

Συστάσεις



Translations proofread by EDPB Members.
This language version has not yet been proofread.

**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**

Έκδοση 2.0

Εγκρίθηκε στις 18 Ιουνίου 2021

Ιστορικό έκδοσης

Έκδοση 2.0	18 Ιουνίου 2021	Έγκριση των συστάσεων μετά από δημόσια διαβούλευση
Έκδοση 1.0	10 Νοεμβρίου 2020	Έγκριση των συστάσεων για δημόσια διαβούλευση

Συνοπτική παρουσίαση

Ο γενικός κανονισμός για την προστασία δεδομένων της ΕΕ (ΓΚΠΔ) εκδόθηκε για να εξυπηρετήσει διττό σκοπό: να διευκολύνει την ελεύθερη ροή δεδομένων προσωπικού χαρακτήρα εντός της Ευρωπαϊκής Ένωσης, προασπίζοντας παράλληλα τα θεμελιώδη δικαιώματα και τις ελευθερίες των ατόμων, ιδίως το δικαίωμά τους στην προστασία των δεδομένων προσωπικού χαρακτήρα.

Στην πρόσφατη απόφασή του C-311/18 (Schrems II), το Δικαστήριο της Ευρωπαϊκής Ένωσης (ΔΕΕ) μας υπενθυμίζει ότι η προστασία των δεδομένων προσωπικού χαρακτήρα στον Ευρωπαϊκό Οικονομικό Χώρο (ΕΟΧ) πρέπει να συνοδεύει τα δεδομένα, οποιοσδήποτε και αν είναι ο προορισμός τους. Η διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες δεν μπορεί να αποτελέσει μέσο υπονόμευσης ή υποβάθμισης της προστασίας που παρέχεται στον ΕΟΧ. Το Δικαστήριο υποστηρίζει περαιτέρω το παραπάνω διευκρινίζοντας ότι το επίπεδο προστασίας σε τρίτες χώρες δεν απαιτείται να είναι ίδιο με εκείνο που διασφαλίζεται εντός του ΕΟΧ αλλά ουσιαστικά ισοδύναμο. Το Δικαστήριο επιβεβαιώνει επίσης το κύρος των τυποποιημένων συμβατικών ρητρών, ως εργαλείο διαβίβασης που μπορεί να χρησιμεύσει για να εξασφαλίσει συμβατικά ένα ουσιαστικά ισοδύναμο επίπεδο προστασίας για δεδομένα που διαβιβάζονται σε τρίτες χώρες.

Οι τυποποιημένες συμβατικές ρήτρες και άλλα εργαλεία διαβίβασης που αναφέρονται στο άρθρο 46 του ΓΚΠΔ δεν λειτουργούν σε συνθήκες νομικού κενού. Το Δικαστήριο διευκρινίζει ότι οι υπεύθυνοι επεξεργασίας ή οι εκτελούντες την επεξεργασία, οι οποίοι ενεργούν ως εξαγωγείς, είναι υπεύθυνοι να ελέγχουν κατά περίπτωση και, ενδεχομένως, σε συνεργασία με τον εισαγωγέα στην τρίτη χώρα, κατά πόσο το δίκαιο ή η πρακτική στην τρίτη χώρα θίγει την αποτελεσματικότητα των κατάλληλων εγγυήσεων που περιέχονται στα εργαλεία διαβίβασης του άρθρου 46 του ΓΚΠΔ. Σε αυτές τις περιπτώσεις, το Δικαστήριο εξακολουθεί να αφήνει ανοιχτό το ενδεχόμενο οι εξαγωγείς να εφαρμόζουν πρόσθετα μέτρα που καλύπτουν τα εν λόγω κενά στην προστασία και επιτυγχάνουν το επίπεδο που απαιτείται από το δίκαιο της Ένωσης. Το Δικαστήριο δεν διευκρινίζει ποια μέτρα θα μπορούσαν να είναι αυτά. Ωστόσο, το Δικαστήριο υπογραμμίζει ότι οι εξαγωγείς θα πρέπει να τα προσδιορίζουν κατά περίπτωση. Το εν λόγω συνάδει με την αρχή της λογοδοσίας του άρθρου 5.2 του ΓΚΠΔ σύμφωνα με το οποίο απαιτείται από τους υπεύθυνους επεξεργασίας να λογοδοτούν και να είναι σε θέση να αποδείξουν τη συμμόρφωση με τις αρχές του ΓΚΠΔ σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Προκειμένου να συνδράμει τους εξαγωγείς (είτε πρόκειται για υπεύθυνους επεξεργασίας ή εκτελούντες την επεξεργασία, είτε για πρόσωπα ιδιωτικού ή δημόσιου δικαίου, που επεξεργάζονται δεδομένα προσωπικού χαρακτήρα εντός του πεδίου εφαρμογής του ΓΚΠΔ) στο περίπλοκο έργο της αξιολόγησης τρίτων χωρών και του προσδιορισμού κατάλληλων πρόσθετων μέτρων, όπου απαιτείται, το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (ΕΣΠΔ) εξέδωσε τις παρούσες συστάσεις. Οι παρούσες συστάσεις παρέχουν στους εξαγωγείς μια σειρά βημάτων που θα πρέπει να ακολουθήσουν, πιθανές πηγές πληροφοριών και ορισμένα παραδείγματα πρόσθετων μέτρων που θα μπορούσαν να εφαρμοστούν.

Ως **πρώτο βήμα**, το ΕΣΠΔ συμβουλεύει εσάς, τους εξαγωγείς, να **γνωρίζετε τις διαβιβάσεις σας**. Η χαρτογράφηση όλων των διαβιβάσεων δεδομένων προσωπικού χαρακτήρα προς τρίτες χώρες μπορεί να είναι ένα δύσκολο εγχείρημα. Η ενημέρωση όσον αφορά τον προορισμό των δεδομένων προσωπικού χαρακτήρα είναι ωστόσο απαραίτητη, ώστε να διασφαλίζεται ότι παρέχεται ένα ουσιαστικά ισοδύναμο επίπεδο προστασίας οπουδήποτε πραγματοποιείται επεξεργασία. Πρέπει επίσης να επαληθεύετε ότι τα δεδομένα που διαβιβάζετε είναι κατάλληλα, συναφή και περιορίζονται σε ό,τι είναι αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία.

Ένα **δεύτερο βήμα** είναι η **επαλήθευση του εργαλείου διαβίβασης στο οποίο βασίζεται η διαβίβασή σας**, μεταξύ εκείνων που απαριθμούνται στο κεφάλαιο V του ΓΚΠΔ. Εάν η Ευρωπαϊκή Επιτροπή έχει ήδη δηλώσει τη χώρα, την περιοχή ή τον τομέα προς τον οποίο διαβιβάζετε τα δεδομένα ως επαρκή, μέσω μίας από τις αποφάσεις της περί επάρκειας βάσει του άρθρου 45 του ΓΚΠΔ ή βάσει της προηγούμενης οδηγίας 95/46, εφόσον η απόφαση εξακολουθεί να ισχύει, δεν θα χρειαστεί να λάβετε

περαιτέρω μέτρα, πέραν της παρακολούθησης ότι η απόφαση περί επάρκειας εξακολουθεί να ισχύει. Ελλείψει απόφασης περί επάρκειας, πρέπει να βασίζεστε σε ένα από τα εργαλεία διαβίβασης που απαριθμούνται στο άρθρο 46 του ΓΚΠΔ. Μόνο σε ορισμένες περιπτώσεις ενδέχεται να μπορείτε να βασιστείτε σε κάποια από τις παρεκκλίσεις που προβλέπονται στο άρθρο 49 του ΓΚΠΔ, εάν πληροίτε τις προϋποθέσεις. Οι παρεκκλίσεις δεν μπορούν να καταστούν «ο κανόνας» στην πράξη αλλά πρέπει να περιορίζονται σε συγκεκριμένες περιπτώσεις.

Ένα **τρίτο βήμα** είναι να **αξιολογήσετε** αν υπάρχει κάτι στη νομοθεσία ή/και στις ισχύουσες πρακτικές της τρίτης χώρας που θα μπορούσε να επηρεάσει την αποτελεσματικότητα των κατάλληλων εγγυήσεων των εργαλείων διαβίβασης στα οποία βασίζεστε, στο πλαίσιο της συγκεκριμένης διαβίβασής σας. Η αξιολόγησή σας θα πρέπει να εστιάζει πρωτίστως στη νομοθεσία της τρίτης χώρας που σχετίζεται με τη διαβίβασή σας και το εργαλείο διαβίβασης του άρθρου 46 του ΓΚΠΔ στο οποίο βασίζεστε. Επίσης, η εξέταση των πρακτικών τις οποίες εφαρμόζουν οι δημόσιες αρχές της τρίτης χώρας θα σας δώσει τη δυνατότητα να επαληθεύσετε αν οι εγγυήσεις που περιλαμβάνονται στο εργαλείο διαβίβασης μπορούν να διασφαλίσουν στην πράξη την αποτελεσματική προστασία των δεδομένων προσωπικού χαρακτήρα που διαβιβάζονται. Η εξέταση των εν λόγω πρακτικών θα έχει ιδιαίτερη σημασία για την αξιολόγησή σας σε περίπτωση που:

(i.) η νομοθεσία της τρίτης χώρας που πληροί επισήμως τα πρότυπα της ΕΕ εμφανώς δεν εφαρμόζεται/τηρείται στην πράξη·

(ii.) υπάρχουν πρακτικές ασύμβατες με τις δεσμεύσεις που έχουν αναληφθεί μέσω του εργαλείου διαβίβασης όποτε δεν υπάρχει σχετική νομοθεσία στην τρίτη χώρα·

(iii.) τα διαβιβαζόμενα δεδομένα σας ή/και ο εισαγωγέας εμπίπτουν ή ενδέχεται να εμπίπτουν στο πεδίο εφαρμογής προβληματικής νομοθεσίας (δηλαδή θίγει τη συμβατική εγγύηση ουσιαστικά ισοδύναμου επιπέδου προστασίας που παρέχει το εργαλείο διαβίβασης και δεν πληροί τα πρότυπα της ΕΕ για τα θεμελιώδη δικαιώματα, την αναγκαιότητα και την αναλογικότητα).

Στις δύο πρώτες περιπτώσεις, θα πρέπει να αναστείλετε τη διαβίβαση ή να εφαρμόσετε επαρκή πρόσθετα μέτρα εφόσον επιθυμείτε να προχωρήσετε στη διαβίβαση.

Στην τρίτη περίπτωση, λαμβανομένων υπόψη των αβεβαιοτήτων που συνδέονται με τη δυνητική εφαρμογή προβληματικής νομοθεσίας στη διαβίβασή σας, μπορείτε να αποφασίσετε: να αναστείλετε τη διαβίβαση, να εφαρμόσετε πρόσθετα μέτρα για να προχωρήσετε στη διαβίβαση ή, εναλλακτικά, μπορείτε να αποφασίσετε να προβείτε στη διαβίβαση χωρίς να εφαρμόσετε πρόσθετα μέτρα εάν πιστεύετε και είστε σε θέση να αποδείξετε και να τεκμηριώσετε ότι δεν έχετε λόγους να πιστεύετε ότι η συναφής και προβληματική νομοθεσία θα ερμηνευτεί ή/και θα εφαρμοστεί στην πράξη κατά τρόπο ώστε να καλύψει τα διαβιβαζόμενα δεδομένα σας και τον εισαγωγέα.

Για την αξιολόγηση των στοιχείων που πρέπει να λαμβάνονται υπόψη κατά την αξιολόγηση της νομοθεσίας τρίτης χώρας που αφορά την πρόσβαση σε δεδομένα από δημόσιες αρχές για σκοπούς επιτήρησης, ανατρέξτε στις συστάσεις των ευρωπαϊκών βασικών εγγυήσεων του ΕΣΠΔ.

Θα πρέπει επίσης να πραγματοποιήσετε αυτήν την αξιολόγηση με τη δέουσα επιμέλεια και να την τεκμηριώσετε ενδελεχώς. Οι αρμόδιες εποπτικές ή/και δικαστικές αρχές σας ενδέχεται να τη ζητήσουν και να σας θεωρήσουν υπεύθυνους για κάθε απόφαση που θα λάβετε επί αυτής της βάσης.

Ένα **τέταρτο βήμα** είναι να **προσδιορίσετε και να θεσπίσετε πρόσθετα μέτρα** που είναι αναγκαία προκειμένου το επίπεδο προστασίας των διαβιβαζόμενων δεδομένων να προσεγγίσει το επίπεδο του προτύπου της ΕΕ όσον αφορά την ουσιαστική ισοδυναμία. Αυτό το βήμα είναι απαραίτητο μόνον εάν από την αξιολόγησή σας προκύψει ότι η νομοθεσία ή/και οι πρακτικές τρίτων χωρών επηρεάζουν την αποτελεσματικότητα του εργαλείου διαβίβασης του άρθρου 46 του ΓΚΠΔ στο οποίο βασίζεστε ή σκοπεύετε να βασιστείτε στο πλαίσιο της διαβίβασής σας. Οι παρούσες συστάσεις περιλαμβάνουν (στο παράρτημα 2) μη εξαντλητικό κατάλογο με παραδείγματα πρόσθετων μέτρων με ορισμένες από τις προϋποθέσεις που απαιτούνται προκειμένου τα μέτρα αυτά να είναι αποτελεσματικά. Όπως και στην περίπτωση των κατάλληλων εγγυήσεων που περιλαμβάνονται στα εργαλεία διαβίβασης του

άρθρου 46, ορισμένα πρόσθετα μέτρα ενδέχεται να είναι αποτελεσματικά σε ορισμένες χώρες, αλλά όχι απαραίτητα σε άλλες. Θα είστε υπεύθυνοι για την αξιολόγηση της αποτελεσματικότητάς τους στο πλαίσιο της διαβίβασης, ερμηνευόμενα υπό το πρίσμα της νομοθεσίας και των πρακτικών της τρίτης χώρας και του εργαλείου διαβίβασης στο οποίο βασίζεστε, καθώς θα θεωρηθείτε υπεύθυνοι για κάθε απόφαση που θα λάβετε επί αυτής της βάσης. Αυτό μπορεί επίσης να απαιτεί από εσάς να συνδυάσετε πολλά πρόσθετα μέτρα. Ενδέχεται τελικά να διαπιστώσετε ότι κανένα πρόσθετο μέτρο δεν μπορεί να διασφαλίσει ένα ουσιαστικά ισοδύναμο επίπεδο προστασίας για τη συγκεκριμένη διαβίβασή σας. Στις περιπτώσεις όπου δεν είναι κατάλληλο κανένα πρόσθετο μέτρο, πρέπει ή να αποφύγετε ή να αναστείλετε ή να τερματίσετε τη διαβίβαση, για να αποφευχθεί η παραβίαση του επιπέδου προστασίας των δεδομένων προσωπικού χαρακτήρα. Θα πρέπει επίσης να πραγματοποιήσετε αυτήν την αξιολόγηση πρόσθετων μέτρων με τη δέουσα επιμέλεια και να την τεκμηριώσετε.

Ένα **πέμπτο βήμα** είναι να **προβείτε** σε τυχόν **τυπικές διαδικαστικές ενέργειες** που μπορεί να απαιτούνται από την έγκριση του πρόσθετου μέτρου σας, ανάλογα με το εργαλείο διαβίβασης του άρθρου 46 του ΓΚΠΔ στο οποίο βασίζεστε. Οι παρούσες συστάσεις καθορίζουν ορισμένες από τις εν λόγω διατυπώσεις. Ίσως χρειαστεί να συμβουλευτείτε τις αρμόδιες εποπτικές αρχές σας για ορισμένες από αυτές.

Το **έκτο και τελευταίο βήμα** είναι να **επανεκτιμάτε** σε τακτά χρονικά διαστήματα το επίπεδο προστασίας των δεδομένων προσωπικού χαρακτήρα που διαβιβάζετε σε τρίτες χώρες και να παρακολουθείτε αν υπήρξαν ή αν υπάρξουν εξελίξεις που μπορεί να τα επηρεάσουν. Η αρχή της λογοδοσίας απαιτεί συνεχή επαγρύπνηση του επιπέδου προστασίας των δεδομένων προσωπικού χαρακτήρα.

Οι εποπτικές αρχές θα εξακολουθήσουν να ασκούν την εντολή τους για την παρακολούθηση της εφαρμογής του ΓΚΠΔ και να τον επιβάλλουν. Οι εποπτικές αρχές θα λάβουν δεόντως υπόψη τα μέτρα που λαμβάνουν οι εξαγωγείς για να διασφαλίσουν ότι τα δεδομένα που διαβιβάζουν χαρακτηρίζονται από ένα ουσιαστικά ισοδύναμο επίπεδο προστασίας. Όπως υπενθυμίζει το Δικαστήριο, οι εποπτικές αρχές θα αναστέλλουν ή θα απαγορεύουν τις διαβιβάσεις δεδομένων στις περιπτώσεις όπου διαπιστώνουν ότι δεν μπορεί να διασφαλιστεί ένα ουσιαστικά ισοδύναμο επίπεδο προστασίας, κατόπιν έρευνας ή καταγγελίας.

Οι εποπτικές αρχές θα συνεχίσουν να εκδίδουν κατευθυντήριες γραμμές για τους εξαγωγείς και να συντονίζουν τις ενέργειές τους στο ΕΣΠΔ, προκειμένου να διασφαλίζεται η συνεκτική εφαρμογή της νομοθεσίας της ΕΕ για την προστασία των δεδομένων.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

1	Λογοδοσία κατά τη διαβίβαση δεδομένων.....	10
2	Χάρτης πορείας: πρακτική εφαρμογή της αρχής της λογοδοσίας κατά τη διαβίβαση δεδομένων 11	
2.1	Βήμα 1: Γνώση των διαβιβάσεών σας.....	12
2.2	Βήμα 2: Προσδιορισμός των εργαλείων διαβιβάσεων στα οποία βασίζεστε	13
2.3	Βήμα 3: Αξιολόγηση του εάν το εργαλείο διαβίβασης του άρθρου 46 του ΓΚΠΔ στο οποίο βασίζεστε είναι αποτελεσματικό υπό το πρίσμα όλων των συνθηκών που περιβάλλουν τη διαβίβαση	17
2.4	Βήμα 4: Εφαρμογή πρόσθετων μέτρων	26
2.5	Βήμα 5: Διαδικαστικά βήματα εάν έχετε προσδιορίσει αποτελεσματικά πρόσθετα μέτρα	30
2.6	Βήμα 6: Επαναξιολόγηση σε τακτά χρονικά διαστήματα.....	32
3	Συμπέρασμα.....	32
	ΠΑΡΑΡΤΗΜΑ 1: ΟΡΙΣΜΟΙ	34
	ΠΑΡΑΡΤΗΜΑ 2. ΠΑΡΑΔΕΙΓΜΑΤΑ ΠΡΟΣΘΕΤΩΝ ΜΕΤΡΩΝ	35
	2.1 Τεχνικά μέτρα.....	35
	2.2 Πρόσθετα συμβατικά μέτρα	48
	2.3 Οργανωτικά μέτρα	58
	ΠΑΡΑΡΤΗΜΑ 3: ΠΙΘΑΝΕΣ ΠΗΓΕΣ ΠΛΗΡΟΦΟΡΙΩΝ ΓΙΑ ΤΗΝ ΑΞΙΟΛΟΓΗΣΗ τρίτης χώρας	62

Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων

Έχοντας υπόψη το άρθρο 70 παράγραφος 1 στοιχείο ε) του κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (εφεξής «ΓΚΠΔ»),

Έχοντας υπόψη τη Συμφωνία για τον Ευρωπαϊκό Οικονομικό Χώρο (ΕΟΧ) και ιδίως το παράρτημα ΧΙ και το πρωτόκολλο 37 αυτής, όπως τροποποιήθηκαν με την απόφαση της Μικτής Επιτροπής του ΕΟΧ αριθ. 154/2018, της 6ης Ιουλίου 2018¹,

Έχοντας υπόψη το άρθρο 12 και το άρθρο 22 του εσωτερικού κανονισμού του

Εκτιμώντας τα ακόλουθα:

(1) Το Δικαστήριο της Ευρωπαϊκής Ένωσης (ΔΕΕ) καταλήγει στην απόφαση C-311/18 της 16ης Ιουλίου 2020 *Επίτροπος προστασίας δεδομένων κατά Facebook Ireland Limited και Maximillian Schrems*, ότι το άρθρο 46 παράγραφος 1 και το άρθρο 46 παράγραφος 2 στοιχείο γ) του ΓΚΠΔ έχει την έννοια ότι οι κατάλληλες εγγυήσεις, τα εκτελεστά δικαιώματα και τα αποτελεσματικά μέσα έννομης προστασίας που απαιτούνται κατά τις διατάξεις αυτές πρέπει να διασφαλίζουν ότι τα δικαιώματα των ατόμων των οποίων τα δεδομένα προσωπικού χαρακτήρα διαβιβάζονται προς τρίτη χώρα βάσει τυποποιημένων ρητρών προστασίας δεδομένων τυχάνουν ενός επιπέδου προστασίας ουσιαστικά ισοδύναμο με εκείνο που εγγυάται εντός της Ευρωπαϊκής Ένωσης ο κανονισμός αυτός, όπως ερμηνεύεται σε συνδυασμό με τον Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης.²

(2) Όπως υπογράμμισε το Δικαστήριο, ένα επίπεδο προστασίας των φυσικών προσώπων το οποίο είναι ουσιαστικά ισοδύναμο με εκείνο που διασφαλίζεται εντός της Ευρωπαϊκής Ένωσης από τον ΓΚΠΔ, και ερμηνεύεται υπό το πρίσμα του Χάρτη, πρέπει να διασφαλίζεται ανεξάρτητα από τη διάταξη του Κεφαλαίου V βάσει του οποίου πραγματοποιείται διαβίβαση δεδομένων προσωπικού χαρακτήρα προς τρίτη χώρα. Οι διατάξεις του κεφαλαίου V αποσκοπούν στη διασφάλιση της συνέχειας αυτού του υψηλού επιπέδου προστασίας σε περίπτωση διαβίβασης δεδομένων προσωπικού χαρακτήρα προς τρίτη χώρα.³

(3) Η αιτιολογική σκέψη 108 και το άρθρο 46 παράγραφος 1 του ΓΚΠΔ προβλέπουν ότι, ελλείψει απόφασης επάρκειας, ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία θα πρέπει να λαμβάνει μέτρα για να αντισταθμίσει την έλλειψη προστασίας των δεδομένων στην τρίτη χώρα μέσω κατάλληλων εγγυήσεων υπέρ του υποκειμένου των δεδομένων. Ένας υπεύθυνος επεξεργασίας ή

¹ Οι αναφορές στα «κράτη μέλη» στο παρόν έγγραφο θα πρέπει να νοούνται ως αναφορές στα «κράτη μέλη του ΕΟΧ».

² Απόφαση του ΔΕΕ της 16ης Ιουλίου 2020, *Επίτροπος προστασίας δεδομένων κατά Facebook Ireland Limited και Maximillian Schrems* (εφεξής: C-311/18 (Schrems II)), δεύτερη διαπίστωση.

³ C-311/18 (Schrems II), σκέψεις 92 και 93.

εκτελών την επεξεργασία μπορεί να παρέχει κατάλληλες εγγυήσεις, χωρίς να απαιτείται ειδική άδεια εποπτικής αρχής, μέσω της χρήσης ενός από τα εργαλεία διαβίβασης που αναφέρονται στο άρθρο 46 παράγραφος 2 του ΓΚΠΔ, όπως οι τυποποιημένες ρήτρες προστασίας δεδομένων.

(4) Το Δικαστήριο διευκρινίζει ότι οι τυποποιημένες ρήτρες προστασίας δεδομένων που εγκρίνονται από την Επιτροπή έχουν ως αποκλειστικό σκοπό να παράσχουν στους εγκατεστημένους εντός της Ευρωπαϊκής Ένωσης υπευθύνους επεξεργασίας ή εκτελούντες την επεξεργασία συμβατικές εγγυήσεις που να εφαρμόζονται ομοιόμορφα σε όλες τις τρίτες χώρες. Λόγω του συμβατικού τους χαρακτήρα, οι τυποποιημένες ρήτρες προστασίας δεδομένων δεν είναι δυνατόν να δεσμεύουν τις δημόσιες αρχές των τρίτων χωρών, δεδομένου ότι δεν είναι μέρη της σύμβασης. Κατά συνέπεια, οι εξαγωγείς δεδομένων ενδέχεται να απαιτηθεί να συμπληρώσουν τις εγγυήσεις που περιέχονται σε αυτές τις τυποποιημένες ρήτρες προστασίας δεδομένων με πρόσθετα μέτρα για τη διασφάλιση της συμμόρφωσης με το επίπεδο προστασίας που απαιτείται βάσει της ενωσιακής νομοθεσίας σε συγκεκριμένη τρίτη χώρα. Το Δικαστήριο αναφέρεται στην αιτιολογική σκέψη 109 του ΓΚΠΔ, η οποία αναφέρει την εν λόγω δυνατότητα και ενθαρρύνει τους υπεύθυνους επεξεργασίας και τους εκτελούντες την επεξεργασία να τη χρησιμοποιούν.⁴

(5) Το Δικαστήριο δήλωσε ότι είναι πρωτίστως καθήκον του εξαγωγέα δεδομένων να ελέγχει κατά περίπτωση και, ενδεχομένως, σε συνεργασία με τον εισαγωγέα των δεδομένων, κατά πόσον το δίκαιο της τρίτης χώρας προορισμού διασφαλίζει ένα ουσιαστικά ισοδύναμο επίπεδο προστασίας, υπό το πρίσμα του ενωσιακού δικαίου, των δεδομένων προσωπικού χαρακτήρα που διαβιβάζονται βάσει τυποποιημένων ρητρών προστασίας δεδομένων, παρέχοντας, εν ανάγκη, πρόσθετα μέτρα πέραν εκείνων τα οποία προσφέρουν οι ρήτρες αυτές.⁵

(6) Σε περίπτωση που ούτε ο εγκατεστημένος εντός της Ένωσης υπεύθυνος επεξεργασίας ούτε ο εγκατεστημένος εντός της Ένωσης εκτελών την επεξεργασία μπορούν να λάβουν επαρκή πρόσθετα μέτρα για τη διασφάλιση ουσιαστικά ισοδύναμου επιπέδου προστασίας σύμφωνα με το δίκαιο της Ένωσης, τότε αυτοί ή, επικουρικώς, η αρμόδια εποπτική αρχή υποχρεούνται να αναστείλουν ή να τερματίσουν τη διαβίβαση δεδομένων προσωπικού χαρακτήρα προς την οικεία τρίτη χώρα.⁶

(7) Ο ΓΚΠΔ ή το Δικαστήριο δεν ορίζουν ούτε προσδιορίζουν τις «πρόσθετες εγγυήσεις», «συμπληρωματικά μέτρα» ή «πρόσθετα μέτρα» στις εγγυήσεις των εργαλείων διαβίβασης που αναφέρονται στο άρθρο 46.2 του ΓΚΠΔ τα οποία οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία μπορούν να εγκρίνουν για να διασφαλίσουν τη συμμόρφωση με το επίπεδο προστασίας που απαιτείται βάσει του δικαίου της Ένωσης σε μια συγκεκριμένη τρίτη χώρα.

⁴ C-311/18 (Schrems II), σκέψεις 132 και 133.

⁵ C-311/18 (Schrems II), σκέψεις 92 και 134.

⁶ C-311/18 (Schrems II), σκέψη 135.

(8) Το ΕΣΠΔ αποφάσισε, με δική του πρωτοβουλία, να εξετάσει το εν λόγω ζήτημα και να παράσχει στους υπεύθυνους επεξεργασίας και στους εκτελούντες την επεξεργασία, οι οποίοι ενεργούν ως εξαγωγείς, συστάσεις σχετικά με τη διαδικασία που μπορούν να ακολουθήσουν για τον προσδιορισμό και την εφαρμογή πρόσθετων μέτρων. Οι εν λόγω συστάσεις αποσκοπούν στην παροχή μεθοδολογίας για τους εξαγωγείς ώστε να αποφασίζουν αν και ποια πρόσθετα μέτρα θα πρέπει να λαμβάνουν για τις διαβιβάσεις τους. Αποτελεί πρωταρχική ευθύνη των εξαγωγέων να διασφαλίζουν ότι τα δεδομένα που διαβιβάζονται τυγχάνουν στην τρίτη χώρα ενός επιπέδου προστασίας ουσιαστικά ισοδύναμου με εκείνο που διασφαλίζεται εντός του ΕΟΧ. Με αυτές τις συστάσεις, το ΕΣΠΔ επιδιώκει να ενθαρρύνει τη συνεκτική εφαρμογή του ΓΚΠΔ και της απόφασης του Δικαστηρίου, σύμφωνα με την εντολή του ΕΣΠΔ.⁷

ΕΞΕΔΩΣΕ ΤΙΣ ΑΚΟΛΟΥΘΕΣ ΣΥΣΤΑΣΕΙΣ:

⁷ Άρθρο 70.1 στοιχείο ε) του ΓΚΠΔ.

1 ΛΟΓΟΔΟΣΙΑ ΚΑΤΑ ΤΗ ΔΙΑΒΙΒΑΣΗ ΔΕΔΟΜΕΝΩΝ

1. Το πρωτογενές δίκαιο της ΕΕ θεωρεί το δικαίωμα της προστασίας των δεδομένων ως θεμελιώδες δικαίωμα.⁸ Ως εκ τούτου, το δικαίωμα της προστασίας των δεδομένων τυγχάνει υψηλού επιπέδου προστασίας και μπορούν να υπάρξουν περιορισμοί μόνο εάν προβλέπονται από τη νομοθεσία, εάν σέβονται το βασικό περιεχόμενο του δικαιώματος, εάν είναι αναλογικοί, αναγκαίοι και αν ανταποκρίνονται πράγματι στους στόχους γενικού συμφέροντος που αναγνωρίζονται από την Ένωση ή από την ανάγκη προστασίας των δικαιωμάτων και των ελευθεριών τρίτων.⁹ Το δικαίωμα της προστασίας των δεδομένων προσωπικού χαρακτήρα δεν είναι απόλυτο δικαίωμα· πρέπει να εξεταστεί σε σχέση με τη λειτουργία του στην κοινωνία και να σταθμίζεται έναντι άλλων θεμελιωδών δικαιωμάτων, σύμφωνα με την αρχή της αναλογικότητας.¹⁰
2. Ένα ουσιαστικά ισοδύναμο επίπεδο προστασίας με εκείνο που είναι εγγυημένο εντός της ΕΕ πρέπει να συνοδεύει τα δεδομένα που διαβιβάζονται σε τρίτες χώρες εκτός του ΕΟΧ για να διασφαλίζεται ότι δεν υπονομεύεται το επίπεδο προστασίας που εγγυάται ο ΓΚΠΔ, τόσο κατά τη διάρκεια της διαβίβασης όσο και μετά από αυτή.
3. Το δικαίωμα της προστασίας των δεδομένων έχει ενεργό χαρακτήρα. Απαιτεί από τους εξαγωγείς και τους εισαγωγείς (είτε πρόκειται για υπεύθυνους επεξεργασίας είτε για εκτελούντες την επεξεργασία) να υπερβαίνουν την αναγνώριση ή την παθητική συμμόρφωση με αυτό το δικαίωμα.¹¹ Οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία πρέπει να επιδιώκουν να συμμορφώνονται με ενεργό και συνεχή τρόπο με το δικαίωμα της προστασίας των δεδομένων, εφαρμόζοντας νομικά, τεχνικά και οργανωτικά μέτρα που εξασφαλίζουν την αποτελεσματικότητά του. Οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία πρέπει επίσης να είναι σε θέση να αποδείξουν αυτές τις προσπάθειες στα υποκείμενα των δεδομένων και στις εποπτικές αρχές προστασίας δεδομένων. Αυτή είναι η λεγόμενη αρχή της λογοδοσίας.¹²
4. Η αρχή της λογοδοσίας, η οποία είναι απαραίτητη για τη διασφάλιση της αποτελεσματικής εφαρμογής του επιπέδου προστασίας που παρέχει ο ΓΚΠΔ ισχύει επίσης για διαβιβάσεις δεδομένων σε τρίτες χώρες¹³ δεδομένου ότι αποτελούν από μόνες τους μια μορφή επεξεργασίας δεδομένων.¹⁴ Όπως υπογράμμισε το Δικαστήριο στην απόφασή του, ένα επίπεδο προστασίας το οποίο είναι ουσιαστικά ισοδύναμο με εκείνο που διασφαλίζεται εντός της Ευρωπαϊκής Ένωσης από τον ΓΚΠΔ, και ερμηνεύεται υπό το πρίσμα του Χάρτη, πρέπει να διασφαλίζεται ανεξάρτητα

⁸ Άρθρο 8, παράγραφος 1, Χάρτης των Θεμελιωδών Δικαιωμάτων και άρθρο 16, παράγραφος 1 ΣΛΕΕ, προοίμιο 1, άρθρο 1 παράγραφος 2 του ΓΚΠΔ.

