DESLOCK
ENCRYPTION BY

ESET

Επισκόπηση του General Data Protection Regulation (GDPR) Πως θα επηρεάσει την επιχείρησή σας

BUSINESS

ENJOY SAFER TECHNOLOGY™

ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2016/679 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΗΣ ΕΠΙΤΡΟΠΗΣ

Της 27 Απριλίου 2016

Για την προστασία των φυσικών προσώπων αναφορικά με την επεξεργασία και ελεύθερη διακίνηση προσωπικών δεδομένων, και αντικατάσταση της Οδηγίας 95/46/EC (Κανονισμός Γενικής Προστασίας Δεδομένων- GDPR)

ΤΙ ΕΙΝΑΙ ΤΟ GDPR?

Προς αντιμετώπιση των δυσκολιών που ανακύπτουν από την Οδηγία, η ΕΕ δημιούργησε ένα νέο καθεστώς προστασίας δεδομένων- το GDPR. Το GDPR αποβλέπει στο να **εναρμονίσει το νομοθετικό καθεστώς προστασίας δεδομένων σε όλη την ΕΕ**, χωρίς προηγούμενη εθνική πράξη ενσωμάτωσης. Στη θεωρία, αυτό σημαίνει ότι οι οργανισμοί έχουν πιο σταθερές προϋποθέσεις για την προστασία δεδομένων στην ΕΕ. Εντούτοις, υπάρχουν συγκεκριμένοι τομείς που παραμένουν ασυντόνιστοι. Σε αυτούς τους τομείς, οι προϋποθέσεις συμμόρφωσης εξακολουθούν να ποικίλλουν από Κράτος Μέλος σε Κράτος Μέλος. Το **GDPR** έχει επίσης σχεδιαστεί για να αντιμετωπίσει τεχνολογικές και κοινωνικές αλλαγές που έλαβαν χώρα τα τελευταία 20 χρόνια, υιοθετώντας μια τεχνολογικά ουδέτερη προσέγγιση στον Κανονισμό. Ο νόμος της ΕΕ για την προστασία δεδομένων επηρεάζει όλους τους οργανισμούς εντός ΕΕ (και κάποιους εκτός ΕΕ). Πολλοί οργανισμοί που είχαν λίγες ή και καθόλου ευθύνες συμμόρφωσης υπό την Οδηγία, τώρα έχουν νέες ή αυξημένες υποχρεώσεις υπό το **GDPR**.

ΤΑ ΣΤΑΔΙΑ ΕΙΣΑΓΩΓΗΣ ΤΟΥ GDPR

- Τον Ιανουάριο 2012, η Ευρωπαϊκή Επιτροπή πρότεινε μια εμπεριστατωμένη μεταρρύθμιση κανόνων για την προστασία προσωπικών δεδομένων στην ΕΕ.

- Στις 15 Δεκεμβρίου 2015, το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο και η Επιτροπή ήρθαν σε συμφωνία αναφορικά με τους νέους κανόνες για την προστασία δεδομένων, εγκαθιδρύοντας ένα σύγχρονο και εναρμονισμένο πλαίσιο προστασίας δεδομένων σε όλη την Ευρώπη. Η επιτροπή πολιτικών ελευθεριών του Ευρωπαϊκού Κοινοβουλίου και η Επιτροπή Μόνιμων Αντιπροσώπων του Συμβουλίου ενέκριναν τις συμφωνίες με μεγάλες πλειοψηφίες.

- Οι συμφωνίες έγιναν επίσης αποδεκτές από το Ευρωπαϊκό Συμβούλιο στις 17-18 Δεκεμβρίου ως ένα μεγάλο βήμα προς την εφαρμογή της Στρατηγικής στην Ελεύθερη Ψηφιακή Αγορά.

- Στις 8 Απριλίου 2016, ο Κανονισμός υιοθετήθηκε από το Συμβούλιο και στις 14 Απριλίου 2016 από το Ευρωπαϊκό Κοινοβούλιο.

- Στις 4 Μαΐου 2016, τα επίσημα κείμενα του Κανονισμού δημοσιεύτηκαν στην Επίσημη Εφημερίδα της ΕΕ σε όλες τις επίσημες γλώσσες.

- Ενώ ο Κανονισμός θα τεθεί σε ισχύ στις 4 Μαΐου 2016, θα εφαρμοστεί από τις 25 Μαΐου 2018. Ο Κανονισμός είναι ένα αναγκαίο βήμα για την ενδυνάμωση των θεμελιωδών δικαιωμάτων των πολιτών στην ψηφιακή εποχή και την διευκόλυνση των επιχειρήσεων απλοποιώντας του κανόνες για τις εταιρείες στην Ελεύθερη Ψηφιακή Αγορά.
  Ο εν λόγω Κανονισμός δεν απαιτεί προηγουμένως συγκεκριμένη νομοθετική πράξη του Κράτους Μέλους προκειμένου να εφαρμοστεί. Αν εκδοθεί ένας τέτοιος νόμος, θα μπορούσε να εξειδικεύσει τους γενικούς όρους του Κανονισμού αυτού, να θεσπίσει ειδικές προϋποθέσεις για τον υπεύθυνο επεξεργασίας, για τα υποκείμενα προσωπικών δεδομένων κπλ.

ΠΡΟΒΛΗΜΑΤΑ ΠΟΥ ΟΔΗΓΟΥΝ ΣΤΗΝ ΕΠΕΙΓΟΥΣΑ ΕΦΑΡΜΟΓΗ ΤΟΥ ΝΕΟΥ ΚΑΝΟΝΙΣΜΟΥ

Πρόβλημα 1: Φραγμοί για επιχειρήσεις και δημόσιες αρχές εξαιτίας του κατακερματισμού, της νομικής αβεβαιότητας και της ασύμφωνης εφαρμογής

Παρά το γεγονός ότι ο σκοπός της Οδηγίας είναι να εξασφαλίζει ένα αντίστοιχο επίπεδο προστασίας δεδομένων εντός της ΕΕ, υπάρχει ακόμη σημαντική διαφοροποίηση στους κανόνες που εφαρμόζονται από τα Κράτη Μέλη. Συνεπώς, οι υπεύθυνοι επεξεργασίας δεδομένων θα πρέπει να αντιμετωπίσουν 27 διαφορετικές εθνικές νομοθεσίες και προϋποθέσεις στην ΕΕ. Το αποτέλεσμα είναι ένα κατακερματισμένο νομικό περιβάλλον που έχει δημιουργήσει νομική αβεβαιότητα και άνιση προστασία των προσώπων. Έτσι, είναι πιο δύσκολο για τα άτομα να εξασκήσουν τα δικαιώματα σε κάποια Κράτη Μέλη από ότι σε άλλα, ειδικώς στο πλαίσιο του διαδικτύου. Αυτό έχει προκαλέσει μη αναγκαία έξοδα και διοικητικά βάρη για τις επιχειρήσεις και συνιστά ένα αντικίνητρο για αυτές, συμπεριλαμβάνοντας τις μικρές εταιρίες, που θα επιθυμήσουν τυχόν διασυνοριακή εξάπλωση τους. Επίσης, οι πόροι κι οι εξουσίες των εθνικών αρχών που είναι υπεύθυνες για την προστασία δεδομένων ποικίλλουν σημαντικώς μεταξύ των Κρατών Μελών. Σε κάποιες περιπτώσεις, αυτό σημαίνει ότι είναι ανίκανοι να εκτελέσουν ικανοποιητικώς τα καθήκοντα επιβολής. Η συνεργασία μεταξύ αυτών των αρχών σε Ευρωπαϊκό επίπεδο – μέσω του υπάρχοντος Συμβουλευτικού Σώματος (Ομάδα Προστασίας Δεδομένων βάσει του Άρθρου 29) δεν οδηγεί πάντα σε σταθερή επιβολή και γι' αυτό χρήζει βελτίωσης.

Πρόβλημα 2: Οι αρχές της επικουρικότητας και της αναλογικότητας υπογραμμίζουν την αναγκαιότητα μιας δράσης σε επίπεδο ΕΕ.

Το δικαίωμα στην προστασία προσωπικών δεδομένων κατοχυρώνεται στο Άρθρο 8 του Χάρτη Θεμελιωδών Δικαιωμάτων. Το Άρθρο 16 της ΣΛΕΕ είναι η νομική βάση για την υιοθέτηση ενωσιακών κανόνων για την προστασία δεδομένων. Επιπροσθέτως, τα προσωπικά δεδομένα μπορούν να μεταφερθούν πέρα από τα εθνικά σύνορα, τόσο εντός των εσωτερικών συνόρων της ΕΕ όσο και προς τρίτες χώρες, σε αυξημένα ποσοστά. Υπάρχουν όμως πρακτικές προκλήσεις κατά την εφαρμογή της νομοθεσίας για την προστασία δεδομένων και μια ανάγκη συνεργασίας μεταξύ των Κρατών Μελών και των αρχών τους, οι οποίες θα πρέπει να οργανωθούν σε ενωσιακό επίπεδο. Αυτή είναι κυρίως η περίπτωση για τα προβλήματα εκείνα που ανακύπτουν από τον κατακερματισμό στις εθνικές νομοθεσίες που εφαρμόζουν το κανονιστικό πλαίσιο της προστασίας δικαιωμάτων στην ΕΕ. Μολονότι θα ήταν εφικτό τα Κράτη Μέλη να εφαρμόσουν πολιτικές που διασφαλίζουν ότι αυτό το δικαίωμα δε θα παραβιαστεί, κάτι τέτοιο δε θα μπορούσε να επιτευχθεί με ομοιογενή τρόπο δεδομένης της απουσίας κοινών ενωσιακών κανόνων και θα δημιουργούσε περιορισμούς στις διασυνοριακές διαρροές προσωπικών δεδομένων.

Οι ενέργειες- στόχοι είναι αναλογικές καθώς εμπίπτουν στο πεδίο αρμοδιοτήτων της ΕΕ, όπως ορίζουν οι Συνθήκες και είναι απαραίτητες για να διασφαλίσουν την ομοιομορφία στην εφαρμογή της ενωσιακής νομοθεσίας, αποβλέποντας στην αποτελεσματική και ισότιμη προστασία των ατομικών θεμελιωδών ικαιωμάτων. Η δράση σε ενωσιακό επίπεδο είναι αναγκαία για να εξακολουθεί να υπάρχει φερεγγυότητα και υψηλό επίπεδο προστασίας δεδομένων σε μια παγκοσμιοποιημένη κοινωνία, ενώ διατηρείται η ελεύθερη διακίνηση εδομένων.

ΠΟΙΕΣ ΕΙΝΑΙ ΟΙ ΑΛΛΑΓΕΣ - ΚΛΕΙΔΙΑ;

Αλλάζουν αρκετά σημεία, αλλά όχι όλα.

