



ΔΙΑΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ (Δ.Π.Μ.Σ.)

«ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ»

ΤΜΗΜΑΤΟΣ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΜΑΚΕΔΟΝΙΑΣ

ΚΑΙ

ΤΜΗΜΑΤΟΣ ΝΟΜΙΚΗΣ ΔΗΜΟΚΡΙΤΕΙΟΥ ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΘΡΑΚΗΣ

Master of Science in «Law and Informatics»

# Η ΕΚΤΙΜΗΣΗ ΑΝΤΙΚΤΥΠΟΥ ΣΤΟ ΠΛΑΙΣΙΟ ΤΗΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Διπλωματική Εργασία

της

Κασσιανής Αποστολοπούλου

Θεσσαλονίκη, Ιανουάριος 2023

**Η ΕΚΤΙΜΗΣΗ ΑΝΤΙΚΤΥΠΟΥ ΣΤΟ ΠΛΑΙΣΙΟ ΤΗΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ**

Κασσιανή Αποστολοπούλου
Πτυχίο Νομικής ΑΠΘ, 2001

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΟ ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέπων Καθηγητής:
Κομνηνός Κόμνιος

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την ηη/μμ/εεεε

| Ονοματεπώνυμο 1 | Ονοματεπώνυμο 2 | Ονοματεπώνυμο 3 |
|---|---|---|
| ..... | ..... | ..... |

Κασσιανή Αποστολοπούλου

**ΠΕΡΙΛΗΨΗ**

Ραγδαία βήματα προόδου έχουν σημειωθεί έως σήμερα στην επιστήμη των πληροφοριών και της τεχνολογίας. Οι δυνατότητες του ατόμου μέσα από την ψηφιακή τεχνολογία είναι σχεδόν απεριόριστες. Οι σύγχρονες αυτές συνθήκες ωστόσο καθιστούν ανεξέλεγκτη τη ροή μεγάλου όγκου προσωπικών πληροφοριών και στοιχείων από και προς ιδιωτικές επιχειρήσεις και δημόσιους οργανισμούς και επιτακτική την ανάγκη για προστασία των φυσικών προσώπων από την παράνομη και σε βάρος των ατομικών τους δικαιωμάτων επεξεργασιών των δεδομένων προσωπικού τους χαρακτήρα. Στο πλαίσιο αυτό πολύτιμο εργαλείο προστασίας της ιδιωτικότητας αποτελεί η μελέτη εκτίμησης αντικτύπου σχετικά με την προστασία των δεδομένων (DPIA) που στόχο έχει μέσα από την σε βάθος επισκόπηση των περιστάσεων που συντρέχουν σε μία συγκεκριμένη επιχείρηση, ιδιωτική ή δημόσια, να εκτιμήσει και προβλέψει, χρησιμοποιώντας αναλυτικές και ενδελεχείς διαδικασίες, τους πιθανούς κινδύνους και τη σοβαρότητα των επιπτώσεών τους, με πρωταρχικό στόχο την πρόβλεψη και τελικά εφαρμογή ειδικών για τις συγκεκριμένες περιστάσεις μέτρων-αντίμετρων.

Στην εργασία που ακολουθεί προσεγγίζονται τα καίρια στάδια εκπόνησης ανάλυσης αντικτύπου για την ιδιωτικότητα με στόχο να μελετηθεί ο κίνδυνος και τα μέτρα προστασίας ως παράμετροι της συμμόρφωσης. Η μεθοδολογία που χρησιμοποιήθηκε είναι η εκτενής βιβλιογραφική επισκόπηση πάνω σε αυτό το νομικό πεδίο, καθώς και η κριτική προσέγγιση των τεχνολογιών και εργαλείων που προτείνονται. Αρχικά, αναλύονται οι διατάξεις του ΓΚΠΔ σχετικά με την εκτίμηση αντικτύπου, αναπτύσσονται οι ισχύουσες κατευθυντήριες οδηγίες και τα μεθοδολογικά κριτήρια, καθώς και το απαιτούμενο περιεχόμενο και μεθοδολογία για την προσήκουσα εκπόνησή της. Στη συνέχεια, παρουσιάζεται αναλυτικά κάθε βήμα εκπόνησής της κατά το πρότυπο της Γαλλικής Αρχής CNIL και το λογισμικό ανοιχτού κώδικα που παρέχεται ως βοήθημα, ακολουθώντας τα στάδια ένα προς ένα.

Στο πλαίσιο της ακολουθούμενης μεθοδολογικής προσέγγισης η συμμόρφωση στηρίζεται σε δύο βασικές συνιστώσες, τα θεμελιώδη δικαιώματα και αρχές κατά τον ΓΚΠΔ και τη διαχείριση των κινδύνων ιδιωτικής ζωής των υποκειμένων των δεδομένων. Τα μεν δικαιώματα των υποκειμένων των δεδομένων και οι αρχές που διέπουν την επεξεργασία αποτελούν τον σκληρό πυρήνα της προστασίας των προσωπικών δεδομένων, η δε διαχείριση των κινδύνων ασφάλειας των δεδομένων καθορίζεται από την εφαρμογή των κατάλληλων τεχνικών και οργανωτικών μέτρων για την προστασία τους.

Στο καταληκτικό τμήμα, γίνεται εκτενής ανάπτυξη των μέτρων ασφάλειας και προστασίας που καλείται να λάβει ένας οργανισμός ή επιχείρηση για να είναι σύννομος. Η παρούσα μελέτη εμπλουτίζεται με πλήθος παραδειγματικών αναφορών, καθώς και ενδεικτική παρουσίαση νομολογίας προς ενίσχυσή της και μπορεί να αποτελέσει βάση αναφοράς για έναν οργανισμό που προτίθεται να εκτελέσει αντίστοιχη μελέτη.

**Λέξεις Κλειδιά:** Εκτίμηση αντικτύπου προστασίας δεδομένων, ΕΑΠΔ, εκτίμηση αντικτύπου ιδιωτικότητας, προσωπικά δεδομένα, υψηλός κίνδυνος, μέτρα ασφάλειας, ασφάλεια πληροφοριών.

**Abstract**

Rapid strides have been made to date in the science of information and technology. The possibilities for an individual through digital technology are almost limitless. However, these modern conditions make the flow of a large amount of personal data and information from and to private companies and public organizations uncontrollable and also make it imperative need to protect natural persons from the illegal processing of their personal data at the expense of their individual rights. In this context, a valuable privacy protection tool is the Data Protection Impact Assessment (DPIA) which aims, through an in-depth overview of the circumstances that occur in a specific company, private or public, to assess and predict, using analytical and thorough procedures, the possible risks and the severity of their effects, with the primary goal to predict and finally implement specific measures-countermeasures for the circumstances.

In the present study that follows, the major key stages of conducting a privacy impact assessment are approached aiming to study the risk and the protection measures as parameters of compliance. The methodology used is the extensive literature review on this legal field, as well as the critical approach of the technologies and tools proposed. First, the articles of the GDPR regarding the data protection impact assessment are analyzed, the applicable guidelines and methodological criteria are developed, as well as the required content and methodology for its appropriate preparation. Subsequently, each step of its preparation according to the French Supervisory Authority CNIL standard and the open source software tool provided as an aid is presented in detail, following the steps one by one.

In the context of the methodological approach followed, compliance is based on two main components, the fundamental rights and principles according to the GDPR and the management of the privacy risks of the data subjects. While the rights of data subjects and the principles governing the processing are the hard core of personal data protection, the management of data security risks is determined by the application of appropriate technical and organizational measures for their protection.

In the concluding section, there is an extensive development of the security and protection measures that an organization or business must take in order to be legal. This study is enriched with a number of exemplary reports, as well as an indicative presentation of jurisprudence to strengthen it and can be a reference basis for an organization that intends to carry out a similar study.

**Keywords:** Data protection impact assessment, DPIA, Privacy impact assessment, personal data, high risk, security measures, information security

Αφιερωμένη,

Στους αγαπημένους μου γονείς

Πάνο και Μάγδα με ευγνωμοσύνη για όσα μου πρόσφεραν και μου προσφέρουν και στις λατρεμένες μου κόρες

Βασιλική και Μαγδαληνή

**Ευχαριστίες**

Για τη διεκπεραίωση της παρούσας Διπλωματικής Εργασίας, θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα καθηγητή μου, κ. Κομνηνό Κόμνιο για την άμεση και γενναιόδωρη παροχή βοήθειας παρά το επιβαρυμένο του πρόγραμμα, τη συνεργασία και την πολύτιμη συμβολή του με τις επισημάνσεις του.

Θα ήθελα επίσης να ευχαριστήσω θερμά την Διευθύντρια του Μεταπτυχιακού Προγράμματος «Δίκαιο και Πληροφορική» κ. Ευγενία Αλεξανδροπούλου, που παρά το φορτίο και τις απαιτήσεις του έργου της ήταν διαρκώς και ουσιαστικά παρούσα, αλλά και όλους τους καθηγητές του προγράμματος, τον καθένα ξεχωριστά, που όχι μόνο με βοήθησαν να διευρύνω τις γνώσεις μου, αλλά με ενέπνευσαν και με συγκίνησαν με το πάθος τους και την αγάπη τους για διδασκαλία.

Τέλος, θα ήθελα να ευχαριστήσω από καρδιάς τις συμφοιτήτριες - φίλες μου Τζωρτζίνα Κρεβάικα και Δέσποινα Βάκκου που υπήρξαν συνοδοιπόροι σε αυτή την προσπάθεια και έκαναν αυτό το ταξίδι ξεχωριστό για μένα.

**ΠΕΡΙΕΧΟΜΕΝΑ**

**ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ**

| | |
|---|---|
| **ΑΠΔΠΧ** | Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα |
| **αρ.** | αριθμός |
| **ΓΚΠΔ** | Γενικός Κανονισμός Προσωπικών Δεδομένων (ΕΕ) 2016/679 |
| **ΔΕΕ** | Δικαστήριο Ευρωπαϊκής Ένωσης |
| **ΔiΜΕΕ** | Δίκαιο Μέσων Ενημέρωσης και Επικοινωνίας (περιοδικό) |
| **ΕΔΔΑ** | Ευρωπαϊκό Δικαστήριο Δικαιωμάτων του Ανθρώπου |
| **ΕΑΠΔ** | Εκτίμηση Αντικτύπου Προσωπικών Δεδομένων |
| **εκδ.** | έκδοση |
| **ΥΠΔ** | Υπεύθυνος Προστασίας Δεδομένων |
| **DPIA** | Data Protection Impact Assessment |
| **GDPR** | General Data Protection Regulation |

## Κεφάλαιο 1 – Η ανάγκη για προστασία της ιδιωτικότητας παράλληλα με την τεχνολογική εξέλιξη

### 1.1 Εισαγωγή

Ραγδαία βήματα προόδου έχουν σημειωθεί έως σήμερα στην επιστήμη των πληροφοριών και της τεχνολογίας. Έχουν κατακτηθεί πολύπλευρα επιστημονικά πεδία που διεύρυναν όχι μόνο τις επιστημονικές γνώσεις και αποκτήματα αλλά και τις ουσιαστικές καθημερινές δραστηριότητες του σύγχρονου ανθρώπου. Οι δυνατότητες του ατόμου μέσα από την ψηφιακή τεχνολογία είναι σχεδόν απεριόριστες. Έχει πλέον εκμηδενιστεί ο χρόνος και η απόσταση με αποτέλεσμα οποιαδήποτε πράξη ή ενέργεια να δύναται να διεκπεραιωθεί από οπουδήποτε, χωρίς τοπικούς περιορισμούς, σε ταχύτατο χρόνο. Μοναδικό προαπαιτούμενο η σύνδεση σε περιβάλλον διαδικτύου.

Για να περατωθεί ωστόσο μία ενέργεια συχνά υπάρχει ροή πλήθους προσωπικών πληροφοριών και στοιχείων, όπως για παράδειγμα ονοματεπώνυμο, διεύθυνση, στοιχεία πιστωτικής κάρτας, διεύθυνση ηλεκτρονικού ταχυδρομείου, αριθμός τηλεφώνου, αλλά και όχι μόνο. Στα πλαίσια μιας διαδικτυακής δραστηριότητας το άτομο αφήνει το ψηφιακό του αποτύπωμα που ενδεικτικά μπορεί να είναι η IP διεύθυνσή του, το είδος της συσκευής που συνδέθηκε, οι διαδικτυακοί τόποι που επισκέφθηκε ή δεδομένα κίνησής του και δεδομένα GPS[1]. Αυτές οι πληροφορίες και οποιεσδήποτε άλλες πληροφορίες που μπορούν, με άμεσο ή έμμεσο τρόπο, να οδηγήσουν σε ταυτοποίηση των στοιχείων ενός φυσικού προσώπου αποτελούν προσωπικά δεδομένα. Με τη χρήση της τεχνολογίας τα δεδομένα αυτά μπορούν να αποθηκεύονται σε υπολογιστικά νέφη (cloud computing), να καταγράφονται από αισθητήρες ή να συλλέγονται μέσω εφαρμογών και να διαβιβάζονται στο διαδίκτυο με νόμιμους ή μη τρόπους[2]. Στην εποχή του διαδικτύου των πραγμάτων (IoT), της τεχνητής νοημοσύνης, των μεγάλων δεδομένων και των «έξυπνων» συσκευών, τα προσωπικά δεδομένα κάθε φυσικού προσώπου βρίσκονται παντού, αναρτημένα σε κοινωνικά δίκτυα, διαδικτυακά φόρουμ, σελίδες εξειδικευμένων υπηρεσιών, κ.α[3].

---

[1] O. Tene, J. Polonetsky, Big Data for All: Privacy and User Control in the Age of Analytics, Northwestern Journal of Technology and Intellectual Property, vol. 11, issue 5, 2013, σελ. 240 και επ.

[2] Βλ. Σ. Τάσση, Τεχνολογία και Ιδιωτικότητα, σε: Κοτσαλή (επιμ.), Προσωπικά Δεδομένα, Εκδ. Νομική Βιβλιοθήκη, 2016, σελ. 331, Ε. Σμυρνάκη, Υπολογιστικό Νέφος (Cloud) και Προσωπικά Δεδομένα – Γενικός Κανονισμός Προστασίας Δεδομένων 679/2016, Pro Justitia, 2016, 254 επ.

[3] Ι. Ιγγλεζάκης, Η εκτίμηση αντικτύπου στην προστασία προσωπικών δεδομένων. Δικαιοπολιτική θεώρηση ενός καινοτόμου εργαλείου προστασίας της ιδιωτικότητας στον 21ο αιώνα, Επιθεώρηση Δικαίου Πληροφορικής, Τομ. 1, τεύχ. 1, 2020, σελ. 8-9.

Οι σύγχρονες αυτές συνθήκες καθιστούν ανεξέλεγκτη τη ροή μεγάλου όγκου προσωπικών πληροφοριών προς ιδιωτικές επιχειρήσεις, δημόσιους οργανισμούς, εταιρείες κολοσσούς με ποικίλες δραστηριότητες ανά τον κόσμο και ιδιαίτερα σημαντική επιρροή στο παγκόσμιο ψηφιακό, οικονομικό, πολιτικό και βιομηχανικό γίγνεσθαι. Η ανεξέλεγκτη αυτή ροή έχει ως αποτέλεσμα να μην μπορεί πάντοτε το υποκείμενο των προσωπικών δεδομένων να γνωρίζει, να δύναται να παρεμβαίνει και να ελέγχει πού βρίσκονται οι προσωπικές του πληροφορίες, στα χέρια ποιου υπευθύνου επεξεργασίας και με τί σκοπό αξιοποίησης. Συνηθισμένη τακτική εμπορικών εταιρειών αποτελεί η παρακολούθηση των προτιμήσεων των πελατών και η δημιουργία προφίλ τους για στοχευμένη συμπεριφορική διαφήμιση προς οικονομικό όφελός τους. Μεγάλες εταιρείες διαχείρισης μηχανών αναζήτησης και κοινωνικών δικτύων καταλήγουν να συλλέγουν και επεξεργάζονται μεγάλο όγκο δεδομένων για μεγάλο πλήθος ατόμων, όπως φωτογραφίες, βίντεο, στιγμές από τη ζωή τους με τα αγαπημένα τους πρόσωπα, πολιτικές, θρησκευτικές, κοινωνικές και άλλες πεποιθήσεις και απόψεις τους, συνήθειές τους, καταναλωτικές προτιμήσεις[4] κ.α. Ακόμη, στο παρελθόν έχουν σημειωθεί πλείστα όσα περιστατικά παράνομης χρήσης και επεξεργασίας προσωπικών δεδομένων με σοβαρές προεκτάσεις, όπως η πολυτάραχη υπόθεση Facebook-Cambridge Analytica στην οποία η εταιρεία Facebook ακολούθησε πρακτικές ελέγχου των χρηστών της και των προσωπικών πληροφοριών τους με σκοπό να επηρεάσει τις εκλογικές τους προτιμήσεις[5].

Με στόχο την προστασία των φυσικών προσώπων από την παράνομη και σε βάρος των ατομικών τους δικαιωμάτων επεξεργασιών των δεδομένων προσωπικού τους χαρακτήρα, λαμβάνουν χώρα συντονισμένες επιστημονικές δράσεις και πρακτικές στη διεθνή κοινότητα, κατ' αρχήν με την σύσταση και λειτουργία ανεξάρτητων εποπτικών αρχών, επιφορτισμένων με καθήκοντα και εξουσίες προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών των φυσικών προσώπων. Ταυτόχρονα και με τη θεσμοθέτηση κατάλληλων νομοθετικών πλαισίων, την διαρκή παροχή έγγραφων οδηγιών, διαρκώς επικαιροποιημένων, παράλληλα και με την αυστηροποίηση του

[4] Βλ. Λ. Κανέλλο, The GDPR Handbook, Εκδ. Νομική Βιβλιοθήκη, 2020, σελ. 89 επ.
[5] https://el.wikipedia.org/wiki/Σκάνδαλο_δεδομένων_Facebook-Cambridge_Analytica, Λ. Κανέλλος, The GDPR Handbook, Εκδ. Νομική Βιβλιοθήκη, 2020, σελ. 91.

κανονιστικού πλαισίου προς τις επιχειρήσεις που συλλέγουν και επεξεργάζονται δεδομένα προσωπικού χαρακτήρα φυσικών προσώπων.

Στη βάση αυτή έχουν προβλεφθεί και θεσμοθετηθεί εργαλεία που παρέχονται προς τους υπεύθυνους επεξεργασίας φορείς ή επιχειρήσεις που κάνουν χρήση προσωπικών δεδομένων ώστε να πραγματοποιείται μία αξιολόγηση των κινδύνων που δύνανται πιθανώς να επέλθουν θίγοντας την ασφάλεια των συστημάτων ενός οργανισμού και τελικά τα δικαιώματα των υποκειμένων των δεδομένων προκαλώντας μικρές ή και ανεπανόρθωτες ζημίες[6].

Ένα τέτοιο εργαλείο προστασίας της ιδιωτικότητας αποτελεί και η εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων[7] (Data Protection Impact Assessment, DPIA) που στόχο έχει μέσα από την σε βάθος επισκόπηση των περιστάσεων που συντρέχουν σε μία συγκεκριμένη επιχείρηση, ιδιωτική ή δημόσια, να εκτιμήσει και προβλέψει, χρησιμοποιώντας αναλυτικές και ενδελεχείς διαδικασίες, τους πιθανούς κινδύνους και τη σοβαρότητα των επιπτώσεών τους, με πρωταρχικό στόχο την πρόβλεψη και τελικά εφαρμογή ειδικών για τις συγκεκριμένες περιστάσεις μέτρων-αντίμετρων.

Θεμέλιο προστασίας όλων των παραπάνω αποτελούν συγκεκριμένες κανονιστικές περιοριστικές διατάξεις που έχουν εφαρμογή μέσα από ένα γενικότερο πλέγμα θεμελιωδών δεσμευτικών κανόνων που καθορίζουν τα πλαίσια της ελεύθερης κυκλοφορίας προσωπικών πληροφοριών.

## 1.2 Κανονιστικό πλαίσιο

Κορμό στην προστασία των προσωπικών δεδομένων αποτελεί ο Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου [Γενικός Κανονισμός για την Προστασία Δεδομένων (ΓΚΠΔ)[8] – General Data Protection Regulation (GDPR)[9]. Στον Γενικό Κανονισμό η πρόβλεψη της υποχρέωσης για τη μελέτη εκτίμησης αντικτύπου, το περιεχόμενό της, οι προϋποθέσεις εκπόνησής της και οι όροι

[6] Βλ. Λ. Κανέλλο, The GDPR Handbook, Εκδ. Νομική Βιβλιοθήκη, 2020, σελ. 93-94.
[7] ΓΚΠΔ, άρθ. 35.
[8] Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 .
[9] Στους βασικούς όρους που αναφέρονται στην παρούσα διπλωματική χρησιμοποιείται και η Αγγλική ορολογία μέσα σε παρένθεση.

προηγούμενης διαβούλευσής της με την εποπτική αρχή ρυθμίζονται στα άρθρα 35 και 36 του 3ου Τμήματος του 4ου Κεφαλαίου, με τις αντίστοιχες αναφορές στο Προοίμιο του Κανονισμού στις με αριθμούς 75 και 84-96 Αιτιολογικές Σκέψεις. Έμφαση στην υποχρεωτικότητα διενέργειας εκτίμησης αντικτύπου σε επεξεργασίες με μεγάλο κίνδυνο αποδίδεται και στην Αστυνομική Οδηγία 2016/680[10] στα άρθρα 27 και 28. Οι προαναφερθείσες αυτές διατάξεις εξετάζονται σε συνδυασμό με τη διάταξη του άρθρου 65 του εθνικού εκτελεστικού νόμου 4624/2019 (ΦΕΚ Α΄137) για την «Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις»[11]. Προσφάτως δε, δημοσιεύθηκε και ο νόμος 5002/2022 (ΦΕΚ Α΄228) που μεταξύ άλλων, τροποποιεί ορισμένες διατάξεις του ν. 4624/2019.

Επιπλέον, η εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων εξετάζεται και μέσα από το κανονιστικό πλαίσιο του Συμβουλίου της Ευρώπης στο άρθρο 10 της Σύμβασης 108[12] όπου ομοίως αποτυπώνεται η ανάγκη ελαχιστοποίησης και αποφυγής των κινδύνων των επεξεργασιών μέσα από επισκόπηση του αντικτύπου τους στα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων.

## 1.3 Ιδιωτικότητα και Προσωπικά Δεδομένα

Η έννοια της ιδιωτικότητας εκφράζει πρωτίστως την ανάγκη αλλά και το δικαίωμα ενός ατόμου να προασπίζει την προσωπικότητά του και τον ιδιωτικό του βίο από τις αδικαιολόγητες παρεμβάσεις τρίτων. Κατά ένα μέρος θα έλεγε κανείς ότι αντανακλά την ανάγκη για διαφύλαξη του απορρήτου της προσωπικής ζωής αλλά επιπρόσθετα και την ανάγκη για ελεύθερη ανάπτυξη της προσωπικότητας, της έκφρασης και των πεποιθήσεων ενός ατόμου, είτε κοινωνικών, πολιτικών, είτε

[10] Βλ. Οδηγία 2016/680 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680 .

[11] https://0076.syzefxis.gov.gr/wp-content/uploads/2019/09/N.-4624_2019.pdf και η Αιτιολογική Έκθεση https://www.ministryofjustice.gr/wp-content/uploads/2019/09/N.-4624_2019-ΑΙΤΙΟΛΟΓΙΚΗ-ΕΚΘΕΣΗ.pdf

[12] https://rm.coe.int/1680078b37

φιλοσοφικών, θρησκευτικών ή άλλων. Αυτή η ανάγκη ακριβώς για προστασία του δικαιώματος της ιδιωτικότητας ενισχύεται συγχρόνως μέσα από το πεδίο προστασίας των δεδομένων προσωπικού χαρακτήρα θέτοντας συγκεκριμένες κανονιστικές ρυθμίσεις, όρια, προϋποθέσεις και εξουσίες[13]. Συνεπώς, από αυτή την οπτική, η ιδιωτικότητα και η προστασία των προσωπικών δεδομένων δείχνουν να είναι δύο έννοιες που οδεύουν παράλληλα και αλληλοσυμπληρώνονται. Γι' αυτό το λόγο συχνά ο όρος «ΕΑΠΔ» και ο όρος «εκτίμηση των επιπτώσεων στην ιδιωτική ζωή» χρησιμοποιείται για να δηλώσει την ίδια έννοια[14].

Ταυτόχρονα όμως υπάρχουν και διαφοροποιήσεις που έγκεινται κυρίως στην εστίαση του κινδύνου από το πρίσμα της ασφάλειας των πληροφοριών. Δηλαδή όταν εξετάζεται ένα ζήτημα από πλευράς ΓΚΠΔ και προστασίας δεδομένων η εστίαση του κινδύνου εντοπίζεται στο Υποκείμενο, ενώ όταν εξετάζεται από πλευράς ασφάλειας πληροφοριών η εστίαση του κινδύνου εντοπίζεται στην επιχείρηση ή τον οργανισμό.

## Κεφάλαιο 2 – Η Εκτίμηση Αντικτύπου σχετικά με την προστασία δεδομένων κατά τον ΓΚΠΔ

### 2.1 Η ΕΑΠΔ ως μέσο εφαρμογής της αρχής λογοδοσίας

Η εκτίμηση αντικτύπου στην προστασία των δεδομένων προσωπικού χαρακτήρα δεν προβλεπόταν στο προ Ευρωπαϊκού Κανονισμού κανονιστικό πλαίσιο. Πλέον, προσδιορίζεται και ρυθμίζεται πρωταρχικά στο άρθρο 35 του ΓΚΠΔ και στο άρθρο 65 του Ν. 4624/2019 και αποτελεί μία διαδικασία επισκόπησης, καταγραφής, μελέτης και προτάσεων πρόσφορων και αποτελεσματικών μέτρων ασφάλειας που πρέπει να πραγματοποιείται από τον υπεύθυνο επεξεργασίας προ της έναρξης μιας επεξεργασίας υψηλού κινδύνου. Πρόκειται δηλαδή για ένα σύνολο ενεργειών κατά την προεργασία μιας επεξεργασίας με επικινδυνότητα προς τα υποκείμενα, που αποτελεί μέσο προσδιορισμού των μέτρων αντιμετώπισης των κινδύνων, περιλαμβανομένων των εγγυήσεων και των μηχανισμών ασφαλείας[15].

[13] Βλ. Λ. Κανέλλο, The GDPR Handbook, Εκδ. Νομική Βιβλιοθήκη, 2020, σελ. 87 επ., Σ. Τάσση, Τεχνολογία και Ιδιωτικότητα, σε: Κοτσαλή (επιμ.), Προσωπικά Δεδομένα Εκδ. Νομική Βιβλιοθήκη, 2016, σελ. 327 επ.
[14] Το ακρωνύμιο «PIA» χρησιμοποιείται εναλλάξιμα για την αναφορά στην Privacy Impact Assessment = Εκτίμηση Αντικτύπου Ιδιωτικότητας και στην Εκτίμηση Αντικτύπου Προστασίας Δεδομένων = Data Protection Impact Assessment «DPIA».
[15] Βλ. Αιτιολ. σκέψη αρ. 90.

Σε αυτή, αναλύεται το είδος της συγκεκριμένης επεξεργασίας ως προς τη φύση της (παράδειγμα, εάν αφορά δεδομένα υγείας, ποινικών αδικημάτων, προσωπικών συμπεριφορών ή προτιμήσεων, καταγραφή δεδομένων ήχου και εικόνας, δεδομένα ευάλωτων κατηγοριών, ανηλίκων κλπ), το πεδίο εφαρμογής (λόγου χάρη, εάν εφαρμόζεται σε δημόσιους ή ιδιωτικούς χώρους, εάν γίνεται μαζική συλλογή δεδομένων, χρήση τεχνολογικών μέσων, μεγάλης κλίμακας δεδομένα, σε ποια έκταση και τί αριθμό ατόμων αφορά κλπ) και το σκοπό της (για παράδειγμα, προασπίζεται τη δημόσια υγεία, την ασφάλεια εγκαταστάσεων υψηλού εξοπλισμού, την περιουσία τρίτων, την ασφάλεια ζωής ή σωματικής ακεραιότητας κλπ). Σταθμίζεται με ιδιαίτερη βαρύτητα η αρχή της αναλογικότητας και η αρχή της αναγκαιότητας και προσφορότητας στην υπό κρίση επεξεργασία. Στη συνέχεια, αποτιμώνται οι κίνδυνοι που τυχόν θα επιφέρει η επεξεργασία στα δικαιώματα και τις ελευθερίες των υποκειμένων, δηλαδή η βλάβη στην οποία θα μπορούσε να οδηγήσει (σωματική, υλική, ηθική)[16] και ταυτόχρονα προσδιορίζονται με ακρίβεια τα συγκεκριμένα τεχνικά και οργανωτικά μέτρα στα οποία θα καταφύγει και τελικά θα εφαρμόσει ο υπεύθυνος επεξεργασίας[17].

Αποτελεί αποκλειστική ευθύνη και υποχρέωση του υπεύθυνου επεξεργασίας και ταυτόχρονα εργαλείο λογοδοσίας του, δηλαδή απόδειξη της συμμόρφωσής του κατά το άρθρο 5 παρ. 2 του ΓΚΠΔ. Αντιθέτως, η μη διενέργειά της στις περιπτώσεις που αυτή δείχνει επιβεβλημένη από τις ως άνω διατάξεις (άρθρο 35 παρ. 1 και 3-4) ή η μη ορθή εκπόνησή της (άρθρο 35 παρ. 2 και 7-9) αποτελεί λόγο επιβολής κυρώσεων από την εποπτική αρχή, είτε σε επίπεδο διοικητικών προστίμων κατ' άρθρο 83 ΓΚΠΔ, είτε σε επίπεδο αποζημιώσεων κατόπιν δικαστικής προσφυγής του καταγγέλοντος κατά του υπευθύνου επεξεργασίας ή του εκτελούντος, κατ' άρθρο 82 ΓΚΠΔ[18]. Ανάλογες συνέπειες έχει και τυχόν παράλειψη διαβούλευσης με την εποπτική αρχή πριν από την επεξεργασία.

Πρέπει επίσης να σημειωθεί ότι η μελέτη εκτίμησης αντικτύπου αποτελεί μια διαδικασία συνεχούς βελτίωσης και αυτοελέγχου που είναι αναγκαίο να εγγυάται την

[16] Βλ. Αιτιολ. σκέψη αρ. 75.
[17] Βλ. Β. Ζορκάδη σε Λ. Κοτσαλή – Κ. Μενουδάκο, Γενικός Κανονισμός για την προστασία των προσωπικών δεδομένων, Νομική διάσταση και πρακτική εφαρμογή, εκδ. Νομ. Βιβλιοθήκη 2021, σελ. 339.
[18] Βλ. Ι. Ιγγλεζάκη, Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων, Εκδ. 2η, Intractive Books, 2018, σελ. 171.

αιτιολογημένη και αξιόπιστη χρήση των προσωπικών δεδομένων καθ' όλη τη διάρκεια της δραστηριότητας επεξεργασίας. Κατ' αυτό τον τρόπο, είναι μία υποχρέωση του υπεύθυνου επεξεργασίας που δεν ολοκληρώνεται άπαξ, παρά απαιτεί διαρκή επίβλεψη, έλεγχο και επαναπροσδιορισμό των μέτρων και ενεργειών.

## 2.2 Οι δικαιολογητικοί λόγοι της υποχρέωσης διενέργειας ΕΑΠΔ

Κατά το παλαιότερο καθεστώς της Οδηγίας 95/46/ΕΚ[19] και του Ν. 2472/1997[20] προβλεπόταν η υποχρέωση γνωστοποίησης της επεξεργασίας στην ελεγκτική αρχή και η λήψη σχετικής άδειας σε περιπτώσεις επεξεργασίας ευαίσθητων δεδομένων. Με τις νεότερες ισχύουσες διατάξεις του ΓΚΠΔ και του ν. 4624/2019 η υποχρέωση αυτή έχει πλέον καταργηθεί και προς αντιστάθμισμα έχει τεθεί η υποχρέωση για τήρηση αρχείου δραστηριοτήτων των υπευθύνων επεξεργασίας και εκτελούντων την επεξεργασία, κατά το άρθρο 30, αλλά και η υποχρέωση για διενέργεια εκτίμησης αντικτύπου[21].

Η αιτιολόγηση της κατάργησης υποχρέωσης γνωστοποίησης στην Αρχή δίνεται στην με αριθμό 89 Αιτιολογική Σκέψη του προοιμίου του ΓΚΠΔ, στην οποία εξηγείται ότι αφενός εξυπηρετεί με την ανακούφιση της εποπτικής αρχής από το διοικητικό και οικονομικό φορτίο που έχει επωμιστεί, αφετέρου «δε συνέβαλε σε όλες τις περιπτώσεις στη βελτίωση της προστασίας των δεδομένων προσωπικού χαρακτήρα». Για τους λόγους αυτούς, κατά την ως άνω σκέψη, προκρίνεται η κατάργηση και αντικατάσταση με αποτελεσματικές διαδικασίες και μηχανισμούς, όπως η μελέτη εκτίμησης αντικτύπου[22].

## 2.3 Περιεχόμενο της υποχρέωσης διενέργειας εκτίμησης αντικτύπου

Καταρχήν, εκτίμηση αντικτύπου πρέπει να διενεργείται έστω και για μία συγκεκριμένη επεξεργασία όταν αυτή πραγματοποιείται με τη χρήση νέων τεχνολογιών και εκτιμάται ότι ενδέχεται να εγκυμονεί υψηλό κίνδυνο για τα δικαιώματα και τις

---

[19] Βλ. άρθρα 18-19 της Οδηγίας 95/46/ΕΚ, https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:31995L0046&from=EL .

[20] Βλ. άρθρο 7 του Ν. 2472/1997, https://www.dpa.gr/sites/default/files/2019-10/2472_97%20%28SEPT2019%29.pdf .

[21] Βλ. Δ. Ζωγραφόπουλο, Η υποχρέωση διενέργειας εκτίμησης αντικτύπου στον Γενικό Κανονισμό για την Προστασία Δεδομένων, Συνήγορος, 120/2017, Ι. Ιγγλεζάκη, Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων, Εκδ. 2η, Intractive Books, 2018, σελ. 169, Γ. Ψαράκη, GDPR και Μελέτη Εκτίμησης Αντικτύπου (DPIA): Better safe than sorry?, Lawspot https://www.lawspot.gr/nomika-blogs/giannis_psarakis/gdpr-kai-meleti-ektimisis-antiktypoy-dpia-better-safe-sorry .

[22] Βλ. σχετικά ΑΠΔΠΧ Απόφαση 46/2018.

ελευθερίες των ατόμων. Είναι βέβαια πιθανό η μελέτη εκτίμησης αντικτύπου να μην αφορά μόνο μία επεξεργασία αλλά ένα σύνολο παρόμοιων πράξεων επεξεργασίας[23] που ενέχουν παρεμφερείς δυσμενείς κινδύνους για τα φυσικά πρόσωπα.

Περαιτέρω, η ανάγκη αυτή πρέπει να εξετάζεται προτού να ξεκινήσει η καθορισμένη πράξη επεξεργασίας διότι οι κίνδυνοι που αυτή δύναται να επιφέρει πρέπει να εξεταστούν και αντιμετωπιστούν από την αρχή και όχι φυσικά μετά τον αντίκτυπό τους. Το ίδιο εξάλλου επιτάσσει και η υποχρέωση προστασίας των δεδομένων ήδη από το σχεδιασμό και εξ ορισμού, κατά το άρθρο 25 του ΓΚΠΔ. Κατ' αυτόν τον τρόπο, μία μελέτη εκτίμησης αντικτύπου πραγματοποιείται κατά την εξέταση εφαρμογής μιας νέας υπηρεσίας ή ενός καινούργιου συστήματος, τη σκέψη εισαγωγής νέων προϊόντων ή παροχών σε μια επιχείρηση, ή κατά το στάδιο του σχεδιασμού μιας νέας εφαρμογής ή προγράμματος σε έναν οργανισμό.

Η εκτίμηση αντικτύπου διενεργείται με αποκλειστική ευθύνη του υπεύθυνου επεξεργασίας[24] (ο εκτελών την επεξεργασία δεν υπέχει τέτοια υποχρέωση). Η ρύθμιση αυτή αποτελεί ένα από τα σημεία που ο Ευρωπαϊκός Κανονισμός εισάγει με τις διατάξεις του αυξημένες υποχρεώσεις για κάποια μέρη υπευθύνων ενώ ταυτόχρονα επιλέγει να ενισχύσει σημαντικά τα δικαιώματα των υποκειμένων των δεδομένων. Ο υπεύθυνος επεξεργασίας βαρύνεται πλέον με την υποχρέωση να εξετάζει και αξιολογεί διαρκώς τις πράξεις επεξεργασίας που εκτελεί αναφορικά με τις επιπτώσεις που αυτές επιφέρουν στα υποκείμενα των δεδομένων αλλά κυρίως να διασφαλίσει την προστασία τους με τη λήψη ειδικών και συγκεκριμένων μέτρων-αντίμετρων[25].

Στο πλαίσιο αυτό ο εκτελών την επεξεργασία έχει την υποχρέωση να παρέχει τη συνδρομή του στον υπεύθυνο επεξεργασίας, όταν προκύψει ανάγκη και εάν του ζητηθεί[26]. Ενισχυτικά, αλλά με προϋποθέσεις[27], υπάρχει πρόβλεψη να δύναται ο υπεύθυνος επεξεργασίας να ζητά τη γνώμη ακόμη και των ίδιων των υποκειμένων που

[23] Βλ. άρθρο 35 παρ. 1 ΓΚΠΔ.
[24] Βλ. Αιτιολ. σκέψη αρ. 84.
[25] Βλ. ΑΠΔΠΧ Γνωμοδότηση με αρ. 1/2017, σκέψη 3, Δ. Ζωγραφόπουλο, Η υποχρέωση διενέργειας εκτίμησης αντικτύπου στον Γενικό Κανονισμό για την Προστασία Δεδομένων, Συνήγορο, 120/2017, Ομάδα εργασίας του άρθρου 29, Γνώμη 1/2010 σχετικά με τις έννοιες του «υπεύθυνου της επεξεργασίας» και του «εκτελούντος την επεξεργασία», επίσης Ομάδα εργασίας 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, όπου «…*Οι υπεύθυνοι επεξεργασίας δεν μπορούν να απεκδύονται την αρμοδιότητά τους μέσω της κάλυψης των κινδύνων με ασφαλιστικές συμβάσεις*», σελ 7 υποσημείωση.
[26] Βλ. Αιτιολ. σκέψη αρ. 95.
[27] Βλ. άρθρο 35 παρ. 9 ΓΚΠΔ.

αφορά η σχεδιαζόμενη επεξεργασία. Δεν γίνεται ειδικότερη αναφορά στο κείμενο του ΓΚΠΔ σχετικά με το σε ποιες περιπτώσεις πρέπει ο υπεύθυνος επεξεργασίας να στρέφεται στη γνώμη των υποκειμένων, ωστόσο κατ΄ εφαρμογή της αρχής της λογοδοσίας μάλλον θα πρέπει ο υπεύθυνος επεξεργασίας να αιτιολογεί το λόγο που δεν ζήτησε τη γνώμη των υποκειμένων στις περιπτώσεις που εκτιμά ότι δεν ενδείκνυται.

