιοθήκη, 2018, σελ.99

[79] Λωσταράκου Κ. *Διεθνείς διαβιβάσεις δεδομένων υπό τον νέο Κανονισμό*, δημοσιευμένο σε Κοτσαλή Λ./ Μενουδάκο Κ. «Γενικός Κανονισμός για την προστασία των προσωπικών δεδομένων (GDPR) Νομική διάσταση και πρακτική εφαρμογή», σελ.363, Νομική Βιβλιοθήκη, 2020

[80] https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_el.pdf

Το ΕΣΠΔ έχει εκδώσει τις Κατευθυντήριες Γραμμές 4/2018[81] της 4ης Ιουνίου 2019 σχετικά με τη διαπίστωση των φορέων πιστοποίησης βάση του άρθρου 43 του ΓΚΠΔ, με τις οποίες επιδιώκεται η παροχή πρακτικής καθοδήγησης και ερμηνευτικής συνδρομής σχετικά με την εφαρμογή του άρθρου 43 ΓΚΠΔ.

### 3.2.3 Παρεκκλίσεις για ειδικές καταστάσεις

Ως έσχατη λύση για τις διαβιβάσεις σε τρίτες χώρες προτείνονται κάποιες παρεκκλίσεις (α.49 ΓΚΠΔ), οι οποίες θα πρέπει να είναι εξαιρετικού χαρακτήρα. Το ως άνω άρθρο χρήζει συσταλτικής ερμηνείας και τυγχάνει εφαρμογής μόνο σε επεξεργασίες περιστασιακού ή μη επαναλαμβανόμενου χαρακτήρα[82]. Οι παρεκκλίσεις δεν παρέχουν από μόνες τους προστασία για τις διασυνοριακές διαβιβάσεις[83], καθώς καλύπτουν τις περιπτώσεις όπου δεν παρέχεται προστασία για τις διαβιβάσεις αυτές στην χώρα προορισμού των δεδομένων. Στην πραγματικότητα γίνονται δεκτές μόνο εφόσον μια επεξεργασία έχει ελάχιστο κίνδυνο ή εφόσον η χρήση τους ευνοεί κοινωνικά συμφέροντα, που υπερισχύουν άλλων δικαιωμάτων και συμφερόντων.

Διαβίβαση, χωρίς απόφαση επάρκειας ή κατάλληλων εγγυήσεων, μπορεί να γίνει κατ'εξαίρεση μόνο εάν συντρέχουν οι παρακάτω περιπτώσεις, ήτοι εφόσον: α) έχει δοθεί η συγκατάθεση του υποκειμένου των δεδομένων, κατόπιν ενημέρωσής του για τους πιθανούς κινδύνους μιας τέτοιας διαβίβασης, ή β) απαιτείται για την εκτέλεση μιας σύμβασης μεταξύ του υποκειμένου των δεδομένων και του υπευθύνου επεξεργασίας ή για την εφαρμογή προσυμβατικών μέτρων, γ) για την εκτέλεση σύμβασης που συνήφθη προς όφελος του υποκειμένου μεταξύ υπευθύνου και άλλου νομικού ή φυσικού προσώπου, για την οποία είναι απαραίτητη η προηγούμενη διαβίβαση, δ) για λόγους δημοσίου συμφέροντος, ε) για τη θεμελίωση, άσκηση ή υπεράσπιση νομικών αξιώσεων, στ) για την προστασία ζωτικών συμφερόντων του υποκειμένου των δεδομένων ή άλλων προσώπων, όταν το υποκείμενο είναι φυσικά ή νομικά ανίκανο να δώσει συγκατάθεση, ζ) τα δεδομένα λαμβάνονται από μητρώο ανοιχτό στο κοινό ή ύστερα από αίτημα σε πρόσωπο που μπορεί να θεμελιώσει έννομο συμφέρον και η) για επιτακτικά έννομα συμφέροντα.

Παράλληλα με την υιοθέτηση των παρεκκλίσεων, θα πρέπει να εκτιμάται κατά πόσο συντρέχει η ανάγκη εφαρμογής πρόσθετων μέτρων, ούτως ώστε να επιτευχθεί επίπεδο επάρκειας προστασίας των δεδομένων υπό διαβίβαση, το οποίο να είναι ισοδύναμο με αυτό της ΕΕ.

---

[81] Κατευθυντήριες γραμμές 1/2019 σχετικά με τους Κώδικες Δεοντολογίας και τους Φορείς Παρακολούθησης στο πλαίσιο του Κανονισμού 2016/679, διαθέσιμο σε https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_el.pdf

[82] 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, διαθέσιμο σε https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/recommendations-012020-measures-supplement_el

[83] Christopher Kuner, *Territorial Scope and Data Transfer Rules in the GPPR: Realising the EU's ambition of borderless Data protection*, σελ. 15, Legal Studies Research Paper Series by University of Cambride, April 2021, διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3827850

### 3.2.4 Οδηγία 2016/680/ΕΕ[84]

Παράλληλα με τον ΓΚΠΔ, η Οδηγία 2016/680/ΕΕ επίσης ενσωματώθηκε στην ελληνική έννομη τάξη με τον Ν.4624/2019. Η ως άνω οδηγία ρυθμίζει τα θέματα της προστασίας των υποκειμένων των δεδομένων έναντι της επεξεργασίας των δεδομένων τους από τις αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων. Τα σχετικά με τις ως άνω διαβιβάσεις θέματα ρυθμίζονται στα άρθρα 75 έως 78 του ως άνω νόμου.

Στο άρθρο 75 του Ν. 4624/2019 προβλέπονται αντίστοιχα οι διαβιβάσεις βάσει αποφάσεως επάρκειας[85], δίνοντας όμως τη διακριτική ευχέρεια στον υπεύθυνο επεξεργασίας να μην τις πραγματοποιήσει -ακόμη και αν συντρέχει λόγος δημοσίου συμφέροντος- εφόσον εκείνος κρίνει ότι δεν παρέχεται επαρκές πλαίσιο προστασίας των δικαιωμάτων του υποκειμένου των δεδομένων. Στη συνέχεια, στο άρθρο 76 προβλέπεται η διαβίβαση ελλείψει απόφασης επάρκειας, μέσω του μηχανισμού των κατάλληλων εγγυήσεων, δηλαδή με νομικά δεσμευτική πράξη, και πάντα κατόπιν θετικής αξιολόγησης του υπευθύνου προστασίας. Το άρθρο 77 προβλέπει τη διαβίβαση βάσει ειδικών καταστάσεων και τέτοιες μπορεί να είναι η αναγκαιότητα μιας τέτοιας διαβίβασης, η προστασία του ζωτικού συμφέροντος του υποκειμένου, ή των εννόμων συμφερόντων του, για την πρόληψη άμεσης και σοβαρής απειλής για τη δημόσια ασφάλεια μιας χώρας, και σε εξατομικευμένες περιστάσεις όπως για τους σκοπούς του άρθρου 43 (πρόληψη, διερεύνηση, ανίχνευση, δίωξη ποινικών αδικημάτων ή εκτέλεση ποινικών κυρώσεων) ή για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων που σχετίζονται με το ως άνω άρθρο. Τέλος, το άρθρο 78 του ως άνω νόμου αναφέρεται στις διαβιβάσεις απευθείας προς αποδέκτες εγκατεστημένους σε τρίτες χώρες, και όχι στις αρμόδιες κρατικές αρχές, εφόσον βέβαια πληρούνται οι προϋποθέσεις που αναλυτικά απαριθμούνται στο άρθρο αυτό.

Κάνοντας μια σύγκριση μεταξύ του ΓΚΠΔ και της Οδηγίας 2016/680 συμπεραίνουμε ότι η ως άνω οδηγία παρέχει αυστηρότερο πλαίσιο από τον ΓΚΠΔ σχετικά με τη διασυνοριακή διαβίβαση προσωπικών δεδομένων. Αυτό εν μέρει είναι αναμενόμενο καθώς η ως άνω οδηγία ρυθμίζει θέματα ιδιαίτερα ευαίσθητα και μεγάλης σημασίας, που μπορεί να οδηγήσουν σε πιθανές καταδίκες, εκτέλεση ποινών κλπ στο τρίτο κράτος[86]. Επίσης, αξίζει να σημειωθεί ότι η ως άνω οδηγία δίνει στον υπεύθυνο επεξεργασίας τεράστια διακριτική ευχέρεια να απορρίψει κάποια διαβίβαση, παρά την ύπαρξη απόφασης επάρκειας, εκδοθείσας από την Επιτροπή. Καλείται, λοιπόν, εκείνος να προβεί σε στάθμιση του δημοσίου συμφέροντος που διευκολύνεται από τη διαβίβαση έναντι της προστασίας των θεμελιωδών δικαιωμάτων του υποκειμένου των δεδομένων.

### 3.2.5 Οδηγία 2016/681[87]

Η Οδηγία 2016/681 ενσωματώθηκε στην ελληνική έννομη τάξη με τον νόμο 4579/2018. Αφορά τα δεδομένα PNR (Passenger Name Record), τα οποία αποτελούν

---

[84] https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016L0680&from=DE

[86] Παναγοπούλου-Κουτνατζή Φ., *Συνταγματικές προεκτάσεις των μηχανισμών διευρύνσεως της προστασίας δεδομένων προσωπικού χαρακτήρα πέραν της ΕΕ: Εξωεδαφική εφαρμογή του ΓΚΠΔ και διασυνοριακή διαβίβαση δεδομένων*, ΔΙΤΕ (π, ΔΙΜΕΕ 4/2019)

[87] https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016L0681&from=EN

πληροφορίες που παρέχουν οι επιβάτες και συλλέγονται από τις αεροπορικές εταιρίες κατά τη διαδικασία κράτησης και ελέγχου των εισιτηρίων. Τα ως άνω δεδομένα τα επεξεργάζονται ταξιδιωτικά γραφεία, ταξιδιωτικοί πράκτορες και πολλοί άλλοι και περιλαμβάνουν διάφορους τύπους πληροφοριών όπως ημερομηνίες ταξιδιού, δρομολόγια ταξιδιών, πληροφορίες εισιτηρίων, στοιχεία επικοινωνίας κλπ. Η αξιολόγηση των στοιχείων αυτών θα μπορούσε να οδηγήσει δυνητικά στην πρόληψη, ανίχνευση, διερεύνηση και πρόληψη τρομοκρατικών και σοβαρών εγκλημάτων. Τα στοιχεία PNR διαβιβάζονται σε τρίτες χώρες κατόπιν σύναψης σχετικών συμφωνιών.

### 3.2.6 Κανονισμός (ΕΕ) 2018/1725[88]

Ο ως άνω κανονισμός 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 παρουσιάζει σημαντικό πρακτικό ενδιαφέρον για τις διαβιβάσεις καθώς τα θεσμικά όργανα και οι οργανισμοί της ΕΕ – αλλά και οι υπεργολάβοι τους- επεξεργάζονται πολλά προσωπικά δεδομένα σε επίπεδο ΕΕ. Επιδιώκεται η εναρμόνιση στην πράξη των διατάξεων του ΓΚΠΔ με τον ως άνω κανονισμό, έτσι ώστε να μην υφίστανται αποκλίσεις που παρακωλύουν την ανταλλαγή των δεδομένων αυτών μεταξύ των οργάνων της ΕΕ, των κρατών μελών του ΕΟΧ, των τρίτων χωρών αλλά και των διεθνών οργανισμών[89].

### 3.3. Το καθεστώς διαβιβάσεων στο Ηνωμένο Βασίλειο

Δημοσιεύθηκε τον Οκτώβριο του 2021 στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης απόφαση της Επιτροπής περί επάρκειας προστασίας των προσωπικών δεδομένων από το Ηνωμένο Βασίλειο (εφεξής 'ΗΒ'), με την οποία διαπιστώθηκε ότι το ως άνω κράτος παρέχει την απαιτούμενη προστασία των προσωπικών δεδομένων. Η ισχύς της απόφασης αυτής λήγει στις 27 Ιουνίου 2025, εκτός και εάν παραταθεί σύμφωνα με την προβλεπόμενη στο άρθρο 93 παρ. 2 του ΓΚΠΔ διαδικασία.

Η Επιτροπή διαπίστωσε ότι το ΗΒ συνεχίζει να συμμορφώνεται με τους κανόνες του ΓΚΠΔ, που εφάρμοζε στην προ- Brexit εποχή, δηλαδή μέχρι τις 31.12.2020,[90] και ότι κατά συνέπεια εξασφαλίζει επαρκές επίπεδο προστασίας των προσωπικών δεδομένων που διαβιβάζονται εντός του πεδίου εφαρμογής του ΓΚΠΔ από την ΕΕ στο ΗΒ. Ρητά εξαιρείται της ανωτέρω απόφασης επάρκειας, η διαβίβαση προσωπικών δεδομένων που αφορούν στους σκοπούς ελέγχου της μετανάστευσης του ΗΒ (Data Protection Act 2018).

Περαιτέρω, τέθηκαν σε ισχύ στις 21 Μαρτίου 2022 νέοι κανόνες για διασυνοριακές διαβιβάσεις προσωπικών δεδομένων από το ΗΒ. Η Αρχή Προστασίας Δεδομένων του ΗΒ (Information Commissioner's Office) υιοθέτησε τα παρακάτω νέα κείμενα[91]: α) τη Συμφωνία για διασυνοριακές διαβιβάσεις δεδομένων (IDTA- International Data Transfer

---

[88] https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32018R1725

[89] Παλιού Ε. *Οι νέες τυποποιημένες συμβατικές ρήτρες της Ευρωπαϊκής Επιτροπής- Η διασυνοριακή διαβίβαση προσωπικών δεδομένων στον απόηχο της νομολογίας Schrems (αποφάσεις του ΔΕΕ υπ'αριθμ. C362/14 και C-311/18),* ΔΙΜΕΕ 4/2021, σελ. 536

[90] https://ec.europa.eu/commission/presscorner/detail/ro/ip_21_3183

[91] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/

Agreement), β) την Τροποποίηση των εν ισχύ τυποποιημένων συμβατικών ρητρών σχετικά με τις διασυνοριακές διαβιβάσεις δεδομένων (UK Addendum- International data transfer Addendum to the European Commission's standard contractual clauses for international data transfers) και γ) ένα κείμενο με μεταβατικές διατάξεις.

Σύμφωνα με τα ανωτέρω, οι εξαγωγείς των δεδομένων θα μπορούν εφεξής να χρησιμοποιούν μόνο την παραπάνω Συμφωνία, ή τις νέες τυποποιημένες συμβατικές ρήτρες, ως τροποποιηθείσες ισχύουν, ως μέσο διαβίβασης προκειμένου να συμμορφώνονται με το άρθρο 46 του ΓΚΠΔ του ΗΒ, όταν διεξάγουν διαβιβάσεις που υπόκεινται σε έλεγχο. Το ως άνω κείμενο τροποποιεί τις ισχύουσες μέχρι την 21.3.2022 τυποποιημένες συμβατικές ρήτρες, λόγω επικαιροποίησής τους σε συνάρτηση με την απόφαση του ΔΕΕ 'Schrems II'.

Η χρήση των τυποποιημένων συμβατικών ρητρών αποτελεί το πιο δημοφιλές μέσο διαβίβασης δεδομένων, ενώ συνδυαστικά με αυτές πρέπει να εξασφαλίζονται τα δικαιώματα και η δικαστική προστασία των υποκειμένων των οποίων τα δεδομένα διαβιβάζονται.

**4. Μηχανισμοί διαβίβασης δεδομένων προς τις ΗΠΑ**

Οι συμφωνίες «Ασφαλούς Λιμένα» (Safe Harbour) και «Ασπίδα Προστασίας ΕΕ-ΗΠΑ για την ιδιωτικότητα» (Privacy Shield), οι οποίες είχαν ψηφιστεί από την Ευρωπαϊκή Επιτροπή, αποτέλεσαν για πολλά χρόνια την κύρια νομική βάση για τη διασυνοριακή διαβίβαση προσωπικών δεδομένων από την ΕΕ προς τις ΗΠΑ[92]. Στην ουσία αποτελούσαν αποφάσεις επάρκειας, οι οποίες -κατόπιν σχετικών προσφυγών του κ.Schrems- αμφότερες τελικά κρίθηκαν ανίσχυρες, λόγω του ότι δεν πληρούσαν τις προϋποθέσεις επάρκειας για την προστασία των προσωπικών δεδομένων. Επί των ως άνω προσφυγών εκδόθηκαν οι κατωτέρω αποφάσεις οι οποίες είναι γνωστές ως 'Schrems I' και 'Schrems II'.

α)**Αρχές του Ασφαλούς Λιμένα**

Ελλείψει ειδικής νομοθεσίας προστασίας προσωπικών δεδομένων μεταξύ ΕΕ και ΗΠΑ, οι διαβιβάσεις που γινόντουσαν από χώρες ΕΕ προς τις ΗΠΑ ρυθμίζονταν από τις 'Αρχές του Ασφαλούς Λιμένα'('Safe Harbor Privacy Principles'), οι οποίες θεσπίστηκαν με την υπ'αρ. 2000/520 απόφαση της Επιτροπής.

