ΣΕΒ
Σύγχρονες Επιχειρήσεις, Σύγχρονη Ελλάδα

Ο νέος Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR)

Εφαρμογή και προκλήσεις για τις επιχειρήσεις στην εποχή της ψηφιοποίησης

Μια πρωτοβουλία της Ομάδας Εργασίας
του ΣΕΒ για τα Προσωπικά Δεδομένα

Αθήνα, Οκτώβριος 2018

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Περιεχόμενα

Διαγράμματα και Πίνακες

Ακρωνύμια

ΑΠΔΠΧ	Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
ΓΕΜΗ	Γενικό Εμπορικό Μητρώο
ΔΕΕ	Δικαστήριο της Ευρωπαϊκής Ένωσης
ΔΠΧ	Δεδομένων Προσωπικού Χαρακτήρα
ΕΑ	Εκτίμηση Αντικτύπου σχετικά με την προστασία δεδομένων
ΕΕ	Ευρωπαϊκή Ένωση
ΕΣΚΑ	Εθνικό Συμβούλιο Καταναλωτή και Αγοράς
ΕΣΥΔ	Εθνικό Σύστημα Διαπίστευσης
ΥΕ	Υπεύθυνος Επεξεργασίας
ΥΠΔ	Υπεύθυνος Προστασίας Δεδομένων
GDPR	General Data Protection Regulation
IAPP	International Association of Privacy
IDC	International Data Corporation
NIS	Network and Information Systems Professionals

Το παρόν συντάχθηκε από τον Τομέα Επιχειρηματικού Περιβάλλοντος και Ρυθμιστικών Πολιτικών του ΣΕΒ, αξιοποιώντας στοιχεία που παράχθηκαν στο πλαίσιο του έργου «Μηχανισμός παρακολούθησης των αλλαγών και υποστήριξης των δράσεων ανάπτυξης και προσαρμοστικότητας της βιομηχανίας», το οποίο συγχρηματοδοτείται από την Ελλάδα και την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο) μέσω του ΕΠ «Ανταγωνιστικότητα, Επιχειρηματικότητα και Καινοτομία».

Την επιστημονική επιμέλεια του παρόντος έργου είχαν οι: Ομάδα Εργασίας ΣΕΒ «Προστασία Προσωπικών Δεδομένων» (Διαρκές Forum), Αθηνά Βουνάτσου, Senior Advisor ΣΕΒ, Σωτηρία Καλαντζή, Advisor ΣΕΒ, Μαρίνα Σπυριδάκη, Διευθύντρια του Τομέα Επιχειρηματικού Περιβάλλοντος και Ρυθμιστικών Πολιτικών του ΣΕΒ, με την υποστήριξη των Γιάννη Λαϊνά, Associate Advisor ΣΕΒ, Αυγή Οικονομίδου, Associate Advisor ΣΕΒ.

Θερμές ευχαριστίες σε όλους όσοι βοήθησαν με τη γνώμη και τις απόψεις τους στην παρούσα έκδοση.

Μήνυμα ΣΕΒ

Άκης Σκέρτσος,
Γενικός Διευθυντής

Τα data είναι το “πετρέλαιο” της 4ης βιομηχανικής επανάστασης. Σύμφωνα με εκτιμήσεις, η αξία της αγοράς των προσωπικών δεδομένων υπολογίζεται ότι θα ανέλθει σε σχεδόν €1 τρισ. το 2020, ενώ έως το 2025 εκτιμάται ότι ο όγκος των δεδομένων θα αυξηθεί από 16,1 ZB σε 163 ZB.
Αναμενόμενα, καθώς τα ίδια τα δεδομένα και η αγορά που διαμορφώνεται γύρω από αυτά διογκώνονται, αυξάνονται εκθετικά και οι κίνδυνοι παραβίασής τους ακόμη και σε μεγάλες επιχειρήσεις, με εξαιρετικά δυσμενείς επιπτώσεις. Ταυτόχρονα, η διαχείρισή τους με σεβασμό στην προσωπικότητα και την ιδιωτική ζωή του καθενός μας, θα γίνει σταδιακά βασικό κριτήριο αξιολόγησης κάθε επιχείρησης που χειρίζεται προσωπικά δεδομένα, δηλαδή πρακτικά όλων.

Πρόσφατα φαινόμενα πλημμελούς προστασίας προσωπικών δεδομένων, αλλά και η ανάγκη ρύθμισης της αγοράς των προσωπικών δεδομένων, οδήγησαν στην αυστηροποίηση του νομικού πλαισίου πανευρωπαϊκά και στη θέσπιση του νέου Γενικού Κανονισμού GDPR. Με έναρξη εφαρμογής την 25η Μαΐου 2018, ο νέος Κανονισμός, προβλέποντας ένα αρκετά αυστηρό και γραφειοκρατικό πλαίσιο, έρχεται να θωρακίσει την ιδιωτικότητα και να μεταθέσει την ευθύνη της προστασίας στην ίδια την επιχείρηση, προβλέποντας κυρώσεις ύψους έως και 4% του παγκόσμιου τζίρου για όσους αποτύχουν να συμμορφωθούν με τις απαιτήσεις του.

Ο ΣΕΒ, αντιλαμβανόμενος την πρόκληση με την οποία έρχονται αντιμέτωπες οι επιχειρήσεις και την εύλογη ανησυχία τους, υπό τον φόβο υψηλών προστίμων, αλλά και απώλειας της εμπιστοσύνης των πελατών και προμηθευτών τους, επιδιώκει να συνεισφέρει ουσιαστικά στις προσπάθειες συμμόρφωσης που καταβάλουν και σε συνεργασία με την αρμόδια ομάδα εργασίας που έχει συστήσεις για το σκοπό αυτό προχώρησε στην κατάρτιση της ειδικής έκδοσης που έχετε στα χέρια σας.

Στόχος μας είναι η κατανόηση και ερμηνεία των προβλέψεων του Κανονισμού, η πρακτική προσαρμογή τους σε όλες τις εκφάνσεις της επιχειρηματικής λειτουργίας, καθώς και η εμπέδωση της νέας φιλοσοφίας σεβασμού και προστασίας των προσωπικών δεδομένων που αυτός εισάγει, πάντοτε με τρόπο που να μην επιβαρύνει αλλά να ωφελεί τις επιχειρήσεις.

Παρότι η «συμμόρφωση» φαίνεται να συνεπάγεται υψηλά κόστη και βαριές διαδικασίες, οι ειδικοί του χώρου επιμένουν: Εκείνος που θα μετατρέψει την κουλτούρα σεβασμού και προστασίας των προσωπικών δεδομένων σε πυρήνα της καθημερινής του λειτουργίας, θα αποκτήσει αυτόματα ένα «ανταγωνιστικό πλεονέκτημα». Γιατί θα είναι εκείνος που θα είναι διαρκώς σε θέση να αποδείξει στον καταναλωτή, τον πελάτη, τον εργαζόμενο, όχι μόνο ότι έχει λάβει τα απαραίτητα μέτρα προστασίας των προσωπικών δεδομένων τους, αλλά και ότι είναι διαρκώς σε θέση να τα διατηρεί προστατευμένα.

Εισαγωγή

Για περισσότερο από τον τελευταίο και πλέον χρόνο, η αγορά κινείται σε πυρετώδεις ρυθμούς GDPR (General Data Protection Regulation), προσπαθώντας να ισορροπήσει ανάμεσα σε εκπαιδευτικά σεμινάρια και ενημερωτικές εκδηλώσεις, να εξοικειωθεί με περίπλοκους τεχνικούς και νομικούς όρους, να εκτιμήσει ορθολογικά το κόστος συμμόρφωσης και να εντοπίσει τους κατάλληλους, βάσει αναγκών και βαλαντίου, συνεργάτες για τη συμμόρφωση αυτή. Ταυτόχρονα, ακόμα αναμένεται η ψήφιση του νόμου που θα ρύθμιζε τις όποιες εκκρεμότητες για την μεταφορά του Κανονισμού (ΕΕ) 2016/679 στην εθνική έννομη τάξη και θα διευκόλυνε την αγορά να συμμορφωθεί στο ομολογουμένως περίπλοκο πλαίσιο υποχρεώσεων.

Παράλληλα, η οικονομία αναζητά να βρει το βηματισμό της και οι επιχειρήσεις να αποκαταστήσουν τις πληγές της βαθιάς οικονομικής ύφεσης που έπληξε τη χώρα τα προηγούμενα χρόνια.

Με την ελληνική οικονομία σε φάση ανάκαμψης, οι επιχειρήσεις καλούνται να εκσυγχρονίσουν τις δομές τους, να επανεξετάσουν ή/και να αναθεωρήσουν το επιχειρηματικό μοντέλο τους, να προσανατολίσουν τη στρατηγική τους προς νέες αγορές του εξωτερικού, αλλά και να αποκτήσουν, ή να αναθεωρήσουν, όλες τις διαδικασίες διαχείρισης των προσωπικών δεδομένων που κατέχουν (π.χ. στοιχεία πελατών, προμηθευτών, εργαζομένων, συμβάσεις κ.λπ.). Παρότι η «συμμόρφωση» φαίνεται να συνεπάγεται υψηλά κόστη και βαριές διαδικασίες, οι ειδικοί του χώρου επιμένουν: **εκείνος που θα μετατρέψει την κουλτούρα σεβασμού και προστασίας των προσωπικών δεδομένων σε πυρήνα της καθημερινής του λειτουργίας, θα αποκτήσει αυτόματα ένα «ανταγωνιστικό πλεονέκτημα»**. Γιατί θα είναι εκείνος που θα είναι διαρκώς σε θέση να αποδείξει στον καταναλωτή, τον πελάτη, τον εργαζόμενο, όχι μόνο ότι έχει λάβει τα απαραίτητα μέτρα προστασίας των προσωπικών δεδομένων τους, αλλά και ότι είναι διαρκώς σε θέση να τα διατηρεί προστατευμένα.

Πρόκειται συνεπώς για μια συνεχή και δυναμική διαδικασία συμμόρφωσης, κατά την οποία οι επιχειρήσεις θα εξασφαλίσουν την ικανοποίηση των απαιτήσεων του Κανονισμού και θα προστατεύσουν τη φήμη τους από πιθανά περιστατικά παραβίασης της ασφάλειας δεδομένων προσωπικού χαρακτήρα.

Προς αυτό το σκοπό φιλοδοξούμε να συμβάλει και η παρούσα Μελέτη που εκτείνεται στις σελίδες που ακολουθούν. Αφενός να παρουσιάσει τα βασικά σημεία του Κανονισμού και αφετέρου να υποστηρίξει τον τρόπο επίτευξης της «έξυπνης» συμμόρφωσης, δηλαδή της αξιοποίησης των ευκαιριών που παρουσιάζονται από τον Κανονισμό. Ειδικότερα στις σελίδες που ακολουθούν παρουσιάζονται τα κάτωθι:

Στο **Κεφάλαιο 1** αναλύονται τα **βασικά χαρακτηριστικά** του Κανονισμού, οι **κύριες αλλαγές** σε σχέση με το προηγούμενο καθεστώς της Οδηγίας 95/46/ΕΚ, αλλά και τα **κοινά** τους **σημεία**. Ιδιαίτερη αναφορά γίνεται στις **αυξημένες** πλέον **υποχρεώσεις και απαιτήσεις** για τους Υπευθύνους Επεξεργασίας (βάρος απόδειξης, οργανωτικά και τεχνικά μέτρα προστασίας, γνωστοποίηση παραβίασης κ.ά.) και την **ενίσχυση των δικαιωμάτων** των υποκειμένων (φορητότητα, λήθη κ.ά.). Για να γίνει κατανοητή όμως η φιλοσοφία του Κανονισμού και οι προβλέψεις του, πρέπει αρχικά να παρουσιαστεί το πλαίσιο το οποίο οδήγησε στην έκδοσή του. Έτσι, αναλύεται αρχικά η **παράμετρος** των **ραγδαίων τεχνολογικών εξελίξεων** (διαδίκτυο, κινητή τηλεφωνία, big data κ.ά.) που οδήγησε στην αύξηση της έκτασης και έντασης της συλλογής, ανταλλαγής και επεξεργασίας δεδομένων προσωπικού χαρακτήρα από ιδιωτικές επιχειρήσεις και δημόσιες αρχές με γεωμετρική πρόοδο, δημιουργώντας επί της ουσίας μια νέα αγορά. Επίσης, αναλύεται ο τρόπος που η τεχνολογική εξέλιξη διευκόλυνε την παραβίαση των δεδομένων, καθιστώντας αναγκαία τη λήψη «θεραπευτικών» μέτρων. Στη συνέχεια, αναλύεται η **παράμετρος** της αναγκαιότητας **ενός συνεκτικού πλαισίου** ώστε αφενός να διασφαλιστεί η ενιαία προστασία της ιδιωτικότητας των Ευρωπαίων πολιτών (οριζόντια προσέγγιση) και αφετέρου να αντιμετωπιστούν τα προβλήματα που προκάλεσαν οι διάσπαρτες και διαφορετικές διατάξεις σε επίπεδο ασφάλειας δικαίου και στρέβλωσης του ανταγωνισμού. Τέλος, γίνεται μια σύντομη **ιστορική αναδρομή** και παρουσιάζονται οι **βασικές έννοιες του Κανονισμού**, προκειμένου να διευκολυνθεί ο αναγνώστης.

Στο **Κεφάλαιο 2** αναλύονται οι **κυριότερες έννοιες** και τα πιο **σημαντικά άρθρα** του Κανονισμού, με τρόπο που διευκολύνει την κατανόησή τους. Τα ζητήματα που χρήζουν μεγαλύτερης προσοχής αφορούν στις προβλέψεις για τις **κυρώσεις** (οι οποίες λόγω υψηλού ύψους έχουν προκαλέσει τη μεγαλύτερη ανησυχία στην επιχειρηματικότητα), για την **ευθύνη** που έχουν τόσο οι Υπεύθυνοι Επεξεργασίας όσο και οι Εκτελούντες την Επεξεργασία, για την εκπόνηση της **Εκτίμησης Αντικτύπου** σχετικά με την προστασία δεδομένων (πότε, ποιοι, γιατί, πώς κ.λπ.), για τον ορισμό του **Υπεύθυνου Προστασίας Δεδομένων** (προϋποθέσεις, ρόλος, χαρακτηριστικά)

και το **δικαίωμα** των υποκειμένων στη **λήθη** (προβλέψεις και προϋποθέσεις). Ακόμα, αναπτύσσεται ολόκληρη ενότητα σχετικά με τη μεταφορά του Κανονισμού στην εθνική νομοθεσία, διότι, καθώς ο Ευρωπαίος νομοθέτης αφήνει στη διακριτική ευχέρεια των κρατών-μελών ορισμένα σημεία για περαιτέρω εξειδίκευση, η ψήφιση εθνικού Νόμου είναι αναγκαία. Η Μελέτη αναλύει το **Σχέδιο Νόμου που τέθηκε σε διαβούλευση** το Φεβρουάριο του 2018, με το τελικό κείμενο ωστόσο να εκκρεμεί ακόμα. Η κατάσταση βέβαια και στα υπόλοιπα κράτη-μέλη δεν είναι ιδιαίτερα διαφορετική, καθώς η πλειοψηφία δεν έχει ακόμα προβεί στις απαιτούμενης ενέργειες μεταφοράς στο εθνικό δίκαιο. Τέλος, αναλύεται η σχετική **νομολογία** που έχει αναπτυχθεί μέχρι σήμερα, με ιδιαίτερη έμφαση στην πολύκροτη υπόθεση **Facebook,** της διαρροής προσωπικών δεδομένων από την **Cambridge Analytica** (η οποία εύληπτα ανέδειξε την αναγκαιότητα ενός συνεκτικού και σύγχρονου πλαισίου προστασίας) και της διαρροής προσωπικών δεδομένων από την British Airways, αλλά και σε πρόσφατες αποφάσεις της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (συστήματα βιντεοεπιτήρησης, υπόθεση εισιτηρίων ΟΑΣΑ, παρακολούθηση Η/Υ εργαζομένου κ.ά.).

Το **Κεφάλαιο 3** είναι αφιερωμένο στις **εποπτικές Αρχές** (τόσο στην εθνική, δηλαδή την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα-ΑΠΔΠΧ, όσο και στην ευρωπαϊκή, δηλαδή το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων) και τον τριπλό ρόλο που κατέχουν (ενημερωτικό, ρυθμιστικό και ελεγκτικό / κυρωτικό). Αρχικά, παρουσιάζονται οι σχετικές **προβλέψεις του Κανονισμού**, ώστε να γίνει κατανοητό το πλαίσιο λειτουργίας των Αρχών (αδειοδοτικές, συμβουλευτικές και διορθωτικές εξουσίες, σχέσεις με τα υποκείμενα αλλά και τον Υπεύθυνο Προστασίας Δεδομένων (ΥΠΔ), ρόλος τους σχετικά με την Εκτίμηση Αντικτύπου, αρμοδιότητες για την πιστοποίηση κ.ά.). Επίσης, παρουσιάζεται το μέχρι σήμερα έργο της ΑΠΔΠΧ (η οποία αποτελεί πλέον την εθνική Αρχή) και στη συνέχεια το κεφάλαιο επικεντρώνεται στο Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων, με έμφαση στο καθήκον του ως προς τη **διασφάλιση της συνεκτικής εφαρμογής** του Κανονισμού.

Στο **Κεφάλαιο 4** παρουσιάζεται ο **βαθμός ετοιμότητας των επιχειρήσεων** σχετικά με τη συμμόρφωσή τους στις διατάξεις του Κανονισμού, **βάσει ερευνών** που έχουν πραγματοποιηθεί τόσο στο εξωτερικό όσο και στην Ελλάδα. Τα ευρήματα δεικνύουν ότι για τις περισσότερες επιχειρήσεις η συμμόρφωση με τον Κανονισμό, έγκαιρα και πλήρως, δεν ήταν εφικτή έως την 25η Μαΐου 2018 και επομένως οι προσπάθειες πρέπει να συνεχιστούν, αλλά και να ενταθούν. Ακόμα, οι έρευνες αναδεικνύουν και άλλα χρήσιμα στοιχεία, όπως **ποιες δράσεις έχουν υλοποιήσει**

οι επιχειρήσεις για την επίτευξη της συμμόρφωσης (π.χ. επένδυση σε προσωπικό και σε τεχνολογία), **ποια οφέλη αναμένουν να καρπωθούν** (π.χ. καλύτερη διαχείριση κινδύνου) και **ποιες διατάξεις παρουσιάζουν τις μεγαλύτερες δυσκολίες** (π.χ. φορητότητα δεδομένων και το δικαίωμα στη λήθη).

Το **Κεφάλαιο 5** αποτελεί έναν **εύχρηστο και πλήρη οδηγό συμμόρφωσης** με τον Κανονισμό για τις επιχειρήσεις. Αρχικά, γίνεται αναφορά στις **τρεις βασικές προϋποθέσεις** με οριζόντια ισχύ, οι οποίες πρέπει να πληρούνται: δέσμευση της ανώτατης διοίκησης, εξασφάλιση του σχετικού προϋπολογισμού και ενημέρωση του συνόλου του προσωπικού για το νέο νομικό πλαίσιο και τις επερχόμενες αλλαγές. Έπειτα, παρουσιάζονται τα **10 βήματα για την επίτευξη της συμμόρφωσης** (σύσταση Ομάδα Εργασίας, ορισμό ΥΠΔ, χαρτογράφηση δεδομένων, "gap analysis", εκπόνηση της ΕΑ, αναθεώρηση των πολιτικών και των διαδικασιών, αξιοποίηση των εργαλείων πληροφορικής, διαδικασίες γνωστοποίησης Αρχής και ανακοίνωσης υποκειμένου, δοκιμαστικοί έλεγχοι, επικαιροποίηση των διαδικασιών και των συστημάτων), τα οποία συνεπικουρούνται από συνεχείς εκπαιδευτικές δράσεις. Συμπληρωματικά παρουσιάζονται **δύο πρακτικά παραδείγματα** (μια επιχείρηση από τον ασφαλιστικό κλάδο και μία από τον κλάδο του λιανεμπορίου και μέλος πολυεθνικού ομίλου), προκειμένου να βοηθηθούν οι υπόλοιπες επιχειρήσεις. Στη συνέχεια, η Μελέτη παρουσιάζει τον τρόπο με τον οποίο η διαδικασία συμμόρφωσης με τον Κανονισμό μπορεί να προσφέρει **σημαντικά οφέλη στις επιχειρήσεις («έξυπνη συμμόρφωση»)**. Ακόμα, δίνεται **έμφαση** σε εκείνα τα **σημεία που πρέπει να προσέξουν οι επιχειρήσεις** κατά την εφαρμογή του Κανονισμού (φορητότητα δεδομένων, δικαίωμα στη λήθη, εξασφάλιση συγκατάθεσης και συμβάσεις με τρίτα μέρη). Στο τέλος, δίνονται αναλυτικές **απαντήσεις σε συχνές ερωτήσεις** που προβληματίζουν τις επιχειρήσεις στην προσπάθεια συμμόρφωσής τους στον Κανονισμό, με τη φιλοδοξία να διευκολυνθούν ουσιαστικά.

Στο **Κεφάλαιο 6** τέλος, **πραγματεύονται** εκείνα **τα ζητήματα που αναμένεται να απασχολήσουν όλους τους εμπλεκομένους** (δημόσια διοίκηση, Αρχές, επιχειρήσεις, υποκείμενα) **κατά το προσεχές διάστημα**, καθώς η έναρξη εφαρμογής του Κανονισμού την 25η Μαΐου 2018 αποτέλεσε απλά το πρώτο ορόσημο. Τα επόμενα βήματα των επιχειρήσεων, ο τρόπος που θα εποπτεύσουν τη συμμόρφωση στην πράξη οι Αρχές, οι επιπρόσθετες διευκρινίσεις (κατευθυντήριες γραμμές) που θα προκύψουν, η εθνική νομοθεσία και άλλα ζητήματα είναι εκείνα που θα καθορίσουν το μέλλον του Κανονισμού και της εφαρμογής του και οι εξελίξεις αναμένεται να είναι συνεχείς.

1. Εισαγωγή στην Προστασία Προσωπικών Δεδομένων

1. Εισαγωγή στην Προστασία Προσωπικών Δεδομένων

Κάθε επιχείρηση που είναι εγκατεστημένη στην Ευρωπαϊκή Ένωση, ή που είναι εγκατεστημένη εκτός Ευρωπαϊκής Ένωσης και χειρίζεται προσωπικά δεδομένα τα οποία αφορούν σε άτομα που βρίσκονται εντός της Ευρωπαϊκής Ένωσης, είναι υποχρεωμένη να συμμορφωθεί πλήρως στις επιταγές του νέου Γενικού Κανονισμού για την Προστασία Δεδομένων (GDPR), ο οποίος τέθηκε σε εφαρμογή την 25η Μαΐου 2018. Ο Κανονισμός, καταργώντας την Οδηγία 95/46/ΕΚ η οποία ως σήμερα αποτελούσε το βασικό νομικό πλαίσιο για την προστασία - του θεμελιώδους δικαιώματος - των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα στην Ευρώπη, αποτελεί μια κανονιστική εξέλιξη στο ρυθμιστικό περιβάλλον, η οποία επήλθε από δυο κύριες παραμέτρους: πρώτον, την τεχνολογική ανάπτυξη (ψηφιακή επανάσταση, διαδίκτυο, κινητή τηλεφωνία, big data κ.ά.), που κατέστησε την Οδηγία παρωχημένη, και δεύτερον, την ασυμμετρία εφαρμογής της Οδηγίας από τα κράτη-μέλη, εξαιτίας της οποίας προέκυψε έλλειμμα προστασίας της ιδιωτικότητας όπως φάνηκε στην πράξη. Έτσι, ο Κανονισμός επιδιώκει να εξισορροπήσει μεταξύ του δικαιώματος της προστασίας των προσωπικών δεδομένων από τη μία πλευρά και του δικαιώματος στην πληροφόρηση, διαφάνεια και δημόσια ασφάλεια από την άλλη, με τρόπο που να προάγει την ελεύθερη και ανεμπόδιστη οικονομική ανάπτυξη και επιχειρηματική δραστηριότητα.

1.1 Τα βασικά χαρακτηριστικά και οι κύριες αλλαγές του Κανονισμού

Ο Γενικός Κανονισμός για την Προστασία Δεδομένων έχει πέντε **κύρια χαρακτηριστικά**:

α) Έχει γενική εφαρμογή, καθώς αφορά τόσο τις επιχειρήσεις του ιδιωτικού τομέα (ανεξαρτήτως μεγέθους και κλάδου δραστηριοποίησης), όσο και τους φορείς του δημοσίου.

β) Είναι άμεσα εφαρμοστέος, με αμετάκλητη ημερομηνία έναρξης εφαρμογής (25/05/2018).

γ) Παρουσιάζει κάποια χαρακτηριστικά Οδηγίας, καθώς αφήνει στη διακριτική ευχέρεια των κρατών-μελών ορισμένα σημεία για περαιτέρω εξειδίκευση[1].

δ) Προβλέπει υψηλά διοικητικά πρόστιμα (έως €20 εκ. ή έως το 4% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών, ανάλογα με το ποιο είναι υψηλότερο), ανάλογα με το είδος της παραβίασης των διατάξεων του Κανονισμού.

[1] Σε 28 άρθρα του Κανονισμού υπάρχει περιθώριο παρέκκλισης για τα κράτη-μέλη.

ε) Αποτέλεσε αντικείμενο έντονων και πολυετών διαπραγματεύσεων[2] μεταξύ των διαφορετικών ομάδων συμφερόντων και τελικά πρόκειται για ένα «προϊόν» συμβιβασμού, γεγονός που δεικνύει τη σπουδαιότητα και τις οικονομικές του επεκτάσεις.

Δ.1 Τα κύρια χαρακτηριστικά του Κανονισμού
✓ Γενική εφαρμογή σε όλες τις επιχειρήσεις, ανεξαρτήτως μεγέθους και κλάδου δραστηριοποίησης, αλλά και τους φορείς δημοσίου
✓ Αμετάκλητη ημερομηνία έναρξης εφαρμογής: 25/05/2018
✓ Αρκετές διατάξεις στη διακριτική ευχέρεια των κρατών-μελών για περαιτέρω εξειδίκευση
✓ Υψηλά διοικητικά πρόστιμα
✓ Έντονες και πολυετείς διαπραγματεύσεις για το τελικό κείμενο

Ο Κανονισμός επιφέρει **σημαντικές αλλαγές** στο ρυθμιστικό περιβάλλον για τους υπεύθυνους επεξεργασίας δεδομένων, δηλαδή για τις επιχειρήσεις και τους δημόσιους φορείς, κυρίως σε τρία επίπεδα:

α) έχει ως κεντρική λογική την ελαχιστοποίηση της συλλογής, διατήρησης και επεξεργασίας δεδομένων προσωπικού χαρακτήρα,
β) επιδιώκει την ενίσχυση της προστασίας των προσωπικών δεδομένων, αναθεωρώντας τις υποχρεώσεις όλων όσοι επεξεργάζονται δεδομένα, καθώς πλέον, οι επονομαζόμενοι «Υπεύθυνοι Επεξεργασίας» αλλά και οι «Εκτελούντες την Επεξεργασία» για λογαριασμό των «Υπευθύνων» φέρουν το βάρος της απόδειξης της συμμόρφωσης στις διατάξεις του Κανονισμού και
γ) ανανεώνει και ενισχύει τα δικαιώματα των υποκειμένων, των ιδιοκτητών δηλαδή προσωπικών δεδομένων, γεγονός στο οποίο οφείλουν να προσαρμοστούν οι υπεύθυνοι επεξεργασίας αλλά και οι «Εκτελούντες την Επεξεργασία» για λογαριασμό των «Υπευθύνων» και συνεπώς να μεταβάλλουν ανάλογα τη λειτουργία και τις αποφάσεις τους.

Εν συντομία, **ο Κανονισμός αποτελεί ένα κοινό πλαίσιο ρυθμίσεων για τον τρόπο με τον οποίο συλλέγονται, επεξεργάζονται, φυλάσσονται, διακινούνται, αξιοποιούνται, αλλά και καταστρέφονται, δεδομένα**

[2] Ενδεικτικό είναι το γεγονός ότι η Ευρωπαϊκή Επιτροπή επισήμανε την ανάγκη τροποποίησης της Οδηγίας από τον Ιανουάριο του 2012, το Ευρωπαϊκό Κοινοβούλιο υπερψήφισε το σχέδιο Κανονισμού το Μάρτιο του 2014 και η τελική συμφωνία μεταξύ του Κοινοβουλίου, της Επιτροπής και του Συμβουλίου επήλθε το Δεκέμβριο του 2015. Ο Κανονισμός ψηφίστηκε το Μάιο του 2016 και δόθηκε διετής περίοδος προσαρμογής στα κράτη-μέλη έως το Μάιο του 2018.

προσωπικού χαρακτήρα των πολιτών της ΕΕ, ανεξαρτήτως του τόπου διαμονής τους, τόσο σε ηλεκτρονική όσο και σε φυσική μορφή. Ταυτίζεται συνεπώς με πολιτικές και διαδικασίες της επιχείρησης (π.χ. για τις συμβάσεις, τη διεξαγωγή διαγωνισμών, την εξυπηρέτηση πελατών), με υποδομές και συστήματα που χρησιμοποιούνται (π.χ. servers, ηλεκτρονικό ταχυδρομείο, USB sticks, CRM, POS), με πράξεις αυτοδέσμευσης της διοίκησης (π.χ. Κώδικες Δεοντολογίας και συστήματα πιστοποίησης), με το ανθρώπινο δυναμικό (π.χ. διαδικασίες προσλήψεων, συμβάσεις προσωπικού, ομαδικά συμβόλαια ασφάλισης, βιογραφικά σημειώματα και συνεντεύξεις), αλλά κυρίως με την κουλτούρα της επιχείρησης. Δηλαδή αποτελεί έναν εναλλακτικό τρόπο οργάνωσης και λειτουργίας της επιχείρησης που θέτει στο επίκεντρο τη διαφύλαξη των προσωπικών δεδομένων. Ή για να ακριβολογούμε, που θέτει στο επίκεντρο την ικανότητα να αποδείξει η επιχείρηση με τεκμήρια ότι κατά τη λειτουργία της λαμβάνει όλα τα αναγκαία μέτρα για να διαφυλάξει τα προσωπικά δεδομένα. Τα υψηλά πρόστιμα που προβλέπονται σε περίπτωση μη συμμόρφωσης καθιστούν επιτακτική την ανάγκη κατανόησης των νέων απαιτήσεων και επομένως η εξασφάλιση της συμμόρφωσης αποτελεί κρίσιμη διαδικασία για κάθε επιχείρηση.

Δ.2 Οι «καινοτομίες» του Κανονισμού σε λέξεις-κλειδιά	
✓ Ενίσχυση δικαιωμάτων υποκειμένων	✓ Αυστηριοποίηση κυρώσεων
✓ Ενίσχυση δικαιώματος στη λήθη	✓ Σύσταση Ευρωπαϊκού Συμβούλιου Προστασίας Δεδομένων
✓ Θέσπιση δικαιώματος στη φορητότητα	✓ Θέσπιση μηχανισμού συνεκτικότητας
✓ Μεταφορά βάρους απόδειξης στους Υπευθύνους Επεξεργασίας (Λογοδοσία)	✓ Θεσμοθέτηση της Αρχής της Διαφάνειας
Σημ.: Παρουσιάζονται στην παρούσα Μελέτη αναλυτικά.	

Κάτι το οποίο δεν έχει ίσως γίνει απόλυτα αντιληπτό από το σύνολο των επιχειρήσεων και της αγοράς είναι ότι ο Κανονισμός δεν αποτελεί το πρώτο νομικό κείμενο που αυτοτελώς πραγματεύεται την προστασία των προσωπικών δεδομένων. Αντίθετα, σε Ευρωπαϊκό επίπεδο, **από το 1995 βρισκόταν σε ισχύ η Οδηγία 95/46/ΕΚ «για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα** και για την ελεύθερη κυκλοφορία των δεδομένων αυτών», η οποία ενσωματώθηκε στο εθνικό δίκαιο βάσει του Ν. 2472/1997 «για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα».

Παρότι λοιπόν τα τελευταία είκοσι χρόνια ισχύει και εφαρμόζεται πανευρωπαϊκά ένα συγκεκριμένο πλαίσιο για την προστασία των προσωπικών δεδομένων, η έλευση του

νέου Κανονισμού έλαβε κατά τον τελευταίο χρόνο τόσο μεγάλη δημοσιότητα που δείχνει σαν η αγορά να είχε ξεχάσει τις υποχρεώσεις που προέβλεπε το προηγούμενο καθεστώς. Το ίδιο ισχύει και για τα υποκείμενα των δεδομένων, τα οποία επίσης φαίνεται να «ξυπνούν» από ένα λήθαργο άγνοιας των δικαιωμάτων για προστασία των προσωπικών τους δεδομένων. Μάλιστα, αξίζει να σημειωθεί ότι στην πραγματικότητα, οι αρχές, οι έννοιες και οι υποχρεώσεις του Κανονισμού δεν είναι και τόσο διαφορετικές από εκείνες της Οδηγίας. Αντίθετα, κατά την πρόσφατη συνεδρίαση του Εθνικού Συμβουλίου Καταναλωτή και Αγοράς (ΕΣΚΑ)[3], εκπρόσωπος της ΑΠΔΧΠ επεσήμανε ότι το 80% των προβλέψεων του Κανονισμού προβλέπονταν ήδη υπό το καθεστώς της Οδηγίας. Η πιθανότερη λογική εξήγηση για τη δημοσιότητα που έχει λάβει η έλευση του Κανονισμού μπορεί να βρίσκεται στο γεγονός ότι πλέον προβλέπονται συγκεκριμένες κυρώσεις που περιλαμβάνουν εξαιρετικά υψηλά διοικητικά πρόστιμα για τους υπεύθυνους επεξεργασίας και ποινικές ευθύνες για τους υπεύθυνους προστασίας σε περιπτώσεις παραβίασης του καθήκοντος εχεμύθειας, κάτι που αφύπνισε την αγορά και την ανάγκασε να στρέψει το βλέμμα της συνολικά στα προσωπικά δεδομένα.

Σημειώνεται ότι η - κάθε - Οδηγία από τη φύση της έχει ένα χαρακτηριστικό το οποίο δε μοιράζεται με τον Κανονισμό. Ως νομοθετική πράξη, θέτει μεν ένα συγκεκριμένο στόχο τον οποίο οφείλουν να επιτύχουν όλα τα κράτη-μέλη, αφήνει ωστόσο αρκετά μεγάλη διακριτική ευχέρεια στην επιλογή των μέσων επίτευξης του στόχου αυτού στους εθνικούς νομοθέτες[4]. Έτσι, κάθε-κράτος μέλος εναρμόνισε την Οδηγία 95/46/ΕΚ με τον τρόπο που κρίθηκε κατά περίπτωση ορθότερος προκειμένου να επιτευχθεί ο κοινός στόχος.

Καθώς λοιπόν η Οδηγία προέβλεπε ένα (σίγουρα περιορισμένο) επίπεδο εναρμόνισης στην ερμηνεία και επιβολή, στην ΕΕ δημιουργήθηκαν 28 διαφορετικές εθνικές νομοθεσίες σχετικά με την προστασία των προσωπικών δεδομένων, με αποτέλεσμα πολλές επιχειρήσεις να αντιμετωπίζουν φραγμούς εισόδου σε νέες αγορές και να υφίστανται περιττά κόστη και διοικητικά βάρη συμμόρφωσης.

Ο Κανονισμός, παρότι διατηρεί το πνεύμα και, σε πολλές περιπτώσεις, το γράμμα της Οδηγίας, έχει στον πυρήνα του ως κεντρικό σκοπό την ελαχιστοποίηση των αποκλίσεων στη νομοθεσία των κρατών-μελών και την επίτευξη μιας όσο το δυνατόν

[3] Πραγματοποιήθηκε την Παρασκευή 23 Μαρτίου 2018.
[4] Από την επίσημη ιστοσελίδα της Επιτροπής https://europa.eu/european-union/eu-law/legal-acts_en

ενιαίας και εναρμονισμένης προστασίας των υποκειμένων στην ενιαία αγορά με κοινή νομική βάση και ίδιο επίπεδο κυρώσεων. Για το λόγο αυτό, παρότι ακόμα και με μια πρώτη ματιά εντοπίζει κανείς γρήγορα τις βασικές ομοιότητες ανάμεσα στα δύο κείμενα, διαβάζοντας πιο προσεκτικά τον Κανονισμό θα αντιληφθεί ότι στο πλαίσιο της ομοιόμορφης εφαρμογής των διατάξεών του και εναρμονισμού των πολιτικών προστασίας σε όλα τα κράτη-μέλη, πλέον υπάρχει εξειδίκευση και διεύρυνση εννοιών, επέκταση της προστασίας δικαιωμάτων, σαφέστερος προσδιορισμός των ουσιωδών αρχών και εκσυγχρονισμός του νομοθετικού πλαισίου με τις νέες τεχνολογικές εξελίξεις.

Επιγραμματικά ωστόσο, αξίζει να αναφερθούν **τα στοιχεία εκείνα που απαντώνται τόσο στην Οδηγία όσο και τον Κανονισμό**, καθώς το γεγονός ότι διατηρούνται υπό το νέο πλαίσιο επιβεβαιώνει την αυξημένη σημασία τους και μπορεί να αποτελέσει σημαντικό σημείο αναφοράς για την ορθή συμμόρφωση των υπεύθυνων επεξεργασίας και προστασίας.

1) Αναγνώριση της σημασίας τήρησης του διπλού σκοπού προστασίας των δεδομένων και επιδίωξης της ελεύθερης κυκλοφορίας τους. Τόσο η Οδηγία (σκέψεις 3, 8 και 10), όσο και ο Κανονισμός που ορίζει ότι «Η ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα εντός της Ένωσης δεν περιορίζεται ούτε απαγορεύεται για λόγους που σχετίζονται με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα», τονίζουν ως βασική αρχή, την ισορροπία ανάμεσα στην προστασία των προσωπικών δεδομένων και στη δυνατότητα ελεύθερης διακίνησής τους, αλλά και στη δυνατότητα διακίνησης της πληροφορίας.
2) Υποχρέωση εφαρμογής των διατάξεων από τον ιδιωτικό και το δημόσιο τομέα.
3) Υποχρέωση εφαρμογής των διατάξεων από υπεύθυνους επεξεργασίας οι οποίοι είναι εγκατεστημένοι στην Ένωση. Ο Κανονισμός βέβαια έρχεται να συμπληρώσει και να εξειδικεύσει το προηγούμενο καθεστώς θέτοντας την προϋπόθεση, η επεξεργασία να βρίσκεται μέσα στο πλαίσιο των δραστηριοτήτων του υπεύθυνου ή του εκτελούντος την επεξεργασία[5].
4) Εξαίρεση από το πεδίο εφαρμογής των δραστηριοτήτων εκείνων με αυστηρά προσωπικό χαρακτήρα.

[5] Ωστόσο πρέπει να σημειωθεί ότι ο Κανονισμός καταλαμβάνει και υπεύθυνους επεξεργασίας/ εκτελούντες την επεξεργασία, μη εγκατεστημένους στην ΕΕ εφόσον η επεξεργασία εκτελείται στην Ένωση. Επίσης, η Οδηγία δεν κάνει αναφορά στους εκτελούντες την επεξεργασία, σε αντίθεση με τον Κανονισμό που τους συμπεριλαμβάνει με ρητή αναφορά.

5) Εφαρμογή των υποχρεώσεων σε αυτοματοποιημένη, μερικώς αυτοματοποιημένη ή μη αυτοματοποιημένη επεξεργασία.
6) Συγκεκριμένος ορισμός της έννοιας των προσωπικών δεδομένων[6].
7) Πλαίσιο προστασίας των ευαίσθητων δεδομένων[7].
8) Προϋπόθεση για ύπαρξη νομικής βάσης για την επεξεργασία δεδομένων, η οποία τις περισσότερες φορές καλύπτεται από τη συγκατάθεση του υποκειμένου των δεδομένων.
9) Τήρηση της αρχής της αναλογικότητας.
10) Αναφορά στον κίνδυνο από την επεξεργασία και τη φύση των δεδομένων που απολαύουν προστασίας[8].
11) Ομάδα προστασίας των προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα (γνωστή και ως «Ομάδα του άρθρου 29» ή «η Ομάδα»)[9].
12) Δικαίωμα πρόσβασης του Υποκειμένου στα δεδομένα του που τηρούνται.
13) Δικαίωμα των υποκειμένων στη λήθη[10].
14) Υποχρεώσεις τήρησης διαδικασιών διαφάνειας και λογοδοσίας καθώς και υποχρεώσεις ενημέρωσης των υποκειμένων και λήψης μέτρων ασφαλείας.
15) Παροχή διακριτικής ευχέρειας των κρατών μελών να υιοθετήσουν συγκεκριμένα μέτρα για τη ρύθμιση ορισμένων ζητημάτων[11].
16) Πρόβλεψη προστασίας δικαιωμάτων έναντι κατάρτισης προφίλ τους από τους υπεύθυνους επεξεργασίας.

1.2 Οι συνθήκες που οδήγησαν στην ανάγκη για τον νέο Κανονισμό

Όπως ήδη αναφέρθηκε, η ανάγκη προστασίας των προσωπικών δεδομένων και το κανονιστικό πλαίσιο που τη διασφαλίζει, δεν είναι κάτι νέο ούτε στην ΕΕ αλλά ούτε και στη χώρα μας. Ήδη από το 1995 ο Ευρωπαίος νομοθέτης εισήγαγε σημαντικές υποχρεώσεις στα κράτη-μέλη (βλ. Οδηγία 95/46/ΕΚ), διασφαλίζοντας αφενός την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα (δηλαδή το σεβασμό στην ιδιωτικότητα) και αφετέρου την εξασφάλιση της

6 Ο Κανονισμός διευρύνει τον ορισμό, προσθέτοντας τα δεδομένα θέσης.
7 Στην περίπτωση του Κανονισμού η έννοια διευρύνεται με την προσθήκη των γενετικών και βιομετρικών δεδομένων.
8 Παρότι η έννοια του κινδύνου αναφέρεται και στην Οδηγία, στον Κανονισμό μεταβάλλεται σε καθοριστικό παράγοντα αντιμετώπισης των ακολουθούμενων πρακτικών και μέτρων ασφαλείας
9 Προβλέπεται στο άρθρο 29 της Οδηγίας και επαναλαμβάνεται στον Κανονισμό.
10 Πρέπει να σημειωθεί ότι το δικαίωμα αυτό ενισχύεται και εξειδικεύεται με τον Κανονισμό καθώς η Οδηγία δεν περιλάμβανε σαφή προσδιορισμό του τρόπου άσκησης του δικαιώματος στη λήθη σε σχέση με τα φυσικά αρχεία.
11 Ο βαθμός της προβλεπόμενης διακριτικής ευχέρειας διατηρείται και στον Κανονισμό, φυσικά σε μικρότερο βαθμό από ό,τι συμβαίνει στην περίπτωση της Οδηγίας.

ελεύθερης κυκλοφορίας των δεδομένων αυτών, ως μέσο επίτευξης οικονομικής και κοινωνικής προόδου.

Ωστόσο, **δύο καθοριστικές παράμετροι κατέστησαν αναγκαία τη μεταρρύθμιση του κανονιστικού πλαισίου**, όπως αυτή εκφράστηκε με τον νέο Κανονισμό, καθώς τα μέτρα πολιτικής που ίσχυσαν μέχρι σήμερα εξάντλησαν την όποια αποτελεσματικότητά τους.

Η πρώτη, αναμενόμενα, αφορά στις **ραγδαίες τεχνολογικές εξελίξεις** που έλαβαν χώρα, αλλάζοντας τον κόσμο όπως τον ξέραμε και καθιστώντας την Οδηγία παρωχημένη.

Η δεύτερη αφορά στην **ασυμμετρία εφαρμογής της Οδηγίας από τα κράτη-μέλη**, αλλά και τελικά στο έλλειμμα προστασίας της ιδιωτικότητας που φάνηκε στην πράξη.

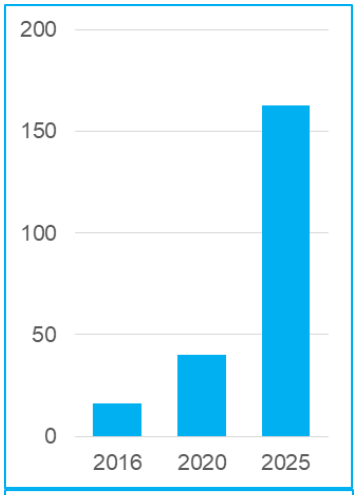
Δ.3 Παράμετροι που οδήγησαν στην ανάγκη για τον νέο Κανονισμό	
Ραγδαίες τεχνολογικές εξελίξεις	– Αύξηση της έκτασης και έντασης της συλλογής, ανταλλαγής και επεξεργασίας δεδομένων προσωπικού χαρακτήρα – Αύξηση περιπτώσεων παραβίασης της ασφάλειας δεδομένων προσωπικού χαρακτήρα
Ασυμμετρία εφαρμογής της Οδηγίας 95/46/ΕΚ από τα κράτη-μέλη	– Ανασφάλεια δικαίου - Αποκλίσεις κατά την εκτέλεση και εφαρμογή – Στρέβλωση του ανταγωνισμού μεταξύ κρατών-μελών

1.2.1 Οι ραγδαίες τεχνολογικές εξελίξεις

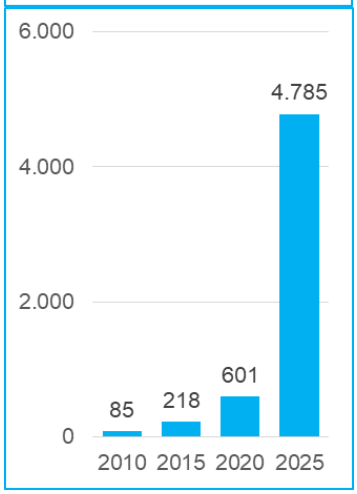
Όταν το 1995 θεσπίστηκε η Οδηγία 95/46/ΕΚ, το διαδίκτυο όχι μόνο δεν ήταν διόλου διαδεδομένο, αλλά πολύ λίγοι ήταν εκείνοι που θα μπορούσαν να προβλέψουν την εξέλιξή του. Μέσα σε λίγα μόλις χρόνια, οι ραγδαίες τεχνολογικές εξελίξεις (διαδίκτυο, κινητή τηλεφωνία, big data κ.ά.) οδήγησαν στην αύξηση της έκτασης και έντασης της συλλογής, ανταλλαγής και επεξεργασίας δεδομένων προσωπικού χαρακτήρα από ιδιωτικές επιχειρήσεις και δημόσιες αρχές με γεωμετρική πρόοδο. Είναι χαρακτηριστικό ότι έως το 2025 εκτιμάται ότι ο όγκος των δεδομένων θα αυξηθεί από

16,1 ZB σε 163 ZB[12], σύμφωνα με μελέτη της εταιρείας επιχειρηματικής πληροφόρησης International Data Corporation (IDC) **(Δ4)**. Τόσο τα προσωπικά, όσο και αλλά πάσης φύσεως δεδομένα, απέκτησαν μια έντονα εμπορική διάσταση, δημιουργώντας μια νέα παγκόσμια αγορά για την εύρυθμη λειτουργία της οποίας απαιτούνταν η ελεύθερη κυκλοφορία τους. Τέλος, μεταβλήθηκε ο τρόπος που τα ίδια τα φυσικά πρόσωπα χειρίζονται τα δεδομένα τους, δημοσιοποιώντας πλέον ολοένα και περισσότερο, αλλά και ευκολότερα, προσωπικές πληροφορίες και κατ' επέκταση καθιστώντας τες διαθέσιμες προς εκμετάλλευση (π.χ. μέσα κοινωνικής δικτύωσης). Στην προαναφερθείσα μελέτη εκτιμάται ότι έως το 2025 ο μέσος άνθρωπος θα έχει αλληλεπίδραση με μία συνδεδεμένη συσκευή σχεδόν 4.800 φορές την ημέρα **(Δ5)**.

Δ.5 Όγκος δεδομένων που δημιουργούνται ανά έτος, σε zettabytes
Πηγή: IDC, "Data Age 2025: The Evolution of Data to Life-Critical", Απρίλιος 2017



Δ.5 Αλληλεπίδραση με μία συνδεδεμένη συσκευή, σε φορές ανά ημέρα
Πηγή: IDC, "Data Age 2025: The Evolution of Data to Life-Critical", Απρίλιος 2017



Οι οικονομικές συνέπειες της ψηφιακής επανάστασης είναι σίγουρα εντυπωσιακές. Σύμφωνα με εκτιμήσεις, **η αξία της αγοράς των προσωπικών δεδομένων υπολογίζεται ότι θα ανέλθει σε σχεδόν €1 τρισ. το 2020[13].**

[12] 1 ZB = 10^{21} bytes
[13] European Commission, "Fact Sheet - Questions and Answers-General Data Protection Regulation", January 2018.

Όμως, η εξέλιξη της τεχνολογίας δεν δημιούργησε απλά μια νέα εκθετικά αναπτυσσόμενη αγορά προσωπικών δεδομένων, διευκολύνοντας τη συγκέντρωση και την επεξεργασία τους, αλλά ταυτόχρονα διευκόλυνε και την παραβίασή τους. Στον πίνακα **(Δ6)** παρουσιάζονται ενδεικτικά ορισμένα πρόσφατα παραδείγματα περιπτώσεων παραβίασης της ασφάλειας δεδομένων προσωπικού χαρακτήρα, τα οποία αιτιολογούν την αναγκαιότητα ενός νέου πλαισίου προστασίας των προσωπικών δεδομένων, αλλά και του κυβερνοχώρου, που να ανταποκρίνεται στη σύγχρονη πραγματικότητα. Για το λόγο αυτό άλλωστε, παράλληλα με τον Κανονισμό, το Μάιο του 2018 ξεκίνησε και η υποχρέωση συμμόρφωσης των κρατών-μελών στην **Οδηγία 1148/2016** σχετικά με τα μέτρα ασφαλείας συστημάτων δικτύου και πληροφοριών (Network and Information Systems - NIS), στο πλαίσιο μιας ολοκληρωμένης ευρωπαϊκής πολιτικής για την κυβερνοασφάλεια.

Η συζήτηση για τον κίνδυνο ανάδυσης μια «ψηφιακής δικτατορίας» μόλις σε μερικές δεκαετίες από σήμερα, η οποία θα αντλεί τη δύναμή της από τον τεράστιο όγκο προσωπικών δεδομένων που θα έχουν κάποιοι λίγοι στα χέρια τους (δείτε **εδώ** την πρόσφατη ομιλία του ιστορικού Yuval Harari), εξηγεί εξίσου την αναγκαιότητα που γέννησε, για κάποιους μάλλον καθυστερημένα[14], το νέο Γενικό Κανονισμό για την Προστασία Δεδομένων. Με άλλα λόγια:

Ο Κανονισμός αποτελεί μια χαρακτηριστική περίπτωση εκ των υστέρων ρύθμισης, όπου ο νομοθέτης έρχεται να θεραπεύσει και όχι να προλάβει, *καθώς η τεχνολογία προπορεύεται κατά πολύ του δικαίου, αλλά και ίσως της ηθικής.*

[14] Ενδεικτικό είναι το γεγονός ότι η Ευρωπαϊκή Επιτροπή επισήμανε την ανάγκη τροποποίησης της Οδηγίας από τον Ιανουάριο του 2012, το Ευρωπαϊκό Κοινοβούλιο υπερψήφισε το σχέδιο Κανονισμού το Μάρτιο του 2014 και η τελική συμφωνία μεταξύ του Κοινοβουλίου, της Επιτροπής και του Συμβουλίου επήλθε το Δεκέμβριο του 2015. Ο Κανονισμός ψηφίστηκε το Μάιο του 2016 και δόθηκε διετής περίοδος προσαρμογής στα κράτη-μέλη έως το Μάιο του 2018.

Δ.6 Παραδείγματα περιπτώσεων παραβίασης της ασφάλειας δεδομένων προσωπικού χαρακτήρα

Περίπτωση Yahoo! Inc.

Προφίλ: Εταιρεία διαδικτυακών υπηρεσιών, με έδρα τις ΗΠΑ
Ημερομηνία συμβάντος: 2013-2014
Ημερομηνία ανακοίνωσης συμβάντος: Σεπτέμβριος 2016 (αρχική) - Οκτώβριος 2017
Περιγραφή συμβάντος: Απώλεια προσωπικών δεδομένων (ονομάτων, ημερομηνιών γέννησης, ηλεκτρονικών διευθύνσεων και κωδικών πρόσβασης) 3 δισ. πελατών.
Εκτίμηση κόστους: $350 εκ. (εκτίμηση για τις απώλειες της αξίας της τιμής της μετοχής της Yahoo! ενόψει της πώλησής της στην Verizon Communications, καθώς εκείνο το διάστημα εξελίσσονταν οι διαπραγματεύσεις)
Άλλα στοιχεία: Η εταιρεία προέβη σε διαδοχικές ανακοινώσεις, το διάστημα από Σεπτέμβριο του 2016 έως τον Οκτώβριο του 2017, σχετικά με τον αριθμό χρηστών των οποίων τα δεδομένα παραβιάστηκαν, αυξάνοντας τον αριθμό από 500 εκ., σε 1 δισ. και τελικά σε 3 δισ. χρήστες. Τα περιστατικά παραβίασης ήταν περισσότερα από ένα, την περίοδο 2013 και 2014.

Περίπτωση Uber Technologies Inc.

Προφίλ: Εταιρεία παροχής υπηρεσιών μετακίνησης, με έδρα τις ΗΠΑ
Ημερομηνία συμβάντος: Οκτώβριος 2016
Ημερομηνία ανακοίνωσης συμβάντος: 22 Νοεμβρίου 2017
Περιγραφή συμβάντος: Κλοπή προσωπικών δεδομένων (ονομάτων, ηλεκτρονικών διευθύνσεων και κινητών τηλεφώνων) 57 εκ. χρηστών και 600 χιλ. οδηγών, λόγω κυβερνοεπίθεσης.
Άλλα στοιχεία: Η εταιρεία, εκτός του ότι προέβη σε ανακοίνωση του συμβάντος με καθυστέρηση σχεδόν ενός έτους, παραδέχτηκε ότι κατέβαλε λύτρα αξίας $100 χιλ. στους χάκερς, προκειμένου να καταστρέψουν τα προσωπικά δεδομένα που απέκτησαν (δίχως βεβαίως να υπάρχει απόδειξη για τις ενέργειες καταστροφής). Το συμβάν προκάλεσε την απόλυση του Διευθυντή Ασφαλείας.

Περίπτωση Target Stores Inc.

Προφίλ: Εταιρεία λιανικού εμπορίου, με έδρα τις ΗΠΑ
Ημερομηνία συμβάντος: Δεκέμβριος 2013
Περιγραφή συμβάντος: Κλοπή προσωπικών δεδομένων (ονομάτων, ταχυδρομικών διευθύνσεων, ηλεκτρονικών διευθύνσεων και τηλεφώνων) 110 εκ. πελατών, λόγω κυβερνοεπίθεσης.
Εκτίμηση κόστους: $162 εκ.
Άλλα στοιχεία: Εκτιμάται ότι οι χάκερς απέκτησαν πρόσβαση στα μηχανήματα υποδοχής καρτών (POS) των πελατών, μέσω ενός τρίτου προμηθευτή της εταιρείας. Η παραβίαση των δεδομένων εκτιμάται ότι αποκαλύφθηκε με καθυστέρηση ορισμένων εβδομάδων. Προκάλεσε την παραίτηση του Διευθυντή Πληροφοριακών Συστημάτων το Μάρτιο του 2014 και του Διευθύνοντα Συμβούλου δύο μήνες μετά.

Περίπτωση Equifax Inc.

Προφίλ: Εταιρεία διαχείρισης πιστωτικών καρτών, με έδρα τις ΗΠΑ
Ημερομηνία συμβάντος: 29 Ιουλίου 2017
Ημερομηνία ανακοίνωσης συμβάντος: 7 Σεπτεμβρίου 2017
Περιγραφή συμβάντος: α) Απώλεια προσωπικών δεδομένων (αριθμών κοινωνικής ασφάλισης, ημερομηνιών γέννησης, ταχυδρομικών διευθύνσεων και διπλωμάτων οδήγησης)

143 εκ. πελατών και β) απώλεια στοιχείων των πιστωτικών καρτών 209 χιλ. πελατών, λόγω κυβερνοεπίθεσης. **Άλλα στοιχεία:** Η παραβίαση των δεδομένων εκτιμάται ότι είχε ξεκινήσει από τα μέσα Μαΐου 2017 και οφειλόταν σε μια ευπάθεια εφαρμογής στην ιστοσελίδα της επιχείρησης.
Περίπτωση Anthem Inc. **Προφίλ:** Ασφαλιστική εταιρεία, με έδρα τις ΗΠΑ **Ημερομηνία συμβάντος:** Ιανουάριος 2015 **Περιγραφή συμβάντος:** Κλοπή προσωπικών δεδομένων (ονομάτων, αριθμών κοινωνικής ασφάλισης, ημερομηνιών γέννησης, ταχυδρομικών διευθύνσεων και ιστορικού απασχόλησης) 78,8 εκ. νυν και πρώην πελατών, λόγω κυβερνοεπίθεσης. **Εκτίμηση κόστους:** $100 εκ. **Άλλα στοιχεία:** Η παραβίαση των δεδομένων εκτιμάται ότι είχε ξεκινήσει από το Φεβρουάριο του 2014, όταν ένας υπάλληλος μιας θυγατρικής εταιρείας του Ομίλου άνοιξε ένα “phishing email”.
Περίπτωση CeX Ltd. **Προφίλ:** Εταιρεία λιανικού εμπορίου (προϊόντων τεχνολογίας, *βιντεοπαιχνιδιών* κ.ά.), με έδρα το Ην. Βασίλειο **Ημερομηνία ανακοίνωσης:** Αύγουστος 2017 **Περιγραφή συμβάντος:** Κλοπή προσωπικών δεδομένων (ονομάτων, ταχυδρομικών διευθύνσεων, ηλεκτρονικών διευθύνσεων και τηλεφώνων, καθώς και μικρού αριθμού κρυπτογραφημένων στοιχείων πιστωτικών καρτών) 2 εκ. πελατών, λόγω κυβερνοεπίθεσης. **Άλλα στοιχεία:** Πρόκειται για επίθεση από χάκερς προς το ηλεκτρονικό κατάστημα του Ομίλου “WeBuy.com”
Πηγή: https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html και https://www.techworld.com/security/uks-most-infamous-data-breaches-3604586/

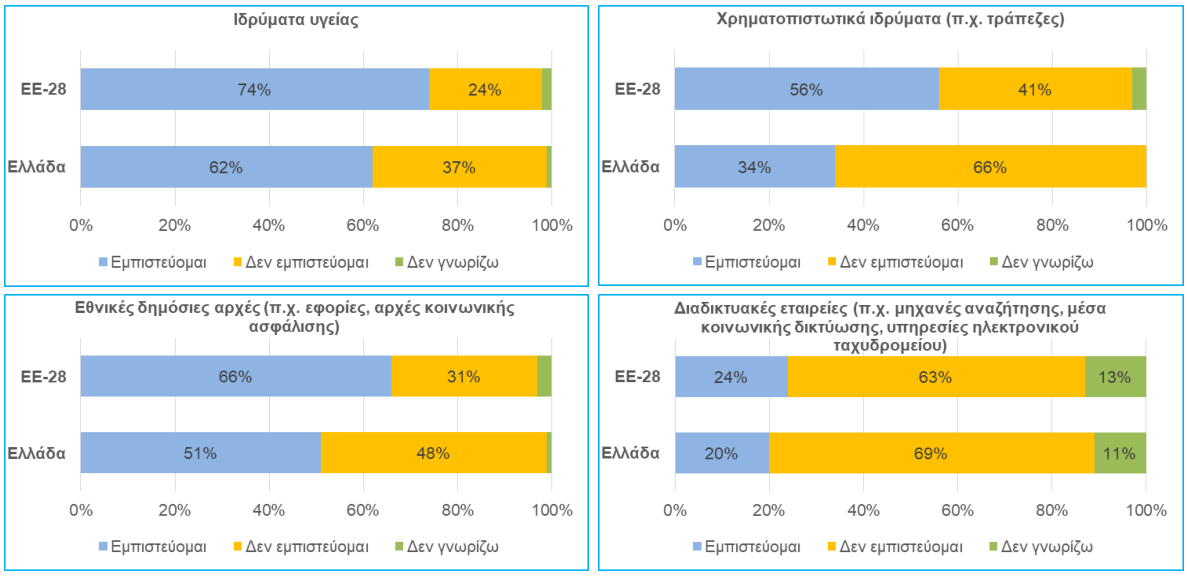
1.2.2 Η ασυμμετρία εφαρμογής της Οδηγίας από τα κράτη-μέλη

Στα παραπάνω έρχεται να προστεθεί και η αποτυχία της ευρωπαϊκής πολιτικής (μέσω της Οδηγίας) να αποτρέψει τον **κατακερματισμό του τρόπου εφαρμογής των διατάξεων για την προστασία των προσωπικών δεδομένων στην ΕΕ**, προκαλώντας ανασφάλεια δικαίου εξαιτίας της ύπαρξης αποκλίσεων, κατά την εκτέλεση και εφαρμογή της, μεταξύ των κρατών-μελών. Οι εν λόγω διαφορές στο επίπεδο προστασίας των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα, όχι μόνο δεν κατάφεραν να προστατεύσουν ενιαία την ιδιωτικότητα των Ευρωπαίων πολιτών, αλλά θεωρήθηκαν και ως εμπόδιο στην ψηφιακή επανάσταση και ως στρέβλωση του ανταγωνισμού. Περαιτέρω, οι διάσπαρτες διατάξεις και οι διαφορετικές ερμηνείες και πρακτικές καθιέρωσαν μια διαδεδομένη αντίληψη στους πολίτες ότι υπάρχουν σημαντικοί κίνδυνοι για την προστασία των προσωπικών τους δεδομένων. Για αυτό το λόγο άλλωστε στον

Κανονισμό έχει δοθεί ιδιαίτερη έμφαση στο ζήτημα της συνεκτικής εφαρμογής του σε ολόκληρη την ΕΕ.

Στα αποτελέσματα της έρευνας του Ευρωβαρόμετρου σχετικά με την προστασία των προσωπικών δεδομένων[15], αποτυπώνεται εύληπτα ότι υπάρχει ανάγκη οριζόντιας διαχείρισης του ζητήματος και μεγάλο περιθώριο βελτίωσης της εμπιστοσύνης μεταξύ των υποκειμένων και των επεξεργαστών δεδομένων. Ειδικότερα, σύμφωνα με την έρευνα, τόσο στην Ελλάδα όσο και στην ΕΕ-28 συνολικά, 9 στους 10 πολίτες δηλώνουν ότι είναι σημαντικό να έχουν τα ίδια δικαιώματα και την ίδια προστασία των προσωπικών τους στοιχείων ανεξάρτητα από τη χώρα στην οποία είναι εγκατεστημένος ο οργανισμός (επιχείρηση ή δημόσιος φορέας) που προβαίνει στην επεξεργασία τους. Ωστόσο, στην Ελλάδα είναι αισθητά χαμηλότερος ο βαθμός εμπιστοσύνης των πολιτών προς τους οργανισμούς που διαχειρίζονται προσωπικά τους δεδομένα από ότι στην ΕΕ **(Δ7)**.

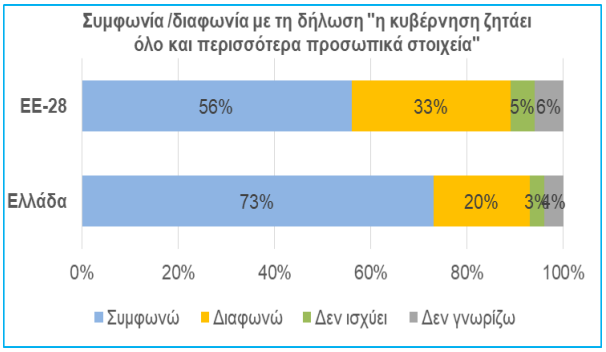
Δ.7 Βαθμός εμπιστοσύνης πολιτών προς επιλεγμένους δημόσιους φορείς και κλάδους επιχειρήσεων σχετικά με την προστασία προσωπικών στοιχείων στην ΕΕ-28
Πηγή: Ευρωβαρόμετρο, Προστασία προσωπικών δεδομένων, Έρευνα 431, Στοιχεία 2015



Τέλος, οι Έλληνες πολίτες παρουσιάζουν σημαντική διαφορά συγκριτικά με το μέσο όρο της ΕΕ ως προς τη στάση της κυβέρνησης σχετικά με τη συγκέντρωση προσωπικών δεδομένων, νιώθοντας ότι συνεχώς τους ζητείται να δώσουν όλο και περισσότερα προσωπικά στοιχεία **(Δ8)**.

[15] Η σχετική έκθεση είναι διαθέσιμη **εδώ**. Σημειώνεται ότι το χρονικό διάστημα διεξαγωγής των συνεντεύξεων ήταν από 28/02 έως 09/03/2015. Το δείγμα για την ΕΕ28 ανήλθε σε 27.980 άτομα και για την Ελλάδα σε 1.004 άτομα.

Δ.8 Αξιολόγηση βαθμού εμπλοκής κυβέρνησης στα προσωπικά στοιχεία
Πηγή: Ευρωβαρόμετρο, Προστασία προσωπικών δεδομένων, Έρευνα 431, Στοιχεία 2015



Το γεγονός αυτό αποτυπώνει, σε ένα βαθμό, το «σκεπτικισμό» και την επιφυλακτικότητα που επικρατεί στην Ελλάδα σχετικά με τα προσωπικά δεδομένα, καθώς συχνά η συγκέντρωση προσωπικών στοιχείων από τους φορείς ταυτίζεται με παραβίαση της ιδιωτικότητας (π.χ. τοποθέτηση καμερών ασφαλείας στους δρόμους, δήλωση ΑΜΚΑ για την αγορά εισιτηρίων αθλητικών γεγονότων κ.λπ.) και όχι με ενέργειες που είναι απαραίτητες για την ασφάλεια ή/και τη καθαυτή λειτουργία του εκάστοτε οργανισμού. Επίσης, αποτυπώνει το έλλειμμα εμπιστοσύνης ότι τα προσωπικά στοιχεία που θα συγκεντρωθούν θα αξιοποιηθούν με σεβασμό στο δικαίωμα προστασίας τους.