Το GDPR κάνει σημαντικές αλλαγές στη ενωσιακή νομοθεσία για την προστασία δεδομένων αλλά αυτό δε συνιστά πλήρη αποξένωση από τις υφιστάμενες αρχές , καθώς πολλές εξακολουθούν να εφαρμόζονται υπό το GDPR.

Εδαφική εφαρμογή

Το GDPR εφαρμόζεται σε εκτός ΕΕ οργανισμούς αν αυτοί: (i) προσφέρουν αγαθά ή υπηρεσίες σε πολίτες της ΕΕ; ή (ii) επιβλέπουν τη συμπεριφορά των πολιτων της ΕΕ. Πολλοί οργανισμοί που δεν υπόκεινται στην ήδη υφιστάμενη – για την προστασία δεδομένων- νομοθεσία της ΕΕ θα υπόκεινται στο GDPR , ιδιαιτέρως οι διαδικτυακές επιχειρήσεις.

Συναίνεση

Η συναίνεση καθιστά δύσκολο για τους οργανισμούς να την αποκτήσουν και να βασιστούν πάνω της. Αξιοσημείωτα, το GDPR αναφέρει ότι η συναίνεση δεν είναι έγκυρη όταν υπάρχει μια «προφανής ανισορροπία» μεταξύ υπεύθυνου επεξεργασίας και υποκειμένου δεδομένων.

Δικαιώματα των υποκειμένων των δικαιωμάτων

Ορισμένα δικαιώματα των υποκειμένων των δικαιωμάτων ενδυναμώνονται από το GDPR (π.χ., το δικαίωμα εναντίωσης) και κάποια καινούρια δικαιώματα θεσπίζονται (π.χ., το δικαίωμα μεταφοράς δεδομένων). Αυτά τα δικαιώματα μπορεί να δυσκολέψουν τις επιχειρήσεις κατά την νόμιμη επεξεργασία προσωπικών δεδομένων.

72ωρη ειδοποίηση σε περίπτωση παραβίασης δεδομένων

Το GDPR απαιτεί από τις επιχειρήσεις να ενημερώνουν την αντίστοιχη αρχή προστασίας δεδομένων σε περίπτωση παραβίασης δεδομένων εντός 72 ωρών από τν εντοπισμού της. Σε ορισμένες επιχειρήσεις θα χρειαστούν ραγδαίες αλλαγές στον εσωτερικό έλεγχο.

Αυξημένες υποχρεώσεις συμμόρφωσης για τους υπεύθυνους επεξεργασίας

Το GDPR επιβάλλει νέες και αυξημένες υποχρεώσεις συμμόρφωσης για τους υπεύθυνους επεξεργασίας (π.χ., να εφαρμόζουν τις κατάλληλες πολιτικές, να διατηρούν αρχεία των δραστηριοτήτων επεξεργασίας, ιδιωτικότητα εκ σχεδιασμού και εξ ορισμού, κλπ.

Άμεσες υποχρεώσεις συμμόρφωσης για τους υπεύθυνους επεξεργασίας

The Directive generally does not impose direct legal compliance obligations on processors. However, under the GDPR, processors do have direct legal compliance obligations, and DPAs can take enforcement action against processors

Διορισμός Υπεύθυνου Επεξεργασίας Δεδομένων

Επιχειρήσεις που τακτικά και συστηματικά επιβλέπουν τα υποκείμενα δικαιωμάτων, ή επεξεργάζονται Ευαίσθητα Προσωπικά Δεδομένα σε μεγάλη κλίμακα, θα πρέπει να διορίζουν έναν Υπεύθυνο Προστασίας Δεδομένων.

Διασυνοριακές μεταφορές δεδομένων

Το GDPR παρέχει ευρύτερη σταθερότητα κατά την εφαρμογή δεσμευτικών εταιρικών κανόνων σε όλα τα Κράτη Μέλη. Το GDPR επίσης αναγνωρίζει έναν αριθμό από άλλους μηχανισμούς μεταφοράς δεδομένων (π.χ., συμμόρφωση σε εγκεκριμένο Κώδικα Συμπεριφοράς).

“The One- stop -shop”

Επιχειρήσεις εγκατεστημένες σε πολλαπλά Κράτη Μέλη μπορούν να επωφεληθούν από μια «κύρια αρχή προστασίας δεδομένων» . Στις περισσότερες περιπτώσεις υπό το GDPR, μια τέτοια επιχείρηση έρχεται σε επαφή μόνο με την «κύρια αρχή προστασίας δεδομένων» για κανονιστικά θέματα και μπορεί να αποφύγει να επικοινωνεί με πολλαπλές «κύριες αρχές προστασίας δεδομένων» σε όλη την ΕΕ.

Αυξημένη εναρμόνιση

Βάσει του GDPR, οι επιχειρήσεις έχουν πιο σταθερές προϋποθέσεις συμμόρφωσης στην ΕΕ. Εντούτοις, θα έπρεπε να ληφθεί υπόψη ότι οι εθνικές διαφοροποιήσεις θα εξακολουθούν να υφίστανται σε κάποιες περιοχές (π.χ., εθνική ασφάλεια; εργατικό δίκαιο; και ελευθερία λόγου)

Λύσεις και ποινές

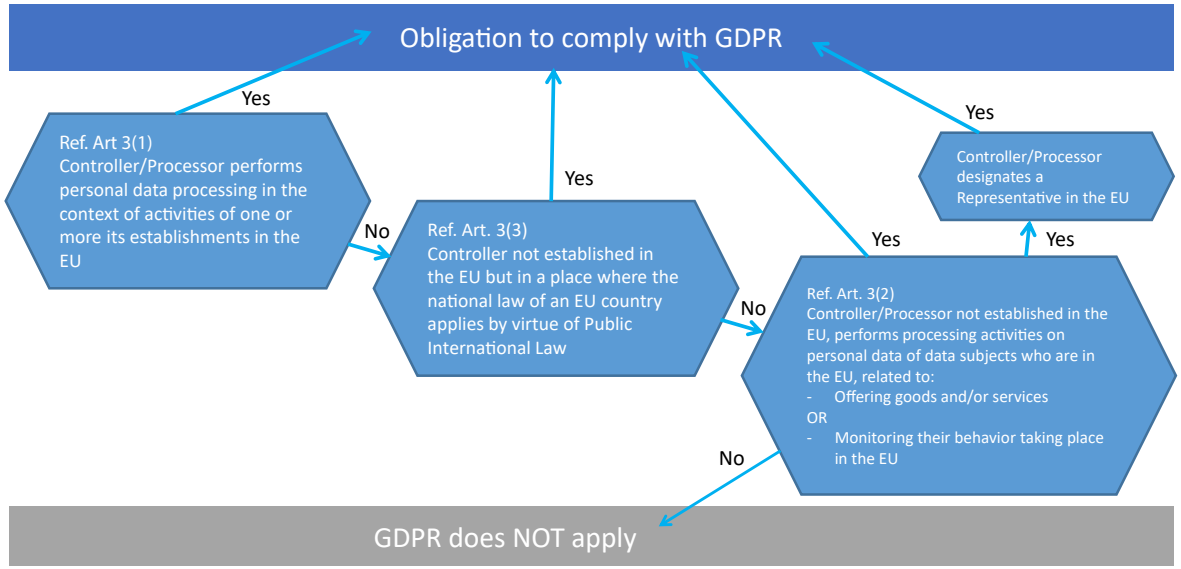
Οι συνέπειες παραβίασης της ενωσιακής νομοθεσίας για την προστασία δεδομένων αυξάνονται ραγδαία υπό το GDPR, το οποίο θέτει ένα μέγιστο πρόστιμο για μονομερή παραβίαση το πολύ €20 εκ., ή 4% των ετήσιων παγκόσμιων πόρων.

ΑΝΑΛΥΣΗ ΤΟΥ ΚΑΝΟΝΙΣΜΟΥ

Ουσιαστικό και εδαφικό πεδίο εφαρμογής

Σύμφωνα με τα Άρθρα 2 και 3, ο εν λόγω Κανονισμός εφαρμόζεται στην επεξεργασία προσωπικών δεδομένων φυσικών προσώπων εν όλω ή εν μέρει με αυτοματοποιημένα μέσα και στην επεξεργασία μη αυτοματοποιημένων μέσων των προσωπικών δεδομένων που συνιστούν μέρος ενός συστήματος αρχειοθέτησης ή σκοπεύουν να γίνουν μέρος αυτού. Αυτή η επεξεργασία πρέπει να λάβει χώρα στο πλαίσιο ενεργειών ενός υπεύθυνου επεξεργασίας ή ενός επεξεργαστή εντός της ΕΕ, ανεξαρτήτως εάν η επεξεργασία λαμβάνει χώρα εντός της ΕΕ ή όχι. Αυτό δηλώνει ότι το **GDPR** εφαρμόζεται επίσης σε επιχειρήσεις που δεν είναι εγκατεστημένες εντός της ΕΕ, αλλά που προσφέρουν αγαθά ή υπηρεσίες ή επιβλέπουν τη συμπεριφορά υποκειμένων δικαιωμάτων στην ΕΕ. Με άλλα λόγια, επιχειρήσεις που στοχεύουν σε πολίτες της ΕΕ μέσω διαδικτύου για υπηρεσίες, αγαθά ή επίβλεψη, θα πρέπει να συμμορφώνονται στους κανόνες της ΕΕ για την ιδιωτικότητα των δεδομένων αυτών των πολιτών. Φαίνεται ότι δημιουργείται ένα ενδιαφέρον δεδικασμένο, όπου οι κανόνες ακολουθούν τα δεδομένα αντί να είναι αυστηρώς εδαφικοί. Κατά συνέπεια, τόσο οι υπεύθυνοι επεξεργασίας όσο και οι επεξεργαστές είναι υποχρεωμένοι να συμμορφώνονται με το νέο Κανονισμό στον οποίο υπόκεινται. Επιπλέον, σε αντίθεση με την Οδηγία, το GDPR εφαρμόζεται στη δικαιοδοσία είτε ο υπεύθυνος επεξεργασίας είτε ο επεξεργαστής είναι εγκατεστημένοι στην ΕΕ, ανεξαρτήτως του πού διεξάγεται η επεξεργασία των δεδομένων, καθώς και όπου ο υπεύθυνος επεξεργασίας είναι μια μη ενωσιακή επιχείρηση αλλά έχει εγκατάσταση σε δικαιοδοσία όπου εφαρμόζεται νομοθεσία Κράτους Μέλους.

