ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ -
ΤΕΧΝΟΛΟΓΙΕΣ ΚΑΙ ΔΙΟΙΚΗΣΗ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

GDPR implications for the banking sector- a case study

(Οι επιπτώσεις του Γενικού Κανονισμού Προστασίας Δεδομένων στον Τραπεζικό Τομέα: Μελέτη Περίπτωσης)

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Ιωάννης Χρ. Κυπραίος
ΑΜ: 323 2016007

Επιβλέπων Καθηγητής : Σπ. Κοκολάκης

Μέλη εξεταστικής επιτροπής: Σπ. Κοκολάκης, Μ. Καρύδα, Π. Ριζομυλιώτης

Σάμος, Ιανουάριος 2018

Η σελίδα αυτή είναι σκόπιμα λευκή.

Πρόλογος και ευχαριστίες

Η ραγδαία εξέλιξη της τεχνολογίας, η δυνατότητα αποθήκευσης τεράστιου όγκου δεδομένων σε πολύ χαμηλό κόστος και η τεχνολογική δυνατότητα για ανάλυση αυτών των δεδομένων (δομημένων και μη) καθώς και η συσχέτιση τους με άλλες πηγές, όπως το διαδίκτυο, σε πολύ μικρό χρόνο, καθιστά την ιδιωτική ζωή και τα προσωπικά δεδομένα περισσότερο ευάλωτα από ποτέ.

Οι Τράπεζες ανήκουν στα Νομικά Πρόσωπα Ιδιωτικού Δικαίου που η φύση των εργασιών τους επιβάλλει την επεξεργασία μεγάλου όγκου προσωπικής πληροφορίας σχετικά με τους πελάτες τους. Για παράδειγμα υπάρχουν νομικές και κανονιστικές απαιτήσεις που επιβάλλουν τη διατήρηση ημερολογίου για τις εγχρήματες συναλλαγές έως και 20 χρόνια για κάθε πελάτη. Η χρήση λογισμικού "Know Your Customer-KYC" (Γνώρισε τον Πελάτη σου) επιβάλλεται κανονιστικά για την αποτροπή ξεπλύματος χρήματος (Anti-Money Laundering – AML) από παράνομες δραστηριότητες μέσω του Τραπεζικού συστήματος. Αντίστοιχες υποχρεώσεις υπάρχουν για την εναρμόνιση με τους κανονισμούς φορολογικής συμμόρφωσης και τη παροχή πληροφοριών στις αρμόδιες κρατικές υπηρεσίες.

Η νέα οδηγία της Ευρωπαϊκής Ένωσης[1] για τις υπηρεσίες πληρωμών και οι εξελίξεις στον τρόπο που θα γίνονται οι συναλλαγές των φυσικών προσώπων, τόσο με τις τράπεζες όσο και μεταξύ τους, θα είναι ραγδαίες και θα αλλάξει δραματικά τη φύση των Τραπεζών όπως τις γνωρίζουμε σήμερα, μετατρέποντας τες σε θεματοφύλακες των πληροφοριών που αφορούν τα φυσικά πρόσωπα.

Η παρούσα εργασία πραγματεύεται την εφαρμογή του νέου Γενικού Κανονισμού Προστασίας Δεδομένων στον Τραπεζικό Τομέα. Οι Τράπεζες, αντιμέτωπες με βαριά πρόστιμα σε περίπτωση μη συμμόρφωσης με τον Κανονισμό ή ακόμη χειρότερα σε περίπτωση παραβίασης των δεδομένων των πελατών τους, καλούνται να πάρουν μια σειρά από οργανωτικά και τεχνολογικά μέτρα προκειμένου να αποτρέψουν οποιαδήποτε βλάβη σε προσωπικά δεδομένα και να μπορούν να αποδείξουν τη συμμόρφωση τους με τον Κανονισμό. Η ανάλυση των σχετικών άρθρων του Γενικού Κανονισμού Προστασίας Δεδομένων, οι επιπτώσεις τους στην Τράπεζες και η μελέτη περίπτωσης που αφορά την προετοιμασία μιας μεγάλης Ελληνικής Τράπεζας για συμμόρφωση με τον Κανονισμό, αποτελούν το αντικείμενο της παρούσας εργασίας.

Θα ήθελα να ευχαριστήσω θερμά τον καθηγητή μου κύριο Σπύρο Κοκολάκη, για την ανεκτίμητη βοήθεια, την καθοδήγηση και την διαρκή συμπαράσταση του στην εκπόνηση της παρούσας εργασίας.

Γιάννης Κυπραίος

[1] PSD2 – Payment Services Directive 2

Πίνακας περιεχομένων

Περίληψη

Ο σκοπός της παρούσας διπλωματικής εργασίας είναι η μελέτη για τις «Επιπτώσεις του Γενικού Κανονισμού Προστασίας Δεδομένων στον Τραπεζικό Τομέα».

Οι Τράπεζες οφείλουν να λάβουν τα κατάλληλα οργανωτικά και τεχνικά μέτρα για την προστασία των δεδομένων των φυσικών προσώπων είτε αυτά είναι πελάτες, υπάλληλοι ή συνεργάτες. Παράλληλα όμως οι Τράπεζες οφείλουν να συμμορφώνονται με τις υπόλοιπες κανονιστικές και νομικές απαιτήσεις που αφορούν το ξέπλυμα χρήματος από παράνομες δραστηριότητες ή την δυνατότητα να παρουσιάσουν στοιχεία – όταν αυτά ζητηθούν από τις αρμόδιες κρατικές αρχές- που αφορούν τη συναλλακτική δραστηριότητα των πελατών τους.

Για το σκοπό αυτό αναλύονται τα κύρια άρθρα του Κανονισμού, συμπεριλαμβανομένων των κατευθυντηρίων γραμμών και των γνωμοδοτήσεων της Ομάδας Εργασίας του Άρθρου 29. Κύριες πηγές για την ανάλυση των άρθρων, πέραν του Κανονισμού όπου τα άρθρα αναλύονται διεξοδικά, είναι και οι αναλύσεις από μερικές από τις μεγαλύτερες και πλέον γνωστές σε παγκόσμιο επίπεδο εταιρείες συμβούλων και αναλυτών όπως οι EY, KPMG, Deloitte, Pricewaterhouse Coopers (PWC), Accenture, Oliver Wyman, Gartner, Forrester κλπ.

Αναλύεται η σχέση του Γενικού Κανονισμού Προστασίας Δεδομένων με τη νέα Οδηγία Εξυπηρέτησης Πληρωμών της Ευρωπαϊκής Ένωσης καθώς και οι δύο μπαίνουν σε εφαρμογή, με 4 μήνες διαφορά, το πρώτο εξάμηνο του 2018. Αναλύονται οι κίνδυνοι σε ότι αφορά την προστασία των προσωπικών δεδομένων των πελατών των Τραπεζών, αλλά και οι ευκαιρίες που δημιουργούνται για να κυριαρχήσουν στην αγορά όσοι καταφέρουν να προσαρμοστούν έγκαιρα στο νέο πλαίσιο. Η εκτίμηση είναι ότι το αμέσως επόμενο χρονικό διάστημα θα βιώσουμε μεγάλες αλλαγές στον τρόπο που πραγματοποιούνται οι τραπεζικές συναλλαγές, σε σύγκριση με ότι ξέρουμε έως σήμερα.

Τέλος ακολουθεί η μελέτη περίπτωσης για τις επιπτώσεις του κανονισμού και τη διαδικασία συμμόρφωσης με αυτόν μιας συστημικής Ελληνικής Τράπεζας. Περιγράφονται και αναλύονται σε υψηλό επίπεδο τα βήματα που ακολουθεί η Τράπεζα προκειμένου να εντοπίσει τις αποκλίσεις συμμόρφωσης και να προβεί σε διορθωτικές/βελτιωτικές ενέργειες.

Η συμμόρφωση με τον Κανονισμό δεν είναι ένα έργο με ημερομηνία λήξης. Είναι μια συνεχής διαδικασία που θα κρατήσει τουλάχιστον για όσο διάστημα είναι ο Κανονισμός σε ισχύ.

Abstract

The purpose of this diploma thesis is to study the "Implications of the General Data Protection Regulation in the Banking Sector".

Banks are required to take appropriate organizational and technical measures to protect the data of individuals whether they are customers, employees or partners. At the same time, however, the Banks have to comply with other regulatory and legal requirements relating to money laundering or the possibility of presenting evidence - when requested by the competent governmental authorities - about the transactional activity of their clients.

To this end, the main articles of the Regulation, including the Article 29 Working Group's Guidelines and Opinions, are analyzed. The main sources for analyzing the articles, apart from the Regulation where the articles are analyzed in detail, are also the various published articles of some of the largest and most renowned global consultants and analysts such as EY, KPMG, Deloitte, Pricewaterhouse Coopers (PWC), Accenture, Oliver Wyman, Gartner, Forrester and others.

The relation between the General Data Protection Regulation and the new Payment Services Directive of the European Union is analyzed as both are implemented with a 4-month difference in the first semester of 2018. The risks generated regarding the protection of the personal data of Bank customers, but also the opportunities created to dominate the market for those who manage to adapt early to the new context. The estimate is that we will experience major changes in the way banking transactions are made compared to what we know about them until to date.

Finally, a case study on the impact of the Regulation and the compliance process with one of the most important Hellenic Bank follows. The steps taken by the Bank are described and analyzed at a high level in order to identify compliance deviations and make corrective / improvement actions.

Compliance with the Regulation is not a project with a maturity date. It is a continuous process that will last at least for as long as the Regulation is in force.

1

Εισαγωγή

1.1 Οι επιπτώσεις του Γενικού Κανονισμού Προστασίας Δεδομένων στον Τραπεζικό Τομέα

Ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ) 679/2016, μετά από τέσσερα χρόνια και 4.000 περίπου τροποποιήσεις που έγιναν πριν την έγκριση του, αντικαθιστά την οδηγία 95/46/ΕΚ για την προστασία των προσωπικών δεδομένων στην Ευρωπαϊκή Ένωση. Ο ΓΚΠΔ γίνεται άμεσα εφαρμοστέος σε ολόκληρη την Ευρωπαϊκή Ένωση στις 25 Μαΐου του 2018. Εισάγει ένα νέο πανευρωπαϊκό σύνολο κανόνων και θεωρείται ορόσημο στην προστασία των προσωπικών δεδομένων. Εναρμονίζει σε μεγάλο βαθμό τους εθνικούς νόμους των κρατών–μελών για την προστασία των δεδομένων που ισχύουν σε όλα τα κράτη μέλη της ΕΕ. Λόγω του ευρύτερου γεωγραφικού του πεδίου, ο ΓΚΠΔ θα έχει αντίκτυπο σε πολλές επιχειρήσεις εντός και εκτός της ΕΕ εφόσον τα δεδομένα αφορούν φυσικά πρόσωπα εντός της Ευρωπαϊκής Ένωσης.

Οι χρηματοπιστωτικοί οργανισμοί, όπως οι τράπεζες, επεξεργάζονται καθημερινά μεγάλο όγκο προσωπικών δεδομένων. Ως αποτέλεσμα του ΓΚΠΔ, οι τράπεζες οι οποίες λειτουργούν ήδη σε ένα πολύπλοκο ρυθμιστικά περιβάλλον, θα υπόκεινται σε νέους κινδύνους με νομικές επιπτώσεις και βαριά πρόστιμα τα οποία μπορεί να ανέλθουν σε 20 εκατομμύρια ευρώ ή στο 4% του ετήσιου κύκλου εργασιών. Για τις τράπεζες η ζημιά μπορεί να είναι ανεπανόρθωτη καθώς η λειτουργία τους βασίζεται στην εμπιστοσύνη των πελατών τους. Η φήμη αποτελεί ίσως το σημαντικότερο περιουσιακό τους στοιχείο και πρέπει να προστατευθεί. Ο ανταγωνισμός είναι ακόμη δυσκολότερος καθώς στην τραπεζική αγορά εισέρχονται οι fintech εταιρείες, με διαφορετικό – πιο «χαλαρό» – ρυθμιστικό καθεστώς και κανονιστικό πλαίσιο. Η ευθύνη για την

προστασία των προσωπικών δεδομένων των πελατών τους εξακολουθεί να βαρύνει τις τράπεζες. (Roland Wollf, 2017).

Οι αλλαγές που φέρνει ο ΓΚΠΔ στις εταιρείες του χρηματοπιστωτικού τομέα και ιδιαίτερα στις τράπεζες είναι:

- Οργανωτικές: Διορισμός Υπευθύνου για την Προστασία των Δεδομένων, αλλαγές και εμπλουτισμός της διακυβέρνησης των δεδομένων, νέες πολιτικές ή βελτιώσεις στις υφιστάμενες, εμπλουτισμός του κώδικα δεοντολογίας.
- Στην επεξεργασία: Απαιτείται σύστημα διαχείρισης για τη συναίνεση, δυνατότητα διόρθωσης των δεδομένων μετά από παρέμβαση του υποκειμένου, ασφαλής διαγραφή και δυνατότητα φορητότητας των δεδομένων.
- Στις τεχνολογίες: Αναγνώριση και κατάλογος περιοχών που έχουν προσωπικά δεδομένα, κρυπτογράφηση ή ψευδωνυμοποίηση, σύστημα διαχείρισης για τα metadata είναι μερικές από τις τεχνολογίες που θα εμπλακούν για την εφαρμογή του ΓΚΠΔ.

1.2 Αντικείμενο διπλωματικής

Σκοπός της παρούσας εργασίας είναι, καταρχήν, η παρουσίαση και, στη συνέχεια, η επισήμανση των άρθρων του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ) που κρίνεται πως επηρεάζουν σημαντικά τα προσωπικά δεδομένα που διαχειρίζεται ο τραπεζικός τομέας.

Στη συνέχεια θα δοθεί ιδιαίτερη έμφαση σε ειδικά θέματα του Κανονισμού για τα οποία έχει εκδώσει συγκεκριμένες κατευθυντήριες γραμμές και διευκρινήσεις η Ομάδα Εργασίας του Άρθρου 29 (Working Party 29 – WP29, στην παρούσα εργασία θα αναφέρεται ως ΟΕ29). Οι συγκεκριμένες κατευθυντήριες γραμμές έχουν άμεση εφαρμογή στη συμμόρφωση των τραπεζών με τον νέο Κανονισμό.

Η χαρτογράφηση της ροής των δεδομένων είναι βασική προϋπόθεση για να γνωρίζουμε τη διαδρομή των δεδομένων, να μπορούμε να καταλάβουμε που μπορεί να ανιχνευθούν αδυναμίες και να προχωρήσουμε στη λήψη των κατάλληλων μέτρων.

Η Οδηγία της Ευρωπαϊκής Ένωσης για τις Υπηρεσίες Πληρωμών, δημιουργεί μια επιπλέον πρόκληση για τις τράπεζες. Το σίγουρο είναι ότι με ραγδαίους ρυθμούς θα αλλάξει η τραπεζική δραστηριότητα όπως τη γνωρίζουμε σήμερα. Ποιος θα είναι ο ρόλος των τραπεζών και πως αυτό αφορά τον ΓΚΠΔ και τις επιπτώσεις του στον τραπεζικό τομέα, αποτελεί ένα από τα ερωτήματα που η παρούσα εργασία θα προσπαθήσει να απαντήσει.

Τέλος θα ακολουθήσει η μελέτη περίπτωσης της Εθνικής Τράπεζας. Θα παρουσιασθούν σε υψηλό επίπεδο όλα τα βήματα που ακολούθησε (και ακολουθεί η Τράπεζα καθώς η διαδικασία είναι σε εξέλιξη) για τη συμμόρφωση με τον ΓΚΠΔ. Καθώς κάποια από τα παραδοτέα εμπίπτουν στα πνευματικά δικαιώματα και ιδιοκτησία της συμβουλευτικής εταιρείας της Τράπεζας για το συγκεκριμένο έργο, θα χρησιμοποιηθούν αντίστοιχα υποδείγματα από το διαδίκτυο τα οποία όμως συμπίπτουν με τα πραγματικά, σε ποσοστό μεγαλύτερο του 95%.

1.3 Δομή της διπλωματικής

Η εργασία χωρίζεται σε 3 λογικές ενότητες.

Η πρώτη ενότητα (Κεφ. 2- Κεφ. 7) παρουσιάζει τα άρθρα του ΓΚΠΔ και τις κατευθυντήριες γραμμές της Ομάδας Εργασίας 29 (ΟΕ29) που αποτελούν το πλαίσιο στο οποίο πρέπει να κινηθούν οι επιχειρήσεις που διαχειρίζονται μεγάλο όγκο προσωπικών δεδομένων όπως οι Τράπεζες. Συγκεκριμένα τα κύρια άρθρα του ΓΚΠΔ αναφέρονται στο Κεφάλαιο 2. Στο Κεφάλαιο 3 παρουσιάζονται οι κατευθυντήριες γραμμές της ΟΕ29 για τη διενέργεια Εκτίμησης Αντικτύπου στην Προστασία Δεδομένων. Οι κατευθυντήριες γραμμές για την Αναγγελία Παραβιάσεων στην Αρχή παρουσιάζονται στο Κεφάλαιο 4. Το Κεφάλαιο 5 αναλύει την γνωμοδότηση της ΟΕ29 για τα προσωπικά δεδομένα των εργαζομένων. Τα θέματα με τη δημιουργία προφίλ αναπτύσσονται στο Κεφάλαιο 6 και στο Κεφάλαιο 7 οι κατευθυντήριες γραμμές της ΟΕ29 για θέματα που σχετίζονται με τον Υπεύθυνο Προστασίας Δεδομένων (ΥΠΔ).

Η δεύτερη ενότητα (κεφ. 8 – κεφ. 10) αναλύει θέματα που αφορούν τον Τραπεζικό Τομέα. Το Κεφάλαιο 8 μελετά τις οργανωτικές επιπτώσεις του ΓΚΠΔ στον Τραπεζικό Τομέα. Τα βασικά θέματα για τη δημιουργία διαγράμματος ροής των δεδομένων αναπτύσσονται στο Κεφάλαιο 9 και το Κεφάλαιο 10 αναπτύσσει την ενδιαφέρουσα σχέση που δημιουργεί ο ΓΚΠΔ με την νέα Οδηγία της Ευρωπαϊκής Ένωσης για τις Υπηρεσίες Πληρωμών.

Η τρίτη ενότητα αποτελείται από τη μελέτη περίπτωσης στην Εθνική Τράπεζα που αναπτύσσεται στο Κεφάλαιο 11.

Με τα συμπεράσματα στο Κεφάλαιο 12 και τις αναφορές στο Κεφάλαιο 13 ολοκληρώνεται η εργασία.

2

Μία σύντομη επισκόπηση του ΓΚΠΔ

2.1 Ιστορικό

Ο Γενικός Κανονισμός για την Προστασία Δεδομένων (ΓΚΠΔ) 2016/679 δημοσιεύθηκε στην Εφημερίδα της Ευρωπαϊκής Ένωσης τον Μάιο του 2016 και θα τεθεί σε εφαρμογή στις 25 Μαΐου του 2018. Αντικαθιστά την Οδηγία 95/46/ΕΚ η οποία στην Ελλάδα είχε νομοθετηθεί με το νόμο 2472/1997 για την «Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα». Σε εθνικό επίπεδο δεν υπάρχει δυνατότητα σημαντικών διαφοροποιήσεων από τον ΓΚΠΔ. Σε αντίθεση με τις οδηγίες (Directives) για τους κανονισμούς (Regulations) δεν απαιτείται νομοθετική παρέμβαση σε εθνικό επίπεδο. Από τις 25 Μαΐου είναι σε πλήρη εφαρμογή (Ευρωπαϊκό Κοινοβούλιο, 2016).

Η διαδικασία για την εναρμόνιση με τον ΓΚΠΔ είναι συνεχής και χωρίς λήξη, για όσο διάστημα θα είναι σε ισχύ ο Κανονισμός. Οι εταιρείες υπόκεινται στον ΓΚΠΔ, στον βαθμό που επεξεργάζονται προσωπικά δεδομένα πολιτών στην Ευρωπαϊκή Ένωση για τα αγαθά και τις υπηρεσίες που τους παρέχουν. Σε κάποιες περιπτώσεις, αλλάζει σε σημαντικό βαθμό ο τρόπος λειτουργίας των επιχειρήσεων.

Ο Κανονισμός αποτελείται από:

- Τον Κανονισμό με τους γενικούς κανόνες για την προστασία των προσωπικών δεδομένων
- Την Οδηγία για την επεξεργασία δεδομένων προσωπικού χαρακτήρα για δικαστικούς σκοπούς και σκοπούς πρόληψης παραβατικών συμπεριφορών.

Οι μεταβολές οι οποίες απορρέουν από την εφαρμογή του Κανονισμού, περιλαμβάνουν μεταξύ άλλων σημαντικές τροποποιήσεις στον τρόπο επεξεργασίας δεδομένων προσωπικού

χαρακτήρα. Επίσης, οι σημαντικές επιπτώσεις που επηρεάζουν τη συμμόρφωση με τους κανονισμούς προστασίας δεδομένων, δημιουργούν την ανάγκη για αναπροσαρμογή του εταιρικού πλαισίου προστασίας δεδομένων των εταιρειών.

Η υλοποίηση των απαιτήσεων του Κανονισμού προϋποθέτει την εφαρμογή μιας ολιστικής προσέγγισης με σκοπό την προστασία των προσωπικών δεδομένων. Επίσης, απαιτείται η υλοποίηση και εφαρμογή ισχυρού πλαισίου που θα αντιμετωπίζει αποτελεσματικά τα όποια ζητήματα προκύπτουν αναφορικά με την επεξεργασία προσωπικών δεδομένων.

Υπάρχουν πέντε σημαντικές τομές αναφορικά με την προστασία προσωπικών δεδομένων που αντικατοπτρίζονται στον Κανονισμό:

- Ευαισθητοποίηση σε σχέση με την προστασία προσωπικών δεδομένων φυσικών προσώπων.
- Ενίσχυση ατομικού ελέγχου.
- Έγκαιρη αντιμετώπιση των παραβιάσεων των δεδομένων.
- Εναρμόνιση και εφαρμογή σε όλους τους οργανισμούς που επεξεργάζονται δεδομένα κατοίκων της Ευρωπαϊκής Ένωσης.
- Ενίσχυση αρμοδιοτήτων των τοπικών Αρχών Προστασίας Προσωπικών Δεδομένων ως προς τη συμμόρφωση των οργανισμών.

2.2 Ορισμοί

Υπεύθυνος της Επεξεργασίας ΥΕ (Controller)

- Εκείνος που καθορίζει τον σκοπό της επεξεργασίας.

Εκτελών την Επεξεργασία ΕΕ (Processor)

- Εκτελεί επεξεργασία για λογαριασμό του Υπεύθυνου.

Ο Εκτελών μπορεί να μετατραπεί σε Υπεύθυνο, εφόσον χρησιμοποιήσει τα δεδομένα που επεξεργάζεται για λογαριασμό του Υπεύθυνου, για δικούς του σκοπούς, άρα θα φέρει πλέον και την ευθύνη (π.χ. μητρική που φυλάει τα δεδομένα της θυγατρικής της).

Οι βασικές κατηγορίες δεδομένων που επεξεργάζονται οι εταιρείες διακρίνονται σε:

- Απλά δεδομένα προσωπικού χαρακτήρα (ΔΠΧ).
- Ειδικές κατηγορίες δεδομένων (πρώην ευαίσθητα).

Δεδομένα προσωπικού χαρακτήρα (ΔΠΧ)

- Κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο (υποκείμενο των δεδομένων), η ταυτότητα του οποίου μπορεί να εξακριβωθεί άμεσα ή έμμεσα ιδίως μέσω αναφοράς σε αναγνωριστικό ταυτότητας (π.χ. όνομα), σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό (online) αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσδιορίζουν τη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου.

- Το εύρος των δεδομένων είναι πολύ μεγάλο και περιλαμβάνει πλέον κάθε αναγνωριστικό (όνομα και αριθμό ταυτότητας, δεδομένα θέσης, διεύθυνση IP, αναγνωριστικά συσκευών, φωτογραφίες, βίντεο, στοιχεία σωματικής, γενετικής, ψυχολογικής, οικονομικής, πολιτιστικής ή κοινωνικής ταυτότητας κ.λπ.).
- Ανεξαρτήτως της μορφής (ηλεκτρονικά ή έντυπα).

Ειδικές κατηγορίες δεδομένων (πρώην ευαίσθητα)

- Φυλετική ή εθνοτική καταγωγή.
- Πολιτικά φρονήματα.
- Θρησκευτικές ή φιλοσοφικές πεποιθήσεις.
- Συμμετοχή σε συνδικαλιστική οργάνωση.
- Γενετικά ή βιομετρικά δεδομένα.
- Δεδομένα υγείας.
- Δεδομένα σεξουαλικής ζωής ή γενετήσιου προσανατολισμού.

Ο διαχωρισμός των δεδομένων ενώ φαίνεται σαφής, δεν είναι. Ένα απλό δεδομένο μπορεί να μετατραπεί, εξαιτίας της χρήσης του από τον Υπεύθυνο Επεξεργασίας (ΥΕ), σε ευαίσθητο. Ο σκοπός συλλογής και ο τρόπος χρήσης είναι καθοριστικής σημασίας για τον αν μια πληροφορία είναι απλή ή ευαίσθητη και για το αν ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των υποκειμένων.

Για παράδειγμα τα βιβλία που αγοράζει ένα υποκείμενο από ένα βιβλιοπωλείο είναι δυνατόν να οδηγήσουν σε συμπεράσματα για τα ενδιαφέροντα, τις πολιτικές πεποιθήσεις ή την υγεία του. Άλλο παράδειγμα είναι η κατανάλωση συγκεκριμένης τροφής (π.χ. κρουασάν), που θα μπορούσε επίσης να οδηγήσει σε συμπεράσματα για την υγεία του υποκειμένου στο άμεσο ή λιγότερο άμεσο μέλλον.

Τα άρθρα 35 και 36 του ΓΚΠΔ αναφέρονται στην Εκτίμηση Αντικτύπου σχετικά με την προστασία δεδομένων και την προηγούμενη διαβούλευση.

Βασικά υποκείμενα των δεδομένων είναι φυσικά πρόσωπα (μόνο):

- Καταναλωτές (πελάτες του Υπεύθυνου Επεξεργασίας – ΥΕ)
- Καταναλωτές (πελάτες πελατών του ΥΕ)
- Συνεργαζόμενοι, προμηθευτές, ατομικές επιχειρήσεις
- Επισκέπτες
- Εργαζόμενοι

2.3 Κύρια Σημεία

Ο ΓΚΠΔ εισάγει νέα και ενισχυμένα δικαιώματα αναφορικά με τα δεδομένα προσωπικού χαρακτήρα (δικαίωμα στη διαφάνεια, δικαίωμα στη λήθη, δικαίωμα στη φορητότητα).

Κύριες αλλαγές:

1) Ενίσχυση των προϋποθέσεων για τη διασφάλιση μιας ενημερωμένης, ελεύθερης και επαληθεύσιμης συγκατάθεσης με δικαίωμα αναίρεσης.

2) Αύξηση της διαφάνειας της επικοινωνίας για τη διευκόλυνση της άσκησης των δικαιωμάτων των υποκειμένων των δεδομένων.
3) Παροχή πληροφοριών σχετικά με την επεξεργασία και τη δυνατότητα πρόσβασης σε δεδομένα προσωπικού χαρακτήρα.
4) Διαγραφή (δικαίωμα στη «λήθη») των προσωπικών δεδομένων από τον υπεύθυνο της επεξεργασίας των δεδομένων.
5) Φορητότητα και απλούστευση της μεταφοράς προσωπικών δεδομένων μεταξύ διαφορετικών υπευθύνων επεξεργασίας δεδομένων.
6) Δικαίωμα ένστασης κατά την επεξεργασία σε συγκεκριμένες περιπτώσεις ως άμεσο marketing.
7) Διακοπή της αυτόματης διαδικασία λήψης αποφάσεων, ιδίως στην περίπτωση δημιουργίας προφίλ.

Νέες δεσμεύσεις και ενίσχυση της υποχρέωσης λογοδοσίας, ορισμός υπεύθυνου για την επεξεργασία προσωπικών δεδομένων.

Κύριες αλλαγές:

8) Ενίσχυση της λογοδοσίας, όσον αφορά τη συμμόρφωση με τις ανατεθειμένες αρμοδιότητες.
9) Δημιουργία και συντήρηση των κατάλληλων εγγράφων που σχετίζονται με τις δραστηριότητες επεξεργασίας.
10) Λήψη μέτρων για την προστασία των δεδομένων προσωπικού χαρακτήρα και για την ασφαλή τους επεξεργασία.
11) Διαδικασία κοινοποίησης σε αρχές και υποκείμενα σχετικά με τις παραβιάσεις των προσωπικών δεδομένων.
12) Ανάγκη για εκτέλεση εκτίμησης των επιπτώσεων σε περιπτώσεις επεξεργασίας δεδομένων υψηλού κινδύνου (Privacy Impact Assessment).
13) Ορισμός Υπεύθυνου Προστασίας Δεδομένων (ΥΠΔ).
14) Εισαγωγή της προστασίας δεδομένων από τον σχεδιασμό.
15) Εισαγωγή της προστασίας δεδομένων εξ ορισμού.

Αυστηρότερο σύστημα ποινών και δυνατότητα επιβολής ποινικών κυρώσεων από τα κράτη-μέλη.

Κύρια σημεία:

16) Πρόστιμα έως και €20εκ ή 4% του συνολικού ετήσιου κύκλου εργασιών.
17) Επιβεβαίωση της συμμόρφωσης με τον κανονισμό μέσω εγκεκριμένου κώδικα δεοντολογίας.
18) Θέσπιση μιας Ευρωπαϊκής Επιτροπής Προστασίας Δεδομένων με στόχο τον συντονισμό των εποπτικών αρχών.
19) Εφαρμογή για όλα τα άτομα που διαμένουν στην ΕΕ, ανεξάρτητα από το αν η επεξεργασία των δεδομένων πραγματοποιείται εντός ή εκτός της ΕΕ.

2.4 Ενίσχυση των αρχών και των δικαιωμάτων

Όροι συναίνεσης (Άρθρα 6,7,8)

- Δικαίωμα να λαμβάνεται το αίτημα για συναίνεση με τρόπο που διακρίνεται σαφώς από τα άλλα θέματα, σε κατανοητή και εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή γλώσσα.
- Δικαίωμα να αποσύρεται η συγκατάθεση ανά πάσα στιγμή, με την ίδια ευκολία που δίνεται.
- Δικαίωμα να λαμβάνεται ένα αίτημα για συναίνεση δωρεάν, σε σχέση με την εκτέλεση μιας συμβάσεως, συμπεριλαμβανομένης της παροχής μιας υπηρεσίας.
- Υποχρέωση του υπεύθυνου επεξεργασίας, να επιδείξει τη συγκατάθεση που έχει ληφθεί για την επεξεργασία προσωπικών δεδομένων.
- Στην περίπτωση των παιδιών, σε σχέση με την προσφορά των υπηρεσιών της κοινωνίας της πληροφορίας, η συναίνεση είναι δυνατή μόνο αν το παιδί έχει συμπληρώσει τα 16 χρόνια. Σε κάθε άλλη περίπτωση, η συγκατάθεση δίνεται ή εξουσιοδοτείται από τον κάτοχο της γονικής μέριμνας.

Δικαίωμα στη διαφάνεια (Άρθρο12)

- Δικαίωμα λήψης των πληροφοριών και επικοινωνίας σχετικά με την άσκηση των δικαιωμάτων του υποκειμένου με μια συνοπτική, διάφανη, κατανοητή και εύκολα προσβάσιμη μορφή, με μια απλή γλώσσα (ιδίως στην περίπτωση των πληροφοριών που απευθύνονται σε ανήλικους).

Δικαίωμα στην πληροφόρηση και πρόσβαση σε δεδομένα (Άρθρα 13,14,15)

- Δικαίωμα να παρέχεται στα υποκείμενα των δεδομένων, σε μια ευρέως χρησιμοποιούμενη μορφή, η πληροφόρηση για την πρόσβαση στα προσωπικά δεδομένα και οι πληροφορίες της επεξεργασίας τους, οι κατηγορίες των υποκειμένων των δεδομένων, η περίοδος διατήρησης τους, οποιοδήποτε τρίτο μέρος που εμπλέκεται και την ύπαρξη αυτόματης λήψης αποφάσεων, συμπεριλαμβανομένης και της κατάρτισης προφίλ.

Δικαίωμα στη «λήθη» (Άρθρα 16, 17)

- Το υποκείμενο των δεδομένων έχει το δικαίωμα να ζητήσει από τον υπεύθυνο επεξεργασίας τη διαγραφή δεδομένων προσωπικού χαρακτήρα που το αφορούν και ο υπεύθυνος επεξεργασίας υποχρεούται να διαγράψει τα δεδομένα προσωπικού χαρακτήρα χωρίς αδικαιολόγητη καθυστέρηση.
- Το δικαίωμα αυτό δεν επιτρέπεται σε ειδικές περιπτώσεις που προβλέπονται από τον νόμο (π.χ. δικαίωμα στην ελευθερία πληροφόρησης, λόγοι δημοσίου συμφέροντος).
- Το δικαίωμα παρέχει τη δυνατότητα διόρθωσης προσωπικών δεδομένων, σε περίπτωση ανακριβειών από τον υπεύθυνο επεξεργασίας.

Δικαίωμα φορητότητας των δεδομένων (Άρθρο 20)

- Το υποκείμενο των δεδομένων έχει το δικαίωμα να λαμβάνει τα δεδομένα προσωπικού χαρακτήρα που το αφορούν και τα οποία έχει παράσχει σε υπεύθυνο επεξεργασίας, σε δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα μορφότυπο, καθώς

και το δικαίωμα να διαβιβάζει τα εν λόγω δεδομένα σε άλλο υπεύθυνο επεξεργασίας στον οποίον παρασχέθηκαν τα δεδομένα προσωπικού χαρακτήρα.

Δικαίωμα εναντίωσης (Άρθρο 21)

- Το υποκείμενο των δεδομένων δικαιούται να αντιτάσσεται, ανά πάσα στιγμή και για λόγους που σχετίζονται με την ιδιαίτερη κατάστασή του, στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που το αφορούν, περιλαμβανομένης της κατάρτισης προφίλ.
- Εάν δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία για σκοπούς απευθείας εμπορικής προώθησης, το υποκείμενο των δεδομένων δικαιούται να αντιταχθεί ανά πάσα στιγμή, περιλαμβανομένης της κατάρτισης προφίλ.