⁹ Άρθρο 52 παράγραφος 1 του Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ.

¹⁰ Αιτιολογική σκέψη 4 του ΓΚΠΔ και C-507/17 Google LLC, διαδόχου της Google Inc. Google Inc. κατά Commission nationale de l'informatique et des libertés (CNIL), σκέψη 60.

¹¹ C-92/09 και C-93/02, Volker und Markus Schecke GbR κατά Land Hessen, προτάσεις της γενικής εισαγγελέως Eleanor Sharpston, της 17ης Ιουνίου 2010, παράγραφος 71.

¹² Άρθρο 5.2 και άρθρο 28.3 στοιχείο η) του ΓΚΠΔ.

¹³ Άρθρο 44 και αιτιολογική σκέψη 101 του ΓΚΠΔ, καθώς και άρθρο 47 παράγραφος 2 στοιχείο δ) του ΓΚΠΔ.

¹⁴ Απόφαση ΔΕΕ της 6ης Οκτωβρίου 2015, Maximilian Schrems κατά Data Protection Commissioner, (εφεξής C-362/14 (Schrems I)), σκέψη 45.

από τη διάταξη του κεφαλαίου βάσει του οποίου πραγματοποιείται διαβίβαση δεδομένων προσωπικού χαρακτήρα προς τρίτη χώρα.¹⁵

5. Στην απόφαση Schrems II, το Δικαστήριο υπογραμμίζει τις ευθύνες των εξαγωγέων και των εισαγωγέων να διασφαλίζουν ότι η επεξεργασία των δεδομένων προσωπικού χαρακτήρα πραγματοποιήθηκε και θα συνεχίσει να πραγματοποιείται σύμφωνα με το επίπεδο προστασίας που ορίζει η νομοθεσία της ΕΕ για την προστασία των δεδομένων και να αναστείλει τη διαβίβαση ή/και να καταγγείλει τη σύμβαση όταν ο εισαγωγέας των δεδομένων δεν είναι, ή δεν είναι πλέον, σε θέση να τηρήσει τις τυποποιημένες ρήτρες προστασίας δεδομένων που ενσωματώνονται στη σχετική σύμβαση μεταξύ του εξαγωγέα και του εισαγωγέα.¹⁶ Ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία που ενεργεί ως εξαγωγέας πρέπει να διασφαλίζει ότι οι εισαγωγείς συνεργάζονται με τον εξαγωγέα, κατά περίπτωση, κατά την εκπλήρωση των εν λόγω αρμοδιοτήτων, διατηρώντας τον ενήμερο, για παράδειγμα, για οποιαδήποτε εξέλιξη επηρεάζει το επίπεδο προστασίας των δεδομένων προσωπικού χαρακτήρα που λαμβάνονται στη χώρα του εισαγωγέα.¹⁷ Οι εν λόγω αρμοδιότητες αποτελούν εφαρμογή της αρχής του ΓΚΠΔ σχετικά με τη λογοδοσία κατά τις διαβιβάσεις δεδομένων.¹⁸

2 ΧΑΡΤΗΣ ΠΟΡΕΙΑΣ: ΠΡΑΚΤΙΚΗ ΕΦΑΡΜΟΓΗ ΤΗΣ ΑΡΧΗΣ ΤΗΣ ΛΟΓΟΔΟΣΙΑΣ ΚΑΤΑ ΤΗ ΔΙΑΒΙΒΑΣΗ ΔΕΔΟΜΕΝΩΝ

6. Ακολουθεί ένας χάρτης πορείας για τα βήματα που πρέπει να ακολουθήσετε προκειμένου να διαπιστώσετε αν εσείς (ο εξαγωγέας δεδομένων) πρέπει να λάβετε πρόσθετα μέτρα προκειμένου να είστε σε θέση να διαβιβάσετε νομίμως δεδομένα εκτός του ΕΟΧ. Ως «εσείς» στο παρόν έγγραφο νοείται ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία ο οποίος ενεργεί ως εξαγωγέας δεδομένων¹⁹ και επεξεργάζεται δεδομένα προσωπικού χαρακτήρα εντός του πεδίου εφαρμογής του ΓΚΠΔ – συμπεριλαμβανομένης της επεξεργασίας από ιδιωτικούς φορείς και δημόσιους οργανισμούς κατά τη διαβίβαση δεδομένων σε ιδιωτικούς οργανισμούς.²⁰ Όσον αφορά τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα μεταξύ δημόσιων φορέων, προβλέπεται ειδική καθοδήγηση στις *Κατευθυντήριες γραμμές 2/2020 σχετικά με το άρθρο 46 παράγραφος 2 στοιχείο α) και το άρθρο 46 παράγραφος 3 στοιχείο β) του κανονισμού 2016/679*

¹⁵ C-311/18 (Schrems II), σκέψεις 92 και 93.

¹⁶ C-311/18 (Schrems II), σκέψεις 134, 135, 139, 140, 141, 142.

¹⁷ C-311/18 (Schrems II), σκέψη 134.

¹⁸ Άρθρο 5 παράγραφος 2 και άρθρο 28 παράγραφος 3 στοιχείο η) του ΓΚΠΔ.

¹⁹ Επομένως, για παράδειγμα, δεν θα θεωρηθείτε εξαγωγέας δεδομένων εάν είστε υποκείμενο δεδομένων που παρέχει τα οικεία δεδομένα προσωπικού χαρακτήρα μέσω διαδικτυακού ερωτηματολογίου σε υπεύθυνο επεξεργασίας εγκατεστημένο σε τρίτη χώρα.

²⁰ Βλ. κατευθυντήριες γραμμές 3/2018 του ΕΣΠΔ σχετικά με το εδαφικό πεδίο εφαρμογής του ΓΚΠΔ (άρθρο 3) https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en

για τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα μεταξύ δημόσιων αρχών και φορέων του ΕΟΧ και φορέων εκτός ΕΟΧ.²¹

7. Θα χρειαστεί να τεκμηριώσετε επαρκώς αυτήν την αξιολόγηση και τα πρόσθετα μέτρα που επιλέγετε και εφαρμόζετε και να θέσετε στη διάθεση της αρμόδιας εποπτικής αρχής την εν λόγω τεκμηρίωση κατόπιν αιτήματος.²²

2.1 Βήμα 1: Γνώση των διαβιβάσεών σας

8. Για να μάθετε τι μπορεί να απαιτείται προκειμένου εσείς (ο εξαγωγέας δεδομένων) να μπορείτε να συνεχίσετε ή να προβείτε σε νέες διαβιβάσεις δεδομένων προσωπικού χαρακτήρα,²³ το πρώτο βήμα είναι να βεβαιωθείτε ότι γνωρίζετε πλήρως τις διαβιβάσεις σας (γνώση των διαβιβάσεών σας). Η καταγραφή και η χαρτογράφηση όλων των διαβιβάσεων μπορεί να είναι μια περίπλοκη άσκηση για οντότητες που συμμετέχουν σε πολλαπλές, διαφορετικές και τακτικές διαβιβάσεις με τρίτες χώρες και χρησιμοποιούν μια σειρά υπεύθυνων επεξεργασίας και υπεργολάβων επεξεργασίας. Η γνώση των διαβιβάσεών σας αποτελεί ένα ουσιαστικό πρώτο βήμα για την εκπλήρωση των υποχρεώσεών σας βάσει της αρχής της λογοδοσίας.
9. Για να αποκτήσετε πλήρη γνώση των διαβιβάσεών σας, μπορείτε να αξιοποιήσετε τα αρχεία των δραστηριοτήτων επεξεργασίας που ενδέχεται να υποχρεωθείτε να τηρήσετε ως υπεύθυνοι επεξεργασίας ή εκτελούντες την επεξεργασία σύμφωνα με το άρθρο 30 του ΓΚΠΔ.²⁴ Προηγούμενες ενέργειες για την εκπλήρωση των υποχρεώσεων ενημέρωσης των υποκειμένων των δεδομένων σύμφωνα με τα άρθρα 13.1 στοιχείο στ) και 14.1 στοιχείο στ) του ΓΚΠΔ σχετικά με τις διαβιβάσεις των προσωπικών σας δεδομένων σε τρίτες χώρες μπορούν επίσης να σας βοηθήσουν.²⁵

²¹ Κατευθυντήριες γραμμές 2/2020 του ΕΣΠΑ σχετικά με το άρθρο 46 παράγραφος 2 στοιχείο β) και το άρθρο 46 παράγραφος 3 στοιχείο β) του κανονισμού 2016/679 για τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα μεταξύ δημόσιων αρχών και φορέων του ΕΟΧ και φορέων εκτός ΕΟΧ· βλ. https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-22020-articles-46-2-and-46-3-b_en

²² Άρθρο 5 παράγραφος 2 του ΓΚΠΔ και άρθρο 24 παράγραφος 1 του ΓΚΠΔ.

²³ Λάβετε υπόψη ότι η απομακρυσμένη πρόσβαση από μια οντότητα από τρίτη χώρα σε δεδομένα που βρίσκονται στον ΕΟΧ θεωρείται επίσης διαβίβαση.

²⁴ Βλ. άρθρο 30 του ΓΚΠΔ και ιδίως τις παραγράφους 1 στοιχείο ε) και 2 στοιχείο γ). Επιπλέον, τα αρχεία επεξεργασίας θα πρέπει να περιέχουν περιγραφή των δραστηριοτήτων επεξεργασίας (συμπεριλαμβανομένων, ενδεικτικά, των κατηγοριών των υποκειμένων των δεδομένων, των κατηγοριών δεδομένων προσωπικού χαρακτήρα και των σκοπών της επεξεργασίας και συγκεκριμένων πληροφοριών σχετικά με τις διαβιβάσεις δεδομένων). Ορισμένοι υπεύθυνοι επεξεργασίας και εκτελούντες την επεξεργασία εξαιρούνται από την υποχρέωση τήρησης αρχείων επεξεργασίας (άρθρο 30.5 του ΓΚΠΔ). Για καθοδήγηση σχετικά με την εν λόγω εξαίρεση, βλ. ομάδα εργασίας του άρθρου 29, έγγραφο θέσης σχετικά με τις παρεκκλίσεις από την υποχρέωση τήρησης αρχείων δραστηριοτήτων επεξεργασίας σύμφωνα με το άρθρο 30.5 του ΓΚΠΔ (εγκρίθηκε από το ΕΣΠΑ στις 25 Μαΐου 2018).

²⁵ Σύμφωνα με τους κανόνες διαφάνειας του ΓΚΠΔ, πρέπει να ενημερώσετε τα υποκείμενα των δεδομένων σχετικά με τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες (άρθρο 13.1 στοιχείο στ) και άρθρο 14.1 στοιχείο στ) του ΓΚΠΔ). Συγκεκριμένα, πρέπει να τα ενημερώσετε για την ύπαρξη ή την απουσία απόφασης επάρκειας από την Ευρωπαϊκή Επιτροπή, ή στην περίπτωση διαβιβάσεων που αναφέρονται στο άρθρο 46 ή στο άρθρο 47 του ΓΚΠΔ, ή στο άρθρο 49.1 δεύτερο εδάφιο του ΓΚΠΔ, να ανατρέξετε στις ενδεδειγμένες ή κατάλληλες εγγυήσεις και στα μέσα με τα οποία μπορείτε να λάβετε αντίγραφο αυτών ή όπου έχουν καταστεί διαθέσιμα. Οι πληροφορίες που παρέχονται στο υποκείμενο των δεδομένων πρέπει να είναι σωστές και επικαιροποιημένες, ιδίως βάσει της νομολογίας του Δικαστηρίου σχετικά με τις διαβιβάσεις.

10. Κατά τη χαρτογράφηση των διαβιβάσεων, μην ξεχάσετε να λάβετε επίσης υπόψη τις περαιτέρω διαβιβάσεις, για παράδειγμα εάν οι εκτελούντες την επεξεργασία εκτός του ΕΟΧ διαβιβάζουν τα δεδομένα προσωπικού χαρακτήρα που τους έχετε εμπιστευτεί σε έναν υπεργολάβο επεξεργασίας σε άλλη τρίτη χώρα ή στην ίδια τρίτη χώρα.²⁶
11. Σύμφωνα με την αρχή της «ελαχιστοποίησης δεδομένων» του ΓΚΠΔ,²⁷ πρέπει να επαληθεύετε ότι τα δεδομένα που διαβιβάζετε είναι κατάλληλα, συναφή και περιορίζονται σε ό,τι είναι αναγκαίο σε σχέση με τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία.
12. Οι εν λόγω δραστηριότητες πρέπει να πραγματοποιηθούν πριν από την εκτέλεση και ενημέρωση οποιασδήποτε διαβίβασης πριν από την επανάληψη των διαβιβάσεων μετά την αναστολή των πράξεων διαβίβασης δεδομένων: πρέπει να γνωρίζετε πού βρίσκονται τα δεδομένα προσωπικού χαρακτήρα που έχετε εξαγάγει ή πού τα επεξεργάστηκαν οι εισαγωγείς (χάρτης προορισμών).
13. Λάβετε υπόψη ότι η απομακρυσμένη πρόσβαση από τρίτη χώρα (για παράδειγμα σε καταστάσεις υποστήριξης) ή/και η αποθήκευση σε υπολογιστικό νέφος που βρίσκεται εκτός του ΕΟΧ από πάροχο υπηρεσιών, θεωρείται επίσης διαβίβαση.²⁸ Ειδικότερα, εάν χρησιμοποιείτε μια διεθνή υποδομή υπολογιστικού νέφους, πρέπει να αξιολογήσετε αν τα δεδομένα σας θα διαβιβασθούν σε τρίτες χώρες καθώς και πού θα διαβιβασθούν, εκτός εάν ο πάροχος του υπολογιστικού νέφους είναι εγκατεστημένος στον ΕΟΧ και δηλώνει σαφώς στη σύμβασή του ότι τα δεδομένα δεν θα υποβληθούν σε καμία επεξεργασία σε τρίτες χώρες.

2.2 Βήμα 2: Προσδιορισμός των εργαλείων διαβιβάσεων στα οποία βασίζεστε

14. Ένα δεύτερο βήμα που πρέπει να κάνετε είναι να προσδιορίσετε τα εργαλεία διαβίβασης στα οποία βασίζεστε μεταξύ των εν λόγω καταλόγων και προβλέψεων του κεφαλαίου V του ΓΚΠΔ.

Αποφάσεις επάρκειας

15. Η Ευρωπαϊκή Επιτροπή μπορεί να αναγνωρίσει μέσω των **αποφάσεων επάρκειας** που λαμβάνει και αφορούν ορισμένες ή όλες τις τρίτες χώρες στις οποίες διαβιβάζετε δεδομένα προσωπικού χαρακτήρα ένα επαρκές επίπεδο προστασίας για τα δεδομένα προσωπικού χαρακτήρα.²⁹
16. Το αποτέλεσμα μιας τέτοιας απόφασης επάρκειας είναι ότι τα δεδομένα προσωπικού χαρακτήρα μπορούν να διαβιβαστούν από τον ΕΟΧ στην εν λόγω τρίτη χώρα χωρίς να απαιτείται κάποιο εργαλείο διαβίβασης του άρθρου 46 του ΓΚΠΔ.

²⁶ Όταν ο υπεύθυνος επεξεργασίας έχει χορηγήσει προηγουμένως ειδική ή γενική γραπτή εξουσιοδότηση σύμφωνα με το άρθρο 28.2 του ΓΚΠΔ.

²⁷ Άρθρο 5.1 στοιχείο γ) του ΓΚΠΔ.

²⁸ Βλ. ΣΕ αριθ. 11 «υπενθυμίζεται ότι ακόμη και η παροχή πρόσβασης σε δεδομένα από τρίτη χώρα, για παράδειγμα για διοικητικούς σκοπούς, ισοδυναμεί επίσης με διαβίβαση», Συχνές Ερωτήσεις ΕΣΠΔ σχετικά με την απόφαση του Δικαστηρίου της Ευρωπαϊκής Ένωσης στην υπόθεση C-311/18 - Επίτροπος προστασίας δεδομένων κατά Facebook Ireland Ltd και Maximilian Schrems της 23ης Ιουλίου 2020.

²⁹ Η Ευρωπαϊκή Επιτροπή έχει την εξουσία να καθορίζει, βάσει του άρθρου 45 του ΓΚΠΔ αν μια χώρα εκτός της ΕΕ παρέχει επαρκές επίπεδο προστασίας δεδομένων. Ομοίως, η Ευρωπαϊκή Επιτροπή έχει την εξουσία να καθορίζει αν ένας διεθνής οργανισμός παρέχει επαρκές επίπεδο προστασίας.

17. Οι αποφάσεις επάρκειας ενδέχεται να καλύπτουν μια χώρα στο σύνολό της ή να περιορίζονται σε ένα μέρος της. Οι αποφάσεις επάρκειας ενδέχεται να καλύπτουν όλες τις διαβιβάσεις δεδομένων σε μια χώρα ή να περιορίζονται σε ορισμένους τύπους διαβιβάσεων (π.χ. σε έναν τομέα).³⁰
18. Η Ευρωπαϊκή Επιτροπή δημοσιεύει τον κατάλογο των αποφάσεων επάρκειας που λαμβάνει στον δικτυακό της τόπο.³¹
19. Εάν διαβιβάζετε δεδομένα προσωπικού χαρακτήρα σε τρίτες χώρες, περιοχές ή τομείς που καλύπτονται από απόφαση επάρκειας της Επιτροπής (στον βαθμό που ισχύει), **δεν υποχρεούστε να λάβετε περαιτέρω μέτρα όπως περιγράφεται στις παρούσες συστάσεις.**³² Ωστόσο, πρέπει να παρακολουθείτε αν οι αποφάσεις επάρκειας που αφορούν τις διαβιβάσεις σας ανακαλούνται ή ακυρώνονται.³³
20. Ωστόσο, οι αποφάσεις επάρκειας δεν εμποδίζουν τα υποκείμενα των δεδομένων να υποβάλουν καταγγελίες. Ούτε εμποδίζουν τις εποπτικές αρχές να παραπέμψουν την υπόθεση ενώπιον εθνικού δικαστηρίου εάν έχουν αμφιβολίες σχετικά με την εγκυρότητα μιας απόφασης, ώστε το εθνικό δικαστήριο να είναι σε θέση να υποβάλει αίτηση έκδοσης προδικαστικής απόφασης στο ΔΕΕ για τον σκοπό εξέτασης της εν λόγω εγκυρότητας.³⁴

Παράδειγμα:

Ένας πολίτης της ΕΕ, ο κ. Schrems, υπέβαλε καταγγελία τον Ιούνιο του 2013 στην Επιτροπή Προστασίας Δεδομένων (ΕΠΔ) της Ιρλανδίας και ζήτησε από αυτήν την εποπτική αρχή να απαγορεύσει ή να αναστείλει τη διαβίβαση των δεδομένων προσωπικού χαρακτήρα του από το Facebook Ιρλανδίας στις Ηνωμένες Πολιτείες, καθώς θεώρησε ότι η νομοθεσία και η πρακτική των Ηνωμένων Πολιτειών δεν εξασφάλιζαν επαρκή προστασία των δεδομένων προσωπικού χαρακτήρα που διατηρούνται στην επικράτεια του έναντι των δραστηριοτήτων επιτήρησης που πραγματοποιούσαν εκεί οι δημόσιες αρχές. Η ΕΠΔ απέρριψε την καταγγελία, με την αιτιολογία,

³⁰ Άρθρο 45.1 του ΓΚΠΔ.

³¹ https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en**Error! Hyperlink reference not valid.**

³² Εφόσον εσείς και ο εισαγωγέας δεδομένων σας εφαρμόζετε μέτρα συμμόρφωσης με τις άλλες υποχρεώσεις βάσει του ΓΚΠΔ· σε άλλη περίπτωση τα εν λόγω μέτρα εφαρμόζονται.

³³ Η Ευρωπαϊκή Επιτροπή πρέπει να επανεξετάζει σε τακτά χρονικά διαστήματα όλες τις αποφάσεις επάρκειας και να παρακολουθεί αν οι τρίτες χώρες που επωφελούνται από αποφάσεις επάρκειας εξακολουθούν να διασφαλίζουν επαρκές επίπεδο προστασίας (βλ. άρθρα 45.3 και 45.4 του ΓΚΠΔ). Επίσης, το ΔΕΕ μπορεί να ακυρώσει τις αποφάσεις επάρκειας (βλ. αποφάσεις του για τις υποθέσεις C-362/14 (Schrems I) και C-311/18 (Schrems II)).

³⁴ C-311/18 (Schrems II), σκέψεις 118 - 120. Οι εποπτικές αρχές δεν μπορούν να αγνοήσουν την απόφαση επάρκειας και να αναστείλουν ή να απαγορεύσουν τη διαβίβαση δεδομένων προσωπικού χαρακτήρα στις εν λόγω χώρες, αναφέροντας μόνο την ανεπάρκεια του επιπέδου προστασίας. Μπορούν μόνο να ασκήσουν την εξουσία τους για αναστολή ή απαγόρευση της διαβίβασης δεδομένων προσωπικού χαρακτήρα στην εν λόγω τρίτη χώρα για άλλους λόγους (π.χ. ανεπαρκή μέτρα ασφαλείας κατά παράβαση του άρθρου 32 του ΓΚΠΔ, καμία νομική βάση δεν υποστηρίζει ορθώς την επεξεργασία δεδομένων ως τέτοια κατά παράβαση του άρθρου 6 του ΓΚΠΔ). Οι εποπτικές αρχές μπορούν να εξετάζουν, με απόλυτη ανεξαρτησία, αν η διαβίβαση των εν λόγω δεδομένων συμμορφώνεται με τις απαιτήσεις που ορίζει ο ΓΚΠΔ και, κατά περίπτωση, να ασκούν προσφυγές ενώπιον των εθνικών δικαστηρίων, εάν έχουν αμφιβολίες ως προς την εγκυρότητα της απόφασης επάρκειας της Επιτροπής, να υποβάλλουν αίτηση έκδοσης προδικαστικής απόφασης ενώπιον του Δικαστηρίου της Ευρωπαϊκής Ένωσης, προκειμένου να εξετάζεται η εγκυρότητά της.

κυρίως, ότι στην απόφαση 2000/520 η Ευρωπαϊκή Επιτροπή θεωρούσε ότι, στο πλαίσιο του καθεστώτος «ασφαλούς λιμένα», οι Ηνωμένες Πολιτείες εξασφάλιζαν επαρκές επίπεδο προστασίας των διαβιβαζόμενων δεδομένων προσωπικού χαρακτήρα (η απόφαση ασφαλούς λιμένα). Ο κ. Schrems αμφισβήτησε την απόφαση της ΕΠΔ και το Ανώτατο Δικαστήριο της Ιρλανδίας υπέβαλε ερώτημα επί του κύρους της απόφασης 2000/520 στο Δικαστήριο της Ευρωπαϊκής Ένωσης (ΔΕΕ). Στη συνέχεια, το ΔΕΕ αποφάσισε να ακυρώσει την απόφαση 2000/520 της Επιτροπής σχετικά με την επάρκεια της προστασίας που παρέχεται από τις αρχές ασφαλούς λιμένα για την προστασία της ιδιωτικής ζωής.³⁵

³⁵ Υπόθεση C-362/14 (Schrems I).

Εργαλεία διαβίβασης του άρθρου 46 του ΓΚΠΔ

21. Το άρθρο 46 του ΓΚΠΔ αναφέρει μια σειρά εργαλείων διαβίβασης που περιλαμβάνουν «κατάλληλες εγγυήσεις» τις οποίες οι εξαγωγείς μπορούν να χρησιμοποιήσουν για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες σε περίπτωση που δεν υπάρχει απόφαση επάρκειας. Οι κύριοι τύποι εργαλείων διαβίβασης του άρθρου 46 του ΓΚΠΔ είναι οι εξής:
- τυποποιημένες συμβατικές ρήτρες προστασίας δεδομένων (ΤΣΡ)
 - δεσμευτικοί εταιρικοί κανόνες (ΔΕΚ)
 - κώδικες δεοντολογίας
 - μηχανισμοί πιστοποίησης
 - ειδικές συμβατικές ρήτρες.
22. Ανεξάρτητα από το εργαλείο διαβίβασης του άρθρου 46 του ΓΚΠΔ που επιλέγετε, πρέπει να διασφαλίζετε ότι, συνολικά, τα διαβιβαζόμενα δεδομένα προσωπικού χαρακτήρα θα τυγχάνουν ενός ουσιαστικά ισοδύναμου επιπέδου προστασίας.
23. Τα εργαλεία διαβίβασης του άρθρου 46 του ΓΚΠΔ περιέχουν κυρίως κατάλληλες εγγυήσεις συμβατικού χαρακτήρα που μπορούν να εφαρμοστούν σε διαβιβάσεις σε όλες τις τρίτες χώρες. Η κατάσταση στην τρίτη χώρα στην οποία διαβιβάζετε δεδομένα ενδέχεται να εξακολουθεί να απαιτεί να συμπληρώσετε τα εν λόγω εργαλεία διαβίβασης και τις εγγυήσεις που περιέχουν πρόσθετα μέτρα («πρόσθετα μέτρα») για να εξασφαλίσετε ένα ουσιαστικά ισοδύναμο επίπεδο προστασίας.³⁶

Παρεκκλίσεις

24. Εκτός από τις αποφάσεις επάρκειας και τα εργαλεία διαβίβασης του άρθρου 46 του ΓΚΠΔ, ο ΓΚΠΔ περιέχει έναν τρίτο τρόπο ο οποίος επιτρέπει τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε ορισμένες περιπτώσεις. Με την επιφύλαξη συγκεκριμένων προϋποθέσεων, ενδέχεται να εξακολουθείτε να μπορείτε να διαβιβάσετε δεδομένα προσωπικού χαρακτήρα βάσει παρέκκλισης που αναφέρεται στο άρθρο 49 του ΓΚΠΔ.
25. Το άρθρο 49 του ΓΚΠΔ είναι εξαιρετικού χαρακτήρα. Οι παρεκκλίσεις που περιλαμβάνει πρέπει να ερμηνεύονται κατά τρόπο που δεν αντίκειται στην ίδια τη φύση των παρεκκλίσεων ως εξαιρέσεων από τον κανόνα ότι τα δεδομένα προσωπικού χαρακτήρα δεν μπορούν να διαβιβάζονται σε τρίτη χώρα εκτός εάν η χώρα προβλέπει επαρκές επίπεδο προστασίας δεδομένων ή, εναλλακτικά, έχουν θεσπιστεί κατάλληλες εγγυήσεις. Οι παρεκκλίσεις δεν μπορούν να καταστούν «ο κανόνας» στην πράξη αλλά πρέπει να περιορίζονται σε συγκεκριμένες περιπτώσεις. Το ΕΣΠΔ εξέδωσε τις κατευθυντήριες γραμμές 2/2018 αναφορικά με τις παρεκκλίσεις που προβλέπονται στο άρθρο 49 του Κανονισμού 2016/679.³⁷
26. Πριν βασιστείτε σε παρέκκλιση του άρθρου 49 του ΓΚΠΔ, πρέπει να ελέγξετε αν η διαβίβασή σας πληροί τις αυστηρές προϋποθέσεις που ορίζει η εν λόγω διάταξη για καθεμία από αυτές.

³⁶ C-311/18 (Schrems II), σκέψεις 130 και 133. Βλ. επίσης επιμέρους τμήμα 2.3 κατωτέρω.

³⁷ Για περαιτέρω καθοδήγηση όσον αφορά αυτό το θέμα, βλ. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_en.

27. Εάν η διαβίβασή σας δεν μπορεί να βασιστεί νομικά σε απόφαση επάρκειας, ούτε σε παρέκκλιση με βάση το άρθρο 49, πρέπει να προχωρήσετε στο βήμα 3.

2.3 Βήμα 3: Αξιολόγηση του εάν το εργαλείο διαβίβασης του άρθρου 46 του ΓΚΠΔ στο οποίο βασίζεστε είναι αποτελεσματικό υπό το πρίσμα όλων των συνθηκών που περιβάλλουν τη διαβίβαση

28. Το επιλεγμένο εργαλείο διαβίβασης του άρθρου 46 του ΓΚΠΔ πρέπει να εξασφαλίζει με αποτελεσματικό τρόπο ότι το επίπεδο προστασίας που εγγυάται ο ΓΚΠΔ δεν υπονομεύεται στην πράξη από τη διαβίβαση.³⁸

29. Ειδικότερα, η προστασία που παρέχεται στα διαβιβαζόμενα δεδομένα προσωπικού χαρακτήρα στην τρίτη χώρα πρέπει να είναι ουσιαστικά ισοδύναμη με την προστασία που εγγυάται ο ΓΚΠΔ στον ΕΟΧ, ερμηνευόμενη υπό το πρίσμα του Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ.³⁹ Αυτό δεν ισχύει εάν ο εισαγωγέας δεδομένων εμποδίζεται να συμμορφωθεί με τις υποχρεώσεις του βάσει του επιλεγμένου εργαλείου διαβίβασης του άρθρου 46 του ΓΚΠΔ λόγω της νομοθεσίας και των πρακτικών της τρίτης χώρας που ισχύουν για τη διαβίβαση, συμπεριλαμβανομένων όσων ισχύουν κατά τη διέλευση των δεδομένων από τον εξαγωγέα στη χώρα του εισαγωγέα.⁴⁰

30. Πρέπει πρώτα να αξιολογήσετε, κατά περίπτωση και σε συνεργασία με τον εισαγωγέα, αν υπάρχει κάτι στη νομοθεσία ή/και στις ισχύουσες πρακτικές⁴¹ της τρίτης χώρας που θα μπορούσε να επηρεάσει την αποτελεσματικότητα των κατάλληλων εγγυήσεων του εργαλείου διαβίβασης του άρθρου 46 του ΓΚΠΔ στο οποίο βασίζεστε, στο πλαίσιο της συγκεκριμένης διαβίβασής σας. Αυτό υποδηλώνει ότι πρέπει να προσδιορίσετε αν η διαβίβασή σας εμπίπτει στο πεδίο εφαρμογής νομοθεσίας ή/και πρακτικών που θα μπορούσαν να επηρεάσουν την αποτελεσματικότητα του οικείου εργαλείου διαβίβασης του άρθρου 46 του ΓΚΠΔ. Η απαιτούμενη αξιολόγηση πρέπει να βασίζεται πρωτίστως στη νομοθεσία που είναι δημοσίως διαθέσιμη.