Επίσης, μπορεί να συμβεί μία εκτίμηση αντικτύπου να πραγματοποιείται για μια επεξεργασία που σχεδιάζεται για να εφαρμοστεί με ίδιες τεχνολογικές μεθόδους σε παρόμοια περιβάλλοντα εργασίας από πολλούς υπεύθυνους επεξεργασίας ή ακόμη ένας δημόσιος φορέας ή οργανισμός να εκπονήσει μία εκτίμηση αντικτύπου για εφαρμογή της από πολλούς υπεύθυνους επεξεργασίας του ίδιου τομέα[28]. Παράδειγμα, η Κεντρική Ένωση Επιμελητηρίων Ελλάδος διεξάγει εκτίμηση αντικτύπου για νέες εφαρμογές και υπηρεσίες που προτίθενται να θέσουν σε εφαρμογή και να υλοποιήσουν τα κατά τόπους Επιμελητήρια της χώρας. Ομοίως, ιδιωτική εταιρεία που έχει αναλάβει την εποπτεία δημόσιων δρόμων και τη ρύθμιση της κυκλοφορίας τους σκοπεύει να εγκαταστήσει συστήματα βιντεοεπιτήρησης για λόγους ασφάλειας και αποφυγής τέλεσης αξιόποινων πράξεων σε όλους τους σταθμούς διοδίων και εκπονεί μελέτη εκτίμησης αντικτύπου.

## 2.4 Προϋποθέσεις διενέργειας εκτίμησης αντικτύπου

Κατά τον ΓΚΠΔ η διενέργεια εκτίμησης αντικτύπου δεν προβλέπεται για πράξη επεξεργασίας που ενδέχεται να επιφέρει κινδύνους για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, παρά είναι υποχρεωτική μόνο όταν η πράξη επεξεργασίας ενδέχεται να εγκυμονεί υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες τους.

Η έννοια του κινδύνου αναλύεται εκτενώς και με ενδεικτικές αναφορές στην με αριθμό 75 Αιτιολογική Σκέψη του προοιμίου του ΓΚΠΔ. Εκεί ο κίνδυνος εστιάζεται στις επεξεργασίες δεδομένων προσωπικού χαρακτήρα που θα μπορούσαν να προκαλέσουν σωματική, υλική ή μη υλική βλάβη στα υποκείμενα. Κατά την Ομάδα Εργασίας του άρθρου 29[29] ως «κίνδυνος» νοείται «μία υπόθεση εργασίας που περιγράφει ένα

[28] Βλ. Αιτιολ. σκέψη αρ. 92.
[29] Βλ. Ομάδα εργασίας 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, σελ. 7.

συμβάν και τις επιπτώσεις του, που έχουν εκτιμηθεί με όρους σοβαρότητας και πιθανότητας επέλευσης». Ενώ κατά τον σχετικό ορισμό της Οδηγίας (ΕΕ) 2016/1148, ως κίνδυνος μπορεί να οριστεί «κάθε ευλόγως αναγνωρίσιμη περίσταση ή γεγονός με ενδεχόμενη (ή πιθανή ή δυνητικώς) δυσμενή επίπτωση στην προστασία δεδομένων»[30]. Σημαντικό κίνδυνο μπορούν να επιφέρουν επεξεργασίες που δύνανται να οδηγήσουν τα υποκείμενα των δεδομένων σε περιορισμό ή στέρηση των δικαιωμάτων και των ελευθεριών τους ή να τα εμποδίσουν από την άσκηση ελέγχου των προσωπικών τους δεδομένων ή από τη χρήση μιας υπηρεσίας ή σύμβασης. Τέτοιες επεξεργασίες είναι κατά τον ΓΚΠΔ αυτές που έχουν ως αποτέλεσμα υψηλό κίνδυνο για τα υποκείμενα και αυτές που θεωρούνται μεγάλης κλίμακας επεξεργασίες.

Κατά τα ανωτέρω, στην περίπτωση που εξετάζεται, της υποχρεωτικής δηλαδή διενέργειας ΕΑΠΔ, ενδιαφέρει πρωτίστως η έννοια του υψηλού κινδύνου. Γι' αυτή γίνεται αναφορά στο άρθρο 35 παρ. 1 του ΓΚΠΔ, με επεξήγηση στην παρ. 3 και συμπλήρωση στην παρ. 4, σε συνδυασμό με τα παραδείγματα των Αιτιολογικών σκέψεων 89-91. Στις διατάξεις αυτές, η εννοιολογική προσέγγιση του υψηλού κινδύνου γίνεται ενδεικτικά, θέτοντας ένα γενικό πλαίσιο και χωρίς να ορίζεται ο τρόπος με τον οποίο εκτιμάται η πιθανότητα επέλευσης του κινδύνου, αλλά αντίθετα μόνο με αναφορά των ενδεχόμενων κινδύνων.

Σύμφωνα με την με αριθμό 89 Αιτιολογική σκέψη, οι πράξεις επεξεργασίας που ενδέχεται να επιφέρουν υψηλό κίνδυνο είναι ιδίως αυτές που περιλαμβάνουν τη χρήση νέων τεχνολογιών ή που είναι νέου τύπου και όταν δεν έχει διενεργηθεί προηγουμένως εκτίμηση αντικτύπου όσον αφορά την προστασία των δεδομένων από τον υπεύθυνο επεξεργασίας ή όταν καθίσταται αναγκαία λόγω του χρόνου που έχει παρέλθει από την αρχική επεξεργασία. Ταυτόχρονα, κατά το άρθρο 35 παρ. 1 του ΓΚΠΔ σε συνδυασμό με την με αριθμό 90 Αιτιολογική σκέψη, πρέπει να συνεκτιμώνται η φύση, η έκταση, το πεδίο εφαρμογής, το πλαίσιο και ο σκοπός της επεξεργασίας.

Παράλληλα, πράξεις επεξεργασίες που ενδέχεται να επιφέρουν υψηλό κίνδυνο θεωρούνται και οι μεγάλης κλίμακας επεξεργασίες. Ως τέτοιες, κατά την με αριθμό 91 Αιτιολογική σκέψη, θεωρούνται αυτές που στοχεύουν στην επεξεργασία σημαντικής ποσότητας δεδομένων προσωπικού χαρακτήρα σε περιφερειακό, εθνικό ή υπερεθνικό

[30] Βλ. Β. Ζορκάδη σε Λ. Κοτσαλή – Κ. Μενουδάκο, Γενικός Κανονισμός για την προστασία των προσωπικών δεδομένων, Νομική διάσταση και πρακτική εφαρμογή, εκδ. Νομ. Βιβλιοθήκη 2021, σελ. 341.

επίπεδο, οι οποίες θα μπορούσαν να επηρεάσουν μεγάλο αριθμό υποκειμένων των δεδομένων και οι οποίες είναι πιθανόν να έχουν ως αποτέλεσμα υψηλό κίνδυνο. Επιδρά δηλαδή αναμφισβήτητα στην επικινδυνότητα μιας επεξεργασίας ο όγκος των δεδομένων, ο αριθμός των υποκειμένων που ενδέχεται να θιγεί και το πεδίο εφαρμογής των δεδομένων. Με το ίδιο σκεπτικό υποχρεωτική είναι επίσης η διενέργεια ΕΑΠΔ όταν τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία ενόψει της λήψης αποφάσεων σε σχέση με συγκεκριμένα φυσικά πρόσωπα έπειτα από συστηματική και εκτενή αξιολόγηση προσωπικών πτυχών που αφορούν φυσικά πρόσωπα και βασίζονται στην κατάρτιση προφίλ και ομοίως για την παρακολούθηση δημόσια προσπελάσιμων χώρων σε μεγάλη κλίμακα[31].

Στην παρ. 3 του άρθρου 35 του ΓΚΠΔ γίνεται ρητή ενδεικτική αναφορά σε περιπτώσεις στις οποίες απαιτείται η διενέργεια εκτίμησης αντικτύπου, ήτοι:

α) συστηματικής και εκτενούς αξιολόγησης 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,

β) μεγάλης κλίμακας επεξεργασίας 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 ή

γ) συστηματικής παρακολούθησης δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα.

## 2.5 Κατάλογος πράξεων επεξεργασίας με υψηλό κίνδυνο

Οι παραπάνω αναφορές αποτελούν ενδεικτικές περιπτώσεις στις οποίες μια πράξη επεξεργασίας είναι πιθανό να οδηγήσει σε υψηλό κίνδυνο. Ωστόσο, υπάρχει πλήθος επεξεργασιών που μπορούν να επιφέρουν σημαντικό αρνητικό αντίκτυπο για τα υποκείμενα που δεν μπορούν να εξαντληθούν σε μία λίστα απαρίθμησης ενώ θα απαιτούνταν γι' αυτές εκτίμηση αντικτύπου.

[31] Βλ. Αιτιολ. σκέψη αρ. 91 για περαιτέρω παραδείγματα και αναφορές.

Για το λόγο αυτό η Ομάδα εργασίας του άρθρου 29, με την έκδοση σχετικών Κατευθυντήριων Γραμμών[32], προχώρησε στη σύνταξη ενός συνεκτικού συνόλου πράξεων επεξεργασίας για τις οποίες απαιτείται η διενέργεια εκτίμησης αντικτύπου, παραθέτοντας εννέα (9) κριτήρια. Αυτά τα κριτήρια θα πρέπει να λαμβάνονται υπόψη για την αξιολόγηση της υποχρεωτικότητας εκπόνησης της ΕΑΠΔ κατά τα εξής:

1. Αξιολόγηση ή βαθμολόγηση προσωπικών πτυχών που αφορούν ιδίως την εργασιακή απόδοση του ατόμου, τις οικονομικές του συνθήκες, την υγεία του, την αξιοπιστία ή συμπεριφορά του, τις προτιμήσεις και προσωπικά ενδιαφέροντα, τη γεωγραφική θέση ή μετακινήσεις, συμπεριλαμβανομένης της κατάρτισης προφίλ και προβλέψεων[33].

2. Λήψη αποφάσεων με αυτοματοποιημένα μέσα που επηρεάζουν σημαντικά τα υποκείμενα και παράγουν έννομες συνέπειες με αρνητικές επιπτώσεις και δυσμενείς διακρίσεις για αυτά[34].

3. Συστηματική παρακολούθηση των υποκειμένων ιδίως μέσω της παρατήρησής τους, παρακολούθησης ή ελέγχου τους, συμπεριλαμβανομένων πληροφοριών που συλλέγονται από δίκτυα ή από συστηματική παρακολούθηση δημοσίων προσβάσιμων χώρων[35]. Το κριτήριο αυτό επιθυμεί να καλύψει και τις περιπτώσεις που τα υποκείμενα δεν έχουν γνώση ότι τα δεδομένα τους συλλέγονται ή χρησιμοποιούνται, ιδιαίτερα όταν πρόκειται για επεξεργασία δεδομένων σε δημοσίως προσβάσιμους χώρους.

4. Ειδικών κατηγοριών δεδομένα ή δεδομένα που αφορούν ιδιαίτερες και ευαίσθητες πτυχές ενός προσώπου κατά το άρθρο 9 και 10 του ΓΚΠΔ. Σημειώνεται ότι

---

[32] Βλ. Ομάδα εργασίας 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.

[33] Βλ. Αιτιολ. σκέψη αρ. 71 και 91, Ομάδα εργασίας άρθρου 29, σελ. 10, όπου ως παραδείγματα αναφέρονται «*η περίπτωση που ένα χρηματοπιστωτικό ίδρυμα ελέγχει τους πελάτες του σε σχέση με μια βάση δεδομένων πιστοληπτικής ικανότητας ή μια βάση δεδομένων για την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και της χρηματοδότησης της τρομοκρατίας ή μια βάση δεδομένων για εγκλήματα απάτης, ή η περίπτωση που μια εταιρεία βιοτεχνολογίας παρέχει απευθείας στους καταναλωτές γενετικές δοκιμές για να εκτιμήσει και να προβλέψει τους κινδύνους νόσου/υγείας ή η περίπτωση που μια εταιρεία δημιουργεί συμπεριφορικά προφίλ ή προφίλ εμπορικής προώθησης βάσει της χρήσης ή πλοήγησης στον δικτυακό της τόπο*».

[34] Βλ. Ομάδα εργασίας άρθρου 29, σελ. 11, ως παράδειγμα αναφέρεται επεξεργασία που μπορεί να οδηγήσει σε αποκλεισμό ή σε διακρίσεις σε βάρος των φυσικών προσώπων.

[35] Στο κριτήριο αυτό η Ομάδα εργασίας (σελ. 11) εντάσσει επεξεργασίες με «συστηματική» παρακολούθηση υπό την έννοια ότι αυτή πραγματοποιείται βάσει ενός συστήματος, με καθορισμένο τρόπο, οργάνωση και μέθοδο, στα πλαίσια ενός γενικού σχεδίου συλλογής πληροφοριών που διενεργείται με συγκεκριμένη στρατηγική. Επίσης, ο όρος «*δημοσίως προσβάσιμος χώρος*» ερμηνεύεται ως «*κάθε χώρος που είναι ανοικτός στο κοινό, όπως μία πλατεία, ένα εμπορικό κέντρο, ένας δρόμος, μια αγορά, ένας σιδηροδρομικός σταθμός ή μια δημόσια βιβλιοθήκη*».

αυξημένο κίνδυνο μπορούν να επιφέρουν δεδομένα που αφορούν οικιακές δραστηριότητες ή δραστηριότητες της προσωπική ζωής ή αυτά που ασκούν επιρροή σε θεμελιώδη ατομικά δικαιώματα ή επηρεάζουν τις καθημερινές συνήθειες του υποκειμένου. Στο κριτήριο αυτό εμπίπτουν και περιπτώσεις προσωπικών εγγράφων και σημειώσεων, περιεχόμενο μηνυμάτων ηλεκτρονικού ταχυδρομείου, ημερολόγια, προσωπικές πληροφορίες σε ηλεκτρονικές εφαρμογές κ.α.

5. Επεξεργασία δεδομένων μεγάλης κλίμακας, κατά την Αιτιολογική σκέψη 91. Στην περίπτωση αυτή εξετάζεται εάν και κατά πόσο επηρεάζεται μεγάλος αριθμός υποκειμένων των δεδομένων, ο όγκος και το εύρος των δεδομένων που επεξεργάζονται, το χρονικό διάστημα επεξεργασίας και η μονιμότητά της, καθώς και οι γεωγραφικές περιοχές στις οποίες εκτείνεται η δραστηριότητα.

6. Συνδυασμός ή αντιστοίχιση δεδομένων από δύο ή περισσότερες διαφορετικές επεξεργασίες, που τελούνται για διαφορετικούς σκοπούς, πιθανώς και για διαφορετικούς υπεύθυνους επεξεργασίας, με τρόπο επιβαρυντικό και δυσχερή για τα υποκείμενα των δεδομένων.

7. Δεδομένα που αφορούν ευάλωτες ομάδες υποκειμένων κατά την με αριθμό 75 Αιτιολογική σκέψη, δηλαδή υποκείμενα που βρίσκονται σε σαφώς μειονεκτική θέση ισχύος σε σχέση με τους υπεύθυνους επεξεργασίας. Συνήθως στα ευάλωτα αυτά άτομα περιλαμβάνονται παιδιά, εργαζόμενοι, σωματικά ή ψυχικά ασθενείς, πρόσφυγες ή μετανάστες, ηλικιωμένοι κ.α.

8. Εφαρμογή νέων πρωτοποριακών τεχνολογιών και χρήση καινοτόμων τεχνικών και λύσεων που μπορεί να περιλαμβάνει νέες μορφές συλλογής και χρήσης δεδομένων διότι θα μπορούσαν να επιφέρουν υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων[36].

9. Επεξεργασία που στοχεύει στο να αποδυναμώσει τα υποκείμενα από την άσκηση των δικαιωμάτων τους ή από τη χρήση μιας υπηρεσίας ή τη σύναψη μιας σύμβασης, κατά το άρθρο 22 του ΓΚΠΔ και την με αριθμό 91 Αιτιολογική σκέψη[37].

[36] Βλ. Ομάδα εργασίας άρθρου 29, σελ. 12-13, όπου ως παραδείγματα αναφέρονται η συνδυασμένη χρήση των δακτυλικών αποτυπωμάτων και η αναγνώριση προσώπου για βελτιωμένο φυσικό έλεγχο πρόσβασης, καθώς επίσης και οι εφαρμογές του «διαδικτύου των πραγμάτων».

[37] Σχετικό παράδειγμα αναφέρει η Ομάδα εργασίας (σελ. 13) την περίπτωση που μια τράπεζα ελέγχει τους πελάτες της χρησιμοποιώντας μια βάση δεδομένων πιστοληπτικής ικανότητας για να αποφασίσει εάν θα τους χορηγήσει δάνειο ή όχι.

Σύμφωνα με τις εν λόγω Κατευθυντήριες Γραμμές, ο υπεύθυνος επεξεργασίας οφείλει να εξετάζει εάν στην επεξεργασία που προτίθεται να προχωρήσει συναντά τουλάχιστο δύο (2) από τα προαναφερόμενα κριτήρια. Κι αυτό διότι η Ομάδα εργασίας του άρθρου 29 αξιολογεί πως όσο περισσότερα από τα προαναφερόμενα εννέα κριτήρια πληρούνται τόσο περισσότερες πιθανότητες υπάρχουν για να τεθούν σε υψηλό κίνδυνο τα δικαιώματα και οι ελευθερίες των υποκειμένων των δεδομένων και ως εκ τούτου να είναι οπωσδήποτε υποχρεωτική η διενέργεια εκτίμησης αντικτύπου. Παρόλα αυτά, εάν ο υπεύθυνος επεξεργασίας κρίνει ότι μία πράξη επεξεργασίας στην οποία πληρείται μόνο ένα κριτήριο μπορεί να επιφέρει αυξημένο κίνδυνο για τα υποκείμενα, ακόμη και τότε θα πρέπει να ολοκληρώσει τη μελέτη εκτίμησης αντικτύπου[38].

Περαιτέρω, στις Κατευθυντήριες Γραμμές, δίνεται και μια σειρά με παραδείγματα και αντιστοίχισή τους με πιθανά συναφή κριτήρια ώστε να βοηθηθούν οι υπεύθυνοι επεξεργασίας ως προς την εφαρμογή των εννέα κριτηρίων[39].

## 2.6 Εθνικός κατάλογος με τα είδη των πράξεων επεξεργασίας που απαιτούν εκτίμηση αντικτύπου

Η εθνική εποπτική αρχή κάθε κράτους μέλους της Ένωσης καταρτίζει και δημοσιοποιεί κατάλογο με τα είδη των πράξεων επεξεργασίας που υπόκεινται υποχρεωτικά στη διενέργεια εκτίμησης αντικτύπου κατ' εφαρμογή της παρ. 4 του άρθρου 35 του ΓΚΠΔ. Ο δικαιολογητικός λόγος της πρόβλεψης αυτής έγκειται κυρίως σε λόγους συνεκτικότητας και προσπάθειας μιας εναρμονισμένης αντιμετώπισης των επεξεργασιών διασυνοριακού χαρακτήρα μεταξύ των κρατών μελών της Ένωσης ώστε να αποφευχθούν τυχόν ανακολουθίες. Στη χώρα μας, η ελληνική αρχή προστασίας δεδομένων με την με αριθμό 65/2018 απόφασή της[40] δημοσίευσε «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» βάσει των συστάσεων της Γνώμης 7/2018 του Ευρωπαϊκού

[38] Βλ. Ομάδα εργασίας άρθρου 29, σελ. 13.
[39] Βλ. Ομάδα εργασίας άρθρου 29, σελ. 13επ.
[40] Βλ. ΦΕΚ Β΄1622/10-05-2019 και https://www.dpa.gr/sites/default/files/2019-09/65_2018anonym.pdf?lspt_context=gdpr

Συμβουλίου Προστασίας Δεδομένων (ΕΣΠΔ)[41] και την ανακοίνωση του τροποποιημένου καταλόγου στο ΕΣΠΔ. Σημειώνεται ότι ο εν λόγω κατάλογος δεν είναι εξαντλητικός και κατατάσσει τις πράξεις επεξεργασίας που υπόκεινται υποχρεωτικά σε ΕΑΠΔ σε τρεις (3) ομαδοποιημένες κατηγορίες, κατά τα εξής: 1η κατηγορία με βάση τα είδη και τους σκοπούς επεξεργασίας, 2η κατηγορία με βάση το είδος των δεδομένων ή και τις κατηγορίες των υποκειμένων και 3η κατηγορία με βάση τα πρόσθετα χαρακτηριστικά ή και τα χρησιμοποιούμενα μέσα επεξεργασίας. Η υποχρέωση διενέργειας ΕΑΠΔ προβλέπεται για τις πράξεις επεξεργασίας που υπάγονται στην 1η ή 2η κατηγορία ή εάν υπάγονται στην 3η κατηγορία και επιπλέον πρόκειται για σκοπούς ή είδη επεξεργασιών της 1ης ή είδη δεδομένων ή κατηγορίες υποκειμένων της 2ης κατηγορίας.

## 2.7 Πράξεις επεξεργασίας που δεν απαιτούν εκτίμηση αντικτύπου

Εξ αντιδιαστολής των διατάξεων που προβλέπουν πότε απαιτείται η εκπόνηση εκτίμησης αντικτύπου, προκύπτουν κατ' αρχήν οι περιπτώσεις κατά τις οποίες δεν προβλέπεται η διενέργειά της. Έτσι, αρχικά, επεξεργασία που δε σχετίζεται με πιθανή πρόκληση υψηλού κινδύνου στα δικαιώματα και τις υποχρεώσεις των υποκειμένων των δεδομένων εντάσσεται σε αυτή την κατηγορία. Το ίδιο ισχύει και στην περίπτωση που η νέα επεξεργασία παρουσιάζει πολλές ομοιότητες ως προς τη φύση, το πεδίο εφαρμογή, το πλαίσιο και το σκοπό επεξεργασίας για την οποία έχει ήδη ολοκληρωθεί εκτίμηση αντικτύπου[42]. Επίσης, δεν απαιτείται, όταν η εποπτική αρχή έχει ήδη καταρτίσει και δημοσιοποιήσει κατάλογο με τα είδη των πράξεων επεξεργασίας για τα οποία δεν απαιτείται εκτίμηση αντικτύπου[43]. Ακόμη, στην ίδια κατηγορία υπάγεται πράξη επεξεργασίας που δυνάμει του άρθρου 6 παρ. 1 στοιχείο γ) ή ε) έχει νομική βάση στο δίκαιο της Ένωσης ή στο δίκαιο του κράτους μέλους στο οποίο υπόκειται ο υπεύθυνος επεξεργασίας, το εν λόγω δίκαιο ρυθμίζει την συγκεκριμένη πράξη επεξεργασίας και έχει διενεργηθεί ήδη εκτίμηση αντικτύπου για αυτή, εκτός εάν τα κράτη μέλη κρίνουν διαφορετικά[44]. Επιπρόσθετα, δεν απαιτείται σε υφιστάμενες πράξεις επεξεργασίας που έχουν ήδη ελεγχθεί από εποπτική αρχή ή τον υπεύθυνο

[41] Βλ. https://edpb.europa.eu/sites/default/files/files/file1/2018-09-25-opinion_2018_art._64_gr_sas_dpia_list_el.pdf
[42] Βλ. άρθρο 35 παρ. 1 ΓΚΠΔ.
[43] Βλ. άρθρο 35 παρ. 5 ΓΚΠΔ.
[44] Βλ. άρθρο 35 παρ. 10 ΓΚΠΔ.

προστασίας δεδομένων πριν από τον Μάιο του 2018 με τον όρο ότι δεν υπάρχει έκτοτε καμία μεταβολή[45]. Ωστόσο, σε υφιστάμενες επεξεργασίες ο υπεύθυνος επεξεργασίας οφείλει να προβαίνει σε επανεξέταση των πράξεων ως προς τους όρους υλοποίησής τους (φύση, πεδίο εφαρμογής, σκοπούς, είδος δεδομένων, περίοδος αποθήκευσης, αποδέκτες κλπ.) και επανεκτίμηση των κινδύνων για τυχόν μεταβολή τους[46].

Ομοίως, η εκτίμηση αντικτύπου δε θα πρέπει να θεωρείται υποχρεωτική όταν η επεξεργασία δεν θεωρείται μεγάλης κλίμακας. Ως τέτοιες αναφέρονται ενδεικτικά οι επεξεργασίες που αφορούν δεδομένα προσωπικού χαρακτήρα ασθενών ή πελατών ιδιώτη ιατρού, άλλου επαγγελματία του τομέα της υγείας ή δικηγόρου[47].

Παραδείγματα επεξεργασιών που αναφέρονται από την Ομάδα εργασίας του άρθρου 29[48] ως μη απαιτούμενες διενέργειας ΕΑΠΔ είναι ηλεκτρονικό περιοδικό που χρησιμοποιεί κατάλογο ηλεκτρονικών διευθύνσεων για να αποστέλλει γενικές ημερήσιες συνόψεις στους συνδρομητές του, δικτυακός τόπος ηλεκτρονικού εμπορίου που διαφημίζει ανταλλακτικά αυτοκινήτων-αντικών και περιλαμβάνει περιορισμένη κατάρτιση προφίλ βάσει των αντικειμένων που έχουν προβληθεί ή αγοραστεί στον δικτυακό του τόπο.

Σε περίπτωση αμφιβολίας βέβαια, συνιστάται δίχως άλλο η διενέργεια εκτίμησης αντικτύπου καθώς μόνο θετικά και χρήσιμα στοιχεία έχει να εισφέρει σε μία επιχείρηση ως ένα χρήσιμο εργαλείο συμμόρφωσης και αυτοελέγχου της[49].

## 2.8 Ο ρόλος του ΥΠΔ στη διαδικασία

Κατά τη διαδικασία εκπόνησης μιας εκτίμησης αντικτύπου ο υπεύθυνος προστασίας δεδομένων του οργανισμού έχει ισχυρό ρόλο. Προβλέπεται πλέον ρητά[50] η υποχρέωση να ζητά ο υπεύθυνος επεξεργασίας τη γνώμη του υπεύθυνου προστασίας δεδομένων (DPO), εφόσον υπάρχει ορισμένος[51], κατά τη διενέργεια της εκτίμησης αντικτύπου. Το ίδιο προβλέπεται ρητά επίσης κατά την απαρίθμηση των καθηκόντων

[45] Βλ. άρθρο 20 της Οδηγίας 95/46/ΕΚ και με αριθμό 171 Αιτιολογική σκέψη κατά την οποία *«Οι αποφάσεις της Επιτροπής και οι εγκρίσεις εποπτικών αρχών που εκδόθηκαν βάσει της οδηγίας 95/46/ΕΚ παραμένουν σε ισχύ μέχρι την τροποποίηση , αντικατάσταση ή κατάργησή τους»*.
[46] Βλ. άρθρο 35 παρ. 11 ΓΚΠΔ.
[47] Βλ. Αιτιολ. σκέψη αρ. 91 τελευταία εδάφια.
[48] Βλ. Ομάδα εργασίας του άρθρου 29, σελ. 14.
[49] Βλ. Ομάδα εργασίας του άρθρου 29, σελ. 9.
[50] Βλ. άρθρο 35 παρ. 2 ΓΚΠΔ.
[51] Βλ. άρθρα 37-39 ΓΚΠΔ.

του υπευθύνου προστασίας δεδομένων όπου επισημαίνεται από πλευράς του η υποχρέωση να παρέχει συμβουλές, όταν του ζητείται, κατά τη διενέργεια της ΕΑΠΔ, αλλά και να παρακολουθεί την υλοποίησή της[52]. Ομοίως, ο υπεύθυνος προστασίας δεδομένων έχει την υποχρέωση να συνεργάζεται με την εποπτική αρχή και να λειτουργεί ως σημείο επαφής για την εποπτική αρχή αλλά και τα υποκείμενα των δεδομένων όπου αυτό απαιτηθεί. Επίσης πρέπει να σημειωθεί ότι το όνομα και τα στοιχεία επικοινωνίας του ΥΠΔ απαιτούνται να γνωστοποιηθούν από τον υπεύθυνο επεξεργασίας και κατά τις περιπτώσεις γνωστοποίησης ενός περιστατικού παραβίασης[53].

Από τα παραπάνω είναι εμφανές ότι αφενός ο ρόλος του υπεύθυνου προστασίας είναι συμμετοχικός, συμβουλευτικός και ανεξάρτητος, αφετέρου εξέχουσας βαρύτητας καθώς, με την εμπειρογνωσία του, δύναται να προνοήσει ένα ζημιογόνο συμβάν, να παρέχει συμβουλές και εποπτεία για την εφαρμογή της συμμόρφωσης, να προετοιμάσει τον οργανισμό για την αντιμετώπιση μιας παραβίασης και να την αποτρέψει και εν γένει να διαχειριστεί καταστάσεις που εγκυμονούν κινδύνους στην ασφάλεια των δεδομένων και την άσκηση των δικαιωμάτων των υποκειμένων.

## 2.9 Μεθοδολογία και Περιεχόμενο της ΕΑΠΔ

Ο ΓΚΠΔ δεν επιτάσσει την υλοποίηση της εκτίμησης αντικτύπου με μία συγκεκριμένη μεθοδολογία. Σύμφωνα με την άποψη της Ομάδας εργασίας του άρθρου 29, η ΕΑΠΔ μπορεί να διενεργηθεί με διαφορετικές μεθοδολογίες που όμως υποχρεωτικά θα πρέπει να ακολουθούν ορισμένα κοινά κριτήρια. Ο υπεύθυνος επεξεργασίας έχει τη διακριτική ευχέρεια να διαμορφώνει το πλαίσιο που εναρμονίζεται με τις πρακτικές της εργασίας του υπό τον όρο ότι η διαδικασία που ακολουθεί πληροί τα συγκεκριμένα κριτήρια.

Στις υπάρχουσες δημοσιευμένες διαδικασίες περιλαμβάνονται ενδεικτικά τόσο γενικά πλαίσια, εθνικά και διεθνή, όσο και ειδικά τομεακά πλαίσια[54]. Η διαδικασία της

[52] Βλ. Γ. Γιαννόπουλο, Λ. Μήτρου, Γρ. Τσόλια, σε Λ. Κοτσαλή – Κ. Μενουδάκο, Γενικός Κανονισμός για την προστασία των προσωπικών δεδομένων, Νομική διάσταση και πρακτική εφαρμογή, εκδ. Νομ. Βιβλιοθήκη 2021, σελ. 286επ, Β. Σωτηρόπουλο, Τα καθήκοντα του ΥΠΔ, Υπεύθυνος Προστασίας Δεδομένων, Εκδ. Σάκκουλα, 2019, σελ. 364, Λ. Κανέλλο, The GDPR Handbook, Εκδ. Νομική Βιβλιοθήκη, 2020, σελ. 428-455.
[53] Βλ. Ομάδα εργασίας του άρθρου 29, Κατευθυντήριες γραμμές σχετικά με τη γνωστοποίηση παραβιάσεων δεδομένων προσωπικού χαρακτήρα δυνάμει του κανονισμού 2016/67, σελ. 33επ.
[54] Βλ. Ομάδα εργασίας του άρθρου 29, σελ. 26, Παράρτημα 1.

ΕΑΠΔ ρυθμίζεται με το διεθνές πρότυπο ISO/IEC 29134:2017 που παρέχει συγκεκριμένες κατευθυντήριες γραμμές για τη διαδικασία, τη δομή και το περιεχόμενο μιας ΕΑΠΔ[55], αλλά και από άλλα σχετικά διεθνή πρότυπα[56].

Στο πρότυπο ISO/IEC 29134:2017 η διαδικασία της ΕΑΠΔ περιγράφεται ως ένα συνολικό έργο με συγκεκριμένα παραδοτέα αρχεία που καταγράφονται μετά από πολλά στάδια. Στην αρχή της διαδικασίας, ιδιαίτερα κατά το σχεδιασμό της εφαρμογής ενός συστήματος ή προγράμματος που πραγματοποιεί επεξεργασίες προσωπικών δεδομένων, αλλά και μεταγενέστερα, κατά την ανάπτυξη και θέση σε λειτουργία του συστήματος ή προγράμματος, πραγματοποιείται μια σειρά ενεργειών προεργασίας. Δημιουργούνται ομάδες επί του έργου με καθορισμένους ρόλους και αρμοδιότητες, ορίζονται συντονιστές και υπεύθυνοι παρακολούθησης της ΕΑΠΔ, εισφέρονται τα δεδομένα, καθορίζεται το πεδίο εφαρμογής και η τεχνογνωσία κατά περίπτωση και πραγματοποιούνται εργασίες καταγραφής, εκτίμησης της σοβαρότητας των κινδύνων και αξιολόγησης των συνεπειών τους. Ταυτόχρονα, καταγράφονται τα εμπλεκόμενα πρόσωπα, ζητείται η γνώμη ειδικών και εμπειρογνωμόνων και προσδιορίζεται προϋπολογισμός του έργου. Στη συνέχεια, αναγνωρίζονται και αναλύονται οι κίνδυνοι στο μεγαλύτερο κατά το δυνατό εύρος τους και γίνεται προσπάθεια συσχετισμού τους με πιθανές πηγές προέλευσής τους και πιθανές επερχόμενες απειλές που μπορεί να προκύψουν. Κατά την αξιολόγηση των κινδύνων σχεδιάζεται πλάνο μετριασμού και ελαχιστοποίησης των αρνητικών αντικτύπων στα δικαιώματα και τις ελευθερίες των φυσικών προσώπων[57].

Περαιτέρω, παραδείγματα εθνικών πλαισίων εισάγονται από τη Γαλλική αρχή ελέγχου (CNIL)[58], η οποία έχει δημοσιεύσει και ένα λογισμικό ανοιχτού κώδικα ως

[55] Βλ. ISO/IEC 29134:2017, Information technology – Security techniques- Privacy impact assessment-Guidelines, International Organization for Standardization (ISO), https://www.iso.org/obp/ui/#iso:std:iso-iec:29134:ed-1:v1:en
[56] ISO/IEC 27000:2016, ISO/IEC 27001, ISO/IEC 27005, ISO/IEC 29100:2011, ISO/IEC 3100, ISO/IEC 27701.
[57] Βλ. Β. Ζορκάδη σε Λ. Κοτσαλή – Κ. Μενουδάκο, Γενικός Κανονισμός για την προστασία των προσωπικών δεδομένων, Νομική διάσταση και πρακτική εφαρμογή, εκδ. Νομ. Βιβλιοθήκη 2021, σελ. 349.
[58] Βλ. https://www.cnil.fr/en/PIA-privacy-impact-assessment-en.

βοήθημα για την εκπόνηση ΕΑΠΔ[59], τη Βρετανική αρχή με δημοσιευμένες οδηγίες[60] και υπόδειγμα[61], την Κυπριακή αρχή[62], Ισπανική κ.α.

Επιπρόσθετα, η ομάδα εργασίας του άρθρου 29 ενθαρρύνει τη δημιουργία ειδικών τομεακών πλαισίων για την εφαρμογή εξειδικευμένης γνώσης σε πράξεις επεξεργασίας με ιδιαίτερα χαρακτηριστικά, όπως το πλαίσιο εκπόνησης εκτίμησης αντικτύπου σε εφαρμογές RFID[63] και τα ευφυή ηλεκτρικά δίκτυα και συστήματα μέτρησης[64].

Συνεπώς, ανεξάρτητα από την ακριβή δομή και μορφή της ΕΑΠΔ που τελικά θα επιλέξει ο υπεύθυνος επεξεργασίας να ακολουθήσει, αυτή θα πρέπει τελικά να αποτελεί μία εις βάθος αξιολόγηση των κινδύνων, ανάλογα με τον τομέα και τα είδη επεξεργασιών που καλείται να αντιμετωπίσει ώστε να ληφθούν τα πλέον στοχευμένα για την περίπτωση μέτρα αντιμετώπισης.

Ωστόσο, πέραν της μεθοδολογίας, ορίζεται ελάχιστο περιεχόμενο της εκτίμησης αντικτύπου στην παρ. 7 του άρθρου 35 του ΓΚΠΔ, σε συνδυασμό με τις αναφορές στις αιτιολογικές σκέψεις 84 και 90 του προοιμίου, ενώ παράλληλα στις κατευθυντήριες γραμμές της ΟΕ29[65] παρέχονται ομαδοποιημένα κριτήρια για την ορθή εκπόνηση μιας εκτίμησης αντικτύπου.

Κατά τα ανωτέρω, η ΕΑΠΔ οφείλει να περιλαμβάνει αναλυτική και συστηματική περιγραφή των πράξεων επεξεργασίας, των σκοπών τους και του κατά περίπτωση εννόμου συμφέροντος που επιδιώκει ο υπεύθυνος επεξεργασίας. Στο σημείο αυτό, λαμβάνονται υπόψη η φύση, η έκταση, το πλαίσιο και οι σκοποί επεξεργασίας, καταγράφονται τα είδη των προσωπικών δεδομένων, οι αποδέκτες και ο χρόνος διατήρησης των δεδομένων. Γίνεται λειτουργική περιγραφή των πράξεων επεξεργασίας, καταγράφεται ο χρησιμοποιούμενος υλικός εξοπλισμός για τις προβλεπόμενες πράξεις επεξεργασίας (στοιχεία υλικού και λογισμικού, δίκτυα,

---

[59] Βλ. https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assessment .
[60] Βλ. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/.
[61] Βλ. https://ico.org.uk/media/2258461/dpia-template-v04-post-comms-review-20180308.pdf.
[62] Βλ. https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/page2c_en/page2c_en?opendocument.
[63] Βλ. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf.
[64] Βλ. https://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf.
[65] Βλ. Ομάδα εργασίας του άρθρου 29, σελ. 28, Παράρτημα 2.

ανθρώπινο δυναμικό κ.α.) και λαμβάνεται υπόψη η συμμόρφωση με εγκεκριμένους κώδικες δεοντολογίας. Κατόπιν, παρουσιάζεται μία εκτίμηση της αναγκαιότητας και αναλογικότητας της σκοπούμενης πράξης επεξεργασίας με αναφορές και τεκμηρίωση στις αρχές και τις νόμιμες βάσεις που διέπουν την επεξεργασία, καθώς και τα μέτρα για τον περιορισμό στα απολύτως αναγκαία για τους σκοπούς της επεξεργασίας. Καθορίζονται τα μέτρα για την προάσπιση των δικαιωμάτων των υποκειμένων των δεδομένων (πρόσβασης, φορητότητας, διόρθωσης, διαγραφής, εναντίωσης, περιορισμού), οι σχέσεις με τους εκτελούντες την επεξεργασία, τα μέτρα προστασίας των διεθνών διαβιβάσεων και τυχόν προηγούμενη διαβούλευση. Στη συνέχεια, η ΕΑΠΔ οφείλει να προβαίνει σε διαχείριση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων σε συνάρτηση με το επίπεδο σοβαρότητας και πιθανότητας επέλευσης, αφού ληφθούν υπόψη οι πηγές κινδύνου και εξακριβωθούν οι πιθανές αρνητικές επιπτώσεις τους στα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Στόχος αυτών των ενεργειών είναι πάντα να αποτυπωθούν οι απειλές ώστε να προβλεφθούν τα κατάλληλα μέτρα αποφυγής των κινδύνων. Τέλος, παρουσιάζονται οι γνώμες των ενδιαφερομένων μερών που συμμετέχουν στη διαδικασία, όπως οι συστάσεις του υπευθύνου προστασίας δεδομένων, οι τυχόν απόψεις των υποκειμένων των δεδομένων και τυχόν συμβουλές - προτάσεις ειδικών και εμπειρογνωμόνων.