1.3 Ιστορική αναδρομή έως την έναρξη εφαρμογής του Κανονισμού

Η εφαρμογή του Γενικού Κανονισμού για την Προστασία Δεδομένων (GDPR) ξεκίνησε επίσημα την 25η Μαΐου 2018, οδηγώντας στην κατάργηση της Οδηγίας 95/46/ΕΚ η οποία ως την ημερομηνία εκείνη αποτελούσε το βασικό νομικό πλαίσιο για την προστασία των δεδομένων προσωπικού χαρακτήρα στην Ευρώπη.

Ο Κανονισμός αποτέλεσε αντικείμενο έντονων διαβουλεύσεων και ενδεικτικό είναι το γεγονός ότι η Ευρωπαϊκή Επιτροπή επισήμανε την ανάγκη τροποποίησης της Οδηγίας από τον Ιανουάριο του 2012, το Ευρωπαϊκό Κοινοβούλιο υπερψήφισε το σχέδιο Κανονισμού το Μάρτιο του 2014 και η τελική συμφωνία μεταξύ του Κοινοβουλίου, της Επιτροπής και του Συμβουλίου επήλθε το Δεκέμβριο του 2015. Ο Κανονισμός ψηφίστηκε το Μάιο του 2016 και δόθηκε διετής περίοδος προσαρμογής στα κράτη-μέλη έως το Μάιο του 2018.

Η πολυετής (6,5 έτη) και σχετικά συγκρουσιακή πορεία έως την κατάρτιση του τελικού κειμένου του Κανονισμού καταδεικνύει την πολυπλοκότητα του συγκεκριμένου πεδίου πολιτικής, την υψηλή τεχνικότητα που το διέπει και την ταχύτητας με την οποία μεταβάλλονται κυρίως οι τεχνολογικοί όροι που το επηρεάζουν (συχνά πριν προλάβει

να ρυθμιστεί το πεδίο η τεχνολογία το έχει ήδη ξεπεράσει). Το τελικό κείμενο αποτέλεσε αντικείμενο έντονων διαπραγματεύσεων μεταξύ των διαφορετικών ομάδων συμφερόντων και τελικά πρόκειται για ένα «προϊόν» συμβιβασμού, γεγονός που δεικνύει τη σπουδαιότητα και τις οικονομικές του επεκτάσεις. Στον παρακάτω πίνακα παρουσιάζονται οι βασικές ημερομηνίες σχετικά με τις ενέργειες που οδήγησαν στην έναρξη του Κανονισμού στις 25 Μαΐου 2018.

Δ.9 Βασικές ημερομηνίες έως την έναρξη εφαρμογής του Κανονισμού

24/10/1995	**Θεσπίζεται η Οδηγία 95/46/ΕΚ.**
25/01/2012	**Η Ευρωπαϊκή Επιτροπή επισημαίνει την ανάγκη τροποποίησης της Οδηγίας.**
07/03/2012	**Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων δημοσιεύει γνώμη επί της προτεινόμενης (από την Επιτροπή) τροποποίησης της Οδηγίας.**
23/03/2012	**Το "Article 29 Working Party" δημοσιεύει γνώμη επί της προτεινόμενης (από την Επιτροπή) τροποποίησης της Οδηγίας.**
05/10/2012	**Το "Article 29 Working Party" δημοσιεύει περαιτέρω σχόλια επί της προτεινόμενης (από την Επιτροπή) τροποποίησης της Οδηγίας.**
12/03/2014	**Το Ευρωπαϊκό Κοινοβούλιο υπερψηφίζει το σχέδιο Κανονισμού.**
15/06/2015	**Το Συμβούλιο καταλήγει σε μια γενική προσέγγιση επί του το σχεδίου Κανονισμού.**
27/07/2015	**Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων δημοσιεύει συστάσεις προς την Επιτροπή σύνταξης του τελικού κειμένου του Κανονισμού.**
15/12/2015	**Επέρχεται τελική συμφωνία μεταξύ του Κοινοβουλίου, της Επιτροπής και του Συμβουλίου.**

02/02/2016	**Το "Article 29 Working Party" δημοσιεύει το χρονοδιάγραμμα υλοποίησης του Κανονισμού.**
24/05/2016	**Δημοσιεύεται ο Κανονισμός.**
10/01/2017	**Η Ευρωπαϊκή Επιτροπή προτείνει δύο νέους Κανονισμούς σχετικά α) με την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες (ePrivacy) και β) τους κανόνες προστασίας δεδομένων που ισχύουν για τα θεσμικά όργανα της ΕΕ (επί του παρόντος Κανονισμός 45/2001) που ευθυγραμμίζουν τους ισχύοντες κανόνες με το Γενικό Κανονισμό.**
06/05/2018	**Έναρξη εφαρμογής της Οδηγίας ΕΕ/2016/680 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών.**
25/05/2018	**Έναρξη εφαρμογής του Κανονισμού 2016/679.**

Πηγή: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation

1.4 Οι βασικές έννοιες του Κανονισμού - Γλωσσάρι

Για την ευκολότερη κατανόηση του Κανονισμού και των διατάξεών του, στον παρακάτω πίνακα παρουσιάζονται οι ορισμοί των κυριότερων εννοιών.

Δ.10 Οι βασικότερες έννοιες του Κανονισμού (με βάση το άρθρο 4 του Κανονισμού)	
Προσωπικά Δεδομένα ή Δεδομένα Προσωπικού Χαρακτήρα	Κάθε πληροφορία που αφορά ταυτοποιημένο, ή ταυτοποιήσιμο, φυσικό πρόσωπο («υποκείμενο των δεδομένων»). Παραδείγματα αποτελούν: όνομα, επώνυμο, αριθμός ταυτότητας, ΑΜΚΑ, ΑΦΜ, τηλέφωνο, ταχυδρομική και ηλεκτρονική διεύθυνση, διεύθυνση πρωτοκόλλου διαδικτύου (IP address), γεωχωρικά δεδομένα (GPS), δηλαδή στοιχεία που μπορούν να ταυτοποιήσουν ένα φυσικό πρόσωπο.
Υποκείμενο των Δεδομένων	Πρόκειται για το φυσικό πρόσωπο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας.
Επεξεργασία δεδομένων	Κάθε πράξη που πραγματοποιείται επί των προσωπικών δεδομένων, όπως συλλογή, καταχώριση, οργάνωση, αποθήκευση, μεταβολή, ανάκτηση, αναζήτηση πληροφοριών, χρήση, διαγραφή, καταστροφή κ.λπ.
Διασυνοριακή επεξεργασία	Αφορά στην επεξεργασία δεδομένων προσωπικού χαρακτήρα η οποία γίνεται στο πλαίσιο των δραστηριοτήτων: α) διάφορων εγκαταστάσεων σε περισσότερα του ενός κράτη μέλη υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία στην ΕΕ, όπου ο υπεύθυνος επεξεργασίας ή ο εκτελών επεξεργασία είναι εγκατεστημένος σε περισσότερα του ενός κράτη μέλη και β) μίας μόνης εγκατάστασης υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία στην ΕΕ, αλλά που επηρεάζει ή ενδέχεται να επηρεάσει ουσιωδώς υποκείμενα των δεδομένων σε περισσότερα του ενός κράτη μέλη.
Υπεύθυνος Επεξεργασίας Δεδομένων	Το φυσικό, ή νομικό, πρόσωπο, ή δημόσια αρχή / υπηρεσία, που καθορίζει τους σκοπούς και τον τρόπο της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα.
Εκτελών την Επεξεργασία	Το φυσικό, ή νομικό, πρόσωπο, ή δημόσια αρχή / υπηρεσία, που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του Υπευθύνου Επεξεργασίας. Παραδείγματα Εκτελούντων την Επεξεργασία αποτελούν οι επιχειρήσεις ενημέρωσης οφειλετών και παροχής υπηρεσιών “cloud”.
Αποδέκτης δεδομένων	Το φυσικό, ή νομικό, πρόσωπο, ή δημόσια αρχή / υπηρεσία / άλλος φορέας, στον οποίο κοινολογούνται τα δεδομένα προσωπικού χαρακτήρα, είτε πρόκειται για τρίτον είτε όχι. Παραδείγματα αποδεικτών δεδομένων για την Τειρεσίας θεωρούνται οι τράπεζες, η Τράπεζα της Ελλάδος, οι φορείς του δημοσίου κ.λπ.

	Σημ.: Οι δημόσιες αρχές που ενδέχεται να λάβουν τέτοια δεδομένα στο πλαίσιο συγκεκριμένης έρευνας δεν θεωρούνται ως αποδέκτες. Η επεξεργασία των δεδομένων αυτών από τις εν λόγω δημόσιες αρχές πραγματοποιείται σύμφωνα με τους ισχύοντες κανόνες προστασίας των δεδομένων ανάλογα με τους σκοπούς της επεξεργασίας.
Υπεύθυνος Προστασίας Δεδομένων	Ορίζεται από τον Υπεύθυνο Επεξεργασίας και τον Εκτελούντα την Επεξεργασία και συμμετέχει, δεόντως και εγκαίρως, σε όλα τα ζητήματα τα οποία σχετίζονται με την προστασία δεδομένων προσωπικού χαρακτήρα. Αποτελεί το πρόσωπο επικοινωνίας τόσο με τα υποκείμενα των δεδομένων όσο και με την εποπτική Αρχή.
Εκτίμηση Αντικτύπου σχετικά με την προστασία δεδομένων	Όταν ένα είδος επεξεργασίας δεδομένων, ιδίως με χρήση νέων τεχνολογιών και συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο Υπεύθυνος Επεξεργασίας οφείλει να διενεργήσει, πριν από την επεξεργασία, εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία προσωπικών δεδομένων.
Συγκατάθεση Υποκειμένου	Κάθε ένδειξη βούλησης (ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει), με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν.
Παραβίαση Δεδομένων Προσωπικού Χαρακτήρα	Παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας αποκάλυψη ή πρόσβαση δεδομένων προσωπικού χαρακτήρα, τα οποία διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία.
Εποπτική Αρχή Προστασίας Δεδομένων	Πρόκειται για την ανεξάρτητη δημόσια Αρχή, καθ' ύλην αρμόδια για την εποπτεία εφαρμογής του Κανονισμού. Ο Κανονισμός ενθαρρύνει την επικοινωνία και συνεργασία μεταξύ των διάφορων Αρχών («μηχανισμός μιας στάσης»), ώστε να διασφαλίζεται ομοιογένεια στην αντιμετώπιση υποθέσεων διευρωπαϊκού ενδιαφέροντος και ασφάλεια δικαίου.
Επικεφαλής Εποπτική Αρχή	Ορίζεται η Αρχή του κράτους-μέλους όπου βρίσκεται η «κύρια εγκατάσταση» (βλ. παρακάτω) του Υπευθύνου Επεξεργασίας.
Ενδιαφερόμενη Εποπτική Αρχή	Ορίζεται η Αρχή, την οποία αφορά η επεξεργασία δεδομένων προσωπικού χαρακτήρα, όταν: α) ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία είναι εγκατεστημένος στο έδαφος του κράτους μέλους της εν λόγω εποπτικής αρχής, β) τα υποκείμενα των δεδομένων που διαμένουν στο κράτος μέλος της εν λόγω εποπτικής αρχής επηρεάζονται ή ενδέχεται να επηρεαστούν ουσιωδώς από την επεξεργασία, ή γ) έχει υποβληθεί καταγγελία στην εν λόγω εποπτική αρχή.
Κύρια Εγκατάσταση	**Για τον Υπεύθυνο Επεξεργασίας:** Σε περίπτωση που έχει εγκαταστάσεις σε περισσότερα του ενός κράτη μέλη,

	πρόκειται για τον τόπο της κεντρικής του διοίκησης στην ΕΕ. Ωστόσο, εάν οι αποφάσεις, όσον αφορά στους σκοπούς και τα μέσα της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, λαμβάνονται σε άλλη εγκατάστασή του στην ΕΕ, και η εγκατάσταση αυτή έχει την εξουσία εφαρμογής των αποφάσεων αυτών, τότε πρόκειται για την εγκατάσταση στην οποία έλαβε αυτές τις αποφάσεις. **Για τον Εκτελούντα την Επεξεργασία:** Σε περίπτωση που έχει εγκαταστάσεις σε περισσότερα του ενός κράτη μέλη, πρόκειται για τον τόπο της κεντρικής του διοίκησης στην ΕΕ. Ωστόσο, εάν δεν έχει κεντρική διοίκηση στην ΕΕ, τότε πρόκειται για την εγκατάστασή του στην ΕΕ όπου εκτελούνται οι κύριες δραστηριότητες επεξεργασίας στο πλαίσιο των δραστηριοτήτων εγκατάστασης του εκτελούντος την επεξεργασία.
Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων	Απαρτίζεται από τον προϊστάμενο μίας εποπτικής Αρχής κάθε κράτους μέλους και από τον Ευρωπαίο Επόπτη Προστασίας Δεδομένων. Έχει ως στόχο να συμβάλλει στη συνεκτική εφαρμογή του Κανονισμού σε ολόκληρη την ΕΕ.
Μηχανισμός Συνεκτικότητας	Ο μηχανισμός με βάση τον οποίο οι εποπτικές Αρχές συνεργάζονται μεταξύ τους, με κύριο στόχο τη συνεκτική εφαρμογή του Κανονισμού στο σύνολο της ΕΕ[16].
Κατάρτιση Προφίλ	Περιλαμβάνει οποιαδήποτε μορφή αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα που συνίσταται στη χρήση δεδομένων προσωπικού χαρακτήρα για την αξιολόγηση ορισμένων προσωπικών πτυχών ενός φυσικού προσώπου, ιδίως για την ανάλυση ή την πρόβλεψη πτυχών που αφορούν στην απόδοση στην εργασία, την οικονομική κατάσταση, την υγεία, τις προσωπικές προτιμήσεις, τα ενδιαφέροντα, την αξιοπιστία, τη συμπεριφορά, τη θέση ή τις μετακινήσεις του εν λόγω φυσικού προσώπου
Ψευδωνυμοποίηση	Πρόκειται για την 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.

[16] Στα άρθρα 64 έως και 67 αναφέρονται προβλέψεις για το ρόλο του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων, την επίλυση διαφορών μεταξύ των εποπτικών Αρχών, τις επείγουσες διαδικασίες και την ανταλλαγή απόψεων.

2. Ο Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων

2. Ο Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων. Παρουσίαση διατάξεων και νομολογία

Ο Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων αποτελεί μια αναγκαία μεταρρύθμιση του υφιστάμενου πλαισίου προστασίας προσωπικών δεδομένων, το οποίο, όπως προαναφέρθηκε, είχε ξεπεραστεί είτε από τις τεχνολογικές εξελίξεις, είτε από την αποτυχία ενιαίου τρόπου εφαρμογής των διατάξεων για την προστασία των προσωπικών δεδομένων στην ΕΕ, με αρνητικές συνέπειες στην ενιαία αγορά και τον ανταγωνισμό. Ωστόσο, το περιεχόμενο του αποτέλεσε, όπως αναπτύχθηκε ανωτέρω, αντικείμενο έντονων και πολυετών διαπραγματεύσεων, με αποτέλεσμα να είναι ένα κείμενο «συμβιβασμού» διαφορετικών τάσεων και προσεγγίσεων[17]. Έτσι, ενώ η αναγκαιότητα μεταρρύθμισης του πλαισίου προστασίας προσωπικών δεδομένων είναι απολύτως επιβεβλημένη και κατανοητή, αυτός που δεν γίνεται κατανοητός είναι ο φορμαλιστικός, γραφειοκρατικός, πολύπλοκος ορισμένες φορές, αλλά και αρκετά κοστοβόρος τρόπος που προβλέπεται τελικά για να το πετύχει. Ενδεικτικά, πρόκειται για ένα εκτεταμένο Κανονισμό, 5 φορές μεγαλύτερο από την Οδηγία, με 99 άρθρα, εκ των οποίων τα 28 αφήνουν περιθώριο παρέκκλισης για τα κράτη-μέλη.

Συνοπτικά, ο νέος Κανονισμός «έρχεται» με την επιδίωξη να ανταπεξέλθει στις προκλήσεις της ψηφιακής εποχής που προαναφέρθηκαν, εισάγοντας δύο ουσιώδεις διαφοροποιήσεις. Πρώτον, εισάγει την αρχή της λογοδοσίας, καθώς μεταφέρει το βάρος για την απόδειξη της συμμόρφωσης από τον ρυθμιστή / ελεγκτή στον ρυθμιζόμενο / ελεγχόμενο. Πλέον, οι επονομαζόμενοι «Υπεύθυνοι Επεξεργασίας» είναι εκείνοι που πρέπει να είναι σε θέση να αποδείξουν ότι έχουν λάβει όλα τα απαραίτητα μέτρα για την προστασία των προσωπικών δεδομένων, με την εποπτική Αρχή να αναλαμβάνει ρόλο και δράση σε δεύτερο χρόνο, ενώ στο παρελθόν ήταν εκείνη που είχε την πρωτοβουλία για την εποπτεία και τον έλεγχο συμμόρφωσης. Δεύτερον, ανανεώνει τα δικαιώματα των υποκειμένων. Δηλαδή, πλέον, οι ιδιοκτήτες των προσωπικών δεδομένων έχουν ενισχυμένα δικαιώματα, γεγονός στο οποίο οι επιχειρήσεις-υπεύθυνοι επεξεργασίας οφείλουν να προσαρμοστούν και συνεπώς να

[17] Αναφερόμαστε ενδεικτικά, σε αντιδράσεις κυρίως από την πλευρά των ΗΠΑ, καθώς οι επιχειρήσεις που χειρίζονται προσωπικά δεδομένα πολιτών της ΕΕ είναι επίσης υπόχρεες. Στις ΗΠΑ η φιλοσοφία του κανονιστικού πλαισίου είναι διαφορετική, με περισσότερα στοιχεία αυτορρύθμισης και θέσπισης κωδίκων δεοντολογίας στη λογική της προστασίας «από κάτω προς τα πάνω». Αντίθετα, στην ΕΕ η προσέγγιση περιλαμβάνει περιοριστικές ρυθμίσεις, στη λογική «από πάνω προς τα κάτω».

μεταβάλλουν ανάλογα τη λειτουργία και τις αποφάσεις τους. Στις επόμενες ενότητες παρουσιάζονται τα κυριότερα άρθρα του, το Σχέδιο Νόμου για την ενσωμάτωσή του στο εγχώριο δίκαιο και η νομολογία που έχει αναπτυχθεί μέχρι σήμερα.

2.1 Οι κυριότερες έννοιες και άρθρα του Κανονισμού

Είναι σημαντικό να αναφερθεί ότι η παρούσα μελέτη συντάχθηκε σε χρόνο κατά τον οποίο το Σχέδιο Νόμου του Υπουργείου Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα σε εφαρμογή του Κανονισμού (ΕΕ) 2016/679 βρισκόταν ακόμη σε στάδιο επεξεργασίας.

Κατά συνέπεια, η ανάλυση των βασικών ζητημάτων που ακολουθεί έχει στηριχθεί πρωτίστως στο κείμενο του Κανονισμού και επικουρικά στις σχετικές διατάξεις του κειμένου του Σχεδίου Νόμου όπως αυτό δημοσιοποιήθηκε κατά τη θέση του σε δημόσια διαβούλευση[18] και αποτυπώνεται υπό την επιφύλαξη τυχόν τροποποιήσεων που ενδέχεται να επέλθουν έως την τελική του δημοσίευση.

2.1.1 Θεμελιώδεις αρχές

Οι βασικές αρχές οι οποίες απαιτείται να τηρούνται κατά την επεξεργασία των προσωπικών δεδομένων από τους Υπεύθυνους Επεξεργασίας και τους Εκτελούντες αυτήν, είναι, σύμφωνα με το άρθρο 5 του Κανονισμού οι εξής:

Η αρχή της νόμιμης, αντικειμενικής και διαφανούς επεξεργασίας που επιβάλει την σύννομη, θεμιτή και με διαφανή τρόπο επεξεργασία αναφορικά με το υποκείμενο των δεδομένων. **Η νομιμότητα** της επεξεργασίας διασφαλίζεται, σύμφωνα με το άρθρο 6 του Κανονισμού, στις περιπτώσεις στις οποίες α) έχει ληφθεί η προηγούμενη συναίνεση του υποκειμένου στην επεξεργασία των δεδομένων του για έναν ή περισσότερους συγκεκριμένους σκοπούς, β) η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης ή για τη συμμόρφωση με έννομη υποχρέωση του Υπευθύνου Επεξεργασίας που απορρέει από άλλο κανόνα δικαίου, γ) η επεξεργασία είναι απαραίτητη για την διαφύλαξη ζωτικού συμφέροντος ή για την εκπλήρωση καθήκοντος προς το δημόσιο συμφέρον ή για την άσκηση δημόσιας εξουσίας ανατεθειμένης στον Υπεύθυνο Επεξεργασίας και τέλος, δ) η επεξεργασία είναι απαραίτητη για τους σκοπούς των εννόμων συμφερόντων που επιδιώκει ο Υπεύθυνος Επεξεργασίας εκτός αν υποκείμενο είναι παιδί, περίπτωση στην οποία υπερισχύει το

[18] Δείτε εδώ το Σχέδιο Νόμου καθώς και τα σχόλια της διαβούλευσης

έννομο συμφέρον προστασίας του τέκνου. Η **διαφάνεια** εξασφαλίζεται μέσω της παροχής κάθε πληροφορίας και ανακοίνωσης σχετικά με την επεξεργασία με **συνοπτικό, διαφανή και κατανοητό τρόπο και σε εύκολα προσβάσιμη μορφή**[19]. Για την παροχή πληροφόρησης ή την διατύπωση της ανακοίνωσης, ιδίως εάν πρόκειται για ενημέρωση ανηλίκων, πρέπει να γίνεται χρήση **σαφούς και απλής διατύπωσης**. Η πληροφορία πρέπει να δίνεται στο υποκείμενο των δικαιωμάτων εντός προθεσμίας ενός μήνα από την παραλαβή του σχετικού αιτήματός του (με δυνατότητα παράτασης για δύο μήνες) ενώ στην περίπτωση που η παροχή της πληροφορίας δεν είναι εφικτή, ο Υπεύθυνος επεξεργασίας οφείλει να ενημερώσει το υποκείμενο για την αδυναμία αυτή καθώς και να το πληροφορήσει για τη δυνατότητα υποβολής καταγγελίας στην αρμόδια εποπτική αρχή και για τη δυνατότητα άσκησης δικαστικής προσφυγής

Η αρχή του σκοπού που εκπληρώνεται όταν η συλλογή και η επεξεργασία γίνονται με στόχο σαφή και καθορισμένο που δεν επιτρέπει την υποβολή των δεδομένων σε περαιτέρω επεξεργασία. Μόνη επιτρεπτή εξαίρεση συνιστά η περαιτέρω επεξεργασία για σκοπούς αρχειοθέτησης που εξυπηρετούν το δημόσιο συμφέρον ή για σκοπούς επιστημονικής ή ιστορικής έρευνας, ή στατιστικούς σκοπούς υπό τον όρο ότι οι χρησιμοποιούμενες μέθοδοι αποκλείουν την ταυτοποίηση των υποκειμένων των δεδομένων και παρέχουν τις κατάλληλες εγγυήσεις για την προστασία των δεδομένων τους.

Η αρχή ελαχιστοποίησης των δεδομένων η οποία πρέπει να εφαρμόζεται τόσο στον όγκο των δεδομένων όσο και στη διάρκεια τήρησης αυτών και βάσει της οποίας τα δεδομένα που τηρούνται πρέπει να είναι κατάλληλα, συναφή και περιορισμένα στα απολύτως απαραίτητα αναφορικά με τους σκοπούς για τους οποίους εκτελείται η επεξεργασία.

Η αρχή της ακρίβειας σύμφωνα με την οποία τα δεδομένα θα πρέπει να είναι ακριβή και, όταν είναι αναγκαίο, να επικαιροποιούνται ενώ το υποκείμενο θα πρέπει να έχει επαρκή ενημέρωση ως προς τα προσωπικά του δεδομένα τα οποία υφίστανται επεξεργασία. Παράλληλα, πρέπει να λαμβάνονται όλα τα εύλογα μέτρα για την άμεση διαγραφή ή διόρθωση δεδομένων προσωπικού χαρακτήρα τα οποία είναι ανακριβή, σε σχέση με τους σκοπούς της επεξεργασίας[20].

---

[19] Δείτε εδώ τις Κατευθυντήριες Οδηγίες της Ομάδας Εργασίας 29 για την αρχή της διαφάνειας.

[20] Από την επίσημη ιστοσελίδα της Ανεξάρτητης Κυπριακής Εποπτικής Αρχής «Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα», δείτε εδώ τη σχετική αναφορά.

Η αρχή του περιορισμού της περιόδου αποθήκευσης, δηλαδή την τήρηση των αρχείων των δεδομένων για όσο διάστημα χρειάζεται για την επίτευξη του σκοπού της επεξεργασίας. Εξαίρεση προβλέπεται στην περίπτωση κατά την οποία η επεξεργασία γίνεται για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς και λαμβάνονται τα κατάλληλα οργανωτικά μέτρα για τη διασφάλιση των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων.

Η αρχή της ακεραιότητας και εμπιστευτικότητας που καλεί για την υποβολή των δεδομένων σε επεξεργασία κατά τρόπο ώστε να 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.

Η αρχή της αναλογικότητας που επιβάλλει να υπάρχει συνάφεια ανάμεσα στα δεδομένα που τηρούνται και στο σκοπό για τον οποίο αυτά συλλέγονται, καθώς και να είναι τα δεδομένα αυτά πρόσφορα και αναγκαία για την εκπλήρωση του σκοπού αυτού. Με τον τρόπο αυτό, η αρχή της αναλογικότητας οδηγεί πρακτικά στην ελαχιστοποίηση των τηρούμενων δεδομένων, αφού το πιθανότερο είναι πως οι προϋποθέσεις αυτές δεν ισχύουν για το σύνολο των δεδομένων που συλλέγονται από τον Υπεύθυνο Επεξεργασίας ή τον Εκτελούντα την Επεξεργασία.

Τέλος, η **αρχή της λογοδοσίας** υπό την οποία ο Υπεύθυνος Επεξεργασίας και ο εκτελών την επεξεργασία φέρουν την ευθύνη να αποδείξουν όχι μόνο την συμμόρφωση στις υποχρεώσεις που θέτει ο Κανονισμός αλλά και την ετοιμότητά τους να συμμορφωθούν. Οι υποχρεώσεις τους δεν είναι προκαθορισμένες και σταθερές αλλά διαμορφώνονται ανάλογα με τον κίνδυνο που ενδέχεται να προκύψει από την επεξεργασία, όπως ο κίνδυνος αυτός εκτιμάται ήδη πριν την έναρξη της επεξεργασίας, βάσει της Εκτίμησης Αντικτύπου σχετικά με την προστασία των δεδομένων.

2.1.2 Σύστημα κυρώσεων

Δομικό στοιχείο του Κανονισμού, της πολιτικής συμμόρφωσης που προβλέπει και κατ' επέκταση της ίδιας της αποτελεσματικότητας εφαρμογής αποτελεί το σύστημα κυρώσεων που περιγράφεται. Και αυτό γιατί, όπως ήδη αναφέρθηκε, το ιδιαίτερα αυστηρό κυρωτικό πλαίσιο του Κανονισμού είναι ίσως ο κύριος λόγος για τη δημοσιότητα που έχει λάβει η εφαρμογή του αλλά και η βασική αιτία για την τόσο γρήγορη διάχυση της πληροφορίας σχετικά με τις νέες υποχρεώσεις των υπεύθυνων επεξεργασίας και την ένταση με την οποία αυξήθηκαν οι δράσεις ενημέρωσης των υποκειμένων των δεδομένων.

Ωστόσο, παρόλη την αναστάτωση που έχει επικρατήσει στην αγορά, πρέπει να σημειωθεί, ότι αν σκοπός του Κανονισμού είναι η ανάπτυξη μιας γενικότερης φιλοσοφίας πρόληψης και μέριμνας για την προστασία των δεδομένων από την πλευρά των επιχειρήσεων, ο σκοπός αυτός έχει, σε μεγάλο βαθμό επιτευχθεί.

Σε αντίθεση με την Οδηγία η οποία άφηνε ιδιαίτερα μεγάλη διακριτική ευχέρεια στα κράτη μέλη να λάβουν «τα κατάλληλα μέτρα» για να εξασφαλίσουν την πλήρη εφαρμογή της -καταλήγοντας τελικά σε εφαρμοστικές αποκλίσεις και αυξάνοντας το κόστος συμμόρφωσης των επιχειρήσεων με διασυνοριακή δράση- ο Κανονισμός προβλέπει ενιαίες, εξαιρετικά αυστηρές διοικητικές κυρώσεις. Η μόνη διακριτική ευχέρεια που καταλείπει στους εθνικούς νομοθέτες αφορά στη δυνατότητα που δίνει στους εθνικούς νομοθέτες για θέσπιση ποινικών κυρώσεων.

Προβλέπεται 2% πρόστιμο για διοικητικές / γραφειοκρατικές παραλείψεις ενώ για υπαίτιες παραβάσεις προβλέπεται η δυνατότητα επιβολής προστίμου ίσου με το 4% του ετήσιου παγκόσμιου τζίρου της επιχείρησης.

Ειδικότερα, οι κατευθύνσεις[21] που δίνονται στις αρμόδιες αρχές ως προς τον υπολογισμό του διοικητικού προστίμου περιλαμβάνονται στο άρθρο 83 όπου, μεταξύ άλλων, πρέπει να συνεκτιμηθούν 11 επιμέρους κριτήρια όπως η φύση, η βαρύτητα και η διάρκεια της παράβασης, το μέγεθος της προσβολής, ο αριθμός των παραβάσεων, οι περιστάσεις τέλεσης της παράβασης, η εν γένει συμπεριφορά του παραβάτη και ο σκοπός της επεξεργασίας ο βαθμός ευθύνης, η υποτροπή, ο βαθμός συνεργασίας με την εποπτική αρχή κ.ά.

[21] Δείτε εδώ τις Κατευθυντήριες Γραμμές της Ομάδας Εργασίας 29 για την εφαρμογή και τον καθορισμό διοικητικών προστίμων για τους σκοπούς του κανονισμού 2016/679.

Περαιτέρω, στο πλαίσιο της άσκησης των αρμοδιοτήτων της και βάσει του άρ. 58 του Κανονισμού (και αντίστοιχα του άρ. 62 του Σχεδίου Νόμου), η Αρχή μπορεί ακόμη να ειδοποιήσει τον υπεύθυνο επεξεργασίας ή τον εκτελούντα αυτήν, για εικαζόμενη παράβαση, να του απευθύνει προειδοποιήσεις, επιπλήξεις και εντολές για συμμόρφωση με συγκεκριμένο τρόπο ή εντός ορισμένης προθεσμίας ή να επιβάλει προσωρινό ή οριστικό περιορισμό, περιλαμβανομένης της απαγόρευσης επεξεργασίας.

Παράλληλα, στο άρθρο 84, δίνεται η δυνατότητα στα κράτη μέλη για θέσπιση ποινικών κυρώσεων, επιλογή για την οποία η νομοπαρασκευαστική επιτροπή δέχθηκε αρνητική κριτική κατά τη δημόσια διαβούλευση του ελληνικού Σχεδίου Νόμου καθώς στο άρθρο 70 αυτού, εξάντλησε τη διακριτική της ευχέρεια προβλέποντας τη δυνατότητα επιβολής ποινών φυλάκισης ή και κάθειρξης καθώς και χρηματικές ποινές που μπορεί να φτάσουν τις €300.000.

Όπως γίνεται αντιληπτό, το γεγονός ότι καταλείπεται αρκετά μεγάλη διακριτική ευχέρεια στην άσκηση των αρμοδιοτήτων τους κατά την εφαρμογή του κυρωτικού πλαισίου, οδηγεί στη δημιουργία προβληματισμού ως προς την εφαρμογή των κυρωτικών διατάξεων από τις αρμόδιες εθνικές αρχές.

Περαιτέρω, αναφορικά με την κατά τόπο αρμοδιότητα των εθνικών αρχών για την αυτεπάγγελτη διαπίστωση παραβάσεων ή για τον έλεγχο καταγγελιών εκ μέρους των υποκειμένων των δεδομένων και για την επιβολή διοικητικών κυρώσεων κρίσιμο παράγοντα αποτελεί ο τόπος διαμονής του υποκειμένου των δεδομένων σύμφωνα με την αιτιολογική σκέψη 122 και το άρθρο 83 του Κανονισμού. Κατά συνέπεια, μόνο εφόσον το υποκείμενο των δεδομένων βρίσκεται στην επικράτεια του κράτους μέλους της εποπτικής αρχής μπορεί εκείνη να ασκήσει τις εξουσίες που της δίνει ο Κανονισμός.

Αντίθετα, σε περίπτωση επεξεργασίας δεδομένων υποκειμένου που διαμένει σε άλλο κράτος μέλος από τον υπεύθυνο επεξεργασίας, ο Κανονισμός καλεί για συνεργασία μεταξύ των Αρχών με υποχρέωση παροχής αμοιβαίας αλληλοϋποστήριξης και συνδρομής, κατά τις αιτιολογικές σκέψεις 130 και 133.

Στην περίπτωση πολλαπλών εγκαταστάσεων του υπεύθυνου επεξεργασίας ή του εκτελούντος αυτή και τη διασυνοριακή επεξεργασία δεδομένων εντός ΕΕ, είναι σκόπιμο να καθοριστεί το κράτος-μέλος της κύριας εγκατάστασής του στην ΕΕ, ώστε να μπορεί να απευθύνεται στην εποπτική Αρχή του κράτους αυτού - η οποία θεωρείται

η επικεφαλής εποπτική Αρχή[22]. Αυτό αποτελεί τον μηχανισμό μίας στάσης ("One stop shop"), σύμφωνα με τον οποίο προβλέπεται συνεργασία μεταξύ της επικεφαλής εποπτικής Αρχής και των ενδιαφερόμενων εθνικών Αρχών στην αρμοδιότητα των οποίων μπορεί να εμπίπτει μια υπόθεση ώστε να διασφαλίζεται ομοιογένεια στην αντιμετώπιση υποθέσεων διευρωπαϊκού ενδιαφέροντος και ασφάλεια δικαίου τόσο για τους υπευθύνους επεξεργασίας όσο και για τους πολίτες της Ένωσης.

Εξάλλου, εντύπωση προκαλεί και η πρωτοφανής θέσπιση στα άρ. 63 έως 76 του Κανονισμού ενός «μηχανισμού συνεκτικότητας» μέσω του οποίου ρυθμίζεται η συνεργασία των εθνικών ελεγκτικών μηχανισμών με τη βοήθεια του «Συμβουλίου Προστασίας Δεδομένων» που συστήνεται για να συντονίζει το έργο τους. Πρέπει ωστόσο να σημειωθεί ότι ο συγκεκριμένος μηχανισμός ενεργοποιείται μόνο εφόσον οι υπεύθυνοι ή εκτελούντες την επεξεργασία είναι εγκατεστημένοι εντός της Ένωσης καθώς, σε διαφορετική περίπτωση, θα πρέπει να γίνεται ad hoc διαχείριση από κάθε εθνική αρχή.

Ως προς την ανάγκη διαπίστωσης επέλευσης συγκεκριμένης βλάβης στο υποκείμενο των δεδομένων από την επεξεργασία ή την ανάγκη για προηγούμενη επίκληση τέτοιας βλάβης εκ μέρους του, το ΣτΕ έκρινε ότι αυτή δεν αποτελεί προϋπόθεση για την επιβολή προστίμου[23]. Στο ίδιο πνεύμα κινήθηκε και το ΔΕΕ σε απόφασή του με την οποία έκρινε ότι ένα σύστημα αντικειμενικής ποινικής ευθύνης που τιμωρεί την παράβαση διατάξεων του Κανονισμού, δεν είναι αυτό καθ' εαυτό ασυμβίβαστο προς το ενωσιακό δίκαιο[24].

Ως προς το κατά πόσο ο Κανονισμός υιοθετεί το σύστημα της αντικειμενικής ευθύνης και την επιβολή κυρώσεων ανεξαρτήτως υπαιτιότητας του παραβάτη των διατάξεων του, παρατηρείται ότι η αναφορά του άρθρου άρ. 83 παρ. 2εδ. β στοιχείο β' ότι «*Κατά τη λήψη απόφασης σχετικά με την επιβολή διοικητικού προστίμου, καθώς και σχετικά με το ύψος του διοικητικού προστίμου για κάθε μεμονωμένη περίπτωση, λαμβάνονται δεόντως υπόψη τα ακόλουθα:…ο δόλος ή η αμέλεια που προκάλεσε την παράβαση*», μάλλον να τεκμηριώνει την άποψη ότι δεν απαιτείται η ύπαρξη πταίσματος του παραβάτη καθώς δε φαίνεται να υποχρεώνει αλλά προτείνει στις αρχές να λαμβάνουν υπόψη το στοιχείο της υπαιτιότητας.

---

[22] Κατεβάστε εδώ τις Κατευθυντήριες γραμμές της Ομάδας Εργασίας άρθρου 29 για τον προσδιορισμό της επικεφαλής εποπτικής αρχής των υπευθύνων επεξεργασίας ή των εκτελούντων την επεξεργασία και Απαντήσεις σε Συχνές Ερωτήσεις.

[23] Βλ. ΣτΕ 1367/2008

[24] Ute Reindl 13.11.2014, C-443/13

Αμφισβητούμενο είναι ακόμη το κατά πόσο τα διοικητικά πρόστιμα προβλέπονται επιπροσθέτως ή αντί των διορθωτικών μέτρων. Σύμφωνα με μια άποψη, τα διοικητικά μέτρα επιβάλλονται σε κάθε περίπτωση[25] ενώ είναι δυνατή και η υποστήριξη της αντίθετης θέσης, ότι η επίπληξη θα μπορούσε να αντικαταστήσει τη διοικητική κύρωση[26].

Ουσιαστικά, ο μόνος περιορισμός που τίθεται στην επιβολή των κυρώσεων που προβλέπει ο Κανονισμός είναι η υποχρέωση σεβασμού της αρχής της αναλογικότητας. Ειδικότερα, βάσει του άρ. 83 παρ. 1, η κύρωση πρέπει να είναι «αποτελεσματική, αναλογική και αποτρεπτική» ενώ στο ενωσιακό δίκαιο εντοπίζονται και άλλοι περιορισμοί στην ελευθερία των εθνικών αρχών κατά την άσκηση των εξουσιών τους, όπως η αρχή της ομοιόμορφης εφαρμογής, της καλόπιστης συνεργασίας[27] και η αρχή της ίσης μεταχείρισης.

Ακόμα και η ενδεχόμενη κακή οικονομική κατάσταση της επιχείρησης στην οποία επιβάλλεται το πρόστιμο σύμφωνα με την αιτιολογική σκέψη 150 του Κανονισμού, δεν πρέπει να λαμβάνεται υπόψη για τον υπολογισμό αυτού.

Ενδεικτικά ακόμη αναφέρεται ότι και η επιβολή διοικητικού προστίμου σε πρωτόπειρο παραβάτη δε μπορεί να θεωρηθεί per se μη αναλογική, καθώς το διοικητικό πρόστιμο θα πρέπει να είναι σημαντικά υψηλότερο από το όποιο υπολογίσιμο κέρδος/ εξοικονόμηση δαπάνης του παραβάτη.

Πρέπει να συνεκτιμάται όμως η ανάγκη για ενιαία εφαρμογή της αρχής της προστασίας δεδομένων έναντι της επεξεργασίας τους, προκειμένου να αποφευχθούν περιπτώσεις «άγρας εποπτικής αρχής» όπως για παράδειγμα τα φαινόμενα forum shopping που έχουν παρατηρηθεί σε άλλους κλάδους του δικαίου (βλ. πτωχευτικό δίκαιο).

Σε κάθε περίπτωση, τον τελικό λόγο θα τον έχει η Αρχή κατά την άσκηση της ad hoc κρίσης της στο πλαίσιο της διακριτικής ευχέρειας που της δίνει ο Κανονισμός στην αιτιολογική σκέψη 150, σύμφωνα με την οποία η εποπτική αρχή πρέπει να έχει «την εξουσία» και όχι την «υποχρέωση» να επιβάλει τα πρόστιμα. Ενδιαφέρον θα έχει

[25] Κατά το γράμμα του άρ. 83 παρ. 2 εδ. α' σε συνδυασμό με την αιτιολογική σκέψη 148 εδ. πρώτο.
[26] Στο ίδιο άρ. 83 παρ. 2 εδ. β' και στην αιτιολογική σκέψη αρ. 148 εδ. δεύτερο, γίνεται λόγος για στοιχεία που πρέπει να λαμβάνονται υπόψη σχετικά με την επιβολή του προστίμου και του ύψους του για κάθε μεμονωμένη περίπτωση, ενώ σε περίπτωση παράβασης ελάσσονος σημασίας, ή αν το πρόστιμο θα αποτελούσε δυσανάλογη επιβάρυνση σε φυσικό πρόσωπο αναφέρεται ότι θα μπορούσε να επιβληθεί επίπληξη αντί προστίμου.
[27] Άρ. 4 παρ. 3 ΣΛΕΕ.

συνεπώς η πρακτική που θα ακολουθήσει κατά την εφαρμογή των διατάξεων του Κανονισμού. Σε κάθε περίπτωση όμως αξίζει να ειπωθεί ότι πρωταρχικός σκοπός του Κανονισμού δεν είναι η τιμωρία του παραβάτη, αλλά η συμμόρφωση του και η πιστή τήρηση των ρυθμίσεων του, με κύριο μήνυμα την αποτροπή και την πρόληψη.

2.1.3 Ευθύνη Υπεύθυνου Επεξεργασίας και Εκτελούντος την Επεξεργασία

Σύμφωνα με τα οριζόμενα στον Κανονισμό, **υπεύθυνος επεξεργασίας είναι κάθε επιχείρηση ή οργανισμός ανεξαρτήτως μεγέθους που συλλέγει και επεξεργάζεται προσωπικά δεδομένα για ίδιο λογαριασμό**. Στην περίπτωση που η επεξεργασία δεν εκτελείται από την ίδια αλλά γίνεται από κάποιο τρίτο μέρη για λογαριασμό της, το μέρος αυτό είτε πρόκειται για φυσικό είτε για νομικό πρόσωπο είναι ο «εκτελών την επεξεργασία» προς τον οποίο ο υπεύθυνος επεξεργασίας οφείλει να περιγράψει το σκοπό και τον τρόπο σύμφωνα με τον οποίο επιθυμεί να εκτελείται η επεξεργασία. Ως τρίτο μέρος νοείται επιχείρηση ή φυσικό πρόσωπο το οποίο δεν αποτελεί μέρος του οργανισμού του Υπεύθυνου επεξεργασίας, όπως οι εργαζόμενοι μιας επιχείρησης που, στο πλαίσιο της εργασίας τους επεξεργάζονται δεδομένα προσωπικού χαρακτήρα[28].

Η έκταση της ευθύνης του υπεύθυνου επεξεργασίας προβλεπόταν ήδη στην Οδηγία, δεν καταλάμβανε όμως και τον εκτελούντα την επεξεργασία, κάτι το οποίο πλέον κάνει ο Κανονισμός που επεκτείνει την ευθύνη και προς το μέρος αυτό, προβλέποντας την εις ολόκληρο ευθύνη του για αποζημίωση αλλά και επιβολή κυρώσεων εφόσον δεν ανταποκρίθηκε στις υποχρεώσεις του Κανονισμού, υπερέβη ή ενήργησε αντίθετα προς τις νόμιμες εντολές του υπευθύνου επεξεργασίας.

Αξίζει να τονιστεί όμως ότι ο υπεύθυνος επεξεργασίας ευθύνη φέρει για τη συνολική ευθύνη τήρησης των διατάξεων του Κανονισμού καθώς, όχι μόνο έχει την υποχρέωση να χρησιμοποιεί «μόνο εκτελούντες την επεξεργασία που παρέχουν επαρκείς διαβεβαιώσεις για την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων, κατά τρόπο ώστε η επεξεργασία να πληροί τις απαιτήσεις του Κανονισμού και να διασφαλίζεται η προστασία των δικαιωμάτων του υποκειμένου των δεδομένων»[29] αλλά οφείλει να ασκεί εποπτεία επί των εκτελούντων στους οποίους έχει αναθέσει την επεξεργασία, προκειμένου να διασφαλίζει το σύννομο των ενεργειών τους.

[28] Κομνηνός Κόμνιος, GDPR: Η σύμβαση με τον εκτελούντα την επεξεργασία
[29] Άρθρο 28 παρ. 1 του Κανονισμού

Ωστόσο, βάσει της Οδηγίας για την επιβολή κυρώσεων και επιδίκαση αποζημίωσης στον υπεύθυνο επεξεργασίας απαιτούνταν να συντρέχουν σωρευτικά, οι ακόλουθες προϋποθέσεις: α) συμπεριφορά (πράξη ή παράλειψη) που παραβιάζει τις διατάξεις του ν.2472/1997 ή (και) των κατ' εξουσιοδότηση αυτού κανονιστικών πράξεων της Αρχής, β) ηθική βλάβη, γ) αιτιώδη συνάφεια μεταξύ της συμπεριφοράς και της ηθικής βλάβης» και δ) υπαιτιότητα, ήτοι γνώση ή υπαίτια άγνοια, αφενός των περιστατικών που συνιστούν την παράβαση και αφετέρου της πιθανότητας να επέλθει η ηθική βλάβη[30]. Ἐβρισκε επομένως εφαρμογή η λειτουργία του συστήματος της νόθου αντικειμενικής ευθύνης, δηλαδή πρακτικά ο υπεύθυνος επεξεργασίας εφόσον αποδείκνυε ότι δεν ευθύνεται για το ζημιογόνο γεγονός που έθεσε σε κίνδυνο προσωπικά δεδομένα μπορούσε να απαλλαγεί.

Αντίθετα, όπως αναφέρθηκε και στις παρατηρήσεις σχετικά με το σύστημα επιβολής κυρώσεων, ο Κανονισμός στρέφεται προς το αντικειμενικό σύστημα, βάσει του οποίου τα στοιχεία του δόλου ή της αμέλειας συνυπολογίζονται μεν κατά τον υπολογισμό του προστίμου, εντούτοις η συνδρομή τους δεν συνιστά προϋπόθεση για την επιβολή κυρώσεων εκ μέρους της εποπτικής Αρχής.

Επιπλέον, παρατηρείται η μεταφορά ευθύνης για την τήρηση των διατάξεων από την Αρχή στο πρόσωπο του υπεύθυνου επεξεργασίας και του εκτελούντα αυτήν. Δεν αρκεί μια απλή τυπική συμπλήρωση ενός "check list», αλλά απαιτείται η αλλαγή φιλοσοφίας και κουλτούρας[31] καθώς και η δημιουργία δεσμών εμπιστοσύνης στις συναλλαγές και στις συμβατικές σχέσεις και εισάγεται ένα νέο μοντέλο σχέσης μεταξύ του υποκειμένου των δεδομένων και του υπεύθυνου επεξεργασίας των δεδομένων, μέσω της ενίσχυσης των δικαιωμάτων του πρώτου και της αύξησης των υποχρεώσεων του δεύτερου.

Ἑνα νέο μοντέλο σχέσης εισάγεται επίσης και μεταξύ της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και του υπεύθυνου επεξεργασίας, μέσω της υποχρέωσης του δεύτερου για ανάληψη όλων των πρωτοβουλιών σε σχέση με την τήρηση των υποχρεώσεών του καθώς οφείλει να ορίσει υπεύθυνο προστασίας προσωπικών δεδομένων και να προβεί σε συγκεκριμένες διαδικασίες που εξασφαλίζουν τη συμμόρφωση (όπως η συγκατάθεση του υποκειμένου, η διεξαγωγή data protection impact assessment κ.ά.).

---

30 ΕφΑθ 1437/2014

31 Βλ. εισήγηση κ. Γ. Γιαννόπουλου, 20 ετήσιο συνέδριο E-themis «Το νέο τοπίο για τις επιχειρήσεις στη διαχείριση των προσωπικών δεδομένων», 11-12 Μαΐου 2018

Αντίθετα βάσει του Κανονισμού, ο υπεύθυνος επεξεργασίας πρέπει να είναι σε θέση να αποδεικνύει τη συμμόρφωση των δραστηριοτήτων επεξεργασίας και την αποτελεσματικότητα των μέτρων που έχει λάβει για την επίτευξη της συμμόρφωσης.

Παρότι η Οδηγία έκανε γενική αναφορά στην προϋπόθεση λήψης των κατάλληλων τεχνικών και οργανωτικών μέτρων για τη διασφάλιση της σύννομης επεξεργασίας, ο Κανονισμός προβαίνει σε μια πιο λεπτομερή ανάπτυξη του θέματος, απαιτώντας όχι μόνο την ενημέρωση της αρχής σε περιπτώσεις παραβάσεων αλλά και την εκπόνηση μιας εκτίμησης του κινδύνου που ενδέχεται να επέλθει από την επεξεργασία.

Για το λόγο αυτό, πριν από την κατασταλτική αρμοδιότητα της Αρχής, τον πρώτο λόγο έχει η υποχρέωση για 72ωρη προειδοποίηση της από τον ΥΕ ή τον ΥΠΔ. Η υποχρέωση αυτή είναι που τεκμηριώνει την νέα εποχή στη προστασία των προσωπικών δεδομένων. Ο Υπεύθυνος Επεξεργασίας ή ο ΥΠΔ οφείλει να ειδοποιήσει την Αρχή γιατί αντιλήφθηκε τη διαρροή. Αλλά μόνος τρόπος να αντιληφθεί κανείς τη διαρροή, πέρα από την καθαρή τύχη είναι να γνωρίζει σε τι συνίσταται η διαρροή, να μπορεί δηλαδή να την αντιληφθεί. Και είναι αδύνατον να μπορέσει να αντιληφθεί τη διαρροή αν δεν παρακολουθεί διαρκώς τις διαδικασίες, τα πρωτόκολλα και τις ροές των δεδομένων που τηρεί.

Στην αφετηρία του λογικού αυτού νήματος βρίσκεται μια μόνο παραδοχή: Η γνώση του υπεύθυνου επεξεργασίας σχετικά με την υποχρέωση προστασίας των δεδομένων. Μόνος λόγος για συστηματική παρακολούθηση των ροών των δεδομένων, είναι η γνώση του ότι οφείλει να τα προστατεύει.

Σε αντίθεση με την πλειοψηφία των υπόλοιπων ρυθμιστικών κανόνων, η υποχρέωση που θέτει ο Κανονισμός για ειδοποίηση της εποπτικής Αρχής σε περίπτωση διαρροής δεδομένων από το Υπεύθυνο Επεξεργασίας, ο Κανονισμός αποδέχεται ότι, είτε από αμέλεια είτε από δόλο, είναι αδύνατον να εκλείψουν τα περιστατικά διαρροής δεδομένων.

Περαιτέρω, ο υπεύθυνος επεξεργασίας οφείλει να ορίζει προθεσμίες για τη διαγραφή των δεδομένων ή για την περιοδική επανεξέτασή τους προκειμένου να διασφαλίσει ότι δε διατηρούνται περισσότερο από όσο είναι αναγκαίο, καθώς και ότι όσα από αυτά δεν είναι ακριβή, διορθώνονται ή διαγράφονται. Η επεξεργασία θα πρέπει να γίνεται με τρόπο που να διασφαλίζει την ενδεδειγμένη προστασία και εμπιστευτικότητα τους, μεταξύ άλλων και για να αποτρέπεται κάθε ανεξουσιοδότητη πρόσβαση σε αυτά και

στον εξοπλισμό που χρησιμοποιείται για την επεξεργασία τους ή η χρήση αυτών και του εν λόγω εξοπλισμού.

2.1.4 Εκπόνηση Εκτίμησης Αντικτύπου σχετικά με την προστασία δεδομένων

Η Εκτίμηση Αντικτύπου σχετικά με την προστασία δεδομένων (Data Privacy Impact Assessment-DPIA) αποτελεί μια έννοια σε απόλυτη σύμπνοια με τη φιλοσοφία του Κανονισμού που καλεί για προστασία των υποκειμένων των δεδομένων από «υψηλούς κινδύνους» μέσω του έγκαιρου σχεδιασμού και λήψης όλων των απαραίτητων προληπτικών μέτρων. Όπως ήδη αναφέρθηκε, ο Υπεύθυνος Επεξεργασίας και ο Εκτελών την Επεξεργασία υποχρεούνται σε τήρηση της αρχής της λογοδοσίας κατά την επεξεργασία δεδομένων, καθώς οι ενέργειές τους δεν αρκεί να είναι σύμφωνες με τα οριζόμενα στον Κανονισμό αλλά πρέπει και να είναι διαρκώς σε θέση να αποδείξουν ότι έχουν λάβει όλα τα ενδεδειγμένα μέτρα για τη συμμόρφωση αυτή. Η Εκτίμηση Αντικτύπου βοηθάει στην εκπλήρωση και των δύο πτυχών της αρχής της λογοδοσίας. Και αυτό γιατί, ανάλογα με τον κίνδυνο που μπορεί να προκύψει από την επεξεργασία των δεδομένων, όπως η στάθμιση του κινδύνου αυτού προέκυψε κατά την εκπόνηση της Εκτίμησης Αντικτύπου, προκύπτουν και τα μέτρα που θα κριθούν ως ενδεδειγμένα για την αντιμετώπισή του.

Σύμφωνα με τις κατευθυντήριες γραμμές της ομάδας του άρθρου 29[32], η Εκτίμηση Αντικτύπου «είναι μια διαδικασία που έχει σχεδιαστεί για να περιγράψει την επεξεργασία, να αξιολογήσει την αναγκαιότητα και την αναλογικότητά της και να συνδράμει στη διαχείριση των κινδύνων για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων που συνεπάγεται η επεξεργασία των δεδομένων προσωπικού χαρακτήρα, με την αξιολόγησή τους και τον καθορισμό μέτρων για την αντιμετώπισή τους»[33].

Η εκτίμηση αυτή είναι απαραίτητη κάθε φορά που η επεξεργασία ενδέχεται να έχει ως αποτέλεσμα υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Σύμφωνα με τον Κανονισμό, η εκπόνηση της απαιτείται α) όταν πραγματοποιείται συστηματική και εκτενής αξιολόγηση προσωπικών πτυχών ενός

[32] Δείτε εδώ τις Κατευθυντήριες γραμμές της Ομάδας Εργασίας του άρθρου 29 για την εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων και τον καθορισμό του κατά πόσον η επεξεργασία «ενδέχεται να επιφέρει υψηλό κίνδυνο» για τους σκοπούς του Κανονισμού 2016/679.

[33] Κατευθυντήριες γραμμές για την εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) και καθορισμός του κατά πόσον η επεξεργασία «ενδέχεται να επιφέρει υψηλό κίνδυνο» για τους σκοπούς του κανονισμού 2016/679.

φυσικού προσώπου, συμπεριλαμβανομένης της κατάρτισης προφίλ[34], β) όταν πραγματοποιείται επεξεργασία ευαίσθητων δεδομένων σε μεγάλη κλίμακα ή γ) όταν παρακολουθούνται συστηματικά δημόσια προσπελάσιμοι χώροι σε μεγάλη κλίμακα.

Οι εθνικές αρχές είναι επιφορτισμένες με τη δημοσιοποίηση καταλόγων με τα είδη των πράξεων επεξεργασίας για τα οποία απαιτείται εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων. Σημειώνεται ότι η σχετική υποχρέωση από την πλευρά της ΑΠΔΠΧ δεν έχει υλοποιηθεί, καθώς το Σχέδιο Νόμου για τη μεταφορά των υποχρεώσεων του Κανονισμού στην ελληνική έννομη τάξη που τη μνημονεύει, παραμένει αδημοσίευτο.

Η Εκτίμηση Αντικτύπου πρέπει να περιλαμβάνει κατ' ελάχιστον: περιγραφή των προβλεπόμενων λειτουργιών επεξεργασίας και των σκοπών της επεξεργασίας, εκτίμηση (α) της ανάγκης και της αναλογικότητας της επεξεργασίας και (β) των κινδύνων που ανακύπτουν για τα υποκείμενα των δεδομένων, κατάλογο με τα μέτρα τα οποία προβλέπονται πρώτον, για να περιοριστούν οι κίνδυνοι αυτοί και δεύτερον, προς συμμόρφωση με τον Κανονισμό.

Όπως γίνεται αντιληπτό, η επιτυχία της Εκτίμησης Αντικτύπου συνδέεται ευθέως με το χρονικό σημείο στο οποίο αυτή θα διεξαχθεί. Όσο νωρίτερα εντοπιστούν κατά το σχεδιασμό ενός νέου έργου, συστήματος ή μιας οποιασδήποτε νέας διαδικασίας, ευρήματα που μπορεί να οδηγούν σε «κίνδυνο» για τα προσωπικά δεδομένα, τόσο μεγαλύτερη θα είναι η ακρίβεια και η αποτελεσματικότητα των μέτρων που θα ληφθούν και θα ενσωματωθούν για την προστασία των δεδομένων αυτών. Η διαδικασία έγκαιρης διάγνωσης, εντοπισμού των πιθανών κινδύνων και ενσωμάτωσης των κατάλληλων μέτρων προστασίας κατά το σχεδιασμό είναι γνωστή ως "privacy by design". Παράλληλα με την έγκαιρη εκπόνησή της, παράγοντα επιτυχίας της Εκτίμησης Αντικτύπου θα αποτελέσει και η εμπλοκή των κατάλληλων ανθρώπων, εκείνων με την κατάλληλη εμπειρία και γνώση και, σε κάθε περίπτωση, του ΥΠΔ.

Ο Κανονισμός δεν περιλαμβάνει πρότυπο της συγκεκριμένης έκθεσης. Ωστόσο, στο Παράρτημα των κατευθυντήριων γραμμών που εξέδωσε η ομάδα του άρθρου 29, περιγράφονται τα «Κριτήρια για μια αποδεκτή Εκτίμηση Αντικτύπου», τα οποία αποτελούν σύνθεση των άρθρων και των αιτιολογικών σκέψεων του Κανονισμού. Έτσι, οι υπεύθυνοι επεξεργασίας μπορούν να ανατρέξουν σε αυτά προκειμένου να αξιολογήσουν κατά πόσο μια Εκτίμηση Αντικτύπου ή μια μεθοδολογία διενέργειας

[34] Δείτε εδώ τις Κατευθυντήριες Γραμμές της Ομάδας Εργασίας άρθρου 29 για την Αυτοματοποιημένη ατομική λήψη αποφάσεων και κατάρτιση προφίλ.

Εκτίμησης Αντικτύπου είναι επαρκώς περιεκτική προκειμένου να συμμορφώνεται με τον Κανονισμό.

Στο πλαίσιο συμμόρφωσης με την υποχρέωση εκπόνησης Εκτίμησης Αντικτύπου, αρκετές επιχειρήσεις έχουν ενσωματώσει τα ISO 27001 (Information Security Management Systems), ISO 27005 (Information technology Security techniques Information security risk management) ή ISO 31000 (Risk Management) προς θεμελίωση ενός αρκετά καλού επιπέδου ικανότητας συμμόρφωσης.

Δεν είναι όμως πάντα ξεκάθαρο εάν ένας υπεύθυνος επεξεργασίας οφείλει να προβεί σε εκπόνηση Εκτίμηση Αντικτύπου. Υπάρχουν περιπτώσεις στις οποίες οι υπεύθυνοι και οι εκτελούντες την επεξεργασία αμφιταλαντεύονται ως προς κατά πόσο πληρούν τις προϋποθέσεις για υποχρεωτική εκπόνηση Εκτίμηση Αντικτύπου και παραμένουν σκεπτικοί ειδικά ενόψει του κόστους το οποίο αυτή συνεπάγεται. Σε κάθε περίπτωση, αφορμή για σκέψη πάνω σε θέματα στάθμισης κόστους- κινδύνου μπορεί να δώσει η διαπίστωση του Richard Clarke, ειδικού συμβούλου σε θέματα κυβερνοασφάλειας του τέως Προέδρου των Ηνωμένων Πολιτειών Ronald Reagan:

> ***« If you spend more on coffee than on IT security, you will be hacked. What's more, you deserve to be hacked»****
>
> ** «Εάν ξοδεύεις περισσότερα χρήματα για καφέ παρά για ασφάλεια πληροφοριακών συστημάτων, θα πέσεις θύμα κακόβουλης επίθεσης. Επιπλέον, θα το αξίζεις.»*

2.1.5 Ορισμός Υπεύθυνου Προστασίας Δεδομένων

Η φιλοσοφία του νέου Κανονισμού φέρνει αρκετές καινοτομίες καθώς εισάγει την αρχή της λογοδοσίας και μεταθέτει την ευθύνη για τη σύννομη τήρηση και επεξεργασία των δεδομένων στον υπεύθυνο επεξεργασίας και τον εκτελούντα την επεξεργασία χωρίς κάποιου είδους προληπτική παρέμβαση η προηγούμενο έλεγχο από την Αρχή όπως όριζε το προηγούμενο καθεστώς.

Επιδίωξη του ενωσιακού νομοθέτη αποτέλεσε η μείωση των γραφειοκρατικών διαδικασιών γνωστοποίησης της επεξεργασίας προσωπικών δεδομένων προς τις εποπτικές αρχές πριν την υιοθέτηση των σχετικών διαδικασιών, αλλά και του

διοικητικού βάρους που συνεπαγόταν η εκ των υστέρων εποπτεία της τήρησης των προϋποθέσεων του σύννομου της επεξεργασίας αυτής. Εξάλλου, από την έκθεση αποτίμησης της εφαρμογής των προβλέψεων του προηγούμενου καθεστώτος αποδείχθηκε η αναποτελεσματικότητα των μέτρων αυτών σε σχέση με το σκοπό για τον οποίο θεσπίστηκαν, δηλαδή την προστασία των δικαιωμάτων.

Στα μέτρα προστασίας των υποκειμένων δεδομένων περιλαμβάνονται τόσο μέτρα καταστολής, μέσω επιβολής κυρώσεων, όσο και μέτρα πρόληψης, ένα εκ των οποίων συνιστά η θέσπιση του νέου ρόλου του Υπεύθυνου Προστασίας που προβλέπεται πλέον ρητά στο άρθρο 39 του Κανονισμού. Ο ΥΠΔ συνομιλεί και συνεργάζεται απευθείας με την Αρχή, αντικαθιστώντας τον Υπεύθυνο Επεξεργασίας ως προς την αρμοδιότητά του αυτή ενεργώντας όχι μόνο ως μοναδικό σημείο επικοινωνίας από την πλευρά του Υπεύθυνου Επεξεργασίας, αλλά και εξυπηρετώντας τους σκοπούς τήρησης της υποχρέωσης προηγούμενης διαβούλευσης με την αρχή.

Ο ρόλος του είναι απόλυτα εναρμονισμένος με την πρωτοβουλία του ενωσιακού νομοθέτη για τη δημιουργία ενός νέου αποτελεσματικού πλαισίου, κεντρικό άξονα του οποίου αποτελεί η πρόληψη και η αποτροπή των φαινομένων παραβίασης της ιδιωτικότητας των υποκειμένων.

Στην προμετωπίδα της συμμόρφωσης, το πρόσωπο αυτό, η «φωνή της συνείδησης της επιχείρησης» όπως έχει χαρακτηριστεί[35] ενημερώνει και συμβουλεύει τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία αναφερόμενος απευθείας στην ανώτατη διοίκηση αλλά και το προσωπικό του οργανισμού σχετικά με τις υποχρεώσεις τους για την προστασία των προσωπικών δεδομένων. Παράλληλα, παρακολουθεί τη συμμόρφωση των πολιτικών που επιλέγει ο υπεύθυνος ή ο εκτελών την επεξεργασία και ελέγχει τη συμβατότητά τους με το σύνολο της ισχύουσας νομοθεσίας για την προστασία των προσωπικών δεδομένων ενώ τέλος παρέχει συμβουλές σχετικά με την υποχρέωση εκτίμησης αντικτύπου και παρακολουθεί την υλοποίησή της.

Στη Γερμανία, ο ρόλος αυτός υπήρχε ήδη από το 2001 υπό το προγενέστερο νομικό καθεστώς βάσει του οποίου θεσπιζόταν ο υποχρεωτικός ορισμός ΥΠΔ σε οργανισμούς με πάνω από εννέα άτομα προσωπικό[36]. Σύμφωνα με τον Thomas Spaeing, Επικεφαλής Οικονομικό Διευθυντή της Γερμανικής Ένωσης Υπεύθυνων Προστασίας

[35] Βλ. εισήγηση κ. Αλέξανδρου Βαρβέρη, 2ο ετήσιο συνέδριο E-themis «Προσωπικά δεδομένα και δικηγορία-Μια νέα πραγματικότητα, ένα νέο κεφάλαιο στο νομικό κόσμο», 11-12 Μαΐου 2018

[36] Paolo Calvi, German GDPR implementing rules

(BvD), ο κύριος ρόλος των ΥΠΔ δεν είναι η προστασία του οργανισμού από τον οποίο έχουν οριστεί, αλλά η προστασία των προσώπων των οποίων τα δεδομένα επεξεργάζεται ο οργανισμός[37].

Η υποχρέωση ορισμού ΥΠΔ ισχύει εφόσον συντρέχουν συγκεκριμένες προϋποθέσεις:

α) Ο Υπεύθυνος επεξεργασίας είναι Δημόσια αρχή ή φορέας, με την εξαίρεση των δικαστηρίων όταν αυτά ενεργούν υπό τη δικαιοδοτική τους αρμοδιότητα.

Ο Κανονισμός δεν περιλαμβάνει ορισμό της έννοιας της Δημόσιας αρχής ή του δημόσιου φορέα, αντίθετα καταλείπεται στην σφαίρα της πρωτοβουλίας του εκάστοτε κράτους μέλους να προβεί στον προσδιορισμό αυτό.

β) Οι βασικές δραστηριότητες του υπευθύνου επεξεργασίας συνιστούν επεξεργασία που απαιτεί την τακτική και συστηματική παρακολούθηση των δεδομένων σε μεγάλη κλίμακα.