31. Αυτή η αξιολόγηση πρέπει να περιέχει στοιχεία που αφορούν την πρόσβαση σε δεδομένα από δημόσιες αρχές της τρίτης χώρας του εισαγωγέα σας όπως:

- στοιχεία σχετικά με το αν οι δημόσιες αρχές της τρίτης χώρας του εισαγωγέα σας θα μπορούσαν να επιδιώξουν να αποκτήσουν πρόσβαση στα δεδομένα εν γνώσει ή εν αγνοία του εισαγωγέα δεδομένων, υπό το πρίσμα της νομοθεσίας, της πρακτικής και αναφερόμενου δικαστικού προηγούμενου·
- στοιχεία σχετικά με το αν οι δημόσιες αρχές της τρίτης χώρας του εισαγωγέα σας θα μπορούσαν να αποκτήσουν πρόσβαση στα δεδομένα μέσω του εισαγωγέα δεδομένων ή μέσω των παρόχων τηλεπικοινωνιών ή των διαύλων επικοινωνίας, υπό το πρίσμα της

³⁸ Άρθρο 44 του ΓΚΠΔ και σκέψεις 126, 137 και 148 της απόφασης C-311/18 (Schrems II).

³⁹ C-311/18 (Schrems II), σκέψη 105 και δεύτερη διαπίστωση.

⁴⁰ Βλ. C-311/18 (Schrems II), σκέψη 183 σε συνδυασμό με τη σκέψη 184.

⁴¹ Βλ. σκέψη 126 της απόφασης C-311/18 (Schrems II) στην οποία το δικαστήριο παραπέμπει ρητά «στο στάδιο εξέλιξης του δικαίου και τις πρακτικές που ισχύουν στην οικεία τρίτη χώρα» και ζητεί «(...) να εξασφαλίσουν, στην πράξη, την αποτελεσματική προστασία των δεδομένων προσωπικού χαρακτήρα που διαβιβάζονται στην οικεία τρίτη χώρα.» (προσθήκη έμφασης) και τη σκέψη 158.

νομοθεσίας, νομικών εξουσιών, τεχνικών, χρηματοοικονομικών και ανθρώπινων πόρων στη διάθεσή τους και βάσει του αναφερόμενου δικαστικού προηγούμενου.

Προσδιορισμός συναφών νόμων και πρακτικών υπό το πρίσμα όλων των συνθηκών της διαβίβασης

32. Θα πρέπει να εξετάσετε τα χαρακτηριστικά καθεμίας από τις διαβιβάσεις σας και να καθορίσετε αν η εσωτερική έννομη τάξη ή/και οι ισχύουσες πρακτικές της χώρας στην οποία διαβιβάζονται τα δεδομένα (ή διαβιβάζονται περαιτέρω) επηρεάζουν τις διαβιβάσεις σας. Επομένως, το πεδίο εφαρμογής της αξιολόγησής σας περιορίζεται στη νομοθεσία και τις πρακτικές που αφορούν την προστασία των συγκεκριμένων δεδομένων που διαβιβάζετε, σε αντίθεση με τις γενικές και ευρείες αξιολογήσεις επάρκειας που διενεργεί η Ευρωπαϊκή Επιτροπή σύμφωνα με το άρθρο 45 του ΓΚΠΔ.
33. Το ισχύον νομικό πλαίσιο ή/και οι πρακτικές θα εξαρτηθούν από τις ειδικές περιστάσεις της διαβίβασής σας, ιδίως:
- Τους σκοπούς για τους οποίους διαβιβάζονται και υποβάλλονται σε επεξεργασία τα δεδομένα (π.χ. μάρκετινγκ, ανθρώπινο δυναμικό, αποθήκευση, υποστήριξη ΤΠ, κλινικές δοκιμές).
 - Τους τύπους φορέων που εμπλέκονται στην επεξεργασία (δημόσιου/ιδιωτικού τομέα, υπεύθυνος επεξεργασίας/εκτελών την επεξεργασία).
 - Τον τομέα στον οποίο πραγματοποιείται η διαβίβαση (π.χ. τεχνολογία διαφήμισης, τηλεπικοινωνίες, χρηματοοικονομικά κ.λπ.).
 - Τις κατηγορίες δεδομένων προσωπικού χαρακτήρα που διαβιβάζονται (π.χ. δεδομένα προσωπικού χαρακτήρα που σχετίζονται με παιδιά ενδέχεται να εμπίπτουν στο πεδίο εφαρμογής ειδικής νομοθεσίας στην τρίτη χώρα)⁴².
 - Αν τα δεδομένα θα αποθηκευτούν στην τρίτη χώρα ή αν υπάρχει μόνο απομακρυσμένη πρόσβαση σε δεδομένα που είναι αποθηκευμένα εντός της ΕΕ/του ΕΟΧ.
 - Τη μορφή των προς διαβίβαση δεδομένων (δηλ. απλού κειμένου/κρυπτογραφημένα ή ψευδωνυμοποιημένα⁴³).
 - Την πιθανότητα τα δεδομένα να υπόκεινται σε περαιτέρω διαβίβαση από την τρίτη χώρα σε άλλη τρίτη χώρα.⁴⁴
34. Η αξιολόγησή σας θα πρέπει να λαμβάνει υπόψη όλους τους παράγοντες που εμπλέκονται στη διαβίβαση (π.χ. υπεύθυνους επεξεργασίας, εκτελούντες την επεξεργασία και υπεργολάβους

⁴² Η διαβίβαση δεδομένων προσωπικού χαρακτήρα είναι πράξη επεξεργασίας (άρθρο 4 παράγραφος 2 του ΓΚΠΔ). Εάν επιθυμείτε να διαβιβάσετε ευαίσθητα δεδομένα που εμπίπτουν στα άρθρα 9 και 10 του ΓΚΠΔ, μπορείτε να πραγματοποιήσετε τη διαβίβαση αυτή μόνο εάν εμπίπτει σε μία από τις παρεκκλίσεις και προϋποθέσεις που ορίζονται στα άρθρα 9 και 10 του ΓΚΠΔ και στο δίκαιο των κρατών μελών της ΕΕ. Σύμφωνα με το άρθρο 32 του ΓΚΠΔ, θα πρέπει επίσης να εφαρμόσετε, μαζί με τον εισαγωγέα που ενεργεί ως υπεύθυνος επεξεργασίας ή εκτελών την επεξεργασία, κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων που προκύπτουν από πιθανή παραβίαση των διαβιβαζόμενων δεδομένων προσωπικού χαρακτήρα (άρθρο 4 παράγραφος 12 του ΓΚΠΔ). Οι κατηγορίες των διαβιβαζόμενων δεδομένων και η ευαισθησία τους θα είναι χρήσιμες για την εκτίμηση του κινδύνου και της καταλληλότητας των μέτρων.

⁴³ Ορισμένες τρίτες χώρες δεν επιτρέπουν την εισαγωγή κρυπτογραφημένων δεδομένων.

⁴⁴ Όταν ο υπεύθυνος επεξεργασίας έχει χορηγήσει προηγουμένως ειδική ή γενική γραπτή εξουσιοδότηση σύμφωνα με το άρθρο 28.2 του ΓΚΠΔ.

επεξεργασίας που επεξεργάζονται δεδομένα στην τρίτη χώρα), όπως προσδιορίζεται στην χαρτογράφηση των διαβιβάσεων. Όσο περισσότεροι υπεύθυνοι επεξεργασίας, εκτελούντες την επεξεργασία ή εισαγωγείς συμμετέχουν, τόσο πιο περίπλοκη θα είναι η αξιολόγησή σας. Θα πρέπει επίσης να λάβετε υπόψη στην αξιολόγησή σας τυχόν προβλεπόμενη μεταγενέστερη διαβίβαση.

35. Σε κάθε περίπτωση θα πρέπει να δώσετε ιδιαίτερη προσοχή σε τυχόν σχετικούς νόμους, ιδίως σε νόμους που ορίζουν απαιτήσεις για την κοινοποίηση δεδομένων προσωπικού χαρακτήρα σε δημόσιες αρχές ή παρέχουν στις εν λόγω δημόσιες αρχές εξουσίες πρόσβασης σε δεδομένα προσωπικού χαρακτήρα (για παράδειγμα για σκοπούς επιβολής της ποινικής νομοθεσίας, κανονιστικής εποπτείας και εθνικής ασφάλειας). Εάν οι εν λόγω απαιτήσεις ή εξουσίες περιορίζουν τα θεμελιώδη δικαιώματα των υποκειμένων των δεδομένων ενώ παράλληλα σέβονται την ουσία τους και είναι αναγκαία και αναλογικά μέτρα σε μια δημοκρατική κοινωνία για τη διασφάλιση σημαντικών στόχων όπως επίσης αναγνωρίζονται στο ενωσιακό δίκαιο ή στο δίκαιο των κρατών μελών της ΕΕ,⁴⁵ ενδέχεται να μην επηρεάζουν τις δεσμεύσεις που περιέχονται στο εργαλείο διαβίβασης του άρθρου 46 του ΓΚΠΔ στο οποίο βασίζεστε.
36. Θα χρειαστεί να αξιολογήσετε συναφείς κανόνες και πρακτικές γενικού χαρακτήρα εφόσον έχουν αντίκτυπο στην αποτελεσματική εφαρμογή των εγγυήσεων που περιέχονται στο εργαλείο διαβίβασης του άρθρου 46 του ΓΚΠΔ.
37. Κατά τη διενέργεια της εν λόγω αξιολόγησης, είναι επίσης χρήσιμες διάφορες πτυχές του νομικού συστήματος της τρίτης χώρας, π.χ. τα στοιχεία που απαριθμούνται στο άρθρο 45 παράγραφος 2 του ΓΚΠΔ. Για παράδειγμα, η κατάσταση του κράτους δικαίου σε μια τρίτη χώρα μπορεί να είναι χρήσιμη για την αξιολόγηση της αποτελεσματικότητας των διαθέσιμων μηχανισμών για την παροχή (έννομης) προστασίας στα άτομα έναντι της παράνομης πρόσβασης εκ μέρους της κυβέρνησης σε δεδομένα προσωπικού χαρακτήρα. Η ύπαρξη ενός γενικού νόμου για την προστασία των δεδομένων ή μιας ανεξάρτητης αρχής προστασίας δεδομένων, καθώς και η τήρηση διεθνών μέσων που προβλέπουν εγγυήσεις προστασίας δεδομένων, μπορούν να συμβάλουν στη διασφάλιση της αναλογικότητας των κυβερνητικών παρεμβάσεων.
38. Οι υποχρεώσεις ή οι εξουσίες που απορρέουν από τους εν λόγω νόμους ή πρακτικές θα θεωρηθεί ότι θίγουν / είναι ασύμβατες με τις δεσμεύσεις που αναλαμβάνονται βάσει του εργαλείου διαβίβασης του άρθρου 46 του ΓΚΠΔ εάν⁴⁶:
 - δεν τηρούν την ουσία των θεμελιωδών δικαιωμάτων και ελευθεριών του Χάρτη Θεμελιωδών Δικαιωμάτων της ΕΕ ή
 - υπερβαίνουν τα απολύτως αναγκαία και αναλογικά σε μια δημοκρατική κοινωνία για τη διασφάλιση ενός από τους σημαντικούς στόχους όπως επίσης αναγνωρίζονται στο ενωσιακό

⁴⁵ Βλ. άρθρα 47 και 52 του Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ, άρθρο 23.1 του ΓΚΠΔ, και συστάσεις 02/2020 του ΕΣΠΔ σχετικά με τις ευρωπαϊκές βασικές εγγυήσεις για τα μέτρα παρακολούθησης, 10 Νοεμβρίου 2020, https://edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_el.pdf

⁴⁶ Βλ. άρθρα 47 και 52 του Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ, άρθρο 23.1 του ΓΚΠΔ, απόφαση C-311/18 (Schrems II), σκέψεις 174 και 187 και συστάσεις 02/2020 του ΕΣΠΔ σχετικά με τις ευρωπαϊκές βασικές εγγυήσεις για τα μέτρα παρακολούθησης, 10 Νοεμβρίου 2020.

δίκαιο ή στο δίκαιο των κρατών μελών, όπως αυτοί που απαριθμούνται στο άρθρο 23 παράγραφος 1 του ΓΚΠΔ.

39. Θα πρέπει να επαληθεύσετε αν οι δεσμεύσεις του εισαγωγέα δεδομένων που επιτρέπουν στα υποκείμενα των δεδομένων να ασκούν τα δικαιώματά τους, όπως προβλέπονται στο εργαλείο διαβίβασης του άρθρου 46 του ΓΚΠΔ [όπως αιτήματα πρόσβασης, διόρθωσης και διαγραφής για διαβιβαζόμενα δεδομένα καθώς και (έννομη) προστασία] μπορούν να εφαρμοστούν αποτελεσματικά στην πράξη και δεν παρακωλύονται από τη νομοθεσία ή/και τις πρακτικές στην τρίτη χώρα προορισμού.
40. Τα πρότυπα της ΕΕ, όπως τα άρθρα 47 και 52 του Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ, πρέπει να χρησιμοποιηθούν ως αναφορά, ιδίως για να αξιολογηθεί αν η πρόσβαση από τις δημόσιες αρχές περιορίζεται στα απολύτως αναγκαία και αναλογικά σε μια δημοκρατική κοινωνία και αν διασφαλίζεται αποτελεσματική επανόρθωση για τα υποκείμενα των δεδομένων.
41. Οι συστάσεις του ΕΣΠΔ για τις ευρωπαϊκές βασικές εγγυήσεις⁴⁷ παρέχουν διευκρινίσεις όσον αφορά τα στοιχεία που πρέπει να αξιολογηθούν για να προσδιοριστεί αν το νομικό πλαίσιο που διέπει την πρόσβαση σε δεδομένα προσωπικού χαρακτήρα από τις δημόσιες αρχές τρίτης χώρας, ως υπηρεσίες εθνικής ασφάλειας ή αρχές επιβολής του νόμου, μπορεί να θεωρηθεί ως δικαιολογημένη ή μη δικαιολογημένη παρέμβαση⁴⁸. Ειδικότερα, αυτό θα πρέπει να εξετάζεται προσεκτικά όταν η νομοθεσία που διέπει την πρόσβαση δημόσιων αρχών σε δεδομένα είναι διφορούμενη ή δεν είναι δημοσίως διαθέσιμη. Η πρώτη απαίτηση των ευρωπαϊκών βασικών εγγυήσεων είναι ότι θα πρέπει να υπάρχει νομικό πλαίσιο που να ορίζει ότι η εν λόγω πρόσβαση, όταν προβλέπεται, είναι δημοσίως διαθέσιμη και επαρκώς σαφής.
42. Οι συστάσεις του ΕΣΠΔ για τις ευρωπαϊκές βασικές εγγυήσεις, εάν εφαρμοστούν στην κατάσταση των διαβιβάσεων δεδομένων βάσει των εργαλείων διαβίβασης του άρθρου 46, μπορούν να βοηθήσουν τον εξαγωγέα δεδομένων να αξιολογήσει αν οι εν λόγω εξουσίες παρεμβαίνουν αδικαιολόγητα στις υποχρεώσεις του εξαγωγέα και του εισαγωγέα δεδομένων να διασφαλίσουν ουσιώδη ισοδυναμία σύμφωνα με τον ΓΚΠΔ ή στις δεσμεύσεις που περιέχονται στο εργαλείο διαβίβασης. Η έλλειψη ενός ουσιαστικά ισοδύναμου επιπέδου προστασίας θα είναι ιδιαίτερα εμφανής όταν η νομοθεσία ή/και οι πρακτικές της τρίτης χώρας που σχετίζονται με τη διαβίβασή σας δεν πληρούν τις απαιτήσεις των ευρωπαϊκών βασικών εγγυήσεων. Το ΕΣΠΔ επαναλαμβάνει ότι οι ευρωπαϊκές βασικές εγγυήσεις συνιστούν ένα πρότυπο αναφοράς για την αξιολόγηση της παρέμβασης, την οποία συνεπάγονται τα μέτρα παρακολούθησης μιας τρίτης χώρας, στο πλαίσιο των διεθνών διαβιβάσεων δεδομένων. Τα παρόντα πρότυπα απορρέουν από το δίκαιο της ΕΕ και τη νομολογία του ΔΕΕ και του ΕΔΔΑ, που έχει δεσμευτική ισχύ για τα κράτη μέλη της ΕΕ.
43. Η αξιολόγησή σας πρέπει να βασίζεται πρωτίστως στη νομοθεσία που είναι δημόσια διαθέσιμη. Επίσης, η εξέταση των πρακτικών που εφαρμόζουν οι δημόσιες αρχές της τρίτης χώρας θα σας δώσει τη δυνατότητα να επαληθεύσετε αν οι εγγυήσεις που περιλαμβάνονται στο εργαλείο διαβίβασης του άρθρου 46 του ΓΚΠΔ μπορούν να αποτελέσουν επαρκές μέσο που θα

⁴⁷ Συστάσεις 02/2020 σχετικά με τις Ευρωπαϊκές Βασικές Εγγυήσεις για τα μέτρα παρακολούθησης, 10 Νοεμβρίου 2020

⁴⁸ Και ότι συνεπώς δεν θίγουν τις δεσμεύσεις που αναλαμβάνονται βάσει του εργαλείου διαβίβασης του άρθρου 46 του ΓΚΠΔ.

διασφαλίσει στην πράξη την αποτελεσματική προστασία των δεδομένων προσωπικού χαρακτήρα που διαβιβάζονται.⁴⁹ Η εξέταση των πρακτικών που ισχύουν στην τρίτη χώρα θα έχει ιδιαίτερη σημασία για την αξιολόγησή σας στις καταστάσεις που περιγράφονται παρακάτω.

43.1 Η σχετική νομοθεσία στην τρίτη χώρα μπορεί να πληροί επισήμως τα πρότυπα της ΕΕ για τα θεμελιώδη δικαιώματα και τις ελευθερίες καθώς και την αναγκαιότητα και την αναλογικότητα των περιορισμών. Ωστόσο, οι πρακτικές των δημόσιων αρχών της (π.χ. η πρόσβαση σε δεδομένα προσωπικού χαρακτήρα που τηρούνται από τον ιδιωτικό τομέα ή κατά την επιβολή ή μη επιβολή νομοθεσίας ως εποπτικοί ή δικαστικοί φορείς) μπορεί να υποδηλώνει με σαφήνεια ότι συνήθως δεν εφαρμόζουν/συμμορφώνονται με τη νομοθεσία που διέπει, επί της αρχής, τις δραστηριότητές τους. Σε αυτή την περίπτωση, στην αξιολόγησή σας πρέπει να λάβετε υπόψη αυτές τις πρακτικές και να θεωρήσετε ότι το εργαλείο του άρθρου 46 του ΓΚΠΔ δεν θα είναι ικανό να διασφαλίσει με αποτελεσματικό τρόπο από μόνο του (δηλαδή χωρίς πρόσθετα μέτρα) ένα ουσιαστικά ισοδύναμο επίπεδο προστασίας. Σε παρόμοια περίπτωση, εάν επιθυμείτε να προβείτε στη διαβίβαση, θα πρέπει να εφαρμόσετε επαρκή πρόσθετα μέτρα.

43.2 Η σχετική νομοθεσία στην τρίτη χώρα (π.χ. σχετικά με την πρόσβαση σε δεδομένα προσωπικού χαρακτήρα που τηρεί ο ιδιωτικός τομέας) μπορεί να μην υπάρχει. Σε αυτή την περίπτωση δεν μπορείτε να συμπεράνετε αυτόματα από την εν λόγω απουσία σχετικής νομοθεσίας ότι το οικείο εργαλείο διαβίβασης του άρθρου 46 του ΓΚΠΔ μπορεί να εφαρμοστεί αποτελεσματικά. Θα πρέπει να ελέγξετε αν υπάρχουν ενδείξεις ότι στη χώρα ισχύουν πρακτικές ασύμβατες με το ενωσιακό δίκαιο και τις δεσμεύσεις που αναλαμβάνονται βάσει του εργαλείου διαβίβασης του άρθρου 46 του ΓΚΠΔ. Εάν υπάρχουν ασύμβατες πρακτικές, το εργαλείο διαβίβασης του άρθρου 46 του ΓΚΠΔ δεν θα είναι σε θέση να διασφαλίσει με αποτελεσματικό τρόπο από μόνο του (δηλαδή χωρίς πρόσθετα μέτρα) ένα ουσιαστικά ισοδύναμο επίπεδο προστασίας. Σε παρόμοια περίπτωση, εάν επιθυμείτε να προβείτε στη διαβίβαση, θα πρέπει να εφαρμόσετε επαρκή πρόσθετα μέτρα.

43.3 Η αξιολόγηση μπορεί να αποκαλύψει ότι η σχετική νομοθεσία στην τρίτη χώρα μπορεί να είναι προβληματική⁵⁰ και ότι τα διαβιβαζόμενα δεδομένα ή/και ο εκάστοτε εισαγωγέας εμπίπτουν ή ενδέχεται να εμπίπτουν στο πεδίο εφαρμογής της εν λόγω προβληματικής νομοθεσίας.⁵¹

⁴⁹ C-311/18 (Schrems II), σκέψη 126.

⁵⁰ Ως «προβληματική νομοθεσία» νοείται η νομοθεσία που 1) επιβάλλει υποχρεώσεις στον αποδέκτη δεδομένων προσωπικού χαρακτήρα από την Ευρωπαϊκή Ένωση ή/και επηρεάζει τα διαβιβαζόμενα δεδομένα με τρόπο που μπορεί να θίξει τη συμβατική εγγύηση ουσιαστικά ισοδύναμου επιπέδου προστασίας που παρέχουν τα εργαλεία διαβίβασης και 2) δεν τηρεί την ουσία των θεμελιωδών δικαιωμάτων και ελευθεριών που αναγνωρίζονται στον Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης ή υπερβαίνει τα απολύτως αναγκαία και αναλογικά σε μια δημοκρατική κοινωνία για τη διασφάλιση ενός από τους σημαντικούς στόχους όπως επίσης αναγνωρίζονται στο ενωσιακό δίκαιο ή στο δίκαιο των κρατών μελών, όπως αυτοί που απαριθμούνται στο άρθρο 23 παράγραφος 1 του ΓΚΠΔ.

⁵¹ Μπορεί να είναι ασαφές αν ο εισαγωγέας ή/και τα διαβιβαζόμενα δεδομένα εμπίπτουν στο πεδίο εφαρμογής των γενικών όρων που χρησιμοποιούνται συχνά στη νομοθεσία περί εθνικής ασφάλειας για τον περιορισμό του πεδίου εφαρμογής τους, όπως για παράδειγμα «πάροχος υπηρεσίας ηλεκτρονικών επικοινωνιών» και «αλλοδαπή υπηρεσία πληροφοριών».

Δεδομένων των αβεβαιοτήτων που σχετίζονται με τη δυνητική εφαρμογή προβληματικής νομοθεσίας στη διαβίβασή σας, μπορείτε να αποφασίσετε:

- να αναστείλετε τη διαβίβαση·
- να εφαρμόσετε πρόσθετα μέτρα⁵² για να αποτρέψετε τον κίνδυνο να εφαρμοστούν δυνητικά στον εισαγωγέα σας ή/και στα διαβιβαζόμενα δεδομένα σας οι νόμοι ή/και οι πρακτικές της τρίτης χώρας του εισαγωγέα δεδομένων, που είναι σε θέση να επηρεάσουν τις συμβατικές εγγυήσεις που παρέχει το εργαλείο διαβίβασης για ένα ουσιαστικά ισοδύναμο επίπεδο προστασίας με αυτό που διασφαλίζεται εντός στον ΕΟΧ· ή
- εναλλακτικά, μπορεί να αποφασίσετε να προβείτε στη διαβίβαση χωρίς να κληθείτε να εφαρμόσετε πρόσθετα μέτρα, εάν θεωρείτε ότι δεν έχετε λόγο να πιστεύετε πως, στην πράξη, θα ισχύσει συναφής και προβληματική νομοθεσία για τα διαβιβαζόμενα δεδομένα σας ή/και τον εισαγωγέα. Θα χρειαστεί να έχετε καταδείξει και να έχετε τεκμηριώσει μέσω της αξιολόγησής σας, κατά περίπτωση και σε συνεργασία με τον εισαγωγέα, ότι η νομοθεσία δεν ερμηνεύεται ή/και δεν εφαρμόζεται στην πράξη έτσι ώστε να καλύπτει τα διαβιβαζόμενα δεδομένα σας και τον εισαγωγέα, λαμβάνοντας επίσης υπόψη την εμπειρία άλλων παραγόντων που δραστηριοποιούνται στον ίδιο τομέα ή/και συνδέονται με παρόμοια διαβιβασθέντα δεδομένα προσωπικού χαρακτήρα και τις πρόσθετες πηγές πληροφόρησης που περιγράφονται στη συνέχεια.⁵³

Επομένως, θα πρέπει να έχετε καταδείξει και να έχετε τεκμηριώσει με λεπτομερή αναφορά⁵⁴ ότι η προβληματική νομοθεσία δεν θα ισχύσει στην πράξη για τα διαβιβαζόμενα δεδομένα σας ή/και τον εισαγωγέα και, συνεπώς, ότι δεν θα εμποδίσει τον εισαγωγέα να εκπληρώσει τις υποχρεώσεις του σύμφωνα με το εργαλείο διαβίβασης του άρθρου 46 του ΓΚΠΔ.⁵⁵

⁵² Βλ. αιτιολογική σκέψη 109 του ΓΚΠΔ και C-311/18 (Schrems II), σκέψη 132.

⁵³ Βλ. σκέψεις 45 έως 47.

⁵⁴ Οι εκθέσεις που θα καταρτίσετε θα πρέπει να περιλαμβάνουν διεξοδικές πληροφορίες για τη νομική αξιολόγηση της νομοθεσίας και των πρακτικών, καθώς και την εφαρμογή τους στις συγκεκριμένες διαβιβάσεις, την εσωτερική διαδικασία για την εκπόνηση της αξιολόγησης (συμπεριλαμβανομένων πληροφοριών για τους παράγοντες που συμμετέχουν στην αξιολόγηση, π.χ. δικηγορικές εταιρείες, συμβούλους ή εσωτερικές υπηρεσίες) και τις ημερομηνίες των ελέγχων. Οι εκθέσεις θα πρέπει να επικυρώνονται από τον νόμιμο εκπρόσωπο του εξαγωγέα.

⁵⁵ Ακόμα και αν καταδείξετε ότι η προβληματική νομοθεσία δεν ισχύει στην πράξη για τα οικεία διαβιβαζόμενα δεδομένα και τον εισαγωγέα, λαμβάνοντας επίσης υπόψη την εμπειρία άλλων παραγόντων που δραστηριοποιούνται στον ίδιο τομέα ή/και συνδέονται με παρόμοια διαβιβασθέντα δεδομένα προσωπικού χαρακτήρα, αυτό δεν σας απαλλάσσει από την υποχρέωση να προβλέψετε τα αναγκαία πρόσθετα μέτρα για την προστασία των δεδομένων προσωπικού χαρακτήρα κατά τη διαβίβαση και την επεξεργασία τους στην τρίτη χώρα προορισμού (π.χ. διατεμαχική κρυπτογράφηση δεδομένων – βλ. παραδείγματα τεχνικών πρόσθετων μέτρων στο παράρτημα 2) εάν κατόπιν ανάλυσης της ισχύουσας νομοθεσίας της τρίτης χώρας προορισμού προκύψει ότι μπορεί επίσης να υπάρξει πρόσβαση στα δεδομένα, ακόμα και χωρίς παρέμβαση του εισαγωγέα, κατά τη διαβίβαση. Ενδεχομένως μπορεί να έχετε ήδη προβλέψει αυτά τα μέτρα με τον εισαγωγέα να ενεργεί ως υπεύθυνος επεξεργασίας ή εκτελών την επεξεργασία σύμφωνα με το άρθρο 32 του ΓΚΠΔ.

Πιθανές πηγές πληροφοριών

44. Ο οικείος εισαγωγέας δεδομένων θα πρέπει να σας παρέχει τις σχετικές πηγές και πληροφορίες σχετικά με την τρίτη χώρα στην οποία είναι εγκατεστημένος, καθώς και τους νόμους και τις πρακτικές που ισχύουν για τη διαβίβαση.
45. Εσείς και ο εισαγωγέας σας μπορείτε να συμπληρώσετε την αξιολόγησή σας με πληροφορίες που θα αποκτήσετε από διάφορες πηγές, όπως αυτές που απαριθμούνται ως παραδείγματα στο παράρτημα 3.
46. Παράλληλα με το νομικό πλαίσιο της τρίτης χώρας που ισχύει για τη διαβίβαση, οι πηγές και οι πληροφορίες πρέπει να είναι συναφείς, αντικειμενικές, αξιόπιστες, επαληθεύσιμες και δημοσίως διαθέσιμες ή άλλως προσβάσιμες για να μπορεί να προσδιοριστεί αν το οικείο εργαλείο διαβίβασης του άρθρου 46 μπορεί να εφαρμοστεί αποτελεσματικά⁵⁶ και θα πρέπει να αξιολογήσετε και να επαληθεύσετε ότι όντως είναι.

Συναφείς: οι πληροφορίες πρέπει να είναι σαφείς με τη συγκεκριμένη διαβίβαση ή/και τον εισαγωγέα και τη συμμόρφωσή του με τις απαιτήσεις που τίθενται στο ενωσιακό δίκαιο και το μέσο διαβίβασης του άρθρου 46 του ΓΚΠΔ και όχι υπερβολικά γενικές ή αφηρημένες.

Αντικειμενικές πληροφορίες: οι πληροφορίες που υποστηρίζονται από εμπειρικά στοιχεία με βάση γνώσεις που έχουν αποκτηθεί στο παρελθόν, όχι παραδοχές για πιθανά γεγονότα και κινδύνους.

Αξιόπιστες: ο εξαγωγέας και ο εισαγωγέας πρέπει να εκτιμούν αντικειμενικά την αξιοπιστία της πηγής πληροφοριών και των ίδιων των πληροφοριών, και να τις αξιολογούν χωριστά.

Επαληθεύσιμες: οι πληροφορίες και τα συμπεράσματα θα πρέπει να είναι επαληθεύσιμα ή να μπορούν να αντιπαραβληθούν με άλλα είδη πληροφοριών ή πηγών, στο πλαίσιο γενικής αξιολόγησης, επίσης για να μπορεί η αρμόδια εποπτική ή δικαστική αρχή να ελέγξει την αντικειμενικότητα και την αξιοπιστία αυτών των πληροφοριών, εάν χρειαστεί.

Δημοσίως διαθέσιμες ή άλλως προσβάσιμες πληροφορίες: οι πληροφορίες θα πρέπει κατά προτίμηση να είναι δημοσιοποιημένες ή τουλάχιστον προσβάσιμες ώστε να διευκολύνεται η επαλήθευση των κριτηρίων που διατυπώθηκαν παραπάνω και να διασφαλίζεται η πιθανή κοινολόγησή τους στις εποπτικές αρχές, τις δικαστικές αρχές και, τελικά, τα υποκείμενα των δεδομένων.