Η εικόνα παρακάτω είναι ενδεικτική του εδαφικού πεδίου εφαρμογής του Κανονισμού:



Νέες μορφές προσωπικών δεδομένων

Το Άρθρο 4 αναφέρεται στους ορισμούς, μερικοί από τους οποίους εισάγονται για πρώτη φορά. Πιο συγκεκριμένα, ο όρος 'προσωπικά δεδομένα' τώρα επεκτάθηκε και περιλαμβάνει – εκτός των άλλων- γενετικά, βιομετρικά, υγείας και ψευδωνυμοποίησης δεδομένα, κάνοντας την εφαρμογή του νέου Κανονισμού επιτακτικής ανάγκης για ολοένα και περισσότερες αγορές. Όπως προκύπτει από το γράμμα του νόμου:

«γενετικά δεδομένα»: τα δεδομένα προσωπικού χαρακτήρα που αφορούν τα γενετικά χαρακτηριστικά φυσικού προσώπου που κληρονομήθηκαν ή αποκτήθηκαν, όπως προκύπτουν, ιδίως, από ανάλυση βιολογικού δείγματος του εν λόγω φυσικού προσώπου και τα οποία παρέχουν μοναδικές πληροφορίες σχετικά με την φυσιολογία ή την υγεία του εν λόγω φυσικού προσώπου,

«βιομετρικά δεδομένα»: δεδομένα προσωπικού χαρακτήρα τα οποία προκύπτουν από ειδική τεχνική επεξεργασία συνδεόμενη με φυσικά, βιολογικά ή συμπεριφορικά χαρακτηριστικά φυσικού προσώπου και τα οποία επιτρέπουν ή επιβεβαιώνουν την αδιαμφισβήτητη ταυτοποίηση του εν λόγω φυσικού προσώπου, όπως εικόνες προσώπου ή δακτυλοσκοπικά δεδομένα,

«δεδομένα που αφορούν την υγεία»: δεδομένα προσωπικού χαρακτήρα τα οποία σχετίζονται με τη σωματική ή ψυχική υγεία ενός φυσικού προσώπου, περιλαμβανομένης της παροχής υπηρεσιών υγειονομικής φροντίδας, και τα οποία αποκαλύπτουν πληροφορίες σχετικά με την κατάσταση της υγείας του,

Είναι προφανές ότι η εισαγωγή προσωπικών δεδομένων των ψευδωνυμοποίησης θολώνει τη διχοτόμηση μεταξύ προσωπικών δεδομένων και ανώνυμων προσωπικών δεδομένων. Η ψευδωνυμοποίηση επιτρέπει τη μείωση συνδεσιμότητας των προσωπικών δεδομένων με το υποκείμενο δικαιωμάτων, και είναι αντίστοιχα ένα χρήσιμο μέτρο ασφάλειας που τοποθετείται στο ενδιάμεσο μεταξύ πληροφοριών που σχετίζονται με ταυτοποιημένα προσωπικά δεδομένα και πληροφοριών από τις οποίες ένα άτομο δεν μπορεί πλέον να ταυτοποιηθεί. Η ψευδωνυμοποίηση επίσης εντάσσεται στα τεχνικά και οργανωτικά μέτρα που είναι σχεδιασμένα για να συμφωνούν με τις αρχές που θέτει ο νέος Κανονισμός, δεδομένου ότι τώρα οι υπεύθυνοι επεξεργασίας πρέπει να εφαρμόζουν το απόρρητο εκ σχεδιασμού.

Ποιες είναι οι προϋποθέσεις- αρχές που διέπουν τη νομική επεξεργασία των προσωπικών δεδομένων;

Η επεξεργασία προσωπικών δεδομένων υπόκειται στις ακόλουθες γενικές αρχές νομικής επεξεργασίας (Άρθρα 5- 11 του Κανονισμού):

1. Αρχή της νομιμότητας, αντικειμενικότητας και διαφάνειας της επεξεργασίας

2. Αρχή περιορισμού του πεδίου εφαρμογής:
τα προσωπικά δεδομένα θα πρέπει να συλλέγονται μόνο για συγκεκριμένους, ρητούς και νόμιμους σκοπούς και δε θα πρέπει να επεξεργάζονται περαιτέρω κατά τρόπο ασύμβατο με αυτούς τους σκοπούς. Εντούτοις, αυτός ο Κανονισμός αναφέρει ότι η περαιτέρω επεξεργασία για σκοπούς αρχειοθέτησης αναφορικά με το δημόσιο συμφέρον ή για σκοπούς επιστημονικούς ή ιστορική έρευνα ή για στατιστικούς λόγους δεν είναι ασύμβατη με τους αρχικούς σκοπούς, όσο πληρούνται οι προϋποθέσεις του Άρθρου 89. Επιπλέον, το Άρθρο 89 απαιτεί τη λήψη τεχνικών και οργανωτικών μέτρων, τα οποία μπορεί να περιέχουν ψευδώνυμα, δεδομένου ότι αυτοί οι σκοποί μπορούν να εκπληρωθούν κατά αυτό τον τρόπο. Κατά συνέπεια των ανωτέρω, οι ερευνητές δε θα είναι υποχρεωμένοι να λαμβάνει συναίνεση για κάθε νέα χρήση των προσωπικών δεδομένων κατά τη διάρκεια της έρευνας (συναίνεση μια φορά). Συγκεκριμένα, το Άρθρο 7 του νέου Κανονισμού σχετικά με τις προϋποθέσεις της συναίνεσης αναφέρει ότι- μεταξύ άλλων- ο υπεύθυνος επεξεργασίας έχει το βάρος απόδειξης για την συναίνεση του υποκειμένου των δεδομένων. Η συγκεκριμένη δήλωση συναίνεσης για την επεξεργασία προσωπικών δεδομένων θα πρέπει να εκφράζεται εκ των προτέρων με απλό και κατανοητό τρόπο, χωρίς καταχρηστικές ρήτρες. Συνεπώς, ο χρήστης των εφαρμογών δε θα πρέπει να θεωρείται ότι έχει συναινέσει αν απλώς αδιαφόρησε ή είχε ελλιπή ενημέρωση για την επεξεργασία. Οι υπεύθυνοι επεξεργασίας θα πρέπει να δίνουν στα υποκείμενα δικαιωμάτων το δικαίωμα να ανακαλέσουν τη συναίνεση τους οποτεδήποτε.

3. Αρχή της ελαχιστοποίησης των προσωπικών δεδομένων:
μόνο τα προσωπικά δεδομένα που είναι αναγκαία για τους αρχικούς σκοπούς θα υπόκεινται σε επεξεργασία.

4. Αρχή της ακρίβειας:
Αυτή η αρχή αναφέρεται στη λήψη όλων εκείνων των μέτρων που επιβεβαιώνουν ότι τα ανακριβή προσωπικά δεδομένα (λαμβάνοντας υπόψη τους σκοπούς για τους οποίους διεξάγεται η επεξεργασία) θα πρέπει να σβήνονται ή να διορθώνονται χωρίς καθυστέρηση.

5. Αρχή περιορισμού του χρόνου αποθήκευσης:
σύμφωνα με την αρχή αυτή, τα προσωπικά δεδομένα δεν θα έπρεπε να διατηρούνται για χρονικό διάστημα μεγαλύτερο από το αναγκαίο για τους σκοπούς που συλλέχθηκαν ή που θα επεξεργαστούν περαιτέρω. Εντούτοις, ο Κανονισμός επιτρέπει την απόκλιση από αυτή την αρχή και την αποθήκευση προσωπικών δεδομένων για μεγαλύτερες χρονικές περιόδους σε περίπτωση που τα προσωπικά δεδομένα διατηρούνται μόνο για σκοπούς αρχειοθέτησης αναφορικά με το δημόσιο συμφέρον, για σκοπούς επιστημονικούς ή ιστορικής έρευνας ή για στατιστικούς σκοπούς, σύμφωνα με το Άρθρο 89§1.

6. Αρχές ακεραιότητας και εμπιστευτικότητας:
τα προσωπικά δεδομένα θα πρέπει να επεξεργάζονται κατά τρόπο που επιτρέπει την κατάλληλη ασφάλεια των προσωπικών δεδομένων, συμπεριλαμβάνοντας την προστασία τους από αυθαίρετη ή παράνομη επεξεργασία και από τυχαία

απώλεια, καταστροφή ή φθορά, χρησιμοποιώντας τα κατάλληλα τεχνικά και οργανωτικά μέτρα. Οι υπεύθυνοι επεξεργασίας είναι αρμόδιοι για να διασφαλίσουν ότι τα προσωπικά δεδομένα διατηρούνται ασφαλή, τόσο κατά των εξωτερικών απειλών (π.χ. κακόβουλοι χάκερς) και εσωτερικές απειλές (π.χ. ανεπαρκώς εκπαιδευμένοι εργαζόμενοι). **Το GDPR τοποθετεί την υποχρέωση αυτή μέσα στους Κανόνες για την Προστασία Δεδομένων**, ενδυναμώνοντας την ιδέα ότι η ασφάλεια των δεδομένων είναι μια **θεμελιώδης υποχρέωση όλων των υπεύθυνων επεξεργασίας.** Εντούτοις, η αρχή καθεαυτή δεν έχει αλλάξει ουσιωδώς.