Σύμφωνα με την ως άνω απόφαση εξασφαλιζόταν ασφαλές επίπεδο προστασίας των δεδομένων που διαβιβάζονταν στις ΗΠΑ εφόσον οι οργανισμοί που εισήγαγαν δεδομένα τηρούσαν τις αρχές αυτές. Η εν λόγω απόφαση προέβλεπε ένα σύνολο κανόνων για την προστασία των προσωπικών δεδομένων, και οι κανόνες αυτοί αποτελούσαν τεκμήριο επαρκούς προστασίας και δέσμευαν τις αμερικανικές εταιρίες. Οι αρχές αυτές περιλαμβάνονταν σε έναν κατάλογο που τηρείτο στο Υπουργείο Εμπορίου των ΗΠΑ.

Το Δικαστήριο της Ευρωπαϊκής Ένωσης (εφεξής 'ΔΕΕ') εξέδωσε επί της υπ'αρ. C-362/14 υπόθεσης, την από 6.10.2015 απόφαση ('Schrems κατά Data Protection Commissioner', γνωστή και ως 'Schrems I'), η οποία έκρινε ως ασύμβατες με την προστασία των προσωπικών δεδομένων τις αρχές του ασφαλούς λιμένα. Η εν λόγω δικαστική απόφαση ακύρωσε την υπ'αρ.2000/520 απόφαση της Επιτροπής λόγω της αποκάλυψης της διαρροής των δεδομένων αυτών στις Υπηρεσίες Ασφαλείας των ΗΠΑ.

[92] https://www.lawspot.gr/nomika-blogs/spiros_tassis/pros-mia-nea-symfonia-diatlantikis-diavivasis-dedomenon?fbclid=IwAR0WeRq_xty-Pn8TJWqj8oJrN9JXH_905ALa-1G0ERV0T2RmPKN-Q2xubpk

Κρίθηκε λοιπόν ότι το ευρωπαϊκό επίπεδο προστασίας των προσωπικών δεδομένων στις ΗΠΑ δεν παρείχε επαρκή προστασία.

**β) Ασπίδα Προστασίας ΕΕ- ΗΠΑ για την ιδιωτικότητα**

Σε συνέχεια των ανωτέρω εξελίξεων, και κατόπιν διαπραγματεύσεων της Ευρωπαϊκής Ένωσης με τις ΗΠΑ για την υιοθέτηση αυστηρότερου πλαισίου προστασίας των προσωπικών δεδομένων, στις 12 Ιουλίου του 2016 καταρτίσθηκε μεταξύ της Ευρωπαϊκής Ένωσης και των ΗΠΑ, η νέα συμφωνία «Ασπίδα Προστασίας ΕΕ-ΗΠΑ για την ιδιωτικότητα» (EU-US Privacy Shield). Προβλέφθηκε με την ως άνω απόφαση ετήσια επανεξέταση της εφαρμογής του ως άνω μηχανισμού από την Ευρωπαϊκή Επιτροπή και το Υπουργείο Εμπορίου των ΗΠΑ, και τυχόν επαναδιαπραγμάτευση των όρων διαβίβασης των προσωπικών δεδομένων μεταξύ της ΕΕ και των ΗΠΑ, εφόσον αυτό κρινόταν αναγκαίο.

Η «Ασπίδα Προστασίας» προέβλεπε αυστηρότερες υποχρεώσεις για τις αμερικανικές εταιρίες που προσχώρησαν στην εν λόγω συμφωνία. Κατόπιν της αυτόβουλης προσχώρησης και αυτοπιστοποίησής τους, οι επιχειρήσεις που εντάχθηκαν στη συμφωνία αυτή έπρεπε να τηρούν τις παρακάτω αρχές της «Ασπίδας Προστασίας» δηλαδή κοινοποίηση, επιλογή, ασφάλεια, ακεραιότητα, περιορισμό του σκοπού της επεξεργασίας, πρόσβαση, ευθύνη για περαιτέρω διαβιβάσεις, προσφυγή, επιβολή, ευθύνη[93]. Η «Ασπίδα Προστασίας» προέβλεπε εντατικοποίηση του ελέγχου των πιστοποιημένων επιχειρήσεων από το Υπουργείο Εμπορίου των ΗΠΑ.

Παράλληλα, θεσπίστηκαν τρεις νέοι μηχανισμοί επίλυσης διαφορών, στις περιπτώσεις κατά τις οποίες τα υποκείμενα των δεδομένων θεωρούσαν ότι έγινε παραβίαση των προσωπικών τους δεδομένων, όπως α) δυνατότητα υποβολής καταγγελίας απευθείας στην εταιρία που επεξεργάστηκε τα δεδομένα, ή β) προσφυγής σε «ανεξάρτητο μηχανισμό», χωρίς χρέωση, ή γ) δυνατότητα υποβολής- εκ μέρους των κρατών μελών- καταγγελίας στις κρατικές εποπτικές αρχές προστασίας δεδομένων, η οποία εν συνεχεία θα προωθούταν στο Υπουργείο Εμπορίου των ΗΠΑ. Μόνο κατόπιν εξάντλησης των ανωτέρω μέσων, τα υποκείμενα των δεδομένων μπορούσαν να προσφύγουν στην ειδική διαδικασία διαιτησίας στην Ασπίδα Προστασίας. Η διαδικασία αυτή επείχε δεσμευτικά αποτελέσματα.

Επίσης, δόθηκε η ευκαιρία στις εταιρίες να συνεργάζονται απευθείας με τις ευρωπαϊκές εποπτικές αρχές προστασίας δεδομένων. Οι εταιρίες που συμμετείχαν στην «Ασπίδα Προστασίας» υπόκειντο σε τακτικό έλεγχο από το Υπουργείο Εμπορίου των ΗΠΑ προκειμένου να ελέγχεται η συμμόρφωσή τους, και σε περίπτωση μη συμμόρφωσής τους διαγραφόντουσαν από τον κατάλογο των εταιριών.

**γ) Αποφάσεις ΔΕΕ: Schrems I και Schrems II**

Ήδη από το 2013 ο Maximilian Schrems, αυστριακός δικηγόρος και ακτιβιστής σε θέματα προστασίας προσωπικών δεδομένων, αμφισβητούσε τις διαβιβάσεις των δεδομένων του (και εν γένει των Ευρωπαίων πολιτών) στις ΗΠΑ από την εταιρία Facebook Ireland σε διακομιστές της Facebook Inc, που είναι εγκατεστημένοι στις ΗΠΑ, όπου τα δεδομένα αυτά υπόκεινται σε επεξεργασία.

[93] Ιγγλεζάκης Ι., *Η ασπίδα προστασίας ΕΕ-ΗΠΑ για την ιδιωτικότητητα (EU-U.S Privacy Shield)*, ΣΥΝ, 113/2016, σελ.68-71

Στην υπ'αρ. C362/2014 υπόθεση του Ευρωπαϊκού Δικαστηρίου της Ευρωπαϊκής Ένωσης (εφεξής 'ΔΕΕ)', ο Maximilian Schrems κατάφερε να εκδοθεί η από 6 Οκτωβρίου 2015 απόφαση (εφεξής 'Schrems I')[94], με την οποία κρίθηκε ανίσχυρη η υπ'αρ. 2000/520 απόφαση (αρχές ασφαλούς λιμένα για την προστασία της ιδιωτικής ζωής).

Ο Schrems αρχικά υπέβαλε καταγγελία στον Επίτροπο της Ιρλανδικής Αρχής Προστασίας Δεδομένων, αμφισβητώντας την εγκυρότητα διαβίβασης- εκ μέρους της Facebook Ιρλανδίας- δεδομένων του στις ΗΠΑ, και τη νομιμότητα της απόφασης 'Ασφαλούς Λιμένα', ζητώντας επί της ουσίας να απαγορευτούν οι διαβιβάσεις αυτές. Ισχυρίστηκε ότι το δίκαιο και οι πρακτικές των ΗΠΑ δεν εξασφαλίζουν ικανοποιητικό επίπεδο προστασίας των προσωπικών δεδομένων που διαβιβάζονται στις ΗΠΑ, στα οποία μπορούν να έχουν πρόσβαση οι δημόσιες αρχές των ΗΠΑ. Ο Επίτροπος απέρριψε την καταγγελία του, με την αιτιολογία ότι η Επιτροπή είχε διαπιστώσει μέσω της απόφασης 'ασφαλούς λιμένα' 2000/520 ότι οι ΗΠΑ εξασφάλιζαν επαρκές επίπεδο προστασίας. Ο Schrems προσέβαλε την ως άνω απορριπτική απόφαση στο High Court και στη συνέχεια το προαναφερθέν δικαστήριο έθεσε προδικαστικό ερώτημα στο ΔΕΕ.

Τελικά, το ΔΕΕ έκρινε τη συμφωνία για τις «Αρχές Ασφαλούς Λιμένα» ως ανίσχυρη, καθώς θεώρησε ότι υιοθετώντας το άρθρο 3 της ως άνω συμφωνίας, η Επιτροπή υπερέβη των εξουσιών της, παρακάμπτοντας τη διαδικασία της επάρκειας προστασίας δεδομένων που θα έπρεπε να είχε ακολουθηθεί με βάση την Οδηγία 95/46/ΕΚ. Το High Court εν συνεχεία ακύρωσε την απορριπτική απόφασή του επί της καταγγελίας του Schrems και παρέπεμψε την καταγγελία στον Επίτροπο Προσωπικών Δεδομένων. Η Facebook εντωμεταξύ στις εξηγήσεις της προς αυτόν ανέφερε ότι η πλειοψηφία των διαβιβάσεων δεδομένων που γίνονται στην Facebook Inc. γίνεται βάσει τυποποιημένων συμβατικών ρητρών προστασίας δεδομένων, οι οποίες περιλαμβάνονται στο παράρτημα της αποφάσεως 2016/2297 της Επιτροπής.

Η απόφαση 'Schrems I' αποτέλεσε το έναυσμα για την υιοθέτηση εκ μέρους της Επιτροπής στις 12.7.2016 της «Ασπίδας Προστασίας της Ιδιωτικής Ζωής» (Privacy Shield Agreement). Οι όροι της συμφωνίας, με τους οποίους πρέπει να συμμορφώνονται οι αμερικανικές επιχειρήσεις που έχουν αυτοπιστοποιηθεί, θα αναλυθούν κατωτέρω.

**δ) Η δικαστική απόφαση Schrems II**

Το ΔΕΕ εξέδωσε την από 16.7.2020 απόφαση 'Schrems II', η οποία έχει σημαντικό αντίκτυπο στην παροχή των υπηρεσιών υπολογιστικού νέφους. Οι πελάτες των υπηρεσιών νέφους των ΗΠΑ πρέπει εφεξής και οι ίδιοι να διαπιστώνουν ότι η χώρα προς την οποία διαβιβάζονται τα δεδομένα συμμορφώνεται με τη νομοθεσία των προσωπικών δεδομένων, να διεξάγουν εκτίμηση ρίσκου και να συνεργάζονται με τους πελάτες τους.

Το ΔΕΕ εξέδωσε την ως άνω απόφαση στα πλαίσια εξέτασης της υπόθεσης C311/18[95] (Επίτροπος της Αρχής Προστασίας της Ιρλανδίας κατά Facebook & Max Schrems) και έκρινε την «Ασπίδα Προστασίας Ιδιωτικότητας μεταξύ ΕΕ- ΗΠΑ» (απόφαση Επιτροπής 2016/250) ανίσχυρη, θεωρώντας ότι δεν παρέχεται επάρκεια προστασίας μέσω αυτής.

Το αιτούν δικαστήριο, δηλαδή το High Court of Justice, υπέβαλε προδικαστικό αίτημα για το εάν ο ΓΚΠΔ έχει εφαρμογή επί των διαβιβάσεων προσωπικών δεδομένων που στηρίζονται στις τυποποιημένες ρήτρες προστασίας που περιλαμβάνονται στην

[94] https://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=EL

[95] https://curia.europa.eu/juris/liste.jsf?num=C-311/18

απόφαση 2010/87, ως προς το επίπεδο προστασίας που απαιτείται για μια τέτοια διαβίβαση και τις υποχρεώσεις των εποπτικών αρχών στο πλαίσιο αυτό.

Στα πλαίσια, λοιπόν, ένδικης διαφοράς μεταξύ του Επίτροπου της Ιρλανδικής Αρχής Προστασίας Δεδομένων, της Facebook Ιρλανδίας και του Maximilian Schrems, με αντικείμενο την καταγγελία του τελευταίου σχετικά με τη διαβίβαση προσωπικών δεδομένων του από την Facebook Ιρλανδίας στην Facebook Inc. στις ΗΠΑ, βάσει των τυποποιημένων ρητρών προστασίας, που περιλαμβάνονται στο Παράρτημα της αποφάσεως 2010/87, το High Court της Ιρλανδίας υπέβαλε στο ΔΕΕ αίτηση προδικαστικής απόφασης με τα κάτωθι αιτήματα:

α) την ερμηνεία του άρθρου 3 παρ.2, α΄περίπτωση, που αφορά στο πεδίο εφαρμογής της Οδηγίας 95/46/ΕΚ και των άρθρων 25 και 26 και 28 παρ.3, σε συνδυασμό με τα άρθρα 7, 8 και 47 του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, της Οδηγίας 95/46/ΕΚ, και γενικότερα σχετικά με το αν η ως άνω διαβίβαση εμπίπτει στον ΓΚΠΔ,

β) την ερμηνεία και το κύρος της απόφασης 2010/87/ΕΕ της Επιτροπής σχετικά με τις τυποποιημένες συμβατικές ρήτρες για τη διαβίβαση προσωπικών δεδομένων σε εκτελούντες επεξεργασία εγκατεστημένους σε τρίτες χώρες, βάσει της Οδηγίας 95/46/ΕΚ, όπως τροποποιήθηκε με την εκτελεστική απόφαση 2016/2297 της Επιτροπής, και

γ) την ερμηνεία και το κύρος της εκτελεστικής απόφασης ΕΕ 2016/1250 της Επιτροπής σχετικά με την επάρκεια της προστασίας που παρέχεται από την «Ασπίδα Προστασίας της Ιδιωτικής Ζωής» (εφεξής 'ΑΠΙΖ').

Επί του υπό στοιχεία (α) αιτήματος ανωτέρω, το ΔΕΕ απεφάνθη ότι εμπίπτει στο πεδίο εφαρμογής του ΓΚΠΔ και το δίκαιο της Ένωσης εν γένει η διαβίβαση προσωπικών δεδομένων, η οποία πραγματοποιείται για εμπορικούς σκοπούς από οικονομικό φορέα εγκατεστημένο σε κράτος μέλος της ΕΕ προς άλλον οικονομικό φορέα εγκατεστημένο σε τρίτη χώρα, ανεξάρτητα από το εάν κατά τη διάρκεια ή μετά την εν λόγω διαβίβαση, τα δεδομένα ενδέχεται να τύχουν επεξεργασίας από τις αρχές της τρίτης χώρας για λόγους εθνικής ασφάλειας, εθνικής άμυνας και ασφάλειας του κράτους (σκέψη 89 της απόφασης Schrems II). Η επεξεργασία αυτή από αρχές τρίτης χώρας, προσθέτει το ΔΕΕ, δεν συνεπάγεται ότι τέτοια διαβίβαση πρέπει να εξαιρείται από το πεδίο εφαρμογής του Κανονισμού.

Επί του υπό στοιχεία (β) αιτήματος, το ΔΕΕ απεφάνθη ότι κατά την εξέταση της από 2010/87/ΕΕ απόφασης υπό το πρίσμα του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, δεν προέκυψε κανένα στοιχείο ικανό να πλήξει το κύρος της. Δεν θίγεται η απόφαση 2010/87/ΕΕ, διευκρίνισε το ΔΕΕ, επειδή απλώς και μόνο οι τυποποιημένες ρήτρες προστασίας, λόγω του συμβατικού τους χαρακτήρα, δεν έχουν δεσμευτική ισχύ έναντι των αρχών της τρίτης χώρας προς την οποία διαβιβάζονται τα δεδομένα. Αντιθέτως, το κύρος αυτών εξαρτάται από το αν συμπεριλαμβάνει μηχανισμούς ικανούς να διασφαλίσουν αποτελεσματικά στην πράξη την τήρηση του απαιτούμενου επίπεδου προστασίας βάσει του ενωσιακού δικαίου, καθώς και από το εάν διασφαλίζεται ότι οι διαβιβάσεις προσωπικών δεδομένων βάσει των τυποποιημένων ρητρών θα αναστέλλονται ή ανατρέπονται σε περίπτωση παράβασής τους ή αδυναμίας τήρησής τους.

Και πράγματι, η απόφαση 2010/87/ΕΕ προβλέπει τους ως άνω μηχανισμούς, προκειμένου να είναι επιτρεπτή διαβίβαση δεδομένων σε εκτελούντες την επεξεργασία εκτός ΕΕ, αφού αφενός υποχρεώνει τον εξαγωγέα των δεδομένων και τον αποδέκτη της διαβίβασης να ελέγχουν εκ των προτέρων εάν το επίπεδο προστασίας των

διαβιβαζόμενων δεδομένων που τηρείται στην οικεία τρίτη χώρα είναι το απαιτούμενο, και αφετέρου εγκαθιδρύει υποχρέωση του αποδέκτη των δεδομένων να ενημερώνει τον εξαγωγέα για τυχόν αδυναμία εκ μέρους του τήρησης των τυποποιημένων ρητρών προστασίας, οπότε και δεσμεύεται να αναστείλει τη διαβίβαση ή/και να καταγγείλει τη μεταξύ τους σύμβαση.