47. Επίσης, μπορείτε να λάβετε υπόψη την τεκμηριωμένη πρακτική εμπειρία του εισαγωγέα σε συναφείς παλαιότερες περιστάσεις υποβολής αιτημάτων για πρόσβαση από τις δημόσιες αρχές της τρίτης χώρας. Θα μπορείτε να χρησιμοποιήσετε την εμπειρία του εισαγωγέα μόνον ως συμπληρωματική πηγή πληροφόρησης εάν το νομικό πλαίσιο της τρίτης χώρας δεν απαγορεύει στον εισαγωγέα την παροχή πληροφοριών σχετικά με αιτήματα κοινολόγησης από δημόσιες αρχές ή με τη μη ύπαρξη τέτοιων αιτημάτων (και θα πρέπει να τεκμηριώσετε και την εν λόγω αξιολόγηση). Ωστόσο, επισημαίνεται ότι η απουσία προηγούμενων αιτημάτων που να έχει λάβει ο εισαγωγέας δεν μπορεί ποτέ να θεωρηθεί, από μόνη της, καθοριστικός παράγοντας για την αποτελεσματικότητα του εργαλείου διαβίβασης του άρθρου 46 του ΓΚΠΔ που επιτρέπει την

⁵⁶ Βλ. παράρτημα 3 για μη διεξοδικό κατάλογο πηγών πληροφοριών που μπορείτε να χρησιμοποιείτε εσείς και ο εισαγωγέας.

υλοποίηση της διαβίβασης χωρίς πρόσθετα μέτρα. Θα μπορείτε να εξετάσετε τις εν λόγω πληροφορίες, μαζί με άλλα είδη πληροφοριών που αποκτώνται από άλλες πηγές, στο πλαίσιο της συνολικής αξιολόγησης των νόμων και πρακτικών της τρίτης χώρας σε σχέση με τη διαβίβασή σας. Η σχετική και τεκμηριωμένη εμπειρία του εισαγωγέα θα πρέπει να επιβεβαιώνεται και να μην αντικρούεται από συναφείς, αντικειμενικές, αξιόπιστες, επαληθεύσιμες και δημοσίως διαθέσιμες ή άλλως προσβάσιμες πληροφορίες σε σχέση με την πρακτική εφαρμογή του σχετικού δικαίου (π.χ. την ύπαρξη ή την απουσία αιτημάτων πρόσβασης που να έχουν ληφθεί από άλλους παράγοντες που δραστηριοποιούνται στον ίδιο τομέα ή/και σχετίζονται με παρόμοια διαβιβασθέντα δεδομένα προσωπικού χαρακτήρα⁵⁷ ή/και την εφαρμογή του δικαίου στην πράξη, όπως η νομολογία και οι εκθέσεις ανεξάρτητων φορέων εποπτείας).

Αποτελέσματα της αξιολόγησής σας

48. Θα πρέπει να διεξαγάγετε αυτή τη συνολική αξιολόγηση του δικαίου και της πρακτικής που ισχύουν στην τρίτη χώρα του εισαγωγέα σας για τη διαβίβασή σας με δέουσα επιμέλεια και να την τεκμηριώσετε εμπεριστατωμένα. Οι αρμόδιες εποπτικές ή/και δικαστικές αρχές σας ενδέχεται να τη ζητήσουν και να σας θεωρήσουν υπεύθυνους για κάθε απόφαση που θα λάβετε επί αυτής της βάσης.⁵⁸
49. Η αξιολόγησή σας μπορεί τελικά να αποκαλύψει ότι το εργαλείο διαβίβασης του άρθρου 46 του ΓΚΠΔ στο οποίο βασίζεστε:
- διασφαλίζει αποτελεσματικά ότι τα διαβιβαζόμενα δεδομένα προσωπικού χαρακτήρα τυγχάνουν ενός επιπέδου προστασίας στην τρίτη χώρα που είναι ουσιαστικά ισοδύναμο με εκείνο που διασφαλίζεται εντός του ΕΟΧ. Η νομοθεσία και οι πρακτικές της τρίτης χώρας που ισχύουν για τη διαβίβαση επιτρέπουν στον εισαγωγέα δεδομένων να συμμορφωθεί με τις υποχρεώσεις του βάσει του επιλεγμένου εργαλείου διαβίβασης. Θα πρέπει να προβαίνετε σε εκ νέου αξιολόγηση σε τακτά χρονικά διαστήματα ή όταν προκύπτουν σημαντικές αλλαγές (βλ. βήμα 6) ή
 - δεν εξασφαλίζει αποτελεσματικά ένα ουσιαστικά ισοδύναμο επίπεδο προστασίας. Ο εισαγωγέας δεδομένων δεν μπορεί να συμμορφωθεί με τις υποχρεώσεις του, λόγω της νομοθεσίας ή/και των πρακτικών που ισχύουν στην τρίτη χώρα για τη διαβίβαση και δεν πληρούν τα πρότυπα της ΕΕ για τα θεμελιώδη δικαιώματα και τις ελευθερίες, καθώς και την αναγκαιότητα και αναλογικότητα των περιορισμών για τη διασφάλιση νόμιμων στόχων δημόσιου συμφέροντος. Το ΔΕΕ υπογράμμισε ότι όταν τα εργαλεία διαβίβασης του άρθρου 46 του ΓΚΠΔ δεν επαρκούν, αποτελεί ευθύνη του εξαγωγέα δεδομένων είτε να εφαρμόσει αποτελεσματικά πρόσθετα μέτρα είτε να μην διαβιβάσει δεδομένα προσωπικού χαρακτήρα.⁵⁹

⁵⁷ Η εμπειρία θα μπορούσε να είναι η εμπειρία άλλων οντοτήτων, της οποίας έχετε άμεση γνώση λόγω παλαιότερων διαβιβάσεων του ίδιου είδους που έχετε υλοποιήσει ή που αναφέρεται σε σχετική νομολογία, εκθέσεις ΜΚΟ κ.λπ. (βλ. παράρτημα 3).

⁵⁸ Άρθρο 5 παράγραφος 2 του ΓΚΠΔ.

⁵⁹ ΔΕΕ C-311/18 (Schrems II), σκέψεις 134 και 135.

Παράδειγμα:

Ιστορικό:

Το ΔΕΕ έκρινε, για παράδειγμα, ότι το τμήμα 702 του νόμου των ΗΠΑ περί παρακολούθησης επικοινωνιών αλλοδαπών υπηρεσιών πληροφοριών (Foreign Intelligence Surveillance Act – FISA) δεν τηρεί τις ελάχιστες εγγυήσεις που απορρέουν από την αρχή της αναλογικότητας βάσει του δικαίου της ΕΕ και δεν μπορεί να θεωρηθεί ότι περιορίζεται στα απολύτως αναγκαία. Αυτό σημαίνει ότι το επίπεδο προστασίας των προγραμμάτων που εγκρίνονται από το τμήμα 702 του FISA δεν είναι ουσιαστικά ισοδύναμο με τις εγγυήσεις που απαιτούνται από το δίκαιο της ΕΕ.

Αξιολόγηση:

Εάν μετά την αξιολόγηση της σχετικής νομοθεσίας των ΗΠΑ καταλήξετε στο συμπέρασμα ότι η διαβίβασή σας ενδέχεται να εμπίπτει στο πεδίο εφαρμογής του τμήματος 702 του FISA αλλά δεν είστε σίγουροι αν εμπίπτει στο πρακτικό πεδίο εφαρμογής του, θα μπορούσατε να αποφασίσετε:

1. να σταματήσετε τη διαβίβαση;
2. να εγκρίνετε κατάλληλα πρόσθετα μέτρα που διασφαλίζουν με αποτελεσματικό τρόπο ένα επίπεδο προστασίας των διαβιβαζόμενων δεδομένων ουσιαστικά ισοδύναμο με το επίπεδο που είναι εγγυημένο στον ΕΟΧ; ή
3. να εξετάσετε άλλες αντικειμενικές, αξιόπιστες, συναφείς, επαληθεύσιμες και, κατά προτίμηση, δημοσίως διαθέσιμες πληροφορίες (οι οποίες μπορεί να περιλαμβάνουν πληροφορίες που σας παρέχει ο οικείος εισαγωγέας δεδομένων) για να αποσαφηνίσετε το πεδίο εφαρμογής που ισχύει στην πράξη βάσει του τμήματος 702 του FISA για τη συγκεκριμένη διαβίβασή σας. Αυτές οι πληροφορίες θα πρέπει να παρέχουν τις απαντήσεις σε ορισμένες σχετικές ερωτήσεις, όπως οι ακόλουθες:

- Οι δημοσίως διαθέσιμες πληροφορίες δείχνουν ότι υπάρχει νομική απαγόρευση ενημέρωσης σχετικά με συγκεκριμένο παραληφθέν αίτημα πρόσβασης σε δεδομένα και εκτεταμένοι περιορισμοί στην παροχή γενικών πληροφοριών για τα ληφθέντα αιτήματα πρόσβασης σε δεδομένα ή για την απουσία ληφθέντων αιτημάτων;

- Ο οικείος εισαγωγέας δεδομένων έχει επιβεβαιώσει ότι έχει λάβει αιτήματα για την παροχή πρόσβασης σε δεδομένα από δημόσιες αρχές των ΗΠΑ στο παρελθόν; Ή έχει επιβεβαιώσει ο οικείος εισαγωγέας δεδομένων ότι δεν έχει λάβει αιτήματα για την παροχή πρόσβασης σε δεδομένα από δημόσιες αρχές των ΗΠΑ στο παρελθόν και ότι δεν απαγορεύεται η παροχή πληροφοριών σε σχέση με τα εν λόγω αιτήματα ή την απουσία τους;

- Μήπως οι δημοσίως διαθέσιμες πληροφορίες που αποκτήσατε από τη νομολογία των ΗΠΑ και τις εκθέσεις φορέων εποπτείας, οργανώσεων της κοινωνίας των πολιτών και ακαδημαϊκών ιδρυμάτων⁶⁰ αποκαλύπτουν ότι εισαγωγείς δεδομένων του ίδιου τομέα με τον εισαγωγέα σας έχουν λάβει στο

⁶⁰ Π.χ. διατάξεις του τμήματος 702 του FISA· εσωτερικός κανονισμός του δικαστηρίου δυνάμει του νόμου περί παρακολούθησης επικοινωνιών αλλοδαπών υπηρεσιών πληροφοριών (FISC), αποχαρακτηρισμένες γνωμοδοτήσεις και αποφάσεις του FISC, νομολογία των δικαστηρίων των ΗΠΑ· εκθέσεις και πρακτικά ακροαματικών διαδικασιών της Επιτροπής Εποπτείας της Ιδιωτικής Ζωής και των Ατομικών Ελευθεριών (PCLOB)· εκθέσεις από το Γραφείο του Γενικού Επιθεωρητή – Υπουργείο Δικαιοσύνης των ΗΠΑ· εκθέσεις από τον Διευθυντή του Γραφείου Ατομικών Ελευθεριών και Ιδιωτικής Ζωής της Εθνικής Υπηρεσίας Ασφαλείας (NSA)· εκθέσεις που έχουν καταρτιστεί από την Υπηρεσία Ερευνών του Κογκρέσου· εκθέσεις από την Αμερικανική Ένωση Ατομικών Ελευθεριών (ACLU).

παρελθόν αιτήματα για την παροχή πρόσβασης σε δεδομένα σε σχέση με παρόμοια διαβιβασθέντα δεδομένα;

Οι απαντήσεις σε αυτές τις ερωτήσεις, τις οποίες αποκτάτε μέσω της συνολικής αξιολόγησης που διενεργείτε, σας οδηγούν στο συμπέρασμα ότι:

- Το τμήμα 702 του FISA ισχύει στην πράξη για τη δική σας συγκεκριμένη διαβίβαση και, συνεπώς, επηρεάζει την αποτελεσματικότητα του εργαλείου διαβίβασης του άρθρου 46 του ΓΚΠΔ. Κατά συνέπεια, εάν επιθυμείτε να προβείτε στη διαβίβαση, πρέπει να συνεκτιμήσετε, κατά περίπτωση σε συνεργασία με τον εισαγωγέα, εάν μπορείτε να θεσπίσετε πρόσθετα μέτρα που διασφαλίζουν με αποτελεσματικό τρόπο ένα επίπεδο προστασίας των διαβιβαζόμενων δεδομένων ουσιαστικά ισοδύναμο με το επίπεδο που είναι εγγυημένο στον ΕΟΧ. Εάν δεν μπορείτε να προσδιορίσετε αποτελεσματικά πρόσθετα μέτρα, δεν πρέπει να διαβιβάσετε τα δεδομένα προσωπικού χαρακτήρα.
ή

- Το τμήμα 702 του FISA δεν ισχύει στην πράξη για τη δική σας συγκεκριμένη διαβίβαση και, συνεπώς, δεν επηρεάζει την αποτελεσματικότητα του εργαλείου διαβίβασης του άρθρου 46 του ΓΚΠΔ. Επομένως, μπορείτε να προχωρήσετε στη διαβίβαση χωρίς κανένα πρόσθετο μέτρο.

2.4 Βήμα 4: Εφαρμογή πρόσθετων μέτρων

50. Εάν η αξιολόγησή σας στο Βήμα 3 αποκαλύψει ότι το εργαλείο διαβίβασης του άρθρου 46 του ΓΚΠΔ δεν είναι αποτελεσματικό, τότε θα πρέπει να εξετάσετε, κατά περίπτωση και σε συνεργασία με τον εισαγωγέα, εάν υπάρχουν πρόσθετα μέτρα, τα οποία, όταν προστίθενται στις εγγυήσεις που περιέχονται στα εργαλεία διαβίβασης, θα μπορούσαν να διασφαλίσουν ότι τα δεδομένα που διαβιβάζονται τυγχάνουν ενός επιπέδου προστασίας στην τρίτη χώρα το οποίο είναι ουσιαστικά ισοδύναμο με αυτό που διασφαλίζεται στο εσωτερικό της ΕΕ.⁶¹ Τα «πρόσθετα μέτρα» εξ ορισμού συμπληρώνουν τις εγγυήσεις που ήδη παρέχει το εργαλείο διαβίβασης του άρθρου 46 του ΓΚΠΔ και κάθε άλλη ισχύουσα απαίτηση ασφάλειας (π.χ. τεχνικά μέτρα ασφάλειας) την οποία καθιερώνει ο ΓΚΠΔ.⁶²

51. Πρέπει να προσδιορίσετε κατά περίπτωση ποια πρόσθετα μέτρα θα μπορούσαν να είναι αποτελεσματικά για ένα σύνολο διαβιβάσεων σε συγκεκριμένη τρίτη χώρα όταν χρησιμοποιείτε συγκεκριμένο εργαλείο διαβίβασης του άρθρου 46 του ΓΚΠΔ. Δεν είναι απαραίτητο να επαναλαμβάνετε την αξιολόγηση κάθε φορά που πραγματοποιείτε την ίδια διαβίβαση συγκεκριμένου είδους δεδομένων στην ίδια τρίτη χώρα. Ορισμένα από τα δεδομένα που έχει προγραμματιστεί να διαβιβαστούν ενδέχεται να χρειάζονται πρόσθετα μέτρα ενώ άλλα δεδομένα μπορεί να μη χρειάζονται (λαμβανομένης υπόψη της επίσημης ή/και πρακτικής εφαρμογής του δικαίου της τρίτης χώρας). Θα είστε σε θέση να αξιοποιήσετε τις προηγούμενες αξιολογήσεις και τα συμπεράσματά σας στο πλαίσιο των βημάτων 1, 2 και 3 ανωτέρω και να ελέγξετε βάσει των ευρημάτων τους την πιθανή αποτελεσματικότητα των πρόσθετων μέτρων στη διασφάλιση του απαιτούμενου επιπέδου προστασίας.

⁶¹ C-311/18 (Schrems II), σκέψη 96.

⁶² Αιτιολογική σκέψη 109 του ΓΚΠΔ και C-311/18 (Schrems II), σκέψη 133.

52. Κατ' αρχήν, τα πρόσθετα μέτρα μπορεί να έχουν συμβατικό, τεχνικό ή οργανωτικό χαρακτήρα. Ο συνδυασμός διαφορετικών μέτρων κατά τρόπο που να υποστηρίζονται αμοιβαία και να αλληλοεξαρτώνται μπορεί να ενισχύσει το επίπεδο προστασίας και, ως εκ τούτου, να συμβάλει στην επίτευξη των προτύπων της ΕΕ.
53. Τα συμβατικά και οργανωτικά μέτρα μόνα τους δεν μπορούν γενικά να αποφύγουν την πρόσβαση σε δεδομένα προσωπικού χαρακτήρα από τις δημόσιες αρχές της τρίτης χώρας βάσει προβληματικής νομοθεσίας ή/και πρακτικών.⁶³ Πράγματι, θα υπάρξουν περιπτώσεις όπου μόνο κατάλληλα εφαρμοσμένα τεχνικά μέτρα θα μπορούσαν να παρεμποδίσουν ή να καταστήσουν αναποτελεσματική την πρόσβαση δημόσιων αρχών τρίτων χωρών σε δεδομένα προσωπικού χαρακτήρα, ιδίως για σκοπούς παρακολούθησης.⁶⁴ Σε αυτές τις περιπτώσεις, συμβατικά ή οργανωτικά μέτρα μπορεί να συμπληρώνουν τα τεχνικά μέτρα και να ενισχύουν το συνολικό επίπεδο προστασίας των δεδομένων (π.χ. θεσπίζοντας ελέγχους και καταργώντας τους αυτοματισμούς στις προσπάθειες των δημόσιων αρχών να αποκτήσουν πρόσβαση σε δεδομένα με τρόπο που δεν συμμορφώνεται με τα πρότυπα της ΕΕ).
54. Μπορείτε, σε συνεργασία με τον εισαγωγέα δεδομένων, κατά περίπτωση, να συμβουλευτείτε τον ακόλουθο (μη εξαντλητικό) κατάλογο παραγόντων για να προσδιορίσετε ποια πρόσθετα μέτρα θα ήταν πιο αποτελεσματικά για την προστασία των δεδομένων που διαβιβάζονται βάσει αιτημάτων δημόσιων αρχών για πρόσβαση σε δεδομένα με βάση προβληματική νομοθεσία που εφαρμόζεται στην πράξη:
- τη μορφή των προς διαβίβαση δεδομένων (δηλ. απλού κειμένου/κρυπτογραφημένα ή ψευδωνυμοποιημένα).
 - τη φύση των δεδομένων (π.χ. στον ΕΟΧ παρέχεται υψηλότερο επίπεδο προστασίας για τις κατηγορίες δεδομένων που καλύπτονται από τα άρθρα 9 και 10 του ΓΚΠΔ).⁶⁵
 - το μήκος και την πολυπλοκότητα της ροής εργασιών επεξεργασίας δεδομένων, τον αριθμό των παραγόντων που συμμετέχουν στην επεξεργασία και τη σχέση μεταξύ τους (π.χ. οι διαβιβάσεις αφορούν πολλούς υπεύθυνους επεξεργασίας ή υπεύθυνους επεξεργασίας και εκτελούντες την επεξεργασία, ή συμμετοχή εκτελούντων την επεξεργασία που θα διαβιβάσουν τα δεδομένα από εσάς στον οικείο εισαγωγέα δεδομένων – λαμβάνοντας

⁶³ Ως «προβληματική νομοθεσία» νοείται η νομοθεσία που 1) επιβάλλει υποχρεώσεις στον αποδέκτη δεδομένων προσωπικού χαρακτήρα από την Ευρωπαϊκή Ένωση ή/και επηρεάζει τα διαβιβαζόμενα δεδομένα με τρόπο που μπορεί να θίξει τη συμβατική εγγύηση ουσιαστικά ισοδύναμου επιπέδου προστασίας που παρέχουν τα εργαλεία διαβίβασης και 2) δεν τηρεί την ουσία των θεμελιωδών δικαιωμάτων και ελευθεριών που αναγνωρίζονται στον Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης ή υπερβαίνει τα απολύτως αναγκαία και αναλογικά σε μια δημοκρατική κοινωνία για τη διασφάλιση ενός από τους σημαντικούς στόχους όπως επίσης αναγνωρίζονται στο ενωσιακό δίκαιο ή στο δίκαιο των κρατών μελών, όπως αυτοί που απαριθμούνται στο άρθρο 23 παράγραφος 1 του ΓΚΠΔ.

⁶⁴ Όταν η εν λόγω πρόσβαση υπερβαίνει ό,τι είναι αναγκαίο και αναλογικό σε μια δημοκρατική κοινωνία· βλ. άρθρα 47 και 52 του Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ, άρθρο 23.1 του ΓΚΠΔ, και συστάσεις 02/2020 του ΕΣΠΔ σχετικά με τις ευρωπαϊκές βασικές εγγυήσεις για τα μέτρα παρακολούθησης, 10 Νοεμβρίου 2020, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.

⁶⁵ Βλ. υποσημείωση 42.

υπόψη τις σχετικές διατάξεις που ισχύουν για αυτούς βάσει της νομοθεσίας της τρίτης χώρας προορισμού).⁶⁶

- την τεχνική ή τις παραμέτρους πρακτικής εφαρμογής του δικαίου της χώρας που έχουν συναφθεί στο βήμα 3·
- την πιθανότητα τα δεδομένα να υπόκεινται σε περαιτέρω διαβιβάσεις, εντός της ίδιας τρίτης χώρας ή ακόμη και σε άλλες τρίτες χώρες (π.χ. συμμετοχή υπεργολάβων επεξεργασίας του εισαγωγέα δεδομένων⁶⁷).

⁶⁶ Ο ΓΚΠΔ εκχωρεί ξεχωριστές υποχρεώσεις σε υπεύθυνους επεξεργασίας και εκτελούντες την επεξεργασία. Οι διαβιβάσεις μπορούν να είναι από υπεύθυνο επεξεργασίας σε υπεύθυνο επεξεργασίας, μεταξύ από κοινού υπεύθυνων επεξεργασίας, από υπεύθυνο επεξεργασίας σε εκτελούντα την επεξεργασία και, με την επιφύλαξη εξουσιοδότησης του υπεύθυνου επεξεργασίας, από εκτελούντα την επεξεργασία σε υπεύθυνο επεξεργασίας ή από εκτελούντα την επεξεργασία σε εκτελούντα την επεξεργασία.

⁶⁷ Βλ. υποσημείωση 26.

Παραδείγματα πρόσθετων μέτρων

55. Μερικά παραδείγματα τεχνικών, συμβατικών και οργανωτικών μέτρων που θα μπορούσαν να εξεταστούν, σε περίπτωση που δεν περιλαμβάνονται ήδη στο χρησιμοποιούμενο εργαλείο διαβίβασης του άρθρου 46 του ΓΚΠΔ, περιλαμβάνονται στους ενδεικτικούς καταλόγους που περιγράφονται στο παράρτημα 2.

56. Εάν εφαρμόζετε αποτελεσματικά πρόσθετα μέτρα τα οποία, σε συνδυασμό με το εργαλείο διαβίβασης του άρθρου 46 του ΓΚΠΔ που έχετε επιλέξει, επιτυγχάνουν το επίπεδο προστασίας που είναι ουσιαστικά ισοδύναμο με το επίπεδο προστασίας που εγγυάται ο ΕΟΧ: μπορείτε να προβείτε στις διαβιβάσεις σας.

57. Όταν δεν μπορείτε να βρείτε ή να εφαρμόσετε αποτελεσματικά πρόσθετα μέτρα που διασφαλίζουν ότι τα διαβιβαζόμενα δεδομένα προσωπικού χαρακτήρα τυγχάνουν ενός ουσιαστικά ισοδύναμου επιπέδου προστασίας,⁶⁸ δεν πρέπει να προβείτε στη διαβίβαση δεδομένων προσωπικού χαρακτήρα στην οικεία τρίτη χώρα βάσει του εργαλείου διαβίβασης του άρθρου 46 του ΓΚΠΔ στο οποίο βασίζεστε. Εάν πραγματοποιείτε ήδη διαβιβάσεις, υποχρεούστε να αναστείλετε ή να τερματίσετε τη διαβίβαση δεδομένων προσωπικού χαρακτήρα.⁶⁹ Σύμφωνα με τις εγγυήσεις που περιλαμβάνονται στο εργαλείο διαβίβασης του άρθρου 46 του ΓΚΠΔ στο οποίο βασίζεστε, τα δεδομένα που έχετε ήδη διαβιβάσει στην εν λόγω τρίτη χώρα και τα αντίγραφά τους θα πρέπει να σας επιστραφούν ή να καταστραφούν στο σύνολό τους από τον εισαγωγέα.⁷⁰

⁶⁸ Όταν η εν λόγω πρόσβαση υπερβαίνει ό,τι είναι αναγκαίο και αναλογικό σε μια δημοκρατική κοινωνία· βλ. άρθρα 47 και 52 του Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ, άρθρο 23.1 του ΓΚΠΔ, και συστάσεις 02/2020 του ΕΣΠΔ σχετικά με τις ευρωπαϊκές βασικές εγγυήσεις για τα μέτρα παρακολούθησης, 10 Νοεμβρίου 2020, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.

⁶⁹ C-311/18 (Schrems II), σκέψη 135.

⁷⁰ Βλ. ρήτρα 12 στο παράρτημα της απόφασης ΤΣΡ 87/2010· βλ. (προαιρετική) πρόσθετη ρήτρα καταγγελίας στο παράρτημα Β της απόφασης ΤΣΡ 2004/915/ΕΚ.

Παράδειγμα:

Παράδειγμα: η νομοθεσία της τρίτης χώρας απαγορεύει τα πρόσθετα μέτρα που έχετε προσδιορίσει (π.χ. απαγορεύει τη χρήση κρυπτογράφησης) ή παρεμποδίζει με άλλο τρόπο την αποτελεσματικότητά τους. Δεν πρέπει να ξεκινήσετε τη διαβίβαση δεδομένων προσωπικού χαρακτήρα στην εν λόγω χώρα ή πρέπει να σταματήσετε τις υπό εξέλιξη υπάρχουσες διαβιβάσεις στην εν λόγω χώρα.

58. Η αρμόδια εποπτική αρχή μπορεί να επιβάλει οποιοδήποτε άλλο επανορθωτικό μέτρο (π.χ. πρόστιμο) εάν, παρά το γεγονός ότι δεν μπορείτε να αποδείξετε ένα ουσιαστικά ισοδύναμο επίπεδο προστασίας στην τρίτη χώρα, ξεκινήσετε ή συνεχίσετε τη διαβίβαση.

2.5 Βήμα 5: Διαδικαστικά βήματα εάν έχετε προσδιορίσει αποτελεσματικά πρόσθετα μέτρα

59. Τα διαδικαστικά βήματα στα οποία ίσως χρειαστεί να προβείτε σε περίπτωση που έχετε προσδιορίσει αποτελεσματικά πρόσθετα μέτρα που πρέπει να τεθούν σε εφαρμογή μπορεί να διαφέρουν ανάλογα με το εργαλείο διαβίβασης του άρθρου 46 του ΓΚΠΔ που χρησιμοποιείτε ή προτίθεστε να χρησιμοποιήσετε.

2.5.1 Τυποποιημένες συμβατικές ρήτρες («ΤΣΡ») (άρθρο 46 παράγραφος 2 στοιχεία γ) και δ) του ΓΚΠΔ)

60. Όταν σκοπεύετε να εφαρμόσετε πρόσθετα μέτρα πλην των ΤΣΡ, δεν απαιτείται να ζητήσετε άδεια από την αρμόδια ΕΑ για να προσθέσετε τέτοιου είδους ρήτρες ή πρόσθετες εγγυήσεις, αρκεί τα πρόσθετα μέτρα που έχετε προσδιορίσει να μην έρχονται σε αντίθεση, άμεσα ή έμμεσα, με τις ΤΣΡ και να επαρκούν για να διασφαλιστεί ότι δεν υπονομεύεται το επίπεδο προστασίας που εγγυάται ο ΓΚΠΔ.⁷¹ Ο εξαγωγέας και ο εισαγωγέας δεδομένων πρέπει να διασφαλίζουν ότι οι πρόσθετες ρήτρες δεν μπορούν με οποιονδήποτε τρόπο να θεωρηθεί ότι περιορίζουν τα δικαιώματα και τις υποχρεώσεις στις ΤΣΡ ή με οποιονδήποτε άλλο τρόπο ότι μειώνουν το επίπεδο προστασίας των δεδομένων. Θα πρέπει να μπορείτε να το αποδείξετε, συμπεριλαμβανομένης της σαφήνειας του συνόλου των ρητρών, σύμφωνα με την αρχή της λογοδοσίας και την υποχρέωσή σας να παρέχετε επαρκές επίπεδο προστασίας των δεδομένων. Οι αρμόδιες εποπτικές αρχές έχουν την εξουσία να επανεξετάζουν τις εν λόγω συμπληρωματικές ρήτρες όπου απαιτείται (π.χ. σε περίπτωση καταγγελίας ή αυτεπάγγελτης έρευνας).

⁷¹ Η αιτιολογική σκέψη 109 του ΓΚΠΔ αναφέρει τα εξής: «Η δυνατότητα του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία να χρησιμοποιεί τυποποιημένες ρήτρες προστασίας των δεδομένων εγκεκριμένες από την Επιτροπή ή από εποπτική αρχή δεν θα πρέπει να εμποδίζει τους υπευθύνους επεξεργασίας ή εκτελούντες την επεξεργασία να ενσωματώνουν τις τυποποιημένες ρήτρες προστασίας δεδομένων σε ευρύτερη σύμβαση, όπως σε σύμβαση μεταξύ του εκτελούντος την επεξεργασία και άλλου εκτελούντος την επεξεργασία, ούτε να προσθέτουν άλλες ρήτρες ή πρόσθετες εγγυήσεις, εφόσον αυτές δεν αντιφάσκουν, άμεσα ή έμμεσα, προς τις εγκεκριμένες από την Επιτροπή ή από εποπτική αρχή τυποποιημένες συμβατικές ρήτρες ούτε θίγουν τα θεμελιώδη δικαιώματα ή τις ελευθερίες των υποκειμένων των δεδομένων.» Παρόμοιες διατάξεις παρέχονται σε σύνολα ΤΣΡ που εγκρίθηκαν από την Ευρωπαϊκή Επιτροπή βάσει της οδηγίας 95/45/ΕΚ.

61. Όταν σκοπεύετε να τροποποιήσετε τις ίδιες τις τυποποιημένες συμβατικές ρήτρες προστασίας δεδομένων ή όταν τα πρόσθετα μέτρα που προστίθενται «αντιτίθενται» άμεσα ή έμμεσα στις ΤΣΡ, δεν θεωρείται πλέον ότι βασίζεστε σε τυποποιημένες συμβατικές ρήτρες⁷² και πρέπει να ζητήσετε εξουσιοδότηση από την αρμόδια εποπτική αρχή σύμφωνα με το άρθρο 46 παράγραφος 3 στοιχείο α) του ΓΚΠΔ.

2.5.2 ΔΕΚ [άρθρο 46 παράγραφος 2 στοιχείο β) του ΓΚΠΔ].

62. Το σκεπτικό της απόφασης Schrems II ισχύει και για άλλα εργαλεία διαβίβασης σύμφωνα με το άρθρο 46 παράγραφος 2 του ΓΚΠΔ, δεδομένου ότι όλα τα εν λόγω εργαλεία είναι ουσιαστικά συμβατικού χαρακτήρα, επομένως οι εγγυήσεις που προβλέπονται και οι δεσμεύσεις που ανέλαβαν τα μέρη δεν μπορούν να δεσμεύουν δημόσιες αρχές τρίτων χωρών.⁷³

63. Η απόφαση Schrems II είναι σημαντική για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα βάσει ΔΕΚ, καθώς οι νομοθεσίες τρίτων χωρών ενδέχεται να επηρεάσουν την προστασία που παρέχεται από αυτά τα εν λόγω εργαλεία.

64. Στις επικαιροποιημένες παραπομπές WP256/257⁷⁴ θα γίνεται αναφορά σε όλες τις δεσμεύσεις που πρέπει να συμπεριληφθούν, με τις οποίες θα πρέπει να εναρμονίσουν τις υφιστάμενες και τις μελλοντικές ΔΕΚ τους όλοι οι όμιλοι που βασίζονται σε ΔΕΚ ως εργαλεία διαβίβασης.