7. Αρχή της ευθύνης:

ο υπεύθυνος επεξεργασίας είναι υπεύθυνος και θα πρέπει να συμμορφώνεται με τις προαναφερθείσες αρχές. Οι εταιρίες θα πρέπει να εφαρμόζουν κατάλληλες ιδιωτικές πολιτικές και σταθερά μέτρα ασφαλείας, να κάνουν αξιολογήσεις της προστασίας δεδομένων σε συγκεκριμένες περιπτώσεις και να διορίζει υπεύθυνο επεξεργασίας υπό συγκεκριμένους όρους. Επιπροσθέτως, τόσο οι υπεύθυνοι επεξεργασίας όσο και οι επεξεργαστές δεδομένων θα πρέπει να **(i) διατηρούν συγκεκριμένα αρχεία για τις ενέργειες επεξεργασίας δεδομένων, (ii) διεξάγουν μια αξιολόγηση για πιο επικίνδυνη επεξεργασία, και (iii) εφαρμόζουν προστασία δεδομένων εκ σχεδιασμού και εξ ορισμού, πχ ελαχιστοποίηση δεδομένων.** Ο υπεύθυνος επεξεργασίας είναι υπεύθυνος για, και πρέπει να δείχνει συμμόρφωση στις Αρχές Προστασίας Δεδομένων. Η σχετική ένδειξη συνιστά βασική διαφορά σε σχέση με την Οδηγία. Συνεπώς, **είναι παραπάνω από επείγον να θεμελιωθεί ένα πλαίσιο που να διαβεβαιώνει τα υποκείμενα δεδομένων ότι οι υπεύθυνοι επεξεργασίας έχουν καθαρές πολιτικές ώστε να αποδείξουν ότι πληρούν τα αναγκαία πρότυπα.**

Δικαιώματα υποκειμένου δεδομένων

I. Δικαίωμα ενημέρωσης (Άρθρο 12): Ο υπεύθυνος επεξεργασίας έχει την υποχρέωση να παρέχει στο χρήστη κάθε πληροφορία που αφορά τη συλλογή και επεξεργασία Ο υπεύθυνος επεξεργασίας έχει την υποχρέωση να παρέχει στο χρήστη δωρεάν κάθε πληροφορία που αφορά τη συλλογή και επεξεργασία προσωπικών δεδομένων κατά ακριβή τρόπο, καθώς και να απαντήσει σε αιτήσεις των χρηστών χωρίς καθυστέρηση εντός συγκεκριμένων προθεσμιών. Σε κάθε περίπτωση, ο υπεύθυνος επεξεργασίας πρέπει να ειδοποιεί το υποκείμενο δεδομένων για τα ακόλουθα:

i. Την ταυτότητα του και την ταυτότητα κάθε πρόσθετου παραλήπτη προσωπικών δεδομένων

ii. Το σκοπό συλλογής ή επεξεργασίας δεδομένων

iii. Το χρόνο αποθήκευσης

iv. Το δικαίωμα υποβολής αίτησης για πρόσβαση, διόρθωση, διαγραφή προσωπικών δεδομένων

v. Το δικαίωμα καταγγελίας που έχει η επιβλέπουσα αρχή

II. Δικαίωμα πρόσβασης

(Άρθρο 15): Το υποκείμενο δεδομένων έχει το δικαίωμα να βεβαιώνεται για το εάν τα δεδομένα το έχουν υποστεί επεξεργασία και να έχει πρόσβαση στην πληροφόρηση για τους σκοπούς της επεξεργασίας, τους παραλήπτες, την περίοδο αποθήκευσης κλπ.

III. Δικαίωμα διόρθωσης

(Άρθρο 16): Το υποκείμενο δεδομένων έχει το δικαίωμα να αιτεί τη διόρθωση ανακριβών δεδομένων ή συμπλήρωση ανολοκλήρωτων δεδομένων που τον αφορούν.

IV. Δικαίωμα διαγραφής- Δικαίωμα στη λήθη

(Άρθρο 17): Δεδομένου ότι η συλλογή και επεξεργασία προσωπικών δεδομένων μπορεί να συνθέσει το προφίλ του υποκειμένου δεδομένων, είναι επιτακτικής ανάγκης να εχει το υποκείμενο δεδομένων το δικαίωμα διαγραφής των δεδομένων του, καθώς αυτά δε θα μπορούσαν να συμβάλουν στη διατήρηση της ιστορικής μνήμης ή στην ελευθερία της ενημέρωσης.

V. Δικαίωμα περιορισμού επεξεργασίας

(Άρθρο 18): Εάν τα δεδομένα υπό επεξεργασία ήταν ανακριβή, άχρηστα ή παραβιάζονταν από μια παράνομα εφαρμοσμένη επεξεργασία, το υποκείμενο έχει το δικαίωμα να ειδοποιεί τον υπεύθυνο επεξεργασίας για το σχετικό γεγονός ώστε να περιορίσει τη λανθασμένη επεξεργασία

VI. Φορητότητα δεδομένων

(Άρθρο 20): Εάν τα προσωπικά δεδομένα υποβληθούν για επεξεργασία με ηλεκτρονικά μέσα και με οργανωτικό τρόπο, το υποκείμενο δεδομένων έχει το δικαίωμα να παραλάβει αντίγραφο από τον υπεύθυνο επεξεργασίας, ο οποίος επιτρέπει περαιτέρω χρήση και μεταφορά δεδομένων σε άλλο πρόσωπο.

VII. Δικαίωμα εναντίωσης

(Άρθρα 21 & 22): Το υποκείμενο δεδομένων έχει το δικαίωμα να εναντιωθεί στην επεξεργασία προσωπικών δεδομένων με αυτοματοποιημένα μέσα και δημιουργία προφίλ με σκοπό να αξιολογήσουν προσωπικά χαρακτηριστικά τα οποία αφορούν το ίδιο πρόσωπο, αναλύοντας ή προβλέποντας την επίδοση του στην εργασία, την οικονομική του κατάσταση, τη θέση του, την υγεία και τη συμπεριφορά του. Η δημιουργία του προφίλ φαίνεται να χρησιμεύει από διαφημιστικούς σκοπούς μέχρι την πρόσληψη προσωπικού βάσει συγκεκριμένων κριτηρίων και θεωρείται η βάση για πιο προσωποποιημένες υπηρεσίες. The aforementioned rights of the data subject can be restricted by a way of legislative measure in the Union or Member State Law, as Article 23 provides.

Το ΝΕΟ Άρθρο 25: Προστασία δεδομένων εκ σχεδιασμού κι εξ ορισμού

Μια από τις αλλαγές που πρέπει να εφαρμοστεί υπό το νέο "GDPR" είναι η ρητή αναγνώριση των εννοιών 'ιδιωτικότητα εκ σχεδιασμού' και 'ιδιωτικότητα εξ ορισμού'. Οι επιχειρήσεις τώρα θα υπόκεινται σε μια συγκεκριμένη υποχρέωση να λαμβάνουν υπόψη τους την ιδιωτικότητα των δεδομένων στα αρχικά στάδια σχεδιασμού ενός project καθώς καθ' όλη τη διάρκεια του κύκλου επεξεργασίας των σχετικών δεδομένων as well as throughout the lifecycle of the relevant data processing.

• Τι προβλέπεται σήμερα;

Η σύγχρονη Οδηγία για την Προστασία Δεδομένων στην ΕΕ δεν έχει τις έννοιες 'ιδιωτικότητα εκ σχεδιασμού' ή 'ιδιωτικότητα εξ ορισμού', ούτε υφίσταται ρητή υποχρέωση που να προβλέπει ότι η ιδιωτικότητα θα έπρεπε να είναι μια μείζονος σημασίας σκέψη κατά το στάδιο σχεδιασμού του project. Εντούτοις, η Οδηγία επιβάλλει μια υποχρέωση στον υπεύθυνο επεξεργασίας να εφαρμόζει τα κατάλληλα τεχνικά και οργανωτικά μέτρα για να προστατεύσουν προσωπικά δεδομένα κατά παράνομης επεξεργασίας. Με την επιβολή μιας συγκεκριμένης 'ιδιωτικότητα εκ σχεδιασμού' προϋπόθεσης, το GDPR επεκτείνει την προϋπόθεση για να εφαρμόσει τα κατάλληλα τεχνικά και οργανωτικά μέτρα για να διασφαλίσει ότι η ιδιωτικότητα και η προστασία δεδομένων δεν είναι πλέον μια εκ των υστέρων σκέψη.

Αφ' ης στιγμής ανακοινώθηκε το προσχέδιο του Κανονισμού το 2012, η 'ιδιωτικότητα εκ σχεδιασμού' ήταν το υποκείμενο των συζητήσεων από πολλούς νομοθέτες προκειμένου να διασφαλίσουν ότι η έννοια επιτυγχάνει την επιθυμητή αποτελεσματικότητα

• Τι θα επιβάλλει ο νέος Κανονισμός;

Ενώ η έννοια 'ιδιωτικότητα εκ σχεδιασμού' υπάρχει, της έχει δοθεί τώρα ιδιαίτερη αναγνώριση και συνδέεται με την επιβολή. Υπό την προτεινόμενη προϋπόθεση 'ιδιωτικότητα εκ σχεδιασμού', οι εταιρείες θα χρειαστούν πολιτικές σύμφωνες με τον σχεδιασμό, διαδικασίες και τα συστήματα κατά την παραγωγή ενός προϊόντος ή επεξεργασία.

Η 'ιδιωτικότητα εκ σχεδιασμού' αρχή περιγράφεται με 7

βασικά χαρακτηριστικά:

1. πρόνοια αντί για επανάληψη δράσης: αποτρεπτικό παρά θεραπεύσιμο (Η βασική ιδέα της αρχής αυτής είναι ότι θα έπρεπε να σκέφτεσαι το απόρρητο δεδομένων κατά την έναρξη του σχεδιασμού επεξεργασίας ασφάλειας των δεδομένων —όχι κατόπιν παραβίασης δεδομένων);
2. προστασία ιδιωτικότητας από την προεπιλεγμένη ρύθμιση των παραμέτρων;
3. προστασία ιδιωτικότητας από τον σχεδιασμό των συστημάτων και τις επιχειρηματικές επεξεργασίες;
4. διασφαλίζει την πλήρη λειτουργικότητα χωρίς να αγνοεί την προστασία προσωπικών δεδομένων;
5. από την αρχή ως το τέλος ασφάλεια για όλο τον κύκλο της ενημέρωσης;
6. οραματικότητα και διαφάνεια;
7. σεβασμός στην ιδιωτικότητα του χρήστη μέσω μιας Χρηστο-Κεντρικής Προσέγγισης.

Κατά την εφαρμογή των κατάλληλων τεχνικών και οργανωτικών μέτρων στο πλαίσιο αυτό, θα έπρεπε να δοθεί βάση στο κόστος εφαρμογής και στην τελευταία λέξη της τεχνολογίας. Φαίνεται σα να υπερέχει η ριψοκίνδυνη προσέγγιση που έχαιρε της προτιμήσεως του Συμβουλίου. Κατά την λήψη της απόφασης πρί καταλλήλων μέτρων, οι επιχειρήσεις θα έπρεπε να λάβουν υπόψη τους τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας καθώς και τους κινδύνους για τα δικαιώματα και τις ελευθερίες των ατόμων. Αυτή η προσέγγιση σημαίνει ότι οι επιχειρήσεις θα έχουν μεγαλύτερη ευελιξία στο να καθορίζουν πώς φαίνεται στην πράξη η συμμόρφωση.

Κάνοντας έναν τέτοιο καθορισμό, οι επιχειρήσεις μπορεί να χρειαστεί να αναλογιστούν θέματα όπως εάν ένα σύστημα επεξεργασίας προσωπικών δεδομένων πελατών/ εργαζομένων θα μπορούσε, για παράδειγμα να:

• Επιτρέπει να αντιπαραβάλλονται τα προσωπικά δεδομένα με ευκολία προκειμένου να συμφωνούν με τις αιτήσεις των υποκειμένων για παροχή πρόσβασης;
• Επιτρέπει την απόκρυψη των δεδομένων των πελατών που έχουν εναντιωθεί στην παραλαβή άμεσης διαφήμισης; ή
• Επιτρέπει στον υπεύθυνο επεξεργασίας να ικανοποιεί τις προϋποθέσεις του Κανονισμού για τη φορητότητα των δεδομένων..