Δικαίωμα να μην υπόκειται σε απόφαση που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης διαδικασίας (Άρθρο 22)

- Το υποκείμενο των δεδομένων έχει το δικαίωμα να μην υπόκειται σε απόφαση που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας, συμπεριλαμβανομένης της κατάρτισης προφίλ, η οποία παράγει έννομα αποτελέσματα που το αφορούν ή το επηρεάζει σημαντικά με παρόμοιο τρόπο (π.χ. η διαδικτυακά αυτόματη απόρριψη αίτησης για χορήγηση πίστωσης).
- Συγκεκριμένα, εφαρμόζεται στην περίπτωση της γενικής εικόνας, που είναι μια μορφή της αυτοματοποιημένης επεξεργασίας των προσωπικών δεδομένων, που αξιολογεί προσωπικές πτυχές που σχετίζονται με ένα φυσικό πρόσωπο, προκειμένου να αναλύσει ή να προβλέψει τις ακόλουθες πτυχές:
  - εργασιακή απόδοση,
  - οικονομική κατάσταση,
  - υγεία,
  - προτιμήσεις ή προσωπικά ενδιαφέροντα,
  - αξιοπιστία ή συμπεριφορά,
  - τοποθεσία ή μετακίνηση.
- Το δικαίωμα αυτό δεν εφαρμόζεται σε περιπτώσεις ρητής συναίνεσης από το υποκείμενο, ή αν είναι απαραίτητο για την ολοκλήρωση/εκτέλεση της σύμβασης.

2.5 Αύξηση των υποχρεώσεων του υπεύθυνου επεξεργασίας και του εκτελούντος την επεξεργασία

Λογοδοσία (Άρθρα 5, 24)

- Υποχρέωση της ανάληψης ευθύνης σε σχέση με τις αρχές που εφαρμόζονται στην επεξεργασία προσωπικών δεδομένων. Η συμμόρφωση πρέπει να αποδεικνύεται από τον υπεύθυνο επεξεργασίας.
- Υποχρέωση να εκπληρώσει και να είναι σε θέση να επιδείξει συμμόρφωση με τον κανονισμό, ιδίως όσον αφορά τα ενδεδειγμένα τεχνικά και οργανωτικά μέτρα.

- Ευρεία διακριτικότητα όσον αφορά το είδος των μέτρων για την εφαρμογή, αλλά, την ίδια στιγμή, με το βάρος της απόδειξης της λογικής διαδικασίας που οδήγησε στην υιοθέτηση τους.

Αρχεία δραστηριοτήτων επεξεργασίας (Άρθρο 30)

- Υποχρέωση να τηρούν μητρώο των δραστηριοτήτων επεξεργασίας προσωπικών δεδομένων, που περιέχουν για παράδειγμα τους σκοπούς, τις κατηγορίες των υποκειμένων και των δεδομένων και των μέτρων ασφαλείας που εφαρμόζονται.
- Η υποχρέωση αναφέρεται σε μια επιχείρηση ή σε ένα οργανισμό με τουλάχιστον 250 άτομα, ή αν η επεξεργασία που πραγματοποιείται είναι πιθανόν να οδηγήσει σε υψηλό κίνδυνο.

Μέτρα ασφαλείας (Άρθρο 32)

- Υποχρέωση να εφαρμοστούν τα ενδεδειγμένα τεχνικά και οργανωτικά μέτρα για να εξασφαλίσουν επίπεδο ασφαλείας ανάλογο προς τους κινδύνους, συμπεριλαμβανομένων της χρήσης ψευδωνύμου και της κρυπτογράφησης δεδομένων προσωπικού χαρακτήρα, τις διαδικασίες διαχείρισης περιστατικών και τη διαδικασία για την αξιολόγηση της αποτελεσματικότητας των μέτρων.
- Οι υποχρεώσεις λαμβάνουν υπόψη τους κινδύνους που παρουσιάζονται από επεξεργασία, ιδίως από τυχαία ή αθέμιτη καταστροφή, απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση σε προσωπικά δεδομένα που διαβιβάζονται, αποθηκεύονται ή επεξεργάζονται με άλλο τρόπο.

Ειδοποίηση παραβίασης δεδομένων (Άρθρα 33, 34)

- Υποχρέωση έγκαιρης ενημέρωσης χωρίς αδικαιολόγητη καθυστέρηση (εντός 72 ωρών), της εποπτεύουσας Αρχής, σε περίπτωση πιθανής παραβίασης προσωπικών δεδομένων.
- Υποχρέωση ειδοποίησης του υποκειμένου των δεδομένων, χωρίς αδικαιολόγητη καθυστέρηση, όταν η παραβίαση προσωπικών δεδομένων είναι πιθανό να οδηγήσει σε υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων.

Εκτίμηση Αντικτύπου στην Προστασία Δεδομένων (Άρθρα 35,36)

- Η Εκτίμηση Αντικτύπου Προστασίας Δεδομένων (ΕΑΠΔ) θα πραγματοποιείται στο πλαίσιο του σχεδιασμού των επιχειρησιακών διαδικασιών κάθε φορά που η επεξεργασία δεδομένων προσωπικού χαρακτήρα περιλαμβάνει πιθανούς κινδύνους για τα δικαιώματα και την ελευθερία των υποκειμένων των δεδομένων.
- Η εκτίμηση πρέπει να περιλαμβάνει εκτίμηση των κινδύνων και αξιολόγηση των μέτρων ασφαλείας για τη διασφάλιση της προστασίας προσωπικών δεδομένων.

Υπεύθυνος Προστασίας Δεδομένων (Άρθρα 37, 38, 39)

- Υποχρέωση για διορισμό ενός υπευθύνου προστασίας δεδομένων, στην περίπτωση επεξεργασίας δεδομένων σε μεγάλη κλίμακα ή/και σε υψηλό κίνδυνο, με βάση τα επαγγελματικά προσόντα και ιδίως της εμπειρίας που διαθέτει στη νομοθεσία περί προστασίας δεδομένων. Είναι υπεύθυνος για
  - παροχή εξειδικευμένης υποστήριξης στον κανονισμό,

- παροχή συμβουλών για την εκτίμηση των επιπτώσεων στην προστασία δεδομένων,
- παρακολούθηση της συμμόρφωσης με τον κανονισμό,
- να ενεργεί ως σημείο επαφής με την εποπτεύουσα αρχή.

Προστασία των δεδομένων από το σχεδιασμό (Άρθρο 25)

- Υποχρέωση να εφαρμόζει, τόσο κατά τη στιγμή του καθορισμού των μέσων για την επεξεργασία όσο και κατά την ίδια την επεξεργασία, τα κατάλληλα τεχνικά και οργανωτικά μέτρα, όπως η χρήση ψευδωνύμου, τα οποία έχουν σχεδιαστεί για να εφαρμόζουν τις αρχές προστασίας δεδομένων της επεξεργασίας.

Προστασία δεδομένων εξ ορισμού (Άρθρο 25)

- Υποχρέωση να εφαρμόζονται τα κατάλληλα τεχνικά και οργανωτικά μέτρα για να εξασφαλιστεί ότι εξ ορισμού, μόνο τα προσωπικά στοιχεία τα οποία είναι απαραίτητα για την επεξεργασία και για συγκεκριμένο σκοπό, θα υποβάλλονται σε επεξεργασία.
- Υποχρέωση να διασφαλίζει ότι εξ ορισμού, τα προσωπικά δεδομένα τηρούνται μόνο για το χρονικό διάστημα το οποίο είναι απαραίτητο, για την παροχή του προϊόντος ή της υπηρεσίας.

3

Κατευθυντήριες γραμμές για τη διενέργεια Εκτίμησης Αντικτύπου στην Προστασία Δεδομένων (ΕΑΠΔ)

3.1 Η Ομάδα Εργασίας του Άρθρου 29-ΟΕ29 (Art. 29WP ή WP29)

Η Ομάδα Εργασίας του Άρθρου 29-ΟΕ29 (Article 29 Working Party - Art. 29 WP ή WP29) είναι ένα συμβουλευτικό σώμα, ο σκοπός και η σύνθεση του οποίου ορίζεται στο Άρθρο 29 της Οδηγίας για την Προστασία Προσωπικών Δεδομένων 95/46/ΕΚ.

Η Ομάδα Εργασίας αποτελείται από[2]:

- Εκπροσώπους των Εθνικών Εποπτικών Αρχών για την προστασία προσωπικών δεδομένων των Κρατών-Μελών της Ευρωπαϊκής Ένωσης.
- Εκπρόσωπο του Ευρωπαίου Επόπτη για την Προστασία Δεδομένων (European Data Protection Supervisor – EDPS).
- Εκπρόσωπο της Ευρωπαϊκής Επιτροπής ο οποίος είναι και ο Γραμματέας της Ομάδας Εργασίας.

Η κύρια αποστολή της ΟΕ29 είναι:

- Παροχή συμβουλών στα κράτη-μέλη για την προστασία των δεδομένων.
- Να προωθήσει την εφαρμογή του κανονισμού και των οδηγιών για την προστασία των δεδομένων σε όλα τα κράτη-μέλη της ΕΕ

[2] https://edps.europa.eu/data-protection/data-protection/glossary/a_en

- Να γνωμοδοτεί στην Ευρωπαϊκή Επιτροπή σχετικά με την κοινοτική νομοθεσία που αφορά την προστασία των προσωπικών δεδομένων
- Να κάνει συστάσεις στο κοινό σχετικά με θέματα που αφορούν την προστασία των ατόμων σε ότι αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στην Ευρωπαϊκή Κοινότητα.

Η Ομάδα Εργασίας έχει έναν πρόεδρο και δύο αντιπροέδρους οι οποίοι εκλέγονται από την Ομάδα Εργασίας. Η θητεία του προέδρου και των αντιπροέδρων είναι διετής και μπορούν να εκλεγούν μόνο μία φορά.

3.2 Κατευθυντήριες Γραμμές για την Διενέργεια Εκτίμησης Αντικτύπου στην Προστασία Δεδομένων στο πλαίσιο του ΓΚΠΔ (WP248, 2017)

3.2.1 Εισαγωγή

Το άρθρο 35 του ΓΚΠΔ εισάγει την έννοια της Εκτίμησης Αντικτύπου στην Προστασία Δεδομένων - ΕΑΠΔ (Data Protection Impact Assessment –DPIA)[3].

Η ΕΑΠΔ είναι μια διαδικασία [Άρθρο 35(7)] που αποσκοπεί

- στην περιγραφή της επεξεργασίας,
- στην εκτίμηση της αναγκαιότητας και της αναλογικότητάς της και
- στη διαχείριση των κινδύνων για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων που προκύπτουν από την επεξεργασία προσωπικών δεδομένων, αξιολογώντας τα και καθορίζοντας τα μέτρα αντιμετώπισής τους.

Αποτελεί το σημαντικό εργαλείο λογοδοσίας, καθώς βοηθά τους Υπεύθυνους Επεξεργασίας (ΥΕ) όχι μόνο να συμμορφώνονται με τις απαιτήσεις του ΓΚΠΔ, αλλά και να αποδείξουν ότι έχουν ληφθεί τα κατάλληλα μέτρα για να διασφαλιστεί η συμμόρφωση με τον κανονισμό [βλ. Άρθρο 24].

Η ΕΑΠΔ είναι η διαδικασία για την οικοδόμηση και την επίδειξη συμμόρφωσης.

Σύμφωνα με το ΓΚΠΔ, η μη συμμόρφωση με τις απαιτήσεις της ΕΑΠΔ μπορεί να οδηγήσει σε πρόστιμα που επιβάλλονται από την αρμόδια Εποπτική Αρχή.

Ως μη συμμόρφωση θεωρείται τόσο η μη εκτέλεση ΕΑΠΔ όταν η επεξεργασία υπόκειται σε εκτίμηση αντικτύπου [Άρθρο 35(1,3-4)], ή η εκτέλεση ΕΑΠΔ με εσφαλμένο τρόπο [Άρθρο 35 (2-7) και Άρθρο 36 (3ε)]. Η μη συμμόρφωση μπορεί να οδηγήσει σε διοικητικό πρόστιμο έως 10 εκατ. ευρώ ή έως 2% επί του συνολικού ετήσιου κύκλου εργασιών παγκοσμίως κατά το προηγούμενο οικονομικό έτος, όποιο είναι υψηλότερο.

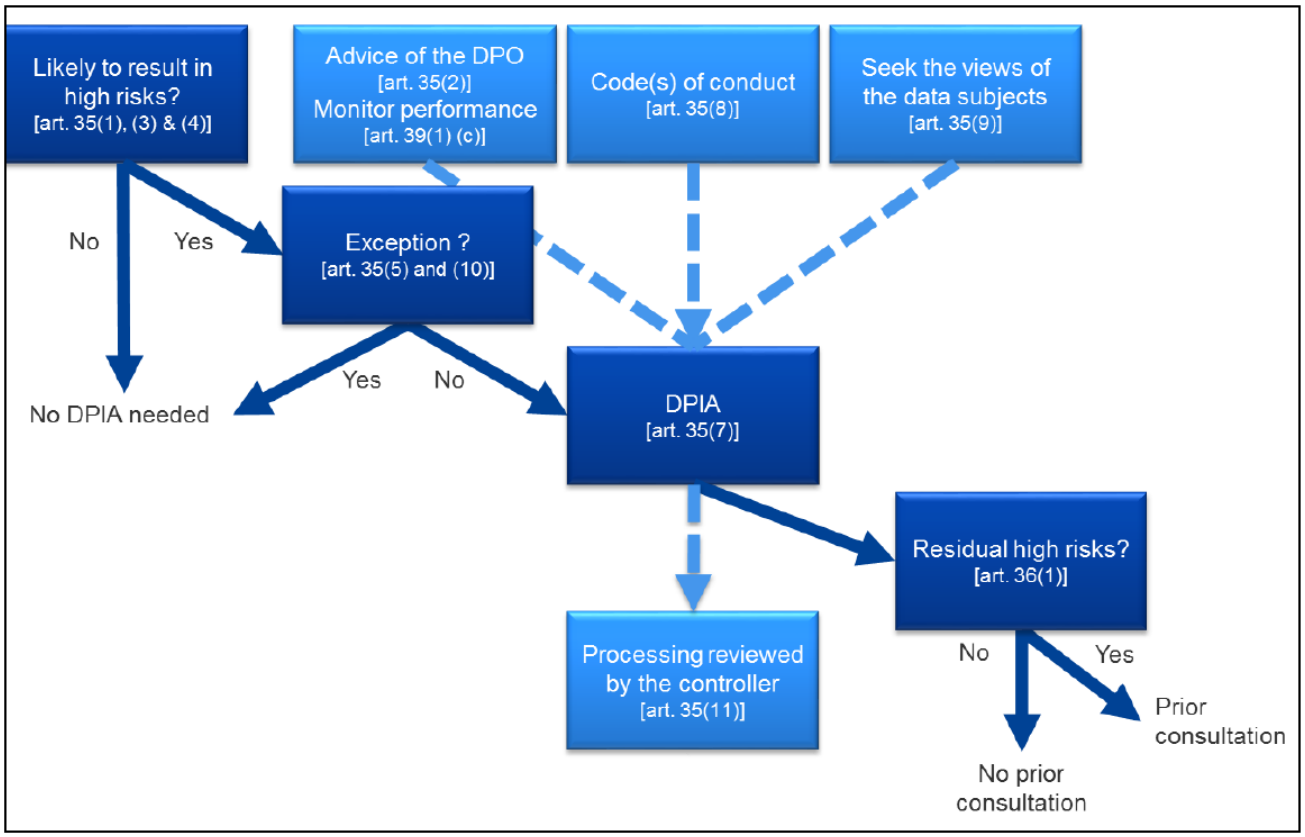
[3] Αναφέρεται και ως Privacy Impact Assessment (PIA) με το ίδιο ακριβώς νόημα.

3.2.2 ΕΑΠΔ

Ο ΓΚΠΔ απαιτεί από τους Υπεύθυνους Επεξεργασίας να εφαρμόσουν τα κατάλληλα μέτρα για να εξασφαλίσουν αλλά και να μπορούν να επιδείξουν συμμόρφωση λαμβάνοντας υπόψη, μεταξύ άλλων, "την σοβαρότητα των διάφορων κινδύνων επί των δικαιωμάτων και ελευθεριών των φυσικών προσώπων" [Άρθρο 24 (1)].

Το Άρθρο 35 αναφέρεται σε πιθανό υψηλό κίνδυνο "των δικαιωμάτων και των ελευθεριών των ατόμων". Η αναφορά στα "δικαιώματα και τις ελευθερίες" των προσώπων αφορά πρωτίστως τα δικαιώματα προστασίας προσωπικών δεδομένων και ιδιωτικής ζωής, αλλά μπορεί επίσης να περιλαμβάνει και άλλα θεμελιώδη δικαιώματα όπως η ελευθερία λόγου, η ελευθερία σκέψης, η ελεύθερη κυκλοφορία, η απαγόρευση των διακρίσεων και η θρησκεία.

Η παρακάτω εικόνα παρουσιάζει τα βασικά βήματα για τη διεξαγωγή Εκτίμησης Αντικτύπου στην Προστασία Δεδομένων στο πλαίσιο του ΓΚΠΔ.



Εικόνα 1: *Η σύνδεση των αντίστοιχων άρθρων του ΓΚΠΔ με τη διενέργεια ΕΑΠΔ* (WP248, 2017)

Η διεξαγωγή ΕΑΠΔ δεν είναι υποχρεωτική για κάθε μορφή επεξεργασίας. Απαιτείται μόνο όταν ένα είδος επεξεργασίας είναι "πιθανό να οδηγήσει σε υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων" [Άρθρο 35(1)]. Το γεγονός ότι δεν πληρούνται οι όροι που συνεπάγονται την υποχρεωτική διεξαγωγή ΕΑΠΔ δεν μειώνει την υποχρέωση των Υπευθύνων Επεξεργασίας να εφαρμόζουν μέτρα για την κατάλληλη διαχείριση των κινδύνων που αφορούν τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων. Στην πράξη, αυτό σημαίνει ότι οι Υπεύθυνοι Επεξεργασίας πρέπει να αξιολογούν συνεχώς τους κινδύνους που

δημιουργούν οι δραστηριότητες επεξεργασίας τους, προκειμένου να προσδιορίσουν πότε ένα είδος επεξεργασίας «ενδέχεται να οδηγήσει σε υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων»[4].

Η ΕΑΠΔ μπορεί να αφορά μόνο μια επεξεργασία δεδομένων ή μπορεί μια ΕΑΠΔ να χρησιμοποιηθεί για να αξιολογήσει πολλαπλές επεξεργασίες που είναι παρόμοιες σε ότι αφορά τη φύση, το πεδίο εφαρμογής, το πλαίσιο, το σκοπό και τους κινδύνους.

ΕΑΠΔ μπορεί επίσης να χρησιμοποιηθεί για την εκτίμηση των επιπτώσεων στην προστασία δεδομένων ενός τεχνολογικού προϊόντος, όπως για παράδειγμα φυσικού εξοπλισμού ή λογισμικού, που είναι πιθανό να χρησιμοποιηθεί από διαφορετικούς Υπεύθυνους Επεξεργασίας δεδομένων για την εκτέλεση διαφορετικών μορφών επεξεργασίας (ο ΥΕ των δεδομένων που χρησιμοποιεί το προϊόν εξακολουθεί να παραμένει υπόχρεος να εκτελεί τη δική του ΕΑΠΔ σε σχέση με την συγκεκριμένη εφαρμογή, συνεπικουρούμενος από την ΕΑΠΔ που συντάχθηκε από τον προμηθευτή του προϊόντος, εάν χρειάζεται).

3.2.3 Πότε είναι υποχρεωτική η ΕΑΠΔ.

Όταν η επεξεργασία είναι "πιθανό να οδηγήσει σε υψηλό κίνδυνο".

Ο ΓΚΠΔ δεν απαιτεί τη διεξαγωγή ΕΑΠΔ για κάθε επεξεργασία που ενδέχεται να δημιουργήσει κινδύνους για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Η εφαρμογή της ΕΑΠΔ είναι υποχρεωτική μόνον όταν η επεξεργασία «ενδέχεται να οδηγήσει σε **υψηλό** κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων» [Άρθρο 35(1,3,4)].

Στις περιπτώσεις όπου δεν είναι σαφές εάν απαιτείται, η ΟΕ29 συνιστά να διενεργηθεί ΕΑΠΔ, καθώς αποτελεί ένα χρήσιμο εργαλείο για να βοηθήσει τους ΥΕ να συμμορφωθούν με τον ΓΚΠΔ.

Προκειμένου να ορισθεί ένα ολοκληρωμένο σύνολο πράξεων "που ενδέχεται να οδηγήσουν σε επεξεργασία υψηλού κινδύνου", πρέπει να εξεταστούν τα ακόλουθα **εννέα κριτήρια**.

1. Αξιολόγηση ή βαθμολόγηση, ιδίως από «πτυχές που αφορούν την απόδοση του ατόμου στο χώρο εργασίας, την οικονομική κατάσταση, την υγεία, τις προσωπικές προτιμήσεις ή συμφέροντα, την αξιοπιστία ή τη συμπεριφορά, την τοποθεσία ή τις μετακινήσεις».

2. Αυτοματοποιημένη λήψη αποφάσεων με νομικές συνέπειες: η επεξεργασία που αποσκοπεί στη λήψη αποφάσεων επί των υποκειμένων των δεδομένων και που παράγουν "έννομα αποτελέσματα για το φυσικό πρόσωπο" ή που "επηρεάζει σημαντικά το φυσικό πρόσωπο" [Άρθρο 35(3α)]. Π.χ. όταν η επεξεργασία μπορεί να οδηγήσει στον αποκλεισμό ή τη διάκριση ατόμων.

[4] Οι κίνδυνοι που αφορούν τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων πρέπει να εντοπίζονται, να αναλύονται, να εκτιμώνται, να αξιολογούνται, να αντιμετωπίζονται (π.χ. μετριάζονται) και να επανεξετάζονται τακτικά. Οι Υπεύθυνοι Επεξεργασίας εξακολουθούν να έχουν την ευθύνη η οποία δεν μεταβιβάζεται με, π.χ., ασφαλιστήρια συμβόλαια.

3. Συστηματική παρακολούθηση: η επεξεργασία που χρησιμοποιείται για την παρακολούθηση ή τον έλεγχο των υποκειμένων των δεδομένων, μέσω δικτύων ή με τη «συστηματική παρακολούθηση μίας προσβάσιμης στο κοινό περιοχής» [Άρθρο 35(3γ)].

4. Ευαίσθητα δεδομένα ή δεδομένα προσωπικού χαρακτήρα: πρόκειται για ειδικές κατηγορίες προσωπικών δεδομένων όπως ορίζονται στο άρθρο 9 (για παράδειγμα πληροφορίες σχετικά με τις πολιτικές απόψεις των πολιτών), καθώς και για δεδομένα προσωπικού χαρακτήρα σχετικά με ποινικές καταδίκες ή αξιόποινες πράξεις, όπως ορίζονται στο άρθρο 10.

5. Δεδομένα που υποβάλλονται σε επεξεργασία μεγάλης κλίμακας: Ο ΓΚΠΔ δεν καθορίζει τι συνιστά μεγάλη κλίμακα. Η ΟΕ29 συνιστά να λαμβάνονται υπόψη οι ακόλουθοι παράγοντες, για να καθοριστεί εάν η επεξεργασία πραγματοποιείται σε μεγάλη κλίμακα:

- τον αριθμό ή το ποσοστό των προσώπων στα οποία αναφέρονται τα δεδομένα,
- τον όγκο δεδομένων ή/και το εύρος των στοιχείων που υφίστανται επεξεργασία,
- τη διάρκεια ή τη μονιμότητα της επεξεργασίας δεδομένων,
- τη γεωγραφική έκταση της επεξεργασίας.

6. Ταυτοποίηση ή συνδυασμός συνόλων δεδομένων (datasets), π.χ. που προέρχονται από δύο ή περισσότερες επεξεργασίες δεδομένων (που εκτελούνται για διαφορετικούς σκοπούς ή/και από διαφορετικούς ΥΕ) κατά τρόπο που υπερβαίνει τα αναμενόμενα και επιτρεπόμενα από το υποκείμενο των δεδομένων.

7. Δεδομένα σχετικά με ευάλωτα πρόσωπα: αποτελεί κριτήριο λόγω της αυξημένης ανισορροπίας ισχύος μεταξύ των προσώπων στα οποία αναφέρονται τα δεδομένα και του ΥΕ, που σημαίνει ότι τα άτομα ενδέχεται να μην είναι σε θέση να συμφωνήσουν ή να αντιταχθούν στην επεξεργασία των δεδομένων.

8. Η καινοτόμος χρήση ή η εφαρμογή νέων τεχνολογικών ή οργανωτικών λύσεων, όπως ο συνδυασμός της χρήσης δακτυλικών αποτυπωμάτων και αναγνώρισης προσώπου για βελτιωμένο έλεγχο της φυσικής πρόσβασης κ.λπ. Ο ΓΚΠΔ καθιστά σαφές [Άρθρο 35(1)] ότι η χρήση νέας τεχνολογίας, απαιτεί τη διενέργεια ΕΑΠΔ. Ο ΥΕ δεδομένων θα μπορεί έτσι να κατανοήσει και να αντιμετωπίσει τους κινδύνους που εισάγονται.

9. Όταν η επεξεργασία αυτή καθαυτή **"εμποδίζει τα πρόσωπα στα οποία αναφέρονται τα δεδομένα να ασκούν τα δικαιώματα τους ή να χρησιμοποιούν κάποια υπηρεσία"** [Άρθρο 22].

3.2.4 Εκτέλεση ΕΑΠΔ

α) Σε ποια χρονική στιγμή θα πρέπει να πραγματοποιηθεί μια ΕΑΠΔ;

Η ΕΑΠΔ πρέπει να εκτελείται "πριν από την επεξεργασία" [Άρθρο 35(1,10)]. Αυτό συμβαδίζει με την αρχή για προστασία των δεδομένων εξ ορισμού και από τον σχεδιασμό (by default & by design) [Άρθρο 25].

Η ΕΑΠΔ θα πρέπει να αρχίζει το συντομότερο δυνατόν κατά τον σχεδιασμό της επεξεργασίας, να επικαιροποιείται καθ' όλη τη διάρκεια του κύκλου ζωής και να εξασφαλίζει ότι λαμβάνεται υπόψη τόσο η προστασία των δεδομένων και η ιδιωτική ζωή όσο και η δημιουργία λύσεων που προάγουν τη συμμόρφωση. Η διεξαγωγή της ΕΑΠΔ είναι μια διαρκής διαδικασία.

β) Ποιος είναι υποχρεωμένος να εκτελέσει την ΕΑΠΔ;

Ο ΥΕ φέρει την ευθύνη για τη διεξαγωγής της ΕΑΠΔ [Άρθρο 35(2)]. Μπορεί να γίνει και από κάποιον τρίτο, μέσα ή έξω από τον οργανισμό, αλλά ο ΥΕ έχει τη συνολική ευθύνη.

Ο ΥΕ πρέπει επίσης να ζητήσει τη συμβουλή του ΥΠΔ και οι αποφάσεις που λαμβάνονται από τον ΥΕ πρέπει να τεκμηριώνονται εντός της ΕΑΠΔ.

Καθοριστικό ρόλο παίζει και η βοήθεια του ΕΕ, λαμβάνοντας υπόψη τη φύση της επεξεργασίας και τις πληροφορίες που διαθέτει ο ΕΕ [Άρθρο 28 (3στ)].

Επίσης συνιστάται η αναζήτηση συμβουλών από ανεξάρτητους εμπειρογνώμονες διαφόρων επαγγελμάτων (δικηγόροι, εμπειρογνώμονες πληροφορικής, εμπειρογνώμονες στον τομέα της ασφάλειας, κοινωνιολόγοι κ.λπ.).

Ο Επικεφαλής Ασφάλειας Πληροφοριών (CISO), καθώς και ο ΥΠΔ (DPO), θα μπορούν να προτείνουν στον ΥΕ να διεξάγει ΕΑΠΔ σε συγκεκριμένη επεξεργασία ανάλογα με τις ανάγκες ασφαλείας ή λειτουργίας.

γ) Ποια είναι η μεθοδολογία για τη διεξαγωγή μιας ΕΑΠΔ;

Ο ΓΚΠΔ ορίζει τα ελάχιστα χαρακτηριστικά της ΕΑΠΔ [Άρθρο 35(7)]:

- περιγραφή της πράξεων και των σκοπών της επεξεργασίας,
- αξιολόγηση της αναγκαιότητας και της αναλογικότητας της επεξεργασίας σε σχέση με τον σκοπό,
- εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των προσώπων στα οποία αναφέρονται τα δεδομένα,
- τα μέτρα που προβλέπονται για αντιμετώπιση των κινδύνων,
- να αποδεικνύεται η συμμόρφωση με τον ΓΚΠΔ,

Η ΕΑΠΔ στοχεύει στη "διαχείριση των κινδύνων" που αφορούν τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, χρησιμοποιώντας τις ακόλουθες διαδικασίες:

- καθορισμός του πλαισίου: «λαμβάνοντας υπόψη τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τον σκοπό της επεξεργασίας και τις πηγές κινδύνου»,
- εκτίμηση των κινδύνων: «εκτίμηση της σοβαρότητας του υψηλού κινδύνου»,
- αντιμετώπιση των κινδύνων: «μετριασμός του κινδύνου», «εξασφάλιση της προστασίας των προσωπικών δεδομένων» και «απόδειξη της συμμόρφωσης με τον παρόντα κανονισμό».

δ) Υπάρχει υποχρέωση δημοσίευσης της ΕΑΠΔ;

Η δημοσίευση της ΕΑΠΔ δεν αποτελεί νομική απαίτηση του ΓΚΠΔ. Ωστόσο, οι ΥΕ θα πρέπει να εξετάσουν τη δημοσίευση τουλάχιστον τμημάτων, όπως περίληψη ή συμπέρασμα της ΕΑΠΔ, καθώς μια τέτοια ενέργεια θα συνέβαλλε στην ενίσχυση της εμπιστοσύνης στις διαδικασίες επεξεργασίας του ΥΕ και θα επιδείκνυε υπευθυνότητα και διαφάνεια.

3.2.5 Συμπεράσματα και Προτάσεις

Οι ΥΕ θα πρέπει να θεωρούν τη διεξαγωγή ΕΑΠΔ ως μια χρήσιμη και θετική δραστηριότητα που βοηθά στη συμμόρφωση με τον ΓΚΠΔ, όπου προγραμματίζεται ή πραγματοποιείται επεξεργασία δεδομένων υψηλού κινδύνου. Αυτό σημαίνει ότι οι Υπεύθυνοι Επεξεργασίας

δεδομένων θα πρέπει να χρησιμοποιούν τα κριτήρια που καθορίζονται στην παράγραφο 4.2.3 για να καθορίσουν εάν πρέπει να διεξαχθεί ή όχι μια ΕΑΠΔ. Η Πολιτική Ασφάλειας του Οργανισμού σε ότι αφορά τα δεδομένα, θα μπορούσε να επεκτείνει αυτόν τον κατάλογο πέρα από τις νομικές απαιτήσεις του ΓΚΠΔ. Αυτό θα οδηγήσει σε μεγαλύτερη εμπιστοσύνη των υποκειμένων των δεδομένων.

Όταν προγραμματίζεται πιθανή επεξεργασία υψηλού κινδύνου, ο ΥΕ πρέπει:

- να επιλέξει μια μεθοδολογία ΕΑΠΔ που είναι συμβατή με τις υπάρχουσες διαδικασίες σχεδιασμού, ανάπτυξης, αλλαγής, κινδύνου και επιχειρησιακής αναθεώρησης σύμφωνα με τις εσωτερικές διαδικασίες, το πλαίσιο και την κουλτούρα,
- να περιλαμβάνει τα ενδιαφερόμενα μέρη και να καθορίζει με σαφήνεια τις ευθύνες τους (Υπεύθυνος Επεξεργασίας, Υπεύθυνος Προστασίας Δεδομένων, υποκείμενο των δεδομένων ή εκπρόσωποί τους, επιχειρήσεις, τεχνικές υπηρεσίες, Εκτελούντες την Επεξεργασία, Υπεύθυνος Ασφάλειας Πληροφοριών κ.λπ.),
- να προσκομίσει την έκθεση ΕΑΠΔ στην αρμόδια Εποπτεύουσα Αρχή όταν ζητηθεί,
- να συμβουλεύεται την Εποπτεύουσα Αρχή όταν δεν έχουν καθοριστεί επαρκή μέτρα για την άμβλυνση των υψηλών κινδύνων,
- να επανεξετάζει περιοδικά την ΕΑΠΔ και την επεξεργασία που αξιολογεί, τουλάχιστον όταν υπάρχει μεταβολή του κινδύνου από την επεξεργασία της πράξης,
- τεκμηριώνει τις αποφάσεις που έχουν ληφθεί.

4

Κατευθυντήριες γραμμές για την Αναγγελία Παραβίασης Δεδομένων (WP250, 2017)

4.1 Εισαγωγή

Ο ΓΚΠΔ εισάγει την υποχρέωση κοινοποίησης στην αρμόδια εθνική εποπτική αρχή της παραβίασης δεδομένων προσωπικού χαρακτήρα και, σε ορισμένες περιπτώσεις, στα φυσικά πρόσωπα των οποίων τα προσωπικά δεδομένα έχουν επηρεαστεί από την παραβίαση.

Η οδηγία 95/46/ΕΚ4 για την προστασία των δεδομένων, την οποία αντικαθιστά ο ΓΚΠΔ, δεν περιέχει συγκεκριμένη υποχρέωση κοινοποίησης παραβίασης και επομένως μια τέτοια απαίτηση θα είναι νέα για πολλούς οργανισμούς.

Ο ΓΚΠΔ περιέχει διατάξεις σχετικά με το πότε πρέπει να κοινοποιηθεί μια παραβίαση και σε ποιον, καθώς και ποιες πληροφορίες θα πρέπει να παρέχονται. Οι πληροφορίες που απαιτούνται για την κοινοποίηση της παραβίασης μπορεί (υπό συνθήκες) να παρέχονται σε φάσεις, αλλά σε κάθε περίπτωση ο ΥΕ θα πρέπει να ενεργεί εγκαίρως για οποιαδήποτε παραβίαση.

Η εποπτική αρχή μπορεί να υποχρεώσει τον ΥΕ να ενημερώσει τα άτομα για την παραβίαση.

4.2 Αναγγελία Παραβίασης Προσωπικών Δεδομένων στο πλαίσιο του ΓΚΠΔ

Α. Βασικές αρχές ασφάλειας

Μία από τις απαιτήσεις του ΓΚΠΔ είναι ότι τα προσωπικά δεδομένα πρέπει να υποβάλλονται σε επεξεργασία κατά τρόπο που να εξασφαλίζεται η ασφάλεια τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και από τυχαία απώλεια ή καταστροφή.