65. Το Δικαστήριο επισήμανε ότι αποτελεί ευθύνη του εξαγωγέα και του εισαγωγέα δεδομένων να αξιολογούν κατά πόσον τηρείται το επίπεδο προστασίας που απαιτείται από το ενωσιακό δίκαιο στην τρίτη χώρα, προκειμένου να καθορίζουν κατά πόσον είναι πρακτικά δυνατή η συμμόρφωση με τις εγγυήσεις που προβλέπονται από τις τυποποιημένες συμβατικές ρήτρες ή τους δεσμευτικούς εταιρικούς κανόνες. Σε διαφορετική περίπτωση, θα πρέπει να αξιολογείτε κατά πόσον μπορείτε να λάβετε πρόσθετα μέτρα για να διασφαλίσετε ένα ουσιαστικά ισοδύναμο επίπεδο προστασίας όπως παρέχεται στον ΕΟΧ, και εάν το δίκαιο ή η πρακτική της τρίτης χώρας δεν θίγει τα πρόσθετα μέτρα σε βαθμό που αποτρέπει την αποτελεσματικότητά τους.

⁷² Βλ. κατά αναλογία, τη γνώμη 17/2020 του ΕΣΠΔ σχετικά με το σχέδιο Τυποποιημένων Συμβατικών Ρητρών που υποβλήθηκε από την εποπτική αρχή της Σλοβενίας (άρθρο 28 παράγραφος 8 του ΓΚΠΔ) όσον αφορά το άρθρο 28 ΤΣΡ που ήδη εγκρίθηκε και περιλαμβάνει παρόμοια διάταξη («Επιπλέον, το ΕΣΠΔ υπενθυμίζει ότι η δυνατότητα χρήσης Τυποποιημένων Συμβατικών Ρητρών που θεσπίστηκαν από μια εποπτική αρχή δεν εμποδίζει τα μέρη να προσθέσουν άλλες ρήτρες ή πρόσθετες διασφαλίσεις, υπό την προϋπόθεση ότι δεν αντιβαίνουν, άμεσα ή έμμεσα, στις θεσπισθείσες ΤΣΡ ούτε θίγουν τα θεμελιώδη δικαιώματα ή τις ελευθερίες των υποκειμένων των δεδομένων. Επιπλέον, όταν τροποποιούνται οι τυποποιημένες συμβατικές ρήτρες δεδομένων, τα μέρη δεν θεωρείται πλέον ότι έχουν εφαρμόσει εγκεκριμένες τυποποιημένες συμβατικές ρήτρες»), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_202017_art28sccs_si_el.pdf.

⁷³ ΔΕΕ, C-311/18 (Schrems II), σκέψη 132.

⁷⁴ Ομάδα του άρθρου 29, Έγγραφο εργασίας για την κατάρτιση πίνακα με τα στοιχεία και τις αρχές που πρέπει να περιέχονται στους δεσμευτικούς εταιρικούς κανόνες, όπως αναθεωρήθηκαν και εγκρίθηκαν τελευταία στις 6 Φεβρουαρίου 2018, WP 256 αναθ. 01· Ομάδα εργασίας του άρθρου 29, Έγγραφο εργασίας για την κατάρτιση πίνακα με τα στοιχεία και τις αρχές που πρέπει να περιέχονται στους δεσμευτικούς εταιρικούς κανόνες, όπως αναθεωρήθηκαν και εγκρίθηκαν τελευταία στις 6 Φεβρουαρίου 2018, WP 257 αναθ. 01.

2.5.3 Ειδικές συμβατικές ρητρες (άρθρο 46.3 στοιχείο α) του ΓΚΠΔ)

66. Το σκεπτικό της απόφασης Schrems II ισχύει και για άλλα εργαλεία διαβίβασης σύμφωνα με το άρθρο 46 παράγραφος 2 του ΓΚΠΔ, δεδομένου ότι όλα τα εν λόγω εργαλεία είναι ουσιαστικά συμβατικού χαρακτήρα, επομένως οι εγγυήσεις που προβλέπονται και οι δεσμεύσεις που ανέλαβαν τα μέρη δεν μπορούν να δεσμεύουν δημόσιες αρχές τρίτων χωρών.⁷⁵ Η απόφαση Schrems II είναι συνεπώς σημαντική για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα βάσει ειδικών συμβατικών ρητρών, καθώς οι νομοθεσίες τρίτων χωρών ενδέχεται να επηρεάσουν την προστασία που παρέχεται από αυτά τα εν λόγω εργαλεία.

2.6 Βήμα 6: Επαναξιολόγηση σε τακτά χρονικά διαστήματα

67. Πρέπει να παρακολουθείτε, σε συνεχή βάση και, κατά περίπτωση, σε συνεργασία με τους εισαγωγείς δεδομένων, τις εξελίξεις στην τρίτη χώρα στην οποία έχετε διαβιβάσει δεδομένα προσωπικού χαρακτήρα, οι οποίες θα μπορούσαν να επηρεάσουν την αρχική αξιολόγησή σας σχετικά με το επίπεδο προστασίας και τις αποφάσεις που ενδέχεται να είχατε λάβει ανάλογα τις διαβιβάσεις σας. Η λογοδοσία είναι μια συνεχής υποχρέωση (άρθρο 5 παράγραφος 2 του ΓΚΠΔ).
68. Θα πρέπει να διαθέτετε επαρκώς αξιόπιστους μηχανισμούς για να διασφαλίσετε την άμεση αναστολή ή τερματισμό των διαβιβάσεων στις περιπτώσεις όπου:
- ο εισαγωγέας έχει παραβιάσει ή δεν είναι σε θέση να τηρήσει τις δεσμεύσεις που έχει αναλάβει στο εργαλείο διαβίβασης του άρθρου 46 του ΓΚΠΔ· ή
 - τα πρόσθετα μέτρα δεν ισχύουν πλέον στην εν λόγω τρίτη χώρα.

3 ΣΥΜΠΕΡΑΣΜΑ

69. Ο ΓΚΠΔ θεσπίζει κανόνες σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα εντός του ΕΟΧ και κατ' αυτόν τον τρόπο επιτρέπει την ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα εντός του ΕΟΧ. Το κεφάλαιο V του ΓΚΠΔ διέπει τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες και θέτει ψηλά τον πήχη: η διαβίβαση δεν πρέπει να υπονομεύει το επίπεδο προστασίας των φυσικών προσώπων που διασφαλίζει ο ΓΚΠΔ (άρθρο 44 του ΓΚΠΔ). Η απόφαση C-311/18 (Schrems II) του ΔΕΕ υπογραμμίζει την ανάγκη διασφάλισης της συνέχειας του επιπέδου προστασίας που παρέχεται στο πλαίσιο του ΓΚΠΔ για τα δεδομένα προσωπικού χαρακτήρα που διαβιβάζονται σε τρίτη χώρα.⁷⁶
70. Για να διασφαλίσετε ένα ουσιαστικά ισοδύναμο επίπεδο προστασίας των δεδομένων σας, πρέπει καταρχάς να γνωρίζετε επαρκώς τις διαβιβάσεις σας. Πρέπει επίσης να ελέγχετε ότι τα δεδομένα που διαβιβάζετε είναι κατάλληλα, συναφή και περιορίζονται σε ό,τι είναι αναγκαίο σε σχέση με τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία.
71. Πρέπει επίσης να προσδιορίζετε το εργαλείο διαβίβασης στο οποίο βασίζεστε για τις διαβιβάσεις σας. Εάν το εργαλείο διαβίβασης δεν είναι μια απόφαση επάρκειας, πρέπει να επαληθεύετε κατά περίπτωση αν η νομοθεσία ή η πρακτική της τρίτης χώρας προορισμού υπονομεύει τις εγγυήσεις που περιλαμβάνονται στο εργαλείο διαβίβασης του άρθρου 46 του ΓΚΠΔ στο πλαίσιο των διαβιβάσεών σας. Όταν μόνο το εργαλείο διαβίβασης του άρθρου 46 του ΓΚΠΔ δεν μπορεί

⁷⁵ ΔΕΕ, C-311/18 (Schrems II), σκέψη 132.

⁷⁶ C-311/18 (Schrems II), σκέψη 93.

να επιτύχει για τα δεδομένα προσωπικού χαρακτήρα που διαβιβάζετε ένα ουσιαστικά ισοδύναμο επίπεδο προστασίας, τα πρόσθετα μέτρα ενδέχεται να καλύψουν το κενό.

72. Όταν δεν μπορείτε να βρείτε ή να εφαρμόσετε αποτελεσματικά πρόσθετα μέτρα που διασφαλίζουν ότι τα διαβιβαζόμενα δεδομένα προσωπικού χαρακτήρα τυγχάνουν ενός ουσιαστικά ισοδύναμου επιπέδου προστασίας, δεν πρέπει να προβείτε στη διαβίβαση δεδομένων προσωπικού χαρακτήρα στην οικεία τρίτη χώρα βάσει του εργαλείου διαβίβασης που έχετε επιλέξει. Εάν πραγματοποιείτε ήδη διαβιβάσεις, υποχρεούστε να αναστείλετε ή να τερματίσετε άμεσα τη διαβίβαση δεδομένων προσωπικού χαρακτήρα.
73. Η αρμόδια εποπτική αρχή έχει την εξουσία να αναστέλλει ή να τερματίζει τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτη χώρα εάν δεν διασφαλίζεται η προστασία των δεδομένων που διαβιβάζονται σύμφωνα με το δίκαιο της ΕΕ, ιδίως τα άρθρα 45 και 46 του ΓΚΠΔ και τον Χάρτη των Θεμελιωδών Δικαιωμάτων.

Για το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων

Η Πρόεδρος

(Andrea Jelinek)

ΠΑΡΑΡΤΗΜΑ 1: ΟΡΙΣΜΟΙ

- Ως «τρίτη χώρα» νοείται κάθε χώρα που δεν είναι κράτος μέλος του ΕΟΧ.
- Ως «ΕΟΧ» νοείται ο Ευρωπαϊκός Οικονομικός Χώρος και περιλαμβάνει τα κράτη μέλη της Ευρωπαϊκής Ένωσης και την Ισλανδία, τη Νορβηγία και το Λιχτενστάιν. Ο ΓΚΠΔ ισχύει για τις τελευταίες δυνάμει της συμφωνίας για τον Ευρωπαϊκό Οικονομικό Χώρο, ιδίως του παραρτήματος XI και του πρωτοκόλλου 37.
- Ο «ΓΚΠΔ» αναφέρεται στον κανονισμό (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων).
- «Ο Χάρτης» αναφέρεται στον Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, ΕΕ C 326 της 26.10.2012, σ. 391–407.
- Οι όροι «ΔΕΕ» ή «το Δικαστήριο» αναφέρονται στο Δικαστήριο της Ευρωπαϊκής Ένωσης. Αποτελεί τη δικαστική αρχή της Ευρωπαϊκής Ένωσης και, σε συνεργασία με τα δικαστήρια των κρατών μελών, διασφαλίζει την ενιαία εφαρμογή και ερμηνεία του δικαίου της ΕΕ.
- Ως «εξαγωγέας δεδομένων» νοείται ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία εντός του ΕΟΧ που μεταφέρει δεδομένα προσωπικού χαρακτήρα σε υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία σε τρίτη χώρα.
- Ως «εισαγωγέας δεδομένων» νοείται ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία σε τρίτη χώρα που λαμβάνει ή αποκτά πρόσβαση σε δεδομένα προσωπικού χαρακτήρα που διαβιβάζονται από τον ΕΟΧ.
- Το «εργαλείο διαβίβασης του άρθρου 46 του ΓΚΠΔ» αναφέρεται στις κατάλληλες εγγυήσεις βάσει του άρθρου 46 του ΓΚΠΔ που οι εξαγωγείς δεδομένων εφαρμόζουν κατά τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτη χώρα, ελλείψει απόφασης επάρκειας σύμφωνα με το άρθρο 45 παράγραφος 3 του ΓΚΠΔ. Το άρθρο 46 παράγραφοι 2 και 3 του ΓΚΠΔ περιέχει τον κατάλογο των εργαλείων διαβίβασης του άρθρου 46 του ΓΚΠΔ που μπορεί να χρησιμοποιούν οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία.
- Ως «ΤΣΡ» νοούνται οι τυποποιημένες συμβατικές ρήτρες προστασίας δεδομένων (ή «τυποποιημένες συμβατικές ρήτρες») που έχουν εγκριθεί από την Ευρωπαϊκή Επιτροπή για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα μεταξύ υπευθύνων επεξεργασίας ή εκτελούντων την επεξεργασία εντός του ΕΟΧ και υπευθύνων επεξεργασίας ή εκτελούντων την επεξεργασία εκτός του ΕΟΧ. Οι τυποποιημένες συμβατικές ρήτρες που εγκρίνονται από την Ευρωπαϊκή Επιτροπή είναι ένα εργαλείο διαβίβασης βάσει του ΓΚΠΔ, σύμφωνα με το άρθρο 46 παράγραφος 2 στοιχείο γ) και παράγραφος 5 του ΓΚΠΔ.

ΠΑΡΑΡΤΗΜΑ 2. ΠΑΡΑΔΕΙΓΜΑΤΑ ΠΡΟΣΘΕΤΩΝ ΜΕΤΡΩΝ

74. Τα μέτρα που ακολουθούν είναι παραδείγματα πρόσθετων μέτρων που θα μπορούσατε να λάβετε υπόψη σας όταν φτάσετε στο Βήμα 4 «Εφαρμογή πρόσθετων μέτρων». Ο κατάλογος είναι ενδεικτικός. Μπορείτε να διερευνήσετε άλλα πρόσθετα μέτρα. Μελλοντικές τεχνολογικές, νομικές ή οργανωτικές εξελίξεις μπορεί να οδηγήσουν στην εμφάνιση νέων πρόσθετων μέτρων για να λάβετε υπόψη. Η επιλογή και η εφαρμογή ενός ή περισσότερων από τα εν λόγω μέτρα δεν διασφαλίζουν απαραίτητα και συστηματικώς ότι η διαβίβασή σας πληροί το ουσιαστικό πρότυπο ισοδυναμίας που απαιτεί η νομοθεσία της ΕΕ. Θα πρέπει να επιλέξετε εκείνα τα πρόσθετα μέτρα που μπορούν να εγγυηθούν αποτελεσματικά αυτό το επίπεδο προστασίας για τις διαβιβάσεις σας.
75. Οποιοδήποτε πρόσθετο μέτρο μπορεί να θεωρηθεί αποτελεσματικό κατά την έννοια της απόφασης του ΔΕΕ «Schrems II» μόνον εάν και στον βαθμό που – το ίδιο το μέτρο μόνο του ή σε συνδυασμό με άλλα – αντιμετωπίζει τις συγκεκριμένες ελλείψεις που εντοπίστηκαν κατά την αξιολόγησή σας σχετικά με την κατάσταση στην τρίτη χώρα, ως προς τους νόμους και τις πρακτικές που ισχύουν για τη διαβίβασή σας. Εάν, τελικά, δεν μπορείτε να διασφαλίσετε ένα ουσιαστικά ισοδύναμο επίπεδο προστασίας, δεν πρέπει να μεταφέρετε τα δεδομένα προσωπικού χαρακτήρα.
76. Ως υπεύθυνος επεξεργασίας ή εκτελών την επεξεργασία, ενδεχομένως σας έχει ήδη ζητηθεί να εφαρμόσετε ορισμένα από τα μέτρα που παρουσιάζονται στο παρόν παράρτημα προκειμένου να συμμορφωθείτε με τον ΓΚΠΔ. Αυτό σημαίνει ότι ενδεχομένως θα χρειαστεί να τεθούν σε εφαρμογή παρόμοια μέτρα για δεδομένα προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία στον ΕΟΧ και διαβιβάζονται σε εισαγωγέα δεδομένων που καλύπτεται από απόφαση περί επάρκειας ή σε άλλες τρίτες χώρες.⁷⁷

2.1 Τεχνικά μέτρα

77. Το παρόν τμήμα περιγράφει με ενδεικτικό τρόπο παραδείγματα τεχνικών μέτρων, τα οποία ενδέχεται να συμπληρώνουν τις εγγυήσεις που περιλαμβάνονται στα εργαλεία διαβίβασης του άρθρου 46 του ΓΚΠΔ για τη διασφάλιση της συμμόρφωσης με το επίπεδο προστασίας που απαιτείται βάσει της νομοθεσίας της ΕΕ στο πλαίσιο της διαβίβασης δεδομένων προσωπικού χαρακτήρα σε τρίτη χώρα. Τα εν λόγω μέτρα θα απαιτηθούν κυρίως όταν το δικαίωμα της εν λόγω χώρας επιβάλλει στον εισαγωγέα δεδομένων υποχρεώσεις οι οποίες είναι αντίθετες με τις εγγυήσεις των εργαλείων διαβίβασης του άρθρου 46 του ΓΚΠΔ και, ιδίως, μπορούν να θίξουν τη συμβατική εγγύηση ενός ουσιαστικά ισοδύναμου επιπέδου προστασίας έναντι της πρόσβασης των δημόσιων αρχών της εν λόγω τρίτης χώρας στα δεδομένα αυτά.⁷⁸
78. Για περισσότερη σαφήνεια, στην παρούσα ενότητα παρουσιάζονται ορισμένα παραδείγματα σεναρίων για τα οποία μερικά τεχνικά μέτρα θα μπορούσαν ενδεχομένως να είναι αποτελεσματικά στη διασφάλιση ενός ουσιαστικά ισοδύναμου επιπέδου προστασίας. Στη συνέχεια της ενότητας παρουσιάζονται ορισμένα σενάρια για τα οποία δεν προσδιορίζονται τα τεχνικά μέτρα για τη διασφάλιση αυτού του επιπέδου προστασίας.

⁷⁷ Άρθρο 5.2 και άρθρο 32 στοιχείο του ΓΚΠΔ.

⁷⁸ C-311/18 (Schrems II), σκέψη 135.

Παραδείγματα σεναρίων που παραπέμπουν σε υποθέσεις στις οποίες
προσδιορίζονται αποτελεσματικά μέτρα

79. Τα μέτρα που παρατίθενται κατωτέρω αποσκοπούν στο να διασφαλίσουν ότι η πρόσβαση στα δεδομένα που διαβιβάζονται από δημόσιες αρχές τρίτων χωρών δεν επηρεάζει την αποτελεσματικότητα των κατάλληλων εγγυήσεων που περιλαμβάνονται στα εργαλεία διαβίβασης του άρθρου 46 του ΓΚΠΔ. Αυτά τα μέτρα κρίνονται απαραίτητα για να εγγυηθούν ένα ουσιαστικά ισοδύναμο επίπεδο προστασίας με εκείνο που διασφαλίζεται στον ΕΟΧ, ακόμα και αν η πρόσβαση των δημόσιων αρχών συμμορφώνεται με το δίκαιο της χώρας του εισαγωγέα όπου, στην πράξη, η εν λόγω πρόσβαση υπερβαίνει ό,τι είναι αναγκαίο και αναλογικό σε μια δημοκρατική κοινωνία.⁷⁹ Τα μέτρα αυτά αποσκοπούν στην αποτροπή ενδεχόμενης παραβίασης της πρόσβασης, εμποδίζοντας τις αρχές να προσδιορίζουν τα υποκείμενα των δεδομένων, να συνάγουν πληροφορίες σχετικά με αυτά, να τα απομονώνουν σε άλλο πλαίσιο ή να συσχετίζουν τα διαβιβαζόμενα δεδομένα με άλλα σύνολα δεδομένων που μπορεί να κατέχουν, μεταξύ άλλων δεδομένων, επιγραμμικά αναγνωριστικά ταυτότητας που παρέχονται από τις συσκευές, τις εφαρμογές, τα εργαλεία και τα πρωτόκολλα που χρησιμοποιούνται από τα υποκείμενα δεδομένων σε άλλα περιβάλλοντα.
80. Οι δημόσιες αρχές σε τρίτες χώρες μπορεί να επιχειρούν να αποκτήσουν πρόσβαση σε διαβιβαζόμενα δεδομένα.
- α) Κατά τη μεταφορά μέσω πρόσβασης στις γραμμές επικοινωνίας που χρησιμοποιούνται για τη διαβίβαση των δεδομένων στην αποδέκτρια χώρα. Η εν λόγω πρόσβαση μπορεί να είναι παθητική, οπότε τα περιεχόμενα της επικοινωνίας, ενδεχομένως μετά από μια διαδικασία επιλογής, απλώς αντιγράφονται. Η πρόσβαση μπορεί, ωστόσο, να είναι επίσης ενεργή υπό την έννοια ότι οι δημόσιες αρχές παρεμβαίνουν στη διαδικασία επικοινωνίας όχι μόνο διαβάζοντας το περιεχόμενο, αλλά και τροποποιώντας ή καταργώντας τμήματα αυτού.
- β) Ενώ φυλάσσονται από έναν παραλήπτη των δεδομένων για τον οποίο προορίζονται είτε μέσω της πρόσβασης στις ίδιες τις εγκαταστάσεις επεξεργασίας, είτε απαιτώντας από τον παραλήπτη των δεδομένων να εντοπίσει και να εξαγάγει δεδομένα που παρουσιάζουν ενδιαφέρον και να τα παραδώσει στις αρχές.
81. Το παρόν τμήμα εξετάζει σενάρια όπου εφαρμόζονται μέτρα που είναι αποτελεσματικά και στις δύο περιπτώσεις. Διαφορετικά πρόσθετα μέτρα ενδέχεται να ισχύουν και να επαρκούν υπό δεδομένες συνθήκες μιας συγκεκριμένης διαβίβασης εάν μόνο ένας τύπος πρόσβασης προβλέπεται από τη νομοθεσία της αποδέκτριας χώρας. Είναι επομένως απαραίτητο για τον εξαγωγέα δεδομένων να αναλύει προσεκτικά, με την υποστήριξη του εισαγωγέα δεδομένων, τις υποχρεώσεις που επιβάλλονται στον τελευταίο.

⁷⁹ Βλ. άρθρα 47 και 52 του Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ, άρθρο 23.1 του ΓΚΠΔ, και συστάσεις 02/2020 του ΕΣΠΔ σχετικά με τις ευρωπαϊκές βασικές εγγυήσεις για τα μέτρα παρακολούθησης, 10 Νοεμβρίου 2020,

Για παράδειγμα, οι εισαγωγείς δεδομένων των ΗΠΑ που υπάγονται στα εδάφια 50 ΚΗΠ § 1881α (FISA 702) έχουν άμεση υποχρέωση να παραχωρήσουν πρόσβαση ή να παραδώσουν τα εισαγόμενα δεδομένα προσωπικού χαρακτήρα που βρίσκονται στην κατοχή, τη φύλαξη ή τον έλεγχό τους. Αυτό μπορεί να επεκταθεί σε τυχόν κρυπτογραφικά κλειδιά που είναι απαραίτητα ώστε να καθίστανται κατανοητά τα δεδομένα.

82. Τα σενάρια περιγράφουν διαφορετικές περιστάσεις και τα μέτρα που λαμβάνονται παρουσιάζονται ως παράδειγμα. Τυχόν αλλαγές στα σενάρια μπορεί να οδηγήσουν σε διαφορετικά συμπεράσματα. Τα σενάρια παραπέμπουν σε καταστάσεις στις οποίες έχει συναχθεί το συμπέρασμα ότι σε πρώτο στάδιο χρειάζονται πρόσθετα μέτρα, δηλαδή όποτε στην πράξη για τη συγκεκριμένη διαβίβαση ισχύει η προβληματική νομοθεσία της τρίτης χώρας.
83. Οι υπεύθυνοι επεξεργασίας ενδέχεται να χρειαστεί να εφαρμόσουν ορισμένα ή όλα τα μέτρα που περιγράφονται εδώ, ανεξαρτήτως του επιπέδου προστασίας που προβλέπεται από τους νόμους που ισχύουν για τον εισαγωγέα δεδομένων, επειδή απαιτείται να συμμορφωθούν με τα άρθρα 25 και 32 του ΓΚΠΔ στις συγκεκριμένες συνθήκες της διαβίβασης. Με άλλα λόγια, μπορεί να ζητηθεί από τους εξαγωγείς να εφαρμόσουν τα μέτρα που περιγράφονται στο παρόν έγγραφο, ακόμη και αν οι εισαγωγείς δεδομένων τους καλύπτονται από μια απόφαση επάρκειας, όπως ακριβώς ενδέχεται να ζητηθεί από τους υπεύθυνους επεξεργασίας και τους εκτελούντες την επεξεργασία να τα εφαρμόζουν όταν υπάρχουν δεδομένα που υποβάλλονται σε επεξεργασία εντός του ΕΟΧ.

Περίπτωση χρήσης 1: Αποθήκευση δεδομένων για σκοπούς δημιουργίας αντιγράφων ασφαλείας και για άλλους σκοπούς που δεν απαιτούν αποκωδικοποιημένη πρόσβαση σε δεδομένα

84. Ένας εξαγωγέας δεδομένων χρησιμοποιεί έναν πάροχο υπηρεσιών φιλοξενίας σε μια τρίτη χώρα για την αποθήκευση δεδομένων προσωπικού χαρακτήρα, π.χ. για λόγους δημιουργίας αντιγράφων ασφαλείας.

Αν

1. τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία χρησιμοποιώντας ισχυρή κρυπτογράφηση πριν από τη διαβίβαση και επαληθεύεται η ταυτότητα του εισαγωγέα,
2. ο αλγόριθμος κρυπτογράφησης και η παραμετροποίησή του (π.χ. μήκος κλειδιού, τρόπος λειτουργίας, κατά περίπτωση) ανταποκρίνονται στο σύγχρονο επίπεδο της τεχνολογίας και μπορούν να θεωρηθούν ισχυρά έναντι της κρυπτανάλυσης που πραγματοποιείται από τις

δημόσιες αρχές στη χώρα παραλήπτη λαμβάνοντας υπόψη τους πόρους και τις τεχνικές δυνατότητες (π.χ. υπολογιστική ισχύς για βίαιες επιθέσεις) που έχουν στη διάθεσή τους,⁸⁰

3. η ισχύς της κρυπτογράφησης και το μήκος κλειδιού λαμβάνουν υπόψη τη συγκεκριμένη χρονική περίοδο κατά την οποία πρέπει να διατηρηθεί η εμπιστευτικότητα των κρυπτογραφημένων δεδομένων προσωπικού χαρακτήρα,⁸¹
4. ο αλγόριθμος κρυπτογράφησης εφαρμόζεται σωστά και από επαρκώς συντηρημένο λογισμικό χωρίς καμία γνωστή ευπάθεια, η συμμόρφωση του οποίου προς την προδιαγραφή του επιλεγμένου αλγορίθμου έχει επαληθευτεί, π.χ. μέσω πιστοποίησης,
5. η διαχείριση των κλειδιών πραγματοποιείται με αξιόπιστο τρόπο (δημιουργία, διαχείριση, αποθήκευση, αν χρειάζεται, σύνδεση με την ταυτότητα ενός παραλήπτη για τον οποίο προορίζονται και ανάκληση),⁸² και
6. τα κλειδιά διατηρούνται αποκλειστικά υπό τον έλεγχο του εξαγωγέα δεδομένων ή μιας οντότητας που εμπιστεύεται ο εξαγωγέας στον ΕΟΧ ή σε δικαιοδοσία που παρέχει ουσιαστικά ισοδύναμο επίπεδο προστασίας με εκείνο που διασφαλίζεται εντός του ΕΟΧ,

τότε το ΕΣΠΔ θεωρεί ότι η κρυπτογράφηση που πραγματοποιείται παρέχει ένα αποτελεσματικό πρόσθετο μέτρο.

Περίπτωση χρήσης 2: Διαβίβαση ψευδωνυμοποιημένων δεδομένων

85. Ένας εξαγωγέας δεδομένων πρώτα ψευδωνυμοποιεί δεδομένα που κατέχει και στη συνέχεια τα διαβιβάζει σε τρίτη χώρα για ανάλυση, π.χ., για σκοπούς έρευνας.

⁸⁰ Όσον αφορά την αξιολόγηση της ισχύος των αλγορίθμων κρυπτογράφησης, τη συμμόρφωσή τους με το σύγχρονο επίπεδο της τεχνολογίας και την ισχύ τους έναντι της κρυπτανάλυσης σε βάθος χρόνου, οι εξαγωγείς δεδομένων μπορούν να βασιστούν στις τεχνικές κατευθυντήριες γραμμές που έχουν δημοσιευτεί από τις επίσημες αρχές ασφάλειας στον κυβερνοχώρο της ΕΕ και των κρατών μελών της. Για παράδειγμα, βλ. την έκθεση της ENISA «What is "state of the art" in IT security? », 2019, <https://www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it-security>, τις κατευθυντήριες γραμμές του Ομοσπονδιακού Γραφείου της Γερμανίας για την ασφάλεια των πληροφοριών στις οικείες τεχνικές κατευθυντήριες γραμμές της σειράς TR-02102 και «[Algorithms, Key Size and Protocols Report \(2018\)](https://www.ecrypt.eu.org/csa/documents/D5.4-FinalAlgKeySizeProt.pdf)», H2020-ICT-2014 – Project 645421, D5.4, [ECRYPT-CSA](https://www.ecrypt.eu.org/csa/documents/D5.4-FinalAlgKeySizeProt.pdf), 02/2018» στη διεύθυνση <https://www.ecrypt.eu.org/csa/documents/D5.4-FinalAlgKeySizeProt.pdf>.

⁸¹ Η ικανότητα προστασίας των αλγορίθμων κρυπτογράφησης υπόκειται σε υποβάθμιση με την πάροδο του χρόνου λόγω της ανακάλυψης νέων τεχνικών κρυπτανάλυσης, της εμφάνισης νέων υπολογιστικών υποδειγμάτων όπως η κβαντική υπολογιστική και της γενικής αύξησης διαθέσιμης υπολογιστικής ισχύος, εκτός εάν οι εφαρμοζόμενοι αλγόριθμοι αποδειχθούν θεωρητικά ασφαλείς για τις πληροφορίες. Αυτή η ανησυχία αφορά ιδίως τους αλγόριθμους δημόσιου κλειδιού που χρησιμοποιούνται ευρέως κατά τον χρόνο σύνταξης των συστάσεων. Κατά συνέπεια, ο εξαγωγέας δεδομένων πρέπει να θεωρήσει ότι οι δημόσιες αρχές μπορούν να αποκτήσουν πρόσβαση σε κρυπτογραφημένα δεδομένα στις περιπτώσεις που περιγράφονται στην παράγραφο αριθ. 80 και να τα αποθηκεύσουν έως ότου οι πόροι τους επαρκούν για αποκρυπτογράφηση. Το πρόσθετο μέτρο μπορεί να θεωρηθεί αποτελεσματικό μόνον εάν η εν λόγω αποκρυπτογράφηση και η επακόλουθη περαιτέρω επεξεργασία εκείνη την περίοδο δεν συνιστούν πλέον παραβίαση των δικαιωμάτων των υποκειμένων των δεδομένων, π.χ. επειδή τα δεδομένα δεν μπορούν πλέον να χρησιμοποιηθούν για την άμηση ή την έμμεση ταυτοποίησή τους.