Ως προς τις βασικές έννοιες που συνθέτουν την πρόταση αυτή, είναι χρήσιμη ίσως η παράθεση ορισμένων παραδειγμάτων και επεξηγήσεων.

«Βασικές δραστηριότητες» είναι εκείνες οι οποίες αποτελούν αναπόσπαστο κομμάτι για την επίτευξη των στόχων του υπευθύνου επεξεργασίας/ εκτελούντα την επεξεργασία. Χαρακτηριστικό τέτοιο παράδειγμα αποτελεί η συλλογή ευαίσθητων δεδομένων από τα νοσοκομεία καθώς η διαδικασία αυτή συνιστά αναπόσπαστο μέρος της βασικής τους δραστηριότητας. Αντίθετα, η συλλογή των προσωπικών δεδομένων του προσωπικού τους δεν αποτελεί βασική τους δραστηριότητα αλλά παραπληρωματική και βοηθητική προς την επίτευξη της βασικής δραστηριότητας.

Ως «τακτική και συστηματική παρακολούθηση» ορίζεται εκείνη που περιλαμβάνει όλες τις μορφές ανίχνευσης και κατάρτισης προφίλ στο διαδίκτυο, συμπεριλαμβανομένων των σκοπών της συμπεριφορικής διαφήμισης, η στοχευμένη επικοινωνία με email, ο γεωεντοπισμός, η χρήση κλειστών κυκλωμάτων παρακολούθησης και άλλες[38].

---

37 David Meier, What will mandatory DPOs look like under the GDPR? Germany could tell you

38 Από την επίσημη ιστοσελίδα της Ευρωπαϊκής Επιτροπής https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations_el

Για τον προσδιορισμό της «μεγάλης κλίμακας» κρίσιμους παράγοντες συνιστούν ο αριθμός των υποκειμένων των δεδομένων, είτε ως συγκεκριμένος αριθμός είτε ως ποσοστό του σχετικού πληθυσμού, ο όγκος των δεδομένων ή / και το εύρος των διαφόρων στοιχείων δεδομένων, η διάρκεια ή η μονιμότητα της δραστηριότητας επεξεργασίας και η γεωγραφική έκταση της δραστηριότητας επεξεργασίας.

Αντίθετα, αδιάφορο είναι το μέγεθος της επιχείρησης που συλλέγει και επεξεργάζεται τα δεδομένα, όπως και η φύση τους (π.χ. ευαίσθητα). Έτσι, ο αριθμός των υποκειμένων τα οποία επηρεάζονται από την επεξεργασία καθώς και το γεωγραφικό εύρος αυτής συμβάλουν στην οριοθέτηση της έννοιας της «μεγάλης κλίμακας». Στο πλαίσιο αυτό, η συλλογή δεδομένων από σύνδεσμο επιχειρήσεων ο οποίος στο πλαίσιο της κύριας δραστηριότητάς του συλλέγει προσωπικά δεδομένα με εδαφικό εύρος που καλύπτει το μεγαλύτερο τμήμα της περιφέρειας Αττικής, θεωρείται μεγάλης κλίμακας καθώς στο σύνολο των δεδομένων της Αττικής, τα δεδομένα αυτά καταλαμβάνουν αρκετά μεγάλο ποσοστό.

γ) Οι βασικές δραστηριότητες του υπευθύνου συνιστούν μεγάλης κλίμακας επεξεργασία ευαίσθητων προσωπικών δεδομένων ή δεδομένων σχετικών με ποινικές καταδίκες και αδικήματα.

δ) Προβλέπεται από το δίκαιο κράτους-μέλους.

Εφόσον ένας οργανισμός ή μια επιχείρηση δεν εμπίπτει στις ανωτέρω περιπτώσεις, παρότι δεν υποχρεούται στον ορισμό ΥΠΔ, μπορεί να επιλέξει να το πράξει εθελοντικά, κάτι το οποίο ωστόσο δε συνεπάγεται μειωμένη ευθύνη απέναντι στις υποχρεώσεις που επιβάλλονται από τον Κανονισμό.

Πρέπει να αναφερθεί ότι η ομάδα του άρθρου 29 προβλέπει ότι σε περίπτωση αμφιβολίας σχετικά με τον ορισμό του, είναι καλύτερο να οριστεί και χαρακτηριστικά προτείνει τη σύνταξη έγγραφης ανάπτυξης του σκεπτικού βάσει του οποίου δεν ορίστηκε.

Ως προς τον ορισμό ΥΠΔ σε όμιλο επιχειρήσεων, ο Κανονισμός δίνει τη δυνατότητα να οριστεί μόνο ένας, ακόμα και σε ομίλους επιχειρήσεων με διασυνοριακή δραστηριότητα, ωστόσο για λόγους αμεσότητας και διευκόλυνσης της επικοινωνίας του με την εκάστοτε αρμόδια τοπική Αρχή αλλά και με τα υποκείμενα των δεδομένων χρήσιμος κρίνεται ο ορισμός και ενός τοπικά αρμόδιου ΥΠΔ.

Η έκταση της ευθύνης του ΥΠΔ περιορίζεται σε λόγους που ανάγονται στην πλημμελή εκτέλεση των υποχρεώσεών του έναντι του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία, επομένως για τις ενέργειες του δε φέρει ευθύνη έναντι του υποκειμένου των δεδομένων ή της Αρχής.

Έχει αναπτυχθεί ιδιαίτερα το ζήτημα πρακτικής εφαρμογής του καθεστώτος ανεξαρτησίας που σύμφωνα με τον κανονισμό πρέπει να απολαμβάνει ο Υπεύθυνος Προστασίας και της δυνατότητας ρεαλιστικής υλοποίησης της απαίτησης αυτής, ειδικά

στην περίπτωση που τη θέση αναλάβει ο διευθυντής της νομικής υπηρεσίας ή της υπηρεσίας πληροφοριακών συστημάτων του οργανισμού.

Σχετικά με το συγκεκριμένο θέμα, το Γερμανικό Δικαστήριο έκρινε ότι στην περίπτωση του υπεύθυνου της υπηρεσίας πληροφοριακών συστημάτων, πράγματι συντρέχουν οι προϋποθέσεις σύγκρουσης συμφερόντων και επομένως δεν αποτελεί ορθή πρακτική η ταυτόχρονη ανάληψη καθηκόντων επικεφαλής IT και ΥΠΔ στον ίδιο οργανισμό[39].

Ως προς την τοποθέτηση ως ΥΠΔ του δικηγόρου-επικεφαλής του νομικού τμήματος, έχει υποστηριχθεί τόσο η άποψη υπέρ μιας τέτοιας ενέργειας,, όσο και η άποψη σύμφωνα με την οποία ιδανικό προφίλ για τη θέση δεν έχει ο δικηγόρος, αλλά ο Υπεύθυνος Κανονιστικής Συμμόρφωσης λόγω μεγαλύτερης εμπειρίας και εξοικείωσής του σε τεχνικά θέματα και οργανωτικά θέματα του οργανισμού.

2.1.6 Η προστασία των δεδομένων ήδη από το σχεδιασμό και εξ ορισμού (Privacy by design και by default)

Όπως ήδη αναφέρθηκε, η εξέλιξη της τεχνολογίας στα χρόνια που ακολούθησαν τη θέσπιση της Οδηγίας 95/46/ΕΚ ήταν αλματώδης. Τα φυσικά πρόσωπα απέκτησαν γρήγορη, εύκολη και οικονομική πρόσβαση σε ηλεκτρονικές συσκευές όπως PC, laptop, tablet, smartphones κ.ά., μέσω των οποίων καθημερινά επέτρεπαν την επεξεργασία, ανταλλαγή και μεταφορά των προσωπικών δεδομένων τους από εφαρμογές, συστήματα και ιστοσελίδες. Η διαδικασία παροχής της συγκατάθεσής τους ωστόσο ήταν άτυπη καθώς γινόταν χωρίς καμία ρητή επισήμανση από την πλευρά των υπεύθυνων επεξεργασίας των δεδομένων και, πολύ συχνά, δεν γινόταν καν αντιληπτή ως τέτοια. Πολύ λιγότερο αντιληπτός γινόταν ο αντίκτυπος που το «χαλαρό» αυτό καθεστώς παροχής συγκατάθεσης είχε στην ιδιωτικότητά τους.

[39] Δείτε σχετικό άρθρο εδώ.

Με τη διάδοση των κοινωνικών δικτύων, ο όγκος και η ποικιλία των προσωπικών δεδομένων που εκτίθενται καθημερινά σε μια ευρεία σφαίρα αποδεκτών και καταλήγουν να είναι διαθέσιμα προς αξιοποίηση και εκμετάλλευση αυξάνεται με εκθετικό βαθμό. Δυστυχώς, η φιλοσοφία σχεδιασμού πολλών διαδικτυακών και μη εφαρμογών ήταν και, σε κάποιες περιπτώσεις παραμένει, τέτοια που να προάγει τη διάδοση και ελεύθερη κυκλοφορία της πληροφορίας χωρίς να ζητά ρητά και με εύληπτο τρόπο τη συγκατάθεση του χρήστη. Μπορεί κανείς να βρει πληθώρα παραδειγμάτων στα οποία ενθαρρύνεται ο διαμοιρασμός των δεδομένων και σε άλλους χρήστες της ίδιας εφαρμογής. Συχνά μάλιστα, ο τρόπος και η απλότητα με την οποία πολλές ιστοσελίδες προωθούν την διάδοση των δεδομένων επέτρεψε και επιτρέπει την απερίσκεπτη έκθεση δεδομένων υποκειμένων τα οποία όχι μόνο δεν συγκατέθεσαν ποτέ σε κάτι τέτοιο, αλλά μάλιστα ουδέποτε υπήρξαν χρήστες τους. Στις περιπτώσεις αυτές, η αρχιτεκτονική των εφαρμογών δεν περιλαμβάνει καμία διασφάλιση της ενημέρωσης του χρήστη σχετικά με τους κανόνες προστασίας της ιδιωτικότητας, συμβάλλοντας εν μέρει στη γενικότερη άγνοια που παρατηρείται σε επίπεδο υποκειμένων των δεδομένων.

Έτσι, η τεχνολογία διαμορφώθηκε σε ένα «αυτοαναιρούμενο αγαθό κοινωνικοποίησης» καθώς ενίσχυσε «σε μεγάλο βαθμό την ανάγκη για διαχωρισμό της παρουσίας μας από τους υπόλοιπους χρήστες της και την ελαχιστοποίηση της φυσικής μας αλληλεπίδρασης με τους φίλους/γνωστούς/συνεργάτες/συντρόφους»[40].

Παράλληλα, υπερέκθεση των δεδομένων οδήγησε και σε φαινόμενα παραβιάσεων με επακόλουθο να αναπτυχθεί η προβληματική ως προς τους τρόπους ενσωμάτωσης στην τεχνολογία, πρακτικών προστασίας των προσωπικών δεδομένων και ειδικότερα η ανάγκη για εφεύρεση μεθόδων που θα διευκόλυναν τη σύννομη επεξεργασία χωρίς να απαιτείται τα υποκείμενα των δεδομένων να προβαίνουν σε πρόσθετες ενέργειες.

Η αρχή αυτή ονομάζεται privacy by default, και συνίσταται στην διασφάλιση της ιδιωτικότητας ως βασική και κατά κανόνα ενσωματωμένη επιλογή ενός συστήματος, μιας εφαρμογής ή μιας επεξεργασίας. Στόχος είναι η προστασία του, μέχρι τώρα αποδεδειγμένα ελάχιστα έως καθόλου ενημερωμένου χρήστη σχετικά με τους κινδύνους κοινοποίησης των δεδομένων του. Η έννοια του privacy by default έχει ιδιαίτερη βαρύτητα, αν αναλογιστεί κανείς ότι η μέχρι τώρα πολιτική προστασίας της ιδιωτικότητας που παρείχαν ορισμένες εφαρμογές εξαντλούνταν στην παροχή

[40] Τάσσης Σπ., βλ. απόσπασμα στο Συλλογικό Τόμο «Προσωπικά Δεδομένα», εκδ. Νομική Βιβλιοθήκη 2016

δυνατότητας στο χρήστη να προβεί με δικές του ενέργειες στην διαφοροποίηση των ρυθμίσεων που επέτρεπαν τη χρήση και επεξεργασία των δεδομένων του. Και συχνά, η σχετική διαδικασία κατέληγε τόσο περίπλοκη και οι σχετικές διατυπώσεις τόσο ασαφείς που οι χρήστες εγκατέλειπαν την προσπάθεια.

Η νέα αυτή παράμετρος φαίνεται να μπορεί να εξασφαλίσει σε ικανοποιητικό βαθμό την επαρκή ενημέρωση και συνειδητοποίηση των υποκειμένων ως προς τις συνέπειες που η έκθεση των δεδομένων τους μπορεί να συνεπάγεται. Η πρακτική της εφαρμογή όμως θα καταδείξει την απώλεια σημαντικής πληροφορίας από τους υπεύθυνους επεξεργασίας για τους οποίους τα δεδομένα αυτά ήταν πολύτιμα όχι μόνο για την διαμόρφωση των επιχειρηματικών πολιτικών τους και την εύρεση ελκυστικών τρόπων επικοινωνίας τους αλλά, σε κάποιο βαθμό, στην βελτίωση των υπηρεσιών και προϊόντων τους προς την πελατεία τους.

Η προστασία της ιδιωτικότητας διά του σχεδιασμού (protection by design) μπαίνει βαθύτερα στο ζήτημα και ουσιαστικά προηγείται του σταδίου privacy by default αφού απαιτεί τη λήψη συγκεκριμένων μέτρων κατά το σχεδιασμό ενός συστήματος ως προς α) τον όγκο και την ποιότητα των δεδομένων των οποίων η επεξεργασία είναι αναγκαία, β) την αξιολόγηση των κινδύνων από την επεξεργασία και των επιπτώσεών τους στην ιδιωτικότητα (στο σημείο αυτό παρατηρούμε ότι, με βάση τα όσα αναφέρθηκαν πιο πάνω, η εκπόνηση έκθεσης εκτίμησης αντικτύπου αποτελεί μέτρο που εντάσσεται στη διαδικασία του σχεδιασμού privacy by design) και γ) την υιοθέτηση της αρχής της εξ' ορισμού προστασίας.

Απαιτείται επομένως να ληφθούν τα κατάλληλα εκείνα οργανωτικά και τεχνικά μέτρα ήδη από το σχεδιασμό κατά τη στιγμή του καθορισμού των μέσων επεξεργασίας όσο και κατά τη στιγμή της επεξεργασίας. Η εκπλήρωση των υποχρεώσεων αυτών συνιστά χρήσιμο εργαλείο για τη σύννομη συμμόρφωση των επιχειρήσεων καθώς ο σχεδιασμός διαδικασιών, συστημάτων και προϊόντων εξαρχής με τη φιλοσοφία της προστασίας των προσωπικών δεδομένων μπορεί να οδηγήσει στην αποτελεσματική διάγνωση και αντιμετώπιση προβλημάτων σε αρχικό επίπεδο και συνεπώς, να μειώσει την πιθανότητα επέλευσης κινδύνων από την επεξεργασία.

Ο Κανονισμός ωστόσο, δεν υπεισέρχεται στον προσδιορισμό των τεχνικών προδιαγραφών που θα πρέπει να πληρούνται προκειμένου να θεωρηθεί σύννομη μια πολιτική προστασίας by default και by design. Αντίθετα, κάνει ενδεικτική αναφορά σε μέτρα όπως η ψευδωνυμοποίηση των δεδομένων ώστε ο υπεύθυνος επεξεργασίας να

είναι σε θέση να βελτιώνει τα χαρακτηριστικά ασφάλειας. Σε κάθε περίπτωση όμως, όπως αναφέρεται και στην αιτιολογική σκέψη 28 του Κανονισμού, «η χρήση της ψευδωνυμοποίησης στα δεδομένα προσωπικού χαρακτήρα μπορεί να μειώσει τους κινδύνους για τα υποκείμενα των δεδομένων και να διευκολύνει τους υπευθύνους επεξεργασίας και τους εκτελούντες την επεξεργασία να τηρήσουν τις οικείες υποχρεώσεις περί προστασίας των δεδομένων. Η ρητή εισαγωγή της «ψευδωνυμοποίησης» του παρόντος κανονισμού δεν προορίζεται να αποκλείσει κάθε άλλο μέτρο προστασίας των δεδομένων».

Η Ομάδα του άρθρου 29, δίνει ένα παράδειγμα privacy by design: Όταν ένας εργοδότης χορηγεί συσκευές με τεχνολογίες εντοπισμού στους εργαζόμενους θα πρέπει να γίνει η επιλογή της πιο συμβατής με την αρχή privacy by design λύσης ενώ θα πρέπει να ληφθεί υπόψη και η αρχή της ελαχιστοποίησης των δεδομένων[41].

Συνεπώς, η λήψη και τήρηση μέτρων προστασίας από το σχεδιασμό αποτελεί ένδειξη συμμόρφωσης, δεν εγγυάται όμως τη συμμόρφωση. Παραμένει στην αρμοδιότητα της Επιτροπής, των αρμόδιων εθνικών Αρχών Προστασίας καθώς και του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων να εκδώσουν σχετικές αναλυτικές κατευθυντήριες οδηγίες που θα εξειδικεύσουν και θα περιγράψουν τα κατάλληλα τεχνικά μέτρα.

2.1.7 Το δικαίωμα στη λήθη

Στο άρθρο 17 ο Κανονισμός αναφέρεται στο δικαίωμα διαγραφής ή αλλιώς «δικαίωμα στη λήθη», όρος ο οποίος τείνει να επικρατήσει ως πιο δημοφιλής. Σύμφωνα με το άρθρο, το υποκείμενο των δεδομένων δικαιούται να ζητήσει από τον υπεύθυνο επεξεργασίας τη διαγραφή δεδομένων προσωπικού χαρακτήρα που το αφορούν και ο υπεύθυνος επεξεργασίας υποχρεούται να διαγράψει τα δεδομένα αυτά, εφόσον συντρέχουν συγκεκριμένες προϋποθέσεις.

Το υποκείμενο των δεδομένων ενισχύεται περαιτέρω κατά την άσκηση του δικαιώματος αυτού καθώς, σύμφωνα με τη σκέψη 66, ο υπεύθυνος επεξεργασίας ο οποίος δημοσιοποίησε τα δεδομένα προσωπικού χαρακτήρα οφείλει να ενημερώνει τους υπευθύνους επεξεργασίας που επεξεργάζονται τα εν λόγω δεδομένα προσωπικού χαρακτήρα ώστε να διαγράψουν οποιουσδήποτε συνδέσμους ή αντίγραφα ή αναπαραγωγή των δεδομένων, λαμβάνοντας τα μέτρα εκείνα που είναι «εύλογα» ώστε

[41] Βλέπε Γνώμη 8/2012

να ενημερωθούν και έχοντας υπόψη του τη διαθέσιμη τεχνολογία και τα μέσα που έχει στη διάθεσή του.

Το δικαίωμα αυτό μπορεί να ασκήσει σύμφωνα με τη σκέψη 65 του Κανονισμού το ενήλικο φυσικό πρόσωπο το οποίο παρείχε τη συγκατάθεσή του για χρήση των δεδομένων στο παρελθόν, όταν ήταν παιδί και κατά το χρόνο εκείνο όπως είναι φυσικό, στερούνταν την κρίσιμη γνώση σχετικά με τους κινδύνους που απορρέουν από την επεξεργασία.

Το υποκείμενο των δεδομένων μπορεί επομένως να ζητήσει, για μια σειρά προσωπικών και ευαίσθητων πληροφοριών που το αφορούν, τη διαγραφή τους από το διαδίκτυο ώστε να μην είναι δυνατή η δημόσια εμφάνισή τους στα αποτελέσματα των ψηφιακών αναζητήσεων.

Το δικαίωμα αυτό δεν είναι απολύτως νέο ούτε στο ενωσιακό ούτε στο εθνικό μας δίκαιο καθώς αν και δεν αναφέρεται ρητά ως τέτοιο, εντούτοις καλύπτεται από ευρύτερες έννοιες όπως η προστασία της ελεύθερης ανάπτυξης της προσωπικότητας, η κατοχύρωση της αξίας του ανθρώπου, το δικαίωμα προστασίας της ιδιωτικής ζωής, της προστασίας των προσωπικών δεδομένων και του πληροφοριακού αυτοκαθορισμού του ατόμου[42], αλλά απαντάται και σε πιο ευθείες αναφορές, όπως η διαγραφή των δεδομένων που δεν είναι αναγκαία για την εκπλήρωση ενός σκοπού επεξεργασίας[43] και η διαγραφή των πράξεων επιβολής ποινικών κυρώσεων μετά από συγκεκριμένο χρόνο[44].

Στην πράξη, παρότι το δικαίωμα στη διαγραφή δεν είχε αναφερθεί αυτολεξεί στα νομικά κείμενα, η Ελληνική Αρχή Προστασίας Προσωπικών Δεδομένων ήδη από το 1999 διατύπωσε ως έκφραση της αρχής της αναλογικότητας την ανάγκη περιορισμού του χρόνου διατήρησης των δυσμενών οικονομικών δεδομένων από την Τειρεσίας Α.Ε ανάλογα με την κατηγορία τους[45]. Ένα χρόνο μετά, το 2010 έκρινε ότι εφημερίδα που δημοσιοποίησε και ανήρτησε στο διαδικτυακό της τόπο ευαίσθητα δεδομένα φυσικού προσώπου, παραβίασε τον ισχύοντα νόμο περί προστασίας προσωπικών δεδομένων. Κατά συνέπεια, προέβη στην επιβολή προστίμου και απηύθυνε σύσταση στον υπεύθυνο επεξεργασίας για εξέταση του δικαιώματος αντίρρησης των υποκειμένων των δεδομένων, ενώ απαγόρευσε την αναδημοσίευση και διέταξε την ανωνυμοποίηση

42 Άρθρο 8 της ΕΣΔΑ και άρθρα 5 παρ.1, 2 παρ. 1, 9 και 9Α του Συντάγματος.
43 Άρθρο 4 παρ. 1 και 2 ν.2472/1997 περί προστασίας δεδομένων προσωπικού χαρακτήρα.
44 Άρθρο 576 Κώδικα Ποινικής Δικονομίας.
45 Απόφαση αρ. 523/1999

των στοιχείων του υποκειμένου στο δημοσίευμα[46]. Την ίδια χρονιά εισηγήθηκε τον χρονικό περιορισμό της ανάρτησης στο διαδίκτυο δυσμενών διοικητικών πράξεων από τη Δημόσια διοίκηση σε βάρος στελεχών της[47].

Πρέπει να σημειωθεί ότι η άσκηση του δικαιώματος στη λήθη αποκλείεται όταν η επεξεργασία είναι απαραίτητη: α) για λόγους που ανάγονται στην ελευθερία της έκφρασης και στο δικαίωμα στην ενημέρωση, β) εφόσον η επεξεργασία επιβάλλεται βάσει του ενωσιακού ή του εθνικού δικαίου του κράτους μέλους στο οποίο υπάγεται ο υπεύθυνος επεξεργασίας ή για λόγους εκπλήρωσης καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο της επεξεργασίας, γ) για λόγους δημόσιου συμφέροντος στον τομέα της δημόσιας υγείας, δ) για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς, εφόσον το δικαίωμα είναι πιθανόν να καταστήσει αδύνατη ή να εμποδίσει σε μεγάλο βαθμό την επίτευξη σκοπών της επεξεργασίας, ή ε) για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων.

Μια από τις σημαντικότερες αποφάσεις του Ευρωπαϊκού Δικαστηρίου ως προς την έκταση της εφαρμογής του δικαιώματος στη λήθη αποτελεί η πρόσφατη υπόθεση Google Spain[48]. Σύμφωνα με το ΔΕΕ, τα θεμελιώδη δικαιώματα του σεβασμού της ιδιωτικής και οικογενειακής ζωής και της προστασίας των δεδομένων προσωπικού χαρακτήρα των άρθρων 7 και 8 του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης καταρχήν υπερέχουν όχι μόνο του οικονομικού συμφέροντος του φορέα εκμετάλλευσης της μηχανής αναζήτησης, αλλά και του συμφέροντος του κοινού να αποκτήσει πρόσβαση στην πληροφορία αυτή στο πλαίσιο αναζήτησης με βάση το ονοματεπώνυμο του εν λόγω υποκειμένου. Παρόλα αυτά, για ειδικούς λόγους, όπως είναι ο ρόλος που διαδραματίζει το υποκείμενο στον δημόσιο βίο, η επέμβαση στα θεμελιώδη δικαιώματά του δικαιολογείται από το υπέρτερο συμφέρον του κοινού για πρόσβαση στην πληροφορία. Μια απόφαση «σταθμός» καθώς «σηματοδότησε τη μετακίνηση από το θεμελιώδες δικαίωμα στην ελευθερία προς ένα περισσότερο αυστηρό περιβάλλον προστασίας δικαιωμάτων, όπως τα προσωπικά δεδομένα και η ιδιωτικότητα»[49].

---

46 Απόφαση 8/2010
47 Γνωμοδότηση αρ. 1/2010
48 Δείτε το κείμενο της απόφασης εδώ.
49 Spiros Tassis and Margarita Peristeraki, The Extraterritorial Scope of the "Right to Be Forgotten" and the Rights and Obligations of Search Engine Operators Located Outside the EU, European Networks Law and Regulation 3/2014, Lexxion Verlagsgesellschaft mbH.

Επί του θέματος, η νομολογία φαίνεται να αποδέχεται ευρύτερα την ανάγκη εξισορρόπησης μεταξύ των δικαιωμάτων, εντοπίζοντας και προσδιορίζοντας την έκταση του δικαιώματος στη λήθη βάσει των τεχνικά εφικτών μεθόδων της αφαίρεσης από τη λίστα αναζήτησης «delisting» ή μεμονωμένης αφαίρεσης από τα τηρούμενα αρχεία «de- indexing» στις μηχανές αναζήτησης.

Ο φόβος που έχει εκφραστεί ευρύτερα από τους παρόχους υπηρεσιών διαδικτυακής αναζήτησης, εκπροσώπους του δημοσιογραφικού χώρου αλλά και της Επιτροπής που υπερασπίζεται το δικαίωμα στην ελευθερία του λόγου[50] είναι ότι τελικά το διαδίκτυο θα καταλήξει να μοιάζει με ένα «ελβετικό τυρί με τρύπες»[51] και μένει να φανεί στην πράξη εάν οι φόβοι αυτοί θα επαληθευτούν.

2.1.8 Η διαχείριση του κινδύνου

Ο Κανονισμός όπως ήδη ειπώθηκε, συνιστά μια ακόμη νομοθετική εξέλιξη που υιοθετήθηκε όχι να προλάβει αλλά για να θεραπεύσει και να περιστείλει μια ήδη

διαπιστωθείσα κατάσταση, αυτήν της εξάπλωσης των φαινομένων παραβίασης των προσωπικών δεδομένων.

Στον Κανονισμό, η έννοια του κινδύνου αποκτά μια διαφορετική και πιο ουσιαστική και προσδιορισμένη θέση και λειτουργία από εκείνη που δίνεται στην Οδηγία 95/46/ΕΚ. Και αυτό γιατί η Οδηγία στο άρθρο 17 «Ασφάλεια της επεξεργασίας» αναθέτει με γενικό τρόπο στα κράτη μέλη τη θέσπιση μέτρων που οφείλει να αναλάβει ο υπεύθυνος της επεξεργασίας «για την προστασία από τυχαία ή παράνομη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση» αναφέροντας ότι «τα μέτρα αυτά πρέπει να εξασφαλίζουν, λαμβανομένης υπόψη της τεχνολογικής εξέλιξης και του κόστους εφαρμογής τους, επίπεδο ασφαλείας ανάλογο προς τους κινδύνους που απορρέουν από την επεξεργασία και τη φύση των δεδομένων που απολαύουν προστασίας».

Αντίθετα, διαβάζοντας το κείμενο του Κανονισμού, γίνεται αντιληπτό ότι πλέον απαιτείται η «αξιολόγηση βάσει αντικειμενικής εκτίμησης» καθώς και η τήρηση συγκεκριμένων υποχρεώσεων ανάλογα με την κατηγοριοποίηση σε περιπτώσεις

[50] Επιτροπή άρθρου 19 της Διεθνούς Διακήρυξης για τα δικαιώματα του Ανθρώπου.
[51] Julia Powels, Right to be forgotten: Swiss cheese internet, or database of ruin? Βρείτε το σχετικό άρθρο εδώ.

«υψηλού» κινδύνου και άλλες. Ο κίνδυνος συνιστά το βασικό άξονα γύρω από τον οποίο και στη βάση του οποίου αναπτύσσονται οι δράσεις και πολιτικές συμμόρφωσης,

Αυτή την προσέγγιση του Κανονισμού παρατηρούμε σε όλα τα άρθρα στα οποία γίνεται αναφορά στον «κίνδυνο».

Συγκεκριμένα, στο άρθρο 24 «ευθύνη του υπεύθυνου επεξεργασίας» παρατηρούμε ότι ο κίνδυνος διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, αποτελεί σημαντική παράμετρο της έκτασης της ευθύνης του υπευθύνου επεξεργασίας σε συνδυασμό με «τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας».

Στο άρθρο 25 «Προστασία των δεδομένων ήδη από το σχεδιασμό και εξ ορισμού» απαντάμε ξανά την έννοια του κινδύνου στις ευθύνες που αποδίδονται στον Υπεύθυνο επεξεργασίας και στις επιμέρους απαιτήσεις όσον αφορά στην προστασία δεδομένων από το σχεδιασμό και εξ᾽ ορισμού.

Περαιτέρω, στο άρθρο 30 «αρχεία των δραστηριοτήτων της επεξεργασίας» ο κίνδυνος συνδέεται με την υποχρέωση τήρησης αρχείων. Στο συγκεκριμένο άρθρο αναγράφονται ρητά οι πληροφορίες που πρέπει να περιλαμβάνονται στο αρχείο των δραστηριοτήτων επεξεργασίας για τις οποίες είναι υπεύθυνος ο υπεύθυνος επεξεργασίας και το οποίο πρέπει να τηρεί σε κάθε περίπτωση επιχείρησης ή οργανισμού που απασχολεί πάνω από 250 άτομα ή, σε κάθε περίπτωση που «η διενεργούμενη επεξεργασία ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων».

Στο άρθρο 32 «ασφάλεια επεξεργασίας», ο κίνδυνος είναι το στοιχείο εκείνο που πρέπει να ληφθεί υπόψη κατά την ανάληψη ενδεικτικών τεχνικών και οργανωτικών μέτρων που οφείλουν να εφαρμόσουν ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία για τη διασφάλιση του κατάλληλου επιπέδου ασφαλείας («προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων»), ενώ στο ίδιο άρθρο, συνίσταται η συνεκτίμηση των κινδύνων που απορρέουν από την επεξεργασία «κατά την εκτίμηση του ενδεδειγμένου επιπέδου ασφάλειας».

Στο άρθρο 33, «γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα στην εποπτική αρχή» είναι πάλι ο κίνδυνος που οδηγεί στη γνωστοποίηση παραβίασης ΔΠΧ στην εποπτική αρχή αφού η υποχρέωση γνωστοποίησης δε συντρέχει, μόνο στην

περίπτωση που «η παραβίαση δεδομένων προσωπικού χαρακτήρα δεν ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων.» Τέλος, στα άρθρα 34, 35 και 36, συναντούμε τη σύνδεση του χαρακτηρισμού της επεξεργασίας «υψηλού κινδύνου» με τις νέες υποχρεώσεις «ανακοίνωσης παραβίασης δεδομένων», «εκτίμησης αντικτύπου» και «διαβούλευσης με τις εποπτικές αρχές» κατά τη διαδικασία διενέργειας της εκτίμησης αντικτύπου αντίστοιχα και φυσικά, ο κίνδυνος συνιστά βασική παράμετρο των καθηκόντων του Υπεύθυνου Προστασίας στο άρθρο 39 παρ. 2.

Όμως ο Κανονισμός είναι τεχνολογικά «ουδέτερος». Σε κανένα σημείο του δεν προσδιορίζονται συγκεκριμένες τεχνολογικές προδιαγραφές, μεθοδολογίες και πρότυπα ως απαιτήσεις συμμόρφωσης. Αντίθετα, απαιτείται διαρκής ανάλυση του κινδύνου στον οποίο υπόκεινται τα προσωπικά δεδομένα βάσει των μεταβαλλόμενων διαδικασιών επεξεργασίας που τηρεί ο υπεύθυνος επεξεργασίας και σε σχεδιασμό των κατάλληλων μέτρων που θα βοηθήσουν στον περιορισμό του σε σταθερή βάση.

Το μοναδικό ίσως «εργαλείο» που υποδεικνύει ξεκάθαρα ο Κανονισμός χωρίς και πάλι να περιορίζει τους υπόχρεους συμμόρφωσης σε πρότυπα και μεθόδους εφαρμογής του, είναι η εκπόνηση έκθεσης εκτίμησης αντικτύπου, η οποία μπορεί να βοηθήσει στην αναγνώριση και την ανάλυση του κινδύνου, την αποτίμηση των πιθανών επιπτώσεών του και τελικά την αξιολόγησή του ώστε να μπορεί ο υπεύθυνος επεξεργασίας να καταλήξει στην επιλογή των απαιτούμενων μέτρων για τη διαχείρισή του.

2.2 Το Σχέδιο Νόμου για την μεταφορά του Κανονισμού στην εθνική νομοθεσία

Όπως ήδη τονίστηκε και κατά το σχολιασμό των κυριότερων άρθρων του Κανονισμού, η μελέτη εκπονήθηκε κατά το χρόνο στον οποίο η επεξεργασία του Σχεδίου Νόμου δεν είχε ολοκληρωθεί, παρά την πάροδο ικανού χρόνου από τη λήξη της δημόσιας διαβούλευσης. Κατά συνέπεια, ο σχολιασμός που ακολουθεί βασίζεται στο κείμενο του Σχεδίου Νόμου, όπως αυτό παρουσιάστηκε στη δημόσια διαβούλευση αλλά ενδέχεται να τροποποιηθεί έως την οριστική ψήφισή του και τη δημοσίευσή του στην Εφημερίδα της Κυβέρνησης.

Παρόλο που ενδεχομένως η ενότητα αυτή χρήζει αλλαγών ακόμη ίσως και πριν τη δημοσιοποίησή της, η συντακτική ομάδα έκρινε αναγκαίο και επέλεξε να συμπεριλάβει

το μέρος αυτό για λόγους ουσιαστικής πληρότητας της μελέτης. Ο τρόπος με τον οποίο ο εθνικός νομοθέτης θα επιλέξει να ασκήσει τα περιθώρια ευελιξίας που του παρέχει ο ευρωπαίος νομοθέτης και κυρίως ο τρόπος με τον οποίο θα επιλέξει να ευθυγραμμίσει τον Κανονισμό με άλλες συνδεόμενες εθνικές νομοθεσίες (πχ εργασιακή νομοθεσία) είναι κομβικός για την αποτελεσματικότητα, την αποδοχή και τελικά τη νομική βεβαιότητα όσων θα κληθούν αν τον εφαρμόσουν.

2.2.1 Γενικά σχόλια

Ο Κανονισμός απαιτεί τη γενικότερη αναβάθμιση των λειτουργικών δομών των επιχειρήσεων και των οργανισμών και τον εκσυγχρονισμό των πολιτικών τήρησης και διαχείρισης των δεδομένων με απώτερο στόχο την ενίσχυση των δεσμών εμπιστοσύνης στις συναλλαγές με τον ιδιωτικό και το δημόσιο τομέα οι οποίοι από τις 25 Μαΐου 2018 θεωρητικά θα πρέπει να είναι σε θέση να επιδείξουν τη δέουσα επιμέλεια, σοβαρότητα και υπευθυνότητα καθώς και να αποδείξουν την ετοιμότητά τους για άμεση ανταπόκριση σε κάθε απαίτηση του νέου πλαισίου.

Κατά συνέπεια, το άνοιγμα της διαβούλευσης του Σχεδίου Νόμου για τη θέσπιση νομοθετικών μέτρων για την εφαρμογή του Κανονισμού στις 20 Φεβρουαρίου 2018 από το αρμόδιο Υπουργείο Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων αποτέλεσε θετική εξέλιξη καθώς στοχεύει στην ομαλή μετάβαση στην εθνική έννομη τάξη, των υποχρεώσεων που απορρέουν από τον Κανονισμό προκειμένου να δημιουργηθεί κοινή αντίληψη όλων των φορέων του ιδιωτικού και του δημόσιου τομέα αλλά και των ίδιων των πολιτών περί της σημασίας διασφάλισης της προστασίας των προσωπικών δεδομένων. Παράλληλα, συμβάλει στην εδραίωση της ασφάλειας των συναλλαγών, καθώς και στην καλύτερη κατανόηση του τρόπου συμμόρφωσης όλων των υπόχρεων με τις απαιτήσεις του Κανονισμού στο πλαίσιο της ελληνικής έννομης τάξης.

Ωστόσο, η μεγάλη καθυστέρηση στη διαμόρφωση και οριστικοποίηση του σχεδίου, η οποία παραμένει μέχρι και σήμερα (δεν υπάρχει εικόνα σχετικά με την τελική μορφή που αυτό θα λάβει, ούτε κάποια πληροφορία αναφορικά με το χρόνο πιθανολογούμενης ψήφισής του) αποτελεί πρόβλημα. Το γεγονός αυτό έχει επιτείνει την αβεβαιότητα των επιχειρήσεων και του Δημόσιου τομέα για το μέγεθος των προσαρμογών στις οποίες πρέπει να προβούν και ειδικά ως προς τις διαφοροποιήσεις που ενδέχεται να περιέχει το νέο εθνικό πλαίσιο συμμόρφωσης σε σχέση με τις

υποχρεώσεις των Υπευθύνων επεξεργασίας, των Υπεύθυνων Προστασίας και των Εκτελούντων την επεξεργασία.

Με το Σχέδιο Νόμου να παραμένει αδημοσίευτο είναι σχεδόν βέβαιο ότι θα υπάρξουν αστοχίες κατά την εκτίμηση ως προς τον ανασχεδιασμό των εσωτερικών διαδικασιών και πρωτοκόλλων, χωρίς καμία ευθύνη από την πλευρά της αγοράς, αλλά και των κρατικών υπηρεσιών.

Επιπρόσθετα, η καθυστέρηση αυτή είναι πολύ πιθανό να επισύρει για τη χώρα τις σχετικές προβλεπόμενες κυρώσεις όπως χαρακτηριστικά τονίζεται και στη σχετική ανακοίνωση της Ευρωπαϊκής Επιτροπής: «Σε περίπτωση που κράτος μέλος δεν λάβει τα αναγκαία μέτρα που απαιτούνται βάσει του κανονισμού, καθυστερήσει να λάβει μέτρα ή χρησιμοποιήσει τις δυνατότητες θέσπισης πιο ειδικών διατάξεων που προβλέπονται στον κανονισμό κατά τρόπο αντίθετο προς τον κανονισμό, η Επιτροπή θα χρησιμοποιήσει όλα τα μέσα που έχει στη διάθεσή της, συμπεριλαμβανομένης της κίνησης διαδικασίας επί παραβάσει»[52].

Ο ΣΕΒ κατά το στάδιο της δημόσιας διαβούλευσης του σχεδίου προέβη στη διατύπωση γενικών και ειδικών παρατηρήσεων στο σχέδιο προκειμένου να συνδράμει στη βέλτιστη δυνατή ευθυγράμμισή του με το πνεύμα του ενωσιακού νομοθέτη, χωρίς την προσθήκη αδικαιολόγητων περιορισμών για τις επιχειρήσεις. Για τον ΣΕΒ, η αποτελεσματική λειτουργία των διατάξεων και η διασφάλιση της συμμόρφωσης των υπόχρεων με αυτές, μπορεί να γίνει με τις εξής κρίσιμες αλλαγές στο Σχέδιο Νόμου:

1) τη **θέσπιση ευέλικτων κανόνων** που δεν εισάγουν περιττά και δυσανάλογα διοικητικά βάρη για τις επιχειρήσεις,
2) την **επαρκή προστασία των δικαιωμάτων των υποκειμένων**,
3) τη **διασφάλιση της απαιτούμενης** από τον Κανονισμό, **δυνατότητας για ενιαία ερμηνεία και συνεκτική εφαρμογή των κανόνων** του προκειμένου να διευκολυνθεί ο προβλεπόμενος διάλογος μεταξύ των εποπτικών αρχών και
4) την **ενιαία υιοθέτηση μιας συνολικής ψηφιακής στρατηγικής του Δημοσίου.**

[52] COM(2018) 43 final, 24.1.2018

Περαιτέρω, αναγκαία κρίνεται η ανάληψη ειδικής μέριμνας για την ενίσχυση της Ανεξάρτητης Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα σε στελεχιακό δυναμικό της οποίας η πρόσφατη αποδυνάμωση εγείρει ανησυχίες ως προς την αποτελεσματικότητα με την οποία θα ασκήσει το δύσκολο έργο που της έχει ανατεθεί.

Τέλος, επείγουσας προτεραιότητας παρέμβαση θεωρείται για τον ΣΕΒ **η νομοθετική κατοχύρωση της δυνατότητας ιεράρχησης των καταγγελιών** για λόγους αποφυγής φαινομένων υπερφόρτωσης των ελεγκτών με κακόβουλες καταγγελίες που είναι πιθανό να παρεμποδίσουν την εκπλήρωση των καθηκόντων τους και να επιφέρουν στρεβλώσεις στην αγορά.

2.2.2 Ειδικότερες παρατηρήσεις και προτάσεις

Ως προς τις ειδικότερες παρατηρήσεις και προτάσεις, η παρέμβαση του ΣΕΒ κινήθηκε γύρω από την αναγκαιότητα τήρησης των ακόλουθων αξόνων:

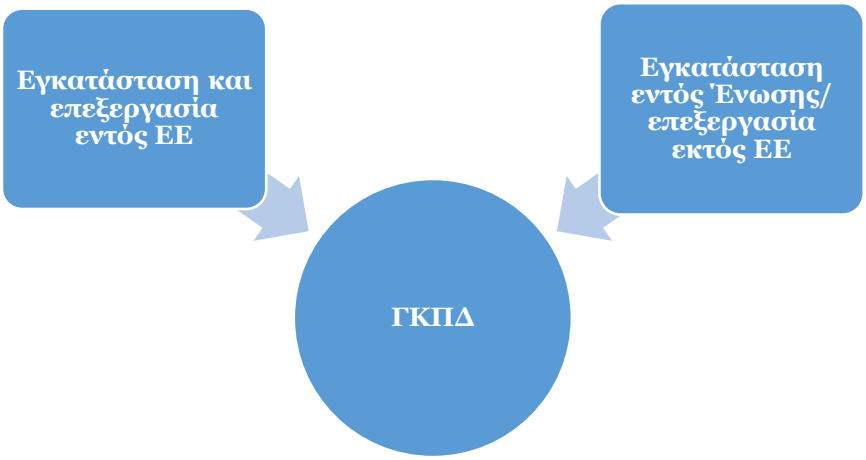
1) εξαίρεση από το πεδίο εφαρμογής των δεδομένων των ατομικών επιχειρήσεων,
2) θέσπιση ειδικότερων ρυθμίσεων για τις μεσαίες και μικρές επιχειρήσεις, ώστε να μειωθεί το διοικητικό βάρος,
3) ρητή αναγραφή των δραστηριοτήτων για τις οποίες απαιτείται η διεξαγωγή έκθεσης εκτίμησης αντικτύπου,
4) επαναφορά του πεδίου εφαρμογής στα οριζόμενα στην Οδηγία και στον Κανονισμό,
5) ρύθμιση της διαδικασίας πρόσβασης σε έγγραφα, τόσο για τον ιδιωτικό όσο και για τον δημόσιο τομέα, και τέλος
6) εισαγωγή συγκεκριμένης πρόβλεψης για τον ορισμό υπεύθυνου επεξεργασίας στις υπηρεσίες του δημόσιου τομέα.

Η κατ᾽ άρθρο ανάλυση που ακολουθεί αφορά στα σημαντικότερα σημεία όπως εντοπίστηκαν από τον ΣΕΒ αλλά και από την πλειοψηφία των συμμετεχόντων στη δημόσια διαβούλευση.

Άρθρο 2 - Πεδίο εφαρμογής

Ο Κανονισμός έχει στόχο την προστασία των υποκειμένων των δεδομένων προσωπικού χαρακτήρα από την επεξεργασία που διενεργούν καταρχήν οι υπεύθυνοι επεξεργασίας ή εκτελούντες την επεξεργασία με εγκατάσταση εντός της ένωσης, ανεξάρτητα από το αν η επεξεργασία αυτή πραγματοποιείται εντός της ένωσης **(Δ11)**.

Δ.11 Πεδίο εφαρμογής του Κανονισμού - περίπτωση Α'



Το πεδίο εφαρμογής του Κανονισμού εκτείνεται επίσης και στην επεξεργασία που διενεργούν υπεύθυνοι ή εκτελούντες την επεξεργασία μη εγκατεστημένοι στην ένωση πάντα όμως υπό την προϋπόθεση ότι τα υποκείμενα των δεδομένων βρίσκονται εντός της ένωσης και υπό τις εξής συνθήκες:

α) η προσφορά αγαθών ή υπηρεσιών στα υποκείμενα αυτά γίνεται στην ένωση, ανεξάρτητα αν απαιτείται πληρωμή **(Δ12)** ή

β) διενεργείται παρακολούθηση της συμπεριφοράς των υποκειμένων στο βαθμό που η συμπεριφορά αυτή λαμβάνει χώρα εντός της ένωσης **(Δ13)**.

Δ.12 Πεδίο εφαρμογής του Κανονισμού - περίπτωση Β'

Δ.13 Πεδίο εφαρμογής του Κανονισμού - περίπτωση Γ'

Με τον προσδιορισμό της έννοιας «εγκατάσταση», το Ευρωπαϊκό Δικαστήριο έχει ασχοληθεί ήδη κατά το παρελθόν, στο πλαίσιο της ερμηνείας που έδωσε ως προς το εδαφικό εύρος της Οδηγίας 95/46. Συγκεκριμένα, στην περίπτωση επεξεργασίας δεδομένων προσωπικού χαρακτήρα από επιχείρηση ηλεκτρονικού εμπορίου και το κατά πόσον αυτή διέπεται από το δίκαιο του κράτους μέλους προς το οποίο η εν λόγω επιχείρηση κατευθύνει τις δραστηριότητές, έκρινε πως η έννοια καλύπτει κάθε πραγματική και ουσιαστικού χαρακτήρα δραστηριότητα, έστω και περιορισμένη, ασκούμενη μέσω μόνιμης εγκαταστάσεως[53]. Το γεγονός ότι η επιχείρηση που είναι υπεύθυνη για την επεξεργασία των δεδομένων δεν διαθέτει ούτε θυγατρική ούτε υποκατάστημα σε κράτος μέλος, δεν αποκλείει το ενδεχόμενο να έχει εγκατάσταση στο κράτος αυτό. Αντίθετα, το Δικαστήριο επεσήμανε ότι δεν μπορεί να θεωρηθεί ότι υφίσταται μία τέτοια εγκατάσταση απλώς και μόνο λόγω του ότι στο κράτος αυτό είναι προσβάσιμος ο ιστότοπος της υπό εξέταση επιχειρήσεως[54].

Αναφορικά με την έκταση εφαρμογής του Νόμου, μένει να αποδειχθεί στην πράξη κατά πόσον οι ευρωπαϊκές Αρχές προστασίας ή οι καταναλωτές θα προβούν σε ενέργειες δικαστικής προστασίας κατά υπεύθυνων επεξεργασίας με έδρα τις Ηνωμένες Πολιτείες, για λόγους παραβίασης των διατάξεων του Κανονισμού. Ωστόσο, αυτή η επέκταση του πεδίου εφαρμογής του ίσως αποτελέσει πρόκληση για τις επιχειρήσεις εκτός ΕΕ, αναγκάζοντάς τες να προβούν σε παροχή εγγυήσεων και στη διατύπωση δηλώσεων στα πλαίσια συμβατικών σχέσεων περί συμβατότητας με «κάθε εφαρμοστέο δίκαιο» ενώ ίσως είναι επίσης πιθανό οι ευρωπαϊκές εποπτικές ή δικαστικές αρχές να απευθύνουν συστάσεις προς τις επιχειρήσεις εντός της ένωσης να παύσουν τις συναλλαγές τους με επιχειρήσεις εκτός ΕΕ που δεν συμμορφώνονται με τις υποχρεώσεις του Κανονισμού[55].

Αναφορικά με την έκταση εφαρμογής του Σχεδίου Νόμου ωστόσο, όπως εντοπίστηκε τόσο από τον ΣΕΒ όσο και από άλλους σχολιαστές στο πλαίσιο της δημόσιας διαβούλευσης αυτού, στο σχετικό άρθρο 2 παραλείπεται η αναφορά στις εν λόγω δύο προϋποθέσεις, με αποτέλεσμα να διευρύνεται το πεδίο εφαρμογής των διατάξεων του Κανονισμού αλλά και της Οδηγίας.

Συγκεκριμένα, το σχέδιο προβλέπει την εφαρμογή των διατάξεών του από υπεύθυνο επεξεργασίας ή/και εκτελούντα την επεξεργασία, ανεξαρτήτως του τόπου

53 ΔΕΕ 1.10.2015, Weltimmo, C-230/2014, σκέψη 31
54 ΔΕΕ 28.7.2016, Verein für Konsumenteninformation/Amazon EU Sàrl, C-191/2015, σκέψη 76
55 W. Scott Blackmer, GDPR: Getting Ready for the New EU General Data Protection Regulation, InfoLawGroup

εγκατάστασης αυτού, εφόσον η επεξεργασία λαμβάνει χώρα στην ελληνική επικράτεια ή, στο πλαίσιο εγκατάστασης του στην ελληνική επικράτεια ακόμη και αν η επεξεργασία λαμβάνει χώρα εκτός επικράτειας.

Συνακόλουθα, εάν ο υπεύθυνος επεξεργασίας ή ο εκτελών αυτήν βρίσκονται εγκατεστημένοι εκτός της ελληνικής επικράτειας, παρόλο που μπορεί να μην παρέχουν αγαθά ή υπηρεσίες ή να μην παρακολουθούν τη συμπεριφορά των υποκειμένων εντός της Ένωσης, θα καταλαμβάνονται, αδικαιολόγητα, από το πεδίο του Νόμου και θα εμπίπτουν στην εποπτεία και τον έλεγχο της Αρχής. Κατά συνέπεια, στην περίπτωση που κατά τη δημοσίευση του οριστικού κειμένου του Νόμου η διεύρυνση αυτή παραμείνει, αναμένεται να δημιουργηθεί αρκετά μεγάλο πεδίο νομοθετικής σαφήνειας την οποία είναι πιθανό να κληθεί να άρει η Αρχή με την έκδοση σχετικής ερμηνείας.

Αντίστοιχη ερμηνεία ενδέχεται να απαιτηθεί από την Αρχή και για την περίπτωση της παρέκκλισης που προβλέπεται από τον Κανονισμό αναφορικά με την εφαρμογή των διατάξεων του στις μεσαίες και μικρές επιχειρήσεις, καθώς στο Σχέδιο Νόμου παρατηρείται σχετική έλλειψη.

Τέλος, ιδιαίτερη αναφορά πρέπει να γίνει στο ζήτημα της εξαίρεσης που προβλέπεται στην αιτιολογική σκέψη 18 του Κανονισμού και στο άρθρο 2 παρ. 7 του σχεδίου του εφαρμοστικού Νόμου από το πεδίο εφαρμογής των διατάξεών τους για την επεξεργασία δεδομένων προσωπικού χαρακτήρα που πραγματοποιείται από φυσικό πρόσωπο στο πλαίσιο αποκλειστικά προσωπικής ή οικιακής δραστηριότητας.

Ίδια εξαίρεση προβλέπεται και στην αιτιολογική σκέψη 14 του Κανονισμού όπου αναφέρεται ότι δεν καλύπτεται από τον Κανονισμό η επεξεργασία δεδομένων προσωπικού χαρακτήρα που αφορά σε νομικά πρόσωπα και ιδίως σε επιχειρήσεις συσταθείσες ως νομικά πρόσωπα, περιλαμβανομένων της επωνυμίας, του τύπου και των στοιχείων επικοινωνίας του νομικού προσώπου. Με δεδομένη την ιδιομορφία της ελληνικής οικονομίας και της δραστηριοποίησης σε αυτήν ενός πολύ μεγάλου ποσοστού ατομικών επιχειρήσεων οι οποίες κατά την εμπορική και φορολογική νομοθεσία αποτελούν φυσικά πρόσωπα βάσει της στενής γραμματικής ερμηνείας του Κανονισμού και, ελλείψει σχετικής ρητής πρόβλεψης του Σχεδίου Νόμου, είναι εύκολο να συμπεράνει κανείς ότι θα έπρεπε και αυτές να υπάγονται στην προστασία των δεδομένων τους.

Ωστόσο, μια τέτοια στενή ερμηνεία δεν ανταποκρίνεται στην πραγματικότητα, καθώς οι ατομικές επιχειρήσεις, στο πλαίσιο της άσκησης της εμπορικής τους δραστηριότητας, αποκτούν κατά το ουσιαστικό κριτήριο την εμπορική ιδιότητα[56] και, συνεπώς όπως και τα νομικά πρόσωπα θα πρέπει ρητά να εξαιρεθούν από το πεδίο εφαρμογής του.

Εξάλλου, η επιβολή τυχόν περιορισμών ή υποχρεώσεων στην επεξεργασία και στην κυκλοφορία δεδομένων των φυσικών προσώπων που αφορούν τη εμπορική τους ιδιότητα ως ατομικών επιχειρήσεων, δε συνάδει όχι μόνο με τις προβλέψεις της εθνικής νομοθεσίας περί Γενικού Εμπορικού Μητρώου αλλά ούτε και με τις διατάξεις του πτωχευτικού δικαίου.

Ειδικότερα, βάσει του άρθρου 2 παρ.1 του Πτωχευτικού Κώδικα, η ιδιότητα του φυσικού προσώπου εκ του Νόμου, να ασκεί εμπορικές πράξεις κατά σύνηθες επάγγελμα ως ατομική επιχείρηση συνδέεται με την απόκτηση πτωχευτική ικανότητας, ενώ στο ν. 3419/2005 οι ατομικές επιχειρήσεις περιλαμβάνονται στους υπόχρεους εγγραφής στο Γενικό Εμπορικό Μητρώο (ΓΕΜΗ) και καταλαμβάνονται από την αρχή της εμπορικής δημοσιότητας.

Βάσει των ανωτέρω σκέψεων αλλά και για λόγους διαφύλαξης της εμπορικής πίστης, της πρόληψης της απάτης, της αξιοπιστίας και ασφάλειας των συναλλαγών, στο Σχέδιο Νόμου θα πρέπει να εισαχθεί διαχωρισμός ως προς τα δεδομένα των φυσικών προσώπων που άπτονται της ιδιωτικής τους σφαίρας και ως προς τα δεδομένα των ατομικών επιχειρήσεων που άπτονται της εμπορικής τους ιδιότητας, εξαιρώντας τα τελευταία από το πεδίο εφαρμογής του Κανονισμού, όπως ισχύει και για τις προσωπικές εταιρείες ως νομικά πρόσωπα.

Άρθρο 4 - Επεξεργασία για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας

Αναφορικά με την επεξεργασία για εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον και απευθύνεται κυρίως σε δημόσιους φορείς, πρέπει να σημειωθεί ότι ο Κανονισμός απαριθμεί και άλλες προϋποθέσεις, οι οποίες καθιστούν σύννομη την επεξεργασία και μπορούν να τύχουν εφαρμογής από υπευθύνους επεξεργασίας του ιδιωτικού τομέα. Μεταξύ αυτών, το άρθρο 6 παρ. 1 εδ. στ, σε συνδυασμό με την αιτιολογική σκέψη 47 του Κανονισμού, καθώς και επιμέρους αναφορές στις Κατευθυντήριες Γραμμές της Ομάδας του Άρθρου 29, αναγνωρίζουν ρητά το έννομο

[56] Βλ. σχετικά Ν.Σ.Κ. 774/1999

συμφέρον του υπεύθυνου επεξεργασίας που επεξεργάζεται δεδομένα αυστηρά για λόγους πρόληψης της απάτης.

Στο πλαίσιο αυτό και, δεδομένου ότι η απάτη αποτελεί μάστιγα για την υγιή επιχειρηματικότητα και η εξάλειψή της βρίσκεται σε προτεραιότητα όχι μόνον για την εγχώρια αλλά για το σύνολο των ευρωπαϊκών αγορών, η αναγνώρισή της ως νομικής βάσης προς θεμελίωση του έννομου συμφέροντος θα διευκόλυνε τις εταιρίες κατά την εκτέλεση των εργασιών τους, υπό την απαραίτητη βέβαια τήρηση των λοιπών όρων της σύννομης επεξεργασίας.

Περαιτέρω, εφόσον το συγκεκριμένο άρθρο αναφέρεται σε επεξεργασία που εκτελείται προς το δημόσιο συμφέρον, είναι μάλλον άσκοπη η πρόβλεψη της παραγράφου 4 για προηγούμενη ενημέρωση του υποκειμένου και για τις περιπτώσεις (β) και (γ). Αντίθετα, η παρ. 4 μπορεί να διαμορφωθεί ως ακολούθως:
«Όταν ο υπεύθυνος επεξεργασίας προτίθεται να διαβιβάσει τα δεδομένα προσωπικού χαρακτήρα για τους σκοπούς που αναφέρονται υπό το στοιχεία α) της παραγράφου 2 του παρόντος άρθρου, θα πρέπει να παρέχει στο υποκείμενο των δεδομένων, πριν από την εν λόγω περαιτέρω επεξεργασία, πληροφορίες για τον σκοπό αυτόν και άλλες τυχόν αναγκαίες πληροφορίες σύμφωνα με το άρθρο 14 παράγραφο 2 του Κανονισμού».

Τέλος, ως προς την υποχρέωση του υπεύθυνου επεξεργασίας της παρ. 2 περ. α να τεκμηριώσει ότι η επεξεργασία είναι απολύτως αναγκαία για τους σκοπούς η εκπλήρωση των οποίων υπερέχει προφανώς των δικαιωμάτων των προσώπων τα οποία αφορούν τα δεδομένα προσωπικού χαρακτήρα, κρίνεται ιδιαίτερα χρήσιμη η προσθήκη διευκρινιστικών στοιχείων αναφορικά με τον τρόπο τεκμηρίωσης της αναγκαιότητας αλλά και η θέσπιση σχετικών κριτηρίων.

Άρθρο 5 - Επεξεργασία δεδομένων εικόνας και ήχου μέσω κλειστού κυκλώματος τηλεόρασης

Η παράγραφος 6 του συγκεκριμένου άρθρου, περιλαμβάνει διατυπώσεις οι οποίες συνεπάγονται εξαιρετικά μεγάλη δυσκολία τεχνικής υλοποίησης από την πλευρά των υπεύθυνων επεξεργασίας. Για λόγους συμβατότητας με τις τεχνικές δυνατότητες που είναι διαθέσιμες από την πλευρά των υπεύθυνων επεξεργασίας, προτείνεται η αναδιατύπωση της παραγράφου 6 του άρθρου 5, ως ακολούθως:

«Σε περίπτωση συμβάντος που αφορά το σκοπό της επεξεργασίας, ο υπεύθυνος της επεξεργασίας επιτρέπεται να τηρεί τις λήψεις, στις οποίες έχει καταγραφεί το συγκεκριμένο συμβάν σε χωριστό αρχείο για 3 μήνες. Μετά την πάροδο του ανωτέρω χρονικού διαστήματος ο υπεύθυνος επεξεργασίας μπορεί να τηρεί τα δεδομένα για μεγαλύτερο, συγκεκριμένο ή συγκεκριμένα προσδιορίσιμο, χρονικό διάστημα μόνο σε εξαιρετικές περιπτώσεις όπου το συμβάν χρήζει περαιτέρω διερεύνησης».

Για τον ίδιο λόγο, καθώς είναι τεχνικά αδύνατη η ενημέρωση σε τρόπο εμφανή για όλα τα στοιχεία που προβλέπονται στην παρ. 9 προτείνεται η τροποποίηση της ως εξής:
«Πριν ένα πρόσωπο εισέλθει στην εμβέλεια του συστήματος βιντεοεπιτήρησης, ο υπεύθυνος επεξεργασίας οφείλει να το ενημερώνει, με τρόπο εμφανή και κατανοητό, ότι πρόκειται να εισέλθει σε χώρο που βιντεοσκοπείται. Προς τούτο, πρέπει: α) να αναρτώνται σε επαρκή αριθμό και εμφανές μέρος ευδιάκριτες πινακίδες, όπου θα αναγράφεται το πρόσωπο για λογαριασμό του οποίου γίνεται η βιντεοσκόπηση (υπεύθυνος επεξεργασίας), καθώς και τα στοιχεία επικοινωνίας του και β) να είναι διαθέσιμη στο κοινό, εφόσον ζητηθεί, με κάθε πρόσφορο τρόπο αναλυτικότερη ενημέρωση».

Τέλος, για λόγους νομοτεχνικής αρτιότητας η φράση «Ο υπεύθυνος επεξεργασίας υποχρεούται να δύναται να πρέπει να είναι σε θέση να αποδεικνύει» θα ήταν ορθότερο να αντικατασταθεί σε «Ο υπεύθυνος επεξεργασίας υποχρεούται να είναι σε θέση να αποδεικνύει».

Άρθρο 6 - Συγκατάθεση παιδιού για την επεξεργασία δεδομένων προσωπικού χαρακτήρα στο πλαίσιο της προσφοράς υπηρεσίας κοινωνίας της πληροφορίας

Η επιλογή του 15ου έτους ως έτος συγκατάθεσης, παρότι αφενός μεν δεν απαγορεύεται από τον Κανονισμό και αφετέρου αποτελεί πάγια επιλογή του Έλληνα νομοθέτη ως ελάχιστο όριο αυτοδιάθεσης του υποκειμένου, εντούτοις είναι πολύ πιθανό να προκαλέσει τεχνικά προβλήματα στην ενιαία και ομοιόμορφη υλοποίηση, δεδομένου ότι στην πλειοψηφία τους, τα υπόλοιπα κράτη-μέλη φαίνεται να έχουν επιλέξει την ηλικία των 13 ετών ως ελάχιστη απαιτούμενη για τη συγκατάθεση του έχοντος τη γονική μέριμνα[57].

[57] Δείτε εδώ τη σχετική αναφορά της ιστοσελίδας Better Internet for Kids η οποία σχεδιάστηκε με πρωτοβουλία της Ευρωπαϊκής Επιτροπής.

Άρθρο 7 - Επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα και Άρθρο 8 - Επεξεργασία δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές διώξεις, μέτρα ασφαλείας και ποινικές καταδίκες

Καθώς εξ' ορισμού η συγκατάθεση του υποκειμένου για επεξεργασία ακόμη και των «απλών» δεδομένων του πρέπει να είναι ρητή, η ξεχωριστή αναγραφή της προϋπόθεσης για ρητή και έγγραφη συγκατάθεση για τα δεδομένα υγείας και τα δεδομένα που αφορούν ποινικές διώξεις, μέτρα ασφαλείας και ποινικές καταδίκες, ενδέχεται να προκαλέσει σύγχυση. Για το λόγο αυτό προτείνεται η διαγραφή της σχετικής αναφοράς.

Περαιτέρω, αναφορικά με την προϋπόθεση περί «έγγραφης» συγκατάθεσης και με δεδομένη την ευρύτατη διάδοση των ηλεκτρονικών μέσων στην καθημερινή επικοινωνία, αλλά και την νομοθετικά αναγνωρισμένη αποδεικτική δύναμη των ηλεκτρονικών εγγράφων, κρίνεται σκόπιμη η πρόβλεψη της δυνατότητας για παροχή συγκατάθεσης με ηλεκτρονικά μέσα.

Άρθρο 9 - Δικαίωμα πρόσβασης σε δεδομένα εικόνας και ήχου

Το συγκεκριμένο άρθρο εισάγει κάποιες υποχρεώσεις εκ μέρους του υπεύθυνου επεξεργασίας, οι οποίες δεν είναι τεχνικά υλοποιήσιμες. Συγκεκριμένα, είναι αμφίβολη η επιτυχία της απαίτησης για τεχνική κάλυψη της εικόνας τρίτων προσώπων, καθώς και της δυνατότητας να γνωρίζει ο υπεύθυνος επεξεργασίας το πρόσωπο των αιτούντων. Πέραν των ανωτέρω, κρίνεται απαραίτητη η παράταση της χρονικής διορίας της παραγράφου 1 σε 30 ημέρες αντί για 15.

Άρθρο 13 - Προηγούμενη διαβούλευση

Το συγκεκριμένο άρθρο ενδεχομένως παρουσιάσει προβλήματα κατά την εφαρμογή του. Ειδικότερα, στην παράγραφο 2 θεσπίζονται έξι περιπτώσεις βάσει των οποίων απαιτείται προηγούμενη διαβούλευση με την Αρχή, επιπλέον των περιπτώσεων του άρθρου 36 παράγραφος 1 του Κανονισμού. Κατά συνέπεια, καθίσταται απαραίτητο να διευκρινιστεί εάν, στις περιπτώσεις αυτές, θα πρέπει να προηγείται χρονικά η διαβούλευση της διενέργειας υφισταμένων ή μελλοντικών επεξεργασιών των κατηγοριών και υποκατηγοριών που αναφέρονται, ανεξαρτήτως εάν η επεξεργασία αυτή ενέχει υψηλό κίνδυνο. Η διάταξη έρχεται σε ανακολουθία με το άρθρο 9 παρ. 4 του Κανονισμού και κατά συνέπεια είναι σημαντικός ο ορισμός του υπόχρεου εκτέλεσης της σχετικής υποχρέωσης.

