Προστασία & Ασφάλεια Δεδομένων στα πλαίσια του GDPR

Βήματα Συμμόρφωσης για τις Επιχειρήσεις

ΔΙΑΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ (ΔΠΜΣ)

«ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ»

Master of Science in «Law and Informatics»

Αλεξάνδρα Δεσποινούδη

Επιβλέπων Καθηγητής: Ιωάννης Μαυρίδης

ΘΕΣΣΑΛΟΝΙΚΗ, Φεβρουάριος 2019

Εικόνα εξωφύλλου: www.freepik.com

Πίνακας περιεχομένων

ΠΕΡΙΛΗΨΗ

Ο Γενικός Κανονισμός Προστασίας Δεδομένων (General Data Protection Regulation – GDPR) που υιοθετήθηκε από το Ευρωπαϊκό Κοινοβούλιο και το Ευρωπαϊκό Συμβούλιο στις 27 Απριλίου 2016 αντικατέστησε την Ευρωπαϊκή Οδηγίας Προστασίας Δεδομένων 95/46/ΕΚ και βρίσκεται σε ισχύ από τις 25 Μαΐου 2018.

Οι στόχοι του νέου Κανονισμού είναι οι εξής:

- Εναρμόνιση των εθνικών νομοθεσιών για την προστασία δεδομένων ανά τα κράτη-μέλη της Ευρώπης. Μέχρι τώρα, τα κράτη-μέλη είχαν εθνικές νομοθεσίες που αντανακλούσαν τις αρχές και τους στόχους της Ευρωπαϊκής Οδηγίας του 1995, η ενσωμάτωση και εφαρμογή της οποίας ήταν στην διακριτική ευχέρεια του κάθε κράτους-μέλους με αποτέλεσμα να υπάρξουν αρκετές αποκλίσεις στην πράξη.

- Εκσυγχρονισμός των κανόνων προστασίας των προσωπικών δεδομένων δεδομένης της κλιμάκωσης των κινδύνων που ελλοχεύουν για την ιδιωτικότητα των υποκειμένων στην πλέον παγκοσμιοποιημένη οικονομία.

- Ενίσχυση των δικαιωμάτων των υποκειμένων των δεδομένων με έμφαση στην διαφάνεια και στην νόμιμη επεξεργασία των προσωπικών δεδομένων, πρόβλεψη του δικαιώματος στην λήθη και εισαγωγή του νέου δικαιώματος της φορητότητας των δεδομένων. Επιπλέον οι κανόνες για την απόκτηση της συγκατάθεσης έγιναν αυστηρότεροι και παρέχουν στους χρήστες περισσότερο έλεγχο επί των δεδομένων τους.

- Υποχρεωτικότητα συμμόρφωσης σε όλα τα επίπεδα· ο Κανονισμός εισάγει βαριές κυρώσεις και πρόστιμα για τους υπευθύνους επεξεργασίας που δεν εκπληρώνουν τις υποχρεώσεις τους είτε εξ αμέλειας είτε εκ δόλου.

Όσον αφορά τις επιχειρήσεις, και ειδικότερα τις μικρομεσαίες, οι οποίες έχουν τον ρόλο είτε του υπεύθυνου επεξεργασίας δεδομένων είτε του εκτελούντος την επεξεργασία, ο Κανονισμός προσφέρει ένα ενιαίο σταθερό έδαφος σε όλη την ΕΕ για να μπορέσουν να αναπτύξουν δραστηριότητα και σε νέες αγορές στα πλαίσια υλοποίησης

της Digital Single Market Strategy for Europe[1]. Οι υποχρεώσεις με τις οποίες βαρύνονται πλέον οι επιχειρήσεις που επεξεργάζονται προσωπικά δεδομένα – ήτοι κάθε πληροφορία που σχετίζεται με ένα ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο (το υποκείμενο των δεδομένων) – έχουν διαμορφωθεί με βάση μία κινδυνοκεντρική (riskbased) προσέγγιση και είναι ανάλογες του επιπέδου του κινδύνου ως προς τα ατομικά δικαιώματα και τις ελευθερίες των φυσικών προσώπων και της πιθανότητας επέλευσής τους. Το πεδίο εφαρμογής των διατάξεων έχει οριζόντιο χαρακτήρα, δηλαδή δεν προβλέπονται απαλλαγές ή ελαφρύτερες υποχρεώσεις ανάλογες με το μέγεθος, τους διαθέσιμους πόρους και τις δυνατότητες μία ς επιχείρησης, πλην μία ς[2]· τόσο οι μεγάλες όσο και οι μικρομεσαίες επιχειρήσεις πρέπει να ενσωματώσουν στις επιχειρησιακές τους διαδικασίες κατάλληλες πολιτικές και αποτελεσματικά μέτρα για την προστασία της ιδιωτικότητας των φυσικών προσώπων. Με μία πρώτην ματιά, το κανονιστικό πλέγμα του Κανονισμού φαίνεται σαν ένα πολύπλοκο και δύσκολα διαχειρίσιμο «βάρος» · ωστόσο οι υπεύθυνοι επεξεργασίας που θα ενσωματώσουν στον πυρήνα των καθημερινών διαδικασιών τους πολιτικές σεβασμού και προστασίας των προσωπικών δεδομένων και θα είναι σε θέση να αποδείξουν ότι έχουν λάβει τα κατάλληλα μέτρα προστασίας για να τα διατηρήσουν ασφαλή, θα αποκτήσουν «ανταγωνιστικό πλεονέκτημα» υπερτερώντας σε αξιοπιστία, φήμη και θα έχουν την ευκαιρία για ορθή διαχείριση της κάθε είδους υλικής και άυλης περιουσίας τους.

Στην παρούσα εργασία αναλύεται αρχικά όλο το πλέγμα των διατάξεων που προδιαγράφουν τις υποχρεώσεις των υπευθύνων επεξεργασίας (Ι.ΝΟΜΙΚΟ-ΡΥΘΜΙΣΤΙΚΟ ΠΛΑΙΣΙΟ) και στην συνέχεια παρουσιάζονται τα βήματα που πρέπει αυτοί να ακολουθήσουν για να επιτύχουν την μέγιστη δυνατή συμμόρφωση (ΙΙ.ΒΗΜΑΤΑ ΣΥΜΜΟΡΦΩΣΗΣ) καθώς και χρήσιμα υποδείγματα για την υλοποίησή της (ΠΑΡΑΡΤΗΜΑ).

Λέξεις Κλειδιά: ***Προσωπικά Δεδομένα, Συμμόρφωση Επιχειρήσεων, Υπεύθυνος Επεξεργασίας, Υπεύθυνος Προστασίας, Πολιτική ιδιωτικότητας, Πολιτική συγκατάθεσης, Απόδειξη Συμμόρφωσης, DPO***

[1] Στα πλαίσια αυτής της Στρατηγικής, το Συμβούλιο έδωσε έμφαση στην διευκόλυνση των επιχειρήσεων στην πρόσβαση στην online αγορά, στην βελτίωση η των ψηφιακών δικτύων και στην ενίσχυση του ψηφιακού μετασχηματισμού των μικρομεσαίων επιχειρήσεων οι οποίες αποτελούν το 99% των επιχειρήσεων στην ΕΕ. Βλ. περισσότερα, https://ec.europa.eu/commission/priorities/digital-single-market_el

[2] Βλ.παρακάτω, σελ. 10-11, *Κριτήριο μεγέθους επιχείρησης.*

Ι. ΝΟΜΙΚΟ-ΡΥΘΜΙΣΤΙΚΟ ΠΛΑΙΣΙΟ GDPR

α. Πεδίο Εφαρμογής[3]

Ουσιαστικό κριτήριο – άρθρο 2 GDPR

Οι διατάξεις του Κανονισμού αφορούν στην προστασία των φυσικών προσώπων από την αυτοματοποιημένη επεξεργασία των προσωπικών τους δεδομένων καθώς και την χειροκίνητη επεξεργασία στα πλαίσια συστήματος αρχειοθέτησης· αρχεία που δεν είναι διαρθρωμένα με συγκεκριμένα κριτήρια δεν υπάγονται στο πεδίο εφαρμογής του Κανονισμού. Οι διατάξεις δεν καλύπτουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα που αφορούν νομικά πρόσωπα και ιδίως επιχειρήσεις συσταθείσες ως νομικά πρόσωπα, συμπεριλαμβανομένης της επωνυμίας, του τύπου και των στοιχείων επικοινωνίας του νομικού προσώπου.

Εδαφικό κριτήριο – άρθρο 3 GDPR

Οι ρυθμίσεις του Κανονισμού ως προς την επεξεργασία δεδομένων προσωπικού χαρακτήρα εφαρμόζονται κατ’ αρχήν σε κάθε επεξεργασία στο πλαίσιο των δραστηριοτήτων ενός υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία εφόσον αυτός διατηρεί εγκατάσταση στην ΕΕ και ανεξάρτητα από το εάν η επεξεργασία καθ’ εαυτή διενεργείται εντός της ΕΕ. Η εγκατάσταση θα πρέπει να έχει σταθερή δομή και νομική υπόσταση (είτε ως θυγατρική είτε ως παράρτημα) και να ασκεί πραγματική και ουσιαστική δραστηριότητα.

Ωστόσο και οι μη εγκατεστημένοι στην ΕΕ υπεύθυνοι επεξεργασίας ή εκτελούντες την επεξεργασία διέπονται από τις διατάξεις του Κανονισμού σε δύο περιπτώσεις. Πρώτον, εφόσον πραγματοποιούν οιαδήποτε επεξεργασία προσωπικών δεδομένων υποκειμένων που βρίσκονται στην ΕΕ και οι δραστηριότητές τους αφορούν παροχή υπηρεσιών ή προσφορά αγαθών. Για να πληρείται η προϋπόθεση της προσφοράς υπηρεσιών ή αγαθών θα πρέπει να εκτιμηθεί κατά πόσο ο υπεύθυνος ή ο εκτελών την επεξεργασία δείχνει σαφή

[3] Βλ. περισσότερα, Σημειώσεις 22-24 Προοίμιο.

πρόθεση να δραστηριοποιηθεί σε κοινό της ΕΕ· ήτοι, η παροχή απλής δυνατότητας πρόσβασης σε ιστοσελίδα ή σε στοιχεία επικοινωνίας του υπευθύνου επεξεργασίας ή του εκτελούντος ή κάποιου ενδιάμεσου παράγοντα δεν καταδεικνύει πρόθεση δραστηριοποίησης στην ΕΕ, ενώ αντίθετα η χρήση γλώσσας ή νομίσματος ενός ή περισσοτέρων κρατών-μελών της ΕΕ και ειδικά σε σελίδες με δυνατότητα παραγγελίας υπηρεσιών και αγαθών καθιστά εμφανή την πρόθεση του υπεύθυνου επεξεργασίας να απευθυνθεί και σε υποκείμενα δεδομένων της ΕΕ. Δεύτερον, εφόσον η επεξεργασία προσωπικών δεδομένων υποκειμένων της ΕΕ συνίσταται στην παρακολούθηση της συμπεριφοράς των εν λόγω υποκειμένων στο πλαίσιο που αυτή αναπτύσσεται μέσα στα όρια της ΕΕ. Προκειμένου να κριθεί εάν μία επεξεργασία συνιστά παρακολούθηση της συμπεριφοράς φυσικών προσώπων πολιτών της ΕΕ θα πρέπει να εκτιμηθεί κατά πόσον καταγράφεται η συμπεριφορά των εν λόγω υποκειμένων στο Διαδίκτυο και πως χρησιμοποιούνται στην συνέχεια οι συλλεγείσες πληροφορίες, ιδίως για την κατάρτιση προφίλ και με σκοπό την αυτοματοποιημένη λήψη αποφάσεων ή την ανάλυση και πρόβλεψη των προσωπικών προτιμήσεών τους με απώτερη εμπορική ή κοινωνικοπολιτική στόχευση.

Κριτήριο μεγέθους επιχείρησης

Προκειμένου να επιτευχθεί η μέγιστη δυνατή προστασία των φυσικών προσώπων, ο Κανονισμός υπαγορεύει την οριζόντια και ενιαία συμμόρφωση των επιχειρήσεων χωρίς δυνατότητα μεθοδεύσεων για την αποφυγή των προβλεπόμενων υποχρεώσεων. Το εάν μία επιχείρηση υπάγεται στις διατάξεις του Κανονισμού ως εν δυνάμει υπεύθυνος επεξεργασίας ή εκτελών την επεξεργασία δεν εξαρτάται από το μέγεθος της επιχείρησης και τους διαθέσιμους πόρους (υλικούς ή ανθρώπινους) αλλά από την φύση της δραστηριότητας που ασκεί· συνεπώς, όλες οι επιχειρήσεις ανεξαρτήτως αριθμού εργαζομένων, ήτοι και οι μικρές και μεσαίες επιχειρήσεις, εφόσον επεξεργάζονται προσωπικά δεδομένα υπόκεινται στο ρυθμιστικό πλαίσιο του Κανονισμού.

Ωστόσο το άρθρο 30 παρ. 5 θέτει μία εξαίρεση για τις μικρομεσαίες

επιχειρήσεις με λιγότερους από 250 εργαζόμενους, αλλά και μία εξαίρεση της εξαίρεσης: κατ' αρχήν τις εξαιρεί από την υποχρέωση τήρησης αρχείων δραστηριοτήτων επεξεργασίας· ωστόσο ορίζει ότι ακόμα και εάν έχουν λιγότερους από 250 εργαζόμενους, εάν η επεξεργασία που εκτελούν ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες του υποκειμένου είτε η διενεργούμενη επεξεργασία δεν είναι περιστασιακή ή περιλαμβάνει ευαίσθητα προσωπικά δεδομένα ή προσωπικά δεδομένα που αφορούν ποινικές καταδίκες, τότε υποχρεούται στην τήρηση αρχείου δραστηριοτήτων επεξεργασίας.

β. Έννοιες: Προσωπικά Δεδομένα και Επεξεργασία, Υπεύθυνος Επεξεργασίας, Εκτελών την Επεξεργασία

Σύμφωνα με τους ορισμούς που παρατίθενται στο άρθρο 4 του Κανονισμού,

> «**Δεδομένα προσωπικού χαρακτήρα**» *συνιστούν κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»)· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στην σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου.*

Οι αρχές της προστασίας δεδομένων πρέπει να εφαρμόζονται σε κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο. Προκειμένου να διαπιστωθεί εάν η ταυτότητα ενός φυσικού προσώπου μπορεί να εξακριβωθεί, θα πρέπει να λαμβάνονται υπόψη όλα τα μέσα τα οποία είναι ευλόγως δυνατό ή πιθανό να χρησιμοποιηθούν· ειδικότερα, θα πρέπει να εκτιμηθούν όλοι οι σχετικοί αντικειμενικοί παράγοντες, όπως το κόστος και ο χρόνος που απαιτούνται για την ταυτοποίηση, καθώς και η υπάρχουσα κατά τον

χρόνο της επεξεργασίας διαθέσιμη τεχνολογία αλλά και η ευλόγως προσδοκώμενη εξέλιξή της πριν την πάροδο του νομίμου χρόνου επεξεργασίας[4]. Αντιθέτως, οι ανώνυμες ή ανωνυμοποιημένες πληροφορίες, ήτοι αυτές που δεν μπορούν να συσχετιστούν με κάποιο συγκεκριμένο φυσικό πρόσωπο και να το προσδιορίσουν, και οι οποίες μπορούν μεταξύ άλλων να χρησιμοποιηθούν για στατιστικούς ή ερευνητικούς σκοπούς, δεν αποτελούν προσωπικά δεδομένα και δεν χρήζουν προστασίας υπό τον παρόντα Κανονισμό. Ωστόσο, οι πληροφορίες που έχουν υποστεί ψευδωνυμοποίηση[5], ήτοι κρυπτογράφηση, εφόσον με την χρήση του κατάλληλου κλειδιού μπορούν να αποδοθούν σε συγκεκριμένο φυσικό πρόσωπο και να το ταυτοποιήσουν, θεωρούνται προσωπικά δεδομένα και καλύπτονται από τις γενικές αρχές που διέπουν την επεξεργασία[6].

Επίσης υπάρχουν ειδικές κατηγορίες δεδομένων, τα λεγόμενα «ευαίσθητα δεδομένα», τα οποία απαιτούν αυξημένη προστασία, υπόκεινται σε ειδικό νομικό καθεστώς και γι' αυτό διακρίνονται από τα υπόλοιπα προσωπικά δεδομένα, τα οποία η θεωρία ονόμασε «απλά»[7]. Η κατηγορία των ευαίσθητων προσωπικών δεδομένων αφορά πληροφορίες οι οποίες εκ φύσεως μπορούν να θέσουν σε κίνδυνο τα θεμελιώδη δικαιώματα και τις ελευθερίες των φυσικών προσώπων και ως εκ τούτου πρέπει να πληρούνται ειδικές προϋποθέσεις και να παρέχονται ειδικές εγγυήσεις για το νόμιμο της επεξεργασίας τους[8].

Στο αρθ. 9 παρ. 1 απαριθμούνται τα ευαίσθητα προσωπικά δεδομένα τα οποία περιλαμβάνουν πληροφορίες σχετικές με:

---

[4] Βλ. περισσότερα, Ομάδα εργασίας του άρθρου 29, Γνώμη 4/2007 σχετικά με την έννοια των δεδομένων προσωπικού χαρακτήρα, WP 136, 20 Ιουνίου 2007

[5] Βλ. περισσότερα παρακάτω, Υποσημειώσεις 41 και 107.

[6] Περισσότερα για την διάκριση ανωνυμοποιημένων και ψευδωνυμοποιημένων δεδομένων βλ. *Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων*, σελ. 52-55.

[7] Στα απλά προσωπικά δεδομένα περιλαμβάνονται το όνομα, το επώνυμο, η κατοικία, το επάγγελμα – αμοιβή – ιστορικό εργασίας, το μορφωτικό επίπεδο, οικογενειακή κατάσταση, κοινωνικές επαφές, οι καταναλωτικές συνήθειες, ενδιαφέροντα – συνήθειες, μετακινήσεις – ταξείδια, περιουσιακά στοιχεία – έσοδα – δάνεια – τραπεζικοί λογαριασμοί, ηλεκτρονικά δεδομένα θέσης και κίνησης, διεύθυνση IP και MAC, κ.α. Βλ. περισσότερα στο Παράρτημα του Εντύπου 2.0 γνωστοποίησης αρχείου προσωπικών δεδομένων της ΑΠΔΠΧ, www.dpa.gr

[8] Σημείωση 51 Προοίμιο: «*Εκτός από τις ειδικές απαιτήσεις στις οποίες υπάγεται η εν λόγω επεξεργασία, θα πρέπει να εφαρμόζονται οι γενικές αρχές και οι λοιποί κανόνες του παρόντος κανονισμού, ιδίως σε ό,τι αφορά τους όρους νόμιμης επεξεργασίας.*»

- την φυλετική ή εθνοτική καταγωγή
- τα πολιτικά φρονήματα
- τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις
- την συμμετοχή σε συνδικαλιστική οργάνωση
- τα γενετικά ή βιομετρικά δεδομένα
- την υγεία
- την σεξουαλική ζωή
- τον γενετήσιο προσανατολισμό
- τις ποινικές διώξεις ή καταδίκες (αρθ. 10)

> **«Επεξεργασία»** *αποτελεί κάθε πράξη ή σύνολο πράξεων που πραγματοποιείται με ή χωρίς την χρήση αυτοματοποιημένων μεθόδων σε προσωπικά δεδομένα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα. Ειδικότερα, η συλλογή, η καταχώριση ή/και η αποθήκευση σε βάση δεδομένων, η οργάνωση ή/και η διάρθρωση σε αρχείο, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών με queries, η χρήση, η κοινολόγηση σε τρίτους με διαβίβασή τους, η διάδοση και κάθε άλλη μορφή διάθεσης σε τρίτους, η συσχέτιση ή/και ο συνδυασμός τους, ο περιορισμός, η μερική ή ολική διαγραφή ή καταστροφή τους.*

Με τον όρο «επεξεργασία» νοείται κυρίως η αυτοματοποιημένη επεξεργασία, ωστόσο περιλαμβάνεται και η μη αυτοματοποιημένη επεξεργασία, δηλαδή αυτή που πραγματοποιείται σε δομημένα αρχεία με συμβατικά τεχνικά ή μη μέσα.

Πρακτικά παραδείγματα επεξεργασίας αποτελούν:

- η διοίκηση προσωπικού και η διαχείριση της μισθοδοσίας

- πρόσβαση σε βάση δεδομένων με προσωπικά δεδομένα

- αποστολή προωθητικών μηνυμάτων*

- καταστροφή εγγράφων που περιέχουν προσωπικά δεδομένα

- αποθήκευση διευθύνσεων IP ή MAC

- βιντεοεπιτήρηση (CCTV)

*Στην περίπτωση των προωθητικών email για λόγους διαφήμισης και marketing θα πρέπει ο υπεύθυνος επεξεργασίας να συμμορφώνεται κατ' αρχήν με τους κανόνες της Οδηγίας ePrivacy[9].

> **«Υπεύθυνος Επεξεργασίας»** *είναι το φυσικό ή νομικό πρόσωπο που μόνο του ή από κοινού με άλλα καθορίζουν τους σκοπούς και τον τρόπο επεξεργασίας προσωπικών δεδομένων.*
>
> **«Εκτελών την επεξεργασία»** *είναι το φυσικό ή νομικό πρόσωπο που υλοποιεί την επεξεργασία των δεδομένων προσωπικού χαρακτήρα για λογαριασμό του υπεύθυνου επεξεργασίας και στα πλαίσια μεταξύ τους σύμβασης.*

Ειδικότερα η κατανομή των αρμοδιοτήτων μεταξύ του υπευθύνου και του εκτελούντος την επεξεργασία έχει ιδιαίτερη σημασία λαμβανομένων υπ' όψιν των υποχρεώσεων και ευθυνών που ο εκάστοτε νομικός χαρακτηρισμός επιφέρει σε καθέναν από τους δύο ρόλους.

Ο υπεύθυνος επεξεργασίας καθορίζει την πολιτική προστασίας των προσωπικών δεδομένων και φέρει την ευθύνη για την εκτελούμενη επεξεργασία είτε την πραγματοποιεί ο ίδιος είτε άλλος για λογαριασμό του· συνήθως είναι νομικό πρόσωπο, μία εταιρεία ή ένας οργανισμός και όχι ένα συγκεκριμένο φυσικό πρόσωπο. Ο χαρακτηρισμός του υπευθύνου μπορεί να του αποδίδεται είτε από τον νόμο είτε εν τοις πράγμασι λόγω άσκησης συγκεκριμένων αρμοδιοτήτων. Ειδικότερα:

α) προσδιορίζει τους στόχους και τους σκοπούς της συλλογής και της επεξεργασίας των προσωπικών δεδομένων,

[9] ΟΔΗΓΙΑ 2002/58/ΕΚ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 12ης Ιουλίου 2002 σχετικάμε την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες), όπως αυτή τροποποιήθηκε από την ΟΔΗΓΙΑ 2009/136/ΕΚ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ, της 25ης Νοεμβρίου 2009. Βλ. περισσότερα παρακάτω, σελ. 84, *Πολιτική Συγκατάθεσης.*

β) παρέχει στα υποκείμενα των δεδομένων την δυνατότητα άσκησης των νομίμων δικαιωμάτων τους,

γ) εξασφαλίζει την συμμόρφωση της επιχείρησής του προς το εφαρμοστέο εθνικό και ενωσιακό δίκαιο και

δ) προβλέπει την λήψη κατάλληλων οργανωτικών και τεχνικών μέτρων για την διασφάλιση της προστασίας και της ασφάλειας των προσωπικών δεδομένων

Ο εκτελών την επεξεργασία αναλαμβάνει υποχρεώσεις και ευθύνες μόνο κατόπιν εντολής από τον υπεύθυνο επεξεργασίας ο οποίος και καθορίζει τα όρια των αρμοδιοτήτων του πρώτου. Ως εκτελών την επεξεργασία μπορεί να οριστεί φυσικό πρόσωπο (π.χ. υπάλληλος του υπευθύνου επεξεργασίας) ή νομικό πρόσωπο με γραπτή συμφωνία εξωτερικής ανάθεσης με προϋπόθεση να παρέχουν επαρκείς βεβαιώσεις για την τεχνική τους κατάρτιση επί του ρόλου που καλούνται να αναλάβουν· σε κάθε περίπτωση – και ειδικότερα στην περίπτωση outsourcing – τα μέτρα εξασφάλισης της ιδιωτικότητας και της ασφάλειας των προσωπικών δεδομένων θα πρέπει να είναι ξεκάθαρα και προσυμφωνημένα, έστω και με γενική περιγραφή[10]. Συγκεκριμένα ο εκτελών την επεξεργασία μπορεί να:

α) προσδιορίζει τους ειδικότερους τεχνικούς τρόπους για την εκτέλεση της επεξεργασίας

β) υλοποίει την καθ' εαυτήν επεξεργασία δεδομένων προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας

γ) εφαρμόζει τα κατάλληλα οργανωτικά και τεχνικά μέτρα ασφαλείας για την προστασία των προσωπικών δεδομένων είτε καθ' υπόδειξη του υπευθύνου επεξεργασίας είτε επιλέγοντάς τα ο ίδιος.

Πρέπει να σημειωθεί, ότι σύμφωνα με την παρ. 9 του αρθ. 28 «*εάν ο εκτελών την επεξεργασία καθορίσει κατά παράβαση του παρόντος κανονισμού τους σκοπούς και τα μέσα της επεξεργασίας, ο εκτελών την επεξεργασία θεωρείται υπεύθυνος επεξεργασίας για την συγκεκριμένη επεξεργασία*».

[10] Βλ. άρθρο 28 Κανονισμού.

γ. Αρχές επεξεργασίας (αρθ. 5)

Ο Κανονισμός επιτάσσει την τήρηση συγκεκριμένων αρχών προκειμένου η επεξεργασία των προσωπικών δεδομένων να θεωρηθεί νόμιμη και θεμιτή. Οι αρχές επεξεργασίες προβλέπονται στο άρθρο 5 του Κανονισμού και είναι οι κάτωθι:

1. Αρχή της νομιμότητας (in principio) και της διαφάνειας (γνώμη ομάδας 29 transparency)

Η αρχή της νομιμότητας υπαγορεύει ότι η επεξεργασία προσωπικών δεδομένων είναι νόμιμη μόνον εάν: είναι σύμφωνη με τον νόμο και επιδιώκει θεμιτό σκοπό[11].

Η αρχή της διαφάνειας είναι η πρωταρχική υποχρέωση των υπευθύνων επεξεργασίας υπό τον νέο Κανονισμό και επικεντρώνεται σε τρία επίπεδα: 1) στην παροχή πληροφοριών στα υποκείμενα των δεδομένων περί των σκοπών της επεξεργασίας, 2) στην γνωστοποίηση των δικαιωμάτων των υποκειμένων των δεδομένων, 3) στην διευκόλυνση των υποκειμένων των δεδομένων ως προς την άσκηση των δικαιωμάτων τους και στην σύννομη διεκπεραίωσή τους.

Θα πρέπει να είναι σαφές για τα φυσικά πρόσωπα ότι δεδομένα προσωπικού χαρακτήρα που τα αφορούν συλλέγονται, χρησιμοποιούνται, ή υποβάλλονται καθ' οιονδήποτε τρόπο σε επεξεργασία. Η αρχή αυτή απαιτεί κάθε πληροφορία και ανακοίνωση σχετικά με την επεξεργασία των εν λόγω δεδομένων προσωπικού χαρακτήρα να είναι εύκολα προσβάσιμη και κατανοητή και να χρησιμοποιεί σαφή και απλή γλώσσα. Ειδικότερα απαιτείται η γνωστοποίηση στα υποκείμενα των δεδομένων της ταυτότητας του υπευθύνου επεξεργασίας και των σκοπών της επεξεργασίας και η

[11] Δικαιολογημένη επέμβαση κατά την ΕΣΔΑ (αρθ. 8 παρ.2) και τον Χάρτην Θεμελιωδών Δικαιωμάτων (αρθ.52). «*Η επεξεργασία προσωπικών δεδομένων ενδέχεται να συνιστά επέμβαση στο δικαίωμα σεβασμού της ιδιωτικής ζωής του υποκειμένου των δεδομένων. Ωστόσο, το δικαίωμα σεβασμού της ιδιωτικής ζωής δεν είναι απόλυτο, πρέπει δε να σταθμίζεται και να εναρμονίζεται με άλλα νόμιμα συμφέροντα, είτε άλλων προσώπων (ιδιωτικά συμφέροντα) είτε της κοινωνίας συνολικά (δημόσιο συμφέρον)*». Βλ. περισσότερα, Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων σελ. 76-83

ενημέρωσή τους για την ύπαρξη κινδύνων, κανόνων, εγγυήσεων και δικαιωμάτων σε σχέση με την επεξεργασία δεδομένων προσωπικού χαρακτήρα και πώς να ασκούν τα δικαιώματά τους σε σχέση με την επεξεργασία αυτή[12].

2. Αρχή του προσδιορισμού του σκοπού

Απαιτείται πάντοτε ένας σκοπός στον οποίο αποβλέπει η επεξεργασία των προσωπικών δεδομένων των υποκειμένων και ο οποίος θέτει τα όρια της ad hoc νομιμότητας· ο σκοπός πρέπει να είναι α) νόμιμος, να είναι σύμφωνος με τα συνταγματικά και τα εθνικά νομικά πλαίσια και β) συγκεκριμένος, ώστε αφ' ενός να μπορέσει το υποκείμενο να ενημερωθεί και να δώσει την συγκατάθεσή του αφ' ετέρου ο υπεύθυνος επεξεργασίας να μην μπορεί αυθαίρετα να χρησιμοποιεί τα δεδομένα για άλλους σκοπούς χωρίς προηγούμενη συγκατάθεση ή στήριξη σε έτερη νομική βάση[13]. Τα ίδια ισχύουν και για τον τρόπο και τα μέσα επεξεργασίας.

3. Αρχή της αναλογικότητας

Σύμφωνα με την οποία πρέπει να υπάρχει αυστηρή αιτιώδης σχέση μεταξύ του σκοπού της επεξεργασίας και των συλλεγόμενων δεδομένωμ· ήτοι αυτά θα πρέπει να είναι κατάλληλα, συναφή και να περιορίζονται στα ελάχιστα αναγκαία προς τους σκοπούς της επεξεργασίας. Η Ε. Αλεξανδροπούλου προτείνει για τον έλεγχο της συμμόρφωσης με την αρχή της αναλογικότητας την «δοκιμασία δύο σταδίων» (two steps test ή épreuve de deux étapes): «*Σε πρώτο στάδιο χρησιμοποιείται το ποιοτικό κριτήριο, το οποίο απαιτεί τα επεξεργαζόμενα δεδομένα να είναι συναφή και κατάλληλα για τον σκοπό της επεξεργασίας· σε δεύτερο στάδιο χρησιμοποιείται το ποσοτικό κριτήριο σύμφωνα με το οποίο τα προς επεξεργασία δεδομένα*

[12] Βλ. σημείωση 39 Προοίμιο.

[13] Νομικές βάσεις νόμιμης επεξεργασίας: συγκατάθεση, έννομη υποχρέωση υπευθύνου, σύμβαση, πρόθεση σύναψης σύμβασης, συμβατός σκοπός, δημόσιο συμφέρον, έννομο συμφέρον υπεύθυνου. Άρθ. 6 Κανονισμού και σημειώσεις 44-50 και 69 Προοίμιου. Βλ. παρακάτω και σελ. 23, *Νομιμότητα της Επεξεργασίας.*

πρέπει να είναι όσο το δυνατόν λιγότερα απαιτούνται για την εξυπηρέτηση του σκοπού της επεξεργασίας. Αν η επεξεργασία δεν πληροί το ποιοτικό κριτήριο, τότε αυτή είναι παράνομη και παρέλκει η εξέταση του ποσοτικού κριτηρίου»[14]. Τα ίδια ισχύουν και για τον τρόπο και τα μέσα επεξεργασίας.

4. Αρχή της ακρίβειας

Σύμφωνα με αυτή τα δεδομένα που τηρούνται σε αρχείο πρέπει να ανταποκρίνονται στην πραγματικότητα, να είναι ακριβή και να επικαιροποιούνται ή μη αναλόγως του επιδιωκόμενου σκοπού. Υπάρχουν περιπτώσεις στις οποίες η επικαιροποίηση των αποθηκευμένων δεδομένων απαγορεύεται διά νόμου, διότι ο κύριος σκοπός της συλλογής και αποθήκευσης των δεδομένων είναι η τεκμηρίωση συμβάντων· αντιθέτως, υπάρχουν περιπτώσεις στις οποίες είναι απολύτως αναγκαίο να ελέγχεται η ακρίβεια των δεδομένων σε τακτά χρονικά διαστήματα και εάν χρειάζεται, να επικαιροποιούνται, λόγω ενδεχόμενης ζημίας που θα μπορούσε να υποστεί το υποκείμενο των δεδομένων εάν αυτά παραμείνουν ανακριβή.

5. Αρχή του περιορισμού της περιόδου αποθήκευσης – εξαίρεση

Σύμφωνα με την εν λόγω αρχή «τα προσωπικά δεδομένα διατηρούνται σε μορφή που επιτρέπει τον προσδιορισμό της ταυτότητας των προσώπων στα οποία αναφέρονται μόνον για χρονική περίοδο που δεν υπερβαίνει την απαιτούμενη για την επίτευξη των σκοπών της συλλογής και της επεξεργασίας τους»· ειδικότερα θα πρέπει το διάστημα αποθήκευσης των δεδομένων προσωπικού χαρακτήρα να περιορίζεται στο ελάχιστο δυνατό. Για να διασφαλιστεί ότι τα δεδομένα προσωπικού χαρακτήρα δεν διατηρούνται περισσότερο από όσο είναι αναγκαίο, ο υπεύθυνος επεξεργασίας θα πρέπει να ορίζει προθεσμίες για την διαγραφή τους ή για την περιοδική επανεξέτασή τους.

Ο χρονικός περιορισμός της αποθήκευσης δεδομένων μπορεί να αρθεί

[14] Ε. Αλεξανδροπούλου-Αιγυπτιάδου, *Προσωπικά Δεδομένα*, Εκδόσεις Νομική Βιβλιοθήκη, σελ. 73-74

σε περιπτώσεις που τα δεδομένα θα υποβάλλονται σε επεξεργασία για σκοπούς αρχειοθέτησης δημοσίου συμφέροντος, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς, εφόσον υποβληθούν στα κατάλληλα τεχνικά μέτρα ώστε να διατηρούνται με μορφή που να μην επιτρέπει την εξακρίβωση της ταυτότητας των προσώπων στα οποία αναφέρονται. Ως εκ τούτου, νόμιμη αποθήκευση για μεγαλύτερα διαστήματα μπορεί να επιτευχθεί εάν αυτά καταστούν ανώνυμα ή ψευδώνυμα κατά τις ειδικότερες επιταγές του άρθρου 89 παρ.1 του Κανονισμού.

6. Αρχή της εμπιστευτικότητας και της ακεραιότητας

Η αρχή της ασφάλειας των προσωπικών δεδομένων συνίσταται στην υποχρέωση λήψης των κατάλληλων οργανωτικών και τεχνικών μέτρων ασφαλείας εκ μέρους του υπευθύνου της επεξεργασίας προκειμένου τα δεδομένα και ο εξοπλισμός που χρησιμοποιείται για την επεξεργασία τους να προστατευθούν από παράνομη ή άνευ εξουσιοδότησης πρόσβαση, αλλοίωση, καταστροφή ή φθορά κατά τις ειδικότερες επιταγές του άρθρο 32 του Κανονισμού.

7. Αρχή της λογοδοσίας

Κατ' επιταγή της νεοεισαχθείσας αυτής αρχής, ο υπεύθυνος επεξεργασίας των δεδομένων θα πρέπει να λογοδοτεί, κατόπιν αιτήματος της ΑΠΔΠΧ, για την συμμόρφωσή του προς τους κανόνες του Κανονισμού και για τα μέτρα που εφαρμόζει για την υλοποίηση των ανωτέρω αναφερόμενων αρχών.

Σύμφωνα με την γνώμη της ομάδας εργασίας του άρθρου 29[15], πυρήνας της αρχής της λογοδοσίας είναι η υποχρέωση του υπεύθυνου επεξεργασίας α) να εφαρμόζει κατάλληλα μέτρα τα οποία –υπό κανονικές συνθήκες– διασφαλίζουν την τήρηση των κανόνων για την προστασία των δεδομένων στο πλαίσιο της επεξεργασίας και β) να διαθέτει έγγραφα τα οποία θα αποδεικνύουν στα υποκείμενα των δεδο-

[15] Ομάδα εργασίας αρθ. 29, *Γνώμη 3/2010 σχετικά με την αρχή της λογοδοσίας*, wp 173, 13/7/2010.

μένων και στις εθνικές αρχές ελέγχου τα ληφθέντα μέτρα για την επίτευξη της συμμόρφωσης προς τους κανόνες του Κανονισμού. Συνεπώς, απαιτείται η ενεργή και εμφανής συμμόρφωση του υπεύθυνου επεξεργασίας χωρίς να χρειάζεται προηγούμενη υπόδειξη τυχόν αδυναμιών της πολιτικής προστασίας από τα υποκείμενα των δεδομένων (π.χ. σε περίπτωση μη νόμιμης επεξεργασίας) ή από τις εθνικές αρχές ελέγχου (π.χ. σε περίπτωση ελέγχου).

δ. Υποχρεώσεις

1. Συμμόρφωση με τις αρχές επεξεργασίας (άρθρο 24)

Στο άρθρο 24 παρ. 1 ορίζεται ως πρωταρχική και ουσιαστική υποχρέωση του υπευθύνου επεξεργασίας η συμμόρφωσή του με τις διατάξεις του Κανονισμού, και κατά συνέπεια η πραγμάτωση της αρχής της λογοδοσίας.

Όπως προαναφέρθηκε, στόχος της αρχής είναι η θέσπιση συγκεκριμένων και πρακτικών μέτρων από τους υπεύθυνους επεξεργασίας που θα μετατρέπουν τις γενικές αρχές για την προστασία των δεδομένων σε συγκεκριμένες πολιτικές και επιχειρησιακές διαδικασίες. Επιπροσθέτως, ο εκάστοτε υπεύθυνος επεξεργασίας πρέπει να αποδεικνύει εκτός του ότι έλαβε συγκεκριμένα μέτρα, ότι αυτά ήταν κατάλληλα και αποτελεσματικά και επίσης να τα επανεξετάζει τακτικά και να τα επικαιροποιεί σύμφωνα με τις πιο πρόσφατες τεχνολογικές εξελίξεις.

Ειδικότερα, η αρχή της λογοδοσίας συντίθεται από δύο βασικά στοιχεία:

- υποχρέωση του υπευθύνου επεξεργασίας να λαμβάνει κατάλληλα και αποτελεσματικά μέτρα για την εφαρμογή των αρχών προστασίας των δεδομένων
- υποχρέωση απόδειξης, κατόπιν αιτήματος της εθνικής αρχής προστασίας προσωπικών δεδομένων, ότι λήφθηκαν κατάλληλα και αποτελεσματικά μέτρα.

Τα εν λόγω μέτρα θα πρέπει να επιλέγονται με βάση την φύση, το πλαίσιο, το

πεδίο εφαρμογής και τους σκοπούς της επεξεργασίας και τον κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων[16]. Η αξιολόγηση της πιθανότητας και της σοβαρότητας του κινδύνου θα πρέπει να γίνεται με αντικειμενικά κριτήρια βάσει των οποίων θα διαπιστώνεται ο βαθμός του κινδύνου που απορρέει από τις συγκεκριμένες πράξεις επεξεργασίας δεδομένων.

Στην παράγραφο 3 του άρθρου 24 αναφέρονται επίσης οι κώδικες δεοντολογίας και οι μηχανισμοί πιστοποίησης ως μέτρα και εργαλεία απόδειξης της συμμόρφωσης μία ς επιχείρησης με τις υποχρεώσεις που δημιουργεί ο Κανονισμός για τους υπεύθυνους επεξεργασίας. Ειδικότερα, οι εγκεκριμένοι κώδικες δεοντολογίας, οι εγκεκριμένες πιστοποιήσεις, οι κατευθυντήριες γραμμές που παρέχονται από το Συμβούλιο Προστασίας Δεδομένων (πρώην Ομάδα Εργασίας άρθρου 29) και οι υποδείξεις που παρέχει ο υπεύθυνος προστασίας δεδομένων μπορούν να καθοδηγήσουν μία επιχείρηση στην υιοθέτηση κατάλληλων μέτρων και στην απόδειξη της συμμόρφωσής της.

Προκειμένου να υπάρξει ασφάλεια δικαίου και να μην πλανώνται οι υπεύθυνοι επεξεργασίας στην αβεβαιότητα ως προς τον βαθμό συμμόρφωσής τους προς τον Κανονισμό, η ομάδα του άρθρου 29 έχει προτείνει έναν ενδεικτικό κατάλογο[17] με κοινά μέτρα λογοδοσίας τα οποία θα πρέπει να κλιμακώνονται και να εξειδικεύονται

[16] Βλ. σημείωση 75 Προοίμιο: Οι κίνδυνοι για τα δικαιώματα και τις ελευθερίες φυσικών προσώπων, ποικίλης πιθανότητας και σοβαρότητας, είναι δυνατόν να προκύπτουν από την επεξεργασία δεδομένων προσωπικού χαρακτήρα η οποία θα μπορούσε να οδηγήσει σε σωματική, υλική ή μη υλική βλάβη, ιδίως όταν η επεξεργασία μπορεί να οδηγήσει σε διακρίσεις, κατάχρηση ή υποκλοπή ταυτότητας, οικονομική απώλεια, βλάβη φήμης, απώλεια της εμπιστευτικότητας των δεδομένων προσωπικού χαρακτήρα που προστατεύονται από επαγγελματικό απόρρητο, παράνομη άρση της ψευδωνυμοποίησης, ή οποιοδήποτε άλλο σημαντικό οικονομικό ή κοινωνικό μειονέκτημα· όταν τα υποκείμενα των δεδομένων θα μπορούσαν να στερηθούν των δικαιωμάτων και ελευθεριών τους ή να εμποδίζονται από την άσκηση ελέγχου επί των δεδομένων τους προσωπικού χαρακτήρα· όταν υπόκεινται σε επεξεργασία δεδομένα προσωπικού χαρακτήρα τα οποία αποκαλύπτουν φυλετική ή εθνική καταγωγή, πολιτικά φρονήματα, θρησκεία ή φιλοσοφικές πεποιθήσεις ή συμμετοχή σε συνδικάτα και γίνεται επεξεργασία γενετικών δεδομένων, δεδομένων που αφορούν την υγεία ή δεδομένων που αφορούν την σεξουαλική ζωή ή ποινικές καταδίκες και αδικήματα ή σχετικά μέτρα ασφαλείας· όταν αξιολογούνται προσωπικές πτυχές, ιδίως όταν επιχειρείται ανάλυση ή πρόβλεψη πτυχών που αφορούν τις επιδόσεις στην εργασία, την οικονομική κατάσταση, την υγεία, προσωπικές προτιμήσεις ή συμφέροντα, την αξιοπιστία ή την συμπεριφορά, την θέση ή μετακινήσεις, προκειμένου να δημιουργηθούν ή να χρησιμοποιηθούν προσωπικά προφίλ· όταν υποβάλλονται σε επεξεργασία δεδομένα προσωπικού χαρακτήρα ευάλωτων προσώπων, ιδίως παιδιών· ή όταν η επεξεργασία περιλαμβάνει μεγάλη ποσότητα δεδομένων προσωπικού χαρακτήρα και επηρεάζει μεγάλο αριθμό υποκειμένων των δεδομένων.

[17] Βλ. Ομάδα εργασίας αρθ. 29, *Γνώμη 3/2010 σχετικά με την αρχή της λογοδοσίας*, wp 173, 13/7/2010, σελ. 13-18.

in concreto αναλόγως του κινδύνου της επεξεργασίας:

- *θέσπιση εσωτερικών διαδικασιών πριν από την δημιουργία νέων εργασιών επεξεργασίας δεδομένων προσωπικού χαρακτήρα (εσωτερικός έλεγχος, αξιολόγηση κ.λπ.)·*
- *θέσπιση γραπτών και δεσμευτικών πολιτικών προστασίας δεδομένων, οι οποίες θα εξετασθούν και θα εφαρμοστούν σε νέες εργασίες επεξεργασίας δεδομένων (π.χ. συμμόρφωση προς την ποιότητα των δεδομένων, κοινοποίηση, (βασικές) αρχές ασφάλειας, πρόσβαση κ.λπ.), οι οποίες πρέπει να είναι διαθέσιμες στα πρόσωπα στα οποία αναφέρονται τα δεδομένα·*
- *χαρτογράφηση διαδικασιών ώστε να διασφαλίζεται κατάλληλη αναγνώριση όλων των εργασιών επεξεργασίας δεδομένων, και διατήρηση καταλόγου εργασιών επεξεργασίας δεδομένων·*
- *διορισμός υπευθύνου για την προστασία των δεδομένων και άλλων προσώπων με ευθύνη για την προστασία των δεδομένων·*
- *παροχή κατάλληλης εκπαίδευσης και κατάρτισης στους υπαλλήλους στην προστασία δεδομένων. Αυτό μπορεί να περιλαμβάνει εκείνους που επεξεργάζονται (ή είναι υπεύθυνοι για) τα δεδομένα προσωπικού χαρακτήρα (όπως τους διευθυντές ανθρώπινων πόρων), αλλά και τους επικεφαλής τμημάτων πληροφορικής, τους υπευθύνους ανάπτυξης και τους διευθυντές υπηρεσιακών μμονάδων. Πρέπει να διατίθενται επαρκείς πόροι για την διαχείριση της ιδιωτικής ζωής κ.λπ.·*
- *θέσπιση διαδικασιών για την διαχείριση των αιτημάτων πρόσβασης, διόρθωσης και διαγραφής, η οποία πρέπει να είναι διάφανη για τα άτομα στα οποία αναφέρονται τα δεδομένα·*
- *εγκαθίδρυση εσωτερικού μηχανισμού χειρισμού καταγγελιών·*
- *θέσπιση εσωτερικών διαδικασιών για την αποτελεσματική διαχείριση και αναφορά παραβιάσεων της ασφάλειας·*
- διενέργεια εκτίμησης αντικτύπου στην ιδιωτική ζωή σε ειδικές περιπτώσεις· εφαρμογή και επίβλεψη διαδικασιών επαλήθευσης, ώστε να διασφαλίζεται ότι όλα τα μέτρα όχι μόνον υπάρχουν στα χαρτιά, αλλά εφαρμόζονται και λειτουργούν στην πράξη (εσωτερικοί ή εξωτερικοί έλεγχοι κ.λπ.).

2. Νομιμότητα της Επεξεργασίας

Όπως αναφέρθηκε ανωτέρω, η αρχή της νομιμότητας επιτάσσει να υπάρχει μία έγκυρη νομική βάση από την οποία ο υπεύθυνος επεξεργασίας να αντλεί την νομιμότητα των πράξεων επεξεργασίας καθορίζοντας περαιτέρω και τον σκοπό τους. Στο άρθρο 6 απαριθμούνται οι συμβατές με τον Κανονισμό νομικές βάσεις εκ των οποίων πρέπει οπωσδήποτε μία να συντρέχει για να κριθεί η επεξεργασία σύννομη. Συγκεκριμένα, η επεξεργασία των απλών προσωπικών δεδομένων[18] είναι νόμιμη εάν ισχύει μία από τις ακόλουθες προϋποθέσεις:

α) το υποκείμενο των δεδομένων έχει συναινέσει στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα του για έναν ή περισσότερους συγκεκριμένους σκοπούς (συγκατάθεση)

β) η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή για να ληφθούν μέτρα κατ' αίτηση του υποκειμένου των δεδομένων πριν από την σύναψη σύμβασης,

γ) η επεξεργασία είναι απαραίτητη για την συμμόρφωση με έννομη υποχρέωση του υπευθύνου επεξεργασίας, η οποία απορρέει είτε από το δίκαιο της Ένωσης είτε από το εθνικό δίκαιο του κράτους μέλους

δ) η επεξεργασία είναι απαραίτητη για την διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου[19]· σημειώνεται ότι αυτού του είδους η νομική βάση επιστρατεύεται μόνο εάν η επεξεργασία δεν μπορεί να στηριχθεί σε άλλη νομική βάση

ε) η επεξεργασία είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας,

στ) η επεξεργασία είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων

[18] Βλ. ανωτέρω την διάκριση απλών – ευαίσθητων προσωπικών δεδομένων, σελ. 12.

[19] «*Τέτοιο συμφέρον, που συνδέεται στενά με την επιβίωση του υποκειμένου των δεδομένων, θα μπορούσε, για παράδειγμα, να είναι η βάση της νόμιμης χρήσης δεδομένων υγείας ή δεδομένων αγνοουμένων*», Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων, σελ. 100.

που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος[20], εκτός εάν έναντι των συμφερόντων αυτών υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων που επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα, ιδίως εάν το υποκείμενο των δεδομένων είναι παιδί.

ζ) η περαιτέρω επεξεργασία για σκοπούς άλλους από εκείνους για τους οποίους τα προσωπικά δεδομένα συλλέχθηκαν αρχικά με νόμιμο τρόπο επιτρέπεται μόνο εφόσον ο σκοπός είναι συμβατός με τους αρχικούς σκοπούς[21].

Όσον αφορά την επεξεργασία των ευαίσθητων προσωπικών δεδομένων αυτή κατ' αρχήν απαγορεύεται. Επιτρέπεται μόνο για τους σαφώς και αποκλειστικώς προβλεπόμενους στο αρθ. 9 παρ. 2 λόγους· εξ αυτών στα πλαίσια της παρούσας εργασίας επισημαίνουμε τους κάτωθι:

---

[20] Σημείωση 47 Προοίμιο: «*Τέτοιο έννομο συμφέρον θα μπορούσε λόγου χάρη να υπάρχει όταν υφίσταται σχετική και κατάλληλη σχέση μεταξύ του υποκειμένου των δεδομένων και του υπευθύνου επεξεργασίας, όπως αν το υποκείμενο των δεδομένων είναι πελάτης του υπευθύνου επεξεργασίας ή βρίσκεται στην υπηρεσία του. Εν πάση περιπτώσει η ύπαρξη έννομου συμφέροντος θα χρειαζόταν προσεκτική αξιολόγηση, μεταξύ άλλων ως προς το κατά πόσον το υποκείμενο των δεδομένων, κατά την χρονική στιγμή και στο πλαίσιο της συλλογής των δεδομένων προσωπικού χαρακτήρα, μπορεί εύλογα να αναμένει ότι για τον σκοπό αυτό μπορεί να πραγματοποιηθεί επεξεργασία. Ειδικότερα, τα συμφέροντα και τα θεμελιώδη δικαιώματα του υποκειμένου των δεδομένων θα μπορούσαν να υπερισχύουν των συμφερόντων του υπευθύνου επεξεργασίας, όταν τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία σε περιπτώσεις κατά τις οποίες το υποκείμενο των δεδομένων δεν αναμένει ευλόγως περαιτέρω επεξεργασία των δεδομένων του. Η επεξεργασία δεδομένων προσωπικού χαρακτήρα, στον βαθμό που είναι αυστηρά αναγκαία για τους σκοπούς πρόληψης της απάτης, συνιστά επίσης έννομο συμφέρον του ενδιαφερόμενου υπευθύνου επεξεργασίας.* ***Η επεξεργασία δεδομένων προσωπικού χαρακτήρα για σκοπούς άμεσης εμπορικής προώθησης μπορεί να θεωρηθεί ότι διενεργείται χάριν έννομου συμφέροντος***».