⁸² NIST Special Publication 800-57, Recommendation for Key Management <https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final>

Αν

1. ένας εξαγωγέας δεδομένων διαβιβάζει δεδομένα προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία με τρόπο τέτοιο ώστε τα δεδομένα προσωπικού χαρακτήρα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο δεδομένων, ούτε να χρησιμοποιηθούν για την εξατομίκευση του υποκειμένου δεδομένων σε μια μεγαλύτερη ομάδα, χωρίς τη χρήση πρόσθετων πληροφοριών,⁸³
2. οι εν λόγω συμπληρωματικές πληροφορίες κατέχονται κατ' αποκλειστικότητα από τον εξαγωγέα δεδομένων και τηρούνται χωριστά σε κράτος μέλος ή σε τρίτη χώρα, από οντότητα που εμπιστεύεται ο εξαγωγέας στον ΕΟΧ ή σε δικαιοδοσία που παρέχει ουσιαστικά ισοδύναμο επίπεδο προστασίας με εκείνο που διασφαλίζεται εντός του ΕΟΧ,
3. η κοινολόγηση ή η μη εξουσιοδοτημένη χρήση των εν λόγω συμπληρωματικών πληροφοριών αποτρέπεται με τη χρήση τεχνικών και οργανωτικών διασφαλίσεων, διασφαλίζεται ότι ο εξαγωγέας δεδομένων διατηρεί τον αποκλειστικό έλεγχο του αλγορίθμου ή του αποθετηρίου που επιτρέπει την εκ νέου ταυτοποίηση χρησιμοποιώντας τις πρόσθετες πληροφορίες, και
4. ο υπεύθυνος επεξεργασίας έχει διαπιστώσει μέσω διεξοδικής ανάλυσης των εν λόγω δεδομένων – λαμβάνοντας υπόψη τυχόν πληροφορίες που αναμένεται να διαθέτουν και να χρησιμοποιούν οι δημόσιες αρχές της αποδέκτριας χώρας – ότι τα ψευδωνυμοποιημένα δεδομένα προσωπικού χαρακτήρα δεν μπορούν να αποδοθούν σε ένα ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο, ακόμη και αν διασταυρώνονται με τις εν λόγω πληροφορίες,

τότε το ΕΣΠΔ θεωρεί ότι η ψευδωνυμοποίηση που πραγματοποιείται παρέχει ένα αποτελεσματικό πρόσθετο μέτρο.

86. Επισημαίνεται ότι σε πολλές περιπτώσεις, παράγοντες που σχετίζονται με τη φυσική, φυσιολογική, γενετική, διανοητική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα ενός φυσικού προσώπου, τη φυσική του τοποθεσία ή την αλληλεπίδρασή του με μια διαδικτυακή υπηρεσία σε συγκεκριμένη χρονική στιγμή⁸⁴ μπορεί να επιτρέψουν την αναγνώριση της ταυτότητας του εν λόγω ατόμου ακόμη και αν παραλείπεται το όνομα, η διεύθυνση ή άλλα απλά αναγνωριστικά ταυτότητας.
87. Αυτό ισχύει ιδιαίτερα όταν τα δεδομένα αφορούν τη χρήση υπηρεσιών παροχής πληροφοριών (χρόνος πρόσβασης, ακολουθία χαρακτηριστικών στα οποία αποκτήθηκε πρόσβαση,

⁸³ Σύμφωνα με το άρθρο 4 παράγραφος 5 του ΓΚΠΔ: ως «ψευδωνυμοποίηση» νοείται η επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο ώστε τα δεδομένα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρωματικές πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλιστεί ότι δεν μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο. Τα πρόσθετα δεδομένα μπορούν να συνίστανται σε πίνακες που παραθέτουν ψευδώνυμα δίπλα από τα αναγνωριστικά χαρακτηριστικά που αντικαθιστούν, κρυπτογραφικά κλειδιά ή άλλες παραμέτρους για τον μετασχηματισμό γνωρισμάτων, ή άλλα δεδομένα που επιτρέπουν την απόδοση των ψευδωνυμοποιημένων δεδομένων σε ταυτοποιημένα ή ταυτοποιήσιμα φυσικά πρόσωπα.

⁸⁴ Άρθρο 4 παράγραφος 1 του ΓΚΠΔ: « “δεδομένα προσωπικού χαρακτήρα”: κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»): το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου».

χαρακτηριστικά της συσκευής που χρησιμοποιείται κ.λπ.). Οι εν λόγω υπηρεσίες ενδέχεται, όπως και για τον εισαγωγέα δεδομένων προσωπικού χαρακτήρα, να υπόκεινται στην υποχρέωση παροχής πρόσβασης στις ίδιες δημόσιες αρχές που υπάγονται στη δικαιοδοσία τους, οι οποίες στη συνέχεια θα διαθέτουν κατά πάσα πιθανότητα δεδομένα σχετικά με τη χρήση των εν λόγω υπηρεσιών παροχής πληροφοριών από τα άτομα για τα οποία προορίζονται.

88. Επιπλέον, δεδομένου ότι η χρήση ορισμένων υπηρεσιών παροχής πληροφοριών είναι από τη φύση της δημόσια, ή η εκμετάλλευσή τους από μέρη με σημαντικούς πόρους, οι υπεύθυνοι επεξεργασίας θα πρέπει να είναι ιδιαιτέρως προσεκτικοί, δεδομένου ότι οι δημόσιες αρχές εντός της δικαιοδοσίας τους διαθέτουν κατά πάσα πιθανότητα δεδομένα σχετικά με τη χρήση υπηρεσιών παροχής πληροφοριών από ένα άτομο για το οποίο προορίζονται.
89. Εάν, στην πορεία υλοποίησης της ψευδωνυμοποίησης, τα γνωρίσματα που περιέχονται στα δεδομένα προσωπικού χαρακτήρα μετασχηματίζονται με τη χρήση αλγορίθμου κρυπτογράφησης, ισχύουν οι κατευθυντήριες γραμμές που παρουσιάζονται στις υποσημειώσεις 80 και 81. Στο εξής, συνιστάται να αποφεύγεται η αποκλειστική χρήση της κρυπτογράφησης και να εφαρμόζονται μετασχηματισμοί που βασίζονται σε μηχανισμούς αναζήτησης σε πίνακες.

Περίπτωση χρήσης 3: Κρυπτογράφηση δεδομένων για να προστατεύονται από την πρόσβαση των δημόσιων αρχών της τρίτης χώρας του εισαγωγέα στο στάδιο διέλευσης μεταξύ του εξαγωγέα και του εισαγωγέα τους

90. Ένας εξαγωγέας δεδομένων επιθυμεί να διαβιβάσει δεδομένα σε προορισμό στον οποίο το δίκαιο ή/και οι πρακτικές προβλέπουν την πρόσβαση των δημόσιων αρχών στα δεδομένα στο στάδιο διέλευσης μεταξύ της χώρας του εξαγωγέα και της χώρας προορισμού.

Av

1. ένας εξαγωγέας δεδομένων διαβιβάσει δεδομένα προσωπικού χαρακτήρα σε εισαγωγέα δεδομένων σε δικαιοδοσία στην οποία το δίκαιο ή/και η πρακτική επιτρέπουν την πρόσβαση των δημόσιων αρχών στα δεδομένα ενώ μεταφέρονται μέσω διαδικτύου στην εν λόγω τρίτη χώρα χωρίς τις ευρωπαϊκές βασικές εγγυήσεις σε σχέση με αυτή την πρόσβαση, χρησιμοποιείται κρυπτογράφηση μεταφοράς για την οποία διασφαλίζεται ότι τα χρησιμοποιούμενα πρωτόκολλα κρυπτογράφησης είναι προηγμένης τεχνολογίας και παρέχουν αποτελεσματική προστασία έναντι ενεργών και παθητικών επιθέσεων με πόρους που είναι γνωστό ότι διαθέτουν οι δημόσιες αρχές της εν λόγω τρίτης χώρας,
2. τα μέρη που συμμετέχουν στη μετάδοση συμφωνούν για μια αξιόπιστη αρχή πιστοποίησης δημόσιου κλειδιού ή υποδομή,
3. χρησιμοποιούνται συγκεκριμένα προστατευτικά και προηγμένης τεχνολογίας μέτρα έναντι ενεργών και παθητικών επιθέσεων στα συστήματα αποστολής και λήψης που παρέχουν κρυπτογράφηση μεταφοράς, συμπεριλαμβανομένων των δοκιμών για τυχόν ευπάθεια του λογισμικού και τις πιθανές κερκόπορτες,
4. σε περίπτωση που η κρυπτογράφηση μεταφοράς δεν παρέχει από μόνη της κατάλληλη ασφάλεια λόγω προηγούμενων εμπειριών ευπάθειας της υποδομής ή του χρησιμοποιούμενου λογισμικού, τα δεδομένα προσωπικού χαρακτήρα κρυπτογραφούνται επίσης διατεμαχικά σε επίπεδο εφαρμογών χρησιμοποιώντας μεθόδους κρυπτογράφησης τελευταίας τεχνολογίας,
5. ο αλγόριθμος κρυπτογράφησης και η παραμετροποίησή του (π.χ. μήκος κλειδιού, τρόπος λειτουργίας, εάν ισχύει) ανταποκρίνονται στο σύγχρονο επίπεδο της τεχνολογίας και μπορούν

να θεωρηθούν ισχυρά έναντι της κρυπτανάλυσης που πραγματοποιείται από τις δημόσιες αρχές στο στάδιο διέλευσης των δεδομένων στην εν λόγω τρίτη χώρα, λαμβάνοντας υπόψη τους πόρους και τις τεχνικές δυνατότητες (π.χ. υπολογιστική ισχύς για βίαιες επιθέσεις) που έχουν στη διάθεσή τους (βλ. υποσημείωση 80 παραπάνω),⁸⁵.

6. η ισχύς της κρυπτογράφησης λαμβάνει υπόψη τη συγκεκριμένη χρονική περίοδο κατά την οποία πρέπει να διατηρηθεί η εμπιστευτικότητα των κρυπτογραφημένων δεδομένων προσωπικού χαρακτήρα,
7. ο αλγόριθμος κρυπτογράφησης εφαρμόζεται σωστά και από επαρκώς συντηρημένο λογισμικό χωρίς καμία γνωστή ευπάθεια, η συμμόρφωση του οποίου προς την προδιαγραφή του επιλεγμένου αλγορίθμου έχει επαληθευτεί, π.χ. μέσω πιστοποίησης,
8. η διαχείριση των κλειδιών πραγματοποιείται με αξιόπιστο τρόπο (δημιουργία, διαχείριση, αποθήκευση, αν χρειάζεται, σύνδεση με την ταυτότητα ενός παραλήπτη για τον οποίο προορίζονται και ανάκληση), από τον εξαγωγέα ή από μια οντότητα που εμπιστεύεται ο εξαγωγέας στο πλαίσιο δικαιοδοσίας που παρέχει ένα ουσιαστικά ισοδύναμο επίπεδο προστασίας,

τότε το ΕΣΠΔ θεωρεί ότι η κρυπτογράφηση μεταφοράς, εάν απαιτείται σε συνδυασμό με τη διατεματική κρυπτογράφηση περιεχομένου, παρέχει ένα αποτελεσματικό πρόσθετο μέτρο.

Περίπτωση χρήσης 4: Προστατευόμενος παραλήπτης

91. Ένας εξαγωγέας δεδομένων διαβιβάζει δεδομένα προσωπικού χαρακτήρα σε έναν εισαγωγέα δεδομένων σε μια τρίτη χώρα που προστατεύεται ειδικά από τη νομοθεσία της εν λόγω χώρας, π.χ. με σκοπό την από κοινού παροχή ιατρικής περίθαλψης για έναν ασθενή ή νομικών υπηρεσιών σε έναν πελάτη.

Αν

1. το δίκαιο τρίτης χώρας απαλλάσσει έναν εισαγωγέα δεδομένων που διαμένει στη χώρα εισαγωγής από ενδεχόμενη παραβίαση της πρόσβασης σε δεδομένα που διατηρεί ο εν λόγω παραλήπτης για τον συγκεκριμένο σκοπό, π.χ. δυνάμει επαγγελματικού απορρήτου που ισχύει για τον εισαγωγέα δεδομένων,
2. η εν λόγω απαλλαγή επεκτείνεται σε όλες τις πληροφορίες που έχει στη διάθεσή του ο εισαγωγέας δεδομένων και που μπορούν να χρησιμοποιηθούν για την παράκαμψη της προστασίας προνομιακών πληροφοριών (κρυπτογραφικά κλειδιά, κωδικοί πρόσβασης, άλλα διαπιστευτήρια κ.λπ.),
3. ο εισαγωγέας δεδομένων δεν χρησιμοποιεί τις υπηρεσίες ενός εκτελούντα την επεξεργασία κατά τρόπο που επιτρέπει στις δημόσιες αρχές να έχουν πρόσβαση στα δεδομένα ενώ διατηρούνται από τον εκτελούντα την επεξεργασία, ούτε ο εισαγωγέας δεδομένων διαβιβάζει τα δεδομένα σε άλλη οντότητα που δεν προστατεύεται, βάσει του εργαλείου διαβίβασης του άρθρου 46 του ΓΚΠΔ,
4. τα δεδομένα προσωπικού χαρακτήρα κρυπτογραφούνται πριν από τη διαβίβασή τους με μια μέθοδο που συμμορφώνεται με την εξέλιξη της τεχνολογίας και εγγυάται ότι η αποκρυπτογράφηση δεν θα είναι δυνατή χωρίς γνώση του κλειδιού αποκρυπτογράφησης

⁸⁵ Βλ. υποσημείωση 80 για ορισμένες παραπομπές στις τεχνικές κατευθυντήριες γραμμές που έχουν δημοσιευτεί από επίσημες αρχές ασφάλειας στον κυβερνοχώρο της ΕΕ και των κρατών μελών της.

(διατεμαχική αποκρυπτογράφηση) για το σύνολο του χρονικού διαστήματος κατά το οποίο πρέπει να προστατεύονται τα δεδομένα,

5. το κλειδί αποκρυπτογράφησης βρίσκεται υπό την αποκλειστική επιμέλεια του προστατευόμενου εισαγωγέα δεδομένων και, πιθανώς, του ίδιου του εξαγωγέα ή άλλης οντότητας που εμπιστεύεται ο εξαγωγέας και η οποία είναι εγκατεστημένη στον ΕΟΧ ή σε δικαιοδοσία που παρέχει ουσιαστικά ισοδύναμο επίπεδο προστασίας με εκείνο που διασφαλίζεται εντός του ΕΟΧ, και προστατεύεται δεόντως από μη εξουσιοδοτημένη χρήση ή κοινολόγηση με τεχνικά και οργανωτικά μέτρα σύμφωνα με την πλέον προηγμένη τεχνολογία, και
6. ο εξαγωγέας δεδομένων έχει αποδείξει με αξιόπιστο τρόπο ότι το κλειδί κρυπτογράφησης που σκοπεύει να χρησιμοποιήσει αντιστοιχεί στο κλειδί αποκρυπτογράφησης που κατέχει ο παραλήπτης,

τότε το ΕΣΠΔ θεωρεί ότι η κρυπτογράφηση μεταφοράς που πραγματοποιείται παρέχει ένα αποτελεσματικό πρόσθετο μέτρο.

Περίπτωση χρήσης 5: Πολυσυμμετοχικός διαχωρισμός ή επεξεργασία

92. Ο εξαγωγέας δεδομένων επιθυμεί την από κοινού επεξεργασία δεδομένων προσωπικού χαρακτήρα από δύο ή περισσότερους ανεξάρτητους εκτελούντες την επεξεργασία που είναι εγκατεστημένοι σε διαφορετικές δικαιοδοσίες χωρίς να τους γνωστοποιήσει το περιεχόμενο των δεδομένων. Πριν από τη μετάδοση, διαχωρίζει τα δεδομένα με τέτοιο τρόπο ώστε κανένα μέρος που λαμβάνει ένας μεμονωμένος εκτελών την επεξεργασία να μην επαρκεί για την ανασύνθεση των δεδομένων προσωπικού χαρακτήρα εν όλω ή εν μέρει. Ο εξαγωγέας δεδομένων λαμβάνει το αποτέλεσμα της επεξεργασίας από καθέναν από τους εκτελούντες την επεξεργασία ανεξάρτητα, και συγχωνεύει τα στοιχεία που ελήφθησαν για να φτάσει στο τελικό αποτέλεσμα το οποίο μπορεί να συνιστά δεδομένα προσωπικού χαρακτήρα ή συγκεντρωτικά δεδομένα.

Αν

1. ένας εξαγωγέας δεδομένων επεξεργάζεται δεδομένα προσωπικού χαρακτήρα με τέτοιο τρόπο ώστε να διαχωρίζονται σε δύο ή περισσότερα μέρη, καθένα από τα οποία δεν μπορεί πλέον να ερμηνευθεί ή να αποδοθεί σε συγκεκριμένο υποκείμενο δεδομένων χωρίς τη χρήση πρόσθετων πληροφοριών,
2. καθένα από τα στοιχεία διαβιβάζεται σε ξεχωριστό εκτελούντα την επεξεργασία που είναι εγκατεστημένος σε διαφορετική δικαιοδοσία,
3. οι εκτελούντες την επεξεργασία επεξεργάζονται προαιρετικά τα δεδομένα από κοινού, π.χ. χρησιμοποιώντας ασφαλή πολυσυμμετοχικό υπολογισμό, με τρόπο που να μην αποκαλύπτονται πληροφορίες σε κανέναν από εκείνους που δεν τα διαθέτουν πριν από τον υπολογισμό,
4. ο αλγόριθμος που χρησιμοποιείται για τον από κοινού υπολογισμό είναι ασφαλής έναντι ενεργών αντιπάλων,
5. ο υπεύθυνος επεξεργασίας έχει διαπιστώσει μέσω διεξοδικής ανάλυσης των εν λόγω δεδομένων, λαμβάνοντας υπόψη τα χαμένα τμήματα πληροφοριών που αναμένεται να διαθέτουν και να χρησιμοποιούν οι δημόσιες αρχές των παραληπτριών χωρών, ότι τα τμήματα δεδομένων προσωπικού χαρακτήρα που διαβιβάζει στους εκτελούντες την επεξεργασία δεν μπορούν να αποδοθούν σε ένα φυσικό πρόσωπο του οποίου η ταυτότητα

έχει εξακριβωθεί ή θα μπορούσε να εξακριβωθεί, ακόμη και αν γίνεται διασταύρωση στοιχείων με τις εν λόγω πληροφορίες,

6. δεν υπάρχουν στοιχεία που να αποδεικνύουν συνεργασία μεταξύ των δημόσιων αρχών που είναι εγκατεστημένες στις αντίστοιχες δικαιοδοσίες όπου είναι εγκατεστημένος καθένας από τους εκτελούντες την επεξεργασία, τα οποία θα τους επέτρεπαν την πρόσβαση σε όλα τα σύνολα δεδομένων προσωπικού χαρακτήρα που διαθέτουν οι εκτελούντες την επεξεργασία και που θα τους επέτρεπαν να προβούν στην ανασύστασή τους και να εκμεταλλευτούν το περιεχόμενο των δεδομένων προσωπικού χαρακτήρα σε σαφή μορφή σε περιπτώσεις όπου η εν λόγω εκμετάλλευση δεν τηρεί την ουσία των θεμελιωδών δικαιωμάτων και ελευθεριών των υποκειμένων των δεδομένων. Ομοίως, οι δημόσιες αρχές οποιασδήποτε εκ των χωρών δεν πρέπει να έχουν την εξουσία πρόσβασης στα δεδομένα προσωπικού χαρακτήρα που διαθέτουν οι εκτελούντες την επεξεργασία σε όλες τις σχετικές δικαιοδοσίες.

τότε το ΕΣΠΔ θεωρεί ότι η επεξεργασία διαχωρισμού που πραγματοποιείται παρέχει ένα αποτελεσματικό πρόσθετο μέτρο.

Παραδείγματα σεναρίων που παραπέμπουν σε υποθέσεις στις οποίες δεν προσδιορίζονται αποτελεσματικά μέτρα

93. Τα μέτρα που περιγράφονται κατωτέρω στο πλαίσιο ορισμένων σεναρίων δεν θα ήταν αποτελεσματικά για τη διασφάλιση ενός ουσιαστικά ισοδύναμου επιπέδου προστασίας για τα δεδομένα που διαβιβάζονται στην τρίτη χώρα. Επομένως, δεν θα μπορούσαν να χαρακτηριστούν ως επαρκή πρόσθετα μέτρα.

Περίπτωση χρήσης 6: Διαβίβαση σε παρόχους υπηρεσιών υπολογιστικού νέφους ή άλλους εκτελούντες την επεξεργασία που απαιτούν αποκωδικοποιημένη πρόσβαση στα δεδομένα

94. Ένας εξαγωγέας δεδομένων διαβιβάζει δεδομένα προσωπικού χαρακτήρα, είτε μέσω ηλεκτρονικής διαβίβασης είτε μέσω της διάθεσής τους σε πάροχο υπηρεσιών υπολογιστικού νέφους ή άλλον εκτελούντα την επεξεργασία, για την επεξεργασία δεδομένων προσωπικού χαρακτήρα σύμφωνα με τις οδηγίες του σε τρίτη χώρα (π.χ. για την παροχή τεχνικής υποστήριξης ή κάθε είδους επεξεργασίας νέφους) και τα εν λόγω δεδομένα δεν είναι ψευδωνυμοποιημένα ούτε μπορούν να ψευδωνυμοποιηθούν όπως περιγράφεται στην περίπτωση χρήσης 2 ή να κρυπτογραφηθούν όπως περιγράφεται στην περίπτωση χρήσης 1 επειδή η επεξεργασία απαιτεί αποκωδικοποιημένη πρόσβαση στα δεδομένα.

Αν

1. ένας υπεύθυνος επεξεργασίας διαβιβάζει δεδομένα προσωπικού χαρακτήρα σε πάροχο υπηρεσιών υπολογιστικού νέφους ή σε άλλον εκτελούντα την επεξεργασία,
2. ο πάροχος υπηρεσιών υπολογιστικού νέφους ή άλλος εκτελών την επεξεργασία χρειάζεται αποκωδικοποιημένη πρόσβαση στα δεδομένα για την εκτέλεση της εργασίας που του έχει ανατεθεί, και
3. η εξουσία που χορηγείται στις δημόσιες αρχές της παραλήπτριας χώρας για την απόκτηση πρόσβασης στα διαβιβαζόμενα δεδομένα υπερβαίνει τα όρια του αναγκαίου και του

αναλογικού σε μια δημοκρατική κοινωνία στην οποία προβληματική νομοθεσία της τρίτης χώρας ισχύει στην πράξη για τις εν λόγω διαβιβάσεις (βλ. βήμα 3).⁸⁶

τότε το ΕΣΠΔ, λαμβάνοντας υπόψη την τρέχουσα εξέλιξη της τεχνολογίας, δεν είναι σε θέση να προβλέψει ένα αποτελεσματικό τεχνικό μέτρο προκειμένου να εμποδίσει την παραβίαση των θεμελιωδών δικαιωμάτων των υποκειμένων των δεδομένων κατά την εν λόγω πρόσβαση. Το ΕΣΠΔ δεν αποκλείει το γεγονός ότι η περαιτέρω τεχνολογική ανάπτυξη μπορεί να προσφέρει μέτρα που επιτυγχάνουν τους επιδιωκόμενους επιχειρηματικούς σκοπούς, χωρίς να απαιτείται αποκωδικοποιημένη πρόσβαση.

95. Στα δεδομένα σενάρια, στις περιπτώσεις που τα μη κρυπτογραφημένα δεδομένα προσωπικού χαρακτήρα είναι απαραίτητα από τεχνικής άποψης για την παροχή της υπηρεσίας από τον εκτελούντα την επεξεργασία, η κρυπτογράφηση της μεταφοράς και η κρυπτογράφηση ήδη αποθηκευμένων δεδομένων ακόμη και αν ληφθούν μαζί υπόψη, δεν αποτελούν πρόσθετο μέτρο που εξασφαλίζει ένα ουσιαστικά ισοδύναμο επίπεδο προστασίας εάν ο εισαγωγέας δεδομένων διαθέτει τα κρυπτογραφικά κλειδιά.

Περίπτωση χρήσης 7: Διαβίβαση δεδομένων προσωπικού χαρακτήρα για επιχειρηματικούς σκοπούς, ακόμα και μέσω απομακρυσμένης πρόσβασης

96. Ένας εξαγωγέας δεδομένων διαβιβάζει δεδομένα προσωπικού χαρακτήρα σε φορείς – σε τρίτη χώρα για να χρησιμοποιηθούν για κοινόχρηστους επιχειρηματικούς σκοπούς – είτε μέσω ηλεκτρονικής διαβίβασης είτε μέσω της διάθεσής τους για απομακρυσμένη πρόσβαση από τον εισαγωγέα δεδομένων – και τα εν λόγω δεδομένα δεν είναι ψευδωνυμοποιημένα ούτε μπορούν να ψευδωνυμοποιηθούν όπως περιγράφεται στην περίπτωση χρήσης 2 ή να κρυπτογραφηθούν όπως περιγράφεται στην περίπτωση χρήσης 1 επειδή η επεξεργασία απαιτεί αποκωδικοποιημένη πρόσβαση στα δεδομένα. Ένα τυπικό δίκτυο μπορεί να αποτελείται από έναν υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία ο οποίος είναι εγκατεστημένος στην επικράτεια κράτους μέλους και που διαβιβάζει δεδομένα προσωπικού χαρακτήρα σε υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία σε τρίτη χώρα, οι οποίοι ανήκουν στον ίδιο όμιλο επιχειρήσεων, ή όμιλο επιχειρήσεων που ασκούν κοινή οικονομική δραστηριότητα. Ο εισαγωγέας δεδομένων μπορεί, για παράδειγμα, να χρησιμοποιήσει τα δεδομένα που λαμβάνει για να παρέχει υπηρεσίες προσωπικού στον εξαγωγέα δεδομένων για τον οποίο χρειάζεται δεδομένα ανθρώπινου δυναμικού ή να επικοινωνήσει με πελάτες του εξαγωγέα δεδομένων που διαμένουν στην Ευρωπαϊκή Ένωση, μέσω τηλεφώνου ή ηλεκτρονικού ταχυδρομείου.

Αν

1. ένας εξαγωγέας δεδομένων διαβιβάζει δεδομένα προσωπικού χαρακτήρα σε εισαγωγέα δεδομένων σε τρίτη χώρα, καθιστώντας τα διαθέσιμα σε ένα σύστημα πληροφοριών με τρόπο που επιτρέπει στον εισαγωγέα άμεση πρόσβαση σε δεδομένα της δικής του επιλογής, ή διαβιβάζοντάς τα απευθείας, μεμονωμένα ή συνολικά, μέσω της χρήσης μιας υπηρεσίας επικοινωνιών,

⁸⁶ Βλ. άρθρα 47 και 52 του Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ, άρθρο 23.1 του ΓΚΠΔ, και συστάσεις 02/2020 του ΕΣΠΔ σχετικά με τις ευρωπαϊκές βασικές εγγυήσεις για τα μέτρα παρακολούθησης, 10 Νοεμβρίου 2020,

2. ο εισαγωγέας⁸⁷ επεξεργάζεται τα δεδομένα σε αποκωδικοποιημένη μορφή στην τρίτη χώρα (και για δικούς του σκοπούς όταν ο εισαγωγέας είναι υπεύθυνος επεξεργασίας),
3. η εξουσία που χορηγείται στις δημόσιες αρχές της παραλήπτριας χώρας για την απόκτηση πρόσβασης στα διαβιβαζόμενα δεδομένα υπερβαίνει τα όρια του αναγκαίου και του αναλογικού σε μια δημοκρατική κοινωνία στην οποία η προβληματική νομοθεσία της τρίτης χώρας ισχύει στην πράξη για τις εν λόγω διαβιβάσεις (βλ. βήμα 3).

τότε το ΕΣΠΔ δεν είναι σε θέση να προβλέψει ένα αποτελεσματικό τεχνικό μέτρο προκειμένου να εμποδίσει την παραβίαση των θεμελιωδών δικαιωμάτων του υποκειμένου των δεδομένων κατά την εν λόγω πρόσβαση.

97. Στα δεδομένα σενάρια, στις περιπτώσεις που τα μη κρυπτογραφημένα δεδομένα προσωπικού χαρακτήρα είναι απαραίτητα από τεχνικής άποψης για την παροχή της υπηρεσίας από τον εκτελούντα την επεξεργασία, η κρυπτογράφηση της μεταφοράς και η κρυπτογράφηση ήδη αποθηκευμένων δεδομένων ακόμη και αν ληφθούν μαζί υπόψη, δεν αποτελούν πρόσθετο μέτρο που εξασφαλίζει ένα ουσιαστικά ισοδύναμο επίπεδο προστασίας εάν ο εισαγωγέας δεδομένων διαθέτει τα κρυπτογραφικά κλειδιά.

⁸⁷ Είτε είναι ο υπεύθυνος επεξεργασίας είτε ο εκτελών την επεξεργασία σε τρίτη χώρα που λαμβάνει ή αποκτά πρόσβαση σε δεδομένα προσωπικού χαρακτήρα που διαβιβάζονται από τον ΕΟΧ.

2.2 Πρόσθετα συμβατικά μέτρα

98. Τα εν λόγω μέτρα θα αποτελούνται εν γένει από μονομερείς, διμερείς ή πολυμερείς⁸⁸ συμβατικές δεσμεύσεις.⁸⁹ Εάν χρησιμοποιείται ένα εργαλείο διαβίβασης του άρθρου 46 του ΓΚΠΔ, στις περισσότερες περιπτώσεις θα περιέχει ήδη ορισμένες (κυρίως συμβατικές) δεσμεύσεις από τον εξαγωγέα δεδομένων και τον εισαγωγέα δεδομένων, οι οποίες στοχεύουν να χρησιμεύσουν ως εγγυήσεις για τα δεδομένα προσωπικού χαρακτήρα.⁹⁰
99. Σε ορισμένες περιπτώσεις, τα εν λόγω μέτρα ενδέχεται να συμπληρώνουν και να ενισχύουν τις εγγυήσεις που μπορεί να παρέχουν το εργαλείο διαβίβασης και η σχετική νομοθεσία της τρίτης χώρας, όταν, λαμβάνοντας υπόψη τις συνθήκες της διαβίβασης, οι τελευταίες δεν πληρούν όλες τις προϋποθέσεις που απαιτούνται για την εξασφάλιση ενός επιπέδου προστασίας ουσιαστικά ισοδύναμου με αυτό που διασφαλίζεται στο εσωτερικό της ΕΟΧ. Λαμβάνοντας υπόψη τη φύση των συμβατικών μέτρων, τα οποία εν γένει δεν είναι ικανά να δεσμεύσουν τις αρχές της εν λόγω τρίτης χώρας, όταν αυτές δεν είναι συμβαλλόμενα μέρη της σύμβασης,⁹¹ τα μέτρα αυτά θα πρέπει να συνδυάζονται με άλλα τεχνικά και οργανωτικά μέτρα για την παροχή του απαιτούμενου επιπέδου προστασίας των δεδομένων. Η επιλογή και η εφαρμογή ενός ή περισσότερων από τα εν λόγω μέτρα δεν διασφαλίζουν απαραίτητα και συστηματικώς ότι η διαβίβασή σας πληροί το ουσιώδες πρότυπο ισοδυναμίας που απαιτεί η νομοθεσία της ΕΕ.
100. Ανάλογα με τα συμβατικά μέτρα που περιλαμβάνονται ήδη στο εργαλείο διαβίβασης του άρθρου 46 του ΓΚΠΔ που χρησιμοποιείται, πρόσθετα συμβατικά μέτρα μπορεί επίσης να είναι χρήσιμα για να επιτρέψουν στους εξαγωγείς δεδομένων που είναι εγκατεστημένοι εντός του ΕΟΧ να παρακολουθούν νέες εξελίξεις που επηρεάζουν την προστασία των δεδομένων που διαβιβάζονται σε τρίτες χώρες
101. Όπως ειπώθηκε, τα συμβατικά μέτρα δεν θα μπορούν να αποκλείσουν την εφαρμογή της νομοθεσίας τρίτης χώρας που δεν πληροί το πρότυπο των ευρωπαϊκών βασικών εγγυήσεων του ΕΣΠΔ στις περιπτώσεις στις οποίες η νομοθεσία υποχρεώνει τους εισαγωγείς να συμμορφωθούν με τις εντολές γνωστοποίησης των δεδομένων που λαμβάνουν από δημόσιες αρχές.⁹²
102. Μερικά παραδείγματα των εν λόγω πιθανών συμβατικών μέτρων παρατίθενται κατωτέρω και ταξινομούνται ανάλογα με τη φύση τους.