Περαιτέρω, με την περ. στ' εντάσσεται και η μεγάλης κλίμακας συστηματική επεξεργασία δεδομένων προσωπικού χαρακτήρα που αφορούν στην οικονομική κατάσταση και συμπεριφορά καθώς και την πιστοληπτική ικανότητα φυσικών προσώπων. Ωστόσο, η περίπτωση αυτή δεν εμπίπτει στο πεδίο των εξαιρέσεων του άρθρου 9 παρ. 4 και του άρθρου 36 παρ. 5 του Κανονισμού, καθώς δεν αποτελεί επεξεργασία για την εκτέλεση καθήκοντος προς το δημόσιο συμφέρον και δεν έχει σχέση με δεδομένα που αφορούν την υγεία ή με βιομετρικά δεδομένα. Συνεπώς, προτάθηκε η διαγραφή της αναφοράς αυτής από την λίστα των δραστηριοτήτων επεξεργασίας που απαιτούν προηγούμενη διαβούλευση με την Αρχή.

Άρθρο 14 - Ορισμός Υπευθύνου Προστασίας Δεδομένων

Στο συγκεκριμένο άρθρο του σχεδίου προκαλεί απορία η επιλογή του νομοθέτη να διατυπώσει την παρ. 1 με τέτοιο τρόπο ώστε τελικά να μη διαφοροποιείται από την περίπτωση β της παραγράφου 1 του άρθρου 37 του Κανονισμού, σε συμπλήρωση της οποίας θεσπίζεται. Επιπρόσθετα, η αναφορά στον «κατάλογο που έχει θεσπίσει η Αρχή» χρήζει διευκρίνισης δεδομένου ότι η Αρχή δεν έχει καταρτίσει κατάλογο πράξεων επεξεργασίας για τις οποίες απαιτείται η προηγούμενη εκπόνηση έκθεσης εκτίμησης αντικτύπου.

Περαιτέρω, στην παρ. 3 τίθεται συγκεκριμένος χρονικός περιορισμός στη διάρκεια ισχύος του ορισμού του υπεύθυνου προστασίας. Ωστόσο, εφόσον ο κάθε υπεύθυνος επεξεργασίας φέρει ευθύνη για την επιλογή του κατάλληλου υπεύθυνου προστασίας, καθίσταται προφανές ότι θα πρέπει να του δοθεί και η ελευθερία επιλογής της ανανέωσης ή μη της σχετικής εντολής. Για τον ίδιο λόγο, θα πρέπει να απαλειφθεί και η φράση «εκτός αν συντρέχει σοβαρός λόγος για την ανάκληση του ορισμού ή την παύση του υπευθύνου προστασίας προσωπικών δεδομένων».

Στην ίδια παράγραφο, η αναφορά στο άρθρο 28 του Κανονισμού που γίνεται εκ παραδρομής καθώς η διάταξη θα έπρεπε να παραπέμπει στο άρθρο 38, θα πρέπει να διορθωθεί προς αποφυγή σύγχυσης.

Τέλος, στην παράγραφο 4 λείπει η αναφορά στην υποχρέωση δημοσιότητας που εισάγει ο Κανονισμός στο άρθρο 37 παράγραφος 7 σύμφωνα με την οποία ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία δημοσιεύουν τα στοιχεία επικοινωνίας του υπεύθυνου προστασίας δεδομένων και τα ανακοινώνουν στην εποπτική αρχή. Συνεπώς χρήζει διευκρίνισης ο τρόπος συμμόρφωσης με αυτήν την υποχρέωση κατά την ελληνική έννομη τάξη.

Άρθρο 15 - Πιστοποίηση και Διαπίστευση φορέων πιστοποίησης

Στο χρονικό διάστημα που προηγήθηκε της δημοσίευσης του Σχεδίου Νόμου, η υπερπροσφορά υπηρεσιών παροχής πιστοποιήσεων Υπευθύνων Προστασίας Δεδομένων οδήγησε σε μια άνευ προηγουμένου σύγχυση στην αγορά ως προς την υποχρεωτικότητα της εν λόγω πιστοποίησης. Η καθυστέρηση έκδοσης του σχεδίου είχε ως αποτέλεσμα την οικονομική επιβάρυνση των επιχειρήσεων οι οποίες θεώρησαν υποχρεωτική τη λήψη της εν λόγω πιστοποίησης, παρότι κάτι τέτοιο δεν προβλεπόταν στο κείμενο του Κανονισμού.

Παρόλα αυτά, τώρα που η αγορά έχει τη σχετική γνώση, η ζήτηση που οδήγησε στη δημιουργία των προγραμμάτων αυτών παραμένει αυξημένη, ενώ έχει ήδη χορηγηθεί διαπίστευση σε φορείς για την πιστοποίηση προσώπων.

Θεωρούμε συνεπώς απαραίτητο να ληφθεί η σχετική μέριμνα στο Σχέδιο Νόμου και να αναθεωρήσει η Αρχή Προστασίας Προσωπικών Δεδομένων την πρόσφατη ανακοίνωσή της περί μη αναγνώρισης τέτοιου συστήματος πιστοποίησης ώστε να καταρτιστεί, σε συνεργασία με τον ΕΟΠΠΕΠ, το ΕΣΥΔ και την Αρχή το κατάλληλο σχήμα πιστοποίησης προκειμένου να εκλείψουν τα φαινόμενα παραπλάνησης, αλλά και προκειμένου να υπάρξει ένα επαρκές πλαίσιο διασφάλισης των επαγγελματικών προσόντων όπως συμβαίνει και σε άλλα επαγγελματικά πλαίσια.

Επιπρόσθετα, ως προς την ανάκληση των διαπιστεύσεων από το Εθνικό Σύστημα Διαπίστευσης Α.Ε., θεωρούμε επιβεβλημένο τον προσδιορισμό του χρονικού σημείου της ανάκλησης καθώς και της διάρκειας ισχύος αυτής. Παράλληλα, αναδιατύπωση απαιτείται στην περίπτωση της παρ. 6, ώστε να προβλέπεται η ανάκληση των διαπιστεύσεων μόνο από το Εθνικό Σύστημα Διαπίστευσης ΑΕ (ΕΣΥΔ), τόσο για λόγους ουσίας, καθώς το ΕΣΥΔ αποτελεί τον αρμόδιο οργανισμό για την υλοποίηση, εφαρμογή και διαχείριση του συστήματος διαπίστευσης της Ελλάδας, βάσει του Κανονισμού 765/2008, όσο και για λόγους απλοποίησης της διαδικασίας αφού διαφορετικά θα απαιτείται η σύμφωνη γνώμη και της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Εξάλλου, η συνεργασία μεταξύ του ΕΣΥΔ και της Αρχής που προβλέπεται στα προηγούμενα στάδια (π.χ. απαιτήσεις συμμόρφωσης) εξασφαλίζει εξ ορισμού το σημαντικό ρόλο της Αρχής.

Τέλος, θα πρέπει να εκδοθεί και να δημοσιοποιηθεί άμεσα ο κατάλογος των κριτηρίων στον οποίο αναφέρεται η παρ. 2. σχετικά με την πιστοποίηση των υπεύθυνων επεξεργασίας.

Άρθρο 17 - Επεξεργασία στο πλαίσιο της απασχόλησης και προστασίας δεδομένων των εργαζομένων

Και στην περίπτωση του συγκεκριμένου άρθρου, ιδιαίτερα κρίσιμη βελτίωση θα μπορούσε να αποτελέσει η προσθήκη ρητής αναφοράς στη δυνατότητα παροχής συγκατάθεσης του υποκειμένου των δεδομένων με ηλεκτρονικά μέσα.

Για λόγους σαφήνειας, σημαντική κρίνεται και η προσθήκη ρητής διευκρίνισης ότι οι περιπτώσεις στις οποίες επιτρέπεται η συλλογή και επεξεργασία δεδομένων είναι διαζευκτική και όχι σωρευτική.

Επιπρόσθετα, στην παρ. 6 η διατύπωση «η συλλογή και επεξεργασία δεδομένων προσωπικού χαρακτήρα των εργαζομένων επιτρέπεται αποκλειστικά [είτε] για σκοπούς που συνδέονται άμεσα με τη σχέση απασχόλησης είτε για σκοπούς που προκύπτουν από διάταξη Νόμου», πρέπει να σημειωθεί ότι έρχεται σε σύγκρουση με την παράγραφο 3 του ίδιου άρθρου. Ο λόγος είναι ότι η παρ. 3 ορίζει ότι η συλλογή και επεξεργασία δεδομένων προσωπικού χαρακτήρα των εργαζομένων από τον εργοδότη επιτρέπεται (εκτός των δύο σκοπών που ορίζει η παράγραφος 6) και για τη διαφύλαξη ζωτικού συμφέροντος του εργαζομένου ή άλλου φυσικού προσώπου, καθώς και εφόσον είναι απαραίτητη για την εκπλήρωση των εννόμων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, εκτός εάν έναντι των συμφερόντων αυτών υπερισχύουν το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του εργαζομένου ως υποκειμένου των δεδομένων. Κατά συνέπεια, χρήσιμη θα ήταν η αποσαφήνιση ότι η παράγραφος 6 (όπως και η παράγραφος 5) αφορούν σε ειδικές κατηγορίες δεδομένων

Και αυτό γιατί στην περίπτωση κατά την οποία η συγκεκριμένη παράγραφος 6 καλύπτει όλες τις κατηγορίες των δεδομένων, θα καταλήξει να περιορίζει σε υπερβολικό βαθμό τη δυνατότητα των επιχειρήσεων να επεξεργάζονται τα προσωπικά δεδομένα των εργαζομένων τους για την επιδίωξη εννόμων συμφερόντων τους, δυνατότητα την οποία αναγνωρίζει και ο Κανονισμός.

Περαιτέρω, στην παράγραφο 9 του ίδιου άρθρου, πρέπει να αποσαφηνιστεί ότι οι περιορισμοί που τίθενται σε σχέση με τη διεξαγωγή ιατρικών εξετάσεων και αναλύσεων καθώς και η ένταξη στις έννοιες αυτές των ψυχολογικών ή ψυχομετρικών τεστ, αφορούν αμιγώς ψυχομετρικά τεστ που στοχεύουν στη διαπίστωση τυχόν διαταραχών της ψυχικής υγείας του εργαζομένου. Χαρακτηριστικά σημειώνεται ότι υπάρχουν πολλές διαφορετικές μορφές ψυχομετρικών τεστ τα οποία σε πολλές

περιπτώσεις δε συνιστούν ιατρική εξέταση, καθώς η δομή τους και τα ζητήματα που εξετάζουν δε στοχεύουν στη διάγνωση κάποιας ψυχικής διαταραχής αλλά στη διαμόρφωση μιας γενικής εκτίμησης σχετικά με την προσωπικότητα του εργαζομένου. Εξάλλου, η χρήση τέτοιων μεθόδων είναι διεθνώς διαδεδομένη καθώς στοχεύει στην καλύτερη κατανόηση της προσωπικότητας των εργαζομένων και κατά συνέπεια, στην καλύτερη διαχείριση των εργασιακών σχέσεων και διαμόρφωση εκπαιδευτικών προγραμμάτων για τη συνολική βελτίωση της συνεργασίας μεταξύ των εργαζομένων καθώς και την ανάθεση καθηκόντων και ρόλων που ταιριάζουν όχι μόνο στο γνωστικό τους αντικείμενο αλλά και στην προσωπικότητά τους.

Για το σκοπό αυτό σκόπιμη κρίνεται η προσθήκη διευκρίνισης ως εξής: «Γενικά τεστ προσωπικότητας που δεν δύνανται να οδηγήσουν σε συμπεράσματα που αφορούν τη ψυχική υγεία του εργαζομένου, παρά μόνο να αναδείξουν στοιχεία της προσωπικότητάς του που σχετίζονται με την επαγγελματική του δραστηριότητα, δεν εμπίπτουν στην έννοια των ανωτέρω ψυχομετρικών τεστ για τους σκοπούς της παρούσας διάταξης».

Ακόμη, στην παρ. 13, εκτός από την προστασία των κρίσιμων υποδομών και υποδομών ζωτικής προστασίας, θα πρέπει να προβλεφθεί και η προστασία των αγαθών, ως δικαιολογητικός λόγος για την συλλογή και επεξεργασία δεδομένων προσωπικού χαρακτήρα μέσω κλειστού κυκλώματος τηλεόρασης, υπό τον όρο ότι οι κάμερες εστιάζουν στο αγαθό που προστατεύουν και όχι στους χώρους εργασίας των εργαζομένων.

Τέλος, στην παρ. 20 θα πρέπει να προσδιοριστούν τα μέσα στα οποία θα αφορά ο Κανονισμός.

Άρθρο 31 - Δικαίωμα ενημέρωσης του υποκειμένου των δεδομένων

Στο άρθρο γίνεται αναφορά στο βασικό δικαίωμα ενημέρωσης του υποκειμένου αναφορικά μόνο με την Ευρωπαϊκή Οδηγία 680/2016, ενώ δεν παρέχονται κατευθυντήριες γραμμές ως προς τα ίδια ζητήματα που άπτονται του πεδίου εφαρμογής του Ευρωπαϊκού Κανονισμού 679/2016.

Ειδικότερα, δεν φαίνεται να επιλύεται θεσμικά το ζήτημα των προτεινόμενων μέσων για την επαρκή και ορθή ενημέρωση του υποκείμενου, ιδίως ως προς τα δεδομένα που δεν συλλέγονται απευθείας από το υποκείμενο (πρβλ. άρθρο 14 του Κανονισμού). Ο Κανονισμός δηλαδή, αναγνωρίζει την αναγκαιότητα ενημέρωσης των υποκειμένων

στις περιπτώσεις αυτές, ωστόσο στο σχέδιο του Νόμου δεν παρέχεται καμία κατευθυντήρια γραμμή για τον τρόπο με τον οποίο ο υπεύθυνος επεξεργασίας θα ικανοποιήσει το δικαίωμα ενημέρωσης του υποκειμένου, που μεταξύ άλλων περιλαμβάνει την ενημέρωση για τη νόμιμη βάση της επεξεργασίας των δεδομένων του, όπως λόγου χάρη μέσω της ανάρτησης της πολιτικής απορρήτου στον επίσημο ιστότοπό του, μέσω της δημοσίευσης σε εφημερίδες ευρείας κυκλοφορίας, μέσω του αποδέκτη των δεδομένων.

Άρθρο 67 - Δικαστική προσφυγή κατά υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία - Αποζημίωση και ευθύνη

Στην παράγραφο 2 δεν καθίσταται σαφές και θα πρέπει να διευκρινιστεί εάν το υποκείμενο των δεδομένων έχει δικαίωμα αξίωσης για καταβολή αποζημίωσης λόγω υλικής ζημίας ή ηθικής βλάβης μόνο κατά του υπεύθυνου επεξεργασίας ή και κατά του εκτελούντος αυτήν.

Άρθρο 69 - Διοικητικά πρόστιμα και Γενικοί όροι επιβολής προστίμων

Υπό το φως της πρόβλεψης του ίδιου του Κανονισμού για επιεικέστερη μεταχείριση των μεσαίων και μικρών επιχειρήσεων, καθίσταται προφανές ότι τα διοικητικά πρόστιμα για τις επιχειρήσεις αυτού του μεγέθους θα πρέπει να διαφοροποιηθούν ώστε να μην καθίσταται η επιβολή προστίμου υπέρμετρα επαχθής σε βαθμό που να απειληθεί η ίδια τους η λειτουργία.

Άρθρο 70 - Ποινικές κυρώσεις

Η επιβολή ποινικών κυρώσεων στον Υπεύθυνο Προστασίας Δεδομένων είναι αντίθετη τόσο με τον ίδιο τον Κανονισμό όσο και με τις Κατευθυντήριες Γραμμές της Ομάδας Εργασίας του άρθρου 29 (WP 243)[58], σύμφωνα με τα οποία ο Υπεύθυνος Προστασίας Δεδομένων δεν φέρει προσωπική ευθύνη, αλλά αντίθετα απολαμβάνει αυτονομία και επαρκή προστασία κατά την εκτέλεση των καθηκόντων του. Εξάλλου, σύμφωνα και με τις διατάξεις του Ποινικού Κώδικα, η παραβίαση επαγγελματικής εχεμύθειας τιμωρείται με χρηματική ποινή ή φυλάκιση μέχρι ενός έτους. Κατά συνέπεια, η σχετική πρόβλεψη δέον να απαλειφθεί ώστε να διασφαλίζεται η αυτονομία του ΥΠΔ κατά την εκτέλεση των καθηκόντων του.

[58] Δείτε εδώ τις Κατευθυντήριες γραμμές της Ομάδας Εργασίας του άρθρου 29 σχετικά με τους Υπεύθυνους Προστασίας Δεδομένων.

Άρθρο 70- Τελικές και μεταβατικές διατάξεις

Δεδομένης της καθυστέρησης δημοσίευσης του νέου Νόμου, πρέπει να εισαχθεί μεταβατική διάταξη για όσες πράξεις επεξεργασίας έγιναν μετά την 25η Μαΐου 2018 και πριν τη δημοσίευση του εθνικού Σχεδίου Νόμου. Ειδικότερα, θα πρέπει να προβλεφθεί ρητά ότι η συμμόρφωση των πράξεων αυτών με το Κείμενο του κανονισμού και το ισχύον νομικό πλαίσιο (Ν. 2472/1997) θεωρείται σύννομη.

Ακόμα, προτείνεται η ρητή κατάργηση ή επικαιροποίηση τέτοιων διατάξεων της εθνικής, οριζόντιας και κλαδικής νομοθεσίας που έρχονται σε αντίθεση με τις απαιτήσεις του σχεδίου και του Κανονισμού.

Ειδικότερα, θα πρέπει να ληφθεί μέριμνα αναφορικά με τις υποχρεώσεις των επιχειρήσεων που προκύπτουν από την εργατική νομοθεσία, όπως η ανάρτηση προσωπικών δεδομένων του προσωπικού, η τήρηση ενσήμων σε έγχαρτη μορφή κ.ά. Περαιτέρω, υποχρεώσεις για το υποκείμενο των δεδομένων, αλλά και για τους υπεύθυνους και εκτελούντες την επεξεργασία, προκύπτουν και σε μια σειρά κλαδικών θεμάτων του τραπεζικού και ασφαλιστικού κλάδου, του κλάδου των μεταφορών, των επιχειρήσεων οπτικοακουστικών μέσων, της σταθερής και κινητής τηλεφωνίας κ.ά., οι οποίες επίσης θα πρέπει να ληφθούν υπόψη. Ενδεικτικά, στην ασφαλιστική νομοθεσία ρητά προβλέπεται υποχρέωση του λήπτη της ασφάλισης να δηλώσει στον ασφαλιστή κάθε στοιχείο ή περιστατικό που γνωρίζει και το οποίο είναι αντικειμενικά ουσιώδες για την εκτίμηση του κινδύνου.

Τέτοιες ειδικότερες ρυθμίσεις δε θα πρέπει να αγνοηθούν από τον εθνικό νομοθέτη, καθώς, διαφορετικά, η σύγκρουση μεταξύ των εννόμων βάσεων για τη συλλογή και επεξεργασία των προσωπικών δεδομένων θα οδηγήσει σε διαφορετικές ερμηνείες από τους υπόχρεους και τελικά στην επιβολή αδικαιολόγητων προστίμων από την εθνική Αρχή.

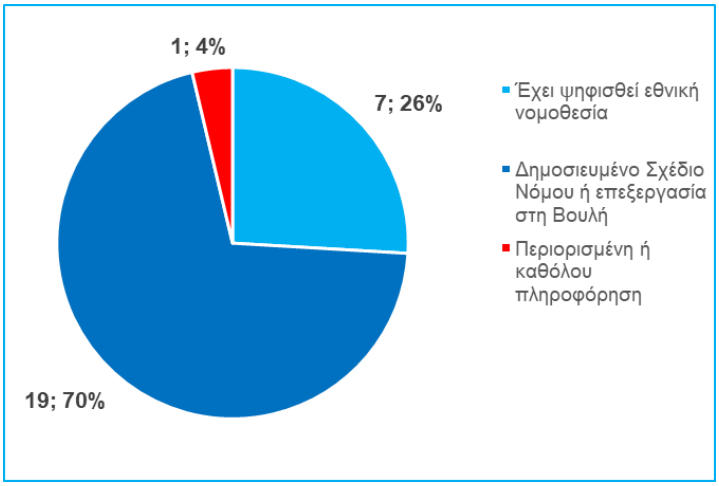
Τέλος, ο Κανονισμός θα πρέπει να ενταχθεί στο πλαίσιο της ψηφιακής στρατηγικής του Δημοσίου. Συγκεκριμένα, πρέπει να προβλεφθούν: α) η ρητή υποχρέωση των Δημοσίων Υπηρεσιών για ηλεκτρονική τήρηση των προσωπικών δεδομένων των πολιτών στις αντίστοιχες βάσεις δεδομένων με επιβολή κύρωσης σε αντίθετη περίπτωση, β) η υποχρέωση συμμόρφωσης και προσαρμογής των ηλεκτρονικών εφαρμογών του Δημοσίου στις νέες διατάξεις και αρχές (ελαχιστοποίηση, επικαιροποίηση πληροφοριών, νομιμότητα, διαφάνεια) και γ) η υποχρεωτική εκπόνηση εκπαιδευτικών σεμιναρίων των δημοσίων υπαλλήλων.

2.3 Η πορεία ενσωμάτωσης στα άλλα κράτη-μέλη

Η ενσωμάτωση του Κανονισμού στην εθνική νομοθεσία των κρατών-μελών αποδεικνύεται ως μια διαδικασία η οποία στην πράξη δεν αποδεικνύεται εύκολη. Είναι χαρακτηριστικό ότι, σύμφωνα με την έρευνα της Baker McKenzie[59], το Μάιο του 2018, μόλις επτά χώρες είχαν ολοκληρώσει τη διαδικασία ενσωμάτωσης του Κανονισμού. Ειδικότερα, η πορεία ενσωμάτωσης στην εθνική νομοθεσία είχε ως εξής:

- **Πλήρης ενσωμάτωση στην εθνική νομοθεσία:** Αυστρία, Γερμανία, Ην. Βασίλειο, Κροατία, Πολωνία, Σλοβακία, Σουηδία (κράτη-μέλη: 7)
- **Δημοσιευμένο Σχέδιο Νόμου σε διαβούλευση ή επεξεργασία στη Βουλή:** Βέλγιο, Βουλγαρία, Γαλλία, Δανία, Ελλάδα, Εσθονία, Ιρλανδία, Ισπανία, Ιταλία, Λετονία, Λιθουανία, Λουξεμβούργο, Ολλανδία, Ουγγαρία, Πορτογαλία, Ρουμανία, Σλοβενία, Τσεχία, Φινλανδία (κράτη-μέλη:19)
- **Περιορισμένη ή καθόλου πληροφόρηση για τον τρόπο και το περιεχόμενο του κειμένου ενσωμάτωσης:** Μάλτα (κράτη-μέλη:1)

Δ.14 Πορεία ενσωμάτωσης Κανονισμού στην εθνική νομοθεσία των κρατών-μελών της ΕΕ
Πηγή: Baker McKenzie, "GDPR National Legislation Survey, 0.3", May 2018



2.4 Η νομολογία που έχει αναπτυχθεί

Το ζήτημα της προστασίας των προσωπικών δεδομένων πέρα από τη νομική, οικονομική και τεχνική του διάσταση, προκάλεσε και το ενδιαφέρον των επιστημόνων στα πεδία της κοινωνιολογίας και της ψυχολογίας. Και αυτό, λόγω της ευρύτατης, καθημερινής και απροβλημάτιστης συγκατάθεσης που παρείχαν τα υποκείμενα των δεδομένων στην επεξεργασία, δημοσίευση, αναδημοσίευση, μεταφορά και αποθήκευση των δεδομένων τους από τα μέσα κοινωνικής δικτύωσης.

[59] Σημειώνεται ότι πρόκειται για τα τελευταία διαθέσιμα συγκεντρωτικά στοιχεία και η πορεία ενσωμάτωσης του Κανονισμού ενδέχεται να έχει αλλάξει. Σημειώνεται επίσης ότι στη μελέτη δεν παρουσιάζονται στοιχεία για την Κύπρο.

Ενδεικτικά, στο διάστημα μεταξύ 1997 και 2017 δημοσιεύτηκαν περισσότερες από 132 μελέτες αναφορικά με τα social media και την κοινωνική δικτύωση εξετάζοντας αυτό ακριβώς το συμπεριφορικό ζήτημα[60] και αναδεικνύοντας τους πιθανούς κινδύνους που η υπερβολική χρήση τέτοιων ιστοσελίδων μπορεί να επιφέρει στην ψυχολογία των υποκειμένων. Σύμφωνα με τις μελέτες, πολλοί χρήστες ειδικά κατά το παρελθόν δεν ήταν καν ενήμεροι σχετικά με τους πιθανούς κινδύνους της έκθεσης των προσωπικών τους δεδομένων σε συγκεκριμένες ιστοσελίδες, ή θεωρούσαν ότι αποτελούν λιγότερο σημαντικό στόχο[61], κάτι το οποίο δυστυχώς φαίνεται να διαψεύδεται από τις μέχρι σήμερα καταγεγραμμένες υποθέσεις στις οποίες δεδομένα «χάθηκαν», είτε λόγω κακής πολιτικής διαχείρισης αυτών, είτε εξαιτίας κακόβουλων επιθέσεων[62].

2.4.1 Η υπόθεση Facebook

Το πρόσφατο σκάνδαλο διαρροής προσωπικών δεδομένων από την εφαρμογή «Facebook» αποτελεί μια ακόμη τέτοια περίπτωση. Η εταιρεία, παρότι κατείχε κυρίαρχη θέση ανάμεσα στο σύνολο των σελίδων κοινωνικής δικτύωσης με 1,97 δισ. χρήστες τον Απρίλιο του 2017 και πάνω από 2 δισ. χρήστες τον Απρίλιο του 2018[63], παρέλειψε να δώσει την απαραίτητη σημασία στην προστασία των δεδομένων των χρηστών της. Έτσι, το 2014 η βρετανική εταιρεία Cambridge Analytica τις υπηρεσίες της οποίας είχε μισθώσει το 2016 η προεκλογική εκστρατεία του Ντόναλντ Τραμπ, ανέκτησε, μέσω ενός ψυχολογικού τεστ στο οποίο είχαν απαντήσει 270.000 μέλη του Facebook, τα δεδομένα 87 εκ. χρηστών. Παρότι το Facebook έλαβε γνώση ένα χρόνο μετά και ζήτησε τη διαγραφή τους, το γεγονός είχε ήδη στο μεταξύ προκαλέσει, όπως ήταν φυσικό, την αντίδραση του Αμερικανικού Κογκρέσου και του βρετανικού κοινοβουλίου που ζήτησαν την κατάθεση του Προέδρου και διευθύνοντος συμβούλου, Mark Zuckerberg.

Παράλληλα, η αρμόδια βρετανική αρχή προστασίας προστασία των προσωπικών δεδομένων ζήτησε ένταλμα για να ερευνήσει τα γραφεία της Cambridge Analytica.

---

60 Kawaljeet Kaur Kapoor & Kuttimani Tamilmani & Nripendra P. Rana & Pushp Patil & Yogesh K. Dwivedi & Sridhar Nerur, Advances in Social Media Research: Past, Present and Future, Information Systems Frontiers, 2017

61 Tow,W. N. F. H., Dell, P., & Venable, J. Understanding information disclosure behaviour in Australian Facebook users, Journal of Information Technology (2010), 25(2), 126–136

62 Βλ. https://vigilante.pw/ ή https://en.wikipedia.org/wiki/List_of_data_breaches

63 Πηγή: Statista 2018

Τελικά, όπως επιβεβαιώνει σήμερα ο εκπρόσωπος τύπου της Κομισιόν (η οποία διατηρεί προφίλ χρήστη στο Facebook[64]), Christian Wigand, τα προσωπικά δεδομένα έως και 2,7 εκ. Ευρωπαίων ή προσώπων που διαμένουν στην ΕΕ, «ενδεχομένως εστάλησαν στην Cambridge Analytica με ανάρμοστο τρόπο» ενώ η Ευρωπαία Επίτροπος αρμόδια για θέματα Δικαιοσύνης Věra Jourová είπε ότι "είναι ξεκάθαρο ότι τα δεδομένα των Ευρωπαίων πολιτών έχουν εκτεθεί σε ένα τεράστιο κίνδυνο και δεν είμαι βέβαιη ότι το Facebook έλαβε όλα τα απαραίτητα βήματα για να εφαρμόσει τις αλλαγές."[65].

Αξίζει να τονιστεί ότι η υπόθεση Facebook αποτελεί χαρακτηριστικό παράδειγμα παραβίασης προσωπικών δεδομένων από την ίδια την επιχείρηση (δηλαδή τον υπεύθυνο επεξεργασίας). Για τη χρήση των δεδομένων από την Cambridge Analytica δεν χρειάστηκε καμία εξωτερική παραβίαση συστημάτων ή κακόβουλη επίθεση από χάκερς. Δυστυχώς, το ίδιο το σύστημα είχε σχεδιαστεί με τέτοιο τρόπο ώστε να είναι δυνατή η χρήση των δεδομένων του χωρίς ιδιαίτερη δυσκολία.

Στις 17 Μαρτίου 2018, ο ελληνικής καταγωγής πρώην Διευθυντής Ασφαλείας του Facebook, Alex Stamos έγραψε στο λογαριασμό του στο Twitter:

> *Alex Stamos, @alexstamos*
>
> ***There are a lot of big problems that the big tech companies need to be better at fixing. We have collectively been too optimistic about what we build and our impact on the world. Believe it or not, a lot of the people at these companies, from the interns to the CEOs, agree.***
>
> *9:01 PM - Mar 17, 2018*

Ποιες ήταν όμως οι επιπτώσεις μετά από αυτήν την, θεωρητικά, καταστροφική για τη φήμη του Facebook υπόθεση; Αρχικά, κατά το πρώτο τρίμηνο του 2018 και ενάντια σε κάθε πρόβλεψη, η επιχείρηση εμφάνισε αύξηση κερδών κατά 63%, αύξηση εσόδων κατά 49% και αύξηση των ενεργών χρηστών της εφαρμογής κατά 13% σε σύγκριση με το ίδιο τρίμηνο πριν από ένα χρόνο[66]. Η συνέχεια αποδεικνύεται να έχει ιδιαίτερο ενδιαφέρον καθώς η εταιρεία έχασε μεν περισσότερα από $100 δισ. σε αξία μέσα στον Απρίλιο του 2018 ωστόσο τις επόμενες ημέρες φαίνεται να σημείωσε ανοδική τάση[67].

64 https://www.facebook.com/European-Union-EU-12088416071/
65 Μπορείτε να δείτε εδώ τη σχετική δήλωση.
66 Spencer Soper, Tina Bass, *Tech Giants' Reports Dispel Doubts About Growth*, Bloomberg
67 https://www.reuters.com/finance/stocks/chart/FB.O

Το επόμενο διάστημα παραμένει εξαιρετικά κρίσιμο, καθώς το Ανώτατο Δικαστήριο της Ιρλανδίας όπου βρίσκεται η ευρωπαϊκή έδρα της εταιρείας, διέταξε την παραπομπή της υπόθεσης στο Ανώτατο Ευρωπαϊκό Δικαστήριο, προκειμένου να αξιολογηθεί η νομιμότητα των μεθόδων μεταφοράς δεδομένων των ευρωπαίων χρηστών του από την ΕΕ στις ΗΠΑ. Και, παρότι σε μια προσπάθεια να καθυστερήσει την εξέταση της υπόθεσης από το Ευρωπαϊκό Δικαστήριο, το Facebook υπέβαλε προς το Ανώτατο Δικαστήριο της Ιρλανδίας έφεση εναντίον της παραπομπής στο Ευρωπαϊκό Δικαστήριο, η οποία ωστόσο απορρίφθηκε.

Η μέθοδος της μεταφοράς δεδομένων έχει χρησιμοποιηθεί στο παρελθόν και από άλλους τεχνολογικούς κολοσσούς όπως η Google και η Apple. Στην περίπτωση επομένως που το Ευρωπαϊκό Δικαστήριο κρίνει, με αφορμή την υπόθεση Facebook ότι η πρακτική αυτή παραβιάζει την ευρωπαϊκή νομοθεσία περί προστασίας των προσωπικών δεδομένων, το τοπίο για τις επιχειρήσεις αναμένεται να αλλάξει ριζικά.

Και ο Andrea Jelinek, Πρόεδρος της Ομάδας εργασίας του άρθρου 29 τοποθετήθηκε λέγοντας «Κατά κανόνα, τα προσωπικά δεδομένα δεν μπορούν να χρησιμοποιούνται χωρίς πλήρη διαφάνεια ως προς τον τρόπο χρήσης τους και τα πρόσωπα προς τα οποία γνωστοποιούνται. Αυτή (η υπόθεση Cambridge Analytica) συνιστά επομένως μια πολύ σοβαρή κατηγορία με μακροχρόνιες επιπτώσεις στο θέμα της προστασίας των δικαιωμάτων των υποκειμένων των δεδομένων και τη δημοκρατική διαδικασία. Η ICO, η Αρχή προστασίας δεδομένων του Ηνωμένου Βασιλείου διεξάγει έρευνα πάνω στο θέμα. Ως Πρόεδρος της Ομάδας εργασίας του άρθρου 29, υποστηρίζω πλήρως την έρευνα αυτή. Τα μέλη του άρθρου 29 θα συνεργαστούν σε αυτήν τη διαδικασία»[68].

Αναφορικά με την αναδρομικότητα της ποινής, η Věra Jourová τόνισε ότι «κυρώσεις δε μπορούν να εφαρμοστούν αναδρομικά, επομένως το Facebook δε θα υποστεί πρόστιμο για τη συγκεκριμένη παράβαση, όταν ο νέος Γενικός Κανονισμός εφαρμοστεί. Ωστόσο, από το Μάιο και έπειτα, δε θα διστάσουμε να χρησιμοποιήσουμε τις υψηλότερες δυνατές ποινές στην περίπτωση που οι Ευρωπαίοι πολίτες υποστούν μεγαλύτερη βλάβη».

Έτσι, σύμφωνα με την έκθεση της Επιτρόπου της Αγγλικής Αρχής, το επαπειλούμενο πρόστιμο ανέρχεται στο, συγκριτικά με τα GDPR δεδομένα, χαμηλό ποσό των 500.000

[68] Από την επίσημη σελίδα της ευρωπαϊκής επιτροπής http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=617458.

λιρών, το οποίο ωστόσο αποτελεί το υψηλότερο βάσει του προϋφιστάμενου καθεστώτος.

Στην υπόθεση «facebook» ωστόσο, άνοιξαν περισσότερα μέτωπα, καθώς με πρόσφατη απόφασή του το ΔΕΕ έκρινε[69] ότι ο διαχειριστής σελίδας (fan page) που φιλοξενείται στο facebook είναι υπεύθυνος από κοινού με το facebook για την επεξεργασία των δεδομένων των επισκεπτών της σελίδας του.

Πρακτικά, οι επιχειρήσεις αυτές (διαχειριστές σελίδων), κάνοντας χρήση των cookies (αναγνωριστικά στοιχεία), λαμβάνουν μέσω της πλατφόρμας του facebook, δεδομένα σχετικά με τους επισκέπτες του. Τέτοιου είδους στοιχεία όπως δημογραφικά και γεωγραφικά δεδομένα, πληροφορίες σχετικά με τον τρόπο ζωής και τα ενδιαφέροντα τους και τις αγοραστικές τους προτιμήσεις, βοηθούν στη διαμόρφωση των εμπορικών πολιτικών και δίνουν τη δυνατότητα στις επιχειρήσεις αυτές να διενεργήσουν στοχευμένες προσφορές, εκδηλώσεις, ή άλλου είδους ενέργειας, κατευθύνοντάς τες στο κατάλληλο κοινό, βάσει των πληροφοριών που συλλέγουν από το facebook.

Κατά συνέπεια, ο φορέας εκμετάλλευσης του μέσου κοινωνικής δικτύωσης (δηλαδή το facebook) και ο διαχειριστής της σελίδας που φιλοξενείται σε αυτό για την επεξεργασία των προσωπικών δεδομένων των επισκεπτών της σελίδας, είναι από κοινού υπεύθυνοι για την τήρηση των προϋποθέσεων προστασίας των προσωπικών δεδομένων των χρηστών. Με την απόφασή του το ΔΕΕ ουσιαστικά καθιστά τους διαχειριστές υπεύθυνους να διασφαλίσουν ότι το Facebook θα παρέχει προς τα υποκείμενα των δεδομένων τις απαραίτητες πληροφορίες προκειμένου να εξασφαλίσουν κι εκείνοι με τη σειρά τους τη νόμιμη συγκατάθεσή για τη συλλογή και επεξεργασία των δεδομένων.

Μάλιστα, στο πλαίσιο επίτευξης της αρχής της συνεκτικότητας, πιθανολογείται η γενίκευση της εφαρμογής των νέων αυτών απαιτήσεων σε όλα τα κράτη- μέλη, τας[70].

Το Δικαστήριο έκρινε ότι, με τον τρόπο αυτό επιτυγχάνεται πληρέστερη προστασία των επισκεπτών τέτοιων σελίδων, σύμφωνα με την Οδηγία 95/46 περί προστασίας των δεδομένων.

---

[69] Δείτε εδώ το κείμενο της απόφασης.
[70] ΔΕΕ υπόθ. C-210/2016, απόφ. της 5.6.2018 (ΔιΜΕΕ 2/2018 με σχόλιο Σπ. Τάσση).

Επιπλέον, το Δικαστήριο με την απόφασή του, ενίσχυσε τη δικαιοδοσία της αρμόδιας αρχής ως εξής:

Στη συγκεκριμένη περίπτωση, ο υπεύθυνος επεξεργασίας (Facebook) είναι εγκατεστημένος εκτός του εδάφους της ΕΕ, αλλά διαθέτει εγκαταστάσεις σε διάφορα κράτη-μέλη.

Ανάμεσα στις εγκαταστάσεις αυτές, ενδέχεται να υπάρχει κάποια, η οποία έχει οριστεί αποκλειστικώς υπεύθυνη για τη συλλογή και την επεξεργασία των δεδομένων προσωπικού χαρακτήρα, σε ολόκληρο το έδαφος της Ένωσης. Στη υπό κρίση υπόθεση, η εγκατάσταση αυτή ήταν η Facebook Ireland. Η Facebook Germany αντίθετα, ήταν ο φορέας εκμετάλλευσης του μέσου κοινωνικής δικτύωσης από το οποίο ο συγκεκριμένος διαχειριστής της σελίδας αντλούσε προσωπικά δεδομένα των χρηστών.

Θα περίμενε κανείς, εφόσον η Facebook Germany είναι επιφορτισμένη μόνο με την πώληση διαφημιστικού χώρου και με άλλες δραστηριότητες μάρκετινγκ στο έδαφος του εν λόγω κράτους μέλους, η αρμόδια γερμανική αρχή, προκειμένου να ασκήσει τις ελεγκτικές της αρμοδιότητες βάσει της Οδηγίας, να καλέσει την ιρλανδική αρχή προστασίας προσωπικών δεδομένων να παρέμβει.

Ωστόσο, το Δικαστήριο έκρινε ότι η γερμανική αρχή μπορεί να στραφεί τόσο κατά του διαχειριστή (Γερμανική επιχείρηση), όσο και κατά του Facebook χωρίς να απαιτείται προηγουμένως να καλέσει την αρχή ελέγχου του άλλου κράτους-μέλους να παρέμβει.

2.4.2 Αποφάσεις και Γνωμοδοτήσεις της Αρχής

Όπως έχουμε ήδη προαναφέρει θεσμικό πλαίσιο για την προστασία προσωπικών στην Ελλάδα ήδη προϋπήρχε και το έργο της ΑΠΔΠΧ ήταν πλούσιο. Στην ενότητα που ακολουθεί παρατίθενται αποφάσεις και γνωμοδοτήσεις της Αρχής, με σκοπό να γίνει κατανοητό το σκεπτικό της, σε σχέση με το σκοπό και τα μέσα επίτευξης της προστασίας των προσωπικών δεδομένων μέχρι σήμερα. Αυτό θεωρούμε ότι θα συμβάλει στην καλύτερη κατανόηση του θεσμικού πλαισίου για τα προσωπικά δεδομένα, αλλά και θα διευκολύνει τους Υπευθύνους Επεξεργασίας για την ορθή εφαρμογή του Κανονισμού, καθώς το πνεύμα των αποφάσεών της που έχουν προηγηθεί χρονολογικά του Κανονισμού, θα μεταφερθεί ενδεχομένως και στην μετέπειτα περίοδο.

2.4.2.1 Απόφαση 19/2017 «Σύσταση για απεγκατάσταση συστήματος βιντεοεπιτήρησης σε συγκρότημα εκπαιδευτικών εγκαταστάσεων»[71]

Υπόθεση

Υποβλήθηκε στην Αρχή ερώτημα από ΙΕΚ, σύμφωνα με το οποίο το ΕΠΑΛ, το οποίο συστεγάζεται με το ΙΕΚ, έχει εγκαταστήσει σύστημα βιντεοεπιτήρησης, που αποτελείται από πέντε κάμερες, οι οποίες βιντεοσκοπούν και καταγράφουν τον χώρο του σχολείου κατά τις βραδινές ώρες, χωρίς να έχει ερωτηθεί και ενημερωθεί το ΙΕΚ. Επίσης, με βάση τα όσα αναφέρονται στην καταγγελία: α) για την λειτουργία του κυκλώματος δεν υπάρχει έγγραφη σχετική άδεια από τη Διεύθυνση Δευτεροβάθμιας Εκπαίδευσης, αλλά προφορική εντολή από τον Δήμαρχο, β) το ωράριο λειτουργίας των καμερών έχει παρουσιαστεί στην καταγγέλλουσα σε τρεις διαφορετικές παραλλαγές, γ) το ΙΕΚ δεν έχει πρόσβαση στον χώρο καταγραφής του υλικού και δ) δεν είναι γνωστός στο ΙΕΚ ο χρόνος διατήρησης του καταγεγραμμένου υλικού.

Απόφαση

Η Αρχή απευθύνει αυστηρή προειδοποίηση προς το ΕΠΑΛ, να προχωρήσει στις ακόλουθες ενέργειες:

α) Να απεγκαταστήσει άμεσα το σύστημα βιντεοεπιτήρησης.

β) Προκειμένου να επιτραπεί η λειτουργία σχετικού συστήματος στο μέλλον, να τηρηθούν οι διατάξεις της Οδηγίας 1/2011. Συγκεκριμένα, να συναποφασίσουν τα όργανα διοίκησης των συστεγαζόμενων ιδρυμάτων, αφού έχουν εκφράσει γνώμη οι σύλλογοι του διδακτικού προσωπικού καθώς και οι εκπαιδευόμενοι.

γ) Σε περίπτωση μελλοντικής νόμιμης λειτουργίας του συστήματος, να διασφαλίσει ότι δεν θα υπάρχει οθόνη παρακολούθησης στο σύστημα, αφού ο σκοπός της εν λόγω επεξεργασίας μπορεί να επιτευχθεί χωρίς τη χρήση οθόνης. Αναφορικά με τη μονάδα αποθήκευσης, τα δεδομένα πρέπει να διαγράφονται κατά την επόμενη εργάσιμη μέρα, εκτός της περίπτωσης συμβάντος, οπότε και θα εφαρμόζονται τα όσα αναφέρονται στις παραγράφους 2, 3, 4 του άρθρου 8 της Οδηγίας 1/2011.

δ) Να ενημερώσει εγγράφως την Αρχή εντός αποκλειστικής προθεσμίας είκοσι ημερών ότι έχει εκπληρώσει τις παραπάνω υποχρεώσεις.

Σκεπτικό

Το σκεπτικό της Αρχής έχει ως εξής:

[71] Δείτε **εδώ** το πλήρες αρχείο.

1. Η λήψη, αποθήκευση ή διαβίβαση εικόνας προσώπου συνιστά επεξεργασία δεδομένων προσωπικού χαρακτήρα, κατά την έννοια του άρθρου 2 στοιχείο δ' του ν. 2472/1997 για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.
2. Βασική προϋπόθεση, κατά το άρθρο 4 παρ. 1 του ν. 2472/1997, για τη νομιμότητα της επεξεργασίας προσωπικών δεδομένων είναι η τήρηση της αρχής της αναλογικότητας, υπό την έννοια ότι τα συλλεγόμενα στοιχεία πρέπει να είναι αναγκαία και πρόσφορα για τον επιδιωκόμενο σκοπό, ο οποίος θα πρέπει να μη δύναται να επιτευχθεί με ηπιότερα μέσα.
3. Το ζήτημα της χρήσης συστημάτων βιντεοεπιτήρησης για το σκοπό της προστασίας προσώπων και αγαθών ρυθμίζεται στην υπ' αριθ. 1/2011 Οδηγία της Αρχής. Όπως επισημαίνεται στο άρθρο 5 αυτής, αναφορικά με την αρχή της αναλογικότητας, τα σημεία εγκατάστασης των καμερών και ο τρόπος λήψης των δεδομένων πρέπει να προσδιορίζονται με τέτοιο τρόπο, ώστε τα δεδομένα που συλλέγονται να μην είναι περισσότερα από όσα είναι απολύτως αναγκαία για την εκπλήρωση του σκοπού της επεξεργασίας και να μη θίγονται τα θεμελιώδη δικαιώματα των προσώπων που ευρίσκονται στο χώρο που επιτηρείται και ιδίως να μην παραβιάζεται αυτό το οποίο μπορεί να θεωρηθεί ως «νόμιμη προσδοκία κάποιου βαθμού προστασίας της ιδιωτικής ζωής» σε κάποιον χώρο (πρβλ. Έγγραφο εργασίας για την επιτήρηση των ηλεκτρονικών επικοινωνιών στον τόπο εργασίας WP55 της 29 Μαΐου 2002 της Ομάδας εργασίας για την προστασία των προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, σελ. 4).
4. Η αρχή της αναλογικότητας, για κάθε επεξεργασία μέσω συστήματος βιντεοπιτήρησης εν όψει του προαναφερθέντος σκοπού, εξειδικεύεται στα άρθρα 6 και 7, αλλά και στο Ειδικό Μέρος της ανωτέρω Οδηγίας. Ειδικότερα, η περίπτωση λειτουργίας συστημάτων βιντεοεπιτήρησης σε σχολεία και λοιπούς χώρους όπου δραστηριοποιούνται ανήλικοι ρυθμίζεται στο άρθρο 18 (Ειδικό Μέρος) της ανωτέρω Οδηγίας. Όπως επισημαίνεται στο άρθρο αυτό, η ύπαρξη και μόνο καμερών σε χώρους όπου δραστηριοποιούνται ανήλικοι χρήζει ιδιαίτερης προσοχής, αφού δεν είναι εύκολο να αξιολογηθούν οι συνέπειες που μια τέτοια επεξεργασία μπορεί να έχει για την ελεύθερη ανάπτυξη της προσωπικότητας των ανηλίκων.

   Η απόφαση για την εγκατάσταση και τη λειτουργία του συστήματος πρέπει να λαμβάνεται από το αρμόδιο όργανο για τη διοίκηση του σχολείου, αφού ληφθεί υπόψη η γνώμη των εκπροσώπων του διδακτικού προσωπικού, του συλλόγου γονέων και των μαθητικών συλλόγων όπου υπάρχουν.

Επίσης, στο ίδιο άρθρο αναφέρεται ότι το σύστημα επιτρέπεται να είναι σε λειτουργία μόνο κατά τις ώρες που το σχολείο δεν λειτουργεί. Οι ώρες λειτουργίας του συστήματος πρέπει να αναγράφονται με σαφήνεια στις σχετικές ενημερωτικές πινακίδες, έτσι ώστε να γνωρίζουν πλήρως όλοι οι μαθητές και οι φορείς της εκπαιδευτικής κοινότητας ότι καθ' όλη τη διάρκεια της παρουσίας τους στο σχολείο δεν παρακολουθούνται. Κατ' εξαίρεση σε περιπτώσεις σχολικών εγκαταστάσεων μεγάλης έκτασης, όπου δεν είναι πρακτικός ο έλεγχος των απομακρυσμένων σημείων των εγκαταστάσεων με ηπιότερα μέσα (π.χ. φύλακες), είναι δυνατόν να επιτραπεί η λειτουργία των καμερών που εστιάζουν στα απομακρυσμένα σημεία και κατά τις ώρες λειτουργίας του σχολείου, μετά από έγκριση της Αρχής.

Τα δεδομένα που καταγράφουν οι κάμερες πρέπει να διαγράφονται κατά την επόμενη εργάσιμη μέρα. Σε περίπτωση συμβάντος εφαρμόζονται οι παράγραφοι 2, 3 και 4 του άρθρου 8. Η διαχείριση του συστήματος μπορεί να πραγματοποιείται μόνο από εξουσιοδοτημένο πρόσωπο.

Η απόφαση για την εγκατάσταση και τη λειτουργία του συστήματος πρέπει να λαμβάνεται από το αρμόδιο όργανο για τη διοίκηση του σχολείου, αφού ληφθεί υπόψη η γνώμη των εκπροσώπων του διδακτικού προσωπικού, του συλλόγου γονέων και των μαθητικών συλλόγων όπου υπάρχουν.

Προτείνεται η λειτουργία του συστήματος να πραγματοποιείται κατ' αρχήν δοκιμαστικά, αφού προηγουμένως γνωστοποιηθεί στην Αρχή, σύμφωνα με το άρθρο 10 της παρούσας Οδηγίας, προκειμένου να διαπιστωθεί η αποτελεσματικότητά του σε σχέση με τον επιδιωκόμενο σκοπό και τις επιπτώσεις του στην ανάπτυξη της προσωπικότητας και την ιδιωτική ζωή των μαθητών. Στη συνέχεια η λειτουργία του συστήματος πρέπει να αξιολογείται από τον υπεύθυνο επεξεργασίας κατά τακτά χρονικά διαστήματα που δεν μπορούν να υπερβαίνουν το ένα έτος, και να σταθμίζεται κάθε φορά εκ νέου η αναγκαιότητα λειτουργίας του. Τα στοιχεία τα σχετικά με την αξιολόγηση του συστήματος πρέπει να είναι διαθέσιμα στην Αρχή. Οι μαθητές, οι γονείς τους, οι εκπαιδευτικοί και οι λοιποί εργαζόμενοι στο σχολείο μπορούν να έχουν πρόσβαση σε αυτά.

5. Από το συνδυασμό των ανωτέρω προκύπτει ότι στην περίπτωση που στον ίδιο χώρο συστεγάζονται περισσότερα του ενός εκπαιδευτικά ιδρύματα, δεν μπορεί μόνο ένα από αυτά να θεωρηθεί αποκλειστικά υπεύθυνος επεξεργασίας του εν λόγου χώρου, ή ακόμα και εάν θεωρηθεί δεν μπορεί να μην ληφθεί υπόψη η γνώμη των εκπροσώπων του διδακτικού προσωπικού καθώς και των εκπαιδευόμενων του συνόλου των συστεγαζόμενων ιδρυμάτων.

Συνεπώς, σε περίπτωση συστέγασης τα συστεγαζόμενα ιδρύματα πρέπει να έχουν όχι μόνο ενημερωθεί για την λειτουργία ενός τέτοιου συστήματος, αλλά και συναποφασίσει μέσω των οργάνων διοίκησής τους, αφού προηγουμένως έχουν εκφράσει γνώμη οι εκπρόσωποι του διδακτικού προσωπικού και οι εκπαιδευόμενοι.

6. Αναφορικά με την λειτουργία οθόνης παρακολούθησης στο γραφείο διεύθυνσης του ΕΠΑΛ, σημειώνεται, επίσης, ότι δεν είναι σύμφωνη με την αρχή της αναλογικότητας, σύμφωνα και με τα όσα αναφέρονται στο άρθρο 15 της Οδηγίας σχετικά με την εγκατάσταση συστήματος παρακολούθησης σε συγκροτήματα κατοικιών ή γραφείων.
7. Από τα παραπάνω στοιχεία, προκύπτουν τα εξής:

   Το εν λόγω σύστημα ήταν σε λειτουργία, χωρίς να έχει ενημερωθεί και συναποφασίσει για αυτό το ΙΕΚ.

   Το εν λόγω σύστημα βιντεοεπιτήρησης δεν πληροί τις προϋποθέσεις νομιμότητας που τίθενται στο άρθρο 18 της Οδηγίας 1/2011 της Αρχής, αφού δεν έχει ληφθεί σύμφωνα με αποφάσεις των οργάνων διοίκησης και των δύο σχολείων λαμβάνοντας υπόψη την γνώμη των εκπροσώπων του συνόλου του διδακτικού προσωπικού και των εκπαιδευομένων.

   Δευτερευόντως, η οθόνη παρακολούθησης ήταν στο γραφείο της Διεύθυνσης του ΕΠΑΛ, χωρίς έχουν διαμορφωθεί κατάλληλες προϋποθέσεις πρόσβασης στο ΙΕΚ.

   Τέλος, η ώρα έναρξης λειτουργίας του συστήματος, όπως αναφέρθηκε σε τηλεφωνικές επικοινωνίες της διευθύντριας του ΙΕΚ με τους εμπλεκόμενους παρουσιάστηκε να κυμαίνεται από τις 21:00 έως τις 22:00. Ως εκ τούτου, συνάγεται ότι έχουν παραβιασθεί και οι θεμελιώδεις επιταγές, που οι διατάξεις του άρ. 4 του ν. 2472/1997 θέτουν για τη νομιμότητα κάθε συλλογής και επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

2.4.2.2 Απόφαση 140/2017 «Μη εφαρμογή κατάλληλων μέτρων για την ταυτοποίηση συνδρομητή, με αποτέλεσμα περιστατικό παραβίασης προσωπικών δεδομένων»[72]

Υπόθεση

Η Αρχή έλαβε καταγγελία του Α (εφεξής «καταγγέλλων») κατά της «Vodafone - Πάναφον» (εφεξής «υπεύθυνος επεξεργασίας») σχετικά με μεταφορά του

[72] Δείτε **εδώ** το πλήρες αρχείο.

τηλεφωνικού του αριθμού σε τρίτο κατόπιν λανθασμένης ταυτοποίησης του συνδρομητή.

Σύμφωνα με τον καταγγέλλοντα, τρίτος, φέρων το ίδιο όνομα και επώνυμο αλλά διαφορετικό πατρώνυμο, προσήλθε σε κατάστημα του υπευθύνου επεξεργασίας και προμηθεύτηκε κάρτα sim με τον τηλεφωνικό αριθμό του καταγγέλλοντος. Την χρησιμοποίησε για περίπου δέκα ημέρες, κατά τις οποίες ελάμβανε τις κλήσεις που προορίζονταν για τον καταγγέλλοντα από συγγενικά του πρόσωπα. Μετά από επίσκεψη του καταγγέλλοντος σε κατάστημα του υπευθύνου του επεστράφη ο τηλεφωνικός του αριθμός. Ο υπεύθυνος επεξεργασίας δήλωσε ότι η ταυτοποίηση του τρίτου κατά τον καταγγέλλοντα έγινε με επίδειξη του δελτίου αστυνομικής ταυτότητας. Τηρούσε στο σύστημά του τον ΑΔΤ του καταγγέλλοντος ο οποίος όμως είχε αλλάξει από το 2014, χωρίς ο καταγγέλλων να ενημερώσει, ως όφειλε, τον υπεύθυνο επεξεργασίας για την αλλαγή αυτή.

Η Αρχή απέστειλε έγγραφο με το οποίο ζητήθηκαν απόψεις του υπευθύνου επεξεργασίας όσον αφορά τον τρόπο ταυτοποίησης του συνδρομητή, τη διαβίβαση δεδομένων του σε τρίτο, την ακρίβεια των δεδομένων που τηρούνται για το συγκεκριμένο συνδρομητή, καθώς και τις επιπτώσεις στην ιδιωτική ζωή των εμπλεκομένων. Ο υπεύθυνος επεξεργασίας απάντησε με υπόμνημα μέσω του οποίου επαναλαμβάνει τις απόψεις που περιλαμβάνονται στην καταγγελία, δηλαδή αρνείται ότι υπήρξε το περιστατικό λάθους ταυτοποίησης.

Απόφαση

Η Αρχή λαμβάνοντας υπόψη τα ανωτέρω,

α) Επιβάλλει στην εταιρεία «Vodafone-Πάναφον» διοικητικό πρόστιμο δύο χιλιάδων (2.000) ευρώ για παραβίαση του άρθρου 10 του ν. 2472/1997, αφού δεν εφαρμόστηκαν τα κατάλληλα οργανωτικά μέτρα ασφάλειας για την ταυτοποίηση του συνδρομητή, με αποτέλεσμα περιστατικό παραβίασης προσωπικών δεδομένων.

β) Απευθύνει σύσταση για την προσαρμογή της διαδικασίας ταυτοποίησης των συνδρομητών όταν επισκέπτονται με φυσική παρουσία καταστήματα του υπευθύνου επεξεργασίας και τον αυστηρό έλεγχο τήρησής τους.

Σκεπτικό

Το σκεπτικό της Αρχής έχει ως εξής:

1. Στο άρθρο 2 στοιχ. α΄ και γ΄ του ν. 2472/1997 ορίζονται οι έννοιες των απλών δεδομένων και του υποκειμένου αυτών αντίστοιχα, ενώ στο στοιχ. δ΄ του ίδιου άρθρου ορίζεται και η έννοια της επεξεργασίας, στην οποία

συμπεριλαμβάνονται *«η συλλογή, …, η διατήρηση ή αποθήκευση, …, η χρήση, …, η διαγραφή, η καταστροφή.»*. Ακολούθως, στο άρθρο 4 του ν. 2472/1997 ορίζονται οι βασικές αρχές της επεξεργασίας, ενώ στο άρθρο 5 του ίδιου Νόμου ορίζονται οι επιμέρους προϋποθέσεις για τη νομιμότητά της.

2. Επιπρόσθετα, στο άρθρο 10 του ίδιου Νόμου ορίζονται οι υποχρεώσεις του υπεύθυνου επεξεργασίας και του εκτελούντος την επεξεργασία σχετικά με το απόρρητο και την ασφάλεια της επεξεργασίας, από όπου προκύπτει ρητά ότι ουσιώδες στοιχείο της νόμιμης επεξεργασίας είναι η λήψη των κατάλληλων μέτρων ασφάλειας και ο έλεγχος αυτών από τον υπεύθυνο επεξεργασίας. Τα μέτρα ασφάλειας πρέπει α) να διασφαλίζουν ότι τα δεδομένα χρησιμοποιούνται μόνον για τον εκάστοτε επιδιωκόμενο σκοπό και β) να εξασφαλίζουν επίπεδο ασφάλειας ανάλογο προς τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των δεδομένων που είναι αντικείμενο της επεξεργασίας λαμβάνοντας υπόψη τις τεχνολογικές εξελίξεις και το κόστος (βλ., ενδεικτικά, Απόφαση 1/2015 της Αρχής).
3. Η διαδικασία που ακολουθεί ο υπεύθυνος επεξεργασίας για την ταυτοποίηση του συνδρομητή, ως οργανωτικό μέτρο ασφάλειας, πρέπει να είναι επαρκής και να εφαρμόζεται σωστά, ώστε να μην έχουν ως αποτέλεσμα κάποιο περιστατικό παραβίασης προσωπικών δεδομένων, όπως αυτό που περιγράφεται στην καταγγελία. Επίσης, όταν ο υπεύθυνος επεξεργασίας λάβει γνώση ενός τέτοιου περιστατικού θα πρέπει να το εξετάσει ενδελεχώς και να επικοινωνήσει με το θύμα της άστοχης εφαρμογής της διαδικασίας ταυτοποίησης, ενημερώνοντάς το για τις συνθήκες του περιστατικού, την έκτασή του και κάνοντας εκ των υστέρων ενέργειες προκειμένου να μειώσει τον όποιο αντίκτυπο από την παράνομη επεξεργασία αυτή στην ιδιωτικότητα και την προσωπικότητά του.
4. Στη συγκεκριμένη περίπτωση ο υπεύθυνος επεξεργασίας με τα υπομνήματά του ισχυρίζεται ότι δεν έχει συμβεί λάθος στην ταυτοποίηση του συνδρομητή, και ότι ο ίδιος ο καταγγέλλων ζήτησε να του δοθεί καινούρια κάρτα sim. Επισημαίνει επίσης ότι δεν υπάρχουν στοιχεία που να τεκμηριώνουν ότι πραγματοποιήθηκε λάθος ταυτοποίηση και ότι ακόμη και εάν υποτεθεί ότι έγινε, η υπαιτιότητα είναι του καταγγέλλοντος, διότι δεν ενημέρωσε εγκαίρως ως όφειλε σχετικά με την αλλαγή της αστυνομικής του ταυτότητας.
5. Από το περιεχόμενο της καταγγελίας, και λαμβάνοντας υπόψη τα όσα προφορικά αναφέρθηκαν εκ μέρους του καταγγέλλοντος κατά τη

συνεδρίαση της 05-07-2017, προκύπτει ότι πράγματι έγινε λάθος ταυτοποίηση, διότι κατά το επίμαχο δεκαήμερο ο τρίτος στον οποίο χορηγήθηκε λόγω πλημμελούς ταυτοποίησης η κάρτα SIM και ο τηλεφωνικός αριθμός που ανήκε στον καταγγέλλοντα απαντούσε σε κλήσεις που έκαναν φιλικά ή συγγενικά πρόσωπα στον καταγγέλλοντα και μάλιστα τους έλεγε ότι ο αριθμός του ανήκει και κακώς ισχυρίζεται ο καταγγέλλων ότι είναι δικός του. Αυτό καταδεικνύει ότι τον αριθμό προηγουμένως τον είχε ο καταγγέλλων και από λάθος ταυτοποίηση δόθηκε στον τρίτο. Άλλωστε όταν υπέπεσε στην αντίληψη του καταγγέλλοντος η παραχώρηση του αριθμού του σε τρίτο πρόσωπο και διαμαρτυρήθηκε στον υπεύθυνο επεξεργασίας, έσπευσαν και του έδωσαν τον αριθμό που του ανήκε, αναγνωρίζοντας έτσι το σφάλμα τους. Όσον αφορά τον ισχυρισμό του υπευθύνου επεξεργασίας ότι δεν είχε ενημερωθεί ο ΑΔΤ του καταγγέλλοντος στα συστήματά της από δική του υπαιτιότητα, δε αίρεται η υπαιτιότητα του υπευθύνου επεξεργασίας για τη μη ορθή ταυτοποίηση του τρίτου ατόμου στο οποίο χορηγήθηκε κατά την αλλαγή της κάρτας ο τηλεφωνικός αριθμός του καταγγέλλοντος, ενόψει του ότι το Δελτίο ταυτότητας που έφερε ο τρίτος οπωσδήποτε δεν είχε τον αυτό αριθμό, αλλά και ούτε τα λοιπά στοιχεία, τα οποία δεν ελεγχθήκαν, όπως το πατρώνυμο του ατόμου που τους επέδειξε το ΑΔΤ, το οποίο διέφερε με τα στοιχεία που είχαν καταχωρημένα στο σύστημα. Ενόψει του ότι πραγματοποιήθηκε η παράδοση της κάρτας στο τρίτο πρόσωπο η ταυτοποίηση που διενεργήθηκε από τον υπεύθυνο επεξεργασίας κρίνεται ως πλημμελής και ελλιπής.

Κατ' ακολουθία των ανωτέρω πρέπει, κατ' εφαρμογή της διατάξεως του άρθρου 21 παρ. 1 εδαφ. β΄ και ε΄ ν. 2472/1997, να επιβληθούν οι διοικητικές κυρώσεις που αναφέρονται στο διατακτικό, λαμβανομένης υπόψη και της βαρύτητας της παράβασης.

2.4.2.3 Γνωμοδότηση 4/2017 «Επανεξέταση γνωστοποίησης του ΟΑΣΑ για επεξεργασία προσωπικών δεδομένων στο πλαίσιο του Ενιαίου Αυτόματου Συστήματος Συλλογής Κομίστρου (Ηλεκτρονικό Εισιτήριο)»[73] και Γνωμοδότηση 1/2017 «Γνωστοποίηση επεξεργασίας προσωπικών δεδομένων στο πλαίσιο του Ηλεκτρονικού Εισιτηρίου του ΟΑΣΑ»[74]

Υπόθεση

Η υπόθεση ξεκίνησε όταν, στις 14 Σεπτεμβρίου 2016, ο ΟΑΣΑ προέβη ως όφειλε, βάσει του σχετικού νομικού πλαισίου, σε γνωστοποίηση προς την ΑΠΔΠΧ, σχετικά με την επεξεργασία προσωπικών δεδομένων στο πλαίσιο του νέου Ενιαίου Αυτόματου Συστήματος Συλλογής Κομίστρου (δηλαδή το γνωστό «ηλεκτρονικό εισιτήριο»).

Με τη γνωστοποίηση αυτή, ο ΟΑΣΑ ενημέρωνε την Αρχή ότι, για τους σκοπούς υλοποίησης του νέου συστήματος, ήταν απαραίτητη η «προσωποποίηση-ταυτοποίηση» των επιβατών μέσω της συλλογής και επεξεργασίας προσωπικών δεδομένων τους όπως ο Αριθμός Μητρώου Κοινωνικής Ασφάλισης (ΑΜΚΑ), το ονοματεπώνυμο, η διεύθυνση κατοικίας κ.ά.

Κατά την εξέταση της γνωστοποίησης από την ΑΠΔΠΧ, τόσο ο τρόπος επεξεργασίας των δεδομένων, όσο και οι σκοποί της επεξεργασίας θεωρήθηκαν ασαφείς. Κατά συνέπεια ζητήθηκαν διευκρινίσεις αναφορικά με το είδος των προσωπικών δεδομένων που θα υφίστανται επεξεργασία, τον τύπο της επεξεργασίας αυτής, τη διαδικασία εγγραφής του χρήστη, τους μηχανισμούς αυθεντικοποίησης, την εξειδίκευση των τηρούμενων δεδομένων, την τήρηση ιστορικότητας των διαδρομών των χρηστών, τα μέτρα ασφάλειας, καθώς και αναφορικά και με τον υποχρεωτικό ή μη χαρακτήρα της διαδικασίας.

Ακολούθησε προφορική ακρόαση και υποβολή εγγράφου με τις τεχνικές προδιαγραφές του συστήματος προκειμένου να παρασχεθούν από την πλευρά του ΟΑΣΑ οι σχετικές απαντήσεις στα ερωτήματα της Αρχής, οι οποίες ωστόσο δεν κρίθηκαν επαρκείς. Για το λόγο αυτό, η Αρχή ζήτησε περαιτέρω αποσαφήνιση ως προς τους διακριτούς σκοπούς επεξεργασίας, το είδος των προσωπικών δεδομένων που απαιτούνται για την επίτευξη του κάθε σκοπού ξεχωριστά αλλά και τον αναγκαίο χρόνο τήρησής τους, καθώς επίσης και τη συσχέτιση του μοναδικού σειριακού αριθμού της κάρτας του ηλεκτρονικού εισιτηρίου με τον κάτοχό του βάσει των στοιχείων που

73 Δείτε **εδώ** το πλήρες αρχείο.
74 Δείτε **εδώ** το πλήρες αρχείο.