[21] Σημείωση 50 Προοίμιο: «*Σε αυτήν την περίπτωση, δεν απαιτείται νομική βάση χωριστή από εκείνη που επέτρεψε την συλλογή των δεδομένων προσωπικού χαρακτήρα. Εάν η επεξεργασία είναι αναγκαία για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας, το δίκαιο της Ένωσης ή κράτους μέλους μπορεί να καθορίζει και να προσδιορίζει τα καθήκοντα και τους σκοπούς για τους οποίους πρέπει να θεωρείται συμβατή και σύννομη η περαιτέρω επεξεργασία. Η περαιτέρω επεξεργασία για λόγους αρχειοθέτησης που άπτονται του δημόσιου συμφέροντος, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς θα πρέπει να θεωρείται συμβατή σύννομη πράξη επεξεργασίας. Για να εξακριβωθεί αν ο σκοπός της περαιτέρω επεξεργασίας είναι συμβατός με τον σκοπό της αρχικής συλλογής των δεδομένων προσωπικού χαρακτήρα, ο υπεύθυνος επεξεργασίας, εφόσον πληροί όλες τις απαιτήσεις για την νομιμότητα της αρχικής επεξεργασίας, θα πρέπει να λάβει υπόψη, μεταξύ άλλων: τυχόν συνδέσμους μεταξύ των σκοπών αυτών και των σκοπών της επιδιωκόμενης περαιτέρω επεξεργασίας· το πλαίσιο στο οποίο έχουν συλλεγεί τα δεδομένα προσωπικού χαρακτήρα, ιδίως τις εύλογες προσδοκίες του υποκειμένου των δεδομένων βάσει της σχέσης του με τον υπεύθυνο επεξεργασίας ως προς την περαιτέρω χρήση τους· την φύση των δεδομένων προσωπικού χαρακτήρα· τις συνέπειες της επιδιωκόμενης περαιτέρω επεξεργασίας για τα υποκείμενα των δεδομένων· και την ύπαρξη κατάλληλων εγγυήσεων τόσο για τις αρχικές όσο και τις σκοπούμενες πράξεις περαιτέρω επεξεργασίας».*

α) το υποκείμενο των δεδομένων έχει παράσχει ρητή συγκατάθεση για την επεξεργασία αυτών των δεδομένων προσωπικού χαρακτήρα για έναν ή περισσότερους συγκεκριμένους σκοπούς, εκτός εάν το δίκαιο της Ένωσης ή κράτους μέλους προβλέπει ότι η απαγόρευση που αναφέρεται στην παράγραφο 1 δεν μπορεί να αρθεί από το υποκείμενο των δεδομένων,

β) η επεξεργασία είναι απαραίτητη για την εκτέλεση των υποχρεώσεων και την άσκηση συγκεκριμένων δικαιωμάτων του υπευθύνου επεξεργασίας ή του υποκειμένου των δεδομένων στον τομέα του εργατικού δικαίου και του δικαίου κοινωνικής ασφάλισης και κοινωνικής προστασίας, εφόσον επιτρέπεται από το δίκαιο της Ένωσης ή κράτους μέλους ή από συλλογική συμφωνία σύμφωνα με το εθνικό δίκαιο παρέχοντας κατάλληλες εγγυήσεις για τα θεμελιώδη δικαιώματα και τα συμφέροντα του υποκειμένου των δεδομένων,

γ) η επεξεργασία είναι απαραίτητη για την προστασία των ζωτικών συμφερόντων του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου, εάν το υποκείμενο των δεδομένων είναι σωματικά ή νομικά ανίκανο να συγκατατεθεί[22],

δ) η επεξεργασία διενεργείται, με κατάλληλες εγγυήσεις, στο πλαίσιο των νόμιμων δραστηριοτήτων ιδρύματος, οργάνωσης ή άλλου μη κερδοσκοπικού φορέα με πολιτικό, φιλοσοφικό, θρησκευτικό ή συνδικαλιστικό στόχο και υπό την προϋπόθεση ότι η επεξεργασία αφορά αποκλειστικά τα μέλη ή τα πρώην μέλη του φορέα ή πρόσωπα τα οποία έχουν τακτική επικοινωνία μαζί του σε σχέση με τους σκοπούς του και ότι τα δεδομένα προσωπικού χαρακτήρα δεν κοινοποιούνται εκτός του συγκεκριμένου φορέα χωρίς την συγκατάθεση των υποκειμένων των δεδομένων,

ε) η επεξεργασία αφορά δεδομένα προσωπικού χαρακτήρα τα οποία έχουν προδήλως δημοσιοποιηθεί από το υποκείμενο των δεδομένων,

στ) η επεξεργασία είναι απαραίτητη για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς

[22] «*Για να νομιμοποιηθεί η επεξεργασία ευαίσθητων δεδομένων επί της βάσης αυτής, απαραίτητη προϋπόθεση είναι να είναι αδύνατον να ερωτηθεί το υποκείμενο των δεδομένων ούτως ώστε να αποφασίσει, διότι π.χ. έχει χάσει τις αισθήσεις του ή απουσιάζει και δεν υπάρχει δυνατότητα επικοινωνίας μαζί του*», Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων, σελ. 106.

σκοπούς σύμφωνα με το άρθρο 89 παράγραφος 1 βάσει του δικαίου της Ένωσης ή κράτους μέλους, οι οποίοι είναι ανάλογοι προς τον επιδιωκόμενο στόχο, σέβονται την ουσία του δικαιώματος στην προστασία των δεδομένων και προβλέπουν κατάλληλα και συγκεκριμένα μέτρα για την διασφάλιση των θεμελιωδών δικαιωμάτων και των συμφερόντων του υποκειμένου των δεδομένων.

i. Συγκατάθεση

Ειδικότερα η παροχή συγκατάθεσης, σε αντίθεση με τις υπόλοιπες νομικές βάσεις που κατά τον έναν ή τον άλλον τρόπο επιβάλλονται από τον νόμο ή κατόπιν στάθμισης δικαιωμάτων-συμφερόντων, δίνει την διακριτική ευχέρεια στο υποκείμενο των δεδομένων να αποφασίζει αυτοβούλως για την τύχη των δεδομένων του. Μέχρι πρόσφατα παρεχόταν η συγκατάθεση για την επεξεργασία των προσωπικών δεδομένων σχεδόν τυφλά από τα υποκείμενα των δεδομένων καθώς δεν είχε αποκαλυφθεί το εύρος των δυνατοτήτων της αξιοποίησής τους ούτε και το μέγεθος του κινδύνου για την ιδιωτική ζωή και την ελεύθερη ανάπτυξη της προσωπικότητας των φυσικών προσώπων.

Η ομάδα εργασίας του άρθρου 29 ήδη από το 2010 σε ανακοίνωση[23] που εξέδωσε δήλωσε σχετικά με το θέμα της συγκατάθεσης:

«*Επιπλέον, στο επιγραμμικό περιβάλλον - δεδομένης της αδιαφάνειας των πολιτικών για την προστασία της ιδιωτικής ζωής – είναι συχνά δυσκολότερο για τα φυσικά πρόσωπα να γνωρίζουν τα δικαιώματά τους και να δίνουν την συγκατάθεσή τους εν πλήρει επιγνώσει. Η κατάσταση περιπλέκεται περισσότερο από το γεγονός ότι σε ορισμένες περιπτώσεις δεν είναι καθόλου σαφές τι αποτελεί ελεύθερη, ρητή και εν πλήρη επιγνώσει συγκατάθεση για την επεξεργασία των προσωπικών δεδομένων, όπως στην περίπτωση της συμπεριφορικής διαφήμισης, στην οποία οι ρυθμίσεις του διαδικτυακού φυλλομετρητή (browser) θεωρούνται από μερικούς, αλλά όχι από άλλους, ότι ισοδυναμούν με την συγκατάθεση του χρήστη.*»

Στο άρθρο 7 του Κανονισμού τίθενται πλέον σαφείς προϋποθέσεις για την παροχή

[23] COM (2010) 609 της 4.11.2010, Συνολική προσέγγιση όσον αφορά την προστασία των δεδομένων προσωπικού χαρακτήρα στην Ευρωπαϊκή Ένωση.

συγκατάθεσης τόσο ως προς τις υποχρεώσεις των υπευθύνων επεξεργασίας όσο και ως προς τα δικαιώματα των υποκειμένων των δεδομένων.

Όταν η επεξεργασία βασίζεται στην συγκατάθεση του υποκειμένου των δεδομένων, ο υπεύθυνος επεξεργασίας θα πρέπει να είναι σε θέση να αποδείξει ότι το υποκείμενο των δεδομένων συναίνεσε στην πράξη επεξεργασίας. Ειδικότερα, αν ζητείται η παροχή συγκατάθεσης γραπτώς σε φόρμα που αφορά και άλλα θέματα θα πρέπει η συγκατάθεση για την επεξεργασία των προσωπικών δεδομένων να είναι σε διακριτό σημείο, σε κατανοητή και εύκολα προσβάσιμη μορφή και με σαφή και απλή διατύπωση χωρίς καταχρηστικές ρήτρες[24].

Προκειμένου η δοθείσα συγκατάθεση να κριθεί έγκυρη θα πρέπει να συντρέχουν τρεις προϋποθέσεις-εγγυήσεις οι οποίες θα οδηγούν στο συμπέρασμα ότι το υποκείμενο των δεδομένων συναίνεσε με την ελεύθερη και ειλικρινή βούλησή του στην πράξη επεξεργασίας:

- η συγκατάθεση θα πρέπει να είναι ελεύθερη· αν δεν δόθηκε από αληθινή ή ελεύθερη επιλογή ή το υποκείμενο των δεδομένων δεν είναι σε θέση να αρνηθεί ή να αποσύρει την συγκατάθεσή του χωρίς να ζημιωθεί, η δοθείσα συγκατάθεση δεν είναι ελεύθερη. Επιπλέον στην παράγραφο 4 γίνεται ιδιαίτερη μνεία ότι *η συγκατάθεση θεωρείται ότι δεν έχει παρασχεθεί ελεύθερα, εάν δεν επιτρέπεται να δοθεί χωριστή συγκατάθεση σε διαφορετικές πράξεις επεξεργασίας δεδομένων προσωπικού χαρακτήρα, ακόμη και αν ενδείκνυται στην συγκεκριμένη περίπτωση, ή όταν η εκτέλεση μία ς σύμβασης, συμπεριλαμβανομένης της παροχής μία ς υπηρεσίας ή απόκτησης αγαθών, προϋποθέτει την συγκατάθεση, ακόμη και αν η συγκατάθεση αυτή δεν είναι αναγκαία για την εν λόγω εκτέλεση*[25].

- η συγκατάθεση θα πρέπει να δοθεί εν επιγνώσει· ο υπεύθυνος επεξεργασίας θα πρέπει να έχει ενημερώσει πλήρως (informed consent) το υποκείμενο των δεδομένων για το αντικείμενο και τις συνέπειες της συγκατάθεσής του ικανοποιώντας έτσι την υποχρέωση που απορρέει από την αρχή της διαφάνειας[26]

[24] Οδηγία 93/13/ΕΟΚ του Συμβουλίου, της 5ης Απριλίου 1993, σχετικά με τις καταχρηστικές ρήτρες των συμβάσεων που συνάπτονται με καταναλωτές (ΕΕ L 95 της 21.4.1993, σ. 29).
[25] Βλ. σημείωση 43 Προοίμιο.
[26] Ως προς το περιεχόμενο της ενημέρωσης βλ. παρακάτω σελ. 29.

- η συγκατάθεση θα πρέπει να είναι ειδική, δηλαδή να αφορά συγκεκριμένο σκοπό επεξεργασίας· δεν μπορεί να δοθεί γενική συγκατάθεση για αόριστες πράξεις επεξεργασίας. Εφόσον ο υπεύθυνος επεξεργασίας επιθυμεί να χρησιμοποιήσει τα συλλεχθέντα δεδομένα για άλλο σκοπό από εκείνον για τον οποίο δόθηκε η αρχική συγκατάθεση, θα πρέπει να ενημερώσει σχετικά το υποκείμενο προκειμένου να δώσει εκ νέου την συγκατάθεσή του. [27]

- η συγκατάθεση θα πρέπει να είναι ρητή, δηλαδή να συνάγεται κατά τρόπο ο οποίος δεν αφήνει αμφιβολία ότι έχει δοθεί[28]. Το να συνάγεται η συγκατάθεση απλώς και μόνο από την αδράνεια ή την σιωπή, για παράδειγμα, δεν αποτελεί ικανή συνθήκη για την σαφή συγκατάθεση. Η εν λόγω προϋπόθεση προβλέπεται σαφώς στο αρθ. 9 παρ. 2α όσον αφορά τα ευαίσθητα προσωπικά δεδομένα και συνάγεται εμμέσως από το αρθ. 7 παρ. 1 για τα απλά δεδομένα από την υποχρέωση με την οποία βαρύνεται ο υπεύθυνος επεξεργασίας, ήτοι να είναι σε θέση να αποδείξει ότι έχει δοθεί έγκυρη συγκατάθεση για την διενεργούμενη επεξεργασία.

Τέλος, στην παράγραφο 2 γίνεται αναφορά για το δικαίωμα ανάκλησης της συγκατάθεσης ανά πάσα στιγμή. Δεν πρέπει να τίθεται απαίτηση αιτιολόγησης της ανάκλησης της συγκατάθεσης ούτε να υφίσταται κίνδυνος αρνητικών συνεπειών, πέραν της παύσης τυχόν ωφελημάτων τα οποία ενδέχεται να απέρρεαν από την προηγουμένως συμφωνηθείσα χρήση των δεδομένων. Συνεπώς η ανάκληση ασκείται για το μέλλον και δεν επηρεάζει την επεξεργασία δεδομένων που έχει ήδη πραγματοποιηθεί εφόσον τα δεδομένα είχαν συλλεχθεί νόμιμα. Ο υπεύθυνος επεξεργασίας δεν απαιτείται ως εκ τούτου να ακυρώσει τις ληφθείσες αποφάσεις ή τις κινηθείσες διαδικασίες που στηρίχθηκαν στα εν λόγω δεδομένα· εντούτοις, αν δεν υπάρχει άλλη νομική βάση που να δικαιολογεί την μεταγενέστερη αποθήκευση των δεδομένων, αυτά τα τελευταία θα πρέπει να διαγράφονται με ευθύνη του.

[27] αρθ. 13 παρ. 3 και αρθ. 14 παρ. 4

[28] «*Παρά το γεγονός ότι η ρητή (explicit) συγκατάθεση παρέχεται παραδοσιακά εγγράφως, είτε σε χαρτί είτε με ηλεκτρονική μορφή, αυτή η προϋπόθεση δεν είναι απαραίτητην και μπορεί επίσης να χορηγηθεί προφορικά. Αυτό επιβεβαιώνεται από το γεγονός ότι η αξίωση να είναι έγγραφη η συγκατάθεση που απαιτείται σύμφωνα με το άρθρο 8 διεγράφη στην τελική έκδοση της οδηγίας. Εντούτοις, όπως καταδεικνύεται στο ίδιο κεφάλαιο, η προφορική συγκατάθεση μπορεί να είναι δύσκολο να αποδειχθεί και, ως εκ τούτου, στην πράξη, συστήνεται στους υπευθύνους επεξεργασίας να προσφεύγουν σε έγγραφη συγκατάθεση για αποδεικτικούς λόγους*». βλ. περισσότερα Γνώμη 15/201 σχετικά με τον ορισμό της συγκατάθεσης, WP 187, 13 Ιουλίου 2011, σελ. 23-32

3. Εξασφάλιση δυνατότητας στα υποκείμενα για άσκηση των δικαιωμάτων τους

Για την αποτελεσματική προστασία των δεδομένων προσωπικού χαρακτήρα σε ολόκληρη την ΕΕ απαιτείται αφενός να καθοριστούν με σαφήνεια και πρακτικό αντίκρισμα τα δικαιώματα των υποκειμένων των δεδομένων και αφ' ετέρου να αναδειχθεί η αντίστοιχη υποχρέωση των υπευθύνων επεξεργασίας να υιοθετούν τρόπους και μηχανισμούς για την διευκόλυνση των υποκειμένων στην άσκηση των δικαιωμάτων τους ώστε να μην καταστούν γράμμα κενό. Ειδικότερα, όταν η συλλογή των δεδομένων γίνεται στο ψηφιακό περιβάλλον, π.χ. μέσω ιστοσελίδας, και/ ή οι πράξεις επεξεργασίας γίνονται με ηλεκτρονικά μέσα ο υπεύθυνος επεξεργασίας θα πρέπει να παρέχει τρόπο για ηλεκτρονική υποβολή των αιτημάτων των υποκειμένων των δεδομένων. Δεδομένης της πολυπλοκότητας των χρησιμοποιούμενων τεχνολογιών στον ψηφιακή παροχή υπηρεσιών/αγαθών αλλά και του μεγάλου εύρους των χρηστών κάθε ανακοίνωση σχετική με τους τρόπους άσκησης των δικαιωμάτων θα πρέπει να είναι σε συνοπτική, κατανοητή και εύκολα προσβάσιμη μορφή και να παρέχεται δωρεάν.

Σε περίπτωση αιτήματος για παροχή πληροφοριών σχετικά με τα αρθ. 15-22 οι υπεύθυνοι επεξεργασίας θα πρέπει να αποκριθούν άμεσα ή εντός μηνός από την παραλαβή του αιτήματος· η εν λόγω προθεσμία μπορεί να παραταθεί για ακόμη 2 μήνες για λόγους φόρτου εργασίας ή πολυπλοκότητας του αιτήματος. Εάν ο υπεύθυνος δεν προτίθεται να ενεργήσει επί του αιτήματος ενημερώνει το υποκείμενο των δεδομένων χωρίς καθυστέρηση και εντός μηνός από την παραλαβή του αιτήματος για τους λόγους αλλά και για την δυνατότητα υποβολής καταγγελίας στην ΑΠΔΠΧ και την άσκηση δικαστικής προσφυγής. Εάν τα αιτήματα του υποκειμένου των δεδομένων είναι προδήλως αβάσιμα ή υπερβολικά μπορεί είτε να επιβάλει την καταβολή ευλόγου τέλους για να καλύψει τα διοικητικά έξοδα είτε να μην ενεργήσει καθόλου ως προς το αίτημα παρέχοντας ειδική αιτιολογία.

i. Δικαίωμα Ενημέρωσης (άρθρα 13-14)

Η αρχή της διαφάνειας και η προϋπόθεση της εν πλήρει επιγνώσει συγκατάθεσης απαιτούν το υποκείμενο να έχει λάβει επαρκή πληροφόρηση πριν συναινέσει στην

συλλογή και επεξεργασία των δεδομένων του. Το κατά πόσον η παρεχόμενη πληροφόρηση είναι επαρκής κρίνεται ad hoc· συνήθως για να κριθεί ότι η συγκατάθεση δόθηκε με πλήρη επίγνωση του υποκειμένου των δεδομένων προηγείται εύληπτη και εκτενής επεξήγηση του σκοπού επεξεργασίας για τον οποίο ζητείται η συγκατάθεση, καθώς και πληροφόρηση για τις συνέπειες της παροχής ή της άρνησης της συγκατάθεσης.

Η πληροφόρηση σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα θα πρέπει να παρέχονται στο υποκείμενο των δεδομένων κατά την συλλογή ή, εάν τα δεδομένα προσωπικού χαρακτήρα έχουν ληφθεί από άλλη πηγή, εντός εύλογης προθεσμίας, αναλόγως των συνθηκών κάθε περίπτωσης. Εάν τα δεδομένα προσωπικού χαρακτήρα επιτρέπεται να κοινολογηθούν σε άλλον αποδέκτη, το υποκείμενο των δεδομένων θα πρέπει να ενημερώνεται, όταν τα δεδομένα του διαβιβάζονται για πρώτη φορά στον αποδέκτη. Επίσης, όταν ο υπεύθυνος επεξεργασίας επιθυμεί να επεξεργαστεί τα δεδομένα προσωπικού χαρακτήρα για σκοπό άλλο από εκείνον για τον οποίο συλλέχθηκαν και για τον οποίο συντρέχει μία εκ των νομικών βάσεων, ο υπεύθυνος επεξεργασίας θα πρέπει να παρέχει στο υποκείμενο των δεδομένων, πριν από την εν λόγω περαιτέρω επεξεργασία, τις αναγκαίες πληροφορίες για αυτήν. Εξαίρεση από την υποχρέωση παροχής πληροφοριών σύμφωνα με τις παραγράφους 4 άρθρο 13 και 5 άρθρου 14 προβλέπεται α) εάν το υποκείμενο διαθέτει ήδη τις πληροφορίες, β) εάν η καταχώριση ή η διαβίβαση των δεδομένων προσωπικού χαρακτήρα σε άλλον αποδέκτη προβλέπεται ρητώς από τον νόμο ή γ) εάν η πληροφόρηση του υποκειμένου των δεδομένων αποδεικνύεται ανέφικτη ή θα απαιτούσε δυσανάλογη προσπάθεια[29]. Συνοπτικά, περιεχόμενο της ενημέρωσης αποτελούν οι εξής πληροφορίες[30]:

- η ταυτότητα και τα στοιχεία επικοινωνίας του υπεύθυνου επεξεργασίας
- τα στοιχεία επικοινωνίας του υπεύθυνου προστασίας δεδομένων
- οι σκοποί, η νομική βάση ή το έννομο συμφέρον (αρθ. 6 παρ. 1στ) για την

[29] Σημείωση 62 Προοίμιο: «*Συναφώς, θα πρέπει να λαμβάνονται υπόψη ο αριθμός των υποκειμένων των δεδομένων, η ηλικία των δεδομένων και τυχόν κατάλληλες εγγυήσεις που θεσπίστηκαν.*»

[30] Βλ. Αναλυτικότερα αρθ. 13 παρ. 2 και αρθ. 14 παρ. 2

συλλογή και την επεξεργασία

- οι αποδέκτες των δεδομένων, εάν υπάρχουν
- η πρόθεση για διαβίβαση των δεδομένων σε τρίτη χώρα ή οργανισμό
- το χρονικό διάστημα επεξεργασίας των δεδομένων
- τα δικαιώματα του υποκειμένου ως προς τα δεδομένα του συμπεριλαμβανομένου του δικαιώματος ανάκλησης της συγκατάθεσης και του δικαιώματος καταγγελίας σε εποπτική αρχή
- ο τυχόν νομικός ή συμβατικός χαρακτήρας της υποχρέωσης του υποκειμένου να παράσχει τα δεδομένα και τις συνέπειες από την μη παροχή τους
- η ύπαρξη αυτοματοματοποιημένης λήξης αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ.

ii. Δικαίωμα πρόσβασης (άρθρο 15)

Το δικαίωμα πρόσβασης του κάθε υποκειμένου στα προσωπικά δεδομένα που το αφορούν αποτελεί αναπόσπαστο κομμάτι της αρχής της νομιμότητας και της διαφάνειας, αλλά και της λογοδοσίας, καθώς με αυτόν τον τρόπο το υποκείμενο μπορεί σε τακτά χρονικά διαστήματα να ελέγχει την νομιμότητα της επεξεργασίας ή τυχόν υπέρβαση των ορίων της. Επομένως κατόπιν αιτήσεως θα πρέπει να ενημερώνεται για τους σκοπούς και το χρονικό διάστημα της επεξεργασίας, τους τυχόν αποδέκτες των προσωπικών του δεδομένων και, αν συντρέχει περίπτωση αυτοματοποιημένης επεξεργασίας των δεδομένων του, και τι συνεπάγεται αυτό για την κοινωνικό-οικονομική ζωή του υποκειμένου. Δεδομένης της ευρύτατης χρήσης της τεχνολογίας και της κατά κύριο λόγο συλλογής και επεξεργασίας των προσωπικών δεδομένων με την χρήση αυτής, ο υπεύθυνος επεξεργασίας θα πρέπει να παρέχει ηλεκτρονική πρόσβαση σε ασφαλές και εύχρηστο ψηφιακό περιβάλλον προκειμένου το υποκείμενο να μπορέσει να έχει άμεσο έλεγχο των πληροφοριών που το αφορούν. Επιπλέον στο ίδιο πλαίσιο της ηλεκτρονικής παροχής υπηρεσιών και της ηλεκτρονικής διασύνδεσης, ο υπεύθυνος επεξεργασίας θα πρέπει να χρησιμοποιεί κάθε εύλογο μέτρο για να επαληθεύει την ταυτότητα του υποκειμένου το οποίο ζητεί πρόσβαση εφαρμόζοντας εξελιγμένο σύστημα

αυθεντικοποίησης[31].

iii. Δικαίωμα διόρθωσης (άρθρο 16)

Σύμφωνα με το αρθ. 16 το υποκείμενο των δεδομένων έχει δικαίωμα να απαιτήσει την διόρθωση ανακριβών δεδομένων προσωπικού χαρακτήρα που το αφορούν, αλλά και να συμπληρώσει τυχόν ελλιπή προσωπικά του δεδομένα, λαμβάνοντας υπ' όψιν και τον σκοπό της επεξεργασίας και το ορθό και ακριβές αυτής. Ο υπεύθυνος επεξεργασίας πρέπει να προχωρήσει στην διόρθωση χωρίς υπαίτια και αδικαιολόγητη καθυστέρηση, άλλως το φυσικό πρόσωπο μπορεί να ασκήσει και το δικαίωμα περιορισμού της επεξεργασίας (Βλ. παρακάτω σελ. 34).

iv. Δικαίωμα διαγραφής (άρθρο 17)

Η εισαγωγή του νέου «δικαιώματος στην λήθη[32]» (right to be forgotten) στο πλαίσιο προστασίας των προσωπικών δεδομένων αποτελεί ένα από τα δυνατά όπλα του Κανονισμού για την προστασία της ιδιωτικότητας των φυσικών προσώπων στο ψηφιακό περιβάλλον που φαίνεται να «μην ξεχνά ποτέ».

Ασκώντας το δικαίωμα διαγραφής το υποκείμενο απαιτεί από τον υπεύθυνο επεξεργασίας να διαγράψει προσωπικά δεδομένα που το αφορούν, να απόσχει από οποιαδήποτε περαιτέρω διάδοση των δεδομένων αυτών, αλλά και να ενημερώσει

---

[31] *«Πρόκειται για διαδικασία με την οποία το πρόσωπο αποδεικνύει ότι είναι ο κάτοχος συγκεκριμένης ταυτότητας και/ή είναι εξουσιοδοτημένο να προβαίνει σε συγκεκριμένες ενέργειες, π.χ. να εισέρχεται σε ελεγχόμενη περιοχή ασφαλείας ή να κάνει ανάληψη μετρητών από τραπεζικό λογαριασμό. Η αυθεντικοποίηση μπορεί να γίνει με σύγκριση βιομετρικών δεδομένων, π.χ. της φωτογραφίας ή των δακτυλικών αποτυπωμάτων σε διαβατήριο με τα δεδομένα του προσώπου που εμφανίζεται, για παράδειγμα στον έλεγχο διαβατηρίων. Μπορεί επίσης να γίνει μέσω πληροφοριών οι οποίες κανονικά είναι γνωστές μόνο σε πρόσωπο με συγκεκριμένη ταυτότητα ή εξουσιοδότηση, όπως ο προσωπικός αναγνωριστικός αριθμός (PIN) ή ο κωδικός πρόσβασης, ή μέσω επίδειξης συγκεκριμένου αδειοδοτικού το οποίο κανονικά βρίσκεται στην αποκλειστική κατοχή προσώπου με συγκεκριμένη ταυτότητα ή εξουσιοδότηση, π.χ. κάρτας με μικροεπεξεργαστή ή κλειδιού χρηματοκιβωτίου. Εκτός από τους κωδικούς πρόσβασης ή τις κάρτες με μικροεπεξεργαστή, ενίοτε σε συνδυασμό με PIN, η ηλεκτρονική υπογραφή είναι ένα εξαιρετικά χρήσιμο μέσο για την εξακρίβωση και την επαλήθευση της ταυτότητας του προσώπου στις ηλεκτρονικές επικοινωνίες.»* Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων, 2014, σελ. 49.

[32] Το δικαίωμα είχε ήδη αναγνωριστεί με την απόφαση της 13ης Μαΐου 2014 (υπόθεση C-131/12) του Δικαστηρίου της ΕΕ – Google Spain. Άρθρο 32, παρ. 2 της Οδηγίας 95/46/ΕΚ, το οποίο ορίζει ότι «*Τα κράτην μέλη επιτρέπουν εν πάση περιπτώσει στο πρόσωπο στο οποίο αναφέρονται τα δεδομένα να επιτυγχάνει , κατόπιν αιτήσεώς του , την διόρθωση , την διαγραφή ή το κλείδωμα των ελλιπών ή ανακριβών δεδομένων ή των δεδομένων που έχουν αποθηκευθεί κατά τρόπο ασυμβίβαστο προς τους νόμιμους σκοπούς τους οποίους επιδιώκει ο υπεύθυνος της επεξεργασίας».*

τρίτους στους οποίους αυτά κοινοποιήθηκαν προκειμένου και αυτοί να διαγράψουν τυχόν συνδέσμους προς αυτά, ή αντίγραφά τους.

Το δικαίωμα διαγραφής μπορεί να ασκηθεί για έναν από τους ακόλουθους λόγους:

(α) τα προσωπικά δεδομένα δεν είναι πλέον απαραίτητα σε σχέση με τους σκοπούς για τους οποίους συνελέγησαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία

(β) το υποκείμενο των δεδομένων αποσύρει την συγκατάθεση στην οποία στηρίζεται η επεξεργασία, και δεν υπάρχει υπέρτερη νομική βάση ή έννομο συμφέρον για την επεξεργασία,

(γ) το υποκείμενο των δεδομένων αντιτίθεται στην επεξεργασία (βλ. παρακάτω Δικαίωμα εναντίωσης, σελ. 35) και δεν υπάρχει υπέρτερη νομική βάση ή έννομο συμφέρον για την επεξεργασία

(δ) τα προσωπικά δεδομένα έτυχαν επεξεργασίας παρανόμως,

(ε) τα προσωπικά δεδομένα πρέπει να διαγραφούν σε συμμόρφωση με νομική υποχρέωση του υπεύθυνου επεξεργασίας που απορρέει από ενωσιακούς ή εθνικούς κανόνες,

(στ) τα προσωπικά δεδομένα έχουν συλλεχθεί σε σχέση με την προσφορά υπηρεσιών της κοινωνίας της πληροφορίας σε παιδιά.

Το δικαίωμα αυτό όμως δεν είναι απόλυτο· στην παράγραφο 3 προβλέπονται εξαιρέσεις που περιορίζουν το πεδίο εφαρμογής του και το υποκείμενο των δεδομένων δεν μπορεί να ασκήσει το εν λόγω δικαίωμα. Συγκεκριμένα, η περαιτέρω διατήρηση των προσωπικών δεδομένων κρίνεται σύννομη όταν είναι αναγκαία για την άσκηση του δικαιώματος ελευθερίας της έκφρασης και ενημέρωσης, για την συμμόρφωση με νομική υποχρέωση, για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας

Για να ενισχυθεί το δικαίωμα στην λήθη στο επιγραμμικό περιβάλλον, το δικαίωμα διαγραφής θα πρέπει επίσης να επεκταθεί με τέτοιο τρόπο ώστε ο υπεύθυνος επεξεργασίας ο οποίος δημοσιοποίησε τα δεδομένα προσωπικού

χαρακτήρα να υποχρεούται να ενημερώνει τους υπευθύνους επεξεργασίας που επεξεργάζονται τα εν λόγω δεδομένα προσωπικού χαρακτήρα ώστε να διαγράψουν οποιουσδήποτε συνδέσμους ή αντίγραφα ή αναπαραγωγή των εν λόγω δεδομένων προσωπικού χαρακτήρα. Όταν το πράττει, ο εν λόγω υπεύθυνος επεξεργασίας θα πρέπει να λαμβάνει εύλογα μέτρα, λαμβάνοντας υπόψη την διαθέσιμη τεχνολογία και τα μέσα που έχει στην διάθεσή του ο υπεύθυνος επεξεργασίας, μεταξύ άλλων και τεχνικά μέτρα, ώστε να ενημερωθούν οι υπεύθυνοι επεξεργασίας που επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα σχετικά με το αίτημα του υποκειμένου των δεδομένων.

v. Δικαίωμα περιορισμού της επεξεργασίας (αρθ. 18)

Μέθοδοι με τις οποίες περιορίζεται η επεξεργασία δεδομένων προσωπικού χαρακτήρα θα μπορούσαν να περιλαμβάνουν, μεταξύ άλλων, την προσωρινή μετακίνηση των επιλεγμένων δεδομένων σε άλλο σύστημα επεξεργασίας, την αφαίρεση της προσβασιμότητας των επιλεγμένων δεδομένων προσωπικού χαρακτήρα από τους χρήστες ή την προσωρινή αφαίρεση δημοσιευμένων δεδομένων από ιστοσελίδα. Στα συστήματα αυτοματοποιημένης αρχειοθέτησης ο περιορισμός της επεξεργασίας θα πρέπει κατ' αρχήν να διασφαλίζεται με τεχνικά μέσα κατά τρόπο ώστε τα δεδομένα προσωπικού χαρακτήρα να μην υπόκεινται σε πράξη περαιτέρω επεξεργασίας και να μην μπορούν να αλλάξουν. Το γεγονός ότι η επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι περιορισμένη θα πρέπει να αναγράφεται στο σύστημα.

vi. Δικαίωμα στην φορητότητα (άρθρο 20)

Το άρθρο 20 του Γενικού Κανονισμού θεσπίζει ένα νέο δικαίωμα για την προστασία των προσωπικών δεδομένων το οποίο παρέχει στα υποκείμενα την δυνατότητα να λαμβάνουν τα προσωπικά δεδομένα που έχουν παράσχει σε υπεύθυνο επεξεργασίας, σε δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα διαλειτουργικό μορφότυπο, καθώς και το δικαίωμα να διαβιβάζουν τα εν λόγω δεδομένα σε άλλον υπεύθυνο επεξεργασίας χωρίς

αντίρρηση.

Το νέο αυτό δικαίωμα έχει ως στόχο να βοηθήσει τους χρήστες να ανακτήσουν τον έλεγχο των προσωπικών τους δεδομένων, διευκολύνοντάς τους να τα διακινούν, να τα αντιγράφουν ή να τα διαβιβάζουν εύκολα από ένα περιβάλλον ΤΠ σε άλλο και από τον έναν υπεύθυνο επεξεργασίας σε άλλον. Το δικαίωμα εφαρμόζεται υπό την αίρεση τριών προϋποθέσεων· ειδικότερα,

1) τα ζητούμενα δεδομένα θα πρέπει να υποβάλλονται σε επεξεργασία με αυτοματοποιημένα μέσα είτε με βάση την προηγούμενη συγκατάθεση του υποκειμένου είτε με βάση τις ανάγκες εκτέλεσης σύμβασης.

2) τα ζητούμενα δεδομένα θα πρέπει να αφορούν το υποκείμενο και να έχουν παρασχεθεί από το ίδιο[33].

3) η άσκηση του δικαιώματος δεν θα πρέπει να επηρεάζει δυσμενώς τα δικαιώματα και τις ελευθερίες τρίτων.

Πρέπει να σημειωθεί ότι όταν ένα υποκείμενο ασκεί το δικαίωμά του στην φορητότητα των δεδομένων αυτό γίνεται με την επιφύλαξη κάθε άλλου δικαιώματος· δηλαδή μπορεί να ασκήσει και οποιοδήποτε άλλο δικαίωμα του παρέχεται για την προστασία της ιδιωτικότητάς του. Επιπροσθέτως, η φορητότητα δεν συνεπάγεται αυτομάτως διαγραφή των δεδομένων από τα συστήματα του υπευθύνου επεξεργασίας, π.χ. το υποκείμενο μπορεί να συνεχίσει να χρησιμοποιεί τις υπηρεσίες του υπεύθυνου επεξεργασίας και ο τελευταίος να συνεχίζει να επεξεργάζεται τα προσωπικά δεδομένα του πρώτου, ακόμα και μετά από την άσκηση του δικαιώματος φορητότητας.

[33] Παράρτημα WP242: «*Τα δεδομένα προσωπικού χαρακτήρα θεωρούνται παρεχόμενα από το υποκείμενο των δεδομένων όταν παρέχονται συνειδητά και ενεργητικά από το υποκείμενο των δεδομένων, όπως στοιχεία σε έναν λογαριασμό (π.χ. διεύθυνση αλληλογραφίας, όνομα χρήστη, ηλικία) που υποβάλλονται μέσω ηλεκτρονικών εντύπων, αλλά και όταν παράγονται και συλλέγονται από τις δραστηριότητες των χρηστών, μέσα από την χρήση μία ς υπηρεσίας ή συσκευής. Απεναντίας, δεδομένα προσωπικού χαρακτήρα τα ποία παράγονται ή συνάγονται από τα δεδομένα που παρέχει το υποκείμενο των δεδομένων, όπως προφίλ χρήστην το οποίο δημιουργείται με ανάλυση επεξεργασμένων δεδομένων από έξυπνο μετρητή, δεν εμπίπτουν στο πεδίο εφαρμογής του δικαιώματος στην φορητότητα των δεδομένων, καθώς δεν παρέχονται από το υποκείμενο των δεδομένων αλλά δημιουργούνται από τον υπεύθυνο επεξεργασίας.*

vii. Δικαίωμα εναντίωσης (άρθρο 21)

Σε περιπτώσεις που τα δεδομένα υποβάλλονται νόμιμα σε επεξεργασία επειδή η επεξεργασία είναι αναγκαία για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας ή για λόγους έννομων συμφερόντων του υπευθύνου επεξεργασίας ή τρίτου μέρους, κάθε υποκείμενο των δεδομένων θα πρέπει να δικαιούται παρ' όλα αυτά να αντιταχθεί στην επεξεργασία τυχόν δεδομένων προσωπικού χαρακτήρα που αφορούν την ιδιαίτερη κατάστασή του. Μετά την άσκηση του δικαιώματος εναπόκειται στον υπεύθυνο επεξεργασίας να αποδείξει ότι τα επιτακτικά έννομα συμφέροντά του υπερισχύουν ενδεχομένως των συμφερόντων ή των θεμελιωδών δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων. Αντιθέτως, σε περιπτώσεις που τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία για σκοπούς απευθείας εμπορικής προώθησης (συμπεριλαμβανομένης της κατάρτισης προφίλ για τους ίδιους σκοπούς), το υποκείμενο έχει το δικαίωμα να αντιτεθεί στην εν λόγω επεξεργασία ανά πάσα στιγμή και δωρεάν.

Το δικαίωμα αυτό θα πρέπει να περιέρχεται ρητά εις γνώσιν του υποκειμένου των δεδομένων και να παρουσιάζεται σαφώς και ξεχωριστά από κάθε άλλη πληροφορία, το αργότερο κατά την πρώτη επικοινωνία του υπευθύνου επεξεργασίας με το φυσικό πρόσωπο.

viii. Μη αυτοματοποιημένη λήψη αποφάσεων (άρθρο 22)

Στο άρθρο 22 του Κανονισμού προβλέπεται το δικαίωμα του υποκειμένου των δεδομένων να μην υπόκειται σε απόφαση με την οποία αξιολογούνται προσωπικές πτυχές που το αφορούν, και η οποία έχει ληφθεί αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας και η οποία παράγει έννομα αποτελέσματα έναντι του προσώπου αυτού ή το επηρεάζει σημαντικά σε οποιονδήποτε τομέα δραστηριότητάς του. Η επεξεργασία αυτή περιλαμβάνει την «κατάρτιση προφίλ»[34],

[34] Το ευρύ φάσμα προσωπικών δεδομένων που είναι διαθέσιμα στο διαδίκτυο αλλά και μέσω των διασυνδεδεμένων συσκευών (IoT) σε συνδυασμό με τις αυξημένες τεχνολογικές δυνατότητες συσχετισμών αυτών των δεδομένων χάρη στις τεχνικές ανάλυσης των big data, στην τεχνική

δηλαδή την με αυτοματοποιημένα μέσα επεξεργασία των προσωπικών δεδομένων με σκοπό την αξιολόγηση προσωπικών πτυχών σχετικά με ένα φυσικό πρόσωπο, ιδίως την ανάλυση ή την πρόβλεψη πτυχών που αφορούν τις επιδόσεις στην εργασία, την οικονομική κατάσταση, την υγεία, τις προσωπικές προτιμήσεις ή συμφέροντα, την αξιοπιστία ή την συμπεριφορά, την θέση ή κινήσεις του υποκειμένου των δεδομένων, και απώτερο σκοπό την λήψη απόφασης με έννομα αποτελέσματα για το υποκείμενο[35].

Σύμφωνα όμως με την σημείωση 71 του Προοιμίου, *η λήψη απόφασης που βασίζεται σε αυτήν την επεξεργασία, συμπεριλαμβανομένης της κατάρτισης προφίλ, επιτρέπεται όταν προβλέπεται ρητά από το δίκαιο της Ένωσης ή κράτους μέλους, στο οποίο υπόκειται ο υπεύθυνος επεξεργασίας, μεταξύ άλλων για σκοπούς παρακολούθησης και πρόληψης της απάτης και της φοροδιαφυγής σύμφωνα με τους κανονισμούς, τα πρότυπα και τις συστάσεις των θεσμικών οργάνων της Ένωσης ή των εθνικών οργάνων εποπτείας και προκειμένου να διασφαλιστεί η ασφάλεια και η αξιοπιστία της υπηρεσίας που παρέχει ο υπεύθυνος επεξεργασίας, ή όταν είναι αναγκαία για την σύναψη ή την εκτέλεση σύμβασης μεταξύ υποκειμένου των δεδομένων και υπευθύνου επεξεργασίας ή όταν το υποκείμενο των δεδομένων παρέσχε την ρητή συγκατάθεσή του. Σε κάθε περίπτωση, η επεξεργασία αυτή θα πρέπει να υπόκειται σε κατάλληλες εγγυήσεις, οι οποίες θα πρέπει να περιλαμβάνουν ειδική ενημέρωση του υποκειμένου των δεδομένων και το δικαίωμα εξασφάλισης ανθρώπινης παρέμβασης, το δικαίωμα διατύπωσης της άποψής του, το δικαίωμα να λάβει αιτιολόγηση της απόφασης που ελήφθη στο πλαίσιο της εν λόγω εκτίμησης και το δικαίωμα αμφισβήτησης της απόφασης.*

Περαιτέρω, η κατάρτιση προφίλ είναι νόμιμη όταν το υποκείμενο δίνει προς τούτο την συγκατάθεσή του· ωστόσο και σε αυτήν την περίπτωση ο Κανονισμός θέτει περιορισμούς και απαιτεί από τον υπεύθυνο επεξεργασίας να παρέχει εγγυήσεις, και συγκεκριμένα «*να χρησιμοποιεί κατάλληλες μαθηματικές ή στατιστικές διαδικασίες για την κατάρτιση του προφίλ, να εφαρμόζει τεχνικά και*

νοημοσύνη και την μηχανική μάθηση έχουν καταστήσει ευκολότερη την κατάρτιση προφίλ χρηστών και την λήψη αυτοματοποιημένων αποφάσεων.

[35] Π.χ. την παροχή ή όχι τραπεζικής πίστωσης η οποία βασίζεται σε αυτοματοποιημένα μοντέλα αποδοχής ή απόρριψης της αίτησης χωρίς ανθρώπινη παρέμβαση, η πρόσληψη ή μη σε θέση εργασίας με βάση την ηλεκτρονική κατάρτιση προφίλ και χωρίς ανθρώπινη αξιολόγηση.

οργανωτικά μέτρα, ώστε να διορθώνονται οι παράγοντες που οδηγούν σε ανακρίβειες σε δεδομένα προσωπικού χαρακτήρα και να ελαχιστοποιείται ο κίνδυνος σφαλμάτων, να καθιστά ασφαλή τα δεδομένα προσωπικού χαρακτήρα κατά τρόπο που να λαμβάνει υπόψη τους πιθανούς κινδύνους που συνδέονται με τα συμφέροντα και τα δικαιώματα του υποκειμένου των δεδομένων και κατά τρόπο που να προλαμβάνει, μεταξύ άλλων, τα αποτελέσματα διακρίσεων σε βάρος φυσικών προσώπων βάσει της φυλετικής ή εθνοτικής καταγωγής, των πολιτικών φρονημάτων, της θρησκείας ή των πεποιθήσεων, της συμμετοχής σε συνδικαλιστικές οργανώσεις, της γενετικής κατάστασης ή της κατάστασης της υγείας ή του γενετήσιου προσανατολισμού, ή μέτρων ισοδύναμου αποτελέσματος[36]».

4. Λήψη οργανωτικών μέτρων - εφαρμογή πολιτικών

Στο άρθρο 24 προβλέπεται η βασική και γενική υποχρέωση του υπευθύνου επεξεργασίας για την λήψη τεχνικών και οργανωτικών μέτρων και την εφαρμογή κατάλληλων πολιτικών για την αποτελεσματική προστασία των προσωπικών δεδομένων που επεξεργάζεται. Το εύρος και η δυναμική των υιοθετούμενων μέτρων και των πολιτικών πρέπει να είναι ανάλογα του επιπέδου κινδύνου που μπορεί να προκύψει από τις συγκεκριμένες πράξεις επεξεργασίας στα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, το είδος της βλάβης[37] που μπορούν να

[36] Βλ. περισσότερα: Σημείωση 71, Προοίμιο.

[37] Σημείωση 75, Προοίμιο: «*Οι κίνδυνοι για τα δικαιώματα και τις ελευθερίες φυσικών προσώπων, ποικίλης πιθανότητας και σοβαρότητας, είναι δυνατόν να προκύπτουν από την επεξεργασία δεδομένων προσωπικού χαρακτήρα η οποία θα μπορούσε να οδηγήσει σε σωματική, υλική ή μη υλική βλάβη. Η επεξεργασία μπορεί να οδηγήσει σε διακρίσεις, κατάχρηση ή υποκλοπή ταυτότητας, οικονομική απώλεια, βλάβη φήμης, απώλεια της εμπιστευτικότητας των προσωπικών δεδομένων που προστατεύονται από επαγγελματικό απόρρητο, παράνομη άρση της ψευδονυμοποίησης, ή οποιοδήποτε άλλο οικονομικό ή κοινωνικό μειονέκτημα. όταν τα υποκείμενα των δεδομένων θα μπορούσαν να στερηθούν των δικαιωμάτων και ελευθεριών τους ή να εμποδίζονται από την άσκηση ελέγχου επί των δεδομένων τους προσωπικού χαρακτήρα· όταν υπόκεινται σε επεξεργασία δεδομένα προσωπικού χαρακτήρα τα οποία αποκαλύπτουν φυλετική ή εθνοτική καταγωγή, πολιτικά φρονήματα, θρησκεία ή φιλοσοφικές πεποιθήσεις ή συμμετοχή σε συνδικάτα και γίνεται επεξεργασία γενετικών δεδομένων, δεδομένων που αφορούν την υγεία ή δεδομένων που αφορούν την σεξουαλική ζωή ή ποινικές καταδίκες και αδικήματα ή σχετικά μέτρα ασφάλειας· όταν αξιολογούνται προσωπικές πτυχές, ιδίως όταν επιχειρείται ανάλυση ή πρόβλεψη πτυχών που αφορούν τις επιδόσεις στην εργασία, την οικονομική κατάσταση, την υγεία, προσωπικές προτιμήσεις ή συμφέροντα, την αξιοπιστία ή την συμπεριφορά, την θέση ή μετακινήσεις, προκειμένου να δημιουργηθούν ή να χρησιμοποιηθούν προσωπικά προφίλ· όταν υποβάλλονται σε επεξεργασία δεδομένα προσωπικού χαρακτήρα ευάλωτων φυσικών προσώπων, ιδίως παιδιών· ή όταν η*

επιφέρουν καθώς και τις πιθανότητες επέλευσης αυτής της βλάβης.

Πρέπει να σημειωθεί ότι δεδομένης της επιταγής για ασφάλεια δικαίου και για σταθερό νομικό περιβάλλον ανάπτυξης επιχειρηματικής δραστηριότητας, δίνεται καθοδήγηση στις επιχειρήσεις και τους οργανισμούς για την υιοθέτηση κατάλληλων μέτρων και την απόδειξη συμμόρφωσής τους· τόσο το Συμβούλιο προστασίας δεδομένων (πρώην ομάδα αρθ. 29) όσο και ο νέος θεσμός του υπευθύνου προστασίας δεδομένων έχουν τον ρόλο αφενός το πρώτο να δίνει τις κατευθυντήριες γραμμές για τον προσδιορισμό των κινδύνων που συνδέονται με την επεξεργασία, την πιθανότητα επέλευσής τους και την ενσωμάτωση των βέλτιστων πρακτικών αποφυγής τους είτε με εγκεκριμένους κώδικες δεοντολογίας είτε εγκεκριμένες πιστοποιήσεις και αφετέρου ο δεύτερος να παρέχει πρακτικές και νομικές συμβουλές για την αποτελεσματική λήψη μέτρων και την συμμόρφωση με τον Κανονισμό. Τέλος και ο ENISA[38] κινούμενος προς την ίδια κατεύθυνση έχει ήδη εκδώσει εγχειρίδιο βέλτιστων πρακτικών για τις μικρομεσαίες επιχειρήσεις[39].

5. Προστασία by design και by default (άρθρο 25)

- by design – τεχνικά και οργανωτικά μέτρα ήδη από τον σχεδιασμό των πληροφοριακών συστημάτων
- by default – εξ ορισμού τα δεδομένα θα πρέπει να απολαύουν υψηλό βαθμό προστασίας ώστε να μην είναι προσβάσιμα σε ακαθόριστο αριθμό ατόμων (min data, min period, min accessibility)

Μια βασική οδηγία και κατεύθυνση προς την αποτελεσματική λήψη τεχνικών και οργανωτικών μέτρων είναι η ενσωμάτωσή τους στις επιχειρησιακές και πληροφοριακές διαδικασίες ήδη από τον σχεδιασμό (by design) και εξ ορισμού (by default). Συγκεκριμένα, ήδη από την σχεδίαση ενός πληροφοριακού συστήματος και τον καθορισμό της ροής των πληροφοριών θα πρέπει να υιοθετούνται οι βέλτιστες τεχνολογικές πρακτικές καθ' υπόδειξη των εξειδικευμένων επαγγελματιών ώστε να

επεξεργασία περιλαμβάνει μεγάλη ποσότητα δεδομένων προσωπικού χαρακτήρα και επηρεάζει μεγάλο αριθμό υποκειμένων των δεδομένων.»

[38] Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών.

[39] https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing

διαφυλάσσεται η ιδιωτικότητα των υποκειμένων των δεδομένων· επιπλέον, οι παράμετροι ιδιωτικότητας θα πρέπει να είναι ενεργοποιημένες εξ αρχής στις εφαρμογές και θα πρέπει τα οργανωτικά μέτρα να ακολουθούνται αυτόματα από τα εμπλεκόμενα στην επεξεργασία μέρη (υπαλλήλους του υπευθύνου επεξεργασίας – εκτελούντες την επεξεργασία) χωρίς να απαιτείται περαιτέρω υπενθύμιση από τον υπεύθυνο ή αίτηση από το υποκείμενο προς τούτο[40].

Οι αρχές της ιδιωτικότητας εξ ορισμού και της ιδιωτικότητας ήδη από τον σχεδιασμό αφορούν δύο εμπλεκόμενα μέρη, τόσο τους υπευθύνους επεξεργασίας που βασίζουν τις επιχειρησιακές τους διαδικασίες σε πληροφορικά προϊόντα και υπηρεσίες όσο και τους σχεδιαστές αυτών των προϊόντων.