## 2.10 Διαβούλευση με την Εποπτική αρχή

Στις περιπτώσεις κατά τις οποίες η διενεργηθείσα εκτίμηση αντικτύπου υποδεικνύει ότι η επεξεργασία θα επέφερε υψηλό κίνδυνο για τα υποκείμενα λόγω έλλειψης μέτρων μετριασμού του κινδύνου, ο υπεύθυνος επεξεργασίας οφείλει πριν την έναρξη της επεξεργασίας να ζητήσει τη γνώμη της εποπτικής αρχής[66]. Στην περίπτωση αυτή, εφόσον η εποπτική αρχή κρίνει ότι η σχεδιαζόμενη επεξεργασία παραβιάζει τον ΓΚΠΔ και ιδίως εάν ο υπεύθυνος επεξεργασίας δεν έχει προσδιορίσει ή μετριάσει επαρκώς τον κίνδυνο, η εποπτική αρχή παρέχει γραπτές συμβουλές προς τον υπεύθυνο επεξεργασίας μέσα σε χρονικό διάστημα 8 εβδομάδων από τη λήψη του αιτήματος διαβούλευσης, που δύναται να παραταθεί αιτιολογημένα έως 6 επιπλέον εβδομάδες. Στην πράξη δηλαδή, καθίσταται υποχρεωτική από την πλευρά του

[66] Βλ. άρθρο 36 ΓΚΠΔ και Αιτιολ. σκέψεις αρ. 84, 94 και 96.

υπευθύνου επεξεργασίας η προηγούμενη διαβούλευση με την εποπτική αρχή προστασίας δεδομένων σε περιπτώσεις όπου τα τεχνικά και οργανωτικά μέτρα που συστήνονται με την διενεργηθείσα ΕΑΠΔ δεν επαρκούν για τον μετριασμό των κινδύνων στα επιτρεπτά επίπεδα. Τέτοια περίπτωση μπορεί να συντρέχει εάν επεξεργασία αφορά δεδομένα υγείας σε ιατρικό κέντρο ή συλλογή οικονομικών στοιχείων που παρά τα υπάρχοντα μέτρα, λόγω έλλειψης ή ανεπαρκούς χρηματοδότησης για επένδυση σε εξοπλισμό ασφάλειας και επιπλέον απαραίτητων τεχνικών μέσων, υπάρχει σοβαρή πιθανότητα να επέλθει υψηλός κίνδυνος (στην υγεία, ακόμη και στη ζωή) των υποκειμένων.

Επίσης, η γνώμη της εποπτικής αρχής οφείλει να ζητείται κατά την εκπόνηση προτάσεων νομοθετικών ή κανονιστικών μέτρων.

Στα πλαίσια της διαδικασίας προηγούμενης διαβούλευσης με την εποπτική αρχή ο υπεύθυνος επεξεργασίας οφείλει να παρέχει προς την αρχή όλες τις απαραίτητες πληροφορίες, ήτοι τις αρμοδιότητές του αναφορικά με την επεξεργασία, καθώς και των από κοινού υπευθύνων επεξεργασίας και εκτελούντων την επεξεργασία, τους σκοπούς και τα μέσα της επεξεργασίας, τα μέτρα και τις εγγυήσεις για την προστασία των δικαιωμάτων και ελευθεριών των υποκειμένων των δεδομένων, στοιχεία επικοινωνίας του υπεύθυνου προστασίας δεδομένων, καθώς και την ήδη διενεργηθείσα εκτίμηση αντικτύπου προς γνώση της αρχής. Μάλιστα, η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα στην Ελλάδα, έχει καθορίσει τη διαδικασία προηγούμενης διαβούλευσης των ενδιαφερόμενων υπευθύνων επεξεργασίας με πρόβλεψη υποβολής σχετικού ηλεκτρονικού αιτήματος[67]. Ενδιαφέρον έχει περίπτωση έκδοσης Γνωμοδότησης της ΑΠΔΠΧ[68] κατόπιν αιτήματος για διαβούλευση που υποβλήθηκε από το Ανώτατο Συμβούλιο Επιλογής Προσωπικού (ΑΣΕΠ) σχετικά με υπολειπόμενο κίνδυνο κατά την ανάρτηση δεδομένων ειδικών κατηγοριών στο διαδικτυακό του τόπο, σύμφωνα με την οποία η Αρχή εξέτασε τα στοιχεία και κατέληξε στην έκδοση Γνωμοδότησης με συγκεκριμένες προτάσεις και όρους υπό τους οποίους πρέπει να ενεργείται η ανάρτηση των πινάκων κατάταξης και διοριστέων στον ιστότοπο του ΑΣΕΠ.

[67] Βλ. https://www.dpa.gr/el/foreis/ektimisi_adiktipou_kai_diavouleush/proigoumeni_diavouleusi .
[68] Βλ. Γνωμοδότηση υπ' αρ. 2/2020 της ΑΠΔΠΧ, https://www.dpa.gr/sites/default/files/2020-05/gnomodotisi%202_2020anonym.pdf

Σχετικά με τη νομική φύση της απάντησης της ΑΠΔΠΧ επί της υποβαλλόμενης εκτίμησης αντικτύπου έχει διατυπωθεί η άποψη[69] ότι κατ' αρχήν είναι συμβουλευτική και όχι υποχρεωτική, διότι περιέχει υποδείξεις προς τον υπεύθυνο επεξεργασίας. Περαιτέρω, εφόσον αυτή διαπιστώνει την ορθή και προσήκουσα υποβολή της, τότε πρόκειται για μια διαπιστωτική εκτελεστική διοικητική πράξη της Αρχής που μπορεί ακόμη και να προσβληθεί ενώπιον του ΣτΕ από τον έχοντα έννομο συμφέρον. Σε κάθε περίπτωση για τη νομιμότητα επεξεργασίας που συνεπάγεται υψηλό κίνδυνο, είναι υποχρεωτική η υποβολή μελέτης εκτίμησης αντικτύπου κατά τις επιταγές του Κανονισμού στην ΑΠΔΠΧ είτε η γνώμη της της Αρχής ήταν θετική προς τον υπεύθυνο επεξεργασίας είτε αρνητική. Κι αυτό διότι στη μεν θετική γνώμη, η υποστηρικτική θέση της Αρχής προς τον υπεύθυνο δεν κωλύει τυχόν παρεμπίπτων δικαστικό έλεγχο νομιμότητας της επεξεργασίας, στη δε αρνητική, η Αρχή δεν κωλύεται στην επιβολή νόμιμων κυρώσεων[70] και τότε η πράξη της έχει εκτελεστό χαρακτήρα.

## Κεφάλαιο 3 – Μεθοδολογία εκπόνησης της ΕΑΠΔ κατά το πρότυπο της γαλλικής αρχής CNIL

### 3.1 Γενικά για τον τρόπο εκπόνησης της Ανάλυσης Αντικτύπου

Από τη Γαλλική Αρχή Προστασίας Δεδομένων (CNIL) παρέχεται ένας οδηγός[71] διενέργειας εκτίμησης αντικτύπου με στόχο την προστασία των προσωπικών δεδομένων αξιοποιώντας τις μεθόδους διαχείρισης των κινδύνων που προτείνονται από τη Γαλλική Εθνική Υπηρεσία Ασφάλειας Δικτύων και Πληροφοριών, σύμφωνα με τα κριτήρια των Κατευθυντήριων Γραμμών της Ομάδας Εργασίας 29 και κατά τα διεθνή πρότυπα διαχείρισης κινδύνων.

Στο πλαίσιο της ακολουθούμενης μεθοδολογικής προσέγγισης η συμμόρφωση στηρίζεται σε δύο βασικές συνιστώσες, τα θεμελιώδη δικαιώματα και αρχές κατά τον ΓΚΠΔ και τη διαχείριση των κινδύνων ιδιωτικής ζωής των υποκειμένων των δεδομένων. Τα μεν δικαιώματα των υποκειμένων των δεδομένων και οι αρχές που διέπουν την επεξεργασία αποτελούν τον σκληρό πυρήνα της προστασίας των προσωπικών δεδομένων, κομβικά στοιχεία θεμελιώδη και αδιαπραγμάτευτα από το νόμο, τα οποία

[69] Βλ. Κ. Χριστοδούλου, Δίκαιο Προσωπικών Δεδομένων, εκδ. Νομ. Βιβλιοθήκη 2020, σελ. 104-5.
[70] Βλ. Κ. Κόμνιο, Γενικοί όροι επιβολής διοικητικών προστίμων, Γενικός κανονισμός για την προστασία δεδομένων, Εκδ. Σάκκουλα, 2020, σελ. 170επ.
[71] Βλ. CNIL, Privacy Impact Assessment (PIA) Methology, 2018.

πρέπει να τηρούνται απαρέγκλιτα σε κάθε υπό εξέταση περίπτωση. Η δε διαχείριση των κινδύνων ασφάλειας των δεδομένων καθορίζεται από την εφαρμογή των κατάλληλων τεχνικών και οργανωτικών μέτρων για την προστασία τους.

Υπό αυτό το πρίσμα, η μεθοδολογία της Γαλλικής Αρχής προσεγγίζει σε (4) βασικά στάδια τη διενέργεια μιας εκτίμησης αντικτύπου ως εξής:

α. Καθορισμός του πλαισίου και περιγραφή των περιστάσεων της επεξεργασίας των υπό ανάλυση δεδομένων προσωπικού χαρακτήρα,

β. Αναγνώριση των υπαρχόντων ή μελλοντικών μέτρων (διαδικαστικών, τεχνικών ή οργανωτικών) που εγγυώνται τη συμμόρφωση τηρώντας τις αρχές της αναλογικότητας και αναγκαιότητας της επεξεργασίας,

γ. Αξιολόγηση των κινδύνων που διατρέχουν τα δικαιώματα και οι ελευθερίες των υποκειμένων των δεδομένων ώστε να επιβεβαιωθεί ότι τα μέτρα διαχείρισης είναι τα κατάλληλα και

δ. Τεκμηρίωση της επικύρωσης της ΕΑΠΔ υπό το φως των ευρημάτων της μελέτης ή λήψη απόφασης για αναθεώρηση των προηγούμενων βημάτων.

Παράλληλα ιδιαίτερη έμφαση δίνεται στο γεγονός ότι η εκπόνηση της μελέτης αποτελεί μία επαναλαμβανόμενη διαδικασία διαρκούς βελτίωσης με πιθανές τροποποιήσεις και επικαιροποιήσεις όπου απαιτούνται, καθώς επίσης και στο ότι πρέπει να υλοποιείται κατά το σχεδιασμό του συστήματος και πριν την έναρξη της επεξεργασίας.

## 3.2 Μελέτη των περιστάσεων- Ανάλυση και περιγραφή των πράξεων επεξεργασίας

Κατά το πρώτο στάδιο εκπόνησης της μελέτης καθορίζεται το γενικό πλαίσιο της ΕΑΠΔ και περιγράφονται οι υπό κρίση συνθήκες. Η διαδικασία αυτή, όπως έχει προαναφερθεί, διεξάγεται από τον ίδιο τον υπεύθυνο επεξεργασίας με τη συνδρομή του υπεύθυνου προστασίας των δεδομένων και τυχόν άλλου αρμόδιου επικεφαλής για την προστασία των δεδομένων.

Στο στάδιο αυτό η κατανόηση των τρόπων επεξεργασίας των προσωπικών δεδομένων είναι σημαντική για την ανάδειξη και διασαφήνιση ακόμη περαιτέρω σημαντικών παραμέτρων, όπως οι φορείς της επεξεργασίας, η έκταση και τα όρια του

πεδίου εφαρμογής του νόμου, οι βασικές αρχές που τη διέπουν την επεξεργασία και η νομιμότητά της. Ενόψει αυτών,

√ επιχειρείται ο προσδιορισμός και μία σύντομη παρουσίαση της υπό εξέταση επεξεργασίας, ως προς τη φύση της, το πεδίο εφαρμογής της και τις περιστάσεις. Για παράδειγμα, εδώ θα μπορούσε να γίνει σύντομη αναφορά του νέου προϊόντος ή συστήματος ή προγράμματος, του τρόπου λειτουργίας του, των συσκευών ή τμημάτων που το συνθέτουν, του τρόπου συνδεσιμότητας, τυχόν διαδραστικότητα που προσφέρει, τα οφέλη του και τους σκοπούς που εξυπηρετεί κλπ.

√ Παράλληλα, παρατίθεται μία συνοπτική ανάλυση των σκοπών της επεξεργασίας και των διακυβευμάτων αυτής, δηλαδή ποια είναι η προσδοκώμενη ωφέλεια για τον φορέα, τα υποκείμενα των δεδομένων και το κοινωνικό σύνολο ή δημόσιο περιβάλλον γενικότερα από την μέλλουσα σε λειτουργία εφαρμογή.

√ Στη συνέχεια, γίνεται προσδιορισμός του υπεύθυνου επεξεργασίας, των εκτελούντων την επεξεργασία και τυχόν τρίτων που εμπλέκονται. Είναι σημαντικό να αναγνωρίζονται οι φορείς της επεξεργασίας και τα εμπλεκόμενα σε αυτή πρόσωπα διότι έτσι μπορούν να διασαφηνιστούν τα όρια μεταξύ τους και να προβούν σε καθορισμό των υποχρεώσεων και καταμερισμό της ευθύνης του καθενός στο μέτρο που του αναλογεί. Ακόμη, είναι σημαντικό να αναγνωρίζονται και τα πρόσωπα που επηρεάζονται γενικότερα από την πράξη επεξεργασίας (και ως εκ τούτου και οι πιθανές απειλές σε επόμενο στάδιο). Στο σημείο αυτό για παράδειγμα θα μπορούσαν να υπάρχουν αναφορές για τον διαχωρισμό των ρόλων και αρμοδιοτήτων του κάθε εμπλεκόμενου, για τις ευθύνες που συνδέονται με την επεξεργασία και ποιους αφορούν αυτές, δηλαδή εάν εντοπίζονται στο πρόσωπο του κατασκευαστή, των εσωτερικών ή εξωτερικών συνεργατών, των εργαζομένων/υπαλλήλων του οργανισμού ή οποιουδήποτε άλλου συμμετέχοντος και εμπλεκόμενου προσώπου με κάθε τρόπο, ακόμη και πολιτών, πελατών, τυχαίων τρίτων προσώπων[72].

√ Λαμβάνονται υπόψη τυχόν πρότυπα που εφαρμόζονται στην επεξεργασία, δηλαδή τομεακά πλαίσια και standards κατά τη διάταξη της παρ. 8 του άρθρου 35 του

[72] Βλ. Felix Bieker, Michael Friedeward, Marit Hansen, Hannah Obersteller and Martin Rost, A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation, Springer, 2016.

ΓΚΠΔ, όπως για παράδειγμα εγκεκριμένοι κώδικες δεοντολογίας[73], πιστοποιήσεις[74], πλάνο ασφάλειας και πλαίσιο ιδιωτικότητας που πρέπει να ληφθούν υπόψη.

Επιπρόσθετα, στο στάδιο αυτό διερευνώνται και εντοπίζονται όλα τα ζητήματα που αφορούν το είδος και τη φύση της επεξεργασίας. Ενδεικτικά, ερευνάται εάν το είδος της επεξεργασίας εμπίπτει στο πεδίο εφαρμογής του νόμου[75], εάν η επεξεργασία πραγματοποιείται από υπεύθυνο επεξεργασίας που είναι εγκατεστημένος στην Ελληνική επικράτεια ή όχι, εάν εμπίπτει στο πεδίο εφαρμογής του νόμου ως προς την αρμοδιότητα εποπτείας και ελέγχου της επεξεργασίας, εάν η επεξεργασία εκτελείται από δημόσιο ή ιδιωτικό φορέα, εάν αποτελεί κύρια ή παρεπόμενη δραστηριότητα[76], εάν πρόκειται για πράξη που πραγματοποιείται με τη χρήση αυτοματοποιημένων μέσων ή με ανθρώπινη παρέμβαση, εάν υπάρχουν διασυνοριακές διαβιβάσεις δεδομένων και άλλα ζητήματα ανάλογα με την υπό εξέταση περίπτωση.

### 3.3 Περιγραφή προσωπικών δεδομένων, αποδέκτες, διάρκεια αποθήκευσης και υποστηρικτικά περιουσιακά στοιχεία

Συνακόλουθα, στα πλαίσια της κατανόησης του τρόπου επεξεργασίας, εξέχουσα σημασία έχει η αναγνώριση και περιγραφή των προσωπικών δεδομένων που υφίστανται την επεξεργασία. Εξετάζονται και προσδιορίζονται οι κατηγορίες των προσωπικών δεδομένων που πρόκειται να τεθούν σε επεξεργασία. Στην έννοια των δεδομένων προσωπικού χαρακτήρα εντάσσεται κάθε πληροφορία που αφορά ταυτοποιημένο, ή ταυτοποιήσιμο, φυσικό πρόσωπο εν ζωή, του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε οποιοδήποτε αναγνωριστικό στοιχείο του που είναι ικανό να το ταυτοποιήσει, είτε μόνο του είτε σε συνδυασμό με άλλα στοιχεία[77].

---

[73] Βλ. άρθρο 40 ΓΚΠΔ.
[74] Βλ. άρθρο 42 ΓΚΠΔ.
[75] Βλ. σχετικά με θετική και αρνητική οριοθέτηση της επεξεργασίας σε Αλεξανδροπούλου-Αιγυπτιάδου Ε., Προσωπικά δεδομένα, εκδ. Νομ. Βιβλιοθήκη 2016, σελ. 56επ και σχετικά με περιορισμούς επεξεργασίας κατά το Λειτουργικό και Εδαφικό κριτήριο σε Φ. Μίτλεττον σε Λ. Κοτσαλή, Προσωπικά Δεδομένα, Ανάλυση-Σχόλια-Εφαρμογή, Εκδ. Νομική Βιβλιοθήκη, 2016, σελ. 52 επ.
[76] Βλ. Αιτιολ. σκέψη αρ. 97 του ΓΚΠΔ και Ομάδα εργασίας του άρθρου 29, Κατευθυντήριες γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων,2017.
[77] Βλ. Λ. Κανέλλο, The GDPR Handbook, Εκδ. Νομική Βιβλιοθήκη, 2020, σελ. 16, Ανάλυση της έννοιας των προσωπικών δεδομένων στη Γνώμη 4/2007 της Ομάδας του άρθρου 29, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf, Ε. Αλεξανδροπούλου - Αιγυπτιάδου, Προσωπικά δεδομένα, εκδ. Νομ. Βιβλιοθήκη 2016, σελ. 43επ, Φ. Μίτλεττον σε Λ. Κοτσαλή, Προσωπικά Δεδομένα, Ανάλυση-Σχόλια-Εφαρμογή, Εκδ. Νομική Βιβλιοθήκη, 2016, σελ. 5 επ., Κ. Χριστοδούλου, Δίκαιο Προσωπικών Δεδομένων, εκδ. Νομ. Βιβλιοθήκη 2020, σελ. 23επ.

Από τη Γαλλική Αρχή προτείνεται η καταγραφή μιας λεπτομερούς λίστας των υπό επεξεργασία προσωπικών δεδομένων, ανά κατηγορία[78]. Τα προσωπικά δεδομένα, γενικά και ενδεικτικά, κατηγοριοποιούνται στα απλά προσωπικά δεδομένα, τα προσωπικά δεδομένα που εκλαμβάνονται ως ευαίσθητα και τα προσωπικά δεδομένα ειδικών κατηγοριών[79]. Στην πρώτη κατηγορία εντάσσονται οι προσωπικές πληροφορίες και στοιχεία ταυτοποίησης (αριθμός δελτίου ταυτότητας, τηλεφωνικός αριθμός, αριθμός πινακίδας αυτοκινήτου κ.α.), ληξιαρχικά στοιχεία, δεδομένα οικογενειακής και περιουσιακής κατάστασης (όπως καταναλωτικές συνήθειες, ταξιδιωτική δραστηριότητα, οικογενειακή κατάσταση), πληροφορίες για την οικονομική κατάσταση (μισθός, τραπεζικοί λογαριασμοί, φορολογική κατάσταση), για την επαγγελματική ζωή (μορφωτικό και εκπαιδευτικό επίπεδο, επαγγελματική θέση, αξιολόγηση), πληροφορίες για τη συνδεσιμότητα στο διαδίκτυο (ηλεκτρονική διεύθυνση, IP διεύθυνση), δεδομένα θέσης και κίνησης (πληροφορίες εντοπισμού γεωγραφικής θέσης (GPS), πληροφορίες από συστήματα κινητής τηλεφωνίας (GSM)). Στην δεύτερη κατηγορία εντάσσονται ο Αριθμός Μητρώου Κοινωνικής Ασφάλισης (ΑΜΚΑ), τα βιομετρικά δεδομένα (δακτυλικά αποτυπώματα, αναγνώριση ίριδας οφθαλμού, αναγνώριση προσώπου, φωνής, σχήμα χεριών, ανάλυση τρόπου βαδίσματος)[80] και δεδομένα τραπεζικής φύσεως. Στην τρίτη κατηγορία εντάσσονται δεδομένα που αφορούν στη φυλετική ή εθνική προέλευση, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, τη συμμετοχή σε συνδικαλιστική οργάνωση, την υγεία, την κοινωνική πρόνοια, στην ερωτική ζωή, τα γενετικά δεδομένα (κληρονομικά χαρακτηριστικά και πληροφορίες που προκύπτουν από ανάλυση βιολογικού δείγματος ενός προσώπου). Ομοίως εδώ υπάγονται και πληροφορίες σχετικά με ποινικές διώξεις ή καταδίκες (ποινικό μητρώο, ένταλμα σύλληψης). Ιδιαίτερης προστασίας απολαμβάνουν τα δεδομένα που αφορούν ανήλικα και ως τέτοια πρέπει να αξιολογούνται με ιδιαίτερη προσοχή.

Ταυτόχρονα, εξετάζεται και ο τρόπος με τον οποίο τα υπό αναγνώριση προσωπικά δεδομένα εισέρχονται τον οργανισμό. Θα μπορούσε αυτά να εισάγονται

[78] Βλ. The open source PIA software helps to carry out data protection impact assessment, https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assessment

[79] Βλ. CNIL, Privacy Impact Assessment (PIA) Knowledge Bases, 2018, σελ. 2επ και Δ. Τζέλλη. Μ. Μυλώση, Εκτίμηση Αντικτύπου στην προστασία προσωπικών δεδομένων, Εκδ. Νομική Βιβλιοθήκη, 2022, σελ. 5 επ.

[80] Βλ. Ε. Βασιλοπούλου, σε Λ. Κοτσαλή – Κ. Μενουδάκο, Γενικός Κανονισμός για την προστασία των προσωπικών δεδομένων, Νομική διάσταση και πρακτική εφαρμογή, εκδ. Νομ. Βιβλιοθήκη 2021, σελ. 93.

από το ίδιο το υποκείμενο των δεδομένων ή μέσω μιας εφαρμογής που διαχειρίζεται τρίτο μέρος στην οποία ο χρήστης πιθανώς να χρειάζεται να δημιουργήσει λογαριασμό ή να πρόκειται για ηχογραφημένα και μαγνητοσκοπημένα αρχεία ήχου, εικόνας ή κίνησης που ο χρήστης καταγράφει και αποθηκεύει σε κινητή ή σταθερή συσκευή του ή σε ένα υπολογιστικό νέφος. Όλα αυτά τα στοιχεία αποτιμώνται στη μελέτη καθώς από την ορθή και έγκαιρη αξιολόγησή τους πιθανόν να προκύψουν οι απειλές και οι κίνδυνοι που εγκυμονούν ώστε τελικά να αποφευχθούν με κατάλληλο σχεδιασμό.

Επιπρόσθετα, επιχειρείται αναγνώριση και καταγραφή των πιθανών προσώπων που έχουν πρόσβαση στα δεδομένα και πιθανών παραληπτών των προσωπικών δεδομένων. Σημειώνονται τα πρόσωπα που έχουν πρόσβαση στις πληροφορίες, αιτιολογείται ο λόγος και οριοθετούνται τα πλαίσια στα οποία δύνανται να δρουν εντός των αρμοδιοτήτων τους. Οι εργαζόμενοι και εσωτερικοί ή εξωτερικοί συνεργάτες πρέπει να είναι εξουσιοδοτημένοι και να διασφαλίζεται η νόμιμη πρόσβασή τους στα προσωπικά δεδομένα με ασφαλή τρόπο. Σημειώνονται οι πιθανοί αποδέκτες των πληροφοριών που συνδέονται με τον υπεύθυνο επεξεργασίας στους οποίους κοινολογούνται τα δεδομένα. Θα μπορούσαν να είναι άλλες συνδεδεμένες εταιρείες, δημόσιοι ή ενδοεπιχειρησιακοί φορείς, συνεργάτες, διαφημιστικές εταιρείες και γενικά κατηγορίες αποδεκτών στους οποίους διαβιβάζονται τα προσωπικά δεδομένα είτε εντός της ίδιας εδαφικής περιφέρειας είτε σε τρίτες χώρες ή διεθνείς οργανισμούς. Η επισκόπηση των ζητημάτων αυτών πριν την έναρξη της επεξεργασίας έχει ιδιαίτερη σημασία καθώς αποφεύγονται τυχόν δυσμενείς συνέπειες για τα υποκείμενα των δεδομένων και εξασφαλίζεται ότι δεν διαβιβάζονται προσωπικά δεδομένα που βρίσκονται σε περιορισμό ή χωρίς νόμιμη δικαιολογητική βάση.

Ακόμη, επιχειρείται προσδιορισμός και καταγραφή του απαιτούμενου χρόνου διάρκειας τήρησης των δεδομένων ανάλογα με τον υπό εξέταση σκοπό της συλλογής και επεξεργασίας τους. Τούτο είναι σημαντικό καθώς, πέραν της υποχρεωτικής επιβολής του προσδιορισμού από τις διατάξεις του νόμου, επηρεάζει και τον τρόπο και τις προβλεπόμενες διαδικασίες καταστροφής των δεδομένων με ευθύνη του υπεύθυνου επεξεργασίας μετά την πάροδο του προβλεπόμενου χρόνου, αλλά και προβλέπει διαδικασίες για τυχόν διατήρησή τους για δευτερεύοντα σκοπό (π.χ. στατιστικό, έρευνας) υπό όρους και υπό τη λήψη των κατάλληλων οργανωτικών μέτρων.

Στη συνέχεια, παρουσιάζεται μία λεπτομερής περιγραφή του κύκλου ζωής των προσωπικών πληροφοριών και του τρόπου επεξεργασίας στην συγκεκριμένη περίπτωση. Αποτυπώνεται δηλαδή ο τρόπος και οι διαδικασίες ροής των προσωπικών δεδομένων από τη συλλογής τους μέχρι τη διαγραφή τους. Θα μπορούσε να εκτεθεί για παράδειγμα ότι αρχικά ο χρήστης δημιουργεί έναν λογαριασμό σε μία εφαρμογή στο κινητό του παρέχοντας προσωπικά του στοιχεία που τον ταυτοποιούν. Ακολούθως, τα δεδομένα του μεταφέρονται και αποθηκεύονται σε εξωτερικό εξυπηρετητή (server) ή σε υπολογιστικό νέφος. Στην εφαρμογή αυτή έχει πρόσβαση με δικό του λογαριασμό και τρίτο μέρος με το οποίο μπορούν να συναλλάσσονται και να μεταφέρουν πληροφορίες για ορισμένο σκοπό. Μερικά από τα προσωπικά δεδομένα, κατόπιν συγκατάθεσης και εντολής, διαβιβάζονται σε εφαρμογές που ελέγχουν τρίτα μέρη ή μοιράζονται στο διαδίκτυο.

Τέλος, αναγνωρίζονται και καταγράφονται τα υποστηρικτικά στοιχεία των προσωπικών δεδομένων δηλαδή τα μέρη του πληροφοριακού συστήματος και γενικά οι υπολογιστικοί πόροι στους οποίους βασίζεται η επεξεργασία. Τέτοια μπορεί να είναι στοιχεία του εξοπλισμού και των ηλεκτρονικών μέσων, όπως κεντρικοί εξυπηρετητές (servers), τερματικά που χρησιμοποιούν οι χρήστες που έχουν πρόσβαση στα προσωπικά δεδομένα, σκληροί δίσκοι, μνήμες, οθόνες, μονάδες USB, δικτυακές συσκευές (δικτυακοί εκτυπωτές, βιντεοπροβολείς (projectors), σαρωτές (scanners), φωτοτυπικά μηχανήματα) και δικτυακές και επικοινωνιακές υποδομές που στηρίζουν τη λειτουργία του οργανισμού (δρομολογητές, μεταγωγείς, ασύρματες δικτυακές συσκευές, καλώδια). Ομοίως, αποτυπώνονται τα λειτουργικά συστήματα (πχ. WINDOWS), τα λογισμικά (πχ. Office), ο τρόπος σύνδεσης στα δίκτυα, ο τρόπος σύνδεσης και πρόσβασης στα λογισμικά (τοπικά, μέσω τοπικού server, μέσω διαδικτύου, ενσύρματη ή απομακρυσμένη πρόσβαση). Παράλληλα, αναγνωρίζεται και καταγράφεται και το ανθρώπινο δυναμικό που συμμετέχει, δηλαδή οι χρήστες, οι υπεύθυνοι ασφάλειας, αντιγράφων ασφαλείας, ασφάλειας δικτύου και πληροφοριακών συστημάτων, διαχείρισης λογαριασμού χρηστών, αναβάθμισης λειτουργικών συστημάτων, παρακολούθησης δικτύων, κρυπτογράφησης αρχείων server κ.α.

Ιδιαίτερη έμφαση αποδίδεται στα παραπάνω ζητήματα καθώς η ανάλυση και λεπτομερής περιγραφή του είδους και της έκτασης της επεξεργασίας καταδεικνύει σε σημαντικό βαθμό τη βαρύτητα και πιθανότητα επέλευσης ενός κινδύνου ώστε αυτός

να αποτιμηθεί κατάλληλα από τον υπεύθυνο επεξεργασίας. Ο στόχος αυτής της εκτίμησης των πιθανών κινδύνων καθορίζει στην ουσία και το σκοπό της διενέργειας της μελέτης εκτίμησης αντικτύπου[81].

## 3.4 Περιπτωσιολογία

Κατόπιν των ανωτέρω ακολουθεί μια συνοπτική και όλως ενδεικτική παρουσίαση περιπτώσεων κατ' εφαρμογή των προεκτεθέντων ζητημάτων.

⇨ Εμπορικό Επιμελητήριο σε έναν νομό διενεργεί εκτίμηση αντικτύπου στα πλαίσια της εφαρμογής τηλεργασίας και πραγματοποίησης τηλεδιασκέψεων λόγω προστασίας της υγείας των υπαλλήλων και της δημόσιας υγείας εν μέσω πανδημίας. Σκοπός της εκπόνησης της μελέτης είναι ο σχεδιασμός και η λήψη κατάλληλων τεχνικών και οργανωτικών μέτρων, ταυτόχρονα με τον καθορισμό του πλαισίου των κανόνων τηλεργασίας και απομακρυσμένης πρόσβασης για τα υπολογιστικά συστήματα του Οργανισμού, όπως και τη λήψη μέτρων για ευαισθητοποίηση των εμπλεκομένων για τους κινδύνους που αφορούν στην προστασία των προσωπικών δεδομένων. Αρχικά παρέχονται πλήρη στοιχεία του υπεύθυνου επεξεργασίας, ήτοι επωνυμία, νομική μορφή, διεύθυνση, ΑΦΜ, ηλεκτρονική διεύθυνση, ιστότοπος, στοιχεία επικοινωνίας υπεύθυνου προστασίας δεδομένων. Γίνεται ανάλυση της κύριας επεξεργασίας (τηλεργασίας και απομακρυσμένης πρόσβασης στα πληροφοριακά συστήματα του οργανισμού) και όλων των σχετιζόμενων επεξεργασιών στον οργανισμό λόγω απομακρυσμένης πρόσβασης. Κατά την περιγραφή της κύριας επεξεργασίας γίνεται αναγνώριση και καταγραφή της απομακρυσμένης πρόσβασης του υπαλλήλου σε πόρους των πληροφορικών συστημάτων του οργανισμού, όπως υπολογιστές εσωτερικού δικτύου και εσωτερικά αρχεία, μέσα από χρήση τερματικής συσκευής (Η/Υ, laptop) και αποθηκευτικών μέσων (πχ. usb stick) που μεταφέρονται εκτός του οργανισμού. Κατά την ανάλυση των λοιπών σχετιζόμενων επεξεργασιών που πραγματοποιούνται στον οργανισμό γίνεται σύντομη περιγραφή κάθε διαδικασίας. Ενδεικτικά, γίνεται ανάλυση της επεξεργασίας που πραγματοποιείται για την τήρηση του Μητρώου Μελών του Επιμελητηρίου, ήτοι κατόπιν αίτησης εγγραφής του μέλους και προσκόμισης των απαιτούμενων δικαιολογητικών συλλέγονται και αρχειοθετούνται

[81] Βλ. Felix Bieker, Michael Friedeward, Marit Hansen, Hannah Obersteller and Martin Rost, A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation, Springer, 2016.

τα προσωπικά δεδομένα (ατομικών επιχειρήσεων και νομίμων εκπροσώπων των εταιρειών) που χειρίζονται οι υπάλληλοι του οργανισμού με τη χρήση συγκεκριμένου πληροφοριακού συστήματος μέσω του οποίου καταχωρούν όλα τα στοιχεία των μελών, έχουν πρόσβαση σε όλο το αρχείο Μητρώου μελών, διαχειρίζονται το Πρωτόκολλο, εκδίδουν πιστοποιητικά και βεβαιώσεις, χορηγούν ταμειακή ενημερότητα κ.α. (παρουσίαση της ροή των προσωπικών δεδομένων). Επίσης, πραγματοποιείται ανάλυση της επεξεργασίας εγγραφής των στοιχείων της κάθε ατομικής επιχείρησης στο Γ.Ε.ΜΗ. (Γενικό Εμπορικό Μητρώο), ήτοι γίνεται καταχώριση των στοιχείων των ατομικών επιχειρήσεων στην ηλεκτρονική πλατφόρμα του Γ.Ε.ΜΗ. όπου καταχωρούνται και οι μεταβολές των εταιρειών από την Εφορία ή η διακοπή μιας επιχείρησης. Ακόμη, παρουσιάζεται η επεξεργασία της μισθοδοσίας των υπαλλήλων, της καταχώρισης και πληρωμής των τιμολογίων με χρήση ξεχωριστών λογιστικών προγραμμάτων και μισθοδοσίας, καθώς και λοιπές επεξεργασίες που πραγματοποιούνται και με απομακρυσμένη πρόσβαση (πρωτόκολλο Επιμελητηρίου, διοργάνωση ανταποδοτικών δράσεων του οργανισμού, ηλεκτρονική επικοινωνία με τα μέλη και τρίτους, έκδοση χρηματικών καταλόγων, τήρηση μητρώου ασφαλιστικών διαμεσολαβητών και μεσιτών ακινήτων κ.α.). Καταγράφονται σε κάθε μία δραστηριότητα οι κατηγορίες των προσωπικών δεδομένων που υφίστανται επεξεργασία, στην προκειμένη περίπτωση αφορούν μόνο σε απλά δεδομένα, όπως ατομικά στοιχεία, διεύθυνση, τηλέφωνα, αριθμός δελτίου ταυτότητας, αντικείμενο εργασιών (ΚΑΔ), οικονομικά στοιχεία και εκκρεμότητες, στοιχεία οικογενειακής κατάστασης για τους υπαλλήλους.

Στη συνέχεια, καταγράφεται η διάρθρωση των υπηρεσιών του οργανισμού, όπως για παράδειγμα τμήμα Εμποροβιομηχανικών θεμάτων, τμήμα Διοικητικού-Οικονομικού, τμήμα Μητρώου- Μηχανογραφικών Εφαρμογών, με κατανεμημένους διακριτούς ρόλους κάθε υπαλλήλου-χρήστη που έχει πρόσβαση στα πληροφοριακά συστήματα, ήτοι χρήστης Α για οικονομικό τμήμα, χρήστης Β για διοικητικό τμήμα, χρήστης Γ για Μητρώο μελών, χρήστης Δ για καταχωρίσεις Γ.Ε.ΜΗ. Διαχωρίζονται οι ρόλοι του υπευθύνου επεξεργασίας και των εκτελούντων την επεξεργασία, όπως παράδειγμα στην περίπτωση επεξεργασίας στοιχείων στο Γ.Ε.ΜΗ. όπου σημειώνεται ως υπεύθυνος επεξεργασίας το Γ.Ε.ΜΗ. και το Επιμελητήριο ως εκτελών την επεξεργασία. Εντοπίζονται οι αποδέκτες στις επεξεργασίες όπου υπάρχουν, όπως κατά

τις διαδικασίες του τμήματος του λογιστηρίου και της εξόφλησης των τιμολογίων αποδέκτες είναι η Δ.Ο.Υ., το Υπουργείο Ψηφιακής Διακυβέρνησης μέσω του προγράμματος ΔΙΑΥΓΕΙΑ, το ΚΗΜΔΗΣ (Κεντρικό Ηλεκτρονικό Μητρώο Δημοσίων Συμβάσεων), τραπεζικά ιδρύματα, το Ελεγκτικό Συνέδριο, κατά τις διαδικασίες σύναψης συμβάσεων του οργανισμού με τρίτους, λήψης και αρχειοθέτησης προσφορών αποδέκτες μπορεί να είναι η ΔΙΑΥΓΕΙΑ και το ΚΗΜΔΗΣ, ενώ για τις διαδικασίες της μισθοδοσίας και καταστάσεων προμηθευτών και πελατών αποδέκτες μπορεί να είναι τραπεζικά ιδρύματα.

Κατόπιν, περιγράφονται η υφιστάμενη τεχνολογική υποδομή και τα πληροφοριακά συστήματα στα οποία έχουν πρόσβαση οι χρήστες. Καταγράφεται ότι η λειτουργία του Επιμελητηρίου υποστηρίζεται από συγκεκριμένο αριθμό εξυπηρετητών (για παράδειγμα τέσσερεις), ήτοι ο ένας εξυπηρετεί τις υπηρεσίες του μητρώου μελών, ο δεύτερος λειτουργία των διαμοιρασμών κοινόχρηστων αρχείων και φακέλων, ο τρίτος τη δημιουργία αντιγράφων ασφαλείας και ο τελευταίος την υπηρεσία του Γ.Ε.ΜΗ. Στον κάθε εξυπηρετητή υπάρχει εξειδικευμένο λειτουργικό σύστημα για την υποστήριξη των λειτουργιών του και χρησιμοποιείται συγκεκριμένο λογισμικό διαχείρισης βάσεων. Καταγράφονται σκληροί δίσκοι που υπάρχουν και ο τρόπος που συνδέονται μεταξύ τους ώστε εάν ο ένας δίσκος καταστραφεί να μπορεί ο άλλος να λειτουργεί χωρίς να χαθούν δεδομένα. Σημειώνονται τα τερματικά που έχουν πρόσβαση στους εξυπηρετητές και ποιες ανάγκες υπηρετεί καθένα. Σε αυτά υπάρχει ενσύρματη πρόσβαση στο τοπικό δίκτυο και στο διαδίκτυο. Επιπρόσθετα, σημειώνονται οι δικτυακές υποδομές και τα επικοινωνιακά συστήματα, ήτοι το τοπικό δίκτυο στο οποίο είναι συνδεδεμένα τα τερματικά χρησιμοποιεί διευθυνσιοδότηση του πρωτοκόλλου IPv4.