τηρούνται στη βάση δεδομένων, υπό το πρίσμα του ότι μία τέτοια συσχέτιση επιτρέπει να εξαχθεί προσωποποιημένη αναλυτική πληροφορία για τις διαδρομές που πραγματοποιεί κάθε επιβάτης.

Στις 20 Ιανουαρίου του 2017, εκδόθηκε η υπ΄ αριθμ 1/2017 γνωμοδότηση της Αρχής η οποία, στη βάση του σκεπτικού που αναπτύσσεται κατωτέρω, κάλεσε τον ΟΑΣΑ στην υποβολή νέας γνωστοποίησης.

Σε συμμόρφωση με την ανωτέρω σύσταση της Αρχής, ο ΟΑΣΑ ανακάλεσε την προηγούμενη γνωστοποίηση και προέβη στην υποβολή νέας, βάσει της οποίας η επεξεργασία των προσωπικών δεδομένων θα γίνεται στη βάση δύο συστημάτων: α) το **«πολλαπλό» σύστημα** το οποίο περιλαμβάνει μια «έξυπνη» μη προσωποποιημένη κάρτα χωρίς επαφή (Contactless Smart Card-SC) στην οποία θα αποθηκεύονται εισιτήρια μικρής αξίας και β) την «**κάρτα**», δηλαδή μια προσωποποιημένη «έξυπνη» κάρτα χωρίς επαφή (Contactless Smart Card - SC) με μικροεπεξεργαστή η οποία θα υποκαταστήσει τις υφιστάμενες μηνιαίες, τριμηνιαίες, εξαμηνιαίες, ετήσιες κάρτες και ελευθέρας.

Σύμφωνα με τη νέα γνωστοποίηση, για την έκδοση, φόρτιση και επικύρωση της κάρτας μοναδικό στοιχείο καταχώρισης και επεξεργασίας θα είναι ο αριθμός της και όχι τα στοιχεία του επιβάτη, ενώ δεν απαιτείται ταύτιση με φυσικό πρόσωπο. Επίσης, κάθε καταγραφή δεδομένων κίνησης των προσωποποιημένων καρτών δεν θα παραπέμπει σε συγκεκριμένο πρόσωπο αλλά σε ένα «ψηφιακό αποτύπωμα» (hash value) το οποίο θα αποτελείται από τον ΑΜΚΑ των Ελλήνων πολιτών ή τον αριθμό διαβατηρίου των αλλοδαπών φυσικών προσώπων και ένα τετραψήφιο κωδικό ασφαλείας, εξασφαλίζει ότι ούτε χρήστες με γνώση της δομής του συστήματος και διαβαθμισμένη πρόσβαση στα δεδομένα αυτού θα είναι σε θέση να προσδιορίσουν την αντιστοιχία αριθμού κάρτας με τον ΑΜΚΑ (και κατά συνέπεια την ταυτότητα) του επιβάτη. Τέλος, η διαδικασία έκδοσης της κάρτας δεν απαιτεί οποιαδήποτε αποθήκευση προσωπικών δεδομένων πλην της καταχώρισης του ΑΜΚΑ για τις ειδικές κατηγορίες, η οποία απαιτείται για λόγους αποτροπής έκδοσης περισσότερων αντιγράφων της κάρτας. Καταλήγοντας, μετά την περιγραφή των ειδικότερων τεχνικών λεπτομερειών του σχεδιασμού του συστήματος, ο ΟΟΣΑ συμπεραίνει, σύμφωνα με τη γνωστοποίησή του, ότι κατοχυρώνει τη δυνατότητα των επιβατών σε πλήρως ανωνυμοποιημένη χρήση των αστικών συγκοινωνιών και εξασφαλίζει την ανωνυμία του χρήστη ακόμα και στην περίπτωση ειδικών κατηγοριών προϊόντων.

Απόφαση

Η ΑΠΔΠΧ για την έκδοση των γνωμοδοτήσεων της στηρίχθηκε στην, βάσει του ν. 2472/1997, αρμοδιότητά της να «γνωμοδοτεί για κάθε ρύθμιση που αφορά την επεξεργασία και προστασία δεδομένων προσωπικού χαρακτήρα» καθώς και στην προβλεπόμενη στο άρθρο 28 της Οδηγίας 95/46/ΕΚ υποχρέωση για έγκαιρη αναζήτηση της γνώμης της Αρχής κατά τον προγραμματισμό λήψης ή αναθεώρησης υφιστάμενων κανονιστικών ρυθμίσεων και διοικητικών μέτρων, καθώς και κατά το σχεδιασμό συγκεκριμένων συστημάτων που ενέχουν επεξεργασία προσωπικών δεδομένων.

Στο πλαίσιο αυτό, κατά την εξέταση της πρώτης υπόθεσης έκρινε ότι, τα χαρακτηριστικά της συγκεκριμένης επεξεργασίας (πληθώρα δεδομένων που αφορά σε ευρύ κοινό, επίτευξη πολλών διαφορετικών σκοπών) επιβάλουν την εκπόνηση έκθεσης εκτίμησης επιπτώσεων στην προστασία των προσωπικών δεδομένων προκειμένου να καταδειχθούν και να αντιμετωπιστούν όλα τα ζητήματα που εγείρονται ως προς την προστασία των προσωπικών δεδομένων και τη λήψη όλων των απαραίτητων μέτρων. Σύμφωνα με το διατακτικό της απόφασης, ο υπεύθυνος επεξεργασίας οφείλει να προβεί στην τήρηση όλων των βασικών προϋποθέσεων νομιμότητας της επεξεργασίας και στη συνέχεια, να υποβάλει νέα γνωστοποίηση.

Στην περίπτωση της δεύτερης γνωστοποίησης του ΟΑΣΑ, η Αρχή γνωμοδότησε θετικά, θεωρώντας ότι το νέο σύστημα έχει εναρμονιστεί σε ικανοποιητικό βαθμό με τις προϋποθέσεις που έθεσε στη Γνωμοδότηση 1/2017. Τόνισε ωστόσο ότι θα πρέπει να γίνουν οι κατάλληλες τροποποιήσεις του συστήματος, ώστε να διασφαλίζεται το δικαίωμα της ανώνυμης μετακίνησης, καθώς δεν μπορεί να αποκλειστεί το ενδεχόμενο, για κάποιες τιμές του ΑΜΚΑ, να προσδιοριστεί μονοσήμαντα το ποια είναι η κάρτα που αντιστοιχεί σε κάθε έναν από τους χρήστες με τις τιμές του ΑΜΚΑ – δηλαδή τελικά να αναγνωριστούν οι κάτοχοι συγκεκριμένων καρτών. Ακόμα, επανέφερε την ανάγκη εκπόνησης μελέτης εκτίμησης επιπτώσεων με τα εξής, τουλάχιστον, στοιχεία: α) συστηματική περιγραφή των προβλεπόμενων πράξεων επεξεργασίας και των σκοπών της επεξεργασίας, β) εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας σε συνάρτηση με τους επιδιωκόμενους σκοπούς, γ) εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων, και δ) τα προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων, περιλαμβανομένων των εγγυήσεων, των μέτρων και μηχανισμών ασφάλειας (όπως ανωνυμοποίηση ή/και ψευδωνυμοποίηση), ώστε να διασφαλίζεται η προστασία των δεδομένων προσωπικού χαρακτήρα. Αναφορικά με τη

δυνατότητα ηλεκτρονικής -μέσω διαδικτύου-υποβολής αίτησης για την έκδοση ηλεκτρονικού εισιτηρίου, η Αρχή έκρινε, ότι «δεν προσκρούει στις θεμελιώδεις αρχές της προστασίας προσωπικών δεδομένων» και συνεπώς επέτρεψε ρητά την συγκεκριμένη μέθοδο.

Σκεπτικό

Βάσει της αρχικής γνωστοποίησης, οι σκοποί για τους οποίους ο ΟΑΣΑ σκόπευε να επεξεργάζεται τα προσωπικά δεδομένα των υποκειμένων ήταν:

α) Η αποφυγή επιβίβασης σε μέσο μεταφοράς χωρίς την καταβολή του προβλεπόμενου κομίστρου
β) Η παροχή νέων υπηρεσιών στο επιβατικό κοινό
γ) Η διευκόλυνση της διαδικασίας ελέγχου παραβάσεων και επιβολής προστίμου
δ) Η παροχή δυνατότητας στον ΟΑΣΑ να εξάγει στατιστικές πληροφορίες που θα του επιτρέψουν να βελτιώσει τις υπηρεσίες του και
ε) Η παροχή της δυνατότητας στον ΟΑΣΑ να γνωρίζει επακριβώς το πλήθος των μετακινήσεων για τις κατηγορίες επιβατών για τους οποίους είναι υποχρεωμένοι οι Δημόσιοι Φορείς, υπό την εποπτεία των οποίων βρίσκονται, να αποζημιώνουν τον ΟΑΣΑ για το μεταφορικό έργο που παρέχει.

Η Αρχή συνεπώς, διερεύνησε τη νομιμότητα της επεξεργασίας ως προς το αν ήταν **αναγκαία για την επίτευξη του επιδιωκόμενου σκοπού** καθώς και ως προς το αν ο συγκεκριμένος σκοπός ήταν **δυνατό να επιτευχθεί με λιγότερο επαχθή** μέσα. Στο πλαίσιο αυτό διερεύνησε:

α) αν η συλλογή των δεδομένων έγινε με **θεμιτό και νόμιμο τρόπο (αρχή της θεμελίωσης της επεξεργασίας στο νόμο)**, για **καθορισμένους, σαφείς και νόμιμους σκοπούς (αρχή του σκοπού)**, καθώς και εάν η επεξεργασία ενόψει των σκοπών αυτών ήταν **θεμιτή και νόμιμη (αρχή της αναλογικότητας της επεξεργασίας).** Ως προς το στοιχείο αυτό, η Αρχή κατέληξε ότι **οι συγκεκριμένοι σκοποί ήταν καθορισμένοι, σαφείς, θεμιτοί και νόμιμοι,** εντάσσονται στις αρμοδιότητες του ΟΑΣΑ όπως αυτές προβλέπονται στις διατάξεις που διέπουν τη λειτουργία του ενώ **η επίτευξη τους χωρίς τη χρήση ηλεκτρονικού εισιτηρίου είναι εξαιρετικά δυσχερής –σε ορισμένες περιπτώσεις δε και αδύνατη–** με την υπάρχουσα έγχαρτη μορφή των εισιτηρίων για τα Μέσα Μαζικής Μεταφοράς που τελούν υπό την εποπτεία του.

β) εάν **τα δεδομένα ήταν συναφή, πρόσφορα, και όχι περισσότερα από όσα απαιτούνταν εν όψει των σκοπών της επεξεργασίας (αρχή της ελαχιστοποίησης των δεδομένων για την επίτευξη του επιδιωκόμενου σκοπού)** και γ) αν ο ΟΑΣΑ έλαβε **τα κατάλληλα οργανωτικά και τεχνικά μέτρα** για την **ασφάλεια των δεδομένων και την προστασία τους** από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας εξασφαλίζοντας **επίπεδο ασφαλείας ανάλογο προς τους κινδύνους** που συνεπάγεται η επεξεργασία και η φύση των δεδομένων.

Για την εκτίμηση της συνδρομής των συγκεκριμένων προϋποθέσεων, η Αρχή έλαβε υπόψη τον καθολικά υποχρεωτικό χαρακτήρα του νέου συστήματος καθώς και το γεγονός ότι αφορά μεγάλο αριθμό υποκειμένων των δεδομένων, κρίνοντας ότι **είναι απολύτως αναγκαίο** κατά το σχεδιασμό του ηλεκτρονικού συστήματος **να διασφαλίζεται ότι πληρούνται οι κατάλληλες προϋποθέσεις για την αντιμετώπιση των κινδύνων ως προς την προστασία των προσωπικών δεδομένων (προστασία των δεδομένων ήδη από το σχεδιασμό - data protection by design.** Έτσι, έκρινε ότι η συλλογή δεδομένων σχετικά με τις διαδρομές που πραγματοποιεί ο εκάστοτε επιβάτης συνεπάγεται κινδύνους για την ελευθερία κίνησης που αποτελεί έκφανση των συνταγματικά κατοχυρωμένων δικαιωμάτων της ελεύθερης ανάπτυξης της προσωπικότητας και της εν γένει προσωπικής ελευθερίας ενώ το γεγονός ότι το εισιτήριο είναι προσωποποιημένο οδηγεί σε απώλεια της ανωνυμίας των επιβατών, με συνέπεια να θίγεται υπέρμετρα το δικαίωμα της πληροφοριακής αυτοδιάθεσης και το δικαίωμα στην ιδιωτική ζωή.

Αντίθετα, στην περίπτωση της δεύτερης γνωστοποίησης, η Αρχή εκτίμησε θετικά ότι α) έχει περιοριστεί το σύνολο των προσωπικών δεδομένων που συλλέγει και επεξεργάζεται ο ΟΑΣΑ εν όψει των επιδιωκόμενων σκοπών, β) ως σχεδιαστικός στόχος τέθηκε η αντιμετώπιση των κινδύνων για την προστασία των προσωπικών δεδομένων που περιέγραψε στην αρχική της Γνωμοδότηση 1/2017, γ) προβλέπεται η δημιουργία ψηφιακού αποτυπώματος με την εισαγωγή κωδικού που θα γνωρίζει μόνο ο χρήστης, δ) η νέα γνωστοποίηση περιέχει όλες τις πληροφορίες που προσδιορίζονται στο άρ. 6 του ν. 2472/1997 και τέλος ε) η αξιοποίηση της διαδικτυακής υπηρεσίας της ΗΔΙΚΑ για τον σκοπό της ακρίβειας των προσωπικών δεδομένων δεν προσκρούει στις θεμελιώδεις αρχές της προστασίας προσωπικών δεδομένων αφού μια τέτοια επεξεργασία γίνεται για σαφή, θεμιτό και νόμιμο σκοπό και δεν έχει ως αποτέλεσμα

τη συλλογή, από πλευράς ΟΑΣΑ, περισσότερων προσωπικών δεδομένων από όσα απαιτούνται για την επίτευξη των επιδιωκόμενων σκοπών του.

Ωστόσο, ως προς τη σύστασή της για εκπόνηση έκθεσης εκτίμησης επιπτώσεων, η Αρχή θεώρησε ότι είναι απαραίτητο να καταδειχτούν και να αντιμετωπιστούν όλα τα ζητήματα που εγείρονται ως προς την προστασία των δεδομένων.

2.4.2.4 Απόφαση 34/2018 «Έλεγχος ηλεκτρονικού υπολογιστή εργαζομένου από τον εργοδότη»[75]

Υπόθεση

Η υπόθεση αφορά στην προσφυγή του Α κατά της εταιρείας Ν. ΚΡΗΤΙΚΟΣ - Γ. ΝΤΑΪΡΤΖΕΣ Α.Ε. ΕΜΠΟΡΙΟ ΧΑΡΤΟΥ στην οποία εργαζόταν ως βοηθός λογιστή.
Κατά τους ισχυρισμούς του, όσο απουσίαζε με αναρρωτική άδεια και χωρίς να έχει προηγουμένως ενημερωθεί και δώσει τη συγκατάθεσή του, η εταιρεία προέβη σε έλεγχο του εταιρικού ηλεκτρονικού του υπολογιστή και αφαίρεση του σκληρού δίσκου, ενώ προσπάθησε να ανακτήσει διαγραφέντα αρχεία του.

Ο ίδιος όταν πληροφορήθηκε εκ των υστέρων για το γεγονός, διαμαρτυρήθηκε ζητώντας τη διακοπή της επεξεργασίας καθώς ανάμεσα στα αρχεία υπήρχαν και προσωπικά του δεδομένα στα οποία επιθυμούσε να έχει πρόσβαση και ζήτησε πληροφορίες για το σκοπό και τη χρονική διάρκεια της επεξεργασίας, τους αποδέκτες των δεδομένων κ.ά.

Δήλωσε ακόμα ότι ουδέποτε ενημερώθηκε πως απαγορεύεται να αποθηκεύσει στον εταιρικό Η/Υ προσωπικά του δεδομένα, ότι η εταιρία δεν διαθέτει σχετικό εσωτερικό Κανονισμό, ούτε περιλαμβανόταν σχετική πρόβλεψη στη σύμβαση εργασίας που υπέγραψε, ενώ ουδέποτε ενημερώθηκε για το ενδεχόμενο και τη δυνατότητα πρόσβασης της εταιρίας στον υπολογιστή που χρησιμοποιούσε για την επεξεργασία μη επαγγελματικών αρχείων.

Η εταιρεία από την πλευρά της αμφισβήτησε τον ισχυρισμό περί απουσίας του Α λόγω αναρρωτικής άδειας αντιλέγοντας ότι ο τελευταίος είχε αποχωρήσει οικειοθελώς από την εταιρεία, έχοντας προηγουμένως προβεί σε παράνομες πράξεις παραβιάζοντας το καθήκον πίστης προς αυτήν.

---

75 Δείτε **εδώ** το πλήρες αρχείο.

Όπως ισχυρίστηκε, το γεγονός αυτό κατέστησε αναγκαίο τον έλεγχο στα αρχεία του ενώ τόσο ο ηλεκτρονικός υπολογιστής όσο και τα περιεχόμενα σε αυτόν έγγραφα και αρχεία ανήκουν στην περιουσία της και συνεπώς η αποθήκευση προσωπικών δεδομένων του χωρίς την προηγούμενη ενημέρωση και έγκρισή της, συνιστά παράνομη ενέργεια.

Τέλος, υποστήριξε ότι ουδέποτε είχε ενημερωθεί από τον προσφεύγοντα για την από μέρους του τυχόν αποθήκευση προσωπικών δεδομένων του σε ηλεκτρονικό υπολογιστή ιδιοκτησίας της, ούτε διαπιστώθηκε τέτοια αποθήκευση δεδομένων και ότι σε κάθε περίπτωση είχε δικαίωμα πρόσβασης σε εταιρικά δεδομένα που ήταν αποθηκευμένα σε εταιρικό υπολογιστή, καθώς και σε ηλεκτρονική αλληλογραφία από και προς εταιρική ηλεκτρονική διεύθυνση. Μάλιστα, η εταιρία υποστήριξε ότι είχε λάβει την συγκατάθεση του πατέρα του προσφεύγοντος, τότε προέδρου της εταιρίας, προς έλεγχο του επίδικου ηλεκτρονικού υπολογιστή.

Απόφαση

Η Αρχή λαμβάνοντας υπόψη τα ανωτέρω:

1. Επιβάλει στην εταιρία Ν. ΚΡΗΤΙΚΟΣ – Γ. ΝΤΑΪΡΤΖΕΣ Α.Ε. ΕΜΠΟΡΙΟ ΧΑΡΤΟΥ πρόστιμο ύψους €3.000,00 για μη εκπλήρωση της υποχρέωσής της να απαντήσει ικανοποιητικά στον προσφεύγοντα.
2. Απευθύνει στην εταιρία σύσταση για κατάρτιση και εφαρμογή εσωτερικού Κανονισμού για την ορθή χρήση και τη λειτουργία του εξοπλισμού και του δικτύου πληροφορικής και επικοινωνιών από τους εργαζόμενους, στο περιεχόμενο της οποίας θα πρέπει ανάμεσα σε άλλα να περιλαμβάνεται:

   Ι. Πολιτική Αποδεκτής Χρήσης των εταιρικών ηλεκτρονικών υπολογιστών (ή άλλου συναφούς εξοπλισμού), του εταιρικού δίκτυο επικοινωνιών (ή άλλης συναφούς υποδομής) και των εταιρικών λογαριασμών ηλεκτρονικής αλληλογραφίας καθώς και τις σχετικές προϋποθέσεις, όρους και διαδικασίες. Σε περίπτωση απαγόρευσης χρήσης του εταιρικού ηλεκτρονικού υπολογιστή για προσωπική χρήση από τους εργαζόμενους, να εξετασθεί η δυνατότητα παραχώρησης της χρήσης ψηφιακού αποθηκευτικού χώρου για προσωπική χρήση, στον οποίο δεν θα είναι επιτρεπτή η πρόσβαση του εργοδότη.

ΙΙ. Πολιτική πρόσβασης και ελέγχου των εταιρικών ηλεκτρονικών υπολογιστών (ή άλλου συναφούς εξοπλισμού) που χρησιμοποιούν οι εργαζόμενοι στην οποία να περιγράφονται κατ' ελάχιστον:

i. οι συναφείς σκοποί (δικαιολογητικοί λόγοι) πρόσβασης και ελέγχου, τηρουμένης της αρχής της αναλογικότητας
ii. η φύση και η έκταση του ελέγχου
iii. η διαδικασία, ο τρόπος και οι όροι πρόσβασης και ελέγχου τόσο σε περίπτωση παρουσίας, όσο και τυχόν απουσίας του εργαζομένου
iv. οι διαδικαστικές εγγυήσεις που αφορούν την πρόσβαση και τον έλεγχο, ιδίως αναφορικά με την διασφάλιση και απόδειξη της ορθότητας και αντικειμενικότητας του καθώς και την παρουσία ή απουσία του εργαζομένου
v. ο τρόπος ενημέρωσης του εργαζομένου για τα ευρήματα του ελέγχου
vi. η διαδικασία που ακολουθείται μετά την ολοκλήρωση του ελέγχου με την οποία τυχόν διενεργείται επεξεργασία προσωπικών δεδομένων επί των ευρημάτων προς επίτευξη των σκοπών του ελέγχου καθώς και η σχετική ενημέρωση του εργαζομένου
vii. η διαδικασία και οι προϋποθέσεις, σύμφωνα με τις οποίες παρέχεται η δυνατότητα αποφυγής της πρόσβασης και ελέγχου του συνόλου των αποθηκευμένων αρχείων, δεδομένων και πληροφοριών με την υιοθέτηση άλλης, λιγότερο επαχθούς, μεθόδου
viii. η προηγούμενη ενημέρωση των εργαζομένων για το ενδεχόμενο πρόσβασης και ελέγχου στους εταιρικούς υπολογιστές (ή σε άλλη συναφή εξοπλισμό) που χρησιμοποιούν καθώς και τις περιπτώσεις εξαίρεσης από την υποχρέωση ενημέρωσης, τηρουμένης της αρχής της αναλογικότητας, και
ix. η προβλεπόμενη από την κείμενη νομοθεσία δυνατότητα προσφυγής των εργαζομένων σε έννομη προστασία.

3. Απευθύνει στην εταιρία σύσταση να μεριμνήσει για τη λήψη των κατάλληλων οργανωτικών και τεχνικών μέτρων ασφάλειας του πληροφοριακού της συστήματος.

Σκεπτικό

1. Η πρόσβαση από τον εργοδότη σε αποθηκευμένα προσωπικά δεδομένα στον υπολογιστή του εργαζομένου συνιστά επεξεργασία δεδομένων προσωπικού χαρακτήρα[76].
2. Η ανωτέρω επεξεργασία είναι νόμιμη στην περίπτωση που είναι απολύτως αναγκαία για την ικανοποίηση του έννομου συμφέροντος του υπεύθυνου επεξεργασίας και υπό τον όρο ότι το συμφέρον αυτό υπερέχει προφανώς των δικαιωμάτων και συμφερόντων του εργαζομένου, χωρίς να θίγονται οι θεμελιώδεις ελευθερίες αυτού[77].
3. Η νομική αυτή βάση υιοθετήθηκε και από το ΕΔΑΑ στην πρόσφατη υπόθεση Barbulescu v. Romania[78], στην οποία αναγνωρίστηκε ότι έννομο συμφέρον του εργοδότη μπορεί να συνιστά η διασφάλιση της εύρυθμης λειτουργίας της επιχείρησης με την εγκαθίδρυση μηχανισμών ελέγχου των εργαζομένων καθώς και η ανάγκη του να προστατέψει την επιχείρηση και την περιουσία της από σημαντικές απειλές, όπως το να εμποδίσει τη διαβίβαση εμπιστευτικών πληροφοριών σε έναν ανταγωνιστή ή να εξασφαλίσει την επιβεβαίωση ή απόδειξη εγκληματικών δράσεων του εργαζομένου
4. Η ικανοποίηση του συμφέροντος αυτού μπορεί να συνίσταται και στην από μέρους του εργοδότη άσκηση του διευθυντικού δικαιώματος, από το οποίο απορρέουν οι παρεπόμενες υποχρεώσεις πίστης προς τον αυτόν, άρα και η υποχρέωση παροχής πληροφοριών προς αυτόν καθώς και ο έλεγχος διαρροής τεχνογνωσίας, εμπιστευτικών πληροφοριών ή εμπορικών/επιχειρηματικών απορρήτων.
5. Από την πλευρά τους, οι εργαζόμενοι έχουν νόμιμη προσδοκία προστασίας της ιδιωτικής ζωής τους στον τόπο εργασίας, ανεξάρτητα από το αν χρησιμοποιούν εξοπλισμό, συσκευές επικοινωνιών ή άλλες επαγγελματικές εγκαταστάσεις ή και υποδομές του εργοδότη[79].
6. Η απλή ενημέρωση από την πλευρά του εργοδότη ότι απαγορεύεται η χρήση των συσκευών αυτών για μη επαγγελματικούς λόγους δεν συνιστά νόμιμο λόγο επιτήρησης ή ελέγχου των δεδομένων προσωπικού χαρακτήρα των εργαζομένων, αλλά απαιτείται ειδικότερη ενημέρωση με τρόπο πρόσφορο και σαφή τον εργαζόμενο για την εισαγωγή και χρήση μεθόδων ελέγχου και

[76] Άρθρο 2 περ. δ' ν. 2472/1997 και ΑΠΔΠΧ 61/2004.
[77] Άρ. 5 εδ. ε', παρ. 2 ν. 2472/1997 και ΑΠΔΠΧ 37/2007.
[78] Ολόκληρο το κείμενο της απόφασης του ΕΔΑΑ εδώ.
[79] Βλ. ΑΠΔΠΧ 61/2004

παρακολούθησης κατά το στάδιο της συλλογής των δεδομένων προσωπικού χαρακτήρα του.

7. Αντίθετα, σύμφωνα και με την ομάδα του άρθρου 29, ο εργοδότης οφείλει να ενημερώνει εκ των προτέρων με τρόπο πρόσφορο και σαφή τον εργαζόμενο για την εισαγωγή και χρήση μεθόδων ελέγχου και παρακολούθησης κατά το στάδιο της συλλογής των δεδομένων[80], ενώ ως προς την παρακολούθηση των επικοινωνιών, οφείλει επιπλέον να θέτει υπόψη του εύληπτη, σαφή και ακριβή δήλωση της Πολιτικής και των Διαδικασιών επιτήρησης.
8. Τέλος, παρότι η εν αγνοία και απουσία του εργαζομένου επιτήρηση και έλεγχος από τον εργοδότη των αποθηκευμένων στον ηλεκτρονικό υπολογιστή δεδομένων προσωπικού χαρακτήρα και επικοινωνιών δεν μπορεί να αποκλειστεί a priori, θα πρέπει να γίνεται μόνο σε εξαιρετικές περιπτώσεις και υπό την προϋπόθεση ότι η ενέργεια αυτή είτε προβλέπεται, είτε δεν αντίκειται στην εθνική νομοθεσία και ότι έχουν ληφθεί τα αναγκαία μέτρα και έχουν προβλεφθεί οι δέουσες διαδικασίες για την πρόσβαση σε επαγγελματική ηλεκτρονική επικοινωνία.
9. Στην υπό κρίση περίπτωση όμως διαπιστώθηκαν τα εξής:
    i. ο έλεγχος του εργοδότη έγινε χωρίς την παρουσία του Α, χωρίς προηγούμενη ενημέρωσή του και χωρίς οποιαδήποτε μέριμνα για την διασφάλιση της νομιμότητας και της αντικειμενικότητας της διαδικασίας ελέγχου
    ii. η συγκατάθεση δεν δόθηκε από το ίδιο το υποκείμενο των δεδομένων όπως προβλέπεται στο νόμο, αλλά από τρίτο πρόσωπο (τον πατέρα του)
    iii. από κανένα στοιχείο δεν προέκυψε η άμεση και επιτακτική ανάγκη διενέργειας ελέγχου του ηλεκτρονικού υπολογιστή και αφαίρεσης του σκληρού δίσκου χωρίς την παρουσία του εργαζομένου, ούτε αιτιολογήθηκε η επιλογή ενός τόσο επαχθούς μέτρου, σε σχέση με κάποιο άλλο όπως π.χ. την προσωρινή απενεργοποίηση και δέσμευση του ηλεκτρονικού υπολογιστή μέχρι την κλήση και παρουσία του προσφεύγοντος
    iv. η εταιρία δεν διέθετε εσωτερικό Κανονισμό για την ορθή χρήση και τη λειτουργία του εξοπλισμού και του δικτύου πληροφορικής και επικοινωνιών από τους εργαζόμενους, από το περιεχόμενο του οποίου θα προέκυπτε αφενός ότι απαγορευόταν η χρήση των ηλεκτρονικών υπολογιστών για προσωπικούς σκοπούς, αφετέρου, θα προβλεπόταν

[80] Βλ. Γνώμη 8/2001, σελ. 25 και Γνώμη 2/2017, σελ. 8

ρητά η δυνατότητα και το ενδεχόμενο ελέγχου αυτών, οι προϋποθέσεις, όροι, διαδικασία, έκταση και εγγυήσεις διενέργειας του ελέγχου

v. η εταιρία ικανοποίησε το δικαίωμα πρόσβασης του Α και συγκεκριμένα δεν απάντησε στο αίτημά του για σαφείς πληροφορίες σχετικά με τα δεδομένα που τον αφορούν, καθώς και σχετικά με οποιοδήποτε άλλο στοιχείο που αφορά στην περαιτέρω επεξεργασία των δεδομένων του, όπως π.χ. οι σκοποί της επεξεργασίας, οι αποδέκτες ή κατηγορίες αποδεκτών, η εξέλιξη της επεξεργασίας για το χρονικό διάστημα από την προηγούμενη ενημέρωσή του κ.α. ούτε κοινοποίησε την απάντηση της στην Αρχή, ενώ παρέλειψε να ενημερώσει τον ενδιαφερόμενο ότι μπορεί να προσφύγει σε αυτήν

vi. αν και δεν αποδείχθηκε η ύπαρξη δεδομένων προσωπικού χαρακτήρα, η εταιρία ως υπεύθυνος επεξεργασίας δεν έλαβε τα αναγκαία τεχνικά και οργανωτικά μέτρα ασφαλείας του πληροφοριακού της συστήματος, μέσω του οποίου διακινούνται και τυγχάνουν επεξεργασίας δεδομένα προσωπικού χαρακτήρα.

3. Ο ρόλος των εποπτικών Αρχών

3. Ο ρόλος των εποπτικών Αρχών

Για τον ΣΕΒ, ο ρόλος των εποπτικών Αρχών στη συμμόρφωση των επιχειρήσεων με το οποιοδήποτε θεσμικό πλαίσιο είναι κομβικός, καθώς:

- ✓ διασφαλίζει την εκπλήρωση του σκοπού του νομοθέτη
- ✓ εγγυάται την ίση μεταχείριση ρυθμιζόμενων και ρυθμιστών (αποφυγή φαινομένων νόθευσης του ανταγωνισμού μεταξύ των συμμορφούμενων και όσων συνειδητά συμμορφώνονται πλημμελώς),
- ✓ μεριμνά για την ελαχιστοποίηση του διοικητικού βάρους συμμόρφωσης και
- ✓ φροντίζει για την αναλογικότητα των διορθωτικών μέτρων και προστίμων.

Ο ρόλος των εποπτικών Αρχών εν γένει είναι άλλωστε πολλαπλός, μεταξύ άλλων ενημερωτικός, ρυθμιστικός και ελεγκτικός / κυρωτικός.

Ο Κανονισμός θέτει μια διαφορετική προσέγγιση από ό, τι μέχρι σήμερα, σε ό,τι αφορά το ρόλο των εποπτικών Αρχών, καθώς πλέον το βάρος απόδειξης λήψης μέτρων για την προστασία των προσωπικών δεδομένων «μετακινείται» στους Υπευθύνους Επεξεργασίας, με τις εποπτικές Αρχές να αναλαμβάνουν δράση σε «δεύτερο χρόνο» και να δίνεται έμφαση στα θέματα εξασφάλισης της συνεκτικής εφαρμογής των διατάξεων (αντί για τον έλεγχο της συμμόρφωσης). Με άλλα λόγια, από ένα πλαίσιο «προληπτικής γραφειοκρατίας»[81] ο Κανονισμός δίνει έμφαση στη νόμιμη και ασφαλή επεξεργασία των προσωπικών δεδομένων από τους ίδιους τους οργανισμούς (επιχειρήσεις και φορείς του δημοσίου). Η εξέλιξη αυτή αποτελεί τομή στη λειτουργία των ρυθμιστικών Αρχών, η οποία κατά τη γνώμη μας θα πυροδοτήσει αλυσιδωτές αντιδράσεις και σε άλλα πεδία πολιτικής.

Ιδίως για τη χώρα μας, όπου ο ρόλος των εποπτικών ή και ρυθμιστικών αρχών δεν είναι πάντα ξεκάθαρος (κυρίως λόγω θεμάτων συναρμοδιότητας με κεντρική διοίκηση), η αποσαφήνιση των αρμοδιοτήτων και του πεδίου δραστηριοποίησης της ΑΠΔΠΧ, του Υπουργείου Δικαιοσύνης και άλλων εμπλεκόμενων δημόσιων φορέων, είναι περισσότερο από καίριος για την εφαρμογή του Κανονισμού.

[81] Ενδεικτικά, αιτήσεις των οργανισμών με προσωπικά δεδομένα προς τις εποπτικές Αρχές για λήψη έγκρισης συλλογής και επεξεργασίας κ.λπ.

Στις επόμενες ενότητες παρουσιάζονται οι προβλέψεις του Κανονισμού για τις εποπτικές Αρχές, το έργο και ο ρόλος της ΑΠΔΠΧ έως σήμερα, καθώς και οι προβλέψεις του Κανονισμού για το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων.

3.1 Οι διατάξεις του Κανονισμού για τις εποπτικές Αρχές

Τα κυριότερα σημεία του Κανονισμού για τις εποπτικές Αρχές[82] προβλέπουν τα εξής:

Γενικά στοιχεία

- Ο Κανονισμός ορίζει ότι στόχος κάθε εποπτικής Αρχής είναι να συμβάλλει στη συνεκτική εφαρμογή του σε ολόκληρη την ΕΕ. Για το λόγο αυτό, προβλέπεται συνεργασία μεταξύ των εποπτικών Αρχών (αρμόδιων και ενδιαφερόμενων) με πολύ συγκεκριμένο τρόπο (π.χ. παροχή πληροφοριών, αμοιβαία συνδρομή, συγκεκριμένα χρονοδιαγράμματα).
- Ως αρμόδια επικεφαλής εποπτική Αρχή[83] ορίζεται η εποπτική αρχή του κράτους μέλους όπου βρίσκεται η κύρια εγκατάσταση του υπευθύνου επεξεργασίας (πρόκειται για τον τόπο κεντρικής διοίκησης ή για τον τόπο όπου λαμβάνονται οι αποφάσεις, όσον αφορά στους σκοπούς και τα μέσα της επεξεργασίας δεδομένων προσωπικού χαρακτήρα).
- Ως ενδιαφερόμενη εποπτική αρχή ορίζεται η Αρχή, την οποία αφορά η επεξεργασία δεδομένων προσωπικού χαρακτήρα, όταν: α) ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία είναι εγκατεστημένος στο έδαφος του κράτους μέλους της εν λόγω εποπτικής Αρχής, β) τα υποκείμενα των δεδομένων που διαμένουν στο κράτος μέλος της εν λόγω εποπτικής Αρχής επηρεάζονται ή ενδέχεται να επηρεαστούν ουσιωδώς από την επεξεργασία, ή γ) έχει υποβληθεί καταγγελία στην εν λόγω εποπτική Αρχή.
- Η επικεφαλής εποπτική Αρχή είναι ο μοναδικός συνομιλητής του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία για τη διασυνοριακή πράξη επεξεργασίας του εν λόγω υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία.
- Ο Κανονισμός προβλέπει πλήρη ανεξαρτησία για τις εποπτικές Αρχές, οι οποίες επιπλέον υπόκεινται σε οικονομικό έλεγχο (δίχως να πλήττεται η ανεξαρτησία). Επίσης, προβλέπεται κατάρτιση ετήσιας έκθεσης των δραστηριοτήτων τους.

[82] Οι εποπτικές Αρχές ανά κράτος-μέλος είναι διαθέσιμες εδώ.
[83] Δείτε εδώ τις Κατευθυντήριες Οδηγίες της Ομάδας Εργασίας άρθρου 29 για τον προσδιορισμό της επικεφαλής εποπτικής αρχής των υπευθύνων επεξεργασίας ή των εκτελούντων την επεξεργασία.

- Η διάρκεια της θητείας του μέλους ή των μελών κάθε εποπτικής Αρχής είναι τουλάχιστον τετραετής[84].
- Κάθε εποπτική Αρχή συμβάλλει στις δραστηριότητες του Συμβουλίου Προστασίας Δεδομένων.

Αδειοδοτικές και συμβουλευτικές εξουσίες

Κάθε αρχή ελέγχου διαθέτει όλες τις ακόλουθες αδειοδοτικές και συμβουλευτικές εξουσίες:

- Παρέχει συμβουλές στον υπεύθυνο επεξεργασίας.
- Εκδίδει, με δική της πρωτοβουλία ή κατόπιν αιτήματος, γνώμες προς το εθνικό κοινοβούλιο, την κυβέρνηση του κράτους μέλους ή, σύμφωνα με το δίκαιο του κράτους μέλους, προς άλλα όργανα και οργανισμούς, καθώς και προς το κοινό, για κάθε θέμα το οποίο σχετίζεται με την προστασία των δεδομένων προσωπικού χαρακτήρα.
- Παρέχει διαπίστευση σε φορείς πιστοποίησης, εκδίδει πιστοποιητικά και εγκρίνει κριτήρια πιστοποίησης.
- Εγκρίνει τυποποιημένες ρήτρες προστασίας δεδομένων, επιτρέπει συμβατικές ρήτρες, επιτρέπει διοικητικές ρυθμίσεις και εγκρίνει δεσμευτικούς εταιρικούς κανόνες.

Διορθωτικές εξουσίες

Κάθε αρχή ελέγχου διαθέτει όλες τις ακόλουθες διορθωτικές εξουσίες:

- Απευθύνει προειδοποιήσεις στον υπεύθυνο επεξεργασίας ή στον εκτελούντα την επεξεργασία ότι σκοπούμενες πράξεις επεξεργασίας είναι πιθανόν να παραβαίνουν διατάξεις του παρόντος κανονισμού.
- Απευθύνει επιπλήξεις στον υπεύθυνο επεξεργασίας ή στον εκτελούντα την επεξεργασία όταν πράξεις επεξεργασίας έχουν παραβεί διατάξεις του Κανονισμού.
- Δίνει εντολή στον υπεύθυνο επεξεργασίας ή στον εκτελούντα την επεξεργασία να συμμορφώνεται προς τα αιτήματα του υποκειμένου των δεδομένων για την άσκηση των δικαιωμάτων του.
- Δίνει εντολή στον υπεύθυνο επεξεργασίας ή στον εκτελούντα την επεξεργασία να καθιστούν τις πράξεις επεξεργασίας σύμφωνες με τις διατάξεις του παρόντος κανονισμού, εάν χρειάζεται, με συγκεκριμένο τρόπο και εντός ορισμένης προθεσμίας.

[84] Με εξαίρεση τον πρώτο διορισμό μετά τις 24 Μαΐου 2016, μέρος του οποίου μπορεί να αφορά συντομότερο διάστημα.

- Δίνει εντολή στον υπεύθυνο επεξεργασίας να ανακοινώνει την παραβίαση δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων.
- Επιβάλλει προσωρινό ή οριστικό περιορισμό, περιλαμβανομένης της απαγόρευσης της επεξεργασίας.
- Δίνει εντολή διόρθωσης ή διαγραφής δεδομένων προσωπικού χαρακτήρα ή περιορισμού της επεξεργασίας.
- Αποσύρει την πιστοποίηση ή διατάσσει τον οργανισμό πιστοποίησης να αποσύρει ένα εκδοθέν πιστοποιητικό.
- Επιβάλλει διοικητικό πρόστιμο, ανάλογα με τις περιστάσεις κάθε μεμονωμένης περίπτωσης.
- Δίνει εντολή για αναστολή της κυκλοφορίας δεδομένων σε αποδέκτη σε τρίτη χώρα ή σε διεθνή οργανισμό.

Θέματα ΥΠΔ

- Η εποπτική Αρχή έχει την πλήρη συνεργασία του ΥΠΔ και οι Υπεύθυνοι Επεξεργασίας ή οι Εκτελούντες την Επεξεργασία υποχρεούνται να δημοσιεύουν τα στοιχεία επικοινωνίας του σε αυτήν. Πρόκειται για μια σχέση άμεσης και συνεχούς επικοινωνίας και διαβούλευσης.

Για την Εκτίμηση Αντικτύπου

- Ο Κανονισμός προβλέπει ότι η εποπτική αρχή καταρτίζει και δημοσιοποιεί κατάλογο με τα είδη των πράξεων επεξεργασίας που υπόκεινται στην απαίτηση για διενέργεια Εκτίμησης Αντικτύπου.
- Περαιτέρω, η εποπτική Αρχή ανακοινώνει τον εν λόγω κατάλογο στο Συμβούλιο Προστασίας Δεδομένων. Οι ίδιες προβλέψεις ισχύουν και για το αντίθετο, δηλαδή για τα είδη των πράξεων επεξεργασίας για τα οποία **δεν** απαιτείται Εκτίμηση Αντικτύπου.
- Προβλέπεται επίσης ότι ο Υπεύθυνος Επεξεργασίας μπορεί να ζητήσει τη γνώμη της εποπτικής Αρχής σχετικά με την σχεδιαζόμενη επεξεργασία και τον κίνδυνο που προκαλεί. Η εποπτική Αρχή οφείλει να παρέχει γραπτώς συμβουλές, σε συγκεκριμένο χρονικό ορίζοντα.

Σχέση με τα υποκείμενα δεδομένων

- Η εποπτική αρχή λαμβάνει καταγγελίες από τα υποκείμενα των δεδομένων (ή από φορέα ή οργάνωση ή ένωση) και είναι αρμόδια για την εξέταση υποβληθείσας καταγγελίας.

- Είναι υποχρεωμένη να ενημερώνει τον καταγγέλλοντα για την πρόοδο και για την έκβαση της έρευνας εντός εύλογου χρονικού διαστήματος.
- Κατόπιν αιτήματος, παρέχει πληροφορίες στα υποκείμενα των δεδομένων όσον αφορά την άσκηση των δικαιωμάτων τους δυνάμει του Κανονισμού.

Περί παραβίασης δεδομένων προσωπικού χαρακτήρα

- Η εποπτική αρχή προβλέπεται να λαμβάνει τη γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα.
- Περαιτέρω, εάν ο υπεύθυνος επεξεργασίας δεν έχει ήδη ανακοινώσει την παραβίαση των δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων, η εποπτική αρχή μπορεί, έχοντας εξετάσει την πιθανότητα επέλευσης υψηλού κινδύνου από την παραβίαση των δεδομένων προσωπικού χαρακτήρα, να του ζητήσει να το πράξει.

Σχετικά με τους Κώδικες Δεοντολογίας

- Η εποπτική αρχή έχει την ευθύνη για την έγκριση των Κωδίκων Δεοντολογίας που ενδέχεται να εκπονήσουν Ενώσεις και άλλοι φορείς που εκπροσωπούν κατηγορίες υπευθύνων επεξεργασίας ή εκτελούντων την επεξεργασία. Η εποπτική αρχή γνωμοδοτεί ως προς τη συμμόρφωση του σχεδίου κώδικα, της τροποποίησης ή της επέκτασης προς τον παρόντα κανονισμό. Μάλιστα η εποπτική αρχή καταχωρίζει και δημοσιεύει τον Κώδικα Δεοντολογίας.

Περί πιστοποίησης

- Η εποπτική αρχή παροτρύνει τη θέσπιση μηχανισμών πιστοποίησης προστασίας δεδομένων και σφραγίδων και σημάτων προστασίας δεδομένων, με σκοπό την απόδειξη της συμμόρφωσης προς τον παρόντα κανονισμό των πράξεων επεξεργασίας από τους υπευθύνους επεξεργασίας και τους εκτελούντες την επεξεργασία.
- Σχετικά, προβλέπεται στον Κανονισμό αρμοδιότητα ή συνεργασία της Αρχής με τον εκάστοτε εθνικό οργανισμό διαπίστευσης (π.χ. για τα κριτήρια διαπίστευσης), με αρμοδιότητα για χορήγηση ή ανάκληση της διαπίστευσης.

Δ.15 Οι κυριότερες διατάξεις του Κανονισμού για τις εποπτικές Αρχές
Στόχος: Εξασφάλιση συνεκτικής εφαρμογής
Πρόβλεψη για: • πλήρη ανεξαρτησία • πλήρη συνεργασία του ΥΠΔ, των Υπευθύνων Επεξεργασίας και των Εκτελούντων την Επεξεργασία
Αρμόδια επικεφαλής εποπτική Αρχή: εποπτική αρχή του κράτους μέλους όπου βρίσκεται η κύρια εγκατάσταση του υπευθύνου επεξεργασίας
Αρμοδιότητες: • Διαθέτει αδειοδοτικές και συμβουλευτικές εξουσίες • Διαθέτει διορθωτικές εξουσίες • Καταρτίζει και δημοσιοποιεί κατάλογο με τα είδη των πράξεων επεξεργασίας που υπόκεινται στην απαίτηση για διενέργεια Εκτίμησης Αντικτύπου • Λαμβάνει καταγγελίες από τα υποκείμενα των δεδομένων • Εγκρίνει τους Κώδικες Δεοντολογίας

3.2 Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ)

Όπως έχει προαναφερθεί ο ρόλος της αρμόδιας εποπτικής Αρχής στην Ελλάδα, εν προκειμένω της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), είναι ιδιαίτερα σημαντικός. Πέρα από τις πρωτοβουλίες που έχει ήδη αναλάβει για την ενημέρωση όλων των εμπλεκομένων (Υπευθύνων Επεξεργασίας και Υποκειμένων), αναμένεται, ειδικά στο αρχικό διάστημα μετά την έναρξη εφαρμογής του Κανονισμού, να έχει ενισχυμένο ρόλο λειτουργώντας ως «σύμμαχος» των επιχειρήσεων στη συμμόρφωση.

Ειδικότερα, εκτιμάται ότι μετά και την ψήφιση του εφαρμοστικού Νόμου του Κανονισμού, η ΑΠΔΠΧ θα προχωρήσει σε αρκετές διευκρινίσεις που θα διευκολύνουν την κατανόηση των απαιτήσεων συμμόρφωσης, ενώ σημαντικές θα είναι και οι πρώτες αποφάσεις και γνωμοδοτήσεις που θα εκδώσει[85].

Σημειώνεται ότι η ΑΠΔΠΧ είναι συνταγματικά κατοχυρωμένη ανεξάρτητη Αρχή, η οποία ιδρύθηκε με το Νόμο 2472/1997 που ενσωμάτωνε την Ευρωπαϊκή Οδηγία 95/46/ΕΚ.

[85] Δείτε **εδώ** το Σχέδιο Νόμου που κατατέθηκε για διαβούλευση έως την 5η Μαρτίου 2018

Στον πίνακα **(Δ16)** αποτυπώνεται συνοπτικά το έργο της Αρχής, το οποίο, παρά την ελλιπή στελέχωσή της[86], είναι ιδιαίτερα σημαντικό. Από τα στοιχεία προκύπτει ότι η ΑΠΔΠΧ λαμβάνει και καλείται να διαχειριστεί σχεδόν δύο καταγγελίες την ημέρα και περισσότερα από τρία ερωτήματα, ενώ εκδίδει μία απόφαση σχεδόν κάθε δεύτερη ημέρα του έτους.

Δ.16 Το έργο της ΑΠΔΠΧ την περίοδο 2008-2016
Πηγή: Ετήσια έκθεση ΑΠΔΠΧ, 2016

	Προσφυγές / Καταγγελίες	Ερωτήματα	Αποφάσεις	Γνωμοδοτήσεις
2008	670	1.118	69	0
2009	702	1.106	91	4
2010	674	1.261	84	4
2011	812	1.432	168	7
2012	675	1.330	194	5
2013	562	1.421	158	6
2014	659	1.615	202	5
2015	506	1.299	138	7
2016	714	1.465	132	8
Μέσος όρος	**664**	**1.339**	**137**	**5**

Με βάση τη νέα φιλοσοφία του Κανονισμού, όπως παρουσιάστηκε προηγουμένως, εύλογα προκύπτει ότι οι προκλήσεις για την ΑΠΔΠΧ αυξάνονται, καθώς η συνεργασία μεταξύ των εποπτικών Αρχών πλέον επιβάλλεται, με συγκεκριμένα μάλιστα χρονοδιαγράμματα. Στο πλαίσιο αυτό, αποτελεί στοίχημα για την ΑΠΔΠΧ να ανταπεξέλθει, ειδικά στην περίπτωση που λειτουργεί ως επικεφαλής εποπτική Αρχή.

3.3 Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων

Ο Κανονισμός προβλέπει ένα επιπλέον ανεξάρτητο, όργανο αυτό του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων (Συμβούλιο εν συντομία). Πρόκειται για όργανο της Ένωσης, με διακριτή νομική προσωπικότητα, το οποίο συμβάλλει στη συνεκτική εφαρμογή του Κανονισμού σε ολόκληρη την ΕΕ, μεταξύ άλλων παρέχοντας συμβουλές στην Επιτροπή, ιδίως για το επίπεδο προστασίας σε τρίτες χώρες ή σε διεθνείς οργανισμούς, και προωθώντας τη συνεργασία των εποπτικών αρχών σε ολόκληρη την ΕΕ.

Σημειώνεται ότι με την έναρξη εφαρμογής του Κανονισμού το Μάιο 2018, το Συμβούλιο αντικατέστησε την «Ομάδα προστασίας των προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα» του άρθρου 29 της Οδηγίας

[86] Στην ετήσια έκθεση του 2016 αναφέρεται ότι υφίστανται 25 οργανικές θέσεις στην ΑΠΔΠΧ, 14 δικηγόρων-ελεγκτών και 11 πληροφορικών-ελεγκτών.

95/46/ΕΚ (γνωστής ως "Article 29 Working Party") επικαιροποιώντας τον Πρακτικό Οδηγό της Ευρωπαϊκής νομοθεσίας προστασίας δεδομένων[87].

Ο Κανονισμός προβλέπει ότι το Συμβούλιο Προστασίας Δεδομένων εκπονεί ετήσια έκθεση όσον αφορά την προστασία των φυσικών προσώπων έναντι της επεξεργασίας στην ΕΕ και, κατά περίπτωση, σε τρίτες χώρες και διεθνείς οργανισμούς. Η έκθεση αυτή δημοσιοποιείται και διαβιβάζεται στο Ευρωπαϊκό Κοινοβούλιο, στο Συμβούλιο και στην Επιτροπή.

Το Συμβούλιο απαρτίζεται από τον προϊστάμενο μίας εποπτικής Αρχής κάθε κράτους μέλους και από τον Ευρωπαίο Επόπτη Προστασίας Δεδομένων[88] ή τους αντίστοιχους εκπροσώπους τους, ενώ σε αυτήν προβλέπεται συμμετοχή εκπροσώπου της Επιτροπής. Αποφασίζει με απλή πλειοψηφία των μελών του.

Κύριο καθήκον του Συμβουλίου είναι η διασφάλιση της συνεκτικής εφαρμογής του Κανονισμού. Ειδικότερα, το Συμβούλιο ακολουθεί και διασφαλίζει την ορθή εφαρμογή του Κανονισμού, με την επιφύλαξη των καθηκόντων των εθνικών εποπτικών αρχών:

- Συμβουλεύει την Επιτροπή για κάθε ζήτημα σχετικό με την προστασία των δεδομένων προσωπικού χαρακτήρα στην Ένωση, συμπεριλαμβανομένης κάθε προτεινόμενης τροποποίησης του Κανονισμού.
- Συμβουλεύει την Επιτροπή σχετικά με τον μορφότυπο και τις διαδικασίες για την ανταλλαγή πληροφοριών μεταξύ υπευθύνων επεξεργασίας, εκτελούντων την επεξεργασία και εποπτικών αρχών για τους δεσμευτικούς εταιρικούς κανόνες.
- Εκδίδει κατευθυντήριες γραμμές, συστάσεις και βέλτιστες πρακτικές σχετικά με τις διαδικασίες για τη διαγραφή συνδέσμων, αντιγράφων ή αναπαραγωγών δεδομένων προσωπικού χαρακτήρα από υπηρεσίες επικοινωνιών διαθέσιμες στο κοινό.
- Εκδίδει κατευθυντήριες γραμμές, συστάσεις και βέλτιστες πρακτικές, με σκοπό να ενθαρρύνει τη συνεκτική εφαρμογή του Κανονισμού.
- Εκδίδει κατευθυντήριες γραμμές, συστάσεις και βέλτιστες πρακτικές για τον περαιτέρω προσδιορισμό των κριτηρίων και των προϋποθέσεων για τη λήψη αποφάσεων που βασίζονται σε κατάρτιση προφίλ

[87] European Union Agency for Fundamental Rights and Council of Europe, "Handbook on European data protection law", 2018.

[88] Ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων προβλέφθηκε στον Κανονισμό 45/2001, με ρόλο να διασφαλίζει ότι κατά την επεξεργασία προσωπικών δεδομένων, τα όργανα και οι οργανισμοί της ΕΕ σέβονται το δικαίωμα των πολιτών για προστασία της ιδιωτικής ζωής.

- Εκδίδει κατευθυντήριες γραμμές, συστάσεις και βέλτιστες πρακτικές σχετικά με τη διαπίστωση των παραβιάσεων των δεδομένων προσωπικού χαρακτήρα και τον καθορισμό της δράσης του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία.
- Εκδίδει κατευθυντήριες γραμμές, συστάσεις και βέλτιστες πρακτικές όσον αφορά στις συνθήκες υπό τις οποίες η παραβίαση δεδομένων προσωπικού χαρακτήρα ενδέχεται να έχει ως αποτέλεσμα υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων.
- Εκδίδει κατευθυντήριες γραμμές, συστάσεις και βέλτιστες πρακτικές για τον περαιτέρω προσδιορισμό των κριτηρίων και των απαιτήσεων για τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα που βασίζονται σε δεσμευτικούς εταιρικούς κανόνες που τηρούν οι υπεύθυνοι επεξεργασίας και δεσμευτικούς εταιρικούς κανόνες που τηρούν οι υπεύθυνοι επεξεργασίας και των περαιτέρω αναγκαίων απαιτήσεων, ώστε να διασφαλίζεται η προστασία των δεδομένων προσωπικού χαρακτήρα των οικείων υποκειμένων των δεδομένων.
- Εκδίδει κατευθυντήριες γραμμές, συστάσεις και βέλτιστες πρακτικές για τους σκοπούς του περαιτέρω προσδιορισμού των κριτηρίων και των απαιτήσεων για τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα.
- Εκπονεί κατευθυντήριες γραμμές για τις εποπτικές αρχές όσον αφορά την εφαρμογή των μέτρων και τον καθορισμό διοικητικών προστίμων.
- Εξετάζει την πρακτική εφαρμογή των κατευθυντήριων γραμμών, των συστάσεων και των βέλτιστων πρακτικών που προαναφέρθηκαν για την εκπόνηση κοινών διαδικασιών.
- Ενθαρρύνει την κατάρτιση κωδίκων δεοντολογίας και τη θέσπιση μηχανισμών πιστοποίησης προστασίας δεδομένων και σφραγίδων και σημάτων προστασίας δεδομένων.
- Εκτελεί τη διαπίστευση των φορέων πιστοποίησης και την περιοδική επανεξέτασή της και τηρεί δημόσιο μητρώο των διαπιστευμένων φορέων.
- Προσδιορίζει τις απαιτήσεις προκειμένου για τη διαπίστευση των φορέων πιστοποίησης και γνωμοδοτεί στην Επιτροπή σχετικά με τις απαιτήσεις πιστοποίησης.
- Παρέχει στην Επιτροπή γνωμοδότηση για την εκτίμηση της επάρκειας του επιπέδου προστασίας σε τρίτη χώρα ή διεθνή οργανισμό, συμπεριλαμβανομένης της εκτίμησης του κατά πόσο μια τρίτη χώρα, ένα έδαφος ή ένας ή περισσότεροι συγκεκριμένοι τομείς στην εν λόγω τρίτη χώρα ή ένας διεθνής οργανισμός δεν διασφαλίζει πλέον επαρκές επίπεδο

προστασίας. Για τον σκοπό αυτό, η Επιτροπή παρέχει στο Συμβούλιο όλη την απαραίτητη τεκμηρίωση, συμπεριλαμβανομένης της αλληλογραφίας με την κυβέρνηση της τρίτης χώρας, όσον αφορά την εν λόγω τρίτη χώρα, το έδαφος ή τον συγκεκριμένο τομέα ή τον διεθνή οργανισμό.

- Εκδίδει γνώμες για σχέδια αποφάσεων των εποπτικών αρχών δυνάμει του μηχανισμού συνεκτικότητας.
- Προωθεί τη συνεργασία και την αποτελεσματική διμερή και πολυμερή ανταλλαγή πληροφοριών και βέλτιστων πρακτικών μεταξύ των εποπτικών αρχών.
- Προωθεί κοινά προγράμματα κατάρτισης και διευκολύνει τις ανταλλαγές υπαλλήλων μεταξύ εποπτικών αρχών και, κατά περίπτωση, με τις εποπτικές αρχές τρίτων χωρών ή με διεθνείς οργανισμούς.
- Προωθεί την ανταλλαγή γνώσεων και τεκμηρίωσης σχετικά με τη νομοθεσία και την πρακτική στον τομέα της προστασίας δεδομένων με τις εποπτικές αρχές προστασίας δεδομένων ανά τον κόσμο.
- Γνωμοδοτεί επί των κωδίκων δεοντολογίας που εκπονούνται σε επίπεδο ΕΕ.
- Διατηρεί δημόσια προσβάσιμο ηλεκτρονικό μητρώο των αποφάσεων που λαμβάνονται από τις εποπτικές αρχές και τα δικαστήρια για ζητήματα που εξετάζονται στο πλαίσιο του μηχανισμού συνεκτικότητας[89].

Δ.17 Ο ρόλος του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων

Από την έναρξη ενάσκησης των καθηκόντων του την 25η Μαΐου 2018 και μέχρι τις αρχές Οκτωβρίου, το Συμβούλιο περιορίστηκε στην αποδοχή των Κατευθύνσεων που είχε εκδώσει με την παρελθούσα ιδιότητα του ως Ομάδα Εργασίας άρθρου 29 και αναμένονται από αυτό μια σειρά από δράσεις στο άμεσο μέλλον. Ένα χαρακτηριστικό παράδειγμα των δράσεων που αναμένεται να κληθεί να αναλάβει το Συμβούλιο απορρέει από διάταξη του Κανονισμού που εξουσιοδοτεί τα κράτη-μέλη να απαιτήσουν την παροχή συγκατάθεσης από τον έχοντα τη γονική μέριμνα του τέκνου, εφόσον το τέκνο δεν υπερβαίνει συγκεκριμένο ηλικιακό όριο. Κάθε κράτος-μέλος έχει τη δυνατότητα, βάσει του Κανονισμού να προσδιορίσει το όριο αυτό, σε οποιαδήποτε ηλικία του τέκνου μεταξύ 13 και 16 ετών.

Η παροχή της διακριτικής αυτής ευχέρειας στον εκάστοτε εθνικό νομοθέτη για την επιλογή διαφορετικού ορίου ηλικίας του τέκνου είναι πολύ πιθανό να προκαλέσει τεχνικά προβλήματα στην ενιαία και ομοιόμορφη υλοποίηση των απαιτήσεων του Κανονισμού από τους Υπεύθυνους Επεξεργασίας.

Ενδεικτικά, είναι αναμενόμενο να προκύψουν ζητήματα χειρισμού και εφαρμογής σε περιπτώσεις στις οποίες το ανήλικο παιδί ηλικίας έστω 13 ετών που διαμένει σε κράτος στο οποίο το ελάχιστο όριο για τη συγκατάθεση είναι τα 13 έτη, αποκτά πρόσβαση σε ιστοσελίδα Υπεύθυνου Επεξεργασίας ο οποίος είναι εγκατεστημένος σε άλλο κράτος-μέλος της ΕΕ όπου η ελάχιστη ηλικία του τέκνου για την παροχή συγκατάθεσης του έχοντος τη γονική μέριμνα έχει οριστεί έστω στα 15 έτη.

[89] Δείτε άρθρα 63 και 64 του Κανονισμού για περισσότερες πληροφορίες.

4. Βαθμός ετοιμότητας των επιχειρήσεων στο εξωτερικό και την Ελλάδα

4. Βαθμός ετοιμότητας των επιχειρήσεων στο εξωτερικό και την Ελλάδα

Στις ακόλουθες ενότητες παρουσιάζεται ο βαθμός ετοιμότητας των επιχειρήσεων σχετικά με τη συμμόρφωσή τους στις διατάξεις του Κανονισμού, βάσει ερευνών που έχουν πραγματοποιηθεί, τόσο στο εξωτερικό όσο και στην Ελλάδα. Σκοπός του Κεφαλαίου είναι να αποτυπωθούν ποσοτικά στοιχεία για το βαθμό συμμόρφωσης των επιχειρήσεων, προκειμένου να καταγραφεί η υφιστάμενη κατάσταση στην Ελλάδα και να είναι δυνατή η παρακολούθηση της πορείας συμμόρφωσης διαχρονικά (και επομένως να καταγραφεί η όποια βελτίωση ή υστέρηση) , αλλά και να υπάρχει ένα μέτρο σύγκρισης (benchmarking) για την εγχώρια αγορά σε σχέση με τις υπόλοιπες χώρες της ΕΕ.

Σημειώνεται ότι οι έρευνες που πραγματοποιήθηκαν έφεραν στην επιφάνεια και άλλα χρήσιμα στοιχεία σχετικά με την πορεία συμμόρφωσης στον Κανονισμό, για τα οποία αξίζει να ληφθεί μέριμνα, καθώς αποτύπωσαν την άποψη των επιχειρήσεων σε ένα θέμα που αναδείχτηκε «βίαια» στην ατζέντα των προτεραιοτήτων τους.

Τέλος, αξίζει να σημειώσουμε ότι παρόλο που στην Ελλάδα ο βαθμός ετοιμότητας των επιχειρήσεων, όπως καταγράφεται στις σχετικές έρευνες, «υπολείπεται» των αντίστοιχων του εξωτερικού, οι επιχειρήσεις όλων των κρατών-μελών αντιμετωπίζουν προκλήσεις στην προσπάθειά τους να προσαρμοστούν στο νέο θεσμικό πλαίσιο για τα προσωπικά δεδομένα.

4.1 Εκτιμήσεις για τη συμμόρφωση των επιχειρήσεων στο εξωτερικό

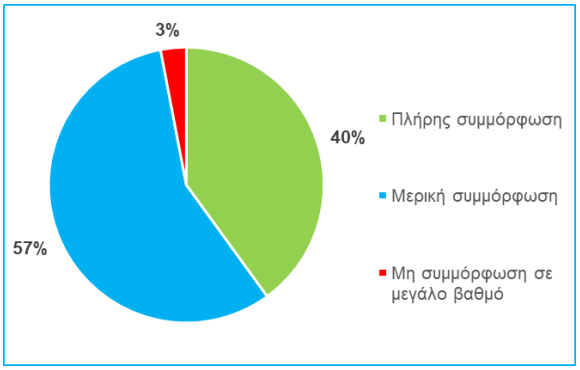
Ο βαθμός ετοιμότητας των επιχειρήσεων στο εξωτερικό κρίθηκε σκόπιμο να παρουσιαστεί μέσα από δύο πρόσφατες και ιδιαίτερα αντιπροσωπευτικές και αξιόπιστες έρευνες, οι οποίες αναδεικνύουν σαν γενικό συμπέρασμα ότι **οι επιχειρήσεις δεν θα καταφέρουν να συμμορφωθούν έγκαιρα και πλήρως στις διατάξεις του Κανονισμού**. Τα βασικά συμπεράσματα των ερευνών παρουσιάζονται με μεγαλύτερη λεπτομέρεια στις επόμενες ενότητες.

4.1.1 Η έρευνα των International Association of Privacy Professionals (IAPP) και ΕΥ

Στη διεθνή έρευνα των International Association of Privacy Professionals (IAPP) και ΕΥ, η οποία πραγματοποιήθηκε το 2017, σχετικά με την πορεία συμμόρφωσης των επιχειρήσεων στον Κανονισμό, προκύπτει ότι **(Δ18)**:

- **Περισσότερες από 1 στις 2 επιχειρήσεις** θεωρούν ότι έως το Μάιο του 2018 θα έχουν καταφέρει να πετύχει **μερική μόνο συμμόρφωση στο νέο Κανονισμό** (57%).
- Ωστόσο, το ποσοστό εκείνων που εκτιμούν ότι θα «απέχουν» σημαντικά από τη συμμόρφωση είναι περιορισμένο (μόλις 3%).