Ως προς το υπό στοιχεία (γ) προδικαστικό αίτημα, που αφορά στην ερμηνεία και στο κύρος της απόφασης 2016/1250 «Ασπίδα προστασίας ΕΕ-ΗΠΑ για την ιδιωτικότητα», το ΔΕΕ το εξέτασε με βάση τον ΓΚΠΔ, τις διατάξεις του Χάρτη των Θεμελιωδών Δικαιωμάτων, που προασπίζουν το σεβασμό της ιδιωτικής και οικογενειακής ζωής, την προστασία των προσωπικών δεδομένων αλλά και με βάση την αποτελεσματική δικαστική προστασία των υποκειμένων των οποίων τα δεδομένα διαβιβάζονται.

Αρχικά το ΔΕΕ επεσήμανε ότι τόσο η απόφαση 2016/1250 όσο και η 2000/520 (απόφαση ασφαλούς λιμένα) καθιερώνουν την υπεροχή των απαιτήσεων που αφορούν την εθνική ασφάλεια, το δημόσιο συμφέρον και την τήρηση της αμερικανικής νομοθεσίας, επιτρέποντας έτσι τυχόν επέμβαση στα θεμελιώδη δικαιώματα των υποκειμένων των οποίων τα δεδομένα διαβιβάζονται προς την τρίτη χώρα[96].

Το ΔΕΕ απεφάνθη ότι η κανονιστική νομοθεσία των ΗΠΑ δεν περιορίζει τις αμερικανικές δημόσιες αρχές ως προς την προστασία των προσωπικών δεδομένων στο απολύτως αναγκαίο, ιδιαίτερα αναφορικά με τα προγράμματα παρακολούθησης (Prism, Upstream) των ΗΠΑ, με αποτέλεσμα να μην παρέχεται ισοδύναμο επίπεδο προστασίας με αυτό που επιβάλει η ευρωπαϊκή νομοθεσία. Επιπρόσθετα, παρά το ότι προβλέπονται στην κανονιστική ρύθμιση των ΗΠΑ απαιτήσεις που πρέπει να τηρούν οι αρχές των ΗΠΑ κατά την εφαρμογή των ως άνω προγραμμάτων παρακολούθησης για τους Αμερικανούς πολίτες, ωστόσο δεν προβλέπεται η ύπαρξη εγγυήσεων για τους ευρωπαίους πολίτες, τους οποίους αφορούν επίσης τα σχετικά προγράμματα, δηλαδή δεν τους παρέχονται εκτελεστά δικαιώματα που να μπορούν να αντιτάξουν έναντι των αμερικανικών αρχών ενώπιον των δικαστηρίων.

Σχετικά με την απαίτηση δικαστικής προστασίας, το ΔΕΕ διατυπώνει την άποψη ότι παρά την απόφαση της Επιτροπής για τον μηχανισμό διαμεσολάβησης που προβλέπεται σε αυτήν, ο μηχανισμός αυτός δεν προσφέρει στα υποκείμενα των δεδομένων μέσο δικαστικής προστασίας ενώπιον οργάνου που να προσφέρει εγγυήσεις ουσιαστικά ισοδύναμες με εκείνες τις οποίες επιβάλλει το δίκαιο της Ένωσης, ώστε να διασφαλίζεται η ανεξαρτησία του θεσμού αυτού, αλλά και η εξουσία να εκδίδει δεσμευτικές αποφάσεις για τις αμερικάνικες υπηρεσίες πληροφοριών.

Για όλους τους ανωτέρω λόγους, το ΔΕΕ κήρυξε την από 2016/1250 απόφαση «Ασπίδα προστασίας ΕΕ-ΗΠΑ για την ιδιωτικότητα» ανίσχυρη.

**ε) Κριτική επισκόπηση της απόφασης Schrems II**

Κάνοντας μια συνοπτική κριτική στην ως άνω απόφαση του ΔΕΕ, διαπιστώνουμε αφενός τη δύναμη της ιδιωτικής πρωτοβουλίας και συγκεκριμένα ενός μεμονωμένου ακτιβιστή, ο οποίος κατάφερε να ανατρέψει δύο διεθνικές συμφωνίες και αφετέρου την

[96] *Βόμβα από το Δικαστήριο της ΕΕ: Ανίσχυρη η απόφαση για διαβίβαση δεδομένων στις ΗΠΑ (Schrems II)*, διαθέσιμο σε lawspot.gr, δημοσιευμένο στις 16.7.2020

ανικανότητα και αδυναμία των θεσμικών οργάνων να προασπίσουν ουσιαστικά τα προσωπικά δεδομένα των φυσικών προσώπων[97].

Η ΕΕ, σε αντίθεση με τις ΗΠΑ, διακηρύσσει ότι απαγορεύονται οι διαβιβάσεις εκτός ΕΕ, πλην ορισμένων εξαιρέσεων. Η τόσο διαφορετική αντίληψη των διαβιβάσεων μεταξύ ΕΕ και ΗΠΑ αποτελεί εμπόδιο για την επίτευξη ουσιαστικού συγκερασμού των απόψεων τους και την κατάληξη σε μια κοινώς αποδεκτή συμφωνία. Επίσης, στη συγκεκριμένη απόφαση διακρίνεται και πάλι η καχυποψία του ΔΕΕ απέναντι στις μαζικές παρακολουθήσεις που επιτελούν συστηματικά οι μυστικές υπηρεσίες των ΗΠΑ.

Η απόφαση Schrems II είχε ως άμεση συνέπεια την κατάργηση της 'Ασπίδας Προστασίας για την Ιδιωτικότητα' και κατά συνέπεια οι οργανισμοί εφεξής μπορούν να καταφύγουν στις ΤΣΡ για διαβίβαση δεδομένων στις ΗΠΑ. Ωστόσο αυστηροποιείται το πλαίσιο χρήσης τους, δηλαδή καλούνται οι εξαγωγείς δεδομένων να ελέγχουν αν η τρίτη χώρα στην οποία διαβιβάζονται δεδομένα εφαρμόζει νομοθεσία ασυμβίβαστη με αυτήν της ΕΕ. Εάν δεν παρέχεται ικανοποιητικό επίπεδο προστασίας, ο εξαγωγέας πρέπει να χρησιμοποιεί πρόσθετα μέτρα. Πρακτικά οι ως άνω υποχρεώσεις κατά την υιοθέτηση των ΤΣΡ, έχουν σαν συνέπεια ότι οι μικρομεσαίες επιχειρήσεις που διαβιβάζουν δεδομένα στις ΗΠΑ θα δυσκολευτούν να εφαρμόσουν τις προϋποθέσεις αυτές, μια που δεν διαθέτουν τους οικονομικούς πόρους, αλλά ούτε την οργάνωση για να γνωρίζουν το δίκαιο της τρίτης χώρας[98]. Άρα ενδεχομένως να εγείρονται και θέματα αθέμιτου ανταγωνισμού στην περίπτωση αυτή, καθώς κάποιοι λιγότερο «ισχυροί» πάροχοι υπηρεσιών cloud εγκατεστημένοι στην ΕΕ θα βρίσκονται σε δυσμενέστερη θέση σε σχέση με κολοσσούς όπως η Facebook κλπ. οι οποίοι διαθέτουν επαρκώς καταρτισμένα νομικά τμήματα αλλά και πόρους για να υποστηρίξουν τέτοιες διαβιβάσεις.

Ένα άλλο ζήτημα που προκύπτει από την ως άνω απόφαση[99], είναι ότι δεν έχουν όλες οι τρίτες χώρες στις οποίες γίνονται διαβιβάσεις ένα ικανοποιητικό επίπεδο προστασίας προσωπικών δεδομένων. Ορισμένα κράτη αδυνατούν να προασπίσουν ακόμη και θεμελιώδη ανθρώπινα δικαιώματα, πόσω μάλλον τα ψηφιακά δικαιώματα των προσώπων. Άρα οι μεγάλοι κολοσσοί όπως για παράδειγμα οι: Facebook, Apple, Microsoft, Google, δεν νοείται να διαβιβάζουν δεδομένα σε κρατικές αρχές επιβολής του νόμου που δεν συμμορφώνονται με τις απαιτήσεις προστασίας των προσωπικών δεδομένων. Κατά συνέπεια, αυτή η απόφαση μπορεί να έχει θετικό αντίκτυπο και να δώσει το έναυσμα σε χώρες με ασθενέστερο επίπεδο προστασίας δεδομένων, όπως είναι η Ινδία ή η Κίνα, για να το ενισχύσουν.

Ανακεφαλαιώνοντας, η παρούσα απόφαση αποτελεί απόφαση-σταθμό σε πολλά επίπεδα. Θα υπάρξει καταλυτική όσον αφορά στη στάση που καλούνται να τηρήσουν οι πάροχοι υπολογιστικού νέφους στο μέλλον, όσον αφορά τις διαβιβάσεις που πραγματοποιούν. Επίσης, σε επίπεδο νομολογίας, θα αποτελέσει σημαντικό προηγούμενο στο επίπεδο των διασυνοριακών διαβιβάσεων εκτός ΕΕ.

---

[97] Καρφή Ζ. *Ανεπαρκές το επίπεδο προστασίας στις ΗΠΑ για τη μαζική διαβίβαση δεδομένων προσωπικού χαρακτήρα από οργανισμούς εγκατεστημένους στην ΕΕ*, ΕΕΕυρΔ 3/2020, σελ364

[98] Καρφή Ζ. *Ανεπαρκές το επίπεδο προστασίας στις ΗΠΑ για τη μαζική διαβίβαση δεδομένων προσωπικού χαρακτήρα από οργανισμούς εγκατεστημένους στην ΕΕ*, ΕΕΕυρΔ 3/2020, σελ. 365

[99] Καρφή Ζ. *Ανεπαρκές το επίπεδο προστασίας στις ΗΠΑ για τη μαζική διαβίβαση δεδομένων προσωπικού χαρακτήρα από οργανισμούς εγκατεστημένους στην ΕΕ*, ΕΕΕυρΔ 3/2020, σελ. 366

**στ) Ισχύον καθεστώς διαβιβάσεων προς τις ΗΠΑ- Διατλαντικό Πλαίσιο Προστασίας Προσωπικών Δεδομένων**

Στις 25.3.2022 η ΕΕ και οι ΗΠΑ κατάφεραν να καταλήξουν σε μια επικαιροποιημένη πολιτική συμφωνία για τη διασυνοριακή διαβίβαση δεδομένων προς τις ΗΠΑ ( Trans-Atlantic Data Privacy Framework)[100]. Η ως άνω συμφωνία, η οποία άτυπα αποκαλείται "Privacy Shield 2.0", σηματοδοτεί το τέλος μιας περιόδου αβεβαιότητας, που προκλήθηκε κατόπιν της έκδοσης της απόφασης Schrems II. Η ως άνω συμφωνία επιδιώκει να επιτύχει προβλεπόμενες και ασφαλείς διαβιβάσεις δεδομένων, ισοσκελίζοντας την ασφάλεια, το δικαίωμα στην ιδιωτικότητα και την προστασία των προσωπικών δεδομένων.

Οι βασικές αρχές της ως άνω συμφωνίας σχετικά με τις διαβιβάσεις που εκτελούνται από την ΕΕ στις ΗΠΑ, έγιναν γνωστές μέσω ενός κοινού δελτίου τύπου ΕΕ-ΗΠΑ, και ορίζουν τα εξής:

Η κυκλοφορία των προσωπικών δεδομένων θα γίνεται ελεύθερα και με ασφάλεια μεταξύ της ΕΕ και των συμμετεχόντων στη συμφωνία αμερικανικών εταιριών. Θεσπίζεται νέα δέσμη μέτρων και δεσμευτικών εγγυήσεων με στόχο την περιορισμένη πρόσβαση στα διαβιβαζόμενα δεδομένα από τις μυστικές υπηρεσίες των ΗΠΑ, στο βαθμό που η πρόσβαση είναι αναγκαία και πρόσφορη για την προστασία της εθνικής ασφάλειας. Οι ως άνω υπηρεσίες θα υιοθετήσουν διαδικασίες οι οποίες θα συμμορφώνονται με τα πρότυπα προστασίας της ιδιωτικότητας και των ατομικών ελευθεριών. Περαιτέρω, ιδρύεται μηχανισμός επανόρθωσης δύο επιπέδων, με επιστέγασμα τη σύσταση νέας ειδικής ανεξάρτητης αρχής, η οποία θα προσομοιάζει σε Δικαστήριο Προσωπικών Δεδομένων, ώστε να μπορούν να προσφεύγουν σε αυτό τα υποκείμενα των δεδομένων, εφόσον θεωρούν ότι τα δεδομένα τους υφίστανται παράνομες δραστηριότητες επεξεργασίας από τις μυστικές υπηρεσίες των ΗΠΑ. Εδραιώνονται ισχυρές υποχρεώσεις για τις εταιρίες που επεξεργάζονται δεδομένα που διαβιβάζονται από την ΕΕ προς τις ΗΠΑ, οι οποίες θα συνεχίσουν να έχουν την υποχρέωση να αυτοπιστοποιούνται, πάντα σε συμμόρφωση με τις επιταγές του Υπουργείου Εμπορίου. Προβλέπεται επίσης μηχανισμός ελέγχου και αναθεώρησης.

Τα οφέλη της ως άνω συμφωνίας είναι πολλαπλά. Παρέχεται μέσω αυτής επαρκής προστασία των δεδομένων των Ευρωπαίων που διαβιβάζονται στις ΗΠΑ, σε εναρμόνιση πάντα με την απόφαση Schrems II. Εγγυάται την ασφαλή διαβίβαση δεδομένων, παρέχει διαρκή και αξιόπιστη νομική βάση και ενισχύει την ψηφιακή οικονομία και την οικονομική συνεργασία των κρατών. Το τελικό κείμενο της εν λόγω συμφωνίας δεν έχει ακόμη δημοσιευτεί.

Πρακτικά δεν μεταβάλλονται πολλά με την παρούσα συμφωνία. Απλά επιλύεται το θέμα των διατλαντικών διαβιβάσεων δεδομένων. Οι Τυποποιημένες Συμβατικές Ρήτρες παραμένουν ο πιο αποτελεσματικός μηχανισμός διαβίβασης και παράλληλα με αυτές θα πρέπει να διεξάγεται η σχετική Εκτίμηση Αντικτύπου Διαβίβασης (Transfer Impact Assessment) για κάθε κατηγορία διαβίβασης.

[100] https://ec.europa.eu/commission/presscorner/detail/en/FS_22_2100

## 4. Νομικά ζητήματα κατά τη διαβίβαση προσωπικών δεδομένων εντός του υπολογιστικού νέφους

### 4.1 Η έννοια της «διαβίβασης»

Το ΕΣΠΔ εξέδωσε τον Ιούνιο του 2021 τις υπ'αρ. 05/2021 Κατευθυντήριες Γραμμές[101], οι οποίες για πρώτη φορά εξειδικεύουν την έννοια της διαβίβασης. Διατυπώνεται ότι δεν υφίσταται διαβίβαση δεδομένων όταν κάτοικοι του ΕΟΧ κοινοποιούν οι ίδιοι οικειοθελώς προσωπικά τους δεδομένα σε εταιρία εκτός ΕΟΧ. Άρα δεν απαιτείται στην ως άνω περίπτωση η εφαρμογή ενός εκ των μηχανισμών διαβίβασης που αναφέρονται στο Κεφάλαιο V του ΓΚΠΔ. Διευκρινίζεται ότι στον ΓΚΠΔ δεν υφίσταται ορισμός της διαβίβασης.

Οι ως άνω κατευθυντήριες γραμμές ορίζουν τη διαβίβαση ως τη δημοσιοποίηση προσωπικών δεδομένων από οργανισμό που υπόκειται στον ΓΚΠΔ σε άλλον οργανισμό που βρίσκεται σε «τρίτη χώρα» ή διεθνή οργανισμό. Τρεις σωρευτικές προϋποθέσεις πρέπει να συντρέχουν προκειμένου να υφίσταται διαβίβαση και αυτές είναι οι εξής:
α) Ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία να υπόκειται στον ΓΚΠΔ για την προστασία των προσωπικών δεδομένων,
β) Ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία (εξαγωγέας δεδομένων) να καθιστά τα προσωπικά δεδομένα διαθέσιμα σε άλλον υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία (εισαγωγέα) και
γ) Ο εισαγωγέας δεδομένων να βρίσκεται σε τρίτη χώρα (ή διεθνή οργανισμό), ανεξάρτητα από το αν υπόκειται άμεσα στον ΓΚΠΔ όσον αφορά τη συγκεκριμένη επεξεργασία.