Οι υπεύθυνοι επεξεργασίας θα έπρεπε να λάβουν υπόψη τους εάν τα σχετικά προσωπικά δεδομένα μπορούν να ψευδωνυμοποιηθούν- ειδική μνεία στην ψευδωνυμοποίηση γίνεται ως ένα παράδειγμα μέτρου που είναι σχεδιασμένο για να ενσωματώνει τις απαραίτητες ασφάλειες στην επεξεργασία προσωπικών δεδομένων.

Το GDPR επίσης εισάγει την ειδική υποχρέωση 'ιδιωτικότητα εξ ορισμού'. Η 'ιδιωτικότητα εξ ορισμού' προβλέπει ότι οι υπεύθυνοι επεξεργασίας εφαρμόζουν τα απαραίτητα τεχνικά και οργανωτικά μέτρα για να επιβεβαιώσουν ότι εξ ορισμού θα επεξεργάζονται μόνο τα προσωπικά εκείνα δεδομένα που είναι απαραίτητα για τον σκοπό αυτό. Το αποτέλεσμα αυτής της προϋπόθεσης είναι ότι οι υπεύθυνοι επεξεργασίας θα πρέπει να ελαχιστοποιήσουν την ποσότητα των συλλεγόμενων δεδομένων, την έκταση της επεξεργασίας, την περίοδο αποθήκευσης και την προσβασιμότητα τους. Σε τελική ανάλυση, εξ ορισμού, οι επιχειρήσεις θα πρέπει να επεξεργάζονται προσωπικά δεδομένα κατά την έκταση που κρίνονται αναγκαία για τους σκοπούς και να μην αποθηκεύονται για παραπάνω χρονικό διάστημα από ότι χρειάζονται προς επίτευξη τους. Συγκεκριμένα, ο υπεύθυνος επεξεργασίας θα πρέπει να επιβεβαιώσει ότι, εξ ορισμού, τα προσωπικά δεδομένα δε θα είναι διαθέσιμα σε αόριστο αριθμό προσώπων χωρίς την προηγούμενη παρεμβολή του ατόμου.

Ενώ η ισχύουσα Οδηγία περιέχει προϋποθέσεις που βεβαιώνουν ότι υπερβολικά προσωπικά δεδομένα δεν επεξεργάζονται/ διατηρούνται για παραπάνω απ' όσο χρειάζονται, ο νέος Κανονισμός περιέχει ρητή υποχρέωση να εφαρμοσθούν τα κατάλληλα τεχνικά και οργανωτικά μέτρα για να πληρούνται οι εν λόγω προϋποθέσεις.

- Ποιες είναι οι πρακτικές συνέπειες;

  Η ρητή αναφορά του νέου Κανονισμού στην 'ιδιωτικότητα εκ σχεδιασμού' και στην 'ιδιωτικότητα εξ ορισμού' σημαίνει ότι οι επιχειρήσεις θα πρέπει να εφαρμόσουν διαδικασίες και ενέργειες που θα πληρούν αυτές τις προϋποθέσεις.

  Κάποια πρακτικά βήματα που θα ήταν άξια συμβουλής είναι:

- Το να διεξάγουν μια μελέτη επιπτώσεων την οποία η επιχείρηση θα μπορεί να συμπληρώνει κάθε φορά που σχεδιάζει, προμηθεύεται ή εφαρμόζει ένα νέο σύστημα template;
- Το να επαναλαμβάνουν προδιατυπωμένες συμβάσεις με επεξεργαστές δεδομένων για να ορίσουν πώς ο κίνδυνος/ ευθύνη καταμερίζεται μεταξύ των μερών σε σχέση με την εφαρμογή των προϋποθέσεων 'ιδιωτικότητας εκ σχεδιασμού' και 'ιδιωτικότητας εξ ορισμού';
- Το να επισκέπτονται ξανά ιστοσελίδες συλλογής δεδομένων για να διαβεβαιώνουν ότι δεν έχουν συλλεγεί υπερβολικά δεδομένα;
- Το να έχουν αυτοματοποιημένες διαδικασίες διαγραφής για συγκεκριμένα προσωπικά δεδομένα, να εφαρμόζουν τεχνικά μέτρα για να επιβεβαιώνουν ότι τα προσωπικά δεδομένα θα διαγράφονται μετά από μια συγκεκριμένη περίοδο κλπ.

Μεταφορά προσωπικών δεδομένων εκτός ΕΕ

Η θέση υπό το νέο Κανονισμό που αφορά τις διεθνείς μεταφορές προσωπικών δεδομένων είναι παρόμοια με το ήδη ισχύον καθεστώς υπό την Οδηγία 95/46. Εντούτοις, υπάρχουν σημαντικές διαφορές που θα έχουν πρακτικές επιπτώσεις.

- Τι προβλέπεται σήμερα;

  Υπό την Οδηγία, οι επιχειρήσεις απαγορεύεται να μεταφέρουν προσωπικά δεδομένα εκτός Ευρωπαϊκής Οικονομικής Περιοχής προς μια τρίτη χώρα που δεν έχει επαρκή προστασία δεδομένων. Η Ευρωπαϊκή Επιτροπή έχει την εξουσία να εγκρίνει συγκεκριμένες χώρες για να τους παρέχεται επαρκές επίπεδο προστασίας δεδομένων, λαμβάνοντας υπόψη τους νόμους περί προστασίας δεδομένων σε ισχύ σε αυτές τις χώρες και τις διεθνείς συνθήκες. Οι επιχειρήσεις μπορεί επίσης να μεταφέρει προσωπικά δεδομένα σε μια τρίτη χώρα επί τη βάσει ενός μηχανισμού από τον οποίο μπορεί να προκύψει ένα

επαρκές επίπεδο προστασίας δεδομένων. Η εφαρμογή κανόνων σε σχέση με τις διεθνείς μεταφορές υπό την Οδηγία ποικίλλει από Κράτος Μέλος σε Κράτος Μέλος.

• Τι θα επιβάλλει ο νέος Κανονισμός;

Το GDPR προβλέπει όχι μόνο για την ανάδειξη μιας τρίτης χώρας αλλά ακόμη και μια περιοχή ή έναν ή περισσότερους τομείς μέσα σε μια τρίτη χώρα ώστε να παρέχεται ένα επαρκές επίπεδο προστασίας δεδομένων. Επιπλέον, αναφέρεται λεπτομερειακά στους παράγοντες που θα έπρεπε να ληφθούν υπόψη κατά την ανάδειξη αυτή.

Είναι προφανές από το νέο Κανονισμό ότι οι αποφάσεις επάρκειας δεν διαρκούν επ' αόριστον. Από τον Κανονισμό προκύπτει ότι οι αποφάσεις επάρκειας δεν είναι απαραίτητο να ισχύουν επ' αόριστον. Το GDPR οραματίζεται ότι η Ευρωπαϊκή Επιτροπή, στο πλαίσιο μιας συγκεκριμένης προδιαγραφής, θα προβλέπει ένα μηχανισμό για περιοδική επιθεώρηση, τουλάχιστον κάθε τέσσερα χρόνια. Η Επιτροπή θα είναι επίσης υποχρεωμένη να επιβλέπει σε συνεχόμενη βάση τις εξελίξεις σε τρίτα κράτη και σε διεθνείς οργανισμούς, οι οποίες θα μπορούσαν να επηρεάσουν τη λειτουργία των αποφάσεων επάρκειας της Επιτροπής, βάσει της Οδηγίας ή του GDPR. Πιο συγκεκριμένα, ο Κανονισμός οραματίζεται την δυνατότητα μιας απόφασης επάρκειας να καταργηθεί, τροποποιηθεί η να ανασταλεί, είτε έχει ληφθεί από την Οδηγία είτε το GDPR (έστω και χωρίς αναδρομικά αποτελέσματα).

Το GDPR εξακολουθεί να επιτρέπει τη μεταφορά προσωπικών δεδομένων βάσει των τυπικών ρητρών για την προστασία των δεδομένων (δηλαδή Model Clauses), τις οποίες υιοθέτησε η Επιτροπή, και να αναγνωρίζει επίσημα τη δυνατότητα μεταφορών βάσει των εγκεκριμένων Δεσμευτικών Εταιρικών Κανόνων ενός οργανισμού. Επισημαίνεται ότι το GDPR δηλώνει ρητά ότι τέτοιου είδους μεταφορών δύνανται να πραγματοποιηθούν χωρίς να απαιτούν συγκεκριμένη αδειοδότηση από μία αρχή προστασίας δεδομένων ("DPA").

Επιπλέον το GDPR αποσκοπεί στην εισαγωγή και άλλων μηχανισμών για τη νομιμοποίηση διεθνών μεταφορών προσωπικών δεδομένων, συμπεριλαμβανομένου, για παράδειγμα:

- Μεταφορές βάσει τυπικών ρητρών προστασίας δεδομένων, υιοθετημένων από μία DPA και εγκεκριμένων από την Επιτροπή,
- Μεταφορές σύμφωνες με συμβατικές ρήτρες μεταξύ του υπεύθυνου επεξεργασίας και του επεξεργαστή, του επεξεργαστή ή του λήπτη των δεδομένων στο τρίτο κράτος (όπου αυτές οι συμβατικές ρήτρες έχουν εγκεκριθεί από την αρμόδιο DPA),
- Μεταφορές βάσει ενός εγκεκριμένου κώδικα συμπεριφοράς (για παράδειγμα ενός κώδικα συμπεριφοράς που αφορά στην μεταφορά προσωπικών δεδομένων σε τρίτα κράτη, ο οποίος έχει εγκεκριθεί από την αντίστοιχη DPA.
- Μεταφορές σύμφωνες με ένα εγκεκριμένο μηχανισμό πιστοποίησης (για παράδειγμα μία σφραγίδα ή σήμα προστασίας δεδομένων η οποία έχει εκδοθεί από ένα ειδικευμένο σώμα πιστοποίησης ή από την αρμόδια DPA βάσει κριτηρίων που έχουν εγκριθεί από την αρμόδια DPA ή από το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων).

Στις δύο τελευταίες περιπτώσεις, οι μεταφορές πρέπει επίσης να βασίζονται σε επιτακτική και εφαρμοστέα δέσμευση του υπεύθυνου επεξεργασίας ή του επεξεργαστή στο τρίτο κράτος να εφαρμόσει τις αντίστοιχες δικλείδες ασφαλείας, συμπεριλαμβανομένων και αυτών που αφορούν στα δικαιώματα των υποκειμένων των δεδομένων.