Η συμμόρφωση με την εν λόγω επιταγή του Κανονισμού αποδεικνύεται με την λήψη τεχνικών μέτρων αλλά και με την ενσωμάτωση των προστατευτικών πολιτικών στις οργανωτικές και διαχειριστικές διαδικασίες μία ς επιχείρησης σε όλο το φάσμα και το εύρος της καθημερινότητάς της. Τα μέτρα θα μπορούσαν να περιλαμβάνουν, μεταξύ άλλων, την ελαχιστοποίηση των προσωπικών δεδομένων στα απολύτως απαραίτητα για την διεκπεραίωση της λειτουργίας της επιχείρησης, την ψευδωνυμοποίηση δεδομένων προσωπικού χαρακτήρα όσο το δυνατόν σε πιο αρχικό στάδιο, την διαφάνεια και την ενημέρωση των χρηστών όσον αφορά την επεξεργασία των δεδομένων τους. Ειδικότερα, κατά την σύλληψη και την ανάπτυξη των χαρακτηριστικών και της αρχιτεκτονικής τόσο ενός συνολικού πληροφοριακού συστήματος όσο και μία ς μεμονωμένης εφαρμογής οι σχεδιαστές θα πρέπει να έχουν ως γνώμονα την συμμόρφωση με το ρυθμιστικό πλαίσιο της προστασίας προσωπικών δεδομένων που εισήχθη με τον Γενικό Κανονισμό. Ακολούθως, οι υπεύθυνοι επεξεργασίας θα πρέπει να επιλέγουν πληροφοριακά προϊόντα και υπηρεσίες που οι τεχνολογικές προδιαγραφές τους εκπληρώνουν τις υποχρεώσεις που τους επιβάλλει ο Κανονισμός. Ωστόσο για τους υπεύθυνους επεξεργασίας η αρχή της ιδιωτικότητας by design δεν εξαντλείται στην σωστή επιλογή τεχνολογικών

[40] Λίλιαν Μήτρου: «*Η privacy by default εμπεριέχει δηλαδή υπό μία έννοια την απαίτηση της ενσωμάτωσης της ιδιωτικότητας κατά τον σχεδιασμό (by design) αλλά περαιτέρω προσδιορίζει ως ειδικότερο σκοπό τον σχεδιασμό ενός προγράμματος ή μία ς εφαρμογής κατά τρόπο ώστε οι χρήστες που επιθυμούν να προστατεύσουν την ιδιωτικότητά τους και τα προσωπικά τους δεδομένα να μην χρειάζεται να τροποποιήσουν τις προεπιλεγμένες ρυθμίσεις*». Βλ. Privacy by design – Η τεχνολογική διάσταση της προστασίας των προσωπικών δεδομένων, ΔιΜΕΕ, τεύχος 1/2013

λύσεων, αλλά στην εξέταση ήδη κατά το στάδιο του σχεδιασμού της όλης ροής και επεξεργασίας δεδομένων: σε ποιο μέτρο, τι είδος και ποιας ποσότητας δεδομένα είναι απαραίτητα για την διεκπεραίωση των σκοπών και των στόχων της επιχείρησης.

6. Τήρηση Αρχείου Δραστηριοτήτων Επεξεργασίας (αρθ.30)

Προκειμένου να μπορούν να αποδείξουν την συμμόρφωση προς τις αρχές και τις διατάξεις του κανονισμού, ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία υποχρεούνται να τηρούν αρχεία των δραστηριοτήτων επεξεργασίας που διενεργούν. Κάθε υπεύθυνος επεξεργασίας και κάθε εκτελών την επεξεργασία είναι υποχρεωμένος να συνεργάζεται με την εποπτική αρχή και κατόπιν αιτήματός της να θέτει στην διάθεσή της τα εν λόγω αρχεία, ώστε να μπορεί να ελέγξει την νομιμότητα των διενεργούμενων πράξεων επεξεργασίας. Σύμφωνα με την διάταξη του Κανονισμού, το εν λόγω αρχείο θα πρέπει να έχει ως ελάχιστο περιεχόμενο της εξής πληροφορίες: α) το όνομα και τα στοιχεία επικοινωνίας του υπευθύνου επεξεργασίας και, κατά περίπτωση, του από κοινού υπευθύνου επεξεργασίας, του εκπροσώπου του υπευθύνου επεξεργασίας και του υπευθύνου προστασίας δεδομένων, β) τους σκοπούς της επεξεργασίας, γ) περιγραφή των κατηγοριών υποκειμένων των δεδομένων και των κατηγοριών δεδομένων προσωπικού χαρακτήρα, τις κατηγορίες αποδεκτών στους οποίους πρόκειται να γνωστοποιηθούν ή γνωστοποιήθηκαν τα δεδομένα προσωπικού χαρακτήρα, περιλαμβανομένων των αποδεκτών σε τρίτες χώρες ή διεθνείς οργανισμούς, ε) όπου συντρέχει περίπτωση, τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα σε τρίτην χώρα ή διεθνή οργανισμό, συμπεριλαμβανομένων του προσδιορισμού της εν λόγω τρίτης χώρας ή του διεθνούς οργανισμού και, σε περίπτωση διαβιβάσεων που αναφέρονται στο άρθρο 49 παράγραφος 1 δεύτερο εδάφιο, της τεκμηρίωσης των κατάλληλων εγγυήσεων, στ) όπου είναι δυνατό, τις προβλεπόμενες προθεσμίες διαγραφής των διάφορων κατηγοριών δεδομένων, ζ) όπου είναι δυνατό, γενική περιγραφή των τεχνικών και οργανωτικών μέτρων ασφάλειας που αναφέρονται στο άρθρο 32 παράγραφος 1 (βλ. περισσότερα σελ. 88, *Τήρηση Αρχείου Δραστηριοτήτων*).

Ο Ευρωπαίος νομοθέτης, θέλοντας να ελαφρύνει τις μικρομεσαίες επιχειρήσεις από την δέσμη των νέων υποχρεώσεων με τις οποίες τις επιβαρύνει, θέσπισε μία εξαίρεση· όπως αναφέρει και στην αιτιολογική σκέψη 13 του Κανονισμού «*για να ληφθεί υπόψη η ειδική κατάσταση των πολύ μικρών, των μικρών και των μεσαίων επιχειρήσεων, ο παρών κανονισμός περιλαμβάνει παρέκκλιση για οργανισμούς που απασχολούν λιγότερα από 250 άτομα όσον αφορά την τήρηση αρχείων*». Έτσι, σύμφωνα με το άρθρο 30 παρ. 5 κατ' αρχήν οι επιχειρήσεις με λιγότερους από 250 εργαζόμενους δεν είναι υποχρεωμένες να τηρούν αρχείο δραστηριοτήτων επεξεργασίας: *επιχείρηση ή οργανισμός που απασχολεί λιγότερα από 250 άτομα, εκτός εάν η διενεργούμενη επεξεργασία ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων, η επεξεργασία δεν είναι περιστασιακή ή η επεξεργασία περιλαμβάνει ειδικές κατηγορίες δεδομένων κατά το άρθρο 9 παράγραφος 1 ή επεξεργασία δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα που αναφέρονται στο άρθρο 10.* Ωστόσο αυτή η εξαίρεση όπως είναι άλλωστε εμφανές, δεν είναι απόλυτη, και επιστρέφει στον γενικό κανόνα της παραγράφου 1 στις εξής περιπτώσεις:

1. η επεξεργασία αποτελεί βασική δραστηριότητα της επιχείρησης
2. η επεξεργασία προκαλεί κίνδυνο για τα δικαιώματα και τις ελευθερίες
3. η επεξεργασία αφορά ευαίσθητα προσωπικά δεδομένα (αρθ. 9 παρ.1)
4. η επεξεργασία αφορά ποινικά δεδομένα (αρθ.10)

Κατά την άποψη της ομάδας του άρθρου 29[41] οι επιχειρήσεις ή οι οργανισμοί που απασχολούν λιγότερους από 250 υπαλλήλους αλλά επεξεργάζονται δεδομένα που εμπίπτουν στις προαναφερθείσες 4 κατηγορίες υποχρεούνται να κρατούν αρχείο δραστηριοτήτων μόνο για την επεξεργασία που αφορά αυτά τα δεδομένα. Για παράδειγμα, μία μικρή επιχείρηση πιθανόν να επεξεργάζεται συχνά τα προσωπικά δεδομένα των υπαλλήλων της· ως εκ τούτου, αυτή η επεξεργασία δεν μπορεί να θεωρηθεί περιστασιακή και θα πρέπει να τηρείται αρχείο δραστηριοτήτων επεξεργασίας. Ωστόσο, άλλες ενέργειες επεξεργασίας προσωπικών δεδομένων που όντως είναι περιστασιακές και επιπλέον δεν επιφέρουν κίνδυνο

[41] Γνωμοδοτικό έγγραφο της ομάδας του αρθ. 29 σχετικά με τις παρεκκλίσεις από την υποχρέωση τήρησης αρχείου δραστηριοτήτων, http://ec.europa.eu/newsroom/article29/itemdetail.cfm?item_id=624045

στις ελευθερίες και τα δικαιώματα των υποκειμένων ούτε εμπίπτουν στην κατηγορία των ευαίσθητων ή των ποινικών δεδομένων δεν χρειάζεται να καταγράφονται.

7. Μέτρα Ασφαλείας (άρθρο 32)

Το τρίπτυχο των αρχών της Εμπιστευτικότητας – Ακεραιότητας – Διαθεσιμότητας (Confidentiality – Integrity – Availability) συνιστά την θεμέλια λίθο της αρχής της ασφάλειας.

Τα προσωπικά δεδομένα που επεξεργάζεται ένας υπεύθυνος επεξεργασίας είτε μέσω πληροφοριακών συστημάτων είτε σε έντυπη μορφή πρέπει να παραμένουν εμπιστευτικά και απόρρητα, και μόνον όποιος έχει έννομο συμφέρον, βάσει ειδικού νόμου, επιτρέπεται να λάβει γνώση αυτών και να έχει πρόσβαση στο περιεχόμενό τους. Επιπλέον, τα δεδομένα θα πρέπει να διατηρούνται ακέραια, δηλαδή να μην αλλοιώνεται με οιονδήποτε τρόπο το περιεχόμενο και το μορφότυπό τους. Τέλος, τα δεδομένα θα πρέπει να είναι ανά πάσα στιγμή διαθέσιμα προκειμένου να έχουν πρόσβαση σε αυτά οι εξουσιοδοτημένοι χρήστες τους για να μπορούν να παράσχουν τις υπηρεσίες τους. Συμπληρωματική αρχή του τρίπτυχου CIA είναι η αρχή της μη αποκήρυξης (no-repudation) βάσει της οποίας ένας υπεύθυνος επεξεργασίας ή ένας εκτελών την επεξεργασία δεν μπορεί να αρνηθεί ότι προέβη σε μία ενέργεια.

Η λήψη μέτρων για την ασφάλεια δεδομένων δεν συνιστά μόνο νομική υποχρέωση των υπευθύνων επεξεργασίας, αλλά και αναπόσπαστο στοιχείο της δομής, οργάνωσης και λειτουργίας μία ς οντότητας με επιχειρησιακές διαδικασίες. Στην σημερινή εποχή της Κοινωνίας της Πληροφορίας η ασφάλεια καθίσταται αναγκαιότητα τόσο λόγω του υποχρεωτικού και αυστηρού ρυθμιστικού πλαισίου του Γενικού Κανονισμού 2016/679 όσο και λόγω της πρακτικής παραδοχής της αύξησης των περιστατικών ασφαλείας παγκοσμίως.

Για την διατήρηση της ασφάλειας αφ’ ενός από εξωτερικές επιθέσεις και αφ’ ετέρου από εσωτερικές παραβάσεις του Κανονισμού, ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία κατόπιν αξιολόγησης της πιθανότητας επέλευσης τινός

κινδύνου και της βαρύτητας των συνεπειών του (risk-based approach) πρέπει να υιοθετεί τα κατάλληλα μέτρα για την αποφυγή επέλευσής του ή τον μετριασμό των συνεπειών του. Κατά την εκτίμηση του κινδύνου για την ασφάλεια των δεδομένων θα πρέπει να ληφθούν υπ' όψιν ως πιθανοί κίνδυνοι: η τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ αδείας κοινολόγηση ή προσπέλαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία η οποία θα μπορούσε να οδηγήσει σε σωματική, υλική ή μη υλική βλάβη. Όταν η επεξεργασία ενδέχεται να έχει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας θα πρέπει να διενεργεί εκτίμηση αντικτύπου στην οποία να αξιολογήσει την προέλευση, την φύση, την πιθανότητα και την σοβαρότητα του εν λόγω κινδύνου και λαμβάνοντας αυτά τα στοιχεία υπ' όψιν να λάβει τα ενδεικνυόμενα μέτρα προκειμένου η διενεργούμενη επεξεργασία να είναι σύμφωνη με τις επιταγές του Κανονισμού.

Το άρθρο 32 αναφέρει ως ενδεικτικά οργανωτικά και τεχνικά μέτρα για την διασφάλιση της ασφάλειας της επεξεργασίας:

α) την κρυπτογράφηση και την ψευδωνυμοποίηση[42] των δεδομένων προσωπικού χαρακτήρα,

β) την πολιτική διασφάλισης του απορρήτου, της ακεραιότητας, της διαθεσιμότητας και της αξιοπιστίας των συστημάτων και των υπηρεσιών,

γ) την πολιτική αποκατάστασης της διαθεσιμότητας και της πρόσβασης στα συστήματα σε σύντομο χρόνο σε περίπτωση επέλευσης κάποιου κινδύνου,

δ) την τήρηση διαδικασιών ελέγχων, δοκιμών και αξιολογήσεων των επιλεχθέντων μέτρων.

Ήδη από το 2010[43] η ομάδα εργασίας του άρθρου 29 στην υπ' αριθμ. 3/2010 γνώμη

[42] Βλ. σημείο 28-30 Προοιμίου. (28) *Η χρήση της ψευδωνυμοποίησης στα δεδομένα προσωπικού χαρακτήρα μπορεί να μειώσει τους κινδύνους για τα υποκείμενα των δεδομένων και να διευκολύνει τους υπευθύνους επεξεργασίας και τους εκτελούντες την επεξεργασία να τηρήσουν τις οικείες υποχρεώσεις περί προστασίας των δεδομένων. Η ρητή εισαγωγή της «ψευδωνυμοποίησης» του παρόντος κανονισμού δεν προορίζεται να αποκλείσει κάθε άλλο μέτρο προστασίας των δεδομένων..*

[43] Και μετά την έγκριση των Διεθνών Προτύπων της Μαδρίτης ("Madrid Resolution" on international privacy standards) κατά την Διεθνή Διάσκεψη επιτρόπων προστασίας δεδομένων και ιδιωτικότητας

της τόνιζε την ανάγκη θέσπισης μία ς αρχής λογοδοσίας δυνάμει της οποίας οι υπεύθυνοι επεξεργασίας να υποχρεούνται να εφαρμόζουν τα αναγκαία μέτρα για την τήρηση και υλοποίηση των αρχών για την προστασία των δεδομένων προσωπικού χαρακτήρα κατά την επεξεργασία και να αποδεικνύουν την συμμόρφωσή τους εφόσον το ζητήσουν οι αρμόδιες αρχές. Στην ίδια γνώμη παρέθεσε και έναν ενδεικτικό κατάλογο με μέτρα που θα αποδεικνύουν την συμμόρφωση με τον όρο ότι θα επαναξιολογούνται τακτικά ως προς την αποτελεσματικότητά τους λαμβανομένων υπ' όψιν οργανωτικών μεταβολών και τεχνολογικών εξελίξεων· τα εν λόγω μέτρα έχουν ενσωματωθεί στο σύνολό τους στον νέο Κανονισμό. Ενδεικτικά,

- θέσπιση γραπτών και δεσμευτικών πολιτικών προστασίας δεδομένων· (αρθ. 32 Κ)
- χαρτογράφηση διαδικασιών ώστε να διασφαλίζεται κατάλληλη αναγνώριση όλων των εργασιών επεξεργασίας δεδομένων, και διατήρηση καταλόγου εργασιών επεξεργασίας δεδομένων· (αρθ. 30 Κ)
- διορισμός υπευθύνου για την προστασία των δεδομένων· (αρθ. 37 Κ)
- παροχή κατάλληλης εκπαίδευσης και κατάρτισης στους υπαλλήλους στην προστασία δεδομένων· (αρθ. 35 Κ)
- θέσπιση διαδικασιών για την διαχείριση των αιτημάτων πρόσβασης, διόρθωσης και διαγραφής, η οποία πρέπει να είναι διαφανής για τα άτομα στα οποία αναφέρονται τα δεδομένα·
- εγκαθίδρυση εσωτερικού μηχανισμού χειρισμού καταγγελιών·
- θέσπιση εσωτερικών διαδικασιών για την αποτελεσματική διαχείριση και αναφορά παραβιάσεων της ασφάλειας· (αρθ. 33 -34 Κ)
- διενέργεια αξιολόγησης του αντικτύπου στην ιδιωτική ζωή σε ειδικές περιπτώσεις· (αρθ. 35)
- εφαρμογή και επίβλεψη διαδικασιών επαλήθευσης, ώστε να διασφαλίζεται ότι όλα τα μέτρα όχι μόνον υπάρχουν στα χαρτιά, αλλά εφαρμόζονται και

όπου περιλήφθηκε η αρχή της λογοδοσίας ως εξής: «*Ο υπεύθυνος οφείλει: «α. να λαμβάνει όλα τα αναγκαία μέτρα για την τήρηση των αρχών και των υποχρεώσεων που περιγράφονται στο παρόν έγγραφο και στην ισχύουσα εθνική νομοθεσία και β. να διαθέτει τους αναγκαίους εσωτερικούς μηχανισμούς ώστε να αποδεικνύει την εν λόγω τήρηση τόσο στα πρόσωπα στα οποία αναφέρονται τα δεδομένα όσο και στις αρχές ελέγχου κατά την άσκηση των εξουσιών τους, όπως προβλέπεται στην παράγραφο 23*». Βλ. περισσότερα, Γνώμη 3/2010 Ομάδα άρθρου 29, σημείωση 7 σελ. 14.

λειτουργούν στην πράξη (εσωτερικοί ή εξωτερικοί έλεγχοι κ.λπ.)· (αρθ. 32)

8. Γνωστοποίηση και ανακοίνωση περιστατικών παραβίασης (αρθ.33-34)

Η παραβίαση δεδομένων [data breach] επέρχεται όταν παραβιαστεί η ασφάλεια του πληροφοριακού συστήματος μίας εταιρείας ή ενός οργανισμού με αποτέλεσμα την παραβίαση του απορρήτου, της διαθεσιμότητας ή της ακεραιότητας των δεδομένων που διατηρεί. Όταν επισυμβεί ένα περιστατικό ασφαλείας είναι πιθανό να τεθούν σε κίνδυνο τα δικαιώματα και οι ελευθερίες φυσικού προσώπου και εάν δεν αντιμετωπιστεί κατάλληλα και έγκαιρα, να έχει ως αποτέλεσμα σωματική, υλική ή μη υλική βλάβη για τα φυσικά πρόσωπα, όπως απώλεια του ελέγχου επί των δεδομένων τους προσωπικού χαρακτήρα ή περιορισμός των δικαιωμάτων τους, διακρίσεις, κατάχρηση ή υποκλοπή ταυτότητας, οικονομική απώλεια, παράνομη άρση της ψευδωνυμοποίησης, βλάβη της φήμης, απώλεια της εμπιστευτικότητας των δεδομένων προσωπικού χαρακτήρα που προστατεύονται από επαγγελματικό απόρρητο ή άλλο σημαντικό οικονομικό ή κοινωνικό μειονέκτημα για το ενδιαφερόμενο φυσικό πρόσωπο. Με τον GDPR καθίσταται πλέον υποχρέωση και των υπευθύνων επεξεργασίας[44] να προβαίνουν κατ' αρχήν: αφενός σε γνωστοποίηση στις εποπτικές Αρχές περιστατικού παραβίασης των δεδομένων που διαχειρίζονται, αφετέρου, αλλά και υπό προϋποθέσεις, σε ανακοίνωση της παραβίασης και στο υποκείμενο τα δεδομένα του οποίου έχουν προσβληθεί. Οι νέες αυτές υποχρεώσεις προβλέπονται στα άρθρα 33 και 34 του Κανονισμού, και αναλύονται περαιτέρω τόσο στις αιτιολογικές σκέψεις του προοιμίου του όσο και στις πρόσφατες κατευθυντήριες γραμμές της Ομάδας Εργασίας του άρθρου 29[45]. Στόχος είναι η κατάλληλη και έγκαιρη αντιμετώπιση της παραβίασης, με τρόπο που να περιορίζει, ει δυνατόν να εξαλείφει τις αρνητικές συνέπειές της, οι οποίες όχι σπάνια, συνίστανται σε σωματική, υλική ή μη υλική βλάβη των θιγόμενων φυσικών

[44] Όχι μόνο για τους παρόχους ψηφιακών υπηρεσιών και των Φορέων εκμετάλλευσης βασικών υπηρεσιών όπως ίσχυε βάσει του προηγούμενου νομοθετικού καθεστώτος (12 παρ.5 έως 10 ν. 3471/2006, του άρθρου 13 Κοινής Πράξης 01/2013 ΑΔΠΔΧ και ΑΔΑΕ, με τις οποίες ενσωματώθηκαν εν πολλοίς στο ελληνικό δίκαιο οι προβλέψεις του άρθρου 4 της οδηγίας 2002/58/ΕΚ όπως τροποποιήθηκε με την οδηγία 2009/136/ΕΚ)

[45] WP250, Guidelines on Personal data breach notification under Regulation 2016/679, Adopted on 3 October 2017.

προσώπων.

i. Γνωστοποίηση

Βάσει του άρθρου αρθ. 34, μόλις ο υπεύθυνος επεξεργασίας λάβει γνώση μία ς παραβίασης δεδομένων προσωπικού χαρακτήρα θα πρέπει αμελλητί και χωρίς υπαίτια καθυστέρηση, εντός 72 ωρών, να γνωστοποιήσει την παραβίαση των δεδομένων προσωπικού χαρακτήρα στην αρμόδια εποπτική αρχή[46]. Ωστόσο, η υποχρέωση αυτή κάμπτεται εάν ο υπεύθυνος επεξεργασίας μπορεί να αποδείξει [αρχή της λογοδοσίας], ότι η προκείμενη παραβίαση των προσωπικών δεδομένων δεν ενδέχεται να επιφέρει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων[47]. Σε περίπτωση που αυτή η γνωστοποίηση δεν δύναται να επιτευχθεί εντός 72 ωρών, η μεταγενέστερη γνωστοποίηση θα πρέπει να συνοδεύεται από αιτιολογία για τους λόγους της καθυστέρησης[48]. Περαιτέρω, και οι εκτελούντες την επεξεργασία είναι επιφορτισμένοι με σημαντικό ρόλο, καθώς πρέπει να ενημερώνουν τον υπεύθυνο επεξεργασίας αμέσως μόλις αντιληφθούν κάποια παραβίαση δεδομένων προσωπικού χαρακτήρα. Πιο συγκεκριμένα:

Όσον αφορά την προθεσμία 72 ωρών για την γνωστοποίηση της παραβίασης, η

[46] Παράρτημα Ι. Παράθεση εντύπου υποβολής γνωστοποίησης περιστατικού ασφαλείας από την ΑΠΔΠΧ.

[47] σελ.15-16, η WP29 εξηγεί ότι η παραβίαση προσωπικών δεδομένων που έχουν κρυπτογραφηθεί με αλγόριθμο σύγχρονης τεχνολογίας πρέπει να κοινοποιηθεί. Ωστόσο, εάν η εμπιστευτικότητα του κλειδιού παραμείνει ανέπαφη, δηλαδή εάν το κλειδί δεν επηρεάστηκε και δημιουργήθηκε έτσι ώστε να παραμένει απρόσβλητο με βάση τα διαθέσιμα τεχνικά μέσα από οποιοδήποτε μη εξουσιοδοτημένο χρήστη, τότε τα δεδομένα είναι, κατ' αρχήν, απροσπέλαστα (δεδομένου ότι παραμένουν "unintelligible"). μία τέτοια παραβίαση είναι απίθανο να θέσει σε κίνδυνο τα δικαιώματα και τις ελευθερίες των ατόμων. Ωστόσο, ακόμη και όταν τα δεδομένα είναι κρυπτογραφημένα, μία απώλεια ή αλλοίωση μπορεί να έχει αρνητικές συνέπειες για τα υποκείμενα των δεδομένων, όπου ο controller δεν έχει διατηρήσει αντίγραφα ασφαλείας. Σε αυτή την περίπτωση, απαιτείται η γνωστοποίηση (και κατ' επέκταση η ανακοίνωση στο υποκείμενο), ακόμη και αν τα ίδια τα δεδομένα διαθέτουν επαρκή κρυπτογράφηση.

[48] Ό.π. Γνώμη Ομάδας 29, σελ 14. Ανάλογα με τις περιστάσεις, μπορεί να αποδειχθεί ιδιαιτέρως χρονοβόρος ο ακριβής προσδιορισμός της έκτασης των παραβιάσεων, οπότε αντί να κοινοποιήσει κάθε παραβίαση ξεχωριστά, ο υπεύθυνος επεξεργασίας ενσωματώνει σε μία συνολική κοινοποίηση τα επιμέρους περιστατικά παραβιάσεων· αυτό οπωσδήποτε προκαλεί καθυστέρηση της κοινοποίησης στην εποπτική αρχή. Τυπικά, άλλωστε, κάθε ατομική παραβίαση αποτελεί ανακοινώσιμο περιστατικό. Ωστόσο, στο προκείμενο παράδειγμα, ο υπεύθυνος επεξεργασίας μπορεί να υποβάλει μία κοινοποίηση που να αντιπροσωπεύει όλες τις παραβιάσεις, υπό την προϋπόθεση ότι αφορούν στον ίδιο τύπο δεδομένων που παραβιάζεται με τον ίδιο τρόπο και μάλιστα σε σχετικά μικρές μεταξύ τους χρονικές αποστάσεις. (Εννοείται πως εάν σημειωθεί σειρά παραβιάσεων που αφορούν σε διαφορετικούς τύπους δεδομένων προσωπικού χαρακτήρα, τα οποία παραβιάζονται με διαφορετικούς τρόπους, τότε η κοινοποίηση πρέπει να λάβει χώρα για κάθε παραβίαση χωριστά).

WP29 υποστηρίζει ότι ο υπεύθυνος επεξεργασίας θεωρείται ενήμερος όταν βεβαιωθεί ότι έχει σημειωθεί περιστατικό παραβίασης, γεγονός που εξαρτάται από τις ιδιαίτερες συνθήκες της συγκεκριμένης παραβίασης. Συνήθως μπορεί να διαπιστωθεί άμεσα η παραβίαση, αλλά υπάρχουν περιπτώσεις που απαιτούν έρευνα στα αρχεία καταγραφής ενεργειών του συστήματος για την διαπίστωση της παραβίασης ή της μη εξουσιοδοτημένης πρόσβασης[49]. Ωστόσο, η έμφαση πρέπει να δοθεί στην άμεση ανάληψη δράσης κατ' αρχάς για την διερεύνηση της παραβίασης και σε δεύτερη φάση για το πώς αυτή μπορεί να επηρεάσει τα υποκείμενα των δεδομένων και για το εάν απαιτείται περαιτέρω ανακοίνωση και σε αυτά για την προστασία τους.

Όσον αφορά τους εκτελούντες την επεξεργασία, οι οποίοι στην πράξη είναι αυτοί που αντιλαμβάνονται την παραβίαση· σύμφωνα με τις κατευθυντήριες γραμμές της Ομάδας του άρθρου 29[50] «ο εκτελών την επεξεργασία πρέπει μόλις διαπιστώσει ότι έχει σημειωθεί παραβίαση να ειδοποιήσει τον υπεύθυνο επεξεργασίας· συνεπώς, κατ' αρχήν, ο υπεύθυνος επεξεργασίας θεωρείται "ενήμερος" από την στιγμή που ο εκτελών τον ενημερώσει σχετικά με την παραβίαση». Η ερμηνεία αυτή της Ομάδας 29 είναι ιδιαίτερα κρίσιμη καθώς ξεκαθαρίζει το χρονικό σημείο από όπου αρχίζει να υπολογίζεται η προθεσμία των 72 ωρών για την γνωστοποίηση στην εποπτική αρχή, δεδομένου ότι η καθυστέρηση ή μη γνωστοποίηση παραβίασης σε ένα υποκείμενο δεδομένων ή στην εποπτική αρχή ενδέχεται να συνεπάγεται την επιβολή κυρώσεων, δυνάμει του άρθρου 83.

Το περιεχόμενο της γνωστοποίησης πρέπει κατ' ελάχιστο να περιλαμβάνει[51]:

i. περιγραφή της φύσης της παραβίασης δεδομένων, συμπεριλαμβανομένων

[49] μία τέτοιου είδους περίπτωση είναι και όταν η ενημέρωση για την παραβίαση προέρχεται από τρίτον ή από τα ΜΜΕ, οπότε για να εντοπιστεί το περιστατικό ασφαλείας και να θεωρηθεί ότι ο υπεύθυνος έλαβε γνώση πρέπει πρώτα να διενεργηθεί η απαραίτητην έρευνα στα πληροφοριακά συστήματα.

[50] Guidelines on Personal data breach notification under Regulation 2016/679, 18/EN WP250rev.01.

[51] Όπου δεν είναι δυνατό να παρασχεθούν οι πληροφορίες ταυτόχρονα, μπορούν να παρέχονται σταδιακά χωρίς αδικαιολόγητην καθυστέρηση, εφόσον ο υπεύθυνος της επεξεργασίας αιτιολογεί την καθυστέρηση, σύμφωνα με το άρθρο 33 παρ.1 και παρ. 4. Κάτι τέτοιο μπορεί να συμβεί σε περιπτώσεις σύνθετων παραβιάσεων, όπου συνήθως απαιτείται η εις βάθος διερεύνηση των συνθηκών της παραβίασης για την πλήρη εξακρίβωση της φύσης της και του βαθμού διακινδύνευσης των προσωπικών δεδομένων.

των κατηγοριών και του κατά προσέγγιση αριθμού των επηρεαζόμενων τόσο υποκειμένων των δεδομένων, όσο και αρχείων δεδομένων. Παρ' όλο που στον Κανονισμό δεν αποσαφηνίζεται σε τι θα συνίσταται η «κατηγοριοποίηση», η Ομάδα 29 θεωρεί ότι οι κατηγορίες θα αφορούν είτε σε διάφορους τύπους ατόμων των οποίων τα προσωπικά δεδομένα έχουν προσβληθεί (ανηλίκους, άλλες ευάλωτες ομάδες, άτομα με αναπηρίες ή ακόμη και το πελατολόγιο μία ς επιχείρησης) είτε σε κατηγορίες αρχείων και τύπων προσωπικών δεδομένων, όπως δεδομένα υγείας, εκπαιδευτικά αρχεία, πληροφορίες κοινωνικής μέριμνας, οικονομικά στοιχεία, αριθμοί τραπεζικών λογαριασμών, αριθμοί διαβατηρίων κλπ. Όπως προαναφέρθηκε, ένας από τους σκοπούς της κοινοποίησης είναι ο περιορισμός της βλάβης των θιγομένων προσώπων· συνεπώς, εάν οι τύποι των προσώπων ή οι τύποι των δεδομένων μεγιστοποιούν την πιθανότητα πρόκλησης βλάβης από την παραβίαση (π.χ. κλοπή ταυτότητας, απάτη, οικονομική ζημία, απειλή επαγγελματικού απορρήτου), τότε είναι σημαντικό η κοινοποίηση να επισημαίνει αυτές τις κατηγορίες, καθώς και τις πιθανές συσχετιζόμενες συνέπειες.

ii. ανακοίνωση του ονόματος και των στοιχείων επικοινωνίας του υπεύθυνου προστασίας δεδομένων (Data Protection Officer - DPO) ή άλλου σημείου επικοινωνίας,

iii. Περιγραφή των ενδεχόμενα επερχόμενων συνεπειών της παραβίασης

iv. Περιγραφή των ήδη ληφθέντων ή των προτεινόμενων προς λήψη μέτρων για την αντιμετώπιση της παραβίασης των δεδομένων, καθώς και μέτρων για τυχόν άμβλυνση των ενδεχόμενων δυσμενών συνεπειών της.

Εξάλλου, η κοινοποίηση στην εποπτική αρχή δίνει την δυνατότητα στον υπεύθυνο επεξεργασίας να ζητήσει οδηγίες και καθοδήγηση ώστε να βεβαιωθεί ότι τα επόμενα βήματά του σχετικά με την ανακοίνωση ή μη στοιχείων στα θιγόμενα πρόσωπα είναι σωστά (αρθ. 58, παρ. 2 περ. ε). Ωστόσο, ο σκοπός της γνωστοποίησης στην εποπτική αρχή δεν είναι μόνο η παροχή καθοδήγησης σχετικά με το αν θα ειδοποιηθούν τα θιγόμενα πρόσωπα. Βέβαια σε ορισμένες περιπτώσεις, λόγω της φύσης της παραβίασης και της σοβαρότητας του κινδύνου, ο υπεύθυνος

της επεξεργασίας θα πρέπει να ειδοποιήσει χωρίς καθυστέρηση τα υποκείμενα των δεδομένων και μάλιστα σε εξαιρετικές περιπτώσεις μπορεί να επιβάλλεται να ενημερώσει πρώτα το υποκείμενο και μετά την αρχή! Γενικότερα, η Ομάδα 29 δέχεται ότι η γνωστοποίηση στην εποπτική αρχή δεν μπορεί να χρησιμεύσει ως δικαιολογία για την μη κοινοποίηση της παραβίασης στο υποκείμενο των δεδομένων.[52]

ii. Ανακοίνωση

Σύμφωνα με το άρθρο 34, όταν η παραβίαση ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων, ο υπεύθυνος επεξεργασίας πρέπει να τα ενημερώνει αμελλητί προκειμένου να μπορέσουν να λάβουν τις αναγκαίες προφυλάξεις. Όπως διευκρινίζει ο Κανονισμός στο προοίμιό του, ο χαρακτήρας της εν λόγω ανακοίνωσης συνίσταται κυρίως στην παροχή ειδικών πληροφοριών και συστάσεων προς τα ενδιαφερόμενα φυσικά πρόσωπα για τον μετριασμό των δυνητικών δυσμενών συνεπειών. Ειδικότερα:

Το περιεχόμενο της ανακοίνωσης πρέπει κατ' ελάχιστο να περιλαμβάνει σαφή περιγραφή της παραβίασης, όνομα και στοιχεία επικοινωνίας του DPO, περιγραφή των ενδεχόμενων συνεπειών της παραβίασης, καθώς και περιγραφή των ληφθέντων ή προτεινόμενων μέτρων αντιμετώπισης ή μετριασμού των δυσμενών συνεπειών, σε αντιστοιχία με το περιεχόμενο της γνωστοποίησης κατ' άρθρο 33 παρ. 3.

Όσον αφορά την σωστή ενημέρωση των υποκειμένων αλλά και την εξασφάλιση ότι αυτή είναι σαφής και κατανοητή, θα πρέπει να χρησιμοποιούνται ειδικά μηνύματα (dedicated messages), τα οποία θα αφορούν μόνο την επίδικη παραβίαση και δεν θα περιλαμβάνουν άλλες πληροφορίες ή ενημερώσεις. Αυτό βοηθά να καταστεί η ανακοίνωση της παραβίασης σαφής, κατανοητή και διαφανής. Παραδείγματα μεθόδων διαφανούς και αξιόπιστης επικοινωνίας περιλαμβάνουν άμεση ανταλλαγή μηνυμάτων (π.χ. emails, SMS, άμεσα μηνύματα), banners ή ειδοποιήσεις pop-up, ταχυδρομική αλληλογραφία και ανακοινώσεις σε έντυπα

[52] Ό.π. Γνώμη Ομάδας αρθ. 29, σελ. 13.

μέσα. Η Ομάδα 29 συνιστά στους controllers να επιλέγουν εκείνο το μέσο που κρίνεται κάθε φορά ότι μεγιστοποιεί την πιθανότητα σωστής επικοινωνίας των πληροφοριών σε όλα τα υποκείμενα δεδομένων που έχουν προσβληθεί.[53]

Σύμφωνα με τις περιοριστικά αναφερόμενα προϋποθέσεις της παραγράφου 3, δεν απαιτείται ανακοίνωση στα υποκείμενα των δεδομένων:

i. Εάν έχουν εφαρμοστεί ήδη τεχνικά και οργανωτικά μέτρα προστασίας που αφορούσαν στα δεδομένα που παραβιάστηκαν και που να τα καθιστούν μη κατανοητά στους μη έχοντες άδεια πρόσβασης (π.χ. κρυπτογράφηση),
ii. Εάν κατόπιν του περιστατικού ασφαλείας εφαρμόστηκαν μέτρα διασφάλισης των δικαιωμάτων και ελευθεριών των υποκειμένων από την επέλευση του υψηλού κινδύνου που αναφέρεται στην παρ.1 και,
iii. Εάν η ανακοίνωση προϋποθέτει δυσανάλογες προσπάθειες, περίπτωση κατά την οποία αντ' αυτής πραγματοποιείται δημόσια ανακοίνωση.

Η Ομάδα 29 επισημαίνει ότι σύμφωνα με την αρχή της λογοδοσίας, ο υπεύθυνος επεξεργασίας θα πρέπει να είναι σε θέση να αποδείξει στην εποπτική αρχή ότι πληρείται τουλάχιστον ένας από τους ως άνω αναφερόμενους όρους. Σημειώνει δε, ότι πρέπει να ληφθεί υπόψη το γεγονός πως κι αν ακόμη δεν διαφαίνεται αρχικά κίνδυνος για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, τίποτε δεν εξασφαλίζει ότι αυτό δεν θα αλλάξει προϊόντος του χρόνου και καθόσον προάγεται η έρευνα. Συνεπώς, το στοιχείο του υψηλού κινδύνου θα πρέπει να επανεκτιμάται.[54]

Σε περίπτωση που ο υπεύθυνος επεξεργασίας αποφασίσει να μην ανακοινώσει το συμβάν στα υποκείμενα, η εποπτική αρχή μπορεί να το απαιτήσει, αν θεωρεί ότι η παραβίαση ενδέχεται να θέσει σε υψηλό κίνδυνο εν λόγω δεδομένα. Εναλλακτικά, μπορεί να θεωρήσει ότι πληρούνται οι προϋποθέσεις της παρ.3, οπότε δεν απαιτείται ανακοίνωση στα θιγόμενα πρόσωπα. Σε κάθε περίπτωση όμως, εάν η εποπτική αρχή κρίνει την απόφαση περί μη ανακοίνωσης αβάσιμη, δύναται να εξετάσει το ενδεχόμενο επιβολής κυρώσεων στο πλαίσιο των από τον Κανονισμό

[53] Ό.π. Γνώμη Ομάδας αρθ. 29, σελ.18.
[54] Ό.π. Γνώμη Ομάδας αρθ. 29, σελ.19.

προβλεπόμενων αρμοδιοτήτων και εξουσιών της.

Συνοψίζοντας το κεφάλαιο των υποχρεώσεων γνωστοποίησης/ανακοίνωσης των περιστατικών ασφαλείας και δεδομένου ότι το αρθ. 83 σε συνδυασμό με το αρθ. 53 παρ. 3 περ. θ, προβλέπει κυρώσεις από την μη ή την μη έγκαιρη γνωστοποίηση/ανακοίνωση περιστατικών ασφαλείας, θα πρέπει να σημειωθεί ότι η εποπτική αρχή έχει κατά κανόνα εξουσία αυτεπάγγελτης παρέμβασης για την διερεύνηση συμβάντων παραβίασης δεδομένων κατά την οποία θα πρέπει να εξακριβώνει «*κατά πόσον έχουν τεθεί σε εφαρμογή όλα τα κατάλληλα μέτρα τεχνολογικής προστασίας και οργανωτικά μέτρα για τον άμεσο εντοπισμό κάθε παραβίασης δεδομένων προσωπικού χαρακτήρα και την άμεση ενημέρωση της εποπτικής αρχής και του υποκειμένου των δεδομένων. Θα πρέπει επίσης να διαπιστώνει ότι η κοινοποίηση πραγματοποιήθηκε χωρίς αδικαιολόγητην καθυστέρηση, λαμβανομένων υπόψη ιδίως της φύσης και της σοβαρότητας της παραβίασης δεδομένων προσωπικού χαρακτήρα, καθώς και των συνεπειών και των δυσμενών αποτελεσμάτων της για το υποκείμενο των δεδομένων*[55]».

9. Εκτίμηση Αντικτύπου (αρθ. 35)

Το προηγούμενο νομικό καθεστώς της οδηγίας 95/46/ΕΚ προέβλεπε γενική υποχρέωση γνωστοποίησης της επεξεργασίας δεδομένων προσωπικού χαρακτήρα στις εποπτικές αρχές ήδη πριν από την εκτέλεση ενεργειών επεξεργασίας. Παρότι η υποχρέωση αυτή συνεπαγόταν διοικητικό και οικονομικό φόρτο, δεν προέβλεπε διαβαθμισμένους μηχανισμούς αυξημένης προστασίας για ειδικές κατηγορίες προσώπων ή δεδομένων με συνέπεια να μην συμβάλει αρκετά και αποτελεσματικά στην βελτίωση της προστασίας τους· ενόψει του GDPR καταργήθηκε και αντικαταστάθηκε με την υποχρέωση εκπόνησης εκτίμησης αντικτύπου, η οποία θα επικεντρώνεται σε εκείνους τους τύπους πράξεων επεξεργασίας που ενδέχεται να έχουν υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων λόγω της φύσης, του πεδίου εφαρμογής, του πλαισίου και των σκοπών τους. Ο υψηλός κίνδυνος της ενέργειας επεξεργασίας μπορεί να συνίσταται στην χρήση

[55] Προοίμιο, σημείωση 87.

νέων τεχνολογιών ή στον νέο τύπο επεξεργασίας για τον οποίο δεν έχει διενεργηθεί προηγουμένως εκτίμηση αντικτύπου ή όταν καθίσταται αναγκαία λόγω του χρόνου που έχει παρέλθει από την αρχική επεξεργασία.

Κατά τις επιταγές του GDPR, οι υπεύθυνοι επεξεργασίας οφείλουν να εφαρμόζουν ενδεδειγμένα μέτρα για να διασφαλίζουν την συμμόρφωσή τους και να είναι σε θέση και να την αποδεικνύουν, λαμβάνοντας υπόψη μεταξύ άλλων «τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων» (άρθρο 24 παράγραφος 1). Η υποχρέωση των υπευθύνων επεξεργασίας για την διενέργεια ΕΑ θα πρέπει να συνδέεται με την γενική τους υποχρέωση να διαχειρίζονται με ενδεδειγμένο τρόπο τους κινδύνους που ενέχει η επεξεργασία των δεδομένων προσωπικού χαρακτήρα[56]. Ως «κίνδυνος» νοείται μία υπόθεση εργασίας που περιγράφει ένα συμβάν ασφαλείας το οποίο έχει σχεδιαστεί και αναλυθεί βάσει κλίμακας πιθανότητας επέλευσης και σοβαρότητας συνεπειών. Περαιτέρω, ως «διαχείριση κινδύνου» νοούνται οι συντονισμένες δραστηριότητες και οι οργανωτικοί μηχανισμοί που έχει ενσωματώσει στις λειτουργίες του ένας οργανισμός προκειμένου να αποφύγει, να ελέγξει και να μετριάσει τις συνέπειες από την επέλευση ενός κινδύνου. Αρμόδιος και τελικός υπεύθυνος για την διασφάλιση της διενέργειας της ΕΑ είναι ο υπεύθυνος επεξεργασίας[57], ωστόσο πρέπει να ζητά τόσο την γνώμη του υπεύθυνου προστασίας δεδομένων (αρθ. 35 παρ.2), αλλά και κάθε αναγκαία συνδρομή και πληροφορίες από τον εκτελούντα την επεξεργασία (άρθρο 28 παρ. 3 στοιχείο στ).

Με γνώμονα την κινδυνοκεντρική προσέγγιση (risk-based approach) που διέπει τον GDPR, δεν απαιτείται η διενέργεια ΕΑ σε κάθε πράξη επεξεργασίας· αντιθέτως, απαιτείται μόνον όταν μία πράξη επεξεργασίας «*ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων*». Στην παράγραφο 3 του αρθ. 35 αναφέρονται ενδεικτικές περιπτώσεις κατά τις οποίες

[56] Πρέπει να επισημανθεί ότι για την διαχείριση των κινδύνων για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, απαιτείται η διαπίστωση, ανάλυση, εκτίμηση, αξιολόγηση, αντιμετώπιση των κινδύνων και η τακτική τους επανεξέταση. Οι υπεύθυνοι επεξεργασίας δεν μπορούν να απεκδύονται των ευθυνών τους μέσω της κάλυψης των κινδύνων με ασφαλιστικές συμβάσεις.

[57] Η ΕΑ μπορεί να πραγματοποιηθεί από άλλο πρόσωπο, εντός ή εκτός του οργανισμού, ωστόσο ο υπεύθυνος επεξεργασίας παραμένει ο τελικός υπεύθυνος για το εν λόγω καθήκον.

κρίνεται υποχρεωτική η εκπόνηση ΕΑ:

i. συστηματική και εκτενής αξιολόγηση προσωπικών πτυχών σχετικά με φυσικά πρόσωπα, η οποία βασίζεται σε αυτοματοποιημένη επεξεργασία, περιλαμβανομένης της κατάρτισης προφίλ, και στην οποία βασίζονται αποφάσεις που παράγουν έννομα αποτελέσματα σχετικά με το φυσικό πρόσωπο ή ομοίως επηρεάζουν σημαντικά το φυσικό πρόσωπο,

ii. μεγάλης κλίμακας επεξεργασία των ειδικών κατηγοριών δεδομένων που αναφέρονται στο άρθρο 9 παράγραφος 1 ή δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα που αναφέρονται στο άρθρο 10

iii. συστηματική παρακολούθηση δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα[58].

Και συμπληρώνει η παρ. 4 του άρθρου με την πρόβλεψη ότι η εποπτική αρχή δύναται να καταρτίζει κατάλογο με πράξεις επεξεργασίας οι οποίες προϋποθέτουν διενέργεια ΕΑ[59]. Σύμφωνα με τις κατευθυντήριες οδηγίες της Ομάδας 29, «*οσάκις δεν είναι σαφές κατά πόσον απαιτείται η διενέργεια ΕΑ, συνιστάται να διενεργείται ΕΑΠΔ, καθώς σε κάθε περίπτωση αποτελεί χρήσιμο εργαλείο για τους υπεύθυνους επεξεργασίας προκειμένου να συμμορφώνονται με την νομοθεσία για την προστασία των δεδομένων*». Επιπλέον, η Ομάδα 29 υποστηρίζει ότι «*αυτό καθαυτό το γεγονός της μη πλήρωσης των όρων που ενεργοποιούν την υποχρέωση διενέργειας ΕΑΠΔ δεν μειώνει, εντούτοις, την γενική υποχρέωση των υπεύθυνων επεξεργασίας να εφαρμόζουν μέτρα για την ενδεδειγμένη διαχείριση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων· στην πράξη, αυτό σημαίνει ότι οι υπεύθυνοι επεξεργασίας πρέπει να αξιολογούν συνεχώς τους*

[58] Προοίμιο, αιτιολογική σκέψη 93: *Εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων απαιτείται επίσης για την παρακολούθηση δημόσια προσπελάσιμων χώρων σε μεγάλη κλίμακα, ιδίως όταν χρησιμοποιούνται οπτικοηλεκτρονικές συσκευές ή για οποιεσδήποτε άλλες εργασίες όποτε η αρμόδια εποπτική αρχή θεωρεί ότι η επεξεργασία ενδέχεται να έχει ως αποτέλεσμα υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων, ιδίως επειδή εμποδίζει τα υποκείμενα των δεδομένων να ασκήσουν κάποιο δικαίωμα ή να χρησιμοποιήσουν μία υπηρεσία ή σύμβαση ή επειδή πραγματοποιούνται συστηματικά σε μεγάλη κλίμακα*. Βλ. και κατευθυντήριες για DPO σχετικά με ην μεγάλη κλίμακα».

[59] Η ΑΠΔΠΧ κατήρτησε τον από 16-10-2018 κατάλογο με τα είδη των πράξεων επεξεργασίας που υπόκεινται στην απαίτηση για διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων σύμφωνα με το άρθρο 35 παρ. 4 του ΓΚΠΔ. Βλ. αναλυτικά, http://www.dpa.gr/portal/page?_pageid=33,223264&_dad=portal&_schema=PORTAL

κινδύνους που απορρέουν από τις δραστηριότητες επεξεργασίας τους, για να εξακριβώνουν πότε ένα είδος επεξεργασίας ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων».

Σύμφωνα με την παράγραφο 7 η εκτίμηση θα πρέπει να έχει ως ελάχιστο περιεχόμενο:

α. συστηματική περιγραφή των προβλεπόμενων πράξεων επεξεργασίας και των σκοπών της επεξεργασίας, περιλαμβανομένου, κατά περίπτωση, του έννομου συμφέροντος που επιδιώκει ο υπεύθυνος επεξεργασίας,
β. εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας σε συνάρτηση με τους σκοπούς,
γ. εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων που αναφέρονται στην παράγραφο 1
δ. τα προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων, περιλαμβανομένων των εγγυήσεων, των μέτρων και μηχανισμών ασφάλειας, ώστε να διασφαλίζεται η προστασία των δεδομένων προσωπικού χαρακτήρα και να αποδεικνύεται η συμμόρφωση προς τον παρόντα κανονισμό, λαμβάνοντας υπόψη τα δικαιώματα και τα έννομα συμφέροντα των υποκειμένων των δεδομένων και άλλων ενδιαφερόμενων προσώπων.

Τόσο ο ίδιος ο Κανονισμός στις αιτιολογικές του σκέψεις όσο και η ομάδα 29 κρίνουν ότι σε αρκετές περιπτώσεις μία επιμέρους εκτίμηση αντικτύπου θα μπορούσε να αποτελέσει το πρότυπο για την εκτίμηση περισσότερων ομοειδών ως προς την φύση, το πεδίο εφαρμογής, τον σκοπό και τους κινδύνους ενεργειών επεξεργασίας που εκτελούνται από διαφορετικούς οργανισμούς οι οποίοι είτε δραστηριοποιούνται στον ίδιο τομέα είτε χρησιμοποιούν κοινές εφαρμογές, κ.ο.κ. *«Πράγματι, σκοπός της ΕΑ είναι η συστηματική μελέτην νέων καταστάσεων που θα μπορούσαν να επιφέρουν υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, και δεν απαιτείται η διενέργεια ΕΑΠΔ σε περιπτώσεις που έχουν ήδη εξεταστεί· αυτή η προσέγγιση θα μπορούσε να εφαρμοστεί σε περιπτώσεις όπου χρησιμοποιούνται παρόμοιες τεχνολογίες για την συλλογή*

ομοειδών δεδομένων για τον ίδιο σκοπό[60]». Στις περιπτώσεις αυτές, θα πρέπει να δημοσιοποιείται ή να διαμοιράζεται η πρότυπη ΕΑ, και στην συνέχεια έκαστος υπεύθυνος επεξεργασίας που θα την υλοποιεί να αιτιολογεί την αναγωγή σε αυτήν και να υιοθετεί τα προτεινόμενα μέτρα.

Η αρχική ΕΑ θα πρέπει να διενεργείται πριν από την επεξεργασία, καθώς και μία πρότυπη ΕΑ θα πρέπει να υιοθετείται πριν από την επεξεργασία· τούτο συνάδει με τις αρχές της εξ ορισμού και της εκ σχεδιασμού προστασίας των δεδομένων. Όλες οι απαιτήσεις που θέτει ο GDPR στους υπεύθυνους επεξεργασίας, είτε ως υποχρεώσεις είτε ως χρήσιμα προαιρετικά εργαλεία συγκλίνουν σε έναν μοναδικό στόχο, την απόδειξη της συμμόρφωσής τους, μέσα από την οποία εξασφαλίζεται και ο απώτερος και κυρίαρχος σκοπός του Κανονισμού, η προστασία των προσωπικών δεδομένων. Συγκεκριμένα, οι κώδικες δεοντολογίας, οι πιστοποιήσεις, τα σήματα και οι σφραγίδες, καθώς και οι εταιρικοί δεσμευτικοί κανόνες, αν και προαιρετικά εργαλεία, μπορούν να παράσχουν ένα ευρύ, γενικό αλλά και σταθερό και ασφαλές για την επιχείρηση πλαίσιο για τον σχεδιασμό και την υλοποίηση μία ς ΕΑ. Πρέπει να σημειωθεί ακόμη, ότι και ο GDPR στο προοίμιό του αλλά και ο ENISA όσον αφορά την διαχείριση του κινδύνου στον ειδικότερο τομέα των προσωπικών δεδομένων παραπέμπουν στις διεθνώς καθορισμένες διαδικασίες της διαχείρισης κινδύνων (λ.χ. ISO 31000[61], 27000[62]).