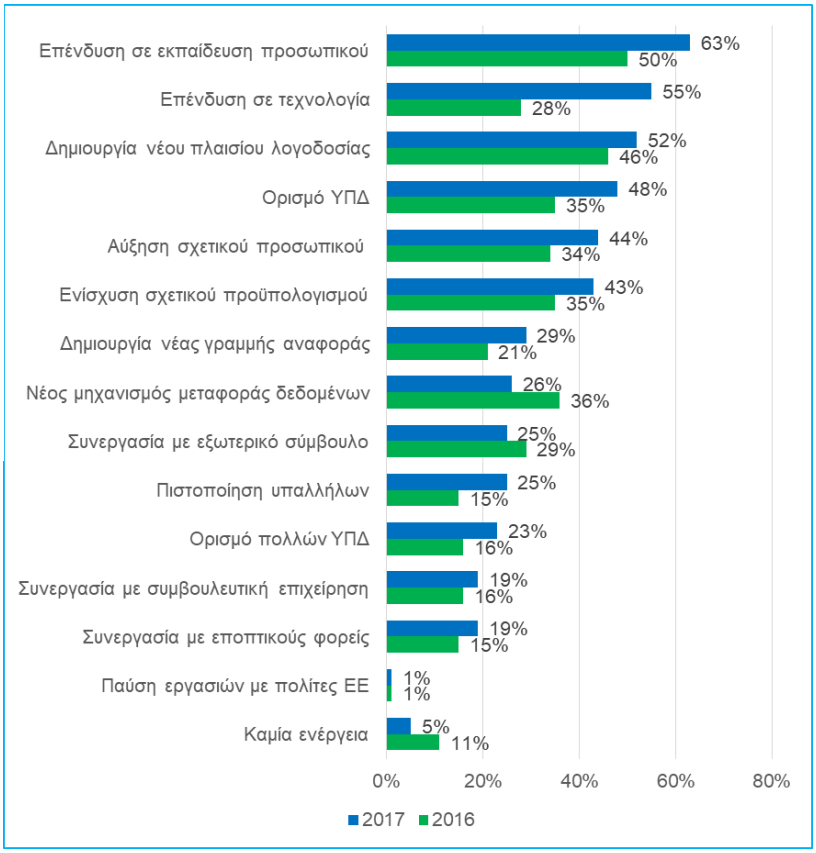
Δ.18 Εκτίμηση βαθμού ετοιμότητας συμμόρφωσης με τις απαιτήσεις του Κανονισμού το Μάιο του 2018
Πηγή: IAPP-EY, "Annual Privacy Governance Report", 2017



Όσον αφορά στις ενέργειες στις οποίες προβαίνουν οι επιχειρήσεις προκειμένου να πετύχουν τη συμμόρφωση στον Κανονισμό, προκύπτει ότι **(Δ19)**:

- **Το 63% των επιχειρήσεων επενδύει πλέον σε δράσεις εκπαίδευσης του προσωπικού** και το 55% σε τεχνολογικά εργαλεία. Τα αντίστοιχα ποσοστά το 2016 ήταν σημαντικά χαμηλότερα (50% και 28% αντίστοιχα).
- Σημαντικά ποσοστά καταλαμβάνουν και οι δράσεις σχετικές με τη λογοδοσία και τον ορισμό του ΥΠΔ (52% και 48% αντίστοιχα).
- Αντίθετα, οι δράσεις που το 2017 κατέλαβαν μικρότερο μερίδιο από ότι το 2016 είναι η εισαγωγή νέου μηχανισμού για τη μεταφορά των δεδομένων και η συνεργασία με εξωτερικό σύμβουλο, δηλαδή δράσεις που εκ φύσεως ήταν - συγκριτικά με τις υπόλοιπες - αναμενόμενο να ξεκινήσουν να υλοποιούνται νωρίτερα.
- Το ποσοστό των επιχειρήσεων, που ακόμα και σήμερα δεν προβαίνει σε καμία ενέργεια σχετικά με τον Κανονισμό, έχει μειωθεί από 11% σε 5%.

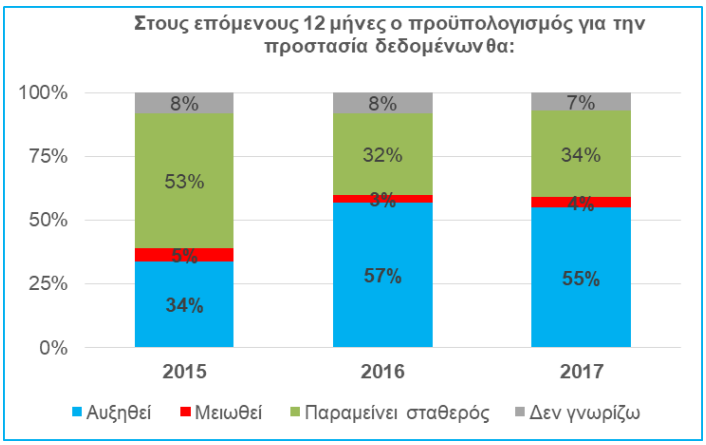
Δ.19 Ενέργειες στις οποίες προβαίνουν οι επιχειρήσεις για τη συμμόρφωσή τους στον Κανονισμό
Σημείωση: Δυνατότητα πολλαπλών επιλογών.
Πηγή: IAPP-EY, "Annual Privacy Governance Report", 2017



Τέλος, σχετικά με το ποσό που έχουν προϋπολογίσει οι επιχειρήσεις για την υλοποίηση δράσεων για την προστασία των δεδομένων, προκύπτει ότι **(Δ20)**:

- Το 2016 αυξήθηκε σημαντικά το ποσοστό των επιχειρήσεων που θεωρεί ότι οι εν λόγω δαπάνες θα αυξηθούν το επόμενο δωδεκάμηνο σε σχέση με το 2015, ενώ οι απαντήσεις των επιχειρήσεων το 2016 και το 2017 κινήθηκαν σε σχετικά όμοια επίπεδα.
- Είναι αξιοσημείωτο ότι, ακόμα και το 2017 (μόλις ένα έτος πριν την έναρξη εφαρμογής του Κανονισμού), **περισσότερες από 1 στις 2 επιχειρήσεις (55%) εξακολουθούν να εκτιμούν ότι ο προϋπολογισμός για την προστασία των δεδομένων θα κινηθεί ανοδικά το επόμενο δωδεκάμηνο**.

Δ.20 Πορεία ύψους προϋπολογισμού των επιχειρήσεων για την προστασία δεδομένων
Πηγή: IAPP-EY, "Annual Privacy Governance Report", 2017

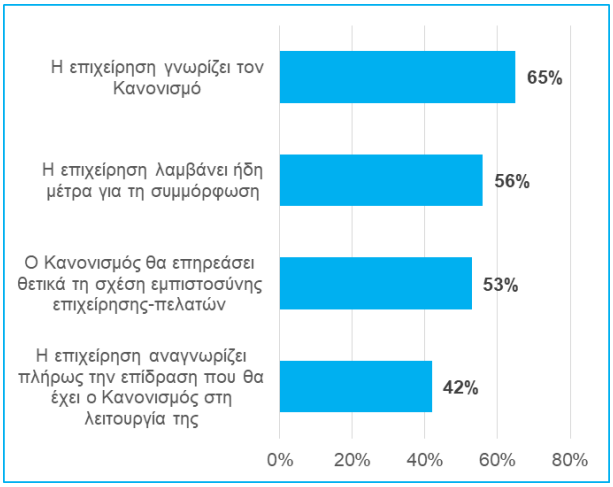


4.1.2 Η έρευνα της SAS

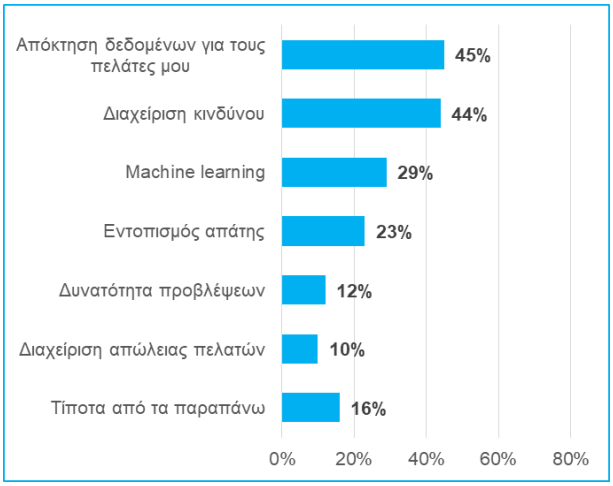
Από τη διεθνή έρευνα που υλοποίησε η SAS το 2017 σχετικά με την πορεία συμμόρφωσης των επιχειρήσεων στον Κανονισμό, προκύπτει ότι[90] **(Δ21)**:

- **Η πλειονότητα των επιχειρήσεων γνωρίζει τον Κανονισμό (65%)** και λαμβάνει ήδη μέτρα για την επίτευξη της συμμόρφωσης (56%).
- **Το 53% δηλώνει ότι η συμμόρφωση στον Κανονισμό θα επηρεάσει θετικά τη σχέση εμπιστοσύνης με τους πελάτες της**, αναδεικνύοντας τη σημαντικότητα της συμμόρφωσης ως ανταγωνιστικό πλεονέκτημα.
- Το ποσοστό των επιχειρήσεων που δηλώνει ότι έχει πλήρη επίγνωση της επίδρασης του Κανονισμού στη λειτουργία της είναι αρκετά μικρότερο από το αντίστοιχο ποσοστό των επιχειρήσεων που ήδη λαμβάνει μέτρα συμμόρφωσης (42% έναντι 56%).

Δ.22 Έρευνα σχετικά με τη συμμόρφωση με τον Κανονισμό
Πηγή: SAS, "Working toward GDPR compliance - Insights from a SAS survey and an end-to-end approach", 2017



Δ.22 Πεδία επιχειρηματικής πληροφόρησης στα οποία αναμένεται να έχει μεγαλύτερη επίδραση η διαδικασία συμμόρφωσης στον Κανονισμό
Σημείωση: Δυνατότητα πολλαπλών επιλογών.
Πηγή: SAS, "Working toward GDPR compliance - Insights from a SAS survey and an end-to-end approach", 2017



[90] Η έρευνα πραγματοποιήθηκε την Άνοιξη του 2017 και το δείγμα ανήλθε σε 347 επιχειρήσεις, εκ των οποίων οι 42 δεν είχαν έδρα στην ΕΕ. Δείτε τη μελέτη **εδώ**.

Επιπλέον, η έρευνα κατέγραψε την άποψη των επιχειρήσεων για τα πεδία επιχειρηματικής πληροφόρησης στα οποία αναμένεται να έχει μεγαλύτερη επίδραση η διαδικασία συμμόρφωσης στον Κανονισμό **(Δ22)**. Τα αποτελέσματα δεικνύουν πόσο σημαντικά οφέλη μπορούν να προκύψουν για τις επιχειρήσεις στην εποχή του ψηφιακού μετασχηματισμού, χάρη στη λήψη μέτρων για την επίτευξη της συμμόρφωσης στον Κανονισμό. Οφέλη όπως: απόκτηση δεδομένων που συμβάλλουν στην καλύτερη γνώση των πελατών της επιχείρησης και των χαρακτηριστικών τους (customer intelligence), καλύτερη διαχείριση κινδύνου (risk management), ενίσχυση του "machine learning", ακόμα και εντοπισμό περιστατικών απάτης.

Τέλος, η εν λόγω έρευνα ανέδειξε τα σημεία της προετοιμασίας συμμόρφωσης με τον Κανονισμό που δυσκολεύουν περισσότερο τις επιχειρήσεις. Όπως προκύπτει:

- Ιδιαίτερα υψηλό είναι το ποσοστό των επιχειρήσεων που εκφράζει αβεβαιότητα για το αν επαρκούν οι ενέργειες συμμόρφωσης που αναλαμβάνει (59%). Το γεγονός αυτό αποτυπώνει τόσο τη γενική δυσκολία κατά την προσπάθεια συμμόρφωσης στον Κανονισμό, όσο και το πλήθος των προκλήσεων που προκύπτουν ειδικά από τις διατάξεις που αφήνουν «γκρίζες ζώνες» για την ερμηνεία τους, προκαλώντας προφανώς ανησυχία και αβεβαιότητα στις επιχειρήσεις.
- Η **φορητότητα δεδομένων** και το **δικαίωμα στη λήθη** αποτελούν τις **υποχρεώσεις** που οι επιχειρήσεις αξιολογούν ως **πιο δύσκολες**.
- Από τις εσωτερικές λειτουργίες των επιχειρήσεων, **ο περιορισμός της πρόσβασης σε προσωπικά δεδομένα μόνο στα άτομα που προβλέπεται ή / και είναι αναγκαίο αποτελεί πρόκληση για μία στις δύο επιχειρήσεις**. Αυτό δεικνύει ότι δεν πρέπει να υποτιμάται καμία εσωτερική πολιτική και διαδικασία, κατά την προσπάθεια συμμόρφωσης στον Κανονισμό, καθώς ακόμα και φαινομενικά απλές λειτουργίες (εν προκειμένω, πρόσβαση στα προσωπικά δεδομένα μόνο από όσους χρειάζεται), τελικά στην πράξη δεν υλοποιούνται τόσο εύκολα.

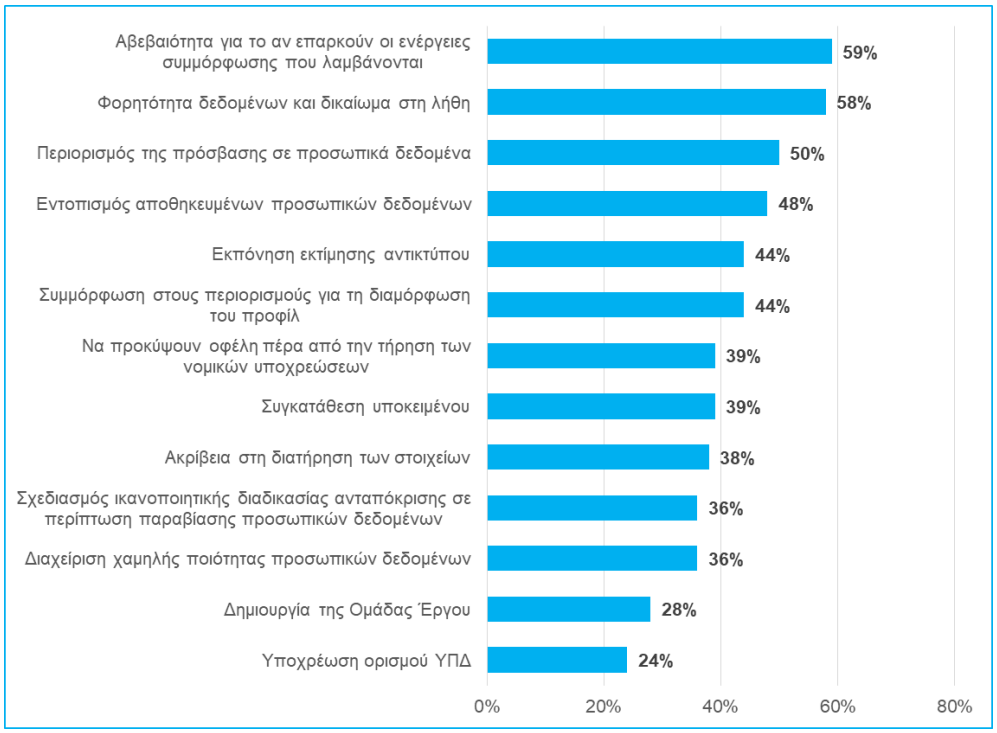
4.1.3 Συνοπτικά συμπεράσματα

Τα βασικά συμπεράσματα των δυο ερευνών συνοψίζονται ως εξής:

- Η πλειονότητα των επιχειρήσεων θα έχει καταφέρει να πετύχει **μερική μόνο συμμόρφωση** στο νέο Κανονισμό έως το Μάιο του 2018.
- Το **ποσοστό των επιχειρήσεων που «απέχουν» σημαντικά από τη συμμόρφωση** και δεν έχουν προβεί σε καμία ενέργεια είναι πλέον ιδιαίτερα **περιορισμένο**.

- Παρά τη μέριμνα και τις προσπάθειες συμμόρφωσης, οι επιχειρήσεις παραμένουν ακόμα **ανώριμες ως προς την πλήρη επίγνωση της επίδρασης του Κανονισμού στη λειτουργία τους**.
- Τα **οφέλη** για τις επιχειρήσεις από τη συμμόρφωση με τον Κανονισμό είναι **πολλαπλά**: βελτίωση σχέσης εμπιστοσύνης με τους πελάτες, καλύτερη γνώση των χαρακτηριστικών των πελατών και των αναγκών τους (customer intelligence), καλύτερη διαχείριση κινδύνων, ενίσχυση του "machine learning" και εντοπισμός περιστατικών απάτης.
- Οι ενέργειες συμμόρφωσης που λαμβάνουν πλέον προτεραιότητα είναι οι **δράσεις εκπαίδευσης του προσωπικού** και η **επένδυση σε τεχνολογικά εργαλεία**.
- Μεταξύ των επιχειρήσεων προκύπτει μια **αβεβαιότητα** για το αν επαρκούν οι ενέργειες συμμόρφωσης που έχουν αναλάβει. Την ίδια στιγμή, οι υποχρεώσεις του Κανονισμού που θέτουν τις **μεγαλύτερες προκλήσεις** είναι η **φορητότητα δεδομένων** και το **δικαίωμα στη λήθη**.
- Ο **προϋπολογισμός** για την προστασία των δεδομένων κινείται **ανοδικά διαχρονικά**.

Δ.23 Σημεία της προετοιμασίας συμμόρφωσης στον Κανονισμό που δυσκολεύουν περισσότερο τις επιχειρήσεις
Σημείωση: Δυνατότητα πολλαπλών επιλογών.
Πηγή: SAS, "Working toward GDPR compliance - Insights from a SAS survey and an end-to-end approach", 2017



4.2 Εκτιμήσεις για τη συμμόρφωση των επιχειρήσεων στην Ελλάδα

Ο βαθμός ετοιμότητας των επιχειρήσεων στην Ελλάδα απασχόλησε έντονα καθ' όλη την περίοδο πριν την ημερομηνία έναρξης εφαρμογής του Κανονισμού (25η Μαΐου 2018), κάτι που αναμένεται να συνεχιστεί και στο μέλλον, όταν για παράδειγμα θα επιχειρηθεί να καταγραφεί εκ νέου ο βαθμός συμμόρφωσης (ενδεικτικά ένα χρόνο μετά).

Στα στοιχεία που παρουσιάζουμε παρακάτω, από δύο πρόσφατες έρευνες που δημοσιοποιήθηκαν, αποτυπώνεται με σχετική αντιπροσωπευτικότητα κατά την άποψη της συντακτικής ομάδας, ο βαθμός ετοιμότητας των επιχειρήσεων και αναδεικνύεται ότι **υπάρχει αρκετός δρόμος ακόμα, προκειμένου οι επιχειρήσεις να καταφέρουν να συμμορφωθούν στις διατάξεις του Κανονισμού**. Τα βασικά συμπεράσματα των ερευνών παρουσιάζονται στις επόμενες ενότητες.

4.2.1 Η έρευνα της ICAP

Η έρευνα της ICAP πραγματοποιήθηκε τον Δεκέμβριο 2017, με ηλεκτρονικό ερωτηματολόγιο και το δείγμα ανήλθε σε 210 επιχειρήσεις[91]. Τα συμπεράσματα που προκύπτουν δεν είναι ιδιαίτερα αισιόδοξα όσον αφορά στο βαθμό ετοιμότητας των επιχειρήσεων **(Δ24)**.

Ειδικότερα, σύμφωνα με την έρευνα:

- 1 στις 4 επιχειρήσεις δηλώνει ότι δεν γνωρίζει τον νέο Κανονισμό. Το ποσοστό αυτό αυξάνεται σε 35% για τις επιχειρήσεις με λιγότερο από 100 εργαζομένους.
- Μερίδιο 22% δηλώνει ότι, ακόμα (Δεκέμβριος 2017), δεν γνωρίζει τον ορισμό των προσωπικών δεδομένων. Το ποσοστό αυτό αυξάνεται σε 32% για τις επιχειρήσεις που δραστηριοποιούνται στον κλάδο του Τουρισμού.

  Εκτιμάται ότι ακόμα και μεταξύ των επιχειρήσεων που δηλώνουν ότι γνωρίζουν τον ορισμό, ενδέχεται να περιλαμβάνονται αρκετές που νομίζουν ότι κατέχουν σχετική γνώση, ενώ στην πραγματικότητα δεν έχουν.
- Σχεδόν 1 στις 3 επιχειρήσεις δηλώνει ότι δεν επεξεργάζεται προσωπικά δεδομένα, εκτός από εκείνα των εργαζομένων της (π.χ. πελατών και προμηθευτών). Αξιοσημείωτο είναι - και αυτήν την περίπτωση - το υψηλότερο ποσοστό των τουριστικών επιχειρήσεων (40%).
- Σχεδόν 1 στις 4 επιχειρήσεις δηλώνει ότι δεν συμμορφώνεται στον Κανονισμό. Σε συνδυασμό με ποσοστό 58% των επιχειρήσεων που δηλώνει ότι συμμορφώνεται

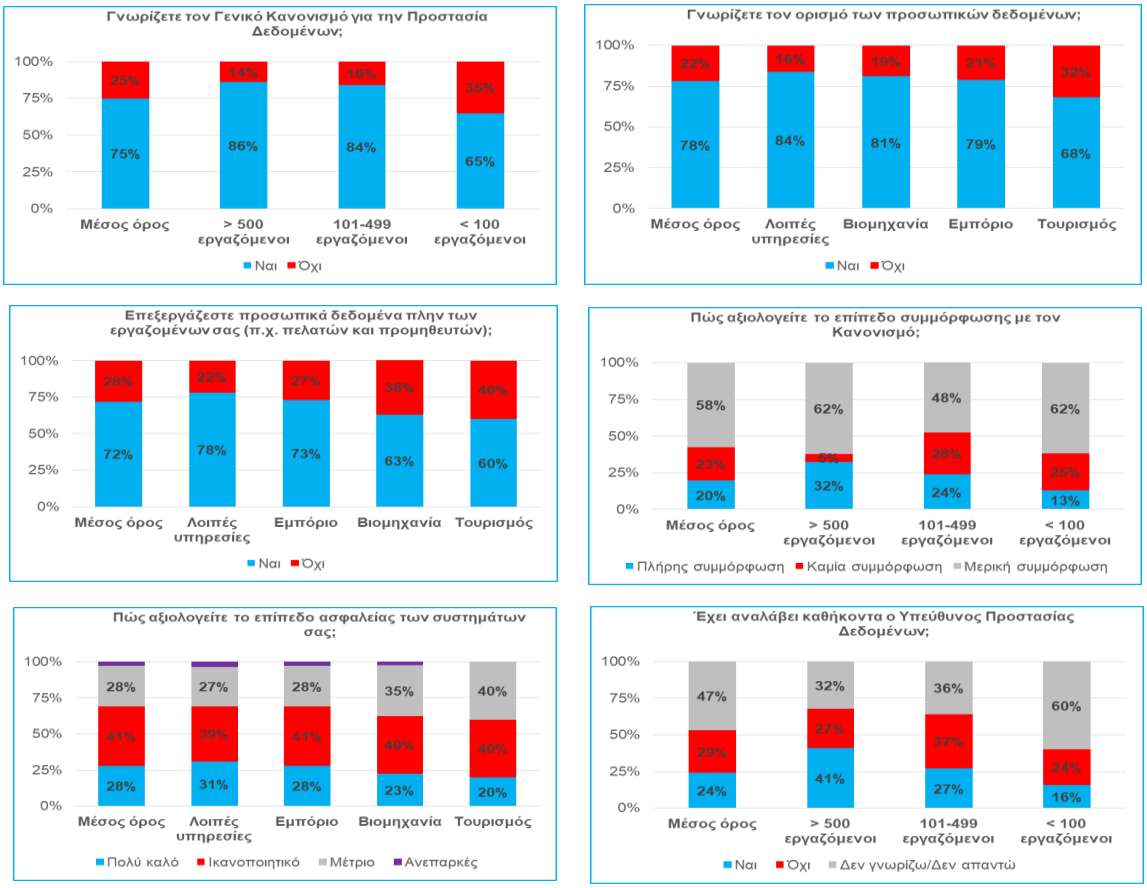
[91] Η έρευνα είναι διαθέσιμη **εδώ.**

μερικώς, διαπιστώνεται ότι απαιτείται άμεση δράση και εντατικοποίηση ενεργειών από την πλειονότητα των επιχειρήσεων. Ειδικά στις επιχειρήσεις με λιγότερους από 100 εργαζόμενους, το σωρευτικό ποσοστό μερική ή μη συμμόρφωσης ανέρχεται σε 87%.

- Μερίδιο 31% αξιολογεί ως μέτριο ή ανεπαρκές το επίπεδο ασφαλείας των συστημάτων του (και κατ' επέκταση των συστημάτων για την προστασία των προσωπικών δεδομένων). Ειδικά στις τουριστικές επιχειρήσεις το ποσοστό αυξάνεται σε 40%.
- Όσον αφορά στην ανάληψη καθηκόντων από τον Υπεύθυνο Προστασίας Δεδομένων, προκύπτει ότι σχεδόν 1 στις 2 επιχειρήσεις είτε δεν έχει κατανοήσει εάν υποχρεούται να προχωρήσει σε ορισμό ΥΠΔ είτε αγνοεί γενικώς τις σχετικές διατάξεις του Κανονισμού. Το ποσοστό αυτό αυξάνεται όσο μικρότερο είναι το μέγεθος των επιχειρήσεων, βάσει αριθμού εργαζομένων. Επομένως, παραμένει αναγκαία η αποσαφήνιση και περαιτέρω ενημέρωση των επιχειρήσεων σχετικά με τον ΥΠΔ.

Δ.24 Έρευνα για το επίπεδο συμμόρφωσης των επιχειρήσεων με τον Κανονισμό στην Ελλάδα

Πηγή: ICAP Management Consultants, Φεβρουάριος 2018



4.2.2 Η έρευνα του ΣΕΒ

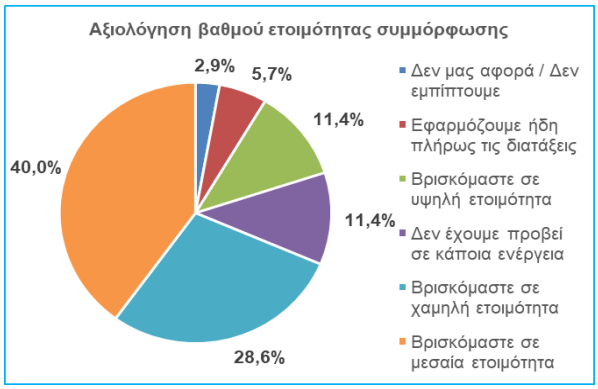
Η συγκεκριμένη - περιορισμένης έκτασης - έρευνα πραγματοποιήθηκε την περίοδο από 13 έως 23 Φεβρουαρίου 2018, αποκλειστικά σε επιχειρήσεις μέλη του ΣΕΒ και το δείγμα ανέρχεται σε 35 επιχειρήσεις.

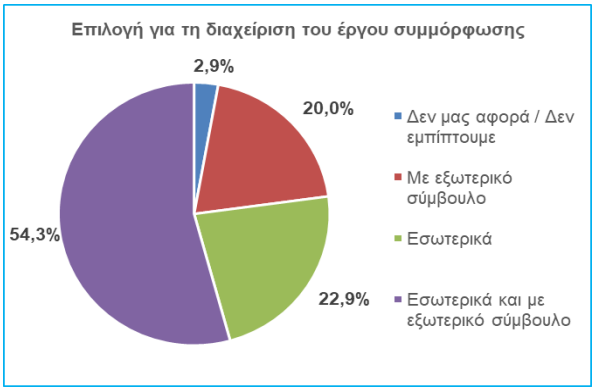
Παρακάτω παρουσιάζονται τα κυριότερα συμπεράσματα, τόσο για το βαθμό ετοιμότητας των επιχειρήσεων, όσο και για μια σειρά από άλλα ποιοτικού χαρακτήρα στοιχεία **(Δ25)**. Ειδικότερα:

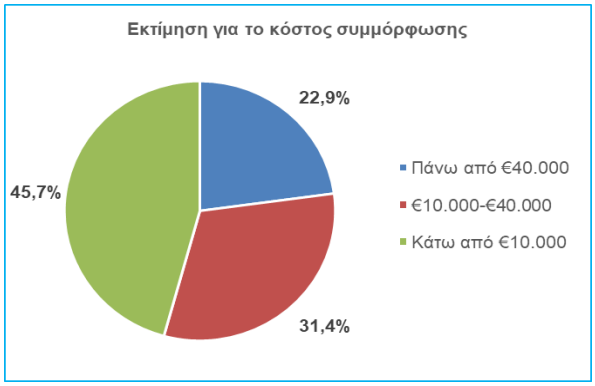
- **8 στις 10 επιχειρήσεις αξιολογούν ως μέτριο ή χαμηλό το βαθμό ετοιμότητας** ως προς τη συμμόρφωση με τον Κανονισμό, ή - χειρότερα - δεν έχουν προβεί ακόμα σε κάποια ενέργεια.
- **Περισσότερες από 1 στις 2 επιχειρήσεις δηλώνουν ότι διαχειρίζονται το έργο συμμόρφωσης συνδυαστικά, τόσο με ίδιες δυνάμεις, όσο και με τη χρήση εξωτερικού συμβούλου.** Το γεγονός αυτό μπορεί να ερμηνευθεί ως μια «ανασφάλεια» των επιχειρήσεων ως προς τη δυνατότητά τους να ανταποκριθούν στις διατάξεις του Κανονισμού και για το λόγο αυτό επιλέγουν και τη συμβολή ενός εξειδικευμένου εξωτερικού συμβούλου.
- Ως προς **το κόστος συμμόρφωσης, αυτό εκτιμάται μικρότερο από €40 χιλ. για το 77,1% του δείγματος.** Σημειώνεται ότι όλες οι επιχειρήσεις που δήλωσαν κόστος μεγαλύτερο από €40 χιλ. παρουσιάζουν Κύκλο Εργασιών πάνω από €100 εκ. (συνεπώς, διαφαίνεται μια συσχέτιση μεταξύ μεγέθους επιχείρησης και κόστους συμμόρφωσης).
- **2 στις 3 επιχειρήσεις αντιμετωπίζουν τον Κανονισμό ως ευκαιρία για ανασχεδιασμό των πολιτικών και διαδικασιών τους**, μήνυμα το οποίο μπορεί να εκληφθεί ως ιδιαίτερα αισιόδοξο, καθώς αποτυπώνει μια θετική νοοτροπία / προσέγγιση προς τον Κανονισμό, ισχυροποιώντας την πεποίθηση του ΣΕΒ περί αξιοποίησης του Κανονισμού και επίτευξης της επονομαζόμενης «έξυπνης συμμόρφωσης», βασισμένη σε τρεις αρχές που αναδεικνύουν εύληπτα και τα οφέλη που προκύπτουν από τον Κανονισμό (αναπτύσσεται αναλυτικά στην ενότητα 5.3).
- Οι **επιχειρήσεις αναγνωρίζουν την αναγκαιότητα πραγματοποίησης εκπαιδευτικών δράσεων**, προκειμένου να διαχυθούν στον οργανισμό τους οι νέες υποχρεώσεις και οι σχετικές πολιτικές και διαδικασίες που προκύπτουν από τον Κανονισμό: σχεδόν όλες έχουν ήδη προβεί, ή υλοποιούν, σχετικές δράσεις (88,6%).
- Η υψηλή τεχνικότητα και ο συνδυασμός ενεργειών που απαιτείται για την επίτευξη συμμόρφωσης στον Κανονισμό αναδεικνύεται εύληπτα στην έρευνα: **1 στις 2**

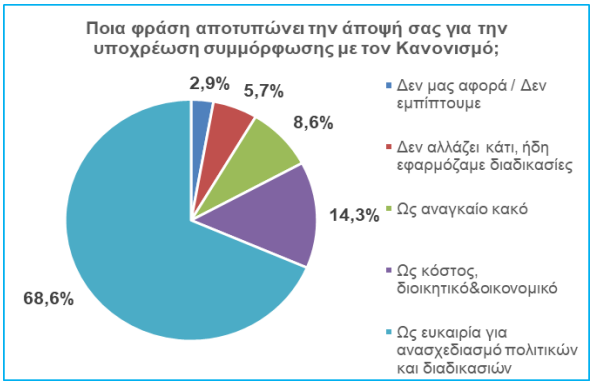
επιχειρήσεις δηλώνει ότι η **διαδικασία συμμόρφωσης περιλαμβάνει πολλαπλές δράσεις**, σε διαφορετικά αντικείμενα και επίπεδα, όπως σε: διαδικασίες και πολιτικές, πληροφοριακά συστήματα, εκπαίδευση προσωπικού, εταιρική κουλτούρα και συστήματα αρχειοθέτησης.

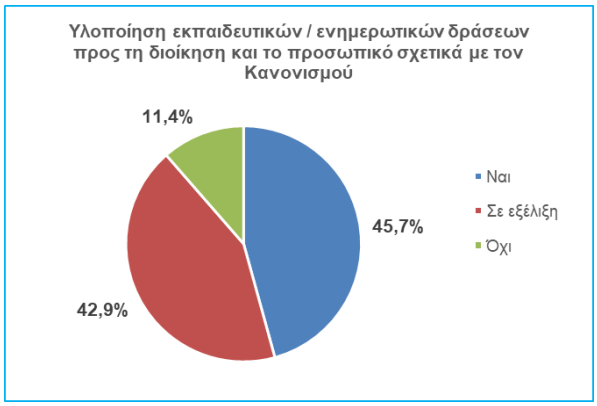
Δ.25 Συμμόρφωση επιχειρήσεων στον Κανονισμό και άλλα στοιχεία
Πηγή: Έρευνα ΣΕΒ, Φεβ. 2018

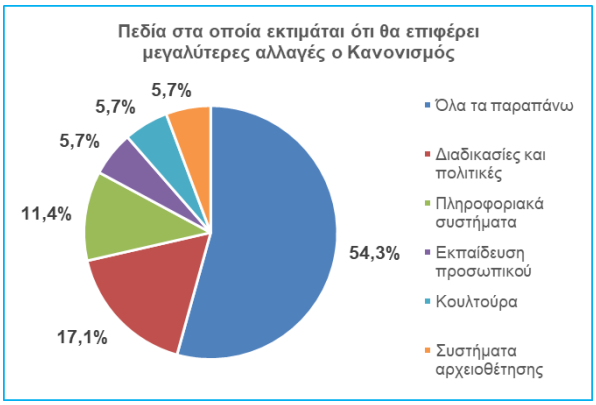












4.2.3 Συνοπτικά συμπεράσματα

Τα βασικά συμπεράσματα των δυο ερευνών συνοψίζονται ως εξής:

- Η πλειονότητα των επιχειρήσεων θα έχει καταφέρει να πετύχει **μερική μόνο συμμόρφωση** στο νέο Κανονισμό έως το Μάιο του 2018, όπως καταγράφεται και στις έρευνες στο εξωτερικό.
- Ωστόσο, ιδιαίτερη ανησυχία προκαλεί ο **χαμηλός βαθμός συμμόρφωσης των επιχειρήσεων με λιγότερους από 100 εργαζόμενους**.
- Η **ανάληψη καθηκόντων από τον ΥΠΔ**, και όπως αυτή συνδέεται ευρύτερα με τα θέματα των καθηκόντων και αρμοδιοτήτων του, φαίνεται να **δυσκολεύει ιδιαίτερα τις ελληνικές επιχειρήσεις**, σε αντίθεση με το εξωτερικό όπου δεν αποτυπώνεται κάτι αντίστοιχο στις έρευνες. Αυτό μπορεί να ερμηνευθεί ότι επιβεβαιώνει τις δυσκολίες της εγχώριας αγοράς να προσαρμοστεί στις απαιτήσεις του νέου Κανονισμού.
- Η **συνεργασία με εξωτερικό σύμβουλο** είναι ιδιαίτερα διαδεδομένη, γεγονός που μπορεί να ερμηνευθεί ως μια «ανασφάλεια» των επιχειρήσεων ως προς τη δυνατότητά τους να ανταποκριθούν στις διατάξεις του Κανονισμού.
- Διαφαίνεται μια **συσχέτιση μεταξύ μεγέθους επιχείρησης βάσει Κύκλου Εργασιών και κόστους του έργου συμμόρφωσης με τον Κανονισμό**. Σε κάθε περίπτωση, η πλειονότητα των επιχειρήσεων δηλώνει ότι το κόστος ήταν χαμηλότερο από €40 χιλ.
- Το κεντρικό μήνυμα που προκύπτει μέσα από τη διαδικασία συμμόρφωσης με τον Κανονισμό είναι ότι αποτελεί **ευκαιρία για ανασχεδιασμό των πολιτικών και διαδικασιών** των επιχειρήσεων.
- Όπως καταγράφεται και στις έρευνες του εξωτερικού, προτεραιότητα λαμβάνουν οι **δράσεις εκπαίδευσης του προσωπικού**.

Με βάση τα συμπεράσματα που προκύπτουν από τις έρευνες, απαιτείται εντατικοποίηση των προσπαθειών των επιχειρήσεων για την επίτευξη της συμμόρφωσης με τον Κανονισμό. Στο επόμενο Κεφάλαιο αναδεικνύονται τα βήματα που οφείλει να ακολουθήσει κάθε οργανισμός προκειμένου, όχι απλά να πετύχει μια τυπική συμμόρφωση, αποφεύγοντας δυσάρεστες εξελίξεις όπως επιβολή προστίμων, αλλά να μεταβάλλει ουσιαστικά τις δομές του, προστατεύοντας τη φήμη του και βελτιώνοντας το επιχειρηματικό του πλάνο.

5. Οδηγός συμμόρφωσης για τις επιχειρήσεις

5. Οδηγός συμμόρφωσης για τις επιχειρήσεις

Κύριος στόχος της παρούσας Μελέτης είναι η ανάπτυξη ενός εύχρηστου «οδηγού συμμόρφωσης» με τον Κανονισμό για τις επιχειρήσεις. Φιλοδοξία της συντακτικής ομάδας αποτελεί το παρόν κείμενο να τις βοηθήσει με πρακτικό τρόπο να κατανοήσουν τα οφέλη που μπορούν να προκύψουν από τη διαδικασία συμμόρφωσης, τις απαιτήσεις συμμόρφωσης και τον τρόπο επίτευξης αυτής. Ιδίως για τις μικρές και μεσαίες επιχειρήσεις, με το κόστος συμμόρφωσης να είναι ενδεχομένως δυσανάλογα μεγάλο, η ύπαρξη ενός απλού εισαγωγικού οδηγού αναμένεται να έχει μεγαλύτερη ωφέλεια, όχι μόνο για την πρώτη περίοδο συμμόρφωσης και τις ελάχιστες αναγκαίες ενέργειες στις οποίες οι επιχειρήσεις αναμένεται ήδη να έχουν προβεί, όσο κυριότερα στον τρόπο με τον οποίο θα προσεγγίζουν το θέμα στο εξής, ενσωματώνοντάς τις αρχές και υποχρεώσεις του Κανονισμού στην κουλτούρα και κατ' επέκταση στη λειτουργία της επιχείρησής τους.

Αξίζει επίσης να σημειωθεί ότι παρόλο που η Μελέτη εστιάζεται αποκλειστικά στις ιδιωτικές επιχειρήσεις, δεν θα πρέπει να παραβλέπει κανείς τις σημαντικές απαιτήσεις συμμόρφωσης που προκύπτουν για τους φορείς του δημοσίου και άρα τη δυνητική ωφέλεια που ο ίδιος αυτός οδηγός μπορεί να έχει και για τους οργανισμούς του δημόσιου τομέα. Με τις απαιτούμενες προσαρμογές, τα βήματα που προβλέπει μπορούν να φανούν χρήσιμα και για τις υπηρεσίες και φορείς του δημοσίου, οι οποίες υπολείπονται στις περισσότερες των περιπτώσεων έναντι των ιδιωτικών επιχειρήσεων ως προς τις δράσεις συμμόρφωσης.

Για ένα μάλλον μεγάλο αριθμό επιχειρήσεων ο νέος Κανονισμός αποτελεί στην πράξη άλλη μια υποχρέωση που «πρέπει να εκπληρώσουν», αναθέτοντας σε κάποιο εξωτερικό σύμβουλο τη σύνταξη κάποιας έκθεσης (την οποία θα διατηρούν «ξεχασμένη» σε κάποιο συρτάρι), αγοράζοντας κάποια πρόσθετα πληροφοριακά συστήματα (τα οποία ούτε καν θα αναβαθμίζουν) και αναθέτοντας την ιδιότητα του ΥΠΔ σε ένα στέλεχος που διαθέτει ήδη μερικές ακόμη (π.χ. Υπεύθυνος Κανονιστικής Συμμόρφωσης, Νομικός Σύμβουλος κ.λπ.). Δηλαδή, ως μια υποχρέωση στατική, σημειακή και πάντως όχι ως οργανικό κομμάτι της λειτουργίας ή της κουλτούρας τους. Αυτή η προσέγγιση πρέπει να αλλάξει πριν καν εδραιωθεί και ο οδηγός που ακολουθεί, όπως και το σύνολο της παρούσας μελέτης μπορεί να συμβάλει στην ανάδειξη της πραγματικής συμβολής του Κανονισμού στον εκσυγχρονισμό των ελληνικών επιχειρήσεων. Για ένα μικρότερο αριθμό επιχειρήσεων (που ευελπιστούμε να μεγαλώσει) ο νέος Κανονισμός αποτελεί μια ευκαιρία να αποκτήσουν ανταγωνιστικό

πλεονέκτημα και να ενισχύσουν την αξία τους, επενδύοντας στην ασφάλεια των δεδομένων, πελατών, προμηθευτών και προσωπικού και αυτό επιδιώκουμε να προβάλουμε.

Για τον ΣΕΒ, σκοπός δεν πρέπει να είναι η εφαρμογή του Κανονισμού «μόνο στα χαρτιά». Πραγματική στόχευση αυτής της «υποχρεωτικής άσκησης» στην οποία θα υποβληθούν όλοι οι οργανισμοί είναι η ουσιαστική αλλαγή της κουλτούρας των επιχειρήσεων, με επίκεντρο τη διαφύλαξη των προσωπικών δεδομένων. Σε αυτό το πλαίσιο, στις επόμενες ενότητες του παρόντος Κεφαλαίου παρουσιάζουμε **τον τρόπο με τον οποίο μπορεί να υπάρξει μια ουσιαστική αλλά και έξυπνη συμμόρφωση**, που δεν θα επιβαρύνει με σημαντικό χρηματικό και διοικητικό κόστος την καθημερινή λειτουργία των επιχειρήσεων.

Ειδικότερα, αναφερόμαστε σε εκείνες τις ενέργειες στις οποίες πρέπει να προβούν οι επιχειρήσεις, προκειμένου να συμμορφωθούν στις απαιτήσεις του Κανονισμού, δηλαδή να είναι σε θέση να αποδείξουν ότι έχουν λάβει όλα τα απαραίτητα μέτρα για την προστασία των προσωπικών δεδομένων που διαχειρίζονται[92] και υποστηρίζουμε ότι μέσα από αυτή τη διαδικασία προκύπτουν πολλαπλά οφέλη.

Είναι σημαντικό να διευκρινιστεί ότι η λίστα των ενεργειών δεν είναι εξαντλητική, ούτε μοναδική (δεν υφίσταται δηλαδή μία λύση για όλους). Όμως, κάθε επιχείρηση, με βάση τις δικές τις ανάγκες, τα χαρακτηριστικά (φύση και όγκος δεδομένων), το μέγεθος, το αντικείμενο των εργασιών και τη στρατηγική της, μπορεί να προσαρμοστεί σε αυτόν τον «οδηγό» και να πετύχει το σκοπό της[93].

Σημειώνεται ότι για τον ΣΕΒ, **τρεις είναι οι βασικές προϋποθέσεις** με οριζόντια ισχύ, **προτού μία επιχείρηση εκκινήσει την προσπάθειά της να ακολουθήσει τα βήματα για την ορθή εφαρμογή του Κανονισμού**, δίχως τις οποίες δεν μπορεί να επιτευχθεί η συμμόρφωση.

[92] Σημειώνεται ότι η λίστα ενεργειών είναι ενδεικτική και αποτελεί ένα «οδηγό κατευθύνσεων» προς τις επιχειρήσεις. Ωστόσο, σε καμία περίπτωση η υιοθέτηση αυτών των βημάτων δεν αποτελεί τεκμήριο πλήρους συμμόρφωσης με τον Κανονισμό. Επιπλέον, μέχρι την ψήφιση του εφαρμοστικού Νόμου, αλλά και την εφαρμογή του Κανονισμού στην πράξη, είναι πιθανό να προκύψουν αλλαγές στα «βήματα συμμόρφωσης» ή νέες συνθήκες στις οποίες θα πρέπει να προσαρμοστούν οι επιχειρήσεις και οι οποίες δεν είναι γνωστές αυτή τη στιγμή.

[93] Σημειώνεται ότι σε αντίστοιχες ενέργειες μπορούν (και πρέπει) να προβούν και οι φορείς του δημοσίου τομέα.

Πρώτον, απαιτείται η ευαισθητοποίηση και δέσμευση της ανώτατης διοίκησης, να κατανοήσει δηλαδή την αναγκαιότητα συμμόρφωσης και έμπρακτα να αποφασίσει να δράσει προς αυτήν την κατεύθυνση.

Δεύτερον, απαιτείται εξασφάλιση του σχετικού προϋπολογισμού, ο οποίος είναι απαραίτητος για την υλοποίηση του πλάνου συμμόρφωσης.

Τρίτον, είναι σημαντικό να ενημερωθεί το σύνολο του προσωπικού για το νέο νομικό πλαίσιο και τις επερχόμενες αλλαγές, διαφορετικά θα προκύψουν προβλήματα στην υλοποίηση.

Δ.26 Οι βασικές προϋποθέσεις για τη συμμόρφωση με τις προβλέψεις του Κανονισμού
✓ Δέσμευση της ανώτατης διοίκησης
✓ Εξασφάλιση του σχετικού προϋπολογισμού
✓ Ενημέρωση του συνόλου του προσωπικού για το νέο νομικό πλαίσιο και τις επερχόμενες αλλαγές

5.1 Τα προτεινόμενα βήματα για την ορθή εφαρμογή του Κανονισμού

Τα προτεινόμενα βήματα για την ορθή εφαρμογή του Κανονισμού από τις επιχειρήσεις έχουν ως εξής:

1ο Βήμα | Σύσταση Ομάδας Εργασίας

Αφορά στη **σύσταση Ομάδα Εργασίας, η οποία θα απαρτίζεται από εκπροσώπους των Διευθύνσεων που εμπλέκονται περισσότερο με την προστασία των προσωπικών δεδομένων.** Ενδεικτικά, αναφέρονται οι Διευθύνσεις Πληροφορικής, Νομικής και Ανθρώπινου Δυναμικού, οι οποίες σχετίζονται εξ ορισμού λόγω του αντικειμένου τους. Στις επιχειρήσεις που τα προσωπικά δεδομένα αποτελούν βασικό αντικείμενο της δραστηριότητας (π.χ. εταιρείες τηλεπικοινωνιών, ασφαλιστικές, τράπεζες), τότε είναι προφανές ότι πρέπει να συμμετέχει και, τουλάχιστον ένας, εκπρόσωπος από κάθε επιχειρησιακή Διεύθυνση (ως "business owner"). Με αυτόν τον τρόπο, εξασφαλίζεται η αρμονική συμμετοχή όλων των εμπλεκομένων και η παροχή της απαιτούμενης βοήθειας και υποστήριξης του ΥΠΔ. Σε κάθε περίπτωση, η Ομάδα Εργασίας πρέπει να έχει μικρό και ευέλικτο μέγεθος, αλλά και δυνατότητα λήψης αποφάσεων.

2ο Βήμα | Ορισμός Υπεύθυνου Προστασίας Δεδομένων (ΥΠΔ)[94]

Πρόκειται για **υποχρεωτικό βήμα για όσες επιχειρήσεις προβαίνουν σε μεγάλης κλίμακας επεξεργασία προσωπικών δεδομένων, προαιρετικό για τις υπόλοιπες**. Ο ΥΠΔ συμβουλεύει την επιχείρηση για τις υποχρεώσεις που απορρέουν από τον Κανονισμό και παρακολουθεί τις ενέργειες συμμόρφωσης με αυτόν. Συμμετέχει ενεργά σε όλα τα ζητήματα που σχετίζονται με τον Κανονισμό και αποτελεί το πρόσωπο επικοινωνίας τόσο με τα υποκείμενα των δεδομένων όσο και με την εποπτική Αρχή. Ο ΥΠΔ πρέπει να είναι άτομο κατάλληλα καταρτισμένο και προσεκτικά επιλεγμένο ώστε να είναι σε θέση να διεκπεραιώσει τις υποχρεώσεις του, δίχως σύγκρουση συμφερόντων. Στους οργανισμούς που κριθεί απαραίτητο (π.χ. λόγω μεγάλου όγκου προσωπικών δεδομένων) ο ΥΠΔ μπορεί να έχει υπό την ευθύνη του ολόκληρη ομάδα στελεχών.

94 Δείτε επιπλέον στοιχεία στην **ενότητα 5.5 «Συχνές Ερωτήσεις και Απαντήσεις για τις επιχειρήσεις»** της παρούσας Μελέτης.

3ο Βήμα| Χαρτογράφηση της ροής των δεδομένων (data mapping)

Η χαρτογράφηση της πορείας των δεδομένων προσωπικού χαρακτήρα που τηρούνται και επεξεργάζονται εντός επιχείρησης (δηλαδή των δεδομένων προσωπικού, πελατών, προμηθευτών και τρίτων προσώπων) **αποτελεί μια διαδικασία μέσω της οποίας απαντώνται τα εξής ερωτήματα: τί είδους δεδομένα, για ποιο σκοπό, πόσο συχνά, πώς αποκτώνται, πού υπάρχουν, ποιος έχει πρόσβαση και τα επεξεργάζεται, για πόσο χρόνο διακρατούνται.** Για την ολοκλήρωση της διαδικασίας χαρτογράφησης, προτείνεται η χρήση ερωτηματολογίων και η πραγματοποίηση συνεντεύξεων ανά Διεύθυνση, προκειμένου να γίνει πλήρης καταγραφή / αποτύπωση της υφιστάμενης κατάστασης της επιχείρησης. Μέσα από αυτή τη διαδικασία, δημιουργείται, επί της ουσίας, το επονομαζόμενο «Αρχείο Δραστηριοτήτων Επεξεργασίας» (άρθρο 30 του Κανονισμού), το οποίο στη συνέχεια πρέπει να είναι συνεχώς επικαιροποιημένο, ώστε, σε ενδεχόμενο έλεγχο, να αποτελεί στοιχείο απόδειξης της συμμόρφωσης της κάθε επιχείρησης. Πρόκειται για ένα πολύ σημαντικό στάδιο της διαδικασίας συμμόρφωσης, το οποίο στην ουσία «ξεκλειδώνει» τα επόμενα βήματα.

4ο Βήμα | Εντοπισμός και ανάλυση κινδύνων και ελλείψεων

Αξιοποιώντας την πλήρη γνώση της ροής των προσωπικών δεδομένων (3ο βήμα), η **επιχείρηση οφείλει να καταγράψει τους πιθανούς κινδύνους και τις ελλείψεις που - ενδεχομένως - εντοπίστηκαν** (να πραγματοποιήσει δηλαδή την επονομαζόμενη “gap analysis”). Έτσι **καταρτίζεται ένας πίνακας ο οποίος περιέχει τις δραστηριότητες που εντοπίστηκαν με ελλείψεις, την προτεραιοποίησή τους με βάση τον κίνδυνο που ενέχουν και τις προτεινόμενες ενέργειες για την αντιμετώπισή τους.** Παραδείγματα σχετικών «κενών» είναι: πολύ μεγάλη περίοδος διατήρησης των δεδομένων άνευ λόγου, διατήρηση των ίδιων δεδομένων σε περισσότερα του ενός σημεία και ανεμπόδιστη πρόσβαση σε δεδομένα από όλα τα στελέχη ενώ δεν χρειάζεται.

5ο Βήμα | Εκπόνηση Εκτίμησης Αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑ)[95]

Πρόκειται για **υποχρεωτικό βήμα για όσες επιχειρήσεις προβαίνουν σε επεξεργασία που ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, προαιρετικό για τις υπόλοιπες**. Η εκπόνηση της ΕΑ εξ ορισμού προηγείται της επεξεργασίας των δεδομένων και **περιλαμβάνει ανάλυση για τις πιθανότητες επέλευσης κινδύνων και τις συνέπειες στα προσωπικά δεδομένα.** Καταλήγει σε κατηγοριοποίηση των δραστηριοτήτων επεξεργασίας σε υψηλού, μεσαίου και χαμηλού κινδύνου και σε επανεξέταση των απαιτούμενων διαδικασιών σε κάθε περίπτωση. Σημειώνεται ότι οι πολιτικές και διαδικασίες της επιχείρησης πρέπει, όπου αυτό είναι δυνατόν, να λαμβάνουν υπόψη την αρχή της προστασίας των δεδομένων ήδη από το σχεδιασμό (privacy by default). Δηλαδή, όποτε αυτό είναι δυνατόν, ο Υπεύθυνος Επεξεργασίας να εφαρμόζει κατά τη στιγμή του καθορισμού των μέσων επεξεργασίας αλλά και της ίδιας της επεξεργασίας, κατάλληλα τεχνικά και οργανωτικά μέτρα, σχεδιασμένα για την εφαρμογή των αρχών προστασίας των δεδομένων.

6ο Βήμα | Αναθεώρηση πολιτικών και διαδικασιών

Με βάση τα συμπεράσματα των βημάτων 4 και 5, η επιχείρηση προβαίνει σε **αναθεώρηση των πολιτικών και των διαδικασιών τήρησης και επεξεργασίας δεδομένων προσωπικού χαρακτήρα[96]**. Τέτοια παραδείγματα αποτελούν ενδεικτικά τα εξής: οριστική διαγραφή και καταστροφή δεδομένων με το πέρας Χ ετών, διαμόρφωση κοινού γλωσσάριου ώστε να υπάρχει σωστή και κοινή κατανόηση από όλο το προσωπικό, θέσπιση πολιτικής «καθαρού γραφείου», απαγόρευση εξόδου από την επιχείρηση USB sticks και laptops, απαγόρευση αντιγραφής αρχείων από το σκληρό δίσκο σε USB sticks και εξωτερικούς δίσκους, ανάπτυξη πολιτικής διαβαθμισμένης πρόσβασης, ανάπτυξη πολιτικής για τις διαδρομές των φυσικών αρχείων εντός της επιχείρησης, θέσπιση ορισμένου χρόνου διατήρησης CVs κ.λπ.

---

95 Δείτε **εδώ** την προτεινόμενη μεθοδολογία της Commission Nationale de l'Informatique et des Libertés - CNIL (Εθνικής Επιτροπής Πληροφορικής και Ελευθεριών) για την εκπόνηση ΕΑ, **εδώ** σχετικό παράδειγμα ειδικά για τις συσκευές "Internet of Things" και **εδώ** κώδικα πρακτικής για τα προτεινόμενα μέτρα ενάντια στους κινδύνους.

96 Οι πολιτικές και διαδικασίες της επιχείρησης πρέπει, όπου αυτό είναι δυνατόν, να λαμβάνουν υπόψη την αρχή της προστασίας των δεδομένων ήδη από το σχεδιασμό (privacy by default). Δηλαδή, όποτε αυτό είναι δυνατόν, ο Υπεύθυνος Επεξεργασίας να εφαρμόζει κατά τη στιγμή του καθορισμού των μέσων επεξεργασίας αλλά και της ίδιας της επεξεργασίας, κατάλληλα τεχνικά και οργανωτικά μέτρα, σχεδιασμένα για την εφαρμογή των αρχών προστασίας των δεδομένων.

7ο Βήμα | Αξιοποίηση των εργαλείων πληροφορικής

Κάθε επιχείρηση ανάλογα με τη φύση των εργασιών της, τα μεγέθη και τις δυνατότητές της, **οφείλει να αξιοποιήσει κάποια από τα εργαλεία πληροφορικής που ενισχύουν την ασφάλεια των συστημάτων**. Ενδεικτικά παραδείγματα αποτελούν: εργαλεία που με αυτοματοποιημένο τρόπο χαρτογραφούν τα δεδομένα (3ο βήμα), εργαλεία που αξιολογούν την αποτελεσματικότητα των πολιτικών και διαδικασιών που έχουν αναπτυχθεί και εργαλεία που βοηθούν στην αποτροπή ή τον εντοπισμό των αποπειρών παραβίασης δεδομένων. Επιπλέον, η κρυπτογράφηση και η ψευδωνυμοποίηση αποτελούν δύο εκ των απλούστερων τεχνικών μέτρων προστασίας (βλ. παρακάτω αναλυτικά).

8ο Βήμα | Ανάπτυξη διαδικασιών γνωστοποίησης εποπτικής Αρχής και ανακοίνωσης υποκειμένου[97]

Πρόκειται για δύο υποχρεωτικές διαδικασίες για κάθε επιχείρηση. Η πρώτη αφορά στη **διαδικασία γνωστοποίησης της παραβίασης δεδομένων προσωπικού χαρακτήρα στην εποπτική Αρχή, εντός μόλις 72 ωρών από τη στιγμή που η επιχείρηση αποκτά γνώση του γεγονότος[98].** Το σύντομο χρονικό διάστημα που προβλέπεται είναι προφανές ότι αυξάνει το βαθμό δυσκολίας. Η δεύτερη αφορά στη **διαδικασία άμεσης ανακοίνωσης της παραβίασης δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων, όταν υπάρχει ενδεχόμενο να τεθούν σε υψηλό κίνδυνο τα δικαιώματα και οι ελευθερίες του[99].** Ο επικοινωνιακός χειρισμός σε αυτήν την περίπτωση είναι κρίσιμης σημασίας και μπορεί να κάνει τη διαφορά όσον αφορά στη φήμη της επιχείρησης.

---

97 Δείτε εδώ τις Κατευθυντήριες Οδηγίες της Ομάδας Εργασίας άρθρου 29 για τη γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα.

98 Κατά το άρθρο 33 του Κανονισμού, η γνωστοποίηση προς την Αρχή πρέπει να περιλαμβάνει, κατ' ελάχιστο: α) τη φύση της παραβίασης, συμπεριλαμβανομένων, όπου είναι δυνατό, των κατηγοριών και του κατά προσέγγιση αριθμού των επηρεαζόμενων υποκειμένων, καθώς και αντίστοιχα των επηρεαζόμενων αρχείων, β) το όνομα και τα στοιχεία επικοινωνίας του ΥΠΔ για περισσότερες πληροφορίες, γ) τις ενδεχόμενες συνέπειες της παραβίασης και δ) τα ληφθέντα, ή έστω τα προτεινόμενα προς λήψη, μέτρα από τον Υπεύθυνο Επεξεργασίας για την αντιμετώπιση της παραβίασης και της άμβλυνσης των ενδεχόμενων δυσμενών συνεπειών.

99 Στο άρθρο 34 του Κανονισμού προβλέπεται ότι στην ανακοίνωση προς το υποκείμενο πρέπει να περιγράφεται με σαφήνεια η φύση της παραβίασης και να περιέχονται τουλάχιστον οι πληροφορίες και τα μέτρα που προαναφέρθηκαν στην περίπτωση της γνωστοποίησης προς την Αρχή. Ωστόσο, υφίστανται εξαιρέσεις για την υποχρέωση ανακοίνωσης, σε συγκεκριμένες περιπτώσεις (π.χ. ο Υπεύθυνος Επεξεργασίας εφάρμοσε κατάλληλα τεχνικά και οργανωτικά μέτρα προστασίας των δεδομένων, έλαβε μέτρα που διασφαλίζουν ότι δεν είναι πλέον πιθανό να προκύψει υψηλός κίνδυνος κ.ά.).

9ο Βήμα | Δοκιμαστικοί έλεγχοι συστημάτων και διαδικασιών

Πρόκειται για το τελευταίο χρονικά στάδιο. Αναφέρεται σε **δοκιμαστικούς ελέγχους επί των συστημάτων και διαδικασιών που έχει αναπτύξει η επιχείρηση στα προηγούμενα βήματα, ώστε να αποδειχθεί ότι μετά την 25η Μαΐου 2018 οι ενέργειες συμμόρφωσης δούλεψαν αποτελεσματικά στην πράξη**. Ενδεχομένως να οδηγήσει σε ανάγκη υλοποίησης διορθωτικών παρεμβάσεων.

10ο Βήμα |Διαρκής παρακολούθηση και επικαιροποίηση των διαδικασιών και των συστημάτων

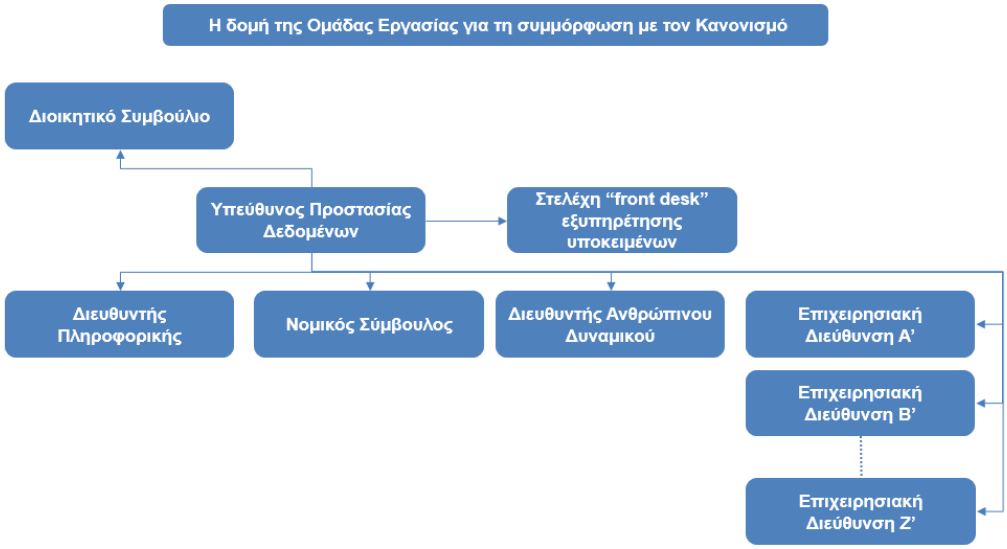
Η συμμόρφωση στον Κανονισμό είναι μια **δυναμική «άσκηση» και στο πλαίσιο αυτό οι επιχειρήσεις οφείλουν συνεχώς να επικαιροποιούν τις διαδικασίες τους** (ή έστω να εξετάζουν την αναγκαιότητα επικαιροποίησής τους) και **να αναβαθμίζουν τα συστήματά τους.** Επιβάλλεται συνεχής επαγρύπνηση και διαρκής παρακολούθηση, καθώς οι κίνδυνοι παραβίασης των δεδομένων είναι πιθανοί ανά πάσα στιγμή. Με άλλα λόγια, όπως στο βήμα 9 συστήνονται δοκιμαστικοί έλεγχοι των συστημάτων και διαδικασιών πριν την έναρξη εφαρμογής του Κανονισμού, όμοια προτείνονται αντίστοιχες δοκιμές και μετά την έναρξη εφαρμογής του.

+1 Βήμα | Εκπαίδευση προσωπικού

Η **επιχείρηση οργανώνει εκπαιδευτικές δράσεις, προς το σύνολο του προσωπικού, προκειμένου να εξασφαλίσει ότι όλοι γνωρίζουν τις πολιτικές και τις διαδικασίες που έχουν αναπτυχθεί για την προστασία των προσωπικών δεδομένων, γιατί είναι σημαντικές για την επιχείρηση, αλλά και τί πρέπει να κάνουν σε περίπτωση που αντιληφθούν απειλή παραβίασης.** Οι εν λόγω δράσεις προτείνεται να επαναλαμβάνονται, με βάση τις ανάγκες και τα χαρακτηριστικά κάθε επιχείρησης (π.χ. δραστηριότητα υψηλού κινδύνου, μεγάλη / συχνή αλλαγή προσωπικού, σημαντικές αλλαγές επί των πολιτικών και διαδικασιών κ.λπ.).

Δ.27 10+1 προτεινόμενα βήματα για την ορθή εφαρμογή του Κανονισμού από τις επιχειρήσεις

Δ.28 Η δομή της Ομάδας Εργασίας για τη συμμόρφωση με τον Κανονισμό



Δ.29 Περί ορισμού του ΥΠΔ

Ένα ζήτημα που απασχολεί αρκετά τους Υπευθύνους Επεξεργασίας είναι ποιο είναι το κατάλληλο πρόσωπο να οριστεί ως ΥΠΔ, εφόσον αυτό προβλέπεται από τον Κανονισμό (ή εφόσον ο ίδιος ο οργανισμός το έχει επιλέξει).

Αφετηρία της απόφασης αυτής αποτελούν τα πραγματικά **προσόντα** του, γι' αυτό και είναι προφανές ότι ο ΥΠΔ πρέπει να έχει μια βαθιά γνώση του Κανονισμού και κατανόηση των προβλέψεών του. Ως εκ τούτου, επαγγελματίες με νομικό υπόβαθρο ή/και τεχνογνωσία στις πρακτικές προστασίας δεδομένων έχουν σαφές «προβάδισμα», δίχως ωστόσο αυτό να είναι περιοριστικό ή να υποδεικνύει περιοριστικά αντικείμενα σπουδών / επαγγελματικούς τίτλους που είναι περισσότερο ενδεδειγμένοι. Ο Κανονισμός δημιουργεί πλέον από μόνος του ένα νέο διεπιστημονικό αντικείμενο και ένα νέο τύπο στελέχους /επαγγελματία.

Όσον αφορά στα **ζητήματα σύγκρουσης συμφερόντων**, απαιτείται ιδιαίτερη προσοχή από τους Υπευθύνους Επεξεργασίας. Είναι προφανές ότι ο ΥΠΔ δεν μπορεί ταυτόχρονα να κατέχει και θέση από την οποία μπορεί να καθορίζει τους σκοπούς και τα μέσα της επεξεργασίας. Για παράδειγμα, ο Διευθυντής Πληροφορικής είναι το άτομο της ανώτατης διοίκησης που αποφασίζει για τα συστήματα και τους μηχανισμούς ασφαλείας για την επεξεργασία δεδομένων στον οργανισμό, επομένως δεν μπορεί να είναι και το άτομο που παρακολουθεί και τη συμμόρφωση με τις προβλέψεις του Κανονισμού. Ομοίως ισχύει και για το Νομικό Σύμβουλο του οργανισμού.