«Καταστροφή» των προσωπικών δεδομένων σημαίνει ότι τα δεδομένα δεν υπάρχουν πλέον ή δεν υπάρχουν σε μορφή που να είναι χρήσιμη για τον ΥΕ. «Απώλεια» των προσωπικών δεδομένων, σημαίνει ότι τα δεδομένα μπορεί να εξακολουθούν να υφίστανται, αλλά ο ΥΕ έχει χάσει τον έλεγχο ή την πρόσβαση σε αυτά, ή δεν τα έχει πλέον στην κατοχή του. Τέλος, η «μη εξουσιοδοτημένη ή παράνομη επεξεργασία» μπορεί να περιλαμβάνει αποκάλυψη προσωπικών δεδομένων σε μη εξουσιοδοτημένους παραλήπτες ή οποιαδήποτε άλλη μορφή επεξεργασίας που παραβιάζει τον ΓΚΠΔ.

Συνεπώς, ο ΓΚΠΔ απαιτεί τόσο από τους ΥΕ όσο και από τους ΕΕ να διαθέτουν κατάλληλα τεχνικά και οργανωτικά μέτρα για να εξασφαλίσουν ένα επίπεδο προστασίας κατάλληλο και ικανό να αποτρέψει μια παραβίαση και, αν συμβεί, να αντιδρά σε αυτήν εγκαίρως.

Β. Τι είναι η παραβίαση προσωπικών δεδομένων;

1. Ορισμός

Ο ΓΚΠΔ ορίζει ως «παραβίαση προσωπικών δεδομένων» [Άρθρο 4(12)] την «παραβίαση της ασφάλειας που οδηγεί στην τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, μη εξουσιοδοτημένη αποκάλυψη ή πρόσβαση σε προσωπικά δεδομένα που μεταδίδονται, αποθηκεύονται ή υποβάλλονται σε άλλη επεξεργασία».

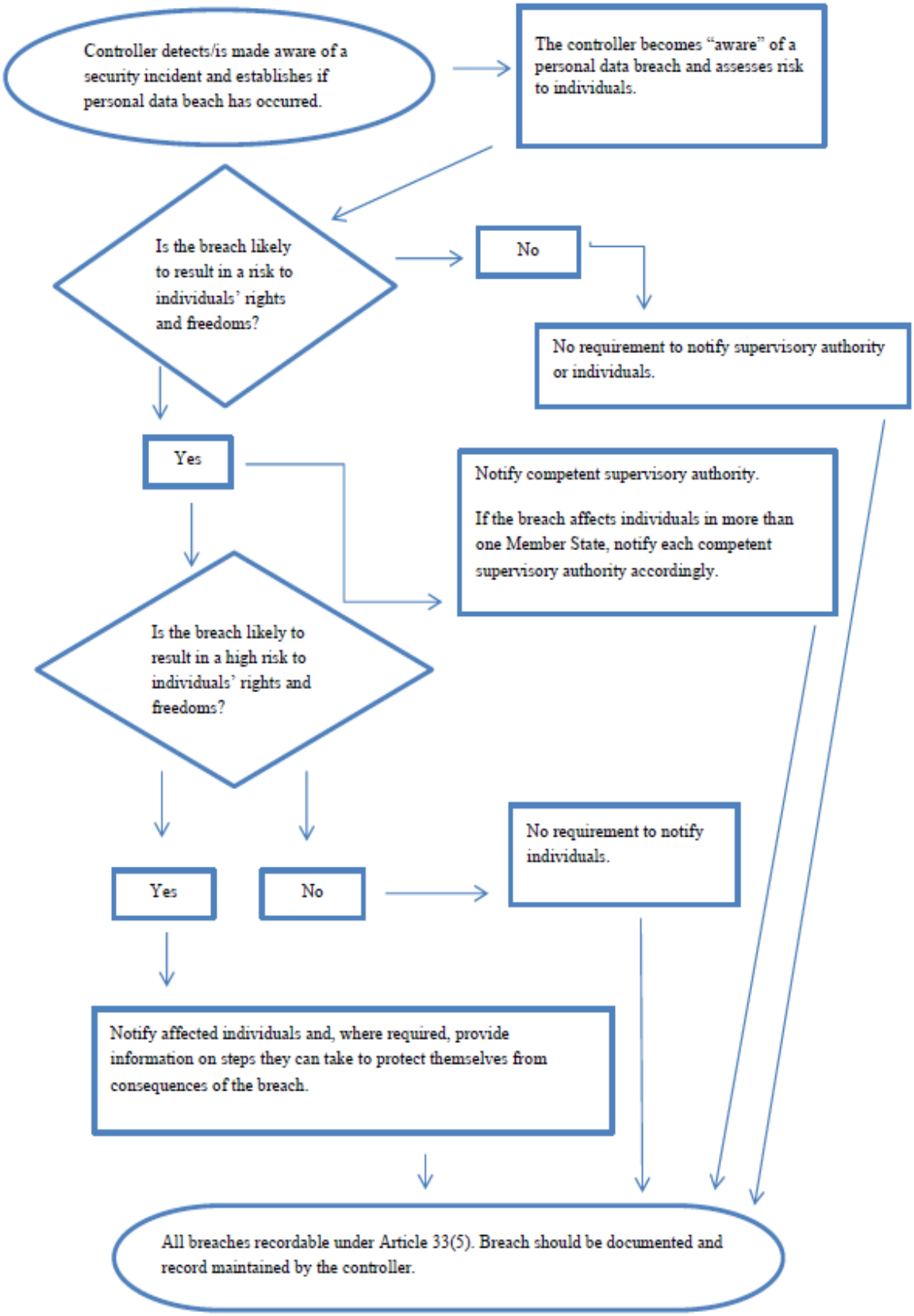
Αυτό που πρέπει να είναι σαφές είναι ότι ενώ μια παραβίαση συνιστά ένα περιστατικό ασφάλειας, **ο ΓΚΠΔ εφαρμόζεται μόνο όταν υπάρχει παραβίαση προσωπικών δεδομένων**. Η συνέπεια μιας τέτοιας παραβίασης είναι ότι ο ΥΕ δεν θα είναι σε θέση να εξασφαλίσει την τήρηση των αρχών σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα, όπως περιγράφονται στο άρθρο 5 του Κανονισμού.

Ενώ όλες οι παραβιάσεις προσωπικών δεδομένων είναι περιστατικά ασφαλείας, δεν είναι όλα τα περιστατικά ασφαλείας αναγκαστικά και παραβιάσεις προσωπικών δεδομένων.

2. Τύποι παραβιάσεων προσωπικών δεδομένων

Οι παραβιάσεις μπορούν να κατηγοριοποιηθούν σύμφωνα με τις ακόλουθες τρεις γνωστές αρχές ασφάλειας πληροφοριών:

- "Παραβίαση της εμπιστευτικότητας" – όταν υπάρχει αποκάλυψη προσωπικών δεδομένων ή πρόσβαση σε αυτά.
- "Παραβίαση διαθεσιμότητας" – όταν υπάρχει απώλεια πρόσβασης ή καταστροφή προσωπικών δεδομένων.
- "Παραβίαση ακεραιότητας" – όταν υπάρχει αλλοίωση των προσωπικών δεδομένων.



Εικόνα 2: *Διάγραμμα Ροής Διαδικασίας Αναγγελίας Παραβίασης Δεδομένων* (WP250, 2017)

Πρέπει επίσης να σημειωθεί ότι, ανάλογα με τις περιστάσεις, μια παραβίαση μπορεί να αφορά ταυτόχρονα την εμπιστευτικότητα, τη διαθεσιμότητα και την ακεραιότητα των προσωπικών δεδομένων, καθώς και οποιοδήποτε συνδυασμό αυτών.

Ένα περιστατικό με το οποίο τα προσωπικά δεδομένα καθίστανται μη διαθέσιμα για μια χρονική περίοδο, αποτελεί παραβίαση της ασφάλειας (και πρέπει να τεκμηριωθεί), αλλά ανάλογα με τις περιστάσεις, μπορεί να μην απαιτείται η κοινοποίηση στην εποπτική αρχή και στα επηρεαζόμενα άτομα. Εάν όμως η έλλειψη διαθεσιμότητας δεδομένων προσωπικού χαρακτήρα ενδέχεται να θέσει σε κίνδυνο τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, τότε ο ΥΕ θα πρέπει να ενημερώσει. Αυτό θα πρέπει να αξιολογείται κατά περίπτωση.

Επιπλέον, πρέπει να σημειωθεί ότι παρόλο που η απώλεια της διαθεσιμότητας των συστημάτων του ελεγκτή μπορεί να είναι μόνο προσωρινή και δεν μπορεί να έχει αντίκτυπο στους ιδιώτες, το γεγονός ότι έχει υπάρξει διείσδυση σε δίκτυο θα μπορούσε ακόμη να θεωρηθεί πιθανή παραβίαση της εμπιστευτικότητας και να απαιτείται κοινοποίηση. Ως εκ τούτου, είναι σημαντικό για τον ΥΕ να εξετάσει όλες τις πιθανές συνέπειες μιας παραβίασης.

3. Οι πιθανές συνέπειες μιας παραβίασης των προσωπικών δεδομένων

Η παραβίαση ενδέχεται να έχει πολλές σημαντικές αρνητικές επιπτώσεις για τα άτομα, γεγονός που μπορεί να έχει ως αποτέλεσμα φυσικές, υλικές ή άυλες συνέπειες. Μπορεί να περιλαμβάνει απώλεια ελέγχου των προσωπικών τους δεδομένων, περιορισμό των δικαιωμάτων τους, διακρίσεις, κλοπή ταυτότητας ή απάτη, οικονομικές απώλειες, βλάβη της φήμης και απώλεια εμπιστευτικότητας προσωπικών δεδομένων που μπορεί να προστατεύονται από το επαγγελματικό απόρρητο.

Ως εκ τούτου, ο ΓΚΠΔ απαιτεί από τον ΥΕ να αναφέρει την παραβίαση στην αρμόδια εποπτική αρχή, εκτός εάν, είναι απίθανο να δημιουργηθεί κίνδυνος δυσμενών επιπτώσεων. Όταν υπάρχει υψηλός κίνδυνος εμφάνισης αυτών των δυσμενών επιπτώσεων, ο ΓΚΠΔ απαιτεί από τον ελεγκτή να κοινοποιήσει την παραβίαση στα θιγόμενα άτομα το συντομότερο δυνατό.

Εάν οι ΥΕ δεν ενημερώσουν είτε την εποπτική αρχή είτε τα πρόσωπα στα οποία αναφέρονται τα δεδομένα ή και τους δύο, τότε η εποπτική αρχή μπορεί να επιβάλλει διορθωτικά μέτρα ή/και διοικητικό πρόστιμο. Είναι επίσης σημαντικό να ληφθεί υπόψη ότι σε ορισμένες περιπτώσεις, η μη αναγγελία παραβίασης θα μπορούσε να αποκαλύψει είτε την έλλειψη μέτρων ασφαλείας είτε την ανεπάρκεια των υφιστάμενων μέτρων ασφαλείας. Στην περίπτωση αυτή, η εποπτική αρχή θα έχει επίσης τη δυνατότητα να επιβάλλει κυρώσεις για μη αναγγελία της παραβίασης (άρθρα 33 και 34), αφενός, και για απουσία (επαρκών) μέτρων ασφαλείας (άρθρο 32), αφετέρου , δεδομένου ότι πρόκειται για δύο χωριστές παραβάσεις.

4.3 Άρθρο 33 – Αναφορά στην Εποπτεύουσα Αρχή

«Σε περίπτωση παραβίασης των προσωπικών δεδομένων, ο ΥΕ ενημερώνει, χωρίς αδικαιολόγητη καθυστέρηση και το αργότερο εντός 72 ωρών, την αρμόδια εποπτική αρχή. Όταν η κοινοποίηση προς την εποπτική αρχή δεν πραγματοποιηθεί εντός 72 ωρών, πρέπει να αιτιολογηθεί η καθυστέρηση». [Άρθρο 33(1)]

Η ΟΕ29 θεωρεί ότι ο ΥΕ θεωρείται ότι έχει «επίγνωση», όταν ο εν λόγω ΥΕ είναι σε λογικό βαθμό βέβαιος ότι έχει συμβεί κάποιο γεγονός που έχει ως αποτέλεσμα την υπονόμευση των προσωπικών δεδομένων. Σε ορισμένες περιπτώσεις, θα είναι σχετικά ξεκάθαρο από την αρχή ότι υπήρξε παραβίαση, ενώ σε άλλες ενδέχεται να χρειαστεί κάποιος χρόνος για να διαπιστωθεί εάν

έχουν διακυβευτεί τα προσωπικά δεδομένα. Ωστόσο, θα πρέπει να δοθεί έμφαση στην άμεση ανάληψη δράσης προκειμένου να διαπιστωθεί κατά πόσον πράγματι παραβιάστηκαν τα προσωπικά δεδομένα και, εάν ναι, να ληφθούν διορθωτικά μέτρα και να κοινοποιηθούν, εφόσον το ζητηθεί. Κατά τη διάρκεια της περιόδου έρευνας, ο ΥΕ δεν θεωρείται «ενήμερος».

Επομένως, ο ΥΕ θα πρέπει να διαθέτει εσωτερικές διαδικασίες, ώστε να είναι σε θέση να ανιχνεύσει και να αντιμετωπίσει μια παραβίαση. Είναι σημαντικό, όταν διαπιστωθεί παραβίαση, να αναφερθεί προς τα πάνω στο κατάλληλο επίπεδο διοίκησης, ώστε να μπορεί να αντιμετωπιστεί και, εάν απαιτείται, να κοινοποιηθεί σύμφωνα με το άρθρο 33 και, εάν είναι απαραίτητο, με το άρθρο 34 (στο υποκείμενο των δεδομένων), όπως περιγράφονται λεπτομερώς στα σχέδια αντιμετώπισης περιστατικών ή / και ρυθμίσεων διακυβέρνησης του ελεγκτή. Αυτά θα βοηθήσουν τον ΥΕ να σχεδιάσει αποτελεσματικά και να καθορίσει ποιος έχει επιχειρησιακή ευθύνη εντός του οργανισμού για τη διαχείριση παραβίασης και πώς ή εάν θα κλιμακωθεί ένα περιστατικό όπως αρμόζει.

Ενώ είναι ευθύνη των ΥΕ και των ΕΕ να θεσπίσουν κατάλληλα μέτρα για να προλαμβάνουν και να αντιμετωπίζουν μια παραβίαση, υπάρχουν ορισμένα πρακτικά βήματα που πρέπει να ληφθούν σε όλες τις περιπτώσεις.

- Οι πληροφορίες σχετικά με τα γεγονότα που σχετίζονται με την ασφάλεια πρέπει να απευθύνονται σε υπεύθυνο πρόσωπο ή σε άτομα που έχουν ως αποστολή την αντιμετώπιση περιστατικών, την ύπαρξη παραβίασης και την εκτίμηση του κινδύνου.
- Θα πρέπει να αξιολογείται ο κίνδυνος για τα άτομα ως αποτέλεσμα παραβίασης, με τα σχετικά τμήματα του οργανισμού να ενημερώνονται.
- Εάν απαιτείται, θα πρέπει να γίνεται κοινοποίηση στην εποπτική αρχή και ενδεχομένως επικοινωνία της παραβίασης με τα ενδιαφερόμενα άτομα.
- Ταυτόχρονα, ο ΥΕ πρέπει να ενεργεί για τον περιορισμό των συνεπειών και τον τερματισμό της παραβίασης.

Θα πρέπει να είναι σαφές ότι ο υπεύθυνος επεξεργασίας υποχρεούται να ενεργεί σε κάθε αρχική καταχώρηση και να διαπιστώνει αν πράγματι σημειώθηκε παραβίαση. Αυτή η σύντομη περίοδος επιτρέπει τη διεξαγωγή ορισμένων ερευνών, τη συλλογή αποδεικτικών στοιχείων και την εκτίμηση του κινδύνου προτού ειδοποιήσει σχετικά ο υπεύθυνος της ελεγκτικής υπηρεσίας. Εάν ένας υπεύθυνος επεξεργασίας δεν ενεργήσει εγκαίρως και είναι εμφανές ότι σημειώθηκε παραβίαση, αυτό θα μπορούσε να θεωρηθεί ως αδυναμία κοινοποίησης σύμφωνα με το άρθρο 33.

Ο ΥΕ διατηρεί τη γενική ευθύνη για την προστασία των δεδομένων προσωπικού χαρακτήρα, αλλά και ο ΕΕ παίζει σημαντικό ρόλο προκειμένου να μπορέσει ο ΥΕ να συμμορφωθεί με τις υποχρεώσεις του. Ο ΕΕ «βοηθά τον ΥΕ να διασφαλίζει την τήρηση των υποχρεώσεων που προβλέπονται στα άρθρα 32 έως 36 λαμβάνοντας υπόψη τη φύση της επεξεργασίας και τις πληροφορίες που διαθέτει» [Άρθρο 28 (3 στ)].

Ο ΓΚΠΔ δεν παρέχει ρητή προθεσμία εντός της οποίας ο ΕΕ πρέπει να ειδοποιεί τον ΥΕ, εκτός από το ότι πρέπει να το πράξει «χωρίς αδικαιολόγητη καθυστέρηση». Ως εκ τούτου, η ΟΕ29 συνιστά άμεση ειδοποίηση για να βοηθηθεί ο ΥΕ να ανταποκριθεί στην απαίτηση κοινοποίησης στην εποπτική αρχή εντός 72 ωρών.

Παροχή πληροφοριών στην εποπτική αρχή

Όταν ο ΥΕ κοινοποιεί παραβίαση στην εποπτική αρχή, το άρθρο 33 παράγραφος 3 ορίζει ότι, τουλάχιστον, πρέπει:

- να περιγράφει τη φύση της παραβίασης των προσωπικών δεδομένων, συμπεριλαμβανομένων, όπου είναι δυνατόν, των κατηγοριών και του κατά προσέγγιση αριθμού των υποκειμένων των δεδομένων,
- να κοινοποιεί το όνομα και τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων ή άλλου σημείου αναφοράς, όπου μπορούν να ληφθούν περισσότερες πληροφορίες,
- να περιγράφει τις πιθανές συνέπειες της παραβίασης των προσωπικών δεδομένων,
- να περιγράφει τα μέτρα που έλαβε ή προτίθεται να λάβει ο ΥΕ για την αντιμετώπιση της παραβίασης των προσωπικών δεδομένων, συμπεριλαμβανομένων, κατά περίπτωση, μέτρων για τον μετριασμό των πιθανών δυσμενών επιπτώσεών του.

Κοινοποίηση σε φάσεις

Ανάλογα με τη φύση μιας παραβίασης, μπορεί να απαιτηθεί περαιτέρω διερεύνηση από τον υπεύθυνο επεξεργασίας για τον προσδιορισμό όλων των σχετικών γεγονότων που σχετίζονται με το περιστατικό. Ο ΓΚΠΔ αναγνωρίζει ότι οι ΥΕ δεν θα έχουν πάντοτε όλες τις απαραίτητες πληροφορίες σχετικά με παραβίαση εντός 72 ωρών από τη στιγμή που θα το γνωρίζουν, καθώς και οι πλήρεις λεπτομέρειες του περιστατικού ενδέχεται να μην είναι πάντα διαθέσιμες κατά τη διάρκεια αυτής της αρχικής περιόδου. Ως εκ τούτου, επιτρέπει την κοινοποίηση σε φάσεις. Αυτό είναι επιτρεπτό, εφόσον ο ΥΕ αιτιολογεί την καθυστέρηση [Άρθρο 33 (1)]. Η εποπτική αρχή πρέπει να συμφωνεί με τον τρόπο και τον χρόνο παροχής πρόσθετων πληροφοριών.

Αν στην επακόλουθη έρευνα ο ΥΕ ενημερώσει την εποπτική αρχή ότι κατά το περιστατικό ασφάλειας δεν σημειώθηκε τελικά παραβίαση, τότε οι πληροφορίες αυτές μπορούν να προστεθούν στις πληροφορίες που έχουν ήδη παρασχεθεί στην εποπτική αρχή και το περιστατικό να καταγραφεί ως μη παραβίαση. Δεν υπάρχει ποινή για την αναφορά περιστατικού που τελικά δεν αποτελεί παραβίαση.

Καθυστερημένες ειδοποιήσεις

Το άρθρο 33 παράγραφος 1 καθιστά σαφές ότι όταν η κοινοποίηση προς την εποπτική αρχή δεν πραγματοποιείται εντός 72 ωρών, η καθυστέρηση πρέπει να αιτιολογηθεί. Αυτό, μαζί με την έννοια της κοινοποίησης σε φάσεις, αναγνωρίζει ότι ο υπεύθυνος επεξεργασίας μπορεί να μην είναι πάντοτε σε θέση να κοινοποιήσει παραβίαση εντός της συγκεκριμένης χρονικής περιόδου και ότι μπορεί να επιτρέπεται μια καθυστερημένη κοινοποίηση.

Παραβιάσεις που αφορούν πολίτες σε περισσότερα του ενός κράτη μέλη

Σε περίπτωση διασυνοριακής επεξεργασίας δεδομένων προσωπικού χαρακτήρα, η παραβίαση μπορεί να επηρεάσει τα υποκείμενα των δεδομένων σε περισσότερα του ενός κράτη μέλη. Το άρθρο 33 παράγραφος 1 καθιστά σαφές ότι, σε περίπτωση παραβίασης, ο υπεύθυνος της επεξεργασίας πρέπει να ειδοποιήσει την αρμόδια εποπτική αρχή σύμφωνα με το άρθρο 55 του ΓΚΠΔ. Το άρθρο 55 παράγραφος 1 αναφέρει ότι:

«Κάθε εποπτική αρχή είναι αρμόδια για την εκτέλεση των καθηκόντων και την άσκηση των αρμοδιοτήτων που της έχουν ανατεθεί σύμφωνα με τον παρόντα κανονισμό στην επικράτεια του κράτους μέλους της».

Αυτό σημαίνει ότι κάθε φορά που μια παραβίαση επηρεάζει τα προσωπικά δεδομένα ατόμων σε περισσότερα του ενός κράτους μέλους και απαιτείται κοινοποίηση, ο υπεύθυνος της επεξεργασίας θα πρέπει να ενημερώσει την κυρία εποπτική αρχή.

Δ. Όροι όπου δεν απαιτείται κοινοποίηση

Το άρθρο 33 παράγραφος 1 καθιστά σαφές ότι οι παραβιάσεις που «είναι απίθανο να θέσουν σε κίνδυνο τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων» δεν απαιτούν κοινοποίηση στην εποπτική αρχή.

Για παράδειγμα η απώλεια κρυπτογραφημένων δεδομένων. Εάν τα προσωπικά δεδομένα έχουν καταστεί μη κατανοητά σε μη εξουσιοδοτημένα μέρη και όταν υπάρχουν αντίγραφα ασφαλείας, ενδέχεται να μην χρειάζεται να ειδοποιηθεί η εποπτική αρχή για παραβίαση εμπιστευτικότητας. Αυτό συμβαίνει επειδή μια τέτοια παραβίαση είναι απίθανο να θέσει σε κίνδυνο τα δικαιώματα και τις ελευθερίες των ατόμων.

Ωστόσο, η μη συμμόρφωση με το άρθρο 33 θα υφίσταται όταν ο υπεύθυνος επεξεργασίας δεν ειδοποιεί την εποπτική αρχή σε περίπτωση που τα δεδομένα δεν έχουν κρυπτογραφηθεί με ασφάλεια.

Η κρυπτογράφηση μπορεί επίσης να θεωρηθεί επί του παρόντος επαρκής από τους ειδικούς σε θέματα ασφάλειας, αλλά ενδέχεται να ξεπεραστεί στο άμεσο ή έμμεσο μέλλον, πράγμα που σημαίνει ότι είναι αμφισβητήσιμο εάν τα δεδομένα θα είναι επαρκώς κρυπτογραφημένα από το συγκεκριμένο προϊόν και θα παρέχουν το κατάλληλο επίπεδο προστασίας.

4.4 Άρθρο 34 – Επικοινωνία με το Υποκείμενο των Δεδομένων

Ενημέρωση ατόμων

Σε ορισμένες περιπτώσεις, μαζί με την κοινοποίηση στην εποπτική αρχή, ο ΥΕ υποχρεούται επίσης να κοινοποιήσει παραβίαση στα άτομα που έχουν προσβληθεί. «Όταν η παραβίαση προσωπικών δεδομένων είναι πιθανό να οδηγήσει σε υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο ΥΕ ενημερώνει το υποκείμενο των δεδομένων χωρίς αδικαιολόγητη καθυστέρηση» [Άρθρο34(1)].

Ο ΓΚΠΔ αναφέρει ότι η επικοινωνία μιας παραβίασης σε άτομα πρέπει να γίνει «χωρίς αδικαιολόγητη καθυστέρηση». Ανάλογα με τη φύση της παραβίασης και τον κίνδυνο που δημιουργείται, η έγκαιρη επικοινωνία θα βοηθήσει τα άτομα να λάβουν μέτρα για να προστατευθούν από τυχόν αρνητικές συνέπειες της παραβίασης.

Πληροφορίες που πρέπει να παρέχονται

Ο ΥΕ θα πρέπει τουλάχιστον να παρέχει τις ακόλουθες πληροφορίες [Άρθρο 33(3)]:

- περιγραφή της παραβίασης,

- το όνομα και τα στοιχεία επικοινωνίας του Υπεύθυνου Προστασίας Δεδομένων ή άλλου σημείου επαφής,
- περιγραφή των πιθανών συνεπειών της παραβίασης και
- περιγραφή των μέτρων που ελήφθησαν ή προτείνονται από τον ΥΕ για την αντιμετώπιση της παραβίασης, συμπεριλαμβανομένων των, κατά περίπτωση, μέτρων για τον μετριασμό των πιθανών δυσμενών επιπτώσεών.

Επαφή με τα άτομα

Καταρχήν, η σχετική παράβαση θα πρέπει να κοινοποιείται απευθείας στα άμεσα θιγόμενα πρόσωπα, εκτός εάν κάτι τέτοιο συνεπάγεται δυσανάλογη προσπάθεια.

Η ΟΕ29 συνιστά στους ΥΕ να επιλέγουν ένα μέσο που να μεγιστοποιεί την πιθανότητα σωστής επικοινωνίας πληροφοριών σε όλα τα άτομα που έχουν προσβληθεί. Ανάλογα με τις περιστάσεις, αυτό μπορεί να σημαίνει ότι ο ΥΕ χρησιμοποιεί διάφορες μεθόδους επικοινωνίας, σε αντίθεση με τη χρήση ενός μοναδικού καναλιού επαφής. Παραδείγματα τέτοιων μεθόδων επικοινωνίας περιλαμβάνουν άμεση ανταλλαγή μηνυμάτων (π.χ. ηλεκτρονικό ταχυδρομείο, SMS, άμεσο μήνυμα), εμφανή διαφημιστικά banners ή ειδοποιήσεις, ταχυδρομικές επικοινωνίες και εμφανείς καταχωρήσεις σε έντυπα μέσα.

Όροι όπου δεν απαιτείται κοινοποίηση

- Ο ΥΕ έχει εφαρμόσει τα κατάλληλα τεχνικά και οργανωτικά μέτρα για την προστασία των δεδομένων προσωπικού χαρακτήρα πριν από την παραβίαση, ιδίως τα μέτρα που καθιστούν τα προσωπικά δεδομένα ακατανόητα σε κάθε άτομο που δεν έχει εξουσιοδότηση πρόσβασης.
- Αμέσως μετά από παραβίαση, ο ΥΕ έλαβε μέτρα για να εξασφαλίσει ότι ο υψηλός κίνδυνος που τίθεται για τα δικαιώματα και τις ελευθερίες των ατόμων δεν είναι πλέον πιθανό να υλοποιηθεί.
- Αν θα συνεπαγόταν δυσανάλογη προσπάθεια για να έλθει σε επαφή με άτομα, των οποίων τα στοιχεία επικοινωνίας έχουν χαθεί ως αποτέλεσμα της παραβίασης ή δεν είναι γνωστά από την αρχή.

Εάν η εποπτική αρχή κρίνει ότι η δεν είναι βάσιμη η απόφαση του ΥΕ να μην κοινοποιήσει τα πρόσωπα στα οποία αναφέρονται τα δεδομένα, μπορεί να εξετάσει το ενδεχόμενο χρησιμοποίησης των διαθέσιμων εξουσιών και κυρώσεων.

4.5 Εκτίμηση Κινδύνου και Υψηλού Κινδύνου

Μόλις γίνει αντιληπτή μια παραβίαση, είναι κρίσιμο ο ΥΕ όχι μόνο να επιδιώξει να περιορίσει το περιστατικό, αλλά και να εκτιμήσει τον κίνδυνο που θα μπορούσε να προκληθεί από αυτό. Υπάρχουν δύο σημαντικοί λόγοι: πρώτον, η γνώση των πιθανών επιπτώσεων στο άτομο θα βοηθήσει τον υπεύθυνο επεξεργασίας να λάβει αποτελεσματικά μέτρα για να περιορίσει και να αντιμετωπίσει την παραβίαση και δεύτερον, θα βοηθήσει να καθορίσει εάν απαιτείται κοινοποίηση στην εποπτική αρχή και, ενδεχομένως, στους ενδιαφερόμενους.

Είναι πιθανό να οδηγήσουν σε υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των ατόμων. Όταν η παραβίαση περιλαμβάνει προσωπικά δεδομένα που αποκαλύπτουν φυλετική ή εθνοτική καταγωγή, πολιτική άποψη, θρησκεία ή φιλοσοφικές πεποιθήσεις ή μέλη συνδικαλιστικών οργανώσεων ή περιλαμβάνουν γενετικά δεδομένα, δεδομένα σχετικά με την υγεία ή δεδομένα σχετικά με τη σεξουαλική ζωή ή ποινικές καταδίκες και αδικήματα, αυτή η βλάβη θα πρέπει να θεωρείται πιθανή.

Κατά την εκτίμηση του κινδύνου πρέπει γενικά να λαμβάνεται υπόψη τόσο η πιθανότητα όσο και η σοβαρότητα του κινδύνου για τα δικαιώματα και τις ελευθερίες των προσώπων στα οποία αναφέρονται τα δεδομένα.

Κατά την εκτίμηση του κινδύνου, ένας βασικός παράγοντας είναι ο τύπος και η ευαισθησία των προσωπικών δεδομένων που έχει υπονομευτεί από την παραβίαση. Συνήθως, όσο πιο ευαίσθητα είναι τα δεδομένα, τόσο μεγαλύτερος είναι ο κίνδυνος βλάβης για τους θιγόμενους, αλλά θα πρέπει επίσης να ληφθούν υπόψη άλλα προσωπικά δεδομένα που ενδέχεται να είναι ήδη διαθέσιμα για το υποκείμενο των δεδομένων. Για παράδειγμα, η αποκάλυψη του ονόματος και της διεύθυνσης ενός ατόμου υπό κανονικές συνθήκες είναι απίθανο να προκαλέσει σημαντική ζημία. Ωστόσο, εάν το όνομα και η διεύθυνση ενός θετού γονέα αποκαλυφθούν στον φυσιολογικό γονέα, οι συνέπειες θα μπορούσαν να είναι πολύ σοβαρές τόσο για τον θετό γονέα όσο και για το παιδί.

Ένας άλλος σημαντικός παράγοντας που πρέπει να εξεταστεί είναι πόσο εύκολο θα είναι για κάποιον που έχει πρόσβαση σε «κλεμμένα» προσωπικά δεδομένα να εντοπίσει συγκεκριμένα άτομα ή να ταιριάξει τα δεδομένα με άλλες πληροφορίες για να εντοπίσει άτομα. Όπως προαναφέρθηκε, τα προσωπικά δεδομένα που προστατεύονται από ένα κατάλληλο επίπεδο κρυπτογράφησης θα είναι ακατανόητα για μη εξουσιοδοτημένα άτομα χωρίς το κλειδί αποκρυπτογράφησης. Η ψευδωνυμοποίηση, κατά την οποία ένα ψευδώνυμο επιτρέπει να συνδέονται τα δεδομένα με ένα συγκεκριμένο άτομο χωρίς να αναγνωρίζεται το άτομο, μπορεί να μειώσει την πιθανότητα ταυτοποίησης ατόμων σε περίπτωση παραβίασης.

Ανάλογα με τη φύση των προσωπικών δεδομένων που εμπλέκονται σε παραβίαση, η ενδεχόμενη βλάβη των ατόμων που μπορεί να προκληθεί μπορεί να είναι ιδιαίτερα σοβαρή, ιδίως όταν η παραβίαση μπορεί να οδηγήσει σε κλοπή ταυτότητας ή απάτη, ψυχολογική βλάβη, ταπείνωση ή βλάβη της φήμης.

Η παραβίαση ενδέχεται να επηρεάσει τα προσωπικά δεδομένα που αφορούν τα παιδιά ή άλλα ευάλωτα άτομα, τα οποία ενδέχεται να διατρέχουν μεγαλύτερο κίνδυνο.

Μια παραβίαση μπορεί να επηρεάσει μόνο ένα ή λίγα άτομα ή αρκετές χιλιάδες, αν όχι πολύ περισσότερα. Γενικά, όσο μεγαλύτερος είναι ο αριθμός των ατόμων που επηρεάζονται, τόσο μεγαλύτερος είναι ο αντίκτυπος μιας παραβίασης. Ωστόσο, μια παραβίαση μπορεί να έχει σοβαρές επιπτώσεις ακόμη και σε ένα άτομο, ανάλογα με τη φύση και το πλαίσιο των προσωπικών δεδομένων που έχουν παραβιαστεί.

Η φύση και ο ρόλος του ΥΕ και οι δραστηριότητές του ενδέχεται να επηρεάσουν το επίπεδο κινδύνου για τα άτομα ως αποτέλεσμα παραβίασης. Για παράδειγμα, ένας ιατρικός οργανισμός θα επεξεργαστεί ειδικές κατηγορίες προσωπικών δεδομένων, πράγμα που σημαίνει ότι υπάρχει μεγαλύτερη απειλή για τα άτομα εάν παραβιαστούν τα προσωπικά τους δεδομένα, σε σύγκριση με μια λίστα αλληλογραφίας μιας εφημερίδας.

Επομένως, κατά την εκτίμηση του κινδύνου που ενδέχεται να προκύψει από παραβίαση, ο Υπεύθυνος της Επεξεργασίας πρέπει να εξετάσει το συνδυασμό της σοβαρότητας του δυνητικού αντίκτυπου στα δικαιώματα και τις ελευθερίες των ατόμων και την πιθανότητα εμφάνισής τους. Σαφώς, όπου οι συνέπειες μιας παραβίασης είναι πιο σοβαρές, ο κίνδυνος είναι υψηλότερος και παρομοίως, όπου η πιθανότητα να συμβεί είναι μεγαλύτερη, αυξάνεται και ο κίνδυνος.