Ως ορθή πρακτική, μία ΕΑ θα πρέπει να επανεξετάζεται και να επαναξιολογείται τακτικά (αρθ. 35 παρ. 11) και ειδικότερα, σε περίπτωση μεταβολής των κινδύνων που συνεπάγονται οι πράξεις επεξεργασίας[63], για παράδειγμα επειδή

[60] Σελ. 8, κατευθυντηρίες γραμμές για ΕΑΠΔ: Για παράδειγμα, ένα σύνολο αρχών της τοπικής αυτοδιοίκησης που εγκαθιστούν παρόμοια συστήματα κλειστού κυκλώματος τηλεόρασης (CCTV) θα μπορούσαν να διενεργήσουν μία μόνο ΕΑΠΔ που να καλύπτει την επεξεργασία από τους εν λόγω ξεχωριστούς υπεύθυνους επεξεργασίας, ή ένας σιδηροδρομικός φορέας (ένας μόνο υπεύθυνος επεξεργασίας) θα μπορούσε να καλύπτει την βιντεοεπιτήρηση σε όλους τους σιδηροδρομικούς σταθμούς της αρμοδιότητάς του με μία μόνο ΕΑΠΔ.

[61] Επικοινωνία και διαβούλευση, ορισμός του πλαισίου, εκτίμηση κινδύνου, αντιμετώπιση κινδύνων, παρακολούθηση και επανεξέταση (βλέπε όρους και ορισμούς και πίνακα περιεχομένων, στην προεπισκόπηση του ISO 31000: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en).

[62] Βλ. παρακάτω σημείωση 91.

[63] Κατευθυντήριες γραμμές για ΕΑΠΔ, υποσημείωση 22: Ως προς το πλαίσιο, τα δεδομένα που έχουν συλλεχθεί, τους σκοπούς, την λειτουργία, τα δεδομένα προσωπικού χαρακτήρα που τίθενται σε επεξεργασία, τους αποδέκτες, τους συνδυασμούς δεδομένων, τους κινδύνους (τα υποστηρικτικά περιουσιακά στοιχεία, τις πηγές των κινδύνων, τις πιθανές επιπτώσεις, τους επαπειλούμενους κινδύνους κ.ο.κ.), τα μέτρα ασφαλείας και τις διεθνείς διαβιβάσεις.

χρησιμοποιείται πλέον μία νέα τεχνολογία ή επειδή τα δεδομένα προσωπικού χαρακτήρα χρησιμοποιούνται για διαφορετικό σκοπό. Αντίστοιχα, η εξέλιξη της τεχνολογίας ενδέχεται να μειώσει τον κίνδυνο και να μην απαιτείται πλέον για ένα είδος επεξεργασίας εκτίμηση του κινδύνου, γλιτώνοντας τον υπεύθυνο από το διοικητικό και το οικονομικό βάρος που αυτή συνεπάγεται.

Για την ασφάλεια δικαίου και την καθοδήγηση των υπευθύνων επεξεργασίας, η Ομάδα του άρθρου 29 έχει καταρτίσει μία λίστα εννέα κριτηρίων προκειμένου να διευκολύνει τους υπεύθυνους επεξεργασίας και να τους παρέχει ένα πιο συνεκτικό σύνολο πράξεων επεξεργασίας που απαιτούν την διενέργεια ΕΑ. Η λίστα περιλαμβάνεται στο κείμενο των κατευθυντήριων γραμμών για την εκτίμηση αντικτύπου και παρατίθεται στο τέλος της παρούσας εργασίας ως Παράρτημα Ι (σελ. 124).

Ακόμα, πρέπει να σημειωθεί ότι η εκτίμηση αντικτύπου κατά τον GDPR αποτελεί ένα εργαλείο διαχείρισης των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων και, επομένως, έχει ως στόχευση την προστασία της ιδιωτικότητας των φυσικών προσώπων· αντιστοίχως, σε άλλους τομείς η διαχείριση των κινδύνων (π.χ. ασφάλεια πληροφοριών) επικεντρώνεται στην οργανωτική διάρθρωση. Ο GDPR παρέχει ευελιξία στους υπεύθυνους επεξεργασίας για τον καθορισμό της δομής και της μορφής της ΕΑ, παραπέμποντας μάλιστα και στις καθιερωμένες τεχνικές διαχείρισης κινδύνου, καθώς σημασία έχει να γίνει μία πραγματική αξιολόγηση των κινδύνων ώστε να μπορέσουν οι υπεύθυνοι επεξεργασίας να λάβουν τα ενδεδειγμένα μέτρα για την αντιμετώπισή τους. Συνεπώς, ένας οργανισμός θα μπορούσε να χρησιμοποιήσει διάφορες μεθοδολογίες καθώς και συνδυασμό αυτών ώστε να υλοποιήσει το δικό του σχέδιο ασφαλείας ανάλογα με τις ανάγκες και τις δυνατότητές του, θα πρέπει όμως να έχει ως οδηγό τα κριτήρια που έχει αναπτύξει η Ομάδα 29 για να προσδιορίσει σε πρακτικό επίπεδο τις βασικές απαιτήσεις του GDPR ώστε να μπορεί να επιτύχει και την συμμόρφωσή του με αυτές. Τα κριτήρια αυτά παρατίθενται στο Παράρτημα ΙΙ (σελ. 127).

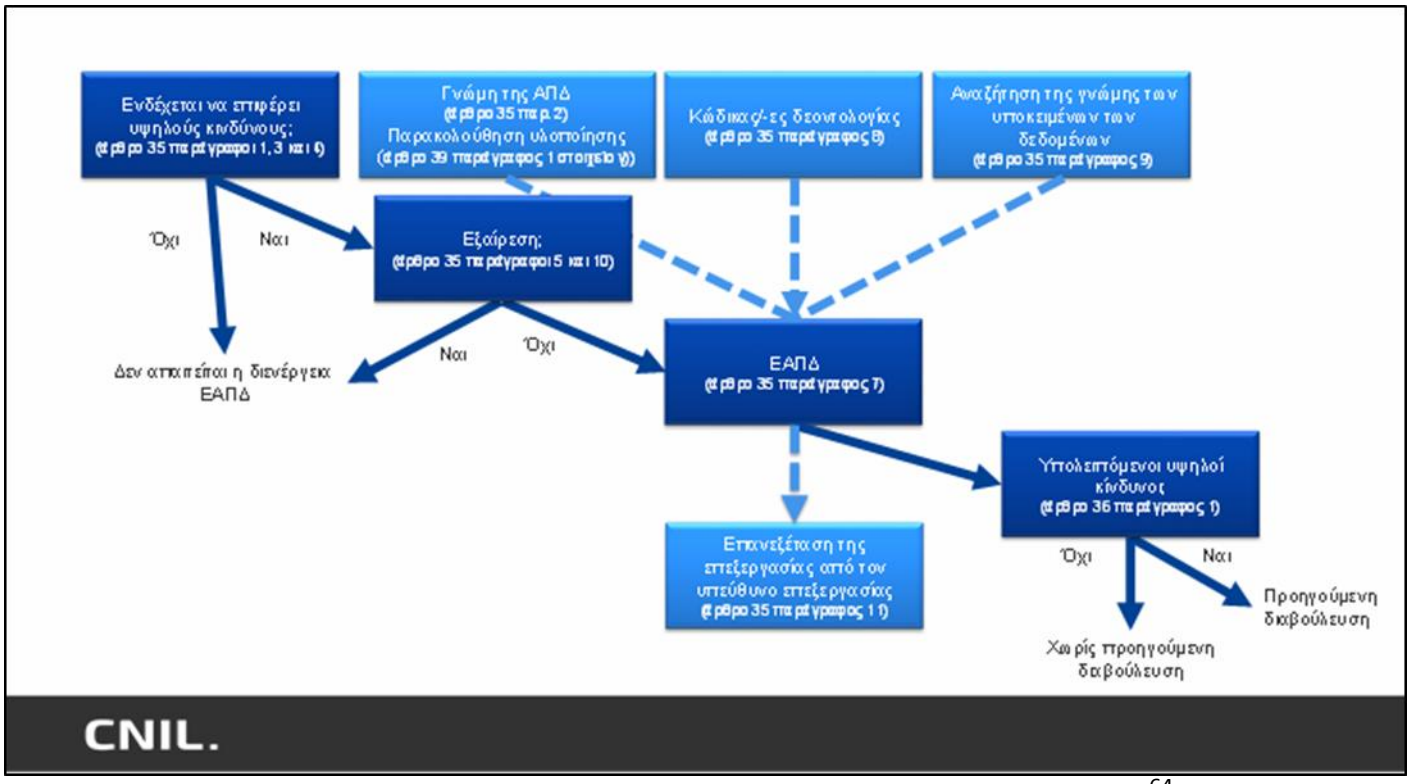
Η Ομάδα 29 θεωρεί ότι η ΕΑΠΔ δεν απαιτείται στις ακόλουθες περιπτώσεις:

- όταν η επεξεργασία δεν «ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων» (άρθρο 35 παράγραφος 1)·

- όταν η φύση, το πεδίο εφαρμογής, το πλαίσιο και οι σκοποί της επεξεργασίας παρουσιάζουν πολλές ομοιότητες με την επεξεργασία για την οποία έχει διενεργηθεί ΕΑΠΔ. Στις εν λόγω περιπτώσεις, μπορούν να χρησιμοποιούνται τα αποτελέσματα της ΕΑΠΔ στις παρόμοιες επεξεργασίες (άρθρο 35 παράγραφος 119)·

  - όταν οι πράξεις επεξεργασίας έχουν ελεγχθεί από εποπτική αρχή πριν από τον Μάιο του 2018 υπό συγκεκριμένους όρους που παραμένουν αμετάβλητοι.
  - όταν η πράξη επεξεργασίας, δυνάμει του άρθρου 6 παράγραφος 1 στοιχείο γ) ή ε), έχει νομική βάση στο δίκαιο της Ένωσης ή στο δίκαιο κράτους μέλους, όταν το εν λόγω δίκαιο ρυθμίζει την συγκεκριμένη πράξη επεξεργασίας και έχει διενεργηθεί ήδη ΕΑΠΔ στο πλαίσιο της θέσπισης της εν λόγω νομικής βάσης (άρθρο 35 παρ. 10), εκτός αν τα κράτη μέλη κρίνουν απαραίτητη την διενέργεια της εν λόγω ΕΑΠΔ πριν από τις δραστηριότητες επεξεργασίας·
  - όταν η επεξεργασία περιλαμβάνεται στον προαιρετικό κατάλογο (που καταρτίζεται από την εποπτική αρχή) των πράξεων επεξεργασίας για τις οποίες δεν απαιτείται η διενέργεια ΕΑΠΔ (άρθρο 35 παρ. 5).

Τέλος, σύμφωνα με το άρθρο 36 και την αιτιολογική σκέψη 92 του Κανονισμού, εάν η εκτίμηση αντικτύπου υποδεικνύει ότι η επεξεργασία προσωπικών δεδομένων, χωρίς μέτρα και μηχανισμούς ασφάλειας, θα είχε ως αποτέλεσμα υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων και ο υπεύθυνος επεξεργασίας θεωρεί ότι ο κίνδυνος δεν είναι δυνατόν να μετριαστεί με εύλογα μέτρα όσον αφορά την διαθέσιμη τεχνολογία και το κόστος εφαρμογής, θα πρέπει να διενεργείται διαβούλευση με την εποπτική αρχή πριν από την έναρξη των δραστηριοτήτων επεξεργασίας, η οποία μπορεί να παρέχει γραπτές συμβουλές και κατευθύνσεις για λήψη μέτρων δυνάμει και των εξουσιών της βάσει του αρθ. 58.



Γράφημα της Γαλλικής ΑΠΔΠΧ σχετικά με την διενέργεια Εκτίμησης Αντικτύπου[64]

10. Ορισμός DPO (αρθ. 37)

Με τον GDPR εισήχθη στο κανονιστικό πλαίσιο της προστασίας της ιδιωτικότητας και ο θεσμός του Υπεύθυνου Προστασίας Δεδομένων (DPO), ενός εξειδικευμένου επαγγελματία με ρόλο αφ' ενός την διευκόλυνση της συμμόρφωσης [και την απόδειξη αυτής] του υπευθύνου επεξεργασίας και του εκτελούντος την επεξεργασία με τις διατάξεις του Γενικού Κανονισμού για την Προστασία Δεδομένων, και αφ' ετέρου την εκπροσώπηση του οργανισμού είτε στην εποπτική-ελεγκτική αρχή είτε στα υποκείμενα των δεδομένων· ως ιδέα είχε διατυπωθεί από την Ομάδα 29 ήδη από το 2010 στα πλαίσια της αρχής λογοδοσίας .

Έτσι, βάσει του άρθρου 37, οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία υποχρεούνται, υπό προϋποθέσεις, να ορίσουν υπεύθυνο προστασίας δεδομένων (Data Protection Officer - DPO) και συγκεκριμένα ο ορισμός DPO είναι

[64] Πηγή: ΟΜΑΔΑ ΕΡΓΑΣΙΑΣ ΤΟΥ ΑΡΘΡΟΥ 29 ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ, *Κατευθυντήριες γραμμές για την εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) και καθορισμός του κατά πόσον η επεξεργασία «ενδέχεται να επιφέρει υψηλό κίνδυνο» για τους σκοπούς του κανονισμού 2016/679*, WP 248 αναθ. 01, 4/10/2017.

υποχρεωτικός στις κάτωθι περιπτώσεις:

α) όταν η επεξεργασία διενεργείται από δημόσια αρχή ή δημόσιο φορέα·

β) όταν οι βασικές δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν πράξεις επεξεργασίας οι οποίες απαιτούν τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε μεγάλη κλίμακα·

γ) όταν οι βασικές δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων ή δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα.

Εκτός από τις περιπτώσεις στις οποίες καταφανώς δεν συντρέχουν οι προϋποθέσεις που θέτει ο Κανονισμός για τον ορισμό DPO, οι υπεύθυνοι επεξεργασίας και οι εκτελούντες καλό θα ήταν να καταγράφουν την εσωτερική εκτίμηση που διενήργησαν για να καταλήξουν στο συμπέρασμα εάν πρέπει ή όχι να ορίσουν DPO, ώστε στα πλαίσια της αρχής της λογοδοσίας να είναι σε θέση να αποδείξουν ότι αξιολόγησαν τους σχετικούς παράγοντες. Σε κάθε περίπτωση, πάντως, οι οργανισμοί μπορούν εθελοντικά να ορίσουν DPO, πέραν των ρητώς προβλεπόμενων στον Κανονισμό περιπτώσεων, τόσο για την καλύτερη διαχείριση των διαδικασιών τους όσο και χάριν ανταγωνιστικού πλεονεκτήματος. Μάλιστα η Ομάδα 29 ενθαρρύνει τέτοιες πρωτοβουλίες καθώς εδραιώνουν και διαδίδουν την ουσία και την κουλτούρα της προστασίας της ιδιωτικότητας.

Πρέπει να σημειωθεί ότι ο DPO, αν και αποτελεί σημαντική συνιστώσα του νέου νομικού πλαισίου, προκύπτει σαφώς από τις διατάξεις του Κανονισμού ότι δεν φέρει προσωπική ευθύνη σε περίπτωση μη συμμόρφωσης του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία. Η συμμόρφωση με τους κανόνες προστασίας των δεδομένων καθώς και η απόδειξή της είναι ευθύνη του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία και ο DPO δρα συμβουλευτικά ως εξειδικευμένος επαγγελματίας.

i. Επεξήγηση των όρων για τον προσδιορισμό της αναγκαιότητας ορισμού DPO

α. «*βασικές δραστηριότητες*»

Οι «βασικές δραστηριότητες» του υπεύθυνου ή του εκτελούντος την επεξεργασία συνίστανται στις αναγκαίες και καίριες ενέργειες για την επίτευξη του σκοπού και των στόχων του οργανισμού ή πράξεις που άπτονται άμεσα του κύριου τομέα δραστηριοποίησης του οργανισμού· σε αυτές δεν συμπεριλαμβάνονται ενέργειες υποστηρικτικές ή παρεπόμενες της λειτουργίας του οργανισμού.

Για παράδειγμα, η βασική δραστηριότητα ενός νοσοκομείου είναι η παροχή υγειονομικής περίθαλψης η οποία μπορεί να εκτελεστεί με ασφαλή και αποτελεσματικό τρόπο μόνο με την επεξεργασία των ιατρικών δεδομένων που περιέχονται στους φακέλους των ασθενών. Η επεξεργασία των εν λόγω δεδομένων θα πρέπει να θεωρείται, επομένως, ως μία από τις βασικές δραστηριότητες κάθε νοσοκομείου και κατά συνέπεια, τα νοσοκομεία οφείλουν να ορίζουν υπεύθυνο προστασίας δεδομένων. Άλλο παράδειγμα είναι οι ιδιωτικές εταιρείες ασφαλείας που αναλαμβάνουν την φύλαξη ιδιωτικών εμπορικών κέντρων και δημόσιων χώρων (με συστήματα βιντεοεπιτήρησης), η οποία ως δραστηριότητα είναι άρρηκτα συνδεδεμένη με την επεξεργασία δεδομένων προσωπικού χαρακτήρα· συνεπώς και οφείλουν να ορίσουν υπεύθυνο προστασίας δεδομένων. Αντιθέτως, ορισμένες δραστηριότητες, κοινές για όλους τους οργανισμούς, όπως, π.χ. η καταβολή των μισθών στους υπαλλήλους ή η ανάπτυξη δραστηριοτήτων υποστήριξης ΤΠ, είναι μεν αναγκαίες, αλλά είναι παρεπόμενες της κύριας επιχειρηματικής δραστηριότητας και γι' αυτές δεν απαιτείται η συνδρομή DPO[65].

β. «μεγάλη κλίμακα»

Συνδυάζοντας την αιτιολογική σκέψη 91[66] και τις κατευθύνσεις της Ομάδας

[65] Ομάδα άρθρου 29, Κατευθυντήριες γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων, σελ. 9.

[66] Ο.π., Κατευθυντήριες γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων, σελ. 10, υποσημ. 14: *Σύμφωνα με την εν λόγω αιτιολογική σκέψη, στην έννοια της «μεγάλης κλίμακας» εμπίπτουν συγκεκριμένα «πράξεις επεξεργασίας μεγάλης κλίμακας που στοχεύουν στην επεξεργασία σημαντικής ποσότητας δεδομένων προσωπικού χαρακτήρα σε περιφερειακό, εθνικό ή υπερεθνικό*

29,προκειμένου να προσδιοριστεί ανά περίπτωση ο όρος «μεγάλη κλίμακα» μπορούν να ληφθούν υπόψη οι ακόλουθοι παράγοντες:

- ο αριθμός των εμπλεκόμενων υποκειμένων των δεδομένων, είτε ως συγκεκριμένος αριθμός είτε ως ποσοστό επί του συναφούς πληθυσμού,
- ο όγκος των δεδομένων και/ή το εύρος των διαφόρων στοιχείων δεδομένων που υφίστανται επεξεργασία,
- η διάρκεια ή ο μόνιμος χαρακτήρας της δραστηριότητας επεξεργασίας δεδομένων,
- η γεωγραφική έκταση της δραστηριότητας επεξεργασίας.

γ. «τακτική και συστηματική παρακολούθηση»

Συνδυάζοντας την αιτιολογική σκέψη 24[67] με την ερμηνεία της Ομάδας 29 η έννοια της «*τακτικής και συστηματικής παρακολούθησης*» αποκτά το εξής περιεχόμενο: περιλαμβάνει κάθε μορφή παρακολούθησης της συμπεριφοράς των υποκειμένων τόσο στο διαδίκτυο όσο και με άλλα αυτοματοποιημένα μέσα καθώς και την κατάρτιση προφίλ, μεταξύ άλλων και για σκοπούς διαφήμισης και προώθησης κάθε είδους υπηρεσιών και προϊόντων.

επίπεδο, οι οποίες θα μπορούσαν να επηρεάσουν μεγάλο αριθμό υποκειμένων των δεδομένων και οι οποίες είναι πιθανόν να έχουν ως αποτέλεσμα υψηλό κίνδυνο». Από την άλλη πλευρά, η αιτιολογική σκέψη προβλέπει ρητά ότι «η επεξεργασία δεδομένων προσωπικού χαρακτήρα δεν θα πρέπει να θεωρείται ότι είναι μεγάλης κλίμακας, εάν η επεξεργασία αφορά δεδομένα προσωπικού χαρακτήρα ασθενών ή πελατών ιδιώτην ιατρού, άλλου επαγγελματία του τομέα της υγείας ή δικηγόρου». Είναι σημαντικό να ληφθεί υπόψη ότι, ενώ στην αιτιολογική σκέψη παρατίθενται παραδείγματα που αφορούν τα δύο άκρα (επεξεργασία από ιδιώτην ιατρό έναντι επεξεργασίας δεδομένων σε εθνικό επίπεδο ή σε ολόκληρη την Ευρώπη), μεταξύ των δύο αυτών άκρων, υπάρχει μία μεγάλη γκρίζα ζώνη. Θα πρέπει να ληφθεί υπόψη επιπλέον ότι η συγκεκριμένη αιτιολογική σκέψη αναφέρεται στις εκτιμήσεις αντικτύπου σχετικά με την προστασία των δεδομένων. Αυτό σημαίνει ότι ορισμένα στοιχεία μπορεί να αφορούν συγκεκριμένα το εν λόγω πλαίσιο και δεν ισχύουν απαραιτήτως κατά τον ίδιο ακριβώς τρόπο για τον ορισμό υπευθύνου προστασίας δεδομένων.

[67] *«Για τον καθορισμό του κατά πόσον μία δραστηριότητα επεξεργασίας μπορεί να θεωρηθεί ότι παρακολουθεί την συμπεριφορά υποκειμένου των δεδομένων, θα πρέπει να εξακριβωθεί κατά πόσον φυσικά πρόσωπα παρακολουθούνται στο Διαδίκτυο, συμπεριλαμβανομένης της δυνητικής μετέπειτα χρήσης τεχνικών επεξεργασίας δεδομένων προσωπικού χαρακτήρα οι οποίες συνίστανται στην διαμόρφωση του "προφίλ" ενός φυσικού προσώπου, ιδίως με σκοπό να ληφθούν αποφάσεις που το αφορούν ή να αναλυθούν ή να προβλεφθούν οι προσωπικές προτιμήσεις, οι συμπεριφορές και οι νοοτροπίες του*». Η εν λόγω αιτιολογική σκέψη αναφέρεται στην εξωεδαφική εφαρμογή του ΓΚΠΔ, και επιπλέον η διατύπωσή της διαφέρει από αυτήν της «τακτικής και συστηματικής παρακολούθησης», γι’ αυτό μόνο συνδυαστικά χρησιμοποιείται στον προσδιορισμό του περιεχομένου της τελευταίας.

Η ομάδα του άρθρου 29 δίνει κάποια παραδείγματα δραστηριοτήτων που συνιστούν ενδεχομένως τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων για την καλύτερη και πληρέστερη κατανόηση του όρου: «λειτουργία δικτύου τηλεπικοινωνιών· παροχή υπηρεσιών τηλεπικοινωνιών· επαναστόχευση μηνυμάτων ηλεκτρονικού ταχυδρομείου· δραστηριότητες μάρκετινγκ βάσει δεδομένων· διαμόρφωση προφίλ και βαθμολόγηση για σκοπούς εκτίμησης κινδύνου (π.χ. για σκοπούς βαθμολόγησης πιστοληπτικής ικανότητας, προσδιορισμού ασφαλίστρων, καταπολέμησης της απάτης, εντοπισμού πρακτικών νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες)· εντοπισμός θέσης, για παράδειγμα, μέσω εφαρμογών για κινητά τηλέφωνα· προγράμματα επιβράβευσης αφοσιωμένων πελατών· συμπεριφορική διαφήμιση· παρακολούθηση δεδομένων σχετικά με την ευεξία, την φυσική κατάσταση και την υγεία μέσω φορέσιμων συσκευών· τηλεόραση κλειστού κυκλώματος· συνδεδεμένες συσκευές, π.χ. έξυπνες συσκευές μέτρησης, έξυπνα αυτοκίνητα, οικιακός αυτοματισμός κ.λπ»[68].

Στην παράγραφο 5 του άρθρου 37 προβλέπεται ότι ο DPO «*διορίζεται βάσει επαγγελματικών προσόντων και ιδίως βάσει της εμπειρογνωσίας που διαθέτει στον τομέα του δικαίου και των πρακτικών περί προστασίας δεδομένων, καθώς και βάσει της ικανότητας εκπλήρωσης των καθηκόντων που αναφέρονται στο άρθρο 39*»[69]. Αν και τα επιμέρους στοιχεία που πρέπει να προσέξει ο υπεύθυνος ή ο εκτελών την επεξεργασία όταν προσλαμβάνει έναν DPO δεν καθορίζονται στον Κανονισμό, αυτά προκύπτουν από τις ίδιες τις ανάγκες και τις δραστηριότητες του οργανισμού. Ειδικότερα, οι απαιτήσεις ως προς τα επαγγελματικά προσόντα και την εμπειρογνωσία ενός DPO πέραν από την γνώση του ευρωπαϊκού και εθνικού δικαίου προστασίας δεδομένων και της πρακτικής εφαρμογής του, είναι ανάλογες με την πολυπλοκότητα των πράξεων επεξεργασίας, το είδος των δεδομένων

[68] Ο.π., Κατευθυντήριες γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων, σελ. 12.

[69] Αιτιολογική σκέψη 97, Προοίμιο: *Στον ιδιωτικό τομέα […] το αναγκαίο επίπεδο εμπειρίας θα πρέπει να καθορίζεται ειδικότερα ανάλογα με τις πράξεις επεξεργασίας δεδομένων που διενεργούνται και από την προστασία την οποία απαιτούν τα δεδομένα προσωπικού χαρακτήρα που επεξεργάζονται ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία. Οι εν λόγω υπεύθυνοι προστασίας δεδομένων, ανεξάρτητα από το κατά πόσον είναι υπάλληλοι του υπευθύνου επεξεργασίας, θα πρέπει να είναι σε θέση να εκτελούν τις υποχρεώσεις και τα καθήκοντά τους με ανεξάρτητο τρόπο.*

(ευαίσθητα-απλά) καθώς και του όγκου αυτών[70]. Για παράδειγμα, εάν ένας οργανισμός διαβιβάζει συστηματικά προσωπικά δεδομένα εκτός Ευρωπαϊκής Ένωσης ο DPO θα πρέπει να έχει εμπειρία στο συγκεκριμένο νομικό πλαίσιο και τις πιθανές πρακτικές εμπλοκές που ενδέχεται να προκύψουν· αντίστοιχα, για έναν οργανισμό που δεν προβαίνει σε διαβιβάσεις εκτός Ε.Ε. δεν είναι ιδιαίτερα χρήσιμη η εν λόγω εμπειρογνωσία.

Η Ομάδα 29 ερμηνεύει την επιταγή του Κανονισμού για «ικανότητα εκπλήρωσης των καθηκόντων» ως προς τον DPO με τις προσωπικές ιδιότητες της ακεραιότητας και του επαγγελματισμού και επισημαίνει ότι «*ο υπεύθυνος προστασίας δεδομένων θα πρέπει να έχει καλή γνώση των πράξεων επεξεργασίας που διενεργούνται, καθώς και των συστημάτων πληροφορικής, και των αναγκών του υπευθύνου επεξεργασίας σε επίπεδο ασφάλειας και προστασίας των δεδομένων*». Αυτονόητο είναι ότι ο DPO ως θεσμοφύλακας των πρακτικών προστασίας της ιδιωτικότητας χάρις στον συμβουλευτικό του ρόλο θα πρέπει να αποβλέπει στην μέγιστη δυνατή συμμόρφωση με τον GDPR με την υιοθέτηση και πραγμάτωση των αρχών του και στην ανάπτυξη νοοτροπίας προστασίας των υποκειμένων των δεδομένων.

ii. Ειδικότερα θέματα σχετικά με τον DPO

α. Θέση και καθήκοντα

Τα άρθρα 38 και 39 του GDPR υποδεικνύουν το εύρος των καθηκόντων και τα πεδία της συμβολής του DPO· ήδη από την 1η παράγραφο του αρθ. 38 με την φράση «*ο υπεύθυνος προστασίας δεδομένων συμμετέχει δεόντως και εγκαίρως, σε όλα τα ζητήματα τα οποία σχετίζονται με την προστασία δεδομένων προσωπικού χαρακτήρα*» διαφαίνεται ο καίριος και ευρύς ρόλος που του αναθέτει ο Κανονισμός. Ειδικότερα, στην αιτιολογική σκέψη 97 επισημαίνεται ότι ο DPO *«θα πρέπει να παρέχει συνδρομή στον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία κατά την παρακολούθηση της εσωτερικής συμμόρφωσης προς τον παρόντα κανονισμό»*· αντιστοίχως και ο υπεύθυνος επεξεργασίας θα πρέπει να μεριμνά για

[70] Βλ. περισσότερα, Ομάδα άρθρου 29, *Κατευθυντήριες γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων*, σελ. 16.

την συμμετοχή του DPO και την διαβούλευση μαζί του, καθώς και με τα αντίστοιχα τμήματα, για όλα τα σχετιζόμενα με την ιδιωτικότητα ζητήματα ήδη από τον σχεδιασμό, αλλά και στις ήδη υπάρχουσες διαδικασίες επεξεργασίας δεδομένων· θα πρέπει να ενημερώνεται έγκαιρα και άμεσα για κάθε θέμα που άπτεται των προσωπικών δεδομένων, να ζητείται η γνώμη του και να δικαιολογείται τυχόν απόκλιση από αυτήν . Πιο συγκεκριμένα τα καθήκοντα του Υπευθύνου Προστασίας ορίζονται στο άρθρο 39 ως εξής:

- ενημέρωση και παροχή συμβουλών στον υπεύθυνο επεξεργασίας ή στον εκτελούντα την επεξεργασία και τους υπαλλήλους που επεξεργάζονται για τις υποχρεώσεις τους που απορρέουν από τον Κανονισμό και από άλλες διατάξεις,
- παρακολούθηση της συμμόρφωσης με τον Κανονισμό και άλλες διατάξεις σχετικά με την προστασία δεδομένων και με τις πολιτικές του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία σε σχέση με την προστασία των δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων της ανάθεσης αρμοδιοτήτων, της ευαισθητοποίησης και της κατάρτισης των υπαλλήλων που συμμετέχουν στις πράξεις επεξεργασίας, και των σχετικών ελέγχων,
- παροχή συμβουλών, όταν ζητείται, όσον αφορά την εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων και παρακολούθηση της υλοποίησή της σύμφωνα με το άρθρο 35[71],

[71] Ομάδα άρθρου 29, *ΠΑΡΑΡΤΗΜΑ - ΚΑΤΕΥΘΥΝΤΗΡΙΕΣ ΓΡΑΜΜΕΣ ΣΧΕΤΙΚΑ ΜΕ ΤΟΥΣ ΥΠΕΥΘΥΝΟΥΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ: ΤΙ ΠΡΕΠΕΙ ΝΑ ΓΝΩΡΙΖΕΤΕ*, Κατευθυντήριες γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων, 5-4-2017: «*Όσον αφορά την εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων, ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία ζητεί την γνώμη του υπευθύνου προστασίας δεδομένων για ζητήματα όπως, ενδεικτικά, τα ακόλουθα: • εάν πρέπει ή όχι να διενεργήσει εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων • ποια μεθοδολογία πρέπει να ακολουθήσει κατά την διενέργεια της εκτίμησης αντικτύπου σχετικά με την προστασία των δεδομένων, • εάν πρέπει να διενεργήσει την εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων εσωτερικά ή να την αναθέσει σε εξωτερικό συνεργάτη, • τι εγγυήσεις (περιλαμβανομένων των τεχνικών και οργανωτικών μέτρων) πρέπει να εφαρμόσει προκειμένου να μετριαστούν οι κίνδυνοι για τα δικαιώματα και τα συμφέροντα των υποκειμένων των δεδομένων, • εάν διενεργήθηκε σωστά ή όχι η εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων και εάν τα συμπεράσματά της (σχετικά με το εάν θα δοθεί ή όχι συνέχεια στην επεξεργασία και τι εγγυήσεις θα εφαρμοστούν) είναι σύμφωνα με τις απαιτήσεις περί προστασίας των δεδομένων. Όσον αφορά τα αρχεία των δραστηριοτήτων επεξεργασίας, η τήρησή τους είναι ευθύνη του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, και όχι του υπευθύνου προστασίας δεδομένων. Πάντως, ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία μπορεί κάλλιστα να αναθέτει στον υπεύθυνο προστασίας δεδομένων το καθήκον να τηρεί τα αρχεία των πράξεων επεξεργασίας για τις οποίες είναι υπεύθυνος ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία. Τα εν λόγω αρχεία θα πρέπει να θεωρούνται ως ένα από τα εργαλεία που επιτρέπουν στον υπεύθυνο προστασίας δεδομένων να επιτελεί δύο από τα καθήκοντά του, ήτοι την*

- συνεργασία με την εποπτική αρχή,
- να ενεργεί ως σημείο επικοινωνίας για την εποπτική αρχή σε ζητήματα που σχετίζονται με την επεξεργασία.

β. Λειτουργική Ανεξαρτησία του DPO

Στο άρθρο 38 παράγραφοι 2 και 3 προβλέπονται οι βασικές εγγυήσεις που θα πρέπει να παρέχει ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία ώστε να διασφαλίζεται ότι ο DPO θα έχει την επαρκή αυτονομία αλλά και τους απαραίτητους πόρους για να εκτελεί αποτελεσματικά τα καθήκοντά του. Κατ' αρχήν, ο DPO, ανεξαρτήτως της εργασιακής του σχέσης με τον υπεύθυνο επεξεργασίας, δεν λαμβάνει εντολές από τον τελευταίο για την άσκηση των καθηκόντων του, αλλά δρα/ενεργεί με ανεξάρτητο τρόπο και με οδηγό την συμμόρφωση με το νομικό πλαίσιο[72]. Αυτό όμως δεν σημαίνει ότι ο DPO είναι και αυτός που παίρνει τις τελικές αποφάσεις· απλώς έχει το δικαίωμα να γνωστοποιήσει την αντίθετή του γνώμη απευθείας στον υπεύθυνο επεξεργασίας, ο οποίος και υποχρεούται απέναντι στον Κανονισμό να αποδείξει την συμμόρφωσή του[73]. Επιπλέον, θα πρέπει να διασφαλιστεί ότι για το πρόσωπο που θα κατέχει την θέση του DPO δεν θα ανακύψει ζήτημα σύγκρουσης συμφερόντων με άλλα καθήκοντά του, είτε αυτά είναι διοικητικής φύσεως είτε διεκπεραιωτικής φύσεως

παρακολούθηση της συμμόρφωσης, και την ενημέρωση και παροχή συμβουλών στον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία».

[72] Αιτιολογική σκέψη 97, Προοίμιο.

[73] Ομάδα άρθρου 29, Κατευθυντήριες γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων, 5-4-2017: «*Η διασφάλιση της αυτονομίας των υπεύθυνων προστασίας δεδομένων δεν σημαίνει, πάντως, ότι αποκτούν εξουσίες λήψης αποφάσεων καθ' υπέρβαση των καθηκόντων τους, όπως αυτά ορίζονται στο άρθρο 39. Ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία είναι αυτός που εξακολουθεί να φέρει την ευθύνη της συμμόρφωσης με το δίκαιο περί προστασίας των δεδομένων και πρέπει να είναι σε θέση να αποδείξει την εν λόγω συμμόρφωση. Αν ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία λαμβάνει αποφάσεις που έρχονται σε σύγκρουση με τον ΓΚΠΔ και με τις συμβουλές του υπευθύνου προστασίας δεδομένων, τότε ο υπεύθυνος προστασίας δεδομένων θα πρέπει να έχει την δυνατότητα να γνωστοποιήσει την αντίθετην γνώμη του στο ανώτατο διοικητικό επίπεδο του οργανισμού και στους υπεύθυνους λήψης των αποφάσεων. Σχετικά με το συγκεκριμένο θέμα, το άρθρο 38 παράγραφος 3 προβλέπει ότι ο υπεύθυνος προστασίας δεδομένων «λογοδοτεί απευθείας στο ανώτατο διοικητικό επίπεδο του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία». Με την απευθείας λογοδοσία διασφαλίζεται η πλήρης ενημέρωση της ανώτερης διοίκησης (π.χ., διοικητικό συμβούλιο) για τις συμβουλές και τις συστάσεις που διατυπώνει ο υπεύθυνος προστασίας δεδομένων στο πλαίσιο του καθήκοντός του να ενημερώνει και να συμβουλεύει τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία. Άλλο παράδειγμα απευθείας λογοδοσίας είναι η κατάρτιση ετήσιας έκθεσης δραστηριοτήτων από τον υπεύθυνο προστασίας δεδομένων και η υποβολή της στο ανώτατο διοικητικό επίπεδο»* .σελ. 20-21.

εφόσον από τις θέσεις αυτές είναι δυνατός ο καθορισμός των σκοπών και των μέσων της επεξεργασίας.

Άλλωστε, σύμφωνα με το άρθρο 38 παράγραφος 3, ο υπεύθυνος προστασίας δεδομένων «δεν απολύεται ούτε υφίσταται κυρώσεις από τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία επειδή επιτέλεσε τα καθήκοντά του»· με την διάταξή αυτή ενισχύεται η αυτονομία και η λειτουργική ανεξαρτησία των υπευθύνων προστασίας προκειμένου να επιτελούν τα καθήκοντά τους χωρίς φόβο. Για παράδειγμα, ο υπεύθυνος προστασίας δεδομένων εκτιμά ότι μία συγκεκριμένη επεξεργασία ενδέχεται να συνεπάγεται υψηλό κίνδυνο και συμβουλεύει τον υπεύθυνο επεξεργασίας να διενεργήσει εκτίμηση αντικτύπου ή προτείνει την υιοθέτηση μέτρων προστασίας τα οποία απαιτούν κάποιες δαπάνες· ο υπεύθυνος επεξεργασίας δεν συμφωνεί, αλλά δεν μπορεί και να απολύσει τον DPO απλώς επειδή ο τελευταίος παρείχε τις συγκεκριμένες «μη αρεστές» συμβουλές.

Τέλος, οι διοικητικοί και οικονομικοί πόροι που θα πρέπει να έχει στην διάθεσή του ο DPO για την απρόσκοπτη και αποτελεσματική εκτέλεση των καθηκόντων του είναι οι ακόλουθοι: ενεργή στήριξη από τα ανώτερα διοικητικά στελέχη και θωράκιση της αυτονομίας του[74], ανακοίνωση της θέσης και των αρμοδιοτήτων του στο προσωπικό, παροχή πρόσβασης στις πληροφορίες και τις διαδικασίες που αφορούν στα καθήκοντά τους και οικονομικοί, υλικοί και ανθρώπινοι πόροι για την ορθή επιτέλεση του έργου τους και δυνατότητα για συνεχή κατάρτιση και επιμόρφωση.

ε. Κώδικες Δεοντολογίας και Πιστοποίηση (αρθ. 40-42)

Σύμφωνα με την παρ. 2 του άρθρου 40 «ενώσεις ή άλλοι φορείς που

[74] Προκειμένου να διαφυλαχθεί η αυτονομία του DPO και να εκτελεί τα καθήκοντά του ανεπηρέαστα χωρίς να φοβάται αν θα απολυθεί εάν εντοπίσει ελλείψεις ή παρατυπίες στο σύστημα διαχείρισης προσωπικών δεδομένων του οργανισμού στον οποίο εργάζεται, το αρθ. 38 παρ. 3 προβλέπει ότι «*ο υπεύθυνος προστασίας δεδομένων δεν απολύεται ούτε υφίσταται κυρώσεις από τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία επειδή επιτέλεσε τα καθήκοντά του*». Εντούτοις, υπεύθυνος προστασίας δεδομένων μπορεί κάλλιστα να απολυθεί νομίμως για λόγους που δεν σχετίζονται με την συγκεκριμένη ιδιότητά του π.χ., σε περίπτωση κλοπής, σωματικής, ψυχολογικής ή σεξουαλικής παρενόχλησης ή συναφούς σοβαρού παραπτώματος.

εκπροσωπούν κατηγορίες υπεύθυνων επεξεργασίας ή εκτελούντων την επεξεργασία μπορούν να εκπονούν κώδικες δεοντολογίας» προκειμένου να συνδράμουν και τις πολύ μικρές, μικρές και μεσαίες επιχειρήσεις που έχουν περιορισμένους πόρους στην συμμόρφωση με το νομικό πλαίσιο του Κανονισμού υιοθετώντας ενδεδειγμένες πολιτικές σε όλο το εύρος των διαδικασιών που σχετίζονται με την επεξεργασία προσωπικών δεδομένων[75]. Την ίδια κατεύθυνση ακολουθεί και το άρθρο 42 βάσει του οποίου παρέχεται η δυνατότητα σε υπεύθυνους και εκτελούντες την επεξεργασία να αποδείξουν την συμμόρφωσή τους με σχετικές πιστοποιήσεις χορηγούμενες από ειδικευμένους προς τούτο φορείς. [76]

στ. Πρόστιμα, κυρώσεις, αποζημίωση

Απώτερο στόχο όλων των προαναφερόμενων διαδικασιών συμμόρφωσης αποτελεί η αποφυγή των πολύ αυστηρών προστίμων - κυρώσεων τις οποίες προβλέπει ο νέος Κανονισμός στο άρθρο 83, το ύψος των οποίων είναι ικανό όχι μόνο να πλήξει τους οικονομικούς πόρους των επιχειρήσεων αλλά και να τους εξαντλήσει. Χαρακτηριστικό είναι ότι τόσο στην πρώτη παράγραφο του άρθρου όσο και στην τελευταία (9η) αναφέρεται ότι τα πρόστιμα πρέπει να είναι «αποτελεσματικά, αναλογικά και αποτρεπτικά» καταδεικνύοντας έτσι την αυξημένη βαρύτητα της έντασης και της στόχευσης των προστίμων, ήτοι την απαρέγκλιτη

[75] Θέματα τα οποία οι κώδικες δεοντολογίας μπορούν να ρυθμίσουν ομοιόμορφα σε οργανισμούς και επιχειρήσεις του ίδιου κλάδου: α) την θεμιτή και με διαφάνεια επεξεργασία, β) τα έννομα συμφέροντα που επιδιώκουν οι υπεύθυνοι επεξεργασίας σε συγκεκριμένα πλαίσια, γ) την συλλογή δεδομένων προσωπικού χαρακτήρα, δ) την ψευδωνυμοποίηση δεδομένων προσωπικού χαρακτήρα, ε) την ενημέρωση του κοινού και των υποκειμένων των δεδομένων, στ) την άσκηση των δικαιωμάτων των υποκειμένων των δεδομένων, ζ) την ενημέρωση και την προστασία των παιδιών και τον τρόπο απόκτησης της συγκατάθεσης του ασκούντος την γονική μέριμνα του παιδιού, η) τα μέτρα και τις διαδικασίες που αναφέρονται στα άρθρα 24 και 25 και τα μέτρα για την διασφάλιση της ασφάλειας της επεξεργασίας που αναφέρεται στο άρθρο 32, θ) την γνωστοποίηση παραβιάσεων δεδομένων προσωπικού χαρακτήρα στις εποπτικές αρχές και την ανακοίνωση των εν λόγω παραβιάσεων δεδομένων προσωπικού χαρακτήρα στα υποκείμενα των δεδομένων, ι) την διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες ή διεθνείς οργανισμούς, ή ια) εξωδικαστικές διαδικασίες και άλλες διαδικασίες επίλυσης διαφορών για την επίλυση διαφορών μεταξύ υπευθύνων επεξεργασίας και υποκειμένων των δεδομένων όσον αφορά την επεξεργασία, με την επιφύλαξη των δικαιωμάτων των υποκειμένων των δεδομένων δυνάμει των άρθρων 77 και 79.

[76] Βλ. περισσότερα στο άρθρο 43 του Κανονισμού και υποσημειώσεις 61 και 93 της παρούσας εργασίας.

εφαρμογή των διατάξεων για την προστασία του εννόμου αγαθού των προσωπικών δεδομένων.

Ωστόσο, ο κανονισμός δεν προβλέπει συγκεκριμένα πρόστιμα για συγκεκριμένες παραβάσεις αλλά θέτει ανώτατο όριο (ανώτατο ποσό) και ειδικότερα, προβλέπονται δύο είδη-ύψη προστίμων ανάλογα με την επισυμβείσα παράβαση: α) Παραβάσεις της παρ. 4[77] επισύρουν, σύμφωνα με την παράγραφο 2, διοικητικά πρόστιμα έως 10.000.000 € ή, σε περίπτωση επιχειρήσεων, έως το 2 % του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους, ανάλογα με το ποιο είναι υψηλότερο και β) Παραβάσεις της παρ. 5[78] επισύρουν, σύμφωνα με την παράγραφο 2, διοικητικά πρόστιμα έως 20.000.000 € ή, σε περίπτωση επιχειρήσεων, έως το 4 % του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους, ανάλογα με το ποιο είναι υψηλότερο.

Η αιτιολογική σκέψη 148[79] προβλέπει την δυνατότητα αντικατάστασης του προστίμου με επίπληξη, σε περίπτωση που ο υπεύθυνος επεξεργασίας των δεδομένων είναι φυσικό πρόσωπο και το πρόστιμο που ενδέχεται να επιβληθεί θα

77

α) οι υποχρεώσεις του υπευθύνου επεξεργασίας και του εκτελούντος την επεξεργασία σύμφωνα με τα άρθρα 8, 11, 25 έως 39 και 42 και 43,
β) οι υποχρεώσεις του φορέα πιστοποίησης σύμφωνα με τα άρθρα 42 και 43,
γ) οι υποχρεώσεις του φορέα παρακολούθησης σύμφωνα με το άρθρο 41 παράγραφος 4.

78

α) οι βασικές αρχές για την επεξεργασία, περιλαμβανομένων των όρων που ισχύουν για την έγκριση, σύμφωνα με τα άρθρα 5, 6, 7 και 9,
β) τα δικαιώματα των υποκειμένων των δεδομένων σύμφωνα με τα άρθρα 12 έως 22,
γ) η διαβίβαση δεδομένων προσωπικού χαρακτήρα σε αποδέκτην σε τρίτην χώρα ή σε διεθνή οργανισμό σύμφωνα με τα άρθρα 44 έως 49,
δ) οποιεσδήποτε υποχρεώσεις σύμφωνα με το δίκαιο του κράτους μέλους οι οποίες θεσπίζονται δυνάμει του κεφαλαίου IX,
ε) μη συμμόρφωση προς εντολή ή προς προσωρινό ή οριστικό περιορισμό της επεξεργασίας ή προς αναστολή της κυκλοφορίας δεδομένων που επιβάλλει η εποπτική αρχή δυνάμει του άρθρου 58 παράγραφος 2 ή μη παροχή πρόσβασης κατά παράβαση του άρθρου 58 παράγραφος 1.

79 «Προκειμένου να ενισχυθεί η επιβολή των κανόνων του παρόντος κανονισμού, κυρώσεις, συμπεριλαμβανομένων των διοικητικών προστίμων, θα πρέπει να επιβάλλονται για κάθε παράβαση του παρόντος κανονισμού, επιπρόσθετα ή αντί των κατάλληλων μέτρων που επιβάλλονται από την εποπτική αρχή σύμφωνα με τον παρόντα κανονισμό. Σε περίπτωση παράβασης ελάσσονος σημασίας ή αν το πρόστιμο που ενδέχεται να επιβληθεί θα αποτελούσε δυσανάλογη επιβάρυνση σε φυσικό πρόσωπο, θα μπορούσε να επιβληθεί επίπληξη αντί προστίμου. Η επιβολή κυρώσεων, συμπεριλαμβανομένων των διοικητικών προστίμων, θα πρέπει να υπόκειται σε κατάλληλες δικονομικές εγγυήσεις σύμφωνα με τις γενικές αρχές του ενωσιακού δικαίου και του Χάρτη, συμπεριλαμβανομένης της πραγματικής δικαστικής προστασίας και της ορθής διαδικασίας»

αποτελούσε δυσανάλογη επιβάρυνση· η εποπτική αρχή είναι αυτή που θα αξιολογήσει κατά πόσο είναι απαραίτητην η επιβολή προστίμου και σε δεύτερο επίπεδο το ύψος του ώστε να επιτευχθεί ο στόχος του διορθωτικού μέτρου, δηλαδή είτε την αποκατάσταση της συμμόρφωσης με τους κανόνες είτε η τιμωρία παράνομης συμπεριφοράς (ή αμφότερα). Ειδικότερα, **στο** άρθρο 83 παράγραφος 2 ορίζεται ότι «[*κ]ατά την λήψη απόφασης σχετικά με την επιβολή διοικητικού προστίμου, καθώς και σχετικά με το ύψος του διοικητικού προστίμου για κάθε μεμονωμένη περίπτωση, λαμβάνονται δεόντως υπόψη τα ακόλουθα*»:

α. **Η φύση, η βαρύτητα και η διάρκεια της παράβασης -** εξετάζεται η ο σκοπός της σχετικής επεξεργασίας, καθώς και ο αριθμός των υποκειμένων των δεδομένων που επηρεάστηκαν από την παράβαση καθώς και ο βαθμός ζημίας που υπέστησαν

β. **Ο δόλος ή η αμέλεια που προκάλεσε την παράβαση**

γ. **Ενέργειες στις οποίες προέβη ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία για να μετριάσει την ζημία που υπέστησαν τα υποκείμενα των δεδομένων**

δ. **Ο βαθμός ευθύνης του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία –** εξετάζεται η αποτελεσματική λήψη τεχνικών και οργανικών μέτρων

ε. **Τυχόν σχετικές προηγούμενες παραβάσεις του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία**

στ. **Ο βαθμός συνεργασίας με την αρχή ελέγχου για την επανόρθωση της παράβασης και τον περιορισμό των πιθανών δυσμενών επιπτώσεών της**

ζ. **Οι κατηγορίες δεδομένων προσωπικού χαρακτήρα που επηρεάζει η παράβαση**

η. **Ο τρόπος με τον οποίο η εποπτική αρχή πληροφορήθηκε την παράβαση, ειδικότερα εάν και κατά πόσο ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία κοινοποίησε την παράβαση –** εξετάζεται αν η ενημέρωση των εποπτικών αρχών είναι έγκαιρη και με διάθεση αποκατάστασης της παράβασης ή τυπική ή

ακόμα και πλημμελής με διάθεση συγκάλυψης της παράβασης

θ. **Σε περίπτωση που διατάχθηκε προηγουμένως η λήψη συγκεκριμένων μέτρων κατά του εμπλεκόμενου υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, σχετικά με το ίδιο αντικείμενο, η συμμόρφωση με τα εν λόγω μέτρα**

ι. **Η τήρηση εγκεκριμένων κωδίκων δεοντολογίας ή εγκεκριμένων μηχανισμών πιστοποίησης από τους υπευθύνους επεξεργασίας κατά τα άρθρα 40 και 42 του κανονισμού**

ια. **Κάθε άλλο επιβαρυντικό ή ελαφρυντικό στοιχείο που προκύπτει από τις περιστάσεις της συγκεκριμένης περίπτωσης, όπως τα οικονομικά οφέλη που αποκομίστηκαν ή ζημιών που αποφεύχθηκαν, άμεσα ή έμμεσα, από την παράβαση**

ΙΙ. ΒΗΜΑΤΑ ΣΥΜΜΟΡΦΩΣΗΣ

Στο πρώτο μέρος της εργασίας αναφέρθηκαν αναλυτικά και εκτεταμένα οι νομικές υποχρεώσεις των υπευθύνων επεξεργασίας και των εκτελούντων την επεξεργασία με βάση τις διατάξεις του Κανονισμού· ωστόσο η συμμόρφωση των οργανισμών και των επιχειρήσεων απαιτεί αποκλειστικά πρακτική εφαρμογή και διαδικαστικά βήματα προκειμένου να επιτευχθούν οι απώτεροι σκοποί της προστασίας της ιδιωτικότητας των φυσικών προσώπων.