Ταυτόχρονα, οι Υπεύθυνοι Επεξεργασίας πρέπει να αντιληφθούν ότι στην ουσία ο ΥΠΔ είναι ένας **project manager** και ως εκ τούτου, η θέση του έχει υψηλές απαιτήσεις για συγκεκριμένα προσόντα και χαρακτηριστικά, όπως υπευθυνότητα και εμπιστευτικότητα, τήρηση χρονοδιαγραμμάτων, τήρηση πολιτικών και διαδικασιών, επικοινωνιακές δεξιότητες, δεξιότητες συντονισμού ομάδας και συνεργασίας κ.ά. Παράλληλα, ο ΥΠΔ πρέπει να έχει αντίληψη του τομέα δραστηριότητας του οργανισμού στον οποίο απασχολείται.

Σε **σχέση με την Ομάδα Εργασίας** και τον ΥΠΔ, υπογραμμίζεται ότι επί της ουσίας ο ΥΠΔ έχει το συντονιστικό ρόλο. Όπως προαναφέρθηκε, είναι σημαντικό στην Ομάδα Εργασίας να συμμετέχει υπεύθυνος εκπρόσωπος από τις Διευθύνσεις Πληροφορικής, Νομικής και Ανθρώπινου Δυναμικού, οι οποίες εμπλέκονται εξ ορισμού λόγω του αντικειμένου τους, Επιπλέον, συστήνεται να συμμετέχει ένας εκπρόσωπος από κάθε επιχειρησιακή Διεύθυνση, ώστε να εξασφαλίζεται ότι η διαδικασία συμμόρφωσης με τον Κανονισμό ευθυγραμμίζεται με τη λειτουργία του οργανισμού, ότι παρέχεται η απαιτούμενη ανατροφοδότηση / επικοινωνία από και προς τις επιχειρησιακές Διευθύνσεις κ.λπ.

Τέλος, ειδικά σε μεγάλους οργανισμούς, βάσει όγκου προσωπικών δεδομένων, είναι προφανές ότι ο ΥΠΔ χρειάζεται να υποστηριχθεί από στελέχη, υπό την επίβλεψή του, για την εξυπηρέτηση των υποκειμένων (ως front desk). Μπορεί κανείς εύκολα να φανταστεί για μια ασφαλιστική επιχείρηση ή μια επιχείρηση κινητής τηλεφωνίας τον όγκο των αιτημάτων προς τον ΥΠΔ, η διαχείριση των οποίων πρέπει να γίνει σε σαφώς ορισμένα χρονοδιαγράμματα από τον Κανονισμό, αλλά κυρίως με τρόπο που θα προστατεύουν τα συμφέροντα και περισσότερο τη φήμη του οργανισμού.

Δ.30 Παράδειγμα Αρχείου Δραστηριοτήτων Επεξεργασίας[100]

1	ΥΠΕΥΘΥΝΟΣ ΕΠΕΞΕΡΓΑΣΙΑΣ					
2	Όνομα και στοιχεία επικοινωνίας		Υπεύθυνος Προστασίας Δεδομένων (αν υφίσταται)		Εκπρόσωπος (αν υφίσταται)	
3	Όνομα		Όνομα		Όνομα	
4	Ταχυδρομική Διεύθυνση		Ταχυδρομική Διεύθυνση		Ταχυδρομική Διεύθυνση	
5	Διεύθυνση Ηλεκτρονικού Ταχυδρομείου		Διεύθυνση Ηλεκτρονικού Ταχυδρομείου		Διεύθυνση Ηλεκτρονικού Ταχυδρομείου	
6	Τηλέφωνο		Τηλέφωνο		Τηλέφωνο	
7						
8	Άρθρο 30 Αρχείο δραστηριοτήτων επεξεργασίας					
9	Λειτουργία Επιχείρησης	Σκοπός της Επεξεργασίας	Όνομα και στοιχεία επικοινωνίας από κοινού υπεύθυνου επεξεργασίας (αν υφίσταται)	Κατηγορίες Υποκειμένων	Κατηγορίες Προσωπικών Δεδομένων	Κατηγορίες Αποδεκτών
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						
21						
22						
23						
24						
25						
26						
27						
28						
29						
30						
31						
32						
33						
34						

Δ.31 Παράδειγμα ανάλυσης κινδύνων και ελλείψεων (gap analysis)[101]

Α/Α	Έλλειψη/Απόκλιση	Ενέργεια συμμόρφωσης	Ενέργεια/ Πρόταση	Βάση απαίτησης	Προτεραιότητα υλοποίησης
1.	Στην είσοδο της Επιχείρησης έχει εγκατασταθεί σύστημα βιντεοεπιτήρησης, από το οποίο δεν γίνεται καταγραφή ήχου, χωρίς όμως να έχει τοποθετηθεί σχετική ενημερωτική πινακίδα.	Προτού ένα πρόσωπο εισέλθει στην εμβέλεια του συστήματος βιντεοεπιτήρησης, η Επιχείρηση, ως Υπεύθυνος Επεξεργασίας, οφείλει να το ενημερώνει, με τρόπο εμφανή και κατανοητό, ότι πρόκειται να εισέλθει σε χώρο που βιντεοσκοπείται. Προς τούτο, οφείλει να τοποθετήσει ευδιάκριτες πινακίδες στις οποίες θα αναγράφονται τα στοιχεία του Υπευθύνου Επεξεργασίας για λογαριασμό του οποίου γίνεται η βιντεοεπιτήρηση, δηλαδή της Επιχείρησης, ο σκοπός της επεξεργασίας, τυχόν έννομα συμφέροντα, τα δικαιώματα που έχουν τα πρόσωπα που καταγράφονται, οι αποδέκτες των δεδομένων, τυχόν διαβίβαση σε χώρα εκτός ΕΕ, το χρονικό διάστημα αποθήκευσης και τα στοιχεία επικοινωνίας του Υπευθύνου Προστασίας (Data Protection Officer). Επιπλέον, θα πρέπει να εξεταστεί η εικόνα που λαμβάνεται, ούτως ώστε να βεβαιωθεί ότι δεν λαμβάνεται εικόνα από εισόδους ή εσωτερικό γειτονικών γραφείων, κατοικιών ή άλλων χώρων. Σε περίπτωση που λαμβάνεται εικόνα από τους ως άνω χώρους, πρέπει να τροποποιηθεί το πεδίο λήψης της κάμερας ώστε να εστιάζει μόνο στο χώρο της εισόδου.	Υποχρεωτική	Άρθρα Κανονισμού: 5, 6, 12, 13 Άρθρο 5 του Σχεδίου Ελληνικού Νόμου για την προστασία δεδομένων προσωπικού χαρακτήρα	Υψηλή

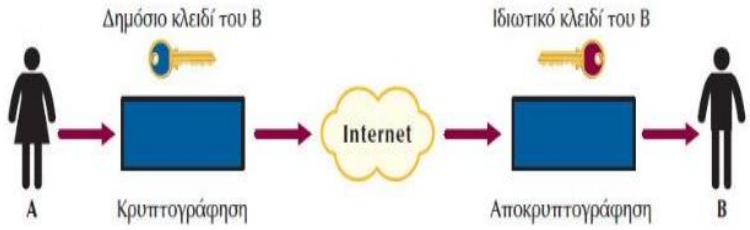
[100] Βλ. εισήγηση κ. Νόπης Τιντζογλίδου, 20 ετήσιο συνέδριο E-themis «Προσωπικά δεδομένα και δικηγορία-Μια νέα πραγματικότητα, ένα νέο κεφάλαιο στο νομικό κόσμο», 11-12 Μαΐου 2018.

[101] Βλ. εισήγηση κ. Νόπης Τιντζογλίδου, 20 ετήσιο συνέδριο E-themis «Προσωπικά δεδομένα και δικηγορία-Μια νέα πραγματικότητα, ένα νέο κεφάλαιο στο νομικό κόσμο», 11-12 Μαΐου 2018.

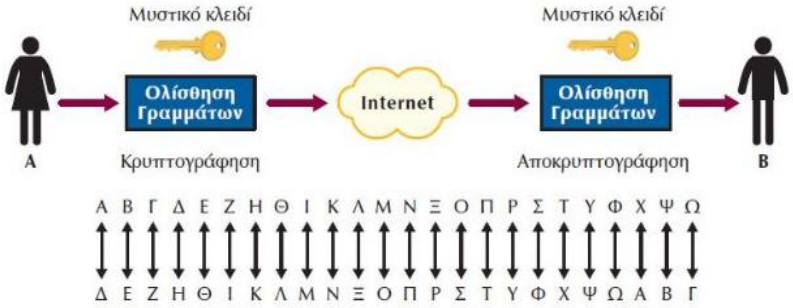
Δ.32 Αξιοποίηση των εργαλείων πληροφορικής[102]

Κρυπτογράφηση: είναι ο μετασχηματισμός δεδομένων σε μορφή που να είναι αδύνατον να διαβαστεί χωρίς τη γνώση της σωστής ακολουθίας bit. Η ακολουθία bit καλείται «κλειδί» και χρησιμοποιείται σε συνδυασμό με κατάλληλο αλγόριθμο / συνάρτηση. Η αντίστροφη διαδικασία είναι η αποκρυπτογράφηση και απαιτεί γνώση του κλειδιού. Η κρυπτογράφηση διακρίνεται σε ασύμμετρη (ζεύγος κλειδιών) και συμμετρική (κοινό κλειδί). Ως καλή πρακτική, σημειώνεται ότι το κλειδί πρέπει να στέλνεται με διαφορετικό τρόπο στο χρήστη από ότι το αρχείο (π.χ. με sms και email αντίστοιχα), καθώς έτσι εξασφαλίζεται μεγαλύτερη ασφάλεια.

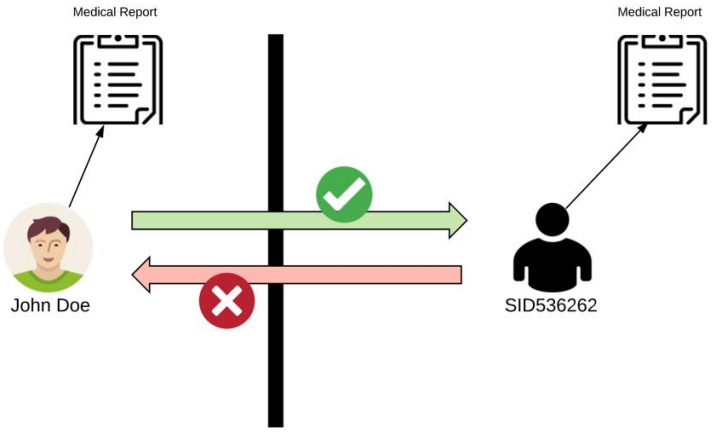
Ασύμμετρη κρυπτογράφηση



Συμμετρική κρυπτογράφηση

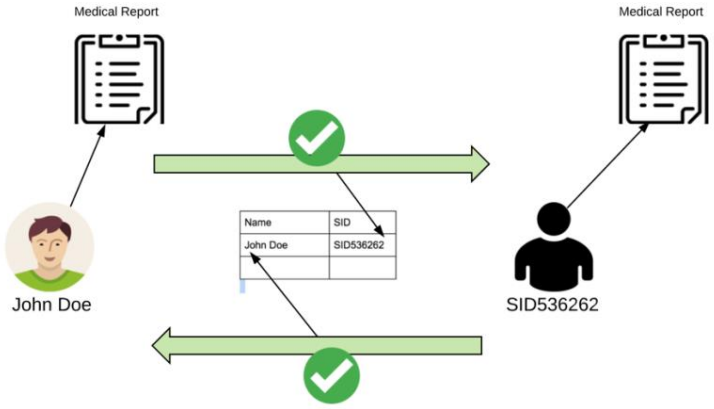


Ανωνυμοποίηση: είναι η διαδικασία απόκρυψης προσωπικών δεδομένων που μοναδικά ταυτοποιούν το φυσικό πρόσωπο, προκειμένου να μην είναι δυνατή η αναγνώρισή του. Κρίσιμο χαρακτηριστικό είναι ότι πρόκειται για μια τεχνική μη αντιστρέψιμη (π.χ. ολική απομάκρυνση των πεδίων που θα μπορούσαν με οποιονδήποτε τρόπο να ταυτοποιήσουν ένα φυσικό πρόσωπο).



[102] Τα στοιχεία προέρχονται από την παρουσίαση των κκ Νίκου Μαρουλιανάκη, Head of Infrastructure & Enterprise Data και Σοφίας Μολίνου, Υπεύθυνη Προστασίας Δεδομένων, Interamerican, Ομάδα Εργασίας ΣΕΒ για τα Προσωπικά δεδομένα.

Ψευδωνυμοποίηση: ορίζεται η επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο ώστε τα δεδομένα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρωματικές πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα. Σε αντίθεση με την ανωνυμοποίηση, πρόκειται για τεχνική αντιστρέψιμη. Περιλαμβάνει τεχνικές όπως data masking (κάλυψη μέρους των δεδομένων με τυχαίους χαρακτήρες ή άλλα δεδομένα), scrambling (ανάμειξη γραμμάτων), tokenization (αντικατάσταση των ευαίσθητων/προσωπικών δεδομένων με μη-ευαίσθητα/προσωπικά τα οποία ονομάζονται "tokens") και blurring (χρήση προσεγγιστικών τιμών των δεδομένων ώστε να καταστήσει αδύνατη την ταυτοποίηση του προσώπου).



5.2 Πρακτικά παραδείγματα συμμόρφωσης στον Κανονισμό

Στην παρούσα ενότητα παρουσιάζονται πρακτικά παραδείγματα για την επίτευξη συμμόρφωσης με τον Κανονισμό, μέσα από την εμπειρία δύο εταιρειών με αυξημένες υποχρεώσεις συμμόρφωσης με τον Κανονισμό και ειδικότερα μία επιχείρηση του ασφαλιστικού κλάδου και μία του οργανωμένου λιανεμπορίου.

5.2.1 Περίπτωση Α': Επιχείρηση από τον ασφαλιστικό κλάδο[103]

Η πορεία συμμόρφωσης με τις διατάξεις του Κανονισμού για τη συγκεκριμένη επιχείρηση ξεκίνησε ήδη από το Σεπτέμβριο του 2016, μέσα σε ένα περιβάλλον «φόβου» για το μέγεθος των αλλαγών που θα απαιτούνταν κυρίως γιατί ο ασφαλιστικός κλάδος, όπως και η τηλεφωνία, οι τράπεζες και ορισμένοι άλλοι κλάδοι κατέχουν μεγάλο όγκο προσωπικών δεδομένων εξ ορισμού.

Η εταιρεία μέσα από τη διαδικασία εκπόνησης Εκτίμησης Αντικτύπου είχε τη δυνατότητα να χαρτογραφήσει την υφιστάμενη κατάστασή της σχετικά με την προστασία δεδομένων, να εντοπίσει ποια κενά υπήρχαν στα συστήματά της και κατ' επέκταση να προσδιορίσει τα μέτρα που έπρεπε να υιοθετήσει προκειμένου να πετύχει το στόχο της συμμόρφωσης.

Ειδικότερα, ακολουθήθηκαν τα εξής βήματα για την επίτευξη της συμμόρφωσης με τον Κανονισμό:

1) Συστάθηκε Ομάδα Εργασίας, με τον ΥΠΔ αλλά και τη συμμετοχή στελεχών όλων των Διευθύνσεων της εταιρείας που σχετίζονται άμεσα με τον Κανονισμό (π.χ. Νομική Διεύθυνση, Διεύθυνση Πληροφορικής, Διεύθυνση Διαχείρισης Κινδύνου, Διεύθυνση Κανονιστικής Συμμόρφωσης κ.λπ.).
2) Οριστήκαν εκείνα τα Τμήματα της εταιρείας που εμπλέκονται με προσωπικά δεδομένα (π.χ. Marketing, Operations και Εξυπηρέτηση Πελατών), με στόχο τη χαρτογράφηση αυτών.

   Σε αυτό το σημείο η εμπειρία της εταιρείας ανέδειξε ότι απαιτείται ιδιαίτερη προσοχή, καθώς πολλές φορές υπάρχουν προσωπικά δεδομένα σε Τμήματα

[103] Η επιλογή της συγκεκριμένης περίπτωσης κρίθηκε περισσότερο κατάλληλη, καθώς τα προσωπικά δεδομένα αποτελούν βασικό αντικείμενο της δραστηριότητας μιας επιχείρησης του ασφαλιστικού κλάδου. Επομένως, η εν λόγω επιχείρηση εξ ορισμού κατέχει μεγάλο όγκο προσωπικών δεδομένων, η πλειοψηφία των οποίων είναι και ευαίσθητα δεδομένα (που έχουν μεγαλύτερες απαιτήσεις συμμόρφωσης), η επεξεργασία τους αφορά όλες τις Διευθύνσεις και η επικοινωνία / σχέση με τα υποκείμενα των δεδομένων είναι συνεχής. Σημειώνεται ότι το περιεχόμενο της ενότητας έχει βασιστεί σε υλικό της επιχείρησης που παρουσιάστηκε στο πλαίσιο του Εργαστηρίου Διαβούλευσης που οργανώθηκε στις 07.02.2018.

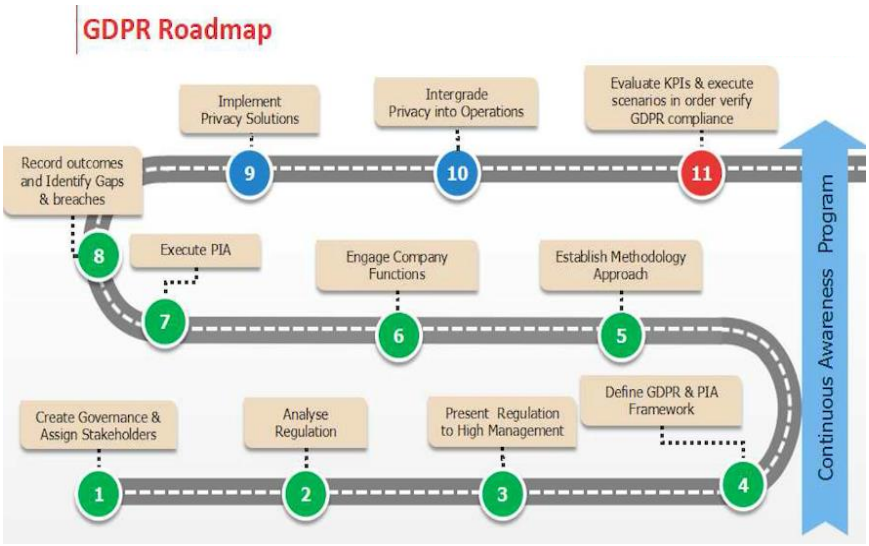
που δεν είναι αναμενόμενο ή άμεσα προφανές. Δύο ενδεικτικά παραδείγματα αποτυπώνουν εύληπτα το γεγονός αυτό: α) με αφορμή πραγματοποίηση διαγωνισμού για συμβόλαιο υγείας από το Τμήμα Δημοσίων Σχέσεων, τελικά εντοπίστηκε ότι το Τμήμα συγκέντρωνε ιατρικά στοιχεία των πελατών/νικητών οι οποίοι επικοινωνούσαν μαζί τους για το συμβόλαιό τους και β) προκλήθηκε προβληματισμός σχετικά με εάν το Τμήμα Ανθρώπινου Δυναμικού μιας εταιρείας πρέπει να έχει πρόσβαση στο ομαδικό συμβόλαιο υγείας των εργαζομένων, καθώς αυτό συνεπάγεται ότι έχει πρόσβαση σε ευαίσθητα προσωπικά δεδομένα, τα οποία ενδεχομένως χρησιμοποιηθούν για την αξιολόγηση στελεχών δίχως αντικειμενικότητα (π.χ. προαγωγή, με βάση το ιατρικό ιστορικό).

Επίσης, κρίσιμο σημείο στη διαδικασία της χαρτογράφησης αποτελεί ο εντοπισμός επαναλήψεων των προσωπικών δεδομένων (να διατηρούνται ακριβώς τα ίδια δεδομένα σε περισσότερα του ενός σημεία στην εταιρεία - duplications).

3) Η Ομάδα Έργου προχώρησε σε ανάλυση και κατανόηση των απαιτήσεων του Κανονισμού.
4) Πραγματοποιήθηκε σχετική παρουσίαση / ενημέρωση προς την ανώτατη Διοίκηση της εταιρείας, ώστε να εξασφαλιστεί η δέσμευση και η διάθεση των απαιτούμενων πόρων για την υλοποίηση του έργου συμμόρφωσης.
5) Εκπονήθηκε Εκτίμηση Αντικτύπου σχετικά με την προστασία δεδομένων, με την ενεργή εμπλοκή όλων των Τμημάτων της εταιρείας. Μέσω αυτής της διαδικασίας, αναδείχθηκαν τα κενά ασφαλείας (gaps), τα οποία έπρεπε να αντιμετωπιστούν. Επιπλέον, η εταιρεία αξιοποίησε τη διαδικασία εκπόνησης της Εκτίμησης Αντικτύπου με τρόπο ώστε ταυτόχρονα να διαγνώσει την ψηφιακή της ετοιμότητα (digital benchmark) και σε δεύτερο χρόνο να αναλάβει δράση για την αναβάθμισή της ως προς το στοιχείο αυτό.
6) Για κάθε κενό ασφαλείας σχεδιάστηκε συγκεκριμένη λύση η οποία στη συνέχεια εναρμονίστηκε με τις πολιτικές και διαδικασίες των Τμημάτων της εταιρείας.
7) Υλοποιήθηκαν δοκιμαστικοί έλεγχοι των συστημάτων και διαδικασιών, με διαφορετικά σενάρια, ώστε να εξασφαλιστεί η όσο το δυνατόν μεγαλύτερη προστασία των προσωπικών δεδομένων (π.χ. για τη φορητότητα, το δικαίωμα στη λήθη, τη γνωστοποίηση παραβίασης δεδομένων).
8) Ορίστηκαν Βασικοί Δείκτες Απόδοσης (Key Performance Indicators - KPIs), προκειμένου η εταιρεία να μπορεί να αξιολογήσει την πορεία συμμόρφωσής της στον Κανονισμό.

9) Οργανώθηκαν εκπαιδευτικές δράσεις για το σύνολο του προσωπικού (π.χ. βίντεο, κουίζ σε ηλεκτρονική πλατφόρμα, παρουσιάσεις), προκειμένου αφενός να ενημερωθούν τα στελέχη και αφετέρου να ενισχυθεί η ευαισθητοποίησή τους σχετικά με την προστασία των προσωπικών δεδομένων. Σημειώνεται ότι η εκπαίδευση του προσωπικού συμβάλλει καταλυτικά στο να αποφευχθούν φαινόμενα απώλειας ή κλοπής δεδομένων. Τέλος, είναι σημαντικό κάθε εταιρεία να πραγματοποιεί εκπαιδευτικές δράσεις σε συνεχή βάση, δεν αποτελεί δηλαδή "one-off" διαδικασία.

Δ.33 Ο δρόμος για την επίτευξη της συμμόρφωσης επιχείρησης από τον ασφαλιστικό κλάδο



Ορισμένες χαρακτηριστικές ενέργειες στις οποίες προέβη η εταιρεία ήταν οι εξής:

- Δόθηκε ιδιαίτερη έμφαση στις φόρμες που συμπληρώνουν οι πελάτες τα στοιχεία τους, ώστε να εξεταστούν εκ νέου υπό το πρίσμα του σκοπού της επεξεργασίας: δηλαδή εάν είναι απαραίτητο κάθε πεδίο (πράγματι αξιοποιείται από τις Λειτουργικές Διευθύνσεις της εταιρείας;) και αν είναι σύννομο.
- Ορίστηκαν συγκεκριμένα και δομημένα χρονικά διαστήματα για τη διατήρηση των προσωπικών δεδομένων (retention periods). Στο πλαίσιο αυτό, διαγράφηκαν ή καταστράφηκαν πολλά δεδομένα, σε ηλεκτρονική ή έντυπη μορφή, που πλέον δεν υπήρχε λόγος να αποθηκεύονται. Μάλιστα, επισημαίνεται ότι η εν λόγω διαδικασία στην πράξη αποδεικνύεται χρονοβόρα και δύσκολη, ενώ συνήθως υποτιμάται.

- Αναθεωρήθηκαν όλα τα συμβόλαια (εκτός όλων όσα έληγαν στον επόμενο χρόνο), ώστε οι όροι να είναι συμβατοί με τον Κανονισμό.
- Επιλέχθηκε εξωτερικός συνεργάτης για την παροχή των εργαλείων και λύσεων πληροφορικής που συμβάλλουν αποτελεσματικά στη διαδικασία συμμόρφωσης (π.χ. χαρτογράφηση προσωπικών δεδομένων, κρυπτογράφηση κ.λπ.).
- Εντάχθηκε στη Διεύθυνση Εσωτερικού Ελέγχου ξεχωριστή λειτουργία για τον έλεγχο του Κανονισμού.
- Αναθεωρήθηκε η πολιτική σχετικά με τη χρήση usb sticks, σκληρών δίσκων και laptops, με τρόπο ώστε να εξασφαλιστεί ότι τίποτα δεν μπαίνει ή βγαίνει από το δίκτυο της εταιρείας.
- Δόθηκε ιδιαίτερη προσοχή στα ζητήματα ασφάλειας των κινητών τηλεφώνων των ασφαλιστών, καθώς αποτελούν βασικό εργαλείο της δουλειάς τους εκτός εταιρείας.
- Δημιουργήθηκε κοινό γλωσσάρι των προσωπικών δεδομένων, ώστε να υπάρχει κοινή κατανόηση των εννοιών και των διαδικασιών από όλους τους εργαζομένους στην εταιρεία.
- Υιοθετήθηκε πολιτική εκκαθάρισης των επιφανειών εργασίας (clean desk assessment) και οργάνωσης των αποθηκευτικών χώρων. Πρόκειται για μια διαδικασία η οποία μπορεί να διαρκέσει περισσότερο από το αναμενόμενο στην αρχική της υλοποίηση. Επίσης, αναδεικνύει τις μεγάλες ανάγκες σε αποθηκευτικό χώρο, ιδίως για τα έγχαρτα αρχεία, γεγονός που συνεπάγεται κόστος για την εταιρεία σε υποδομές και εξοπλισμό. Σημειώνεται ότι η δράση συνδέεται και με την πολιτική για τη διατήρηση των δεδομένων (retention periods).
- Υιοθετήθηκαν πολιτικές καταγραφής του ιστορικού των δεδομένων (data lineage) και τήρησης αρχείου επεξεργασίας προσωπικών δεδομένων (personal data processing registry), με ιδιαίτερη επισήμανση των προσωπικών και ευαίσθητων δεδομένων, καθώς και των δεδομένων με αξία για την εταιρεία.
- Δημιουργήθηκε διαδικασία ελέγχου κίνησης δεδομένων (data traffic control) ώστε για οποιοδήποτε εξερχόμενο να ακολουθείται συγκεκριμένη διαδικασία.
- Εντοπίστηκαν τα περιττά (waste) αλλά και τα αδόμητα δεδομένα (unstructured). Η εμπειρία της εταιρείας ανέδειξε ότι ο όγκος τους ήταν μεγαλύτερος από τον εκτιμώμενο. Σημειώνεται ότι απαιτείται διαρκής παρακολούθηση και εκκαθάριση των εν λόγω δεδομένων, δεν αποτελεί δηλαδή “one-off” διαδικασία.

5.2.2 Περίπτωση Β': Επιχείρηση από το οργανωμένο λιανεμπόριο (μέλος πολυεθνικού ομίλου)[104]

Για τον πολυεθνικό όμιλο στον οποίο ανήκει η εταιρεία του παραδείγματός μας, η διαδικασία συμμόρφωσης στις νέες διατάξεις αντιμετωπίστηκαν εξ αρχής ως «ευκαιρία» και όχι ως «πρόκληση». Το γεγονός ότι στον Όμιλο προϋπήρχε του Κανονισμού η κουλτούρα σεβασμού των προσωπικών δεδομένων, αποτέλεσε σημαντική βοηθητική παράμετρο, καθώς υπήρχε όχι μόνο η σχετική εμπειρία αλλά κυριότερα η ευαισθητοποίηση της διοίκησης και των στελεχών.

Ο Όμιλος προέβη σε συγκεκριμένες ενέργειες προκειμένου να εναρμονίσει τις πολιτικές και τις διαδικασίες του στις προβλέψεις του Κανονισμού, υπό το πρίσμα ότι επεξεργάζεται προσωπικά δεδομένα τεσσάρων κατηγοριών: α) προμηθευτών, β) πελατών, γ) υπαλλήλων και δ) τρίτων προσώπων. Ειδικότερα, η διαδικασία επίτευξης της συμμόρφωσης ξεκίνησε το Φεβρουάριο του 2017 (περισσότερο από ένα χρόνο πριν την έναρξη εφαρμογής του Κανονισμού) και πραγματοποιήθηκαν σταδιακά τα ακόλουθα βήματα:

1) Συστάθηκε Ομάδα Εργασίας, σε κάθε επιχείρηση του Ομίλου, για την παρακολούθηση της προόδου του έργου συμμόρφωσης (αποτελούμενη από στελέχη κυρίως της Νομικής Διεύθυνσης και της Διεύθυνσης Πληροφοριακών Συστημάτων). Από τους πρώτους στόχους κάθε Ομάδας ήταν η εξασφάλιση της δέσμευσης των ιεραρχικά ανώτερων στελεχών για τη διάθεση των απαιτούμενων πόρων για τους σκοπούς του έργου (π.χ. προϋπολογισμός, τεχνικοί και ανθρώπινοι πόροι). Προς την κατεύθυνση αυτή, οργανώθηκαν ενημερώσεις προς τους Γενικούς Διευθυντές.
2) Πραγματοποιήθηκαν στοχευμένες ενημερώσεις προς το σύνολο των Τμημάτων που διαχειρίζονται προσωπικά δεδομένα. Σημειώνεται ότι «κλειδί» σε αυτό το στάδιο είναι η εκάστοτε Ομάδα Εργασίας να αναγνωρίσει επιτυχώς ποιοι διαχειρίζονται προσωπικά δεδομένα εντός της επιχείρησης (σημ.: δεν είναι πάντοτε προφανές και εύκολα αναγνωρίσιμο).

[104] Η επιλογή της συγκεκριμένης περίπτωσης κρίθηκε περισσότερο κατάλληλη, για δύο λόγους: α) αποτελεί μέλος πολυεθνικού ομίλου (άρα αναδεικνύεται η επιρροή στην κουλτούρα για την προστασία προσωπικών δεδομένων από το εξωτερικό) και β) δραστηριοποιείται σε κλάδο που τα προσωπικά δεδομένα δεν αποτελούν το βασικό αντικείμενο της δραστηριότητας (επομένως αναδεικνύεται ο τρόπος με τον οποίο τα βήματα συμμόρφωσης στον Κανονισμό μπορούν να προσφέρουν πολλαπλά οφέλη). Σημειώνεται ότι το περιεχόμενο της ενότητας έχει βασιστεί σε υλικό της επιχείρησης που παρουσιάστηκε στο πλαίσιο του Εργαστηρίου Διαβούλευσης που οργανώθηκε στις 07.02.2018.

3) Δημιουργήθηκαν ερωτηματολόγια προς τα ως άνω Τμήματα για την καταγραφή των προσωπικών δεδομένων (π.χ. τι είδους δεδομένα, για ποιο σκοπό, για πόσο κ.λπ.) και την κατηγοριοποίηση αυτών με βάση το επίπεδο κινδύνου (π.χ. χαμηλού, μεσαίου, υψηλού).
4) Με αφετηρία τα ερωτηματολόγια, συντάχθηκαν περισσότερο αναλυτικά αρχεία για κάθε επεξεργασία, τα επονομαζόμενα "record keepings", με στόχο τον αναλυτικό προσδιορισμό των τηρούμενων διαδικασιών και των αρμοδίων προσώπων σχετικά με τα προσωπικά δεδομένα. Ενδεικτικά, ποιος είναι ο υπεύθυνος επεξεργασίας και ποιος ο εκτελών την επεξεργασία, που διαβιβάζονται τα δεδομένα, ποια συστήματα εμπλέκονται σε αυτή τη διαδικασία, ποια είναι η περίοδος διατήρησης των δεδομένων (retention period) κ.ά.
5) Αξιοποιώντας τα δύο προηγούμενα στάδια, καταγράφηκαν τα κενά (gaps) στα οποία έπρεπε να δοθεί μεγαλύτερη προσοχή. Στον Όμιλο το κυριότερο κενό αφορούσε την περίοδο διατήρησης των δεδομένων (retention period), καθώς δεν γινόταν διαγραφή δεδομένων.
6) Ενημερώθηκαν τα αρμόδια στελέχη σχετικά με τα εντοπισμένα κενά και οργανώθηκαν οι επόμενες ενέργειες ώστε να αντιμετωπιστούν.
7) Εκπονήθηκε Εκτίμηση Αντικτύπου σχετικά με την προστασία δεδομένων.

Με βάση τα στάδια (6) και (7), λήφθηκαν συγκεκριμένες αποφάσεις και αναπτύχθηκαν σχετικές πολιτικές, με στόχο την εξασφάλιση της προστασίας των προσωπικών δεδομένων. Ενδεικτικά, αναφέρονται:

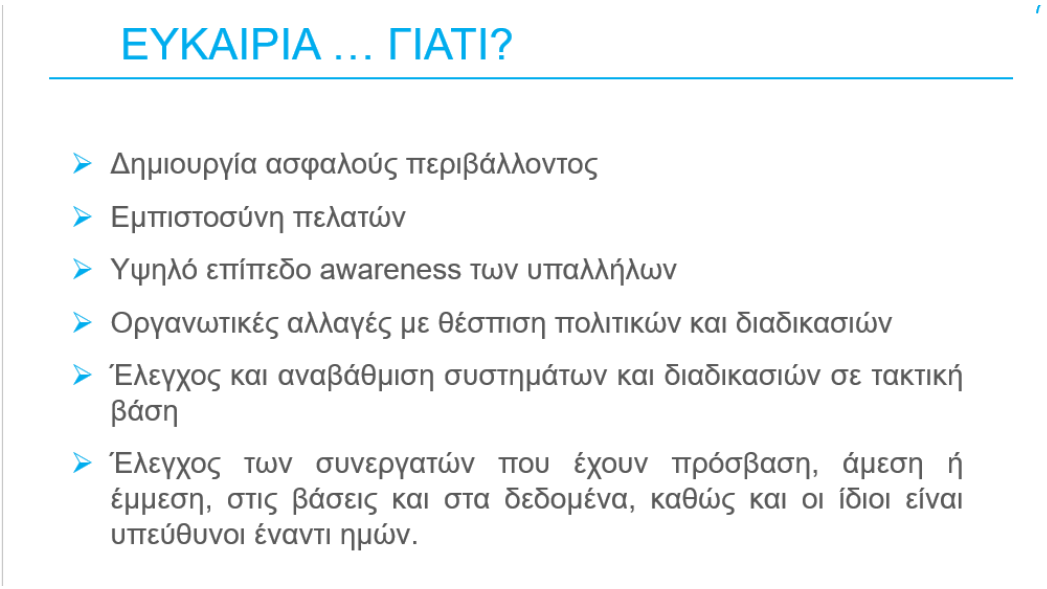
- Αλλαγή του τρόπου ενημέρωσης των υποκειμένων όσον αφορά στα σχήματα πιστότητας (loyalty schemes).
- Ορισμό συγκεκριμένου χρόνου διατήρησης των βιογραφικών σημειωμάτων για την αναζήτηση νέων στελεχών.
- Αλλαγές των όρων των συμβάσεων με προμηθευτές.
- Αξιολόγηση του επιπέδου συμμόρφωσης με τον νέο Κανονισμό των συνεργατών που έχουν, άμεση ή έμμεση, πρόσβαση στις βάσεις και στα δεδομένα, καθώς έχουν και οι ίδιοι ευθύνη.
- Ανάθεση διακριτών ρόλων και ανάλογης διαβάθμισης της δυνατότητας πρόσβασης στα προσωπικά δεδομένα, ανάλογα με το ρόλο / θέση κάθε στελέχους.
- Αλλαγές στις διαδικασίες για τα φυσικά αρχεία με προσωπικά δεδομένα (π.χ. φύλλα παραπόνων στα καταστήματα) και τις διαδρομές που ακολουθούν εντός της επιχείρησης.
- Ανάληψη δράσεων εκπαίδευσης και ενημέρωσης του συνόλου του προσωπικού, ώστε να γίνει αντιληπτός από όλους ο λόγος για τον οποίο καλούνται να

ακολουθήσουν μια συγκεκριμένη – νέα – διαδικασία και ποια είναι αυτή. Οι δράσεις εκπαίδευσης προτείνεται να οργανωθούν σε στάδια, π.χ. πρώτα στους πλέον άμεσα εμπλεκόμενους και σε δεύτερο χρόνο στο σύνολο του προσωπικού.

Τα κυριότερα οφέλη που αποκομίζει ο Όμιλος μέσα από τη διαδικασία συμμόρφωσης στον Κανονισμό συνοψίζονται στα εξής:

- ✓ Δημιουργία αισθήματος ασφαλούς περιβάλλοντος στον πελάτη, το οποίο συνεπάγεται την εμπιστοσύνη του πελάτη και κατ' επέκταση εξασφαλίζει την πιστότητά του.
- ✓ Ανάδειξη ευκαιριών για οργανωτικές αλλαγές στην επιχείρηση.
- ✓ Κίνητρο για έλεγχο και αναβάθμιση των συστημάτων και των διαδικασιών, σε τακτική βάση.

Δ.34 Τα οφέλη από τη συμμόρφωση με τον Κανονισμό



5.2.3 Χρήσιμες συμβουλές για τις μικρές και μεσαίες επιχειρήσεις για την συμμόρφωση στον Κανονισμό

Όπως ήδη προαναφέρθηκε για τις μικρές και μεσαίες επιχειρήσεις το κόστος συμμόρφωσης είναι, ενδεχομένως, δυσανάλογα μεγάλο. Ειδικά για τις επιχειρήσεις αυτές, παραθέτουμε παρακάτω ορισμένες χρήσιμες συμβουλές στην προσπάθειά τους να προσαρμοστούν στον Κανονισμό, ώστε να διευκολυνθούν στην «αγωνία» τους να συμμορφωθούν και να αποφύγουν τα υψηλά πρόστιμα, τα οποία σε περίπτωση επιβολής θα ήταν για αυτές παράγοντας επιβίωσης.

Δ.35 Χρήσιμες συμβουλές για τις μικρές και μεσαίες επιχειρήσεις για την συμμόρφωση στον Κανονισμό
1. Προσαρμογή των βημάτων συμμόρφωσης στην κατάλληλη κλίμακα Κάθε επιχείρηση οφείλει να προσαρμόσει τα βήματα και τις έξυπνες αρχές συμμόρφωσης, με βάση τις δικές της ανάγκες, τα χαρακτηριστικά (φύση και όγκος δεδομένων), το μέγεθος, το αντικείμενο των εργασιών και τη στρατηγική της.
2. Μικρό μέγεθος επιχείρησης δεν σημαίνει και μικρή επεξεργασία Ιδιαίτερη προσοχή απαιτείται, στην περίπτωση που οι επιχειρήσεις είναι μικρού μεγέθους (βάσει κύκλου εργασιών ή /και προσωπικού), ωστόσο προβαίνουν σε εκτενή επεξεργασία προσωπικών δεδομένων, κυρίως λόγω της δραστηριότητάς τους (π.χ. μια εταιρεία παροχής υπηρεσιών φύλαξης, ή μια εταιρεία παροχής υπηρεσιών “cloud”). Με άλλα λόγια, η έμφαση που πρέπει να δοθεί από τον κάθε επιχειρηματία που εξετάζει κατά πόσο επηρεάζεται από τις απαιτήσεις του Κανονισμού είναι στον όγκο και στο βαθμό επεξεργασίας των προσωπικών δεδομένων που κατέχει και όχι στο μέγεθός του.
3. Αποφυγή υπερβολών σε πολιτικές και διαδικασίες Σκοπός είναι η επίτευξη της συμμόρφωσης δίχως να επιβαρυνθούν περισσότερο με περιττά βάρη και πολύπλοκες ή ανεφάρμοστες διαδικασίες οι μικρομεσαίες επιχειρήσεις, οι οποίες διαθέτουν περιορισμένους πόρους. Κάθε επιχείρηση πρέπει να υιοθετήσει εκείνα τα μέτρα προστασίας προσωπικών δεδομένων που τις ταιριάζουν και που σκοπεύει έμπρακτα να εφαρμόσει (όχι δηλαδή απλά για τους τύπους), κάποια εκ των οποίων δε είναι ανέξοδα (π.χ. οριστική διαγραφή δεδομένων που δεν χρησιμοποιούνται κ.λπ.).

5.3 Τα οφέλη του Κανονισμού στην επιχειρηματική στρατηγική - Πρόταση ΣΕΒ: «έξυπνη» συμμόρφωση

Στον ΣΕΒ πιστεύουμε ότι ο Κανονισμός παρουσιάζει σημαντικές ευκαιρίες, που αν αξιοποιηθούν, μπορούν να συμβάλουν στην ουσιαστική βελτίωση του τρόπου λειτουργίας του επιχειρηματικού μοντέλου, με αποτέλεσμα όχι απλά την τυπική συμμόρφωση, αλλά την επίτευξη θετικού προσήμου μέσα από την εν λόγω διαδικασία. Αυτό μπορεί να επιτευχθεί εάν οι επιχειρήσεις, αντί για ένα ακόμα «στείρο» νομικό κείμενο υποχρεώσεων, εκλάβουν τον Κανονισμό ως υποχρεωτική «άσκηση» χάρη στην οποία θα αλλάξουν την επιχειρηματική κουλτούρα προς όφελός τους, δίχως να επιβαρυνθούν με σημαντικό χρηματικό και διοικητικό κόστος. Αυτό στον ΣΕΒ θέλουμε να αποκαλούμε **«έξυπνη συμμόρφωση», βασισμένη σε τρεις αρχές που αναδεικνύουν εύληπτα και τα οφέλη που προκύπτουν από τον Κανονισμό**.

Η πρώτη αρχή αφορά στο «νοικοκύρεμα» των (προσωπικών) δεδομένων. Μέχρι σήμερα οι επιχειρήσεις, κατά συνήθη πρακτική, επιδίδονται σε ένα «κυνήγι όγκου» δεδομένων, γεγονός που συνεπάγεται σημαντικό κόστος συγκέντρωσης, καταχώρισης, ψηφιοποίησης, φύλαξης, επεξεργασίας, ανάλυσης κ.λπ. Ο Κανονισμός «αναγκάζει» τις επιχειρήσεις να επανεξετάσουν τα δεδομένα τους, αλλά και τις δομές, τις εσωτερικές λειτουργίες και τις διαδικασίες τους σε σχέση με αυτά. Δηλαδή τις καλεί να επανεξετάσουν ποια δεδομένα διατηρούν, πώς τα συλλέγουν, για ποιο σκοπό, για πόση διάρκεια, ποιος έχει πρόσβαση σε αυτά και πώς φυλάσσονται[105].

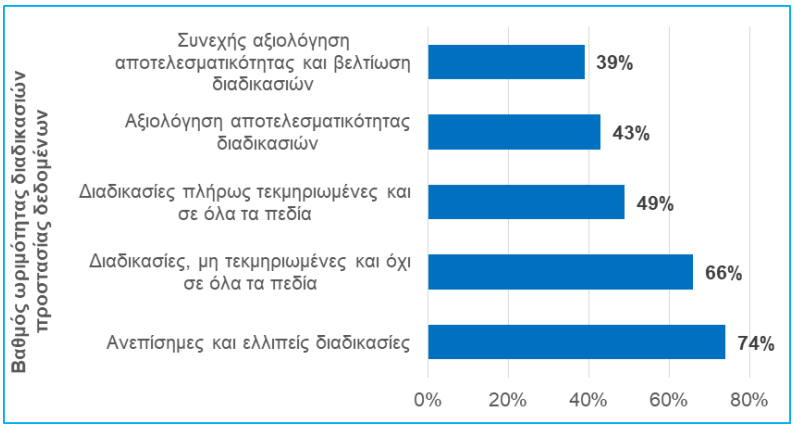
Μέσα από αυτή τη διαδικασία είναι βέβαιο ότι θα προκύψουν χρήσιμα συμπεράσματα σχετικά με το αν τα δεδομένα αξιοποιούνται επαρκώς από την επιχείρηση, ή μήπως πολύτιμες πληροφορίες μένουν ανεκμετάλλευτες χάνοντας επιχειρηματικές ευκαιρίες (π.χ. πληροφορίες σχετικές με το προφίλ των πελατών). Παράλληλα, θα αναδειχθούν οι κίνδυνοι που αφορούν τις συνθήκες ασφάλειας των δεδομένων (π.χ. το σύνολο του προσωπικού έχει πρόσβαση σε ευαίσθητα δεδομένα δίχως αυτό να είναι απαραίτητο για την εργασία του, ή παλαιά προσωπικά δεδομένα φυλάσσονται ακόμα, δίχως πραγματικό πλέον λόγο και μάλιστα σε χώρους με ανεμπόδιστη πρόσβαση). Ως εκ τούτου, θα αναδειχθούν τα αναγκαία μέτρα προφύλαξης που πρέπει να υιοθετηθούν και τα οποία προστατεύουν τις επιχειρήσεις από νομικούς και οικονομικούς κινδύνους,

[105] Σημειώνεται ότι αυτή η διαδικασία χαρτογράφησης δεν είναι απαραίτητο να αφορά μόνο τα προσωπικά δεδομένα, αλλά ανάλογα με τα χαρακτηριστικά της επιχείρησης, να επεκταθεί και σε άλλες (ή και όλες τις) κατηγορίες δεδομένων, με πολλαπλασιαστικά οφέλη.

όπως η επιβολή προστίμων από την εποπτική Αρχή. Τέλος, είναι προφανές ότι όσο μικρότερος είναι ο όγκος των δεδομένων που διατηρούνται, τόσο μειώνεται το κόστος όπως αυτό εκφράζεται σε εργατοώρες, υλικοτεχνικό εξοπλισμό και έπιπλα, χώρο γραφείων, σε χρόνο και χώρο για backup κ.λπ. Επομένως, τα οφέλη της ελαχιστοποίησης των προσωπικών δεδομένων είναι πολλαπλά.

Στον πίνακα **(Δ36)** αποτυπώνεται η θετική συσχέτιση που υπάρχει μεταξύ: α) του βαθμού ωριμότητας των επιχειρήσεων όσον αφορά στις διαδικασίες τους για την προστασία των δεδομένων (υπό μία έννοια, του βαθμού συμμόρφωσης δηλαδή με τον Κανονισμό) και β) της οικονομικής ζημίας από την παραβίαση της ασφάλειας δεδομένων. Ειδικότερα, σύμφωνα με διεθνή μελέτη της Cisco, το 74% των επιχειρήσεων που είχαν υιοθετήσει ανεπίσημες και ελλιπείς διαδικασίες προστασίας δεδομένων αντιμετώπισαν απώλειες μεγαλύτερες από $500 χιλ. εξαιτίας παραβιάσεων των δεδομένων τους κατά το προηγούμενο έτος. Για τις επιχειρήσεις που είχαν βελτιστοποιήσει αυτές τις διαδικασίες, το ποσοστό ήταν 39%.

Δ.36 Ποσοστό επιχειρήσεων, με απώλειες από παραβίαση ασφάλειας δεδομένων μεγαλύτερες από $500 χιλ. το προηγούμενο έτος, ανά βαθμό ωριμότητας ως προς την προστασία των δεδομένων
Πηγή: CISCO, "Privacy Maturity Benchmark Study", 2018



Η δεύτερη αρχή αφορά στη μετατροπή της υποχρέωσης συμμόρφωσης σε ανταγωνιστικό πλεονέκτημα. Όταν ακόμη οι αναζητήσεις μας στο διαδίκτυο αποκαλύπτουν τις προσωπικές ή επαγγελματικές προτιμήσεις μας και το κινητό μας «εκπέμπει» τα προσωπικά μας δεδομένα, είναι εύλογο ότι ο τρόπος προστασίας τους γρήγορα θα αποτελέσει κριτήριο για τις επιλογές που θα κάνουν οι πελάτες, οι προμηθευτές και οι ίδιοι οι εργαζόμενοι. Είναι δε χαρακτηριστικό ότι έχει ήδη ξεκινήσει διεθνώς μια πολύ ζωντανή και ενδιαφέρουσα συζήτηση γύρω από την προστασία των προσωπικών δεδομένων και την ανάγκη αυτορρύθμισης των επιχειρήσεων, ώστε να αποφευχθούν δυστοπικά σενάρια μιας επερχόμενης «ψηφιακής δικτατορίας».

Υπό αυτήν την έννοια, η προστασία των προσωπικών δεδομένων σχετίζεται άμεσα με την εμπιστοσύνη πελατών, προμηθευτών και εργαζομένων και κατ' επέκταση με τη φήμη της επιχείρησης. Αυτό που είναι σημαντικό για κάθε επιχείρηση είναι να μπορεί να αποδείξει (σε όλες τις προαναφερθείσες κατηγορίες ενδιαφερομένων) ότι προστατεύει τα προσωπικά τους δεδομένα από τις τέσσερις βασικές περιπτώσεις παραβίασής τους: α) την εισβολή, δηλαδή το να εισέρχεται μια επιχείρηση στον προσωπικό χώρο κάποιου υποκειμένου, να επικοινωνεί μαζί του και να του υποδεικνύει τί να κάνει, β) τη συγκέντρωση δεδομένων σε βαθμό που να εισπράττει το υποκείμενο ότι παρακολουθείται σε μεγαλύτερη έκταση από αυτή που θα έπρεπε, γ) την επεξεργασία δεδομένων με τρόπο που να εισπράττει το υποκείμενο ότι μια επιχείρηση κατέχει πολλά προσωπικά του δεδομένα και προβαίνει σε επεξεργασία αυτών και δ) την αποκάλυψη των δεδομένων του από την επιχείρηση με τρόπο που το υποκείμενο δεν είναι σύμφωνο.

Συνεπώς, η επιχείρηση που θα κάνει το σεβασμό της προσωπικότητας και της ιδιωτικότητας στοιχείο της κουλτούρας της και θα το εντάξει στην επιχειρηματική της στρατηγική θα αποκτήσει σαφές ανταγωνιστικό πλεονέκτημα έναντι των υπολοίπων.

Τέλος, η τρίτη αρχή αφορά στην επένδυση σε λύσεις που προσφέρει η τεχνολογία και, μέσω αυτής της διαδικασίας, στην είσοδο στην εποχή της ψηφιακής οικονομίας. Είναι γεγονός ότι η ενσωμάτωση των ψηφιακών τεχνολογιών στην επιχειρηματική λειτουργία αποτελεί πλέον μονόδρομο για την επιβίωση και ανάπτυξη των επιχειρήσεων. Υπό αυτήν την έννοια, ο Κανονισμός μπορεί να αποτελέσει πύλη εισόδου στη ψηφιακή κοσμογονία (ενδεικτικά, business analytics, big data), καθώς οι τεχνολογίες πληροφορικής και επικοινωνιών παρέχουν όχι μόνο εργαλεία συμμόρφωσης χαμηλού κόστους (π.χ. cloud computing, firewalls, κρυπτογράφηση, ψευδωνυμοποίηση κ.ά.), αλλά και λύσεις που τελικά θα αναβαθμίσουν το ίδιο το επιχειρηματικό μοντέλο.

Με άλλα λόγια, όπως αναφέρθηκε στην αρχή της παρούσας έκθεσης, οι τεχνολογικές εξελίξεις ήταν αυτές που σε μεγάλο βαθμό προκάλεσαν την ανάγκη μετάβασης από την Οδηγία στον Κανονισμό για την προστασία των προσωπικών δεδομένων, αλλά ταυτόχρονα είναι εκείνες που προσφέρουν και τις λύσεις συμμόρφωσης σε αυτόν. Μέσω αυτής της διαδικασίας, οι επιχειρήσεις καλούνται να εξοικειωθούν, προβληματιστούν, ερευνήσουν, ανασχεδιάσουν τις δομές και τις λειτουργίες τους με βάση τα εργαλεία που προσφέρει η τεχνολογία συνολικά, όχι μόνο για τις ανάγκες

συμμόρφωσης στο νέο κανονιστικό πλαίσιο. Εξάλλου, η ενσωμάτωση των ψηφιακών τεχνολογιών στην επιχειρηματική στρατηγική αποτελεί πλέον προαπαιτούμενο για την επιβίωση και ανάπτυξη των επιχειρήσεων[106].

Δ.37 Οι αρχές για έξυπνη συμμόρφωση με τον Κανονισμό και τα οφέλη για την επιχείρηση	
Νοικοκύρεμα των (προσωπικών) δεδομένων	✓ Ανάδειξη δεδομένων που - ενδεχομένως -συνδέονται με επιχειρηματικές ευκαιρίες ✓ Ανάδειξη κινδύνων που αφορούν τις συνθήκες ασφάλειας των δεδομένων και κατ' επέκταση ενέργειες για αποτελεσματική προστασία ✓ Μείωση όγκου δεδομένων που διατηρούνται και κατ' μείωση κόστους (σε εργατοώρες, υλικοτεχνικό εξοπλισμό και έπιπλα, χώρο γραφείων, χρόνο και χώρο για backup κ.ά.)
Μετατροπή της υποχρέωσης συμμόρφωσης σε ανταγωνιστικό πλεονέκτημα	✓ Εμπιστοσύνη πελατών, προμηθευτών και εργαζομένων ✓ Προστασία φήμης της επιχείρησης
Επένδυση σε λύσεις που προσφέρει η τεχνολογία	✓ Ενσωμάτωση των ψηφιακών τεχνολογιών στην επιχειρηματική λειτουργία

[106] Δείτε **εδώ** το Special Report για το στρατηγικό σχέδιο του ΣΕΒ για μια ψηφιακά ανεπτυγμένη Ελλάδα

5.4 Ποια σημεία πρέπει να προσέξουν οι επιχειρήσεις κατά την εφαρμογή του Κανονισμού

Ο Κανονισμός θέτει νέες κανονιστικές απαιτήσεις προς τις επιχειρήσεις, οι οποίες έρχονται να προστεθούν στις ήδη υφιστάμενες για την προστασία των προσωπικών δεδομένων (αλλά και φυσικά σε όλες τις υπόλοιπες απαιτήσεις που προκύπτουν από το λοιπό θεσμικό πλαίσιο κάθε κλάδου). Έχει πολύ μεγαλύτερο πεδίο εφαρμογής από ό,τι η Οδηγία, αφορά πολύ περισσότερες επιχειρήσεις, «καταργεί» τα σύνορα δραστηριοποίησης, προβλέπει πολύ μεγαλύτερες ποινές, στρέφει όλο το βάρος της απόδειξης συμμόρφωσης στις επιχειρήσεις δίνοντας «δευτερεύοντα» ρόλο στις εποπτικές Αρχές και στην κατεύθυνση αυτή θέτει πολύ συγκεκριμένες απαιτήσεις που εξασφαλίζουν τη συμμόρφωση.

Δ.38 Ποια σημεία πρέπει να προσέξουν οι επιχειρήσεις κατά την εφαρμογή του Κανονισμού
✓ Διαχείριση του κόστους που επιβαρύνει την καθημερινή λειτουργία για την επίτευξη συμμόρφωσης
✓ Επιλογή των κατάλληλων στελεχών ή / και εξωτερικών συνεργατών (κύριο κριτήριο επιλογής: αξιοπιστία και αποτελεσματικότητα)
✓ Λανθασμένη εντύπωση ότι δεν εμπίπτουν στον Κανονισμό και ως εκ τούτου ότι δεν χρειάζεται να προβούν σε καμία δράση συμμόρφωσης.
✓ Λανθασμένη εντύπωση ότι δεν απειλούνται από περιστατικά παραβίασης των συστημάτων τους και ότι είναι ασφαλείς
✓ Σημεία υψηλής τεχνικότητας: ○ Φορητότητα των δεδομένων ○ Δικαίωμα στη λήθη ○ Εξασφάλιση συγκατάθεσης υποκειμένου ○ Συμβάσεις με τρίτα μέρη - Σχέσεις με Εκτελούντες την Επεξεργασία
Πηγή: Ομάδα Εργασίας ΣΕΒ «Προσωπικά δεδομένα»

5.4.1 Γενικές προκλήσεις και παγίδες

Αναλυτικότερα, με τον Κανονισμό προκύπτουν **κόστη που επιβαρύνουν την καθημερινή λειτουργία** των επιχειρήσεων και ο τρόπος που θα επιδιώξουν να τα διαχειριστούν αποτελεί σημαντική πρόκληση:

- Συγκρότηση και μισθοδοσία της Ομάδας Εργασίας ή /και του ΥΠΔ που θα αναλάβει τις ενέργειες συμμόρφωσης στον Κανονισμό.
- Εκπόνηση της εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων, είτε αξιοποιηθούν ίδιες δυνάμεις της επιχείρησης, είτε υπάρξει συνεργασία με εξωτερικό σύμβουλο.

- Ανασχεδιασμό των συστημάτων σχετικά με τον τρόπο εξασφάλισης της συγκατάθεσης των υποκειμένων.
- Ανασχεδιασμό όλων των πληροφοριακών συστημάτων για την ενίσχυση της προστασίας από επιθέσεις παραβίασης ασφάλειας.
- Διαμόρφωση των νέων πολιτικών και διαδικασιών για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα.
- Διάδοση και κατανόηση εντός της επιχείρησης των νέων υποχρεώσεων, πολιτικών και διαδικασιών που προκύπτουν.

Τα κόστη αυτά είναι αναμενόμενο ότι προκαλούν - το λιγότερο - προβληματισμό όσον αφορά στον τρόπο που μπορεί να κερδηθεί το στοίχημα της συμμόρφωσης με τον Κανονισμό, ειδικά τη στιγμή που η ελληνική επιχειρηματικότητα, και κυρίως οι μικρομεσαίες επιχειρήσεις, αντιμετωπίζει δύσκολες οικονομικές συνθήκες, παρά τα - διστακτικά - σημάδια ανάκαμψης.

Επιπροσθέτως, αποτελεί πρόκληση για τις επιχειρήσεις η **επιλογή των κατάλληλων στελεχών ή / και συνεργατών** που θα τους βοηθήσουν στην ικανοποίηση των απαιτήσεων του Κανονισμού, καθώς ήδη «ανοίγεται» μια νέα αγορά παροχής συμβουλευτικών και εκπαιδευτικών υπηρεσιών, αλλά και στελεχών ΥΠΔ, η οποία προφανώς δεν μπορεί να είναι όλη υψηλού επιπέδου. Απαιτείται επομένως, ιδιαίτερη προσοχή στον τρόπο και τα κριτήρια επιλογής, αλλά και προσεκτική αξιολόγηση των προσφερόμενων υπηρεσιών κάθε συνεργάτη. Η αξιοπιστία και η αποτελεσματικότητα πρέπει να αποτελούν τη βάση επιλογής, με τις επιχειρήσεις να εστιάζουν σε επιλογές που ταιριάζουν στα δικά τους χαρακτηριστικά, ανάγκες, πληροφοριακά συστήματα κ.λπ. Κατά τη γνώμη μας, οι επιχειρήσεις μπορούν να θέσουν σε δεύτερο επίπεδο το καθαρά οικονομικό κόστος, καθώς αυτό που είναι σημαντικό είναι ότι μέσα από τη διαδικασία συμμόρφωσης στον Κανονισμό φιλοδοξείται να προκύψουν οφέλη που θα αναμορφώσουν συνολικά το επιχειρηματικό μοντέλο και την επιχειρηματική κουλτούρα.

Σημαντική «παγίδα» για τις επιχειρήσεις αποτελεί επίσης, το γεγονός λανθασμένα **να έχουν την πεποίθηση ότι δεν εμπίπτουν στον Κανονισμό** και ως εκ τούτου να θεωρούν ότι δεν χρειάζεται να προβούν σε καμία δράση συμμόρφωσης. Η αντίληψη αυτή είναι ιδιαίτερα επικίνδυνη καθώς μπορεί να φέρει τις επιχειρήσεις αντιμέτωπες με υψηλά πρόστιμα και ισχυρό πλήγμα στη φήμη τους και για το λόγο αυτό καλούμε για την ιδιαίτερη προσοχή τους. Ενδεικτικά, οι επιχειρήσεις μπορεί να μην έχουν αντιληφθεί ότι κατέχουν και επεξεργάζονται προσωπικά δεδομένα, ή να μην

κατανοούν πώς αυτά ορίζονται, ή να νομίζουν ότι μόνο οι μεγάλες επιχειρήσεις πρέπει να λάβουν μέτρα κ.ο.κ.

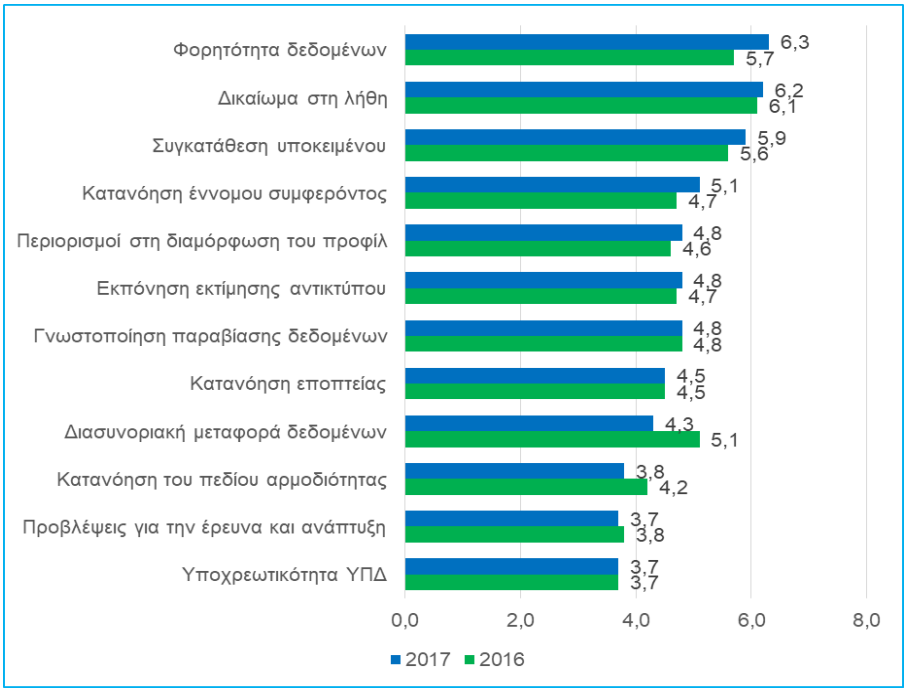
Τέλος, η πεποίθηση ορισμένων επιχειρήσεων ότι **δεν απειλούνται από περιστατικά παραβίασης των συστημάτων τους** πρόκειται περί πλάνης. Παραφράζοντας τον πρώην Διευθυντή του FBI, Robert S. Mueller III, οι οργανισμοί διακρίνονται σε τρεις κατηγορίες: α) σε εκείνους που έχουν ήδη πέσει θύμα παραβίασης των δεδομένων τους και το έχουν αντιληφθεί, β) σε εκείνους που έχουν ήδη πέσει θύμα παραβίασης των δεδομένων τους και δεν το αντιληφθεί ακόμα και γ) σε εκείνους που δεν έχουν ακόμα πέσει θύμα παραβίασης των δεδομένων τους, αλλά θα πέσουν στο προσεχές μέλλον. Πρέπει επομένως να γίνει απόλυτα κατανοητό ότι κανένας οργανισμός (επιχείρηση ή δημόσιος φορέας) δεν έχει συστήματα 100% ασφαλή έναντι περιστατικών παραβίασης δεδομένων, για αυτό άλλωστε χρειάζεται επαγρύπνηση και διαρκής παρακολούθηση.

5.4.2 Περιοχές υψηλής τεχνικότητας

Πλέον των όσων ήδη προαναφέρθηκαν, οι επιχειρήσεις έρχονται αντιμέτωπες και με ορισμένες υψηλής «τεχνικότητας» διατάξεις, που χρήζουν ιδιαίτερης προσοχής. Σύμφωνα με τη διεθνή έρευνα των IAPP και EY, αυτές αποτελούν: **α) η φορητότητα των δεδομένων** (με αξιοσημείωτη διαφορά από το προηγούμενο έτος, γεγονός που σημαίνει ότι όσο πλησιάζει η έναρξη εφαρμογής του Κανονισμού, γίνεται αντιληπτή η δυσκολία σχετικά με την ικανοποίηση της συγκεκριμένης πρόβλεψης) και **β) το δικαίωμα στη λήθη (Δ39).**

Συμπληρωματικά στις εν λόγω διατάξεις, κατά την κρίση της συγγραφικής ομάδας, οι διατάξεις για την εξασφάλιση της συγκατάθεσης και οι συμβάσεις με τρίτα μέρη αποτελούν άλλα δύο σημεία του Κανονισμού που παρουσιάζουν υψηλή τεχνικότητα. Στο πλαίσιο αυτό, στις επόμενες ενότητες παρέχονται χρήσιμες διευκρινίσεις που διευκολύνουν το έργο συμμόρφωσης των υπόχρεων επιχειρήσεων.

Δ.39 Σημεία συμμόρφωσης στον Κανονισμό που δυσκολεύουν τις επιχειρήσεις, 2016-2017
Σημείωση: Κλίμακα 0 έως 10 (0: Κανένας βαθμός δυσκολίας, 10: Πάρα πολύ υψηλός βαθμός δυσκολίας), Δυνατότητα πολλαπλών επιλογών.
Πηγή: IAPP-EY, "Annual Privacy Governance Report", 2017



5.4.2.1 Φορητότητα δεδομένων[107]

Στο άρθρο 20 του Κανονισμού προβλέπεται ότι το υποκείμενο έχει το δικαίωμα **να λαμβάνει** τα δεδομένα προσωπικού χαρακτήρα που το αφορούν από τον Υπεύθυνο Επεξεργασία στον οποίο τα έχει παράσχει, σε δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα μορφότυπο. Περαιτέρω, έχει το δικαίωμα **να διαβιβάζει** τα εν λόγω δεδομένα σε άλλον Υπεύθυνο Επεξεργασίας, όταν η επεξεργασία: α) βασίζεται σε συγκατάθεση και β) διενεργείται με αυτοματοποιημένα μέσα. Σε αυτές τις περιπτώσεις, έχει το δικαίωμα να ζητά την **απευθείας** διαβίβαση των δεδομένων του από έναν Υπεύθυνο Επεξεργασίας σε άλλον, σε περίπτωση που αυτό είναι τεχνικά εφικτό (π.χ. αλλαγή παρόχου κινητής/σταθερής τηλεφωνίας).