Περαιτέρω, γίνεται εκτίμηση των υποστηρικτικών πόρων που θα απαιτηθούν στο πλαίσιο της τηλεργασίας και καθορίζονται οι κανόνες απομακρυσμένης πρόσβασης. Αρχικά, προϋπόθεση για την πραγματοποίηση της τηλεργασίας είναι η δυνατότητα πρόσβασης στο δίκτυο. Απαραίτητη είναι η διασφάλιση ότι δεν υπάρχει δυνατότητα μη ασφαλούς απομακρυσμένης πρόσβασης σε πόρους των πληροφορικών συστημάτων του Οργανισμού, όπως υπολογιστές εσωτερικού δικτύου και εσωτερικά αρχεία. Η ασφαλής σύνδεση μπορεί να επιτευχθεί, για παράδειγμα, μέσω εικονικού ιδιωτικού δικτύου στο οποίο πραγματοποιείται κρυπτογράφηση των δεδομένων και

αυθεντικοποίηση των χρηστών (π.χ. IPSec VPN). Καθορίζονται και περιορίζονται οι πόροι στους οποίους επιτρέπεται η απομακρυσμένη πρόσβαση στα απολύτως απαραίτητα πεδία για την εργασία τους, ανάλογα με τα καθήκοντα που επιτελεί ο τηλεργαζόμενος. Η σύνδεση σε υπολογιστικά συστήματα του οργανισμού μέσω υπηρεσίας «απομακρυσμένης επιφάνειας εργασίας» ("Remote Desktop Protocol – RDP"), επιτυγχάνεται μόνο μέσω ασφαλούς εικονικού ιδιωτικού δικτύου (VPN). Γίνεται χρήση ασφαλούς πρωτοκόλλου WPA2 με ισχυρό κωδικό, όταν η σύνδεση της συσκευής του τηλεργαζόμενου στο διαδίκτυο γίνεται μέσω ασύρματου δικτύου (Wi-Fi). Τούτο ισχύει ακόμα και όταν μετά τη σύνδεση στο διαδίκτυο, γίνεται ασφαλής σύνδεση στο δίκτυο του Οργανισμού π.χ. με χρήση VPN. Αποφεύγεται η αποθήκευση αρχείων με προσωπικά δεδομένα σε υπηρεσίες διαδικτυακής αποθήκευσης (λ.χ. Dropbox, One Drive google drive), εκτός κι αν υπάρχουν τα κατάλληλα εχέγγυα, όπως παράδειγμα να πρόκειται για υπηρεσία που παρέχεται, με κατάλληλα μέτρα ασφάλειας από τον οργανισμό ή να υπάρχει η δυνατότητα να αποθηκεύονται τα δεδομένα αποκλειστικά σε κατάλληλα κρυπτογραφημένη μορφή.

Όταν ο υπάλληλος κάνει χρήση τερματικής συσκευής και αποθηκευτικών μέσων τηρούνται συγκεκριμένα μέτρα, ήτοι εγκατάσταση και τακτική ενημέρωση αντιϊκού προγράμματος και «αναχώματος ασφαλείας» (firewall) στη συσκευή (λ.χ. υπολογιστής, laptop) μέσω της οποίας πραγματοποιείται η τηλεργασία, εγκατάσταση των πλέον πρόσφατων ενημερώσεων λογισμικού εφαρμογών και λειτουργικού συστήματος της συσκευής των υπαλλήλων, χρήση ενημερωμένων εκδόσεων προγραμμάτων πλοήγησης στο Διαδίκτυο (π.χ. Firefox, Chrome κλπ) και μη τήρηση ιστορικού (ανώνυμη περιήγηση) ή διαγραφή από το ιστορικό των συνδέσμων που σχετίζονται με την τηλεργασία κατά το τέλος της εργασίας, διαχωρισμός των αρχείων που περιέχουν προσωπικά δεδομένα, τα οποία σχετίζονται με την εργασία από προσωπικά αρχεία που τηρεί ο υπάλληλος στη συσκευή (παράδειγμα σε σαφώς διακριτούς φακέλους, με κατάλληλη προσδιοριστική ονομασία), υποστήριξη από τον οργανισμό διαδικασιών κατάλληλης κρυπτογράφησης αρχείων που περιέχουν προσωπικά δεδομένα, ιδίως όταν τηρούνται σε φορητό - αποσπώμενο μέσο αποθήκευσης (π.χ. usb stick). Ανά περίπτωση, εξετάζεται και το ενδεχόμενο κρυπτογράφησης των αρχείων και στην κυρίως συσκευή από την οποία πραγματοποιείται η τηλεργασία (Η/Υ, laptop), ιδίως για δεδομένα υψηλού κινδύνου, ο

οργανισμός πρέπει να υποστηρίζει διαδικασίες λήψης αντιγράφων ασφαλείας για αρχεία με προσωπικά δεδομένα, στα οποία πραγματοποιείται επεξεργασία στο πλαίσιο δραστηριοτήτων τηλεργασίας και «κλείδωμα» της συσκευής από την οποία γίνεται η τηλεργασία (λ.χ. προφύλαξη οθόνης, με κωδικό απενεργοποίησης) εφόσον μείνει, για κάποιο λόγο, χωρίς επιτήρηση. Στην περίπτωση φορητού εξοπλισμού, ο οποίος μπορεί να μεταφερθεί εκτός οργανισμού, τηρούνται πρόσθετες απαιτήσεις ασφάλειας, όπως δεν περιέχονται ευαίσθητα δεδομένα, είναι πλήρως ενημερωμένος ως προς το λογισμικό και τις διορθώσεις ασφάλειας των εφαρμογών, η χρήση του καθορίζεται σαφώς κατά την παραλαβή του, είναι κρυπτογραφημένος ο σκληρός δίσκος, διαθέτει εγκατεστημένο antitheft λογισμικό, έχει εγκατεστημένο και ενημερωμένο αντιϊκό (antivirus) κ.α.

Ως εκ τούτου η τηλεργασία πραγματοποιείται από ασφαλή χώρο σύμφωνα με συγκεκριμένες διαδικασίες, όπως καθορισμός στατικής IP για ασφαλή σύνδεση μέσω VPN, καθορισμός των χρηστών που θα έχουν δικαίωμα πρόσβασης, ο φορητός υπολογιστής είναι πάντοτε υπό την επίβλεψη του υπαλλήλου και να κλειδώνεται πάντα σε περίπτωση απουσίας αυτού, δεν επιτρέπεται η χρήση του υπολογιστή από τρίτα πρόσωπα πέραν του εξουσιοδοτημένου υπαλλήλου, ο οποίος για την εργασία αυτή έχει λάβει σχετική γραπτή έγκριση από τον Υπεύθυνο Επεξεργασίας.

Κατά την πραγματοποίηση τηλεδιασκέψεων αξιοποιούνται πλατφόρμες που υποστηρίζουν υπηρεσίες ασφαλείας (κρυπτογράφηση). Για παράδειγμα, πρέπει να αποφεύγεται λογισμικό τηλεδιάσκεψης που δεν εξασφαλίζει κρυπτογράφηση από άκρη σε άκρη (end-to-end encryption). Σε περίπτωση προγραμματισμένης τηλεδιάσκεψης, πρέπει να προστατεύονται οι σύνδεσμοι (links) αυτής και πρέπει να επιδεικνύεται ιδιαίτερη μελέτη των όρων χρήσης και των όρων προστασίας προσωπικών δεδομένων κατά τη χρήση της τηλεδιάσκεψης.

## Κεφάλαιο 4 – Μελέτη των θεμελιωδών Αρχών

### 4.1 Αξιολόγηση των προτιθέμενων δράσεων κατ’ εφαρμογή της αρχής αναλογικότητας και αναγκαιότητας

Στο δεύτερο στάδιο της μεθοδολογίας της εκτίμησης αντικτύπου κατά τη Γαλλική Αρχή, προβλέπεται η μελέτη των θεμελιωδών αρχών[82]. Πρωταρχική σημασία πριν την εφαρμογή ενός συστήματος έχει ο έλεγχος για την τήρηση των αρχών επεξεργασίας σε κάθε πράξη ή δραστηριότητα που αναλαμβάνεται από τον υπεύθυνο ή εκτελούντα την επεξεργασία και περιέχει προσωπικά δεδομένα, κατά τις διατάξεις του άρθρου 5 του ΓΚΠΔ.

Σύμφωνα με τις επιταγές του Ευρωπαϊκού Κανονισμού σε συνδυασμό και με τον εθνικό εκτελεστικό νόμο 4624/2019[83], κομβικό στοιχείο για την προστασία των προσωπικών δεδομένων αποτελεί η τήρηση των αρχών σύννομης επεξεργασίας τους[84] οι οποίες πρέπει να συντρέχουν σωρευτικά[85]. Το βάρος απόδειξης φέρει πάντα ο υπεύθυνος επεξεργασίας σύμφωνα με την αρχή της λογοδοσίας[86]. Ακολουθεί ειδικότερη ανάπτυξη.

### 4.1.1. Προσδιορισμός του σκοπού της επεξεργασίας

Μετά την ανάλυση και περιγραφή της επεξεργασίας, που ήδη έχει προηγηθεί από τον ιδιοκτήτη του έργου, πρωταρχικό και αναγκαίο βήμα για την εγγύηση της συμμόρφωσης αποτελεί ο προσδιορισμός, η καταγραφή και η αιτιολόγηση του σκοπού της συγκεκριμένης επεξεργασίας που προτίθεται να ξεκινήσει.

Σύμφωνα με την αρχή του «περιορισμού του σκοπού» τα προσωπικά δεδομένα πρέπει να συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και να μην υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς[87]. Αυτό σημαίνει ότι η επεξεργασία των δεδομένων πρέπει να υπηρετεί συγκεκριμένο, σαφή και νόμιμο σκοπό και αυτός να καθορίζεται πριν καν αρχίσει η επεξεργασία[88]. Η αρχή αυτή έχει ιδιαίτερη βαρύτητα διότι επηρεάζει άμεσα τον

[82] Βλ. CNIL, Privacy Impact Assessment (PIA) Methology, 2018, σελ. 5.
[83] Βλ. άρθρο 45 του Ν. 4624/2019.
[84] Βλ. Λ. Μήτρου, Ο γενικός κανονισμός προστασίας προσωπικών δεδομένων, νεό δίκαιο – νέες υποχρεώσεις – νέα δικαιώματα, εκδ. Σάκκουλα 2017, σελ. 57.
[85] Βλ. ΑΠΔΠΧ απόφαση 26/2019, σκ. 5, Δικαστήριο Ευρωπαϊκής Ένωσης (ΔΕΕ) απόφαση της 16-01-2019 στην υπόθεση C-496/2017 Deutsche Post AG κατά Hauptzollamt Koln., σκ. 57, Ι. Ιγγλεζάκη, Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων, Εκδ. 2η, Intractive Books, 2018, σελ. 63.
[86] Βλ. άρθρο 5 παρ. 2 ΓΚΠΔ.
[87] Βλ. άρθρο 5 παρ. 1 στοιχ. β, 85, 88 και 89 ΓΚΠΔ, Αιτιολ. σκέψεις αρ. 50, 159, 160 και 162, καθώς και άρθρα 27-30, 45 παρ. 1 στοιχ. β του Ν. 4624/2019.
[88] Βλ. Ομάδα εργασίας του άρθρου 29, Opinion 3/2013 on purpose limitation, WP 203, 2 Απριλίου 2013, επιπλέον βλ. Κατάλογο με κωδικούς σκοπών και συνοπτική περιγραφή τους, όπως αποτελούσε παράρτημα του εντύπου της Αρχής 2.0 «Γνωστοποίηση τήρησης Αρχείου Προσωπικών Δεδομένων», σε Ε. Αλεξανδροπούλου-Αιγυπτιάδου, Προσωπικά δεδομένα, εκδ. Νομ. Βιβλιοθήκη 2016, σελ. 589.

καθορισμό της νομιμότητας της επεξεργασίας, οριοθετεί το είδος των δεδομένων που θα συλλεγούν, την έκταση της επεξεργασίας, τους αποδέκτες και το χρονικό διάστημα αποθήκευσης. Στην ουσία αποτελεί έναν τρόπο ελέγχου των διατιθέμενων πληροφοριών των υποκειμένων ώστε να μην προσβάλλονται τα δικαιώματά τους ούτε να χρησιμοποιούνται τα δεδομένα εν αγνοία τους[89].

Ακόμη, δεν επιτρέπεται η επεξεργασία μετά τη συλλογή των δεδομένων να διευρυνθεί κατόπιν και σε περαιτέρω πεδία και χρήσεις που να εξυπηρετούν διαφορετικούς σκοπούς ασύμβατους με τον αρχικά καθορισμένο[90]. Εξαίρεση από την απαγόρευση αυτή προβλέπεται ρητά[91] μόνο σε περαιτέρω επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς, υπό τον όρο ωστόσο της διασφάλισης κατάλληλων εγγυήσεων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων, την εφαρμογή ορθών τεχνικών και οργανωτικών μέτρων και την πρόβλεψη παρεκκλίσεων, όπου αυτές είναι απαραίτητες για την εκπλήρωση των σκοπών[92].

Αξίζει να επισημανθεί ότι με τον εθνικό εφαρμοστικό νόμο προβλέπεται, κατ᾽ απόκλιση του Ευρωπαϊκού Κανονισμού, σκοπός για τον οποίο επιτρέπεται η επεξεργασία δεδομένων προσωπικού χαρακτήρα των εργαζομένων στο πλαίσιο των εργασιακών σχέσεων για σκοπούς σύναψης σύμβασης εργασίας είτε κατά την κατάρτιση αυτής εάν κρίνεται απολύτως απαραίτητο, είτε μετά τη σύναψή της για λόγους που αφορούν στην εκτέλεσή της[93].

Ειδικότερες αναφορές για την υποχρέωση τήρησης των γενικών αρχών επεξεργασίας προσωπικών δεδομένων γίνονται για τις περιπτώσεις που ο κύριος σκοπός της επεξεργασίας είναι η πρόληψη, διερεύνηση, ανίχνευση ή δίωξη ποινικών αδικημάτων ή η εκτέλεση ποινικών κυρώσεων, περιλαμβανομένων της προστασίας από απειλές κατά της δημόσιας ασφάλειας και της αποτροπής τους[94].

---

[89] Βλ. D. Solove, Nothing to Hide, The False Tradeoff Between Privacy and Security, Yale University Press, 2011, σελ. 33επ.

[90] Παράνομη η επεξεργασία δεδομένων προσωπικού χαρακτήρα για μη καθορισμένους και/ή μη περιορισμένους σκοπούς, σημειώνεται σε (FRA) Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων, έκδ. 2018, σελ. 157.

[91] Βλ. άρθρο 5 παρ. 1 στοιχ. β ΓΚΠΔ και Αιτιολ. Σκέψη 50.

[92] Βλ. Στις εγγυήσεις προτείνονται η τήρηση της αρχής ελαχιστοποίησης και η χρήση ψευδωνύμων ή η ανωνυμοποίηση, σε άρθρο 89 ΓΚΠΔ, Αιτιολ. σκέψεις αρ. 159 και άρθρα 29-30 του Ν. 4624/2019.

[93] Βλ. άρθρα 27-30 του Ν. 4624/2019, όπως και ΑΠΔΠΧ Γνωμοδότηση 1/2020 επί των διατάξεων του Ν. 4624/2019, σελ. 16, https://www.dpa.gr/sites/default/files/2020-01/gnomodotisi%201_2020.pdf.

[94] Βλ. άρθρα 43, 45, 47 και 48 του Ν. 4624/2019.

Ενόψει των ανωτέρω εκτιμάται ότι δεν είναι σύννομες και άρα επιτρεπτές επεξεργασίες που δίνουν τη δυνατότητα να πραγματοποιούνται μη συμβατές χρήσεις ή καταχρήσεις, ενώ σε κάθε περίπτωση συστήνονται τα μέτρα της ανωνυμοποίησης των δεδομένων άμεσα, της λήψης μέτρων για την αποφυγή μη εξουσιοδοτημένης πρόσβασης από τρίτους, καθώς και οργανωτικός και χωροταξικός διαχωρισμός της κάθε επεξεργασίας από τις λοιπές[95].

### 4.1.2. Δικαιολόγηση της νομικής βάσης

Η θεμελίωση της υπό εξέταση επεξεργασίας σε νόμιμη βάση αποτελεί αναμφισβήτητα πρωταρχικό μέλημα και υποχρέωση του υπεύθυνου επεξεργασίας πριν ακόμη προχωρήσει στην επεξεργασία[96]. Η **αρχή της νομιμότητας, αντικειμενικότητας και διαφάνειας**[97] ρυθμίζει το πλαίσιο του επιτρεπτού και σύννομου της επεξεργασίας. Ειδικότερα, σύμφωνα με την αρχή της νομιμότητας η επεξεργασία πρέπει να πραγματοποιείται με νόμιμο τρόπο, ο οποίος οριοθετείται περιοριστικά με έξι απαριθμούμενους επιτρεπόμενους λόγους επεξεργασίας ως εξής:

- ύπαρξη ελεύθερης, έγγραφης και θετικής συγκατάθεσης[98] του υποκειμένου των δεδομένων, το οποίο θα πρέπει να δύναται οποιαδήποτε στιγμή να ανακαλέσει (άρθρο 6 παρ. 1 στοιχ. α ΓΚΠΔ)[99]. Σε περίπτωση ανηλίκου η συγκατάθεση παρέχεται από τους ασκούντες τη γονική μέριμνα αυτού[100], ενώ το όριο ψηφιακής ενηλικίωσης έχει προσδιοριστεί στα 15 έτη[101].
- να είναι αναγκαία για την εκτέλεση της σύμβασης ή για το προσυμβατικό στάδιο (άρθρο 6 παρ. 1 στοιχ. β ΓΚΠΔ), όπως για παράδειγμα η συμφωνία για

---

[95] Βλ. Δ. Τζέλλη. Μ. Μυλώση, Εκτίμηση Αντικτύπου στην προστασία προσωπικών δεδομένων, Εκδ. Νομική Βιβλιοθήκη, 2022, σελ. 32 επ.

[96] Βλ. άρθρο 6 και 9 ΓΚΠΔ, Αιτιολ. σκέψεις αρ. 40 – 49 και 51επ, καθώς και άρθρα 21, 23-30 του Ν. 4624/2019, Λ. Μήτρου, Η θεμελίωση της νομιμότητας της επεξεργασίας, Ο γενικός κανονισμός προστασίας προσωπικών δεδομένων, νεό δίκαιο – νέες υποχρεώσεις – νέα δικαιώματα, εκδ. Σάκκουλα 2017, σελ. 69επ.

[97] άρθρο 5 παρ. 1 στοιχ. α ΓΚΠΔ και άρθρο 45 παρ. 1 στοιχ. α του Ν. 4624/2019.

[98] Βλ. Ομάδα εργασίας του άρθρου 29, Γνώμη 15/2011 σχετικά με τον ορισμό της συγκατάθεσης, WP 187, 13 Ιουλίου 2011 και CNIL, Privacy Impact Assessment (PIA), Knowledge bases, Obtaining consent, 2018, σελ. 72επ.

[99] Βλ. άρθρο 44 παρ. 1 στοιχ. ιζ και άρθρο 49 του Ν. 4624/2019, Ε. Αλεξανδροπούλου-Αιγυπτιάδου, Προσωπικά δεδομένα, εκδ. Νομ. Βιβλιοθήκη 2016, σελ. 87επ, Ι. Ιγγλεζάκη, Η συγκατάθεση στο δίκαιο προστασίας προσωπικών δεδομένων, σε Λ. Κοτσαλή Προσωπικά δεδομένα, Ανάλυση Σχόλια Εφαρμογή, εκδ. Νομ. Βιβλιοθήκη 2016, σελ. 95επ.

[100] Ειδικότερα για ζητήματα ανηλίκων και το πρόβλημα της προστασία τους βλ. σε Κ. Χριστοδούλου, Η δικαιοπρακτική ικανότητα του υποκειμένου προς συγκατάθεση στην επεξεργασία των δεδομένων του, σε Λ. Κοτσαλή – Κ. Μενουδάκο, Γενικός Κανονισμός για την προστασία των προσωπικών δεδομένων, Νομική διάσταση και πρακτική εφαρμογή, εκδ. Νομ. Βιβλιοθήκη 2021, σελ. 55επ., βλ. και για προϋποθέσεις συγκατάθεσης παιδιού σε https://www.dpa.gr/polites/prostasia .

[101] Βλ. άρθρο 21 του Ν. 4624/2019.

πραγματοποίηση κράτησης σε ένα ξενοδοχειακό κατάλυμμα, η πώληση μέσω εφαρμογής των υπηρεσιών εκγύμνασης από ένα γυμναστήριο και η επιλογή προπονητικού προγράμματος μέσω αυτής εκ των προτέρων,

- να είναι αναγκαία για τη συμμόρφωση με έννομη υποχρέωση του υπεύθυνου επεξεργασίας (άρθρο 6 παρ. 1 στοιχ. γ ΓΚΠΔ), όπως η επεξεργασία στοιχείων των εργαζομένων από μία επιχείρηση για φορολογικούς ή ασφαλιστικούς σκοπούς,
- να απαιτείται λόγω ζωτικών συμφερόντων του υποκειμένου ή άλλου προσώπου (άρθρο 6 παρ. 1 στοιχ. δ ΓΚΠΔ), όπως για παράδειγμα διαφύλαξη της δικής του υγείας ή της δημόσιας υγείας.
- να είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας (άρθρο 6 παρ. 1 στοιχ. ε ΓΚΠΔ), όπως λόγου χάρη η απόδοση εργοδοτικών εισφορών σε ασφαλιστικό οργανισμό ή η τήρηση μητρώου μελών σε εκτέλεση του καταστατικού σκοπού ενός οργανισμού-νομικού προσώπου δημοσίου δικαίου,
- να εξυπηρετεί τους σκοπούς των εννόμων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ής τρίτος (άρθρο 6 παρ. 1 στοιχ. στ ΓΚΠΔ), όπως για λόγους άμεσης εμπορικής προώθησης προϊόντων ή για σκοπούς πρόληψης απάτης[102].

Η αρχή της αντικειμενικότητας προβλέπει την υποχρέωση του υπεύθυνου επεξεργασίας να ενημερώνει τα υποκείμενα ή όποιον επηρεάζεται από την επεξεργασία για τον σύννομο και διαφανή τρόπο επεξεργασίας των δεδομένων τους και να είναι σε θέση να εγγυηθεί τη συμμόρφωση ανά πάσα στιγμή. Αφορά δηλαδή κυρίως τη σχέση του υπεύθυνου επεξεργασίας με το υποκείμενο των δεδομένων. Ενδιαφέρον έχει να

[102] Κατά τη νομολογία του ΔΕΕ στην περίπτωση αυτής της νομικής βάσης θα πρέπει να συντρέχουν σωρευτικά τρεις προϋποθέσεις: πρώτον, ο τρίτος στον οποίο κοινοποιούνται τα δεδομένα πρέπει να επιδιώκει έννομο συμφέρον, δεύτερον, η επεξεργασία των δεδομένων πρέπει να είναι αναγκαία για τους σκοπούς των επιδιωκόμενων έννομων συμφερόντων και τρίτον, τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου να μην υπερτερούν των εννόμων συμφερόντων του υπεύθυνου επεξεργασίας ή τρίτου, βλ. σε (FRA) Οργανισμό Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων, έκδ. 2018, σελ. 196.

σημειωθεί επίσης ότι η νομική βάση επεξεργασίας των προσωπικών δεδομένων επηρεάζει και το ποια δικαιώματα των υποκειμένων τυγχάνουν εφαρμογής[103].

Σύμφωνα με την αρχή της διαφάνειας ο υπεύθυνος επεξεργασίας οφείλει να εφαρμόζει μέτρα ώστε να εξασφαλίζει ότι παρέχει προς το υποκείμενο ακριβείς και σαφείς πληροφορίες για την επεξεργασία, με σύντομο και κατανοητό τρόπο και σε εύκολα προσβάσιμη μορφή, και επιπλέον να μπορεί το υποκείμενο να ασκήσει τα δικαιώματα ενημέρωσης και πρόσβασης στα δεδομένα του. Η υποχρέωση ενημέρωσης εντοπίζεται προς τρεις κατευθύνσεις, πρώτη, της ενημέρωσης του υποκειμένου, δεύτερη, της ενημέρωσης των αποδεκτών και τρίτη, την ενημέρωση περαιτέρω υπευθύνων επεξεργασίας σε περιπτώσεις διαγραφής δεδομένων[104]. Ιδιαίτερο βάρος έχει η αρχή αυτή όταν αφορά ανηλίκους.

Η επεξεργασία ειδικών κατηγοριών δεδομένων τυγχάνει αυστηρότερης προστασίας και απαγορεύεται ρητά πλην των ειδικά προβλεπόμενων εξαιρέσεων της διάταξης της παρ. 2 του άρθρου 9 ΓΚΠΔ. Παρεκκλίσεις από τη διάταξη αυτή, με διεύρυνση των εξαιρέσεων, εισάγονται με τις διατάξεις των άρθρων 22, 24 και 25 του Ν. 4624/2019 για τα δεδομένα ειδικών κατηγοριών από δημόσιους και ιδιωτικούς φορείς[105].

Επίσης, ειδικότερες διατάξεις[106] θεσπίζουν τους όρους επιτρεπόμενης επεξεργασίας δεδομένων προσωπικού χαρακτήρα και συγκατάθεσης για τους εργαζόμενους στα πλαίσια των σχέσεων απασχόλησης, την επεξεργασία μέσω συστήματος βιντεοεπιτήρησης και τους όρους εγκατάστασης και λειτουργίας καμερών. Η επεξεργασία προσωπικών δεδομένων από δημόσιες αρχές για την πρόληψη, διερεύνηση, ανίχνευση ή δίωξη ποινικών αδικημάτων ή εκτέλεση ποινικών κυρώσεων ρυθμίζεται επίσης ειδικότερα[107] και επιτρέπεται μόνο κατόπιν επαρκών εγγυήσεων και κατάλληλων διασφαλίσεων για τα προστατευόμενα έννομα συμφέροντα του

[103] Βλ. Πίνακα με σύνοψη δικαιωμάτων που μπορούν να ασκηθούν ανά νομική βάση επεξεργασίας, σε Δ. Τζέλλη, Μ. Μυλώση, Εκτίμηση Αντικτύπου στην προστασία προσωπικών δεδομένων, Εκδ. Νομική Βιβλιοθήκη, 2022, σελ. 42.

[104] Βλ. Φ. Παναγοπούλου - Κουτνατζή, Η αρχή της διαφάνειας κατά την επεξεργασία δεδομένων προσωπικού χαρακτήρα, σε Λ. Κοτσαλή – Κ. Μενουδάκο, Γενικός Κανονισμός για την προστασία των προσωπικών δεδομένων, Νομική διάσταση και πρακτική εφαρμογή, εκδ. Νομ. Βιβλιοθήκη 2021, σελ. 325επ.

[105] Βλ. Λ. Κανέλλο, Επεξεργασία δεδομένων ειδικών κατηγοριών, The GDPR Handbook, Εκδ. Νομική Βιβλιοθήκη, 2020, σελ. 266 επ.

[106] Άρθρο 27 του Ν. 4624/2019 και Λ. Κανέλλο, Εθνικά μέτρα εφαρμογής ΓΚΠΔ-Ν. 4624/2019, The GDPR Handbook, Εκδ. Νομική Βιβλιοθήκη, 2020, σελ. 242 επ.

[107] Βλ. άρθρο 10 ΓΚΠΔ και άρθρο 46-48 του Ν. 4624/2019.

υποκειμένου. Κατάλληλα μέτρα που μπορούν να εφαρμοστούν σε αυτή την ειδική κατηγορία δεδομένων αποτελούν ενδεικτικά περιορισμοί στις αρμοδιότητες και στην πρόσβαση των υπαλλήλων των διωκτικών αρχών, περιορισμοί στην περαιτέρω επεξεργασία και στην λήψη αποφάσεων με αυτοματοποιημένα μέσα και εξειδικευμένα μέτρα ασφάλειας[108].

Στα πλαίσια των προεκτεθέντων θεωρητικών ρυθμίσεων παρατίθενται ορισμένες συνιστώμενες πρακτικές που διασφαλίζουν την εφαρμογή της αρχή της νομιμότητας, αντικειμενικότητας και διαφάνειας[109]. Αφού πρωτευόντως εντοπιστεί και δικαιολογηθεί η νομική βάση στην οποία στηρίζεται η επεξεργασία, κατόπιν διασφαλίζεται με κάθε τρόπο ότι παρέχεται στα υποκείμενα η δυνατότητα να ασκήσουν τα δικαιώματά τους. Αυτό μπορεί να διασφαλίζεται είτε μέσω μιας έντυπης έγγραφης πληροφόρησης- ενημέρωσης των υποκειμένων κατά τη συμπλήρωση μιας φόρμας, όπως για παράδειγμα κατά τη συμπλήρωση αίτησης ενώπιον ενός οργανισμού τοπικής αυτοδιοίκησης για λήψη ενός βοηθήματος/επιδόματος ή κατά τη συμπλήρωση της καρτέλας άφιξης πελάτη (registration form), είτε μέσω της πολιτικής προστασίας προσωπικών δεδομένων στην ιστοσελίδα μιας επιχείρησης, είτε με άλλο τρόπο. Επίσης, ο υπεύθυνος επεξεργασίας, όπως προαναφέρθηκε, εν όψει της αρχής της λογοδοσίας, θα πρέπει να δύναται να αιτιολογήσει και αποδείξει τη νομιμότητα κάθε επεξεργασίας, όπως για παράδειγμα το νόμιμο τρόπο λήψης ελεύθερης και αδιαμφισβήτητης συγκατάθεσης του υποκειμένου ή στην περίπτωση της επίκλησης του έννομου συμφέροντος του υπεύθυνου επεξεργασίας, να αποδεικνύει την προηγούμενη στάθμιση του έννομου αυτού συμφέροντος με τα δικαιώματα και τις ελευθερίες των υποκειμένων. Ομοίως, σε δημόσιους κυρίως φορείς, όταν η επεξεργασία στηρίζεται σε έννομη υποχρέωση του υπευθύνου επεξεργασίας ή σε εκπλήρωση καθήκοντος προς το δημόσιο συμφέρον ή την άσκηση δημόσιας εξουσίας είναι αναγκαίο να σημειώνεται η συγκεκριμένη διάταξη νόμου που προβλέπει την υποχρεωτικότητα της επεξεργασίας[110]. Περαιτέρω, συχνή είναι η περίπτωση που σύνολο πράξεων επεξεργασίας μπορεί να στηρίζεται σε περισσότερες από μία νόμιμη βάση, όπως για παράδειγμα συνάπτεται σύμβαση μίσθωσης (άρα νομική βάση είναι η εκτέλεση της

[108] Βλ. Δ. Τζέλλη. Μ. Μυλώση, Εκτίμηση Αντικτύπου στην προστασία προσωπικών δεδομένων, Εκδ. Νομική Βιβλιοθήκη, 2022, σελ. 47.
[109] Επίσης Δ. Τζέλλη. Μ. Μυλώση, σελ. 40 επ.
[110] Βλ. CNIL, Privacy Impact Assessment (PIA), Knowledge bases, 2018, σελ. 40.

σύμβασης - κύρια επεξεργασία) κατά την κράτηση δωματίου από πελάτη σε ξενοδοχείο και κατόπιν αποστέλλονται ενημερωτικά ηλεκτρονικά μηνύματα (newsletters) με προσφορές και εκπτώσεις του ξενοδοχείου προς τον πελάτη για προωθητικούς και εμπορικούς σκοπούς (άρα απαιτείται συγκατάθεση - δευτερεύουσα επεξεργασία). Σε παρόμοια περίπτωση είναι σημαντικό να προηγείται ενημέρωση των υποκειμένων με όλες τις απαιτούμενες πληροφορίες κατά τη διάταξη του άρθρου 13 του ΓΚΠΔ και οπωσδήποτε ενημέρωση για το δικαίωμα ανάκλησης της συγκατάθεσής του[111]. Οι σκοποί της επεξεργασίας και η κάθε διαφορετική νομική βάση πρέπει να είναι γνωστοί και σαφείς στα υποκείμενα των δεδομένων, διαφορετικά η επεξεργασία είναι παράνομη. Ομοίως, δεν είναι επιτρεπτή επεξεργασία με σιωπηρή μετάβασή της από μία προηγούμενα υφιστάμενη. Κάτι τέτοιο θα συνιστούσε παραβίαση της αρχής της διαφάνειας. Για τον ίδιο λόγο δεν είναι επιτρεπτή η μετάβαση σε νέα επεξεργασία μετά από μία μεταβολή συνθηκών που μεταβάλει και το σκοπό της επεξεργασίας χωρίς να έχει προηγηθεί ενημέρωση του υποκειμένου και επαναπροσδιορισμός του νέου νομικού ερείσματος.

Στις περιπτώσεις της ηλεκτρονικής συγκατάθεσης η σχετική Οδηγία 2/2011[112] (ΦΕΚ Β΄/889/19-05-2011) που εκδόθηκε στο πλαίσιο του άρθρου 11 του Ν. 3471/2006, παρέχει μια σειρά από βέλτιστες πρακτικές, μεταξύ των οποίων η χρήση διαδικασίας διπλής επιβεβαιωμένης συγκατάθεσης του συνδρομητή ή χρήστη («double opt-in») κατά την οποία ο υπεύθυνος επεξεργασίας τοποθετεί στο πεδίο φόρμας της ιστοσελίδας του κατάλληλο κείμενο ενημέρωσης των χρηστών. Ο ενδιαφερόμενος πρώτα αποδέχεται το κείμενο ενημέρωσης και κατόπιν καταχωρεί τη δεύθυνση ηλεκτρονικής αλληλογραφίας του και η ενέργειά του αυτή λαμβάνεται ως δήλωση συγκατάθεσης. Κατόπιν, ο χρήστης λαμβάνει αυτοματοποιημένο μήνυμα στην ηλεκτρονική του διεύθυνση, με το οποίο γίνεται επιβεβαίωση των στοιχείων του και του ζητείται να ενεργοποιήσει τη συγκατάθεσή του. Στη συνέχεια, αφού προβεί σε ενεργοποίηση της συγκατάθεσης ο χρήστης, ο υπεύθυνος επεξεργασίας αποστέλλει νέο αυτόματο μήνυμα που τον ενημερώνει για την αποδοχή που έκανε και να του

[111] Βλ. Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (ΕΣΠΔ), Κατευθυντήριες Γραμμές 5/2020 σχετικά με τη συγκατάθεση βάσει του Κανονισμού 2016/697, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf, Ομάδα εργασίας του άρθρου 29, Γνώμη 15/2011 σχετικά με τον ορισμό της συγκατάθεσης, WP 187, 13 Ιουλίου 2011.
[112] Βλ. άρθρο 4 Οδηγίας 2/2011της ΑΠΔΠΧ με το επισυναπτόμενο σε αυτή Παράρτημα παραδειγμάτων, σελ. 21, www.dpa.gr, https://www.dpa.gr/sites/default/files/2020-01/2994_2_2011.PDF

παρέχει τη δυνατότητα να κάνει ακύρωση της εγγραφής, δηλαδή ανάκληση της συγκατάθεσης[113].

### 4.1.3. Διασφάλιση της ελαχιστοποίησης των δεδομένων

Ξεχωριστή θέση στις παραμέτρους της συμμόρφωσης έχει η αρχή της ελαχιστοποίησης[114] των δεδομένων σύμφωνα με την οποία τα δεδομένα προσωπικού χαρακτήρα πρέπει να είναι κατάλληλα, συναφή και να περιορίζονται στα απόλυτα αναγκαία για τους σκοπούς που εξυπηρετεί η συγκεκριμένη επεξεργασία. Η εν λόγω αρχή σχετίζεται άμεσα με την αρχή της αναλογικότητας και της αναγκαιότητας των δεδομένων που προβλέπουν βαθιά στάθμιση κάθε φορά της καταλληλότητας και της συνάφειας των πληροφοριών που χρησιμοποιούνται σε σχέση με αυτές που πραγματικά είναι απαραίτητες για την εκπλήρωση του νόμιμου σκοπού της υπό κρίση επεξεργασίας[115]. Ταυτόχρονα, στάθμιση των συμφερόντων και των σκοπών της επεξεργασίας πραγματοποιείται ώστε να μην υπάρχει δυσανάλογη επέμβαση στα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων. Η επεξεργασία επιτρέπεται να διενεργείται μόνο στην περίπτωση που ο σκοπός της δεν μπορεί να επιτευχθεί με διαφορετικά μέσα[116].

Ως εκ τούτων, πριν την έναρξη της επεξεργασίας εξετάζεται προσεκτικά ότι το εύρος των δεδομένων που συλλέγονται περιορίζεται στο απολύτως αναγκαίο για την επίτευξη του νόμιμου σκοπού της. Σε διαφορετική περίπτωση η συλλογή τους δεν είναι επιτρεπτή. Διασφαλίζεται ότι δε θα χρησιμοποιηθούν δεδομένα που μπορούν να επιφέρουν επιβαρυντικές ή δυσμενείς συνέπειες στα δικαιώματα και τις ελευθερίες των υποκειμένων. Στο πλαίσιο αυτό βοηθάει η εκ των προτέρων καταγραφή και κατηγοριοποίηση του είδους των προσωπικών δεδομένων που είναι απαραίτητη και αντίστοιχη αιτιολόγηση της χρήσης τους, ώστε να αναδειχθούν τυχόν πλεονασμοί. Η συλλογή τυχόν ειδικών κατηγοριών προσωπικών δεδομένων καταρχήν απαγορεύεται λόγω του ευαίσθητου χαρακτήρα τους, εκτός από εξαιρετικές περιστάσεις που

[113] Για τον τομέα των ηλεκτρονικών επικοινωνιών βλ. και Ι. Ιγγλεζάκη, Η συγκατάθεση στο Ν. 3471/2006, σε Λ. Κοτσαλή Προσωπικά δεδομένα, Ανάλυση Σχόλια Εφαρμογή, εκδ. Νομ. Βιβλιοθήκη 2016, σελ. 106επ.
[114] Βλ. άρθρο 5 παρ. 1 στοιχ. γ του ΓΚΠΔ και άρθρο 45 παρ. 1 στοιχ. γ του Ν. 4624/2019.
[115] Βλ. Λ. Μήτρου, Η αρχή της ελαχιστοποίησης, Ο γενικός κανονισμός προστασίας προσωπικών δεδομένων, νεό δίκαιο – νέες υποχρεώσεις – νέα δικαιώματα, εκδ. Σάκκουλα 2017, σελ. 63επ.
[116] Βλ. (FRA) Οργανισμό Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων, έκδ. 2018, σελ. 160.

αιτιολογούνται σύμφωνα με το νόμο. Επεξεργασίες που αφορούν ανήλικα περιορίζονται στις εξαιρετικά αναγκαίες και λαμβάνονται κατάλληλα μέτρα προστασίας. Επίσης, εάν κατά τη αξιολόγηση δεν καταδειχθεί συγκεκριμένος λόγος αναγκαιότητας και προσφορότητας της επεξεργασίας τότε ο σκοπός της επανεξετάζεται. Ορίζονται τακτά χρονικά διαστήματα ελέγχου και επαναπροσδιορισμού των επεξεργασιών. Συστήνεται η ανωνυμοποίηση των δεδομένων όπου είναι δυνατή[117]. Συστήνεται η αποφυγή ελεύθερων πεδίων κειμένων που να μπορεί να συμπληρώσει χωρίς περιορισμούς ο χρήστης διότι έτσι αυξάνεται ο κίνδυνος καταχώρισης επιπλέον των απαιτούμενων πληροφοριών[118]. Σε συσκευές αποθήκευσης ηλεκτρονικών αρχείων συστήνεται η χρήση ασφαλούς λογισμικού προγράμματος διαγραφής των δεδομένων.