Οι αποκλίσεις που προβλέπονται στην Οδηγία θα εξακολουθούν να βρίσκονται σε ισχύ, με την εξαίρεση κάποιων τροποποιήσεων, για παράδειγμα απαιτείται ρητή συναίνεση στις προτεινόμενες μεταφορές εάν αυτές πραγματοποιούνται

βάσει απόκλισης ως προς τη συναίνεση. Το GDPR υπογραμμίζει την περιορισμένη εφαρμογή αυτών των αποκλίσεων περιγράφοντάς αυτές ως «Παρεκκλίσεις για συγκεκριμένες καταστάσεις».

Επιπροσθέτως, το GDPR εισάγει μία νέα παρέκκλιση στην περίπτωση όπου η μεταφορά δεν μπορεί να πραγματοποιηθεί βάσει των μηχανισμών που περιγράφονται στο GDPR ή όταν καμία από τις αποκλείσεις δεν τυγχάνουν εφαρμογή, και συγκεκριμένα εάν η μεταφορά είναι απαραίτητη για λόγους αναγκαίων εννόμων συμφερόντων του υπεύθυνου επεξεργασίας, οι οποίοι δεν υπερισχύουν τα συμφέροντα, δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων. Οποιοσδήποτε υπεύθυνος επεξεργασίας επιδιώκει να στηριχθεί σε αυτήν την παρέκκλιση, οφείλει να έχει εκτιμήσει όλες τις παραμέτρους των μεταφορών δεδομένων και βάσει αυτής της εκτίμησης να έχει προσκομίσει κατάλληλες εγγυήσεις όσον αφορά την προστασία των δεδομένων προστασίας. Η απόκλιση είναι περιορισμένη και θα εφαρμοσθεί μόνο εάν η μεταφορά δεν είναι επαναλαμβανόμενη και αφορά μόνο έναν περιορισμένο αριθμό υποκειμένων δεδομένων. Επιπλέον, ο υπεύθυνος επεξεργασίας υπόκειται σε σημαντικές ενημερωτικές απαιτήσεις – ο υπεύθυνος επεξεργασίας οφείλει να ενημερώσει το υποκείμενο δεδομένων σχετικά με τη μεταφορά και τα αναγκαία έννομα συμφέροντα που επιδιώκει ο υπεύθυνος επεξεργασίας. Ο υπεύθυνος επεξεργαστής δεδομένων οφείλει να ενημερώσει τη DPA ως προς τη μεταφορά.

Το GDPR προβλέπει επίσημη αναγνώριση στους δεσμευτικούς εταιρικούς κανόνες ως μέσο για τη νόμιμη μεταφορά προσωπικών δεδομένων εκτός της Ευρωπαϊκής Οικονομικής Περιοχής. Θεσπίζει επίσης ενιαία κριτήρια προς έγκριση από τους δεσμευτικούς εταιρικούς κανόνες τα οποία ισχύουν σε ολόκληρη την Ευρωπαϊκή Ένωση και κάνει τη διαδικασία έγκρισης από τους δεσμευτικούς εταιρικούς κανόνες να υπόκειται στο σταθερό μηχανισμό που προσδιορίζει το GDPR (μέσω των οποίων οι αρχές προστασίας δεδομένων υποχρεούνται να συνεργάζονται μεταξύ τους και όπου χρειάζεται και με την Ευρωπαϊκή Επιτροπή). Το GDPR αφαιρεί επίσης οποιαδήποτε υποχρέωση λήψης περεταίρω έγκρισης από αρχές προστασίας δεδομένων για μεταφορές προσωπικών δεδομένων βάσει των δεσμευτικών εταιρικών κανόνων.

Το GDPR εισάγει μία διάταξη σύμφωνα με την οποία οποιαδήποτε κρίση του δικαστηρίου και οποιαδήποτε απόφαση μιας διοικητικής αρχής του τρίτου κράτους που να απαιτεί από τον υπεύθυνο επεξεργασίας ή τον επεξεργαστή να μεταφέρει ή να γνωστοποιήσει προσωπικά δεδομένα θα αναγνωρίζεται ή θα έχει ισχύ μόνο εφόσον βασίζεται σε ισχύουσα διεθνή συμφωνία μεταξύ του αιτούντος τρίτου κράτους και την Ευρωπαϊκή Ένωση ή το Κράτος – Μέλος από το οποίο ζητούνται τα δεδομένα (για παράδειγμα: μία κοινή συνθήκη νομικής βοήθειας) Επομένως, για παράδειγμα, οι υπεύθυνοι επεξεργασίας και οι επεξεργαστές απαγορεύεται να συμμορφωθούν με την απαίτηση ενός δικαστηρίου εκτός της ΕΕ για γνωστοποίηση προσωπικών δεδομένων σύμφωνα με το GDPR όταν αυτή η απαίτηση δεν βασίζεται σε αντίστοιχη διεθνή συμφωνία. Ωστόσο το Ηνωμένο Βασίλειο επέλεξε να μην εμπίπτει στον συγκεκριμένο περιορισμό.

- Ποιες είναι οι πρακτικές επιπτώσεις;

  Λόγω της σαφήνειας και της αυξανόμενης απλότητας που εισάγεται όσον αφορά τους δεσμευτικούς εταιρικούς κανόνες, είναι πιθανό ότι περισσότερες επιχειρήσεις θα επιλέξουν τους δεσμευτικούς εταιρικούς κανόνες ως μέσο για τη νομιμοποίηση των διεθνών μεταφορών προσωπικών δεδομένων. Αυτή η τάση είναι πιθανό να αυξηθεί και στις εφαρμογές δεσμευτικών εταιρικών κανόνων για τους επεξεργαστές (χωρίς ωστόσο ο Κανονισμός να αναφέρει τους δεσμευτικούς εταιρικούς κανόνες για τους επεξεργαστές).

  Το γεγονός ότι το GDPR απασχολείται με την ανάγκη να γνωστοποιεί ή να αποκτά έγκριση από τη DPA, εάν οι προϋποθέσεις του GDPR ικανοποιούνται διαφορετικώς,

πιθανόν να σημάνει ουσιώδη αλλαγή στο πλαίσιο των διεθνών μεταφορών. Η απόκτηση της ευρωπαϊκής σφραγίδας προστασίας δεδομένων ή άλλης αναγνωρισμένης σφραγίδας θα αποτελέσει πιθανότατα μία εναλλακτική στο προσεχές μέλλον.

Επιπλέον, είναι πιθανό οι επιχειρήσεις να δύνανται να επωφεληθούν από την πρόσθετη παρέκκλιση, δηλαδή από το γεγονός ότι η μεταφορά πραγματοποιείται βάση των εννόμων συμφερόντων του επεξεργαστή – αυτή η παρέκκλιση μπορεί να είναι ιδιαίτερα χρήσιμη στο πλαίσιο της εφάπαξ μεταφοράς ενός περιορισμένου αριθμού προσωπικών δεδομένων, οπότε ήταν δύσκολη η απόκτηση συναίνεσης (και συγκεκριμένα ρητή συναίνεση). Ωστόσο, είναι αρκετά περιοριστικό εκ φύσεως και στην πρακτική χρησιμοποιείται περιοριστικά.

Όπου η αίτηση για προσωπικά δεδομένα λαμβάνεται από ένα δικαστήριο εκτός ΕΕ ή αρχή (η οποία δεν βασίζεται σε κατάλληλη διεθνή συμφωνία), οι επιχειρήσεις των κρατών μελών της ΕΕ, εκτός του Ηνωμένου Βασιλείου, θα βρίσκονται στην δύσκολη θέση να αποφασίσουν είτε να παραβιάσουν το GDPR ή τους νόμους του κράτους του οποίου τα δικαστήρια ή οι αρχές επιδιώκουν την γνωστοποίηση προσωπικών δεδομένων.

Οι εταιρίες που παραβαίνουν τις διατάξεις του Κανονισμού που αφορούν στη διεθνή μεταφορά προσωπικών δεδομένων μπορεί να υπόκεινται σε διοικητικά πρόστιμα τα οποία ανέρχονται έως το ποσό των 20.000.000 ευρώ ή, στην περίπτωση επιχείρησης, έως 4% του συνολικού παγκόσμιου κύκλου εργασίας του προηγούμενου έτους χρήσης, όποιο είναι υψηλότερο. Βάσει του επιπέδου των κυρώσεων, θα ήταν συνετό για τις επιχειρήσεις να ελέγχουν τις ροές των δεδομένων τους σε αυτή τη φάση και να εξασφαλίζουν ότι θα συμμορφώνονται με τον Κανονισμό μέχρι τη στιγμή που θα αρχίσουν να ισχύουν οι νέοι κανόνες. Οι εταιρείες θα έπρεπε επίσης να εξετάσουν το ενδεχόμενο να θέσουν μία πρακτική σε ισχύ όσον αφορά στις αιτήσεις για προσωπικά δεδομένα από μία αρχή επιβολής του νόμου εκτός ΕΕ –αυτή θα μπορούσε να είναι μέρος μίας πρακτικής όσον αφορά αιτήσεις για προσωπικά δεδομένων από αρχές επιβολής του νόμου εν γένει.

Το σύστημα εποπτείας: Ανεξάρτητες εθνικές αρχές και το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων

Ο Κανονισμός επιβεβαιώνει την υπάρχουσα υποχρέωση για τα Κράτη Μέλη να θεσπίζουν μια ανεξάρτητη εποπτική αρχή σε εθνικό επίπεδο. Τα Άρθρα 51-59 περιγράφουν τις προϋποθέσεις λειτουργίας των αρχών αυτών. Όπως γίνεται σαφές, «κάθε εποπτική αρχή εκτελεί τα καθήκοντά της και ασκεί τις εξουσίες της σύμφωνα με τον παρόντα κανονισμό με πλήρη ανεξαρτησία» και θα πρέπει να τα εκτελούν «χωρίς εξωτερικές επιρροές, είτε άμεσες είτε έμμεσες, και να μη ζητούν ούτε λαμβάνουν οδηγίες από κανέναν».

Ο Κανονισμός επίσης στοχεύει στην θέσπιση μηχανισμών που θα δημιουργήσουν σταθερότητα στην εφαρμογή της νομοθεσίας για την προστασία δεδομένων σε όλη την ΕΕ. Πιο συγκεκριμένα, σε κρίσιμες διασυνοριακές υποθέσεις όπου εμπλέκονται διάφορες εθνικές εποπτικές αρχές, μόνο μια εποπτική απόφαση λαμβάνεται. Αυτή η αρχή, γνωστή ως "the one-stop-shop", σημαίνει ότι μια εταιρεία με θυγατρικές σε διάφορα Κράτη Μέλη πρέπει να διαχειριστεί μόνο την αρχή προστασίας δεδομένων στο Κράτος Μέλος της κύριας έδρας της.