Ο Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) της Ευρωπαϊκής Ένωσης έχει εκδώσει συστάσεις (ENISA, 2009) για τη μεθοδολογία εκτίμησης της σοβαρότητας μιας παραβίασης, τις οποίες οι ΥΕ και οι ΕΕ μπορεί να βρουν χρήσιμες κατά το σχεδιασμό του πλάνου αντιμετώπισης της διαχείρισης παραβιάσεων.

5

Κατευθυντήριες Γραμμές για την Επεξεργασία Δεδομένων των Εργαζομένων (WP249, 2017)

5.1 Εισαγωγή

Η ταχεία υιοθέτηση νέων τεχνολογιών πληροφόρησης στον χώρο εργασίας, όσον αφορά την υποδομή, τις εφαρμογές και τις έξυπνες συσκευές, επιτρέπει τη δημιουργία νέων τύπων συστηματικής και ενδεχομένως επεμβατικής επεξεργασίας δεδομένων στην εργασία. Για παράδειγμα:

- οι τεχνολογίες που επιτρέπουν την επεξεργασία δεδομένων στην εργασία μπορούν τώρα να υλοποιηθούν σε ένα κλάσμα του κόστους σε σχέση με πριν από μερικά χρόνια, ενώ η ικανότητα επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αυτές τις τεχνολογίες έχει αυξηθεί εκθετικά,
- οι νέες μορφές επεξεργασίας, όπως εκείνες που αφορούν τα προσωπικά δεδομένα σχετικά με τη χρήση ηλεκτρονικών υπηρεσιών ή/και δεδομένων θέσης από μια έξυπνη συσκευή, είναι πολύ λιγότερο ορατές στους εργαζομένους από άλλες πιο παραδοσιακές μορφές, όπως οι εμφανείς κάμερες CCTV. Αυτό εγείρει ερωτήματα σχετικά με το βαθμό στον οποίο οι εργαζόμενοι γνωρίζουν τις τεχνολογίες αυτές, δεδομένου ότι οι εργοδότες θα μπορούσαν να εφαρμόσουν παράνομα αυτή τη επεξεργασία χωρίς προηγούμενη ειδοποίηση προς τους εργαζομένους, και
- τα όρια μεταξύ οικίας και εργασίας έχουν γίνει όλο και πιο ασαφή. Για παράδειγμα, όταν οι εργαζόμενοι εργάζονται εξ αποστάσεως (π.χ. από το σπίτι) ή ενώ ταξιδεύουν για επαγγελματικούς σκοπούς, μπορεί να παρακολουθούνται οι δραστηριότητες του εκτός του

φυσικού εργασιακού περιβάλλοντος και μπορεί ενδεχομένως να περιλαμβάνει παρακολούθηση του ατόμου σε ιδιωτικό πλαίσιο.

Παρόλο που η χρήση τέτοιων τεχνολογιών μπορεί να βοηθήσει στην ανίχνευση ή στην πρόληψη της απώλειας της πνευματικής και υλικής ιδιοκτησίας της εταιρείας, στη βελτίωση της παραγωγικότητας των εργαζομένων και στην προστασία των προσωπικών δεδομένων για τα οποία είναι υπεύθυνος ο ΥΕ, δημιουργούνται επίσης σημαντικές προκλήσεις για την προστασία της ιδιωτικής ζωής και των προσωπικών δεδομένων των εργαζομένων.

Ως «υπάλληλοι» δεν νοούνται μόνο άτομα με σύμβαση εργασίας αναγνωρισμένη ως τέτοια βάσει της ισχύουσας εργατικής νομοθεσίας. Τις τελευταίες δεκαετίες, τα νέα επιχειρηματικά μοντέλα που εξυπηρετούνται από διαφορετικούς τύπους εργασιακών σχέσεων και, ιδίως από την ελεύθερη εργασία, έχουν γίνει πιο συνηθισμένα. Οι Κατευθυντήριες Γραμμές για την Επεξεργασία Δεδομένων των Εργαζομένων (WP249, 2017) στοχεύουν να καλύψουν όλες τις περιπτώσεις στις οποίες υφίσταται σχέση εργασίας, ανεξάρτητα από το αν η σχέση αυτή βασίζεται σε σύμβαση εργασίας.

Οι εργαζόμενοι σπάνια είναι σε θέση να αρνηθούν ή να ανακαλέσουν τη συγκατάθεσή τους, δεδομένης της εξάρτησης που προκύπτει από τη σχέση εργοδότη / εργαζομένου. Εκτός από εξαιρετικές καταστάσεις, οι εργοδότες θα πρέπει να βασίζονται σε ένα άλλο νομικό πλαίσιο παρά στη συγκατάθεση – όπως η ανάγκη επεξεργασίας των δεδομένων για το νόμιμο συμφέρον τους. Ωστόσο, ένα νόμιμο συμφέρον από μόνο του δεν επαρκεί για να παρακάμψει τα δικαιώματα και τις ελευθερίες των εργαζομένων.

Τα μέτρα που πρέπει να ληφθούν για να διασφαλιστεί η ιδιωτική ζωή, το απόρρητο των επικοινωνιών καθώς και ότι οι παραβιάσεις των δικαιωμάτων περιορίζονται στο ελάχιστο, μπορεί να αποτελέσουν μέρος μιας Εκτίμησης Αντικτύπου Προστασίας Δεδομένων (ΕΑΠΔ).

5.2 Νομικό Πλαίσιο

Συνοπτικά, οι εργοδότες πρέπει να λάβουν υπόψη τα ακόλουθα [Άρθρα 7 & 8]:

- για την πλειονότητα των επεξεργασιών δεδομένων στην εργασία, η νομική βάση δεν μπορεί και δεν πρέπει να είναι η συναίνεση των εργαζομένων [Άρθρο 7 (α)] λόγω της φύσης της σχέσης μεταξύ εργοδότη και εργαζομένου,
- η επεξεργασία μπορεί να είναι αναγκαία για την εκτέλεση μιας σύμβασης [Άρθρο 7 (β)] σε περιπτώσεις όπου ο εργοδότης πρέπει να επεξεργάζεται δεδομένα προσωπικού χαρακτήρα του εργαζομένου για την εκπλήρωση των υποχρεώσεων αυτών,
- το εργατικό δίκαιο μπορεί να επιβάλλει νομικές υποχρεώσεις [άρθρο 7 (γ)] που απαιτούν την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Σε τέτοιες περιπτώσεις ο εργαζόμενος πρέπει να είναι σαφώς και πλήρως ενημερωμένος σχετικά με την επεξεργασία αυτή (εκτός αν ισχύει εξαίρεση),
- σε περίπτωση που ένας εργοδότης επιδιώκει να στηριχθεί σε έννομο συμφέρον [Άρθρο 7(στ)], ο σκοπός της επεξεργασίας πρέπει να είναι νόμιμος, η επιλεγείσα μέθοδος ή τεχνολογία πρέπει να είναι αναγκαία, αναλογική και να εφαρμόζεται με τον λιγότερο παρεμβατικό τρόπο, παράλληλα με την ικανότητα του εργοδότη να αποδείξει ότι έχουν

ληφθεί τα κατάλληλα μέτρα για την εξασφάλιση ισορροπίας με τα θεμελιώδη δικαιώματα και τις ελευθερίες των εργαζομένων,

- οι διαδικασίες επεξεργασίας πρέπει επίσης να πληρούν τις απαιτήσεις διαφάνειας [Άρθρα 10 και 11] και οι εργαζόμενοι πρέπει να είναι σαφώς και πλήρως ενημερωμένοι για την επεξεργασία των προσωπικών τους δεδομένων, συμπεριλαμβανομένης της ύπαρξης οιασδήποτε παρακολούθησης και
- θα πρέπει να ληφθούν κατάλληλα τεχνικά και οργανωτικά μέτρα για την ασφάλεια της επεξεργασίας [άρθρο 17].

Τα πιο σχετικά κριτήρια βάσει του άρθρου 7 αναλύονται παρακάτω.

Η ΟΕ29 έχει περιγράψει προηγουμένως στη γνωμοδότηση 8/2001 ότι όταν ένας εργοδότης πρέπει να επεξεργάζεται δεδομένα προσωπικού χαρακτήρα των υπαλλήλων του είναι παραπλανητικό να ξεκινάμε με την υπόθεση ότι η επεξεργασία μπορεί να νομιμοποιηθεί με τη συναίνεση των εργαζομένων. Έτσι, για την πλειοψηφία των περιπτώσεων επεξεργασίας δεδομένων προσωπικού χαρακτήρα, η νομική βάση αυτής της επεξεργασίας δεν μπορεί και δεν πρέπει να είναι η συγκατάθεση των εργαζομένων, επομένως απαιτείται διαφορετική νομική βάση.

- Εκτέλεση σύμβασης [Άρθρο 7 (β)]. Οι σχέσεις εργασίας συχνά βασίζονται σε σύμβαση εργασίας μεταξύ του εργοδότη και του εργαζομένου. Κατά την εκπλήρωση των υποχρεώσεων που απορρέουν από την σύμβαση, όπως η καταβολή του μισθού, ο εργοδότης υποχρεούται να επεξεργάζεται ορισμένα προσωπικά δεδομένα.
- Νομικές υποχρεώσεις [Άρθρο 7 (γ)]. Το εργατικό δίκαιο επιβάλλει στον εργοδότη νομικές υποχρεώσεις, οι οποίες απαιτούν την επεξεργασία δεδομένων προσωπικού χαρακτήρα (π.χ. για τον υπολογισμό του φόρου και τη διαχείριση μισθών). Είναι σαφές ότι σε τέτοιες περιπτώσεις ένας τέτοιος νόμος αποτελεί τη νομική βάση για την επεξεργασία δεδομένων.
- Δικαιολογημένο συμφέρον [Άρθρο 7 (στ)]. Ο σκοπός της επεξεργασίας πρέπει να είναι νόμιμος και η επιλεγείσα μέθοδος ή η συγκεκριμένη τεχνολογία με την οποία πρόκειται να διεξαχθεί η επεξεργασία, πρέπει να είναι αναγκαία για το νόμιμο συμφέρον του εργοδότη. Η επεξεργασία πρέπει επίσης να είναι ανάλογη με τις επιχειρηματικές ανάγκες, δηλ. τον σκοπό, που προορίζεται.

Οι απαιτήσεις διαφάνειας των άρθρων 10 και 11 ισχύουν για την επεξεργασία δεδομένων κατά την εργασία. Οι υπάλληλοι πρέπει να ενημερώνονται για την ύπαρξη τυχόν παρακολούθησης, τους σκοπούς για τους οποίους πρέπει να διεκπεραιώνονται τα δεδομένα προσωπικού χαρακτήρα και οποιεσδήποτε άλλες πληροφορίες είναι απαραίτητες για την εξασφάλιση δίκαιης μεταχείρισης.

Με τις νέες τεχνολογίες, η ανάγκη για διαφάνεια γίνεται πιο εμφανής, καθώς καθιστά δυνατή τη συλλογή και περαιτέρω επεξεργασία ενδεχομένως τεράστιων ποσοτήτων προσωπικών δεδομένων με συγκεκαλυμμένο τρόπο.

Το άρθρο 15 παρέχει επίσης στα πρόσωπα στα οποία αναφέρονται τα δεδομένα το δικαίωμα να μην υπόκεινται σε απόφαση βασιζόμενη αποκλειστικά στην αυτοματοποιημένη επεξεργασία

όταν η απόφαση παράγει έννομα αποτελέσματα ή επηρεάζει σημαντικά τα ίδια και η οποία βασίζεται αποκλειστικά στην αυτοματοποιημένη επεξεργασία δεδομένων που αποσκοπούν στην εκτίμηση ορισμένων προσωπικών στοιχείων , όπως η απόδοση στην εργασία, εκτός εάν η απόφαση είναι αναγκαία για τη σύναψη ή την εκτέλεση μιας σύμβασης, η οποία επιτρέπεται από το δίκαιο της Ένωσης ή του κράτους μέλους ή βασίζεται στη ρητή συγκατάθεση του υποκειμένου των δεδομένων.

Το άρθρο 88 του ΓΚΠΔ ορίζει ότι τα κράτη μέλη μπορούν να προβλέπουν, μέσω νόμου ή συλλογικών συμβάσεων, ειδικούς κανόνες για την εξασφάλιση της προστασίας των δικαιωμάτων και των ελευθεριών όσον αφορά την επεξεργασία των προσωπικών δεδομένων των εργαζομένων στο πλαίσιο της απασχόλησης. Ειδικότερα, οι κανόνες αυτοί μπορούν να παρέχονται για σκοπούς όπως η:

- πρόσληψη,
- εκτέλεση της σύμβασης εργασίας (συμπεριλαμβανομένης της εκπλήρωσης υποχρεώσεων που προβλέπονται από το νόμο ή από τις συλλογικές συμβάσεις),
- διαχείριση, σχεδιασμός και οργάνωση της εργασίας,
- ισότητα και ποικιλομορφία στον χώρο εργασίας,
- υγεία και ασφάλεια στην εργασία,
- προστασία της περιουσίας του εργοδότη ή του πελάτη,
- άσκηση (σε ατομική βάση) δικαιωμάτων και παροχών που σχετίζονται με την απασχόληση και
- λήξη της εργασιακής σχέσης.

Σύμφωνα με το άρθρο 88 παράγραφος 2, οι κανόνες αυτοί πρέπει να περιλαμβάνουν κατάλληλα και ειδικά μέτρα για τη διασφάλιση της ανθρώπινης αξιοπρέπειας, των θεμιτών συμφερόντων και των θεμελιωδών δικαιωμάτων του υποκειμένου των δεδομένων, ιδίως όσον αφορά:

- τη διαφάνεια της επεξεργασίας,
- τη διαβίβαση δεδομένων προσωπικού χαρακτήρα εντός ομάδας επιχειρήσεων ή ομίλου επιχειρήσεων που ασκούν κοινή οικονομική δραστηριότητα και
- συστήματα παρακολούθησης στο χώρο εργασίας

Η Ομάδα Εργασίας του Άρθρου 29 προσδιόρισε κατευθυντήριες γραμμές για τη νόμιμη χρήση της νέας τεχνολογίας σε ορισμένες ειδικές καταστάσεις, παρέχοντας λεπτομερή και ειδικά μέτρα για τη διαφύλαξη της ανθρώπινης αξιοπρέπειας, του νόμιμου συμφέροντος και των θεμελιωδών δικαιωμάτων των εργαζομένων.

5.3 Κίνδυνοι

Οι σύγχρονες τεχνολογίες επιτρέπουν την παρακολούθηση των εργαζομένων με την πάροδο του χρόνου, σε όλους τους χώρους εργασίας και τα σπίτια τους, μέσω πολλών διαφορετικών συσκευών, όπως smartphones, επιτραπέζιους υπολογιστές, tablet, οχήματα και φορητά. Εάν δεν υπάρχουν όρια στην επεξεργασία και εάν δεν είναι διαφανής, υπάρχει υψηλός κίνδυνος το νόμιμο

συμφέρον των εργοδοτών να βελτιώσουν την αποτελεσματικότητα και την προστασία των περιουσιακών στοιχείων της εταιρείας να μετατραπεί σε αδικαιολόγητο και παρεμβατικό έλεγχο.

Οι τεχνολογίες που παρακολουθούν τις επικοινωνίες μπορούν επίσης να επηρεάσουν τα θεμελιώδη δικαιώματα των εργαζομένων (συμπεριλαμβανομένου του δικαιώματος αναζήτησης πληροφοριών).

Η αύξηση του αριθμού των δεδομένων που παράγονται στο περιβάλλον εργασίας, σε συνδυασμό με νέες τεχνικές ανάλυσης δεδομένων και διασταυρούμενης επεξεργασίας, μπορεί επίσης να δημιουργήσει κινδύνους μη συμβατής περαιτέρω επεξεργασίας.

Ως αποτέλεσμα, η παρακολούθηση αυτή ενδέχεται να παραβιάζει τα δικαιώματα ιδιωτικού απορρήτου των εργαζομένων, ανεξάρτητα από το εάν η παρακολούθηση πραγματοποιείται συστηματικά ή περιστασιακά.

Η εκτεταμένη χρήση των τεχνολογιών παρακολούθησης ενδέχεται επίσης να περιορίσει την προθυμία των εργαζομένων (και τα κανάλια με τα οποία θα μπορούσαν) να ενημερώσουν τους εργοδότες σχετικά με τις παρατυπίες ή τις παράνομες ενέργειες ανώτερων και / ή άλλων εργαζομένων που απειλούν να βλάψουν την επιχείρηση (ιδίως τα δεδομένα πελατών) ή τον χώρο εργασίας. Η ανωνυμία είναι συχνά απαραίτητη προκειμένου ένας ευσυνείδητος υπάλληλος να αναλάβει δράση και να αναφέρει τέτοιες καταστάσεις.

5.4 Συμπεράσματα και προτάσεις

Κατά την επεξεργασία των προσωπικών δεδομένων των εργαζομένων:

- οι εργοδότες πρέπει πάντα να λαμβάνουν υπόψη τις θεμελιώδεις αρχές προστασίας δεδομένων, ανεξάρτητα από την χρησιμοποιούμενη τεχνολογία,
- το περιεχόμενο των ηλεκτρονικών επικοινωνιών που προέρχονται από επαγγελματικούς χώρους πρέπει να έχει το ίδιο επίπεδο προστασίας με τις αναλογικές επικοινωνίες,
- η συγκατάθεση είναι εξαιρετικά απίθανο να αποτελέσει νομική βάση για την επεξεργασία δεδομένων στην εργασία, εκτός εάν οι εργαζόμενοι μπορούν να αρνηθούν χωρίς δυσμενείς συνέπειες,
- στο πλαίσιο της εκτέλεσης σύμβασης ή/και νόμιμων συμφερόντων, εφόσον η επεξεργασία είναι απολύτως απαραίτητη για νόμιμο σκοπό και είναι σύμφωνη με την αρχή της αναλογικότητας,
- οι εργαζόμενοι πρέπει να λαμβάνουν αποτελεσματικές πληροφορίες σχετικά με την παρακολούθηση που πραγματοποιείται και
- οποιαδήποτε διεθνή διαβίβαση δεδομένων προσωπικού χαρακτήρα θα πρέπει να πραγματοποιείται μόνο εφόσον εξασφαλίζεται επαρκές επίπεδο προστασίας.

Πρέπει να παρέχεται στους υπαλλήλους αποτελεσματική επικοινωνία σχετικά με κάθε παρακολούθηση που πραγματοποιείται, τους σκοπούς αυτής της παρακολούθησης και τις περιστάσεις, καθώς και τις δυνατότητες των εργαζομένων να αποτρέπουν την καταγραφή των δεδομένων τους από τεχνολογίες παρακολούθησης. Οι πολιτικές και οι κανόνες σχετικά με τη

νόμιμη παρακολούθηση πρέπει να είναι σαφείς και εύκολα προσβάσιμοι. Η Ομάδα Εργασίας συνιστά τη συμμετοχή αντιπροσωπευτικού δείγματος εργαζομένων στη δημιουργία και αξιολόγηση τέτοιων κανόνων και πολιτικών, καθώς η μεγαλύτερη παρακολούθηση έχει τη δυνατότητα να παραβιάζει την ιδιωτική ζωή των εργαζομένων.

Η επεξεργασία δεδομένων στην εργασία πρέπει να αποτελεί αναλογική απάντηση στους κινδύνους που αντιμετωπίζει ένας εργοδότης. Για παράδειγμα, η κατάχρηση του διαδικτύου μπορεί να ανιχνευθεί χωρίς την αναγκαιότητα ανάλυσης του περιεχομένου (π.χ., χρησιμοποιώντας φίλτρα ιστού).

Η χρήση των περισσότερων εφαρμογών στο σύννεφο θα έχει ως αποτέλεσμα τη διεθνή μεταφορά δεδομένων των εργαζομένων. Πρέπει να διασφαλιστεί ότι τα δεδομένα προσωπικού χαρακτήρα που μεταφέρονται σε τρίτη χώρα εκτός της ΕΕ πραγματοποιούνται μόνο όταν εξασφαλίζεται επαρκές επίπεδο προστασίας και ότι τα δεδομένα που είναι κοινά εκτός ΕΕ / ΕΟΧ και η επακόλουθη πρόσβαση από άλλες οντότητες εντός του ομίλου παραμένει περιορισμένη στο ελάχιστο αναγκαία για τους επιδιωκόμενους σκοπούς.

6

Κατευθυντήριες Γραμμές για την Αυτοματοποιημένη Λήψη Αποφάσεων και τη Δημιουργία Προφίλ (WP251, 2017)

6.1 Εισαγωγή

Η χρήση προφίλ και η αυτοματοποιημένη λήψη αποφάσεων χρησιμοποιούνται σε έναν αυξανόμενο αριθμό τομέων, τόσο ιδιωτικών όσο και δημόσιων. Οι Τράπεζες με τα συστήματα KYC (Know Your Customer) για τις χρηματοδοτήσεις, η υγειονομική περίθαλψη, η φορολογία, η ασφάλιση, το μάρκετινγκ και η διαφήμιση είναι μόνο μερικά παραδείγματα των τομέων στους οποίους πραγματοποιείται η τακτική κατάρτιση προφίλ για την υποστήριξη της λήψης αποφάσεων.

Οι πρόοδοι στην τεχνολογία και οι δυνατότητες των μεγάλων αναλυτικών δυνατοτήτων, της τεχνητής νοημοσύνης και της μηχανικής μάθησης έχουν διευκολύνει τη δημιουργία προφίλ και τη λήψη αυτοματοποιημένων αποφάσεων με δυνατότητες να επηρεάσουν σημαντικά τα δικαιώματα και τις ελευθερίες των ατόμων.

Η αυξημένη διαθεσιμότητα προσωπικών δεδομένων στο Διαδίκτυο και από συσκευές Διαδικτύου των Πραγμάτων (Internet of Things - IoT), καθώς και η δυνατότητα συσχέτισης και δημιουργίας συνδέσμων, μπορούν να καθορίσουν, να αναλύσουν και να προβλέψουν πτυχές της προσωπικότητας ή της συμπεριφοράς, των συμφερόντων και των συνηθειών ενός ατόμου.

Η επεξεργασία και η αυτοματοποιημένη λήψη αποφάσεων μπορεί να είναι χρήσιμη τόσο για τα άτομα όσο και για τους οργανισμούς καθώς και για την οικονομία και την κοινωνία ως σύνολο, παρέχοντας οφέλη όπως αυξημένη αποτελεσματικότητα και εξοικονόμηση πόρων.

Έχουν πολλές εμπορικές εφαρμογές, για παράδειγμα, μπορούν να χρησιμοποιηθούν για την καλύτερη κατανομή των αγορών και την προσαρμογή των υπηρεσιών και των προϊόντων ώστε να ευθυγραμμιστούν με τις ατομικές ανάγκες. Η ιατρική, η εκπαίδευση, η υγειονομική περίθαλψη και οι μεταφορές μπορούν επίσης να επωφεληθούν από αυτές τις διαδικασίες

Ωστόσο, η δημιουργία προφίλ και η αυτοματοποιημένη λήψη αποφάσεων μπορεί να δημιουργήσει σημαντικούς κινδύνους για τα δικαιώματα και τις ελευθερίες των ατόμων που απαιτούν κατάλληλες διασφαλίσεις.

Η δημιουργία προφίλ μπορεί να διαιωνίσει τα υπάρχοντα στερεότυπα και τον κοινωνικό διαχωρισμό. Μπορεί επίσης να κλειδώσει ένα άτομο σε μια συγκεκριμένη κατηγορία και να τα περιορίσει στις προτεινόμενες προτιμήσεις τους. Αυτό μπορεί να υπονομεύσει την ελευθερία τους να επιλέγουν, για παράδειγμα, ορισμένα προϊόντα ή υπηρεσίες, όπως βιβλία, μουσική ή κατηγορία ειδήσεων. Μπορεί να οδηγήσει σε ανακριβείς προβλέψεις, άρνηση υπηρεσιών και αγαθών και αδικαιολόγητη διάκριση σε ορισμένες περιπτώσεις.

6.2 Ορισμοί

Ο ΓΚΠΔ εισάγει διατάξεις που εξασφαλίζουν ότι η δημιουργία προφίλ και η αυτοματοποιημένη ατομική λήψη αποφάσεων (ανεξάρτητα από το αν αυτό περιλαμβάνει ή όχι το σχεδιασμό) δεν χρησιμοποιούνται με τρόπους που έχουν αδικαιολόγητη επίδραση στα δικαιώματα των ατόμων.

Προφίλ [Άρθρο 4(4)]: Κάθε μορφή αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα, ιδίως για την ανάλυση ή την πρόβλεψη πτυχών σχετικά με την απόδοση του ατόμου στην εργασία, την οικονομική κατάσταση, την υγεία, τις προσωπικές προτιμήσεις, τα συμφέροντα, την αξιοπιστία, τη συμπεριφορά, την τοποθεσία ή τις μετακινήσεις. Η προφιλοποίηση στον ΓΚΠΔ έχει τρία χαρακτηριστικά:

- πρέπει να είναι μια αυτοματοποιημένη μορφή επεξεργασίας,
- πρέπει να διεξάγεται σε δεδομένα προσωπικού χαρακτήρα και
- ο στόχος του προφίλ πρέπει να είναι η αξιολόγηση των προσωπικών πτυχών ενός φυσικού προσώπου.

Επομένως, η απλή αξιολόγηση ή ταξινόμηση των ατόμων με βάση χαρακτηριστικά όπως η ηλικία, το φύλο και το ύψος τους θα μπορούσε να θεωρηθεί ως προφίλ, ανεξάρτητα από οποιοδήποτε προγνωστικό σκοπό.

Τα τρία διακριτά στάδια του προφίλ:

- συλλογή δεδομένων·
- αυτοματοποιημένη ανάλυση για τον προσδιορισμό των συσχετισμών·
- εφαρμογή της συσχέτισης με ένα άτομο για τον προσδιορισμό των χαρακτηριστικών της παρούσας ή της μελλοντικής συμπεριφοράς.

Αυτοματοποιημένη λήψη αποφάσεων είναι η ικανότητα λήψης αποφάσεων με τεχνολογικά μέσα χωρίς ανθρώπινη συμμετοχή. Οι αυτοματοποιημένες αποφάσεις μπορούν να βασίζονται σε οποιοδήποτε τύπο δεδομένων, για παράδειγμα:

- δεδομένα που παρέχονται απευθείας από τα ενδιαφερόμενα άτομα (όπως απαντήσεις σε ερωτηματολόγιο),
- στοιχεία που έχουν παρατηρηθεί σχετικά με τα άτομα (όπως τα δεδομένα τοποθεσίας που συλλέγονται μέσω μιας αίτησης),
- ή δεδομένα όπως το προφίλ του ατόμου που έχει ήδη δημιουργηθεί (π.χ. πιστωτικό αποτέλεσμα).

Οι αυτοματοποιημένες αποφάσεις μπορούν να λαμβάνονται με ή χωρίς προφίλ, ο προσδιορισμός προφίλ μπορεί να γίνει χωρίς να ληφθούν αυτοματοποιημένες αποφάσεις. Ωστόσο, ο σχεδιασμός και η αυτοματοποιημένη λήψη αποφάσεων δεν είναι απαραίτητα ξεχωριστές δραστηριότητες. Κάτι που ξεκινάει ως μια απλή αυτοματοποιημένη διαδικασία λήψης αποφάσεων θα μπορούσε να γίνει μία με βάση το προφίλ, ανάλογα με τον τρόπο χρήσης των δεδομένων.

Παράδειγμα η επιβολή προστίμων για την υπέρβαση της ταχύτητας με βάση στοιχεία από κάμερες ταχύτητας είναι μια αυτοματοποιημένη διαδικασία λήψης αποφάσεων που δεν συνεπάγεται υποχρεωτικά τη δημιουργία προφίλ.

Θα αποτελούσε, ωστόσο, η απόφαση να είναι βασισμένη στο προφίλ του ατόμου αν παρακολουθούνταν με την πάροδο του χρόνου και το ύψος του επιβληθέντος προστίμου είναι το αποτέλεσμα μιας διαδικασίας που περιλαμβάνει και άλλους παράγοντες, όπως το κατά πόσον συχνά επαναλαμβάνεται το συγκεκριμένο αδίκημα ή αν ο οδηγός είχε άλλες πρόσφατες παραβιάσεις του ΚΟΚ.

6.3 Ειδικές διατάξεις για την αυτόματη λήψη αποφάσεων

Το άρθρο 22 παράγραφος 1 λέει ότι το υποκείμενο των δεδομένων έχει το δικαίωμα να μην υπόκειται σε απόφαση που βασίζεται αποκλειστικά στην αυτοματοποιημένη επεξεργασία, συμπεριλαμβανομένης της μορφοποίησης, η οποία παράγει έννομα αποτελέσματα για το ίδιο ή που το επηρεάζει σημαντικά.

Συνοπτικά, το άρθρο 22 προβλέπει ότι:

(i) κατά κανόνα, υπάρχει απαγόρευση πλήρως αυτοματοποιημένης ατομικής λήψης αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ που έχει νομική ή παρόμοια σημαντική επίδραση·

(ii) υπάρχουν εξαιρέσεις από τον κανόνα·

(iii) θα πρέπει να ληφθούν μέτρα για τη διασφάλιση των δικαιωμάτων και των ελευθεριών και των έννομων συμφερόντων του υποκειμένου των δεδομένων.

Αυτές οι διασφαλίσεις, που αναλύονται λεπτομερέστερα κατωτέρω, περιλαμβάνουν το δικαίωμα ενημέρωσης (που αναφέρεται στα άρθρα 13 και 14 – συγκεκριμένα σημαντικές πληροφορίες σχετικά με την επεξεργασία, καθώς και τη σημασία και τις προβλεπόμενες συνέπειες

για το υποκείμενο των δεδομένων), την παρέμβαση και το δικαίωμα προσφυγής κατά της απόφασης (που αναφέρεται στο άρθρο 22 παράγραφος 3).

Η απαγόρευση του άρθρου 22 παράγραφος 1 εφαρμόζεται μόνο όταν μια απόφαση που βασίζεται αποκλειστικά στην αυτοματοποιημένη επεξεργασία, συμπεριλαμβανομένης της μορφοποίησης, έχει νομική επίπτωση ή επηρεάζει σημαντικά κάποιον με παρόμοιο τρόπο.

Το άρθρο 22, παράγραφος 1, αναφέρεται σε αποφάσεις που «βασίζονται αποκλειστικά» στην αυτοματοποιημένη επεξεργασία. Αυτό σημαίνει ότι δεν υπάρχει ανθρώπινη συμμετοχή στη διαδικασία λήψης αποφάσεων.

Ο ΥΕ δεν μπορεί να αποφύγει τις διατάξεις του άρθρου 22 «επινοώντας» την ανθρώπινη συμμετοχή. Προκειμένου να χαρακτηριστεί ως ανθρώπινη παρέμβαση, ο ΥΕ πρέπει να διασφαλίσει ότι οποιαδήποτε εποπτεία της απόφασης είναι ουσιαστική, και όχι απλώς μια συμβολική χειρονομία.

Ακόμη και αν η διαδικασία λήψης αποφάσεων δεν έχει επίπτωση στα νόμιμα δικαιώματα των πολιτών, θα μπορούσε ακόμη να εμπίπτει στο πεδίο εφαρμογής του άρθρου 22, εάν παράγει αποτελέσματα ισοδύναμα ή παρόμοια σημαντικά όσον αφορά τον αντίκτυπό του.

Εξαιρέσεις από την απαγόρευση [Άρθρο22(2)]. Ο ΥΕ δεν πρέπει να αναλάβει την επεξεργασία που περιγράφεται στο άρθρο 22 παράγραφος 1 εκτός εάν εφαρμόζεται μία από τις ακόλουθες εξαιρέσεις:

i. η επεξεργασία είναι αναγκαία για την εκτέλεση ή τη σύναψη σύμβασης,

ii. η επεξεργασία έχει εγκριθεί από το δίκαιο της Ένωσης ή του κράτους μέλους στην οποία υπόκειται ο ΥΕ και ο οποίος έχει επίσης προβλέψει κατάλληλα μέτρα για τη διασφάλιση των δικαιωμάτων των ελευθεριών και των έννομων συμφερόντων του προσώπου στο οποίο αναφέρονται τα δεδομένα,

iii. η επεξεργασία γίνεται βάσει της ρητής συναίνεσης του υποκειμένου των δεδομένων.

6.4 Δικαιώματα του υποκειμένου των δεδομένων

Εάν ο ΥΕ λαμβάνει αυτοματοποιημένες αποφάσεις όπως περιγράφονται στο άρθρο 22 παράγραφος 1, τότε οφείλει:

- να ενημερώσει το υποκείμενο των δεδομένων ότι εμπλέκεται σε αυτό το είδος δραστηριότητας,
- να παρέχει ουσιαστικές πληροφορίες σχετικά με την «εμπλεκόμενη λογική», όπως για παράδειγμα το σκεπτικό και τα κριτήρια που βασίζεται η λήψη της απόφασης και
- να εξηγήσει τη σημασία και τις προβλεπόμενες συνέπειες της επεξεργασίας.

Η τήρηση αυτών των τριών συγκεκριμένων απαιτήσεων διαφάνειας θα βοηθήσει τους υπεύθυνους επεξεργασίας να ενημερώσουν καλύτερα τα υποκείμενα των δεδομένων σχετικά με το είδος της επεξεργασίας και τις συνέπειες [Άρθρο 22(1)].

Σημαντικές πληροφορίες σχετικά με τη «λογική που εμπλέκεται»

Η ανάπτυξη και η πολυπλοκότητα της μηχανικής μάθησης μπορεί να καταστήσει δύσκολη την κατανόηση του τρόπου με τον οποίο λειτουργεί μια αυτοματοποιημένη διαδικασία λήψης αποφάσεων ή η δημιουργία προφίλ.

6.5 Δημιουργία κατάλληλων διασφαλίσεων

Το υποκείμενο των δεδομένων θα μπορεί να αμφισβητήσει μια απόφαση ή να εκφράσει την άποψή του μόνο εάν κατανοήσει πλήρως τον τρόπο με τον οποίο έχει ληφθεί η απόφαση.

Τα σφάλματα ή η μεροληψία στη συλλογή των δεδομένων ή στην αυτοματοποιημένη διαδικασία λήψης αποφάσεων μπορεί να έχουν ως αποτέλεσμα:

- εσφαλμένες ταξινομήσεις,
- εκτιμήσεις που βασίζονται σε ανακριβείς υποθέσεις και
- να έχει αρνητικό αντίκτυπο στα άτομα.