### 4.1.4. Διασφάλιση της ποιότητας των δεδομένων

Δικλίδα ασφαλείας στα μέτρα προστασίας της συμμόρφωσης αποτελεί η αρχή της ακρίβειας των δεδομένων[119], σύμφωνα με την οποία τα δεδομένα πρέπει να είναι ακριβή, δηλαδή να ανταποκρίνονται στην πραγματικότητα και όταν είναι απαραίτητο να επικαιροποιούνται, ενώ στην περίπτωση που διαπιστώνονται ανακριβή να λαμβάνονται άμεσα τα κατάλληλα μέτρα διαγραφής ή διόρθωσής τους. Η υποχρέωση αυτή βαρύνει τον υπεύθυνο επεξεργασίας, ο οποίος πρέπει να προβεί άμεσα και αυτόβουλα στις αναγκαίες διορθώσεις, ακόμη και χωρίς σχετικό αίτημα του υποκειμένου[120].

Προς διασφάλιση της ορθότητας και της ποιότητας των δεδομένων είναι ορθό να προβλέπονται τακτικά διαδικασίες ελέγχου και επικαιροποίησης των δεδομένων από το ίδιο το υποκείμενο. Ο έλεγχος αυτός βοηθά και σχετίζεται τόσο με τις πληροφορίες που ταυτοποιούν άμεσα το υποκείμενο όσο και με τις λοιπές πληροφορίες που το επηρεάζουν[121]. Για το λόγο αυτό συστήνεται επιπρόσθετα η άμεση διαγραφή ή διόρθωση των δεδομένων από τον υπεύθυνο επεξεργασίας μόλις διαπιστωθεί απόκλιση των δεδομένων από τα πραγματικά. Ακόμη, η αυτονόητη καταγραφή και

[117] Βλ. Δ. Τζέλλη. Μ. Μυλώση, Εκτίμηση Αντικτύπου στην προστασία προσωπικών δεδομένων, Εκδ. Νομική Βιβλιοθήκη, 2022, σελ. 68επ.
[118] Βλ. CNIL, Privacy Impact Assessment (PIA), Knowledge bases, 2018, σελ. 63επ.
[119] Βλ. άρθρο 5 παρ. 1 στοιχ. δ του ΓΚΠΔ και άρθρο 45 παρ. 1 στοιχ. ε, άρθρα 70-73 του Ν. 4624/2019.
[120] Βλ. Ι. Ιγγλεζάκη, Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων, Εκδ. 2η, Intractive Books, 2018, σελ. 66.
[121] Βλ. Δ. Τζέλλη. Μ. Μυλώση, Εκτίμηση Αντικτύπου στην προστασία προσωπικών δεδομένων, Εκδ. Νομική Βιβλιοθήκη, 2022, σελ. 73 επ.

κατηγοριοποίηση των δεδομένων πάντα, όπως έχει προαναφερθεί, βοηθά τη λήψη μέτρων ασφάλειας και ελέγχου των δεδομένων, πολύ δε περισσότερο για τα δεδομένα ειδικών κατηγοριών.

### 4.1.5. Προσδιορισμός του χρόνου τήρησης των δεδομένων

Σε απόλυτη συνάρτηση με τις προηγούμενες αρχές και τα μέτρα προστασίας των προσωπικών δεδομένων είναι και η αρχή του περιορισμού της περιόδου αποθήκευσης[122] κατά την οποία τα δεδομένα επιτρέπεται να διατηρούνται στη μορφή που μπορούν να ταυτοποιούν τα υποκείμενα, μόνο για το χρονικό διάστημα που απαιτείται για το σκοπό της επεξεργασίας, ενώ για το μετέπειτα διάστημα και μόνο για τους σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς θα πρέπει να τηρούνται κατάλληλα τεχνικά και οργανωτικά μέτρα. Αυτό σημαίνει ότι ο υπεύθυνος επεξεργασίας οφείλει να ορίζει προθεσμίες τήρησής τους, να προβλέπει διαδικασίες διαγραφής και να επιβλέπει την εφαρμογή τους με τακτικούς ελέγχους υπ' ευθύνη του. Νόμιμη διατήρηση των δεδομένων πέραν του οριζόμενου χρόνου και σκοπού δεν επιτρέπεται παρά μόνο μετά από ανωνυμοποίησή τους.

Τα επιτρεπόμενα χρονικά διαστήματα τήρησης των δεδομένων προβλέπονται από σχετικές διατάξεις νόμων ανάλογα με την κατηγορία τους, δηλαδή διαφορετικοί χρόνοι ορίζονται για φορολογικούς και ασφαλιστικούς φορείς, διαφορετικοί για τραπεζικά ιδρύματα, για νοσηλευτικά θεραπευτήρια, ηλεκτρονικές επικοινωνίες, βιογραφικά πρόσληψης κ.α.[123]

Σε συμμόρφωση με την παραπάνω αρχή ο υπεύθυνος επεξεργασίας προσδιορίζει για κάθε κατηγορία δεδομένων που συλλέγει, περιορισμένο και συγκεκριμένο χρόνο τήρησής τους ανάλογα με το σκοπό και τις νομικές απαιτήσεις της επεξεργασίας. Ο οριζόμενος αυτός χρόνος καταγράφεται στα αρχεία της συμμόρφωσης του οργανισμού ή της επιχείρησής του και στις διαδικασίες του και είναι υπεύθυνος για την εφαρμογή των διαδικασιών και τη διαγραφή τους. Ο υπεύθυνος επεξεργασίας διασφαλίζει ότι τα τεχνικά μέτρα που προβλέπονται στις διαδικασίες είναι

[122] Βλ. άρθρο 5 παρ. 1 στοιχ. ε του ΓΚΠΔ και άρθρο 45 παρ. 1 στοιχ. ε, άρθρο 73 του Ν. 4624/2019.
[123] Βλ. καταγραφή στο Παράρτημα 7, Κατηγορίες και χρόνοι διατήρησης δεδομένων, Λ. Κανέλλο, The GDPR Handbook, Εκδ. Νομική Βιβλιοθήκη, 2020, σελ. 492 επ.

σε θέση να εφαρμοστούν και στην πράξη και να μην παρουσιάζεται μόνο κατά πλάσμα, δηλαδή να δείχνει ότι έχει διαγραφεί αλλά στην πραγματικότητα να βρίσκεται ακόμη αποθηκευμένο στη βάση δεδομένων[124]. Αυτοματοποιημένες σχετικές λειτουργίες όταν εφαρμόζονται ορθά βοηθάνε[125].

### 4.1.6. Περιπτωσιολογία και Νομολογιακή Επισκόπηση

Μια Κοινωφελής Δημοτική Επιχείρηση ενός Δήμου προβαίνει σε επεξεργασία πλήθους δεδομένων προσωπικού χαρακτήρα των υπαλλήλων του, των πολιτών-δημοτών και ανηλίκων, των προμηθευτών του, ευπαθών ομάδων κ.α. για δραστηριότητες όπως η τήρηση φακέλων προγράμματος «βοήθεια στο σπίτι», τήρηση βιβλίου μητρώου ωφελούμενων, τήρηση παρεχόμενων υπηρεσιών και τήρηση αρχείου αστέγων, τήρηση μητρώου βρεφονηπιακού σταθμού, τήρηση ατομικών φακέλων για φιλοξενούμενα παιδιά, η τήρηση μητρώου μελών παιδικού σταθμού, η μισθοδοσία, η καταχώριση και εξόφληση τιμολογίων προμηθευτών κ.α. Οι πληροφορίες που αφορούν τα προγράμματα κοινωνικής μέριμνας είναι ασφαλώς ευαίσθητα προσωπικά δεδομένα, η επεξεργασία των οποίων για να είναι σύννομη θα πρέπει να στηρίζεται στη διάταξη του άρθρου 9 παρ. 2 β΄ ΓΚΠΔ. Το ίδιο ισχύει και για το τμήμα που αφορά παιδιά με αναπηρία. Η κοινωφελής επιχείρηση θα πρέπει να μπορεί να αποδεικνύει και να εφαρμόζει με τον καταλληλότερο τρόπο τα όσα προβλέπει ο Γενικός Κανονισμός. Οφείλει να αναλάβει όλες τις κατάλληλες τεχνικές, οργανωτικές, διοικητικές, νομικές ενέργειες που να αποδεικνύουν τα μέτρα προστασίας για τη συμμόρφωση, τόσο εξωτερικά όσο και εσωτερικά.

Μία ιδιαίτερα σημαντική απόφαση της ΑΠΔΠΧ είναι η 26/2019 με την οποία, μετά από καταγγελία που απευθύνθηκε ενώπιόν της, έκρινε αιτιολογημένα καίρια ζητήματα που αφορούν τη νομιμότητα των επεξεργασιών, τη συγκατάθεση και τις υποχρεώσεις του υπεύθυνου επεξεργασίας. Ειδικότερα, τέθηκαν προς την Αρχή σημαντικά ζητήματα παράνομης επεξεργασίας δεδομένων προσωπικού χαρακτήρα των εργαζομένων στην εταιρεία PRICEWATERHOUSECOOPERS από την Ένωση Λογιστών Ελεγκτών Περιφέρειας Αττικής μετά από διαπίστωσή της ότι η εν λόγω εταιρεία,

[124] Βλ. CNIL, Privacy Impact Assessment (PIA), Knowledge bases, 2018, σελ. 29επ.
[125] Βλ. Δ. Τζέλλη. Μ. Μυλώση, Εκτίμηση Αντικτύπου στην προστασία προσωπικών δεδομένων, Εκδ. Νομική Βιβλιοθήκη, 2022, σελ. 76 επ.

εκμεταλλευόμενη την σαφώς μειονεκτική θέση ισχύος των εργαζομένων ως ευάλωτα άτομα απέναντί της ως υπεύθυνο επεξεργασίας, εξανάγκαζε αυτούς έμμεσα να αποδεχτούν εγγράφως υποχρεώσεις, ευθύνες και περιορισμούς στους όρους επεξεργασίας των δεδομένων που τους αφορούσαν, θέτοντας την υπογραφή τους σε σχετικά έντυπα, να παρέχουν τη ρητή συναίνεσή τους στη χρήση προσωπικών τους στοιχείων, ακόμη και μελλοντικά συλλεχθέντων, στις βάσεις δεδομένων της εταιρείας, χωρίς ύπαρξη νομίμου λόγου, καθώς επίσης να παρέχουν εν λευκώ τη συγκατάθεσή τους σε περαιτέρω κοινοποίηση των προσωπικών δεδομένων των εργαζομένων σε τρίτους προς εξυπηρέτηση των δικών της επιχειρηματικών συμφερόντων. Στο σκεπτικό της η υπό κρίση διατυπώνει ξεκάθαρα ότι για να είναι νόμιμα τα προσωπικά δεδομένα[126], θα πρέπει να διασφαλίζεται η σωρευτική εφαρμογή και τήρηση των αρχών του άρθρου 5 παρ. 1 ΓΚΠΔ. Η θεμελίωση μιας επεξεργασίας σε μία από τις νομικές βάσεις του Κανονισμού δεν απαλλάσσει τον υπεύθυνο επεξεργασίας από την υποχρέωσή του να τηρεί και εφαρμόζει τις αρχές της αναγκαιότητας, αναλογικότητας και ελαχιστοποίησης. Με σαφήνεια η ΑΠΔΠΧ διατυπώνει ότι η ύπαρξη μιας νόμιμης βάσης δεν δύναται να θεραπεύσει παραβιάσεις των αρχών και ως εκ τούτου σε τέτοια περίπτωση η επεξεργασία είναι παράνομη και παρέλκει η εξέταση τυχόν προϋποθέσεων ύπαρξης άλλων νόμιμων βάσεων. Συμπληρωματικά σημειώνεται ότι προϋπόθεση της θεμιτής και νόμιμης επεξεργασίας αποτελεί η προηγούμενη ενημέρωση του υποκειμένου των δεδομένων πριν από την επεξεργασία των προσωπικών του δεδομένων.

Η ενημέρωση αυτή οφείλει να γίνεται με τρόπο διαφανή και νόμιμο κατ' εφαρμογή της αρχής της λογοδοσίας. Ο υπεύθυνος επεξεργασίας είναι υποχρεωμένος πριν τη συλλογή και επεξεργασία των δεδομένων προσωπικού χαρακτήρα να αποκαλύπτει στο υποκείμενο όλες τις αναγκαίες πληροφορίες. Κατά την σκέψη της ΑΠΔΠΧ[127] αυτό ισχύει διότι η υποχρέωση για ενημέρωση τελεί σε άμεση σχέση τόσο κατ' αρχήν με την αρχή της θεμιτής και δίκαιης επεξεργασίας, όπως και του περιορισμού του σκοπού και κατ' επέκταση με την ορθή επιλογή του νόμιμου θεμελίου της επεξεργασίας, όσο και με τα ίδια τα δικαιώματα των υποκειμένων που δύνανται να έχουν εφαρμογή σε κάθε περίπτωση. Στη σκέψη αυτή μάλιστα η Αρχή εισχωρεί και σε

[126] Βλ. ΑΠΔΠΧ Απόφαση 26/2019, Σκέψη 5, https://www.dpa.gr/sites/default/files/2020-05/26_2019anonym.pdf.
[127] Ομοίως Σκέψη 6.

βαθύτερη ανάλυση αναδύοντας τα ζητήματα της δίκαιης και διαφανούς επεξεργασίας και από την ηθική τους πλευρά, θέτοντας επί της ουσίας τον υπεύθυνο επεξεργασίας υπεύθυνο και υπόλογο στην σχέση εμπιστοσύνης που αναπόφευκτα δημιουργείται μεταξύ αυτού και του υποκειμένου από την αρχή της σχέσης τους και η οποία οφείλει ο υπεύθυνος επεξεργασίας να φροντίσει, με κατάλληλες ενέργειες, να μη διαρραγεί ακόμη και μετέπειτα, καθ' όλη τη διάρκεια της όποιας επεξεργασίας προσωπικών δεδομένων του υποκειμένου, όχι μόνο για λόγους νομιμότητας αλλά εξίσου και για λόγους ηθικής τάξης.

Στο πλαίσιο των εργασιακών σχέσεων, η ΑΠΔΠΧ επισημαίνει[128] ότι η επεξεργασία των δεδομένων δικαιολογούνται μόνο για σκοπούς που απορρέουν από τη σύμβαση εργασίας και τις αναγκαίες από αυτή εκ του νόμου υποχρεώσεις. Τυχόν επεξεργασία δεδομένων εργαζομένου που πραγματοποιείται καθ' υπέρβαση του αρχικού σκοπού της καθίσταται μη νόμιμη ακόμη κι αν ο εργαζόμενος έχει συγκατατεθεί σε αυτή, διότι είναι αυταπόδεικτη η ανισότητα της σχέσης εργοδότη-εργαζομένου δεδομένου ότι ο εργαζόμενος δεν μπορεί να θεωρηθεί ότι παρέχει τη συγκατάθεσή του ελεύθερα, αλλά αντίθετα εξαναγκαστικά, καθώς εξαρτάται η πρόσληψή του και η εξέλιξη της εργασιακής του σχέσης από τις αποφάσεις και ενέργειες του εργοδότη του. Περαιτέρω, η ΑΠΔΠΧ αποδοκιμάζει την τακτική του υπεύθυνου επεξεργασίας να μεταθέτει την ευθύνη της επεξεργασίας στο πρόσωπο του εργαζομένου μέσω τάχα της παροχής συγκατάθεσης που στην πραγματικότητα είναι εξαναγκαστική ενώ η υποχρέωση της συμμόρφωσης βαρύνει αποκλειστικά τον υπεύθυνο επεξεργασίας. Σε κάθε περίπτωση, εάν υπάρχουν αμφιβολίες ως προς τη νομιμότητα μιας επεξεργασίας ο υπεύθυνος επεξεργασίας οφείλει να απέχει από αυτή μέχρι την άρση των αμφιβολιών.

## 4.2 Αξιολόγηση των μέτρων που διασφαλίζουν την ικανοποίηση των δικαιωμάτων των Υποκειμένων των δεδομένων

Κατά το επόμενο βήμα της μελέτης έμφαση δίνεται στην αναγνώριση και στον καθορισμό των μέτρων που προβλέπεται να εφαρμοστούν και να διασφαλίσουν ότι τα υποκείμενα των δεδομένων μπορούν να ασκήσουν τα νόμιμα δικαιώματά τους.

[128] Σκέψη 9,10,18.

Ακολουθώντας το πνεύμα του ΓΚΠΚ που εμφανέστατα στόχο είχε την ενδυνάμωση των δικαιωμάτων των υποκειμένων, είναι σημαντικό να προσδιοριστούν και περιγραφούν τα τυχόν ήδη υπάρχοντα ή μελλοντικά μέτρα - τεχνικά, οργανωτικά ή διαδικασίες – που είναι απαραίτητα για την ικανοποίηση των νομικών απαιτήσεων[129] και τη διαχείριση των κινδύνων της ιδιωτικότητας, κατ΄εφαρμογή πάντα της αρχής της αναλογικότητας.

### 4.2.1. Καταγραφή των μέτρων για ενημέρωση των Υποκειμένων των δεδομένων

Η συμμόρφωση απαιτεί πρώτιστα να μπορεί να τεκμηριωθεί ότι το υποκείμενο των δεδομένων έχει στη διάθεσή του όλες τις πληροφορίες για την πράξη της επεξεργασίας και τους σκοπούς της, σύμφωνα με την αρχή της διαφάνειας[130]. Με τον τρόπο αυτό διασφαλίζεται η γνώση του υποκειμένου για τη συλλογή των δεδομένων του και του τρόπου που αυτά θα χρησιμοποιηθούν και αποφεύγεται η εν αγνοία του χρήση τους.

Το υποκείμενο έχει δικαίωμα να γνωρίζει και ο υπεύθυνος επεξεργασίας υποχρέωση να παράσχει πληροφορίες, με απλό και σαφή τρόπο, που αφορούν τα πλήρη στοιχεία ταυτότητας και επικοινωνίας του, το νόμιμο λόγο συλλογής των δεδομένων του, το χρόνο διατήρησής τους και τους αποδέκτες τους. Ο χρόνος της ενημέρωσης διαφέρει ανάλογα με το εάν η συλλογή γίνεται απευθείας από το υποκείμενο ή εάν γίνεται από τρίτο πρόσωπο. Επιτακτικότερη βέβαια κρίνεται η ανάγκη ενημέρωσης όταν τα υποκείμενα είναι παιδιά[131]. Εξαιρέσεις από το δικαίωμα της πληροφόρησης -που θα πρέπει να αιτιολογούνται ειδικά- προβλέπονται όταν το υποκείμενο έχει ήδη τις πληροφορίες, όταν η πληροφόρηση είναι αδύνατη, όταν τα δεδομένα πρέπει να παραμείνουν εμπιστευτικά ή όταν η συλλογή πραγματοποιείται για δημοσιογραφικούς σκοπούς και αφορά δημόσια πρόσωπα[132].

---

[129] Βλ. άρθρα 12-22 ΓΚΠΔ, Αιτιολ. σκέψεις αρ. 58 - 71, καθώς και άρθρα 31-35 του Ν. 4624/2019.

[130] Βλ. CNIL, Privacy Impact Assessment (PIA) Methology, 2018, σελ. 5 και Ομάδα εργασίας του άρθρου 29, Κατευθυντήριες γραμμές σχετικά με τη διαφάνεια βάσει του κανονισμού 2016/679, https://ec.europa.eu/newsroom/article29/items/622227/en .

[131] Βλ. Φ. Παναγοπούλου - Κουτνατζή, Το νέο πλαίσιο των ανανεωμένων δικαιωμάτων, Προστασία των δικαιωμάτων των παιδιών, σε Λ. Κοτσαλή– Κ. Μενουδάκο, Γενικός Κανονισμός για την προστασία των προσωπικών δεδομένων, Νομική διάσταση και πρακτική εφαρμογή, εκδ. Νομ. Βιβλιοθήκη 2021, σελ. 9επ.

[132] Βλ. Ι. Ιγγλεζάκη, Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων, 2018, σελ. 97, Ε. Αλεξανδροπούλου-Αιγυπτιάδου, Προσωπικά δεδομένα, εκδ. Νομ. Βιβλιοθήκη 2016, σελ. 133επ.

Ως πρακτικά μέτρα για το δικαίωμα των υποκειμένων στην πληροφόρηση συστήνονται η δημοσίευση των όρων χρήσης και εμπιστευτικότητας, η χρήση εύκολων και κατανοητών όρων, η πρόβλεψη εξατομικευμένων ρητρών ανάλογα με το είδος της συσκευής, η γνωστοποίηση στον χρήστη των δικαιωμάτων του και του τρόπου που μπορεί να τα ασκήσει, η ενημέρωση του χρήστη εάν μία εφαρμογή έχει πρόσβαση στα αναγνωριστικά στοιχεία της όποιας συσκευής του (tablet, pc, smartphone), σημειώνοντας εάν αυτά γνωστοποιούνται σε τρίτους, ο προσδιορισμός της μεθόδου ασφαλούς αποθήκευσης δεδομένων, ιδίως σε περίπτωση εξωτερικής ανάθεσης[133]. Προτεινόμενες ενέργειες επίσης είναι σε περίπτωση επιχείρησης η ενσωμάτωση της πολιτικής προστασίας προσωπικών δεδομένων και στον Κανονισμό Εργασίας που εφαρμόζει ή στην περίπτωση συλλογής πληροφοριών μέσω ιστοσελίδας η ανάρτηση κατάλληλης ενημέρωσης στην αρχική σελίδα του υπεύθυνου επεξεργασίας με όλες τις πληροφορίες για την προστασία των προσωπικών δεδομένων και της ιδιωτικότητας, καθώς επίσης, σε περιπτώσεις αυτοματοποιημένης λήψης αποφάσεων ή κατάρτισης προφίλ, ο σχεδιασμός προηγούμενης ενημέρωσης των υποκειμένων με όλες τις απαιτούμενες από το νόμο πληροφορίες[134].

Με κάθε τρόπο ο υπεύθυνος επεξεργασίας οφείλει να διασφαλίσει τη δίκαιη και διαφανή επεξεργασία των δεδομένων του υποκειμένου με το να αξιολογεί τα μέτρα για πληροφόρηση που λαμβάνει κατά περίπτωση και παράλληλα να είναι σε θέση να αποδείξει ότι σέβεται το δικαίωμα του υποκειμένου για ενημέρωση.

### 4.2.2. Καταγραφή των μέτρων για τη λήψη συγκατάθεσης

Η εξέταση του ορθού τρόπου λήψη συγκατάθεσης και η καταγραφή αυτού στη μελέτη αποτελεί σημαντικό στοιχείο της συμμόρφωσης δεδομένου ότι η συναίνεση αποτελεί ταυτόχρονα αυτοτελή βάση νομιμότητας της επεξεργασίας. Έχει ιδιαίτερη σημασία κατ' αρχήν να αποκλειστούν της εφαρμογής τους οι λοιπές νομικές βάσεις των άρθρων 6 και 9 του ΓΚΠΔ και στη συνέχεια να διασφαλιστεί ότι η λήψη της συγκατάθεσης έγινε ρητά και με ελεύθερη ενέργεια ή δήλωση του υποκειμένου πριν τη συλλογή ή τη γνωστοποίηση των δεδομένων του σε τρίτους.

[133] Βλ. Δ. Τζέλλη. Μ. Μυλώση, σελ. 81 επ.
[134] Βλ. Ομάδα εργασίας του άρθρου 29, Κατευθυντήριες γραμμές για την αυτοματοποιημένη λήψη αποφάσεων και για την κατάρτιση προφίλ για τους σκοπούς του κανονισμού 2016/679, https://ec.europa.eu/newsroom/article29/items/612053/en .

Σύμφωνα με τις επισημάνσεις της Γαλλικής Αρχής[135] ορθά μέτρα αποτελούν μεταξύ άλλων ο διαχωρισμός της συγκατάθεσης ανάλογα με τον τύπο των δεδομένων και της επεξεργασίας, η παροχή της συγκατάθεσης σε απλό, κατανοητό περιεχόμενο και εύκολα προσβάσιμη μορφή, προσαρμοσμένη στον αναγνώστη και το σκοπό της επεξεργασίας, σε περίπτωση παρόδου μεγάλου χρονικού διαστήματος από την αρχική συναίνεση χωρίς χρήση να ζητηθεί εκ νέου συναίνεση όταν ο χρήστης επανέλθει, σε περίπτωση συγκατάθεσης ειδικών δεδομένων, όπως η γεωγραφική θέση, να είναι ξεκάθαρο στον χρήστη ότι η διεπαφή (π.χ. εμφάνιση εικονιδίου ή ενδεικτικής λυχνίας) σημαίνει πως εκείνη τη στιγμή πραγματοποιείται επεξεργασία των δεδομένων του, καθώς επίσης να διασφαλίζεται η διατήρηση των όρων στους οποίους έχει συγκατατεθεί ο χρήστης ακόμη και μετά από αλλαγή της συσκευής του (π.χ. κινητού, tablet, pc) και επανεγκατάστασης της εφαρμογής.

Εξίσου σημαντικό είναι να διασφαλίζεται, μετά από ενημέρωση, η δυνατότητα ανάκλησης της συγκατάθεσης χωρίς βλάβη του υποκειμένου και βέβαια ο υπεύθυνος επεξεργασίας να τηρεί αρχείο λήψης των δηλώσεων συγκατάθεσης ώστε να είναι σε θέση ανά πάσα στιγμή να αποδείξει την παροχή της κατά την αρχή της λογοδοσίας[136].

### 4.2.3. Καταγραφή των μέτρων για τα δικαιώματα πρόσβασης και φορητότητας

Επιπρόσθετα, σύμφωνα με τους σκοπούς του Κανονισμού, ο υπεύθυνος επεξεργασίας οφείλει να διασφαλίσει την εφαρμογή του δικαιώματος πρόσβασης του υποκειμένου στα δικαιώματά του, δηλαδή το δικαίωμά του να λαμβάνει, έπειτα από αίτημά του, επαρκείς πληροφορίες και επιβεβαίωση για τα δεδομένα προσωπικού χαρακτήρα που το αφορούν και υφίστανται ή όχι επεξεργασία.

Ενόψει αυτών έχει ιδιαίτερη σημασία να αναγνωριστούν και καθοριστούν μέτρα και διαδικασίες που να εξασφαλίζουν ότι το υποκείμενο μπορεί να ασκήσει το εν λόγω δικαίωμα και να λάβει πλήρη απάντηση με ενδελεχή πληροφόρηση. Απαραίτητο είναι να επαληθεύεται με βεβαιότητα η ταυτότητα του ατόμου που υποβάλλει το αίτημα. Μέτρα που προτείνονται σχετικά[137] είναι η ύπαρξη δυνατότητας πρόσβασης και

[135] Βλ. CNIL, Privacy Impact Assessment (PIA) Templates, 2018, σελ. 6.
[136]Βλ. Ομάδα εργασίας του άρθρου 29, Κατευθυντήριες γραμμές για τη συγκατάθεση σύμφωνα με τον Κανονισμό 2016/679, https://ec.europa.eu/newsroom/article29/items/623051/en
[137] Βλ. CNIL, Privacy Impact Assessment (PIA) Templates, 2018, σελ. 7.

μάλιστα εύκολης, χωρίς ταλαιπωρία και κόστος για τον αιτούντα, σε όλα τα προσωπικά του δεδομένα μέσω των συνηθισμένων καθημερινών διεπαφών, η δυνατότητα ελέγχου με απόλυτη ασφάλεια στα ίχνη χρήσης που αφορούν τον χρήστη, καθώς και η εν τοις πράγμασι φροντίδα ώστε να είναι δυνατή η λήψη ηλεκτρονικά του απαντητικού αρχείου προς τον αιτούντα. Την ίδια συλλογιστική ακολουθούν και οι Κατευθυντήριες Γραμμές του ΕΣΠΔ[138] στο πλαίσιο στόχευσης χρηστών μέσω κοινωνικής δικτύωσης, επισημαίνοντας ότι οι υπεύθυνοι επεξεργασίας (πχ. πάροχοι μέσων κοινωνικής δικτύωσης, διαφημιστές) οφείλουν να διασφαλίσουν τη λειτουργία κατάλληλου μηχανισμού που να επιτρέπει στα υποκείμενα να ελέγχουν το προφίλ τους και τις πληροφορίες που περιλαμβάνονται σε αυτό.

Περαιτέρω, για την άσκηση του δικαιώματος στη φορητότητα, κρίσιμο είναι σε περιπτώσεις επεξεργασίας με αυτοματοποιημένα μέσα, να υπάρχουν προβλεπόμενες διαδικασίες και μέτρα που να διασφαλίζουν το δικαίωμα του υποκειμένου να λαμβάνει από τον υπεύθυνο επεξεργασίας τα προσωπικά δεδομένα που το αφορούν σε δομημένο, κοινά χρησιμοποιούμενο διαλειτουργικό μορφότυπο. Αυτό σημαίνει ότι ο υπεύθυνος επεξεργασίας θα πρέπει να καταστήσει τεχνικά εφικτή τη δυνατότητα να ανακτήσει το υποκείμενο σε δομημένο και αναγνωρίσιμο από τα μηχανήματα μορφότυπο με τρόπο που να μπορεί να τα μεταφέρει σε άλλη υπηρεσία ή πάροχο και σε κάθε περίπτωση σε άλλο υπεύθυνο επεξεργασίας. Συστήνεται σχετικά[139] η καθιέρωση μιας διαδικασίας ενημέρωσης του υποκειμένου αναφορικά με την κατάσταση της αίτησής του και την εξέλιξη αυτής, καθώς επίσης, σε περιπτώσεις που εντοπίζονται πρακτικές δυσκολίες άσκησης του δικαιώματος να προβλέπονται εφεδρικές λύσεις.

### 4.2.4. Καταγραφή των μέτρων για τα δικαιώματα διόρθωσης και διαγραφής

Επίσης εξετάζεται στο πλαίσιο της συμμόρφωσης η κατοχύρωση του δικαιώματος διόρθωσης και του δικαιώματος διαγραφής. Το μεν πρώτο συνίσταται στη δυνατότητα του υποκειμένου να ζητήσει από τον υπεύθυνο επεξεργασίας την

[138]Βλ. ΕΣΠΔ Κατευθυντήριες Γραμμές 8/2020 σχετικά με τη στόχευση χρηστών μέσων κοινωνικής δικτύωσης, https://edpb.europa.eu/system/files/2021-11/edpb_guidelines_082020_on_the_targeting_of_social_media_users_el_0.pdf

[139] Βλ. Δ. Τζέλλη. Μ. Μυλώση, σελ. 93 επ.

διόρθωση ανακριβών ή εσφαλμένων προσωπικών του στοιχείων από τα αρχεία του ή τη συμπλήρωση στοιχείων που εκλείπουν, κατ' εφαρμογή της αρχής της ακρίβειας, το δε δεύτερο στη δυνατότητα του υποκειμένου να αιτηθεί τη διαγραφή προσωπικών του στοιχείων χωρίς αδικαιολόγητη καθυστέρηση και δίχως επιπρόσθετες αιτιολογήσεις. Υπάρχουν ωστόσο και περιπτώσεις που τα δικαιώματα αυτά περιορίζονται[140].

Κατά συνέπεια, ιδιαίτερη σημασία έχει να διασφαλιστεί η δυνατότητα ύπαρξης και εφαρμογής αντίστοιχων πρακτικών μέσων και διαδικασιών διόρθωσης και διαγραφής προσωπικών δεδομένων με εύκολες και απλές διαδικασίες για το υποκείμενο και χωρίς βέβαια κάποιο κόστος ή αρνητική συνέπεια για εκείνο. Καλή πρακτική αποτελεί η καθιέρωση μιας διαδικασίας ενημέρωσης του υποκειμένου εκ των προτέρων, η διαβεβαίωση ότι έχει επαληθευτεί με έγκυρα μέσα (πχ. επίδειξη δελτίου ταυτότητας ή προσκόμιση αντιγράφου) η ταυτότητα του προσώπου που είναι και ο αιτών, καθώς και η επιβεβαίωση εκ των υστέρων ότι πράγματι έχει συντελεστεί η πράξη της διόρθωσης ή διαγραφής[141]. Παράλληλα, συστήνεται η υπόδειξη του είδους των δεδομένων που υποχρεωτικά θα αποθηκεύονται για λόγους που το επιβάλουν, όπως τεχνικές απαιτήσεις ή επιταγές νομικών διατάξεων και ο σχεδιασμός ειδικών διαδικασιών για την άσκηση του δικαιώματος διαγραφής στα ανήλικα[142]. Προτείνεται ακόμη, να προβλέπονται ξεκάθαρες οδηγίες και απλά βήματα για τη διαγραφή δεδομένων σε περιπτώσεις όπως πριν την καταστροφή μιας συσκευής, να δίνονται σαφείς συμβουλές για επαναφορά των ρυθμίσεων μιας συσκευής πριν την πώλησή της, όπως επίσης και η πρόβλεψη δυνατότητας απομακρυσμένης διαγραφής των δεδομένων σε περίπτωση κλοπής της συσκευής.

### 4.2.5. Καταγραφή των μέτρων για τα δικαιώματα περιορισμού της επεξεργασίας και εναντίωσης

Ένα ακόμη δικαίωμα που έχει το υποκείμενο στο οπλοστάσιό του είναι να μπορεί να ζητήσει από τον υπεύθυνο επεξεργασίας τον περιορισμό της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα που το αφορούν, σε περιπτώσεις που αμφισβητείται η ακρίβειά τους ή η επεξεργασία είναι παράνομη ή οι πληροφορίες για

[140] Βλ. άρθρα 29 παρ. 3, 30 παρ. 2, 34 του Ν. 4624/2019, άρθρο 17 παρ. 3 ΓΚΠΔ.
[141] Βλ. Δ. Τζέλλη. Μ. Μυλώση, σελ. 103 επ.
[142] Βλ. CNIL, Privacy Impact Assessment (PIA) Templates, 2018, σελ. 10.

το υποκείμενο δεν είναι πλέον απαραίτητες στον υπεύθυνο επεξεργασίας για τους σκοπούς της επεξεργασίας αλλά πρέπει να διατηρηθούν για την άσκηση ή την υποστήριξη νομικών αξιώσεων ή το υποκείμενο έχει αντιρρήσεις ως προς την επεξεργασία τους[143]. Πρόκειται για ένα δικαίωμα που στην ουσία παρέχει προσωρινή προστασία στο υποκείμενο εωσότου εξεταστεί και διελευκανθεί η νομιμότητα της υπό κρίση επεξεργασίας[144].

Ο περιορισμός της επεξεργασίας μπορεί να γίνει με διάφορες διεργασίες, όπως παροδική μεταφορά συγκεκριμένων δεδομένων σε διαφορετικό σύστημα επεξεργασίας, απαγόρευση πρόσβασης στα δεδομένα από τρίτους χρήστες ή προσωρινή απόσυρση προσωπικών πληροφοριών[145].

Εξίσου σημαντικό όπλο για την προστασία του υποκειμένου αποτελεί το δικαίωμά του να εναντιωθεί οποτεδήποτε ζητήσει στην επεξεργασία των δεδομένων του από τον υπεύθυνο επεξεργασίας για σκοπούς κατάρτισης προφίλ ή απευθείας εμπορικής προώθησης[146].

Συνεπώς, για την προστασία των προαναφερόμενων δικαιωμάτων των φυσικών προσώπων έχει μεγάλη σημασία να περιγραφούν και καθοριστούν ειδικά μέτρα και μέθοδοι. Κατ' αρχήν, ο υπεύθυνος επεξεργασίας είναι υποχρεωμένος να ενημερώνει, επί ποινή κυρώσεων, κάθε αποδέκτη των δεδομένων για την άσκηση των δικαιωμάτων διόρθωσης, διαγραφής και περιορισμού, καθώς επίσης και να παράσχει στο υποκείμενο κάθε πληροφορία σχετική με αυτούς, εφόσον ζητηθεί[147]. Καλές πρακτικές αποτελούν η ύπαρξη σχετικών πολιτικών που να προβλέπουν τον τρόπο αντιμετώπισης τέτοιων αιτημάτων, η ουσιαστική διασφάλιση από τον υπεύθυνο επεξεργασίας της μετέπειτα απαγόρευσης των επίμαχων δεδομένων, η παροχή δυνατότητας στον χρήστη για επανεξέταση και αλλαγή των εξ ορισμού ρυθμίσεων, η ενσωμάτωση μηχανισμών γονικού ελέγχου για περιπτώσεις επεξεργασιών από ανήλικα, ο αποκλεισμός δημιουργίας αυτόματου προφίλ για παιδιά κάτω των 15 ετών. Επίσης, σε περιπτώσεις εναντίωσης με αυτοματοποιημένα μέσα, όπως επεξεργασία για σκοπούς υπηρεσιών

[143] Βλ. άρθρο 18 ΓΚΠΔ.
[144] Βλ. Φ. Παναγοπούλου - Κουτνατζή, Το νέο πλαίσιο των ανανεωμένων δικαιωμάτων, Δικαίωμα περιορισμού της επεξεργασίας, σε Λ. Κοτσαλή – Κ. Μενουδάκο, Γενικός Κανονισμός για την προστασία των προσωπικών δεδομένων, Νομική διάσταση και πρακτική εφαρμογή, εκδ. Νομ. Βιβλιοθήκη 2021, σελ. 33.
[145] Βλ. (FRA) Οργανισμό Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων, έκδ. 2018, σελ. 285.
[146]Βλ. άρθρο 18 ΓΚΠΔ.
[147] Βλ. Λ. Κανέλλο, The GDPR Handbook, Εκδ. Νομική Βιβλιοθήκη, 2020, σελ. 154.

της κοινωνίας των πληροφοριών[148], οι υπεύθυνοι επεξεργασίας οφείλουν να εφαρμόζουν τις κατάλληλες τεχνικές ρυθμίσεις και διαδικασίες ώστε μετά την άσκηση του δικαιώματος εναντίωσης να επιβάλλεται φραγή των cookies στις ιστοσελίδες ή απενεργοποίηση του εντοπισμού της πλοήγησης στο διαδίκτυο[149].

### 4.2.6. Καταγραφή των μέτρων για τους Εκτελούντες την επεξεργασία

Όπως είναι γνωστό, ο εκτελών την επεξεργασία επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπεύθυνου επεξεργασίας και έχει ανεξάρτητο διακριτό ρόλο ως οντότητα σε σχέση με τον τελευταίο (φυσικό ή νομικό πρόσωπο, δημόσια αρχή, επιχείρηση, οργανισμός ή φορέας). Ουσιαστική παράμετρο στη σχέση τους αποτελεί η μεταξύ τους συμφωνία για τη ρύθμιση των εκατέρωθεν ρόλων και υποχρεώσεων. Για το λόγο αυτό, η συμφωνία τους επιβάλλεται να είναι έγγραφη και λεπτομερής, τουλάχιστο σύμφωνα με το περιεχόμενο που υπαγορεύει η διάταξη του άρθρου 28 του ΓΚΠΔ[150]. Η μη κατάρτιση τέτοιας σύμβασης αποτελεί παράβαση της αρχής της λογοδοσίας και μπορεί να επιφέρει κυρώσεις.