Επιπλέον, σύμφωνα με το Άρθρο 37, κάθε εταιρεία που διαχειρίζεται και επεξεργάζεται προσωπικά δεδομένα είναι υποχρεωμένη να διορίζει έναν υπεύθυνο προστασίας δεδομένων, ο οποίος θα έχει γνώση της νομοθεσίας για την προστασία δεδομένων και τις αντίστοιχες πρακτικές.

Η συμφωνία περιλαμβάνει επίσης την ίδρυση ενός Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων. Όπως διαφαίνεται από τα Άρθρα 68-76, αυτό το Συμβούλιο θα αποτελείτο από εκπροσώπους από όλες τις 28 ανεξάρτητες εποπτικές αρχές και θα **αντικαθιστούσε την υπάρχουσα ομάδα προστασίας των προσώπων του Άρθρου 29.**

Αναγνωρίζει το δικαίωμα των υποκειμένων των δεδομένων να παραπονούνται επισήμως σε μια εποπτική αρχή, καθώς και το δικαίωμα τους στην δικαστική αποκατάσταση, αποζημίωση και ευθύνη. Για να εξασφαλίσουν την εγγύτητα των ατόμων για τις αποφάσεις που τους αφορούν, τα υποκείμενα δεδομένων θα έχουν το δικαίωμα να ελεγχθεί η απόφαση της αρχής προστασίας δεδομένων από το εθνικό τους δικαστήριο. Αυτό είναι ανεξάρτητα από το κράτος μέλος στο οποίο είναι εγκατεστημένος ο υπεύθυνος επεξεργασίας που τον αφορά.
Προβλέπονται πολύ σοβαρές κυρώσεις κατά των υπεύθυνων επεξεργασίας ή τω επεξεργαστών που παραβιάζουν τους κανόνες προστασίας δεδομένων. Οι υπεύθυνοι επεξεργασίας μπορεί να έρθει αντιμέτωπος με πρόστιμο έως και €20 million ή 4% των ετήσιων παγκόσμιων πόρων. Αυτές οι διοικητικές κυρώσεις θα επιβληθούν από τις εθνικές αρχές προστασίας δεδομένων.

Ποινές- Ευθύνη

- Τι προβλέπεται σήμερα;

  Βάσει των ισχύοντων ενωσιακών κανόνων για την προστασία δεδομένων, οι πάροχοι υπηρεσιών που επεξεργάζονται προσωπικά δεδομένα για λογαριασμό άλλων επιχειρήσεων δεν μπορούν να φέρουν άμεση ευθύνη για μια παραβίαση ασφάλειας δεδομένων.
  Εάν οι επεξεργαστές δεδομένων είναι υπαίτιοι για παραβιάσεις δεδομένων, τότε ο υπεύθυνος επεξεργασίας που συναλλάχθηκε μαζί τους είναι αυτός που ευθύνεται για κάθε μη επίδειξη συμμόρφωσης προς τους νόμους περί προστασίας δεδομένων, παρ' όλο που ο επεξεργαστής δεδομένων θα μπορούσε να ευθύνεται απέναντι στον υπεύθυνο επεξεργασίας βάσει της σύμβασης τους.

- Τι θα επιβάλλει ο νέος Κανονισμός;

  Ο Κανονισμός αναφέρεται σε αυτό τον παραλογισμό αλλά κάνει μια διάκριση μεταξύ του μέγιστου προστίμου που οι αρχές προστασίας δεδομένων θα μπορούν να επιβάλλουν κατά του υπεύθυνου επεξεργασίας και του αντίστοιχου προστίμου κατά των επεξεργαστών δεδομένων για αποτυχίες στην ασφάλεια των δεδομένων.
  Οι σχετικές προβλέψεις για την ασφάλεια των δεδομένων περιλαμβάνονται στα Άρθρα 5 και 32 του Κανονισμού.
  Το Άρθρο 5 θεσπίζει βασικούς κανόνες για τα προσωπικά δεδομένα που εφαρμόζονται μόνο στους υπεύθυνους επεξεργασίας, οι οποίοι θεωρούνται ως θεμελιώδεις για την προστασία δεδομένων. Ένας από αυτούς τους κανόνες προβλέπει ότι οι υπεύθυνοι επεξεργασίας πρέπει να διαβεβαιώνουν ότι τα προσωπικά δεδομένα «υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλεια των δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά, με τη χρησιμοποίηση κατάλληλων τεχνικών ή οργανωτικών μέτρων».
  Σύμφωνα με τις διατάξεις του Άρθρου 83 του Κανονισμού για τα διοικητικά πρόστιμα, όταν οι υπεύθυνοι επεξεργασίας παραβιάζουν την προϋπόθεση αυτή του Άρθρου 5, θα τους επιβληθεί το υψηλότερο πρόστιμο που θα μπορούσαν οι αρχές προστασίας δεδομένων να επιβάλλουν, υπό το μεταρρυθμισμένο πλαίσιο Στον αντίποδα, αν οι επεξεργαστές δεδομένων παραβιάσουν τις καταστατικές τους υποχρεώσεις για την ασφάλεια των δεδομένων, όπως θεσπίζονται στο Άρθρο32, το οποίο επιτάσσει να «εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων» που αφορούν την επεξεργασία προσωπικών δεδομένων, τότε θα μπορούσε να τους επιβληθεί πρόστιμο το πολύ μέχρι €10εκ ή 2% των ετήσιων παγκόσμιων πόρων.

Οι υπεύθυνοι επεξεργασίας υπόκεινται επίσης στις υποχρεώσεις του Άρθρου 32. Φαίνεται συνεπώς ανοικτό στις εθνικές αρχές προστασίας δεδομένων να επιβάλουν πρόστιμο στους υπεύθυνους επεξεργασίας για κάθε αποτυχία κατά την ασφάλεια των δεδομένων υπό το Άρθρο 5 ή 32. Η επιλογή τους υπό αυτές τις συνθήκες θα επηρέαζε τη σοβαρότητα των προστίμων που θα μπορούσαν να επιβάλουν.
Το εάν τα μέτρα ασφαλείας είναι κατάλληλα σε κάθε περίσταση εξαρτάται από «την τελευταία λέξη της τεχνολογίας, τα έξοδα εφαρμογής, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας καθώς και τον τυχόν μεγάλο και σοβαρό κίνδυνο για τα δικαιώματα και ελευθερίες των φυσικών προσώπων», σύμφωνα με τον Κανονισμό αυτό.

- **Ποιες είναι οι πρακτικές συνέπειες;**

  Ο νέος Κανονισμός θα είναι στο σύνολο του αυστηρότερος και θα περιλαμβάνει μεγαλύτερες ποινές για εκείνες τις επιχειρήσεις που ΔΕΝ εφαρμόζουν τον Κανονισμό. Ο πίνακας που ακολουθεί δείχνει τις συγκεκριμένες ποινές που υπάρχουν, λαμβάνοντας υπόψη τις διαφορετικές περιστάσεις:

Θέμα	Η Οδηγία	Ο νέος Κανονισμός	Συνέπεια
Αποζημίωση κι ευθύνη Η ενωσιακή νομοθεσία για την προστασία δεδομένων παρουσιάζει την εικόνα ότι οι υπεύθυνοι επεξεργασίας (και πιο συχνά οι επεξεργαστές) θα έπρεπε να είναι υπεύθυνοι να πληρώνουν αποζημίωση στα υποκείμενα των δικαιωμάτων σε περίπτωση παράνομης επεξεργασίας των προσωπικών δεδομένων.	**Αρθ.23** Ένα υποκείμενο δεδομένων που έχει υποστεί ζημία λόγω παράνομης επεξεργασίας των δικών του προσωπικών δεδομένων δικαιούται να λάβει αποζημίωση από τον υπεύθυνο επεξεργασίας για τη ζημία αυτή. Ο υπεύθυνος επεξεργασίας μπορεί να εξαιρεθεί από αυτή την ευθύνη εν όλω ή εν μέρει αν αποδείξει ότι δεν είναι υπεύθυνος για το ζημιογόνο γεγονός.	Αρθ.82(1)-(2), (4) Ένα υποκείμενο δεδομένων που έχει υποστεί ζημία λόγω παράνομης επεξεργασίας των δικών του προσωπικών δεδομένων δικαιούται να λάβει αποζημίωση από τον υπεύθυνο επεξεργασίας ή τον επεξεργαστή για τη ζημία αυτή	Ο νέος Κανονισμός **επεκτείνει** το πεδίο **ευθύνης** για καταπατήσεις του ενωσιακού δικαίου αναφορικά με την προστασία δεδομένων **τόσο στους υπεύθυνους επεξεργασίας όσο και στους επεξεργαστές.**

Ευθύνη συνδεδεμένων **υπεύθυνων επεξεργασίας**	Αρθ.23(2) Ο υπεύθυνος επεξεργασίας μπορεί να εξαιρεθεί από την ευθύνη εν όλω ή εν μέρει, εάν αποδείξει ότι δεν έχει ευθύνη για το ζημιογόνο γεγονός .	• Κάθε υπεύθυνος επεξεργασίας που εμπλέκεται στην επεξεργασία έχει ευθύνη για το ζημιογόνο γεγονός που προκάλεσε • Ένας επεξεργαστής έχει ευθύνη για την προκληθείσα ζημία από κάποια από τις ενέργειες επεξεργασίας (του ιδίου ή υπο-επεξεργαστή) που δεν είναι σύμφωνες με τις υποχρεώσεις που θέτει ο νέος Κανονισμός ή που παραβιάζει τις οδηγίες του υπεύθυνου επεξεργασίας • Για τη διασφάλιση αποτελεσματικής αποζημίωσης, κάθε υπεύθυνος επεξεργασίας ή επεξεργαστής θα φέρουν ευθύνη για το σύνολο της προκληθείσας ζημίας, εάν εμπλέκονται στην ίδια επεξεργασία και ευθύνονται για τη ζημία αυτή. Αρθ.26(3), 82(3)-(5) Τα υποκείμενα δικαιωμάτων έχουν δικαίωμα να στραφούν κατά οιουδήποτε συνδεδεμένου υπεύθυνου επεξεργασίας. Κάθε συνδεδεμένος υπεύθυνος επεξεργασίας φέρει ευθύνη για το σύνολο της ζημίας, παρ ΄όλο	 καθιστά τους συνδεδεμένους υπεύθυνους επεξεργασίας πλήρως υπεύθυνους. Αν η «πλήρης αποζημίωση» αποδοθεί στο ζημιωμένο υποκείμενο δεδομένων, οι συνδεδεμένοι υπεύθυνοι επεξεργασίας