Ιδιαίτερα για τις μικρομεσαίες επιχειρήσεις οι αναγκαίες αλλαγές στην λειτουργία και την διαχείριση των δεδομένων τους λόγω της υποχρεωτικής εφαρμογής του Κανονισμού συνιστούν μεγάλη πρόκληση καθώς απαιτούν μεγάλο οικονομικό αλλά και οργανωτικό κόστος στο οποίο δύσκολα μπορούν να ανταπεξέλθουν δεδομένης της εθνικής αλλά και παγκόσμιας οικονομικής κατάστασης. Βέβαια όπως προελέχθη και στην εισαγωγή, ο Κανονισμός αποτελεί μία καλή μία καλή ευκαιρία «τακτοποίησης» και εσωτερικής (ανα)διοργάνωσης των επιχειρήσεων για καλύτερη διαχείριση όλου του εύρους των δεδομένων τους, ανεξαρτήτως νομικής υποχρέωσης ή φόβου επιβολής κυρώσεων.

1. ΧΑΡΤΟΓΡΑΦΗΣΗ - ΔΙΑΧΕΙΡΙΣΗ ΔΕΔΟΜΕΝΩΝ

Πρωταρχικό και καίριο βήμα είναι ο εντοπισμός όλων των δεδομένων που συλλέγει και χρησιμοποιεί η επιχείρηση μέσω του πληροφοριακού της συστήματος[80]· θα πρέπει να καταγραφεί ο τρόπος συλλογής, ο σκοπός συλλογής, η νομιμοποίηση, το μέσο αποθήκευσης, η διάρκεια διατήρησης και η πρόσβαση. Τα δεδομένα αυτά, είτε είναι δομημένα και βρίσκονται σε ηλεκτρονική μορφή είτε αδόμητα και βρίσκονται σε έγγραφα, μπορούν να ανευρεθούν με αυτοματοποιημένα εργαλεία, ερωτηματολόγια και συνεντεύξεις στο προσωπικό σχετικά με τις διαδικασίες που εκτελούν και οι οποίες αφορούν με οποιονδήποτε

[80] Σύνολο διαδικασιών, ανθρώπινου δυναμικού και αυτοματοποιημένων υπολογιστικών συστημάτων, που προορίζονται για την συλλογή, εγγραφή, ανάκτηση, επεξεργασία, αποθήκευση και ανάλυση πληροφοριών.

τρόπο προσωπικά δεδομένα. Υπάρχουν εξειδικευμένες εφαρμογές για την εν λόγω χαρτογράφηση[81] που όχι μόνο ανασύρουν δεδομένα κάθε μορφής από έγγραφα και emails, αλλά τα ταξινομούν και τα αρχειοθετούν με την χρήση ετικετών (tags) και την δημιουργία μεταδεδομένων (metadata). Αφού χαρτογραφηθούν οι ροές δεδομένων[82] από τις εξωτερικές πηγές προς τις εσωτερικές διεργασίες θα πρέπει, ιδανικά, να ενσωματωθούν σε ένα κεντρικό σύστημα διαχείρισης-αρχειοθέτησης, ή εναλλακτικά σε επιμέρους συστήματα, και να κατηγοριοποιηθούν αναλόγως με την επικινδυνότητα (ευαίσθητα ή μη), την νομική βάση της συλλογής, την επιτρεπόμενη διάρκεια διατήρησης ώστε να διαγραφούν όσα δεν πληρούν τις προϋποθέσεις νομιμότητας, ικανοποιώντας έτσι και τις αρχές της ιδιωτικότητας εξ ορισμού και ήδη από τον σχεδιασμό[83].

Άλλωστε, το πρώτο βήμα για την εκπόνηση της Εκτίμησης Επικινδυνότητας, σύμφωνα και με τον Enisa[84], αποτελεί ο προσδιορισμός των εκτελούμενων από την επιχείρηση ειδών επεξεργασίας καθώς των ειδικών χαρακτηριστικών τους, αφού ληφθούν υπ' όψιν όλες οι φάσεις της επεξεργασίας (συλλογή, αποθήκευση, χρήση, μεταφορά, διαγραφή, κτλ). Ειδικότερα, για να εκτιμηθεί η πιθανότητα επέλευσης κάποιου κινδύνου και οι τυχόν επιπτώσεις που θα επηρεάσουν τα υποκείμενα των δεδομένων θα πρέπει να αναλυθούν και να συγκεκριμενοποιηθούν κατά περίπτωση και κατά δραστηριότητα επεξεργασίας τα εξής στοιχεία: η φύση των επεξεργαζόμενων δεδομένων (ευαίσθητα ή μη), ο σκοπός και τα μέσα της συγκεκριμένης επεξεργασίας, τα υποκείμενα των δεδομένων (πελάτες, εργαζόμενοι, κ.α.) και οι τυχόν τρίτοι αποδέκτες των δεδομένων.

[81] https://blogs.opentext.com/opentext-file-intelligence/

[82] Η περιγραφή του πληροφοριακού συστήματος αποτελείται από το διάγραμμα ροής δεδομένων, το διάγραμμα δικτύου και την περιγραφή τεχνικής υποδομής και του εξοπλισμού (hardware & software). Τα εν λόγω στοιχεία είναι αναγκαία προκειμένου να μπορεί να καθοριστεί η διαδρομή των προσωπικών δεδομένων μέσα στο πληροφοριακό σύστημα, οι πηγές άντλησής τους, τα ενδιάμεσα σημεία αποθήκευσής τους καθώς και το σημείο τερματισμού τους, ώστε να διασφαλιστεί η ασφάλειά τους σε όλο το μήκος και εύρος της ροής. Βλ. Περισσότερα: Α. Χρυσάνθου, Ζητήματα Ασφαλείας δεδομένων, σε Λ. Κοτσαλής, Προσωπικά Δεδομένα, σελ. 391.

[83] https://www.avepoint.com/blog/manage/data-discovery-data-mapping-gdpr-compliance/

[84] Handbook on Security of Personal Data Processing, σελ. 10.

2. ΚΑΤΑΡΤΙΣΗ ΠΟΛΙΤΙΚΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ

Συγχρόνως και συμπληρωματικά στην διεργασία της χαρτογράφησης θα πρέπει να σχηματιστεί κατ' αρχήν, σε δεύτερο στάδιο να συνταχθεί και σε τρίτο στάδιο να δημοσιοποιηθεί ως προς τα βασικά της σημεία η πολιτική ιδιωτικότητας της επιχείρησης· θα πρέπει δηλαδή να ληφθούν υπ' όψιν οι γενικές αρχές της προστασίας των προσωπικών δεδομένων για ολόκληρο τον «κύκλο ζωής» τους (συλλογή-αποθήκευση-επεξεργασία-διαγραφή) και να διαμορφωθεί η νοοτροπία και η κουλτούρα της επιχείρησης – τουλάχιστον σε θεωρητικό επίπεδο – όσον αφορά την ιδιωτικότητα. Έτσι, στην πορεία κατά την επιλογή πρακτικών λύσεων για την διενέργεια της επεξεργασίας ο οργανισμός θα δημιουργεί επιχειρησιακές διαδικασίες αλλά και θα αναπτύσσει ή θα επιλέγει λογισμικό με γνώμονα την καθορισμένη πολιτική ιδιωτικότητας πραγματώνοντας μ' αυτόν τον τρόπο και τις βασικές αρχές της προστασίας ήδη από τον σχεδιασμό και εξ ορισμού.

Μερικές «στρατηγικές»[85] που θα μπορούσε να ακολουθήσει ένας οργανισμός κατά τον σχεδιασμό της πολιτικής ιδιωτικότητάς του είναι οι εξής:

1. ΕΛΑΧΙΣΤΟΠΟΙΗΣΗ

Η πιο βασική στρατηγική ιδιωτικότητας είναι η ελαχιστοποίηση δεδομένων, με την έννοια ότι τα προσωπικά δεδομένα που υπόκεινται σε επεξεργασία πρέπει να είναι τα ελάχιστα δυνατά. Εξασφαλίζοντας ότι δεν συλλέγονται μη απαραίτητα δεδομένα μειώνεται ο πιθανός αντίκτυπος στην ιδιωτική ζωή των φυσικών προσώπων.

Τακτικές:

Επιλογή: επιλογή μόνο των σχετικών προσώπων και των σχετικών στοιχείων που πρέπει να συλλεχθούν για σαφώς προσδιορισμένο σκοπό.

Απόρριψη: άμεση απόρριψη όλων των δεδομένων που δεν έχουν επιλεχθεί προς επεξεργασία και δεν σχετίζονται με σαφώς προσδιορισμένο σκοπό επεξεργασίας.

[85] Jaap-Henk Hoepman, Privacy Design Strategies, https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf . Βλ. περισσότερα, ENISA, ***Privacy and Data Protection by Design – from policy to engineering,*** December 2014.

Αφαίρεση: (Μερική) αφαίρεση δεδομένων μόλις αυτά δεν είναι πλέον χρήσιμα ή μόλις λήξει το χρονικό περιθώριο το οποίο έχει προσδιοριστεί για την νόμιμη διατήρησή τους (μπορεί να χρησιμοποιηθεί η τεχνική της ανωνυμοποίησης) – αφορά το λογισμικό (application layer)

Καταστροφή: Ολική διαγραφή δεδομένων χωρίς δυνατότητα επαναφοράς (χρήση ασφαλών και αποτελεσματικών μεθόδων διαγραφής από σκληρούς δίσκους και backups) – αφορά τις συσκευές (hardware - physical layer)

Συνήθεις Πρακτικές:

- εγγραφή τυχαίων δεδομένων πολλές φορές σε σκληρό δίσκο ώστε να διαγραφούν οριστικά τα προσωπικά δεδομένα και να μην μπορούν να ανακτηθούν
- κρυπτογράφηση backup και καταστροφή του μυστικού κλειδιού αποκρυπτογράφησης

2. ΑΠΟΚΡΥΨΗ

«Κάθε προσωπική πληροφορία που τυγχάνει επεξεργασίας θα πρέπει να μην είναι εμφανής σε κοινή θέα». Η ratio αυτής της στρατηγικής έγκειται στο ότι η απόκρυψη των προσωπικών δεδομένων έχει ως αποτέλεσμα την μείωση του κινδύνου παραβίασής τους· το υποκείμενο από το οποίο θα πρέπει να αποκρύπτονται οι πληροφορίες αλλάζει αναλόγως των περιστάσεων προκειμένου να επιτευχθεί ο μέγιστος βαθμός εμπιστευτικότητας.

Τακτικές:

Περιορισμός: Περιορισμός της πρόσβασης στα αρχεία προσωπικών δεδομένων· υιοθέτηση αυστηρής πολιτικής ελέγχου βάσει της οποίας θα έχουν πρόσβαση σε αυτά μόνο όσοι «πρέπει» να τα γνωρίζουν προκειμένου να καταστεί όσο το δυνατόν δυσκολότερη η τυχαία διαρροή τους.

Κατακερματισμός: Κρυπτογράφηση των δεδομένων ώστε να είναι ακατάληπτα χωρίς την κατοχή του μυστικού κλειδιού

Αποσύνδεση: Αφαίρεση των συσχετισμών μεταξύ γεγονότων, προσώπων και δεδομένων ώστε να μην μπορούν να ταυτοποιήσουν συγκεκριμένο πρόσωπο.

Ανάμειξη: Ανάμειξη και ανωνυνοποίηση των δεδομένων για να αποκρυβούν πιθανοί συσχετισμοί.

Συνήθεις πρακτικές:

- η χρήση τεχνικών κρυπτογράφησης είτε τοπικά για τα αποθηκευμένα δεδομένα (data at rest) είτε με την χρήση του πρωτοκόλλου SSL[86] για τα δεδομένα που μεταδίδονται στο δίκτυο (data at transit),
- η ανωνυμοποίηση και ψευδωνυμοποίηση δεδομένων[87]
- χρήση πολλαπλών διακομιστών (mix networks[88]) προκειμένου να μην καταγραφεί η κίνηση των δεδομένων ή να υποκλαπούν κατά την μεταφορά τους

3. ΔΙΑΧΩΡΙΣΜΟΣ

Με τον διαχωρισμό και την αποκέντρωση της επεξεργασίας ή της αποθήκευσης των πολλαπλών δεδομένων του ίδιου φυσικού προσώπου, επιτυγχάνεται ο κατακερματισμός τους και η αποφυγή δημιουργίας ολοκληρωμένου προφίλ. Συγκεκριμένα, τα προσωπικά δεδομένα που προέρχονται από διαφορετικές πηγές θα πρέπει να αποθηκεύονται και σε ξεχωριστές βάσεις δεδομένων, όπως επίσης και οι συγκεντρωτικές βάσεις δεδομένων θα πρέπει να διαχωρίζονται με βάση τον σκοπό επεξεργασίας. Στόχος είναι να μην συγκεντρώνεται το σύνολο των πληροφοριών σε μία μόνο βάση δεδομένων καθώς οι εκτελούντες μία συγκεκριμένη επεξεργασία όταν θα αντλούν τα απαραίτητα γι' αυτούς δεδομένα θα μπορούν ταυτόχρονα να έχουν πρόσβαση και στα υπόλοιπα που δεν χρειάζονται.

Τακτικές:

Απομόνωση: Συλλογή και επεξεργασία προσωπικών δεδομένων σε διαφορετικές

[86] https://el.wikipedia.org/wiki/SSL
[87] Βλ. παρακάτω, σελ. 106.
[88] https://en.wikipedia.org/wiki/Mix_network

βάσεις δεδομένων και εφαρμογές, δηλαδή είτε οι βάσεις δεδομένων θα είναι διαχωρισμένες με αυστηρό λογικό τρόπο ή θα τρέχουν σε διαφορετικά μηχανήματα – ακόμα κι αν αυτά ελέγχονται κεντρικά.

Διανομή: Διανομή της συλλογής και της επεξεργασίας των προσωπικών δεδομένων σε διαφορετικές φυσικές τοποθεσίες χρησιμοποιώντας βάσεις δεδομένων και συστήματα που δεν ελέγχονται κεντρικά από ένα σημείο ή οργανισμό. Χρήση αποκεντρωμένης ή διανεμημένης αρχιτεκτονικής συστήματος αντί για κεντρικοποιημένη.

Συνήθεις πρακτικές:

- τοπική αποθήκευση στην συσκευή του χρήστη (υπολογιστή, smartphone κ.τ.λ.) όλων των δεδομένων (συζητήσεις, φωτογραφίες, ρυθμίσεις, κτλ)
- χρήση δικτύου peer-to-peer[89] ώστε να μην αποθηκεύονται ή τυγχάνουν επεξεργασίας από μία κεντρικοποιημένη οντότητα τα δεδομένα που ανταλλάσσονται στο δίκτυο

4. ΑΦΑΙΡΕΣΗ

Η εν λόγω στρατηγική καλεί για όσο το δυνατόν μεγαλύτερη μείωση των λεπτομερειών των προσωπικών δεδομένων· ενώ η στρατηγική της «ελαχιστοποίησης» καλεί τον υπεύθυνο επεξεργασίας να αποφασίσει εάν χρειάζεται να επεξεργαστεί μία συγκεκριμένη κατηγορία δεδομένων, η στρατηγική της «αφαίρεσης» τον καλεί να αποφασίσει σε τι επίπεδο λεπτομέρειας θα επεξεργαστεί μία κατηγορία δεδομένων. Με τον περιορισμό της ποσότητας των λεπτομερειών των προσωπικών δεδομένων ή με την επεξεργασία των λεπτομερειακών πληροφοριών σε ομαδικό επίπεδο και όχι για κάθε φυσικό πρόσωπο ξεχωριστά, αυτές οι πληροφορίες δεν καθίστανται τόσο «ευαίσθητες» καθώς δεν μπορούν να δημιουργήσουν ένα ολοκληρωμένο λεπτομερειακό προφίλ ή δεν μπορούν να αποδοθούν σε συγκεκριμένο πρόσωπο και να το ταυτοποιήσουν.

Επίσης, η διατήρηση λεπτομερών αρχείων καταγραφής σε ένα σύστημα είναι

[89] https://el.wikipedia.org/wiki/Peer-to-peer

απαραίτητη για να ενεργήσει κανείς γρήγορα σε περίπτωση παραβίασης, αλλά συνήθως αυτά καθίστανται λιγότερο σχετικά με την πάροδο του χρόνου, ενώ μία πιο συγκεντρωτική (στατιστικού τύπου) εικόνα είναι πιο χρήσιμη· συνεπώς προτείνεται η κατά διαστήματα εκκαθάρισή τους.

Τακτικές:

Σύνοψη: Σύνοψη λεπτομερειακών χαρακτηριστικών σε ποιο γενικευμένα χαρακτηριστικά , όπου είναι δυνατόν, π.χ. χρήση ηλικιακής κατηγορίας αντί για έτος γέννησης, ή πόλη κατοικίας αντί για πλήρη διεύθυνση.

Ομαδοποίηση: Συγκέντρωση και επεξεργασία πληροφοριών για μία ομάδα ατόμων αντί για επεξεργασία προσωπικών δεδομένων για κάθε άτομο ξεχωριστά, δημιουργώντας ομαδικά προφίλ με μία κοινή βάση χαρακτηριστικών όλων των ατόμων που συνθέτουν την ομάδα.

Παραμόρφωση: Επεξεργασία της πληροφορίας με μικρή απόκλιση από την πραγματική της «τιμή», π.χ. αντί της χρήσης της ακριβούς τοποθεσίας ενός φυσικού προσώπου, χρήση τυχαίας τοποθεσίας σε μία απόσταση από την πραγματική.

Συνήθεις πρακτικές:

- χρήση τεχνικών επεξεργάσιμης κρυπτογράφησης ώστε ο κάθε χρήστης του συστήματος να λαμβάνει γνώση μόνο των απαραίτητων για την διεκπεραίωση των καθηκόντων του προσωπικών δεδομένων

5. ΠΛΗΡΟΦΟΡΗΣΗ

Η στρατηγική της «πληροφόρησης» πραγματώνει την αρχή της διαφάνειας και εκπληρώνει την υποχρέωση της ενημέρωσης. Τα υποκείμενα των δεδομένων θα πρέπει να ενημερώνονται επαρκώς και με σαφήνεια όταν τυγχάνουν επεξεργασίας οι προσωπικές τους πληροφορίες και συγκεκριμένα για το ποιες πληροφορίες, για ποιους σκοπούς και με ποιους τρόπους συλλέγονται και υπόκεινται σε επεξεργασία, αλλά και για τυχόν τρίτους στους οποίους μπορεί να κοινοποιηθούν αυτά· επίσης, θα πρέπει να ενημερώνονται για τα μέσα προστασίας που χρησιμοποιεί ο εκάστοτε

υπεύθυνος επεξεργασίας κατά παραβιάσεων και υποκλοπών.

Τακτικές:

Ενημέρωση: Παροχή πληροφοριών σχετικά με το είδος των δεδομένων που υπόκεινται σε επεξεργασία, τον τρόπο και τους σκοπούς επεξεργασίας. Σαφής προσδιορισμός του χρονικού διαστήματος που διατηρούνται τα προσωπικά δεδομένα και του τρόπου διαγραφής τους και ενημέρωση σχετικά με τρίτους στους οποίους κοινοποιούνται τα δεδομένα. Εύκολος και εμφανής τρόπος επικοινωνίας των υποκειμένων με τον οργανισμό σχετικά με την πολιτική ιδιωτικότητας, αλλά και με την Εποπτική Αρχή.

Επεξήγηση: Παροχή των παραπάνω πληροφοριών με σαφή και εύληπτο τρόπο ώστε να είναι κατανοητές και σε κάποιον μη σχετικό με τις έννοιες των προσωπικών δεδομένων.

Κοινοποίηση: Ειδοποίηση των χρηστών σε πραγματικό χρόνο την στιγμή που συλλέγονται τα δεδομένα τους ή που κοινοποιούνται σε τρίτους ή αμέσως μόλις γίνει αντιληπτή παραβίαση στο σύστημα. Διαμόρφωση ξεκάθαρης και απλής πολιτικής ως προς τα γεγονότα που πρέπει να κοινοποιηθούν, παρέχοντας την δυνατότητα στους χρήστες να επιλέγουν για ποια από αυτά επιθυμούν να λαμβάνουν ειδοποιήσεις.

Συνήθεις πρακτικές:

- Χρήση εικονιδίων σχετικών με την ιδιωτικότητα ώστε με μία πρώτην ματιά να μπορεί ο χρήστης να καταλάβει την πολιτική συλλογής και προστασίας των προσωπικών του δεδομένων
- Πίνακας ρυθμίσεων (dashboard) από όπου ο χρήστης μπορεί να δει τα προσωπικά δεδομένα που έχουν συλλεχθεί, να κατεβάσει αντίγραφό τους, να αλλάξει τους όρους συγκατάθεσής του, να επικοινωνήσει με τον DPO.

Εικονίδια Ιδιωτικότητας[90]

6. ΕΛΕΓΧΟΣ

Τα φυσικά πρόσωπα θα πρέπει να διατηρούν τον έλεγχο επί των δεδομένων τους και να τα διαχειρίζονται κατά βούληση διατηρώντας το δικαίωμα να αποφασίζουν εάν επιθυμούν να τύχουν επεξεργασίας ή όχι – εκτός από πολύ συγκεκριμένες και ρητώς προβλεπόμενες περιπτώσεις όπου υπερισχύει το δημόσιο συμφέρον.

Η στρατηγική του Ελέγχου είναι αναπόσπαστο συμπλήρωμα της στρατηγικής της Ενημέρωσης καθώς εάν το φυσικό πρόσωπο δεν μπορεί να ελέγξει την επεξεργασία των δεδομένων του, η πληροφόρησή του σχετικά με την συλλογή τους καθίσταται άνευ σημασίας. Η έννοια του ελέγχου υπερβαίνει αυτήν της «συγκατάθεσης κατόπιν ενημέρωσης» και περιλαμβάνει επίσης τα δικαιώματα του υποκειμένου ως προς την διαχείριση των προσωπικών του δεδομένων (δικαίωμα πρόσβασης, διόρθωσης, διαγραφής, κ.τ.λ.), την δυνατότητα αλλαγής των προτιμήσεων ιδιωτικότητας μέσω της αντίστοιχης διεπαφής.

Τακτικές:

Συγκατάθεση: Απόκτηση ρητής συγκατάθεσης από τα υποκείμενα για την νόμιμη επεξεργασία των δεδομένων κατόπιν σχετικής ενημέρωσης για το ποια δεδομένα συλλέγονται, για ποιους σκοπούς, με ποιον τρόπο μπορεί να ανακληθεί ή να περιοριστεί η συγκατάθεση.

[90] Πηγή: https://image.flaticon.com/sprites/new_packs/1105000-privacy-policy.png

Επιλογή: Παροχή πραγματικής επιλογής – οι βασικές λειτουργικότητες – τουλάχιστον– θα πρέπει να είναι διαθέσιμες ακόμα και για τα υποκείμενα που δεν συναινούν στην συλλογή των προσωπικών τους δεδομένων

Επικαιροποίηση: Παροχή δυνατότητας στους χρήστες να ανασκοπήσουν και να επικαιροποιήσουν τις προτιμήσεις τους σχετικά με τα συλλεγόμενα γι' αυτούς προσωπικά δεδομένα.

Ανάκληση: Παροχή δυνατότητας ανάκλησης της συγκατάθεσης ή διαγραφής των προσωπικών δεδομένων που έχουν συλλεχθεί

Συνήθεις πρακτικές:

- χρήση επιλογών opt-in (εγγραφή) αντί για επιλογή opt-out (απεγγραφή) – συνεπώς, τα σχετικά με την συγκατάθεση πεδία-κουτάκια δεν θα πρέπει να είναι από πριν τσεκαρισμένα, αλλά ο χρήστης να τα επιλέγει με δική του ενέργεια (π.χ. για την εγγραφή σε newsletter ή για την αποστολή διαφημίσεων από τρίτους)
- δυνατότητα επιλογής διαφορετικών ειδών cookies – απαραίτητα για ανώνυμη στατιστική, για καταγραφή επιδόσεων, για διαφημιστικούς σκοπούς, από τρίτους – χωρίς να αποκόπτεται η πρόσβαση στον ιστότοπο εάν δεν επιλεγούν όλα.

7. ΣΥΜΜΟΡΦΩΣΗ

Η στρατηγική της Συμμόρφωσης εξασφαλίζει ότι το πληροφοριακό σύστημα του οργανισμού συμβαδίζει με το ισχύον νομικό πλαίσιο και ανανεώνεται με βάση τις τροποποιήσεις αυτού. Όμως πέραν της κατάρτισης της πολιτικής ιδιωτικότητας θα πρέπει να γίνουν οι απαραίτητες ενέργειες για την πρακτική εφαρμογή της σε οργανωτικό και τεχνικό επίπεδο. Είναι απαραίτητο για την αποτελεσματική ενσωμάτωσή της να συμβαδίζει με τις γενικότερες επιχειρησιακές πολιτικές του οργανισμού.

Τακτικές:

Δημιουργία: Ο οργανισμός θα πρέπει να υιοθετήσει την νοοτροπία προστασίας των προσωπικών δεδομένων και να δεσμευτεί στην πρακτική εφαρμογή της πολιτικής ήδη από τα ανώτερα κλιμάκια, αλλά και με την χρήση των απαραίτητων πόρων.

Διατήρηση: Εξασφάλιση της εσωτερικής εφαρμογής της πολιτικής ιδιωτικότητας με οργανωτικά και τεχνικά μέτρα καθώς και με την εκπαίδευση του προσωπικού.

Επικαιροποίηση: Συνεχής επικαιροποίηση των στοιχείων της πολιτικής ιδιωτικότητας τόσο με βάση τις προϋποθέσεις της νόμιμης επεξεργασίας όσο και με βάση τις τεχνολογικές εξελίξεις.

Συνήθεις πρακτικές:

- απόκτηση πιστοποίησης σχετικής με την ασφάλεια πληροφοριών (ISO 27001)[91].
- εκπόνηση εκτίμησης κινδύνου και εκτίμησης αντικτύπου[92]
- προσδιορισμός προδιαγραφών για την ανάπτυξη ή την αγορά προϊόντων και υπηρεσιών τεχνολογίας (privacy by design)

8. ΑΠΟΔΕΙΞΗ ΣΥΜΜΟΡΦΩΣΗΣ

Η τελευταία στρατηγική της «Απόδειξης της συμμόρφωσης» είναι επιβεβλημένη πλέον μετά την έναρξη ισχύος του GDPR, καθώς οι υπεύθυνοι επεξεργασίας υποχρεούνται να αποδείξουν ότι έχουν λάβει υπ' όψιν το ισχύον νομικό – ευρωπαϊκό- πλαίσιο και ότι έχουν προβεί στις κατάλληλες οργανωτικές και τεχνικές βελτιώσεις ως προς την εξασφάλιση της προστασίας των προσωπικών δεδομένων κατά την συλλογή και την επεξεργασία τους – αρχή λογοδοσίας. Η εν λόγω στρατηγική απευθύνεται κυρίως στις εθνικές ή κοινοτικές Αρχές Προστασίας Προσωπικών Δεδομένων (συνήθως με δίαυλο επικοινωνίας τον υπεύθυνο προστασίας).

Τακτικές:

Καταγραφή: Καταγραφή όλων των σημαντικών των σχετικών με την ιδιωτικότητα

[91] βλ. παρακάτω, υποσημείωση 93.
[92] Βλ. παρακάτω. 5. Ανάλυση Κινδύνου και Έκθεση Εκτίμησης Αντικτύπου (DPIA), σελ. 90.

ενεργειών στις οποίες προβαίνει ο υπεύθυνος επεξεργασίας και τήρηση αρχείου δραστηριοτήτων.

Έλεγχος: Τακτικός έλεγχος των αρχείων καταγραφής αλλά και των επιχειρησιακών διαδικασιών γενικότερα για τον τρόπο επεξεργασίας των προσωπικών δεδομένων.

Συνήθεις πρακτικές:

- εκπόνηση έκθεσης εκτίμησης αντικτύπου και καταγραφή των αποφάσεων που λαμβάνονται με βάση τα αποτελέσματά της· θα πρέπει να επαναλαμβάνεται εκ νέου
- απόκτηση πιστοποίησης σχετικής με την ασφάλεια πληροφοριών (ISO 27000)[93] ή με την επιχειρησιακή συνέχεια (ISO 22301)

Τέλος, σε αυτό το στάδιο αφού συγκεκριμενοποιηθεί η πολιτική του οργανισμού ως προς την πολιτική επεξεργασίας και την πολιτική προστασίας θα πρέπει να δημοσιοποιηθούν τα καίρια στοιχεία αυτής καθώς και να καταστούν σαφείς και εμφανείς οι τρόποι με τους οποίους θα μπορέσει ένα φυσικό πρόσωπο να ασκήσει τα δικαιώματά του· η δημοσιοποίηση αυτή μπορεί να γίνει εγγράφως με υπογραφή του πελάτη σε έγγραφο ότι έλαβε γνώση αυτής ή με αντίστοιχους τρόπους στο ηλεκτρονικό περιβάλλον: π.χ. ενσωμάτωση στην ιστοσελίδα πεδίων με τους σκοπούς επεξεργασίας ώστε το φυσικό πρόσωπο να μπορεί να «τικάρει» αυτά στα

[93] Βλ. περισσότερα, Χρίστος Κόζιαρης, *ISO 27000 και GDPR*: «*Το πρότυπο ISO 27001:2013 ασχολείται με την ασφάλεια της πληροφορίας (International Organization for Standardization, 2018) και έχει αρκετά κοινά σημεία με τον κανονισμό GDPR. Στο παράρτημα Α, του προτύπου ISO 27001 περιγράφονται οι στόχοι και τα σημεία ελέγχου, που απαιτεί το πρότυπο… [τα οποία] μπορούν να χρησιμοποιηθούν για την υποστήριξη συμμόρφωσης με τον κανονισμό GDPR και σχετικά του άρθρα. Συνοπτικά η δημιουργία ενός ολοκληρωμένου συστήματος διαχείρισης της ασφάλειας των πληροφοριών (ΣΔΑΠ | Information Security Management System, ISMS), όπως προτείνεται από το πρότυπο ISO 27001, επιτρέπει στους οργανισμούς που επεξεργάζονται δεδομένα προσωπικού χαρακτήρα, να αποδεικνύουν ότι οι κίνδυνοι για τα προσωπικά δεδομένα επανεξετάζονται (άρθρα 32.1(δ), 32.2), και οι σχετικές διαδικασίες ενημερώνονται και βελτιώνονται συνεχώς. Ένα εδραιωμένο ΣΔΑΠ είναι το ιδανικό πλαίσιο για την διαχείριση των κινδύνων για όλα τα περιουσιακά στοιχεία της επιχείρησης, συμπεριλαμβανομένων των ΠΔ και μπορεί να παρέχει την συνεχή διαβεβαίωση ότι ο οργανισμός λαμβάνει σοβαρά υπόψη τις προδιαγραφές ασφάλειας ISO 27001 αλλά και του ΓΚΠΔ (άρθρο 32). Συμπερασματικά η συμμόρφωση με το πρότυπο ISO 27001 μπορεί να λειτουργήσει συμπληρωματικά για την συνολική συμμόρφωση με τον ΓΚΠΔ, διότι ότι οι απαιτήσεις συμμόρφωσης του ΓΚΠΔ επεκτείνονται και στην συμμόρφωση του οργανισμού με της αρχές επεξεργασίας, την εξασφάλιση της άσκησης των δικαιωμάτων των φυσικών προσώπων και την γενικότερη ισορροπία μεταξύ της ελεύθερης κυκλοφορίας των ΠΔ και της προστασίας της ελευθερίας και των δικαιωμάτων των φυσικών προσώπων*». Πηγή: https://www.securitymanager.gr/iso-270001-kai-gdpr/

οποία επιθυμεί να συμμετέχει, έγγραφο στο οποίο ο πελάτης δηλώνει αν και για ποιους σκοπούς επιθυμεί την χρήση των δεδομένων του, εμφανής και εύκολος τρόπος ανάκλησης συναίνεσης επεξεργασίας τόσο στο φυσικό όσο και στο επιγραμμικό περιβάλλον, κ.α.

3. ΠΟΛΙΤΙΚΗ ΣΥΓΚΑΤΑΘΕΣΗΣ

Ο υπεύθυνος επεξεργασίας θα πρέπει να αναπτύξει την πολιτική που θα ακολουθήσει ως προς την νόμιμη λήψη συγκατάθεσης από τα υποκείμενα για την επεξεργασία των δεδομένων τους είτε σε έντυπη μορφή είτε ηλεκτρονικά μέσω ιστοσελίδας είτε μέσω ηλεκτρονικής αλληλογραφίας.

α. έντυπη συγκατάθεση

Το έντυπο συγκατάθεσης θα πρέπει να έχει το εξής ελάχιστο περιεχόμενο: τους σκοπούς επεξεργασίας, τον χρόνο διατήρησης των δεδομένων, την τυχόν προώθηση των δεδομένων σε τρίτους, την κατάρτιση προφίλ με ξεχωριστά πεδία συναίνεσης για κάθε μία από τις παραπάνω κατηγορίες, ώστε το υποκείμενο να μπορεί δηλώσει ξεχωριστά και ειδικά την βούλησή του. Επιπλέον το έντυπο συναίνεσης θα πρέπει να περιέχει σύνοψη της πολιτικής ιδιωτικότητας και παραπομπή σε άλλο έντυπο ή ιστότοπο για το πλήρες κείμενο, τον τρόπο ανάκλησης της συγκατάθεσης, τα στοιχεία επικοινωνίας του υπεύθυνου επεξεργασίας και του υπευθύνου προστασίας (εάν υπάρχει), καθώς και τις συνέπειες της μη παροχής συγκατάθεσης για έναν ή όλους τους σκοπούς επεξεργασίας. Υπόδειγμα εντύπου συγκατάθεσης παρατίθεται στο Παράρτημα V (σελ.139-140).

β. συγκατάθεση μέσω ιστοσελίδας - cookies

Σύμφωνα με την παράγραφο 3 του άρθρου 5 της Οδηγίας ePrivacy[i] «*Τα κράτη μέλη μεριμνούν ώστε η αποθήκευση πληροφοριών ή η απόκτηση πρόσβασης σε ήδη αποθηκευμένες πληροφορίες στον τερματικό εξοπλισμό συνδρομητή ή χρήστη*

επιτρέπεται μόνον εάν ο συγκεκριμένος συνδρομητής ή χρήστης έχει δώσει την συγκατάθεσή του με βάση σαφείς και εκτενείς πληροφορίες σύμφωνα με την οδηγία 95/46/ΕΚ, μεταξύ άλλων για το σκοπό της επεξεργασίας. Τούτο δεν εμποδίζει οιαδήποτε τεχνικής φύσεως αποθήκευση ή πρόσβαση, αποκλειστικός σκοπός της οποίας είναι η διενέργεια της διαβίβασης μία ς επικοινωνίας μέσω δικτύου ηλεκτρονικών επικοινωνιών ή που είναι απολύτως αναγκαία για να μπορεί ο πάροχος υπηρεσίας της κοινωνίας της πληροφορίας την οποία έχει ζητήσει ρητά ο συνδρομητής ή ο χρήστης να παρέχει την συγκεκριμένη υπηρεσία».

Ο τρόπος αποθήκευσης πληροφοριών στο τερματικό του χρήστη ή απόκτησης πρόσβασης στις ήδη αποθηκευμένες σε αυτό πληροφορίες είναι τα cookies[94] - τεχνολογία την οποία όλες οι ιστοσελίδες και τα ηλεκτρονικά καταστήματα χρησιμοποιούν πλέον cookies καθώς αποτελούν το χρησιμότερο εργαλείο για σκοπούς διαφήμισης και προώθησης.

Κατηγορίες cookies[95]:

Απολύτως απαραίτητα cookies: είναι ουσιαστικής σημασίας για την ορθή από τεχνικής απόψεως λειτουργία του ιστότοπου. καθώς επιτρέπουν τον χρήστη να χρησιμοποιεί τις λειτουργίες του ιστότοπου, όπως πρόσβαση σε ασφαλείς περιοχές ή χρήση του καλαθιού αγοράς. Αυτά τα cookies δεν ταυτοποιούν τον χρήση και χωρίς αυτά, η ομαλή λειτουργία του ιστότοπου δεν είναι δυνατή. Δεν απαιτείται η συναίνεση του χρήστη.

Cookies λειτουργικότητας: έχουν ως αποκλειστικό σκοπό την διευκόλυνση της επικοινωνίας και την απρόσκοπτη παροχή βελτιωμένων online υπηρεσιών την οποία έχει ζητήσει ρητά ο χρήστης ή ο συνδρομητής, καθώς επιτρέπουν στον ιστότοπο να θυμάται προτιμήσεις όπως το όνομα χρήστη και το συνθηματικό. Δεν παρακολουθούν την δραστηριότητα των επισκεπτών σε άλλους ιστοτόπους και η

[94] Μικρά αρχεία κειμένου τα οποία αποθηκεύονται από τον Διακομιστή (server) μίας ιστοσελίδας στον σκληρό δίσκο του υπολογιστή ή άλλης ηλεκτρονικής συσκευής κατά την πλοήγησή του στο διαδίκτυο.

[95] Τα cookies επίσης διακρίνονται και με βάση τον χρόνο ζωής τους σε session cookies (cookies συνεδρίας) τα οποία αποθηκεύονται στην συσκευή για όσο διάστημα είναι ανοικτός ο περιηγητής (browser) και διαγράφονται με το κλείσιμό του –δεν θεωρούνται επεμβατικά – και τα persistent cookies (επίμονα cookies) τα οποία διατηρούνται αποθηκευμένα στην συσκευή ακόμα και μετά το κλείσιμο της ιστοσελίδας αλλά και του περιηγητή.

απενεργοποίησή τους μπορεί να επηρεάσει την απόδοση της ιστοσελίδας.

Cookies επιδόσεων και επισκεψιμότητας (web analytics): έχουν ως σκοπό την συλλογή στατιστικών ανώνυμων πληροφοριών σχετικά με τον τρόπο χρήσης του εκάστοτε ιστότοπου ή ηλεκτρονικής υπηρεσίας, π.χ. τις σελίδες που επισκέπτεται συχνότερα ο χρήστης, την σελίδα προέλευσης της επίσκεψης του χρήστη, τον τύπο του browser και άλλα τεχνικά χαρακτηριστικά της συσκευής του, την τοποθεσία και την γλώσσα του, κ.α. με χρήση εργαλείων από τρίτους παρόχους (third party[96]) όπως το πολύ διαδεδομένο Google Analytics[97].

Cookies για την προβολή εξατομικευμένων διαφημίσεων (third party): έχουν ως στόχο την παρακολούθηση της συμπεριφοράς του χρήστη και την καταγραφή πληροφοριών ως προς τις προτιμήσεις του με σκοπό την προβολή εξατομικευμένων διαφημίσεων με χρήση εργαλείων από τρίτους παρόχους όπως η επίσης διαδεδομένη υπηρεσία της Google DoubleClick[98].

Οι δύο τελευταίες κατηγορίες είναι και οι προβληματικές όσον αφορά την προστασία της ιδιωτικότητας καθώς μπορούν να ταυτοποιήσουν τους χρήστες και να χρησιμοποιηθούν για την κατάρτιση προφίλ· συνεπώς τα εν λόγω cookies εμπίπτουν στην κατηγορία των προσωπικών δεδομένων και η χρήση τους θα πρέπει να συμμορφώνεται με όλο το ρυθμιστικό πλαίσιο του GDPR και ειδικότερα με την υποχρέωση της διαφάνειας, της παροχής ενημέρωσης, της λήψης συγκατάθεσης πριν την εγκατάστασή τους στην συσκευή του χρήστη καθώς και την δυνατότητα ανάκλησης της συναίνεσής του και την ενημέρωση σχετικά με τον τρόπο διαγραφής τους από το σύστημα του χρήστη. Ειδικότερα, ο υπεύθυνος επεξεργασίας θα πρέπει να ενσωματώσει στην αρχική σελίδα του ιστοτόπου του σε ευκρινές σημείο ενημέρωση σχετικά με την χρήση cookies, το είδος των cookies και την δυνατότητα επιλογής του χρήστη ως προς τα ποια cookies επιθυμεί να εγκατασταθούν στην συσκευή του, καθώς και την γενικότερη πολιτική cookies που ακολουθεί η επιχείρηση ενημερώνοντας για τυχόν third party cookies.

[96] Πρόκειται για cookies που χρησιμοποιούνται από τρίτα μέρη, όπως π.χ. κοινωνικά δίκτυα, για να παρακολουθούν τις επισκέψεις των χρηστών από και προς διάφορους ιστότοπους στους οποίους διαφημίζονται· ο διαχειριστής του ιστοτόπου δεν έχει έλεγχο σε αυτά τα cookies τρίτων μερών.
[97] Βλ. περισσότερα, https://marketingplatform.google.com/about/analytics/?hl=el
[98] Βλ. περισσότερα, https://en.wikipedia.org/wiki/DoubleClick

Ενδεδειγμένη μορφή ενημέρωσης και λήψης συγκατάθεσης για την χρήση cookies[99]

γ. συγκατάθεση μέσω ηλεκτρονικής αλληλογραφίας (e-mail)

Το email marketing[100] έχει αναδειχθεί σε μία από τις αποτελεσματικότερες, γρηγορότερες και με χαμηλό κόστος μεθόδους προώθησης προϊόντων και υπηρεσιών καθώς οι πληροφορίες φτάνουν άμεσα σε πολύ μεγάλο κοινό (ανάλογο της λίστας επαφών). Ωστόσο η απόκτηση αυτού του κοινού και η στοχευμένη ανά κατηγορία ατόμων διαφήμιση πρέπει να συμβαδίζει κατ' αρχήν με τις επιταγές της Οδηγίας ePrivacy και σε δεύτερο επίπεδο με τον GDPR σε περιπτώσεις που ζητείται για πρώτη φορά η συγκατάθεση σε επεξεργασία προσωπικών δεδομένων. Ειδικότερα, η οδηγία στο άρθρο 13 ορίζει: 1. *Η χρησιμοποίηση αυτόματων συστημάτων κλήσης και επικοινωνίας χωρίς ανθρώπινη παρέμβαση (συσκευές αυτόματων κλήσεων), τηλεομοιοτυπικών συσκευών (φαξ) ή ηλεκτρονικού ταχυδρομείου για σκοπούς απευθείας εμπορικής προώθησης μπορεί να επιτρέπεται μόνο στην περίπτωση συνδρομητών ή χρηστών οι οποίοι έχουν δώσει εκ των προτέρων την συγκατάθεσή τους.* 2. *Παρά την παράγραφο 1, αν ένα φυσικό ή νομικό πρόσωπο αποκτά από τους πελάτες του στοιχεία επαφής του ηλεκτρονικού*

[99] Πηγή: https://www.greatway.gr/gdpr-kai-cookies-ti-prepei-na-gnorizo-einai-symvati-i-chrisi-ton-cookie-moy/#close-modal

[100] Είδη email marketing: *α) Τα Newsletters, που αποτελούν ενημερωτικά email, τα οποία αποστέλλονται σε συνδρομητές οι οποίοι έχουν ζητήσει να τα λαμβάνουν και συνήθως έχουν ως στόχο το brand awareness. β) Τα emails συναλλαγών ή transactional emails, τα οποία αποστέλλονται ύστερα από συγκεκριμένες ενέργειες πελατών, για παράδειγμα προκειμένου να επιβεβαιωθεί μία συναλλαγή. Ωστόσο, δεδομένου ότι έχουν αρκετά υψηλό Open Rate, συχνά οι marketers τα εκμεταλλεύονται προκειμένου να προωθήσουν τις πωλήσεις. γ) Τα άμεσα emails ή direct emails, τα οποία χρησιμοποιούνται προκειμένου να ενημερώσουν τους πελάτες ή ενδεχόμενους πελάτες για νέα προϊόντα και ειδικές προσφορές.* Πηγή: https://www.greekinternetmarketing.com/blog/web-promotion/email-marketing-οδηγός-και-συμβουλές-για-αρχάριους

ταχυδρομείου τους στο πλαίσιο της πώλησης ενός προϊόντος ή μία ς υπηρεσίας, σύμφωνα με την οδηγία 95/46/ΕΚ, μπορεί να χρησιμοποιεί τα εν λόγω στοιχεία για την απευθείας εμπορική προώθηση των δικών του παρόμοιων προϊόντων ή υπηρεσιών, υπό την προϋπόθεση ότι οι πελάτες του έχουν σαφώς και ευδιάκριτα την ευκαιρία να αντιτάσσονται, δωρεάν και εύκολα, σε αυτή την συλλογή και χρησιμοποίηση ηλεκτρονικών στοιχείων επαφής κατά την στιγμή της συλλογής τους, και τούτο με κάθε μήνυμα, σε περίπτωση που ο χρήστης αρχικά δεν είχε διαφωνήσει με αυτή την χρήση.

Συνεπώς το ισχύον νομικό πλαίσιο, ανεξάρτητα από τον GDPR, δίνει την δυνατότητα στους υπευθύνους επεξεργασίας να διαφημίζουν προϊόντα και υπηρεσίες στους πελάτες τους και χωρίς την προηγούμενη ρητή συγκατάθεσή τους (opt-in), αρκεί: α) να έλαβαν την διεύθυνση ηλεκτρονικού ταχυδρομείου νομίμως στο πλαίσιο πώλησης ή άλλης παρόμοιας συναλλαγής (soft opt-in), β) να παρείχαν σαφή ενημέρωση κατά την στιγμή συλλογής του email ότι θα το χρησιμοποιήσουν για εμπορική προώθηση (π.χ. αποστολή newsletter, προσφορών, κτλ), γ) να διαφημίζουν παρόμοια προϊόντα και δ) να δίνουν την δυνατότητα εύκολης και χωρίς κόστος διαγραφής σε κάθε μήνυμα[101].

4. ΤΗΡΗΣΗ ΑΡΧΕΙΟΥ ΔΡΑΣΤΗΡΙΟΤΗΤΩΝ

Στην συνέχεια θα πρέπει να καταρτιστεί και το αρχείο δραστηριοτήτων (data inventory) που προβλέπεται στο άρθρο 30 – με την εξαίρεση που τίθεται στην παρ. 5 –[102] προκειμένου να υπάρχει ορθή διαχείριση επί των υφιστάμενων και νέων δεδομένων, το οποίο στην ουσία θα υλοποιεί και την πολιτική ιδιωτικότητας της επιχείρησης.

Η Κυπριακή Αρχή Προστασίας Προσωπικών Δεδομένων έχει ετοιμάσει ένα

[101] Βλ. περισσότερα, *Γιατί η αποστολή email «συγκατάθεσης» για τον GDPR είναι λάθος;* https://www.lawspot.gr/nomika-nea/giati-i-apostoli-email-sygkatathesis-gia-ton-gdpr-einai-lathos

[102] βλ. παραπάνω σελ.41 και βλέπε περισσότερα, ARTICLE 29 DATA PROTECTION WORKING PARTY, ***WORKING PARTY POSITION PAPER on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR*.**

υπόδειγμα αρχείο δραστηριοτήτων (ΠΑΡΑΡΤΗΜΑ V – σελ. 138) με οδηγίες συμπλήρωσής του και προτρέπει στην τήρησή του όχι μόνο για την εκπλήρωση των υποχρεώσεων του Κανονισμού και την απόδειξη συμμόρφωσης, αλλά και ως εργαλείο εσωτερικής (αναδι)οργάνωσης· ειδικότερα, το προτεινόμενο αρχείο δραστηριοτήτων περιλαμβάνει τις εξής απαιτούμενες από τον Κανονισμό πληροφορίες:

- Την περιγραφή της κάθε δραστηριότητας του οργανισμού
- Αν η δραστηριότητα είναι κύρια ή παρεπόμενη
- Την νομική βάση της επεξεργασίας
- Τα στοιχεία του υπεύθυνου ή/και του εκτελούντος την επεξεργασία
- Τον σκοπό της επεξεργασίας
- Τις κατηγορίες των υποκειμένων των δεδομένων
- Τις κατηγορίες των προσωπικών δεδομένων
- Τις κατηγορίες των αποδεκτών
- Την διαβίβαση σε τρίτες χώρα/ διεθνή οργανισμό
- Την διαγραφή των δεδομένων
- Τα τεχνικά και οργανωτικά μέτρα ασφάλειας

Ως προς το ποιος είναι υπεύθυνος για την συμπλήρωση και την ενημέρωση του αρχείου δραστηριοτήτων, η Κυπριακή ΑΠΠΔ λέει χαρακτηριστικά: *«την ευθύνη τήρησης του Αρχείου έχουν κατά περίπτωση, ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία ή οι τυχόν εκπρόσωποί τους. Ωστόσο, μπορούν να αναθέσουν αυτό το καθήκον σε κάποιο υπάλληλό τους ή σε κάποιο εξωτερικό ειδικό. Αν ο οργανισμός έχει υποχρέωση να ορίσει Υπεύθυνο Προστασίας Δεδομένων συστήνεται όπως ο Πίνακας συμπληρωθεί από τον ΥΠΔ. Σε κάθε περίπτωση, το πρόσωπο που θα αναλάβει αυτό το καθήκον πρέπει να έχει ολοκληρωμένη εικόνα για όλες τις δραστηριότητες του οργανισμού. Αν είναι υπάλληλος του οργανισμού, συστήνεται να είναι υψηλόβαθμο παρά χαμηλόβαθμο στέλεχος, αφού θα πρέπει να έχει συνεχή επαφή με την διεύθυνση και πρόσβαση σε όλα τα τμήματα του οργανισμού, ώστε να καταγράψει όλες τις πράξεις επεξεργασίας προσωπικών δεδομένων. Αν είναι εξωτερικός συνεργάτης, ο*

οργανισμός πρέπει να του παράσχει τις απαραίτητες διευκολύνσεις για την σωστή συμπλήρωση του Πίνακα. Για μη σωστή συμπλήρωση του Πίνακα μπορεί να επιβληθεί διοικητική κύρωση (Άρθρο 58) σε ένα οργανισμό, ή διοικητικό πρόστιμο (Άρθρο 83). Αυτά, επιβάλλονται στον οργανισμό και όχι, στο πρόσωπο που συμπλήρωσε τον Πίνακα. Το πρόσωπο που θα συμπληρώσει τον Πίνακα δεν χρειάζεται κατ' ανάγκη να είναι νομικός ή τεχνικός πληροφορικής. Όμως, πρέπει να έχει γνώση του Κανονισμού και όλων των νομοθεσιών που εφαρμόζει ο οργανισμός ή που ρυθμίζουν τον τομέα στον οποίο δραστηριοποιείται, καθώς και στοιχειώδεις τουλάχιστο γνώσεις πληροφορικής».[103]

Τέλος, πρέπει να σημειωθεί ότι η τήρηση του αρχείου είναι μία συνεχής διαδικασία αφού, όταν διαφοροποιείται ή αλλάζει μία υφιστάμενη δραστηριότητα επεξεργασίας ή προστίθεται μία καινούργια, το Αρχείο πρέπει να επικαιροποιείται και αναλόγως, εάν χρειάζεται, να αναπροσαρμόζεται και η πολιτική ιδιωτικότητας.