Οι ΥΕ θα πρέπει να πραγματοποιούν συχνές αξιολογήσεις/εκτιμήσεις σχετικά με τα σύνολα δεδομένων που επεξεργάζονται και να αναπτύσσουν τρόπους αντιμετώπισης τυχόν ζημιογόνων επιπτώσεων όπως με τη χρήση συστημάτων που ελέγχουν τους αλγόριθμους της αυτοματοποιημένης λήψης αποφάσεων.

Οι υπεύθυνοι επεξεργασίας πρέπει να θεσπίσουν κατάλληλες διαδικασίες και μέτρα για την πρόληψη σφαλμάτων, ανακριβειών ή διακρίσεων. Θα πρέπει, δε, να χρησιμοποιούνται σε κυκλική βάση και όχι μόνο στο στάδιο του σχεδιασμού, αλλά συνεχώς.

6.6 Γενικές διατάξεις σχετικά με τη χάραξη προφίλ και την αυτόματη λήψη αποφάσεων

Η δημιουργία προφίλ μπορεί να περιλαμβάνει τη χρήση προσωπικών δεδομένων που συλλέχθηκαν αρχικά για άλλο σκοπό.

Το κατά πόσο αυτή η πρόσθετη επεξεργασία είναι συμβατή με τους αρχικούς σκοπούς για τους οποίους συλλέχθηκαν τα δεδομένα εξαρτάται από ένα φάσμα παραγόντων, συμπεριλαμβανομένων των πληροφοριών σχετικά με την εύλογη επεξεργασία που ο ελεγκτής παρείχε αρχικά στο υποκείμενο των δεδομένων. Αυτοί οι παράγοντες αντικατοπτρίζονται στον ΓΚΠΔ και συνοψίζονται παρακάτω:

- τη σχέση μεταξύ των σκοπών για τους οποίους συλλέχθηκαν τα δεδομένα και των σκοπών της περαιτέρω επεξεργασίας·
- το πλαίσιο στο οποίο συλλέχθηκαν τα δεδομένα και οι εύλογες προσδοκίες των υποκειμένων των δεδομένων σχετικά με την περαιτέρω χρήση τους·
- τη φύση των δεδομένων και τον αντίκτυπο της περαιτέρω επεξεργασίας στα πρόσωπα στα οποία αναφέρονται τα δεδομένα και

- τα μέτρα που εφαρμόζει ο υπεύθυνος επεξεργασίας για τη διασφάλιση της δίκαιης επεξεργασίας και την αποτροπή αδικαιολόγητων επιπτώσεων στα πρόσωπα στα οποία αναφέρονται τα δεδομένα.

Οι επιχειρηματικές ευκαιρίες που δημιουργούνται από τη δημιουργία προφίλ, το φθηνότερο κόστος αποθήκευσης και η δυνατότητα επεξεργασίας μεγάλου όγκου πληροφοριών μπορούν να ενθαρρύνουν τους οργανισμούς να συλλέγουν περισσότερα προσωπικά δεδομένα από ό,τι πραγματικά χρειάζονται. Οι ΥΕ θα πρέπει να είναι σε θέση να εξηγούν και να αιτιολογούν με σαφήνεια την ανάγκη συλλογής και κατοχής προσωπικών δεδομένων [Άρθρο 5(1)].

Εάν τα δεδομένα που χρησιμοποιούνται σε μια αυτοματοποιημένη διαδικασία λήψης αποφάσεων ή δημιουργίας προφίλ είναι ανακριβή, οποιαδήποτε τελική απόφαση ή προφίλ θα είναι εσφαλμένη. Οι αποφάσεις μπορούν να λαμβάνονται βάσει παρωχημένων δεδομένων ή εσφαλμένης ερμηνείας εξωτερικών δεδομένων. Οι υπεύθυνοι επεξεργασίας πρέπει να θεσπίσουν αυστηρά μέτρα για να επαληθεύουν και να διασφαλίζουν σε συνεχή βάση ότι τα δεδομένα που επαναχρησιμοποιούνται ή αποκτώνται έμμεσα είναι ακριβή και ενημερωμένα. Αυτό ενισχύει τη σημασία της παροχής σαφών πληροφοριών σχετικά με τα δεδομένα που επεξεργάζονται, ώστε το υποκείμενο των δεδομένων να μπορεί να διορθώσει τυχόν ανακρίβειες και να βελτιώσει την ποιότητα των δεδομένων.

Οι αλγόριθμοι εκμάθησης μηχανών σχεδιάζονται για να επεξεργάζονται μεγάλους όγκους πληροφοριών και να δημιουργούν συσχετισμούς. Η αποθήκευση δεδομένων που συλλέγονται για μεγάλες χρονικές περιόδους σημαίνει ότι οι οργανισμοί θα είναι σε θέση να δημιουργήσουν ολοκληρωμένα προφίλ των ατόμων, δεδομένου ότι θα υπάρχουν περισσότερα δεδομένα για να χρησιμοποιήσει ο αλγόριθμος. Ακόμη και αν η συλλογή των πληροφοριών πληροί τις απαιτήσεις των προδιαγραφών και της καταλληλόλητας του σκοπού, η αποθήκευση τους για μεγάλο χρονικό διάστημα μπορεί να έρχεται σε σύγκρουση με την εκτίμηση της αναλογικότητας, δηλαδή η μέθοδος μπορεί να είναι υπερβολικά παρεμβατική όσον αφορά το δικαίωμα του ατόμου στην ιδιωτική ζωή. Η διατήρηση δεδομένων προσωπικού χαρακτήρα για μεγάλο χρονικό διάστημα επίσης αυξάνει τον κίνδυνο ανακριβειών.

Οι υπεύθυνοι επεξεργασίας που επιδιώκουν να βασίζονται στη συγκατάθεση ως βάση για τη διαμόρφωση του προφίλ πρέπει να αποδείξουν ότι τα υποκείμενα των δεδομένων κατανοούν ακριβώς τι συμφωνούν. Σε όλες τις περιπτώσεις, τα υποκείμενα των δεδομένων θα πρέπει να διαθέτουν αρκετές σχετικές πληροφορίες σχετικά με την προβλεπόμενη χρήση και τις συνέπειες της επεξεργασίας, ώστε να εξασφαλίζεται ότι η συναίνεση που παρέχουν αποτελεί μια ενημερωμένη επιλογή [Άρθρο 6(1)].

Όταν το υποκείμενο των δεδομένων δεν έχει άλλη επιλογή, όπως για παράδειγμα, σε περιπτώσεις όπου η συγκατάθεση για τη δημιουργία προφίλ είναι προϋπόθεση για την πρόσβαση στις υπηρεσίες του ΥΕ ή όταν υπάρχει ανισορροπία ισχύος, όπως σε σχέση εργοδότη / εργαζομένου, η συγκατάθεση δεν αποτελεί κατάλληλη βάση για τη επεξεργασία.

Το πρόσωπο στο οποίο αναφέρονται τα δεδομένα, έχει το δικαίωμα να λαμβάνει λεπτομερή στοιχεία σχετικά με τα δεδομένα προσωπικού χαρακτήρα που χρησιμοποιούνται για τη δημιουργία προφίλ [Άρθρο 15].

6.7 Προφίλ & Εκτίμηση Αντικτύπου στην Προστασία (ΕΑΠΔ)

Ο ΥΕ οφείλει να προχωρήσει σε ΕΑΠΔ στην περίπτωση αποφάσεων που βασίζονται στην αυτοματοποιημένη επεξεργασία, συμπεριλαμβανομένου του προφίλ, με σημαντικές επιπτώσεις στο υποκείμενο των δεδομένων [Άρθρο 35(3α)]. Οι ΥΕ θα μπορούσαν να εξετάσουν πρόσθετα μέτρα όπως:

- ενημέρωση του υποκειμένου δεδομένων σχετικά με την ύπαρξη και τη λογική που εμπλέκεται στην αυτοματοποιημένη διαδικασία λήψης αποφάσεων,
- να εξηγήσουν τη σημασία και τις προβλεπόμενες συνέπειες της επεξεργασίας για το υποκείμενο των δεδομένων,
- να παρέχουν στο πρόσωπο στο οποίο αναφέρονται τα δεδομένα τα μέσα για να αντιταχθεί στην απόφαση, και
- να επιτρέπουν στο υποκείμενο των δεδομένων να εκφράσει την άποψή του.

7

Κατευθυντήριες Γραμμές για τους Υπεύθυνους Προστασίας Δεδομένων (ΥΠΔ ή DPO)

7.1 Εισαγωγή

Σύμφωνα με τον ΓΚΠΔ όλες οι δημόσιες αρχές και φορείς (ανεξάρτητα από το ποια δεδομένα επεξεργάζονται) και οι οργανισμοί που – ως κύρια δραστηριότητα – επεξεργάζονται προσωπικά δεδομένα συστηματικά και σε μεγάλη κλίμακα, υποχρεούνται να ορίσουν έναν Υπεύθυνο Προστασίας Δεδομένων-ΥΠΔ (Data Protection Officer-DPO).

Οι ΥΠΔ δεν φέρουν προσωπική ευθύνη σε περίπτωση μη συμμόρφωσης με τον ΓΚΠΔ. Ο ΓΚΠΔ καθιστά σαφές ότι ο ΥΕ ή ο ΕΕ υποχρεούται να εξασφαλίζει και να είναι σε θέση να αποδείξει ότι η επεξεργασία πραγματοποιείται σύμφωνα με τις διατάξεις του Κανονισμού [Άρθρο 24 (1)]. Η συμμόρφωση της προστασίας δεδομένων αποτελεί ευθύνη του ΥΕ ή του ΕΕ.

Ο ορισμός ενός ΥΠΔ αποτελεί ένα πρώτο βήμα, αλλά οι ΥΠΔ πρέπει επίσης να διαθέτουν επαρκή αυτονομία και πόρους για την αποτελεσματική εκτέλεση των καθηκόντων τους.

7.2 Υποχρεωτικός ορισμός ΥΠΔ

Το άρθρο 37 παράγραφος 1 του ΓΚΠΔ απαιτεί τον ορισμό ενός ΥΠΔ σε τρεις ειδικές περιπτώσεις:

i. όταν η επεξεργασία πραγματοποιείται από δημόσια αρχή ή οργανισμό,

ii. όταν οι βασικές δραστηριότητες του ΥΕ ή του ΕΕ συνίστανται σε εργασίες επεξεργασίας, οι οποίες απαιτούν τακτική και συστηματική παρακολούθηση των δεδομένων των υποκειμένων σε μεγάλη κλίμακα,

iii. όταν οι βασικές δραστηριότητες του ΥΕ ή του ΕΕ συνίστανται σε επεξεργασία μεγάλης κλίμακας ειδικών κατηγοριών δεδομένων ή δεδομένα που αφορούν ποινικές καταδίκες και αδικήματα.

Ο ΓΚΠΔ δεν ορίζει τι συνιστά «δημόσια αρχή ή οργανισμό». Η ΟΕ29 θεωρεί ότι μια τέτοια έννοια πρέπει να καθορίζεται από το εθνικό δίκαιο. Οι δημόσιες αρχές και οι οργανισμοί περιλαμβάνουν εθνικές, περιφερειακές και τοπικές αρχές, αλλά η έννοια, σύμφωνα με την ισχύουσα εθνική νομοθεσία, περιλαμβάνει κατά κανόνα και σειρά άλλων οργανισμών Δημοσίου Δικαίου. Στις περιπτώσεις αυτές, ο καθορισμός ενός ΥΠΔ είναι υποχρεωτικός.

Οι «βασικές δραστηριότητες» μπορούν να θεωρηθούν ως οι βασικές λειτουργίες που απαιτούνται για την επίτευξη των στόχων του ΥΕ ή του ΕΕ.

Ωστόσο, οι «βασικές δραστηριότητες» δεν πρέπει να ερμηνεύονται ως δραστηριότητες στις οποίες η επεξεργασία δεδομένων δεν αποτελεί αναπόσπαστο μέρος των εργασιών του ΥΕ ή του ΕΕ. Για παράδειγμα, η βασική δραστηριότητα ενός νοσοκομείου είναι η παροχή υγειονομικής περίθαλψης. Ωστόσο, ένα νοσοκομείο δεν θα μπορούσε να παράσχει υγειονομική περίθαλψη με ασφάλεια και αποτελεσματικότητα χωρίς επεξεργασία δεδομένων υγείας, όπως τα αρχεία υγείας των ασθενών. Ως εκ τούτου, επεξεργασία αυτών τα δεδομένων πρέπει να θεωρείται ως μία από τις βασικές δραστηριότητες του νοσοκομείου και επομένως πρέπει να ορισθεί ΥΠΔ.

Ο ΓΚΠΔ δεν καθορίζει τι συνιστά «μεγάλη κλίμακα». Δεν είναι δυνατόν να δοθεί ακριβής αριθμός όσον αφορά το μέγεθος των δεδομένων που υποβλήθηκαν σε επεξεργασία ή τον αριθμό των ενδιαφερομένων. Αυτό δεν αποκλείει, ωστόσο, την πιθανότητα να αναπτυχθεί με την πάροδο του χρόνου μια τυποποιημένη πρακτική για τον ακριβή ποσοτικό προσδιορισμό του τι συνιστά «μεγάλη κλίμακα» όσον αφορά ορισμένες μορφές κοινών δραστηριοτήτων επεξεργασίας. Η ΟΕ29 σχεδιάζει επίσης να συμβάλει στην εξέλιξη αυτή, μέσω της κοινής χρήσης και δημοσιοποίησης παραδειγμάτων των σχετικών ορίων για τον ορισμό ενός ΥΠΔ.

Η ΟΕ29 συνιστά να λαμβάνονται ιδιαίτερα υπόψη οι ακόλουθοι παράγοντες για τον καθορισμό του κατά πόσον η επεξεργασία πραγματοποιείται σε μεγάλη κλίμακα:

- Ο αριθμός των ενδιαφερόμενων προσώπων στα οποία αναφέρονται τα δεδομένα - είτε ως συγκεκριμένος αριθμός είτε ως ποσοστό του σχετικού πληθυσμού.
- Ο όγκος δεδομένων και/ή το φάσμα των διαφορετικών στοιχείων δεδομένων που υποβάλλονται σε επεξεργασία.
- Η διάρκεια ή η μονιμότητα της δραστηριότητας επεξεργασίας δεδομένων.
- Η γεωγραφική έκταση της δραστηριότητας επεξεργασίας.

Παραδείγματα επεξεργασίας μεγάλης κλίμακας περιλαμβάνουν:

- επεξεργασία δεδομένων ασθενών από νοσοκομείο,
- επεξεργασία δεδομένων μετακίνησης ατόμων που χρησιμοποιούν το σύστημα δημόσιων συγκοινωνιών της πόλης (π.χ. παρακολούθηση μέσω ηλεκτρονικών καρτών),

- επεξεργασία δεδομένων γεωγραφικής θέσης σε πραγματικό χρόνο των πελατών μιας διεθνούς αλυσίδας γρήγορου φαγητού για στατιστικούς σκοπούς από εταιρεία ειδικευμένη στην παροχή αυτών των υπηρεσιών,
- επεξεργασία δεδομένων πελατών από ασφαλιστική εταιρεία ή τράπεζα,
- επεξεργασία προσωπικών δεδομένων για ανάλυση συμπεριφοράς με σκοπό τη διαφήμιση από μια μηχανή αναζήτησης,
- επεξεργασία δεδομένων (περιεχόμενο, κίνηση, τοποθεσία) από παρόχους υπηρεσιών Διαδικτύου.

Παραδείγματα που δεν αποτελούν επεξεργασία μεγάλης κλίμακας περιλαμβάνουν:

- επεξεργασία δεδομένων ασθενών από μεμονωμένο ιατρό,
- την επεξεργασία προσωπικών δεδομένων σχετικά με ποινικές καταδίκες και αδικήματα από μεμονωμένο δικηγόρο.

Το άρθρο 37 ισχύει τόσο για τους ΥΕ όσο και για τους ΕΕ όσον αφορά τον ορισμό ενός ΥΠΔ. Ανάλογα με το ποιος πληροί τα κριτήρια για τον υποχρεωτικό χαρακτηρισμό, τόσο ο υπεύθυνος επεξεργασίας όσο και ο ΕΕ καλούνται να διορίσουν από έναν ΥΠΔ (οι οποίοι θα πρέπει στη συνέχεια να συνεργάζονται μεταξύ τους).

Το άρθρο 37 παράγραφος 2 επιτρέπει σε μια ομάδα επιχειρήσεων να ορίσουν έναν ενιαίο ΥΠΔ υπό τον όρο ότι θα είναι «εύκολα προσβάσιμος από κάθε εγκατάσταση». Η έννοια της προσβασιμότητας αναφέρεται στα καθήκοντα του ΥΠΔ ως σημείο επαφής σε ότι αφορά τα πρόσωπα στα οποία αναφέρονται τα δεδομένα, την εποπτική αρχή αλλά και εσωτερικά εντός του οργανισμού, θεωρώντας ότι ένα από τα καθήκοντα του ΥΠΔ είναι «να ενημερώνει και να συμβουλεύει τον υπεύθυνο επεξεργασίας τον ΕΕ και τους υπαλλήλους που πραγματοποιούν την επεξεργασία σύμφωνα με τον παρόντα κανονισμό».

Προκειμένου να διασφαλιστεί η πρόσβαση του ΥΠΔ, εσωτερικού ή εξωτερικού, είναι σημαντικό να διασφαλιστεί ότι τα στοιχεία επικοινωνίας του είναι διαθέσιμα σύμφωνα με τις απαιτήσεις του ΓΚΠΔ.

Ο ΥΠΔ πρέπει να είναι σε θέση να επικοινωνεί αποτελεσματικά με τα υποκείμενα των δεδομένων και να συνεργάζεται με τις αρμόδιες εποπτικές αρχές. Αυτό σημαίνει επίσης ότι αυτή η επικοινωνία πρέπει να πραγματοποιείται στη γλώσσα ή τις γλώσσες που χρησιμοποιούν οι εποπτικές αρχές και τα ενδιαφερόμενα πρόσωπα στα οποία αναφέρονται τα δεδομένα.

Σύμφωνα με το άρθρο 37 παράγραφος 3, μπορεί να οριστεί ένας ΥΠΔ για περισσότερες δημόσιες αρχές ή οργανισμούς, λαμβάνοντας υπόψη την οργανωτική δομή και το μέγεθος τους. Ισχύουν τα ίδια σε ότι αφορά τους πόρους και την επικοινωνία.

Η προσωπική διαθεσιμότητα ενός ΥΠΔ (είτε είναι φυσικά στους ίδιους χώρους όπως οι υπάλληλοι, είτε μέσω ανοικτής γραμμής ή άλλου ασφαλούς μέσου επικοινωνίας) είναι ουσιαστικής σημασίας για να διασφαλιστεί ότι τα υποκείμενα των δεδομένων θα μπορούν να επικοινωνούν μαζί του. Ο ΥΠΔ δεσμεύεται από το απόρρητο ή την εμπιστευτικότητα όσον αφορά την εκτέλεση των καθηκόντων του, σύμφωνα με το δίκαιο της Ένωσης ή του κράτους μέλους [Άρθρο 38(5)]. Η υποχρέωση τήρησης απορρήτου / εμπιστευτικότητας δεν εμποδίζει τον ΥΠΔ να επικοινωνεί και να ζητεί συμβουλές από την εποπτική αρχή.

Το άρθρο 37 παράγραφος 5 ορίζει ότι ο ΥΠΔ «ορίζεται βάσει των επαγγελματικών προσόντων και, ειδικότερα, των γνώσεων του σχετικά με τη νομοθεσία και τις πρακτικές προστασίας δεδομένων και την ικανότητα εκπλήρωσης των καθηκόντων που αναφέρονται στο άρθρο 39». Το απαιτούμενο επίπεδο ειδικών γνώσεων πρέπει να καθορίζεται ανάλογα με τις διεργασίες επεξεργασίας δεδομένων που πραγματοποιούνται και την προστασία που απαιτείται για την επεξεργασία των προσωπικών δεδομένων.

Παρόλο που το άρθρο 37 παράγραφος 5 δεν διευκρινίζει τις επαγγελματικές ιδιότητες που πρέπει να λαμβάνονται υπόψη κατά τον ορισμό του ΥΠΔ, είναι σημαντικό το γεγονός ότι οι ΥΠΔ πρέπει να έχουν πείρα σε εθνικές και ευρωπαϊκές νομοθεσίες και πρακτικές για την προστασία των δεδομένων και σε μια βαθιά κατανόηση του ΓΚΠΔ. Είναι επίσης χρήσιμο οι εποπτικές αρχές να βοηθήσουν στην επαρκή και τακτική κατάρτιση για τους ΥΠΔ.

Η γνώση του επιχειρηματικού τομέα και της οργάνωσης του ΥΕ είναι χρήσιμη. Ο ΥΠΔ πρέπει επίσης να έχει επαρκή κατανόηση των διεξαγόμενων εργασιών επεξεργασίας, καθώς και των συστημάτων πληροφοριών και των απαιτήσεων ασφάλειας και προστασίας των δεδομένων του υπεύθυνου επεξεργασίας.

Στην περίπτωση δημόσιας αρχής ή φορέα, ο ΥΠΔ πρέπει επίσης να έχει καλή γνώση των διοικητικών κανόνων και διαδικασιών του οργανισμού.

Ο πρωταρχικός στόχος του ΥΠΔ πρέπει να είναι η συμμόρφωση με το ΓΚΠΔ. Ο ΥΠΔ διαδραματίζει βασικό ρόλο στην καλλιέργεια μιας κουλτούρας ασφάλειας και προστασίας των δεδομένων εντός του οργανισμού και συμβάλλει στην υλοποίηση των βασικών αρχών του ΓΚΠΔ, όπως οι αρχές επεξεργασίας δεδομένων, τα δικαιώματα των προσώπων στα οποία αναφέρονται τα δεδομένα, η προστασία δεδομένων από το σχεδιασμό και εξ ορισμού, τα αρχεία των δραστηριοτήτων επεξεργασίας, την ασφάλεια της επεξεργασίας και την αναγγελία των παραβιάσεων των δεδομένων.

Ο ρόλος του ΥΠΔ μπορεί επίσης να ασκείται βάσει σύμβασης παροχής υπηρεσιών που συνάπτεται με ιδιώτη ή οργανισμό εκτός του οργανισμού του υπεύθυνου επεξεργασίας.

Το άρθρο 37 παράγραφος 7 του ΓΚΠΔ απαιτεί από τον ΥΕ ή τον ΕΕ:

- να δημοσιεύσει τα στοιχεία επικοινωνίας του ΥΠΔ,
- να κοινοποιήσει τα στοιχεία επικοινωνίας στις αρμόδιες εποπτικές αρχές.

Στόχος αυτών των απαιτήσεων είναι να διασφαλιστεί ότι τα υποκείμενα των δεδομένων (εντός και εκτός του οργανισμού) και οι εποπτικές αρχές μπορούν να επικοινωνούν εύκολα, άμεσα και εμπιστευτικά με τον ΥΠΔ χωρίς να χρειάζεται να έρθουν σε επαφή με άλλο τμήμα του οργανισμού.

Τα στοιχεία επικοινωνίας του ΥΠΔ πρέπει να περιλαμβάνουν πληροφορίες που επιτρέπουν στα υποκείμενα των δεδομένων και στις εποπτικές αρχές να φτάσουν στον ΥΠΔ με εύκολο τρόπο (ταχυδρομική διεύθυνση, αποκλειστικός τηλεφωνικός αριθμός και ειδική διεύθυνση ηλεκτρονικού ταχυδρομείου). Όπου ενδείκνυται, για σκοπούς επικοινωνίας με το κοινό, θα μπορούσαν επίσης να παρασχεθούν και άλλα μέσα επικοινωνίας, για παράδειγμα, ειδική τηλεφωνική γραμμή ή ειδική φόρμα επικοινωνίας στον ιστότοπο του οργανισμού για τον ΥΠΔ.

Ο Υπεύθυνος Προστασίας Δεδομένων πρέπει να συμμετέχει από το αρχικό στάδιο σε όλα τα ζητήματα που αφορούν την προστασία των δεδομένων. Επιπλέον, είναι σημαντικό ο ΥΠΔ να

θεωρείται εταίρος συζήτησης στο πλαίσιο του οργανισμού και ότι αυτός ή αυτή αποτελεί μέρος των σχετικών ομάδων εργασίας που ασχολούνται με δραστηριότητες επεξεργασίας δεδομένων εντός του οργανισμού.

Κατά συνέπεια, ο οργανισμός πρέπει να διασφαλίσει, ότι:

- Ο ΥΠΔ καλείται να συμμετέχει τακτικά σε συνεδριάσεις ανώτερων και μεσαίων στελεχών.
- Συνιστάται η παρουσία του/της ΥΠΔ όταν λαμβάνονται αποφάσεις με συνέπειες προστασίας δεδομένων. Όλες οι σχετικές πληροφορίες πρέπει να διαβιβάζονται έγκαιρα προκειμένου να του επιτρέψουν να παρέχει επαρκείς συμβουλές.
- Πρέπει πάντοτε να λαμβάνεται υπόψη η γνώμη του ΥΠΔ. Σε περίπτωση διαφωνίας, η ΟΕ29 συνιστά, ως ορθή πρακτική, να τεκμηριωθούν οι λόγοι για τους οποίους δεν ακολουθήθηκε η συμβουλή του ΥΠΔ.
- Ο υπεύθυνος προστασίας δεδομένων πρέπει να ενημερώνεται αμέσως μόλις έχει σημειωθεί παραβίαση δεδομένων ή άλλο περιστατικό.

Όπου ενδείκνυται, ο ΥΕ ή ο ΕΕ θα μπορούσε να αναπτύξει κατευθυντήριες γραμμές ή προγράμματα σχετικά με την προστασία δεδομένων, τα οποία καθορίζονται όταν πρέπει να συμβουλευτεί ο ΥΠΔ.

Το άρθρο 38 παράγραφος 2 του ΓΚΠΔ απαιτεί από τον οργανισμό να υποστηρίζει τον ΥΠΔ του με «την παροχή των αναγκαίων πόρων για την εκτέλεση των καθηκόντων του και την πρόσβαση σε δεδομένα προσωπικού χαρακτήρα και τις εργασίες επεξεργασίας και για τη διατήρηση των ειδικών γνώσεων του». Ειδικότερα, πρέπει να λαμβάνονται υπόψη τα εξής:

- Ενεργός υποστήριξη της λειτουργίας του ΥΠΔ από ανώτατα στελέχη (όπως σε επίπεδο διοικητικών συμβουλίων).
- Ένας επαρκής χρόνος για να εκπληρώσουν τα καθήκοντά τους οι ΥΠΔ. Αυτό είναι ιδιαίτερα σημαντικό όταν ο ΥΠΔ διορίζεται με μερική απασχόληση ή ασκεί και άλλα καθήκοντα. Διαφορετικά, οι αντικρουόμενες προτεραιότητες θα μπορούσαν να οδηγήσουν στην παραμέληση των καθηκόντων του ΥΠΔ.
- Επαρκής στήριξη όσον αφορά τους οικονομικούς πόρους, την υποδομή (χώρους, εγκαταστάσεις, εξοπλισμό) και το προσωπικό, όπου ενδείκνυται.
- Επίσημη ανακοίνωση του ορισμού του ΥΠΔ σε όλο το προσωπικό, ώστε να διασφαλιστεί ότι η ύπαρξή του και η λειτουργία του είναι γνωστά στον οργανισμό.
- Απαραίτητη πρόσβαση σε άλλες υπηρεσίες, όπως το Ανθρώπινο Δυναμικό, τη Νομική Υπηρεσία, την Πληροφορική, την Ασφάλεια κ.λπ., ώστε οι ΥΠΔ να μπορούν να λαμβάνουν ουσιαστική υποστήριξη και πληροφορίες από αυτές τις υπηρεσίες.
- Συνεχής εκπαίδευση. Οι ΥΠΔ πρέπει να έχουν τη δυνατότητα να ενημερώνονται σχετικά με τις εξελίξεις στον τομέα της προστασίας δεδομένων. Θα πρέπει να ενθαρρυνθούν να συμμετάσχουν σε μαθήματα κατάρτισης σχετικά με την προστασία των δεδομένων και άλλες μορφές επαγγελματικής ανάπτυξης, όπως η συμμετοχή σε φόρουμ για την προστασία της ιδιωτικής ζωής, σε εργαστήρια κ.λπ.
- Δεδομένου του μεγέθους και της διάρθρωσης της οργάνωσης, μπορεί να χρειαστεί να δημιουργηθεί μια Ομάδα Προστασίας Προσωπικών Δεδομένων (ο ΥΠΔ και το αντίστοιχο

προσωπικό). Σε τέτοιες περιπτώσεις, η εσωτερική δομή της ομάδας και τα καθήκοντα και οι αρμοδιότητες κάθε μέλους της πρέπει να καταρτίζονται σαφώς. Ομοίως και όταν η λειτουργία του ΥΠΔ ασκείται από εξωτερικό πάροχο υπηρεσιών.

- Το άρθρο 38 παράγραφος 3 θεσπίζει ορισμένες βασικές εγγυήσεις για να διασφαλίσει ότι οι ΥΠΔ είναι σε θέση να εκτελούν τα καθήκοντά τους αυτόνομα εντός του οργανισμού. Ειδικότερα, οι ΥΕ/ΕΕ καλούνται να διασφαλίσουν ότι ο ΥΠΔ «δεν λαμβάνει οδηγίες σχετικά με την άσκηση των καθηκόντων του».

Αυτό σημαίνει ότι, κατά την εκπλήρωση των καθηκόντων τους βάσει του άρθρου 39, οι ΥΠΔ δεν πρέπει να «κατευθύνονται» για το πώς να χειριστούν ένα θέμα, για παράδειγμα ποιο αποτέλεσμα πρέπει να επιτευχθεί, πώς να διερευνήσει μια καταγγελία ή αν πρέπει να συμβουλευθεί την εποπτική αρχή. Επιπλέον, δεν πρέπει να τους δοθεί η εντολή να λάβουν ορισμένη άποψη/απόφαση σχετικά με ένα ζήτημα που σχετίζεται με το δίκαιο προστασίας των δεδομένων, για παράδειγμα, μια συγκεκριμένη ερμηνεία του νόμου.

Το άρθρο 38, παράγραφος 3, επιβάλλει επίσης ότι οι ΥΠΔ «δεν πρέπει να απορρίπτονται ή να τιμωρούνται από τον ΥΕ ή τον ΕΕ για την εκτέλεση των καθηκόντων του». Η απαίτηση αυτή ενισχύει επίσης την αυτονομία των ΥΠΔ και διασφαλίζει ότι ενεργούν ανεξάρτητα και απολαμβάνουν επαρκούς προστασίας κατά την εκτέλεση των καθηκόντων τους για την προστασία των δεδομένων.

Η έλλειψη σύγκρουσης συμφερόντων συνδέεται στενά με την απαίτηση ο ΥΠΔ να ενεργεί με ανεξάρτητο τρόπο. Παρόλο που οι ΥΠΔ επιτρέπεται να ασκούν και άλλες λειτουργίες, μπορούν, μόνον εφόσον δεν δημιουργούνται συγκρούσεις συμφερόντων. Αυτό συνεπάγεται ειδικότερα ότι ο ΥΠΔ δεν μπορεί να κατέχει θέση εντός του οργανισμού που τον οδηγεί να προσδιορίσει τους σκοπούς και τα μέσα επεξεργασίας των δεδομένων προσωπικού χαρακτήρα. Λόγω της συγκεκριμένης οργανωτικής δομής σε κάθε οργανισμό, αυτό πρέπει να λαμβάνεται υπόψη κατά περίπτωση.

Οι ΥΕ και τους ΕΕ προτείνεται:

- να προσδιορίσουν τις θέσεις που θα ήταν ασυμβίβαστες με τη λειτουργία του ΥΠΔ,
- να εκπονήσουν εσωτερικούς κανόνες για το σκοπό αυτό, προκειμένου να αποφευχθούν συγκρούσεις συμφερόντων,
- να συμπεριλάβουν διασφαλίσεις στους εσωτερικούς κανόνες του οργανισμού και να διασφαλίσουν ότι η προκήρυξη κενής θέσης για τη θέση του ΥΠΔ είναι επαρκώς ακριβής και λεπτομερής προκειμένου να αποφευχθεί η σύγκρουση συμφερόντων. Στο πλαίσιο αυτό, πρέπει επίσης να ληφθεί υπόψη ότι οι συγκρούσεις συμφερόντων μπορούν να λάβουν διάφορες μορφές ανάλογα με το εάν ο ΥΠΔ προσλαμβάνεται εσωτερικά ή εξωτερικά.

7.3 Καθήκοντα του ΥΠΔ

Βασικό καθήκον του ΥΠΔ είναι η παρακολούθησης της συμμόρφωσης με τον ΓΚΠΔ.

Ο έλεγχος της συμμόρφωσης δεν σημαίνει ότι ο ΥΠΔ είναι υπεύθυνος προσωπικά όταν υπάρχει περίπτωση μη συμμόρφωσης. Ο ΓΚΠΔ καθιστά σαφές ότι απαιτείται από τον ΥΕ και όχι από τον ΥΠΔ, να «εφαρμόσει τα κατάλληλα τεχνικά και οργανωτικά μέτρα για να εξασφαλίσει

και να αποδείξει ότι η επεξεργασία πραγματοποιείται σύμφωνα με τον παρόντα κανονισμό» [Άρθρο 24(1)]. Η συμμόρφωση με την προστασία δεδομένων αποτελεί εταιρική ευθύνη του Υπεύθυνου Επεξεργασίας των δεδομένων και όχι του ΥΠΔ.

Σύμφωνα με το άρθρο 35, παράγραφος 1, ο Υπεύθυνος της Επεξεργασίας και όχι ο ΥΠΔ, οφείλουν να διεξάγουν, εφόσον είναι αναγκαίο, ΕΑΠΔ. Σύμφωνα με την αρχή της προστασίας των δεδομένων από το σχεδιασμό [Άρθρο 35(2)] απαιτεί συγκεκριμένα ότι ο ΥΕ «ζητά τη συμβουλή» του ΥΠΔ κατά τη διεξαγωγή της ΕΑΠΔ. Επίσης ο ΥΠΔ έχει την υποχρέωση «να παρέχει συμβουλές, εφόσον ζητηθεί, σε ότι αφορά την ΕΑΠΔ και να παρακολουθεί την εξέλιξή της» [Άρθρο 39(1γ)].