Ο ως άνω ορισμός της διαβίβασης, επιφέρει τις παρακάτω συνέπειες:
1.Το ΕΣΠΔ διατύπωσε την άποψη ότι δεν υφίσταται διαβίβαση όταν τα φυσικά πρόσωπα παρέχουν τα προσωπικά τους δεδομένα με δική τους πρωτοβουλία. Στην περίπτωση για παράδειγμα που κάποιος αγοράσει ένα προϊόν από ηλεκτρονικό κατάστημα εταιρίας εκτός ΕΕ, και συμπληρώσει τα προσωπικά του στοιχεία στο σχετικό ηλεκτρονικό έντυπο παραγγελίας, τότε η κοινοποίηση των προσωπικών του δεδομένων δεν συνιστά διαβίβαση. Εάν όμως η ίδια εταιρία, με έδρα εκτός ΕΟΧ, συλλέξει τα δεδομένα αυτά με δική της πρωτοβουλία, τότε ισχύουν οι κανόνες της διαβίβασης. Σε κάθε περίπτωση είναι κάπως ασαφές το τι ακριβώς αποτελεί πρωτοβουλία ενός υποκειμένου σχετικά με την κοινολόγηση των προσωπικών του δεδομένων και αυτό μπορεί να δημιουργήσει παρεξηγήσεις[102].
2. Το ΕΣΠΔ, μέσω των ως άνω κατευθυντήριων γραμμών, ορίζει ότι δεν τίθεται θέμα διαβίβασης όταν τα δεδομένα παραμένουν στην κατοχή του ίδιου οργανισμού εντός και εκτός ΕΕ/ΕΟΧ. Για παράδειγμα, δεν αποτελεί διαβίβαση εάν οι εργαζόμενοι μιας εταιρίας του ΕΟΧ ταξιδέψουν σε τρίτη χώρα και έχουν απομακρυσμένη πρόσβαση στο σύστημα της εταιρίας τους και κατ'επέκταση στα δεδομένα που αυτή διατηρεί. Εάν όμως διαβιβάζουν τα δεδομένα αυτά σε άλλη οντότητα εντός του ίδιου ομίλου εταιριών, τότε έχουμε διαβίβαση. Σε αυτές τις οντότητες που αποτελούν μέρος του ίδιου εταιρικού

[101] https://edpb.europa.eu/system/files/2021-11/edpb_guidelinesinterplaychapterv_article3_adopted_en.pdf

[102] Κωνσταντίνου Στ., *EDPB: Αλλάζει το τοπίο για τις Διεθνείς Διαβιβάσεις*, διαθέσιμο σε https://www.lawspot.gr/nomika-blogs/stergios_konstantinoy/edpb-allazei-topio-gia-tis-diethneis-diavivaseis-dedomenon

ομίλου μπορεί οι τελούντες επεξεργασία να χαρακτηριστούν Αυτοτελώς Υπεύθυνοι Επεξεργασίας ή Εκτελούντες την επεξεργασία.
3. Οι Κατευθυντήριες Γραμμές διευκρινίζουν επιπλέον ότι όταν ένας εκτελών την επεξεργασία εντός ΕΟΧ επεξεργάζεται προσωπικά δεδομένα για λογαριασμό Υπευθύνου Επεξεργασίας εκτός ΕΟΧ και αποστέλλει τα δεδομένα στον εν λόγω Υπεύθυνο Επεξεργασίας, πρέπει να συμμορφώνεται με τους περιορισμούς του ΓΚΠΔ για τη διαβίβαση δεδομένων. Αυτό τελεί σε σύμπνοια και με το νέο πακέτο Τυποποιημένων Συμβατικών Ρητρών (ΤΣΡ), το οποίο παρέχει μια νέα ενότητα διαβίβασης μεταξύ Εκτελούντος την Επεξεργασία προς τον Υπεύθυνο Επεξεργασίας εκτός ΕΟΧ. Αυτό το σχήμα ευνοεί περιπτώσεις όπου ο Εκτελών την Επεξεργασία υπόκειται μεν στον ΓΚΠΔ, αλλά δεν συνεπάγεται ότι η διαβίβαση δεδομένων προς τον Υπεύθυνο Επεξεργασίας απαιτεί μηχανισμό μεταφοράς προσωπικών δεδομένων από τον Εκτελούντα την επεξεργασία.

Παρά το γεγονός ότι οι Κατευθυντήριες Γραμμές δεν είναι νομικά δεσμευτικές, ωστόσο φέρουν σημαντικό βάρος καθώς αντικατοπτρίζουν την στάση και αντιμετώπιση των εποπτικών αρχών της ΕΕ αναφορικά με την ερμηνεία και την προστασία των προσωπικών δεδομένων[103]. Ωστόσο, αφήνουν ένα περιθώριο κινδύνου, γεγονός που σημαίνει ότι οι εισαγωγείς και οι εξαγωγείς των προσωπικών δεδομένων οφείλουν οι ίδιοι να προβαίνουν σε εκτίμηση ρίσκου σχετικά με το εάν μια διαβίβαση προστατεύει τα δεδομένα σε επίπεδο ισοδύναμο με αυτό που παρέχεται από τον ΓΚΠΔ.

**4.2 Οι διαβιβάσεις στο περιβάλλον του υπολογιστικού νέφους**

Η συχνή και συνεχής αλλαγή του τόπου αποθήκευσης των δεδομένων στο περιβάλλον του υπολογιστικού νέφους, αλλά και η διαβίβαση αυτών, μπορεί να εμπεριέχει διακίνηση προσωπικών δεδομένων[104], καθώς οι πάροχοι των υπηρεσιών αυτών χρησιμοποιούν υποδομές και εξοπλισμό που βρίσκονται διάσπαρτοι σε περισσότερες χώρες. Οι διαβιβάσεις στο υπολογιστικό νέφος ενέχουν κινδύνους ως προς την προστασία των προσωπικών δεδομένων των υποκειμένων των δεδομένων.

Ο ΓΚΠΔ, όπως προαναφέραμε, έχει – μεταξύ άλλων- σαν βασικό σκοπό την προστασία των προσωπικών δεδομένων κατά τη διασυνοριακή διαβίβασή τους. Οι λόγοι για τους οποίους οι διασυνοριακές διαβιβάσεις προσωπικών δεδομένων χρήζουν προστασίας[105] είναι οι εξής:

α) Τυχόν διαρροή στο διαδίκτυο και στο υπολογιστικό νέφος δεδομένων σε τρίτη μη ασφαλή χώρα, θα ακύρωνε την προστασία που παρέχει ο ΓΚΠΔ. Άρα δημιουργείται η ανάγκη για τη δημιουργία προϋποθέσεων επέκτασης του ΓΚΠΔ και σε τρίτες χώρες.

β) Η σύνθεση των διασυνοριακά διαβιβαζόμενων πληροφοριών μπορεί να οδηγήσει στη δημιουργία ενός τέλειου προφίλ των υποκειμένων των δεδομένων. Συνεπώς, οι πληροφορίες αυτές πρέπει να προστατεύονται επαρκώς και να μην μένουν εκτεθειμένες.

---

[103] *Personal Data Protection Digest* by Personal Data Protection Commission Singapore, 2021, διαθέσιμο σε https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Commissions-Decisions/2021-Personal-Data-Protection-Digest.ashx

[104] Μήτρου Λ. *Προστασία προσωπικών δεδομένων και υπολογιστικό νέφος*, ΔΙΜΕΕ 4/2015, σελ. 544

[105] Παναγοπούλου-Κουντατζή Φ., *Συνταγματικές προεκτάσεις των μηχανισμών διευρύνσεως της προστασίας των προσωπικών δεδομένων προσωπικού χαρακτήρα πέραν της ΕΕ: εξωεδαφική εφαρμογή του ΓΚΠΔ και διασυνοριακή διαβίβαση δεδομένων*, ΔΙΜΕΕ 4/2019

γ) Η διασυνοριακή διαβίβαση πληροφοριών είναι απαραίτητη για το διεθνές εμπόριο και τη διεθνή συνεργασία. Ως εκ τούτου η διακίνηση αυτών των δεδομένων είναι θεμελιώδους οικονομικής σημασίας.

δ) Μέσω της διασυνοριακής διαβίβασης δεδομένων καταδεικνύεται ότι η κάθε έννομη τάξη παρέχει το δικό της επίπεδο προστασίας. Υφίσταται ως εκ τούτου η ανάγκη εναρμόνισης της προστασίας αυτής και η δημιουργία ενός ενιαίου κανονιστικού πλαισίου για τα δεδομένα που προστατεύονται από τον ΓΚΠΔ.

Όπως προαναφέρθηκε στην παρούσα εργασία, γενική αρχή των διαβιβάσεων, άρα και στο υπολογιστικό νέφος, είναι ότι αυτές είναι ελεύθερες μεταξύ των χωρών ΕΕ/ΕΟΧ. Αντίθετα, διαβιβάσεις σε τρίτες χώρες, δηλαδή που γίνονται σε πάροχο εκτός ΕΕ/ΕΟΧ, επιτρέπονται μόνο εφόσον εφαρμόζονται οι μηχανισμοί διαβίβασης που αναλύθηκαν διεξοδικά ανωτέρω και εφόσον τηρούνται κάποιες προϋποθέσεις από τον υπεύθυνο επεξεργασίας και από τον εκτελούντα την επεξεργασία, με κοινό σκοπό ότι δεν υπονομεύεται το επίπεδο προστασίας που επιτάσσει ο ΓΚΠΔ. Οι ως άνω διαβιβάσεις προϋποθέτουν πάντα τη συμμόρφωση με τις αρχές του άρθρου 5 ΓΚΠΔ, με τις νόμιμες βάσεις του άρθρου 6 ΓΚΠΔ και με τα όσα ορίζονται στο άρθρο 9 ΓΚΠΔ σχετικά με την επεξεργασία ευαίσθητων δεδομένων.

Πρώτος έγκυρος μηχανισμός διαβίβασης θεωρείται η απόφαση επάρκειας από την Επιτροπή. Ελλείψει τέτοιας, διαβιβάσεις μπορεί να γίνουν βάσει επαρκών εγγυήσεων όσον αφορά την προστασία της ιδιωτικότητας και των θεμελιωδών δικαιωμάτων και των ελευθεριών των φυσικών προσώπων και την άσκηση των αντίστοιχων δικαιωμάτων που προκύπτουν, ιδίως από τις συμβατικές ρήτρες. Τέλος, ως έσχατο μέσο επιτρέπονται οι διαβιβάσεις βάσει παρεκκλίσεων.

Ωστόσο, μετά την απόφαση Schrems II το σκηνικό ως προς τις διαβιβάσεις σε τρίτες χώρες/διεθνείς οργανισμούς έχει διαμορφωθεί ως εξής[106]:

Ως προς τις διαβιβάσεις στις ΗΠΑ, τυχόν διαβίβαση βάσει του πλαισίου της «Ασπίδας Προστασίας της Ιδιωτικότητας», είναι παράνομη. Το ΔΕΕ κήρυξε άκυρη την ως άνω συμφωνία, λόγω του βαθμού επέμβασης που δημιουργεί η νομοθεσία των ΗΠΑ στα θεμελιώδη δικαιώματα των προσώπων, των οποίων τα δεδομένα διαβιβάζονται στην τρίτη χώρα. Τα αποτελέσματά της ως άνω απόφασης δεν διατηρούνται, καθώς κρίθηκε ότι η νομοθεσία των ΗΠΑ δεν παρείχε ισοδύναμο επίπεδο προστασίας με εκείνο της ΕΕ. Εν αναμονή λοιπόν, της οριστικοποίησης του τελικού κειμένου του Διατλαντικού Πλαισίου Προστασίας Προσωπικών Δεδομένων μεταξύ ΕΕ και ΗΠΑ, οπότε και οι διαβιβάσεις μεταξύ ΕΕ και ΗΠΑ θα μπορούν να γίνονται ελεύθερα με βάση την ως άνω συμφωνία, η οποία θα επέχει θέση απόφασης επάρκειας.

Μια λύση για τη διαβίβαση προσωπικών δεδομένων στις ΗΠΑ είναι οι ΤΣΡ, ωστόσο η διαβίβαση θα εξαρτηθεί από το αποτέλεσμα της αξιολόγησης των δεδομένων και των περιστάσεων της διαβίβασης από τον υπεύθυνο επεξεργασίας, καθώς και των πρόσθετων μέτρων που αυτός μπορεί να εφαρμόσει. Τα πρόσθετα μέτρα, θα πρέπει συνδυαστικά με τις ΤΣΡ, μετά την κατά περίπτωση ανάλυση των περιστάσεων, να διασφαλίζουν ότι η νομοθεσία των ΗΠΑ εγγυάται επαρκές επίπεδο προστασίας των προσωπικών δεδομένων. Εάν κριθεί ότι δεν επιτυγχάνεται τέτοια προστασία, ο

---

[106] ΕΣΠΔ, *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*, διαθέσιμο σε https://edpb.europa.eu/sites/default/files/files/file1/20200724_edpb_faqoncjeuc31118_el.pdf

υπεύθυνος επεξεργασίας υποχρεούται να αναστείλει ή να τερματίσει τη διαβίβαση. Εάν αποφασίσει να τη συνεχίσει παρά τα ανωτέρω, θα πρέπει να ενημερώσει την αρμόδια εποπτική αρχή. Σε κάθε περίπτωση, ο εξαγωγέας των δεδομένων μπορεί να επικοινωνεί με τον εισαγωγέα των δεδομένων στην τρίτη χώρα και να συνεργαστεί μαζί του για την ως άνω αξιολόγηση.

Το ΔΕΕ διευκρίνισε ότι οι ΤΣΡ αλλά και τα λοιπά εργαλεία διαβίβασης του α.46 ΓΚΠΔ, χρησιμοποιούνται εντός συγκεκριμένου νομικού πλαισίου. Οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία οι οποίοι δρουν ως εξαγωγείς των δεδομένων, έχουν την ευθύνη του ελέγχου ανά περίπτωση, και σε συνεργασία πολλές φορές με τους εισαγωγείς των δεδομένων στις τρίτες χώρες, ως προς το κατά πόσο το δίκαιο της τρίτης χώρας ή οι πρακτικές που χρησιμοποιούνται σε αυτήν, θίγουν την αποτελεσματικότητα των κατάλληλων εγγυήσεων του α.46 ΓΚΠΔ. Το ΔΕΕ αφήνει στους εξαγωγείς το περιθώριο να εφαρμόζουν πρόσθετα μέτρα που θα θεραπεύουν τα όποια κενά στην προστασία των προσωπικών δεδομένων και θα συντελούν στην κατάκτηση του επιπέδου προστασίας που επιτάσσει η ΕΕ. Τα παραπάνω τελούν σε αρμονία με την αρχή της λογοδοσίας του άρθρου 5.2 ΓΚΠΔ, η οποία θέλει τον υπεύθυνο επεξεργασίας να λογοδοτεί και να μπορεί να αποδείξει ότι συμμορφώνεται με τις αρχές του ΓΚΠΔ σχετικά με την επεξεργασία προσωπικών δεδομένων.

Η επιλογή των δεσμευτικών εταιρικών κανόνων για τη διαβίβαση προσωπικών δεδομένων, θα εξαρτηθεί από το αποτέλεσμα της αξιολόγησης των δεδομένων και των περιστάσεων της διαβίβασης από τον υπεύθυνο επεξεργασίας, καθώς και των πρόσθετων μέτρων που αυτός μπορεί να εφαρμόσει. Τα πρόσθετα μέτρα, θα πρέπει συνδυαστικά με τους δεσμευτικούς εταιρικούς κανόνες, μετά την κατά περίπτωση ανάλυση των περιστάσεων, να διασφαλίζουν ότι η νομοθεσία των ΗΠΑ εγγυάται επαρκές επίπεδο προστασίας τους. Αντίστοιχα με τις ΤΣΡ, εάν κριθεί ότι δεν επιτυγχάνεται τέτοια προστασία, ο υπεύθυνος επεξεργασίας υποχρεούται να αναστείλει ή να τερματίσει τη διαβίβαση. Εάν αποφασίσει να τη συνεχίσει παρά τα ανωτέρω, θα πρέπει να ενημερώσει την αρμόδια εποπτική αρχή.

Ως προς τα λοιπά εργαλεία του α.46 ΓΚΠΔ, η απόφαση Schrems II διευκρινίζει ότι για την υιοθέτηση των κατάλληλων εγγυήσεων το επιθυμητό επίπεδο προστασίας είναι αυτό της «ουσιαστικής ισοδυναμίας».

Συνεχίζει εντωμεταξύ να υφίσταται και η επιλογή των παρεκκλίσεων του άρθρου 49 ΓΚΠΔ ως μέσο διαβίβασης από τον ΕΟΧ στις ΗΠΑ, εφόσον τηρούνται οι σχετικές κατευθυντήριες γραμμές του ΕΣΠΔ. Εάν οι διαβιβάσεις βασίζονται στη συγκατάθεση, αυτή θα πρέπει να είναι ρητή, ειδική και να παρέχεται εν πλήρει επιγνώσει. Εάν οι διαβιβάσεις είναι απαραίτητες για την εκτέλεση σύμβασης μεταξύ του υπευθύνου επεξεργασίας και του υποκειμένου των δεδομένων, θα πρέπει να γίνεται δεκτή μόνο εφόσον η διαβίβαση αυτή έχει περιστασιακό χαρακτήρα. Τέλος, αν η διαβίβαση γίνεται για σημαντικούς λόγους δημοσίου συμφέροντος, το ΕΣΠΔ διατυπώνει την άποψη ότι πρέπει να διαπιστωθεί σημαντικό δημόσιο συμφέρον, πάλι όμως λαμβάνοντας υπόψη ότι δεν μπορεί να εφαρμοστεί σε μεγάλη κλίμακα και με συστηματικό τρόπο. Γενικότερα, ο εξαγωγέας των δεδομένων θα πρέπει να υιοθετεί τον μηχανισμό των παρεκκλίσεων κατ'εξαίρεση και μόνο εφόσον η διαβίβαση πληροί το κριτήριο της αναγκαιότητας.