Όταν ανακύπτει ζήτημα ευθύνης σε περίπτωση συνδεδεμένων υπεύθυνων επεξεργασίας , η ενωσιακή νομοθεσία για την προστασία δεδομένων θέτει σε προτεραιότητα την διασφάλιση προστασίας του υποκειμένου δεδομένων. Η ερώτηση για το πώς θα διαμοιραστεί η ευθύνη μεταξύ των συνδεδεμένων υπεύθυνων επεξεργασίας είναι μια δευτερεύουσα ερώτηση από την οπτική του ενωσιακού δικαίου για την προστασία των δεδομένων.		που το εθνικό δίκαιο μπορεί να διαμοιράζει την ευθύνη ανάμεσα τους. Εάν ο ένας συνδεδεμένος υπεύθυνος επεξεργασίας έχει πληρώσει όλη την αποζημίωση, μπορεί μετά να στραφεί κατά των λοιπών συνδεδεμένων υπεύθυνων επεξεργασίας για να καλύψουν το μερίδιο της ζημίας.	θα στραφούν μεταξύ τους αναγωγικά. Αυτό σημαίνει ότι κάποιοι συνδεδεμένοι υπεύθυνοι επεξεργασίας μπορεί να έχουν μεγαλύτερη ευθύνη για αξιώσεις αποζημίωσης υπό το καθεστώς του νέου Κανονισμού.
Εξαιρέσεις από την ευθύνη Αναφορικά με τις γενικές αρχές περί ευθύνης, ο υπεύθυνος επεξεργασίας ή ο επεξεργαστής εξαιρούνται από την ευθύνη στο βαθμό που δεν ήταν υπεύθυνοι για την σχετική ζημία.	Αρθ.23(2) Ο υπεύθυνος επεξεργασίας μπορεί να εξαιρείται από την ευθύνη, εν όλω ή εν μέρει, εάν αποδείξει ότι δεν φέρει ευθύνη για το ζημιογόνο γεγονός. Μπορεί επίσης να είναι μια άμυνα για να δείξει ότι η ευθύνη ανέκυψε εν όλω ή εν μέρει από ανωτέρα βια.	Αρθ.82(3) Ο υπεύθυνος επεξεργασίας ή ο επεξεργαστής εξαιρούνται από την ευθύνη εάν αποδείξουν ότι δεν φέρουν ευθύνη για το ζημιογόνο γεγονός. Δεν υφίσταται αναφορά σε περιπτώσεις ανωτέρας βίας.	Ο νέος Κανονισμός δημιουργεί την πιθανότητα **άμεσης ευθύνης των επεξεργαστών** και έτσι επεκτείνει την εξαίρεση στους επεξεργαστές. Σε κάθε περίπτωση, αυτή η αρχή παραμένει ίδια από την Οδηγία. Η Οδηγία εξαιρεί τους υπεύθυνους επεξεργασίας από την ευθύνη για ζημία που ανακύπτει σε περίπτωση ανωτέρας βίας . Ο νέος Κανονισμός δεν περιέχει τέτοια εξαίρεση, με την έννοια ότι οι υπεύθυνοι επεξεργασίας μπορεί να αναλαμβάνουν τον κίνδυνο σε περιπτώσεις ανωτέρας βίας.

Διοικητικά πρόστιμα Όπως συνηθίζεται σε άλλους τομείς του κανονιστικού δικαίου, ένα σύστημα ποινών και διοικητικά πρόστιμα υπάρχει για να διασφαλίζει συμμόρφωση προς τις προϋποθέσεις που θέτει το ενωσιακό δίκαιο για την προστασία των δεδομένων. Εναπόκειται στις εθνικές αρχές προστασίας δεδομένων να αποφασίσουν αν θα επιβάλλουν τέτοιο πρόστιμο και ,αν ναι, να αποφασίσουν ποιο θα έπρεπε να είναι το ποσό του προστίμου αυτού.	Αρθ.8(5), 24 Τα Κράτη Μέλη θέτουν τους δικούς τους κανόνες αναφορικά με τους μηχανισμούς βάσει των οποίων αποφασίζουν και επιβάλλουν διοικητικά πρόστιμα. Γενικά, οι αρχές προστασίας δεδομένων έχουν ευρεία διακριτική ευχέρεια αναφορικά με τις περιστάσεις στις οποίες επιβάλλουν πρόστιμο στο ποσό που θα ανέρχεται το πρόστιμο.	Αρθ.83 Κάθε αρχή προστασίας δεδομένων πρέπει να διασφαλίζει ότι επιβάλλει ποινές και διοικητικά πρόστιμα κατά τρόπο αποτελεσματικό και αναλογικό. Όταν το νομικό σύστημα ενός Κράτους Μέλους δεν προβλέπει διοικητικά πρόστιμα, μπορεί να δημιουργηθούν πρόστιμα από τις αρχές προστασίας δεδομένων και να επιβάλλονται από τα εθνικά δικαστήρια.	 Η έννοια των διοικητικών προστίμων για τις παραβιάσεις του ενωσιακού δικαίου για την προστασία δεδομένων αλλάζει μόνο ελάχιστα υπό το νέο Κανονισμό. Εντούτοις, είναι σημαντικό να σημειωθεί ότι, υπάρχουν βασικές αλλαγές τόσο για το ποσό των προστίμων όσο και οι τομείς που σχετίζονται με τη λήψη αποφάσεων για τα πρόστιμα.
Μέγιστα διοικητικά πρόστιμα Όπως ισχύει σε πολλούς άλλους τομείς του κανονιστικού δικαίου, το ενωσιακό δίκαιο προστασίας δεδομένων έχει την έννοια ενός μέγιστου προστίμου, προκειμένου να βοηθήσει να διασφαλίσει ότι τα πρόστιμα εφαρμόζονται σε μια ευρεία διαρκή και αναλογική κλίμακα.	Αρθ. 24 Στην πλειονότητα των περιπτώσεων, το μέγιστο πρόστιμο υπό το εθνικό δίκαιο προστασίας δεδομένων για μια μόνο παραβίαση είναι λιγότερο από €1 εκ. (παρ' όλο που η Γαλλία είναι στη διαδικασία αύξησης των προστίμων που εφαρμόζονται υπό το εθνικό της δίκαιο).	Αρθ.83(5)-(6) Το μέγιστο πρόστιμο που μπορεί να επιβληθεί για σοβαρές παραβιάσεις του νέου Κανονισμού είναι το πολύ €20 εκ. ή 4% των παγκόσμιων εσόδων για την προηγούμενη οικονομική χρονιά.	 Ο νέος Κανονισμός θέτει νέα μέγιστα το πολύ €20 εκ. ή 4% των παγκόσμιων εσόδων για την προηγούμενη οικονομική χρονιά, αλλάζοντας δραστικά τις πιθανές οικονομικές επιπτώσεις παραβίασης του ενωσιακού δικαίου για την προστασία δεδομένων.

Εφαρμογή διοικητικών **προστίμων από τις αρχές προστασίας δεδομένων** Το θέμα του πώς οι αρχές προστασίας δεδομένων αποφασίζουν αν θα επιβάλλουν ένα πρόστιμο και, αν ναι, ποιο θα είναι το ύψος του, είναι θεμελιώδες για να διασφαλίσει τη διαρκή εφαρμογή της ενωσιακής νομοθεσίας για την προστασία δεδομένων.	Η Οδηγία δεν διατείνεται για το πώς θα πρέπει οι αρχές προστασίας δεδομένων να αποφασίσουν εάν θα επιβάλλουν ένα διοικητικό πρόστιμο, ή για το ύψος του προστίμου.	Αρθ.83(2) Όταν λαμβάνεται η απόφαση για το εάν θα επιβληθεί ένα πρόστιμο και ποιο θα είναι το ύψος αυτού, οι αρχές προστασίας δεδομένων θα πρέπει να επιδείξουν προσοχή στα εξής: • Τη φύση, βαρύτητα και διάρκεια της παραβίασης; • Τον αριθμό των ζημιωθέντων υποκειμένων δεδομένων και το βαθμό της προκληθείσας ζημίας; • Τον σκόπιμο ή εκ παραλείψεως χαρακτήρα της παραβίασης; • Κάθε ενέργεια του υπεύθυνου επεξεργασίας ή του επεξεργαστή για να περιορίσουν τη ζημία; • Κάθε σχετική προηγούμενη παραβίαση από τον υπεύθυνο επεξεργασίας ή τον επεξεργαστή; • Το βαθμό συνεργασίας με την αντίστοιχη αρχή προστασίας δεδομένων; • Εάν κάποια παραβίαση καταγγέλθηκε από τον ίδιο τον ζημιώσαντα υπεύθυνο επεξεργασίας ή τον επεξεργαστή; και • Κάθε άλλος επιβαρυντικός ή ελαφρυντικός παράγοντας.	By explaining the factors that are relevant to determining the imposition and amount of a fine, the GDPR provides organisations with significantly greater certainty regarding the risk of a fine.

Ποινές και ποινικές κυρώσεις Για κάθε παραβίαση ενωσιακού δικαίου για την προστασία δεδομένων που δεν υπόκειται σε διοικητικά πρόστιμα, τα Κράτη Μέλη μπορεί να εξειδικεύσουν πρόσθετες ποινές.	Αρθ.24 Τα Κράτη Μέλη θεσπίζουν τους δικούς τους κανόνες αναφορικά με τους μηχανισμούς απόφασης και εφαρμογής ποινών.	Αρθ.84 Τα Κράτη Μέλη θεσπίζουν τους δικούς τους κανόνες αναφορικά με τις ποινές που εφαρμόζονται σε περιπτώσεις παραβιάσεων του νέου Κανονισμού και συγκεκριμένα αυτές οι παραβιάσεις που δεν υπόκεινται σε διοικητικά πρόστιμα. Μπορούν επίσης να θεσπίζουν τους δικούς τους κανόνες για ποινικές κυρώσεις επί παραβίασης του GDPR.	 Σε ένα πρακτικό επίπεδο, είναι πιθανό να συνεχίσουν να υπάρχουν κάποιες διαφορές μεταξύ εφαρμογής ποινών, εξαιτίας της ποικιλίας των εθνικών νομοθεσιών των Κρατών Μελών. Η ενδεχόμενη εισαγωγή ποινικών κυρώσεων για παράνομη επεξεργασία προσωπικών εμφανίζει σημαντικό κίνδυνο για τις επιχειρήσεις, καθώς εξαρτάται από το πώς ερμηνεύουν τα Κράτη Μέλη και εφαρμόζουν αυτή την εξουσία.

Το παρόν κείμενο αποτελεί παρουσίαση των βασικών σημείων του νέου Κανονισμού 2016/679 επί της προστασίας των προσωπικών δεδομένων

PMN