Οι ΥΠΔ πρέπει να ιεραρχήσουν τις δραστηριότητές τους και να επικεντρώσουν τις προσπάθειές τους σε θέματα που παρουσιάζουν υψηλότερους κινδύνους προστασίας δεδομένων [Άρθρο 39(2)].

Τέλος το άρθρο 39 παράγραφος 1 προβλέπει έναν κατάλογο των καθηκόντων που πρέπει να έχει ο ΥΠΔ ως ελάχιστο.

8

Επιπτώσεις στον Τραπεζικό Τομέα

8.1 Γενικά

Οι Τράπεζες είναι ανάμεσα στις εταιρείες που επηρεάζονται στο μέγιστο βαθμό από την εφαρμογή του ΓΚΠΔ καθώς έχουν στην κατοχή τους μεγάλο όγκο προσωπικών δεδομένων. Εκτός από τα υψηλά χρηματικά πρόστιμα, ένα κενό στην προστασία δεδομένων μιας τράπεζας, αν αποκαλυφθεί, μπορεί να οδηγήσει σε καταστροφικές συνέπειες στη φήμη της και στις σχέσεις της με την πελατεία της. Ειδικά στον Τραπεζικό Τομέα η φήμη είναι για κάποιες τράπεζες το σπουδαιότερο περιουσιακό αγαθό – έναντι των fintech εταιρειών.

Τα δεδομένα των πελατών μπορεί να κρατούνται σε περισσότερα από 100 διαφορετικά συστήματα. Με δεδομένο το γεγονός ότι οι αλλαγές σε κάθε ένα από αυτά τα συστήματα διαρκούν έως και αρκετούς μήνες για να υλοποιηθούν, γίνεται αντιληπτός ο όγκος των εργασιών που πρέπει να ολοκληρωθούν σε σύντομο χρονικό διάστημα αλλά και η πολυπλοκότητα του.

8.2 Διακυβέρνηση Προγράμματος

Η διακυβέρνηση του προγράμματος συμμόρφωσης με τον ΓΚΠΔ δεν είναι μόνο πρόβλημα της Πληροφορικής αλλά πολλά περισσότερα από αυτό. Το νομικό τμήμα και η ομάδα διαχείρισης λειτουργικών κινδύνων πρέπει να συνεργαστούν με το προσωπικό που έρχεται σε επαφή με την πελατεία (front-office).

Δεν είναι σαφές ποιος πρέπει να έχει την εποπτεία για τη συμμόρφωση με τον ΓΚΠΔ. Ο ΓΚΠΔ από τη φύση του είναι τόσο πολύπλευρος, που καθιστά πολύ δύσκολο για τις τράπεζες να αναθέσουν την ευθύνη σε κάποιο συγκεκριμένο τμήμα για τον συντονισμό των ενεργειών. Η αιτία

είναι ότι οι τράπεζες έχουν χιλιάδες συστήματα, τεχνολογίες και διαδικασίες, σε βαθμό που να μην υπάρχει ένα μόνο άτομο που θα μπορούσε να ηγηθεί και να εποπτεύσει το πρόγραμμα συμμόρφωσης.

8.3 Ορισμός Υπεύθυνου Προστασίας Δεδομένων (ΥΠΔ) [Data Protection Officer (DPO)]

Ο Υπεύθυνος Προστασίας Δεδομένων (ΥΠΔ) είναι ένας ρόλος που απορρέει ως υποχρέωση του ΓΚΠΔ – με αρμοδιότητες Νομικές, Πληροφορικής και Επιχειρηματικές.

Ο ρόλος του είναι να συντονίζει όλες τις ενέργειες σχετικά με την προστασία των προσωπικών δεδομένων στο πλαίσιο του ΓΚΠΔ και να παρακολουθεί την εξέλιξη των σχετικών δράσεων.

Ο τίτλος του Υπεύθυνου Προστασίας Δεδομένων δεν πρέπει να δημιουργεί σύγχυση. Ο ΥΠΔ είναι εστιασμένος περισσότερο στη συμμόρφωση με τον ΓΚΠΔ παρά στην προστασία των δεδομένων. Η τελευταία είναι αρμοδιότητα του Επικεφαλής Ασφάλειας Πληροφοριών (Chief Information Security Officer-CISO) της Τράπεζας.

Ο ΓΚΠΔ προβλέπει συγκεκριμένα ότι ο ΥΠΔ θα πρέπει να χαίρει ανεξαρτησίας και θα πρέπει η δομή αναφοράς να αντικατοπτρίζει αυτήν την απαίτηση.

8.4 Ευθυγράμμιση του Προγράμματος με τις αρχές του ΓΚΠΔ

Ορισμός και αναθεώρηση του μοντέλου της προστασίας των προσωπικών δεδομένων σύμφωνα με τις αρμοδιότητες που αναφέρονται στον νέο κανονισμό.

Ρύθμιση ενός μητρώου των πράξεων επεξεργασίας προσωπικών δεδομένων. Βάσει του ΓΚΠΔ η Τράπεζα έχει την υποχρέωση να τηρεί αρχείο τεκμηρίωσης των ενεργειών που σχετίζονται με τις δραστηριότητες επεξεργασίας προσωπικών δεδομένων. Η υποχρέωση αυτή προσδιορίζεται σαφώς ως προς το περιεχόμενο. Επιπλέον το αρχείο αυτό θα πρέπει να είναι διαθέσιμο σε ενδεχόμενο έλεγχο προς τις εποπτικές αρχές (όπως η Αρχή Προστασίας Προσωπικών Δεδομένων).

- Ορισμός ή αναθεώρηση των πολιτικών και διαδικασιών για τη διασφάλιση της λογοδοσίας.
- Αναθεώρηση των πολιτικών ιδιωτικότητας για τη συλλογή της δήλωσης συγκατάθεσης και για την εξασφάλιση δίκαιης και διαφανούς επεξεργασίας.
- Αναγνώριση των ελέγχων και των εκθέσεων για την παρακολούθηση της συμμόρφωσης στο χρόνο.

8.5 Αλλαγές σε Οργανωτική Δομή & Διαδικασίες

- Αναθεώρηση των διαδικασιών για τη διαχείριση της συναίνεσης και τις διαδικασίες των αιτήσεων από τα ενδιαφερόμενα φυσικά πρόσωπα (δικαίωμα στη λήθη, την πρόσβαση σε δεδομένα και της φορητότητας των δεδομένων).
- Αναθεώρηση του μοντέλου διακυβέρνησης για το διορισμό του Υπεύθυνου Προστασίας Δεδομένων.
- Ορισμός ενός σχεδίου κατάρτισης και ενημέρωσης των εργαζομένων.
- Χαρτογράφηση των δεδομένων προσωπικού χαρακτήρα και της μεταφοράς τους σε τρίτους.

8.6 Σχέσεις με τρίτους

- Αναθεώρηση των συμβάσεων με τρίτους για την εξασφάλιση της συμμόρφωσης με το νέο ΓΚΠΔ από την άποψη της πληροφορικής.
- Αναθεώρηση ή/και ταυτοποίηση των κανόνων για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα εντός των εταιρειών του ομίλου από την άποψη της πληροφορικής.
- Βελτίωση των υφιστάμενων δεσμευτικών εταιρικών κανόνων για υιοθέτηση νέων για τη μεταφορά των δεδομένων (KPMG, 2017).

8.6.1 Αναθεώρηση των συμβάσεων

Η αναθεώρηση όλων των συμβάσεων με τους πελάτες και τους συνεργάτες για την εξασφάλιση της συμμόρφωσης είναι μια διαδικασία που δεν πρέπει να υποτιμάται λόγω του τεραστίου όγκου συμβάσεων και συμβολαίων που πρέπει να αναδιαμορφωθούν. Η διαδικασία αναθεώρησης των συμβάσεων αφορά τόσο τους Υπεύθυνους Επεξεργασίας (ΥΕ) – που πρακτικά σημαίνει όλες τις Τράπεζες – όσο και τους Εκτελούντες την Επεξεργασία (ΕΕ), οι οποίοι χειρίζονται προσωπικά δεδομένα για λογαριασμό των ΥΕ. (KPMG, 2017)

Ο ΓΚΠΔ εισάγει νέες απαιτήσεις για τους ΥΕ, οι οποίοι καλούνται να πάρουν ρητή συγκατάθεση από τα υποκείμενα των δεδομένων (στη συγκεκριμένη περίπτωση των τραπεζών, υποκείμενα των δεδομένων είναι οι πελάτες, οι υπάλληλοι και οι προμηθευτές/συνεργάτες), για το πώς θα χρησιμοποιούν και θα φυλάσσουν τα προσωπικά τους δεδομένα.

Ο ΓΚΠΔ απαιτεί ειδικές ρήτρες στις συμβάσεις με τους ΕΕ για τον σκοπό της επεξεργασίας των προσωπικών δεδομένων των υποκειμένων, τη διάρκεια και τη φύση της επεξεργασίας καθώς και τον τύπο των εμπλεκομένων προσωπικών δεδομένων. Στις συμβάσεις πρέπει να επιβεβαιώνεται ότι η επεξεργασία δεδομένων γίνεται με την προσήκουσα εμπιστευτικότητα, ότι οι ΕΕ κρυπτογραφούν τα δεδομένα με τις κατάλληλες μεθόδους κρυπτογράφησης και θα διαγράφουν τα προσωπικά δεδομένα στο τέλος της διάρκειας της σύμβασης.

Η αναθεώρηση των συμβάσεων με τους πελάτες πρέπει να γίνει σχεδόν ταυτόχρονα προκειμένου να αποφευχθεί να υπάρχουν διαφορετικές συμφωνίες με τους πελάτες για την ίδια παρεχόμενη υπηρεσία.

Σε κάποιες περιπτώσεις είναι πιθανόν να χρειάζεται να ακυρωθούν οι συμβάσεις και να δημιουργηθούν νέες προκειμένου να καλυφθούν οι απαιτήσεις του ΓΚΠΔ σε ότι αφορά τη σαφή αδειοδότηση για τη χρήση των δεδομένων.

Οι εταιρείες συμβούλων συνιστούν στις εταιρείες του χρηματοπιστωτικού τομέα, να επικεντρωθούν στις συμβάσεις «υψηλού κινδύνου», δηλαδή σε αυτές που αφορούν την επεξεργασία μεγάλου όγκου προσωπικών δεδομένων, καθώς είναι πρακτικά αδύνατον λόγω του όγκου και της πολυπλοκότητας να γίνουν όλες οι αναθεωρήσεις των συμβάσεων παράλληλα και άμεσα.

9

Έλεγχος του Data Flow Mapping-Compliance Check List

9.1 Αξιολόγηση νομιμότητας και προσδιορισμός διαδικασίας

Για κάθε Data Flow πρέπει να αξιολογούνται τα ακόλουθα:

1. Ποια είναι η πηγή των δεδομένων.
2. Για ποιόν σκοπό συλλέγονται.
3. Τι δεδομένα συλλέγονται για τον σκοπό αυτό.
4. Ποια είναι η πραγματική χρήση τους.
5. Ποιοι είναι οι αποδέκτες τους (ποιοι τα βλέπουν, σε ποιους κοινοποιούνται κλπ.).

Για όλα τα παραπάνω πρέπει να συντρέχουν συγκεκριμένες νόμιμες προϋποθέσεις και να γίνονται με νόμιμες διαδικασίες. Για όλα πρέπει να σχεδιάζονται και να εφαρμόζονται ενδεδειγμένα μέτρα ασφαλείας.

9.2 Ποια είναι η πηγή των δεδομένων

Η ενημέρωση των υποκειμένων διαφοροποιείται αναλόγως με την πηγή των δεδομένων (άρθρα 13 και 14):

- Εφόσον συλλέγονται από το ίδιο το υποκείμενο – κατά το χρόνο της συλλογής
- Εφόσον συλλέγονται από άλλη πηγή:
    - Εντός εύλογης προθεσμίας (το αργότερο 30 ημέρες από τη λήψη).
    - Το αργότερο κατά την πρώτη επικοινωνία αν η χρήση είναι για επικοινωνία.

Η αρχή της διαφάνειας απαιτεί οποιαδήποτε ενημέρωση απευθύνεται στο κοινό γενικά (π.χ. άρθρο 34) ή στο υποκείμενο ειδικά (π.χ. άρθρα 13 και 14) να πληροί τα ακόλουθα κριτήρια (Προοίμιο 58):

- Συνοπτική
- Εύκολα προσβάσιμη
- Εύκολα κατανοητή
- Σαφής και απλή διατύπωση
- (κατά περίπτωση) απεικόνιση
- (για τα παιδιά) με σαφή και απλή γλώσσα, κατανοητή για τα παιδιά.

Η ενημέρωση επιτρέπεται να γίνεται και με ηλεκτρονική μορφή. Στην περίπτωση «εγγράφου» πρέπει να γίνεται χωριστά από το υπόλοιπο «κείμενο».

Η ενημέρωση δεν απαιτείται (άρθρο 14 παρ.5) εάν:

- Το υποκείμενο διαθέτει ήδη τις πληροφορίες (εφόσον τα δεδομένα λαμβάνονται από τρίτη πηγή και μόνον).
- Η καταχώρηση ή η κοινολόγηση των δεδομένων προβλέπεται ρητώς από το νόμο.
- Η παροχή των πληροφοριών στο υποκείμενο αποδεικνύεται ανέφικτη ή θα απαιτούσε δυσανάλογη προσπάθεια.
- Τα δεδομένα πρέπει να παραμείνουν εμπιστευτικά δυνάμει υποχρέωσης επαγγελματικού απορρήτου.

9.3 Για ποιόν σκοπό συλλέγονται

Ο σκοπός συλλογής των δεδομένων αποτελεί τον κορμό και καθορίζει τις προϋποθέσεις για τις διαδικασίες νομιμότητας της επεξεργασίας.

- Χαρακτηριστικά:
    - Νόμιμος
    - Συγκεκριμένος
    - Σαφής
    - Προσδιορισμένος
- Κρίνονται κατά τον χρόνο συλλογής των δεδομένων

Επεξεργασία για περαιτέρω σκοπούς (από αυτούς που είχαν αρχικά συλλεγεί) επιτρέπεται μόνο υπό συγκεκριμένες προϋποθέσεις.

1. Ανεξάρτητα από την συμβατότητα των σκοπών
    a. Εφόσον υπάρχει συγκατάθεση του υποκειμένου.
    b. Εφόσον βασίζεται σε νομική υποχρέωση του ΥΕ.
2. Εφόσον υπάρχει συμβατότητα του αρχικού σκοπού και των περεταίρω (άρθρο 6 παρ.4)
    a. Σε κάθε άλλη νομική βάση επεξεργασίας.

Και στις δύο περιπτώσεις (1 και 2) απαιτείται προηγούμενη ειδική ενημέρωση του υποκειμένου. (Priority, 2017)

9.4 Ποια δεδομένα συλλέγονται

Τα χαρακτηριστικά των δεδομένων κρίνονται πάντοτε με βάση τον σκοπό. Πρέπει να είναι πάντοτε τα λιγότερο δυνατά για την επίτευξη του σκοπού (άρθρο 5 παρ. 1γ). Συγκεκριμένα πρέπει να είναι κατάλληλα, συναφή και να περιορίζονται στο αναγκαίο (πρόσφορα, αναλογικά και ηπιότερα για τον ίδιο σκοπό).

Τα δεδομένα πρέπει να είναι πάντοτε ακριβή και όταν είναι αναγκαίο να επικαιροποιούνται (άρθρο 5 παρ. 1δ).

Γενική Αρχή είναι η λήψη εύλογων μέτρων ότι τα μη ακριβή στοιχεία διορθώνονται ή διαγράφονται (Προοίμιο 39 - θέσπιση παραμέτρων περιοδικού ελέγχου για τη διατήρηση δεδομένων προσωπικού χαρακτήρα).

Ο χρόνος διατήρησης των δεδομένων πρέπει να περιορίζεται μόνο στο διάστημα που απαιτείται για την επίτευξη των σκοπών της επεξεργασίας (άρθρο 5 παρ.1). Ο χρόνος διατήρησης των δεδομένων αποτελεί ένα σύνθετο και περίπλοκο πρόβλημα καθώς πρέπει να γίνει στάθμιση του χρόνου διατήρησης σε σχέση με την Υποχρέωση Λογοδοσίας (Accountability) και το Βάρος Απόδειξης.

9.4.1 Ποια η χρήση τους – Απλά δεδομένα (Άρθρο 6 παρ.2)

- Συγκατάθεση
- Απαραίτητη για την εκτέλεση της σύμβασης
- Απαραίτητη για τη συμμόρφωση ΥΕ με έννομη υποχρέωση
- Απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος
- Απαραίτητη για την εκπλήρωση καθήκοντος για το δημόσιο συμφέρον ή άσκησης δημόσιας εξουσίας
- Απαραίτητη για το έννομο συμφέρον που επιδιώκει ο ΥΕ

Χαρακτηριστικά (Προοίμιο 32):

- Σαφής θετική ενέργεια
- Ελεύθερη
- Συγκεκριμένη
- Ρητή
- Εν πλήρει επιγνώσει ένδειξη της συμφωνίας του υποκειμένου των δεδομένων

Η Συγκατάθεση πρέπει είναι σαφής θετική ενέργεια και όχι να εννοείται. Θα πρέπει να καλύπτει το σύνολο των δραστηριοτήτων επεξεργασίας που διενεργείται για τον ίδιο σκοπό ή τους ίδιους σκοπούς (π.χ. προώθηση προϊόντων, αποτίμηση ρίσκου κ.λπ.).

Όταν η χρήση αφορά πολλαπλούς σκοπούς, η συγκατάθεση θα πρέπει να δίδεται για όλους τους σκοπούς (Προοίμιο32). Αν δεν έχει δοθεί χωριστή συγκατάθεση σε κάθε διαφορετικές πράξεις επεξεργασίας, τότε δεν θεωρείται ότι έχει δοθεί ελεύθερα (Προοίμιο 43).

Η Συγκατάθεση δεν έχει δοθεί ελεύθερα εάν δεν επιτρέπεται να δοθεί χωριστή συγκατάθεση σε διαφορετικές πράξεις επεξεργασίας (Προοίμιο 43).

Προσοχή: Η συγκατάθεση δεν νομιμοποιεί τον σκοπό της επεξεργασίας ούτε τα χαρακτηριστικά των δεδομένων. (Priority, 2017)

Η συγκατάθεση δεν θεωρείται ελεύθερη στις παρακάτω προϋποθέσεις (Προοίμιο 42 και 43):

- Όταν το υποκείμενο των δεδομένων δεν έχει αληθινή ή ελεύθερη επιλογή ή δεν είναι σε θέση να αρνηθεί ή να αποσύρει την συγκατάθεση του χωρίς να ζημιωθεί (πχ. εργαζόμενοι, βλ. και Οδηγία 115/2001 ΑΠΔΠΧ).
- Σε περίπτωση σαφούς ανισότητας μεταξύ του υποκειμένου και του ΥΕ (πχ. εργαζόμενοι, Γενικοί Όροι Συμβάσεων -ΓΟΣ- τραπεζών, ασφαλιστικών κοκ).
- Όταν δεν έχει δυνατότητα να δώσει ξεχωριστή συγκατάθεση για κάθε διαφορετική πράξη επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

Θα πρέπει να υπάρχει **δυνατότητα ανάκλησης** της (opt out) οποτεδήποτε με ισχύ για το μέλλον. Η ανάκληση της συγκατάθεσης θα πρέπει να γίνεται εξίσου εύκολα με την παροχή της.

Συγκατάθεση ανηλίκων:

- Ειδική πρόβλεψη για υπηρεσίες της κοινωνίας της πληροφορίας.
- Στις περιπτώσεις που νόμιμη βάση είναι η συγκατάθεση.
- Για ανήλικους κάτω των 16 ετών, η συγκατάθεση είναι νόμιμη μόνο αν παρέχεται ή εγκρίνεται από τον ασκούντα την γονική μέριμνα.
- Ο ΥΕ είναι υποχρεωμένος να καταβάλει εύλογες προσπάθειες επαλήθευσης βάσει της διαθέσιμης τεχνολογίας.

9.4.2 Ποια η χρήση τους – Ειδικά («ευαίσθητα») δεδομένα (άρθρο 9 παρ. 2)

Για τις ειδικές κατηγορίες δεδομένων απαιτείται επίταση όλων των υφισταμένων προϋποθέσεων και αρχών νομιμότητας καθώς και όλων των θεμάτων που σχετίζονται με την ασφάλεια (ενδεδειγμένα μέτρα).

Επιπλέον απαιτείται επίταση όλων των θεμάτων που σχετίζονται με την επικινδυνότητα των δεδομένων και **ρητή υποχρέωση** για Εκτίμηση Αντικτύπου στην Ιδιωτικότητα (Privacy Impact Assessment – PIA).

Η Συγκατάθεση επιβάλλεται να είναι ρητή και με έγγραφη δήλωση του υποκειμένου (μπορεί να γίνει και με ηλεκτρονικά μέσα – Προοίμιο 32).

Ιδιαίτερη προσοχή πρέπει να δοθεί και πάλι στο θέμα της ελευθερίας της συγκατάθεσης σε περίπτωση ανισότητας των μερών. Υποχρεωτική σώρευση και άλλης προϋπόθεσης νομιμότητας από τις αναφερόμενες στο άρθρο 9 παρ. 2 πχ. για τις ασφάλειες περίθαλψης (υγείας) συνδ α.9 π 2

α) ζ) για λόγους ουσιαστικού δημοσίου συμφέροντος βάσει δικαίου ΕΕ ή κ/μ και η) απαραίτητη για την παροχή υγειονομικής περίθαλψης.

9.5 Αποδέκτες των δεδομένων

Οι αποδέκτες των δεδομένων μπορεί να είναι:

- Ο **Υπεύθυνος Επεξεργασίας ΥΕ**: Είναι εκείνος που καθορίζει τον **σκοπό** της επεξεργασίας.
- Ο **Εκτελών την Επεξεργασία ΕΕ**: Εκτελεί επεξεργασία **για λογαριασμό** του Υπεύθυνου.
- Οποιοσδήποτε Τρίτος.

Το υποκείμενο πρέπει να ενημερώνεται για τους αποδέκτες ή τις κατηγορίες των αποδεκτών.

Ο Εκτελών την Επεξεργασία πρέπει να έχει σύμβαση με το ΥΕ (γραπτώς ή σε ηλεκτρονική μορφή) με συγκεκριμένο περιεχόμενο (άρθρο 14 παρ.1). Οι όροι χρήσης στη σελίδα ενός ΕΕ ισοδυναμούν με σύμβαση.

Βασική υποχρέωση του ΕΕ είναι να επικουρεί τον ΥΕ για την άσκηση των δικαιωμάτων των υποκειμένων.

Όπως αναφέρθηκε στο κεφ. 2.2 ο Εκτελών μπορεί να μετατραπεί σε Υπεύθυνο. Θα πρέπει να πληρούνται όλοι οι όροι νομιμότητας της επεξεργασίας για να είναι δυνατή η περαιτέρω επεξεργασία των δεδομένων.

Την ευθύνη της ορθής επιλογής του Εκτελούντος την Επεξεργασία την έχει ο Υπεύθυνος (άρθρο 77). Τα υποκείμενα των δεδομένων μπορούν να ασκήσουν προσφυγή τόσο κατά του Υπευθύνου όσο και κατά του Εκτελούντος και να απαιτήσουν την επανόρθωση της ζημίας τους (άρθρο 82).

Ο Εκτελών ευθύνεται μόνον αν δεν τήρησε τους κανόνες που τον αφορούν ή αν παραβίασε εντολή του Υπεύθυνου (άρθρο 82 παρ.2).

Ωστόσο ευθύνη εις ολόκληρον απέναντι στο υποκείμενο έχουν τόσο ο Υπεύθυνος όσο και ο Εκτελών, εφόσον ευθύνονται από κοινού για την ζημία, προκειμένου να διασφαλιστεί αποτελεσματική αποζημίωση του υποκειμένου των δεδομένων.

9.6 Συνοψίζοντας

Με βάση τα παραπάνω καθορίζονται και τα ακόλουθα:

- Τα δικαιώματα των υποκειμένων και πώς αυτά ασκούνται.
- Διαβιβάσεις δεδομένων εντός και εκτός Ευρωπαϊκής Ένωσης.
- Ποια είναι η ενδεδειγμένη ασφάλεια.
- Αν η επεξεργασία (ενδέχεται να) επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες και πρέπει να διενεργηθεί Εκτίμηση Αντικτύπου στην Προστασία των Δεδομένων (υποχρεωτική στα «ευαίσθητα»).
- Διαδικασίες για την ασφάλεια, τις γνωστοποιήσεις σε περίπτωση περιστατικού.

- Ορισμός Υπεύθυνου Προστασίας Δεδομένων (Data Protection Officer – DPO).

Τα βήματα που προτείνεται να γίνουν εν συντομία είναι:

- Προσδιορισμός των πηγών από τις οποίες συλλέγονται τα δεδομένα.
  - Το ίδιο το υποκείμενο.
  - Τρίτες πηγές.
- Προσδιορισμός του σκοπού για τον οποίο συλλέγονται τα δεδομένα.
  - Έλεγχος ότι χρησιμοποιούνται για τον σκοπό αυτό.
- Έλεγχος και επιβεβαίωση ότι έχουν ενημερωθεί τα υποκείμενα σωστά και κατανοητά για τον σκοπό τον οποίο συλλέγονται τα δεδομένα.
- Επιβεβαίωση ότι έχει ληφθεί συγκατάθεση για τον συγκεκριμένο σκοπό και αν η συγκατάθεση αποτελεί επαρκή νομική βάση ή χρειάζονται επιπλέον ενέργειες.
- Έλεγχος των «χαρακτηριστικών» των δεδομένων που τηρούνται. Αν τηρούνται ευαίσθητα προσωπικά δεδομένα ή αν η επεξεργασία μπορεί να μετατρέψει απλά δεδομένα σε ευαίσθητα (τα οποία ενδέχεται να επιφέρουν υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των υποκειμένων).
- Επιλογή των κατάλληλων συνεργατών (Εκτελούντες την Επεξεργασία) που να μπορούν να εξασφαλίσουν το απαραίτητο επίπεδο προστασίας (hosting provider, cloud provider, courier, εταιρείες φύλαξης αρχείων, logistic providers κ.λπ.).
- Έλεγχος αν έχουν υιοθετηθεί οι διαδικασίες ανταπόκρισης των δικαιωμάτων των υποκειμένων που προβλέπονται στον Κανονισμό.
- Έλεγχος αν χρειάζεται να γίνει Εκτίμηση Αντικτύπου.
- Διερεύνηση ποια είναι τα κατάλληλα και ενδεδειγμένα τεχνολογικά μέτρα που πρέπει να ληφθούν.

Αν διαπιστωθεί απόκλιση σε οτιδήποτε από τα παραπάνω, τότε πρέπει να γίνει αναθεώρηση των διαδικασιών, των εγγράφων, των τεχνολογικών υποδομών που χρησιμοποιούνται και των συνεργασιών (ανά περίπτωση και όπου κρίνεται ότι υπάρχει ανάγκη) ώστε να αναπληρωθούν τα κενά.

10

PSD II και GDPR

10.1 Οδηγία για Υπηρεσίες Πληρωμών ΙΙ

Η Οδηγία για Υπηρεσίες Πληρωμών ΙΙ (Payment Service Directive II ή PSD II) είναι μια οδηγία του Ευρωπαϊκού Κοινοβουλίου και του Ευρωπαϊκού Συμβουλίου (2015/2366/EU) η οποία είναι σε ισχύ σε όλα τα κράτη-μέλη της Ευρωπαϊκής Ένωσης από τις 12 Ιανουαρίου του 2016, ενώ μπαίνει σε εφαρμογή στις 13 Ιανουαρίου 2018. (Ευρωπαϊκή Επιτροπή, 2016)

Εν συντομία η PSD II επιτρέπει στους πελάτες των Τραπεζών, είτε απλούς καταναλωτές είτε επιχειρήσεις, να χρησιμοποιούν τρίτους παρόχους για παροχή οικονομικών υπηρεσιών. Στο πολύ άμεσο μέλλον θα μπορεί κάποιος χρησιμοποιώντας το Facebook ή το Google να πληρώνει τους λογαριασμούς του, να πραγματοποιεί P2P (Peer-to-Peer)[5] συναλλαγές και να έχει ανάλυση των εξόδων του και των υπολοίπων των λογαριασμών του, ενώ τα χρήματα του είναι με ασφάλεια στον τραπεζικό του λογαριασμό.

Οι Τράπεζες (στην PSD II αναφέρονται και ως Account Servicing Payment Services Provider – ASPSP) είναι υποχρεωμένες να παρέχουν, σε αυτούς τους τρίτους παρόχους, πρόσβαση στους λογαριασμούς των πελατών τους μέσω API (Application Program Interface). Έτσι, τρίτοι θα μπορούν να δημιουργήσουν οικονομικές υπηρεσίες πάνω στα δεδομένα και τις πληροφοριακές υποδομές των Τραπεζών.

Οι Τράπεζες (οι οποίες θα μπορούν και αυτές να «καταναλώνουν» τα API των άλλων Τραπεζών) πλέον θα ανταγωνίζονται όχι μόνο άλλες Τράπεζες αλλά οποιονδήποτε προσφέρει

[5] P2P (Peer-to-Peer) στην Οικονομία, είναι ένα αποκεντρωμένο μοντέλο συναλλαγών όπου οι συναλλασσόμενοι πραγματοποιούν συναλλαγές απευθείας ο ένας με τον άλλον

οικονομικές υπηρεσίες. Το PSD II θα αλλάξει ριζικά τον τρόπο που γινόντουσαν οι πληρωμές έως σήμερα. Μέσω του PSD II η Ευρωπαϊκή Επιτροπή στοχεύει στο να προάγει την καινοτομία, να ενισχύσει την προστασία των συμφερόντων του καταναλωτή και να βελτιώσει την ασφάλεια των πληρωμών μέσω του διαδικτύου και την πρόσβαση σε λογαριασμούς εντός της Ευρωπαϊκής Ένωσης.

Η PSD II εισάγει δύο νέους τύπους παρόχων υπηρεσιών:

- Τους Παρόχους Υπηρεσιών Πληροφοριών Λογαριασμών (Account Information Service Provider – AISP). Θα αποτελεί μια online υπηρεσία για την παροχή πληροφορίας για έναν ή περισσότερους λογαριασμούς που χρησιμοποιούνται από τον χρήστη της υπηρεσίας πληρωμών.
- Τους Παρόχους Υπηρεσιών Εκκίνησης Πληρωμών (Payment Initiation Service Provider – PISP). Οι PISP είναι οι πάροχοι υπηρεσιών που ξεκινούν τη διαδικασία πληρωμών εκ μέρους του χρήστη. Οι μεταφορές χρημάτων τύπου P2P και οι πληρωμές λογαριασμών θα είναι οι συνηθέστερες υπηρεσίες PISP που θα λαμβάνουν χώρα όταν μπει σε εφαρμογή η PSD II. (EVRY, 2017)

10.2GDPR και PSD II: Η πρόκληση για τον Τραπεζικό Τομέα

Η Payment Service Directive II (PSD II) και ο General Data Protection Regulation (GDPR) έρχονται να κάνουν ακόμη πιο επίπονη την προσπάθεια που καταβάλουν οι τράπεζες στο πλαίσιο του ψηφιακού μετασχηματισμού τους. Είναι δύο κανονιστικές υποχρεώσεις οι οποίες φαίνεται να σπρώχνουν τις τράπεζες προς αντίθετες κατευθύνσεις. Από τη μια η PSD II υποχρεώνει τις τράπεζες να «ανοίξουν» τα δεδομένα των πελατών τους συμπεριλαμβανομένων των λογαριασμών τους σε τρίτες εταιρείες, από την άλλη ο ΓΚΠΔ θέτει αυστηρές απαιτήσεις – συνοδευόμενες από βαριά πρόστιμα – για την προστασία των δεδομένων των πελατών.

Στην πραγματικότητα οι δύο αυτές κανονιστικές υποχρεώσεις είναι σε άμεση συνάρτηση μεταξύ τους. Καθώς δε τίθενται σε εφαρμογή και οι δύο στο πρώτο εξάμηνο του 2018 με διαφορά λίγο μηνών μεταξύ τους, οι τράπεζες (και γενικότερα οι οργανισμοί του χρηματοπιστωτικού τομέα) πρέπει να αντιμετωπίσουν και τις δύο με ένα κοινό και ολοκληρωμένο τρόπο αντί για δύο ξεχωριστά έργα. Από την άλλη όμως η διαφορά στην ημερομηνία υλοποίησης έχει σπρώξει τα στελέχη των τραπεζών να εστιάζουν περισσότερο στη PSD II, γεγονός που αυξάνει σημαντικά το συντελεστή δυσκολίας στην υλοποίηση του ΓΚΠΔ.

10.3Πρόσβαση Τρίτων στα Δεδομένα

Παρόμοια με τον ΓΚΠΔ, η PSD II ενισχύει την έννοια της κυριότητας των δεδομένων επιτρέποντας στα υποκείμενα να επιλέξουν τον τρίτο πάροχο της αρεσκείας τους για πραγματοποίηση πληρωμών ή πρόσβαση στα οικονομικά δεδομένα τους, καθώς η Οδηγία PSD II σχεδιάστηκε για να εντείνει τον ανταγωνισμό και την καινοτομία ανάμεσα στις εταιρείες προς όφελος των καταναλωτών.

Σύμφωνα με την PSD II, οι εξωτερικοί αδειοδοτημένοι πάροχοι (συμπεριλαμβανομένων των άλλων τραπεζών) θα μπορούν:

- Να ξεκινούν συναλλαγές πληρωμών σε λογαριασμούς που τηρούνται στις τράπεζες των πελατών τους, χρησιμοποιώντας τις Διεπαφές Προγραμματισμού Εφαρμογών (Application Program Interface – API) των τραπεζών. Η οδηγία αναφέρεται σε αυτούς τους παρόχους ως Payment Initiation Service Providers (PISP) (βλ. και σελ.22).
- Να χρησιμοποιούν τα APIs των τραπεζών προκειμένου να αναλύσουν τα τραπεζικά υπόλοιπα και την κίνηση των λογαριασμών των πελατών τους, με σκοπό να προσφέρουν υπηρεσίες και προϊόντα. Η οδηγία αναφέρεται σε αυτούς τους παρόχους ως Account Information Service Providers (AISP).