5. ΑΝΑΛΥΣΗ ΚΙΝΔΥΝΟΥ & ΕΚΘΕΣΗ ΕΚΤΙΜΗΣΗΣ ΑΝΤΙΚΤΥΠΟΥ (DPIA)

Σύμφωνα με το άρθρο 35 παρ. 1 του Κανονισμού ο υπεύθυνος επεξεργασίας υποχρεούται να εκπονήσει εκτίμηση αντικτύπου για τις πράξεις επεξεργασίας που ενεργεί [όπως αυτές χαρτογραφήθηκαν με την ανωτέρω περιγραφείσα διαδικασία] και οι οποίες ενδέχεται να επιφέρουν υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων με τους όρους και τις προϋποθέσεις που αναλύθηκαν στο Πρώτο Μέρος της Εργασίας για την Εκπόνηση της Εκτίμησης Αντικτύπου. Η διαδικασία εκπόνησης μία ς ανάλυσης εκτίμησης επικινδυνότητας και αντικτύπου έχει 3 στάδια: α) εκτίμηση αντικτύπου σε σχέση με τις δραστηριότητες επεξεργασίας που ενεργεί η επιχείρηση, β) εκτίμηση πιθανότητας επέλευσης κινδύνων και γ) συνολική εκτίμηση κινδύνου.

Σε πρακτικό επίπεδο, ο CNIL και ο ENISA έχουν κατηγοριοποιήσει τους βαθμούς κινδύνου ώστε να μπορέσει ένας υπεύθυνος επεξεργασίας να εντάξει στην

[103] Βλ. περισσότερα: *ΟΔΗΓΟΣ ΣΥΜΠΛΗΡΩΣΗΣ ΑΡΧΕΙΟΥ ΔΡΑΣΤΗΡΙΟΤΗΤΩΝ ΕΠΕΞΕΡΓΑΣΙΑΣ,* ΓΡΑΦΕΙΟ ΕΠΙΤΡΟΠΟΥ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ.

αντίστοιχη κατηγορία τις ενδεχόμενες συνέπειες των πράξεων επεξεργασίας που ενεργεί και στην συνέχεια να λάβει και τα κατάλληλα μέτρα ασφαλείας:

ΕΠΙΠΕΔΟ ΚΙΝΔΥΔΟΥ	ΠΕΡΙΓΡΑΦΗ
ΧΑΜΗΛΟ	Τα φυσικά πρόσωπα ενδέχεται να συναντήσουν κάποιες ασήμαντες δυσκολίες, τις οποίες μπορούν να ξεπεράσουν χωρίς ιδιαίτερη προσπάθεια (π.χ. απώλεια χρόνου για να εισάγουν εκ νέου τα στοιχεία τους, εκνευρισμός, κ.τ.λ.)
ΜΕΤΡΙΟ	Τα φυσικά πρόσωπα μπορεί να συναντήσουν σημαντικές δυσκολίες τις οποίες θα μπορέσουν να ξεπεράσουν με κάποια προσπάθεια (π.χ. επιπλέον κόστος, άρνηση πρόσβασης σε επαγγελματικές υπηρεσίες, φόβος, στρες, κ.τ.λ.)
ΥΨΗΛΟ	Τα φυσικά πρόσωπα μπορεί να συναντήσουν σημαντικές επιπτώσεις, τις οποίες θα μπορέσουν να ξεπεράσουν με μεγάλη προσπάθεια (υπεξαίρεση πόρων, στιγματισμός σε οικονομικά ιδρύματα, περιουσιακή βλάβη, απώλεια εργασίας, κλήτευση, χειροτέρευση υγείας, κ.τ.λ.)
ΠΟΛΥ ΥΨΗΛΟ	Τα φυσικά πρόσωπα μπορεί να συναντήσουν σοβαρές, ακόμα και μη αναστρέψιμες συνέπειες, τις οποίες μπορεί να μην μπορέσουν να ξεπεράσουν (αδυναμία για εργασία, μακροχρόνιες ψυχολογικές ή σωματικές ασθένειες, θάνατος, κ.τ.λ.)

Πίνακας 1: Επίπεδο Κινδύνου

Όπως είναι εμφανές το επίπεδο του κινδύνου είναι άρρηκτα συνδεδεμένο με την βαρύτητα των συνεπειών που θα επιφέρει μία ενδεχόμενη παραβίαση ασφαλείας. Επιβοηθητικά για τους υπεύθυνους επεξεργασίας, ο ENISA προτείνει να ληφθούν υπ' όψιν οι κάτωθι παράμετροι για την εκτίμηση του κινδύνου:

- Το είδος των προσωπικών δεδομένων (απλά – ευαίσθητα)

- Η κρισιμότητα των πράξεων επεξεργασίας - ενδεχόμενη κατάρτιση προφίλ ή παρακολούθηση των ιδιωτών, ειδικότερα εάν γίνεται σε μεγάλη κλίμακα
- Τομέας δραστηριοποίησης του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία (π.χ. μεγαλύτερος κίνδυνος από παραβίαση επισυμβείσα σε αρχεία κλινικής απ' ό,τι σε πελατολόγιο βιβλιοπωλείου)
- Ειδικά χαρακτηριστικά των υποκειμένων των δεδομένων (π.χ. μειονότητες, ευπαθείς ομάδες, πολιτικά πρόσωπα)

Για να βοηθήσει τις επιχειρήσεις – και ειδικά τις μικρομεσαίες – στην εκτίμηση του αντικτύπου ο ENISA έχει συντάξει ένα ερωτηματολόγιο το οποίο αφορά σε κάθε μία από τις τρεις βασικές αρχές της ασφάλειας πληροφοριών, δηλαδή στην εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα:

ΕΚΤΙΜΗΣΗ	**ΕΠΙΠΕΔΟ ΚΙΝΔΥΝΟΥ**
Αναλογιστείτε τις συνέπειες που θα είχε μία χωρίς εξουσιοδότηση πρόσβαση - γνωστοποίηση (παραβίαση εμπιστευτικότητας) στα προσωπικά δεδομένα για ένα φυσικό πρόσωπο **Παραδείγματα:** • **Απώλεια εγγράφου ή λάπτοπ** • **Απόρριψη μηχανημάτων χωρίς την καταστροφή των προσωπικών δεδομένων που περιέχουν** • **Δημοσίευση προσωπικών δεδομένων σε μη εξουσιοδοτημένους παραλήπτες** • **Πρόσβαση χρηστών σε λογαριασμούς άλλων χρηστών σε online υπηρεσία.** • **Κλοπή CD με αρχείο προσωπικών δεδομένων από τις εγκαταστάσεις της επιχείρησης** • **Σφάλμα σε ιστοσελίδα επιτρέπει την πρόσβαση σε απόρρητες πληροφορίες εγγεγραμμένων χρηστών**	☐ Χαμηλό ☐ Μέτριο ☐ Υψηλό ☐ Πολύ Υψηλό

Αναλογιστείτε τις συνέπειες που θα είχε μία χωρίς εξουσιοδότηση μεταβολή (παραβίαση ακεραιότητας) στα προσωπικά δεδομένα για ένα φυσικό πρόσωπο **Παραδείγματα:** • **Ένα αρχείο που είναι απαραίτητο για την παροχή online υπηρεσίας έχει μεταβληθεί με συνέπεια το φυσικό πρόσωπο να μπορεί να εξυπηρετηθεί μόνο με συμβατικό τρόπο** • **Ένα αρχείο που είναι σημαντικό για την ακρίβεια του διαδικτυακού ιατρικού φακέλου ενός ατόμου έχει αλλαχθεί.**	☐ Χαμηλό ☐ Μέτριο ☐ Υψηλό ☐ Πολύ Υψηλό
Αναλογιστείτε τις συνέπειες που θα είχε μία χωρίς εξουσιοδότηση καταστροφή ή απώλεια (παραβίαση διαθεσιμότητας) των προσωπικών δεδομένων ενός φυσικού προσώπου **Παραδείγματα:** • **Απώλεια αρχείου ή βάσης δεδομένων χωρίς να υπάρχει back-up** • **Μια σημαντική διαδικτυακή υπηρεσία δεν είναι διαθέσιμη και δεν μπορεί να ανακτηθεί άμεσα (π.χ. πλήρης online ιατρικός φάκελος)** • **Αλλοίωση βάσης δεδομένων για την επαναφορά της οποίας απαιτείται χρόνος και κόστος τεχνικής υποστήριξης**	☐ Χαμηλό ☐ Μέτριο ☐ Υψηλό ☐ Πολύ Υψηλό

Πίνακας 2: Ερωτήσεις για την εκτίμηση του κινδύνου

Στην συνέχεια, ο υπεύθυνος επεξεργασίας θα πρέπει να αναλογιστεί τις ενδεχόμενες απειλές και παραβιάσεις που θα μπορούσαν να επισυμβούν, καθώς και την πιθανότητα επέλευσής τους· παραδείγματα πιθανών κινδύνων είναι η επίθεση με κακόβουλο λογισμικό για την απόκτηση πρόσβασης στα προσωπικά

δεδομένα που είναι αποθηκευμένα στο σύστημα, η υποκλοπή από εργαζόμενο αρχείων προσωπικών δεδομένων από το εσωτερικό σύστημα, εξ αμελείας ή εκ δόλου μεταβολή κρίσιμου στοιχείου σε ιατρικό φάκελο ασθενή από εργαζόμενο, κ.α. Συγκεκριμένα, οι κίνδυνοι που πιθανόν να αντιμετωπίσει το πληροφοριακό σύστημα μία ς επιχείρησης αφορούν τα εξής πεδία:

- Τεχνολογικό υλικό και δίκτυο (hardware και software): Το δίκτυο κινδυνεύει τόσο από εξωτερικές απειλές από hackers που θα προσπαθήσουν να αποκτήσουν απομακρυσμένη πρόσβαση σε αυτό, όσο και από εσωτερικούς παράγοντες, όπως κενά ασφαλείας. Επίσης τόσο ο τεχνολογικός εξοπλισμός όσο και οι εφαρμογές και τα προγράμματα που χρησιμοποιεί ο οργανισμός μπορούν να αποτελέσουν πηγή κινδύνου εάν δεν διαθέτουν τις τελευταίες ενημερώσεις, εάν δεν έχουν παραμετροποιηθεί από ειδικό, κ.τλ.

- Εμπλοκή πολλών και διαφορετικών τμημάτων ή προσώπων και έλλειψη αυστηρώς οριοθετημένων επιχειρησιακών διαδικασιών. Κίνδυνο για την ασφάλεια των προσωπικών δεδομένων αποτελεί και η έλλειψη εσωτερικής οργάνωσης και υιοθέτησης ορθών πρακτικών και πολιτικών ως προς την διαχείρισής τους· καθώς παραβιάσεις μπορούν να προκύψουν και από τα ίδια τα στελέχη της επιχείρησης είτε με δόλο είτε τυχαία είτε από ανθρώπινο λάθος.

- Επιχειρηματικός κλάδος και κλίμακα επεξεργασίας: όσο μεγαλύτερη αξία έχει η βάση των προσωπικών δεδομένων για μία επιχείρηση και το ενεργητικό της και όσο μεγαλύτερη μερίδα του πληθυσμού αφορά τόσο περισσότερο ενδιαφέρον μπορεί να έχει για τους πιθανούς επιτιθέμενους η απόκτηση πρόσβασης σε αυτήν.

Στο ΠΑΡΑΡΤΗΜΑ ΙΙΙ (σελ. 130) παρουσιάζεται ένα ερωτηματολόγιο που προτείνει ο ENISA στους υπευθύνους επεξεργασίας προκειμένου να προσδιορίσουν το είδος και την πιθανότητα επέλευσης πιθανών κινδύνων καθώς και την μεθοδολογία για την τελική εκτίμηση του κινδύνου η οποία και θα καθορίσει την ανάγκη εκπόνησης εκτίμησης αντικτύπου.

6. ΕΝΣΩΜΑΤΩΣΗ ΜΕΤΡΩΝ ΑΣΦΑΛΕΙΑΣ ΣΤΗΝ ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΤΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Μετά την εκτίμηση του επιπέδου κινδύνου, ο οργανισμός μπορεί να προχωρήσει στην υλοποίηση της πολιτικής ιδιωτικότητας και στην λήψη των κατάλληλων μέτρων ασφαλείας για την αποτελεσματική προστασία των προσωπικών δεδομένων. Δύο είναι τα κύρια είδη μέτρων ασφαλείας: τα οργανωτικά και τα τεχνικά, αμφότερα εξίσου σημαντικά. Παρακάτω παρουσιάζονται τα προτεινόμενα (και) από τον ENISA μέτρα ασφαλείας αναλόγως με το εκτιμώμενο επίπεδο κινδύνου.

Ι. ΟΡΓΑΝΩΤΙΚΑ ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ

Ι.1. ΔΙΑΧΕΙΡΙΣΗ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ (security management)

Ι.1.1. ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ & ΣΧΕΔΙΟ ΑΣΦΑΛΕΙΑΣ

Η πολιτική ασφαλείας (security policy) αποτελεί ένα υψηλών προδιαγραφών έγγραφο στο οποίο τίθενται οι βασικές αρχές για την ασφάλεια και την προστασία των συστημάτων, των δικτύων και των δεδομένων (συμπεριλαμβανομένων των προσωπικών) του οργανισμού και το οποίο αποδεικνύει την γενικότερη δέσμευση και προσέγγιση της διοίκησης του οργανισμού προς την ασφάλεια και την προστασία της ιδιωτικότητας. Συνιστά την θεωρητική βάση για την υλοποίηση των επιταγών των άρθρων 32 και 24 του Κανονισμού. Ειδικότερα, θα πρέπει να περιλαμβάνει κατ’ ελάχιστο: α) τις βασικές αρχές ασφαλείας που ακολουθεί ο οργανισμός σε όλες τις επιχειρησιακές του διαδικασίες σε ολόκληρο τον κύκλο ζωής του πληροφοριακού συστήματος (από την συλλογή των δεδομένων μέχρι την καταστροφή τους), β) τα αγαθά (πόροι υλικοί ή άυλοι) που χρήζουν προστασίας, γ) την οργανωτική δομή αρμοδιοτήτων και καθηκόντων των υπαλλήλων καθ’ όλη την πορεία της επεξεργασίας, δ) την διαδικασία ανάθεσης μέρους ή ολόκληρης της επεξεργασίας σε εκτελούντες και ε) την διαδικασία εσωτερικών ελέγχων της ορθής και αποτελεσματικής υλοποίησης της πολιτικής ασφαλείας μέσω των εφαρμοζόμενων μέτρων ασφαλείας και την διαδικασία αναθεώρησής της.

Το σχέδιο ασφαλείας (security plan) αποτελεί το αναγκαίο συμπλήρωμα της πολιτικής ασφαλείας· συντίθεται από την πολιτική ασφαλείας και από τα τεχνικά και οργανωτικά μέτρα που επιλέγει ο υπεύθυνος ασφαλείας να εφαρμόσει για την υλοποίηση αυτής. Ειδικότερα, το σχέδιο ασφαλείας περιλαμβάνει κατ' ελάχιστο: α) την περιγραφή των πληροφοριακών συστημάτων του οργανισμού, β) τα οργανωτικά μέτρα ασφαλείας, γ) τα τεχνικά μέτρα ασφαλείας, δ) τα μέτρα φυσικής ασφάλειας και ε) τις διαδικασίες εσωτερικών ελέγχων για την αποτελεσματικότητα των υιοθετούμενων μέτρων ασφαλείας και την ανάγκη αναθεώρησής τους σύμφωνα με τις τελευταίες τεχνολογικές εξελίξεις.

Ι.1.2. ΔΙΑΧΕΙΡΙΣΗ ΠΟΡΩΝ ΣΥΣΤΗΜΑΤΟΣ (asset management)

Η ορθή διαχείριση της τεχνολογικής υποδομής και των δικτύων σε συνδυασμό με την χαρτογράφηση της ροής των δεδομένων παίζουν καίριο ρόλο στην διατήρηση της ασφάλειας των προσωπικών δεδομένων καθώς υποδεικνύουν τα μέσα τα οποία χρησιμοποιεί ο οργανισμός για την διεκπεραίωση της επεξεργασίας των προσωπικών και τα οποία χρήζουν προστασίας.

Στην πράξη:

- Ο οργανισμός θα πρέπει να διατηρεί επικαιροποιημένο κατάλογο όλων των πόρων που χρησιμοποιεί για την επεξεργασία προσωπικών δεδομένων (συσκευές, λογισμικό και δίκτυα) ο οποίος θα πρέπει να περιλαμβάνει τουλάχιστον το είδος της υποδομής (π.χ. server, σταθμός εργασίας) και την τοποθεσία (φυσική ή ηλεκτρονική).
- Καταγραφή οποιασδήποτε ενέργειας μεταφοράς προσωπικών δεδομένων σε φορητές συσκευές από υπαλλήλους του οργανισμού (π.χ. με σκληρό δίσκο, USB, ή laptop) κατόπιν έγκρισης του υπευθύνου επεξεργασίας ή του υπεύθυνου ασφαλείας.
- Ύπαρξη συγκεκριμένου σχεδίου οργάνωσης και αρχειοθέτησης του φυσικού αρχείου του οργανισμού (φυσικοί φάκελοι) και προκαθορισμένα δικαιώματα πρόσβασης σε αυτό.
- Τα πληροφοριακά αγαθά θα πρέπει να κατηγοριοποιούνται με βάση το

είδος και την κρισιμότητά τους και βάσει αυτής της διαβάθμισης να παρέχεται δικαίωμα πρόσβασης ή/και διαχείρισης σε συγκεκριμένους υπαλλήλους.

- Διαχείριση και αναβάθμιση της τεχνολογικής υποδομής σε ετήσια βάση.

Ι.1.3. ΔΙΑΧΕΙΡΙΣΗ ΑΛΛΑΓΩΝ ΣΥΣΤΗΜΑΤΟΣ (change management)

Η διαχείριση των αλλαγών συστήματος στοχεύει στην κεντρική εποπτεία όλων των αλλαγών που συμβαίνουν στο πληροφοριακό σύστημα της επιχείρησης και αποτελεί σημαντικό μέτρο ασφαλείας καθώς μία αλλαγή μπορεί να οδηγήσει σε καταστροφή, αλλοίωση ή παράνομη πρόσβαση σε αρχείο προσωπικών δεδομένων.

Στην πράξη:

- Όλες οι αλλαγές στο πληροφοριακό σύστημα πρέπει να καταγράφονται και να παρακολουθούνται από τον Υπεύθυνο Ασφαλείας.
- Η inhouse ανάπτυξη λογισμικού πρέπει να διενεργείται σε ειδικό προγραμματιστικό περιβάλλον που δεν συνδέεται με το γενικότερο πληροφοριακό σύστημα και να μην χρησιμοποιούνται αληθινά προσωπικά δεδομένα για την δοκιμή του.
- Τήρηση γραπτής πολιτικής για την διαχείριση των αλλαγών συστήματος όπου θα καθορίζονται οι υπάλληλοι που έχουν δικαίωμα διενέργειας αλλαγών καθώς οι διαδικασίες ενσωμάτωσης αυτών στο σύστημα.

Ι.2. ΔΙΑΧΕΙΡΙΣΗ ΑΝΘΡΩΠΙΝΟΥ ΔΥΝΑΜΙΚΟΥ (human resources)

Ι.2.1. ΡΟΛΟΙ & ΑΡΜΟΔΙΟΤΗΤΕΣ

Σύμφωνα με την παρ. 4 του αρθ. 32 του Κανονισμού «*Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία λαμβάνουν μέτρα ώστε να διασφαλίζεται ότι κάθε φυσικό πρόσωπο που ενεργεί υπό την εποπτεία του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία το οποίο έχει πρόσβαση σε δεδομένα προσωπικού χαρακτήρα τα επεξεργάζεται μόνο κατ' εντολή*

του υπευθύνου επεξεργασίας, εκτός εάν υποχρεούται προς τούτο από το δίκαιο της Ένωσης ή του κράτους μέλους». Συνεπώς, η εξασφάλιση της προστασίας των προσωπικών δεδομένων από εσωτερικές παραβιάσεις μπορεί να πραγματωθεί με σαφή καθορισμό των ρόλων και αρμοδιοτήτων όλου του προσωπικού.

Στην πράξη:

- Η ανάθεση αρμοδιοτήτων και καθηκόντων στο προσωπικό θα πρέπει να είναι σύμφωνη με τον ρόλο που έχει ο κάθε υπάλληλος στην επιχείρηση και θα πρέπει να γίνεται εγγράφως.
- Πρόβλεψη σαφούς διαδικασίας για την ανάκληση δικαιωμάτων και εξουσιοδοτήσεων σε περίπτωση εσωτερικής αναδιοργάνωσης, λήξης σύμβασης ή απόλυσης και ειδικότερα μέτρα προστασίας όπως: επιστροφή οποιουδήποτε εξοπλισμού της επιχείρησης είχε παραχωρηθεί στον υπάλληλο, κατάργηση όλων των λογαριασμών και των αντίστοιχων κωδικών του υπαλλήλου και μη επαναχρησιμοποίησή τους.
- Ρητή ανάθεση αρμοδιοτήτων σε συγκεκριμένους υπαλλήλους σχετικών με την διενέργεια εργασιών ασφαλείας, καθώς και διορισμός του υπευθύνου ασφαλείας, οι οποίοι πρέπει να διαθέτουν αποδεδειγμένες γνώσεις και εμπειρία σχετικά με την ασφάλεια πληροφοριακών συστημάτων. Ο ορισμός του Υπευθύνου Ασφαλείας (ή της ομάδας ασφαλείας) καθώς και ο καθορισμός των αρμοδιοτήτων του πρέπει να γίνει εγγράφως. Τα καθήκοντά του πρέπει κατ' ελάχιστον να περιλαμβάνουν την επίβλεψη της εφαρμογής της πολιτικής ασφαλείας και τον έλεγχο των μέτρων ασφαλείας.
- Σύμφωνα με το άρθρο 37 ο οργανισμός μπορεί ή υποχρεούται να ορίσει Υπεύθυνο Προστασίας Προσωπικών Δεδομένων και τα καθήκοντά του περιλαμβάνουν κατ' ελάχιστο την επίβλεψη της συμμόρφωσης της επιχείρησης με τον Κανονισμό, την παροχή συμβουλών για την ορθή εκπλήρωση των υποχρεώσεων του Κανονισμού και την διενέργεια της επικοινωνίας με τα υποκείμενα και τις εποπτικές αρχές.
- Διαχωρισμός τυχόν συγκρουόμενων αρμοδιοτήτων του Υπευθύνου Ασφαλείας και του Υπευθύνου Προστασίας ώστε να ελαχιστοποιηθούν οι πιθανότητες για μη εξουσιοδοτημένη ή μη ηθελημένη μεταβολή ή

κατάχρηση προσωπικών δεδομένων.

Ι.2.2. ΕΛΕΓΧΟΣ ΠΡΟΣΒΑΣΗΣ (access control policy)

Συμπληρωματικά με το προηγούμενο μέτρο ασφαλείας του σαφούς καθορισμού ρόλων, είναι εξίσου σημαντικός και ο καθορισμός των δικαιωμάτων πρόσβασης στο σύστημα επεξεργασίας προσωπικών δεδομένων. Ο έλεγχος πρόσβασης στο οργανωτικό επίπεδο σε συνδυασμό με τους αντίστοιχους μηχανισμούς ελέγχου πρόσβασης[104] εκπληρώνουν και την βασική αρχή του Κανονισμού για την ελαχιστοποίηση των δεδομένων, με την έννοια ότι οι υπάλληλοι έχουν πρόσβαση μόνο σε όσα δεδομένα είναι απαραίτητα για την εκτέλεση των καθηκόντων τους.

Στην πράξη:

- Θα πρέπει να δοθούν συγκεκριμένα δικαιώματα πρόσβασης ανάλογα με τον ρόλο και τις αρμοδιότητες κάθε υπαλλήλου ώστε αυτός να μπορεί να γνωρίζει μόνο τα προσωπικά δεδομένα που είναι απαραίτητα για την εκτέλεση των καθηκόντων του.
- Η πολιτική ελέγχου πρόσβασης θα πρέπει να είναι λεπτομερής και να τηρείται γραπτώς· θα πρέπει να προσδιορίζονται ρητά τα δικαιώματα και οι περιορισμοί πρόσβασης κάθε κατηγορίας χρηστών-υπαλλήλων που ασχολούνται με την επεξεργασία των προσωπικών δεδομένων.
- Οι χρήστες-υπάλληλοι με αυξημένα ή/και συγκεντρωτικά δικαιώματα πρόσβασης θα πρέπει να είναι σαφώς καθορισμένοι και περιορισμένοι σε αριθμό.

Ι.2.3. ΡΗΤΡΑ ΕΧΕΜΥΘΕΙΑΣ ΤΟΥ ΠΡΟΣΩΠΙΚΟΥ (confidentiality)

Σε συμμόρφωση προς την προαναφερθείσα παράγραφο 4 του άρθρου 32 αλλά και την παράγραφο 1 του άρθρου 5, ο υπεύθυνος επεξεργασίας πρέπει να διασφαλίζει ότι οι υπάλληλοί του έχουν τα απαραίτητα επαγγελματικά προσόντα όχι μόνο από πλευράς τεχνικών γνώσεων αλλά και από πλευράς προσωπικής ακεραιότητας ως προς την τήρηση του απορρήτου.

[104] Βλ. παρακάτω, σελ. 104.

Στην πράξη:

- Ο οργανισμός πρέπει να εξασφαλίσει ότι όλοι οι εργαζόμενοι αντιλαμβάνονται τις νομικές και τεχνικές υποχρεώσεις που αναλαμβάνουν σχετικά με την επεξεργασία των προσωπικών δεδομένων. Η υποχρέωση τήρησης του επαγγελματικού απορρήτου θα πρέπει να αποσαφηνίζεται πλήρως κατά την πρόσληψη ή την εκπαίδευση.
- Πριν αναλάβουν καθήκοντα, οι υπάλληλοι θα πρέπει να διαβάσουν και να αποδεχθούν την πολιτική ασφαλείας του οργανισμού και να υπογράψουν σχετικό συμφωνητικό εχεμύθειας και τήρησης απορρήτου.
- Υπάλληλοι του οργανισμού που εμπλέκονται σε ενέργειες επεξεργασίας με υψηλό βαθμό κινδύνου θα πρέπει να δεσμεύονται από εξειδικευμένες ρήτρες εχεμύθειας (είτε στην σύμβαση πρόσληψης είτε με πράξη άλλης νομικής μορφής).

Ι.2.4. ΕΚΠΑΙΔΕΥΣΗ

Η εκπαίδευση του προσωπικού όσον αφορά τις διαδικασίες ασφαλείας και προστασίας προσωπικών δεδομένων είναι άκρως σημαντική για την ορθή υλοποίηση των υιοθετούμενων οργανωτικών και τεχνικών μέτρων ασφαλείας, διαφορετικά η πολιτική ασφαλείας θα καθίστατο γράμμα κενό.

Στην πράξη:

- Ο οργανισμός πρέπει να εξασφαλίσει ότι όλοι οι εργαζόμενοι είναι επαρκώς ενημερωμένοι για όλους τους ελέγχους ασφαλείας του πληροφοριακού συστήματος που θα συναντούν καθημερινά στην εργασία τους. Επιπλέον οι εργαζόμενοι που επεξεργάζονται και προσωπικά δεδομένα θα πρέπει να εκπαιδεύονται-ενημερώνονται τακτικά για τυχόν νέες προδιαγραφές προστασίας και νομικές υποχρεώσεις στον τομέα της προστασίας της ιδιωτικότητας.
- Χρήσιμο θα ήταν να βρίσκονται αναρτημένες βασικές οδηγίες ασφαλείας σε κάποιο εσωτερικό δικτυακό portal ή και εγγράφως, όπως οδηγίες για χρήση

μη προβλέψιμων κωδικών πρόσβασης, ορθή χρήση εταιρικών e-mail, ορθή και αποδεκτή χρήση φορητών μέσων αποθήκευσης, διαδικασία αναφοράς περιστατικών ασφαλείας, κ.α.

- Ο οργανισμός πρέπει να διοργανώνει τακτικά εκπαιδευτικά προγράμματα για τους υπαλλήλους, συμπεριλαμβανομένων ειδικών σεμιναρίων για τους νέο-προσλαμβανόμενους.
- εξειδικευμένη εκπαίδευση θα πρέπει να παρέχεται στον Υπεύθυνο Ασφαλείας και στην ομάδα του προκειμένου να είναι ενημερωμένοι για τις τελευταίες εξελίξεις στον χώρο της ασφάλειας πληροφοριακών συστημάτων τόσο από άποψη νέων μορφών επιθέσεων όσο και από άποψη νέων μέτρων ασφαλείας. Το ίδιο ισχύει και για τον DPO ως προς την περαιτέρω κατάρτισή του σε θέματα που άπτονται των αρμοδιοτήτων του (παρ. 2 άρθρο 37).

Ι.2.5. ΕΚΤΕΛΟΥΝΤΕΣ ΤΗΝ ΕΠΕΞΕΡΓΑΣΙΑ

Σύμφωνα με το άρθρο 28, ο υπεύθυνος επεξεργασίας μπορεί να χρησιμοποιεί εκτελούντες για την διενέργεια μέρους ή και του συνόλου της επεξεργασίας εφόσον υπάρχουν οι απαραίτητες εγγυήσεις τεχνικής κατάρτισης αλλά και δέσμευσης στην πολιτική ασφαλείας και προστασίας προσωπικών δεδομένων που ο πρώτος ακολουθεί.

<u>Στην πράξη:</u>

- Σε περίπτωση ανάθεσης της επεξεργασίας σε εκτελούντες (εργολάβους/εξωτερικούς συνεργάτες), αυτή θα πρέπει να γίνει γραπτώς με σύμβαση ή άλλη νομική πράξη η οποία κατ’ αρχήν ορίζει ότι ο εκτελών διεξάγει την επεξεργασία μόνο κατ’ εντολή του υπευθύνου και βαρύνεται με υποχρεώσεις ασφαλείας τουλάχιστον αντίστοιχου βαθμού (αν όχι μεγαλύτερου) με αυτόν που ακολουθεί ο υπεύθυνος στις λοιπές επιχειρησιακές του διαδικασίες.
- Η γραπτή σύμβαση ανάθεσης θα πρέπει να περιλαμβάνει κατ’ ελάχιστο: το είδος των προσωπικών δεδομένων που αναλαμβάνει ο εκτελών, τον σκοπό επεξεργασίας, τις εγκαταστάσεις που θα εκτελείται η επεξεργασία, την

διαδικασία επεξεργασίας, την διαδικασία καταστροφής ή επιστροφής των δεδομένων και των αντιγράφων αυτών μετά την λήξη της σύμβασης, τις εγγυήσεις τεχνογνωσίας και τήρησης ασφάλειας που πρέπει να επιτυγχάνει ο εκτελών.

- Τήρηση καταλόγου με όλους τους εκτελούντες με τους οποίους έχει συμβληθεί ο υπεύθυνος είτε η επεξεργασία γίνεται εντός είτε εκτός των εγκαταστάσεών του.
- Οι εκτελούντες την επεξεργασία θα πρέπει να τηρούν συγκεκριμένες προδιαγραφές αξιοπιστίας και επαγγελματικής κατάρτισης τις οποίες ο υπεύθυνος θα επανεκτιμά τακτικά.
- Οι υπάλληλοι του εκτελούντος την επεξεργασία θα πρέπει να υπογράφουν συμφωνητικό εχεμύθειας και τήρησης απορρήτου.

Ι.3. ΔΙΑΧΕΙΡΙΣΗ ΚΙΝΔΥΝΩΝ & ΕΠΙΧΕΙΡΗΣΙΑΚΗ ΣΥΝΕΧΕΙΑ

Ι.3.1. ΔΙΑΧΕΙΡΙΣΗ ΠΕΡΙΣΤΑΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ (incident response)

Στην περίπτωση που θα επισυμβεί κάποιο περιστατικό ασφαλείας, ο υπεύθυνος επεξεργασίας θα πρέπει να εκτιμήσει εάν αυτό οδηγεί σε «*τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ αδείας κοινολόγηση ή προσπέλαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία*» και αναλόγως να εκπληρώσει τις υποχρεώσεις που απορρέουν από τα άρθρα 33 και 34 για έγκαιρη ενημέρωση της εποπτικής αρχής και των υποκειμένων των δεδομένων. Υποχρέωση γνωστοποίησης περιστατικού ασφαλείας έχει και ο εκτελών προς τον υπεύθυνο επεξεργασίας.

Στην πράξη:

- Εκπόνηση σχεδίου απόκρισης σε περιστατικά ασφαλείας για την άμεση αντιμετώπιση και την όσο το δυνατόν μεγαλύτερη μείωση των συνεπειών ενός συμβάντος παραβίασης. Θα πρέπει να προβλεφθούν διαδικασίες για την διερεύνηση του περιστατικού (χρήση εφαρμογών ελέγχου ασφαλείας), το προσωπικό που θα επιληφθεί, την πλήρη καταγραφή του γεγονότος και

την αναφορά του.

- Τα περιστατικά ασφαλείας πρέπει να αναφέρονται αμελλητί στην διοίκηση από τους αρμόδιους υπαλλήλους τόσο του υπευθύνου όσο και του εκτελούντος την επεξεργασία.
- Πρόβλεψη διαδικασίας υποβολής αναφοράς στην εποπτική Αρχή και γνωστοποίησης στα υποκείμενα των δεδομένων εφόσον κρίνεται απαραίτητο[105].
- Τα περιστατικά ασφαλείας και οι παραβιάσεις προσωπικών δεδομένων θα πρέπει να καταγράφονται λεπτομερώς σε συνδυασμό με τις ενέργειες που τελέστηκαν για την μείωση των συνεπειών. Ειδικότερα, θα πρέπει να καταγραφεί ο χρόνος που τελέστηκε το περιστατικό και ο χρόνος που ήρθε σε γνώση του προσωπικού, το πρόσωπο που το ανέφερε, την κρισιμότητα του περιστατικού και μία πρώτη εκτίμηση των ενδεχόμενων συνεπειών του καθώς και ποιες διαδικασίες διόρθωσης ακολουθήθηκαν.

Ι.3.2. ΣΧΕΔΙΟ ΑΝΑΚΑΜΨΗΣ & ΕΠΙΧΕΙΡΗΣΙΑΚΗ ΣΥΝΕΧΕΙΑ (business continuity)

Προκειμένου να διασφαλιστεί η άμεση και αποτελεσματική ανάκαμψη των πληροφοριακών συστημάτων και της τεχνολογικής υποδομής (επικοινωνία, δίκτυο, διαθεσιμότητα) του οργανισμού σε περιπτώσεις επιθέσεων/εισβολών, φυσικών καταστροφών ή άλλων περιπτώσεων έκτακτης ανάγκης, θα πρέπει να εκπονηθεί Σχέδιο Ανάκαμψης (Recovery and Contingency Plan) όπου θα αναφέρονται οι διαδικασίες και τα τεχνικά μέτρα αποκατάστασης και διατήρησης της επιχειρησιακής λειτουργίας, συνεπώς αποτελεί αναπόσπαστη συνέχεια του σχεδίου ασφαλείας.

Στην πράξη:

- Σχεδιασμός των ενεργειών και διαδικασιών που θα ακολουθηθούν ώστε να εξασφαλιστεί το μέγιστο δυνατόν επίπεδο συνέχειας και διαθεσιμότητας του πληροφοριακού συστήματος σε περίπτωση παραβίασης ή επίθεσης.

[105] Βλ. ανωτέρω, σελ. 46 επ., *Γνωστοποίηση & ανακοίνωση περιστατικών παραβίασης (αρθ.33-34)*.

- Βασικές περιπτώσεις έκτακτης ανάγκης που πρέπει να ληφθούν υπ' όψιν και ήδη με την κατάρτιση του σχεδίου ασφαλείας και την επιλογή τεχνικών μέτρων να προβλεφθούν είναι: κακόβουλο λογισμικό, διακοπή παροχής ηλεκτρονικού ρεύματος, πυρκαγιά, άλλες φυσικές καταστροφές (πλημμύρα, σεισμός, κ.α.),
- Τα προβλεπόμενα μέτρα πρέπει να στοχεύουν στον περιορισμό της ζημιάς και την αποφυγή κλιμάκωσής της, στην εκ των προτέρων ύπαρξη εναλλακτικής τεχνολογικής υποδομής, στην εκπαίδευση και στην ετοιμότητα του προσωπικού να ανταποκρίνεται στις διαδικασίες ανάκαμψης, στην ελαχιστοποίηση του απαιτούμενου χρονικού διαστήματος για επιστροφή στην ομαλή λειτουργία, στην ελαχιστοποίηση των οικονομικών επιπτώσεων.
- Το πλάνο επιχειρησιακής συνέχειας θα πρέπει να είναι λεπτομερές και να περιλαμβάνει σαφείς ενέργειες και αρμοδιότητες, συγκεκριμένα μέλη του προσωπικού που θα κληθούν να τις διεκπεραιώσουν καθώς και την σχετική εκπαίδευσή τους, κατάλογο με προμηθευτές τεχνολογικής υποδομής (συσκευές και λογισμικό), σειρά προτεραιότητας υπηρεσιών που θα πρέπει να καταστούν άμεσα διαθέσιμες τόσο για την εσωτερική λειτουργία της επιχείρησης όσο και για την εξυπηρέτηση πελατών-χρηστών, διαδικασία για τον υπολογισμό της ζημιάς και χρονοδιάγραμμα για την επιστροφή στην ομαλή λειτουργία του οργανισμού αναλόγως του είδους της καταστροφής.
- Πρόβλεψη για εναλλακτικό χώρο τήρησης αντιγράφων ασφαλείας ή ακόμα και συνολικών εγκαταστάσεων αναλόγως του όγκου του οργανισμού και των αποδεκτών χρονικών ορίων μη διαθεσιμότητας των υπηρεσιών.

ΙΙ. ΤΕΧΝΙΚΑ ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ

ΙΙ.1. ΕΛΕΓΧΟΣ ΠΡΟΣΒΑΣΗΣ & ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗ (authentication)

Η υλοποίηση της πολιτικής ασφαλείας ως προς τα δικαιώματα και την εξουσιοδότηση πρόσβασης πραγματώνεται με τον την χρήση ειδικών τεχνικών

πρόσβασης και αυθεντικοποίησης[106].

Στην πράξη:

- Εφαρμογή συστήματος διαχείρισης πρόσβασης για όλους τους εσωτερικούς χρήστες που θέλουν να χρησιμοποιήσουν το πληροφοριακό σύστημα. Πρέπει να γίνει χρήση μηχανισμών οι οποίοι θα εξασφαλίζουν την ορθή ταυτοποίηση και την αυθεντικοποίηση των χρηστών και δεν θα επιτρέπουν την πρόσβαση σε πόρους του συστήματος σε μη εξουσιοδοτημένους χρήστες.
- Ο υπεύθυνος επεξεργασίας πρέπει να τηρεί συγκεκριμένη διαδικασία διαχείρισης των λογαριασμών των χρηστών, οι οποίες να περιλαμβάνουν την δημιουργία, την μεταβολή, την επισκόπηση και την διαγραφή λογαριασμών. Επιπλέον θα πρέπει να αποδοθούν συγκεκριμένοι ρόλοι και εξουσιοδοτήσεις σε κάθε κατηγορία χρηστών ή σε κάθε χρήστη ξεχωριστά.
- Πρέπει να υιοθετηθεί συγκεκριμένος μηχανισμός αυθεντικοποίησης και ταυτοποίησης προκειμένου να επιτραπεί η είσοδος στο σύστημα· κατ' ελάχιστο ένας συνδυασμός ονόματος χρήστη/κωδικού.
- Συνιστάται σε ιδιαίτερα κρίσιμες επεξεργασίες με υψηλή επικινδυνότητα να προτιμώνται μέθοδοι ταυτοποίησης με πολλαπλούς παράγοντες (multifactor authentication), όπως μίας χρήσης κωδικό με sms ή email (one time password - OTP), μικροσυσκευή που παράγει μίας χρήσης κωδικούς ή βιομετρική ταυτότητα μπορούν να αποτελέσουν τον δεύτερο παράγοντα αυθεντικοποίησης σε συνδυασμό με το δίπτυχο του username/password.
- Τήρηση συγκεκριμένης πολιτικής και παροχή οδηγιών στο προσωπικό για την δημιουργία συνθηματικών (password policy)[107]: ελάχιστος αριθμός χαρακτήρων (προτείνονται 8 και πάνω), αποδεκτοί χαρακτήρες –όσο περισσότεροι (πεζά-κεφαλαία-αριθμοί-ειδικοί χαρακτήρες) τόσο μεγαλύτερη η πολυπλοκότητά του –, συχνότητα αλλαγής και μη επαναχρησιμοποίησης καθώς και όριο ανεπιτυχών προσπαθειών σύνδεσης μετά το πέρας του οποίου ο λογαριασμός θα κλειδώνει.

[106] https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/authentication-methods
[107] https://en.wikipedia.org/wiki/Password_policy

- Τα συνθηματικά δεν θα πρέπει να αποθηκεύονται στον server στην πραγματική τους μορφή, αλλά κρυπτογραφημένα-κατακερματισμένα (hashed) χωρίς δυνατότητα ανάκτησής τους.
- Περίπτωση υπολογιστή σε κατάσταση αδράνειας: θα πρέπει να ρυθμιστούν οι υπολογιστές ώστε εάν τεθούν σε κατάσταση αδράνειας ή προφύλαξης οθόνης να απαιτείται εκ νέου η πληκτρολόγηση κωδικού ώστε να αποφευχθεί η μη εξουσιοδοτημένη πρόσβαση σε προσωπικά δεδομένα.

II.2. ΤΗΡΗΣΗ ΑΡΧΕΙΩΝ ΚΑΤΑΓΡΑΦΗΣ (log files)

Η τήρηση αρχείων καταγραφής όλων των ενεργειών που επηρεάζουν το σύστημα –από τους χρήστες, από τους διαχειριστές, από μη εξουσιοδοτημένους τρίτους– αποτελεί καίριο μέτρο ασφαλείας καθώς βάσει αυτών μπορεί να ταυτοποιηθεί πιθανή εσωτερική ή εξωτερική απόπειρα παραβίασης.

Στην πράξη:

- Τα log files αποτελούν τον πυρήνα της ασφάλειας των πληροφοριακών συστημάτων· γι’ αυτό και η ίδια η πρόσβαση σε αυτά πρέπει να καταγράφεται και να γίνεται μόνο από ρητά εξουσιοδοτημένους χρήστες (όπως τον Υπεύθυνο Ασφαλείας και την ομάδα του).
- Αρχεία καταγραφής πρέπει να τηρούνται για κάθε ένα σύστημα/εφαρμογή που χρησιμοποιείται στην επεξεργασία των προσωπικών δεδομένων και θα πρέπει να αφορούν κάθε ενέργεια που πραγματοποιείται επί αυτών – πρόσβαση, αλλαγή, διαγραφή.
- Το ελάχιστο περιεχόμενο των αρχείων καταγραφής πρέπει να αποτελείται από: το αναγνωριστικό του χρήστη που έκανε την ενέργεια, την ημερομηνία και την ώρα της ενέργειας (timestamp), το σύστημα μέσω του οποίου έκανε την ενέργεια (συσκευή, εφαρμογή) και το αποτέλεσμα της ενέργειας. Επίσης πρέπει να καταγράφονται τα αιτήματα εκτύπωσης προσωπικών δεδομένων, οι αλλαγές σε κρίσιμες ρυθμίσεις του συστήματος ή στα δικαιώματα πρόσβασης των χρηστών.

- Η διαγραφή των αρχείων καταγραφής δεν θα πρέπει να επιτρέπεται ή τουλάχιστον να γίνεται με την ταυτόχρονη παρουσία και έγκριση τουλάχιστον 2 ατόμων επιφορτισμένων με διαφορετικούς ρόλους (π.χ. Υπεύθυνος Ασφαλείας και διοικητικός διευθυντής).
- Το σύστημα ελέγχου των αρχείων καταγραφής θα πρέπει να ρυθμιστεί ώστε να δημιουργεί αναφορές σε τακτά χρονικά διαστήματα και να στέλνει ειδοποιήσεις σε περίπτωση πιθανού κινδύνου.

II.3. ΑΣΦΑΛΕΙΑ ΒΑΣΕΩΝ ΔΕΔΟΜΕΝΩΝ (database security)

Η εν λόγω κατηγορία μέτρων ασφαλείας αφορά τα δεδομένα που είναι αποθηκευμένα σε βάση δεδομένων ή σε άλλα παρόμοια συστήματα (συμπεριλαμβανομένων των βάσεων δεδομένων στο cloud) και τα δεδομένα που επεξεργάζεται το προσωπικό με την χρήση συγκεκριμένων σταθμών εργασίας ή συγκεκριμένων συσκευών – διακρίνονται από την κατηγορία δεδομένων που μεταδίδονται μέσω δικτύου ή μέσω συσκευών.

II.3.1. ΑΣΦΑΛΕΙΑ ΔΙΑΚΟΜΙΣΤΩΝ (server security)

Οι διακομιστές και οι βάσεις δεδομένων αποτελούν την ραχοκοκκαλιά των πληροφοριακών συστημάτων που επεξεργάζονται προσωπικά δεδομένα· ως εκ τούτου τα σχετικά μέτρα ασφαλείας πρέπει να είναι ενισχυμένα ώστε να εξασφαλιστεί ένα ασφαλές λειτουργικό και παραγωγικό περιβάλλον για την επεξεργασία.

Στην πράξη:

- Οι βάσεις δεδομένων και οι διακομιστές εφαρμογών θα πρέπει να παραμετροποιηθούν ώστε να «τρέχουν» σε διαφορετικό λογαριασμό με ελάχιστα δικαιώματα παραμετροποίησης του λειτουργικού συστήματος προκειμένου να λειτουργούν σωστά.
- Οι βάσεις δεδομένων και οι διακομιστές πρέπει να επεξεργάζονται μόνο τα προσωπικά δεδομένα που είναι απαραίτητα για να πετύχουν τους στόχους

επεξεργασίας (αρχή της ελαχιστοποίησης δεδομένων).

- Χρήση λογισμικών διαχείρισης και ανίχνευσης εισβολών (intrusion detection and prevention systems[108]) καθώς και λογισμικών ανίχνευσης και διαχείρισης διαρροής δεδομένων (data leakage prevention[109]) τόσο σε επίπεδο δικτύου όσο και σε επίπεδο εφαρμογών.
- Οι υπολογιστές που χρησιμοποιούνται ως servers δεν μπορούν να λειτουργούν και ως σταθμοί εργασίας για το προσωπικό.
- Χρήση μεθόδου ψευδωνυμοποίησης[110] με κάποια από τις εξής τεχνικές:
  - Data Masking: τεχνική κάλυψης η οποία καλύπτει ένα μέρος των δεδομένων με τυχαίους χαρακτήρες ή άλλα δεδομένα. Παράδειγμα: 5500 000 000 0004 ◊ xxxx xxx xxxx 0004
  - Hashing με ή χωρίς την χρήση κλειδιού
  - Tokenization: αντικατάσταση των ευαίσθητων/προσωπικών δεδομένων με μη-ευαίσθητα/προσωπικά τα οποία λέγονται “tokens” και δεν έχουν καμία ιδιαίτερη ή εκμεταλλεύσιμη αξία.
  - Θόλωμα (Blurring): χρήση προσεγγιστικών τιμών των επίμαχων δεδομένων ώστε να καταστήσει αδύνατη την ταυτοποίηση του προσώπου.
- Κρυπτογράφηση του συνόλου ή μέρους των αποθηκευμένων δεδομένων. Προτείνεται: α) η τεχνική της κρυπτογράφησης με δυνατότητα αναζήτησης (searchable encryption) όπου ο χρήστης μπορεί να αναζητήσει μόνο τα

---

[108] «*Το Σύστημα Ανίχνευσης Εισβολής αποτελεί σύστημα παρακολούθησης και ανάλυσης των συμβάντων, τα οποία λαμβάνουν χώρα τόσο στους ίδιους τους ηλεκτρονικούς υπολογιστές όσο και στα δίκτυα υπολογιστών. Στόχος είναι ο εντοπισμός ενδείξεων για πιθανές προσπάθειες εισβολής, κατά τις οποίες συχνά εντοπίζονται ίχνη παραβίασης της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητας των πληροφοριακών πόρων. Οι προσπάθειες παράκαμψης των μηχανισμών ασφαλείας μπορεί να προέρχονται από εξωτερικούς χρήστες, προς το εσωτερικό εταιρικό δίκτυο, στους οποίους δεν επιτρέπεται η πρόσβαση στο υπάρχον πληροφοριακό σύστημα. Επίσης, οι προσπάθειες παράκαμψης πιθανόν να προέρχονται από εσωτερικούς χρήστες, με περιορισμένα δικαιώματα πρόσβασης».* Οι βασικές κατηγορίες είναι τα δικτυακά συστήματα ανίχνευσης (NIDS) - τα οποία αναλύουν την διαδικτυακή ροή δεδομένων προς το σύστημα – και τα host-based συστήματα ανίχνευσης – τα οποία αναλύουν τα καίρια αρχεία του λειτουργικού συστήματος. Πηγή: https://en.wikipedia.org/wiki/Intrusion_detection_system

[109] Εξειδικευμένο λογισμικό που αποτρέπει την διαρροή δεδομένων σε χρήση (data in use), δεδομένων σε κίνηση (data in motion) και δεδομένων σε ακινησία (data at rest).

[110] Άρθρο 4 GDPR: «*Ως ψευδωνυμοποίηση ορίζεται η επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο ώστε τα δεδομένα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς την χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρωματικές πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλιστεί ότι δεν μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο*».
https://en.wikipedia.org/wiki/Pseudonymization

δεδομένα που τον ενδιαφέρουν και εφόσον έχει στην κατοχή του το κλειδί να τα αποκρυπτογραφήσει[111] και β) η ομομορφική κρυπτογράφηση η οποία επιτρέπει την επεξεργασία και την εκτέλεση υπολογισμών με τα κρυπτογραφημένα δεδομένα χωρίς να απαιτείται γνώση των πραγματικών (αποκρυπτογραφημένων) δεδομένων[112].

II.3.2. ΑΣΦΑΛΕΙΑ ΣΤΑΘΜΩΝ ΕΡΓΑΣΙΑΣ (workstation security)

Τα μέτρα ασφαλείας αυτής της κατηγορίας αφορούν κυρίως τις ρυθμίσεις που πρέπει να γίνουν στους σταθμούς εργασίας ή στις συσκευές των υπαλλήλων ώστε να μην μπορούν να προβαίνουν σε ενέργειας που θα θέσουν σε κίνδυνο το σύστημα (όπως απενεργοποίηση antivirus ή firewall, εγκατάσταση μη εγκεκριμένου λογισμικού, κ.α.).

Στην πράξη:

- Όλοι οι σταθμοί εργασίας αλλά και οι servers πρέπει απαραιτήτως να έχουν εγκατεστημένα προγράμματα firewall, antimalware και antispyware[113] και να εγκαθιστούν αυτόματα τις πιο πρόσφατες ενημερώσεις χωρίς να μπορούν οι χρήστες να τα παραμετροποιήσουν ή να τα απενεργοποιήσουν.
- Οι απλοί χρήστες δεν θα πρέπει να έχουν δικαιώματα εγκατάστασης προγραμμάτων.
- Η δυνατότητα μεταφοράς δεδομένων από τον σταθμό εργασίας σε εξωτερικές συσκευές αποθήκευσης θα πρέπει να είναι εξ ορισμού απενεργοποιημένη.
- Κατ' αρχήν οι σταθμοί εργασίας που χρησιμοποιούνται για την επεξεργασία προσωπικών δεδομένων δεν θα πρέπει να έχουν σύνδεση στο internet εκτός και αν διαθέτουν προγράμματα ασφαλείας για την αποτροπή κακόβουλων επιθέσεων.