⁸⁸ Π.χ. στο πλαίσιο ΔΕΚ που θα πρέπει σε κάθε περίπτωση να ρυθμίζουν ορισμένα από τα μέτρα που παρατίθενται κατωτέρω.

⁸⁹ Θα είναι προσωπικού χαρακτήρα και δεν θα θεωρούνται διεθνείς συμφωνίες βάσει του δημόσιου διεθνούς δικαίου. Συνεπώς, συνήθως δεν θα μπορούν να δεσμεύσουν τη δημόσια αρχή της τρίτης χώρας ως μη συμβαλλόμενα μέρη της σύμβασης όταν αυτή έχει συναφθεί με ιδιωτικούς φορείς σε τρίτες χώρες, όπως υπογράμμισε το Δικαστήριο στην απόφασή του C-311/18 (Schrems II), σκέψη 125.

⁹⁰ Βλ. απόφαση C-311/18 (Schrems II), σκέψη 137 όπου το Δικαστήριο συνεπώς αναγνώρισε ότι οι ΤΣΡ περιλαμβάνουν «αποτελεσματικούς μηχανισμούς που να διασφαλίζουν, στην πράξη, ότι τηρείται το απαιτούμενο από το δίκαιο της Ένωσης επίπεδο προστασίας και ότι οι διαβιβάσεις δεδομένων προσωπικού χαρακτήρα βάσει τέτοιων ρητρών αναστέλλονται ή απαγορεύονται σε περίπτωση παράβασης των ρητρών αυτών ή αδυναμίας τήρησής τους»: βλ. επίσης σκέψη 148).

⁹¹ C-311/18 (Schrems II), σκέψη 125.

⁹² ΔΕΕ, απόφαση C-311/18 (Schrems II), σκέψη 132.

Πρόβλεψη για συμβατική υποχρέωση χρήσης ειδικών τεχνικών μέτρων

103. Ανάλογα με τις ειδικές συνθήκες των διαβιβάσεων (συμπεριλαμβανομένης της πρακτικής εφαρμογής της νομοθεσίας της τρίτης χώρας), η σύμβαση ενδέχεται να χρειαστεί να προβλέπει ότι για τη διαβίβαση θα πρέπει να εφαρμοστούν συγκεκριμένα τεχνικά μέτρα (βλ. ανωτέρω τα προτεινόμενα τεχνικά μέτρα).

104. Προϋποθέσεις αποτελεσματικότητας:

- Αυτή η ρήτρα θα μπορούσε να παράγει έννομα αποτελέσματα σε περιπτώσεις όπου ο εξαγωγέας έχει επισημάνει την ανάγκη λήψης τεχνικών μέτρων. Στη συνέχεια, θα πρέπει να παρέχεται σε νομική μορφή για να διασφαλίζεται ότι ο εισαγωγέας δεσμεύεται επίσης να εφαρμόσει τα απαραίτητα τεχνικά μέτρα, εάν χρειαστεί.

Υποχρεώσεις διαφάνειας:

105. Ο εξαγωγέας θα μπορούσε να προσθέσει στη σύμβαση παραρτήματα με πληροφορίες που θα έχει παράσχει ο εισαγωγέας πριν από τη σύναψη της σύμβασης, με τη μέγιστη δυνατή επιμέλεια, όσον αφορά την πρόσβαση των δημόσιων αρχών στα δεδομένα, μεταξύ άλλων στον τομέα των πληροφοριών εφόσον η νομοθεσία συμμορφώνεται με τις ευρωπαϊκές βασικές εγγυήσεις του ΕΣΠΔ, στη χώρα προορισμού. Αυτό μπορεί να βοηθήσει τον εξαγωγέα δεδομένων να εκπληρώσει την υποχρέωσή του να τεκμηριώσει την αξιολόγησή του σχετικά με το επίπεδο προστασίας στην τρίτη χώρα. Μπορεί επίσης να τονίσει την υποχρέωση του εισαγωγέα να υποστηρίξει τον εξαγωγέα στην αξιολόγησή του και να θέσει ζήτημα ευθύνης του για την παροχή πληροφοριών που είναι αντικειμενικές, αξιόπιστες, συναφείς, επαληθεύσιμες και δημοσιώς διαθέσιμες ή με άλλο τρόπο προσβάσιμες.

106. Θα μπορούσε για παράδειγμα να απαιτηθεί από τον εισαγωγέα:

(1) να απαριθμήσει τους νόμους και τους κανονισμούς της χώρας προορισμού που ισχύουν για τον εισαγωγέα ή τους υπεργολάβους επεξεργασίας/εκτελούντες την επεξεργασία και που θα επέτρεπαν την πρόσβαση των δημόσιων αρχών σε δεδομένα προσωπικού χαρακτήρα που υπόκεινται στη διαβίβαση, ιδίως στον τομέα των πληροφοριών, της επιβολής του νόμου, της διοικητικής και κανονιστικής εποπτείας που ισχύει για τα διαβιβαζόμενα δεδομένα·

(2) ελλείψει νόμων που διέπουν την πρόσβαση των δημόσιων αρχών στα δεδομένα, να παρέχει πληροφορίες και στατιστικά στοιχεία βάσει της εμπειρίας του εισαγωγέα ή αναφορές από διάφορες πηγές (π.χ. συνεργάτες, πηγές ελεύθερης πρόσβασης, εθνική νομολογία και αποφάσεις από όργανα εποπτείας) σχετικά με την πρόσβαση των δημόσιων αρχών σε δεδομένα προσωπικού χαρακτήρα σε καταστάσεις της εκάστοτε διαβίβασης δεδομένων (δηλαδή στον ειδικό ρυθμιστικό τομέα· σχετικά με τον τύπο των οντοτήτων στις οποίες ανήκει ο εισαγωγέας δεδομένων...), κ.λπ.

(3) να αναφέρει ποια μέτρα λαμβάνονται για την αποτροπή της πρόσβασης στα διαβιβαζόμενα δεδομένα (εάν υπάρχουν)·

(4) να παρέχει επαρκώς λεπτομερείς πληροφορίες σχετικά με όλα τα αιτήματα πρόσβασης σε δεδομένα προσωπικού χαρακτήρα από δημόσιες αρχές, τα οποία ο εισαγωγέας έχει

λάβει εντός ορισμένου χρονικού διαστήματος,⁹³ ιδίως στους τομείς που αναφέρονται στο σημείο (1) ανωτέρω και περιλαμβάνουν πληροφορίες σχετικά με τα ληφθέντα αιτήματα, τα δεδομένα που ζητήθηκαν, τον αιτούντα φορέα και τη νομική βάση για τη γνωστοποίηση, καθώς και σε ποιο βαθμό ο εισαγωγέας έχει γνωστοποιήσει το αίτημα υποβολής δεδομένων.⁹⁴

(5) να διευκρινίζει αν και σε ποιο βαθμό απαγορεύεται εκ του νόμου στον εισαγωγέα να παρέχει τις πληροφορίες που αναφέρονται στα σημεία (1) – (5) ανωτέρω.

107. Οι εν λόγω πληροφορίες θα μπορούσαν να παρασχεθούν μέσω δομημένων ερωτηματολογίων που θα συμπληρώνει και θα υπογράφει ο εισαγωγέας, τα οποία συνοδεύονται με τη συμβατική υποχρέωση του εισαγωγέα να δηλώνει εντός καθορισμένου χρονικού διαστήματος οποιαδήποτε πιθανή αλλαγή σε αυτές τις πληροφορίες, σύμφωνα με την τρέχουσα πρακτική για τις διαδικασίες δέουσας επιμέλειας.

108. Προϋποθέσεις αποτελεσματικότητας:

- Ο εισαγωγέας πρέπει να είναι σε θέση να παρέχει στον εξαγωγέα αυτού του είδους τις πληροφορίες εξ όσων γνωρίζει και αφού έχει καταβάλει κάθε δυνατή προσπάθεια για να τις αποκτήσει.
- Η εν λόγω υποχρέωση που επιβάλλεται στον εισαγωγέα αποτελεί ένα μέσο διασφάλισης ότι ο εξαγωγέας θα ενημερωθεί και θα παραμένει ενήμερος για τους κινδύνους που συνδέονται με τη διαβίβαση δεδομένων σε τρίτη χώρα. Θα επιτρέψει ως εκ τούτου στον εξαγωγέα να απόσχει από τη σύναψη της σύμβασης, ή εάν οι πληροφορίες αλλάξουν μετά τη σύναψή της, να εκπληρώσει την υποχρέωσή του να αναστείλει τη διαβίβαση ή/και να καταγγείλει τη σύμβαση εάν το δίκαιο της τρίτης χώρας, οι εγγυήσεις που περιλαμβάνονται στο εργαλείο διαβίβασης του άρθρου 46 του ΓΚΠΔ που χρησιμοποιείται και τυχόν πρόσθετες εγγυήσεις που μπορεί να εφαρμόζει δεν μπορούν πλέον να διασφαλίσουν ένα επίπεδο προστασίας ουσιαστικά ισοδύναμο με αυτό που διασφαλίζεται εντός της ΕΟΧ. Ωστόσο, η εν λόγω υποχρέωση δεν μπορεί να δικαιολογήσει τη γνωστοποίηση δεδομένων προσωπικού χαρακτήρα του εισαγωγέα ούτε να δημιουργήσει την προσδοκία ότι δεν θα υπάρξουν περαιτέρω αιτήματα πρόσβασης.

109. Ο εξαγωγέας θα μπορούσε επίσης να προσθέσει ρήτρες σύμφωνα με τις οποίες ο εισαγωγέας πιστοποιεί ότι (1) δεν έχει δημιουργήσει σκόπιμα κερκόπορτες (back doors) ή παρόμοια προγράμματα που θα μπορούσαν να χρησιμοποιηθούν για την πρόσβαση στο σύστημα ή και σε δεδομένα προσωπικού χαρακτήρα, (2) δεν έχει δημιουργήσει ή τροποποιήσει σκόπιμα τις επιχειρηματικές του διαδικασίες με τρόπο που διευκολύνει την πρόσβαση σε δεδομένα

⁹³ Η διάρκεια της περιόδου θα πρέπει να εξαρτάται από τον κίνδυνο για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων των οποίων τα δεδομένα υπόκεινται στην υπό εξέταση διαβίβαση – π.χ. το τελευταίο έτος πριν από το κλείσιμο του εργαλείου εξαγωγής δεδομένων με τον εξαγωγέα δεδομένων.

⁹⁴ Η συμμόρφωση με αυτό το καθήκον δεν ισοδυναμεί από μόνη της με την εξασφάλιση κατάλληλου επιπέδου προστασίας. Ταυτόχρονα, κάθε ακατάλληλη γνωστοποίηση που έχει συμβεί στην πραγματικότητα οδηγεί στην ανάγκη εφαρμογής πρόσθετων μέτρων.

προσωπικού χαρακτήρα ή συστήματα, και (3) η εθνική νομοθεσία ή η κυβερνητική πολιτική δεν απαιτεί από τον εισαγωγέα να δημιουργήσει ή να διατηρήσει κερκόπορτες ή να διευκολύνει την πρόσβαση σε δεδομένα προσωπικού χαρακτήρα ή συστήματα ή να έχει ο εισαγωγέας στην κατοχή του ή να παραδώσει το κλειδί κρυπτογράφησης.⁹⁵

110. Προϋποθέσεις αποτελεσματικότητας:

- Η ύπαρξη νομοθεσίας ή κυβερνητικών πολιτικών που εμποδίζουν τους εισαγωγείς να γνωστοποιούν τις εν λόγω πληροφορίες μπορεί να καταστήσει αυτή τη ρήτρα αναποτελεσματική. Ο εισαγωγέας δεν θα είναι επομένως σε θέση να συνάψει σύμβαση ή θα πρέπει να γνωστοποιήσει στον εξαγωγέα την αδυναμία του να εξακολουθήσει να συμμορφώνεται με τις συμβατικές δεσμεύσεις του.
- Η σύμβαση πρέπει να περιλαμβάνει κυρώσεις ή/και τη δυνατότητα για τον εξαγωγέα να καταγγείλει τη σύμβαση εντός σύντομου χρονικού διαστήματος στις περιπτώσεις στις οποίες ο εισαγωγέας δεν αποκαλύπτει την ύπαρξη κερκόπορτας ή παρόμοιου προγράμματος ή χειραγωγούμενων επιχειρηματικών διαδικασιών ή οποιασδήποτε απαίτησης για την εφαρμογή οποιουδήποτε εκ των ανωτέρω ή δεν ενημερώσει τον εξαγωγέα αμέσως μόλις λάβει σχετική γνώση.
- Στις περιπτώσεις στις οποίες ο εισαγωγέας δεδομένων γνωστοποίησε διαβιβασθέντα δεδομένα προσωπικού χαρακτήρα κατά παράβαση των δεσμεύσεων που περιέχονται στο επιλεγμένο εργαλείο διαβίβασης, η σύμβαση μπορεί επίσης να περιλαμβάνει αποζημίωση από τον εισαγωγέα δεδομένων σε ένα υποκείμενο δεδομένων για κάθε ουσιώδη και μη ουσιώδη ζημία που θα υποστεί.

111. Ο εξαγωγέας θα μπορούσε να ενισχύσει την εξουσία του να διενεργεί ελέγχους⁹⁶ ή επιθεωρήσεις των εγκαταστάσεων επεξεργασίας δεδομένων του εισαγωγέα, επί τόπου ή/και εξ αποστάσεως, για να επαληθεύει αν γνωστοποιήθηκαν δεδομένα στις δημόσιες αρχές και υπό ποιες προϋποθέσεις (πρόσβαση που δεν υπερβαίνει τα όρια του αναγκαίου και του αναλογικού σε μια δημοκρατική κοινωνία), για παράδειγμα με την παροχή έγκαιρης προειδοποίησης και μηχανισμών που διασφαλίζουν την ταχεία παρέμβαση φορέων ελέγχου και την ενίσχυση της αυτονομίας του εξαγωγέα κατά την επιλογή των φορέων ελέγχου.

112. Προϋποθέσεις αποτελεσματικότητας:

- Το αντικείμενο του ελέγχου θα πρέπει να καλύπτει από νομικής και τεχνικής άποψης οποιαδήποτε επεξεργασία πραγματοποιείται από τους εκτελούντες την επεξεργασία ή τους υπεργολάβους επεξεργασίας του εισαγωγέα των δεδομένων προσωπικού χαρακτήρα που διαβιβάζονται στην τρίτη χώρα για να είναι πλήρως αποτελεσματικό.
- Τα αρχεία καταγραφής πρόσβασης και άλλα παρόμοια ίχνη θα πρέπει να είναι απαραβίαστα [π.χ. θα πρέπει να καθίστανται αναλλοίωτα με τη χρήση προηγμένων τεχνικών

⁹⁵ Η εν λόγω ρήτρα είναι σημαντική για την εξασφάλιση επαρκούς επιπέδου προστασίας των δεδομένων προσωπικού χαρακτήρα που διαβιβάζονται και συνήθως θα πρέπει να απαιτείται.

⁹⁶ Βλ., για παράδειγμα, ρήτρα 5 στοιχείο στ) των ΤΣΡ μεταξύ υπεύθυνων επεξεργασίας και εκτελούντων την επεξεργασία, απόφαση 2010/87/ΕΕ, οι έλεγχοι θα μπορούσαν επίσης να παρέχονται σε έναν κώδικα δεοντολογίας ή μέσω πιστοποίησης.

κρυπτογράφησης όπως κλείδωμα (hashing) και επίσης να διαβιβάζονται συστηματικά στον εξαγωγέα σε περιοδική βάση], έτσι ώστε οι ελεγκτές να μπορούν να βρουν αποδεικτικά στοιχεία γνωστοποίησης Τα αρχεία καταγραφής πρόσβασης και άλλα παρόμοια ίχνη θα πρέπει επίσης να κάνουν τη διάκριση μεταξύ της πρόσβασης λόγω τακτικών επιχειρησιακών δραστηριοτήτων και της πρόσβασης λόγω εντολών ή αιτημάτων πρόσβασης.

113. Όταν η νομοθεσία και η πρακτική της τρίτης χώρας του εισαγωγέα αρχικά έχουν αξιολογηθεί και έχει κριθεί ότι παρέχουν ένα ουσιαστικά ισοδύναμο επίπεδο προστασίας, όπως προβλέπεται στην ΕΕ για δεδομένα που διαβιβάζονται από τον εξαγωγέα, ο εξαγωγέας εξακολουθεί να μπορεί να ενισχύει την υποχρέωση του εισαγωγέα δεδομένων, σε περίπτωση αλλαγής της κατάστασης, να ενημερώνει άμεσα τον εξαγωγέα δεδομένων σχετικά με την αδυναμία του να συμμορφωθεί με τις συμβατικές δεσμεύσεις και, ως εκ τούτου, με το απαιτούμενο πρότυπο «ουσιαστικά ισοδύναμου επιπέδου προστασίας δεδομένων».⁹⁷
114. Αυτή η αδυναμία συμμόρφωσης μπορεί να προκύψει από αλλαγές στη νομοθεσία ή την πρακτική της τρίτης χώρας.⁹⁸ Οι ρήτρες θα μπορούσαν να ορίζουν συγκεκριμένες και αυστηρές προθεσμίες και διαδικασίες για την ταχεία αναστολή της διαβίβασης δεδομένων ή/και την καταγγελία της σύμβασης και την επιστροφή ή τη διαγραφή των δεδομένων που ελήφθησαν από τον εισαγωγέα. Η παρακολούθηση των αιτημάτων που λαμβάνονται, του αντικειμένου τους και της αποτελεσματικότητας των μέτρων που λαμβάνονται για την αντιμετώπισή τους, πρέπει να παρέχει στον εξαγωγέα επαρκείς ενδείξεις για να ασκήσει το καθήκον της αναστολής ή του τερματισμού της διαβίβασης ή/και της καταγγελίας της σύμβασης.
115. Προϋποθέσεις αποτελεσματικότητας:
- Η ειδοποίηση πρέπει να πραγματοποιηθεί πριν από την πρόσβαση στα δεδομένα. Διαφορετικά, τη στιγμή που ο εξαγωγέας θα λάβει την ειδοποίηση, τα δικαιώματα του ατόμου ενδέχεται να έχουν ήδη παραβιαστεί εάν το αίτημα βασίζεται σε νόμους της εν λόγω τρίτης χώρας, οι οποίοι υπερβαίνουν αυτό που επιτρέπει το επίπεδο προστασίας των δεδομένων που παρέχεται βάσει της νομοθεσίας της ΕΕ. Η ειδοποίηση μπορεί να εξακολουθήσει να χρησιμεύει για την αποτροπή μελλοντικών παραβιάσεων και για να επιτρέπει στον εξαγωγέα να εκπληρώσει το καθήκον αναστολής της διαβίβασης δεδομένων προσωπικού χαρακτήρα στην τρίτη χώρα ή/και καταγγελίας της σύμβασης.
 - Ο εισαγωγέας δεδομένων πρέπει να παρακολουθεί τυχόν νομικές ή πολιτικές εξελίξεις που ενδέχεται να οδηγήσουν στην αδυναμία του να συμμορφωθεί με τις υποχρεώσεις του, και να ενημερώσει αμέσως τον εξαγωγέα των δεδομένων για τυχόν τέτοιες αλλαγές και εξελίξεις,

⁹⁷ Ρήτρα 5 στοιχείο α) και στοιχείο δ) σημείο i) των ΤΣΡ, απόφαση 2010/87/ΕΕ.

⁹⁸ Βλ. C-311/18 (Schrems II), σκέψη 139 στην οποία το Δικαστήριο υποστήριξε ότι «μολονότι η ρήτρα 5, στοιχείο δ) σημείο i), επιτρέπει στον αποδέκτη των δεδομένων προσωπικού χαρακτήρα να μην γνωστοποιήσει στον εγκατεστημένο εντός της Ένωσης υπεύθυνο επεξεργασίας ένα νομικώς δεσμευτικό αίτημα κοινοποίησης δεδομένων προσωπικού χαρακτήρα που υποβάλλεται από αρχή επιβολής του νόμου, εντούτοις ο αποδέκτης οφείλει, δυνάμει της ρήτρας 5, στοιχείο α) του παραρτήματος της αποφάσεως ΤΣΡ να ενημερώσει τον υπεύθυνο επεξεργασίας για την αδυναμία του να συμμορφωθεί με τις τυποποιημένες ρήτρες προστασίας δεδομένων.»

και, εάν είναι δυνατόν, πριν από την εφαρμογή τους, ώστε ο εξαγωγέας των δεδομένων να είναι σε θέση να ανακτήσει τα δεδομένα από τον εισαγωγέα δεδομένων.

- Οι ρήτρες θα πρέπει να προβλέπουν έναν γρήγορο μηχανισμό μέσω του οποίου ο εξαγωγέας των δεδομένων επιτρέπει στον εισαγωγέα των δεδομένων να εγγυηθεί αμέσως την ασφάλεια των δεδομένων ή να επιστρέψει τα δεδομένα στον εξαγωγέα των δεδομένων ή, εάν αυτό δεν είναι εφικτό, να διαγράψει ή να κρυπτογραφήσει με ασφάλεια τα δεδομένα χωρίς να αναμένει απαραίτητα τις οδηγίες του εξαγωγέα, εάν πληρούνται ένα ειδικό όριο⁹⁹ που πρέπει να συμφωνηθεί μεταξύ του εξαγωγέα των δεδομένων και του εισαγωγέα των δεδομένων. Ο εισαγωγέας θα πρέπει να εφαρμόζει αυτόν τον μηχανισμό από την αρχή της διαβίβασης δεδομένων και να τον ελέγχει τακτικά για να διασφαλίσει ότι μπορεί να εφαρμοστεί εντός σύντομου χρονικού διαστήματος.
- Άλλες ρήτρες θα μπορούσαν να επιτρέψουν στον εξαγωγέα να παρακολουθήσει τη συμμόρφωση του εισαγωγέα με τις εν λόγω υποχρεώσεις μέσω ελέγχων, επιθεωρήσεων και άλλων μέτρων επαλήθευσης και να τις επιβάλει μέσω κυρώσεων στον εισαγωγέα ή/και την ικανότητα του εξαγωγέα να αναστείλει τη διαβίβαση ή/και να καταγγείλει αμέσως τη σύμβαση.

116. Στο μέτρο που επιτρέπεται από την εθνική νομοθεσία στην τρίτη χώρα, η σύμβαση θα μπορούσε να ενισχύσει τις υποχρεώσεις διαφάνειας του εισαγωγέα, προβλέποντας τη μέθοδο «Warrant Canary», σύμφωνα με την οποία ο εισαγωγέας δεσμεύεται να δημοσιεύει τακτικά (π.χ. τουλάχιστον κάθε 24 ώρες) ένα κρυπτογραφικά υπογεγραμμένο μήνυμα με το οποίο ενημερώνει τον εξαγωγέα ότι μετά από μια συγκεκριμένη ημερομηνία και ώρα δεν έχει λάβει καμία εντολή γνωστοποίησης δεδομένων προσωπικού χαρακτήρα ή παρόμοια. Η απουσία επικαιροποίησης της εν λόγω ειδοποίησης θα αποτελεί ένδειξη για τον εξαγωγέα ότι ο εισαγωγέας ενδέχεται να έχει λάβει μια εντολή.

117. Προϋποθέσεις αποτελεσματικότητας:

- Οι κανονισμοί της τρίτης χώρας πρέπει να επιτρέπουν στον εισαγωγέα δεδομένων να εκδίδει αυτή τη μορφή παθητικής ειδοποίησης στον εξαγωγέα.
- Ο εξαγωγέας δεδομένων πρέπει να παρακολουθεί αυτόματα τις ειδοποιήσεις Warrant Canary.
- Ο εισαγωγέας δεδομένων πρέπει να διασφαλίζει ότι το ιδιωτικό κλειδί για την υπογραφή της Warrant Canary διατηρείται ασφαλές και ότι δεν μπορεί να αναγκαστεί να εκδώσει ψευδείς Warrant Canaries με βάση τους κανονισμούς της τρίτης χώρας. Για τον σκοπό αυτό, μπορεί να είναι χρήσιμο να απαιτούνται πολλές υπογραφές από διαφορετικά άτομα ή/και η Warrant Canary να εκδίδεται από άτομο εκτός της δικαιοδοσίας της τρίτης χώρας.

⁹⁹ Αυτό το όριο θα πρέπει να διασφαλίζει ότι τα υποκείμενα των δεδομένων συνεχίζουν να απολαύουν ενός επιπέδου προστασίας ισοδύναμου με εκείνο που διασφαλίζεται εντός του ΕΟΧ.

Υποχρεώσεις για τη λήψη συγκεκριμένων μέτρων

118. Ο εισαγωγέας θα μπορούσε να δεσμευτεί να επανεξετάσει, σύμφωνα με το δίκαιο της χώρας προορισμού, τη νομιμότητα οποιασδήποτε εντολής για τη γνωστοποίηση δεδομένων, ιδίως εάν παραμένει στο πλαίσιο των εξουσιών που παραχωρούνται στην αιτούσα δημόσια αρχή, και να αμφισβητήσει την εντολή εάν, κατόπιν προσεκτικής αξιολόγησης, καταλήξει στο συμπέρασμα ότι υφίστανται λόγοι βάσει της νομοθεσίας της χώρας προορισμού να το πράξει. Κατά την αμφισβήτηση μιας εντολής, ο εισαγωγέας δεδομένων θα πρέπει να εφαρμόσει προσωρινά μέτρα για την αναστολή των αποτελεσμάτων της εντολής έως ότου το δικαστήριο αποφασίσει επί της ουσίας. Ο εισαγωγέας θα έχει την υποχρέωση να μην αποκαλύπτει τα δεδομένα προσωπικού χαρακτήρα που ζητούνται έως ότου απαιτηθεί να το πράξει σύμφωνα με τους ισχύοντες κανόνες εφαρμογής. Ο εισαγωγέας δεδομένων θα μπορούσε επίσης να δεσμευτεί να παρέχει τις ελάχιστες επιτρεπόμενες πληροφορίες κατά την απάντηση στην εντολή, βάσει μιας εύλογης ερμηνείας της εντολής.

119. Προϋποθέσεις αποτελεσματικότητας:

- Η έννομη τάξη της τρίτης χώρας πρέπει να προσφέρει αποτελεσματικές νομικές οδούς για την αμφισβήτηση εντολών γνωστοποίησης δεδομένων.
- Αυτή η ρήτρα θα προσφέρει πάντα μια εξαιρετικά περιορισμένη πρόσθετη προστασία, καθώς η εντολή γνωστοποίησης δεδομένων μπορεί να είναι νόμιμη σύμφωνα με την έννομη τάξη της τρίτης χώρας, αλλά η εν λόγω έννομη τάξη ενδέχεται να μην πληροί τα πρότυπα της ΕΕ. Αυτό το συμβατικό μέτρο θα πρέπει απαραίτητα να είναι συμπληρωματικό άλλων πρόσθετων μέτρων.
- Οι προσφυγές κατά των εντολών πρέπει να έχουν ανασταλτικό αποτέλεσμα σύμφωνα με το δίκαιο της τρίτης χώρας. Διαφορετικά, οι δημόσιες αρχές θα εξακολουθήσουν να έχουν πρόσβαση στα δεδομένα των ατόμων και οποιαδήποτε επακόλουθη ενέργεια υπέρ συγκεκριμένου ατόμου θα έχει το περιορισμένο αποτέλεσμα να του επιτρέπει να απαιτήσει αποζημιώσεις για αρνητικές συνέπειες που προκύπτουν από τη γνωστοποίηση των δεδομένων.
- Ο εισαγωγέας θα πρέπει να είναι σε θέση να τεκμηριώνει και να αποδεικνύει στον εξαγωγέα τα μέτρα που έχει λάβει, καταβάλλοντας κάθε δυνατή προσπάθεια για την εκπλήρωση της εν λόγω δέσμευσης.

120. Στην ίδια κατάσταση όπως αυτή που περιγράφεται ανωτέρω, ο εισαγωγέας θα μπορούσε να δεσμευτεί να ενημερώσει την αιτούσα δημόσια αρχή για την ασυμβατότητα της εντολής με τις εγγυήσεις που περιλαμβάνονται στο εργαλείο διαβίβασης του άρθρου 46 του ΓΚΠΔ¹⁰⁰ και την επακόλουθη σύγκρουση υποχρεώσεων για τον εισαγωγέα. Ο εισαγωγέας θα ειδοποιεί

¹⁰⁰ Για παράδειγμα, οι ΤΣΡ προβλέπουν ότι η επεξεργασία δεδομένων, συμπεριλαμβανομένης της διαβίβασής τους, πραγματοποιείται και θα εξακολουθήσει να πραγματοποιείται σύμφωνα με την «ισχύουσα νομοθεσία για την προστασία των δεδομένων». Ο νόμος αυτός ορίζεται ως «η νομοθεσία που προστατεύει τα θεμελιώδη δικαιώματα και ελευθερίες των ατόμων, και ιδίως το δικαίωμα προστασίας της ιδιωτικής τους ζωής από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, η οποία εφαρμόζεται σε υπεύθυνο επεξεργασίας δεδομένων στο κράτος μέλος στο οποίο είναι εγκατεστημένος ο εξαγωγέας δεδομένων». Το ΔΕΕ επιβεβαιώνει ότι οι διατάξεις του ΓΚΠΔ, ερμηνευόμενες υπό το πρίσμα του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, αποτελούν μέρος αυτής της νομοθεσίας, βλ. ΔΕΕ C-311/18 (Schrems II), σκέψη 138.

ταυτόχρονα και το συντομότερο δυνατό τον εξαγωγέα ή/και την αρμόδια εποπτική αρχή από τον ΕΟΧ, στο μέτρο του δυνατού βάσει της έννομης τάξης της τρίτης χώρας.

121. Προϋποθέσεις αποτελεσματικότητας:

- Οι εν λόγω πληροφορίες σχετικά με την προστασία που παρέχει το δίκαιο της ΕΕ και τη σύγκρουση υποχρεώσεων θα πρέπει να έχουν κάποια νομική επίπτωση στην έννομη τάξη της τρίτης χώρας, όπως δικαστικό ή διοικητικό έλεγχο της εντολής ή αίτημα πρόσβασης, απαίτηση έκδοσης δικαστικού εντάλματος, ή/και προσωρινή αναστολή της εντολής για την ενίσχυση της προστασίας των δεδομένων.
- Το νομικό σύστημα της χώρας δεν πρέπει να εμποδίζει τον εισαγωγέα να ειδοποιεί τον εξαγωγέα ή τουλάχιστον την αρμόδια εποπτική αρχή από τον ΕΟΧ για την εντολή ή το αίτημα πρόσβασης που έχει ληφθεί.
- Ο εισαγωγέας θα πρέπει να είναι σε θέση να τεκμηριώνει και να αποδεικνύει στον εξαγωγέα τα μέτρα που έχει λάβει, καταβάλλοντας κάθε δυνατή προσπάθεια για την εκπλήρωση της εν λόγω δέσμευσης.