Οι τράπεζες δεν έχουν το δικαίωμα να αρνηθούν την πρόσβαση στους αδειοδοτημένους παρόχους (έως τη στιγμή που γράφεται η παρούσα εργασία δεν έχουν ξεκαθαρίσει από τη ρυθμιστική αρχή οι συνθήκες που θα μπορούν οι τράπεζες να αρνηθούν την πρόσβαση). Αναμένεται στο άμεσο μέλλον να υπάρχει πρόβλεψη. (PricewaterhouseCoopers PWC, 2017)

10.3.1 Η αξία των πληρωμών είναι στα δεδομένα

Η PSD II εκτός από τα θέματα που εισάγει, είναι συγχρόνως και μια ευκαιρία για τις τράπεζες, καθώς θα μπορούν οι ίδιες να λειτουργήσουν συγχρόνως ως PISP και AISP. Αυτό θα είναι μια καλή στρατηγική για τις τράπεζες, δεδομένου ότι δεν γνωρίζει κανένας άλλος πάροχος καλύτερα τον τομέα των πληρωμών και των οικονομικών από τις ίδιες τις τράπεζες.

Το ενδιαφέρον ίσως να μην είναι καν στις πληρωμές αυτές καθ' εαυτές (εξάλλου τα περιθώρια κέρδους και οι προμήθειες των τραπεζών είναι πολύ περιορισμένα και εξακολουθούν να ακολουθούν πτωτική πορεία). Η πραγματική ευκαιρία που ανοίγεται είναι στην προστιθέμενη αξία από την συλλογή και ανάλυση σε πραγματικά δεδομένα των καταναλωτών, προκειμένου στη συνέχεια να τους προσφέρουν καινοτόμες υπηρεσίες και προϊόντα.

10.3.2 Η αξία των μεταδεδομένων (metadata)

Οι πάροχοι υπηρεσιών επικοινωνίας και κοινωνικής δικτύωσης γνωρίζουν πολύ καλά ότι ισοδύναμη ή και μεγαλύτερη αξία από την πληροφορία που υπάρχει στο κινητό μας ή στο email μας, στα tweets και στο chat, υπάρχει στον τρόπο που επικοινωνούμε. Παρόμοια όταν φθάνουμε στον τομέα των πληρωμών, υπάρχει μεγαλύτερη αξία για τον «ψηφιακό έμπορο» στην πληροφορία που εμπεριέχεται στη συναλλαγή παρά η συναλλαγή η ίδια. (PricewaterhouseCoopers PWC, 2017)

Η αξιοποίηση των πληροφοριών που συνοδεύουν τις πληρωμές έχουν πολύ μεγάλη αξία για όποιον θέλει να καταλάβει πως λειτουργεί ο πελάτης και πήρε την απόφαση να προχωρήσει στην αγορά, ή ακόμα και στο πως μπορεί να επηρεάσει ή και να αλλάξει την κατάλληλη στιγμή την απόφαση του. Οι πληροφορίες που υπάρχουν στα metadata των συναλλαγών μπορεί να περιλαμβάνουν σχετικά με τους καταναλωτές:

- Τι αγόρασαν;

- Από πού το αγόρασαν;
- Πότε το αγόρασαν;
- Πως ήταν ο καιρός τη στιγμή της αγοράς;
- Σε τι διάθεση ήταν οι πελάτες;
- Τι «ανέβασαν» στα μέσα κοινωνικής δικτύωσης (social media) πριν ή μετά την αγορά;
- Ποια μέρη είχαν επισκεφθεί ή που ακριβώς βρισκόταν πριν την αγορά;
- Με ποιους άλλους ήταν μαζί;
- Τι αγόραζαν οι άλλοι την ίδια στιγμή;

Η στιγμή που ο καταναλωτής ξοδεύει τα χρήματα του είναι πολύ σημαντική για αρκετούς και διαφορετικούς λόγους. Πρώτα από όλα για τον ίδιο τον καταναλωτή καθώς τη στιγμή που πραγματοποιεί την πληρωμή είναι περισσότερο συγκεντρωμένος σε αυτό που κάνει σε σύγκριση με τη στιγμή που στέλνει ένα email ή κάνει post κάτι στα social media. Η στιγμή που λαμβάνει χώρα μια πληρωμή είναι παράλληλα η τέλεια στιγμή για:

- Απευθείας διαφημίσεις.
- Προσφορά δανειοδότησης.
- Συλλογή δεδομένων για την αγοραστική συμπεριφορά του καταναλωτή.
- Παροχή χρήσιμων συμβουλών που ο καταναλωτής θα δείξει ενδιαφέρον.

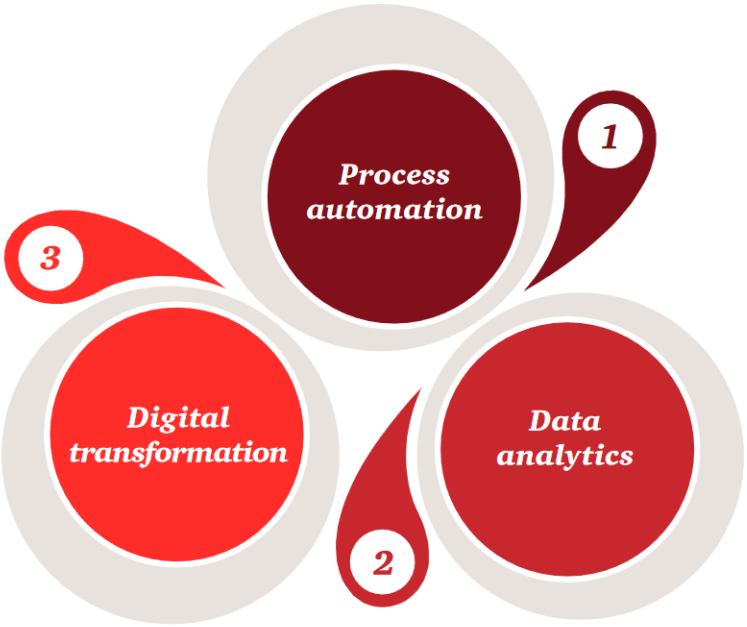
Όλα τα δεδομένα και κυρίως τα μεταδεδομένα που εισάγονται με την PSD II και αφορούν τα προσωπικά δεδομένα και την ιδιωτική ζωή του ατόμου, αποτελούν το αντικείμενο της επόμενης γενιάς κανονισμών όπως ο ΓΚΠΔ.

Η δυνατότητα της συλλογής, ανάλυσης και επεξεργασίας μεγάλου όγκου πληρωμών καθώς και των πληροφοριών και των metadata που σχετίζονται με αυτές μέσα στο νέο ψηφιακό οικοσύστημα, δίνει ισχυρό προβάδισμα σε αυτούς που θα επιδείξουν συναίσθηση και σεβασμό στα προσωπικά δεδομένα του ατόμου.

10.4 Ψηφιακός Μετασχηματισμός και Τράπεζες

Οι τράπεζες, παρά τις δυσοίωνες προβλέψεις περί «Ψηφιακής Διακοπής» (digital disruption) από τις εταιρείες τεχνολογίας που προσφέρουν οικονομικές υπηρεσίες (Fintech) φαίνεται ότι κατάφεραν και προσαρμόστηκαν γρήγορα στη νέα κατάσταση, κυρίως χάρει στην εμπειρία τους να ευθυγραμμίζονται γρήγορα με τις αλλαγές στο ρυθμιστικό και κανονιστικό πλαίσιο που διέπει τον τραπεζικό τομέα.

Το μερίδιο της αγοράς που κατάφεραν να πάρουν από τις τράπεζες οι fintech εταιρείες, όπως νέοι πάροχοι πληρωμών και ηλεκτρονικές (mobile) μόνο τράπεζες, είναι από μηδενικό έως ασήμαντο. Παρόλα αυτά τα κεφάλαια που επενδύονται στις fintech διαρκώς αυξάνονται και το κανονιστικό πλαίσιο σε πολλές χώρες γίνεται ευνοϊκό για αυτές καθιστώντας τον Ψηφιακό Μετασχηματισμό για τις τράπεζες από επιλογή σε μονόδρομο.



Source: Q4 2016 CBI/PwC survey

Στο διπλανό σχήμα είναι οι κύριοι τομείς όπου εκτιμάται ότι θα επενδύσουν οι FinTech στα επόμενα τρία χρόνια σύμφωνα με την έρευνα που πραγματοποίησαν οι CBI/PwC. (PricewaterhouseCoopers PWC, 2017)

Σύμφωνα με την ίδια έρευνα το 71% των τραπεζών διακρίνουν ο ανταγωνισμός να έρχεται από τους νέους παίκτες. Για παράδειγμα οι «καινοτόμες υπηρεσίες» των τραπεζών, όπως το phone banking, το mobile και το internet banking θα βρεθούν να ανταγωνίζονται καινοτόμες νεοφυείς εταιρείες, τηλεπικοινωνιακούς οργανισμούς, εταιρείες υψηλής τεχνολογίας κ.λπ.

Λόγω της πολυπλοκότητας που έχουν οι τράπεζες, ο μετασχηματισμός κρίσιμων παραδοσιακών υποδομών τεχνολογίας και δεδομένων έχει δημιουργήσει μια νέα αναδυόμενη αγορά και ένα νέο μοντέλο επιχειρηματικότητας. Το νέο αυτό μοντέλο προσπαθεί να επωφεληθεί από τα δεδομένα των τραπεζών, την πρόσβαση στους πελάτες και την τήρηση του κανονιστικού πλαισίου το οποίο γίνεται διαρκώς αυστηρότερο και παράλληλα να δημιουργήσει ένα ψηφιακό οικοσύστημα όπου οι καινοτόμες και πολύ περισσότερο ευέλικτες Fintech εταιρείες θα μπορούν να παρέχουν νέες και πρωτότυπες υπηρεσίες στους πελάτες των τραπεζών. Τα τελευταία λόγια έχει γίνει πολύ συζήτηση για την Uberοποίηση των πάντων. Εμπνευσμένες από την επικράτηση στην αγορά του Uber, του Airbnb και του Spotify που κερδίζουν προμήθεια απλά και μόνο με το να φέρνουν σε επαφή τους καταναλωτές με τους παρόχους των υπηρεσιών, οι τράπεζες έχουν αρχίσει να σκέφτονται για υπηρεσίες πέραν από τον έλεγχο της πρόσβασης στα δεδομένα των πελατών και στις διαδικασίες πληρωμών. Μπορούν ανοίγοντας την πρόσβαση σε τρίτους παρόχους να αυξήσουν την καθαρή θέση τους (Return Of Equity – ROE) αυξάνοντας τις πωλήσεις και βελτιστοποιώντας τις επενδύσεις (sales/assets).

10.4.1 APIs, ο δρόμος προς τον ψηφιακό μετασχηματισμό

Μια αρχιτεκτονική βασιζόμενη σε API και σύμφωνη με τις επιταγές του PSD II είναι ο πιο απλός τρόπος για να μετασχηματισθεί μια παραδοσιακή τράπεζα. Όλες οι συστημικές τράπεζες της Ελλάδας και όλες οι σημαντικότερες τράπεζες της Ευρωπαϊκής Ένωσης έχουν ετοιμάσει API προς χρήση από τους προγραμματιστές των τρίτων παρόχων προκειμένου να δημιουργήσουν τις τελικές εφαρμογές που θα «βλέπουν» οι πελάτες. Οι τράπεζες ισχυρίζονται ότι η τεχνολογία και οι έλεγχοι που περιβάλλουν τα API είναι ώριμη και κατανοητή και ότι το επόμενο λογικό βήμα είναι να ανοιχθούν, με την δέουσα προσοχή, τα API σε τρίτους.

10.5Σύνδεση GDPR και PSD II

10.5.1 Συγκατάθεση, Σκοπός και Διάρκεια τήρησης των δεδομένων

Ενώ οι «ψηφιακοί έμποροι» είναι ενθουσιασμένοι στην ευκαιρία που προσφέρεται από την PSD II να αυξήσουν τις πωλήσεις τους χρησιμοποιώντας τα δεδομένα και τα metadata των πελατών τους, ο ΓΚΠΔ το απαγορεύει αν δεν υπάρχει η σαφής συγκατάθεση του πελάτη, με οριοθετημένο σκοπό και διάρκεια. Ο πελάτης θα μπορεί επιπλέον να άρει την συγκατάθεση που είχε δώσει νωρίτερα και να απαιτήσει την διαγραφή όλων των προσωπικών του δεδομένων από την τράπεζα ή τον τρίτο πάροχο.

Ο ΓΚΠΔ προβλέπει ότι τόσο οι οργανισμοί (στην συγκεκριμένη περίπτωση οι τράπεζες) όσο και οι τρίτοι πάροχοι πρέπει να έχουν την σαφή και ρητή συγκατάθεση του πελάτη προκειμένου να χρησιμοποιήσουν τα δεδομένα του. Η συγκατάθεση αφορά και στον τρόπο που θα χρησιμοποιηθούν τα δεδομένα του πελάτη. Αν τα δεδομένα χρησιμοποιηθούν από τρίτο πάροχο πρέπει να υπάρχει η συγκατάθεση και για το ποιος είναι αυτός ο πάροχος και το πώς θα χρησιμοποιηθούν τα δεδομένα του από αυτόν.

Οι οργανισμοί και οι εταιρείες θα πρέπει να είναι σε θέση να διαχειριστούν το δικαίωμα που έχει κάθε άτομο να μπορεί να αναιρέσει τη συγκατάθεση του. Πρακτικά αυτό σημαίνει ότι οι επιχειρήσεις θα πρέπει να είναι σε θέση να σταματήσουν αμέσως την χρήση των δεδομένων του ατόμου και σε κάποιες περιπτώσεις να μπορούν να διαγράφουν τα δεδομένα από τον οργανισμό. Στην αγορά κυκλοφορούν προϊόντα για «Σύστημα Διαχείρισης Συγκατάθεσης» (Consent Management System) τα οποία εστιάζουν στη διευκόλυνση των εταιρειών για αποτελεσματική διαχείριση της συγκατάθεσης.

10.5.2 Το "Open Banking" αυξάνει την πιθανότητα περιστατικών, ο ΓΚΠΔ αυξάνει τις συνέπειες

Η PSD II επιτρέπει σε τρίτα μέρη να παρέχουν στο κοινό υπηρεσίες και προσβάσεις σε οικονομικά δεδομένα τα οποία παραδοσιακά τα ήλεγχαν οι τράπεζες. Δεδομένου ότι το ρυθμιστικό πλαίσιο δεν προβλέπει συμβατικές ευθύνες ανάμεσα στις εμπλεκόμενες επιχειρήσεις και τις τράπεζες, οι τελευταίες θα έχουν πολύ περιορισμένο έλεγχο στο πως θα διαχειρίζονται οι τρίτοι τα δεδομένα.

Για παράδειγμα θα μπορούσε ο τρίτος πάροχος να:

- χρησιμοποιεί τα δεδομένα που έχουν οι τράπεζες για παραπλανητικές πωλήσεις (misselling),
- παραβιάσει τους όρους της συγκατάθεσης του πελάτη για τη χρήση των δεδομένων του,
- διευκολύνει (εν αγνοία του) κακόβουλους τρίτους να παρακάμψουν την κυβερνοασφάλεια των τραπεζών,
- συγκεντρώνει και μεταπωλεί τα δεδομένα των πελατών σε τρίτους,
- συνδυάσει οικονομικά και ασφαλιστικά στοιχεία του πελάτη και να προχωρήσει σε υποκλοπή ταυτότητας με σκοπό την απάτη (ή και χειρότερα),
- εκθέσει το API σε επιθέσεις άρνησης πρόσβασης (Denial of Service – DoS), το οποίο θα δημιουργούσε σοβαρό πρόβλημα στους πελάτες που χρειάζονται πρόσβαση στις υπηρεσίες πληρωμών.

Σε όλα τα παραπάνω σενάρια, ο κίνδυνος για τις τράπεζες πηγάζει από το ρόλο τους ως θεματοφύλακας των δεδομένων των πελατών της και ως υπεύθυνες για τις σχέσεις με τους πελάτες. Ακόμη και αν ο τρίτος πάροχος είναι η αιτία μη συμμόρφωσης με τις απαιτήσεις του ΓΚΠΔ και η τράπεζα μπορεί να αποδείξει ότι είχε πράξει όλα τα προβλεπόμενα από τον κανονισμό (πρακτικά οι οργανισμοί δύσκολα μπορούν να αντέξουν σε ένα τέτοιο έλεγχο), η βλάβη στη φήμη και οι συνέπειες της θα επηρεάσει περισσότερο την τράπεζα παρά τον τρίτο (που όπως αναφέρθηκε θα μπορούσε να είναι και μια νεοφυής εταιρεία fintech). Αυτό θα συμβεί γιατί η κοινή γνώμη και αντίληψη είναι ότι, είναι ευθύνη της τράπεζας η προστασία των δεδομένων των πελατών της. Ακόμη και αν υπάρχει η ρητή συγκατάθεση του πελάτη, δεν θα είναι κατανοητές οι συνέπειες της ενέργειας του σε ένα τόσο πολύπλοκο οικοσύστημα «ανοιχτής τραπεζικής» και τελικά η ευθύνη θα γυρίσει στις τράπεζες.

Η ρητή συγκατάθεση, ο σκοπός και η διάρκεια πρέπει να μπορούν να αποδειχτούν προκειμένου η τράπεζα να μπορεί να αμυνθεί σε μια διένεξη με τον πελάτη ή σε περίπτωση κακής χρήσης του API της τράπεζας από τον τρίτο πάροχο. Παρόμοια και όπου το δικαίωμα στη λήθη (right to be forgotten) δεν μπορεί να εφαρμοσθεί λόγω κανονιστικών απαιτήσεων, οι τράπεζες θα πρέπει να είναι σε θέση να αποδείξουν στον έλεγχο της ρυθμιστικής αρχής ότι έχουν λάβει όλα τα απαραίτητα μέτρα για την προστασία των δεδομένων.

11

Μελέτη Περίπτωσης – Εθνική Τράπεζα

11.1Εισαγωγή

Η Εθνική Τράπεζα (στο εξής θα αναφέρεται και ως «Τράπεζα») εφαρμόζει ήδη τα προβλεπόμενα στο ισχύον κανονιστικό και νομικό πλαίσιο, όπως απορρέουν από το Ν. 2472/1997, και τις αποφάσεις της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ ή «Αρχή»). Ο ΓΚΠΔ επιφέρει σημαντικές αλλαγές στην προστασία δεδομένων προσωπικού χαρακτήρα και απαιτείται η επισκόπηση των μεταβολών σε σχέση με τις υφιστάμενες πολιτικές, διαδικασίες, τεχνικά μέσα και πρακτικές που καλύπτουν τις μέχρι σήμερα απαιτήσεις του νομικού πλαισίου. Βασικός στόχος για τη συμμόρφωση με τον ΓΚΠΔ είναι ο εντοπισμός αποκλίσεων και η καταγραφή συγκεκριμένων ενεργειών ανά επιχειρησιακή περιοχή της Τράπεζας, με σκοπό την ευθυγράμμιση με τις απαιτήσεις του ΓΚΠΔ κατά την ημέρα της εφαρμογής του (25 Μαΐου 2018).

Για τη συμμόρφωση με τον Κανονισμό ενεπλάκησαν πολλές Μονάδες της Τράπεζας με στελέχη, μεταξύ άλλων, από τις παρακάτω Γενικές Διευθύνσεις:

- Γ. Διεύθυνση Κανονιστικής Συμμόρφωσης και Εταιρικής Διακυβέρνησης
- Γ. Διεύθυνση Νομικών Υπηρεσιών
- Γ. Διεύθυνση Ανθρώπινου Δυναμικού
- Γ. Διεύθυνση Λιανικής Τραπεζικής
- Γ. Διεύθυνση Λειτουργικής Στήριξης (υπάγονται οι Δ/νσεις Πληροφορικής και το Γραφείο CISO)

11.2 Φάση 1: Χαρτογράφηση περιβάλλοντος επεξεργασίας προσωπικών δεδομένων (Data Mapping & Data Flow)

Σε αυτή τη φάση, πραγματοποιήθηκε επισκόπηση των διαθέσιμων επιχειρησιακών, τεχνικών και λειτουργικών διαδικασιών της Τράπεζας. Διοργανώθηκαν συνεντεύξεις με τα αρμόδια στελέχη της Τράπεζας προκειμένου να αναγνωριστούν οι περιοχές όπου πραγματοποιείται επεξεργασία προσωπικών δεδομένων (data processing areas). Πιο συγκεκριμένα, κατά τη διάρκεια αυτής της φάσης αναπτύχθηκε η βασική κατανόηση των εμπλεκομένων μερών (άνθρωποι, διαδικασίες και τεχνολογία) στην επεξεργασία προσωπικών δεδομένων καθ' όλη τη διάρκεια του κύκλου ζωής τους, δίνοντας κατ' επέκταση στην Τράπεζα την δυνατότητα να αναγνωρίσει και να κατανοήσει τους σχετικούς κινδύνους και τις δικλείδες ασφάλειας.

Μεταξύ των στοιχείων που συγκεντρώθηκαν προς αξιολόγηση περιλαμβάνονται τα παρακάτω:

- Οργανωτικά Διαγράμματα της εσωτερικής δομής της Τράπεζας.
- Πληροφορίες για τους υπάρχοντες ρόλους και τις υποχρεώσεις (συμπεριλαμβανομένων, όπου ήταν διαθέσιμα, πολιτικών ή περιγραφών θέσεων εργασίας που καθορίζουν τα παραπάνω).
- Αντιπροσωπευτικό δείγμα συμβολαίων με εξωτερικούς συνεργάτες.
- Καταγεγραμμένες πολιτικές, διαδικασίες, οδηγίες εργασίας κ.λπ.
- Πολιτικές και Διαδικασίες Ασφάλειας Πληροφοριακών Συστημάτων, σχετικές οδηγίες κ.λπ.
- Υφιστάμενες κοινοποιήσεις στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.
- Αποτελέσματα από τις υφιστάμενες μελέτες εκτίμησης κινδύνων ασφάλειας πληροφοριών, πληροφοριακών συστημάτων και διαβάθμισης πληροφοριών.

Ένα από τα βασικά αποτελέσματα αυτού του σταδίου ήταν η δημιουργία και εμπλουτισμός του αρχείου δραστηριοτήτων προσωπικών δεδομένων (σε γενικό επίπεδο) της Τράπεζας (high-level data process and asset registers) και η δημιουργία και ο εμπλουτισμός των καταλόγων δραστηριοτήτων και πόρων επεξεργασίας για τις επεξεργασίες προσωπικών δεδομένων υψηλού κινδύνου της Τράπεζας, κατά τα οριζόμενα στο άρθρο 30 του ΓΚΠΔ. Το αρχείο δραστηριοτήτων και πόρων επεξεργασίας της Τράπεζας περιλαμβάνει:

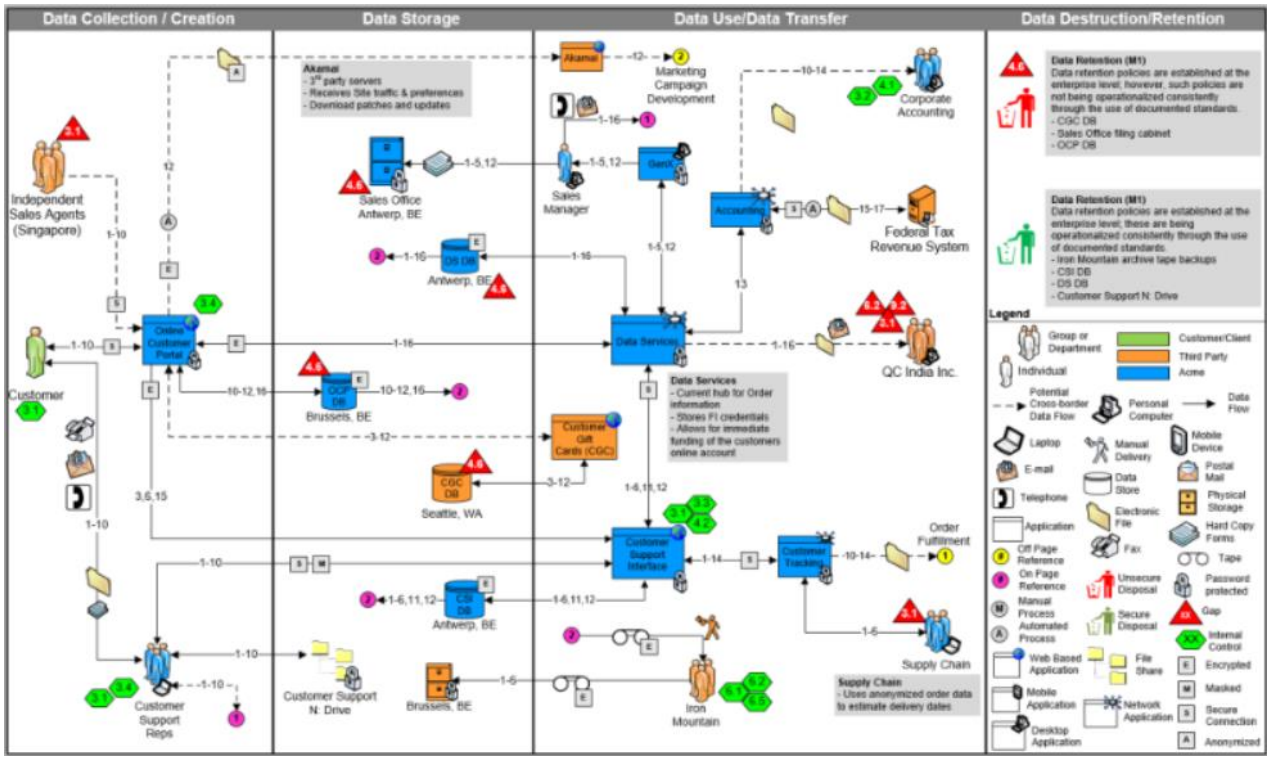
- Το όνομα και τα στοιχεία επικοινωνίας του Υπεύθυνου Επεξεργασίας, του εκπροσώπου του Υπεύθυνου Επεξεργασίας και του Υπεύθυνου Προστασίας Δεδομένων.
- Τους σκοπούς επεξεργασίας δεδομένων.
- Περιγραφή των Υποκειμένων των Δεδομένων και των κατηγοριών προσωπικών δεδομένων.
- Τις κατηγορίες των αποδεκτών στους οποίους έχουν ή πρόκειται να κοινοποιηθούν, συμπεριλαμβανομένων και αποδεκτών τρίτων χωρών ή διεθνών οργανισμών.
- Όπου υφίστανται, τα προβλεπόμενα χρονικά όρια για τη διαγραφή των διαφόρων κατηγοριών δεδομένων.

- Όπου υφίστανται, τις γενικές περιγραφές των τεχνικών και οργανωτικών δικλείδων ασφάλειας.
- Το όνομα και τα στοιχεία των Εκτελούντων ή των Υπεύθυνων Επεξεργασίας εκ μέρους των οποίων οι Εκτελούντες ενεργούν και, όπου υφίστανται, τα στοιχεία των εκπροσώπων των Εκτελούντων και των Υπεύθυνων Επεξεργασίας και του Υπεύθυνου Προστασίας Προσωπικών Δεδομένων.
- Τις κατηγορίες επεξεργασίας δεδομένων που εκτελούνται εκ μέρους του κάθε Υπεύθυνου Επεξεργασίας.

Το όφελος σε αυτή τη φάση είναι ότι σχηματίσθηκε μια καθαρή εικόνα των ροών προσωπικών δεδομένων και στη συνέχεια έγινε η χαρτογράφηση αυτών. Τα διαγράμματα ροής προσωπικών δεδομένων αποτυπώνουν τις φάσεις του κύκλου ζωής των δεδομένων, από τη συλλογή, καταχώρηση, οργάνωση, χρήση, αποθήκευση, μεταφορά έως την καταστροφή τους.

11.2.1 Δραστηριότητες που έλαβαν χώρα στην 1η φάση

- Επισκόπηση των διαθέσιμων επιχειρησιακών, τεχνικών και λειτουργικών διαδικασιών προκειμένου να γίνει κατανοητή η υφιστάμενη επεξεργασία προσωπικών δεδομένων και η σχετική τεχνολογική υποδομή.
- Αναγνώριση όλων των περιοχών που μπορούσε να πραγματοποιηθεί Εκτίμηση Αντικτύπου για την Προστασία Δεδομένων (ΕΑΠΔ). Πραγματοποιήθηκαν πολλές συναντήσεις με στελέχη της Τράπεζας από διάφορους χώρους προκειμένου να γίνει μια ολιστική επισκόπηση των επιχειρησιακών διαδικασιών και λειτουργιών της Τράπεζας, καθώς και των εφαρμογών και των συστημάτων που χρησιμοποιούνται. Για το σκοπό εκτελέσθηκαν οι παρακάτω διεργασίες:
    1. Αναγνώριση των συστημάτων.
    2. Αναγνώριση των προσωπικών δεδομένων (σε ηλεκτρονική ή έντυπη μορφή).
    3. Αναγνώριση των Υποκειμένων των Δεδομένων (πελάτες, προμηθευτές, υπάλληλοι κ.λπ).
    4. Αποτύπωση των συστημάτων και των εφαρμογών σε σχέση με τρίτα μέρη.
    5. Αναγνώριση και αποτύπωση των διοικητικών ρόλων της Τράπεζας (υπεύθυνοι επιχειρησιακών διαδικασιών και συστημάτων).
- Δημιουργία και εμπλουτισμός αρχείου δραστηριοτήτων προσωπικών δεδομένων και πόρων επεξεργασίας της Τράπεζας (high-level data process and asset registers).
- Δημιουργία και εμπλουτισμός καταλόγων δραστηριοτήτων προσωπικών δεδομένων και πόρων επεξεργασίας (data process and asset registers) για τις επεξεργασίες προσωπικών δεδομένων υψηλού κινδύνου της Τράπεζας, σύμφωνα με τα οριζόμενα στο άρθρο 30 του ΓΚΠΔ.
- Καταγραφή της ροής των δεδομένων προσωπικού χαρακτήρα (που σχετίζονται με τον ΓΚΠΔ) σε γενικό επίπεδο (high level data flow), η οποία θα περιλαμβάνει όλες τις κύριες πηγές, καθώς και τα μέσα συλλογής και αποθήκευσης δεδομένων της Τράπεζας.



Εικόνα 4: *Παράδειγμα Χαρτογράφησης Προσωπικών Δεδομένων. Συνιστάται να υπάρχει αντίστοιχο σχεδιάγραμμα για κάθε επεξεργασία προσωπικών δεδομένων* (Πηγή: Deloitte)

11.3 Φάση 2: Διαγνωστική μελέτη ανάλυσης αποκλίσεων σε σχέση με τις απαιτήσεις του Γενικού Κανονισμού για την Προστασία Δεδομένων (Gap Analysis)

Στόχος της διαγνωστικής μελέτης ανάλυσης αποκλίσεων σε σχέση με τις απαιτήσεις του ΓΚΠΔ, ήταν η έγκαιρη αναγνώριση των βασικών κενών και περιοχών προς βελτίωση στην Τράπεζα ως προς τη συμμόρφωση με τον Κανονισμό.

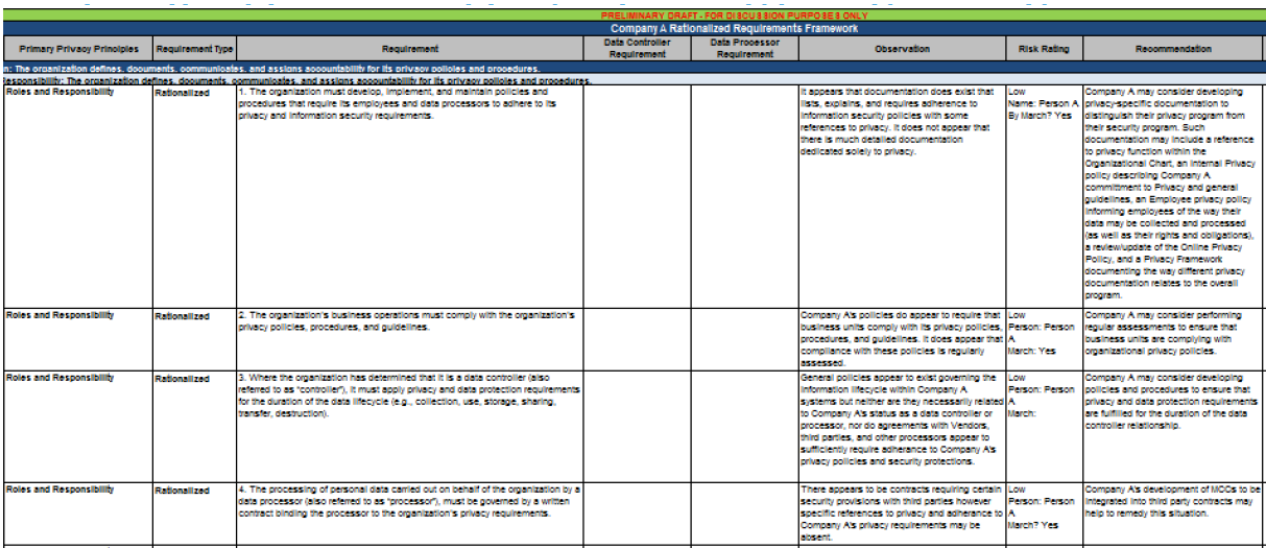
Το όφελος σε αυτή τη φάση ήταν ότι η Τράπεζα απόκτησε μια καθαρή εικόνα για τις περιοχές ελέγχου που θα χρειασθούν τις περισσότερες βελτιώσεις.

Κάθε απόκλιση που αναγνωρίσθηκε ανά περιοχή ελέγχου, συνοδευόταν από μια σύντομη περιγραφή προκειμένου να αναγνωρισθούν γρήγορα τα πιθανά θέματα που σχετίζονται με τις αποκλίσεις αυτές.

11.3.1 Δραστηριότητες που έλαβαν χώρα στη 2η φάση

- Διαγνωστική μελέτη των υφιστάμενων διαδικασιών, δεδομένων (και της διαβάθμισης τους) και συστημάτων πληροφορικής.
- Αναγνώριση των σχετικών απαιτήσεων του ΓΚΠΔ ως προς τις περιοχές επεξεργασίας προσωπικών δεδομένων.

- Ανάλυση των αποκλίσεων σχετικά με την Προστασία Προσωπικών Δεδομένων σύμφωνα με τον Κανονισμό.