Συνεπώς, πρώτιστο μέλημα για τον προσδιορισμό των μέτρων που αφορούν στους εκτελούντες την επεξεργασία αποτελεί η υπογραφή έγγραφης σύμβασης εκτέλεσης της επεξεργασίας με κάθε έναν ξεχωριστά, που να καθορίζει με ακρίβεια το πεδίο εφαρμογής και τη διάρκεια της σύμβασης, τις δραστηριότητες που αναλαμβάνει και για ποιο σκοπό, τις πληροφορίες στις οποίες θα έχει πρόσβαση, το χρονικό διάστημα αποθήκευσής τους και τους αποδέκτες στους οποίους θα διαβιβαστούν[151]. Επίσης, είναι απαραίτητο να προβλέπεται ρητά η δέσμευση του εκτελούντος την επεξεργασία για προηγούμενη ρητή έγκριση του υπεύθυνου επεξεργασίας σε περίπτωση που επιθυμεί να προσλάβει άλλον εκτελούντα την επεξεργασία προς αντικατάσταση του υπάρχοντος, καθώς επίσης και σε περίπτωση υπεργολαβίας. Ακόμη, τεκμήριο συμμόρφωσης αποτελεί αναμφισβήτητα η λήψη και συγκέντρωση

[148] Περισσότερα για γονικό έλεγχο πρόσβασης παιδιών σε ψηφιακές υπηρεσίες, διασυνδεδεμένα παιχνίδια, παροχή υπηρεσιών σε παιδικό κοινό, βλ. σε Λ. Κανέλλο, The GDPR Handbook, Εκδ. Νομική Βιβλιοθήκη, 2020, σελ. 257επ.
[149] Βλ. CNIL, Privacy Impact Assessment (PIA) Templates, 2018, σελ. 11 και (FRA) Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων, έκδ. 2018, σελ. 290.
[150] Αντικείμενο και διάρκεια της επεξεργασίας, τη φύση και το σκοπό της, το είδος των δεδομένων, τις κατηγορίες των υποκειμένων των δεδομένων και τις υποχρεώσεις και δικαιώματα του υπεύθυνου επεξεργασίας.
[151] Κ. Κόμνιος, GDPR: Η σύμβαση με τον εκτελούντα την επεξεργασία, https://www.capital.gr/me-apopsi/3288247/gdpr-i-sumbasi-me-ton-ektelounta-tin-epexergasia#0

οποιουδήποτε στοιχείου του εκτελούντος την επεξεργασία που μπορεί να αποδεικνύει τη δική του συμμόρφωση ως ξεχωριστή νομική οντότητα, όπως για παράδειγμα η πολιτική που εφαρμόζει στην ασφάλεια των πληροφοριακών του συστημάτων, τις αντίστοιχες πιστοποιήσεις του και βεβαιώσεις συμμόρφωσης, τα οποία με τη σειρά τους μπορούν να αποτελούν αναπόσπαστα παραρτήματα της σύμβασης προς τεκμηρίωση των μέτρων που λαμβάνονται από τον υπεύθυνο επεξεργασίας[152]. Εξίσου απόδειξη της συμμόρφωσης αποτελεί η προσχώρηση του εκτελούντος την επεξεργασία σε συγκεκριμένο κώδικα δεοντολογίας ή εγκεκριμένο μηχανισμό πιστοποίησης[153]. Επί της ουσίας ο υπεύθυνος επεξεργασίας πρέπει να ελέγχει ότι επιλέγει για εκτελούντες την επεξεργασία εταιρείες, επιχειρήσεις ή οργανισμούς που να παρέχουν επαρκείς διαβεβαιώσεις για την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων.

### 4.2.7. Καταγραφή των μέτρων για διαβιβάσεις προσωπικών δεδομένων εκτός Ευρωπαϊκής Ένωσης

Στην περίπτωση που λαμβάνουν χώρα διασυνοριακές διαβιβάσεις δεδομένων προσωπικού χαρακτήρα είναι υποχρεωτικό να διερευνηθεί και να εντοπιστεί εάν χρησιμοποιείται κάποιος έγκυρος μηχανισμός διαβίβασης από αυτούς που προβλέπονται στις διατάξεις των άρθρων 44-50 του ΓΚΠΔ. Αρχικά, είναι καλό να καταγραφεί η γεωγραφική θέση που βρίσκεται ο υλικός φορέας που πρόκειται να αποθηκευτούν τα δεδομένα και στη συνέχεια να αιτιολογηθεί ειδικότερα ο λόγος που οδηγεί στην απομακρυσμένη διαβίβαση. Κατόπιν, είναι σημαντικό να προσδιοριστούν οι συγκεκριμένες προϋποθέσεις που τυχόν δικαιολογούν τη νομιμότητα της διαβίβασης.

Κατ' αρχήν, εξετάζεται εάν υπάρχει απόφαση επάρκειας από την Ευρωπαϊκή Επιτροπή, δηλαδή εάν έχει κριθεί ότι διασφαλίζεται επαρκές επίπεδο προστασίας από την τρίτη χώρα ή τον διεθνή οργανισμό, οπότε και η διαβίβαση επιτρέπεται. Ακόμη κι έχει εκδοθεί τέτοια απόφαση, εξετάζεται επιπρόσθετα, εάν στην υπό κρίση περίπτωση ο αποδέκτης εγγυάται κατάλληλη προστασία των θεμελιωδών δικαιωμάτων και

[152] Βλ. ΕΣΠΔ, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, σελ. 29 επ. και Δ. Τζέλλη. Μ. Μυλώση, σελ. 147 επ.
[153] Άρθρα 40 και 42 ΓΚΠΔ.

εννόμων συμφερόντων του υποκειμένου. Σε αντίθετη περίπτωση που δεν υπάρχει απόφαση επάρκειας, για το επιτρεπτό της διαβίβασης εξετάζεται εάν ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία παρέχει κατάλληλες εγγυήσεις και υπό την προϋπόθεση ότι υφίστανται εκτελεστά δικαιώματα και αποτελεσματικά ένδικα μέσα για τα υποκείμενα των δεδομένων[154]. Τέτοιες εγγυήσεις προβλέπονται, σύμφωνα με τις διατάξεις του Κανονισμού, μέσω ενός νομικά δεσμευτικού και εκτελεστού μέσου μεταξύ δημοσίων αρχών ή φορέων, δεσμευτικών εταιρικών κανόνων, τυποποιημένων ρητρών προστασίας δεδομένων, εγκεκριμένου κώδικα δεοντολογίας ή εγκεκριμένου μηχανισμού πιστοποίησης. Ειδικότερες εγγυήσεις παρέχονται για την προστασία των προσωπικών δεδομένων ειδικών κατηγοριών, όπως περιορισμοί για τις περαιτέρω διαβιβάσεις και κοινοποιήσεις των δεδομένων εκτός της Ευρωπαϊκής Ένωσης και η υποχρέωση του αποδέκτη να λαμβάνει προηγούμενη έγκριση της διαβιβάζουσας αρχής[155]. Μπορούν επίσης να αξιολογηθούν και ληφθούν υπόψη ειδικότερες συμφωνίες συνεργασίας (πχ. μεταξύ Europol ή Eurojust και τρίτων χωρών) και προβλεπόμενες υποχρεώσεις εμπιστευτικότητας.

Ελλείψει των ανωτέρω, αναζητείται η ύπαρξη δεσμευτικών εταιρικών κανόνων. Ορθό είναι να εξασφαλιστεί ότι η χρήση των δεσμευτικών αυτών εταιρικών κανόνων περιορίζεται στη διαβίβαση προσωπικών δεδομένων εντός του ομίλου επιχειρήσεων διεθνώς και μεταξύ των επιμέρους εταιρειών.

Περαιτέρω, για ειδικές καταστάσεις προβλέπονται παρεκκλίσεις από τη διάταξη του άρθρου 49 του ΓΚΠΔ, στις οποίες θα πρέπει να γίνεται ειδική αναφορά και αιτιολόγηση ως προς το λόγο νομιμότητας της διαβίβασης, την ημερομηνία και ώρα που έλαβε χώρα, τα στοιχεία του αποδέκτη και το είδος των δεδομένων που διαβιβάστηκαν, ενώ παράλληλα ο υπεύθυνος επεξεργασίας πρέπει να είναι σε θέση να θέσει τα στοιχεία αυτά στη διάθεση της ΑΠΔΠΧ, εφόσον ζητηθούν.

### 4.3. Περιπτωσιολογία και Νομολογιακή Επισκόπηση

Σε αίτηση που υποβάλλει φυσικό πρόσωπο προς ένα Επιμελητήριο για καταχώρηση στο Γενικό Εμπορικό Μητρώο (Γ.Ε.ΜΗ.) στοιχείων της ατομικής του

[154] Άρθρο 46 του ΓΚΠΔ.
[155] Βλ. Δ. Τζέλλη. Μ. Μυλώση, σελ. 164επ.

επιχείρησης θα πρέπει να τίθεται επαρκής και σε απλή γλώσσα ενημέρωση από την Κεντρική Υπηρεσία Γ.Ε.ΜΗ προς τους αιτούντες- υποκείμενα των δεδομένων, ότι κάθε διενεργούμενη επεξεργασία προσωπικών δεδομένων, η οποία εντάσσεται στη διάρθρωση και λειτουργία του Γενικού Ευρετηρίου Επωνυμιών, τη Μερίδα και το Φάκελο, εξυπηρετεί λόγους δημοσίου συμφέροντος, σκοπούς αρχειοθέτησης και εκπλήρωση νομίμων καθηκόντων, αλλά και οποιαδήποτε άλλη επεξεργασία διενεργείται να αναφέρονται ρητά οι νόμιμοι σκοποί. Επιβεβλημένη είναι επίσης η ενημέρωση, μεταξύ άλλων και για το χρόνο αποθήκευσης όσο και για τα δικαιώματα των υποκειμένων, μαζί με υπόδειξη του τρόπου άσκησής τους. Βέβαια για να διασφαλιστεί ο σχεδιασμός και η επί της ουσίας ύπαρξη μέτρων πρέπει να προβλέπονται μέσα σε έναν οργανισμό ή εταιρεία οι αντίστοιχες διαδικασίες και φόρμες εντύπων υποβολής των σχετικών αιτημάτων των υποκειμένων, διαχείρισης και καταστροφής των δεδομένων.

Σχετικά με το δικαίωμα πρόσβασης, φορολογική αρχή έχει τέτοιο δικαίωμα σε πληροφορίες φορολογικού και οικονομικού ενδιαφέροντος φυσικών προσώπων, χωρίς υποχρέωση προηγούμενης ενημέρωσης και συγκατάθεσης των προσώπων που τα αφορά, διότι το δικαίωμα αυτό στηρίζει τη νομιμοποιητική του βάση σε ειδικότερες διατάξεις νόμων περί φορολογίας εισοδήματος για σκοπούς δημόσιου φορολογικού ελέγχου και διασταυρώσεων[156].

Περίπτωση υποβολής αιτήματος από το Υπουργείο Ανάπτυξης για παροχή στοιχείων των μελών ενός Επιμελητηρίου προς διενέργεια συγκεκριμένης μελέτης και έρευνας. Τα Επιμελητήρια αποτελούν βεβαίως Νομικά Πρόσωπα Δημοσίου Δικαίου και συμμορφώνονται με το σύνολο της Επιμελητηριακής νομοθεσίας (όπως το Ν. 4497/2017), το σύνολο των οικείων Υπουργικών Αποφάσεων και Εγκυκλίων, τη νομοθεσία που διέπει τη λειτουργία του ως Ν.Π.Δ.Δ., όπως ενδεικτικά τον Κώδικα Διοικητικής Διαδικασίας κ.α. και ασκούν τις αρμοδιότητες που προβλέπονται στη νομοθεσία και εντός του πλαισίου των καταστατικών τους σκοπών. Περαιτέρω, η ελευθερία της έρευνας αποτελεί μεν συνταγματικά κατοχυρωμένο δικαίωμα (κατά το άρθρο 16 παρ. 1 Σ), ωστόσο η ελευθερία της έρευνας ενδέχεται να υπόκειται σε περιορισμούς που θεσπίζονται από γενικούς νόμους, που έχουν ως στόχο την

[156] Βλ. σε Λ. Κανέλλο, The GDPR Handbook, Εκδ. Νομική Βιβλιοθήκη, 2020, σελ. 300.

αντικειμενική προάσπιση ενός προστατευόμενου έννομου αγαθού και οι οποίοι δεν στρέφονται εναντίον ενός ορισμένου προσώπου, ούτε καθιστούν αδύνατη ή δυσχεραίνουν υπερβολικά την έρευνα. Ο ερευνητής συνεπώς κατά τη διάρκεια της έρευνάς του υπόκειται σε περιορισμούς, οι οποίοι απορρέουν από τις διατάξεις του Ν. 4624/2019 που κατοχυρώνουν την προστασία των προσωπικών δεδομένων και οι οποίες έχουν θεσπιστεί ως προέκταση του άρθρου 9 Α του Συντάγματος. Οπωσδήποτε τυγχάνουν εφαρμογής οι αρχές που διέπουν την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και σίγουρα τυγχάνει εφαρμογής και η αρχή της ελαχιστοποίησης των δεδομένων κατά την οποία τα δεδομένα προσωπικού χαρακτήρα πρέπει να περιορίζονται στα απολύτως αναγκαία για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία. Επιπρόσθετα, σύμφωνα με την αρχή της αναγκαιότητας και της προσφορότητας η επεξεργασία είναι σύννομη μόνο όταν δικαιολογείται για συγκεκριμένο σκοπό ή για την άσκηση συγκεκριμένων έννομων δικαιωμάτων. Συνεπώς, η επεξεργασία προσωπικών δεδομένων για σκοπούς επιστημονικής ή ιστορικής έρευνας δεν θεωρείται ασύμβατη με τους αρχικούς σκοπούς εφόσον η συγκεκριμένη επεξεργασία δεν επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων και παρέχονται κατάλληλες εγγυήσεις για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων, όπως η ψευδωνυμοποίηση δεδομένων. Ομοίως, προκύπτει ως απαραίτητη προϋπόθεση για την περαιτέρω επεξεργασία προσωπικών δεδομένων για ερευνητικούς σκοπούς η συγκεκριμένη επεξεργασία να μην επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων. Με τον τρόπο αυτό, διασφαλίζεται η προηγούμενη ανωνυμοποίηση των προσωπικών δεδομένων που έχουν συλλεχθεί από τον ερευνητή, πριν τη δημοσίευση των αποτελεσμάτων της έρευνας. Ενόψει αυτών θα πρέπει να προκύπτει σε ποιο συγκεκριμένο λόγο συνίσταται η αναγκαιότητα και προσφορότητα της διαβίβασης των στοιχείων που ζητούνται και βέβαια να υπάρχουν οι κατάλληλες εγγυήσεις και τα κατάλληλα μέτρα ασφάλειας. Δεδομένου ότι πολλές από τις επιχειρήσεις των Επιμελητηρίων δεν είναι μόνο νομικά πρόσωπα, αλλά κυρίως φυσικά πρόσωπα και ατομικές επιχειρήσεις, προφανώς εντάσσονται στις διατάξεις του Κανονισμού, κατά το μέτρο που εκτελούν επαγγελματικές επεξεργασίες και θα πρέπει να αιτιολογείται ο τρόπος και ο σκοπός για τον οποίο πιθανόν να δικαιολογείται η διαβίβαση από έναν τέτοιο Οργανισμό προς μία εταιρεία, διαφορετικά δεν θα διαβιβαστούν προσωπικά δεδομένα χωρίς να υπάρχει

κίνδυνος παραβίασής τους. Σε κάθε περίπτωση, συνιστάται η προηγούμενη ενημέρωση των μελών με προβλεπόμενη προθεσμία για τη δυνατότητα άσκησης του δικαιώματος εναντίωσης από πλευράς τους.

Υποβολή αιτήματος από πολίτη προς αρμόδιο Δήμο για χορήγηση αντιγράφων από το αρχείο του Δήμου, επικαλούμενη έννομο συμφέρον προς υποστήριξη κατηγορίας σε εκκρεμή δίκη σε βάρος της. Σύμφωνα με το άρθρο 5 του Κώδικα Διοικητικής Διαδικασίας κάθε ενδιαφερόμενος έχει το δικαίωμα, ύστερα από γραπτή αίτησή του να λαμβάνει γνώση των διοικητικών εγγράφων. Η αιτούσα -εάν κριθεί ad hoc ότι έχει «εύλογο ενδιαφέρον»[157] με βάση τα στοιχεία της αίτησής της- έχει πιθανόν δικαίωμα να λάβει αντίγραφα των εγγράφων, τα οποία όμως ενδέχεται να περιλαμβάνουν και προσωπικά δεδομένων τρίτων προσώπων και τα οποία δεν θα πρέπει σε καμία περίπτωση να τύχουν επεξεργασίας για μη νόμιμο σκοπό. Για το λόγο αυτό πιθανόν να κριθεί σκόπιμο να χορηγηθούν τα αντίγραφα, ωστόσο με την επισήμανση προς την αιτούσα της επιφύλαξης να χρησιμοποιηθούν αποκλειστικά και μόνο για το σκοπό που τα προορίζει (υπεράσπιση των εννόμων συμφερόντων της στη συγκεκριμένη δίκη) και όχι για διαφορετικό σκοπό.

Σχετικά με το δικαίωμα των υποκειμένων των δεδομένων για ενημέρωση, πρόσφατα με την απόφαση 958/2022 του Αρείου Πάγου εξετάστηκε περίπτωση κατά την οποία η αναιρεσείουσα Τράπεζα είχε διαβιβάσει προσωπικά δεδομένα για ληξιπρόθεσμες οφειλές του αναιρεσίβλητου σε εταιρεία ενημέρωσης οφειλετών, χωρίς προηγούμενη ενημέρωσή του για τη διαβίβαση αυτή. Αρχικά με την προσβαλλόμενη απόφαση είχε γίνει δεκτό ότι η Τράπεζα, πέραν της ενημέρωσης που πραγματοποίησε κατά τη συλλογή των δεδομένων του οφειλέτη, όφειλε περαιτέρω να προβεί και σε ενημέρωσή του για τη διαβίβαση κατόπιν των προσωπικών του δεδομένων προς την εταιρία ενημέρωσης οφειλετών. Ωστόσο, ο Άρειος Πάγος έκρινε ότι η αρχική ενημέρωση κατά τη συλλογή των δεδομένων, ήταν πλήρης, σαφή και νόμιμη κατά τις προϋποθέσεις του νόμου, ενώ ταυτόχρονα ο οφειλέτης αναιρεσίβλητος είχε συναινέσει εγγράφως στη διαβίβαση των προσωπικών του δεδομένων προς τους συγκεκριμένους αποδέκτες. Μάλιστα στο σκεπτικό της απόφασης αναλύεται ότι όταν ο υπεύθυνος

[157] Βλ. Σπ. Βλαχόπουλο, Πρόσβασε στα δημόσια έγγραφα, σε Κοτσαλή Λ.- Μενουδάκο Κ., Γενικός Κανονισμός για την προστασία των προσωπικών δεδομένων, Νομική διάσταση και πρακτική εφαρμογή, εκδ. Νομ. Βιβλιοθήκη 2018, σελ. 44 επ.

επεξεργασίας των δεδομένων μεταβιβάσει αυτά στον εκτελούντα την επεξεργασία, ο οποίος υπάγεται σε μία από τις κατηγορίες αποδεκτών για την οποία είχε γίνει η ενημέρωση, τότε δεν είναι υποχρεωμένος ο υπεύθυνος επεξεργασίας να προβεί και σε νέα ενημέρωση προς το υποκείμενο των δεδομένων τη στιγμή που ανακοινώνει στον εκτελούντα την επεξεργασία τις πληροφορίες για το υποκείμενο. Κι αυτό διότι ο εκτελών την επεξεργασία ενεργεί πράξεις για λογαριασμό του υπεύθυνου την επεξεργασία και όχι για δικό του λογαριασμό. Επομένως, η αναιρεσείουσα Τράπεζα δεν είχε υποχρέωση να ενημερώσει τον αναιρεσίβλητο για την εταιρεία ενημέρωσης οφειλετών στην οποία θα διαβίβαζε τα προσωπικά του δεδομένα, καθώς και η ίδια θα τον καλούσε προς ενημέρωση και διευθέτηση της οφειλής του.

Επίσης πρόσφατα, κατά την εξέταση από το Συμβούλιο της Επικρατείας ζητημάτων περί νομιμότητας της ηλεκτρονικής ψηφοφορίας στις εκλογές των εκπαιδευτικών για την ανάδειξη αιρετών εκπροσώπων στα υπηρεσιακά τους συμβούλια και συγκεκριμένα αιτήσεων ακύρωσης των δευτεροβάθμιων συνδικαλιστικών ενώσεων των εκπαιδευτικών πρωτοβάθμιας και δευτεροβάθμιας εκπαίδευσης κατά κοινής υπουργικής απόφασης με την οποία ρυθμίστηκε η διαδικασία της ηλεκτρονικής ψηφοφορίας τους κατά τις εκλογές του έτους 2020, όπως προβλέπεται από το άρθρο 22 του ν. 4728/2020, το ΣτΕ έκρινε μεταξύ άλλων, ότι η εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων λόγω ενδεχόμενης επέλευσης υψηλού κινδύνου για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, γίνεται από τον υπεύθυνο επεξεργασίας πριν από τη διενέργεια της επεξεργασίας και, ως εκ τούτου, δεν προκύπτει αντίθεση προς τη διάταξη του άρθρου 35 παρ. 1 του ΓΚΠΔ, από τη μη διενέργεια εκτίμησης αντικτύπου πριν από την ψήφιση της διάταξης του άρθρου 22 του ν. 4728/2020 ή πριν από την έκδοση της προσβαλλόμενης κ.υ.α., ανεξαρτήτως αν στην υπό κρίση περίπτωση συνέτρεχαν οι προϋποθέσεις του άρθρου αυτού για διενέργεια εκτίμησης αντικτύπου πριν από την επεξεργασία[158].

Με την με αριθμό 12/2022 απόφασή της η ΑΠΔΠΧ επέβαλε διοικητικό χρηματικό πρόστιμο κατόπιν καταγγελίας εργαζομένης για μη ικανοποίηση του δικαιώματος

[158] Βλ. ΣτΕ Γ΄7μ. 2112-2114/2022, http://www.adjustice.gr/webcenter/portal/ste/pageste/epikairotita/apofaseis?contentID=DECISION-TEMPLATE1666858349681&_afrLoop=692943933383129#!%40%40%3F_afrLoop%3D692943933383129%26centerWidth%3D65%2525%26contentID%3DDECISION-TEMPLATE1666858349681%26leftWidth%3D0%2525%26rigthWidth%3D35%2525%26showFooter%3Dfalse%26showHeader%3Dtrue%26_adf.ctrl-state%3Dm7igkug5m_120.

εναντίωσής της από την εργοδότριά της. Ειδικότερα, η εργοδότρια, ιδιοκτήτρια φροντιστηρίου, παρενέβαινε διαρκώς και παρακολουθούσε τα διαδικτυακά μαθήματα της καταγγέλλουσας καθηγήτριας που παρέδιδε στους μαθητές μέσω της διαδικτυακής πλατφόρμας «zoom». Στην εν λόγω περίπτωση, η καταγγελλόμενη εργοδότρια είχε την ιδιότητα του υπεύθυνου επεξεργασίας και καθόριζε τους σκοπούς και τον τρόπο επεξεργασίας, δηλαδή την παρακολούθηση εικόνας και ήχου με αυτοματοποιημένα μέσα κι ως εκ τούτου είχε όλες τις υποχρεώσεις της συμμόρφωσης. Ωστόσο, παρά τη σαφή εναντίωση της καταγγέλλουσας στην συγκεκριμένη επεξεργασία μέσω γραπτών ηλεκτρονικών μηνυμάτων emails και viber, η εργοδότρια συνέχιζε την επεξεργασία επικαλούμενη ως νόμιμη βάση τη συγκατάθεση. Η Αρχή έκρινε ότι εν προκειμένω η συγκατάθεση δεν μπορεί να θεωρηθεί θεμιτή νομική βάση δεδομένης της ανισορροπίας που υπάρχει στην εργασιακή σχέση μεταξύ εργοδότη και εργαζομένου και λόγω ανυπαρξίας άλλης νόμιμης βάσης, η συγκεκριμένη επεξεργασία δεν μπορούσε να βρει νόμιμο θεμέλιο ενώ ταυτόχρονα υπήρξε και παραβίαση των βασικών αρχών.

Ομοίως χρηματικό πρόστιμο επιβλήθηκε από την ΑΠΔΠΧ με την με αριθμό 25/2022 απόφασή της σε υπόθεση καταγγελίας οφειλέτριας προς εταιρεία διαχείρισης απαιτήσεων από δάνεια και πιστώσεις, η οποία δεχόταν αδιάκοπες τηλεφωνικές οχλήσεις από την τελευταία για ρύθμιση τάχα οφειλών από τις οποίες στην πραγματικότητα είχε ήδη απαλλαγεί με δικαστικές αποφάσεις περί υπερχρεωμένων νοικοκυριών. Η καταγγέλλουσα οφειλέτρια υπέβαλε δήλωση εναντίωσης της επεξεργασίας και διαγραφής των προσωπικών της δεδομένων χωρίς ωστόσο τη συμμόρφωση της καταγγελλόμενης.

Άσκηση δικαιώματος διόρθωσης αναγνώρισε η ΑΠΔΠΧ απευθύνοντας επίπληξη δυνάμει της με αριθμό 29/2022 απόφασής της σε δημότη που έκανε καταγγελία στον αρμόδιο Δήμο για μερική μόνο ικανοποίηση του δικαιώματος διόρθωσης του επωνύμου της μητέρας του στη ληξιαρχική πράξη γέννησής του και στο πληροφοριακό σύστημα Μητρώου Πολιτών λόγω του ότι υπήρξε μόνο ιδιόγραφη διόρθωση των στοιχείων της μητέρας του και αντίστοιχη διόρθωση στο πληροφοριακό σύστημα των προσωπικών δεδομένων, χωρίς ωστόσο να σημειωθεί η μεταβολή αυτή στο περιθώριο της πρωτότυπης καταχώρησης της πράξης στο ληξιαρχικό τόμο και χωρίς να γίνει μνεία στο πεδίο «Διορθώσεις/Μεταβολές» στο σύστημα Μητρώου Πολιτών, γεγονός που

αντίκειται στην αρχή της ακρίβειας. Σημειώνεται στην απόφαση ότι η μη καταχώριση αυτής της μεταβολής και η μη τήρηση ορθής διαδικασίας αρχειοθέτησης ενδέχεται να προκαλέσει προβλήματα στην ιδιωτική και επαγγελματική ζωή του καταγγέλοντα πολίτη διότι δεν καθίσταται ευκρινής στους τρίτους και στη διοίκηση η σειρά των γεγονότων και της διενεργηθείσας διόρθωσης με τις πρόσθετες πληροφορίες που την αφορούν, όπως πότε συντελέστηκε, από ποιον και με ποια νομική βάση.

# Κεφάλαιο 5 – Μελέτη των κινδύνων σε συνάρτηση με την Ασφάλεια των δεδομένων

## 5.1 Εκτίμηση και διαχείριση των κινδύνων

Στο επόμενο τρίτο στάδιο εκπόνησης της μελέτης εκτίμησης αντικτύπου ο υπεύθυνος επεξεργασίας αναγνωρίζει και προσδιορίζει τους πιθανούς κινδύνους που ενδεχομένως μπορούν να παρουσιαστούν κατά την διαδικασία της επεξεργασίας σε σχέση με την προστασία των δεδομένων προσωπικού χαρακτήρα, με στόχο βέβαια τον περιορισμό στο ελάχιστο της επέλευσης της ζημίας στα φυσικά πρόσωπα.

Η βασική διαφορά της εκτίμησης αντικτύπου στην προστασία της ιδιωτικότητας και στην ασφάλεια των πληροφοριών έγκειται στην προσέγγιση και διαχείριση του κινδύνου. Στην προστασία των δεδομένων προσωπικού χαρακτήρα κατά τον ΓΚΠΔ υπάρχει εστίαση του κινδύνου στο Υποκείμενο των δεδομένων, δηλαδή ενδιαφέρει τί επιπτώσεις θα υπάρχουν για το υποκείμενο, ενώ αντίθετα στον τομέα της ασφάλειας των πληροφοριών υπάρχει εστίαση του κινδύνου στον Οργανισμό, δηλαδή ενδιαφέρει τί επιπτώσεις θα υπάρχουν για τον Οργανισμό. Συνεπώς, κατά την εκπόνηση της ανάλυσης αντικτύπου για την ιδιωτικότητα ο υπεύθυνος επεξεργασίας θα πρέπει να εξετάσει τον τρόπο με τον οποίο η πράξη επεξεργασίας τυχόν να επηρεάσει τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων. Βεβαίως συνήθως το ένα συνέχει με το άλλο, δηλαδή οι κίνδυνοι για τα υποκείμενα συνεπάγονται και κινδύνους για την ίδια την επιχείρηση ή τον οργανισμό.

Σημαντικό είναι να περιγραφεί τί είναι ο κίνδυνος κατά της ιδιωτικότητας[159]. Κίνδυνος στον τομέα της ασφάλειας των προσωπικών δεδομένων είναι ένα ενδεχόμενο υποθετικό σενάριο σύμφωνα με το οποίο οι υφιστάμενες πηγές κινδύνου μιας

[159] Βλ. CNIL, Privacy Impact Assessment (PIA) Μεθοδολογία, 2018, σελ. 6, σε συνδυασμό με άρθρο 32 του ΓΚΠΔ και Αιτιολογικές σκέψεις αρ. 75,76 και 83 ΓΚΠΔ.

εταιρείας, ενός οργανισμού ή φορέα, μέσα σε ένα πλαίσιο συγκεκριμένων απειλών, θα μπορούσαν να εκμεταλλευτούν ευπάθειες των αγαθών που υποστηρίζουν την επεξεργασία προσωπικών δεδομένων προκαλώντας την πραγματοποίηση περιστατικού παραβίασης που θα έχει επιπτώσεις στην ιδιωτικότητα των υποκειμένων των δεδομένων. Κίνδυνος θα μπορούσε να είναι η αθέμιτη πρόσβαση σε προσωπικά δεδομένα, η ανεπιθύμητη τροποποίηση προσωπικών δεδομένων ή ακόμη η μη διαθεσιμότητά τους.

Ένας κίνδυνος, σύμφωνα με το μοντέλο αξιολόγησης της CNIL, εξετάζεται σε συνάρτηση με δύο παράγοντες: πρώτον, την πιθανότητα εμφάνισης ενός ανεπιθύμητου γεγονότος και δεύτερον, της σοβαρότητας του αντικτύπου αυτού του γεγονότος. Κατ' επέκταση, η κλιμάκωση των κινδύνων είναι καθοριστική για τον καθορισμό των μέτρων προστασίας του υπεύθυνου επεξεργασίας.

### 5.1.1 Πηγές κινδύνων, Απειλές, Ευπάθειες

Προκειμένου να προβλεφθεί ο κίνδυνος είναι σημαντικό να αναγνωριστούν οι πηγές των κινδύνων στο συγκεκριμένο περιβάλλον της μελέτης. Προκειμένου να γίνει αυτό ο υπεύθυνος επεξεργασίας θα πρέπει να αναζητήσει κάποιον ή κάτι που θα μπορούσε να ασκήσει αρνητική επιρροή κατά την εξέλιξη μιας επεξεργασίας και να οδηγήσει στην εμφάνιση ενός κινδύνου.

Μια τέτοια πηγή κινδύνου μπορεί να αποτελέσει κατ' αρχήν ο ανθρώπινος παράγοντας στο εσωτερικό ενός οργανισμού[160]. Σε αυτή την κατηγορία μπορούν να υπαχθούν οι εργαζόμενοι στον οργανισμό (υπάλληλοι), οι διαχειριστές συστημάτων πληροφορικής (IT), οι εκπαιδευόμενοι και τα διευθυντικά στελέχη (διευθυντές, διοίκηση), οι οποίοι μπορεί να ενεργήσουν είτε συνειδητοποιημένα, υπηρετώντας κάποια σκοπιμότητα (όπως από ανταγωνισμό ή εκδίκηση προς συνάδελφό τους ή τη διοίκηση, ή για οικονομικά κίνητρα ή προσωπική ανέλιξη), είτε από λάθος και χωρίς κάποια πρόθεση (όπως σε περιπτώσεις λάθους χειρισμού, άγνοιας χρήσης των πληροφοριακών συστημάτων, αβλεψία της στιγμής, ελλειπή εκπαίδευση κ.α.).

Δεύτερη κατηγορία πηγών κινδύνου μπορεί να αποτελέσει ο ανθρώπινος παράγοντας στο εξωτερικό ενός οργανισμού. Σε αυτή μπορεί να υπαχθούν οι

[160] Βλ. CNIL, Privacy Impact Assessment (PIA) Knowledge Bases, 2018, σελ. 3 και Δ. Τζέλλη. Μ. Μυλώση, Εκτίμηση Αντικτύπου στην προστασία προσωπικών δεδομένων, Εκδ. Νομική Βιβλιοθήκη, 2022, σελ. 7.

αποδέκτες των προσωπικών δεδομένων, εξουσιοδοτημένοι εξωτερικοί συνεργάτες ή δημόσιες αρχές ή δικαστικοί υπάλληλοι κατά την εκτέλεση των καθηκόντων τους, πάροχοι υπηρεσιών, κακόβουλοι χρήστες, hackers, επισκέπτες, πρώην εργαζόμενοι, ανταγωνιστές, συντηρητές, δημοσιογράφοι, μη κυβερνητικές οργανώσεις, εγκληματικές και τρομοκρατικές οργανώσεις κ.α., οι οποίοι ομοίως μπορεί να ενεργήσουν είτε με πρόθεση να προκαλέσουν κίνδυνο είτε κάποια σκοπιμότητα.

Τρίτη κατηγορία πηγών κινδύνου ενδέχεται να αποτελέσει ο,τιδήποτε βρίσκεται έξω από τη σφαίρα του ανθρώπινου παράγοντα, όπως κακόβουλο λογισμικό άγνωστης προέλευσης (για παράδειγμα ιοί, σκουλίκια), πηγές νερού (σωλήνες, υδρορροές), εύφλεκτα ή εκρηκτικά υλικά, φυσικές καταστροφές, επιδημίες, υποδομές, μηχανήματα.

Επίσης, θα πρέπει να προσδιοριστούν οι απειλές[161] και οι ευπάθειες. Απειλή είναι η πιθανή αιτία πρόκλησης ενός περιστατικού παραβίασης των δεδομένων προσωπικού χαρακτήρα που μπορεί να προκαλέσει αρνητικές επιπτώσεις για τα υποκείμενα των δεδομένων. Κατά τον ΓΚΠΔ ως παραβίαση δεδομένων προσωπικού χαρακτήρα ορίζεται η παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία[162].

Οι απειλές μπορεί να προκαλούνται από φυσικούς παράγοντες (όπως έκτακτα καιρικά φαινόμενα, φυσικές καταστροφές, φωτιά, πλημμύρα, σεισμός), παράγοντες τεχνικής φύσης (όπως τεχνικές βλάβες, διακοπή ηλεκτροδότησης, αστοχία λογισμικού συστήματος και εφαρμογών, βλάβη εξυπηρετητή και δικτύου) και ανθρώπινους παράγοντες (όπως μη εξουσιοδοτημένη πρόσβαση σε δεδομένα, κλοπή υλικού ή λογισμικού, εισαγωγή κακόβουλου λογισμικού, εσφαλμένη διαγραφή ή αποκάλυψη δεδομένων). Ειδικότερα, απειλή μπορεί να αποτελέσει περιστατικό που να οδηγήσει σε μη ορθή χρήση των πληροφοριακών πόρων, σε παρακολούθηση αυτών, υπερφόρτωση, καταστροφή ή βλάβη ή ακόμη τροποποίηση ή απώλεια. Οι απειλές των πληροφοριακών πόρων μπορεί να οδηγήσουν σε απειλές κατά της Εμπιστευτικότητας,

[161] Βλ. Κ. Λαμπρινουδάκη, Λ. Μήτρου, Στ. Γκρίτζαλη, Σ. Κάτσικα, Προστασία της Ιδιωτικότητας, Τεχνολογίες Πληροφορικής και Επικοινωνιών, Τεχνικά και Νομικά Θέματα, Απειλές ασφάλειας και ιδιωτικότητας, εκδ. Παπασωτηρίου 2010, σελ. 78-79.
[162] Άρθρο 4 του ΓΚΠΔ.

της Ακεραιότητας και της Διαθεσιμότητας των προσωπικών δεδομένων. Την εμπιστευτικότητα για παράδειγμα μπορούν να πλήξουν περιστατικά χρήσης ακατάλληλων αποθηκευτικών μέσων (όπως τα usb sticks, οι σκληροί δίσκοι), κλοπής φορητού υπολογιστή, αποστολής ανεπιθύμητων ηλεκτρονικών μηνυμάτων μέσω προγράμματος ηλεκτρονικού ταχυδρομείου, μόλυνσης από κακόβουλο λογισμικό, υποκλοπής τηλεφωνικών συνδιαλέξεων κ.α. Η ακεραιότητα μπορεί να πληγεί από περιστατικά που μπορούν να οδηγήσουν σε ανεπιθύμητη τροποποίηση προσωπικών δεδομένων, όπως για παράδειγμα, λάθη συστήματος μέσω αναβαθμίσεων, εσφαλμένη συντήρηση υλισμικού ή λογισμικού, σύνδεση μη συμβατού υλισμικού με αποτέλεσμα δυσλειτουργίες, διαγραφή αρχείων από σφάλμα, άγχος και υψηλός φόρτος εργασίας λόγω υπερφόρτωσης του ανθρώπινου δυναμικού κ.α. Αντίστοιχα, τη διαθεσιμότητα είναι ικανά να πλήξουν περιστατικά φυσικών καταστροφών, ακατάλληλης προσωπικής χρήσης αρχείων, εσφαλμένων κινήσεων χειριστών που συνεπάγονται τη διαγραφή δεδομένων, υπέρβασης μεγέθους της βάσης δεδομένων, άστοχοι χειρισμοί κατά τη συντήρηση κ.α.[163]

Ωστόσο, για να καταφέρει μία απειλή να ασκήσει την βλαπτική της επιρροή μέσα σε έναν οργανισμό θα πρέπει να βρει αυτά τα τρωτά σημεία και τις αδυναμίες του που αν τα εκμεταλλευτεί θα προκαλέσει αρνητικές συνέπειες στην ιδιωτική ζωή των υποκειμένων των δεδομένων. Ενδεικτικά, τέτοια τρωτά σημεία σε έναν οργανισμό ενδέχεται να είναι ευπάθειες υλικού, όπως εσφαλμένες πρακτικές για απόσυρση υλικού (σκληροί δίσκοι, μονάδες USB flash), χρήση υλικών για άλλο σκοπό από τον προβλεπόμενο, χαμηλές ικανότητες αποθήκευσης και επεξεργασίας, διατήρηση υλικών σε μη ενδεδειγμένες περιβαλλοντολογικές συνθήκες (θερμοκρασία, υγρασία, σκόνη). Ομοίως, αδυναμίες σε έναν οργανισμό ενδέχεται να αποτελούν ευπάθειες λογισμικού, όπως η παράλειψη αποσύνδεσης χρηστών, εσφαλμένες δυνατότητες παραμετροποίησης, επιλογή προγραμματιστών και συντηρητών με περιορισμένες γνώσεις και ικανότητες. Επίσης, στα τρωτά σημεία μπορούν να αναφερθούν οι ευπάθειες δικτύου, όπως για παράδειγμα χρήση δημόσιων δικτύων χωρίς επαρκή ασφάλεια και η μη κρυπτογραφημένη μετάδοση εμπιστευτικών δεδομένων. Επιπλέον,

[163] Βλ. CNIL, Privacy Impact Assessment (PIA) Knowledge Bases, 2018, σελ. 6 επ. και Δ. Τζέλλη. Μ. Μυλώση, Εκτίμηση Αντικτύπου στην προστασία προσωπικών δεδομένων, Εκδ. Νομική Βιβλιοθήκη, 2022, σελ. 16-29.

οι ευπάθειες στο ανθρώπινο δυναμικό δεν μπορούν να παραβλεφθούν, όπως είναι η επιπολαιότητα, η έλλειψη εχεμύθειας, ο ευάλωτος και επιρρεπής χαρακτήρας, η ανεπάρκεια σε εκπαίδευση, γνώσεις και δεξιότητες, η άγνοια του νομοθετικού πλαισίου, η απουσία διαδικασιών και πολιτικών κ.α. Επιπρόσθετα, ευπάθειες μπορούν να αναφερθούν σε εγκαταστάσεις σε μη ασφαλείς περιοχές, που πλήττονται από ακραία καιρικά φαινόμενα ή σε τοποθεσίες που το δίκτυο ηλεκτροδότησης είναι ασταθές.