Η απόφαση Schrems II λοιπόν μας υπενθυμίζει ότι η προστασία των προσωπικών δεδομένων στον ΕΟΧ πρέπει να συνοδεύει τα δεδομένα, ανεξάρτητα από τον προορισμό διαβίβασής τους. Όταν μιλάμε για διαβίβαση σε τρίτες χώρες, το ΔΕΕ αποφάνθηκε ότι το επίπεδο προστασίας που οι τρίτες χώρες πρέπει να παρέχουν δεν απαιτείται να είναι ίδιο

με εκείνο που διασφαλίζεται εντός του ΕΟΧ αλλά ουσιαστικά ισοδύναμο. Το ΔΕΕ επιβεβαίωσε επίσης το κύρος των ΤΣΡ, ως έγκυρο μηχανισμό διαβίβασης, που μπορεί να εξασφαλίσει συμβατικά ένα ουσιαστικά ισοδύναμο επίπεδο προστασίας για δεδομένα που διαβιβάζονται σε τρίτες χώρες.

Το ΕΣΠΔ προκειμένου να συνδράμει τους εξαγωγείς δεδομένων στο δύσκολο έργο τους, με τις υπ'αρ. 01/2020 Συστάσεις του[107], παρέχει μια σειρά βημάτων που θα πρέπει να ακολουθήσουν, πιθανές πηγές πληροφοριών αλλά και ορισμένα παραδείγματα πρόσθετων μέτρων που πρέπει να εφαρμόσουν. Το πρώτο βήμα που καλούνται να κάνουν είναι να χαρτογραφήσουν τις διαβιβάσεις τους προς τρίτες χώρες, δηλαδή να τελούν σε γνώση του προορισμού των δεδομένων, και να επαληθεύουν ότι τα δεδομένα που διαβιβάζουν είναι κατάλληλα, συναφή και ότι περιορίζεται η επεξεργασία τους στους σκοπούς για τους οποίους διαβιβάζονται. Το δεύτερο βήμα που πρέπει να κάνουν είναι να εντοπίσουν τον κατάλληλο μηχανισμό διαβίβασης στον οποίο θα βασίζεται η διαβίβαση. Τρίτο βήμα είναι η αξιολόγηση της νομοθεσίας ή της πρακτικής της τρίτης χώρας, έτσι ώστε να επιτευχθεί η αποτελεσματικότητα των κατάλληλων εγγυήσεων των εργαλείων διαβίβασης. Στο τέταρτο βήμα, ο υπεύθυνος επεξεργασίας θα πρέπει να προσδιορίσει τα πρόσθετα μέτρα που είναι αναγκαία για να προσεγγίσει την ισοδυναμία του επιπέδου προστασίας της ΕΕ. Το πέμπτο βήμα επιβάλλει να προβεί σε τυχόν τυπικές διαδικαστικές ενέργειες για την έγκριση του πρόσθετου μέτρου, ενώ το έκτο και τελευταίο βήμα είναι να κάνει σε τακτά χρονικά διαστήματα επανεκτίμηση του επιπέδου προστασίας των δεδομένων που διαβιβάζει σε τρίτες χώρες και να παρακολουθεί εάν αλλάζουν οι συνθήκες προστασίας σε αυτές.

### **4.3**. **Το εδαφικό πεδίο εφαρμογής του ΓΚΠΔ**

Στο εικονικό περιβάλλον του υπολογιστικού νέφους, οι υπηρεσίες που παρέχονται αφορούν- μεταξύ άλλων- και διαβιβάσεις προσωπικών δεδομένων, δηλαδή δεδομένων που μπορούν να ταυτοποιήσουν ένα πρόσωπο. Η διαβίβαση και η αποθήκευσή τους σε εξυπηρετητές ή σε κέντρα δεδομένων, στα οποία τα δεδομένα μπορεί να βρίσκονται το πρωϊ σε ένα κέντρο και το βράδυ σε άλλο κέντρο άλλης ηπείρου, δημιουργούν ασάφειες και δυσκολίες, καθώς ο χρήστης τελεί σε πλήρη άγνοια για την τοποθεσία ύπαρξής τους. Δεν νοείται λοιπόν τοπική αποθήκευση, αλλά ούτε και σταθερή τοποθεσία των δεδομένων στο υπολογιστικό νέφος.

Τίθεται λοιπόν το θέμα του εφαρμοστέου δικαίου και της δικαιοδοσίας καθώς παρατηρείται ότι οι περισσότεροι πάροχοι διατηρούν τις εγκαταστάσεις τους και τον εξοπλισμό τους εκτός ΕΕ, δηλαδή εκτός εμβέλειας της ευρωπαϊκής νομοθεσίας. Είναι ο ΓΚΠΔ το νομοθετικό εργαλείο που μπορεί να ρυθμίσει μια διαβίβαση εντός του υπολογιστικού νέφους;

Ο ΓΚΠΔ δεν κάνει ειδική αναφορά στο υπολογιστικό νέφος, ωστόσο θα πρέπει να θεωρηθεί ότι οι διατάξεις του το αφορούν καθώς η ισχύς του εκτείνεται πολύ ευρύτερα από το πεδίο εφαρμογής του. Ο ΓΚΠΔ μπορεί να εφαρμόζεται είτε στον πάροχο των υπηρεσιών υπολογιστικού νέφους, είτε στον χρήστη του, είτε και στους δύο.

Το εδαφικό πεδίο εφαρμογής του ΓΚΠΔ ρυθμίζεται στο άρθρο 3 αυτού. Βασική αρχή είναι ότι το άρθρο αυτό εφαρμόζεται όταν υφίσταται επεξεργασία προσωπικών δεδομένων στο πλαίσιο των δραστηριοτήτων μιας εγκατάστασης ενός υπευθύνου

---

[107] https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/recommendations-012020-measures-supplement_el

επεξεργασίας ή εκτελούντος την επεξεργασία στην ΕΕ, ανεξάρτητα από το εάν η επεξεργασία αυτή λαμβάνει χώρα εντός ή εκτός της ΕΕ. Ορίζει δύο κριτήρια προκειμένου να προσδιοριστεί η εδαφική ισχύς του και αυτά είναι το κριτήριο της εγκατάστασης του υπευθύνου επεξεργασίας και το κριτήριο της στόχευσης[108].

Στην αιτιολογική σκέψη 22 του ΓΚΠΔ ορίζεται ότι «*η εγκατάσταση προϋποθέτει την ουσιαστική και πραγματική άσκηση δραστηριότητας….*». Το ΔΕΕ έχει διευρύνει την έννοια της εγκατάστασης, ορίζοντας ότι εγκατάσταση μπορεί να υπάρξει εφόσον υπάρχει άσκηση πραγματικής και αποτελεσματικής δραστηριότητας σε ένα κράτος, ακόμη και μικρής έκτασης, αν συνοδεύεται από επαρκώς σταθερά μέσα[109]. Η νομική μορφή της εγκατάστασης είναι αδιάφορη, το ίδιο και ο βαθμός σταθερότητας της εγκατάστασης.

Στην παράγραφο 2 του άρθρου 3 γίνεται αναφορά στο κριτήριο της στοχεύσεως, το οποίο εστιάζει στον τόπο στον οποίο «βρίσκεται» το υποκείμενο των δεδομένων, ούτως ώστε να προσδιορισθεί το πεδίο εδαφικής εφαρμογής του ΓΚΠΔ. Δεν αποτελεί προϋπόθεση για την εφαρμογή του, η ύπαρξη νομικού δεσμού μεταξύ του υποκειμένου των δεδομένων και της ΕΕ, όπως η ύπαρξη ιθαγένειας ή συνήθους διαμονής.

Πρακτικά διαπιστώνεται ότι είναι ουτοπικό να μην διέπεται το υπολογιστικό νέφος από τις διατάξεις του ΓΚΠΔ, καθώς για να συνέβαινε αυτό θα έπρεπε να συτρέχουν οι παρακάτω προϋποθέσεις: α) είτε ο πάροχος, είτε ο χρήστης να μην είχαν εγκατάσταση στην ΕΕ ή στον ΕΟΧ, β) είτε να μην γινόταν επεξεργασία προσωπικών δεδομένων των -εντός ΕΕ/ΕΟΧ- υποκειμένων των δεδομένων από εγκατάσταση σε τρίτο κράτος, που σχετίζεται με τα κριτήρια του άρθρου 3 παρ.2 του ΓΚΠΔ, δηλαδή που έχει να κάνει με την προσφορά αγαθών ή υπηρεσιών στα εν λόγω υποκείμενα ή με την παρακολούθηση της συμπεριφοράς τους[110].

**4.4 Τεχνικά και Οργανωτικά μέτρα**

Άλλο ζήτημα που ανακύπτει σχετικά με τη διαβίβαση δεδομένων και την προστασία των προσωπικών δεδομένων στο υπολογιστικό νέφος είναι η υιοθέτηση τεχνικών και οργανωτικών μέτρων από τον υπεύθυνο επεξεργασίας. Ο συνδυασμός των διατάξεων των άρθρων 25 (προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού) και α.32 (ασφάλεια επεξεργασίας) θα μας απασχολήσουν στην παρούσα ενότητα.

Η επεξεργασία από τον σχεδιασμό, σύμφωνα με τις επιταγές του ΓΚΠΔ, επιβάλλει να προλαμβάνεται -ει δυνατόν- η όποια επέμβαση στην ιδιωτική σφαίρα των χρηστών, με τη λήψη κατάλληλων μέτρων, ώστε να εξασφαλίζεται νόμιμη επεξεργασία των δεδομένων. Η επεξεργασία εξ ορισμού επιτάσσει ότι πρέπει να γίνεται επεξεργασία μόνο σε όσα δεδομένα είναι απαραίτητα για κάθε σκοπό επεξεργασίας. Ως προς τα κατάλληλα μέτρα ασφαλείας που πρέπει να λαμβάνονται, τέτοια είναι ενδεικτικά η

---

[108] Κουσουνή- Πανταζοπούλου Α. *Cloud Computing & νομικά ζητήματα*, Νομική Βιβλιοθήκη, 2020, σελ.148

[109] Παναγοπούλου-Κουτνατζή Φ., *Συνταγματικές προεκτάσεις των μηχανισμών διευρύνσεως της προστασίας δεδομένων προσωπικού χαρακτήρα πέραν της ΕΕ: Εξωεδαφική εφαρμογή του ΓΚΠΔ και διασυνοριακή διαβίβαση δεδομένων*, ΔΙΤΕ (π. ΔΙΜΕΕ 4/2019)

[110] Κουσουνή- Πανταζοπούλου Α. *Cloud Computing & νομικά ζητήματα*, Νομική Βιβλιοθήκη, 2020, σελ.149-150

ψευδωνυμοποίηση και η κρυπτογράφηση, προκειμένου να αποφευχθούν οι κίνδυνοι για τα δικαιώματα των υποκειμένων των δεδομένων.

Στο περιβάλλον του νέφους, πέραν των ανωτέρω, προστίθενται και η εξασφάλιση της διαθεσιμότητας, της ακεραιότητας αλλά και της εμπιστευτικότητας των δεδομένων, που αποτελούν γενικές αρχές ασφάλειας εν γένει, αλλά και για τη λειτουργία του νέφους.

Σε επίπεδο κινδύνων όσον αφορά το υπολογιστικό νέφος, ισχύουν αφενός οι γενικοί κίνδυνοι ασφάλειας που υφίστανται για τις τεχνολογίες της πληροφορίας, δηλαδή τυχόν κενά ασφαλείας κ.λ.π., και αφετέρου ειδικοί κίνδυνοι, οι οποίοι μπορεί να σχετίζονται είτε με αδυναμία ελέγχου της δραστηριότητας των εξουσιοδοτημένων υπεργολάβων, είτε με δυσκολία ελέγχου της διαγραφής των δεδομένων του χρήστη κατά τη λήξη της μεταξύ τους σύμβασης.

Πέραν όμως των ανωτέρω, για κάθε υπηρεσία υπολογιστικού νέφους ελλοχεύουν διαφορετικοί κίνδυνοι. Ενδεικτικά στο μοντέλο της Υποδομής ως υπηρεσίας (IaaS) ο κίνδυνος μπορεί να συνίσταται στη φυσική ασφάλεια των εγκαταστάσεων ή στην φθορά των συστημάτων λειτουργίας πάνω στα οποία βασίζεται η υποδομή[111].

Στο υπ'αρ. 2 Παράρτημα των υπ'αρ. 01/2020 Συστάσεων του ΕΣΠΔ αναφέρονται τεχνικά μέτρα, τα οποία ενδέχεται να συμπληρώνουν τις εγγυήσεις που περιλαμβάνονται στα εργαλεία διαβίβασης του α.46 του ΓΚΠΔ για τη διασφάλιση της συμμόρφωσης με το απαιτούμενο επίπεδο προστασίας σύμφωνα με τη νομοθεσία της ΕΕ. Αυτά θα απαιτηθούν στην περίπτωση που το δίκαιο της τρίτης χώρας στην οποία διαβιβάζονται τα δεδομένα, επιβάλλει στον εισαγωγέα δεδομένων υποχρεώσεις που είναι αντίθετες με τις εγγυήσεις των εργαλείων διαβίβασης του α.46 ΓΚΠΔ, ειδικά εφόσον μπορεί να πλήξουν τη συμβατική εγγύηση ενός ουσιαστικά ισοδύναμου επίπεδου προστασίας έναντι της πρόσβασης των δημόσιων αρχών της εν λόγω τρίτης χώρας στα δεδομένα αυτά.

Τέτοια τεχνικά μέτρα μπορεί να είναι η αποθήκευση δεδομένων για σκοπούς δημιουργίας αντιγράφων ασφαλείας και για άλλους σκοπούς που δεν απαιτούν αποκωδικοποιημένη πρόσβαση σε δεδομένα, η διαβίβαση ψευδωνυμοποιημένων δεδομένων, η διαβίβαση κρυπτογραφημένων δεδομένων εφόσον διέρχονται απλώς από τρίτες χώρες, η διαβίβαση σε προστατευόμενο παραλήπτη, ο πολυσυμμετοχικός διαχωρισμός δεδομένων όταν υφίσταται από κοινού επεξεργασία προσωπικών δεδομένων ή από δύο ή περισσότερους ανεξάρτητους εκτελούντες την επεξεργασία που είναι εγκατεστημένοι σε διαφορετικές δικαιοδοσίες χωρίς να τους γνωστοποιήσει το περιεχόμενο των δεδομένων και η απομακρυσμένη πρόσβαση σε δεδομένα για επιχειρηματικούς σκοπούς.

Οργανωτικά μέτρα μπορεί να είναι εσωτερικές πολιτικές, οργανωτικές μέθοδοι και πρότυπα, τα οποία μπορούν να εφαρμόσουν οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία για τους ίδιους, και να τα επιβάλουν στους εισαγωγείς των δεδομένων σε τρίτες χώρες. Ωστόσο η επιλογή και η εφαρμογή ενός ή περισσότερων από τα ως άνω μέτρα, δεν διασφαλίζουν απαραίτητα και συστηματικά ότι η διαβίβαση πληροί το απόλυτο επίπεδο ισοδυναμίας που επιβάλλει η νομοθεσία της ΕΕ.

---

[111] Κουσουνή- Πανταζοπούλου Α. *Cloud Computing & νομικά ζητήματα*, Νομική Βιβλιοθήκη, 2020, σελ.159

Η αξιολόγηση των πιο κατάλληλων μέτρων πρέπει να γίνεται ανά περίπτωση, λαμβάνοντας πάντα υπόψη την ανάγκη τήρησης της αρχής της λογοδοσίας από τους υπεύθυνους και τους εκτελούντες την επεξεργασία.

**4.5 Νόμιμη βάση επεξεργασίας**

Για τη νόμιμη επεξεργασία των προσωπικών δεδομένων στο περιβάλλον του υπολογιστικού νέφους, θα πρέπει να ερευνηθεί ποια εκ των νομίμων βάσεων του άρθρου 6 παρ. 1 ΓΚΠΔ τυγχάνει εφαρμογής, καθώς και του άρθρου 9 ΓΚΠΔ για τα ευαίσθητα δεδομένα.

Αρχικά, θα μπορούσαμε να συμπεράνουμε ότι η ύπαρξη του εννόμου συμφέροντος του υπευθύνου επεξεργασίας ή του τρίτου που επιτελεί την επεξεργασία, είναι η κατάλληλη νόμιμη βάση (άρθρο 6 περ. στ ΓΚΠΔ)[112]. Εάν υποθέσουμε ότι είναι ευχερές να εντοπισθεί το έννομο συμφέρον του υπευθύνου επεξεργασίας ή του τρίτου που διενεργεί επεξεργασία, θα αντιμετωπίσουμε δυσκολία κατά τη στάθμιση του συμφέροντος αυτών έναντι του συμφέροντος του υποκειμένου των δεδομένων ή των θεμελιωδών δικαιωμάτων και των ελευθεριών αυτού.

Εναλλακτικά, θα μπορούσαμε να προσφύγουμε στη λύση της εκτέλεσης σύμβασης με τον πάροχο (α.6 περ.1, εδ.β ΓΚΠΔ). Δεδομένου ότι είναι οικειοθελής η σύναψη της ως άνω σύμβασης, θα πρέπει να ερευνηθεί εάν μια τέτοια επεξεργασία από τον υπεύθυνο επεξεργασίας ή τρίτο είναι απαραίτητη στα πλαίσια της συγκεκριμένης σύμβασης και εάν υπερβαίνει το μέτρο του αναγκαίου[113].