PRELIMINARY DRAFT - FOR DISCUSSION PURPOSES ONLY

Company A Rationalized Requirements Framework

Primary Privacy Principles	Requirement Type	Requirement	Data Controller Requirement	Data Processor Requirement	Observation	Risk Rating	Recommendation
n: The organization defines, documents, communicates, and assigns accountability for its privacy policies and procedures.							
esponsibility: The organization defines, documents, communicates, and assigns accountability for its privacy policies and procedures.							
Roles and Responsibility	Rationalized	1. The organization must develop, implement, and maintain policies and procedures that require its employees and data processors to adhere to its privacy and information security requirements.			It appears that documentation does exist that lists, explains, and requires adherence to information security policies with some references to privacy. It does not appear that there is much detailed documentation dedicated solely to privacy.	Low Name: Person A By March? Yes	Company A may consider developing privacy-specific documentation to distinguish their privacy program from their security program. Such documentation may include a reference to privacy function within the Organizational Chart, an internal Privacy policy describing Company A commitment to Privacy and general guidelines, an Employee privacy policy informing employees of the way their data may be collected and processed (as well as their rights and obligations), a review/update of the Online Privacy Policy, and a Privacy Framework documenting the way different privacy documentation relates to the overall program.
Roles and Responsibility	Rationalized	2. The organization's business operations must comply with the organization's privacy policies, procedures, and guidelines.			Company A's policies do appear to require that business units comply with its privacy policies, procedures, and guidelines. It does appear that compliance with these policies is regularly assessed.	Low Person: Person A March: Yes	Company A may consider performing regular assessments to ensure that business units are complying with organizational privacy policies.
Roles and Responsibility	Rationalized	3. Where the organization has determined that it is a data controller (also referred to as "controller"), it must apply privacy and data protection requirements for the duration of the data lifecycle (e.g., collection, use, storage, sharing, transfer, destruction).			General policies appear to exist governing the information lifecycle within Company A systems but neither are they necessarily related to Company A's status as a data controller or processor, nor do agreements with Vendors, third parties, and other processors appear to sufficiently require adherence to Company A's privacy policies and security protections.	Low Person: Person A March:	Company A may consider developing policies and procedures to ensure that privacy and data protection requirements are fulfilled for the duration of the data controller relationship.
Roles and Responsibility	Rationalized	4. The processing of personal data carried out on behalf of the organization by a data processor (also referred to as "processor"), must be governed by a written contract binding the processor to the organization's privacy requirements.			There appears to be contracts requiring certain security provisions with third parties however specific references to privacy and adherence to Company A's privacy requirements may be absent.	Low Person: Person A March? Yes	Company A's development of MOCs to be integrated into third party contracts may help to remedy this situation.

Εικόνα 5: *Παράδειγμα παραδοτέου της μελέτης αποκλίσεων από τον ΓΚΠΔ* (Πηγή: Deloitte)

11.4 Φάση 3: Μελέτη Επιπτώσεων (Privacy Impact Assessment)

Στη φάση αυτή πραγματοποιήθηκε μελέτη των επιπτώσεων στην Προστασία Προσωπικών Δεδομένων με βάση τις απαιτήσεις του ΓΚΠΔ.

Συγκεκριμένα εκτελέστηκαν οι παρακάτω ενέργειες:

i. Περιγραφή των ροών πληροφορίας προσωπικών δεδομένων

Καθορισμός του είδους της πληροφορίας που χρησιμοποιείται, του σκοπού για τον οποίο χρησιμοποιείται, του λήπτη της πληροφορίας και της οντότητας που χρησιμοποιείται η πληροφορία.

Μερικές από τις ροές που αναλύθηκαν αφορούν:

- Τις συγκαταθέσεις επεξεργασίας προσωπικών δεδομένων.
- Την επεξεργασία προσωπικών δεδομένων, όπως:
    - Επεξεργασίες προσωπικών δεδομένων στο πλαίσιο των διαδικασιών που απαιτούνται για την πώληση των τραπεζικών προϊόντων (καταθετικά, επενδυτικά και χορηγητικά προϊόντα).
    - Διαβίβαση προσωπικών δεδομένων στη διατραπεζική εταιρία «Τειρεσίας Α.Ε.».
    - Διαβίβαση δεδομένων σε ασφαλιστικές επιχειρήσεις στο πλαίσιο τραπεζοασφαλιστικών (bancassurance) δραστηριοτήτων.
    - Επεξεργασίες προσωπικών δεδομένων στο πλαίσιο της λειτουργικής και μηχανογραφικής εξυπηρέτησης της συναλλακτικής σχέσης του πελάτη και της

Τράπεζας ή για σκοπούς διαφήμισης ή προώθησης προς αυτούς προϊόντων ή υπηρεσιών (marketing).

- Επεξεργασίες δεδομένων πελατών από τις Διευθύνσεις καρτών και προϊόντων καταναλωτικής πίστεως.
- Επεξεργασίες προσωπικών δεδομένων κατά τη σύναψη συμβάσεων χρηματιστηριακής παραγγελίας, καθώς και στο πλαίσιο της αξιολόγησης καταλληλόλητας/συμβατότητας βάσει MiFID II[6].
- Επεξεργασίες προσωπικών δεδομένων στο πλαίσιο των διαδικασιών καθυστερήσεων - ιδίως ως προς τη διαβίβαση προσωπικών δεδομένων πελατών σε τρίτους (π.χ. εταιρίες διαχείρισης ληξιπρόθεσμων οφειλών).
- Την επεξεργασία προσωπικών δεδομένων στο πλαίσιο διαχείρισης των εξασφαλίσεων (collateral) των πελατών.

- Επεξεργασίες προσωπικών δεδομένων στο πλαίσιο των διαδικασιών ανθρώπινου δυναμικού - ιδίως ως προς την τήρηση και επεξεργασία προσωπικών δεδομένων στο πλαίσιο των σχέσεων εργασίας (Οδηγία ΑΠΔΠΧ 115/2001).
- Επεξεργασίες προσωπικών δεδομένων στο πλαίσιο των διαδικασιών ανθρώπινου δυναμικού (π.χ. πρόσληψη, μισθοδοσία, προγράμματα παροχών, κ.λπ.) - ιδίως ως προς τη συλλογή και επεξεργασία υπαλλήλων της Τράπεζας που αφορούν σε δραστηριότητες εκτός των καθηκόντων που απορρέουν από την σχέση εργασίας με την Τράπεζα (π.χ. συμμετοχή σε διοικητικά συμβούλια, ενώσεις, οργανισμούς).
- Καταγεγραμμένες διαδικασίες που περιλαμβάνουν επεξεργασία προσωπικών δεδομένων στο πλαίσιο των διαδικασιών για την αξιολόγηση της πιστοληπτικής ικανότητας του υποψήφιου δανειολήπτη μέσω ενός συστήματος πιστοληπτικής διαβάθμισης (credit scoring).
- Καταγεγραμμένες διαδικασίες που περιλαμβάνουν επεξεργασία προσωπικών δεδομένων στο πλαίσιο των διαδικασιών εσωτερικού ελέγχου της Τράπεζας.
- Διαδικασία καταγγελίας δυσλειτουργιών ("Whistleblowing policy").
- Υφιστάμενες γνωστοποιήσεις στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.
- Καταγεγραμμένες διαδικασίες που περιλαμβάνουν επεξεργασία προσωπικών δεδομένων, όπως:
  - Διαβίβαση δεδομένων στις εποπτικές αρχές (π.χ. Τράπεζα της Ελλάδος, Ενιαίος Εποπτικός Μηχανισμός (SSM)), σύμφωνα με τις κανονιστικές υποχρεώσεις.
  - Διαβίβαση δεδομένων στις φορολογικές αρχές (π.χ. Γενική Γραμματεία Δημοσίων Εσόδων) σύμφωνα με τις κείμενες υποχρεώσεις (π.χ. Ν 4378/2016 και Ν 4428/2016 (CRS) ή FATCA[7]).

[6] Markets in Financial Instruments Directive. Τέθηκε σε ισχύ στις 3 Ιανουαρίου 2018 με στόχο την προστασία των επενδυτών.

[7] Foreign Account Tax Compliance Act. Διακρατική συμφωνία με ΗΠΑ για φορολογική συμμόρφωση.

- Επεξεργασίες προσωπικών δεδομένων στο πλαίσιο των διαδικασιών «Γνώρισε τον Πελάτη σου» (βάσει των απαιτήσεων του AML/CFT πλαισίου (π.χ. N 3691/200

ii. Αναγνώριση των σχετικών κινδύνων

Αναγνώριση και αξιολόγηση των κινδύνων σε επίπεδο φυσικών προσώπων (π.χ. ζημιά που ενδέχεται να προκληθεί από ανακριβή δεδομένα ή από παραβίαση ασφάλειας ή πρόκληση δυσαρέσκειας) και κίνδυνοι σε επίπεδο οργανισμού (απόκλιση συμμόρφωσης με κανονιστικές και νομικές ρυθμίσεις ή ζημιά στη φήμη του οργανισμού ή παραβίαση της ασφάλειας προσωπικών δεδομένων με τελικό αποτέλεσμα την πρόκληση σημαντικού οικονομικού κόστους).

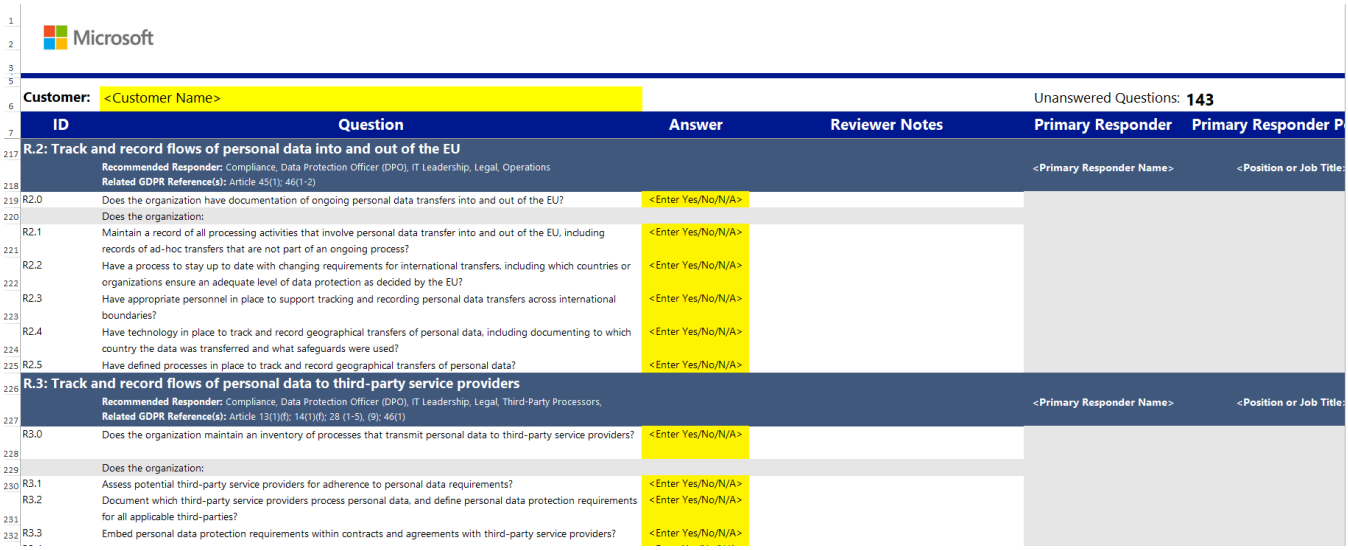
iii. Αναγνώριση και αξιολόγηση λύσεων σχετικά με την προστασία προσωπικών δεδομένων

Αναγνώριση και αξιολόγηση του τρόπου που κάθε κίνδυνος μπορεί να αντιμετωπιστεί ή να μετριασθεί σε αποδεκτά επίπεδα.

Με βάση τα αποτελέσματα των προηγούμενων φάσεων διενεργείται (η διαδικασία είναι συνεχής) εκτίμηση επιπτώσεων κατά περίπτωση (δηλαδή για τις περιοχές επεξεργασίας δεδομένων υψηλού κινδύνου). Για κάθε εύρημα, συντάσσονται οι αντίστοιχες οι αντίστοιχες διορθωτικές ενέργειες.

11.4.1 Δραστηριότητες που έλαβαν χώρα στην 3η φάση

Διενέργεια Εκτίμησης Αντικτύπου στην Προστασία Προσωπικών Δεδομένων (ΕΑΠΔ) για τις υψηλού κινδύνου περιοχές επεξεργασίας δεδομένων κατά την έννοια του άρθρου 35 του ΓΚΠΔ και όπως αυτό εξειδικεύτηκε στις Κατευθυντήριες Γραμμές της Ομάδας Εργασίας 29 (WP 248, βλ. Κεφ. 3 – Κατευθυντήριες Γραμμές για τη Διενέργεια ΕΑΠΔ)



Microsoft

Customer: <Customer Name> — Unanswered Questions: **143**

ID	Question	Answer	Reviewer Notes	Primary Responder	Primary Responder P
R.2: Track and record flows of personal data into and out of the EU	**Recommended Responder:** Compliance, Data Protection Officer (DPO), IT Leadership, Legal, Operations **Related GDPR Reference(s):** Article 45(1); 46(1-2)			<Primary Responder Name>	<Position or Job Title>
R2.0	Does the organization have documentation of ongoing personal data transfers into and out of the EU?	<Enter Yes/No/N/A>			
	Does the organization:				
R2.1	Maintain a record of all processing activities that involve personal data transfer into and out of the EU, including records of ad-hoc transfers that are not part of an ongoing process?	<Enter Yes/No/N/A>			
R2.2	Have a process to stay up to date with changing requirements for international transfers, including which countries or organizations ensure an adequate level of data protection as decided by the EU?	<Enter Yes/No/N/A>			
R2.3	Have appropriate personnel in place to support tracking and recording personal data transfers across international boundaries?	<Enter Yes/No/N/A>			
R2.4	Have technology in place to track and record geographical transfers of personal data, including documenting to which country the data was transferred and what safeguards were used?	<Enter Yes/No/N/A>			
R2.5	Have defined processes in place to track and record geographical transfers of personal data?	<Enter Yes/No/N/A>			
R.3: Track and record flows of personal data to third-party service providers	**Recommended Responder:** Compliance, Data Protection Officer (DPO), IT Leadership, Legal, Third-Party Processors, **Related GDPR Reference(s):** Article 13(1)(f); 14(1)(f); 28 (1-5), (9); 46(1)			<Primary Responder Name>	<Position or Job Title>
R3.0	Does the organization maintain an inventory of processes that transmit personal data to third-party service providers?	<Enter Yes/No/N/A>			
	Does the organization:				
R3.1	Assess potential third-party service providers for adherence to personal data requirements?	<Enter Yes/No/N/A>			
R3.2	Document which third-party service providers process personal data, and define personal data protection requirements for all applicable third-parties?	<Enter Yes/No/N/A>			
R3.3	Embed personal data protection requirements within contracts and agreements with third-party service providers?	<Enter Yes/No/N/A>			

Εικόνα 6: *Παράδειγμα εργαλείου για τη διενέργεια Εκτίμησης Αντικτύπου στα Προσωπικά Δεδομένα*
(Πηγή:https://partner.microsoft.com/en-us/marketing/details/gdpr#/)

11.5 Φάση 4: Καταγραφή σχεδίου διορθωτικών ενεργειών

Βάσει των αποτελεσμάτων των προηγούμενων φάσεων, καταγράφηκε αναλυτικό και σαφές σχέδιο στο οποίο περιλαμβάνονται οι προτάσεις βελτίωσης ανά περιοχή / μονάδα της Τράπεζας, με σκοπό την αντιμετώπιση των ελλείψεων ή και των αποκλίσεων σε σχέση με τις απαιτήσεις του ΓΚΠΔ. Το σχέδιο επέτρεψε στην Τράπεζα να ορίσει προτεραιότητες σχετικά με τις διορθωτικές ενέργειες για την αποτελεσματική και αποδοτική κάλυψη των αποκλίσεων.

11.5.1 Δραστηριότητες που έλαβαν χώρα στην 4η φάση

Καθορισμός μακροπρόθεσμης στρατηγικής συμμόρφωσης με τον ΓΚΠΔ

- Καταγραφή αναλυτικού και σαφούς σχεδίου στο οποίο συμπεριλήφθηκαν οι προτάσεις βελτίωσης ανά περιοχή. Τα σχέδιο περιέχει:
    i. Λίστα αποκλίσεων που πρέπει να καλυφθούν
    ii. Προσέγγιση και προσδιορισμό συγκεκριμένων εργασιών ώστε να βελτιωθεί κατά το δυνατόν πιο άμεσα το επίπεδο συμμόρφωσης
- Σε αυτή τη φάση χρησιμοποιήθηκαν διαγνωστικά εργαλεία και μέσα auto-discovery επικεντρωμένα στη συμμόρφωση με τον ΓΚΠΔ, την ανεύρεση των δεδομένων που χρησιμοποιούνται στο περιβάλλον της Τράπεζας καθώς και την αποτύπωση των ροών τους.

11.6 Φάση 5: Υλοποίηση απαιτούμενων ενεργειών

Βάσει των αποτελεσμάτων της προηγούμενης φάσης ορίστηκαν από την Τράπεζα οι προτεραιότητες σχετικά με τις διορθωτικές ενέργειες. Η υλοποίηση συγκεκριμένων εργασιών για τη διασφάλιση της συμμόρφωσης σύμφωνα με το νέο πλαίσιο είναι σε εξέλιξη.

11.6.1 Δραστηριότητες που έλαβαν χώρα στην 5η φάση

Υλοποίηση εργασιών για τη διασφάλιση της συμμόρφωσης με το νέο πλαίσιο:

- Βελτίωση Πολιτικής Ασφαλείας Δεδομένων η οποία στοχεύει στα ακόλουθα:
    - Να διασφαλίσει την ασφαλή τήρηση, επεξεργασία και μετάδοση των πληροφοριών.
    - Να εξασφαλίσει την πλήρη συμμόρφωση της Τράπεζας με τις σχετικές κείμενες νομικές και κανονιστικές απαιτήσεις.

- Να προστατεύσει την Τράπεζα και όσων συναλλάσσονται με αυτή για τη χρήση και διακίνηση των προσωπικών δεδομένων τους.
- Στην προστασία των υπολογιστικών πόρων και της διακινούμενης πληροφορίας από κάθε απειλή, εσωτερική ή εξωτερική, σκόπιμη ή τυχαία.
- Στις ασφαλείς διαδικασίες ανάπτυξης και συντήρησης εφαρμογών και υπηρεσιών πληροφορικής.
- Στον άμεσο και αποτελεσματικό χειρισμό περιστατικών και παραβιάσεων ασφάλειας.

- Κώδικας Δεοντολογίας σχετικά με την Επεξεργασία Προσωπικών Δεδομένων
- Τροποποίηση Συμβάσεων

Σε αυτή τη φάση χρησιμοποιήθηκαν υφιστάμενες και υλοποιήθηκαν νέες μηχανογραφικές λύσεις για τα δομημένα και τα μη δομημένα δεδομένα που τηρούνται σε ψηφιακή μορφή.

Συγκεκριμένα χρησιμοποιήθηκαν λύσεις για:

- Ανίχνευση προσωπικών δεδομένων.
- Κρυπτογράφηση και ψευδωνυμοποίηση.
- Προστασίας Διαρροής Δεδομένων.
- Ενίσχυσης της περιμετρικής ασφάλειας για αποτροπή και ανίχνευση παραβιάσεων που θα μπορούσαν να οδηγήσουν σε κλοπή, απώλεια ή αθέμιτη τροποποίηση προσωπικών δεδομένων.

11.7Φάση 6: Εκπαίδευση

Κατά τη φάση αυτή αναπτύχθηκε το πρόγραμμα εκπαίδευσης σε σχέση με τον ΓΚΠΔ.

11.7.1 Δραστηριότητες που έλαβαν χώρα στην 6η φάση

- Ανάπτυξη προγράμματος εκπαίδευσης / ευαισθητοποίησης του προσωπικού της Τράπεζας για τα ευαίσθητα δεδομένα και τον ΓΚΠΔ. Το πρόγραμμα εκπαίδευσης περιλαμβάνει μεταξύ άλλων τις παρακάτω ενότητες:
  - Εισαγωγή στις απαιτήσεις του ΓΚΠΔ.
  - Εφαρμογή των βασικών άρθρων του κανονισμού στο περιβάλλον της Τράπεζας.
  - Εκπαίδευση σε σχέση με τα εργαλεία που υποστηρίζουν τη συμμόρφωση με τις απαιτήσεις του ΓΚΠΔ.
  - Εκπαίδευση για την υλοποίηση πλαισίου παρακολούθησης των απαιτήσεων συμμόρφωσης με τον ΓΚΠΔ.

- Υλοποίηση εκπαιδευτικών ημερίδων με σκοπό την ευαισθητοποίηση του προσωπικού της Τράπεζας με τη συμμετοχή των εκπροσώπων όλων των εμπλεκομένων Διευθύνσεων της Τράπεζας.

11.8 Φάση 7: Δειγματοληπτικός έλεγχος και καταγραφή διορθωτικών ενεργειών

Στη φάση αυτή εκπονήθηκε ένα ολοκληρωμένο πρόγραμμα για τη διενέργεια ελέγχων συμμορφώσεως των Μονάδων της Τράπεζας βάσει των απαιτήσεων του Κανονισμού.

11.8.1 Δραστηριότητες που έλαβαν χώρα στην 7η φάση

- Ανάπτυξη προγράμματος διενέργειας ελέγχων συμμορφώσεως των Μονάδων της τράπεζας, σύμφωνα με τις απαιτήσεις του Κανονισμού.
- Υλοποίηση δειγματοληπτικού ελέγχου διαδικασιών και συστημάτων για εντοπισμό τυχόν ελλείψεων.
- Περιγραφή διορθωτικών ενεργειών για αποκατάσταση τυχόν ευρημάτων από τον δειγματοληπτικό έλεγχο.

11.9 Προβλήματα κατά τη συμμόρφωση με τον ΓΚΠΔ

Καθώς η διαδικασία συμμόρφωσης με τον ΓΚΠΔ είναι σε εξέλιξη και θα συνεχίσει να είναι και μετά την εφαρμογή του στις 25 Μαΐου του 2018, αναφέρονται μερικά από τα σημαντικά προβλήματα / εμπόδια που παρουσιάστηκαν.

11.9.1 Ασαφές πλαίσιο ελέγχου συμμόρφωσης με τον ΓΚΠΔ

Δεν έχει καθοριστεί έως την παρούσα στιγμή (4 μήνες πριν την εφαρμογή του ΓΚΠΔ) το πλαίσιο του ελέγχου συμμόρφωσης με τον ΓΚΠΔ σε επίπεδο Ευρωπαϊκής Ένωσης. Αυτό πρακτικά σημαίνει ότι αφενός δεν υπάρχει ένα σαφές πλαίσιο που θα ακολουθήσει ο φορέας που θα πραγματοποιήσει τον έλεγχο (εσωτερική ή εξωτερική επιθεώρηση) και αφετέρου οι οργανισμοί και οι εταιρείες δεν γνωρίζουν με σαφήνεια πως θα ελεγχθούν.

11.9.2 Ανοχή του ΓΚΠΔ στη μη διενέργεια Εκτίμησης Αντικτύπου στην Προστασία Δεδομένων έως τις 25 Μαΐου – Ασάφεια στο άρθρο 35

Ο ΓΚΠΔ δεν ορίζει με σαφήνεια στο άρθρο 35 τι θεωρεί επεξεργασία μεγάλης κλίμακας ώστε να απαιτείται η διενέργεια ΕΑΠΔ. Επίσης η εφαρμογή του Κανονισμού στις 25 Μαΐου του 2018

αφήνει περιθώριο για τη διεξαγωγή ΕΑΠΔ μετά την ημερομηνία αυτή σε όσες εφαρμογές έχουν υλοποιηθεί και ολοκληρωθεί έως τότε.

Ο επιχειρηματικός χώρος θεωρεί πως καλό είναι να αποφευχθεί η διενέργεια ΕΑΠΔ ακόμη και για περιπτώσεις που ο Κανονισμός περιγράφει με σαφήνεια ότι απαιτείται. Το έντονα ανταγωνιστικό περιβάλλον δεν αφήνει ανοχή για οποιαδήποτε καθυστέρηση στην ολοκλήρωση των έργων που είναι σε εξέλιξη και αναμένεται να ολοκληρωθούν πριν τις 25 Μαΐου. Αυτό πιθανόν να έχει αρνητικές συνέπειες στις υλοποιήσεις που θα έχουν ολοκληρωθεί έως την εφαρμογή του Κανονισμού καθώς σε εύλογο χρονικό διάστημα θα πρέπει να υπάρξει πλήρης συμμόρφωση με τον Κανονισμό.

Αντιμετώπιση

Η αντιμετώπιση του θέματος είναι εξαιρετικά δύσκολη καθώς η όποια διοικητική απόφαση θα πρέπει να ληφθεί με γνώμονα τα άμεσα και έμμεσα οφέλη και κόστη για την Τράπεζα.

11.9.3 Πολλαπλά Σημεία Αποθήκευσης Προσωπικών Δεδομένων – Αντίσταση στην αλλαγή

Η Τράπεζα έχει ενιαίο Σύστημα Διαχείρισης Πελατείας (ΣΔΠ). Σε αυτό το σύστημα υπάρχουν όλες οι απαραίτητες πληροφορίες για τους πελάτες. Στην περίπτωση που κάποιος πελάτης επιθυμεί τη λήθη, θα αρκούσε η διαγραφή του από το ΣΔΠ. Παρατηρήθηκε ειδικά στο Δίκτυο Καταστημάτων, ότι υπάλληλοι και ανώτερα στελέχη διατηρούν προσωπικά αρχεία με στοιχεία επικοινωνίας των πελατών για λόγους ευκολίας. Αυτό δημιουργεί σοβαρά θέματα στην ενιαία διαχείριση των προσωπικών δεδομένων της πελατείας, ενώ παρουσιάστηκε και περίπτωση αντίδρασης στη διαγραφή των προσωπικών αρχείων.

Αντιμετώπιση

- Μέσω του προγράμματος εκπαίδευσης γίνεται η ευαισθητοποίηση του προσωπικού σε θέματα ασφάλειας.
- Τροποποιήθηκε κατάλληλα η Πολιτική Ασφάλειας και δεν επιτρέπει την τήρηση προσωπικών δεδομένων σε προσωπικά αρχεία.
- Μέσω του εργαλείου «Ανεύρεσης Δεδομένων» και του συστήματος «Προστασίας Διαρροής Δεδομένων» ανιχνεύονται προσωπικά δεδομένα όπως Ονοματεπώνυμο, Διεύθυνση, ΑΜΚΑ, ΑΦΜ, Αρ. Λογαριασμού, Διεύθυνση κ.λπ. είτε αυτά είναι αποθηκευμένα (at rest) είτε κατά την απόπειρα εξαγωγής τους από τα συστήματα της Τράπεζας (in motion).

11.9.4 Σκιώδης Πληροφορική (Shadow IT)

Η Τράπεζα αντιμετωπίζει με επιτυχία το θέμα της «Σκιώδους Πληροφορικής». Παρόλα αυτά είναι δυνατόν να λειτουργούν αυτόνομες εφαρμογές στο cloud για κάποιος επιχειρηματικούς χώρους εν αγνοία της Πληροφορικής. Αυτό δημιουργεί πολλαπλά προβλήματα στη διαχείριση (π.χ. στη διαγραφή) και στην προστασία των δεδομένων.

Αντιμετώπιση

- Τροποποίηση της Πολιτικής Ασφάλειας και των διαδικασιών για την προμήθεια λογισμικού και υπηρεσιών.
- Συνεργασία Διεύθυνσης Προμηθειών με τις Διευθύνσεις Πληροφορικής για την ικανοποίηση των σχετικών αιτημάτων.
- Λειτουργία συστήματος CASB (Cloud Access Security Broker). Με το CASB ανιχνεύεται η πρόσβαση σε εφαρμογές στο cloud.

12

Επίλογος - Συμπεράσματα

12.1 Οι επιπτώσεις από την εφαρμογή του ΓΚΠΔ στον Τραπεζικό Τομέα

Ο Γενικός Κανονισμός Προστασίας Δεδομένων δεν αποτελεί επιλογή αλλά νομική απαίτηση η οποία είναι άμεσα εφαρμοστέα από τις 25 Μαΐου του 2018. Εισάγει ένα νέο πανευρωπαϊκό σύνολο κανόνων και θεωρείται ορόσημο στην προστασία των προσωπικών δεδομένων. Εναρμονίζει σε μεγάλο βαθμό τους εθνικούς νόμους των κρατών–μελών για την προστασία των δεδομένων που ισχύουν άμεσα σε όλα τα κράτη μέλη της ΕΕ. Λόγω του ευρύτερου γεωγραφικού του πεδίου, ο ΓΚΠΔ έχει αντίκτυπο σε πολλές επιχειρήσεις εντός και εκτός της ΕΕ εφόσον τα δεδομένα αφορούν φυσικά πρόσωπα εντός της Ευρωπαϊκής Ένωσης.

Οι κύριες επιπτώσεις από την εφαρμογή του ΓΚΠΔ στον τραπεζικό τομέα αφορούν τόσο τις σχέσεις των τραπεζών με τους πελάτες, το προσωπικό και τους προμηθευτές όσο και οργανωτικές αλλαγές και τεχνολογικές βελτιώσεις που πρέπει να υλοποιηθούν.

Οι σημαντικότερες προκλήσεις που πρέπει οι τράπεζες να είναι σε θέση να ανταποκριθούν αφορούν:

- Τη ρητή συναίνεση του υποκειμένου των δεδομένων
- Το δικαίωμα στη λήθη και στη φορητότητα των δεδομένων
- Τη διαχείριση μιας πιθανής παραβίασης με στόχο την προστασία των προσωπικών δεδομένων των φυσικών προσώπων. Η διαχείριση συμπεριλαμβάνει:
  - Άμεσες ενέργειες για τη διακοπή της παραβίασης
  - Εκτίμηση για τη φύση και το μέγεθος των δεδομένων που διέρρευσαν

– Έγκαιρη αναφορά στις Αρχές και στα υποκείμενα των δεδομένων

Οι αλλαγές που έφερε ο ΓΚΠΔ στις εταιρείες του χρηματοπιστωτικού τομέα και ιδιαίτερα στις τράπεζες αφορούν:

- Οργανωτικές: Διορισμό Υπεύθυνου για την Προστασία των Δεδομένων, αλλαγές και εμπλουτισμός της διακυβέρνησης των δεδομένων, νέες πολιτικές ή βελτιώσεις στις υφιστάμενες, εμπλουτισμός του κώδικα δεοντολογίας.
- Στην επεξεργασία: Απαιτείται σύστημα διαχείρισης για τη συναίνεση, δυνατότητα διόρθωσης των δεδομένων μετά από παρέμβαση του υποκειμένου, ασφαλής διαγραφή και δυνατότητα φορητότητας των δεδομένων.
- Στις τεχνολογίες: Αναγνώριση και κατάλογος περιοχών που έχουν προσωπικά δεδομένα, κρυπτογράφηση ή ψευδωνυμοποίηση, σύστημα διαχείρισης για τα metadata είναι μερικές από τις τεχνολογίες που θα εμπλακούν για την εφαρμογή του ΓΚΠΔ.

Μια επιπλέον συνέπεια μια πιθανής παραβίασης είναι τα βαριά πρόστιμα που προβλέπονται στον ΓΚΠΔ. Στην περίπτωση των τραπεζών όμως καθώς κλονίζεται πιθανόν ανεπανόρθωτα η φήμη και η εμπιστοσύνη της πελατείας προς την τράπεζα, διακυβεύεται η ίδια η ύπαρξη τους.

Τα παραπάνω σε συνδυασμό με την νέα Οδηγία της Ευρωπαϊκής Ένωσης για τις Υπηρεσίες Πληρωμών δημιουργούν ένα περιβάλλον όπου θα ξεχωρίσουν οι τράπεζες που θα μπορούν να ενισχύσουν τη θέση τους, επιδεικνύοντας στην πελατεία τους την ωριμότητα τους σε θέματα διακυβέρνησης των δεδομένων με τη συμμόρφωση τους με τον Γενικό Κανονισμό Προστασίας Δεδομένων.

Η μελέτη περίπτωσης της Εθνικής Τράπεζας δείχνει:

– η επιτυχία της συμμόρφωσης με τον Κανονισμό εξαρτάται από την υποστήριξη της ανώτατης διοίκησης της Τράπεζας,
– την ικανότητα και ωριμότητα που έχουν οι τράπεζες να ανταποκρίνονται γρήγορα και να προσαρμόζονται στις αλλαγές στο ρυθμιστικό περιβάλλον,
– ότι ο υψηλός βαθμός ασφάλειας και οι καλά σχεδιασμένες διαδικασίες αποτελούν σημαντικό ανταγωνιστικό πλεονέκτημα,
– ότι ο Κανονισμός περιέχει ασάφειες οι οποίες πρέπει να διευκρινιστούν,
– η συμμόρφωση με τον κανονισμό είναι μια συνεχής διαδικασία η οποία δεν θα έχει ημερομηνία λήξης τουλάχιστον για όσο διάστημα είναι σε ισχύ ο Κανονισμός.

13

Αναφορές

Deloitte. (2017). *GDPR and Industries: impact on Financial Services.* Ανάκτηση από www.deloitte.nl/gdpr

ENISA. (2009, Δδ). *Good Practices on Reporting Security Incidents.* ENISA.

EVRY. (2017). Ανάκτηση από https://www.evry.com/en/news/articles/psd2-the-directive-that-will-change-banking-as-we-know-it/

Gartner, ID: G00319929. (2017). *The Impacts of General Data Protection Regulation on MDM.*

Gartner, ID: G00326561. (2017). *Six Steps to PSD2 – Digital Banking Reimagined in Europe and Beyond.*

Gartner, ID: G00333107. (2017). *ID: G00333107, GDPR Clarity: 19 Frequently Asked Questions Answered.*

KPMG. (2017). *Ready for GDPR? Five steps to turn compliance into your advantage.*

Oliver Wyman, Tom Ivell, Barrie Wilkinson, Ben Helps. (2017). *Future Proofing Privacy: GDPR Compliance in a networked Banking System.* Oliver Wyman.

PricewaterhouseCoopers PWC. (2017). *Customer centric banking: Aligning the GDPR and PSD II.* Ανάκτηση από http://www.pwc.com/gdpr

Priority. (2017). *GDPR Holistic Approach Seminar.* Αθήνα. Ανάκτηση από www.priority.com.gr

Roland Wollf, L. M. (2017, 1 25). *Banking Hub.* Ανάκτηση από Banking Hub: https://www.bankinghub.eu/banking/finance-risk/general-data-protection-regulation

WP248, W. (2017). *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/670.*

WP249, W. (2017). *Opinion 2/2017 on data processing at work.*

WP250, W. (2017). *Guidelines on Personal data breach notification under Regulation 2016/670.*

WP251, W. (2017). *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679.*

Ευρωπαϊκή Επιτροπή. (2016). Ανάκτηση από https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366/law-details_en

Ευρωπαϊκό Κοινοβούλιο. (2016). ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2016/679 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα κα. *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, (L119/1, 4.5.2016)*.