[111] Yunling Wang, Jianfeng Wang, Xiaofeng Chen, *Secure searchable encryption: a survey*, Journal of Communications and Information Networks, December 2016, Volume 1, Issue 4, pp 52–65 |
[112] https://en.wikipedia.org/wiki/Homomorphic_encryption
[113] Είδη κακόβουλου λογισμικού: ransomware, keyloggers, backdoors, rootkits, Trojans, σκουλήκια (worms), κακόβουλα LSPs, dialers, fraudtools, spam και phishing επιθέσεις. Spyware = κακόβουλο λογισμικό κατασκοπίας-παρακολούθησης. Αναλυτικότερα, https://en.wikipedia.org/wiki/Malware

- Χρήση λογισμικών διαχείρισης και ανίχνευσης εισβολών (intrusion detection and prevention systems[114]) καθώς και λογισμικών ανίχνευσης και διαχείρισης διαρροής δεδομένων (data leakage prevention[115]) τόσο σε επίπεδο δικτύου όσο και σε επίπεδο εφαρμογών.
- Ασφάλεια λειτουργικού συστήματος: Έλεγχος και προστασία από μη εξουσιοδοτημένη πρόσβαση ή προσπάθεια τροποποίησης των λειτουργικών αρχείων (system files), των δεδομένων ελέγχου και του πηγαίου κώδικα (source code) των προγραμμάτων

II.4. ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΟΥ (network security)

Η ασφάλεια επικοινωνιών είναι εξαιρετικά σημαντική για την προστασία των προσωπικών δεδομένων από επιθέσεις υποκλοπής, αλλοίωσης ή και διαγραφής τους· τόσο όσον αφορά την σύνδεση σε εξωτερικά δίκτυα (π.χ. το ίντερνετ), όσο και την διασύνδεση με άλλα συστήματα του οργανισμού.

Στην πράξη:

- Η πρόσβαση στο διαδίκτυο θα πρέπει να γίνεται μέσω ασφαλούς καναλιού επικοινωνίας με χρήση κρυπτογραφημένων πρωτοκόλλων (δημοσίου κλειδιού) ώστε τα δεδομένα που ανταλλάσσονται να μην μπορούν να υποκλαπούν, π.χ. Transport Security Layer (TLS) ή Secure File Transport Protocol (SFTP), HTTPS για ασφαλή σύνδεση, επικοινωνία και ανταλλαγή

[114] «*Το Σύστημα Ανίχνευσης Εισβολής αποτελεί σύστημα παρακολούθησης και ανάλυσης των συμβάντων, τα οποία λαμβάνουν χώρα τόσο στους ίδιους τους ηλεκτρονικούς υπολογιστές όσο και στα δίκτυα υπολογιστών. Στόχος είναι ο εντοπισμός ενδείξεων για πιθανές προσπάθειες εισβολής, κατά τις οποίες συχνά εντοπίζονται ίχνη παραβίασης της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητας των πληροφοριακών πόρων. Οι προσπάθειες παράκαμψης των μηχανισμών ασφαλείας μπορεί να προέρχονται από εξωτερικούς χρήστες, προς το εσωτερικό εταιρικό δίκτυο, στους οποίους δεν επιτρέπεται η πρόσβαση στο υπάρχον πληροφοριακό σύστημα. Επίσης, οι προσπάθειες παράκαμψης πιθανόν να προέρχονται από εσωτερικούς χρήστες, με περιορισμένα δικαιώματα πρόσβασης».* Οι βασικές κατηγορίες είναι τα δικτυακά συστήματα ανίχνευσης (NIDS) - τα οποία αναλύουν την διαδικτυακή ροή δεδομένων προς το σύστημα – και τα host-based συστήματα ανίχνευσης – τα οποία αναλύουν τα καίρια αρχεία του λειτουργικού συστήματος. Πηγή: https://en.wikipedia.org/wiki/Intrusion_detection_system

[115] Εξειδικευμένο λογισμικό που αποτρέπει την διαρροή δεδομένων σε χρήση (data in use), δεδομένων σε κίνηση (data in motion) και δεδομένων σε ακινησία (data at rest).

δεδομένων[116], χρήση του λογισμικού κρυπτογράφησης PGP (Pretty Good Privacy) που επιτρέπει την ανταλλαγή αρχείων και μηνυμάτων μέσω ηλεκτρονικού ταχυδρομείου διασφαλίζοντας το απόρρητο και την πιστοποίηση ταυτότητας[117].

- Η ασύρματη σύνδεση στο πληροφοριακό σύστημα θα πρέπει να επιτρέπεται μόνο για συγκεκριμένους χρήστες και για συγκεκριμένες διεργασίες και θα πρέπει να προστατεύεται από μηχανισμούς κρυπτογράφησης.
- Η απομακρυσμένη πρόσβαση (remote access) στο πληροφοριακό σύστημα κατ' αρχήν δεν θα πρέπει να επιτρέπεται. Σε μικρές επιχειρήσεις που δεν διαθέτουν τμήμα πληροφορικής και η απομακρυσμένη πρόσβαση αποτελεί μονόδρομο για εργασίες επίλυσης τεχνικών προβλημάτων ή εργασίες συντήρησης των συστημάτων, η σύνδεση θα πρέπει να γίνεται μέσω ασφαλών καναλιών με εποπτεία και έλεγχο του υπευθύνου επεξεργασίας ή κάποιου διοικητικού υπαλλήλου.
- Η κίνηση από και προς το πληροφοριακό σύστημα θα πρέπει να καταγράφεται και να ελέγχεται μέσω τειχών προστασίας και συστημάτων ανίχνευσης εισβολών. Ο υπεύθυνος επεξεργασίας πρέπει να προστατεύει το δίκτυο από αυξημένη κίνηση είτε πραγματική είτε τεχνητή ως μέθοδο κακόβουλης επίθεσης[118], προβαίνοντας στις κατάλληλες ενέργειες και τεχνικές διαχείρισης (επέκταση-αναβάθμιση-παραμετροποίηση) ώστε να εξασφαλίζεται η διαθεσιμότητα αλλά και η ποιοτική απόδοση του δικτύου
- Ο Υπεύθυνος Ασφαλείας θα πρέπει να προβεί στις κατάλληλες ενέργειες διαχωρισμού του εσωτερικού δικτύου από εξωτερικά δίκτυα και κατάτμησής του σε υποδίκτυα ή ζώνες ασφαλείας ώστε να ελέγχονται καλύτερα οι ροές

[116] Βλ. περισσότερα, https://www.websecurity.symantec.com/security-topics/what-is-ssl-tls-https
[117] Βλ. περισσότερα, https://en.wikipedia.org/wiki/Pretty_Good_Privacy
[118] «*Επιθέσεις Άρνησης Υπηρεσιών (Dos Attack - Denial of Service) ονομάζονται γενικά οι επιθέσεις εναντίον ενός υπολογιστή, ή μία ς υπηρεσίας που παρέχεται, οι οποίες έχουν ως σκοπό να καταστήσουν τον υπολογιστή ή την υπηρεσία ανίκανη να δεχτεί άλλες συνδέσεις και έτσι να μην μπορεί να εξυπηρετήσει άλλους πιθανούς πελάτες. Αν και ο όρος αφορά κυρίως δικτυακές υπηρεσίες, δεν περιορίζεται μόνο σε αυτές αλλά αναφέρεται και σε άλλα πεδία όπως ο μικροεπεξεργαστής (CPU) όπου μία αντίστοιχη επίθεση καταναλώνει τους πόρους του μικροεπεξεργαστή. Υπάρχουν γενικά δύο μορφές αυτής της επίθεσης. Η μία είναι η επίθεση κατά την οποία η υπηρεσία αναγκάζεται να καταρρεύσει και να πρέπει να επανεκκινηθεί και η άλλη είναι η αποστολή υπερβολικά μεγάλου αριθμού ψεύτικων αιτήσεων για εξυπηρέτηση με αποτέλεσμα η υπηρεσία να μην μπορεί να εξυπηρετήσει αυτούς που πραγματικά θέλουν την υπηρεσία».* (Wikipedia)

δεδομένων και να ανιχνεύονται τυχόν προσπάθειες εισβολής· προτείνεται η χρήση εικονικών ιδιωτικών δικτύων (Virtual Private Networks[119]) για επιχειρήσεις που έχουν υποκαταστήματα και εγκαταστάσεις σε διαφορετικές τοποθεσίες.

II.5. ΑΝΤΙΓΡΑΦΑ ΑΣΦΑΛΕΙΑΣ (back-up)

Ένα εφεδρικό σύστημα είναι απαραίτητο για την αποκατάσταση του αρχείου μετά από τυχόν απώλεια ή καταστροφή δεδομένων και η τήρησή του εκπληρώνει την υποχρέωση για διαθεσιμότητα και δυνατότητα πρόσβασης στα δεδομένα (αρθ. 32). Η τήρηση αντιγράφων ασφαλείας είναι μεν απαραίτητη, αλλά η συχνότητα και το είδος των δεδομένων εξαρτώνται από διάφορους παράγοντες, όπως το είδος του οργανισμού, το είδος των επεξεργαζόμενων δεδομένων, το μέγεθος της επιχείρησης, κτλ.

Στην πράξη:

- Πολιτική λήψης back-up : περιλαμβάνει την επιλογή των πόρων (εφαρμογές, αρχεία, αρχεία καταγραφής, κ.α.), την συχνότητα λήψης αντιγράφων ασφαλείας, την ασφαλή αποθήκευσή τους, την διαδικασία ορθής ανάκτησής τους, τον έλεγχο της αξιοπιστίας των λαμβανομένων αντιγράφων.
- Πλήρης λήψη back-up θα πρέπει να γίνεται τακτικά αναλόγως του οργανισμού και του είδους των προσωπικών δεδομένων που επεξεργάζεται.
- Τα αντίγραφα ασφαλείας θα πρέπει να ελέγχονται περιοδικά για την ορθή εξαγωγή τους και την ακεραιότητά τους ώστε να εντοπιστεί τυχόν αστοχία του λογισμικού δημιουργίας τους.
- Οι συσκευές που χρησιμοποιούνται για την αποθήκευση των αντιγράφων ασφαλείας θα πρέπει να ελέγχονται τακτικά ως προς την λειτουργικότητά τους και την ανάγκη αναβάθμισής τους.

[119] «*Ιδεατό ιδιωτικό δίκτυο είναι ένα δίκτυο που χρησιμοποιεί κατά κύριο λόγο δημόσια τηλεπικοινωνιακή υποδομή, όπως το Διαδίκτυο, και δίνει την δυνατότητα σε απομακρυσμένα γραφεία ή σε χρήστες που ταξιδεύουν να έχουν πρόσβαση σε ένα κεντρικό οργανωτικό δίκτυο. Συνήθως απαιτεί από τους απομακρυσμένους χρήστες του δικτύου πιστοποίηση, και συχνά ασφαλίζει τα δεδομένα με τεχνολογίες κρυπτογράφησης για να εμποδιστεί η διάδοση των ιδιωτικών πληροφοριών σε μη εξουσιοδοτημένους τρίτους.*» (Wikipedia)

- Αντίγραφα του back-up πρέπει να τηρούνται κρυπτογραφημένα και σε διαφορετικές ασφαλείς τοποθεσίες.
- Σε περίπτωση που χρησιμοποιείται εξωτερική υπηρεσία για την αποθήκευση των αντιγράφων ασφαλείας, ο υπεύθυνος επεξεργασίας πρέπει να τα παραδίδει κρυπτογραφημένα.

II.6. ΦΟΡΗΤΕΣ ΣΥΣΚΕΥΕΣ

Οι φορητές συσκευές μπορεί να διευκολύνουν τις εσωτερικές διαδικασίες και την εξ αποστάσεως εργασία, ταυτοχρόνως όμως αυξάνουν την πιθανότητα κλοπής ή τυχαίας απώλειας των δεδομένων.

Στην πράξη:

- Κατ' αρχήν δεν θα πρέπει να υπάρχει δυνατότητα εξαγωγής δεδομένων από το σύστημα με χρήση αποσπώμενων συσκευών παρά μόνο με έγκριση του υπευθύνου επεξεργασίας ή του υπεύθυνου ασφαλείας.
- Θα πρέπει να υπάρχει συγκεκριμένη διαδικασία χρήσης φορητών συσκευών: χρήση συσκευών με προκαθορισμένες προδιαγραφές, καταγραφή του περιεχομένου πριν την σύνδεση και μετά την αποσύνδεση από το πληροφοριακό σύστημα, διαδικασία ασφαλούς διαγραφής-καταστροφής.
- Ισχυρή κρυπτογράφηση φορητών αποθηκευτικών μέσων στα οποία τηρούνται αρχεία προσωπικών δεδομένων.
- Φύλαξη των αποσπώμενων συσκευών σε ασφαλή σημεία (κλειδωμένα ή με κωδικό ασφαλείας) και όχι εκτεθειμένα σε ευκόλως προσβάσιμους χώρους ή σε κοινή θέα.

II.7. ΑΣΦΑΛΕΙΑ ΛΟΓΙΣΜΙΚΟΥ (software security)

Στο άρθρο 25 του Κανονισμού εισάγονται οι έννοιες της εξ ορισμού και ήδη από τον σχεδιασμό ιδιωτικότητας οι οποίες απαιτούν ο υπεύθυνος επεξεργασίας ο υπεύθυνος επεξεργασίας να σχεδιάζει και να υιοθετεί εφαρμογές και διαδικασίες επεξεργασίας με γνώμονα την προστασία προσωπικών δεδομένων.

Στην πράξη:

- Κατά την ανάπτυξη λογισμικού πρέπει να ακολουθούνται οι βέλτιστες πρακτικές, η πιο πρόσφατη τεχνολογία και ευρέως αποδεκτές μέθοδοι ασφαλείας.
- Οι προδιαγραφές ασφαλείας και προστασίας των δεδομένων θα πρέπει να καθοριστούν στο αρχικό στάδιο της ανάπτυξης του λογισμικού – privacy by design.
- Κατά την ανάπτυξη λογισμικού πρέπει να χρησιμοποιούνται συγκεκριμένες τεχνικές, που έχουν σχεδιαστεί με σκοπό την διασφάλιση της ιδιωτικότητας και την προστασία δεδομένων (Privacy Enhancing Technologies – PETs[120]) σε συνδυασμό με μηχανισμούς ασφαλείας για την αποτροπή τυχαίας ή αθέμιτης καταστροφής ή αλλοίωσης, χωρίς εξουσιοδότηση πρόσβαση ή διάδοση ή επεξεργασία. Το ίδιο ισχύει και κατά την επιλογή λογισμικού που έχει αναπτυχθεί από τρίτους.
- Τήρηση ασφαλών τεχνικών προγραμματισμού· κατά την διαδικασία ανάπτυξης ή αναβάθμισης του λογισμικού θα πρέπει να χρησιμοποιούνται τεχνητά (dummy data) και όχι εξαχθέντα από το πραγματικό σύστημα δεδομένα.
- Σε περίπτωση ανάπτυξης του λογισμικού από εξωτερικό συνεργάτη θα πρέπει να συμφωνηθούν γραπτώς οι προδιαγραφές ασφαλείας και τεχνικών προγραμματισμού.
- Πριν την υλοποίηση του λογισμικού (ή τυχόν αναβαθμίσεών του), αυτό θα πρέπει να ελεγχθεί για τυχόν αστοχίες, ευπάθειες και κενά ασφαλείας σε δοκιμαστικό περιβάλλον και όχι στο αυτούσιο πληροφοριακό σύστημα.

[120] Ορισμός από τους van Blarkom, G.W., Borking, J.J. : "Ένα ενιαίο σύστημα με μέτρα βασισμένα στις τεχνολογίες πληροφορικής και επικοινωνιών, που προστατεύει την ιδιωτικότητα εξαλείφοντας ή μειώνοντας τα προσωπικά δεδομένα ή εμποδίζοντας την περιττή ή/και ανεπιθύμητην επεξεργασία προσωπικών δεδομένων, και όλα αυτά χωρίς να χάνεται ή να παρεμποδίζεται η λειτουργικότητα του πληροφοριακού συστήματος». Παραδείγματα Τεχνολογιών Ενίσχυσης ιδιωτικότητας: ελαχιστοποίηση δεδομένων, ανωνυμοποίηση, ψευδωνυμοποίηση, τεχνικές κρυπτογράφησης, ασφαλή πρωτόκολλα επικοινωνιών, τεχνικές διατήρησης ιδιωτικότητας στις βάσεις δεδομένων (k-ανωνυμία, privacy-preserving data mining – PPDM) κ.α.

ΙΙ.8. ΚΑΤΑΣΤΡΟΦΗ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΑΠΟΘΗΚΕΥΤΙΚΩΝ ΜΕΣΩΝ

Σύμφωνα με το άρθρο 6 τα προσωπικά δεδομένα δεν θα πρέπει να διατηρούνται για χρονικό διάστημα μεγαλύτερο από αυτό που είναι απαραίτητο για την εκπλήρωση των σκοπών για τους οποίους συλλέχθηκαν. Συνεπώς, ο υπεύθυνος επεξεργασίας πρέπει να καταστρέψει ή να διαγράψει τα δεδομένα με τρόπο που να μην μπορούν να ανακτηθούν. Επιπλέον, πριν την απόρριψη παλαιών ή άχρηστων συσκευών, θα πρέπει να διασφαλίζεται ότι όλα τα δεδομένα που περιέχουν έχουν διαγραφεί αποτελεσματικά. Ήδη από το 2005 η ΑΠΔΠΧ με την υπ' αρ. 1/2005 Οδηγία της προέβλεψε τις προϋποθέσεις και τις προδιαγραφές «για την ασφαλή καταστροφή των προσωπικών δεδομένων μετά το πέρας της περιόδου που απαιτείται για την πραγματοποίηση του σκοπού της επεξεργασίας». Συγκεκριμένα, ως ασφαλής τρόπος καταστροφής των δεδομένων ορίστηκε «η χρήση διαδικασιών που μετά από την ολοκλήρωση της εφαρμογής τους δεν είναι δυνατό να αναγνωρισθούν τα υποκείμενα των δεδομένων και η καταστροφή είναι μη αναστρέψιμη, δηλαδή δεν είναι δυνατή η ανάκτηση των δεδομένων με τεχνικά ή άλλα μέσα» (παρ. 4 και 5 αρθ.3 ως άνω Οδηγίας).

<u>Στην πράξη:</u>

- Αναλόγως της πολιτικής ιδιωτικότητας του οργανισμού και των σκοπών επεξεργασίας, τα δεδομένα μπορούν να διατηρηθούν στα συστήματα του υπεύθυνου επεξεργασίας για συγκεκριμένο χρονοδιάγραμμα, μετά το πέρας του οποίου θα πρέπει να σβηστούν, είτε αυτομάτως με την αντίστοιχη παραμετροποίηση των βάσεων δεδομένων είτε κατόπιν ειδοποίησης των αρμόδιων υπαλλήλων ώστε να εκτελεστεί χειροκίνητα η προβλεπόμενη διαδικασία.
- Χρήση καταστροφέα εγγράφων για την ασφαλή καταστροφή του φυσικού αρχείου. (βλ. και αρθ. 5 της υπ' αρ. 1/2005 Οδηγίας της ΑΠΔΠΧ)
- Πριν την απόρριψη συσκευών που έχουν χρησιμοποιηθεί στην επεξεργασία προσωπικών δεδομένων θα πρέπει να εφαρμοστεί η τεχνική της πολλαπλής αντικατάστασης των δεδομένων αυτών με τυχαία αρχεία (overwrite) ή και η

τεχνική μορφοποίησης του υλικού υποστρώματος (format) [121]. Εάν αυτό δεν είναι εφικτό, ο σκληρός δίσκος των συσκευών θα πρέπει να καταστραφεί με φυσικά μέσα[122].

- Εάν την διαδικασία καταστροφής δεδομένων και αποθηκευτικών μέσων την έχει αναλάβει εξωτερικός συνεργάτης, η διαδικασία θα πρέπει να ολοκληρώνεται στις εγκαταστάσεις του υπεύθυνου επεξεργασίας και να τηρείται ιστορικό με όλες τις ενέργειες.
- Η πολιτική καταστροφής των δεδομένων πρέπει να περιλαμβάνει και την καταστροφή όλων των αντιγράφων ασφαλείας (back up) που τηρεί ο υπεύθυνος επεξεργασίας.

[121] Οδηγία 1/2005 ΑΠΔΠΧ, παρ. 1 αρθ. 6: «*Για την ασφαλή καταστροφή δεδομένων σε ηλεκτρονική μορφή δεν επαρκεί η απλή διαγραφή τους (π.χ. με την εντολή «DELETE»), καθώς κατά τον τρόπο αυτό διαγράφεται μόνο η αναφορά στα δεδομένα, ενώ τα ίδια τα δεδομένα ενδέχεται να είναι ανακτήσιμα με χρήση ειδικών προγραμμάτων λογισμικού*».

[122] Ό.π. παρ. 3 αρθ. 6: «*…ένας εναλλακτικός τρόπος καταστροφής (για ιδιαίτερα κρίσιμα δεδομένα) είναι και η φυσική καταστροφή του ίδιου του υλικού υποστρώματος (π.χ. με θρυματισμό, κονιορτοποίηση, αποτέφρωση, με την επιφύλαξη ειδικών διατάξεων σχετικά με τη διαχείριση ειδικών αποβλήτων / προστασία του περιβάλλοντος).*

ΙΙΙ.ΜΕΤΡΑ ΦΥΣΙΚΗΣ ΑΣΦΑΛΕΙΑΣ

Η φυσική ασφάλεια των εγκαταστάσεων και της τεχνολογικής υποδομής από μη εξουσιοδοτημένη πρόσβαση αλλά και από πιθανές ζημιές φυσικής ή κακόβουλης προέλευσης είναι εξίσου σημαντική με τα τεχνολογικά μέτρα ασφαλείας.

ΙΙΙ.1. ΕΛΕΓΧΟΣ ΦΥΣΙΚΗΣ ΠΡΟΣΒΑΣΗΣ

Ο έλεγχος της φυσικής πρόσβασης στα πληροφοριακά συστήματα αποτελεί την βάση της πολιτικής ασφαλείας.

- Η φυσική πρόσβαση στον χώρο της τεχνολογικής υποδομής του πληροφοριακού συστήματος θα πρέπει να επιτρέπεται μόνο σε εξουσιοδοτημένο προσωπικό.
- Χώροι στους οποίους βρίσκεται ο δικτυακός εξοπλισμός, οι servers, τα αντίγραφα ασφαλείας, κ.α. θα πρέπει να είναι κλειδωμένοι ή/και να προστατεύονται με κλειστό κύκλωμα τηλεόρασης.
- Τήρηση καταλόγου με τα δικαιώματα φυσικής πρόσβασης του προσωπικού καθώς και με το προσωπικό που διαθέτει κλειδιά, κάρτες εισόδου και κωδικούς ασφαλείας.

ΙΙΙ.2. ΑΣΦΑΛΕΙΑ ΕΓΚΑΤΑΣΤΑΣΕΩΝ

Αναγκαία κρίνεται η λήψη μέτρων για την προστασία των εγκαταστάσεων από φυσικές ζημιές που μπορεί να προκληθούν είτε από φυσικά αίτια είτε από κακόβουλες ενέργειες, όπως διακοπή ρεύματος, πυρκαγιά, πλημμύρα, διάρρηξη-κλοπή, κ.α.

Βασικά μέτρα ασφαλείας και διαβάθμισή τους αναλόγως με την φύση του οργανισμού και το είδος των δεδομένων που επεξεργάζεται: αδιάλειπτη παροχή ρεύματος μέσω γεννητριών (ups), πόρτες και παράθυρα ασφαλείας, πυροπροστασία και ανιχνευτής πυρκαγιάς, αυτόματο σύστημα συναγερμού για τυχόν εξωτερική παραβίαση των εγκαταστάσεων, κλειστό κύκλωμα τηλεόρασης,

ανιχνευτής θερμοκρασίας και υγρασίας, σύστημα εξαερισμού και κλιματισμού.

III.3. ΠΡΟΣΤΑΣΙΑ ΦΥΣΙΚΟΥ ΑΡΧΕΙΟΥ

- Οι φυσικοί φάκελοι που περιέχουν προσωπικά δεδομένα δεν θα πρέπει να αφήνονται εκτεθειμένοι σε κοινή θέα και χωρίς επίβλεψη πάνω στα γραφεία (clean desk policy)· θα πρέπει να τοποθετούνται και να αποθηκεύονται σε ντουλάπια ή ειδικούς χώρους τήρησης αρχείου.
- Η χρήση συσκευών αναπαραγωγής εγγράφων (φωτοαντιγραφικά, εκτυπωτές, κ.α.) δεν θα πρέπει να είναι εύκολα προσβάσιμη στον καθένα.

7. ΕΡΓΑΛΕΙΑ ΣΥΜΜΟΡΦΩΣΗΣ

Έχουν ήδη αναπτυχθεί εμπορικές εφαρμογές και πλατφόρμες εργαλείων διαχείρισης[123] για την υποστήριξη των επιχειρήσεων στην διαδικασία συμμόρφωσής τους με τον Κανονισμό, ωστόσο δεν υπάρχει κάποιο λογισμικό για την ολιστική συμμόρφωση με τις υποχρεώσεις του Κανονισμού. Η συμμόρφωση απαιτεί μελέτη, αλλαγή επιχειρησιακής νοοτροπίας και οργανωτικές επιλογές και δεν αρκεί μόνο η επένδυση σε τεχνολογικές λύσεις. Ωστόσο κάποια από τα προαναφερόμενα βήματα συμμόρφωσης μπορούν να πραγματωθούν ευκολότερα, γρηγορότερα και αποτελεσματικότερα (με μικρό οικονομικό και επιχειρησιακό κόστος) με την χρήση τεχνολογικών εργαλείων και εξειδικευμένου λογισμικού.

Υπάρχουν διαφορετικά είδη εργαλείων που μπορούν να ελαφρύνουν τον φόρτο εργασίας στην προσπάθεια συμμόρφωσης με τον Κανονισμό:

- **Λίστα ελέγχου συμμόρφωσης:** Αυτού του είδους τα εργαλεία καθοδηγούν τον υπεύθυνο επεξεργασίας σε όλα τα απαραίτητα βήματα συμμόρφωσης.
- **Εργαλεία εκπόνησης ΕΑ:** Πρότυπα εκπόνησης εκτίμησης αντικτύπου σε μορφή υπολογιστικών φύλλων (Excel), ήδη διαμορφωμένα με βάση το είδος

[123] Avepoint Compliance Guardian https://www.avepoint.com/products/hybrid/compliance-guardian/ Privacy Perfect GDPR Compliance Toolkit https://www.privacyperfect.com/en

της επεξεργασίας.

- **Εργαλεία τήρησης αρχείου δραστηριοτήτων:** Διάφορες εμπορικές τεχνολογικές λύσεις προσφέρονται για την διευκόλυνση εκπλήρωσης και αυτής της υποχρέωσης· ακόμα και έτοιμα πρότυπα σε μορφή Excel από διάφορες εθνικές εποπτικές αρχές.
- **Εργαλεία ειδοποίησης παραβιάσεων δεδομένων:** Υπάρχουν επίσης διάφορα εμπορικά εργαλεία, αλλά και ελεύθερα εργαλεία, για την ανίχνευση παραβιάσεων ή διαρροής δεδομένων και την άμεση ειδοποίηση του υπευθύνου επεξεργασίας.
- **Εργαλεία ανάλυσης big data:** Αυτά τα εργαλεία στοχεύουν να εντοπίσουν τις ροές προσωπικών δεδομένων σε δομημένα ή αδόμητα σύνολα δεδομένων. Βοηθούν στην χαρτογράφηση των αναγνωρίσιμων προσωπικών δεδομένων στο πληροφοριακό σύστημα.

Επισημαίνεται ότι αν και η ενσωμάτωση όλων αυτών των εργαλείων απαιτεί χρόνο και κόπο για τον υπεύθυνο επεξεργασίας, στην πορεία αποδεικνύονται πολύ χρήσιμα, εύχρηστα και λειτουργικά καθώς ελέγχουν και εξυπηρετούν διακριτές μεν υποχρεώσεις συμμόρφωσης, όλα όμως συγκλίνουν στην ολική διαχείριση των δεδομένων του πληροφοριακού συστήματος.

8. ΟΡΙΣΜΟΣ DPO – inhouse ή outsourcing

Όσον αφορά τον ορισμό DPO ο υπεύθυνος επεξεργασίας έχει δύο επιλογές: να αναθέσει την άσκηση καθηκόντων Υπευθύνου Προστασίας σε κάποιον εξωτερικό συνεργάτη (φυσικό ή νομικό πρόσωπο) με βάση σύμβαση παροχής υπηρεσιών ή να επιλέξει κάποιο μέλος του προσωπικού το οποίο έχει σχετικές γνώσεις ή το οποίο μπορεί να εκπαιδευτεί σχετικά. Και στις δύο περιπτώσεις ο υπεύθυνος επεξεργασίας πρέπει να διασφαλίσει ότι το πρόσωπο που θα ασκεί τα καθήκοντα του DPO είναι καταρτισμένος όσον αφορά τα θέματα προστασίας προσωπικών

δεδομένων τόσο από νομικής απόψεως όσο και από τεχνικής[124]. Οι κύριοι παράγοντες που πρέπει να ληφθούν υπ' όψιν για την λήψη της σχετικής απόφασης είναι οι εξής: ως προς την εξωτερική ανάθεση ανακύπτουν τα ζητήματα του κόστους και της παροχής πρόσβασης στον πυρήνα του πληροφοριακού συστήματος και στα πιο κρίσιμα πληροφοριακά αγαθά του οργανισμού· αντιθέτως, τα πλεονεκτήματα της κατάρτισης και της εμπειρογνωσίας των εξειδικευμένων επαγγελματιών προστασίας προσωπικών δεδομένων προσφέρουν όχι μόνο ταχύτητα συμμόρφωσης αλλά και μικρότερη πιθανότητα λανθασμένων χειρισμών υπερτερώντας της επιλογής της εκ του μηδενός εκπαίδευσης ενός στελέχους της επιχείρησης. Αντιστοίχως, η εσωτερική ανάθεση έχει το πλεονέκτημα της διατήρησης του ελέγχου των πληροφοριακών αγαθών εντός του πλαισίου του οργανισμού αλλά και της καλύτερης συνεργασίας μεταξύ της διοίκησης και του εσωτερικού DPO σε σύγκριση με έναν εξωτερικό πάροχο ο οποίος έχει χαλαρότερη σύνδεση με την επιχείρηση και πιθανόν να μην κατανοεί πλήρως τις επιχειρησιακές διαδικασίες, την αρχιτεκτονική του πληροφοριακού συστήματος και τους σκοπούς επεξεργασίας.

Ειδικότερα, για την εξωτερική ανάθεση καθηκόντων DPO, η Ομάδα του άρθρου 29[125] διευκρινίζει: «*Εάν ο υπεύθυνος προστασίας δεδομένων είναι εξωτερικός, τότε ισχύουν όλες οι απαιτήσεις των άρθρων 37 έως 39. Όπως αναφέρεται στις κατευθυντήριες γραμμές, όταν τα καθήκοντα του υπευθύνου προστασίας δεδομένων ασκούνται από εξωτερικό πάροχο υπηρεσιών, η αποτελεσματική άσκησή τους είναι δυνατό να εξασφαλιστεί με την σύσταση ομάδας στους κόλπους της εν λόγω οντότητας, τα μέλη της οποίας συνεργάζονται μεταξύ τους υπό την ευθύνη ατόμου το οποίο έχει οριστεί επικεφαλής επικοινωνίας και «υπεύθυνος» για*

[124] ΠΑΡΑΡΤΗΜΑ - ΚΑΤΕΥΘΥΝΤΗΡΙΕΣ ΓΡΑΜΜΕΣ ΣΧΕΤΙΚΑ ΜΕ ΤΟΥΣ ΥΠΕΥΘΥΝΟΥΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ: ΤΙ ΠΡΕΠΕΙ ΝΑ ΓΝΩΡΙΖΕΤΕ, (σελ. 31) : «Ο υπεύθυνος προστασίας δεδομένων πρέπει να διαθέτει, μεταξύ άλλων, τις ακόλουθες δεξιότητες *και εμπειρογνωμοσύνη: • εμπειρογνωσία στον τομέα του δικαίου και των πρακτικών περί προστασίας δεδομένων, τόσο σε εθνικό όσο και σε ευρωπαϊκό επίπεδο, καθώς και άριστη γνώση του ΓΚΠΔ, • γνώση των πράξεων επεξεργασίας που διενεργούνται, • γνώση του τομέα των τεχνολογιών πληροφοριών και της ασφάλειας δεδομένων, • γνώση του τομέα δραστηριότητας και του οργανισμού, • ικανότητα ανάπτυξης νοοτροπίας προστασίας των δεδομένων στους κόλπους του οργανισμού».*

[125] Ομάδα άρθρου 29, *ΠΑΡΑΡΤΗΜΑ - ΚΑΤΕΥΘΥΝΤΗΡΙΕΣ ΓΡΑΜΜΕΣ ΣΧΕΤΙΚΑ ΜΕ ΤΟΥΣ ΥΠΕΥΘΥΝΟΥΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ: ΤΙ ΠΡΕΠΕΙ ΝΑ ΓΝΩΡΙΖΕΤΕ*, Κατευθυντήριες γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων (σελ. 30)

κάθε πελάτη. Σ' αυτήν την περίπτωση, είναι σημαντικό κάθε μέλος του εξωτερικού οργανισμού που ασκεί καθήκοντα υπευθύνου προστασίας δεδομένων να πληροί όλες τις σχετικές απαιτήσεις του ΓΚΠΔ. Για λόγους νομικής σαφήνειας και καλής οργάνωσης, συστήνεται να υπάρχει στην σύμβαση παροχής υπηρεσιών, σαφής καταμερισμός των καθηκόντων στους κόλπους της ομάδας του εξωτερικού υπευθύνου προστασίας δεδομένων και να ορίζεται ένα μόνο άτομο ως επικεφαλής επικοινωνίας και υπεύθυνος για κάθε πελάτη».

Η απόφαση παραμένει στα χέρια της διοίκησης η οποία θα πρέπει να σταθμίσει τους προαναφερόμενους παράγοντες σε συνδυασμό με το είδος και τον όγκο των δεδομένων που επεξεργάζεται, τις πιθανότητες επέλευσης κάποιου συμβάντος παραβίασης καθώς και την κρισιμότητα του τομέα επιχειρηματικής δραστηριοποίησής της.

9. ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ ΕΡΓΑΖΟΜΕΝΩΝ

Πρέπει να επισημανθεί ότι η υποχρέωση συμμόρφωσης με τον Κανονισμό δεν εξαντλείται με τον σεβασμό και την προστασία των προσωπικών δεδομένων των πελατών· και οι εργαζόμενοι του υπευθύνου προστασίας απολαύουν των ίδιων δικαιωμάτων στα πλαίσια των εργασιακών τους σχέσεων[126]. Συνεπώς, και για την επεξεργασία των προσωπικών δεδομένων των εργαζομένων απαιτείται η ύπαρξη νόμιμης βάσης η οποία μπορεί να ανευρεθεί κατ' αρχήν στο άρθρο 7. Σύμφωνα με την Ομάδα του άρθρου 29[127], «*εάν το είδος των δεδομένων προσωπικού χαρακτήρα που υφίστανται επεξεργασία περιλαμβάνει ειδικές κατηγορίες (όπως αναλύονται στο άρθρο 8), η επεξεργασία απαγορεύεται εκτός εάν ο εργοδότης μπορεί να επικαλεστεί μία από τις παρακάτω εξαιρέσεις σε συνδυασμό με την νομική βάση του άρθρου 7*». Οι

[126] Στο άρθρο 88 ορίζεται ότι «*τα κράτη μέλη, μέσω της νομοθεσίας ή μέσω των συλλογικών συμβάσεων, μπορούν να θεσπίζουν ειδικούς κανόνες προκειμένου να διασφαλίζουν την προστασία των δικαιωμάτων και των ελευθεριών έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα των εργαζομένων στο πλαίσιο της απασχόλησης. […] Οι εν λόγω κανόνες περιλαμβάνουν κατάλληλα και ειδικά μέτρα για τη διαφύλαξη της ανθρώπινης αξιοπρέπειας, των έννομων συμφερόντων και των θεμελιωδών δικαιωμάτων του προσώπου στο οποίο αναφέρονται τα δεδομένα, με ιδιαίτερη έμφαση στη διαφάνεια της επεξεργασίας, τη διαβίβαση δεδομένων προσωπικού χαρακτήρα εντός ομίλου επιχειρήσεων, ή ομίλου εταιρειών που ασκούν κοινή οικονομική δραστηριότητα και τα συστήματα παρακολούθησης στο χώρο εργασίας».*

[127] Γνώμη 2/2017 σχετικά με την επεξεργασία προσωπικών δεδομένων στην εργασία, 8 Ιουνίου 2017.

νομικές βάσεις τις οποίες μπορεί να επικαλεστεί ο εργοδότης για να αποδείξει την νομιμότητα της επεξεργασίας των προσωπικών δεδομένων είναι οι εξής:

- **Εκτέλεση σύμβασης [άρθρο 7 στοιχείο β] –** Οι σχέσεις εργασίας συνήθως βασίζονται σε σύμβαση εργασίας μεταξύ του εργοδότη και του εργαζομένου· για την εκπλήρωση των υποχρεώσεων που απορρέουν από τη σύμβαση αυτή, όπως η καταβολή στον εργαζόμενο των αποδοχών του, ο εργοδότης χρειάζεται να προβαίνει στην επεξεργασία ορισμένων δεδομένων προσωπικού χαρακτήρα.
- **Εκ του νόμου υποχρέωση [άρθρο 7 στοιχείο γ] -** Η εργατική νομοθεσία επιβαρύνει τον εργοδότη με υποχρεώσεις η εκπλήρωση των οποίων απαιτεί επεξεργασία δεδομένων προσωπικού χαρακτήρα (π.χ. για σκοπούς υπολογισμού του φόρου και διαχείρισης μισθών).
- **Έννομο συμφέρον [άρθρο 7 στοιχείο στ]** – Για την επίκληση του έννομου συμφέροντος του εργοδότη ως προς την διενέργεια συγκεκριμένης επεξεργασίας, ο επιδιωκόμενος σκοπός πρέπει να είναι νόμιμος, και η διαδικασία ή τεχνολογία που θα χρησιμοποιηθεί για την υλοποίησή της να είναι απαραίτητη και ανάλογη προς τον σκοπό αυτό. Η επεξεργασία δεδομένων στην εργασία θα πρέπει να διενεργείται με τον λιγότερο δυνατόν παρεμβατικό τρόπο και να επικεντρώνεται στον συγκεκριμένο τομέα κινδύνου. Προκειμένου να γίνει επίκληση του άρθρου 7 στοιχείο στ) ως νομική βάση επεξεργασίας, είναι απαραίτητο να υπάρχουν ειδικά μέτρα μετριασμού ώστε να διασφαλίζεται η δίκαιη ισορροπία μεταξύ του έννομου συμφέροντος του εργοδότη και των θεμελιωδών δικαιωμάτων και ελευθεριών των εργαζομένων. Τα μέτρα αυτά, ανάλογα με τη μορφή της παρακολούθησης, θα πρέπει να περιλαμβάνουν περιορισμούς της παρακολούθησης ώστε να διασφαλίζεται ότι δεν θα παραβιάζεται η ιδιωτικότητα του. Πιο συγκεκριμένα, το έννομο συμφέρον του εργοδότη μπορεί να δικαιολογήσει την βιντεοεπιτήρηση των υπαλλήλων για τον έλεγχο και την αποτροπή κλοπής της φυσικής περιουσίας ή της πνευματικής ιδιοκτησίας της επιχείρησης, για την παρακολούθηση της αποδοτικότητας και της παραγωγικότητας των υπαλλήλων, κ.α. Ωστόσο, δεν μπορεί να δικαιολογήσει την χωρίς περιορισμούς επεξεργασία των προσωπικών δεδομένων των υπαλλήλων και την χωρίς όρους και προϋποθέσεις παρακολούθησή τους στον εργασιακό χώρο· π.χ. απαγορεύεται το κλειστό κύκλωμα παρακολούθησης στους χώρους υγιεινής και στους χώρους

διαλείμματος, η κρυφή μαγνητοσκόπηση χωρίς την υποψία τέλεσης ποινικού αδικήματος, η λήψη αυτοματοποιημένων αποφάσεων σε σχέση με την αποδοτικότητα.

Ο εργοδότης ως υπεύθυνος επεξεργασίας πρέπει να ενημερώνει τους εργαζομένους για τα δεδομένα τους που τυγχάνουν επεξεργασίας, για τους τρόπους και την αναγκαιότητα επεξεργασίας και για τα δικαιώματά τους. Η ενημέρωση αυτή μπορεί να γίνει με εσωτερικό έντυπο δήλωσης ιδιωτικότητας ή με ανάρτηση στο portal ή σε κάποια εφαρμογή της επιχείρησης στην οποία έχουν πρόσβαση όλοι οι εργαζόμενοι και πρέπει να έχει ως ελάχιστο περιεχόμενο τα εξής:

- η χρήση ή μη κλειστών συστημάτων βιντεοεπιτήρησης
- οι σκοποί και τα μέσα επεξεργασίας των προσωπικών δεδομένων
- ο χρόνος διατήρησης των προσωπικών δεδομένων
- τα μέτρα ασφαλείας
- τα δικαιώματα των εργαζομένων

Τέλος, ο εργοδότης υποχρεούται να συμπεριλαμβάνει όρους και ρήτρες για την προστασία των προσωπικών δεδομένων των εργαζομένων σε κάθε συμφωνία με τρίτο πάροχο υπηρεσιών ο οποίος θα αναλάβει την επεξεργασία τους, όπως γραφεία ευρέσεως εργασίας, λογιστές, διαχειριστές μισθοδοσίας, ασφαλιστικές εταιρείες, κ.τ.λ.

ΙΙΙ. ΕΠΙΛΟΓΟΣ

Σύμφωνα με την πολύ πρόσφατη έρευνα της εταιρείας Cisco, "Data Privacy Benchmark Study 2019"[128], η οποία διεξήχθη σε πάνω από 3.200 ειδικούς ασφαλείας πληροφοριών σε 18 χώρες, αποτελεί κοινή παραδοχή ότι η επένδυση στην ιδιωτικότητα και στην προστασία των προσωπικών δεδομένων μεταφράζεται σε ανταγωνιστικό επιχειρηματικό πλεονέκτημα. Οι επιχειρήσεις που προετοιμάστηκαν ή είναι στην διαδικασία συμμόρφωσης με τις επιταγές του Κανονισμού αντιμετωπίζουν πλέον λιγότερα και διαχειρίσιμα περιστατικά ασφαλείας και δεν χάνουν πελάτες εξαιτίας επιφυλάξεων σε θέματα ιδιωτικότητας και ασφάλειας δεδομένων. Η πλειοψηφία των επιχειρήσεων υποστηρίζει ότι η επένδυση στην ιδιωτικότητα φέρνει πολλές επιπρόσθετες ωφέλειες, όπως καινοτομία και εναλλακτικές τεχνολογικές λύσεις, ανταγωνιστικό πλεονέκτημα και όχι απλώς ανταγωνισμό, μεγαλύτερη λειτουργικότητα και αποδοτικότητα συστημάτων και διαδικασιών και έλξη επενδυτών. Επιπλέον, οι επιχειρήσεις που έχουν συμμορφωθεί με το σύνολο ή με τις περισσότερες επιταγές του GDPR αντιμετώπισαν λιγότερα περιστατικά παραβιάσεων τον τελευταίο χρόνο, αλλά και όταν αυτά συνέβησαν, η οικονομική ζημιά ήταν σημαντικά λιγότερη, καθώς επηρεάστηκε μικρότερο εύρος των συστημάτων και ο χρόνος απόκρισης και αποκατάστασης ήταν ταχύτερος. Αλλά και στον τομέα των πωλήσεων, οι επιχειρήσεις που έχουν ενσωματώσει τα απαραίτητα μέτρα προστασίας και ασφάλειας της ιδιωτικότητας αντιμετώπισαν λιγότερες και πιο βραχυχρόνιες καθυστερήσεις για την σύναψη της τελικής συμφωνίας με πελάτες που είχαν ενδοιασμούς και απαιτήσεις σε θέματα ιδιωτικότητας.

[128] https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/dpbs-2019.pdf

ΠΑΡΑΡΤΗΜΑΤΑ

ΠΑΡΑΡΤΗΜΑ Ι – Κριτήρια για την υποχρεωτικότητα διενέργειας Εκτίμησης Αντικτύπου[129]

Η Ομάδα του άρθρου 29 έχει καταρτίσει μία λίστα αναλυτικών κριτηρίων σε συμπλήρωση του αρθ. 35 για το πότε πρέπει να εκπονηθεί ΕΑ.

1. Αξιολόγηση ή βαθμολόγηση, περιλαμβανομένης της κατάρτισης προφίλ και προβλέψεων, ιδίως «πτυχών που αφορούν τις επιδόσεις στην εργασία, την οικονομική κατάσταση, την υγεία, τις προσωπικές προτιμήσεις ή συμφέροντα, την αξιοπιστία ή την συμπεριφορά, την θέση ή κινήσεις του υποκειμένου των δεδομένων» (αιτιολογικές σκέψεις 71 και 91). Σχετικό παράδειγμα θα μπορούσε να είναι η περίπτωση που ένα χρηματοπιστωτικό ίδρυμα ελέγχει τους πελάτες του σε σχέση με μία βάση δεδομένων πιστοληπτικής ικανότητας ή μία βάση δεδομένων για την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και της χρηματοδότησης της τρομοκρατίας (ΚΞΧ/ΧΤ) ή μία βάση δεδομένων για εγκλήματα απάτης, ή η περίπτωση που μία εταιρεία βιοτεχνολογίας παρέχει απευθείας στους καταναλωτές γενετικές δοκιμές για να εκτιμήσει και να προβλέψει τους κινδύνους νόσου/υγείας ή η περίπτωση που μία εταιρεία δημιουργεί συμπεριφορικά προφίλ ή προφίλ εμπορικής προώθησης βάσει της χρήσης ή πλοήγησης στον δικτυακό της τόπο.
2. Λήψη αυτοματοποιημένων αποφάσεων που παράγουν έννομα αποτελέσματα ή σημαντικά αποτελέσματα κατά ανάλογο τρόπο: επεξεργασία που αποσκοπεί στην λήψη αποφάσεων που αφορούν υποκείμενα δεδομένων και παράγουν «έννομα αποτελέσματα σχετικά με το φυσικό πρόσωπο» ή που «ομοίως επηρεάζουν σημαντικά το φυσικό πρόσωπο» [άρθρο 35 παράγραφος 3 στοιχείο α)]. Για παράδειγμα, η επεξεργασία μπορεί να οδηγήσει σε αποκλεισμό ή σε διακρίσεις σε βάρος των φυσικών προσώπων. Επεξεργασία με μικρό ή μηδαμινό αντίκτυπο στα φυσικά πρόσωπα δεν πληροί τους όρους του συγκεκριμένου κριτηρίου. Περαιτέρω επεξηγήσεις των εν λόγω εννοιών θα περιλαμβάνονται στις επερχόμενες κατευθυντήριες γραμμές της ομάδας εργασίας του άρθρου 29 για την κατάρτιση προφίλ.
3. Συστηματική παρακολούθηση: επεξεργασία για την παρατήρηση, την παρακολούθηση ή τον έλεγχο των υποκειμένων των δεδομένων, περιλαμβανομένων των δεδομένων που συλλέγονται μέσω δικτύων ή «συστηματική παρακολούθηση δημοσίως προσβάσιμου χώρου» [άρθρο 35 παράγραφος 3 στοιχείο γ)]. Αυτό το είδος παρακολούθησης αποτελεί κριτήριο, διότι τα δεδομένα προσωπικού χαρακτήρα μπορεί να συλλέγονται σε περιστάσεις κατά τις οποίες τα υποκείμενα των δεδομένων ενδέχεται να μην έχουν επίγνωση του ποιος συλλέγει τα δεδομένα τους και του πώς θα χρησιμοποιηθούν. Επιπρόσθετα, τα φυσικά πρόσωπα ενδεχομένως να είναι αδύνατο να αποφύγουν

[129] Enisa, *Guidelines for SMEs on the security of personal data processing*, σελ. 25-31.

την εν λόγω επεξεργασία των δεδομένων τους σε δημόσιο/-ους (ή δημοσίως προσβάσιμο/-ους) χώρο/-ους.

4. Ευαίσθητα δεδομένα ή δεδομένα εξαιρετικά προσωπικού χαρακτήρα: σε αυτά περιλαμβάνονται ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα, όπως ορίζονται στο άρθρο 9 (για παράδειγμα, πληροφορίες για τα πολιτικά φρονήματα φυσικών προσώπων), καθώς και δεδομένα προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες ή αδικήματα, όπως ορίζονται στο άρθρο 10. Σχετικό παράδειγμα θα μπορούσαν να είναι τα ιατρικά αρχεία ασθενών που τηρεί ένα γενικό νοσοκομείο ή τα προσωπικά στοιχεία παραβατών που τηρεί ένας πράκτορας ιδιωτικών ερευνών. Εκτός από τις εν λόγω διατάξεις του ΓΚΠΔ, ορισμένες κατηγορίες δεδομένων μπορεί να θεωρηθεί ότι αυξάνουν τον δυνητικό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Τα εν λόγω δεδομένα προσωπικού χαρακτήρα θεωρούνται ευαίσθητα (όπως κοινώς νοείται ο εν λόγω όρος), επειδή συνδέονται με οικιακές δραστηριότητες και δραστηριότητες του ιδιωτικού βίου (όπως, οι ηλεκτρονικές επικοινωνίες, των οποίων θα πρέπει να διαφυλάττεται η εμπιστευτικότητα) ή επειδή επηρεάζουν την άσκηση ενός θεμελιώδους δικαιώματος (όπως δεδομένα τοποθεσίας με την συλλογή των οποίων διαμφισβητείται η ελευθερία κυκλοφορίας) ή επειδή η παραβίασή τους σαφώς επηρεάζει σημαντικά την καθημερινή ζωή του υποκειμένου των δεδομένων (όπως τα οικονομικά δεδομένα που θα μπορούσαν να χρησιμοποιηθούν σε τέλεση απάτης πληρωμών). Εν προκειμένω, σημασία μπορεί να έχει και το κατά πόσον τα δεδομένα έχουν δημοσιοποιηθεί από το υποκείμενο των δεδομένων ή από τρίτα πρόσωπα. Ο δημόσιος χαρακτήρας των δεδομένων προσωπικού χαρακτήρα μπορεί να εξετάζεται ως παράμετρος για να εκτιμηθεί αν τα δεδομένα αναμενόταν να χρησιμοποιηθούν περαιτέρω για συγκεκριμένους σκοπούς. Στο παρόν κριτήριο μπορεί επίσης να περιλαμβάνονται δεδομένα όπως προσωπικά έγγραφα, μηνύματα ηλεκτρονικού ταχυδρομείου, ημερολόγια, σημειώσεις από ηλεκτρονικό αναγνώστη (e-reader) που προσφέρει δυνατότητες τήρησης σημειώσεων, και πολύ προσωπικές πληροφορίες που περιλαμβάνονται σε εφαρμογές καταγραφής βίου («lifelogging»).
5. Δεδομένα μεγάλης κλίμακας επεξεργασίας: ο ΓΚΠΔ δεν ορίζει τι συνιστά μεγάλης κλίμακας επεξεργασία, ωστόσο η αιτιολογική σκέψη 91 παρέχει ορισμένες κατευθύνσεις. Σε κάθε περίπτωση, η ομάδα εργασίας του άρθρου 29 συνιστά να λαμβάνονται συγκεκριμένα υπόψη οι ακόλουθες παράμετροι κατά τον προσδιορισμό του κατά πόσον η επεξεργασία τελείται σε μεγάλη κλίμακα: α. ο αριθμός των εμπλεκόμενων υποκειμένων των δεδομένων, είτε ως συγκεκριμένος αριθμός είτε ως ποσοστό επί του συναφούς πληθυσμού· β. ο όγκος των δεδομένων και/ή το εύρος των διαφόρων στοιχείων δεδομένων που υποβάλλονται σε επεξεργασία· γ. η διάρκεια ή ο μόνιμος χαρακτήρας της δραστηριότητας επεξεργασίας δεδομένων· δ. το γεωγραφικό εύρος της δραστηριότητας επεξεργασίας.
6. Η αντιστοίχιση ή ο συνδυασμός συνόλων δεδομένων που απορρέουν, για παράδειγμα, από δύο ή περισσότερες πράξεις επεξεργασίας δεδομένων που υλοποιούνται για διαφορετικούς σκοπούς και/ή από διαφορετικούς υπεύθυνους επεξεργασίας με τρόπο που θα μπορούσε να υπερβαίνει τις εύλογες προσδοκίες

του υποκειμένου των δεδομένων.