Κατά κανόνα όμως, η επεξεργασία των προσωπικών δεδομένων σε επίπεδο υπολογιστικού νέφους γίνεται με βάση τη συγκατάθεση (άρθρο 6 περ.1 εδ.α). Η συγκατάθεση θα πρέπει να συμπεριλαμβάνει όλα τα εμπλεκόμενα μέρη, δηλαδή τυχόν επεξεργασία ακόμη και από υπεργολάβους, για τους οποίους θα πρέπει να γίνεται εκ των προτέρων ειδική μνεία. Ως γνωστόν, η συγκατάθεση θα πρέπει να είναι ρητή και ελεύθερη (άρθρο 7 ΓΚΠΔ) και να μην καλύπτεται μέσα στο σύνολο των ΓΟΣ της σύμβασης, αλλά και να μπορεί να αποδειχθεί και να τεκμηριωθεί ανά πάσα στιγμή[114]. Ο χρήστης έχει την ευχέρεια να την ανακαλέσει όποτε το επιθυμεί και να προσφύγει σε άλλες λύσεις πιο συμφέρουσες γι'αυτόν. Τέλος, στην περίπτωση κατά την οποία ο χρήστης εκτελεί ο ίδιος επεξεργασία προσωπικών δεδομένων άλλων προσώπων, όπως π.χ στην περίπτωση ενός εργοδότη που επεξεργάζεται τα δεδομένα των εργαζομένων του, θα πρέπει πάντα να διερευνάται η ισοτιμία της σχέσης τους και το κατά πόσο το υποκείμενο των δεδομένων ήταν σε θέση ισχύος ώστε να μπορεί να αρνηθεί την επεξεργασία αυτή[115].

Ανακεφαλαιώνοντας σχετικά με τις νόμιμες βάσεις επεξεργασίας σε επίπεδο υπολογιστικού νέφους, πρώτον έχουμε διαπιστώσει ότι οι πάροχοι των υπηρεσιών αυτών αναφέρουν στις συμβάσεις τους πλείστες νόμιμες βάσεις και σκοπούς επεξεργασίας, με

---

[112] Κουσουνή- Πανταζοπούλου Α. *Cloud Computing & νομικά ζητήματα*, Νομική Βιβλιοθήκη, 2020, σελ.156

[113] Κουσουνή- Πανταζοπούλου Α. *Cloud Computing & νομικά ζητήματα*, Νομική Βιβλιοθήκη, 2020 σελ.156

[114] Κουσουνή- Πανταζοπούλου Α. *Cloud Computing & νομικά ζητήματα*, Νομική Βιβλιοθήκη, 2020, σελ.157

[115] Κουσουνή- Πανταζοπούλου Α. *Cloud Computing & νομικά ζητήματα*, Νομική Βιβλιοθήκη, 2020, σελ.157

αποτέλεσμα να αδυνατεί ο χρήστης να κατανοήσει σε ποια βάση στηρίζεται η επεξεργασία των δεδομένων του ή για ποιον σκοπό γίνεται, και ως εκ τούτου να μην μπορεί να αξιολογήσει τη νομιμότητα αυτής[116]. Δεύτερον, οι πάροχοι υπηρεσιών νέφους πρέπει να έχουν πολιτική διαφάνειας. Αυτή περιλαμβάνει την πολιτική ιδιωτικότητας του παρόχου, αλλά και ενημέρωση του χρήστη σχετικά με τα μέτρα προστασίας προσωπικών δεδομένων που εφαρμόζει ο πάροχος (μέτρα ασφαλείας, κοινοποίηση περιστατικών ασφαλείας, συνέπειες επεξεργασίας, πορίσματα δικών του ερευνών σχετικά με τη συμμόρφωσή του οργανισμού του με τις απαιτήσεις ασφαλείας κλπ[117]).

## 5. Λοιπά νομικά θέματα διαβιβάσεων σε σχέση με το υπολογιστικό νέφος

### 5.1. Επεξεργασία των δεδομένων

Οι πάροχοι υπηρεσιών υπολογιστικού νέφους συλλέγουν, αποθηκεύουν, επεξεργάζονται και διαβιβάζουν δεδομένα διαφόρων κατηγοριών[118]. Μπορεί να είναι δεδομένα που παράγονται είτε αυτομάτως από την υπηρεσία, είτε στο πλαίσιο λειτουργίας της, είτε δεδομένα που δίνει οικειοθελώς ο ίδιος ο χρήστης του «νέφους» στο πλαίσιο της χρήσης μιας υπηρεσίας ή δεδομένα που συλλέγονται για διαφημιστικούς σκοπούς.

Το κανονιστικό πλαίσιο που ρυθμίζει τα δεδομένα αυτά, εδράζεται στον χαρακτηρισμό των δεδομένων αυτών ως «δεδομένων προσωπικού χαρακτήρα»[119] ή κατά την παλιότερη ορολογία «προσωπικών δεδομένων», δηλαδή ως πληροφοριών που ταυτοποιούν ένα πρόσωπο, με αποτέλεσμα η ταυτότητα του προσώπου να γίνεται γνωστή ή να μπορεί να εξακριβωθεί, και αυτό καλείται «υποκείμενο των δεδομένων».

Κατά κανόνα, στο υπολογιστικό νέφος ο χρήστης μεταφέρει αρχικά όλα του τα δεδομένα σε διακομιστή του παρόχου, όπου αυτά πρέπει να τηρούνται με ασφάλεια, για την εκπλήρωση των υποχρεώσεων που έχουν αναληφθεί ως προς την παροχή της συμφωνηθείσας υπηρεσίας[120]. Η δυνατότητα εξακρίβωσης της ταυτότητας ενός προσώπου αποτελεί το κύριο στοιχείο της επεξεργασίας στο περιβάλλον του υπολογιστικού νέφους. Η δυνατότητα αυτής της εξακρίβωσης πρέπει να αξιολογείται πάντα σε συνάρτηση με το τρέχον επίπεδο της τεχνολογίας. Η πρόσβαση στην πληροφορία αλλά και η πιθανότητα συγκέντρωσής της στο περιβάλλον του υπολογιστικού νέφους, ευνοούν την μελλοντική εξακρίβωση του υποκειμένου των δεδομένων. Αυτός ο κίνδυνος, δηλαδή της πραγματικής εξακρίβωσης της ταυτότητας του υποκειμένου, αποτελεί έναν από τους σοβαρούς κινδύνους που ελλοχεύουν στο υπολογιστικό νέφος.

---

[116] Κουσουνή- Πανταζοπούλου Α. *Cloud Computing & νομικά ζητήματα*, υποσημ. 542, Νομική Βιβλιοθήκη, 2020, σελ.156

[117] Κουσουνή- Πανταζοπούλου Α. *Cloud Computing & νομικά ζητήματα*, Νομική Βιβλιοθήκη, 2020, σελ.158

[118] Μήτρου Λ. *Προστασία Προσωπικών Δεδομένων και Υπολογιστικό Νέφος*, ΔΙΜΕΕ 4/2015

[119] Μήτρου Λ. *Προστασία Προσωπικών Δεδομένων και Υπολογιστικό Νέφος*, ΔΙΜΕΕ 4/2015

[120] Κουσουνή- Πανταζοπούλου Α. *Cloud Computing & νομικά ζητήματα*, Νομική Βιβλιοθήκη, 2020, σελ.150

**5.2 Ο ρόλος του Υπευθύνου Επεξεργασίας και του Εκτελούντος την Επεξεργασία**

Στο περιβάλλον του υπολογιστικού νέφους ο χρήστης μεταφέρει τα δεδομένα του στον διακομιστή του παρόχου, κρυπτογραφημένα ή μη, όπου τηρούνται με ασφάλεια και χρησιμοποιούνται για την παροχή της εκάστοτε συμφωνηθείσας υπηρεσίας.

Στο υπολογιστικό νέφος, ένα από τα νομικά ζητήματα που ανακύπτει αφορά στο ποιος είναι ο υπεύθυνος και ποιος ο εκτελών την επεξεργασία των προσωπικών δεδομένων.

Είναι σημαντική η διάκριση του υπευθύνου και του εκτελούντος την επεξεργασία στο υπολογιστικό νέφος προκειμένου να μπορούν να αποδοθούν ευθύνες. Ωστόσο δεν είναι εύκολη, παρά το ότι στις σχετικές συμβάσεις αποτυπώνονται συνήθως οι ρόλοι του καθενός[121]. Η δυσκολία έγκειται επίσης στο ότι πολλές φορές εμπλέκονται διαφορετικά μέρη στην παροχή των ως άνω υπηρεσιών, δηλαδή άλλος μπορεί να προσφέρει την πλατφόρμα και την τεχνική υποδομή, άλλος την εφαρμογή, με αποτέλεσμα να περιπλέκονται οι αρμοδιότητες και οι ευθύνες.

Η κατανομή των αρμοδιοτήτων και κατ'επέκταση των ευθυνών κατά την παροχή υπηρεσιών υπολογιστικού νέφους είναι θεμελιώδης[122]. Η κάθε περίπτωση είναι διαφορετική και θα πρέπει να συνυπολογίζονται κάθε φορά οι διαφορετικές συνθήκες, καθώς και το είδος της κάθε υπηρεσίας που παρέχεται. Είναι όμως σαφές ότι όσο εκτενέστερη είναι η επεξεργασία των προσωπικών δεδομένων που γίνεται από τον πάροχο, τόσο αυξάνει αναλογικά και η ευθύνη του.

Ο γενικός κανόνας ορίζει ότι, όσον αφορά τη χρήση του υπολογιστικού νέφους, υπεύθυνος επεξεργασίας είναι ο χρήστης, καθώς αυτός καθορίζει τον σκοπό της τελικής επεξεργασίας, παρά το ότι την έχει αναθέσει σε τρίτο μέρος[123]. Ο πάροχος θεωρείται εκτελών την επεξεργασία καθώς αυτός παρέχει απλώς τα μέσα για την επεξεργασία, και ενεργεί στο όνομά του χρήστη και υπό τις οδηγίες του. Ως εκτελών την επεξεργασία ευθύνεται για την τήρηση των κατάλληλων τεχνικών και οργανωτικών μέτρων (α.28 ΓΚΠΔ), για τον ορισμό εκπροσώπου στην ΕΕ (α.27 ΓΚΠΔ) και για την επικοινωνία του με τις αρμόδιες εποπτικές αρχές (α.31 ΓΚΠΔ). Η μοναδική περίπτωση κατά την οποία ο πάροχος μπορεί να θεωρηθεί ότι λειτουργεί ως υπεύθυνος επεξεργασίας είναι όταν επεξεργάζεται τα δεδομένα αυτά για δικούς του σκοπούς ή για νέους σκοπούς, όπως στην περίπτωση της διαβίβασης σε τρίτους, σε ενέργειες προωθητικές κλπ.

Πρέπει να επισημανθεί ότι όταν, στα πλαίσια της επεξεργασίας των δεδομένων από τον πάροχο, γίνεται κακή χρήση των δεδομένων του υποκειμένου ή χρήση για σκοπό διαφορετικό από τον αρχικό, ο πάροχος θα θεωρείται ότι ενεργεί ως υπεύθυνος επεξεργασίας, λαμβάνοντας υπόψη ότι τις περισσότερες φορές εντός του «νέφους» ο χρήστης δεν έχει έλεγχο των δεδομένων του. Είναι θεμελιώδους λοιπόν σημασίας η τήρηση της αρχής του περιορισμού του σκοπού και σε αυτού του είδους την επεξεργασία και πρέπει να γίνεται ρητή αναφορά της στη σύμβαση παροχής των υπηρεσιών νέφους.

---

[121] Κουσουνή- Πανταζοπούλου Α. *Cloud Computing & νομικά ζητήματα*, Νομική Βιβλιοθήκη, 2020, σελ.151

[122] Κουσουνή- Πανταζοπούλου Α. *Cloud Computing & νομικά ζητήματα*, Νομική Βιβλιοθήκη, 2020, σελ.151

[123] Κουσουνή- Πανταζοπούλου Α. *Cloud Computing & νομικά ζητήματα*, Νομική Βιβλιοθήκη, 2020, σελ.152

Είναι γνωστό ότι ο ΓΚΠΔ δεν εφαρμόζεται σε επεξεργασίες που γίνονται στα πλαίσια προσωπικής ή οικιακής δραστηριότητας (α.2 παρ.2 εδ.γ ΓΚΠΔ), που δεν συνδέονται δηλαδή με κάποια επαγγελματική ή εμπορική δραστηριότητα του χρήστη (πχ. λήψη ηλεκτρονικής αλληλογραφίας, πλοήγηση στο διαδίκτυο, συμμετοχή σε δίκτυα κοινωνικής δικτύωσης). Ωστόσο, σύμφωνα με την αιτιολογική σκέψη 18 του ΓΚΠΔ, αυτός εφαρμόζεται σε υπεύθυνους επεξεργασίας ή εκτελούντες την επεξεργασία, οι οποίοι παρέχουν τα μέσα επεξεργασίας των δεδομένων αυτών για προσωπικές ή οικιακές δραστηριότητες. Άρα, ο ΓΚΠΔ δεν θα έχει μεν εφαρμογή στον χρήστη που χρησιμοποιεί για παράδειγμα το ηλεκτρονικό ταχυδρομείο αλλά θα έχει εφαρμογή στον πάροχο του υπολογιστικού νέφους που παρέχει την υπηρεσία αυτή, κατά τον βαθμό που αυτός καθορίζει τα μέσα και τους σκοπούς της επεξεργασίας, οπότε και θα κριθεί τελικά εάν ενεργεί ως υπεύθυνος ή εκτελών την επεξεργασία.

Κατά περίπτωση θα μπορούσαν να κριθούν ως από κοινού υπεύθυνοι επεξεργασίας ο πάροχος των υπηρεσιών νέφους και ο χρήστης αυτού. Είναι ασαφή ωστόσο τα όρια για να κριθεί πότε γίνεται από κοινού επεξεργασία από τα ως άνω μέρη. Ποιος είναι ο βαθμός επίδρασης του καθενός στην εν λόγω επεξεργασία; Καθορίζουν από κοινού τον σκοπό και τα μέσα της επεξεργασίας;

Όλα τα ανωτέρω θα μπορούσαν να προσδιορίσουν αν υφίσταται από κοινού επεξεργασία. Για παράδειγμα, αυτό θα μπορούσε να συναχθεί εύκολα στο πλαίσιο ενός ομίλου επιχειρήσεων ή εταιριών. Εάν μια θυγατρική τηρούσε μια κοινή βάση δεδομένων των πελατών της εντός του «νέφους», την οποία θα καθιστούσε προσβάσιμη σε άλλες εταιρίες του ομίλου για λόγους κοινής διαφημιστικής εκστρατείας, στην περίπτωση αυτή θα μπορούσαμε να μιλήσουμε για από κοινού καθορισμό του σκοπού της επεξεργασίας, ως ορίζεται στο άρθρο 26 ΓΚΠΔ. Συνάγεται εκ των ανωτέρω, ότι οι εταιρίες αυτές θα θεωρηθούν από κοινού υπεύθυνες επεξεργασίας για την επεξεργασία των προσωπικών δεδομένων όσον αφορά τη συγκεκριμένη διαφημιστική ενέργεια[124].

Σε κάθε περίπτωση όμως, ακόμη και αν ήθελε θεωρηθεί ότι υπάρχει από κοινού ευθύνη του υπεύθυνου επεξεργασίας και του εκτελούντος την επεξεργασία, σύμφωνα με το άρθρο 26 παρ.2 του ΓΚΠΔ, η κατανομή των ρόλων δεν θα πρέπει να γίνεται ελεύθερα, αλλά θα πρέπει η μεταξύ τους συμφωνία να αντανακλά δεόντως τους αντίστοιχους ρόλους και τις σχέσεις τους έναντι των υποκειμένων των δεδομένων, να λαμβάνονται δηλαδή υπόψη οι πραγματικές περιστάσεις της κάθε περίπτωσης επεξεργασίας[125].

**5.3 Ουσιαστικές Νομικές Υποχρεώσεις**

Η κακή χρήση των δεδομένων που διακινούνται στο περιβάλλον του υπολογιστικού νέφους, αλλά και η χρήση τους για σκοπούς που δεν έχουν λάβει έγκριση από τον πελάτη των υπηρεσιών αυτών, αποτελούν σοβαρό κίνδυνο αναφορικά με την προστασία των προσωπικών δεδομένων.

Κακή χρήση μπορεί, για παράδειγμα, να κάνει ένας πάροχος όταν δεν ασκεί προσηκόντως τον φυσικό έλεγχο που έχει επί των δεδομένων που έχει στην κατοχή του, ούτε την πρόσβαση σε αυτά, συνδέοντας και συνδυάζοντας δεδομένα περισσότερων πελατών και πηγών. Κακή χρήση επίσης συνιστά η χρήση των δεδομένων για

[124] Κουσουνή- Πανταζοπούλου Α. *Cloud Computing & νομικά ζητήματα*, Νομική Βιβλιοθήκη, 2020, σελ.153

[125] Κουσουνή- Πανταζοπούλου Α. *Cloud Computing & νομικά ζητήματα*, Νομική Βιβλιοθήκη, 2020, σελ.154

διαφημιστικούς σκοπούς, χωρίς να έχει δοθεί σχετική συναίνεση από τον πελάτη. Πολλοί πάροχοι, θέλοντας να αποκτήσουν όσο περισσότερα δεδομένα γίνεται για να κάνουν εξόρυξη δεδομένων (data mining), δελεάζουν τους χρήστες τους να παρέχουν προσωπικές τους πληροφορίες, παρέχοντας τους σαν «αντάλλαγμα» δήθεν δωρεάν υπηρεσίες, με αποτέλεσμα οι πάροχοι να αυξάνουν τις διαφημιστικές δραστηριότητές τους και τα έσοδά τους.