Ως εκ τούτου, ο υπεύθυνος επεξεργασίας κατά την εκπόνηση της μελέτης εκτίμησης αντικτύπου προσπαθεί να αναγνωρίσει και να καταγράψει τις πιθανές απειλές για κάθε εκτελούμενη επεξεργασία και να την αντιμετωπίσει ανάλογα με την πηγή που μπορεί να την προκαλέσει, τους αντίστοιχους πληροφοριακούς πόρους που συνδέονται με αυτή και ανάλογα με την κατηγορία ευπάθειας. Κατόπιν καταγράφει τα σχεδιαζόμενα μέτρα ασφάλειας που σχετίζονται με την απειλή.

### 5.1.2 Επίπτωση

Κατά τη Γαλλική Αρχή Προστασίας Προσωπικών Δεδομένων οι παράγοντες που λαμβάνονται υπόψη για την εκτίμηση των κινδύνων είναι η σοβαρότητα και η πιθανότητα. Η σοβαρότητα αναφέρεται στο μέγεθος του κινδύνου και εκτιμάται σε συνάρτηση με το κόστος της ζημίας που θα προκύψει στα υποκείμενα των δεδομένων μετά το υπό εξέταση περιστατικό παραβίασης της ιδιωτικότητας. Η πιθανότητα αναφέρεται στο ποσοστό δυνατότητας να συμβεί συγκεκριμένος αριθμός περιστατικών παραβίασης ασφάλειας μέσα σε ένα συγκεκριμένο χρονικό διάστημα.

Λεπτομερέστερα, η σοβαρότητα αντιπροσωπεύει το μέγεθος του κινδύνου, δηλαδή των επιπτώσεων μιας απειλής[164]. Επίπτωση είναι η δυσχερής κατάσταση στην οποία περιέρχεται το υποκείμενο, εξαιτίας του περιστατικού παραβίασης μέσα στο επιχειρησιακό περιβάλλον του υπεύθυνου επεξεργασίας και μπορεί να είναι είτε φυσικής-σωματικής φύσης, είτε υλικής φύσης, είτε ηθικής-συναισθηματικής φύσης. Σωματικής φύσης επιπτώσεις ενδέχεται να είναι ένα είδος σωματικής πάθησης του υποκειμένου ήπιας ή πολύ σοβαρής με μακροπρόθεσμες συνέπειες για το ίδιο, πρόκληση σοβαρών συνεπειών για την υγεία με μακροπρόθεσμη βλάβη στο

[164] Βλ. CNIL, Privacy Impact Assessment (PIA) Knowledge Bases, 2018, σελ. 4 και Δ. Τζέλλη. Μ. Μυλώση, Εκτίμηση Αντικτύπου στην προστασία προσωπικών δεδομένων, Εκδ. Νομική Βιβλιοθήκη, 2022, σελ. 9-13.

υποκείμενο λόγω παράδειγμα ακατάλληλης ιατρικής φροντίδας, πρόκληση μόνιμης βλάβης στην υγεία λόγω απώλειας πρόσβασης σε συστήματα κρίσιμων υποδομών. Υλικής φύσης επιπτώσεις ενδέχεται να είναι η πρόκληση ζημιών στην οικονομική και περιουσιακή κατάσταση του υποκειμένου, απώλεια εισοδήματος, απροσδόκητη και εσφαλμένη απαίτηση πληρωμών, απώλεια οικονομικών ευκαιριών, απώλεια επαγγελματικής προαγωγής κ.α. Τέλος, ηθικής-συναισθηματικής φύσης επιπτώσεις εννοούνται αυτές που επιδρούν στην ψυχολογική κατάσταση του υποκειμένου των δεδομένων και προκαλούν αναστάτωση, ενόχληση, φόβο, συναισθηματική ταλαιπωρία, κατάθλιψη και ηθική βλάβη, όπως για παράδειγμα, εκφοβισμός μέσω των κοινωνικών δικτύων και παρενόχληση, συναισθηματική διαταραχή λόγω διάδοσης προσωπικών δεδομένων και αμαύρωσης της εικόνας του υποκειμένου.

Ο υπολογισμός της βαρύτητας του κινδύνου αποτυπώνεται σε επίπεδα διαβάθμισης με κλίμακα 1-4, όπου αντίστοιχα χαρακτηρίζεται ως Αμελητέα, Περιορισμένη, Σημαντική και Μέγιστη, ανάλογα με το πόσο επηρεάζονται τα υποκείμενα, τί ενδέχεται να αντιμετωπίσουν και πόσο εύκολα μπορούν να ξεπεραστούν οι δυσκολίες.

Κατά τα ανωτέρω λοιπόν ο υπεύθυνος επεξεργασίας κατά τη μελέτη αντικτύπου προβαίνει σε καταγραφή των επιπτώσεων για κάθε απειλή και κατόπιν υπολογισμό του επιπέδου της σοβαρότητας της κάθε επίπτωσης.

### 5.1.3 Πιθανότητα

Η πιθανότητα εκφράζει τη δυνατότητα επέλευσης του κινδύνου, δηλαδή το πόσο εφικτό είναι να βρει πεδίο δράσης μία απειλή και αυτό εξαρτάται άμεσα από το επίπεδο ευπάθειας που εμφανίζουν οι πληροφοριακοί πόροι όταν βρίσκονται υπό απειλή και το επίπεδο των υφιστάμενων τεχνικών και οργανωτικών μέτρων στο συγκεκριμένο επιχειρησιακό περιβάλλον.

Η ίδια ως άνω κλίμακα 1-4, με χαρακτηρισμούς Αμελητέα, Περιορισμένη, Σημαντική και Μέγιστη, χρησιμοποιείται και για τον υπολογισμό της πιθανότητας εμφάνισης περιστατικών παραβίασης της ιδιωτικότητας, ανάλογα με το πόσο εύκολα

ή δύσκολα μπορεί μία πηγή κινδύνου να υλοποιήσει την απειλή μέσω στοιχείων του συστήματος[165].

Επομένως, ο κίνδυνος αποτιμάται με το γινόμενο της πιθανότητας να συμβεί ένας συγκεκριμένος αριθμός περιστατικών παραβίασης ασφάλειας μέσα σε ένα συγκεκριμένο χρονικό διάστημα επί το κόστος της ζημίας που θα προκύψει.

## 5.2 Αξιολόγηση των μέτρων Ασφάλειας

### 5.2.1 Ειδικά μέτρα στα υπό επεξεργασία προσωπικά δεδομένα

Προκειμένου να διασφαλιστεί ότι τα δικαιώματα και οι ελευθερίες των υποκειμένων των δεδομένων δεν διατρέχουν κινδύνους κατά την επεξεργασία των προσωπικών τους δεδομένων, ο υπεύθυνος επεξεργασίας περιγράφει και αξιολογεί τα μέτρα που εφαρμόζονται για την αντιμετώπιση των κινδύνων που επηρεάζουν την ασφάλειά τους.

Κατά τον ΓΚΠΔ, η ασφάλεια της επεξεργασίας προσωπικών δεδομένων καθίσταται θέμα τόσο μείζονος σημασίας ώστε να συμπεριλαμβάνεται, μαζί με την ακεραιότητα και εμπιστευτικότητα, στις γενικές αρχές επεξεργασίας δεδομένων[166].

Στο άρθρο 32 του ΓΚΠΔ γίνεται ρητή αναφορά και προσδιορίζεται πλέον επίσημα η αρχή αυτή, ορίζοντας ότι αποτελεί υποχρέωση του υπεύθυνου επεξεργασίας και του εκτελούντος την επεξεργασία να εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα για την ασφάλεια της επεξεργασίας[167]. Τα μέτρα αυτά πρέπει να περιλαμβάνουν κατά περίπτωση τέτοιες τεχνικές ώστε να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων[168]. Ο Υπόχρεος στη λήψη μέτρων πρέπει να λάβει υπόψη του διάφορες παραμέτρους όπως: α) τις τελευταίες εξελίξεις στην τεχνολογία, β) το κόστος εφαρμογής των μέτρων, καθώς, για παράδειγμα, επηρεάζεται το κόστος από το αν γίνει χρήση τυποποιημένου λογισμικού ή απαιτείται η προσαρμογή ή κατασκευή νέου λογισμικού, όπως επίσης, επιπλέον μέτρα ασφάλειας απαιτούν

[165] Βλ. CNIL, Privacy Impact Assessment (PIA) Knowledge Bases, 2018, σελ. 6 και Δ. Τζέλλη. Μ. Μυλώση, Εκτίμηση Αντικτύπου στην προστασία προσωπικών δεδομένων, Εκδ. Νομική Βιβλιοθήκη, 2022, σελ. 13-15.
[166] Βλ. άρθρο 5 παρ. 1 στοιχ. στ΄ ΓΚΠΔ.
[167] Βλ. Σ. Κάτσικα, Στ. Γκρίτζαλη, Κ. Λαμπρινουδάκη, Ασφάλεια Πληροφοριών και Συστημάτων στον Κυβερνοχώρο, Οι απαιτήσεις ασφάλειας στον ΓΚΠΔ, εκδ. Νέων Τεχνολογιών 2021, σελ. 91-99.
[168] Βλ. Αιτιολ. σκέψη αρ. 83.

αυξημένες υπολογιστικές δυνατότητες και γ) τους κινδύνους, δηλαδή να προβεί σε αξιολόγηση της πιθανότητας επέλευσης και σοβαρότητας των κινδύνων[169].

Από αυτά καταλαβαίνουμε ότι δεν υφίσταται απόλυτο επίπεδο ασφάλειας, αλλά τα μέτρα λαμβάνονται in concreto, κατά τις περιστάσεις της συγκεκριμένης περίπτωσης.

Παράδειγμα, έχει κριθεί παλαιότερα, στην υπόθεση Ι. κατά Φιλανδίας[170], ότι υπήρξε παραβίαση του άρθρου 8 της ΕΣΔΑ, όταν η προσφεύγουσα αδυνατούσε να αποδείξει ότι ο φάκελος υγείας της είχε προσπελαστεί αθέμιτα από άλλους εργαζόμενους του νοσοκομείου στο οποίο εργαζόταν και η ίδια και τα εθνικά δικαστήρια απέρριψαν την προσφυγή της, κρίθηκε τελικά από το ΕΔΔΑ, ότι παραβιάστηκε το δικαίωμα προστασίας των δεδομένων της, διότι το σύστημα μητρώου φακέλων υγείας του νοσοκομείου δεν έδινε τη δυνατότητα να διαπιστωθεί αναδρομικά η χρήση των φακέλων των ασθενών, δεδομένου ότι εμφάνιζε μόνο τις πέντε τελευταίες ιατρικές επισκέψεις, τα δε στοιχεία αυτά διαγράφονταν μόλις ο φάκελος επέστρεφε στο αρχείο.

Επίσης, κριτήριο για το αναγκαίο επίπεδο ασφάλειας αποτελεί κατά τον Κανονισμό το πλαίσιο και οι σκοποί επεξεργασίας. Πάνω σε αυτό, η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα με απόφασή της[171] τονίζει την ανάγκη λήψης απαραίτητων μέτρων ασφαλείας για τη νόμιμη λειτουργία αρχείου της ΤΕΙΡΕΣΙΑΣ ΑΕ, βασικό στοιχείο των οποίων αποτελεί ο λογικός διαχωρισμός των δεδομένων που τηρούνται για κάθε ένα από τους διακριτούς σκοπούς που επιδιώκει η ΤΕΙΡΕΣΙΑΣ ΑΕ, ώστε να διασφαλίζεται ότι αυτά χρησιμοποιούνται μόνο για τον εκάστοτε επιδιωκόμενο σκοπό. Λογικός διαχωρισμός υπάρχει όταν το λογισμικό, όλων των επιπέδων, που χρησιμοποιείται για πρόσβαση στα δεδομένα που τηρούνται για την ικανοποίηση ενός συγκεκριμένου σκοπού είναι διακριτό και λογικά απομονωμένο από το λογισμικό που χρησιμοποιείται για πρόσβαση σε δεδομένα που τηρούνται για άλλους σκοπούς.

Στον ΓΚΠΔ γίνεται ενδεικτική αναφορά στη λήψη συγκεκριμένων μέτρων ασφάλειας, με στόχο την πρόληψη των κινδύνων, ανεξάρτητα από το εάν έχουν λάβει χώρα περιστατικά παραβίασης. Στα μέτρα περιλαμβάνονται ρητά η ψευδωνυμοποίηση

[169] Βλ. και Ε. Αλεξανδροπούλου-Αιγυπτιάδου, Προσωπικά δεδομένα, εκδ. Νομ. Βιβλιοθήκη 2016, σελ. 129 και σελ. 181.
[170] ΕΔΔΑ, Ι κατά Φινλανδίας, προσφυγή αριθ. 20511/03, 17 Ιουλίου 2008.
[171] Υπ' αρ. 186/2014 απόφαση της Αρχής, www.dpa.gr

και η κρυπτογράφηση προσωπικών δεδομένων, ως τέτοια που μπορούν να μειώσουν σημαντικά τους κινδύνους που σχετίζονται με την επεξεργασία δεδομένων.

Πέραν αυτών, βασικοί στόχοι της ασφάλειας δεδομένων και πληροφοριακών συστημάτων συνιστούν η διασφάλιση του απορρήτου[172], της ακεραιότητας, της διαθεσιμότητας και αξιοπιστίας των συστημάτων και των υπηρεσιών επεξεργασίας σε συνεχή βάση. Δομική αρχή της ασφάλειας των δεδομένων είναι η αρχή της CIA (Confidentiality, Integrity, Availability), ήτοι Εμπιστευτικότητα, Ακεραιότητα και Διαθεσιμότητα.

Εμπιστευτικότητα σημαίνει τον αποκλεισμό πρόσβασης σε εμπιστευτικές ή ευαίσθητες πληροφορίες από μη εξουσιοδοτημένα πρόσωπα, για παράδειγμα τα φορολογικά στοιχεία ενός φυσικού προσώπου είναι εμπιστευτικά και απόρρητα και ως εκ τούτου επιτρέπεται να λάβει γνώση αυτών μόνο οποιοσδήποτε τρίτος έχει έννομο συμφέρον (πχ. Σώμα Δίωξης Οικονομικού Εγκλήματος). Η ακεραιότητα αναφέρεται στη διατήρηση των δεδομένων ενός πληροφοριακού συστήματος σε μία δομημένη κατάσταση, χωρίς παρεμβάσεις από μη εξουσιοδοτημένα πρόσωπα, όπως λόγου χάρη, η ιατρική γνωμάτευση ενός ασθενή θα πρέπει να τηρείται όπως ακριβώς συντάχθηκε από το θεράποντα ιατρό, ενώ η διαθεσιμότητα των δεδομένων και των υπολογιστικών πόρων αναφέρεται στη διασφάλιση της διατήρησης των υπολογιστών, δικτύων και δεδομένων στη διάθεση των χρηστών[173]. Για παράδειγμα, τα δεδομένα ενός πελάτη μιας τράπεζας πρέπει να είναι διαρκώς προσβάσιμα τόσο σε αυτόν όσο και σε εξουσιοδοτημένους υπαλλήλους της τράπεζας[174].

Η παραβίαση των αρχών αυτών μπορεί να επιφέρει σοβαρούς κινδύνους. Από τις πιο επικίνδυνες περιπτώσεις περιστατικών ασφάλειας είναι βέβαια αυτές με ευαίσθητα προσωπικά δεδομένα. Το 2015 παράδειγμα, ανακοινώθηκε από την Αμερικανική εταιρία ασφαλίσεων υγείας Premera ότι έπεσε θύμα κυβερνοεπίθεσης, κατά την οποία οι επιτιθέμενοι απέκτησαν πρόσβαση σε προσωπικά δεδομένα εκατομμυρίων πελατών της, που περιλάμβαναν μεταξύ άλλων, στοιχεία επικοινωνίας, αριθμό κοινωνικής ασφάλισης, τραπεζικούς λογαριασμούς κ.α.[175] Παρόμοιο

[172] Βλ. Ε. Αλεξανδροπούλου-Αιγυπτιάδου, Προσωπικά δεδομένα, εκδ. Νομ. Βιβλιοθήκη 2016, σελ. 129.
[173] Βλ. Ι. Ιγγλεζάκη, Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων, 2018, σελ. 149.
[174] Βλ. Λ. Κοτσαλή, Προσωπικά δεδομένα, εκδ. Νομ. Βιβλιοθήκη 2016, σελ. 383 επ.
[175]ανακτήθηκε 08/12/2022 από:
https://www.npr.org/sections/alltechconsidered/2015/03/18/393868160/premera-blue-cross-cyberattack-exposed-millions-of-customer-records,

περιστατικό κινδύνου μπορεί να επέλθει από αποτυχία του λογισμικού επεξεργασίας δεδομένων. Επιπρόσθετα, περιστατικό που τέθηκε σε κίνδυνο η ακεραιότητα των δεδομένων υπήρξε για παράδειγμα, όταν το 2011 η ΑΠΔΠΧ αντιμετώπισε περίπτωση ινστιτούτου υγείας, από το οποίο εκλάπησαν τέσσερις υπολογιστές που περιείχαν ευαίσθητα προσωπικά δεδομένα υγείας χιλιάδων παιδιών[176]. Τα εν λόγω δεδομένα ανακτήθηκαν από παλαιότερο αντίγραφο ασφαλείας.

Ειδικότερα τώρα, ως κρυπτογράφηση, νοείται η εφαρμογή μιας διαδικασίας μετασχηματισμού δεδομένων με τη βοήθεια αλγορίθμων και με τη χρήση κλειδιών κρυπτογράφησης ενός συνόλου προσωπικών δεδομένων σε μη κατανοητή μορφή, ώστε να μην μπορούν να αναγνωστούν παρά μόνο με τη βοήθεια ενός κλειδιού αποκρυπτογράφησης.

Το πλεονέκτημα αυτής της τεχνικής είναι ότι μπορεί να αποτρέψει την πρόσβαση σε τρίτους, ωστόσο, τα κρυπτογραφημένα δεδομένα δε θεωρούνται εξίσου εύχρηστα, καθώς η επεξεργασία τους (αναζήτηση, ανάλυση) απαιτεί πρώτα την αποκρυπτογράφησή τους – άρα πρόσθετο χρόνο και υπολογιστικούς πόρους. Επιπλέον, κρίσιμη είναι η διαχείριση και προστασία των κλειδιών κρυπτογράφησης αφού απώλεια των κλειδιών σημαίνει και απώλεια των δεδομένων. Ως εκ τούτου, ίσως να μην αποτελεί πρακτική επιλογή προστασίας σε περιπτώσεις μεγάλου όγκου δεδομένων με συχνή καθημερινή βάση, αλλά μάλλον αποδεικνύεται αποτελεσματικότερη η χρήση της κρυπτογράφησης σε περιπτώσεις αποθήκευσης δεδομένων για μεσοπρόθεσμη ή μακροπρόθεσμη χρήση ή σε περιπτώσεις που απαιτείται ασφαλής μετάδοση μεταξύ δύο ή περισσότερων τελικών χρηστών μέσω ενός επικοινωνιακού συστήματος[177].

Για να αποφευχθούν περιστατικά παραβίασης, χρήσιμη θα ήταν η εφαρμογή σύγχρονων αλγορίθμων και η ύπαρξη επαρκούς μήκους κλειδιών. Η ύπαρξη αυτών των δύο στοιχείων εξασφαλίζει μεγαλύτερη αποτελεσματικότητα των μέτρων. Σημαντική τεχνική θα ήταν η συνάρτηση κατακερματισμού με μυστικό κλειδί, καθώς επίσης και η ασφαλής διαγραφή μυστικού κλειδιού.

[176] Βλ. ΑΠΔΠΧ, απόφαση 60/2011.
[177] Βλ. Ν. Λουκά, Τεχνικά μέτρα του Γενικού Κανονισμού για την προστασία δεδομένων, Κρυπτογράφηση και Ψευδωνυμοποίηση, Συνήγορος 123/2017, σελ. 46 επ.

Μία καλή πρακτική εφαρμογή της κρυπτογράφησης θα μπορούσε να είναι για παράδειγμα, σε περίπτωση που ασθενής σε νοσοκομείο δίνει τα στοιχεία του κατά την εισαγωγή του και κρυπτογραφούνται με το δημόσιο κλειδί του γιατρού. Κατόπιν, ο γιατρός τα αποκρυπτογραφεί με το ιδιωτικό κλειδί του. Βέβαια, ο υπεύθυνος προστασίας πρέπει να μεριμνά για την προστασία του κλειδιού κρυπτογράφησης και το κλειδί να υπόκειται σε μέτρα ασφάλειας (όπως για παράδειγμα, να φυλάσσεται το κλειδί εκτός χώρου της εταιρίας ή του φορέα κ.α.)[178]. Σε κάθε περίπτωση, η παράλληλη εφαρμογή και χρήση και των δύο τεχνικών ψευδωνυμοποίησης και κρυπτογράφησης σίγουρα συνιστάται.

Περαιτέρω, ο υπεύθυνος επεξεργασίας καλείται να προσδιορίσει το στοιχεία που πρέπει να κρυπτογραφηθούν, όπως ένας σκληρός δίσκος εν όλω ή εν μέρει, περιορισμένα αρχεία, δεδομένα σε μία βάση δεδομένων ή σε κανάλι επικοινωνίας, να επιλέξει το είδος της κρυπτογράφησης (συμμετρική ή ασύμμετρη), να χρησιμοποιήσει εργαλεία ανάλογα του απαιτούμενου επιπέδου ασφάλειας, εγκεκριμένα και πιστοποιημένα, όπως συστήματα προστασίας ιδιωτικών κλειδιών, μονάδες κρυπτογράφησης και αποκρυπτογράφησης, καθώς επίσης να καθιερώσει μέτρα που να διασφαλίζουν την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των πληροφοριών που είναι αναγκαίες για την ανάκτηση χαμένων μυστικών κωδικών (αντίγραφα ασφαλείας, κωδικοί πρόσβασης διαχειριστή)[179].

Αντίθετα με τα παραπάνω, στην ανωνυμοποίηση[180] γίνεται αφαίρεση των αναγνωριστικών στοιχείων προσωπικού χαρακτήρα σε εγγραφές δεδομένων, έτσι ώστε να μην είναι εφικτό να συσχετιστούν με το υποκείμενο των δεδομένων, με τη χρήση των κατάλληλων τεχνικών.

Η ομάδα εργασίας του άρθρου 29 (WP 29) το 2014[181] επιχείρησε να αναλύσει την αποτελεσματικότητα και τα όρια των τεχνικών ανωνυμοποίησης και κατέληξε στο συμπέρασμα ότι οι τεχνικές αυτές μπορούν να παράσχουν εγγυήσεις για την προστασία

[178] Σιουγλέ Ευφροσύνη, (2019, Νοέμβριος), «Ενίσχυση της ασφάλειας δεδομένων στο ΓΚΠΔ: ψευδωνυμοποίηση και κρυπτογράφηση», Εισήγηση που παρουσιάστηκε στην ημερίδα του ΕΚΔΔΑ «Ασφάλεια Δεδομένων: η εφαρμογή του Γενικού Κανονισμού προστασίας δεδομένων», ανακτήθηκε 08/12/2022 από: https://diavlos.grnet.gr/room/3983?eventid=7007&vod=7194_event.

[179] Βλ. CNIL, Privacy Impact Assessment (PIA) Knowledge Bases, 2018, σελ. 14 επ. και Δ. Τζέλλη. Μ. Μυλώση, Εκτίμηση Αντικτύπου στην προστασία προσωπικών δεδομένων, Εκδ. Νομική Βιβλιοθήκη, 2022, σελ. 213.

[180] Βλ. Αιτιολογική σκέψη αρ. 26 ΓΚΠΔ.

[181] Βλ. Ομάδα εργασίας του άρθρου 29 (WP 29), Γνώμη 05/2014 σχετικά με τις τεχνικές ανωνυμοποίησης.

της ιδιωτικής ζωής, με την προϋπόθεση ότι η εφαρμογή τους έχει σχεδιαστεί με κατάλληλο τρόπο.

Απλά παραδείγματα παρεμπόδισης εξακρίβωσης της ταυτότητας θα μπορούσαν να είναι, αντί της αναφοράς ακριβούς ηλικίας (πχ. 35 ετών), να τεθούν κατηγορίες ηλικίας (πχ. 30-35, 35-40), ή αντί αναφοράς του φύλου θα μπορούσε να σημειωθεί 1 για άντρες και 2 για γυναίκες.

Σύμφωνα με τον Κανονισμό, οι γενικές αρχές προστασίας δεδομένων δεν εφαρμόζονται σε ανώνυμες πληροφορίες. Αντίθετα, τα δεδομένα προσωπικού χαρακτήρα που έχουν υποστεί ψευδωνυμοποίηση, συνεχίζουν να θεωρούνται πληροφορίες και να υπάγονται στο πεδίο εφαρμογής του ΓΚΠΔ. Έτσι, η ανωνυμοποίηση είναι μία καλή επιλογή του υπεύθυνου επεξεργασίας ή του εκτελούντος ώστε να διαφύγει του πεδίου εφαρμογής του ΓΚΠΔ. Ωστόσο, η ανωνυμοποίηση είναι μία μη αναστρέψιμη διαδικασία κι έτσι μπορεί να έχει ως αποτέλεσμα την υποβάθμιση της χρησιμότητας και χρηστικότητας των δεδομένων[182]. Για το λόγο αυτό συνιστάται ο υπεύθυνος επεξεργασίας να καθορίζει ακριβώς τα δεδομένα που πρέπει να ανωνυμοποιηθούν κατά περίπτωση και κατόπιν να φροντίσει ώστε η διαδικασία να γίνει με τρόπο μη αναστρέψιμο και επιλέγοντας ορθά εργαλεία.

Επιπλέον, ιδιαίτερα καλή πρακτική αποτελεί η κατανομή των προσωπικών δεδομένων κάθε επεξεργασίας συγκεκριμένου σκοπού μέσα στο πληροφοριακό σύστημα ενός οργανισμού ή επιχείρησης. Ένας τρόπος δηλαδή πρόληψης και περιορισμού των κινδύνων είναι για κάθε επιχειρησιακή διεργασία να προσδιορίζονται τα απολύτως απαραίτητα για το σκοπό της δεδομένα και να διαχωρίζεται με ασφάλεια η δυνατότητα πρόσβασης και επεξεργασίας μόνο στα άτομα ή τους εργαζόμενους που είναι αρμόδιοι. Αυτό μπορεί να επιτευχθεί με τη λήψη μέτρων ασφαλείας σε επίπεδο ελέγχου πρόσβασης στα πληροφοριακά συστήματα του οργανισμού, όπως για παράδειγμα κεντρική διαχείριση λογαριασμών των χρηστών, μοναδικοί κωδικοί πρόσβασης στους ηλεκτρονικούς υπολογιστές, ανάθεση των δικαιωμάτων των χρηστών στα αρχεία ανάλογα με το ρόλο και την αρμοδιότητά τους και κατάργηση της κοινής χρήσης αρχείων χωρίς έλεγχο. Λόγου χάρη, σε ένα Επιμελητήριο το τμήμα του ΓΕ.ΜΗ. να μην έχει πρόσβαση στα αρχεία του τμήματος του Λογιστηρίου, όπως και το

[182] Βλ. Λουκά Ν., Τεχνικά μέτρα του Γενικού Κανονισμού για την προστασία δεδομένων, Κρυπτογράφηση και Ψευδωνυμοποίηση, Συνήγορος 123/2017, σελ. 48.

τμήμα του Μητρώου ομοίως. Με τον τρόπο αυτό επιτυγχάνεται η μείωση της πιθανότητας συσχέτισης των προσωπικών δεδομένων και ως εκ τούτου σε τυχόν περιστατικό παραβίασης περιορίζεται η ζημία.

Έτσι λοιπόν, ο υπεύθυνος επεξεργασίας καλείται να περιγράψει πώς γίνεται ο λογικός διαχωρισμός των προσωπικών δεδομένων σύμφωνα με τις καθορισμένες αρμοδιότητες και το κάθε επιχειρησιακό τμήμα, να δημιουργήσει ένα ειδικό περιβάλλον πληροφορικής με αυξημένη ασφάλεια για τα συστήματα που επεξεργάζονται ειδικών κατηγοριών δεδομένα και να εφαρμόζει τακτικούς ελέγχους για τη σωστή κατανομή των παραπάνω.

### 5.2.2 Τεχνικά μέτρα ασφάλειας

Επιπλέον των προαναφερόμενων μέτρων, προκειμένου να περιοριστεί σημαντικά η πιθανότητα και η σοβαρότητα ενός αρνητικού αντίκτυπου στην επιχείρηση ή στον οργανισμό ο υπεύθυνος επεξεργασίας περιγράφει και αξιολογεί γενικά μέτρα ασφάλειας στα υποστηρικτικά στοιχεία που χρησιμοποιούνται για τις διεξαγόμενες επεξεργασίες κατά τη λειτουργία του οργανισμού. Κάθε συσκευή και λογισμικό που εντάσσεται στο πληροφοριακό του σύστημα ή επικοινωνεί άμεσα με αυτό πρέπει να εγγυάται ένα επαρκές επίπεδο ασφάλειας. Για το λόγο αυτό, ο υπεύθυνος επεξεργασίας καταγράφει τις διαδικασίες που αφορούν τη λειτουργική ασφάλεια σε έγγραφα, φροντίζει για την επικαιροποίησή τους και την αντίστοιχη ενημέρωση όλων των εμπλεκόμενων χρηστών. Τηρεί έναν ενημερωμένο κατάλογο του λογισμικού και υλισμικού του οργανισμού. Σε αυτά τα αρχεία αποτυπώνει ενδεχομένως, μεταξύ άλλων, τον κωδικό κάθε μηχανήματος εξοπλισμού, τον τύπο, τον σκληρό δίσκο, τη μνήμη, το λειτουργικό, το λογισμικό, την ακριβή θέση που βρίσκεται εντός των εγκαταστάσεων, ποιος χρήστης έχει πρόσβαση σε αυτό κ.α. Ενεργοποιεί συστήματα αυτόματης ενημέρωσης λογισμικού και καταγράφει τις διαδικασίες αυτές. Σε περίπτωση αναβάθμισης λογισμικού αποτιμά την εξάρτησή του από το λειτουργικό σύστημα που χρησιμοποιείται στο αντίστοιχο υλικό. Ελέγχει την εγκατάσταση, τη διαμόρφωση, τη χρήση και τη συντήρηση του εξοπλισμού δίνοντας έμφαση σε ό,τι αφορά στα χαρακτηριστικά ασφάλειας και τις δυνατότητες ασφάλειας. Κατά την εγκατάσταση λογισμικού ελέγχει τη συμμόρφωσή του με καθιερωμένα διεθνή πρότυπα ή διεθνώς διαδεδομένες πρακτικές. Αποτιμά τον κίνδυνο που μπορεί

να προκύψει από ενδεχόμενη δυσλειτουργία του εγκατεστημένου εξοπλισμού. Καθορίζει την πρόσβαση στον εγκατεστημένο εξοπλισμό από αντίστοιχη Πολιτική, το εξουσιοδοτημένο προσωπικό ενημερώνεται σχετικά με κάθε ζήτημα που ανακύπτει, αξιολογεί άμεσα τις σχετικές πληροφορίες και προβαίνει στις κατάλληλες αναβαθμίσεις. Κατά τη διαδικασία διευθυνσιοδότησης εξοπλισμού δεν χρησιμοποιούνται δημοσίως γνωστά δικτυακά αναγνωριστικά (διευθύνσεις IP, hostnames κλπ.). Αποτιμά τις δικτυακές διευθύνσεις, θύρες και πρωτόκολλα με βάση τα οποία δρομολογούνται δεδομένα από έναν δρομολογητή και φροντίζει ώστε η διαχείριση του εξοπλισμού από απόσταση να γίνεται μέσα από ασφαλείς διαύλους επικοινωνίας. Κατά το στάδιο της απεγκατάστασης λογισμικού και εξοπλισμού από τα πληροφοριακά συστήματα διασφαλίζει ότι η πληροφορία που έχει εγγραφεί μόνιμα στον συγκεκριμένο εξοπλισμό - όπως σε μνήμες ROM, σκληρούς δίσκους, μαγνητικές ταινίες – διαγράφεται οριστικά και δεν μπορεί να χρησιμοποιηθεί από τρίτους ώστε να παραβιαστεί η ασφάλεια.

Ακόμη, κατά το στάδιο αυτό, ο υπεύθυνος επεξεργασίας περιγράφει και αξιολογεί τα μέτρα που λαμβάνονται για την διασφάλιση της διαθεσιμότητας, της ακεραιότητας και της εμπιστευτικότητας των προσωπικών δεδομένων μέσα από τη δημιουργία αντιγράφων ασφαλείας. Η δημιουργία αντιγράφων ασφαλείας των αρχείων αποσκοπεί στην προστασία των προσωπικών δεδομένων από τη μόνιμη απώλεια, την αλλαγή τους σε περίπτωση ακούσιας διαγραφής, επίθεσης από κακόβουλο λογισμικό ή σε περίπτωση αστοχίας του λογισμικού ή του υλικού. Ο υπεύθυνος επεξεργασίας λοιπόν καταρτίζει Πολιτικές, εφαρμόζει διαδικασίες και εκτελεί ελέγχους που να διασφαλίζουν ότι ο εξοπλισμός και τα δεδομένα μπορούν να ανακτηθούν μετά από οποιαδήποτε ζημιά. Αντίγραφα μπορεί να λαμβάνονται στα δεδομένα διάρθρωσης των δικτυακών μονάδων, στο λογισμικό συστήματος, στα αρχεία σύνθεσης του λογισμικού, στα αρχεία των βάσεων δεδομένων, στα αρχεία των χρηστών ή στα αρχεία λειτουργίας του οργανισμού. Σε έναν οργανισμό τυχόν καταστροφή μιας μονάδας σκληρού δίσκου, ένα κακόβουλο λογισμικό ή μια φυσική καταστροφή θα μπορούσε στιγμιαία να έχει ως συνέπεια την απώλεια ή διαρροή ευαίσθητων προσωπικών δεδομένων. Έτσι πρέπει να εξασφαλιστεί ότι  λαμβάνονται τακτικά αντίγραφα ασφαλείας των πληροφοριών που επεξεργάζεται ο οργανισμός για τη διασφάλιση ότι η λειτουργία μπορεί να ανακάμψει αποτελεσματικά μετά από κάποια καταστροφή, αποτυχία μέσου ή σφάλμα. Τα αντίγραφα λαμβάνονται βάσει καθορισμένης συχνότητας και εξασφαλίζεται πλήρης

τεκμηρίωση της λήψης εφεδρικών αντιγράφων τα οποία φυλάσσονται σε ασφαλές χώρο εντός ή εκτός των εγκαταστάσεων. Καλή πρακτική συνιστά η εκτέλεση τακτικών ασκήσεων ανάκτησης αποθηκευμένων πληροφοριών για τη διασφάλιση της αξιοπιστίας των μέσων και της διαδικασίας αποθήκευσης. Τα αντίγραφα ασφαλείας καλό είναι να διαθέτουν το ίδιο επίπεδο προστασίας με τα αρχικά στοιχεία, καθώς επίσης, τα εφεδρικά αντίγραφα να αποθηκεύονται με ασφαλή τρόπο σε αρχεία μόνο αναγνώσιμα με τρόπο που τα αποθηκευμένα δεδομένα να μην επιγράφονται ακούσια και να εξασφαλίζεται ότι είναι προσβάσιμα μόνο σε εξουσιοδοτημένο προσωπικό. Επίσης, ένα καλό μοντέλο εφαρμογής αποτελεί η τριπλή τήρηση αρχείων ασφαλείας, δηλαδή η τήρηση κρυπτογραφημένων αντιγράφων στα πληροφορικά συστήματα, στους κεντρικούς διακομιστές και σε απομακρυσμένο διακομιστή (υπηρεσία Cloud) εκτός των εγκαταστάσεων.

Έπειτα, βασικό μέτρο αποτελεί η θέσπιση και περιγραφή διαδικασιών αποτροπής, ανίχνευσης και αντιμετώπισης κακόβουλων λογισμικών έτσι ώστε να εξασφαλίζεται στο μέγιστο δυνατό βαθμό η προστασία των πληροφοριακών συστημάτων και των προσωπικών δεδομένων που διαθέτει και επεξεργάζεται ο οργανισμός. Τα κακόβουλα λογισμικά εξαπλώνονται από έναν η/υ σε έναν άλλο και παρεμβαίνουν στη λειτουργία του. Ένα κακόβουλο λογισμικό μπορεί να καταστρέψει ή να διαγράψει δεδομένα σε έναν η/υ, να χρησιμοποιήσει ένα πρόγραμμα ηλεκτρονικού ταχυδρομείου για να μεταδώσει τον εαυτό του σε άλλους υπολογιστές ή ακόμα να διαγράψει όλα τα αρχεία από τον σκληρό δίσκο. Μερικές από τις καταστροφές που μπορούν να προκαλέσουν είναι η καταστροφή, η υποκλοπή, η παρακολούθηση και καταγραφή ενεργειών του χρήστη ή η υποκλοπή διαβαθμισμένων-απόρρητων πληροφοριών. Όλα τα συστήματα του οργανισμού που είναι ευαίσθητα σε επιθέσεις κακόβουλου λογισμικού, ειδικά αυτά που έχουν πρόσβαση στο διαδίκτυο, συστήνεται να έχουν εγκατεστημένο ένα ολοκληρωμένο λογισμικό ανίχνευσης και αντιμετώπισης κακόβουλων λογισμικών (antivirus). Το λογισμικό αυτό είναι καλό να εγκρίνεται από την ομάδα αντιμετώπισης κακόβουλου λογισμικού που απαρτίζεται από τον υπεύθυνο ασφαλείας, τον υπεύθυνο πληροφοριακών συστημάτων, τον υπεύθυνο πρόσβασης και τον υπεύθυνο αντιγράφων ασφαλείας. Το απαραίτητο λογισμικό εφαρμόζεται σε όλες τις υπηρεσίες, εφαρμογές και εισερχόμενα δεδομένα που διαχειρίζεται ο χρήστης. Τα antivirus συστήνεται να παρέχουν προστασία από κάθε

είδους κακόβουλου λογισμικού (όπως worms, trojan, rootkits, spyware και adware), να είναι ρυθμισμένα να ελέγχουν τη μνήμη του η/υ, τα εκτελέσιμα αρχεία, τα προστατευμένα και κρυφά αρχεία, τα αφαιρούμενα μέσα αποθήκευσης (CDs, DVDs, USB συσκευές), την εισερχόμενη και εξερχόμενη δικτυακή κίνηση του οργανισμού, να είναι ρυθμισμένα να πραγματοποιούν ελέγχους (σαρώσεις) σε πραγματικό χρόνο και όχι μετά από απαίτηση του χρήστη, να έχουν τη δυνατότητα να απομονώνουν το ύποπτο λογισμικό για περαιτέρω ανάλυση και να διαθέτουν μηχανισμό ειδοποίησης στην περίπτωση που είναι ανενεργά. Η εγκατάσταση του λογισμικού καλό είναι να μην επιτρέπεται από οποιονδήποτε χρήστη αλλά μόνο από τον υπεύθυνο πληροφοριακών συστημάτων. Επίσης, σωστό είναι να μην επιτρέπεται το άμεσο μοίρασμα σκληρών δίσκων με read/write δικαιώματα εάν αυτό δεν είναι απαραίτητο για τη διεκπεραίωση κάποιας συγκεκριμένης εργασίας. Συστήνεται να ενσωματώνονται μηχανισμοί προγραμματισμένης και αυτοματοποιημένης ενημέρωσης για προσθήκες και βελτιώσεις. Σημαντικό επίσης είναι να προβλέπεται σε Πολιτικές του οργανισμού ότι οι χρήστες των πληροφοριακών συστημάτων οφείλουν να ενημερώνουν άμεσα την ομάδα αντιμετώπισης κακόβουλου λογισμικού σε περίπτωση που διαπιστώσουν κάποια περίεργη ή ασυνήθιστη συμπεριφορά μηχανήματος που χειρίζονται, να προβλέπεται ακόμη στην Πολιτική κατάρτιση σχετικών αναφορών αντιμετώπισης περιστατικών και παράδοση της αναφοράς στον υπεύθυνο ασφαλείας ώστε να πραγματοποιούνται κατόπιν κατάλληλες διορθωτικές αλλαγές και προσθήκες στην ασφάλεια των πληροφοριακών συστημάτων.