Ενίσχυση των υποκειμένων των δεδομένων για την άσκηση των δικαιωμάτων τους

122. Η σύμβαση θα μπορούσε να προβλέπει ότι τα δεδομένα προσωπικού χαρακτήρα που διαβιβάζονται με τη μορφή απλού κειμένου στο πλαίσιο της κανονικής δραστηριότητας (συμπεριλαμβανομένων των περιπτώσεων υποστήριξης) μπορούν να προσπελαστούν μόνο με τη ρητή ή σιωπηρή συγκατάθεση του εξαγωγέα ή/και του υποκειμένου των δεδομένων για συγκεκριμένη πρόσβαση στα δεδομένα.

123. Προϋποθέσεις αποτελεσματικότητας:

- Αυτή η ρήτρα θα μπορούσε να είναι αποτελεσματική σε περιπτώσεις στις οποίες οι εισαγωγείς λαμβάνουν αιτήματα από δημόσιες αρχές για συνεργασία σε εθελοντική βάση, σε αντίθεση π.χ. με την πρόσβαση δημόσιων αρχών σε δεδομένα, η οποία πραγματοποιείται χωρίς τη γνώση του εισαγωγέα δεδομένων ή παρά τη θέλησή του.
- Σε ορισμένες περιπτώσεις, το υποκείμενο των δεδομένων ενδέχεται να μην είναι σε θέση να αντιταχθεί στην πρόσβαση ή να παράσχει μια συναίνεση που πληροί όλες τις προϋποθέσεις που ορίζονται δυνάμει του δικαίου της ΕΕ (ελεύθερη, επί συγκεκριμένου θέματος, κατόπιν ενημέρωσης και σαφής συναίνεση) (π.χ. στην περίπτωση των εργαζομένων).¹⁰¹
- Οι εθνικοί κανονισμοί ή πολιτικές που υποχρεώνουν τον εισαγωγέα να μην αποκαλύψει την εντολή πρόσβασης ενδέχεται να καταστήσουν την παρούσα ρήτρα αναποτελεσματική, εκτός εάν μπορεί να υποστηριχθεί από τεχνικές μεθόδους που απαιτούν την παρέμβαση του εξαγωγέα ή του υποκειμένου των δεδομένων για την πρόσβαση στα δεδομένα υπό μορφή απλού κειμένου. Παρόμοια τεχνικά μέτρα για τον περιορισμό της πρόσβασης θα πρέπει να προβλέπονται, ιδίως εάν η πρόσβαση παρέχεται μόνο σε συγκεκριμένες περιπτώσεις υποστήριξης ή παροχής υπηρεσίας, αλλά τα ίδια τα δεδομένα αποθηκεύονται στον ΕΟΧ.

¹⁰¹ Άρθρο 4 παράγραφος 11 του ΓΚΠΔ.

124. Η σύμβαση θα μπορούσε να υποχρεώσει τον εισαγωγέα ή/και τον εξαγωγέα να ενημερώσει αμέσως το υποκείμενο των δεδομένων σχετικά με το αίτημα ή την εντολή που έλαβε από τις δημόσιες αρχές της τρίτης χώρας ή για την αδυναμία του εισαγωγέα να συμμορφωθεί με τις συμβατικές δεσμεύσεις, ώστε να επιτρέψει στο υποκείμενο των δεδομένων να αναζητήσει πληροφορίες και αποτελεσματική έννομη προστασία (π.χ. υποβάλλοντας καταγγελία στην αρμόδια εποπτική αρχή ή/και δικαστική αρχή και προσφεύγοντας στα δικαστήρια της τρίτης χώρας), συμπεριλαμβανομένης της αποζημίωσης από τον εισαγωγέα δεδομένων για κάθε ουσιώδη και μη ουσιώδη ζημία που υπέστη λόγω της κοινολόγησης των διαβιβασθέντων οικείων δεδομένων προσωπικού χαρακτήρα στο πλαίσιο του επιλεγμένου εργαλείου διαβίβασης κατά παράβαση των δεσμεύσεων που περιέχει.

125. Προϋποθέσεις αποτελεσματικότητας:

- Η εν λόγω γνωστοποίηση θα μπορούσε να ειδοποιεί το υποκείμενο των δεδομένων σε περίπτωση ενδεχόμενης πρόσβασης από δημόσιες αρχές τρίτων χωρών στα δεδομένα του/της. Θα μπορούσε συνεπώς να επιτρέψει στο υποκείμενο των δεδομένων να ζητήσει πρόσθετες πληροφορίες από τους εξαγωγείς και να ασκήσει αγωγή ενώπιον της αρμόδιας εποπτικής αρχής του/της. Αυτή η ρήτρα θα μπορούσε επίσης να εξετάσει ορισμένες από τις δυσκολίες που μπορεί να αντιμετωπίσει ένα άτομο κατά την άσκηση προσφυγής (έννομο συμφέρον) ενώπιον δικαστηρίων τρίτων χωρών καταγγέλλοντας την πρόσβαση των δημόσιων αρχών στα δεδομένα του/της.
- Οι εθνικοί κανονισμοί και πολιτικές ενδέχεται να παρεμποδίσουν την εν λόγω ειδοποίηση προς το υποκείμενο των δεδομένων. Ωστόσο, ο εξαγωγέας και ο εισαγωγέας θα μπορούσαν να δεσμευτούν να ενημερώσουν το υποκείμενο των δεδομένων αμέσως μετά την άρση των περιορισμών γνωστοποίησης δεδομένων και να καταβάλουν κάθε δυνατή προσπάθεια για την άρση της απαγόρευσης γνωστοποίησης. Ο εξαγωγέας ή η αρμόδια εποπτική αρχή θα μπορούσαν τουλάχιστον να ενημερώσουν το υποκείμενο των δεδομένων σχετικά με την αναστολή ή τον τερματισμό της διαβίβασης των προσωπικών του/της δεδομένων λόγω της αδυναμίας του εισαγωγέα να συμμορφωθεί με τις συμβατικές του δεσμεύσεις κατόπιν της παραλαβής του αιτήματος πρόσβασης.

126. Η σύμβαση θα μπορούσε να δεσμεύει τον εξαγωγέα και τον εισαγωγέα να συνδράμουν το υποκείμενο των δεδομένων κατά την άσκηση των δικαιωμάτων του στη δικαιοδοσία τρίτης χώρας μέσω ειδικών μηχανισμών προσφυγής και παροχής νομικών συμβουλών.

127. Προϋποθέσεις αποτελεσματικότητας

- Ορισμένοι εθνικοί κανονισμοί ενδέχεται να μην επιτρέπουν στον εισαγωγέα δεδομένων να παρέχει αυτό το είδος υποστήριξης απευθείας στα υποκείμενα δεδομένων, παρότι ενδέχεται να επιτρέπουν στον εισαγωγέα δεδομένων να παρέχει αυτή τη στήριξη για τα υποκείμενα δεδομένων.
- Οι εθνικοί κανονισμοί και πολιτικές ενδέχεται να επιβάλλουν όρους που ενδέχεται να υπονομεύσουν την αποτελεσματικότητα των προβλεπόμενων ειδικών μηχανισμών προσφυγής.
- Η παροχή νομικών συμβουλών θα μπορούσε να είναι χρήσιμη για το υποκείμενο των δεδομένων, ιδίως λαμβάνοντας υπόψη πόσο περίπλοκο και δαπανηρό μπορεί να είναι για

ένα υποκείμενο δεδομένων να κατανοήσει το νομικό σύστημα τρίτης χώρας και να ασκήσει νομικές ενέργειες από το εξωτερικό, ενδεχομένως σε ξένη γλώσσα. Ωστόσο, αυτή η ρήτρα θα προσφέρει πάντα μια περιορισμένη πρόσθετη προστασία, δεδομένου ότι η παροχή συνδρομής και νομικών συμβουλών σε υποκείμενα δεδομένων δεν μπορεί από μόνη της να αποκαταστήσει την αδυναμία της έννομης τάξης τρίτης χώρας να παράσχει ένα επίπεδο προστασίας ουσιαστικά ισοδύναμο με αυτό που διασφαλίζεται εντός της ΕΕ. Αυτό το συμβατικό μέτρο θα πρέπει απαραίτητως να είναι συμπληρωματικό άλλων πρόσθετων μέτρων.

- Αυτό το πρόσθετο μέτρο θα ήταν αποτελεσματικό μόνον εφόσον το δίκαιο της τρίτης χώρας προβλέπει την άσκηση ένδικων μέσων ενώπιον των εθνικών της δικαστηρίων ή εφόσον υφίσταται ειδικός μηχανισμός προσφυγών, μεταξύ άλλων κατά των μέτρων παρακολούθησης.

2.3 Οργανωτικά μέτρα

128. Τα πρόσθετα οργανωτικά μέτρα μπορεί να αποτελούνται από εσωτερικές πολιτικές, οργανωτικές μεθόδους και πρότυπα τα οποία θα μπορούσαν να εφαρμόσουν οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία για τους ίδιους και να τα επιβάλουν στους εισαγωγείς δεδομένων σε τρίτες χώρες. Μπορούν να συμβάλουν στη διασφάλιση της συνοχής κατά την προστασία των δεδομένων προσωπικού χαρακτήρα καθ' όλη τη διάρκεια του κύκλου επεξεργασίας. Τα οργανωτικά μέτρα ενδέχεται επίσης να βελτιώσουν την ευαισθητοποίηση των εξαγωγέων σχετικά με τον κίνδυνο και τις προσπάθειες απόκτησης πρόσβασης στα δεδομένα σε τρίτες χώρες, καθώς και την ικανότητά τους να αντιδρούν σε αυτά. Η επιλογή και η εφαρμογή ενός ή περισσότερων από τα εν λόγω μέτρα δεν διασφαλίζουν απαραίτητως και συστηματικώς ότι η διαβίβασή σας πληροί το ουσιώδες πρότυπο ισοδυναμίας που απαιτεί η νομοθεσία της ΕΕ. Ανάλογα με τις ειδικές συνθήκες της διαβίβασης και την αξιολόγηση που διενεργείται βάσει της νομοθεσίας της τρίτης χώρας, απαιτούνται οργανωτικά μέτρα για τη συμπλήρωση συμβατικών ή/και τεχνικών μέτρων, προκειμένου να διασφαλιστεί ένα επίπεδο προστασίας των δεδομένων προσωπικού χαρακτήρα το οποίο θα είναι ουσιαστικά ισοδύναμο με εκείνο που διασφαλίζεται εντός του ΕΟΧ.
129. Η αξιολόγηση των καταλληλότερων μέτρων πρέπει να πραγματοποιείται κατά περίπτωση, λαμβάνοντας υπόψη την ανάγκη τήρησης της αρχής της λογοδοσίας από τους υπεύθυνους επεξεργασίας και τους εκτελούντες την επεξεργασία. Το ΕΣΠΔ παραθέτει κατωτέρω ορισμένα παραδείγματα οργανωτικών μέτρων που μπορούν να εφαρμόσουν οι εξαγωγείς, αν και ο κατάλογος είναι ενδεικτικός και άλλα μέτρα μπορεί επίσης να είναι κατάλληλα.

Εσωτερικές πολιτικές για τη διαχείριση των διαβιβάσεων ιδίως με ομίλους επιχειρήσεων

130. Εφαρμογή κατάλληλων εσωτερικών πολιτικών με σαφή κατανομή αρμοδιοτήτων για τη διαβίβαση δεδομένων, δίαυλοι αναφοράς και τυποποιημένες διαδικασίες λειτουργίας για περιπτώσεις μυστικών ή επίσημων αιτημάτων από δημόσιες αρχές για την πρόσβαση στα δεδομένα. Ιδίως στην περίπτωση διαβιβάσεων μεταξύ ομίλων επιχειρήσεων, αυτές οι πολιτικές μπορεί να περιλαμβάνουν, μεταξύ άλλων, τον διορισμό μιας συγκεκριμένης ομάδας, η οποία θα αποτελείται από εμπειρογνώμονες στον τομέα της ΤΠ, της νομοθεσίας για την προστασία των δεδομένων και της ιδιωτικής ζωής, για την αντιμετώπιση αιτημάτων που περιλαμβάνουν δεδομένα προσωπικού χαρακτήρα που διαβιβάζονται από την ΕΕ· την κοινοποίηση στα ανώτερα διευθυντικά και νομικά στελέχη και στον εξαγωγέα δεδομένων κατόπιν παραλαβής των εν λόγω αιτημάτων· τα διαδικαστικά βήματα για την καταγγελία δυσανάλογων ή παράνομων αιτημάτων και την παροχή διαφανών πληροφοριών στα υποκείμενα των δεδομένων.
131. Ανάπτυξη ειδικών διαδικασιών παροχής κατάρτισης για το προσωπικό που είναι υπεύθυνο για τη διαχείριση αιτημάτων πρόσβασης των δημόσιων αρχών σε δεδομένα προσωπικού χαρακτήρα, οι οποίες θα πρέπει να επικαιροποιούνται σε τακτά χρονικά διαστήματα ώστε να αντικατοπτρίζουν νέες νομοθετικές και νομολογιακές εξελίξεις στην τρίτη χώρα και στον ΕΟΧ. Οι διαδικασίες κατάρτισης θα πρέπει να περιλαμβάνουν τις απαιτήσεις της νομοθεσίας της ΕΕ σχετικά με την πρόσβαση των δημόσιων αρχών σε δεδομένα προσωπικού χαρακτήρα, ιδίως σύμφωνα με το άρθρο 52 παράγραφος 1 του Χάρτη των Θεμελιωδών Δικαιωμάτων. Θα πρέπει να αυξηθεί η ευαισθητοποίηση του προσωπικού ιδίως μέσω της αξιολόγησης πρακτικών

παραδειγμάτων των αιτημάτων πρόσβασης των δημόσιων αρχών στα δεδομένα και εφαρμόζοντας το πρότυπο που απορρέει από το άρθρο 52 παράγραφος 1 του Χάρτη των Θεμελιωδών Δικαιωμάτων στα εν λόγω πρακτικά παραδείγματα. Αυτή η εκπαίδευση θα πρέπει να λαμβάνει υπόψη τη συγκεκριμένη κατάσταση του εισαγωγέα δεδομένων, π.χ. τη νομοθεσία και τους κανονισμούς της τρίτης χώρας στα οποία υπόκειται ο εισαγωγέας δεδομένων και θα πρέπει να αναπτυχθεί, όπου είναι δυνατόν, σε συνεργασία με τον εξαγωγέα δεδομένων.

132. Προϋποθέσεις αποτελεσματικότητας:

- Αυτές οι πολιτικές μπορούν να προβλέπονται μόνο στις περιπτώσεις όπου το αίτημα των δημόσιων αρχών στην τρίτη χώρα είναι συμβατό με το δίκαιο της ΕΕ.¹⁰² Όταν το αίτημα είναι μη συμβατό, οι εν λόγω πολιτικές δεν αρκούν για τη διασφάλιση ισοδύναμου επιπέδου προστασίας των δεδομένων προσωπικού χαρακτήρα και, όπως προαναφέρθηκε, πρέπει να σταματήσουν οι διαβιβάσεις ή να εφαρμοστούν κατάλληλα πρόσθετα μέτρα για την αποφυγή της πρόσβασης.

Μέτρα διαφάνειας και λογοδοσίας.

133. Τήρηση εγγράφων και αρχείων των αιτημάτων πρόσβασης που ελήφθησαν από τις δημόσιες αρχές και η απάντηση που δόθηκε, παράλληλα με το νομικό σκεπτικό και τους εμπλεκόμενους παράγοντες (π.χ. εάν ο εξαγωγέας έχει ειδοποιηθεί καθώς και η απάντησή του, η αξιολόγηση της ομάδας που είναι υπεύθυνη για την αντιμετώπιση των εν λόγω αιτημάτων κ.λπ.). Τα εν λόγω αρχεία πρέπει να διατίθενται στον εξαγωγέα δεδομένων, ο οποίος με τη σειρά του θα πρέπει να τα παρέχει στα ενδιαφερόμενα υποκείμενα των δεδομένων.

134. Προϋποθέσεις αποτελεσματικότητας:

- Η εθνική νομοθεσία στην τρίτη χώρα μπορεί να αποτρέψει τη γνωστοποίηση των αιτημάτων ή σημαντικών πληροφοριών που περιέχονται σε αυτά και, επομένως, να καταστήσει την πρακτική αυτή αναποτελεσματική. Ο εισαγωγέας δεδομένων θα πρέπει να ενημερώνει τον εξαγωγέα για την αδυναμία του να παράσχει τα εν λόγω έγγραφα και αρχεία, προσφέροντας έτσι στον εξαγωγέα τη δυνατότητα να αναστείλει τις διαβιβάσεις, εάν η αδυναμία αυτή θα οδηγούσε στη μη παροχή επαρκούς επιπέδου προστασίας.

135. Τακτική δημοσίευση εκθέσεων διαφάνειας ή περιλήψεων σχετικά με κυβερνητικά αιτήματα πρόσβασης στα δεδομένα και το είδος της απάντησης που παρέχεται, εφόσον η δημοσίευση επιτρέπεται από την τοπική νομοθεσία.

136. Προϋποθέσεις αποτελεσματικότητας:

- Οι παρεχόμενες πληροφορίες θα πρέπει να είναι σχετικές, σαφείς και όσο το δυνατόν πιο λεπτομερείς. Η εθνική νομοθεσία στην τρίτη χώρα μπορεί να παρεμποδίζει τη γνωστοποίηση λεπτομερών πληροφοριών. Σε αυτές τις περιπτώσεις, ο εισαγωγέας δεδομένων θα πρέπει να

¹⁰² Βλ. υπόθεση C-362/14 («Schrems I»), σκέψη 94· υπόθεση C-311/18 (Schrems II), σκέψεις 168, 174, 175 και 176.

καταβάλλει κάθε δυνατή προσπάθεια για τη δημοσίευση στατιστικών πληροφοριών ή παρόμοιων τύπων συγκεντρωτικών πληροφοριών.

Μέθοδοι οργάνωσης και μέτρα ελαχιστοποίησης δεδομένων

137. Οι ήδη υπάρχουσες οργανωτικές απαιτήσεις σύμφωνα με την αρχή της λογοδοσίας, όπως η εφαρμογή αυστηρών και λεπτομερών πολιτικών πρόσβασης στα δεδομένα και εμπιστευτικότητας και βέλτιστων πρακτικών, βάσει μιας αυστηρής αρχής της ανάγκης γνώσης, που παρακολουθούνται με τακτικούς ελέγχους και επιβάλλονται μέσω πειθαρχικών μέτρων μπορεί επίσης να αποτελούν χρήσιμα μέτρα σε ένα πλαίσιο διαβίβασης. Η ελαχιστοποίηση των δεδομένων θα πρέπει εν προκειμένω να εξεταστεί, προκειμένου να περιοριστεί η έκθεση των δεδομένων προσωπικού χαρακτήρα σε μη εξουσιοδοτημένη πρόσβαση. Για παράδειγμα, σε ορισμένες περιπτώσεις ενδέχεται να μην είναι απαραίτητη η διαβίβαση ορισμένων δεδομένων (π.χ. σε περίπτωση απομακρυσμένης πρόσβασης σε δεδομένα του ΕΟΧ, όπως σε περιπτώσεις υποστήριξης, όταν παρέχεται περιορισμένη πρόσβαση αντί για πλήρη πρόσβαση ή όταν η παροχή μιας υπηρεσίας απαιτεί μόνο τη διαβίβαση ενός περιορισμένου συνόλου δεδομένων και όχι ολόκληρης της βάσης δεδομένων).

138. Προϋποθέσεις αποτελεσματικότητας:

- Θα πρέπει να διενεργούνται τακτικοί έλεγχοι και να εφαρμόζονται αυστηρά πειθαρχικά μέτρα προκειμένου να παρακολουθείται και να επιβάλλεται η συμμόρφωση με τα μέτρα ελαχιστοποίησης των δεδομένων επίσης στο πλαίσιο διαβίβασης.
- Ο εξαγωγέας δεδομένων πραγματοποιεί αξιολόγηση των δεδομένων προσωπικού χαρακτήρα που έχει στην κατοχή του πριν από τη διαβίβαση, προκειμένου να προσδιορίσει τα σύνολα δεδομένων που δεν είναι απαραίτητα για τους σκοπούς της διαβίβασης και, ως εκ τούτου, δεν θα κοινοποιηθούν στον εισαγωγέα δεδομένων.
- Τα μέτρα ελαχιστοποίησης των δεδομένων θα πρέπει να συνοδεύονται από τεχνικά μέτρα ώστε να διασφαλίζεται ότι τα δεδομένα δεν υπόκεινται σε μη εξουσιοδοτημένη πρόσβαση. Για παράδειγμα, η εφαρμογή ασφαλών μηχανισμών πολυσυμμετοχικού υπολογισμού και η εξάπλωση κρυπτογραφημένων συνόλων δεδομένων μεταξύ διαφορετικών αξιόπιστων οντοτήτων μπορεί να αποτρέψει ήδη από τον σχεδιασμό την κοινοποίηση αναγνωρίσιμων δεδομένων που μπορεί να προκληθεί από οποιαδήποτε μονομερή πρόσβαση.

139. Ανάπτυξη βέλτιστων πρακτικών για την κατάλληλη και έγκαιρη συμμετοχή και πρόσβαση του υπεύθυνου προστασίας δεδομένων σε πληροφορίες, εάν υπάρχει, και στις νομικές και εσωτερικές υπηρεσίες ελέγχου για θέματα που σχετίζονται με διεθνείς διαβιβάσεις δεδομένων προσωπικού χαρακτήρα.

140. Προϋποθέσεις αποτελεσματικότητας:

- Ο υπεύθυνος προστασίας δεδομένων, εάν υπάρχει, και η νομική και εσωτερική ομάδα ελέγχου θα λάβουν όλες τις σχετικές πληροφορίες πριν από τη διαβίβαση και θα ζητηθεί η γνώμη τους σχετικά με την αναγκαιότητα της διαβίβασης και τις πρόσθετες εγγυήσεις, εάν υπάρχουν.

- Οι σχετικές πληροφορίες θα πρέπει να περιλαμβάνουν, για παράδειγμα, την αξιολόγηση της αναγκαιότητας της διαβίβασης των συγκεκριμένων δεδομένων προσωπικού χαρακτήρα, μια επισκόπηση της ισχύουσας νομοθεσίας της τρίτης χώρας και των εγγυήσεων που δεσμεύεται να εφαρμόσει ο εισαγωγέας.

Θέσπιση προτύπων και βέλτιστων πρακτικών

141. Θέσπιση αυστηρών πολιτικών για την ασφάλεια των δεδομένων και το απόρρητο των δεδομένων, βάσει πιστοποίησης της ΕΕ ή κωδίκων δεοντολογίας ή διεθνών προτύπων (π.χ. πρότυπα ISO) και βέλτιστων πρακτικών (π.χ. ENISA), λαμβάνοντας δεόντως υπόψη την εξέλιξη της τεχνολογίας, σύμφωνα με τον κίνδυνο των κατηγοριών των δεδομένων που υποβάλλονται σε επεξεργασία.

Άλλα

142. Θέσπιση και τακτική επανεξέταση των εσωτερικών πολιτικών για την αξιολόγηση της καταλληλότητας των εφαρμοζόμενων πρόσθετων μέτρων και τον εντοπισμό και την εφαρμογή πρόσθετων ή εναλλακτικών λύσεων, όταν κρίνεται απαραίτητο, για να διασφαλιστεί ότι διατηρείται ισοδύναμο επίπεδο προστασίας των διαβιβαζόμενων δεδομένων προσωπικού χαρακτήρα με αυτό που διασφαλίζεται εντός της ΕΕ.

143. Δεσμεύσεις από τον εισαγωγέα δεδομένων ότι δεν θα προβεί σε περαιτέρω διαβίβαση των δεδομένων προσωπικού χαρακτήρα εντός της ίδιας χώρας ή άλλων τρίτων χωρών, ή ότι θα αναστείλει τις υπό εξέλιξη διαβιβάσεις όταν δεν μπορεί να διασφαλιστεί επίπεδο προστασίας των δεδομένων προσωπικού χαρακτήρα στην τρίτη χώρα ισοδύναμο με αυτό που διασφαλίζεται εντός της ΕΕ.¹⁰³

¹⁰³ C-311/18 (Schrems II), σκέψεις 135 και 137.

ΠΑΡΑΡΤΗΜΑ 3: ΠΙΘΑΝΕΣ ΠΗΓΕΣ ΠΛΗΡΟΦΟΡΙΩΝ ΓΙΑ ΤΗΝ ΑΞΙΟΛΟΓΗΣΗ ΤΡΙΤΗΣ ΧΩΡΑΣ

144. Ο οικείος εισαγωγέας δεδομένων θα πρέπει να είναι σε θέση να σας παρέχει συναφείς πηγές και πληροφορίες σχετικά με την τρίτη χώρα στην οποία είναι εγκατεστημένος, καθώς και με τους νόμους και τις πρακτικές που ισχύουν για τον εισαγωγέα και τα διαβιβαζόμενα δεδομένα. Εσείς και οι εισαγωγέας μπορείτε να ανατρέξετε σε πολλές πηγές πληροφοριών, όπως αυτές που απαριθμούνται ενδεικτικά παρακάτω και παρουσιάζονται με σειρά προτεραιότητας:

- Νομολογία του Δικαστηρίου της Ευρωπαϊκής Ένωσης (ΔΕΕ) και του Ευρωπαϊκού Δικαστηρίου των Δικαιωμάτων του Ανθρώπου (ΕΔΔΑ)¹⁰⁴ όπως αναφέρεται στις συστάσεις των ευρωπαϊκών βασικών εγγυήσεων.¹⁰⁵
- Αποφάσεις επάρκειας στη χώρα προορισμού εάν η διαβίβαση βασίζεται σε διαφορετική νομική βάση.¹⁰⁶
- Ψηφίσματα και εκθέσεις διακυβερνητικών οργανισμών, όπως το Συμβούλιο της Ευρώπης,¹⁰⁷ άλλων περιφερειακών οργάνων,¹⁰⁸ και οργάνων και υπηρεσιών του ΟΗΕ (π.χ. Συμβούλιο Ανθρωπίνων Δικαιωμάτων των ΗΕ,¹⁰⁹ Επιτροπή Ανθρωπίνων Δικαιωμάτων¹¹⁰).
- Εκθέσεις και ανάλυση από αρμόδια ρυθμιστικά δίκτυα, όπως η Παγκόσμια Συνέλευση Προστασίας Απορρήτου (GPA).¹¹¹
- Εθνική νομολογία ή αποφάσεις που λαμβάνονται από ανεξάρτητες δικαστικές ή διοικητικές αρχές αρμόδιες για το απόρρητο των δεδομένων και την προστασία των δεδομένων τρίτων χωρών.
- Εκθέσεις ανεξάρτητων εποπτικών ή κοινοβουλευτικών φορέων.
- Εκθέσεις βασισμένες στην πρακτική εμπειρία σε παλαιότερες περιστάσεις αιτημάτων κοινολόγησης από δημόσιες αρχές, ή στην απουσία παρόμοιων αιτημάτων, από φορείς που δραστηριοποιούνται στον ίδιο τομέα με τον εισαγωγέα.
- Ειδοποιήσεις Warrant canary άλλων οντοτήτων που επεξεργάζονται δεδομένα στο ίδιο πεδίο με τον εισαγωγέα.

¹⁰⁴ Βλ. ενημερωτικό δελτίο της νομολογίας του ΕΔΔΑ σχετικά με τη μαζική παρακολούθηση: https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf

¹⁰⁵ Συστάσεις του ΕΣΠΔ 02/2020 σχετικά με τις Ευρωπαϊκές Βασικές Εγγυήσεις για τα μέτρα παρακολούθησης, 10 Νοεμβρίου 2020, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en

¹⁰⁶ C-311/18 (Schrems II), σκέψη 141. βλ. αποφάσεις επάρκειας στη διεύθυνση https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

¹⁰⁷ <https://www.coe.int/en/web/data-protection/reports-studies-and-opinions>

¹⁰⁸ Βλ., για παράδειγμα, εκθέσεις χωρών της Διαμερικανικής Επιτροπής Ανθρωπίνων Δικαιωμάτων (IACHR), <https://www.oas.org/en/iachr/reports/country.asp>.

¹⁰⁹ Βλ. <https://www.ohchr.org/EN/HRBodies/UPR/Pages/Documentation.aspx>

¹¹⁰ Βλ.:

https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=8&DocTypeID=5

¹¹¹ Π.χ. βλ. https://globalprivacyassembly.org/wp-content/uploads/2020/10/Day-1-1_2a-Day-3-3_2b-v1_0-Policy-Strategy-Working-Group-WS1-Global-frameworks-and-standards-Report-Final.pdf

- Εκθέσεις που καταρτίζονται ή ανατίθενται από εμπορικά επιμελητήρια, εμπορικές, επαγγελματικές και κλαδικές ενώσεις, κρατικούς διπλωματικούς, εμπορικούς και επενδυτικούς οργανισμούς του εξαγωγέα ή άλλων τρίτων χωρών που πραγματοποιούν εξαγωγές στην τρίτη χώρα στην οποία γίνεται η διαβίβαση·
- Εκθέσεις ακαδημαϊκών ιδρυμάτων και οργανώσεων της κοινωνίας των πολιτών (π.χ. ΜΚΟ)·
- Εκθέσεις από ιδιωτικούς παρόχους εμπορικών πληροφοριών για χρηματοοικονομικούς, ρυθμιστικούς κινδύνους και κινδύνους φήμης για τις εταιρείες·
- Ειδοποιήσεις Warrant canary του ίδιου του εισαγωγέα¹¹²
- Εκθέσεις διαφάνειας, υπό τον όρο ότι αναφέρουν ρητά το γεγονός ότι δεν ελήφθησαν αιτήματα παροχής πρόσβασης. Εκθέσεις διαφάνειας που αποσιωπούν αυτό το σημείο δεν θα χαρακτηρίζονται ως επαρκής απόδειξη καθώς αυτές οι εκθέσεις επικεντρώνονται, ως επί το πλείστον, σε αιτήματα πρόσβασης που λαμβάνονται από αρχές επιβολής του νόμου και παρέχουν αριθμητικά στοιχεία μόνο γι' αυτή την πτυχή ενώ δεν κάνουν αναφορά στα αιτήματα πρόσβασης που λαμβάνουν για σκοπούς εθνικής ασφάλειας. Αυτό δεν σημαίνει ότι δεν ελήφθησαν αιτήματα παροχής πρόσβασης αλλά περισσότερο ότι αυτές οι πληροφορίες δεν μπορούν να κοινοποιηθούν¹¹³
- Εσωτερικές δηλώσεις ή αρχεία του εισαγωγέα που αναφέρουν ρητά ότι δεν έχουν ληφθεί αιτήματα πρόσβασης για αρκετά μεγάλο χρονικό διάστημα· προτιμώνται οι δηλώσεις και τα αρχεία που θέτουν ζήτημα ευθύνης του εισαγωγέα ή/και εκδίδονται από εσωτερικές θέσεις με κάποια αυτονομία όπως εσωτερικούς ελεγκτές, υπεύθυνους προστασίας δεδομένων κ.λπ.¹¹⁴

¹¹² Βλ. προϋποθέσεις για την εξέταση της τεκμηριωμένης πρακτικής εμπειρίας του εισαγωγέα σε σχετικές παλαιότερες περιστάσεις αιτημάτων παροχής πρόσβασης που ελήφθησαν από δημόσιες αρχές της τρίτης χώρας στη σκέψη 47·

¹¹³ Ό.π.

¹¹⁴ Ό.π.