Όμως εφόσον κατά τα ανωτέρω οι πάροχοι προβαίνουν σε αποθήκευση και εν γένει επεξεργασία των προσωπικών δεδομένων των χρηστών τους, οι αρχές που διέπουν την προστασία τους εφαρμόζονται και στο περιβάλλον του υπολογιστικού νέφους, και τέτοιες αρχές είναι η αρχή του προσδιορισμού και του περιορισμού του σκοπού και η αρχή της αναλογικότητας. Η αρχή του περιορισμού του σκοπού, στο περιβάλλον του υπολογιστικού νέφους, επιτάσσει να μην τα χρησιμοποιεί ο πάροχος για σκοπούς διαφορετικούς από την παροχή της αιτηθείσας υπηρεσίας στον πελάτη.

Για να πραγματοποιηθούν τα ως άνω, επιβάλλεται να υπάρχει έλεγχος στο σύστημα πρόσβασης στα δεδομένα, ούτως ώστε να μπορούν να έχουν πρόσβαση σε αυτά μόνο εξουσιοδοτημένοι υπάλληλοι και πιστοποιημένοι χρήστες του νέφους. Θα πρέπει να γίνεται λογικός διαχωρισμός των δεδομένων, ούτως ώστε να αποφεύγεται η επεξεργασία τους για παράνομους σκοπούς.

Όσον αφορά το δικαίωμα πρόσβασης του α.15 ΓΚΠΔ, δέον είναι να διασταυρώνει ο πάροχος την ταυτότητα του υποκειμένου των δεδομένων, χρησιμοποιώντας κάθε εύλογο μέτρο ανάλογα με την περίσταση. Ιδιαίτερα ως προς το νέφος, όπου χρησιμοποιούνται σε περιβάλλον διαδικτύου αναγνωριστικά στοιχεία ταυτότητας, ο πάροχος θα πρέπει να προβαίνει σε ταυτοποίηση του αιτούντος, άλλως μπορεί να ζητά συμπληρωματικά στοιχεία κατά το άρθρο 12 παρ. 6 του ΓΚΠΔ.

Ως προς το δικαίωμα διαγραφής των δεδομένων, ο χρήστης του νέφους ως υπεύθυνος επεξεργασίας μπορεί να αιτηθεί από τον πάροχο, υπό την ιδιότητά του εκτελούντος, τη διαγραφή των δεδομένων που τηρεί ο τελευταίος ή υπεργολάβοι του στο υπολογιστικό νέφος. Η αρχιτεκτονική του υπολογιστικού νέφους, της οποίας κύριο χαρακτηριστικό είναι ο διαμοιρασμός των πόρων σε περισσότερους χρήστες (multi tenant)[126], δημιουργεί αντικειμενικές δυσκολίες ως προς τη δυνατότητα πραγματικής καταστροφής των δεδομένων και διαγραφής τους, πάντα λαμβάνοντας υπόψη και τον κίνδυνο που κάτι τέτοιο μπορεί να επιφέρει και σε άλλα πρόσωπα. Το γεγονός, ότι μπορεί να υφίστανται διάσπαρτα πολλά αντίγραφα ασφαλείας (backups) καθιστά ιδιαιτέρως δυσχερή έως και αδύνατη την άμεση διαγραφή των δεδομένων, παρά την παροχή σχετικών εργαλείων από τον πάροχο των υπηρεσιών νεφοϋπολογιστικής. Γι'αυτό, προτιμάται από τους παρόχους να ορίζεται ρητά στη μεταξύ τους σύμβαση ένα συγκεκριμένο χρονικό πλαίσιο εντός του οποίου οι πάροχοι υποχρεούνται να ολοκληρώσουν τη διαγραφή όλων των αιτηθέντων δεδομένων[127].

Ως προς το δικαίωμα στη φορητότητα των δεδομένων του άρθρου 20 του ΓΚΠΔ, δηλαδή στο δικαίωμα του υποκειμένου των δεδομένων να λαμβάνει τα προσωπικά δεδομένα του σε δομημένο, κοινώς χρησιμοποιούμενο κα αναγνώσιμο από μηχανήματα μορφότυπο, καθώς και να τα διαβιβάζει περαιτέρω σε άλλον υπεύθυνο επεξεργασίας,

---

[126] Κουσουνή- Πανταζοπούλου Α. *Cloud Computing & νομικά ζητήματα*, Νομική Βιβλιοθήκη, 2020, σελ. 170

[127] Κουσουνή- Πανταζοπούλου Α. *Cloud Computing & νομικά ζητήματα*, Νομική Βιβλιοθήκη, 2020, σελ. 171

είναι απαραίτητη η χορήγηση συγκατάθεσης ή η σύναψη σύμβασης και η διενέργεια της φορητότητας με αυτοματοποιημένα μέσα. Είναι συνήθως δυσχερής η άσκηση του ως άνω δικαιώματος στο υπολογιστικό νέφος καθώς πολλές φορές τα συστήματα που χρησιμοποιούν οι πάροχοι είναι ασύμβατα μεταξύ τους, με αποτέλεσμα είτε να μην μπορεί να ασκηθεί το δικαίωμα, είτε μέρος των δεδομένων να χάνεται[128]. Επιπλέον, μπορεί να μην δύναται να ασκηθεί αποτελεσματικά το ως άνω δικαίωμα, υπό την έννοια ότι γνωρίζοντας τη δυσκολία απόδειξης της ακεραιότητας των δεδομένων εντός του νέφους, καθίσταται μη εφικτός ο έλεγχος των δεδομένων κατά το στάδιο της φορητότητας.

**5.4 Ανάκτηση «απολεσθέντος» ελέγχου**

Στο περιβάλλον του υπολογιστικού νέφους παρατηρείται ενίοτε «απώλεια ελέγχου» επί των δεδομένων[129]. Η Ομάδα του Άρθρου 29 ορίζει ως «έλλειψη ελέγχου» τη μη δυνατότητα άσκησης αποκλειστικού ελέγχου του πελάτη επί των δεδομένων του. Ο πάροχος των υπηρεσιών νέφους μπορεί να αντισταθμίσει την ως άνω «απώλεια ελέγχου» διασφαλίζοντας αφενός τη δυνατότητα παρέμβασης όσον αφορά τα αποθηκευμένα δεδομένα, και αφετέρου τη διαφάνεια, όσον αφορά στο πόσοι και ποιοι εμπλέκονται στην αλυσίδα επεξεργασίας, καθώς και στο που λαμβάνει χώρα η εν λόγω επεξεργασία. Αφενός δηλαδή ο πάροχος θα πρέπει να διευκολύνει τη δυνατότητα εκ μέρους του χρήστη άσκησης των δικαιωμάτων πρόσβασης, διόρθωσης, διαγραφής κ.λ.π, και αφετέρου να παρέχει μια πολιτική διαφάνειας έναντι του πελάτη του. Θα πρέπει να γνωστοποιεί στον πελάτη κάθε σχετικό μέτρο που μπορεί να ενδυναμώνει ή να αποδυναμώνει τη νομιμότητα της επεξεργασίας, δηλαδή να αναφέρει τα υιοθετούμενα από αυτόν μέτρα ασφάλειας, την κοινοποίηση συμβάντων ασφαλείας, τις συνέπειες της επεξεργασίας κ.λ.π

Θα πρέπει ο πάροχος να ενημερώνει τους χρήστες σχετικά με τα εμπλεκόμενα μέρη στην αλυσίδα της επεξεργασίας, όπως για υπεργολάβους ή άλλους εκτελούντες την επεξεργασία, προκειμένου και οι ίδιοι να διασφαλίζουν τη συμμόρφωση με το νόμο. Θέτοντας εκ των προτέρων υπόψη στον πελάτη τα ως άνω δεδομένα, καθίσταται και αυτός συμμέτοχος στην επεξεργασία του παρόχου.

Τέλος, θεμελιώδης είναι η διαφάνεια σχετικά με τον τόπο επεξεργασίας των δεδομένων. Η γνώση του πελάτη σχετικά με τον τόπο στον οποίο βρίσκονται τα δεδομένα είναι σημαντική, προκειμένου να αίρονται τυχόν επιφυλάξεις και φόβοι, ως προς την απώλεια των δεδομένων του. Ειδικότερα, είναι απαραίτητο ο χρήστης να γνωρίζει τις περιοχές εντός των οποίων μετακινούνται τα δεδομένα, τον τόπο αποθήκευσης αυτών, καθώς και τον χρόνο μετακίνησής τους κατά τη διάρκεια της παροχής των υπηρεσιών νέφους. Αυτό βέβαια καθίσταται δύσκολο χάρη στη σύνθετη αρχιτεκτονική του «νέφους». Κάποια σχετική αναφορά σε ιστότοπους που ενημερώνουν τους χρήστες για το που βρίσκονται τα δεδομένα τους, θα ήταν ιδιαίτερα βοηθητική.

**5.5 Λογοδοσία και ευθύνη κατά τη διαβίβαση**

Σύμφωνα με τις *Συστάσεις υπ'αρ. 01/2020 του ΕΣΠΔ σχετικά με τα μέτρα που συμπληρώνουν τα εργαλεία διαβίβασης για τη διασφάλιση της συμμόρφωσης με το επίπεδο*

[128] Κουσουνή- Πανταζοπούλου Α. *Cloud Computing & νομικά ζητήματα*, Νομική Βιβλιοθήκη, 2020, σελ. 172

[129] Μήτρου Λ., Προστασία προσωπικών δεδομένων και υπολογιστικό νέφος, ΔΙΜΕΕ 4/2015, σελ.541

*προστασίας δεδομένων προσωπικού χαρακτήρα στην ΕΕ*, το δικαίωμα της προστασίας των προσωπικών δεδομένων αποτελεί θεμελιώδες δικαίωμα. Το ως άνω δικαίωμα χρήζει υψηλής προστασίας, ωστόσο μπορεί να υπάρξουν περιορισμοί που προβλέπονται από τη νομοθεσία, εφόσον σέβονται το περιεχόμενο του δικαιώματος, είναι αναλογικοί και αναγκαίοι και ανταποκρίνονται πράγματι στους στόχους γενικού συμφέροντος που αναγνωρίζονται από την ΕΕ.

Όπως προαναφέρθηκε, απαιτείται ένα ουσιαστικό επίπεδο προστασίας προσωπικών δεδομένων, ισοδύναμο με εκείνο που εγγυάται η ΕΕ ακόμη και όταν δεδομένα διαβιβάζονται σε τρίτες χώρες για να διασφαλίζεται το επίπεδο προστασίας που εγγυάται ο ΓΚΠΔ.

Οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία καλούνται να συμμορφώνονται με ενεργό και συνεχή τρόπο με το δικαίωμα της προστασίας των δεδομένων, εφαρμόζοντας τα απαραίτητα τεχνικά και οργανωτικά μέτρα που εξασφαλίζουν την αποτελεσματικότητά του. Πρέπει επίσης να μπορούν να αποδείξουν τις προσπάθειες αυτές στα υποκείμενα, των οποίων τα δεδομένα επεξεργάζονται, στο ευρύ κοινό αλλά και στις αρμόδιες εποπτικές αρχές. Αυτή είναι η αποκαλούμενη αρχή της λογοδοσίας.

Η αρχή της λογοδοσίας, η οποία αποτελεί θεμελιώδη αρχή για την αποτελεσματική εφαρμογή του ΓΚΠΔ, ισχύει και στις διαβιβάσεις δεδομένων σε τρίτες χώρες εντός του υπολογιστικού νέφους. Στην απόφαση Schrems II, το ΔΕΕ τόνισε τις ευθύνες των εξαγωγέων και των εισαγωγέων δεδομένων, υπό την έννοια ότι πρέπει να διασφαλίζουν ότι η επεξεργασία/διαβίβαση που τελούν, γίνεται σύμφωνα με το επίπεδο προστασίας που ορίζει η νομοθεσία της ΕΕ για την προστασία των δεδομένων και ότι οφείλουν να αναστέλλουν μια τέτοια διαβίβαση ή να καταγγέλλουν τη σχετική σύμβαση, εάν διαπιστώσουν ότι ο εισαγωγέας των δεδομένων δεν δύναται να τηρήσει τις τυποποιημένες ρήτρες προστασίας δεδομένων που ενσωματώνονται στη σχετική σύμβαση μεταξύ εισαγωγέα και εξαγωγέα δεδομένων.

Επιπλέον, ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία, που ενεργεί ως εξαγωγέας, πρέπει να διασφαλίζει ότι υπάρχει μεταξύ τους συνεργασία και ότι θα βρίσκονται σε συνεχή επικοινωνία σε περίπτωση οιασδήποτε εξέλιξης ως προς το επίπεδο προστασίας των δεδομένων που διαβιβάζονται στη χώρα του εισαγωγέα.

Προκειμένου λοιπόν να καταλογισθεί ευθύνη κατά τη διαβίβαση και επεξεργασία των προσωπικών δεδομένων[130], θα πρέπει να εντοπιστεί κατά πόσο και σε ποιο βαθμό η κατανομή των υποχρεώσεων και των ευθυνών πρέπει να καταλείπεται στη διακριτική ευχέρεια των μερών ή αν πρέπει να προσδιορίζεται συγκεκριμένα στον νόμο ή σε πρότυπες συμβατικές ρήτρες. Φρόνιμο είναι να προβλεφθεί εκ των προτέρων συμβατικά η ευθύνη των εμπλεκόμενων μερών, αλλά και οι συνέπειες αυτής της ευθύνης σε περίπτωση συμβάντος (incident).

Σχετικά δε με τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα μεταξύ δημόσιων φορέων, προβλέπονται ειδικές συστάσεις στις *Κατευθυντήριες Γραμμές 2/2020 σχετικά με το άρθρο 46 παρ.2 στοιχείο α) και 46 παρ.3 στοιχείο β) του Κανονισμού 2016/679 για διαβιβάσεις δεδομένων προσωπικού χαρακτήρα μεταξύ δημόσιων αρχών και φορέων του ΕΟΧ και εκτός του ΕΟΧ.*

[130] Μήτρου Λ. *Προστασία προσωπικών δεδομένων και υπολογιστικό νέφος*, ΔΙΜΕΕ 4/2015, σελ.542

**6. Συμπεράσματα**

Όπως προαναφέραμε και ανωτέρω, το φαινόμενο της νεφοϋπολογιστικής βρίσκεται σε πλήρη άνθηση και εξέλιξη, καθώς άπαντες σήμερα έχουν πρόσβαση στην τεχνολογία. Οι ΗΠΑ κατέχουν την πρωτοκαθεδρία στην παροχή υπηρεσιών νεφοϋπολογιστικής, διαθέτοντας τον μεγαλύτερο αριθμό παρόχων, ενώ ακολουθεί η Ασία με πρωτεργάτη την Κίνα[131].

Η νέα τεχνολογία edge computing (αποκεντρωμένη υπολογιστική)[132] απειλεί την νεφοϋπολογιστική καθώς ευνοεί την επεξεργασία των δεδομένων μέσω της ίδιας της συσκευής ή μέσω ενός τοπικού υπολογιστή ή διακομιστή. Οπότε τα δεδομένα με αυτό τον τρόπο δεν χρειάζεται να αποστέλλονται σε κέντρα δεδομένων απομακρυσμένα, αλλά αντιθέτως η επεξεργασία τους λαμβάνει χώρα πιο κοντά στο σημείο που παράγονται, με αποτέλεσμα να διευκολύνεται η επεξεργασία τους σε πραγματικό χρόνο. Επίσης, παύει η εξάρτηση από το ασύρματο δίκτυο (wi-fi).

Το υπολογιστικό νέφος αποτελεί το απόλυτο εργαλείο για τις διασυνοριακές διαβιβάσεις δεδομένων, καθώς αυτός ο τρόπος αποθήκευσης, διαχείρισης και διακίνησης των δεδομένων ευνοεί την αθρόα διακίνηση τους, ανά τον κόσμο. Όλες οι επιχειρήσεις και οι κυβερνήσεις κλήθηκαν να υιοθετήσουν ευρέως τις υπηρεσίες cloud και να μετασχηματισθούν ψηφιακά, χάρη στην πανδημία COVID-19, προκειμένου να ανταπεξέλθουν στις προκλήσεις του σύγχρονου ψηφιακού κόσμου. Επαναλαμβάνουμε ότι γενικός κανόνας είναι ότι οι διαβιβάσεις δεδομένων προς τρίτες χώρες απαγορεύονται, εκτός και αν παρέχεται επαρκές επίπεδο προστασίας αυτών από την τρίτη χώρα προορισμού.