7. Δεδομένα που αφορούν ευάλωτα υποκείμενα δεδομένων (αιτιολογική σκέψη 75): η επεξεργασία του εν λόγω τύπου δεδομένων αποτελεί κριτήριο λόγω της αυξημένα άνισης σχέσης ισχύος μεταξύ των υποκειμένων των δεδομένων και του υπεύθυνου επεξεργασίας, με την έννοια ότι τα φυσικά πρόσωπα ενδέχεται να μην είναι σε θέση να συναινέσουν ή να εναντιωθούν με ευκολία στην επεξεργασία των δεδομένων τους ή να ασκήσουν τα δικαιώματά τους. Στα ευάλωτα υποκείμενα δεδομένων ενδέχεται να περιλαμβάνονται παιδιά (τα οποία μπορεί να θεωρηθεί ότι δεν είναι σε θέση να εναντιωθούν ή να συναινέσουν μετά λόγου γνώσης ή συνειδητά στην επεξεργασία των δεδομένων τους), εργαζόμενοι, πιο ευάλωτα τμήματα του πληθυσμού που χρήζουν ειδικής προστασίας (ψυχικά νοσούντες, αιτούντες άσυλο ή ηλικιωμένοι, ασθενείς κ.ο.κ.), και σε κάθε περίπτωση που εξακριβώνεται άνιση σχέση μεταξύ της θέσης του υποκειμένου των δεδομένων και του υπεύθυνου επεξεργασίας.
8. Καινοτόμος χρήση ή εφαρμογή νέων τεχνολογικών ή οργανωτικών λύσεων, όπως η συνδυασμένη χρήση των δακτυλικών αποτυπωμάτων και η αναγνώριση προσώπου για βελτιωμένο φυσικό έλεγχο πρόσβασης κ.ο.κ. Ο ΓΚΠΔ καθιστά σαφές (άρθρο 35 παράγραφος 1 και αιτιολογικές σκέψεις 89 και 91) ότι η χρήση νέων τεχνολογιών, που ορίζονται «σύμφωνα με τα υφιστάμενα επίπεδα τεχνολογικής γνώσης» (αιτιολογική σκέψη 91), μπορεί να καταστήσει αναγκαία την διενέργεια ΕΑΠΔ. Και τούτο διότι η χρήση μία ς τέτοιας τεχνολογίας μπορεί να περιλαμβάνει νέες μορφές συλλογής και χρήσης δεδομένων, πιθανώς με υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Πράγματι, οι προσωπικές και κοινωνικές επιπτώσεις από την χρήση μία ς νέας τεχνολογίας ενδέχεται να είναι άγνωστες. Η διενέργεια ΕΑΠΔ θα βοηθήσει τον υπεύθυνο επεξεργασίας να κατανοήσει και να αντιμετωπίσει τους εν λόγω κινδύνους. Για παράδειγμα, συγκεκριμένες εφαρμογές του «διαδικτύου των πραγμάτων» θα μπορούσαν να έχουν σημαντικό αντίκτυπο στην καθημερινή ζωή και την ιδιωτική ζωή των φυσικών προσώπων· και, ως εκ τούτου, απαιτείται η διενέργεια σχετικής ΕΑΠΔ.
9. Όταν η επεξεργασία αυτή καθαυτήν «εμποδίζει τα υποκείμενα των δεδομένων να ασκήσουν κάποιο δικαίωμα ή να χρησιμοποιήσουν μία υπηρεσία ή σύμβαση» (άρθρο 22 και αιτιολογική σκέψη 91). Εδώ περιλαμβάνονται πράξεις επεξεργασίας που έχουν σκοπό να επιτρέψουν, να τροποποιήσουν ή να αρνηθούν στα υποκείμενα των δεδομένων την πρόσβαση σε υπηρεσία ή την σύναψη σύμβασης. Σχετικό παράδειγμα είναι η περίπτωση που μία τράπεζα ελέγχει τους πελάτες της χρησιμοποιώντας μία βάση δεδομένων πιστοληπτικής ικανότητας για να αποφασίσει αν θα τους χορηγήσει δάνειο ή όχι. Στις περισσότερες περιπτώσεις, ο υπεύθυνος επεξεργασίας μπορεί να θεωρεί ότι σε μία επεξεργασία που πληροί δύο κριτήρια θα απαιτούνταν η διενέργεια ΕΑΠΔ. Εν γένει, η ομάδα εργασίας του άρθρου 29 θεωρεί ότι όσο περισσότερα κριτήρια πληρούνται με την επεξεργασία, τόσο πιθανότερο είναι να τίθενται σε υψηλό κίνδυνο τα δικαιώματα και οι ελευθερίες των υποκειμένων των δεδομένων και, ως εκ τούτου, να απαιτείται η διενέργεια ΕΑΠΔ, ανεξάρτητα από τα προβλεπόμενα μέτρα του υπεύθυνου επεξεργασίας.

ΠΑΡΑΡΤΗΜΑ ΙΙ – Κριτήρια για μία αποδεκτή Εκτίμηση Αντικτύπου

Η ομάδα εργασίας του άρθρου 29[130] προτείνει τα ακόλουθα κριτήρια, τα οποία οι υπεύθυνοι επεξεργασίας μπορούν να χρησιμοποιούν για να αξιολογούν κατά πόσο μία ΕΑΠΔ ή μία μεθοδολογία διενέργειας ΕΑΠΔ είναι επαρκώς περιεκτική προκειμένου να συμμορφώνεται με τον GDPR:

- ☐ <u>παρέχεται συστηματική περιγραφή των πράξεων επεξεργασίας</u> [άρθρο 35 παράγραφος 7 στοιχείο α)]:
  - ☐ λαμβάνονται υπόψη η φύση, η έκταση, το πλαίσιο και οι σκοποί της επεξεργασίας (αιτιολογική σκέψη 90)·
  - ☐ καταγράφονται τα δεδομένα προσωπικού χαρακτήρα, οι αποδέκτες και η περίοδος αποθήκευσης των δεδομένων προσωπικού χαρακτήρα·
  - ☐ παρέχεται λειτουργική περιγραφή της πράξης επεξεργασίας·
  - ☐ προσδιορίζονται τα στοιχεία του ενεργητικού στα οποία εναποτίθενται τα δεδομένα (υλισμικό, λογισμικό, δίκτυα, πρόσωπα, έντυπα ή δίαυλοι διαβίβασης εντύπων)·
  - ☐ λαμβάνεται υπόψη η συμμόρφωση με εγκεκριμένους κώδικες δεοντολογίας (άρθρο 35 παράγραφος 8)·
- ☐ <u>εκτιμώνται η αναγκαιότητα και η αναλογικότητα</u> [άρθρο 35 παράγραφος 7 στοιχείο β)]·
  - ☐ καθορίζονται τα προβλεπόμενα μέτρα συμμόρφωσης με τον κανονισμό [άρθρο 35 παράγραφος 7 στοιχείο δ) και αιτιολογική σκέψη 90], λαμβάνοντας υπόψη:
    - ☐ τα μέτρα που κατατείνουν στην αναλογικότητα και την αναγκαιότητα της επεξεργασίας βάσει:
      - ☐ καθορισμένων, ρητών και νόμιμων σκοπών [άρθρο 5 παράγραφος 1 στοιχείο β)]·
      - ☐ της νομιμότητας της επεξεργασίας (άρθρο 6)·
      - ☐ κατάλληλων, συναφών και περιορισμένων στα αναγκαία δεδομένων [άρθρο 5 παράγραφος 1 στοιχείο γ)]·
      - ☐ της περιορισμένης διάρκειας αποθήκευσης [άρθρο 5 παράγραφος 1

[130] Ομάδα Προστασίας των προσώπων έναντι της Επεξεργασίας δεδομένων προσωπικού Χαρακτήρα του άρθρου 29, *Κατευθυντήριες γραμμές για την εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) και καθορισμός του κατά πόσον η επεξεργασία «ενδέχεται να επιφέρει υψηλό κίνδυνο» για τους σκοπούς του κανονισμού 2016/679*, WP 248 αναθ. 01, 4 Οκτωβρίου 2017, σελ. 28-29.

στοιχείο ε)]·

- ☐ μέτρα που συμβάλλουν στην διαφύλαξη των δικαιωμάτων των υποκειμένων των δεδομένων:
  - ☐ πληροφορίες που παρέχονται στο υποκείμενο των δεδομένων (άρθρα 12, 13 και 14):
  - ☐ δικαίωμα πρόσβασης και δικαίωμα στην φορητότητα των δεδομένων (άρθρα 15 και 20)·
  - ☐ δικαίωμα διόρθωσης και διαγραφής (άρθρα 16, 17 και 19)·
  - ☐ δικαίωμα εναντίωσης και περιορισμού της επεξεργασίας (άρθρα 18, 19 και 21)·
  - ☐ σχέσεις με τους εκτελούντες την επεξεργασία (άρθρο 28)·
  - ☐ διασφαλίζονται οι περιστάσεις που περιβάλλουν την διεθνή διαβίβαση ή τις διεθνείς διαβιβάσεις (Κεφάλαιο V)·
  - ☐ προηγούμενη διαβούλευση (άρθρο 36).

☐ <u>τελούν υπό διαχείριση οι κίνδυνοι για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων</u> [άρθρο 35 παράγραφος 7 στοιχείο γ)]:

- ☐ έχουν αξιολογηθεί η προέλευση, η φύση, η ιδιαιτερότητα και η σοβαρότητα των κινδύνων (πρβλ. αιτιολογική σκέψη 84) ή ειδικότερα κάθε κίνδυνος (αθέμιτη πρόσβαση, ανεπιθύμητη τροποποίηση, και εξαφάνιση δεδομένων) από την οπτική των υποκειμένων των δεδομένων·
  - ☐ έχουν ληφθεί υπόψη οι πηγές των κινδύνων (αιτιολογική σκέψη 90)·
  - ☐ εξακριβώνονται οι δυνητικές επιπτώσεις στα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων σε περιπτώσεις συμβάντων που περιλαμβάνουν αθέμιτη πρόσβαση, ανεπιθύμητη τροποποίηση και εξαφάνιση δεδομένων·
  - ☐ εξακριβώνονται απειλές που θα μπορούσαν να επιφέρουν αθέμιτη πρόσβαση, ανεπιθύμητη τροποποίηση και εξαφάνιση δεδομένων·
  - ☐ εκτιμώνται η πιθανότητα και η σοβαρότητα (αιτιολογική σκέψη 90)·
- ☐ καθορίζονται τα προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων (άρθρο 35 παράγραφος 7 στοιχείο δ) και

αιτιολογική σκέψη 90)·

☐ <u>συμμετέχουν τα ενδιαφερόμενα μέρη</u>:

- ☐ ζητείται η γνώμη του ΥΠΔ (άρθρο 35 παράγραφος 2)·
- ☐ ζητείται η γνώμη των υποκειμένων των δεδομένων ή των εκπροσώπων τους, όταν ενδείκνυται (άρθρο 35 παράγραφος 9).

ΠΑΡΑΡΤΗΜΑ ΙΙΙ - ΜΕΘΟΔΟΛΟΓΙΑ ΓΙΑ ΕΚΤΙΜΗΣΗ ΚΙΝΔΥΝΟΥ & ΑΝΤΙΚΤΥΠΟΥ

ΤΕΧΝΟΛΟΓΙΚΟΣ ΕΞΟΠΛΙΣΜΟΣ & ΔΙΚΤΥΟ	
1. Διενεργείται κάποιο μέρος/στάδιο της επεξεργασίας μέσω διαδικτύου; **<u>Παραδείγματα:</u>** • **ηλεκτρονικό κατάστημα που επιτρέπει την αγορά αγαθών διαδικτυακά** • **ηλεκτρονική πύλη ενημέρωσης η οποία προσφέρει εξατομικευμένη πληροφόρηση σε εγγεγραμμένους χρήστες**	Όταν η επεξεργασία διενεργείται αποκλειστικά ή μερικά μέσω του διαδικτύου, οι ενδεχόμενες απειλές από εξωτερικούς επιτιθέμενους αυξάνονται (άρνηση υπηρεσιών, SQL injection) ειδικά όταν η υπηρεσία είναι διαθέσιμη σε όλους τους χρήστες του internet.
2. Είναι δυνατή η πρόσβαση μέσω ίντερνετ στο εσωτερικό σύστημα διαχείρισης προσωπικών δεδομένων; **<u>Παραδείγματα:</u>** • **Ασφαλιστική εταιρεία επιτρέπει στα στελέχη της την απομακρυσμένη πρόσβαση (μέσω ίντερνετ) στους φακέλους των πελατών** • **Εταιρεία παρέχει απομακρυσμένη πρόσβαση στο σύστημά της σε εξωτερικούς τεχνικούς υποστήριξης**	Με την παροχή πρόσβασης στο εσωτερικό σύστημα διαχείρισης προσωπικών δεδομένων μέσω internet η πιθανότητα επέλευσης εξωτερικών κινδύνων αυξάνεται. Ταυτοχρόνως η πιθανότητα τυχαίας ή δόλιας εσωτερικής παραβίασης των προσωπικών δεδομένων επίσης αυξάνεται (π.χ. τυχαία αποκάλυψη προσωπικών πληροφοριών όταν κάποιος εργάζεται σε δημόσιους χώρους). Επίσης πρέπει να δοθεί προσοχή σε περιπτώσεις απομακρυσμένης πρόσβασης στο πληροφοριακό σύστημα της επιχείρησης.
3. Το σύστημα διαχείρισης και επεξεργασίας προσωπικών δεδομένων είναι συνδεδεμένο με άλλο εξωτερικό ή εσωτερικό πληροφοριακό σύστημα ή ηλεκτρονική υπηρεσία; **<u>Παράδειγμα:</u>** **Ένα ηλεκτρονικό βιβλιοπωλείο συνδέεται με ένα ηλεκτρονικό τραπεζικό σύστημα για την πραγματοποίηση ηλεκτρονικών αγορών.** **Το πληροφοριακό χρηματοπιστωτικό σύστημα μία ς μικρής κλινικής είναι συνδεδεμένο με το εθνικό πληροφοριακό ασφαλιστικό σύστημα για να μπορεί να ταυτοποιείται η ασφαλιστική ενημερότητα των ασθενών.**	Η διασύνδεση με εξωτερικά πληροφοριακά συστήματα μπορεί να δημιουργήσει περισσότερες απειλές λόγω των κινδύνων και των πιθανών κενών ασφαλείας που είναι εγγενή στην διασύνδεση συστημάτων. Το ίδιο ισχύει και με τα εσωτερικά συστήματα, αν ληφθεί υπ' όψιν ότι η μη ορθή παραμετροποίηση των συνδέσεων μπορεί να επιτρέψει την πρόσβαση σε προσωπικά δεδομένα σε περισσότερα άτομα του οργανισμού.
4. Μπορούν εύκολα μη εξουσιοδοτημένοι χρήστες	Αν και ιδιαίτερη έμφαση έχει δοθεί στα

να αποκτήσουν πρόσβαση στο περιβάλλον επεξεργασίας προσ. **δεδομένων;** **<u>Παραδείγματα:</u>** • **Μια μικρομεσαία επιχείρηση δεν διαθέτει ξεχωριστό γραφείο υπολογιστών για την διαχείριση-επίβλεψη του λογισμικού επεξεργασίας προσωπικών δεδομένων.** • **Μια μικρομεσαία επιχείρηση έχει νοικιάσει απομακρυσμένα αποθηκευτικό χώρο για τα δεδομένα της και δεν είναι σαφές ποια μέτρα ασφαλείας έχει λάβει η εταιρεία για την φύλαξη των εγκαταστάσεων του data center.**	ηλεκτρονικά συστήματα και τα δίκτυα, το φυσικό περιβάλλον που τα αφορά είναι επίσης κρίσιμο, και αν δεν φυλάσσεται επαρκώς μπορεί κάλλιστα να διακινδυνεύσει η ασφάλεια (π.χ. επιτρέποντας μη εξουσιοδοτημένα άτομα να πάρουν τον φυσικό έλεγχο του τεχνολογικού εξοπλισμού και του δικτύου)
5. Το σύστημα διαχείρισης των προσωπικών δεδομένων έχει σχεδιαστεί, υλοποιηθεί και συντηρηθεί ακολουθώντας τεκμηριωμένες καλές πρακτικές; **<u>Παραδείγματα καλών πρακτικών:</u>** • **Η προμήθεια του hardware και του software της επιχείρησης γίνεται από εγκεκριμένους επαγγελματίες με επίσημες συναλλακτικές διαδικασίες.** • **Υπάρχει πλάνο συντήρησης και υποστήριξης όλου του πληροφοριακού συστήματος, περιλαμβανομένου του τακτικού ελέγχου του δικτύου, των διασυνδεδεμένων συσκευών και των χρησιμοποιούμενων εφαρμογών.**	Το κακώς σχεδιασμένο, υλοποιημένο ή/και συντηρημένο hardware και software μπορεί να αποδειχθεί σοβαρή απειλή για την ασφάλεια του πληροφοριακού συστήματος. Για τον σκοπό αυτό, οι καλές πρακτικές πρέπει να ακολουθούνται ως πρακτικές οδηγίες για την αποφυγή δυσλειτουργιών και την επίτευξη ενός επιπέδου ελαστικότητας.
ΕΠΙΧΕΙΡΗΣΙΑΚΕΣ ΔΙΑΔΙΚΑΣΙΕΣ ΣΧΕΤΙΚΕΣ ΜΕ ΤΗΝ ΕΠΕΞΕΡΓΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ	
6. Μήπως οι ρόλοι και οι αρμοδιότητες των υπαλλήλων σχετικά με την επεξεργασία προσωπικών δεδομένων δεν είναι ξεκάθαροι και σαφώς προκαθορισμένοι; **<u>Παραδείγματα:</u>** • **Οι βοηθοί στο Λογιστήριο έχουν την δυνατότητα όχι μόνο να εισάγουν στοιχεία, αλλά και να τα τροποποιούν και να τα διαγράφουν, όπως και οι προϊστάμενοι.** • **Οι νοσοκόμες μία ς κλινικής μπορούν να τροποποιούν τον ιατρικό φάκελο ενός**	Όταν οι ρόλοι και οι αρμοδιότητες δεν είναι σαφώς προσδιορισμένοι, η πρόσβαση (και η περαιτέρω επεξεργασία) των προσωπικών δεδομένων μπορεί να καταστεί ανεξέλεγκτη, με συνέπεια την μη εξουσιοδοτημένη χρήση τους και την διακινδύνευση της ασφάλειάς τους εν γένει.

ασθενή, αν και μόνο οι γιατροί θα έπρεπε να έχουν τέτοια δυνατότητα.	
7. Μήπως η αποδεκτή χρήση του δικτύου, του συστήματος και των φυσικών πόρων της επιχείρησης δεν είναι σαφής ή σαφώς προσδιορισμένη; **<u>Παραδείγματα:</u>** • **Δεν είναι ξεκάθαρο εάν οι εργαζόμενοι μπορούν να χρησιμοποιούν την επαγγελματική τους ηλεκτρονική διεύθυνση για προσωπικές τους επικοινωνίες.** • **Δεν υπάρχει εσωτερική πολιτική στην επιχείρηση για το επιτρεπόμενο επίπεδο bandwidth που μπορούν να χρησιμοποιούν οι εργαζόμενοι σε καθημερινή βάση.**	Εάν η πολιτική ορθή χρήσης των πόρων δεν είναι σαφής, μπορεί να ανακύψουν ζητήματα ασφαλείας είτε λόγω παρανόησης των κανόνων είτε λόγω ηθελημένης κακοδιαχείρισης του συστήματος.
8. Επιτρέπεται οι εργαζόμενοι να χρησιμοποιούν δικές τους συσκευές για να συνδέονται στο σύστημα διαχείρισης προσωπικών δεδομένων; **<u>Παραδείγματα:</u>** **Οι εργαζόμενοι μπορούν να συνδέονται στο δίκτυο της επιχείρησης από το tablet τους ή άλλη smart συσκευή ή ακόμα και να επεξεργάζονται προσωπικά δεδομένα χρησιμοποιώντας συγκεκριμένες εφαρμογές εγκατεστημένες στις προσωπικές τους συσκευές.**	Αυτές οι πρακτικές αυξάνουν τον κίνυδνο της διαρροής δεδομένων ή της μη εξουσιοδοτημένης πρόσβασης στο πληροφοριακό σύστημα. Επιπλέον, μία ς και οι συσκευές δεν είναι πλήρως ελέγξιμες, μπορεί να εισάγουν ιούς ή άλλα σφάλματα στο σύστημα.
9. Επιτρέπεται οι εργαζόμενοι να μεταφέρουν, να αποθηκεύουν ή να επεξεργάζονται με οποιονδήποτε τρόπο έξω από τις εγκαταστάσεις της επιχείρησης προσωπικά δεδομένα που ανήκουν σε αυτήν; **<u>Παραδείγματα:</u>** **Ένα τουριστικό πρακτορείο επιτρέπει στους υπαλλήλους του να χρησιμοποιούν τα επαγγελματικά τους laptops εκτός γραφείου προκειμένου να επεξεργαστούν αρχεία πελατών.**	Η επεξεργασία δεδομένων εκτός γραφείου μπορεί να προσφέρει μεγάλη ευελιξία, αλλά ταυτοχρόνως δημιουργεί επιπρόσθετους κινδύνους, τόσο λόγω της μετάδοσης των δεδομένων μέσω ανασφαλών συνδέσεων όσο και λόγω πιθανής μη εξουσιοδοτημένης χρήσης τους.
10. Είναι δυνατόν να εκτελεστούν ενέργειας επεξεργασίας προσωπικών δεδομένων χωρίς την αντίστοιχη δημιουργία αρχείων log (αρχείο	Η απουσία επαρκούς καταγραφικής και ελέγχουν των μηχανισμών μπορεί να αυξήσει

καταγραφής δραστηριότητας; **<u>Παραδείγματα:</u>** • **Δεν υπάρχει λίστα με τους υπαλλήλους που έχουν πρόσβαση στο γραφείο υπολογιστών σε καθημερινή βάση.** • **Δεν απαιτούνται κωδικοί πρόσβασης από τον χρήστη για να συνδεθεί στο αρχείο ιατρικών φακέλων των ασθενών.** • **Δεν έχει συνταχθεί πολιτική σχετικά με την επίβλεψη των αρχείων καταγραφής δραστηριοτήτων και την επέμβαση σε περίπτωση επανειλημμένων περιπτώσεων κακοδιαχείρισης.**	την τυχαία ή την επί τούτου κακοδιαχείριση των διαδικασιών κσι των πόρων, καταλήγοντας στην αναπόφευκτη κακοδιαχείριση των δεδομένων.
Ο ΑΝΘΡΩΠΙΝΟΣ ΠΑΡΑΓΟΝΤΑΣ ΣΤΗΝ ΕΠΕΞΕΡΓΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ	
11. Η επεξεργασία των προσωπικών δεδομένων εκτελείται από ακαθόριστο αριθμό υπαλλήλων; **<u>Παραδείγματα:</u>** **Όλοι οι υπάλληλοι έχουν πρόσβαση στο σύστημα διαχείρισης ανθρώπινου δυναμικού.** **Τα ιατρικά αρχεία των ασθενών μπορούν να τα επεξεργαστεί και το διοικητικό προσωπικό αν και θα έπρεπε να έχει πρόσβαση σε αυτά μόνο το νοσηλευτικό προσωπικό.**	Όταν η πρόσβαση και η επεξεργασία των προσωπικών δεδομένων είναι ανοιχτή σε μεγάλο αριθμό υπαλλήλων, οι πιθανότητες κακοδιαχείρισης λόγω του ανθρώπινου παράγοντα αυξάνεται. Ο σαφής προσδιορισμός για το ποιος πρέπει να έχει πρόσβαση στα δεδομένα και ο περιορισμός της πρόσβασης μόνο σε αυτούς συμβάλλει στην ασφάλειά τους.
12. Μέρος της επεξεργασίας των δεδομένων εκτελείται από εργολάβο ή τρίτο; **<u>Παράδειγμα:</u>** **Το πληροφοριακό σύστημα ενός ιδιωτικού σχολείου φιλοξενείται σε ένα εξωτερικό data center.** **Εξωτερικοί συνεργάτες μία ς ασφαλιστικής εταιρείας επεξεργάζονται τα αρχεία των πελατών της.** **Μια κλινική έχει συμβληθεί με εξειδικευμένη εταιρία για την καταστροφή των αρχείων των ασθενών.**	Όταν η επεξεργασία διενεργείται από εξωτερικούς συνεργάτες, ο οργανισμός μπορεί να χάσει μερικώς τον έλεγχο επί των προσωπικών δεδομένων που Επιπλέον, μπορεί να προκύψουν επιπρόσθετοι κίνδυνοι ασφαλείας λόγω των κινδύνων που ενυπάρχουν ήδη εξ ορισμού σε αυτές τις συμβάσεις. Η κάθε επιχείρηση θα πρέπει να δείχνει ιδιαίτερη προσοχή στους συνεργάτες που επιλέγει και να προκαθορίζει σαφώς το εύρος της επεξεργασίας που τους ανατίθεται.

13. Οι υποχρεώσεις και τα καθήκοντα των μερών και των προσώπων που εμπλέκονται στην επεξεργασία είναι σαφώς καθορισμένες εκ των προτέρων; **<u>Παράδειγμα:</u>** **Οι υπάλληλοι δεν έχουν ενημερωθεί ότι επεξεργάζονται εμπιστευτικές πληροφορίες οι οποίες δεν πρέπει να κοινοποιηθούν σε τρίτους.** **Οι εξωτερικοί συνεργάτες της επιχείρησης δεν έχουν λάβει σαφείς οδηγίες σχετικά με το επίπεδο ασφαλείας των προσωπικών δεδομένων που έχουν αναλάβει να επεξεργαστούν.**	Εάν οι υπάλληλοι δεν είναι επαρκώς ενημερωμένοι για τις υποχρεώσεις και τα καθήκοντά τους, μπορεί ανακύψουν παραβιάσεις από τυχαία ή εξ αμελείας κοινοποίηση πληροφοριών.
14. Είναι εκπαιδευμένο το προσωπικό που εμπλέκεται στην επεξεργασία προσωπικών δεδομένων σε θέματα ασφαλείας;	Όταν οι υπάλληλοι δεν είναι ενημερωμένοι για την ανάγκη χρήσης μέτρων ασφαλείας, αποτελούν δυνητικά κίνδυνο για το σύστημα. Η εκπαίδευσή τους είναι απαραίτητη τόσο για την κατανόηση των υποχρεώσεών τους όσο και για την εκμάθηση χρήσης και εφαρμογής συγκεκριμένων μέτρων ασφαλείας.
15. Τα άτομα που εμπλέκονται με την επεξεργασία των προσωπικών δεδομένων αδιαφορούν για την ασφαλή αποθήκευση ή καταστροφή τους; **<u>Παράδειγμα:</u>** **Αντίγραφα τιμολογίων με πληροφορίες πιστωτικών καρτών ή τραπεζικών λογαριασμών δεν καταστρέφονται μετά την επεξεργασία τους.** **Τα αρχεία του υπαλληλικού προσωπικού δεν αποθηκεύονται σε ασφαλή συρτάρια που κλειδώνουν.**	Πολλές παραβιάσεις προσωπικών δεδομένων συμβαίνουν λόγω έλλειψης φυσικών μέτρων προστασίας, όπως κλειδαριές και καταστροφείς εγγράφων. Τα φυσικά έγγραφα αποτελούν σύνηθες μέσο της ροής του πληροφοριακού συστήματος και περιλαμβάνουν προσωπικές πληροφορίες οι οποίες θα πρέπει να προστατεύονται από την δημοσίευσή τους σε μη εξουσιοδοτημένους χρήστες.
ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΣ ΚΛΑΔΟΣ ΚΑΙ ΚΛΙΜΑΚΑ ΕΠΕΞΕΡΓΑΣΙΑΣ	
16. Ο τομέας δραστηριοποίησής σας είναι πιθανός στόχος επιθέσεων; **<u>Παραδείγματα</u>** **Αρκετές επιχειρήσεις (του ίδιου κλάδου) δέχθηκαν επίθεση πρόσφατα.** **Έχει δοθεί δημοσιότητα σε πιθανούς κινδύνους και σε κενά ασφαλείας σε συγκεκριμένο επιχειρηματικό κλάδο (π.χ. ως αποτέλεσμα**	Όταν έχουν ήδη λάβει χώρα επιθέσεις ασφαλείας σε κάποιον επιχειρηματικό κλάδο, υπάρχει ένδειξη ότι η επιχειρήσεις του κλάδου αυτού θα πρέπει να λάβουν επιπρόσθετα μέτρα ασφαλείας.

επιστημονικής μελέτης)	
17. Έχει δεχθεί η επιχείρησή σας κάποια κυβερνοεπίθεση ή άλλου είδους παραβίαση ασφαλείας τα τελευταία δύο χρόνια; **<u>Παραδείγματα</u>** **Οι κλειδαριές στο κεντρικό data center βρέθηκαν παραβιασμένες.** **Το Τμήμα Πληροφορικής έχει ανιχνεύσει πολλές ανεπιτυχείς προσπάθειες για απόκτηση μη εξουσιοδοτημένης πρόσβασης στην βάση δεδομένων.**	Εάν ο οργανισμός έχει ήδη δεχθεί επίθεση ή υπάρχουν ενδείξεις ότι έχει γίνει στόχος, πρέπει να ληφθούν πρόσθετα μέτρα ασφαλείας.
18. Έχει λάβει η επιχείρησή σας ειδοποιήσεις ή παράπονα σχετικά με την ασφάλεια του πληροφοριακού σας συστήματος (το οποίο χρησιμοποιείται και για την επεξεργασία προσωπικών δεδομένων) τον τελευταίο χρόνο; **<u>Παράδειγμα:</u>** **Οι χρήστες ενός διαδικτυακού καταστήματος έχουν αναφέρει ότι κατά λάθος το σύστημα τους έδωσε πρόσβαση σε λογαριασμούς άλλων χρηστών.**	Τυχόν κενά ασφαλείας μπορούν να χρησιμοποιηθούν για την εκτέλεση επιθέσεων (ψηφιακών ή φυσικών) στο σύστημα και στις παρεχόμενες υπηρεσίες. Πληροφορίες σχετικά με τέτοιες ολοκληρωμένες επιθέσεις ή απόπειρες αυτών πρέπει να αξιολογούνται και να προλαμβάνονται.
19. Οι δραστηριότητες επεξεργασίας της επιχείρησής σας αφορούν μεγάλη κλίμακα πληθυσμού; **<u>Παράδειγμα</u>** **Μια ιστοσελίδα γνωριμιών όπου αποθηκεύονται τα προφίλ εκατοντάδων χρηστών.**	Το είδος και ο όγκος των επεξεργαζόμενων προσωπικών δεδομένων μπορούν να τα καταστήσουν ελκυστικά για εξαπόλυση επιθέσεων (λόγω της εγγενούς αξίας τους).
20. Έχουν προβλεφθεί καλές πρακτικές για τον επιχειρηματικό κλάδο που δραστηριοποιείστε τις οποίες δεν έχετε ενσωματώσει στο πληροφοριακό σας σύστημα; **<u>Παραδείγματα:</u>** **Μια εταιρεία πρέπει να λάβει συγκεκριμένα μέτρα ασφαλείας για ιατρικές συσκευές, οικονομικές υπηρεσίας ή υπηρεσίες τηλεπικοινωνιών.**	Τα συγκεκριμένα ανά κλάδο μέτρα ασφαλείας είναι προσαρμοσμένα στις ανάγκες και τους κινδύνους που σχετίζονται με τον εκάστοτε κλάδο. Η μη συμμόρφωση με αυτές τις καλές πρακτικές αποτελεί ένδειξη ελλιπούς πολιτικής ασφαλείας.

Πίνακας 3: Ερωτηματολόγιο για τον προσδιορισμό των κινδύνων και της πιθανότητας πραγμάτωσής τους

Εφόσον απαντηθεί το ερωτηματολόγιο η εκάστοτε επιχείρηση είναι σε θέση να αντιληφθεί πληρέστερα τους κινδύνους που συνδέονται με τις πράξεις επεξεργασίας που εκτελεί, την πιθανότητα επέλευσης αυτών, καθώς και το γενικότερο πλαίσιο της πολιτικής προστασίας που θα πρέπει να ακολουθήσει. Όπως επισημαίνει και ο Enisa, ως συντάκτης του ως άνω ερωτηματολογίου, οι ερωτήσεις αν και στοχεύουν να καλύψουν μεγάλο μέρος τόσο των εξωτερικών όσο και των εσωτερικών κινδύνων ασφαλείας, δεν μπορεί να θεωρηθούν ότι εξαντλούν την ανάγκη εκτίμησης της επικινδυνότητας· θα πρέπει να ληφθούν υπ' όψιν όχι μόνο επιπρόσθετοι παράγοντες, ανάλογοι του τομέα δραστηριοποίησης της κάθε επιχείρησης, αλλά και οι ειδικότερες συνθήκες εκτέλεσης των πράξεων επεξεργασίας της εκάστοτε επιχείρησης.

Όπως προαναφέρθηκε και για την εκτίμηση του επιπέδου του κινδύνου, η διαβάθμιση μπορεί να είναι μόνο ποιοτική και να συνδέεται με τις συγκεκριμένες συνθήκες του εκάστοτε περιβάλλοντος επεξεργασίας προσωπικών δεδομένων. Ως εκ τούτου και τα επίπεδα πιθανότητας επέλευσης του κινδύνου είναι ανάλογα· δηλαδή:

Υψηλό: ο κίνδυνος μάλλον θα επέλθει

Μέτριο: ο κίνδυνος είναι πιθανόν να επέλθει

Χαμηλό: ο κίνδυνος δεν είναι πιθανόν να επέλθει

Στο προτελευταίο στάδιο θα πρέπει να γίνει μία γενική εκτίμηση της πιθανότητας επέλευσης κινδύνων στους διαφορετικούς τομείς που καθορίζονται στο ερωτηματολόγιο του Πίνακα 3. Σύμφωνα με τον 4ο Πίνακα του Enisa, η επιχείρηση που έχει απαντήσει θετικά σε όλες τις ερωτήσεις του εκάστοτε τομέα θα πρέπει να θέσει το επίπεδο επικινδυνότητας στο υψηλό, ενώ εάν έχει απαντήσει αρνητικά στις ερωτήσεις του εκάστοτε τομέα θα θέσει το επίπεδο επικινδυνότητας στο χαμηλό. Στις περιπτώσεις με 2-3 θετικές απαντήσεις το επίπεδο επικινδυνότητας προσδιορίζεται σε μέτριο.

ΤΟΜΕΑΣ	**ΠΙΘΑΝΟΤΗΤΑ**	
	ΕΠΙΠΕΔΟ	**ΒΑΘΜΟΙ**
ΤΕΧΝΟΛΟΓΙΚΟΣ ΕΞΟΠΛΙΣΜΟΣ & ΔΙΚΤΥΟ	☐ ΧΑΜΗΛΟ	1
	☐ ΜΕΤΡΙΟ	2
	☐ ΥΨΗΛΟ	3

ΕΠΙΧΕΙΡΗΣΙΑΚΕΣ ΔΙΑΔΙΚΑΣΙΕΣ ΣΧΕΤΙΚΕΣ ΜΕ ΤΗΝ ΕΠΕΞΕΡΓΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ	☐ ΧΑΜΗΛΟ	1
	☐ ΜΕΤΡΙΟ	2
	☐ ΥΨΗΛΟ	3
Ο ΑΝΘΡΩΠΙΝΟΣ ΠΑΡΑΓΟΝΤΑΣ ΣΤΗΝ ΕΠΕΞΕΡΓΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ	☐ ΧΑΜΗΛΟ	1
	☐ ΜΕΤΡΙΟ	2
	☐ ΥΨΗΛΟ	3
ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΣ ΚΛΑΔΟΣ ΚΑΙ ΚΛΙΜΑΚΑ ΕΠΕΞΕΡΓΑΣΙΑΣ	☐ ΧΑΜΗΛΟ	1
	☐ ΜΕΤΡΙΟ	2
	☐ ΥΨΗΛΟ	3

Πίνακας 4: Εκτίμηση πιθανότητας επέλευσης κινδύνου ανά τομέα

Η συνολική εκτίμηση της πιθανότητας επέλευσης κινδύνων γίνεται με την πρόσθεση των βαθμών που συγκεντρώνει η κάθε κατηγορία του Πίνακα 4:

ΒΑΘΜΟΙ ΠΙΘΑΝΟΤΗΤΑΣ ΕΠΕΛΕΥΣΗΣ ΚΙΝΔΥΝΟΥ	**ΕΠΙΠΕΔΟ ΠΙΘΑΝΟΤΗΤΑΣ ΕΠΕΛΕΥΣΗΣ ΚΙΝΔΥΝΟΥ**
4-5	ΧΑΜΗΛΟ
6-8	ΜΕΤΡΙΟ
9-12	ΥΨΗΛΟ

Πίνακας 5: Εκτίμηση πιθανότητας επέλευσης κινδύνου

Η τελική Εκτίμηση του Κινδύνου και του Αντικτύπου προκύπτει συνδυάζοντας τα αποτελέσματα που δίνουν οι Πίνακες 2 και 5 ως εξής:

		ΕΠΙΠΕΔΟ ΑΝΤΙΚΤΥΠΟΥ		
		ΧΑΜΗΛΟ	ΜΕΤΡΙΟ	ΥΨΗΛΟ
ΠΙΘΑΝΟΤΗΤΑ	ΧΑΜΗΛΟ			
ΕΠΕΛΕΥΣΗΣ	ΜΕΤΡΙΟ			
ΚΙΝΔΥΝΟΥ	ΥΨΗΛΟ			

ΧΑΜΗΛΟ ΜΕΤΡΙΟ ΥΨΗΛΟ

Πίνακας 6: Εκτίμηση Κινδύνου

ΠΑΡΑΡΤΗΜΑ IV – ΥΠΟΔΕΙΓΜΑ ΑΡΧΕΙΟΥ ΤΗΡΗΣΗΣ ΔΡΑΣΤΗΡΙΟΤΗΤΩΝ

(1) Δραστηριότητα Επεξεργασίας	(2) Κύρια ή Παρεπόμενη	(3) Νομική Βάση	(4) Υπεύθυνος ή Εκτελών την Επεξεργασία ή τυχόν εκπρόσωπός τους		(5) Σκοπός	(6) Κατηγορίες (α) Υποκειμένων Δεδομένων και (β) Προσωπικών Δεδομένων		(7) Κατηγορίες Αποδεκτών	(8) Διαβίβαση Δεδομένων σε τρίτην χώρα διεθνή οργανισμό	(9) Προβλεπό-μενη Περίοδος Διαγραφής	(10) Τεχνικά και Οργανωτικά Μέτρα Ασφάλειας	(11) Εκτίμηση αντίκτυπου / προηγούμενη διαβούλευση		(12) Ενημέρωση στα Υποκείμενα Δεδομένων
			(α) Ιδιότητα	(β) Όνομα & Στοιχεία Επικ/νίας		(α)	(β)					(α) Ε.Α.	(β) Προηγού-μενη διαβούλευση	

ΠΑΡΑΡΤΗΜΑ V - ΣΥΓΚΑΤΑΘΕΣΗ

Έντυπο Ενημέρωσης & Δήλωσης Συναίνεσης

για την επεξεργασία προσωπικών δεδομένων σύμφωνα με τον Γενικό Κανονισμό για την Προστασία Δεδομένων Ε.Ε. 679/2016

Η Εταιρεία δηλώνει ότι στα πλαίσια άσκησης των δραστηριοτήτων της και για την παροχή των υπηρεσιών της συλλέγει, φυλάσσει και επεξεργάζεται Δεδομένα Προσωπικού Χαρακτήρα (Προσωπικά Δεδομένα) των συμβαλλόμενων φυσικών προσώπων, σύμφωνα με τον Γενικό Κανονισμό Προστασίας Δεδομένων ΕΕ 2016/679 και την εκάστοτε εν ισχύϊ εθνική Νομοθεσία, όπως αυτά εκάστοτε τροποποιούνται, για τους παρακάτω σκοπούς:

1. Την καταχώριση και την τήρηση των προσωπικών μου δεδομένων στα συστήματα της εταιρείας προκειμένου να εκπληρωθούν ομαλά οι υποχρεώσεις των μερών της σύμβασης, με δικαίωμα πρόσβασης σε αυτά αποκλειστικά του προσωπικού της εταιρείας και μόνο για την συμφωνημένη παροχή υπηρεσιών.

Συναινώ Δεν συναινώ

2. Την προώθηση και εμπορική επικοινωνία για άλλες υπηρεσίες ή προϊόντα της επιχείρησης που σχετίζονται ή όχι με την ήδη καταρτισθείσα σύμβαση.

Συναινώ Δεν συναινώ

3. Την προώθηση και εμπορική επικοινωνία για συναφείς υπηρεσίες ή προϊόντων συνεργαζόμενων τρίτων επιχειρήσεων.

Συναινώ Δεν συναινώ

4. Την διαμόρφωση προφίλ σχετικά με την συμπεριφορά και τις προτιμήσεις μου με σκοπό την παροχή εξειδικευμένης εξυπηρέτησης και πρότασης εξατομικευμένων λύσεων.

Συναινώ Δεν συναινώ

II. Συνέπειες μη παροχής συναίνεσης ή ανάκλησής της

[……]

III. Δηλώνω ότι προ και δια της υπογραφής της παρούσας έλαβα γνώση των ειδικότερων δικαιωμάτων που μου παρέχει ο ως άνω Κανονισμός (ΕΕ) 2016/679, και ειδικότερα:

- Το δικαίωμα πληροφόρησης και λήψης επιβεβαίωσης για το εάν τα δεδομένα προσωπικού χαρακτήρα που με αφορούν και βρίσκονται στην κατοχή του υφίστανται επεξεργασία, εντός μηνός από την υποβολή του αιτήματος.
- Το δικαίωμα πρόσβασής μου στα δεδομένα προσωπικού χαρακτήρα.
- Το δικαίωμα προηγούμενης ενημέρωσής μου και συγκατάθεσής μου για την κοινοποίηση/ διαβίβαση δεδομένων μου προς πιθανούς αποδέκτες στους οποίους μπορεί να κοινολογηθούν τα δεδομένα προσωπικού χαρακτήρα, ιδίως τους αποδέκτες σε τρίτες χώρες ή διεθνείς οργανισμούς.

- Το δικαίωμά μου για την υποβολή αιτήματος περί διόρθωσης ή διαγραφής δεδομένων προσωπικού χαρακτήρα ή περιορισμό της επεξεργασίας αυτών.

- Το δικαίωμα λήψης αντιγράφων, και σε ηλεκτρονική μορφή, δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία.

- Έλαβα επίσης γνώση ότι προσωπικά δεδομένα μου θα αποθηκευτούν για ορισμένο χρονικό διάστημα, σχετιζόμενο με τους σκοπούς της επεξεργασίας αυτών αποκλειστικά για ιατρικούς λόγους.

- Το δικαίωμά μου να αντιταχθώ στο μέλλον στην επεξεργασία προσωπικών δεδομένων μου.

- Το δικαίωμά μου να ανακαλέσω την παρούσα συγκατάθεση, ανά πάσα στιγμή.

- Το δικαίωμά μου να υποβάλλω καταγγελία στην Αρχή Προστασίας Προσωπικών Δεδομένων, ως εποπτική αρχή του υπεύθυνου επεξεργασίας, εάν κρίνω ότι υφίσταται παραβίαση των δικαιωμάτων μου.

IV.Για την άσκηση των παραπάνω δικαιωμάτων σας και για οποιοδήποτε ερώτημα, παράπονο που αφορά προσωπικά δεδομένα, μπορείτε να απευθύνεστε στον Υπεύθυνο Προστασίας Δεδομένων:

- με αποστολή e-mail στην διεύθυνση με θέμα GDPR ….

- με αποστολή σχετικής επιστολής, με την ένδειξη “GDPR” ….

Στοιχεία επικοινωνίας και προσφυγής προς την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα:

Ιστοσελίδα: www.dpa.gr

Ταχυδρομική Διεύθυνση: Λεωφόρος Κηφισίας 1-3, Τ.Κ. 115 23, Αθήνα

Τηλεφωνικό Κέντρο: +30 210 6475600 Fax: +30 210 6475628

Ηλεκτρονικό Ταχυδρομείο: contact@dpa.gr

V. Έχω επίσης ενημερωθεί ότι: - η Πολιτική Προστασίας Δεδομένων Προσωπικού Χαρακτήρα της Εταιρείας είναι διαθέσιμη στον ιστότοπο ……

Ο/η κάτωθι υπογραφόμενος/η διάβασε με προσοχή την παρούσα Ενημέρωση και Δήλωση Συναίνεσης για την προστασία των προσωπικών δεδομένων και την αποδέχεται δίνοντας την ελεύθερη, ειδική, ρητή και με πλήρη επίγνωση συγκατάθεσή του/της.

Ημερομηνία …….. Τόπος υπογραφής ……

ΒΙΒΛΙΟΓΡΑΦΙΑ

Αλεξανδροπούλου – Αιγυπτιάδου Ευγενία, *Προσωπικά Δεδομένα*, Νομική Βιβλιοθήκη, 2016.

Ιγγλεζάκης Ιωάννης, *Δίκαιο Πληροφορικής*, Εκδόσεις Σάκκουλας, 2018.

Κοτσαλής Λεωνίδας, *Προσωπικά Δεδομένα*, Νομική Βιβλιοθήκη, 2016.

Jaap-Henk Hoepman, *Privacy Design Strategies – The Little Blue Book*, January 2019.

Enisa, *Guidelines for SMEs on the security of personal data processing*, www.enisa.europa.eu, Δεκέμβριος 2016.

Enisa, *Handbook on Security of Personal Data Processing*, www.enisa.europa.eu, Δεκέμβριος 2017.

Enisa, *Recommendations on shaping technology according to GDPR provisions - An overview on data pseudonymisation*, www.enisa.europa.eu, Δεκέμβριος 2018.

Enisa, *Privacy and Data Protection by Design – from policy to engineering*, www.enisa.europa.eu, Δεκέμβριος 2014.

Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (FRA) & Συμβούλιο της Ευρώπης, *Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων*, 2014.

European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European data protection law*, 2018. https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law

Ομάδα Προστασίας των προσώπων έναντι της Επεξεργασίας δεδομένων προσωπικού Χαρακτήρα του άρθρου 29, *Γνώμη 4/2007 σχετικά με την έννοια των δεδομένων προσωπικού χαρακτήρα*, WP 136, 20 Ιουνίου 2007.

Ομάδα Προστασίας των προσώπων έναντι της Επεξεργασίας δεδομένων προσωπικού Χαρακτήρα του άρθρου 29, *Γνώμη 1/2010 σχετικά με τις έννοιες του «υπευθύνου της επεξεργασίας» και του «εκτελούντος την επεξεργασία»*, wp 169, 16 Φεβρουαρίου 2010.

Ομάδα Προστασίας των προσώπων έναντι της Επεξεργασίας δεδομένων προσωπικού Χαρακτήρα του άρθρου 29, *Γνώμη 3/2010 σχετικά με την αρχή της λογοδοσίας*, WP 173, 13 Ιουλίου 2010.

Ομάδα Προστασίας των προσώπων έναντι της Επεξεργασίας δεδομένων προσωπικού Χαρακτήρα του άρθρου 29, *Κατευθυντήριες γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων*, wp 243 rev. 01, 5 Απριλίου 2017.

Ομάδα Προστασίας των προσώπων έναντι της Επεξεργασίας δεδομένων προσωπικού Χαρακτήρα του άρθρου 29, *Κατευθυντήριες γραμμές σχετικά με το δικαίωμα στη φορητότητα των δεδομένων*, WP 242 rev.01, 5 Απριλίου 2017.

Ομάδα Προστασίας των προσώπων έναντι της Επεξεργασίας δεδομένων προσωπικού Χαρακτήρα του άρθρου 29, *Γνώμη 2/2017 σχετικά με την επεξεργασία δεδομένων στην εργασία*, WP 249, 8 Ιουνίου 2017.

ARTICLE 29 DATA PROTECTION WORKING PARTY, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, WP 251, 3 October 2017.

Ομάδα Προστασίας των προσώπων έναντι της Επεξεργασίας δεδομένων προσωπικού Χαρακτήρα του άρθρου 29, *Κατευθυντήριες γραμμές για την εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) και καθορισμός του κατά πόσον η επεξεργασία «ενδέχεται να επιφέρει υψηλό κίνδυνο» για τους σκοπούς του κανονισμού 2016/679*, WP 248 αναθ. 01, 4 Οκτωβρίου 2017.

Ομάδα Προστασίας των προσώπων έναντι της Επεξεργασίας δεδομένων προσωπικού Χαρακτήρα του άρθρου 29, *Κατευθυντήριες γραμμές σχετικά με τη συγκατάθεση*

βάσει του κανονισμού 2016/679, WP259 αναθ.01, 10 Απριλίου 2018.

Απόφαση 205/2013 της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.) – Κανονισμός για την Ασφάλεια και την Ακεραιότητα Δικτύων και Υπηρεσιών Ηλεκτρονικών Επικοινωνιών, ΦΕΚ Β΄, Φ. 1742/15-7-2013.

01/2013 Κοινή Πράξη της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Α.Π.Δ.Π.Χ.) και της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.) ως προς τις υποχρεώσεις των παρόχων για την προστασία και ασφάλεια των δεδομένων σύμφωνα με τις διατάξεις του άρθρου 7 του ν. 3917/2011, ΦΕΚ Β΄, Φ. 3433/31-12-2013.

Gabriel Maldoff, *The Risk-based Approach in the GDPR: Interpretation and Implications*, International Association of Privacy Professionals (IAPP). https://iapp.org/media/pdf/resource_center/GDPR_Study_Maldoff.pdf

Information Commissioner's Office, *Guidance on the rules on use of cookies and similar technologies*, Privacy and Electronic Communications Regulations. https://ico.org.uk/media/for-organisations/documents/1545/cookies_guidance.pdf

Θανάσης Δαβαλάς**,** *GDPR και cookies | Τι χρειάζεται να γνωρίζω; | Συμμορφώνεται η ιστοσελίδα μου με την χρήση cookies;*, https://www.dreamweaver.gr/gdpr-cookies.php?fbclid=IwAR0iQiwcA9j4bcTcZ3A7oKs9kHN0J6sOSvlk0oXmUYx5vR4OG9JLSCPdp1M

Κωνσταντίνος Φ. Μενουδάκος, *Ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR): ευκαιρίες και προκλήσεις για τις επιχειρήσεις στην εποχή της ψηφιοποίησης*, ΤΕΥΧΟΣ 23 | 14 Μαρτίου 2018, ΟΙΚΟΝΟΜΙΑ & ΕΠΙΧΕΙΡΗΣΕΙΣ, ΣΕΒ.

http://www.sev.org.gr/Uploads/Documents/50953/SPECIAL%20REPORT_14_3_2018.pdf

Sean Cox, The Pros and Cons of Internal vs. Outsourced Information Technology and Data Privacy Management, March 2017

https://www.hospitalityupgrade.com/_magazine/MagazineArticles/The-Pros-and-

Cons-of-Internal-vs-Outsourced-Information-Technology-and-Data-Privacy-Management.asp

Robert Waitman, Companies worldwide recognize business benefits of privacy, Feb 2019.

https://iapp.org/news/a/companies-worldwide-recognize-business-benefits-of-privacy/#

- http://www.dpa.gr
- http://www.dataprotection.gov.cy
- https://www.lawspot.gr/GDPR