5.4.2.2 Δικαίωμα διαγραφής (εναλλακτικά, Δικαίωμα στη λήθη)

Στο άρθρο 17 του Κανονισμού προβλέπεται ότι ο Υπεύθυνος Επεξεργασίας υποχρεούται να διαγράψει τα δεδομένα προσωπικού χαρακτήρα, **χωρίς**

[107] Κατεβάστε εδώ τις Κατευθυντήριες Γραμμές της Ομάδας Εργασίας του άρθρου 29 σχετικά με το δικαίωμα στη φορητότητα των δεδομένων και Απαντήσεις σε Συχνές Ερωτήσεις

αδικαιολόγητη καθυστέρηση, σε περίπτωση που το υποκείμενο των δεδομένων υποβάλλει σχετικό αίτημα, με την προϋπόθεση ότι ισχύει έστω μία από τις ακόλουθες συνθήκες[108]: α) τα δεδομένα να μην είναι πλέον απαραίτητα για τους σκοπούς για τους οποίους συλλέχθηκαν ή υποβλήθηκαν σε επεξεργασία, β) το υποκείμενο να ανακαλέσει τη συγκατάθεσή του, γ) το υποκείμενο να αντιτίθεται στην επεξεργασία και δ) τα δεδομένα υποβλήθηκαν σε επεξεργασία παράνομα. Ιδιαίτερη προσοχή χρειάζεται από τις επιχειρήσεις στην περίπτωση που έχουν δημοσιοποιήσει τα εν λόγω δεδομένα. Ο Κανονισμός προβλέπει ότι οφείλουν να τα διαγράψουν, λαμβάνοντας υπόψη τη διαθέσιμη τεχνολογία και αναλαμβάνοντας το κόστος εφαρμογής της ενέργειας. Είναι προφανές ότι οι προκλήσεις για τους Υπευθύνους Επεξεργασίας είναι πολύ υψηλές, καθώς θα πρέπει να εξασφαλίζουν την πλήρη διαγραφή των δεδομένων ενδεικτικά από τις μηχανές αναζήτησης, αρχεία εφημερίδων κ.λπ.

5.4.2.3 Εξασφάλιση συγκατάθεσης[109]

Στα άρθρα 7 και 8 του Κανονισμού προβλέπεται ότι δεν νοείται επεξεργασία δεδομένων προσωπικού χαρακτήρα δίχως να έχει προηγηθεί η εξασφάλιση συγκατάθεσης του υποκειμένου. Σχετικά, απαιτείται ιδιαίτερη προσοχή από τους Υπευθύνους Επεξεργασίας ως προς τα εξής σημεία: α) πρέπει να είναι σε θέση να αποδείξουν τη λήψη συγκατάθεσης ανά πάσα στιγμή[110], β) η διατύπωση της δήλωσης συγκατάθεσης πρέπει να είναι σαφής και απλή, ενώ η μορφή της πρέπει να είναι κατανοητή και εύκολα προσβάσιμη, γ) το υποκείμενο πρέπει να προβαίνει σε συγκεκριμένη θετική ενέργεια (επομένως, προσυμπληρωμένα πεδία και γενικότερα αυτοματοποιημένες διαδικασίες δεν γίνονται αποδεκτές από τον Κανονισμό), δ) η συγκατάθεση πρέπει να είναι διακριτή από άλλα θέματα (π.χ. δεν μπορεί να συμπεριλαμβάνεται εντός των Γενικών Όρων Συναλλαγής) και να μην αποτελεί προϋπόθεση για εκτέλεση σύμβασης (π.χ. παροχή υπηρεσίας όταν δεν είναι αναγκαίο) και ε) το υποκείμενο πρέπει να μπορεί να ανακαλέσει τη συγκατάθεσή του οποτεδήποτε, με αντίστοιχα εύκολο τρόπο με την παροχή της[111].

---

[108] Ο Κανονισμός προβλέπει και ορισμένες άλλες περιπτώσεις οι οποίες για λόγους συντόμευσης δεν αναφέρονται. Δείτε αναλυτικά το άρθρο 17 εδώ.

[109] Δείτε εδώ τις Κατευθυντήριες Οδηγίες της Ομάδας Εργασίας άρθρου 29 για τη συγκατάθεση.

[110] Στην πράξη αυτό σημαίνει ότι συστήνεται στον Υπεύθυνο Επεξεργασίας να τηρεί αρχεία συγκατάθεσης, τα οποία μεταξύ άλλων θα περιέχουν τόσο την ημερομηνία λήψης της συγκατάθεσης (timestamp, χρονολογημένο έγγραφο), όσο και το ακριβές περιεχόμενο αυτής (αντίγραφο συμφωνίας και πολιτικής), ώστε να έχει άμεση πρόσβαση στους συγκεκριμένους όρους που συμφωνήθηκαν την εκάστοτε χρονική στιγμή.

[111] Ειδικές προβλέψεις υφίστανται στην περίπτωση παιδιών κάτω των 16 ετών, οπότε απαιτείται συγκατάθεση από το πρόσωπο που έχει τη γονική μέριμνα, με τον Υπεύθυνο Επεξεργασίας να οφείλει να καταβάλλει εύλογες προσπάθειες για να επαληθεύσει ότι πράγματι το σωστό άτομο υποβάλλει τη συγκατάθεση.

5.4.2.4 Συμβάσεις με τρίτα μέρη - Σχέσεις με Εκτελούντες την Επεξεργασία

Τα άρθρα 28 και 29 του Κανονισμού προβλέπουν συγκεκριμένες διατάξεις για τις περιπτώσεις εκείνες που η επεξεργασία πρόκειται να διενεργηθεί, για λογαριασμό του υπευθύνου επεξεργασίας, από εκτελούντα την επεξεργασία. Συνοπτικά, προβλέπεται ότι ο υπεύθυνος επεξεργασίας χρησιμοποιεί μόνο εκτελούντες που παρέχουν επαρκείς διαβεβαιώσεις για την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων, κατά τρόπο ώστε η επεξεργασία να πληροί τις απαιτήσεις του Κανονισμού και να διασφαλίζεται η προστασία των δικαιωμάτων του υποκειμένου των δεδομένων. Επίσης, τονίζεται ρητά ότι ο εκτελών την επεξεργασία λειτουργεί μόνον κατ' εντολή του υπευθύνου επεξεργασίας.

Η επεξεργασία από τον εκτελούντα την επεξεργασία διέπεται από σύμβαση, η οποία δεσμεύει τον εκτελούντα την επεξεργασία σε σχέση με τον υπεύθυνο επεξεργασίας και καθορίζει το αντικείμενο, τη διάρκεια της επεξεργασίας, τη φύση της επεξεργασίας, το σκοπό της επεξεργασίας, το είδος των δεδομένων προσωπικού χαρακτήρα, τις κατηγορίες των υποκειμένων των δεδομένων και τις υποχρεώσεις και τα δικαιώματα του Υπευθύνου Επεξεργασίας.

Δ.40 Βασικές συμβουλές για τη σύμβαση μεταξύ Υπευθύνου Επεξεργασίας και Εκτελούντα την Επεξεργασία

Η σύμβαση μεταξύ Υπευθύνου Επεξεργασίας και Εκτελούντα την Επεξεργασία προτείνεται να περιλαμβάνει όρους που να εξασφαλίζουν τα ακόλουθα:

- Ο Εκτελών την Επεξεργασία ενεργεί μόνο με γραπτή εντολή του Υπευθύνου Επεξεργασίας.
- Τα άτομα που επεξεργάζονται τα δεδομένα υπογράφουν σύμβαση εχεμύθειας και εμπιστευτικότητας.
- Ο Εκτελών την Επεξεργασία λαμβάνει τα κατάλληλα οργανωτικά και τεχνικά μέτρα για να εξασφαλίσει την ασφάλεια της επεξεργασίας.
- Ο Εκτελών την Επεξεργασία δύναται να εμπλέκει υπό-εκτελούντες (sup-processors) στην επεξεργασία μόνο με την προηγούμενη συγκατάθεση του Υπεύθυνου Επεξεργασίας και βάσει της γραπτής σύμβασης.
- Ο Εκτελών την Επεξεργασία οφείλει να βοηθά τον Υπεύθυνο Επεξεργασίας στα αιτήματα πρόσβασης των υποκειμένων στα δεδομένα τους επιτρέποντας τους να ασκούν τα δικαιώματά τους βάσει του Κανονισμού.
- Ο Εκτελών την Επεξεργασία οφείλει να επικουρεί τον Υπεύθυνο Επεξεργασίας στην εκπλήρωση των υποχρεώσεών του Κανονισμού σε σχέση με την ασφάλεια της επεξεργασίας, την γνωστοποίηση των παραβιάσεων των προσωπικών δεδομένων και την Εκτίμηση Αντικτύπου σχετικά με την προστασία δεδομένων.

Επιπλέον, επισημαίνεται ότι:

- Ο Εκτελών την Επεξεργασία δεν μπορεί να προσλάβει άλλον εκτελούντα την επεξεργασία χωρίς προηγούμενη ειδική ή γενικά άδεια του υπευθύνου επεξεργασίας.
- Ο Εκτελών την Επεξεργασία επεξεργάζεται τα δεδομένα προσωπικού χαρακτήρα μόνο βάσει καταγεγραμμένων εντολών του Υπευθύνου Επεξεργασίας.

Η σύμβαση αποτελεί αντικείμενο διαπραγμάτευσης μεταξύ των δύο μερών, ωστόσο είναι προφανές ότι ο Υπεύθυνος Επεξεργασίας έχει αυξημένη ισχύ στη διαδικασία διατύπωσης ή αναδιατύπωσης των όρων. Μάλιστα, υπάρχει νομική βάση για προσβολή υφιστάμενης σύμβασης σε περίπτωση που Εκτελών την Επεξεργασία δεν υπογράφει τους νέους όρους (σχετικούς με τον Κανονισμό) της σύμβασης.

Πηγή: Ομάδα Εργασίας ΣΕΒ «Προσωπικά δεδομένα»

5.5 Συχνές Ερωτήσεις και Απαντήσεις

Στην παρούσα ενότητα παρουσιάζονται απαντήσεις σε συχνές ερωτήσεις των επιχειρήσεων σχετικά με τον Κανονισμό και τις υποχρεώσεις που απορρέουν από αυτόν[112].

5.5.1 Σχετικά με τον Υπεύθυνο Προστασίας Δεδομένων (ΥΠΔ)

Η ΑΠΔΠΧ δημοσίευσε τον Φεβρουάριο του 2018 τις ακόλουθες απαντήσεις σε συχνές ερωτήσεις των υπόχρεων σχετικά με τον ΥΠΔ.

1. Ποιοι οργανισμοί πρέπει να ορίζουν ΥΠΔ;

Ο ορισμός ΥΠΔ είναι υποχρεωτικός όταν:

- Η επεξεργασία διενεργείται από δημόσια αρχή ή δημόσιο φορέα (συμπεριλαμβανομένων και φυσικών ή νομικών προσώπων δημοσίου ή ιδιωτικού δικαίου που ασκούν δημόσια εξουσία). Εξαιρούνται τα δικαστήρια όταν ενεργούν υπό τη δικαιοδοτική τους αρμοδιότητα.
- Οι βασικές δραστηριότητες του υπευθύνου επεξεργασίας συνιστούν τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε μεγάλη κλίμακα (π.χ. ασφαλιστικές ή τραπεζικές υπηρεσίες, υπηρεσίες τηλεφωνίας ή διαδικτύου, παροχή υπηρεσιών ασφαλείας, όλες οι μορφές παρακολούθησης και διαμόρφωσης «προφίλ» στο διαδίκτυο, όπως για σκοπούς συμπεριφορικής διαφήμισης).
- Διενεργείται μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων (π.χ. στο πλαίσιο παροχής υπηρεσιών υγείας από νοσοκομεία) ή δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα.
- Προβλέπεται από το δίκαιο κράτους-μέλους

Ως «βασικές δραστηριότητες» θεωρούνται όσες αποτελούν αναπόσπαστο κομμάτι για την επίτευξη των στόχων του υπευθύνου επεξεργασίας ή του εκτελούντα την επεξεργασία. **Για τον προσδιορισμό της μεγάλης κλίμακας επεξεργασίας** πρέπει να λαμβάνονται υπόψη: α) ο αριθμός των εμπλεκομένων υποκειμένων, είτε ως συγκεκριμένος αριθμός είτε ως ποσοστό επί του πληθυσμού, β) ο όγκος και το εύρος των δεδομένων, γ) η διάρκεια ή ο μόνιμος χαρακτήρας της επεξεργασίας και δ) η

[112] Οι απαντήσεις διαμορφώθηκαν κατά την εκτίμηση των συγγραφέων της παρούσας έκθεσης. Σε καμία περίπτωση δεν δεσμεύουν τον ΣΕΒ και η υιοθέτησή τους δεν αποτελεί τεκμήριο πλήρους συμμόρφωσης με τον Κανονισμό.

γεωγραφική έκταση της επεξεργασίας. **Παραδείγματα που <u>δεν</u> συνιστούν επεξεργασία μεγάλης κλίμακας είναι, μεταξύ άλλων, η επεξεργασία δεδομένων ασθενών από ιδιώτη ιατρό και η επεξεργασία δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα από ιδιώτη δικηγόρο.**[113]

2. Δεν υποχρεούμαι, αλλά επιθυμώ να ορίσω ΥΠΔ στην επιχείρησή μου. Τι ισχύει σε αυτή την περίπτωση;

Κάθε οργανισμός μπορεί να ορίσει ΥΠΔ. Ακόμη και στις περιπτώσεις που ο ορισμός ΥΠΔ δεν είναι υποχρεωτικός, ενθαρρύνονται τέτοιου είδους εθελοντικές ενέργειες. Όταν ένας οργανισμός ορίζει ΥΠΔ σε εθελοντική βάση, σε σχέση με τον ορισμό, τη θέση και τα καθήκοντά του θα ισχύουν οι ίδιες απαιτήσεις ως εάν ο ορισμός να ήταν υποχρεωτικός (βλ. ερώτηση 5).

3. Μπορεί να οριστεί ένας ΥΠΔ για περισσότερους φορείς ή οργανισμούς;

Ναι. Όμιλος επιχειρήσεων ή περισσότεροι δημόσιοι φορείς, λαμβάνοντας υπόψη το μέγεθος και την οργανωτική τους δομή, μπορούν να ορίσουν έναν μόνο ΥΠΔ, υπό την προϋπόθεση **να είναι διαθέσιμος και εύκολα προσβάσιμος** σε κάθε εγκατάσταση ή φορέα είτε με φυσική παρουσία στις ίδιες εγκαταστάσεις με τους υπαλλήλους, είτε μέσω ανοικτής τηλεφωνικής γραμμής ή άλλου ασφαλούς μέσου επικοινωνίας και σε γλώσσα που χρησιμοποιούν οι ενδιαφερόμενες εποπτικές αρχές και τα οικεία υποκείμενα των δεδομένων.

4. Ποια είναι τα καθήκοντα του ΥΠΔ;

Ο ΥΠΔ προάγει την κουλτούρα της προστασίας προσωπικών δεδομένων εντός του οργανισμού ή φορέα. Τα ελάχιστα καθήκοντα του ΥΠΔ είναι τα ακόλουθα:

- Να ενημερώνει και να συμβουλεύει τον οργανισμό και τους υπαλλήλους του σχετικά με τις υποχρεώσεις τους που απορρέουν από τον Κανονισμό και άλλες διατάξεις περί προστασίας δεδομένων.
- Να παρακολουθεί την εσωτερική συμμόρφωση με τον Κανονισμό και άλλες διατάξεις περί προστασίας δεδομένων (π.χ. προσδιορισμός και διαχείριση δραστηριοτήτων επεξεργασίας, εκπαίδευση προσωπικού, διενέργεια εσωτερικών ελέγχων).
- Να παρέχει συμβουλές για την εκτίμηση αντικτύπου και να παρακολουθεί την υλοποίησή της.

[113] Επισημαίνεται ότι οι Υπεύθυνοι Επεξεργασίας δεν θα πρέπει να συγχέουν την επεξεργασία μεγάλης κλίμακας με το μέγεθος της επιχείρησης, βάσει Κύκλου Εργασιών. Αυτό που είναι σημαντικό είναι ο **όγκος** των προσωπικών δεδομένων και η **έκταση** της επεξεργασίας.

- Να είναι το πρώτο σημείο επαφής για τις εποπτικές αρχές και τα υποκείμενα των δεδομένων (εργαζόμενοι, πελάτες κ.λπ.).
- Να συνεργάζεται με την εποπτική αρχή.

5. Ποιες είναι οι υποχρεώσεις του εργοδότη ενός ΥΠΔ;

Ο εργοδότης υποχρεούται να δημοσιεύσει τα στοιχεία επικοινωνίας του ΥΠΔ και να τα ανακοινώσει στην εποπτική αρχή. Επίσης, οφείλει να διασφαλίζει ότι ο ΥΠΔ:

- Συμμετέχει σε όλα τα ζητήματα σχετικά με την προστασία προσωπικών δεδομένων (π.χ. παρουσία σε συσκέψεις ανώτερων και μεσαίων στελεχών της διοίκησης και κατά τη λήψη αποφάσεων, καταγραφή λόγων διαφωνίας με τις συμβουλές του, έγκαιρη διαβίβαση πληροφοριών για παροχή γνώμης, άμεση λήψη γνώμης σε περίπτωση περιστατικού παραβίασης).
- Έχει ελεύθερη πρόσβαση σε δεδομένα και πράξεις επεξεργασίας
- Έχει στη διάθεσή του τους απαραίτητους πόρους για την εκπλήρωση των καθηκόντων του (π.χ. ενεργή στήριξη από τα ανώτερα διοικητικά στελέχη, οικονομικοί πόροι, υποδομές, συνεχής κατάρτιση).
- Εκπληρώνει τα καθήκοντά του με ανεξάρτητο τρόπο (δεν λαμβάνει εντολές για την άσκηση των καθηκόντων του) και δεν απολύεται ούτε υφίσταται κυρώσεις επειδή επιτέλεσε τα καθήκοντά του.
- Λογοδοτεί απευθείας στο ανώτατο διοικητικό επίπεδο του εργοδότη.
- Όταν ασκεί πρόσθετα καθήκοντα, αυτά να μην συνεπάγονται σύγκρουση συμφερόντων (π.χ. δεν μπορεί να κατέχει θέση από την οποία μπορεί να καθορίζει τους σκοπούς και τα μέσα της επεξεργασίας, όπως θέσεις ανώτερης διοίκησης).
- Δεσμεύεται από την τήρηση του απορρήτου ή της εμπιστευτικότητας σχετικά με την εκτέλεση των καθηκόντων του.

6. Ο ΥΠΔ είναι υπάλληλος ή εξωτερικός συνεργάτης;

Είτε το ένα είτε το άλλο. Ο ΥΠΔ μπορεί να είναι μέλος του προσωπικού του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία (εσωτερικός υπεύθυνος προστασίας δεδομένων) ή να ασκεί τα καθήκοντά του βάσει σύμβασης παροχής υπηρεσιών (εξωτερικός συνεργάτης). Σε κάθε περίπτωση, μπορεί να συνεπικουρείται από ομάδα, εφόσον απαιτείται. Συνιστάται δε να είναι εγκατεστημένος εντός ΕΕ, ανεξάρτητα από το εάν ο Υπεύθυνος Επεξεργασίας ή ο Εκτελών την Επεξεργασία είναι ή όχι εγκατεστημένοι στην ΕΕ.

7. Τι επαγγελματικά προσόντα θα πρέπει να έχει ο ΥΠΔ; Προβλέπεται σχετική πιστοποίηση;

Ο ΥΠΔ διορίζεται ιδίως βάσει της εμπειρογνωσίας που διαθέτει στον τομέα του δικαίου και των πρακτικών περί προστασίας δεδομένων, καθώς και βάσει της ικανότητας εκπλήρωσης των καθηκόντων του. Το αναγκαίο επίπεδο εμπειρογνωσίας θα πρέπει να καθορίζεται ανάλογα με τις πράξεις επεξεργασίας δεδομένων που διενεργούνται και από την προστασία την οποία απαιτούν τα δεδομένα προσωπικού χαρακτήρα που υφίστανται επεξεργασία. Παράλληλα, ο ΥΠΔ πρέπει να έχει γνώση του τομέα δραστηριότητας του οργανισμού ή φορέα στον οποίο απασχολείται αλλά και των τεχνολογιών πληροφορίας και ασφάλειας των δεδομένων.

Ο Κανονισμός **δεν θέτει κάποια υποχρεωτική απαίτηση για πιστοποίηση του ΥΠΔ**, ούτε καν ενθαρρύνει σχετική πιστοποίηση σε προαιρετική βάση (βλ. την υπ' αριθμ. πρωτ. Γ/ΕΞ/6007/09-08-2017 **Ανακοίνωση** και τη **Γνωμοδότηση 7/2017** της Αρχής).

Συμπληρωματικά στις ως άνω διευκρινίσεις της Αρχής, αναφέρουμε και τα ακόλουθα σχετικά με το **ζήτημα της ευθύνης του ΥΠΔ έναντι του υποκειμένου ή / και της Αρχής**: ο ΥΠΔ δεν φέρει ευθύνη έναντι του υποκειμένου ή / και της Αρχής, αλλά την ευθύνη έχει ο Υπεύθυνος και ο Εκτελών την Επεξεργασία. Ο ΥΠΔ ευθύνεται μόνο ως προς την πλημμελή εκτέλεση των υποχρεώσεών του (δηλαδή την ποιότητα των υπηρεσιών του) προς τον Υπεύθυνο Επεξεργασίας που τον έχει προσλάβει. Σημειώνεται ότι ισχύουν για τον ΥΠΔ οι γενικές διατάξεις αστικής και ποινικής ευθύνης, δίχως να υπάρχει προσωπική δίωξη κατά αυτού.

5.5.2 Σχετικά με την Εκτίμηση Αντικτύπου (ΕΑ)

Στην παρούσα ενότητα παρουσιάζονται οι απαντήσεις σε συχνές ερωτήσεις των υπόχρεων σχετικά με την ΕΑ.

1. Πρέπει η επιχείρησή μου να εκπονήσει σε Εκτίμηση Αντικτύπου (ΕΑ) σχετικά με την προστασία δεδομένων και ποια είναι τα οφέλη;
Όταν ένα είδος επεξεργασίας ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα των φυσικών προσώπων, τότε ο Υπεύθυνος Επεξεργασίας διενεργεί, πριν από την επεξεργασία, εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα (άρθρο 35).

Επομένως, η φράση-κλειδί για την υποχρεωτικότητα εκπόνησης ΕΑ είναι **«ενδέχεται να επιφέρει υψηλό κίνδυνο»**. Σχετικά, στο άρθρο 57 του Κανονισμού προβλέπεται ότι η εποπτική Αρχή καταρτίζει και διατηρεί κατάλογο σε σχέση με την απαίτηση για διενέργεια ΕΑ. Επομένως, αναμένεται μετά την ψήφιση του εφαρμοστικού Νόμου η ΑΠΔΧΠ να προβεί σε σχετικές ενέργειες που θα συμβάλλουν στην αποσαφήνιση της υποχρεωτικότητας.

Έως τότε, εύλογα διατηρείται το ερώτημα στις επιχειρήσεις σχετικά με το αν πρέπει να εκπονήσουν ΕΑ, καθώς αυτή θα έπρεπε να έχει ολοκληρωθεί πριν την επεξεργασία των προσωπικών δεδομένων και επομένως πριν την έναρξη εφαρμογής του Κανονισμού στις 25 Μαΐου 2018. Σε κάθε όμως περίπτωση, συστήνεται στις επιχειρήσεις που συνεχίζουν να αμφιταλαντεύονται σχετικά, να προχωρήσουν σε εκπόνηση ΕΑ, καθώς τα οφέλη που προκύπτουν είναι πολλαπλά:

Η εκπόνηση ΕΑ αποτελεί για μια διαδικασία κατά την οποία ο Υπεύθυνος Επεξεργασίας εντοπίζει, αξιολογεί και μετριάζει τους κινδύνους που προκύπτουν από την επεξεργασία των δεδομένων. Περιλαμβάνει: α) τη συστηματική περιγραφή των πράξεων και των σκοπών της επεξεργασίας, συμπεριλαμβανομένου του έννομου συμφέροντος που επιδιώκεται, β) την εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας σε συνάρτηση με τους σκοπούς, γ) την εκτίμηση των κινδύνων που προκύπτουν για τα υποκείμενα και δ) τα προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων, περιλαμβανομένων των εγγυήσεων, των μέτρων και μηχανισμών ασφάλειας, ώστε να διασφαλίζεται η προστασία των δεδομένων. Δηλαδή, η ΕΑ αποτελεί ένα ευέλικτο εργαλείο ανάλυσης κινδύνων για τις επιχειρήσεις, βοηθώντας τες να κατανοήσουν και να μετριάσουν τους κινδύνους από τους οποίους

απειλούνται, όχι μόνο κατά την τήρηση των προσωπικών δεδομένων, αλλά και ως μέρος της γενικότερης πολιτικής ασφαλείας που έτσι και αλλιώς θα έπρεπε να ακολουθούν.

2. Πόσο συχνά πρέπει η επιχείρηση να προβαίνει σε ΕΑ σχετικά με την προστασία δεδομένων;
Ο Κανονισμός δεν ορίζει ρητά πόσο συχνά πρέπει να εκπονείται μια ΕΑ. Ενδεχομένως, στον εφαρμοστικό Νόμο να υπάρξουν σχετικές προβλέψεις. Σε κάθε περίπτωση, αυτό που είναι σημαντικό να γίνει κατανοητό είναι ότι η ΕΑ αποτελεί μια δυναμική «άσκηση» για κάθε Υπεύθυνο Επεξεργασίας, δεν είναι μια μελέτη που εκπονείται "one-off".

Ως «οδηγό» για τις επιχειρήσεις, με ιδιαίτερη προσοχή στην εφαρμογή της, μπορεί να χρησιμοποιηθεί η συμβουλή ότι, εφόσον δεν αλλάζει κάτι στις διαδικασίες της επιχείρησης, τότε δεν χρειάζεται η επικαιροποίηση της ΕΑ.

5.5.3 Σχετικά με λοιπά θέματα

Στην παρούσα ενότητα παρουσιάζονται οι απαντήσεις σε συχνές ερωτήσεις των υπόχρεων που δεν σχετίζονται με τον ΥΠΔ και την εκπόνηση ΕΑ.

1. Πότε τα προσωπικά δεδομένα που κατέχει η επιχείρησή μου δεν εμπίπτουν στο πεδίο εφαρμογής του Κανονισμού;
Προσωπικά δεδομένα που έχουν κρυπτογραφηθεί ή ψευδωνυμοποιηθεί κ.λπ., αλλά μπορούν να χρησιμοποιηθούν για την επαναναγνώριση ενός φυσικού προσώπου παραμένουν προσωπικά δεδομένα που εμπίπτουν στο πεδίο εφαρμογής του Κανονισμού.

Αντίθετα, τα προσωπικά δεδομένα που έχουν καταστεί ανώνυμα με τέτοιο τρόπο ώστε πλέον το φυσικό πρόσωπο να μην αναγνωρίζεται, δεν θεωρούνται πλέον δεδομένα προσωπικού χαρακτήρα.

Σημειώνεται ότι το κρίσιμο στοιχείο είναι η ανωνυμοποίηση να είναι μη αναστρέψιμη. Μόνο τότε τα δεδομένα είναι πραγματικά ανώνυμα και δεν εμπίπτουν στο πεδίο εφαρμογής του Κανονισμού.

2. Είναι υποχρεωτικό να πιστοποιηθεί η επιχείρησή μου για την προστασία προσωπικών δεδομένων και ποια είναι η διαδικασία;

Τα άρθρα 42 και 43 του Κανονισμού αναφέρονται στη θέσπιση μηχανισμών πιστοποίησης προστασίας δεδομένων. Δηλαδή, ο Κανονισμός παροτρύνει την υιοθέτηση συστημάτων πιστοποίησης από τους Υπευθύνους Επεξεργασίας και τους Εκτελούντες την Επεξεργασία, δίχως ωστόσο να τη θέτει υποχρεωτική. Σημειώνεται ότι οι φορείς πιστοποίησης που θα προσφέρουν τις υπηρεσίες τους στο εν λόγω πεδίο θα πρέπει πρώτα να διαπιστευθούν ανάλογα με τις απαιτήσεις που θα ορίσει η αρμόδια εποπτική Αρχή (εν προκειμένω η ΑΠΔΧΠ) και ο οργανισμός διαπίστευσης (εν προκειμένω το Εθνικό Σύστημα Διαπίστευσης-ΕΣΥΔ). Επομένως, στην Ελλάδα είναι πρώιμο να γίνεται συζήτηση για πιστοποίηση προστασίας δεδομένων, είναι ζήτημα που θα απασχολήσει τις επιχειρήσεις μετά την ψήφιση του εθνικού Νόμου και τις σχετικές αποφάσεις των ΑΠΔΧΠ και ΕΣΥΔ. Σημειώνεται ότι η διαπίστευση με σχετικό μηχανισμό πιστοποίησης συμβάλλει στην κατεύθυνση της απόδειξης λήψης των απαραίτητων μέτρων για την προστασία δεδομένων, δίχως ωστόσο να συνεπάγεται ότι δεν πρόκειται να επιβληθεί πρόστιμο σε οργανισμό που έχει πιστοποιηθεί σε περίπτωση παραβίασης.

3. Οι προηγούμενες άδειες της ΑΠΔΧΠ έχουν ισχύ μετά την 25η Μαΐου 2018;

Οι άδειες επεξεργασίας προσωπικών δεδομένων που έχει ήδη εκδώσει η Αρχή δεν έχουν πλέον κάποια τυπική ισχύ. Παρόλα αυτά, εξακολουθούν να αποτελούν ενισχυτικά στοιχεία για την απόδειξη της νομιμότητας προς την εποπτική Αρχή. Τέλος, εκτιμάται ότι στον εφαρμοστικό Νόμο του Κανονισμού θα υπάρχουν σχετικές προβλέψεις (π.χ. μεταβατικές διατάξεις, διευκρινίσεις).

4. Οι προηγούμενες γνωμοδοτήσεις της ΑΠΔΧΠ έχουν ισχύ μετά την 25η Μαΐου 2018;

Ναι, εφόσον το περιεχόμενό τους δεν έρχεται σε αντίθεση με το πνεύμα του Κανονισμού. Σχετικά με το παρόν ερώτημα αναφέρουμε συμπληρωματικά το ζήτημα που προαναφέρθηκε στην ενότητα 2.4.1 για την υπόθεση Facebook, όπου αναφορικά με την αναδρομικότητα της ποινής, η Věra Jourová τόνισε ότι «κυρώσεις δε μπορούν να εφαρμοστούν αναδρομικά, επομένως το Facebook δε θα υποστεί πρόστιμο για τη συγκεκριμένη παράβαση, όταν ο νέος Γενικός Κανονισμός εφαρμοστεί. Ωστόσο, από το Μάιο και έπειτα, δε θα διστάσουμε να χρησιμοποιήσουμε τις υψηλότερες δυνατές ποινές στην περίπτωση που οι Ευρωπαίοι πολίτες υποστούν μεγαλύτερη βλάβη».

5. Θέλω να συνεχίσω να διανέμω το newsletter της επιχείρησής μου στους πελάτες μου, πρέπει να ξαναζητήσω τη συγκατάθεσή τους;

Το συγκεκριμένο ζήτημα αποτελεί προϊόν ελλιπούς ενημέρωσης σχετικά με το πεδίο εφαρμογής του Κανονισμού. Και αυτό γιατί, για την περίπτωση των ηλεκτρονικών επικοινωνιών, δεν εφαρμόζεται ο Κανονισμός GDPR, αλλά η Οδηγία 2002/58/ΕΚ (ή Οδηγία e-Privacy όπως έγινε ευρέως γνωστή).

Πράγματι, στο κείμενο του Κανονισμού αναφέρεται ρητά ότι «Ο παρών κανονισμός δεν επιβάλλει πρόσθετες υποχρεώσεις σε φυσικά ή νομικά πρόσωπα σε σχέση με την επεξεργασία όσον αφορά την παροχή υπηρεσιών ηλεκτρονικών επικοινωνιών διαθέσιμων στο κοινό σε δημόσια δίκτυα επικοινωνίας στην Ένωση σε σχέση με θέματα τα οποία υπόκεινται στις ειδικές υποχρεώσεις με τον ίδιο στόχο που ορίζεται στην οδηγία 2002/58/ΕΚ.»

Άρα, βάσει των διατάξεων της Οδηγίας e-Privacy και του εθνικού Νόμου που την ενσωμάτωσε στην ελληνική έννομη τάξη, για να συνεχίσει να στέλνει ηλεκτρονικά στα email των πελατών το newsletter της μια επιχείρηση, αρκεί να μπορεί να αποδείξει ένα από τα παρακάτω:

1. Ότι απέκτησε το email με τη συγκατάθεση του πελάτη
2. Ότι απέκτησε το email στο πλαίσιο συναλλαγής με τον πελάτη κατά τη στιγμή της οποίας τον ενημέρωσε ότι θα το χρησιμοποιήσει και για διαφήμιση, να διαφημίζει παρόμοια προϊόντα και να του δίνει τη δυνατότητα για δωρεάν και εύκολη διαγραφή σε κάθε μήνυμα.

Σε αυτήν την περίπτωση δηλαδή η επιχείρηση ΔΕΝ χρειάζεται να προβεί σε ενέργειες ζητώντας συγκατάθεση.

Σε αντίθετη περίπτωση (δηλαδή μη τήρηση του σημείου 1 ή 2 άνω), το να διατηρεί τα emails των πελατών, όσο και να τους αποστέλλει email ζητώντας τη συγκατάθεσή τους για να συνεχίσει να τους αποστέλλει το newsletter, είναι παράνομα.

6. Επόμενα βήματα και αναμενόμενες εξελίξεις

6. Επόμενα βήματα και αναμενόμενες εξελίξεις

Βρισκόμενοι μόλις πέντε μήνες μετά την έναρξη εφαρμογής του Κανονισμού για την προστασία των προσωπικών δεδομένων, τα ερωτήματα που παραμένουν «ανοιχτά», τόσο σε επίπεδο ΕΕ, όσο και σε εθνικό επίπεδο, είναι πολλά. Ενδεικτικά, αναφέρουμε παρακάτω τα κυριότερα σημεία προβληματισμού για την επόμενη ημέρα του Κανονισμού, όπως τα έχουμε καταγράψει από την επικοινωνία με τις επιχειρήσεις, από επαφές με εμπειρογνώμονες, ειδικούς και στελέχη των αρχών και των συναρμόδιων υπουργείων, καθώς και από την παρακολούθηση της ευρωπαϊκής επικαιρότητας (αρθρογραφία, νομολογία, ευρωπαϊκός δημόσιος διάλογος κ.ά.).

Δ.41 Οι προκλήσεις της επόμενης ημέρας την έναρξης εφαρμογής του Κανονισμού
1. Ψήφιση εθνικής νομοθεσίας που είναι σε εκκρεμότητα
2. Αυξημένες ευθύνες για την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
3. Βαθμός ανταπόκρισης Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, με δεδομένη την υποστελέχωσή της
4. Τρόπος λειτουργίας Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων
5. Βαθμός ανταπόκρισης επιχειρήσεων στις υποχρεώσεις
6. Βαθμός ανταπόκρισης υποκειμένων
7. Βαθμός ανταπόκρισης φορέων δημόσιου τομέα
8. Αρμονική συνύπαρξη μεταξύ δυνατοτήτων που προσφέρουν οι τεχνολογικές εξελίξεις και προστασίας προσωπικών δεδομένων

1. Εθνική νομοθεσία

Το Σχέδιο Νόμου του Υπουργείου Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα σε εφαρμογή του Κανονισμού (ΕΕ) 2016/679, παρά τη διαβούλευση που πραγματοποιήθηκε στα τέλη Φεβρουαρίου, δεν έχει ακόμα ψηφιστεί. Πρόκειται για μια βασική εκκρεμότητα που δυσκολεύει τόσο τους οργανισμούς στην προσπάθεια συμμόρφωσής τους με τις νέες διατάξεις, όσο και την ίδια την ΑΠΔΠΧ, καθώς ο Κανονισμός αφήνει αρκετούς βαθμούς ελευθερίας στον εθνικό νομοθέτη, όπως έχει προαναφερθεί.

Ενδεικτικά αναφέρεται ότι δίχως την ψήφιση της εθνικής νομοθεσίας δεν είναι ξεκάθαρο το πεδίο σχετικά με τα συστήματα πιστοποίησης για την προστασία προσωπικών δεδομένων (θα είναι υπεύθυνη για τη χορήγηση η ΑΠΔΠΧ, ποια θα είναι

η εμπλοκή του ΕΣΥΔ κ.λπ.) με αποτέλεσμα να έχουν ήδη δημιουργηθεί φαινόμενα παραπλάνησης. Επιπλέον αναγκαία κρίνεται η θέσπιση ειδικότερων προβλέψεων και ο καθορισμός ζητημάτων που ανακύπτουν αναφορικά με σημαντικά καίρια θέματα όπως η επεξεργασία γενετικών, βιομετρικών ή δεδομένων υγείας, ο ορισμός του ορίου της ηλικίας του παιδιού κατά το οποίο θα απαιτείται η συγκατάθεση του προσώπου που έχει την γονική μέριμνα, οι ποινικές κυρώσεις του υπεύθυνου επεξεργασίας ή/και του υπεύθυνου προστασίας δεδομένων κ.ά.

Η αναγκαιότητα άμεσης ολοκλήρωσης της εθνικής νομοθεσίας, λαμβάνοντας υπόψη τις (ομολογουμένως πολλές σε αριθμό) προτεινόμενες βελτιωτικές παρεμβάσεις που έχουν κατατεθεί από τα εμπλεκόμενα μέρη κατά τη διαβούλευση, είναι προφανής. Κυρίως γιατί η καθυστέρηση ολοκλήρωσης της εθνικής νομοθεσίας αποτελεί ένδειξη **λανθασμένης σηματοδότησης** (signaling) προς την αγορά, σε σχέση με την υποχρέωση συμμόρφωσης, τον έλεγχο, τη σημαντικότητα του Κανονισμού κ.ά., με πολλαπλές πιθανές αρνητικές συνέπειες στην ουσία του σκοπού του νομοθέτη.

2. ΑΠΔΠΧ

Ο Κανονισμός αυξάνει τις προκλήσεις για την ΑΠΔΠΧ σε δύο κυρίως διαστάσεις:

α) οι ευθύνες είναι ιδιαίτερα αυξημένες, λόγω των υψηλών προστίμων που προβλέπονται και της ενίσχυσης των δικαιωμάτων των υποκειμένων, και

β) η συνεργασία μεταξύ των εποπτικών Αρχών είναι πλέον επιβεβλημένη, με συγκεκριμένα μάλιστα χρονοδιαγράμματα.

Στο πλαίσιο αυτό, αποτελεί στοίχημα για την ΑΠΔΠΧ ο τρόπος με τον οποίο θα καταφέρει να ανταπεξέλθει, ειδικά στην περίπτωση που λειτουργεί ως επικεφαλής εποπτική Αρχή και λαμβάνοντας υπόψη την αποδυνάμωση του στελεχιακού δυναμικού που έχει υποστεί λόγω αποχωρήσεων. Με δεδομένη λοιπόν, την ελλιπή στελέχωσή της ΑΠΔΠΧ, εγείρονται πλέον σοβαρά ερωτηματικά για τον τρόπο και την ταχύτητα ανταπόκρισής της σε ζητήματα που θα προκύψουν στο νέο ρυθμιστικό πλαίσιο που βρίσκεται στην αιχμή της επικαιρότητας. Παρά τη σχετική πρόβλεψη ενίσχυσης του δυναμικού στο Σχέδιο Νόμου, εύλογα εκφράζονται ανησυχίες για την περίοδο που θα απαιτηθεί για την ολοκλήρωση της διαδικασίας στην πράξη (ιδίως εάν αναλογιστούμε ότι ο νόμος δεν έχει ακόμη ψηφιστεί).

Είναι προφανές ότι η επιβολή των πρώτων προστίμων για παραβίαση των διατάξεων του Κανονισμού αποτελεί ένα κρίσιμο ορόσημο της επόμενης ημέρας που ενδιαφέρει τον επιχειρηματικό κόσμο (π.χ. σκεπτικό, έκταση, αυστηρότητα κ.λπ.).

Ιδίως εάν αναλογιστούμε ότι, ο προβληματισμός που προκλήθηκε για ένα σενάριο αύξησης των καταγγελιών για παραβίαση της προστασίας προσωπικών δεδομένων (πραγματικές, προσχηματικές ή και κακόβουλες από υποκείμενα ή / και ανταγωνιστές) μετά την 25η Μαΐου 2018, τελικά αποδείχθηκε στην πράξη όχι και τόσο υπερβολικός, τουλάχιστον στο εξωτερικό. Ήδη από την πρώτη μέρα εφαρμογής του Κανονισμού, το Facebook και η Google βρέθηκαν αντιμέτωπες με αγωγές για διεκδίκηση αποζημίωσης δισεκατομμυρίων ευρώ, από τον γνωστό ακτιβιστή σε θέματα ιδιωτικότητας, Max Schrems, κατηγορούμενες ενθαρρύνουν τους χρήστες τους να μοιράζονται τα προσωπικά τους δεδομένα. Στην Ελλάδα, δύο μήνες μετά την έναρξη εφαρμογής του Κανονισμού, η επιφυλακτικότητα των καταναλωτών μπορεί να παραμένει σε υψηλά επίπεδα, δεν έχουν ωστόσο διαπιστωθεί ακόμη φαινόμενα μαζικών καταγγελιών σε βάρος υπεύθυνων επεξεργασίας.

3. Εξελίξεις σε ευρωπαϊκό επίπεδο - Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων

Καθώς μετά την έναρξη εφαρμογής του Κανονισμού, το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων αντικατέστησε την Ομάδα Εργασίας του άρθρου 29, αναμένονται νέες διευκρινίσεις και γνωμοδοτήσεις σε περιοχές που είτε ήδη έχουν εντοπιστεί δυσκολίες (για παράδειγμα στην περίπτωση του διαφορετικού ηλικιακού ορίου για την παροχή συγκατάθεσης από τον έχοντα τη γονική μέριμνα του τέκνου), είτε ενδέχεται να αναδειχθούν νέα ζητήματα κατά την εφαρμογή στην πράξη. Ήδη το Συμβούλιο δημοσίευσε, την πρώτη ημέρα έναρξης εφαρμογής του Κανονισμού, Κατευθυντήριες Οδηγίες σχετικά με τα άρθρα 42 «Πιστοποίηση» και 43 «Φορείς Πιστοποίησης» και Κατευθυντήριες Οδηγίες σχετικά με το άρθρο 49 «Παρεκκλίσεις για ειδικές καταστάσεις». Στο πλαίσιο αυτό, οι επιχειρήσεις καλούνται να παρακολουθούν τις εξελίξεις και να παραμένουν συνεχώς ενημερωμένες. Έτσι, όπως και στην περίπτωση της ΑΠΔΠΧ, αποτελεί πρόκληση για την εφαρμογή του Κανονισμού ο τρόπος συνεργασίας, ανταλλαγής πληροφοριών και συντονισμού μεταξύ όλων των Αρχών των κρατών-μελών.

4. Βαθμός ανταπόκρισης επιχειρήσεων

Οι έρευνες που πραγματοποιήθηκαν κατά το διάστημα πριν την 25η Μαΐου 2018 στην Ελλάδα έδειξαν ότι ο βαθμός ετοιμότητας των επιχειρήσεων σχετικά με τη συμμόρφωσή τους στις διατάξεις του Κανονισμού είναι μάλλον «μέτριος». Η επόμενη ημέρα της έναρξης εφαρμογής του Κανονισμού έφερε μεγάλη αναστάτωση στις επιχειρήσεις, η οποία αποτυπώθηκε μέσω της αποστολής μηνυμάτων ηλεκτρονικού ταχυδρομείου προς τα υποκείμενα των δεδομένων, τα οποία τηρούσαν, ζητώντας τη συγκατάθεσή τους για την διατήρηση των δεδομένων και την επεξεργασία αυτών. Ακόμα όμως και οι επιχειρήσεις που δεν είχαν ολοκληρώσει τα βήματα συμμόρφωσης συνεχίζουν να λαμβάνουν τα κατάλληλα μέτρα ώστε να το πράξουν τουλάχιστον έως την ημερομηνία δημοσίευσης του εθνικού Νόμου. Προκύπτουν όμως ακόμα ερωτήματα όπως: θα αναδειχθεί η συμμόρφωση στον Κανονισμό ως μια πραγματικά δυναμική άσκηση στην πράξη, μέσω της οποίας βελτιώνεται το ίδιο το επιχειρηματικό μοντέλο; Ποια θα είναι η αντίδραση στην επιβολή των πρώτων προστίμων; Ποια θα είναι η αντίδραση στα πρώτα αιτήματα διαγραφής ή φορητότητας δεδομένων;

5. Βαθμός ανταπόκρισης υποκειμένων

Μια παράμετρος που επηρεάζει την εφαρμογή, και υπό μία έννοια την επιτυχία, του Κανονισμού στην πράξη είναι και ο τρόπος που τα υποκείμενα των δεδομένων θα ανταπεξέλθουν στο νέο πλαίσιο. Ο όγκος των πληροφοριών με τον οποίο έχουν βομβαρδιστεί και η εξειδικευμένη ορολογία του Κανονισμού έχουν οδηγήσει σε σύγχυση, τόσο ως προς τα δικαιώματα που τους παρέχονται, όσο και ως προς τις υποχρεώσεις που βαρύνουν τους υπεύθυνους επεξεργασίας και τους εκτελούντες την επεξεργασία. Είναι συνεπώς αρκετά πιθανό να δημιουργηθούν παρερμηνείες και εσφαλμένες εντυπώσεις, οδηγώντας τα υποκείμενα σε βεβιασμένες κινήσεις όπως αβάσιμες καταγγελίες κατά υπεύθυνων επεξεργασίας. Δεν αποκλείεται όμως και το ενδεχόμενο, τα υψηλά πρόστιμα που προβλέπει ο Κανονισμός, να πυροδοτήσουν μια βιομηχανία κακόβουλων καταγγελιών από όσους θελήσουν να εκμεταλλευτούν τη συγκυρία. Εύλογα επομένως οι Υπεύθυνοι Επεξεργασίας ανησυχούν: θα έρθω αντιμέτωπος με πληθώρα αιτημάτων των υποκειμένων; Θα αντιμετωπίσω κακόβουλες καταγγελίες; Θα επιδείξουν την πρέπουσα ωριμότητα τα υποκείμενα;

6. Βαθμός ανταπόκρισης φορέων δημόσιου τομέα

Όπως έχει αναφερθεί πολλές φορές στην παρούσα Μελέτη, ο Κανονισμός δεν αφορά μόνο τους ιδιωτικούς οργανισμούς, αλλά και τους δημόσιους. Έτσι, αντίστοιχα με την περίπτωση της ανταπόκρισης των επιχειρήσεων στις νέες διατάξεις, κρίσιμος είναι και ο βαθμός ανταπόκρισης των φορέων του δημόσιου τομέα. Με δεδομένο το γεγονός ότι η προετοιμασία των δημόσιων φορέων είναι ομολογουμένως βραδύτερη, καθώς δε υφίσταται σχετική εμπειρία σε κανονιστικές διατάξεις, αλλά και οι ρυθμοί ενσωμάτωσης προτύπων, διαδικασιών και ενιαίων κανόνων για το σύνολο των δημοσίων οργανισμών είναι κ των πραγμάτων εξίσου αργοί, είναι λογικό να εκφράζονται σχετικές ανησυχίες. Στο πλαίσιο αυτό, η συμμόρφωση στον Κανονισμό και η εποπτεία αυτής κινδυνεύει να εισέλθει - λανθασμένα - σε μια λογική «δύο ταχυτήτων» (άλλες απαιτήσεις για τις ιδιωτικές επιχειρήσεις και άλλες απαιτήσεις για το δημόσιο τομέα). Η έναρξη εφαρμογής του Κανονισμού πρέπει να αποτελέσει μια ευκαιρία για τους φορείς του δημοσίου, μέσω της οποίας να λάβουν ώθηση προς την κατεύθυνση της ενσωμάτωσης των ψηφιακών τεχνολογιών στην καθημερινότητά τους, στις λειτουργίες τους και κατ' επέκταση στη συναλλαγή τους με τις επιχειρήσεις, με πολλαπλά οφέλη και για τα δύο μέρη (π.χ. ταχύτητα εξυπηρέτησης, διαφάνεια, απλοποίηση διαδικασιών, εξοικονόμηση κόστους).

7. Τεχνολογικές εξελίξεις και Κανονισμός

Όπως έχει αναφερθεί, οι τεχνολογικές εξελίξεις ήταν μία από τις παραμέτρους που ανέδειξαν την αναγκαιότητα θέσπισης του Κανονισμού. Οι τεχνολογικές εξελίξεις είναι αυτές που θέτουν επίσης, προκλήσεις - ως προς την εφαρμογή - στον ίδιο τον Κανονισμό από την αρχή της ισχύος του. Πιο χαρακτηριστικό είναι το παράδειγμα της «σύγκρουσης» μεταξύ των διατάξεων του Κανονισμού για τη λήψη συγκατάθεσης (συγκέντρωση προσωπικών δεδομένων με ξεκάθαρο τον σκοπό επεξεργασίας) από τη μία πλευρά και των δυνατοτήτων που προσφέρει η μηχανική μάθηση (machine learning) και η επεξεργασία μεγάλων δεδομένων (big data) από την άλλη, όπου συχνά δεν είναι δυνατόν ο σκοπός (ή οι σκοποί) επεξεργασίας να είναι προσδιορισμένος από την αρχή (συχνά, δεν μπορούμε καν να τον φανταστούμε με τη σημερινή γνώση). Επομένως, εύλογα προκύπτουν ερωτήματα σχετικά με το πώς μπορεί να βρεθεί η ισορροπία στην πράξη, με τρόπο που να βοηθάει τόσο την τεχνολογική εξέλιξη και τα οφέλη που προκύπτουν, όσο και την προστασία των δικαιωμάτων των υποκειμένων.

7. Επίλογος και συμπεράσματα

7. Επίλογος και συμπεράσματα

Τα δεδομένα είναι το «πετρέλαιο» της 4ης βιομηχανικής επανάστασης. Σύμφωνα με εκτιμήσεις, **η αξία της αγοράς των προσωπικών δεδομένων υπολογίζεται ότι θα ανέλθει σε σχεδόν €1 τρισ. το 2020**, ενώ έως το 2025 εκτιμάται ότι ο όγκος των δεδομένων θα αυξηθεί από 16,1 ZB σε 163 ZB. Αναμενόμενα, καθώς τα ίδια τα δεδομένα και η αγορά που διαμορφώνεται γύρω από αυτά διογκώνονται, αυξάνονται εκθετικά και οι κίνδυνοι παραβίασής τους, ακόμη και σε μεγάλες επιχειρήσεις, με εξαιρετικά δυσμενείς επιπτώσεις. Ταυτόχρονα, η διαχείρισή τους με σεβασμό στην προσωπικότητα και την ιδιωτική ζωή των πολιτών, θα γίνει σταδιακά βασικό κριτήριο αξιολόγησης κάθε επιχείρησης που χειρίζεται προσωπικά δεδομένα, δηλαδή πρακτικά όλων. Επιχειρηματικοί κολοσσοί όπως η Yahoo!, η Uber και η Target, όταν ήρθαν αντιμέτωπες εσωτερικά με σοβαρές υποθέσεις παραβίασης ή διαρροής προσωπικών δεδομένων, δεν έχασαν μόνο δεδομένα αξίας εκατομμυρίων ευρώ, αλλά και μέρος του σημαντικότερου περιουσιακού στοιχείου της επιχείρησης: αυτό της καλής φήμης και της αξιοπιστίας.

Η αλυσίδα τέτοιων φαινομένων, καθώς και η ανάγκη ενιαίας ρύθμισης της αγοράς των προσωπικών δεδομένων, οδήγησαν στην αυστηροποίηση του νομικού πλαισίου πανευρωπαϊκά και στη **θέσπιση του νέου Γενικού Κανονισμού GDPR**. Με έναρξη εφαρμογής την 25η Μαΐου 2018, ο νέος Κανονισμός, αν και με ένα αρκετά αυστηρό και γραφειοκρατικό πλαίσιο, ήρθε να θωρακίσει την ιδιωτικότητα και να μεταθέσει την ευθύνη της προστασίας στην ίδια την επιχείρηση, προβλέποντας κυρώσεις ύψους έως και 4% του παγκόσμιου τζίρου για όσους αποτύχουν να συμμορφωθούν με τις απαιτήσεις του. Συνεπώς η συμμόρφωση με τις απαιτήσεις του Ευρωπαϊκού Κανονισμού παρουσιάζει ένα δίλημμα για τον επιχειρηματικό κόσμο: **θα την αντιμετωπίσουμε ως άλλη μια κανονιστική υποχρέωση - δηλαδή σαν βάρος - ή σαν μια ευκαιρία ουσιαστικής και εκ βαθών αλλαγής του επιχειρηματικού μοντέλου και εισαγωγής των ελληνικών επιχειρήσεων στον κόσμο της ψηφιακής οικονομίας;**

Παρότι η συμμόρφωση φαίνεται να συνεπάγεται υψηλά κόστη και βαριές διαδικασίες, οι ειδικοί του χώρου επιμένουν: Εκείνος που θα μετατρέψει την κουλτούρα σεβασμού και προστασίας των προσωπικών δεδομένων σε πυρήνα της καθημερινής του λειτουργίας, θα αποκτήσει αυτόματα ένα «ανταγωνιστικό πλεονέκτημα». Γιατί θα είναι εκείνος που θα είναι διαρκώς σε θέση να αποδείξει στον καταναλωτή, τον πελάτη, τον εργαζόμενο, όχι μόνο ότι έχει λάβει τα απαραίτητα μέτρα προστασίας των

προσωπικών δεδομένων τους, αλλά και ότι είναι διαρκώς σε θέση να τα διατηρεί προστατευμένα.

Στην παρούσα Μελέτη επικεντρωθήκαμε σε δύο κυρίως ζητήματα: α) στην **παρουσίαση των βασικών σημείων** του Κανονισμού με τρόπο απλό και κατανοητό και β) στην **καθοδήγηση των επιχειρήσεων σχετικά με τον τρόπο επίτευξης της «έξυπνης» συμμόρφωσης**, δηλαδή της αξιοποίησης των ευκαιριών που παρουσιάζονται από τον Κανονισμό.

Συνοψίζοντας, θα θέλαμε να σημειώσουμε ότι τα κύρια σημεία του Κανονισμού που διαφαίνεται να δυσκολεύουν τις επιχειρήσεις στην πορεία συμμόρφωσης, στη δεδομένη χρονική στιγμή (δηλαδή τους πρώτους μήνες συμμόρφωσης) είναι: α) οι υποχρεώσεις γύρω από τον ΥΠΔ (κυρίως ποιο είναι το σωστό πρόσωπο και πώς θα ασκήσει τα καθήκοντά του στην πράξη), β) τα ζητήματα σχετικά με την εκπόνηση Εκτίμησης Αντικτύπου, γ) η ετοιμότητα για τη διαχείριση των περιπτώσεων παραβίασης των δεδομένων, δ) ο χειρισμός του δικαιώματος στη λήθη, ε) ο τρόπος εξασφάλισης της συγκατάθεσης, ζ) ο χειρισμός των αιτημάτων περί φορητότητας δεδομένων και η) οι όροι των συμβάσεων με τρίτα μέρη. Είναι κατανοητό ότι όσο οι επιχειρήσεις, αλλά και τα υποκείμενα προσωπικών δεδομένων, εξοικειώνονται με τις υποχρεώσεις και τις απαιτήσεις του Κανονισμού, τόσο τα πεδία που σήμερα φαίνονται να προβληματίζουν θα εξαλείφονται ή θα αντικαθίστανται από άλλα.

Όσον αφορά στη διαδικασία συμμόρφωσης, παρουσιάσαμε πώς, με την τεχνολογία πολύτιμο συμπαραστάτη, και ακολουθώντας τα 10 + 1 βήματα για έξυπνη συμμόρφωση που ο ΣΕΒ προτείνει, είναι εφικτή η υιοθέτηση λύσεων προσαρμοσμένων στις ανάγκες και τις ιδιαιτερότητες κάθε οργανισμού. Το «νοικοκύρεμα» των προσωπικών δεδομένων, η μετατροπή της υποχρέωσης συμμόρφωσης σε ανταγωνιστικό πλεονέκτημα και η επένδυση σε λύσεις που προσφέρει η τεχνολογία και, μέσω αυτής της διαδικασίας, η είσοδος στην εποχή της ψηφιακής οικονομίας, αποτελούν τις βασικές αρχές που θα πρέπει να διέπουν κάθε οργανισμό.

Εν κατακλείδι, είναι σημαντικό οι επιχειρήσεις να κατανοήσουν ότι η διαδικασία συμμόρφωσης με τον Κανονισμό αφενός επιφέρει οφέλη στη λειτουργία τους, σε επίπεδο φήμης και αναδιοργάνωσης και αφετέρου ότι πρόκειται για ένα ταξίδι που δεν τελείωσε με την παρέλευση της 25ης Μαΐου, ούτε με την ολοκλήρωση των ενεργειών συμμόρφωσης. Αντιθέτως, είναι ένα συνεχές ταξίδι συμμόρφωσης που μπορεί να αναδειχθεί σε ταξίδι επιχειρηματικής επιτυχίας.

Βιβλιογραφία και πηγές

Βιβλιογραφία και πηγές

Βιβλία, έρευνες και αρθρογραφία

- Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, Ετήσια Έκθεση 2016, 2016.
- Βαρβέρης Α., Τεχνικά και οργανωτικά θέματα - η «υποχρεωτική» τοποθέτηση Υπεύθυνου Προστασίας Δεδομένων, ΕφημΔΔ 2017, 206 επ.
- Γιαννόπουλος Γ., Γενικός Κανονισμός Προστασίας Δεδομένων: οι νέες υποχρεώσεις και η ευθύνη του Υπεύθυνου Επεξεργασίας, ΕφημΔΔ 2017, 199 επ.
- Δελλής Γ., Για μια αποτελεσματική δημόσια προστασία των προσωπικών δεδομένων: ο «θαυμαστός καινούργιος κόσμος» του Κανονισμού (ΕΕ) 679/2016, ΕφημΔΔ 2017, 2 επ.
- Ιγγλεζάκης Ι., Ζητήματα εναρμόνισης της νομοθεσίας για την προστασία προσωπικών δεδομένων στην ΕΕ, ΔιΜΕΕ 2012, 314.
- Κόμνιος Κ., Οι γενικοί όροι επιβολής διοικητικών προστίμων κατά τον Γενικό Κανονισμό για την Προστασία Δεδομένων: Συμβολή στην ερμηνεία του άρθρου 83 του Γενικού Κανονισμού για την Προστασία Δεδομένων, ΔιΜΕΕ 2017, 502 επ.
- Λουκάς Ν., Η Έννοια και η Διαχείριση του «Κινδύνου» στον Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR), ΔιΜΕΕ 2017, 544 επ.
- Λωσταράκου Κ., Ο νέος Κανονισμός της Ευρωπαϊκής Ένωσης για την Προστασία των προσωπικών Δεδομένων. Οικονομικές επιπτώσεις στις επιχειρήσεις-ειδικές υποχρεώσεις για τους παρόχους υπολογιστικού νέφους, ΔιΜΕΕ 2013, 353.
- Μήτρου Λ., Privacy by Design- η τεχνολογική διάσταση της προστασίας προσωπικών δεδομένων, ΔιΜΕΕ 2013, 14 επ.
- Τάσσης Σπ., Επεξεργασία δεδομένων - Ευθύνη διαχειριστή σελίδας και Facebook ΔΕΕ υπόθ. C-210/2016, απόφ. της 5.6.2018, ΔιΜΕΕ 2018.
- Τάσσης Σπ., Η ιδιωτικότητα ως πεδίο εμπορικής διαμάχης ΕΕ και ΗΠΑ, ΔιΜΕΕ 2013, 1 επ.
- Ομάδα Εργασίας άρθρου 29, «Κατευθυντήριες γραμμές για την εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων και καθορισμός του κατά πόσον η επεξεργασία «ενδέχεται να επιφέρει υψηλό κίνδυνο» για τους σκοπούς του Κανονισμού 2016/679», Οκτώβριος 2017.
- Ομάδα Εργασίας άρθρου 29, «Κατευθυντήριες γραμμές για την εφαρμογή και τον καθορισμό διοικητικών προστίμων για τους σκοπούς του κανονισμού 2016/679», Οκτώβριος 2017.

- Ομάδα Εργασίας άρθρου 29, «Κατευθυντήριες γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων», Απρίλιος 2017.
- Ομάδα Εργασίας άρθρου 29, «Κατευθυντήριες γραμμές για τον προσδιορισμό της επικεφαλής εποπτικής αρχής των υπευθύνων επεξεργασίας ή των εκτελούντων την επεξεργασία», Απρίλιος 2017.
- Ομάδα Εργασίας άρθρου 29, «Κατευθυντήριες γραμμές σχετικά με το δικαίωμα στη φορητότητα των δεδομένων», Απρίλιος 2017.
- Παναγοπούλου-Κουτνατζή Φ., Τα νέα δικαιώματα για τους πολίτες βάσει του Γενικού κανονισμού προστασίας δεδομένων: μια πρώτη αποτίμηση και συνταγματική αξιολόγηση, ΕφημΔΔ 2017, 81 επ.
- Παναγοπούλου-Κουτνατζή Φ., Το δικαίωμα στη λήθη στην εποχή της αβάσταχτης μνήμης: Σκέψεις αναφορικά με την Πρόταση Κανονισμού Προστασίας Δεδομένων, ΕφημΔΔ 2012, 264 επ.
- Παναγοπούλου-Κουτνατζή Φ., Ο Γενικός Κανονισμός για την Προστασία Δεδομένων 679/2016/ΕΕ. Εισαγωγή και Προστασία Δικαιωμάτων, Εκδόσεις Σάκκουλα, 2017.
- Περράκη Π., Ο νέος Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων και η εργασιακή σχέση, ΔΕΕ 2016, 323 επ.
- ΣΕΒ, Special Report «Ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR): ευκαιρίες και προκλήσεις για τις επιχειρήσεις στην εποχή της ψηφιοποίησης», Μάρτιος 2018.
- ΣΕΒ, Special Report «Το στρατηγικό σχέδιο του ΣΕΒ για μια ψηφιακά ανεπτυγμένη Ελλάδα», Μάιος 2017.
- ΣΕΒ, Εργαστήριο Διαβούλευσης «Ευκαιρίες και προκλήσεις από την εφαρμογή του νέου Κανονισμού για τα προσωπικά δεδομένα (GDPR)», Φεβρουάριος 2018.
- ΣΕΒ, Έρευνα για το βαθμό ετοιμότητας των επιχειρήσεων για τη συμμόρφωση με τον Κανονισμό, Φεβρουάριος 2018.
- ΣΕΒ, Ομάδα Εργασίας για τα Προσωπικά Δεδομένα, Απρίλιο-Ιούνιος 2018.
- Τιντζογλίδου Ν., Εισήγηση «Οι ενέργειες του νομικού συμβούλου για τη συμμόρφωση των επιχειρήσεων με τον Κανονισμό GDPR», 2ο ετήσιο συνέδριο E-themis «Προσωπικά δεδομένα και δικηγορία-Μια νέα πραγματικότητα, ένα νέο κεφάλαιο στο νομικό κόσμο», 11-12 Μαΐου 2018.

- Baker McKenzie, "GDPR National Legislation Survey, 0.3", May 2018.
- CISCO, "Privacy Maturity Benchmark Study", 2018
- Commission Nationale de l'Informatique et des Libertés (CNIL), “Privacy Impact Assessment: methodology”, February 2018
- Commission Nationale de l'Informatique et des Libertés (CNIL), “Privacy Impact Assessment: knowledge bases”, February 2018
- Commission Nationale de l'Informatique et des Libertés (CNIL), “Privacy Impact Assessment: application to IoT devices”, February 2018
- European Commission, “Fact Sheet - Questions and Answers-General Data Protection Regulation”, January 2018.
- European Commission, “Special Eurobarometer 431 - Data Protection”, June 2015.
- European Data Protection Board (EDPB), “Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679”, May 2018.
- European Data Protection Board (EDPB), “Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679”, May 2018.
- European Union Agency for Fundamental Rights and Council of Europe, “Handbook on European data protection law”, 2018.
- IAPP-EY, "Annual Privacy Governance Report", 2017.
- ICAP Management Consultants, “GDPR survey”, January 2018.
- IDC, “Data Age 2025: The Evolution of Data to Life-Critical”, April 2017.
- SAS, "Working toward GDPR compliance - Insights from a SAS survey and an end-to-end approach", 2017.
- Tassis Spiros and Margarita Peristeraki, The Extraterritorial Scope of the “Right to Be Forgotten” and the Rights and Obligations of Search Engine Operators Located Outside the EU, European Networks Law and Regulation 3/2014, Lexxion Verlagsgesellschaft mbH.
- Working Group Article 29, “Guidelines on Personal data breach notification under Regulation 2016/679”, February 2018.
- Working Group Article 29, “Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679”, February 2018.
- Working Group Article 29, “Guidelines on Consent under Regulation 2016/679”, November 2017.
- Working Group Article 29, “Guidelines on Transparency under Regulation 2016/679”, 2017.

Ιστοσελίδες

- https://www.cnil.fr
- https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html
- http://www.dataprotection.gov.cy
- http://www.dpa.gr/
- http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358
- http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612080
- https://edpb.europa.eu/
- https://edps.europa.eu/
- https://eur-lex.europa.eu/homepage.html
- https://iapp.org/
- https://www.lawspot.gr/
- https://www.techworld.com/security/uks-most-infamous-data-breaches-3604586/

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Αθήνα, Οκτώβριος 2018