Μελέτη που εκπόνησε η Ευρωπαϊκή Επιτροπή το 2021 με τίτλο 'The European Data Flow Monitoring'[133], σχετικά με τις ροές των δεδομένων εντός του υπολογιστικού νέφους, εντόπισε τον όγκο και τον τύπο των ροών, καθώς και το που διαβιβάζονται δεδομένα εντός της ΕΕ. Από τη μελέτη αυτή προέκυψε ότι στις 27 χώρες της ΕΕ οι ροές των δεδομένων προέρχονται από επιχειρήσεις που αγοράζουν υπηρεσίες υπολογιστικού νέφους από το διαδίκτυο. Ο μεγαλύτερος αριθμός επιχειρησιακών ροών προέρχεται από υποδομές cloud και edge στην Γερμανία. Το 2020 η Γερμανία έλαβε 151.968 TB ροών ανά μήνα από άλλες χώρες. Ο αριθμός αυτός αντιπροσωπεύει το 30,7% των ροών εντός της ΕΕ. Δεύτερη σε σειρά χώρα είναι η Ολλανδία. Η ίδια μελέτη κατέδειξε ότι η μεγαλύτερη διακίνηση δεδομένων ανά τομέα εντός ΕΕ το 2020 έλαβε χώρα πρώτα στον τομέα της υγείας, μετά στον τομέα της λιανικής και χονδρικής πώλησης και τέλος στην εκπαίδευση. Τέλος, η ίδια μελέτη σε συγκεντρωτικό της πίνακα αναδεικνύει ότι η Ελλάδα παραμένει πολύ μικρός παίκτης στην αγορά των υπηρεσιών νεφοϋπολογιστικής με ροές δεδομένων που ανήρθαν το 2020[134] στα 3.296 TB ανά μήνα, ενώ το 2025 εκτιμάται ότι θα ανέρθουν στα 15.916 TB και το 2030 στα 65.304TB.

Η εγγενής διασυνοριακή φύση των υπηρεσιών νέφους, όπως αναλύσαμε ανωτέρω, δημιουργεί πολλαπλές δυσχέρειες σε διάφορα επίπεδα, αλλά κυρίως σε επίπεδο νομικό, στο επίπεδο δηλαδή των διασυνοριακών διαβιβάσεων προσωπικών

---

[131] Κουσουνή-Πανταζοπούλου Α. *Cloud computing & νομ342ικά ζητήματα*, Νομική Βιβλ. 2021, σελ. 217

[132] Κουσουνή-Πανταζοπούλου Α. *Cloud computing & νομικά ζητήματα*, Νομική Βιβλ. 2021, σελ. 223

[133] Study on Mapping Data Flows, Final Report, European Commision, 2021,διαθέσιμο σε https://digital-strategy.ec.europa.eu/en/library/study-mapping-data-flows

[134] https://digital-strategy.ec.europa.eu/en/policies/european-data-flow-monitoring

δεδομένων και της σύναψης συμβάσεων παροχής υπηρεσιών νεφοϋπολογιστικής μεταξύ των παρόχων και των πελατών τους, όπου εμπλέκονται διαφορετικά εφαρμοστέα δίκαια και διαφορετικές δικαιοδοσίες. Κάθε διακίνηση δεδομένων, όπως προαναφέραμε, δεν αποτελεί απαραίτητα διαβίβαση που εμπίπτει στο Κεφάλαιο V του ΓΚΠΔ. Παρόλα ταύτα κάθε διακίνηση δεδομένων που ενέχει επεξεργασία μπορεί να συνοδεύεται από επικείμενους κινδύνους, ενδεικτικά λόγω της εθνικής νομοθεσίας που μπορεί να αλληλοσυγκρούεται με τον ΓΚΠΔ ή λόγω της πρόσβασης των κυβερνητικών αρχών στα δεδομένα τρίτης χώρας ή ακόμα και λόγω δυσκολιών ως προς την εφαρμογή μέτρων αποζημίωσης.

Η απόφαση Schrems II άλλαξε ριζικά το τοπίο των διαβιβάσεων σε ό,τι αφορά το περιβάλλον της νεφοϋπολογιστικής. Ως επικρατέστερη λύση για τη διαβίβαση δεδομένων σε τρίτες χώρες κατά την τρέχουσα χρονική περίοδο όταν ο πάροχος βρίσκεται εκτός ΕΕ κρίνεται η χρήση είτε των δεσμευτικών εταιρικών κανόνων, είτε των τυποποιημένων συμβατικών ρητρών. Ωστόσο πρέπει να διευκρινιστεί εκ νέου ότι πριν λάβει χώρα η διαβίβαση πρέπει πάντα να λαμβάνεται υπόψη το επίπεδο προστασίας των δεδομένων στην χώρα προορισμού καθώς και ότι η ισχύς των παραπάνω εργαλείων διαβίβασης επιβάλλει την παράλληλη χρήση συμπληρωματικών μέτρων ως επιπρόσθετη εγγύηση. Επίσης, υπενθυμίζεται ότι οι δεσμευτικοί εταιρικοί κανόνες και οι τυποποιημένες συμβατικές ρήτρες αποτελούν συμφωνίες που δεν δεσμεύουν τις κυβερνητικές υπηρεσίες των ΗΠΑ.

Η απόφαση Schrems II επισήμανε ξεκάθαρα ότι το υψηλό επίπεδο προστασίας δεδομένων που επιτάσσει ο ΓΚΠΔ και ο Χάρτης των Θεμελιωδών Δικαιωμάτων, είναι αναγκαίο για την αποτροπή των εξωτερικών κινδύνων που αφορούν στην προστασία των δικαιωμάτων των προσωπικών δεδομένων πολιτών της ΕΕ. Συνακόλουθα, εάν προκύψουν προβλήματα ή σύγκρουση μεταξύ του ΓΚΠΔ και των κανόνων περί διαβιβάσεων, αυτά θα πρέπει να επιλυθούν εφαρμόζοντας τη μέγιστη δυνατή προστασία για τα υποκείμενα των δεδομένων, όπως αυτή ερμηνεύεται στις αποφάσεις του ΔΕΕ.

Δεδομένου ότι η πλειοψηφία των παρόχων υπηρεσιών cloud βρίσκεται στις ΗΠΑ, με την διατλαντική συμφωνία μεταξύ ΗΠΑ και ΕΕ, η οποία αναμένεται να υπογραφεί περί τα τέλη του τρέχοντος έτους, προσδοκάται η επίτευξη μιας συμφωνίας η οποία θα επιτρέπει την ασφαλή διαβίβαση των δεδομένων από την ΕΕ στις ΗΠΑ. Ωστόσο ο νομικός κόσμος είναι επιφυλακτικός για το αν η συμφωνία «Privacy Shield 2.0» θα καταφέρει να «σταθεί» χωρίς να αποτελέσει και αυτή αντικείμενο ακύρωσης, και να αποτελέσει μία νέα απόφαση Schrems III. Αμφισβητείται εντόνως αν η νομοθεσία των μυστικών υπηρεσιών των ΗΠΑ θα μπορέσει να παράσχει την απολύτως αναγκαία προστασία στο μέλλον, ανάλογη δηλαδή αυτής που επιτάσσει ο ΓΚΠΔ. Στην πραγματικότητα αυτό δεν είναι εφικτό λόγω των συνταγματικών, θεσμικών και πρακτικών/πολιτικών εμποδίων των ΗΠΑ που παρεμποδίζουν την υιοθέτηση τέτοιων νόμων[135].

Όπως διατυπώνεται ευρέως, εάν οι ΗΠΑ και η ΕΕ λάβουν νομοθετικά μέτρα που προασπίζουν τα δικαιώματα των υποκειμένων των δεδομένων, και εάν οι ΗΠΑ μεταρρυθμίσουν τη νομοθεσία τους περί παρακολούθησης και τις σχετικές με αυτήν πρακτικές, οι οποίες θα βασίζονται εφεξής στην αποτελεσματική ένδικη προστασία των υποκειμένων των δεδομένων, τη διασφάλιση της αναγκαιότητας και της προσφορότητας της επιτήρησης, αλλά και στο κράτους δικαίου, τότε μια νέα συμφωνία μεταξύ ΕΕ και ΗΠΑ με γνώμονα την αυτοπιστοποίηση των επιχειρήσεων των ΗΠΑ θα μπορεί να

[135] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3884896

επιτευχθεί. Τούτο θα έχει ως αποτέλεσμα να καταστεί πιθανή η έκδοση μιας απόφασης επάρκειας για τις ΗΠΑ, η οποία θα περιορίζεται μόνο στη διαβίβαση δεδομένων από ευρωπαϊκούς οργανισμούς σε επιχειρήσεις των ΗΠΑ που έχουν αυτοπιστοποιηθεί εθελοντικά ως προς τη συμμόρφωσή τους με τα επιθυμητά επίπεδα προστασίας που επιτάσσει ο ΓΚΠΔ[136].

Εν κατακλείδι, συμπεραίνουμε ότι για τις διαβιβάσεις δεδομένων που εκτελούνται από παρόχους υπηρεσιών νεφοϋπολογιστικής εντός και εκτός ΕΕ θεμέλιο λίθο αποτελεί ο ΓΚΠΔ, ο οποίος αποτελεί την πλέον αποτελεσματική νομοθεσία. Ο κανονισμός αυτός μπορεί να εφαρμόζεται είτε στον πάροχο των υπηρεσιών είτε στον χρήστη αυτών. Σε κάθε περίπτωση, οι πάροχοι πρέπει να είναι σε θέση να διασφαλίσουν ανά πάσα στιγμή ότι τελούν σε γνώση των υποχρεώσεών τους, αλλά και ότι έχουν μεριμνήσει για την εφαρμογή των τεχνικών και οργανωτικών μέτρων που απαιτούνται και ότι εν γένει συμμορφώνονται με τις επιταγές του ΓΚΠΔ, εφόσον εμπίπτουν σε αυτόν. Αντίστοιχα, οι πελάτες του νέφους θα πρέπει να επιδεικνύουν ιδιαίτερη επιμέλεια κατά την επιλογή παρόχου και να ερευνούν οι ίδιοι αν αυτός συμμορφώνεται με τις επιταγές του ΓΚΠΔ.

Το υπολογιστικό νέφος λόγω της -εκ φύσεως- ελευθερίας του ως προς οιονδήποτε χωροθετικό περιορισμό, μπορεί να προωθήσει δυναμικά την ενιαία ψηφιακή αγορά σε ένα νέο επίπεδο[137]. Όπως προαναφέραμε, οι διαβιβάσεις που εκτελούνται εντός αυτού αποτελούν ένα εγγενές στοιχείο του και ως εκ τούτου δεν θα μπορούσε να υφίσταται χωρίς αυτές. Εν αναμονή λοιπόν της έκδοσης της πολυπόθητης απόφασης επάρκειας μεταξύ ΗΠΑ και ΕΕ, επισημαίνεται διαρκώς η κοινή ανάγκη των κρατών για αμοιβαία ρύθμιση των θεμάτων που άπτονται της προστασίας των προσωπικών δεδομένων και της εφαρμογής των θεμελιωδών αρχών προστασίας δεδομένων που θεμελιώνονται στον ΓΚΠΔ.

[136] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3884896

[137] Λωσταράκου Κυριακή, *Ο νέος Κανονισμός της Ευρωπαϊκής Ένωσης για την προστασία των προσωπικών δεδομένων- Οικονομικές επιπτώσεις στις επιχειρήσεις- Ειδικές υποχρεώσεις για τους παρόχους υπολογιστικού νέφους*, ΔΙΤΕ 3/2013

**ΕΛΛΗΝΙΚΗ ΒΙΒΛΙΟΓΡΑΦΙΑ**

- Γιαννόπουλος Γιώργος, Εισαγωγή στη Νομική Πληροφορική, Νομική Βιβλιοθήκη, 2018
- Ιγγλεζάκης Ιωάννης, *Δίκαιο Πληροφορικής*, Εκδόσεις Σάκκουλα, Αθήνα-Θεσσαλονίκη, 3η έκδοση, 2018
- Ιγγλεζάκης Ιωάννης, *Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων*, 2η έκδοση, Interactive Learning, 2018
- Κανέλλος Λεωνίδας, *The GDPR Handbook*, Νομική Βιβλιοθήκη, 2020
- Κοτσαλής Λεωνίδας, Μενουδάκος Κων/νος, *Γενικός Κανονισμός για την προστασία των προσωπικών δεδομένων (GDPR), Νομική διάσταση και πρακτική εφαρμογή*, Νομική Βιβλιοθήκη, 2020
- Κουσουνή- Πανταζοπούλου Αφροδίτη, *Cloud Computing & Νομικά ζητήματα*, Νομική Βιβλιοθήκη, 2022
- Μήτρου Λίλιαν, Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων, Σάκκουλας 2017
- Παπαχρίστου Θ.Κ., Βερναρδάκης Χ., Θεοδόσης Γ., Καμτσίδου Ι., Μανωλάκου Κ., Μήτρου Λ., Παπακωνσταντίνου Β., Ρεθυμιωτάκη Ε., Στρατηλάτης Κ., Τασόπουλος Γ., *(Αυτό)ρύθμιση στον κυβερνοχώρο;* , Εκδόσεις Σάκκουλα, 2005
- Ρεθυμιωτάκη Ελένη, Πηγές του δικαίου και νομικός πλουραλισμός στην ΕΕ, Αθήνα-Θεσσαλονίκη, Εκδόσεις Σάκκουλα, 2012λό

**ΕΛΛΗΝΙΚΗ ΑΡΘΡΟΓΡΑΦΙΑ ΣΕ ΝΟΜΙΚΑ ΠΕΡΙΟΔΙΚΑ/ΙΣΤΟΣΕΛΙΔΕΣ**

- Ιγγλεζάκης Ιωάννης, *Η ασπίδα προστασίας ΕΕ-ΗΠΑ για την ιδιωτικότητα (EU-US Privacy Shield)*, ΣΥΝ, 113/2016
- *Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων, Οργανισμός θεμελιωδών δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ευρώπης*, έκδοση 2018
- Καρφή Ζ. *Ανεπαρκές το επίπεδο προστασίας στις ΗΠΑ για τη μαζική διαβίβαση δεδομένων προσωπικού χαρακτήρα από οργανισμούς εγκατεστημένους στην ΕΕ*, ΕΕυρΔ 3/2020
-Κίτσος Π./ Παππά Π., *Η προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής στις υπηρεσίες του υπολογιστικού νέφους*, ΔΙΜΕΕ 2012
- Κωνσταντίνου Στ. EDPB: *Αλλάζει το τοπίο για τις διεθνείς διαβιβάσεις*, lawpspot.gr
- Κουσουνή-Πανταζοπούλου Α., *Νομικές διαστάσεις του cloud computing*, ΔΙΜΕΕ 2012
- Λωσταράκου Κυριακή, *Ο νέος Κανονισμός της Ευρωπαϊκής Ένωσης για την προστασία των προσωπικών δεδομένων- Οικονομικές επιπτώσεις στις επιχειρήσεις- Ειδικές υποχρεώσεις για τους παρόχους υπολογιστικού νέφους*, ΔΙΤΕ 3/2013
- Μήτρου Λίλιαν, *Προστασία προσωπικών δεδομένων και υπολογιστικό νέφος*, ΔΙΜΕΕ 4/2015
- Παλιού Ελίνα, *Οι νέες τυποποιημένες συμβατικές ρήτρες της ΕΕ: η διασυνοριακή διαβίβαση προσωπικών δεδομένων στον απόηχο της νομολογίας Schrems*, ΔΙΜΕΕ 4/2021
- Παναγοπούλου-Κουντατζή Φ. *Συνταγματικές προεκτάσεις των μηχανισμών διευρύνσεως της προστασίας δεδομένων προσωπικού χαρακτήρα πέραν της ΕΕ: Εξωεδαφική εφαρμογή του ΓΚΠΔ και διασυνοριακή διαβίβαση δεδομένων*, ΔΙΤΕ 4/2019
- Παπαδόπουλος Μαρίνος, Ευγενίδης Παντελής, *Νεφοϋπολογιστική (cloud computing) και προστασία προσωπικών δεδομένων*, ΔΙΜΕΕ 2/2016
- *Βόμβα από το Δικαστήριο της ΕΕ: Ανίσχυρη η απόφαση για διαβίβαση δεδομένων στις ΗΠΑ (Schrems II)*, www.lawspot.gr, 16/7/2020

**ΞΕΝΗ ΒΙΒΛΙΟΓΡΑΦΙΑ**

-Murray Andrew, *Information Technology Law*, 4th edition, Oxford University Press, 2019

- Handbook on European Data Protection Law, European Union Agency for fundamental rights and Council of Europe, 2018 edition

**ΞΕΝΗ ΑΡΘΡΟΓΡΑΦΙΑ ΣΕ ΝΟΜΙΚΑ ΠΕΡΙΟΔΙΚΑ/ΙΣΤΟΣΕΛΙΔΕΣ**

-*Unleashing the Potential of Cloud Computing in Europe*, COM(2012), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, διαθέσιμο σε https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF

- P. Mell/ T.Grance, *The NIST Definition of Cloud Computing*, National Institute of Standards and Technology, 2009, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

- Boudewijn de Bruin, Luciano Floridi, *The Ethics of Cloud Computing*, διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3835151

- Christopher Kuner, *Territorial Scope and Data Transfer Rules in the GPPR: Realising the EU's ambition of borderless Data protection*, σελ. 15, Legal Studies Research Paper Series by University of Cambride, April 2021, διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3827850

-*Personal Data Protection Digest* by Personal Data Protection Commission Singapore, 2021, διαθέσιμο σε https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Commissions-Decisions/2021-Personal-Data-Protection-Digest.ashx

-Study on Mapping Data Flows, Final Report, European Commision, 2021,διαθέσιμο σε https://digital-strategy.ec.europa.eu/en/library/study-mapping-data-flows

**ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ**

Παντελιάς Ιωάννης, *Νομικά ζητήματα συμφωνιών επιπέδου υπηρεσιών σε συμβάσεις αποθήκευσης ψηφιακών δεδομένων σε υπολογιστικό νέφος (cloud SLAs) στην Ευρώπη*, Πανεπιστήμιο Πειραιώς, 2018

1