Στην ίδια κατεύθυνση, ο υπεύθυνος επεξεργασίας διασφαλίζει τη λειτουργία των σταθμών εργασίας με κάθε τρόπο που μειώνει την πιθανότητα παραβίασης των προσωπικών δεδομένων και περιγράφει τα μέτρα που εφαρμόζονται ομοίως. Τέτοια μέτρα είναι η διασφάλιση αυτόματης αποσύνδεσης του χρήστη (log out) σε αδρανοποιημένο υπολογιστή, η εξασφάλιση ενεργοποιημένου τοίχους προστασίας, λειτουργίας κωδικού πρόσβασης για την είσοδο στο σύστημα, ενεργοποίησης περιορισμών πρόσβασης σε εφαρμογές. Ακόμη, ιδιαίτερα σημαντική είναι η λήψη μέτρων προστασίας και σε μικρότερους σταθμούς εργασίας, όπως οι φορητοί υπολογιστές, που είναι ευπρόσβλητοι σε κλοπές, ο εξοπλισμός με κλειδαριά καλωδίου ασφαλείας σε περίπτωση μη εποπτευόμενου χώρου. Καλή πρακτική αποτελεί η ανάκτηση των δεδομένων που είναι απαραίτητα από τον σταθμό εργασίας προτού

ανατεθεί σε άλλο άτομο, η διαγραφή τους από τον σταθμό εργασίας όταν πρόκειται να ανατεθούν σε άλλο άτομο ή να τεθούν σε λειτουργία κοινής χρήσης, ή η διαγραφή των δεδομένων που έχουν προσωρινά αποθηκευτεί στον σταθμό εργασίας πριν τη σύνδεση σε αυτόν από επόμενο χρήστη.

Επιπλέον, ο υπεύθυνος επεξεργασίας φροντίζει ώστε ο ιστότοπος που διατηρεί να συγκεντρώνει τα χαρακτηριστικά εκείνα που να μειώνουν τον κίνδυνο παραβίασης των προσωπικών δεδομένων στο ελάχιστο δυνατό[183]. Για το σκοπό αυτό συνιστάται κρυπτογράφηση της κίνησης δικτύου με πρωτόκολλο TLS, στο ιστολόγιο να χρησιμοποιείται επιπλέον όνομα τομέα το οποίο να έχει πιστοποίηση SSL για προστασία και κρυπτογράφηση των δεδομένων του επισκέπτη, να τίθενται στη διάθεση του επισκέπτη κείμενα για την Πολιτική Απορρήτου, την Πολιτική για τα Cookies και την Πολιτική Ασφάλειας.

Περαιτέρω, κατά την πραγματοποίηση εργασιών συντήρησης του υλισμικού και λογισμικού συνιστάται υπευθυνότητα, καταγραφή του τρόπου περάτωσης της φυσικής συντήρησης του hardware, του τρόπου που αυτή ανατίθεται σε εξωτερικούς συνεργάτες, καθώς και περιγραφή εάν εξουσιοδοτείται η απομακρυσμένη συντήρηση των εφαρμογών (apps) και με ποιους όρους.

Ιδιαίτερη βαρύτητα δίνεται στα μέτρα φυσικής ασφάλειας που λαμβάνει ο υπεύθυνος επεξεργασίας. Σημαντικό μέρος αυτής αποτελεί ο έλεγχος φυσικής πρόσβασης σε εγκαταστάσεις, εξοπλισμό δικτύου και computer room, δηλαδή να υπάρχουν τα κατάλληλα μέτρα ελέγχου φυσικής πρόσβασης στους χώρους του φυσικού εξοπλισμού (τηλεπικοινωνιακή και δικτυακή καλωδίωση), ώστε να επιτρέπεται η πρόσβαση μόνο σε εξουσιοδοτημένα πρόσωπα, οι εγκαταστάσεις του computer room να προστατεύονται από συστήματα συναγερμού και από κλειστό κύκλωμα παρακολούθησης CCTV και να διατηρείται επικαιροποιημένος κατάλογος με τα δικαιώματα φυσικής πρόσβασης του προσωπικού, καθώς και με το προσωπικό που διαθέτει κλειδιά για πρόσβαση σε κρίσιμους χώρους. Επίσης εφιστάται η προσοχή στη λήψη μέτρων περιβαλλοντικής ασφάλειας, δηλαδή μέτρων για την προστασία των κτιρίων και των κρίσιμων χώρων γραφείων, εξοπλισμών, computer room από

[183] Η Γαλλική Αρχή CNIL παραπέμπει στην εφαρμογή των «Συστάσεων για την ασφάλεια των ιστοτόπων» της ANSSI, σε https://www.ssi.gouv.fr/uploads/IMG/pdf/NP_Securite_Web_NoteTech.pdf

πλημμύρα, υπερθέρμανση, πυρκαγιά, διαρροή νερού, διακοπή ρεύματος, διάρρηξη/κλοπή κ.α., με ενδεικτικά μέτρα όπως τοποθέτηση συναγερμού με κωδικό, πόρτες και παράθυρα ασφαλείας, εξασφάλιση της ασφάλειας των κλειδιών, απομάκρυνση εξοπλισμού από υγρασία, εγκατάσταση ανιχνευτών καπνού και πόρων πυρόσβεσης με παράλληλο περιοδικό έλεγχό τους. Ακολούθως, η προστασία έγχαρτων εγγράφων με ειδικές επισημάνσεις επάνω τους, προστασία κατά τη διακίνησή τους, χρήση καταστροφέων, τοποθέτησή τους σε φωριαμούς, καταγραφή μεταφοράς φακέλων σε διαφορετικές οργανωτικές μονάδες, καθαρά γραφεία δίχως εκτεθειμένα έγγραφα. Ακόμη, η προστασία φορητών μέσων αποθήκευση, δηλαδή να φυλάσσονται σε ασφαλή σημεία όταν δεν είναι σε χρήση και να είναι πάντα υπό επίβλεψη.

### 5.2.3 Οργανωτικά μέτρα ασφάλειας

Ταυτόχρονα με όλα τα παραπάνω, ο υπεύθυνος επεξεργασίας φροντίζει να αναπτύσσει κατάλληλη διοικητική δομή και επαρκή βαθμό οργάνωσης στο εσωτερικό του οργανισμού του με στόχο να διαχειρίζεται και ελέγχει την προστασία των προσωπικών δεδομένων που επεξεργάζεται. Ορίζει τους ρόλους που είναι απαραίτητοι για τη διαχείριση της ασφάλειας, καθορίζει αρμοδιότητες για κάθε ρόλο και αναθέτει ρόλους στα κατάλληλα άτομα. Ενσωματώνει -εάν δεν έχει- στο οργανόγραμμα του οργανισμού του νέους ρόλους που σχετίζονται με την ασφάλεια της επεξεργασίας των προσωπικών δεδομένων, όπως του υπεύθυνου προστασίας προσωπικών δεδομένων, του υπεύθυνου ασφαλείας, του υπεύθυνου αντιγράφων ασφαλείας, του υπεύθυνου πρόσβασης, του υπεύθυνου ασφάλειας δικτύων και του υπεύθυνου πληροφοριακών συστημάτων.

Καθορίζει τους οργανωτικούς ρόλους για συγκεκριμένες εργασίες εντός του οργανισμού και συνδέει το προσωπικό με τους αντίστοιχους ρόλους. Υπάρχει σαφής διαχωρισμός και ανάθεση καθηκόντων και αρμοδιοτήτων σε κάθε ρόλο. Οι ρόλοι ανατίθενται επίσημα, εγγράφως. Οι εργαζόμενοι έχουν δικαίωμα πρόσβασης μόνο στα απολύτως απαραίτητα δεδομένα προσωπικού χαρακτήρα, βάσει των αρμοδιοτήτων και καθηκόντων που τους έχουν ανατεθεί και υπαγορεύονται από το ρόλο τους. Προβλέπονται διαδικασίες για περιοδική επανεξέταση και αναθεώρηση των εξουσιοδοτήσεων και δικαιωμάτων πρόσβασης μετά από μετακίνηση ενός εργαζομένου ή αλλαγή στα καθήκοντά του. Προβλέπονται ειδικότερες διαδικασίες για

την περίπτωση αποχώρησης ενός εργαζομένου, οι οποίες περιλαμβάνουν κατάργηση των λογαριασμών πρόσβασης, των εξουσιοδοτήσεων, των κωδικών-συνθηματικών του που καθίστανται ανενεργοί, κατάργηση των λογαριασμών ηλεκτρονικού ταχυδρομείου, επιστροφή τυχόν παρασχεθέντος εξοπλισμού ή αποσπώμενων μέσων και αντίστροφα στην περίπτωση πρόσληψης.

Καταρτίζει και εφαρμόζει διαδικασία τήρησης μητρώου πληροφοριακών συστημάτων και πόρων που ανήκουν στον οργανισμό. Καταρτίζει και εφαρμόζει Πολιτική διαχείρισης και εγκατάστασης Λογισμικού και Υλικού. Ενσωματώνει μηχανισμούς διαβάθμισης των δεδομένων που επεξεργάζεται σύμφωνα με το είδος και την κρισιμότητά τους (όπως δεδομένα προσωπικού χαρακτήρα ή μη, ειδικών ή απλών κατηγοριών) και προβλέπει συγκεκριμένες διαδικασίες διαχείρισής τους με βάση τη διαβάθμιση αυτή. Το φυσικό αρχείο που εμπεριέχει ευαίσθητα προσωπικά δεδομένα αρχειοθετείται σε ειδικό φάκελο με ειδική ένδειξη. Η μεταφορά ή η καταστροφή του φυσικού αρχείου διενεργείται σε συνεργασία με τον υπεύθυνο ασφαλείας και καταγράφεται σε ειδικό μητρώο καταγραφής προσωπικών δεδομένων ειδικών κατηγοριών.

Το προσωπικό του οργανισμού (υφιστάμενοι και νέοι) που εμπλέκονται στις επεξεργασίες προσωπικών δεδομένων εκπαιδεύονται στα θέματα ασφάλειας, λαμβάνουν γνώση των Πολιτικών ασφαλείας, των επιμέρους πολιτικών και των σχετικών Διαδικασιών και αποδέχονται όλα αυτά θέτοντας την υπογραφή τους στα αντίστοιχα έντυπα.

Τηρείται κατάλογος με τα στοιχεία όλων των εκτελούντων την επεξεργασία που χειρίζονται προσωπικά δεδομένα για λογαριασμό του υπεύθυνου επεξεργασίας είτε εντός είτε εκτός των εγκαταστάσεών του. Η ανάθεση της επεξεργασίας προς αυτούς γίνεται οπωσδήποτε εγγράφως και προβλέπονται όλοι οι όροι διεξαγωγής της επεξεργασίας καθώς και οι υποχρεώσεις που βαρύνουν εκατέρωθεν τα μέρη.

Καταρτίζεται και εφαρμόζεται διαδικασία διαχείρισης συμβάντων παραβίασης-διαρροής προσωπικών δεδομένων. Σε περίπτωση που συμβεί περιστατικό παραβίασης ο υπεύθυνος επεξεργασίας προβαίνει σε εμπεριστατωμένη ανάλυση των συμβάντων και αιτίων της παραβίασης προτείνοντας παράλληλα τα κατάλληλα αντίμετρα. Συμπληρώνεται η αναφορά παραβίασης προσωπικών δεδομένων και αξιολογείται η σπουδαιότητα του περιστατικού. Εάν κριθεί ότι το περιστατικό ενδέχεται να

προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ακολουθεί γνωστοποίηση του περιστατικού στην Αρχή προστασίας δεδομένων προσωπικού χαρακτήρα. Το περιστατικό καταγράφεται στο μητρώο παραβιάσεων προσωπικών δεδομένων και σημειώνονται πληροφορίες που αφορούν την ημερομηνία και ώρα της παραβίασης, περιγραφή του περιστατικού, ημερομηνία που κοινοποιήθηκε η παραβίαση στην Εποπτική Αρχή, ο χρόνος που παρήλθε έως την κοινοποίηση, οι πιθανές συνέπειες για τα υποκείμενα των δεδομένων, καθώς και οι διορθωτικές ενέργειες.

Παράλληλα με τα παραπάνω, είναι ιδιαίτερα σημαντικό να εφαρμόζονται μηχανισμοί ελέγχου και την παρακολούθησης της αποτελεσματικότητας και της επάρκειας των μέτρων ιδιωτικότητας που λαμβάνονται στον οργανισμό. Όσο πιο αποτελεσματικά μέτρα ασφάλειας και ιδιωτικότητας εφαρμόζονται εντός του οργανισμού, τόσο πιο έγκαιρα μπορούν να ανιχνευτούν περιστατικά που απαιτούν διαχείριση. Για το λόγο αυτό ο υπεύθυνος επεξεργασίας, ήδη από τα στάδια του σχεδιασμού, ενσωματώνει στην ανάπτυξη του λογισμικού του πρακτικές ιδιωτικότητας ώστε να διασφαλίζει στα υποκείμενα των δεδομένων καλύτερο επίπεδο ελέγχου στα δεδομένα τους, περιορισμό των σφαλμάτων και ανακριβειών, περιορισμό της μη εξουσιοδοτημένης πρόσβασης σε αυτά και της λανθασμένης χρήσης τους. Αυτά μπορούν να επιτευχθούν με την τήρηση κατάλληλων καταγραφών, αρχείου συμβάντων ασφαλείας με συγκεκριμένες αναφορές στο χρονικό σημείο του συμβάντος, με ομαδοποίηση των αρχείων καταγραφής σε διαφορετικά διακριτά συστήματα συλλογής, με την πρόβλεψη δυνατότητα εξαγωγής των αρχείων αυτών, την εξασφάλιση επαρκούς αποθηκευτικού χώρου για αντίστοιχο όγκο αρχείων, της συμβατότητας των μορφών δεδομένων ανάλογα με το χρόνο διατήρησης, λήψη μέτρων για την εξασφάλιση του απορρήτου και της εμπιστευτικότητας, γρήγορη ανωνυμοποίηση, ανάπτυξη μορφών κατά τη συλλογή των δεδομένων που να ελαχιστοποιούν τον όγκο συλλογής τους και βέβαια με τακτές αναλύσεις των καταγεγραμμένων πληροφοριών ώστε να αξιολογούνται οι ευπάθειες και οι πιθανοί κίνδυνοι[184].

[184]Βλ. CNIL, Privacy Impact Assessment (PIA) Knowledge Bases, 2018, σελ. 82 επ. και Δ. Τζέλλη. Μ. Μυλώση, Εκτίμηση Αντικτύπου στην προστασία προσωπικών δεδομένων, Εκδ. Νομική Βιβλιοθήκη, 2022, σελ. 231επ.

## 5.3 Περιπτωσιολογία και Νομολογιακή Επισκόπηση

Τα περιστατικά απειλών και κινδύνων ασφάλειας των δεδομένων και των πληροφοριακών συστημάτων μιας επιχείρησης ή ενός οργανισμού είναι καθημερινά και πλέον μόνο αυξάνονται[185]. Παράδειγμα παραβίασης της αρχής της εμπιστευτικότητας αποτελεί το περιστατικό ασφάλειας τον Φεβρουάριο του 2017 στην αλυσίδα καταστημάτων fast food της Arby με διαρροή στοιχείων περίπου 355.000 πιστωτικών και χρεωστικών καρτών πελατών της όταν κακόβουλο λογισμικό εγκαταστάθηκε σε συστήματα καρτών πληρωμής σε πολλές τοποθεσίες των εστιατορίων της[186].

Τον Μάρτιο του 2020 στην εταιρία Interserve έλαβε χώρα κυβερνοεπίθεση που επηρέασε το απόρρητο και τη διαθεσιμότητα 113.000 προσωπικών δεδομένων εργαζομένων της λόγω ευπαθειών στα συστήματα ασφαλείας τους που επέτρεψαν την παράνομη πρόσβαση σε πληροφορίες όπως αριθμούς τηλεφώνων, διευθύνσεις email, στοιχεία τραπεζικών λογαριασμών, αριθμό ασφάλισης, οικογενειακή κατάσταση, ημερομηνία γέννησης, εκπαίδευση, μισθό, πληροφορίες για την υγεία[187].

Από τις πιο επικίνδυνες περιπτώσεις αποτελούν οι ιοί τύπου ransomware, οι οποίοι κρυπτογραφούν αρχεία και μετά εκβιάζουν τα θύματα να πληρώσουν «λύτρα» προκειμένου να τους χορηγήσουν το κλειδί αποκρυπτογράφησης. Στις περιπτώσεις αυτές, εάν υπάρχει αντίγραφο ασφαλείας, μπορεί ο χρήστης να επαναφέρει τα δεδομένα, εάν δεν υπάρχει εξαναγκάζεται να πληρώσει τα χρήματα[188]. Τέτοιο περιστατικό αντιμετώπισε το καλοκαίρι του 2021 ο Δήμος Θεσσαλονίκης όταν αρχεία από το εσωτερικό του δίκτυο που συμπεριελάμβαναν ονόματα και στοιχεία μισθοδοσίας, έγιναν στόχος μετά από επίθεση ransomware και οι δράστες ζητούσαν λύτρα για να ξεκλειδώσουν αρχεία[189]. Τέτοια περιστατικά εμπεριέχουν παραβιάσεις τόσο σε επίπεδο εμπιστευτικότητας, όταν τα αρχεία όχι μόνο κρυπτογραφούνται αλλά και υποκλέπτονται από τον ιό, όσο και σε απώλεια διαθεσιμότητας, εφόσον οι κρυπτογραφημένες πληροφορίες δεν είναι διαθέσιμες προς χρήση, αλλά και σε επίπεδο

[185] The 15 data breaches of the 21st century, σε https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

[186] Βλ. Cyber Security Case Studies, σε https://www.cybersecuritycasestudies.com/library/data-breach-of-customer-credit-card-data .

[187] https://www.theguardian.com/business/2022/oct/24/outsourcer-interserve-fined-4-point-4m-cyber-attack-failings-data-breach-personal-information

[188] Βλ. Λ. Κοτσαλή, Προσωπικά Δεδομένα, Ανάλυση-Σχόλια-Εφαρμογή, εκδ. Νομ. Βιβλιοθήκη 2016, σελ. 384επ.

[189] https://www.kathimerini.gr/society/561442918/kyvernoepithesi-ston-dimo-thessalonikis-kleidosan-archeia-toy-esoterikoy-diktyoy-zitontas-lytra/

ακεραιότητας, εφόσον από το συμβάν θα μπορούσε να επέλθει αλλοίωση των δεδομένων λόγω του ιού.

Από πλευράς νομολογίας της Εποπτικής Αρχής μας ιδιαίτερης σημασίας είναι η με αριθμό 4/2022 απόφαση ΑΠΔΠΧ[190] τόσο για τα ζητήματα ασφάλειας που αναδύονται όσο και για την αυστηρότητα σε επίπεδο προστίμου με την οποία τα αντιμετώπισε η Αρχή. Στην υπό κρίση περίπτωση έλαβε χώρα περιστατικό παραβίασης προσωπικών δεδομένων συνδρομητών της εταιρείας Cosmote όταν αρχείο προσωπικών δεδομένων που περιελάμβανε μεταξύ άλλων (τηλεφωνικούς αριθμούς, διάρκεια κλήσης, ένδειξη παρόχου, ηλικία, φύλο, είδος προγράμματος) και δεδομένα κίνησης, όπως συντεταγμένες σταθμών βάσης, διέρρευσε προς άγνωστους τρίτους το 2020 λόγω επιτυχούς επίθεσης ασφαλείας που πραγματοποιήθηκε. Μετά τη διερεύνηση της υπόθεσης από την ελληνική Εποπτική Αρχή προέκυψαν πλήθος παραβιάσεων μεταξύ των οποίων -πλην των παραβιάσεων της αρχής της νομιμότητας, της διαφάνειας, της ελλιπούς ενημέρωσης- υπήρξαν και παραβιάσεις λόγω ελλιπών μέτρων ασφάλειας αλλά και πλημμελούς διεξαγωγής της μελέτης εκτίμησης αντικτύπου. Διαπιστώθηκαν ευπάθειες στα μέτρα ασφάλειας, τις οποίες αξιοποίησε ο επιτιθέμενος για να πετύχει το σκοπό του. Ειδικότερα, στο επίπεδο αυτό υπέχουν ευθύνη τόσο η εταιρεία της Cosmote όσο και του ΟΤΕ καθόσον οι δύο εταιρείες επικαλούνταν ότι δρούσαν από κοινού ως προς τα συστήματά τους αλλά ανεξάρτητα κατά τα λοιπά, ενώ σε αντίθεση με την αρχή της λογοδοσίας, δεν υπήρχε πουθενά καταγεγραμμένη η μεταξύ τους συμφωνία, ούτε σαφής κατανομή των αρμοδιοτήτων καθεμιάς από αυτές, ούτε διαχωρισμός της ευθύνης της καθεμίας για την επιλογή των απαραίτητων μέσω επεξεργασίας. Η Αρχή επισήμανε τη σπουδαιότητα του να βασίζεται η συνεργασία των φορέων και η κατανομή των μεταξύ τους ρόλων είτε σε γραπτή συμφωνία, όπως προβλέπεται για τους από κοινού υπεύθυνους επεξεργασίας στο άρθρο 26 του ΓΚΠΔ, είτε σε σύμβαση, είτε σε άλλη νομική πράξη ανάθεσης επεξεργασίας, ως μέτρο ασφάλειας, κάτι που στην εν λόγω περίπτωση δεν συνέβαινε (σκ. 21-22). Ακόμη, προέκυψε κατά την έρευνα της υπόθεσης ότι δεδομένα που έπρεπε να είναι ανωνυμοποιημένα για το σκοπό της επεξεργασίας τους ήταν τελικά μόνο ψευδωνυμοποιημένα σύμφωνα με τη διαδικασία που τηρούνταν κι ως εκ τούτου

190 https://www.dpa.gr/el/enimerwtiko/prakseisArxis/epiboli-prostimoy-gia-peristatiko-parabiasis-prosopikon-dedomenon-kai-mi

η εφαρμοζόμενη διαδικασία ανωνυμοποίησης του αρχείου δεν διασφάλιζε τελικά την ανωνυμία των τηρούμενων δεδομένων παρά μόνο την τήρησή τους σε ψευδωνυμοποιημένη μορφή, ενώ επιπρόσθετα δεν υπήρξε ούτε ενημέρωση προς τα υποκείμενα των δεδομένων για αυτή την επεξεργασία που πραγματοποιούνταν (σκ. 19). Παράλληλα, η Αρχή διαπίστωσε ότι η εκπόνηση της εκτίμησης αντικτύπου από την Cosmote δεν έγινε με ορθό τρόπο καθώς οι απαντήσεις που παρείχε η Cosmote ως υπεύθυνη επεξεργασίας ήταν αναιτιολόγητες και δεν έπειθαν ότι είχε προηγηθεί εκτίμηση και αξιολόγηση των κινδύνων και των ευπαθειών του οργανισμού, ούτε παρείχε στοιχεία για την εκτίμηση της αναγκαιότητας και αναλογικότητας των πράξεων επεξεργασίας σε σχέση με τους σκοπούς που υπηρετούν (σκ. 16). Για τους λόγους αυτούς, η Αρχή διαπίστωσε παράβαση του άρθρου 35 παρ. 7 του ΓΚΠΔ διότι το περιεχόμενο της εκτίμησης αντικτύπου δεν ήταν επαρκές, αιτιολογημένο και τεκμηριωμένο κατά τις αρχές της αναγκαιότητας και αναλογικότητας. Για το σύνολο των διαπιστωμένων παραβάσεων η Αρχή επέβαλε στην Cosmote πρόστιμο ύψους 5.850.000 ευρώ και στον ΟΤΕ ύψους 3.250.000 ευρώ, κατόπιν αυστηρής κρίσης της.

Η ΑΠΔΠΧ με την με αριθμό 44/2019 απόφασή της έκρινε ότι υπήρξε παραβίαση των αρχών της ασφαλούς επεξεργασίας, κυρίως της αρχής της εμπιστευτικότητας, σε υπόθεση κατά την οποία η εταιρεία ABS, θυγατρική της μητρικής AMPNI, υποστήριξε ότι υπήρξε από τη δεύτερη παράνομη αντιγραφή του συνόλου του περιεχομένου του διακομιστή της πρώτης, λόγω απουσίας των κατάλληλων τεχνικών και οργανωτικών μέτρων και ότι με τον τρόπο αυτό η AMPNI επεξεργάστηκε δεδομένα προσωπικού χαρακτήρα σε υπολογιστική υποδομή (υλικού και λογισμικού-διακομιστή) κατά παράβαση των αρχών του ΓΚΠΔ και ιδιαίτερα χωρίς τη λήψη μέτρων που αφορούν τον φυσικό και λογικό διαχωρισμό υλικού και λογισμικού. Συγκεκριμένα, η εταιρεία ABS ισχυρίστηκε ότι άτομα από τις εταιρείες AMPNI και ΕΥ ΕΛΛΑΣ εισήλθαν παράνομα στο χώρο του data room της και χωρίς νόμιμο δικαίωμα αντέγραψαν σε φορητά μέσα αποθήκευσης το σύνολο του περιεχομένου του διακομιστή της που περιείχε προσωπικά δεδομένα εργαζομένων και τρίτων δημιουργώντας έτσι ένα «κλωνοποιημένο» νέο αρχείο από αντιγραφή του πρωτοτύπου. Στην πολύ ενδιαφέρουσα αυτή υπόθεση η Αρχή πραγματεύτηκε πολλά ζητήματα, μεταξύ των οποίων και το τί συμβαίνει όταν εταιρείες που ανήκουν στον ίδιο Όμιλο ή και τρίτες εκτός του Ομίλου, χρησιμοποιούν την ίδια υπολογιστική υποδομή (υλικού και

λογισμικού) για τη διεκπεραίωση των emails των εργαζομένων και στελεχών τους. Η Αρχή έκρινε στην υπό κρίση περίπτωση ότι κατ' αρχήν η μητρική εταιρεία, η θυγατρικές εντός του Ομίλου της αλλά και τρίτες εταιρείες εκτός Ομίλου, έκαναν χρήση και είχαν φυσική πρόσβαση στον ίδιο περιβάλλοντα χώρο που ήταν εγκατεστημένοι και λειτουργούσαν οι διακομιστές όλων των εταιρειών και επίσης διαπίστωσε ότι υπήρχε φυσική και λογική πρόσβαση στην ίδια υπολογιστική υποδομή για τη διεκπεραίωση της ηλεκτρονικής αλληλογραφίας των εργαζομένων και στελεχών τους προβαίνοντας σε επεξεργασία των συστημάτων αρχειοθέτησης ηλεκτρονικών επικοινωνιών. Ωστόσο, έκρινε ότι αυτές οι προσβάσεις και επεξεργασίες πραγματοποιούνταν χωρίς τη λήψη μέτρων για τον φυσικό και λογικό διαχωρισμό τους, χωρίς την σύναψη τυπικών συμβάσεων αδειοδότησης και παροχής υπηρεσιών με την εταιρεία του λογισμικού τους και χωρίς ύπαρξη συμφωνιών φιλοξενίας και παροχής υπηρεσιών μεταξύ των εταιρειών εντός και εκτός Ομίλου και γενικά χωρίς την λήψη τεχνικών και οργανωτικών μέτρων εσωτερικής συμμόρφωσης κατά τον ΓΚΠΔ, με αποτέλεσμα να δημιουργούνται πλείστα ζητήματα περί ιδιοκτησίας των δεδομένων προσωπικού χαρακτήρα και όχι μόνο. Τονίζεται επιτακτικά ότι αποτελεί παραβίαση της αρχής της εμπιστευτικότητας η μη εξουσιοδοτημένη πρόσβαση σε προσωπικά δεδομένα, καθώς επίσης ότι η αρχή της λογοδοσίας επιτάσσει μεταξύ άλλων την εφαρμογή κατάλληλων εγγράφων πολιτικών. Η Αρχή με την απόφασή της αυτή επέβαλλε χρηματικό διοικητικό πρόστιμο στην AMPNI και επιπλέον διέταξε τη λήψη όλων των αναγκαίων μέτρων εσωτερικής συμμόρφωσης και λογοδοσίας.

Επίσης, ιδιαίτερα άξια αναφοράς και σχολιασμού είναι η στάση της Εποπτικής μας Αρχής στο ζήτημα της διερεύνησης της συμβατότητας της σύγχρονης εξ αποστάσεως εκπαίδευσης στις σχολικές μονάδες της πρωτοβάθμιας και δευτεροβάθμιας εκπαίδευσης κατά τις διατάξεις του ΓΚΠΔ και του ν. 4624/2019, μετά τις απρόοπτες και πρωτοφανείς συνθήκες που επιβλήθηκαν με την εμφάνιση της πανδημίας. Μετά από αναφορές της Ομοσπονδίας Ιδιωτικών Εκπαιδευτικών Λειτουργών Ελλάδος και της Διδασκαλικής Ομοσπονδίας Ελλάδος σε βάρος του Υπουργείου Παιδείας και Θρησκευμάτων (Υ.ΠΑΙ.Θ), ζητήθηκε η παρέμβαση της Αρχής επί του θέματος, η οποία εν συνεχεία εξέδωσε κατ' αρχήν την με αριθμό 4/2020

Γνωμοδότηση[191], στην οποία αναλύονται και διερευνώνται σημαντικά ζητήματα νομιμότητας της επεξεργασίας ή όχι και αποτίμησης της ήδη τότε διενεργηθείσας ΕΑΠΔ από το Υ.ΠΑΙ.Θ. Αρχικά, κρίθηκε νόμιμη η επεξεργασία την οποία συνεπάγεται η παροχή σύγχρονης εξ αποστάσεως εκπαίδευσης, ερειδόμενη στη βάση της συμμόρφωσης με έννομη υποχρέωση και της εκπλήρωσης καθήκοντος που εκτελείται προς το έννομο συμφέρον και κατόπιν επισημάνθηκαν αναλυτικά και τεκμηριωμένα ελλείψεις στην τότε εκπονηθείσα ΕΑΠΔ, της οποίας η τροποποίηση και συμπλήρωση κρίθηκε επιτακτική. Ειδικότερα, η Αρχή επισήμανε σφάλμα της ΕΑΠΔ ως προς την κρίση σε σχέση με την αναλογικότητα του μέτρου στην περίπτωση της «ταυτόχρονης» μετάδοσης του μαθήματος της σχολικής αίθουσας σε μαθητές που απουσιάζουν. Κρίθηκε ότι αποτελεί σημαντικό παράγοντα που δεν αξιολογήθηκε ορθά από την ΕΑΠΔ, ενώ ενδέχεται να επηρεάζει σε σημαντικό βαθμό την κρίση για την αναγκαιότητα και την αναλογικότητα της επεξεργασίας το γεγονός της επέμβασης στο δικαίωμα της εκπαίδευσης των μαθητών που βρίσκονται εντός της αίθουσας, εξαιτίας της μετάδοσης του μαθήματος στους μαθητές που απουσιάζουν. Επισημάνθηκε ότι θα πρέπει επιπρόσθετα να συνυπολογίζεται η διαφοροποίηση των αναγκών και των συνθηκών ανά βαθμίδα εκπαίδευσης και ως εκ τούτου απαιτείται μελέτη περισσότερων εναλλακτικών λύσεων και μεθόδων και προσδιορισμός ειδικών μέτρων και τεχνικών που να ελαχιστοποιούν τις επιπτώσεις στα δικαιώματα των υποκειμένων των δεδομένων, προσαρμοσμένων ανά ηλικιακή ομάδα. Επιπλέον, επισήμανε η Αρχή ότι εσφαλμένα δεν ζητήθηκε για την υλοποίηση της ΕΑΠΔ η γνώμη των υποκειμένων των δεδομένων ή των εκπροσώπων τους για τη σχεδιαζόμενη επεξεργασία. Τονίστηκε ότι η επεξεργασία αφορά μεγάλο αριθμό ευάλωτων υποκειμένων (μαθητών και εργαζομένων) ενώ, έμμεσα ή άμεσα, επηρεάζεται και το οικογενειακό περιβάλλον των μαθητών. Τα επηρεαζόμενα δικαιώματα συνδέονται όχι μόνο με την προστασία των προσωπικών δεδομένων, αλλά και με την εκπαίδευση και την υγεία. Συνεπώς, ο υπεύθυνος επεξεργασίας που προτίθεται να εισάγει μία καινοφανή λύση, όπως της «ταυτόχρονης» τηλεκπαίδευσης, οφείλει να ακολουθεί συστηματική προσέγγιση ως προς τον εντοπισμό και την αντιμετώπιση των κινδύνων και τέτοια αποτελεί η εμπλοκή

[191] Βλ. Υπ' αρ. 4/2020 Γνωμοδότηση της Αρχής, https://www.dpa.gr/el/enimerwtiko/prakseisArxis?field_year_from=2020&field_year_to=2020&field_category=238&field_thematic=All&field_protocol_number=4&field_keywords=.

των υποκειμένων των δεδομένων που επηρεάζονται άμεσα ή έμμεσα, καθώς και των κατάλληλων εμπειρογνωμόνων (όπως ακαδημαϊκών φορέων, δημόσιων φορέων εκπαιδευτικής πολιτικής). Περαιτέρω, σημειώθηκαν αστοχίες και παραλείψεις της ΕΑΠΔ, όπως ότι δεν αποδεικνύεται ο χρόνος εκπόνησης και ολοκλήρωσης της ΕΑΠΔ, ενώ θα έπρεπε, καθώς επίσης και ότι δεν προκύπτει με ποιο τρόπο έχει εφαρμοστεί η μεθοδολογία της μελέτης, ποια άτομα και με ποιο τρόπο έχουν εμπλακεί στην εκπόνησή της. Επιπλέον, τονίζεται ότι υπάρχουν ελλείψεις ως προς την ανάλυση των χαρακτηριστικών της επεξεργασίας, τον προσδιορισμό των πηγών των κινδύνων, των δυνητικών επιπτώσεων στα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων, την εξακρίβωση πιθανών απειλών και τον καθορισμό ή των αποδοχή των μέτρων αντιμετώπισης των κινδύνων. Σειρά από κινδύνους απουσιάζουν ή δεν αναλύονται επαρκώς, όπως απουσιάζει εκτίμηση και ανάλυση της επέμβασης ανά εκπαιδευτική βαθμίδα προσαρμοσμένη στις ιδιαιτερότητες των μαθητών. Ακόμη, απουσιάζουν κίνδυνοι από τη χρήση εξοπλισμού που δεν βρίσκεται στην ευθύνη του υπεύθυνου επεξεργασίας, δηλαδή από τη χρήση προσωπικής συσκευής του εκπαιδευτικού για υπηρεσιακούς σκοπούς, καθώς επίσης και κίνδυνοι από διαβιβάσεις δεδομένων εκτός Ε.Ε., κίνδυνοι που απορρέουν από την έλλειψη όρων στη σύμβαση με τον εκτελούντα την επεξεργασία (Cisco) σε περίπτωση περιστατικού παραβίασης ή κίνδυνοι από τη προσωπικών ηλεκτρονικών διευθύνσεων των εκπαιδευτικών αντί για λογαριασμών του σχολικού δικτύου. Αποτέλεσμα όλων των ελλείψεων που αποτυπώθηκαν στην εν λόγω Γνωμοδότηση ήταν η Αρχή να απευθύνει αυστηρές συστάσεις στο Υ.ΠΑΙ.Θ. με προθεσμία τριών μηνών για την ολοκλήρωση διορθώσεων της ΕΑΠΔ.

Κατόπιν αυτής, η Αρχή το Νοέμβριο του 2021, επανεξέτασε αυτεπάγγελτα τα ζητήματα που είχαν επισημανθεί προς το Υ.ΠΑΙ.Θ. και διαπίστωσε παραβιάσεις κατά τα εξής[192]: Σε σχέση με τα ζητήματα νομιμότητας της επεξεργασίας διαπιστώθηκε παραβίαση από το Υπουργείο, καθώς για την εξαγωγή στατιστικών και ερευνητικών συμπερασμάτων χρησιμοποιούνται τόσο δεδομένα που προέρχονται από την τερματική συσκευή του εκάστοτε χρήστη (όπως λογισμικό φυλλομετρητή, διεύθυνση

[192] Βλ. απόφαση ΑΠΔΠΧ υπ' αρ. 50/2021, https://www.dpa.gr/el/enimerwtiko/prakseisArxis?field_year_from=2021&field_year_to=2021&field_category=239&field_thematic=All&field_protocol_number=50&field_keywords=

IP, τύπος υλισμικού, διεύθυνση MAC, κ.α.), όσο και δεδομένα που παράγονται κατά τη χρήση της υπηρεσίας (όπως ενέργειες που έγιναν, πληροφορίες συνόδου συνάντησης). Δεδομένου ότι η εξαγωγή στατιστικών και ερευνητικών συμπερασμάτων σε σχέση με τη διαδικασία της εξ αποστάσεως εκπαίδευσης δεν είναι απαραίτητη για την παροχή της υπηρεσίας της κοινωνίας της πληροφορίας, νόμιμη βάση για την πρόσβαση σε αυτές τις πληροφορίες μπορεί να είναι μόνο η συγκατάθεση του χρήστη, καθώς έχουμε δεδομένα που χρησιμοποιούνται για σκοπό διαφορετικό από τον αρχικό, επομένως δεν μπορεί να τεκμηριωθεί νομιμότητα. Ακόμη, η Αρχή διαπίστωσε παραβιάσεις σε σχέση με τα ζητήματα διαφάνειας και την παροχή των απαιτούμενων πληροφοριών για την επεξεργασία. Διαπιστώθηκε δηλαδή ότι το Υπουργείο παρείχε πληροφορίες λιγότερες από όσες επιβάλλει ο ΓΚΠΔ, ότι οι πληροφορίες δεν είναι σε κατανοητή και εύκολα προσβάσιμη μορφή, δεν χρησιμοποιείται σαφής και απλή διατύπωση, ιδίως στις πληροφορίες που απευθύνονται σε παιδιά. Επίσης, διαπίστωσε παραβιάσεις σχετικά με τους κινδύνους που ενέχει η συγκεκριμένη επεξεργασία, καθώς τα λαμβανόμενα τεχνικά και οργανωτικά μέτρα δεν προστατεύουν επαρκώς τα δικαιώματα των υποκειμένων των δεδομένων, όπως δεν διασφαλίζει τον έλεγχο ταυτοπροσωπίας για τον περιορισμό της πρόσβασης τρίτων στις «ψηφιακές τάξεις» με το να παρέχει κατάλληλες οδηγίες και εκπαίδευση στο προσωπικό του (εκπαιδευτικούς). Επιπλέον, διαπίστωσε παραβιάσεις σε σχέση με την έκφραση γνώμης των υποκειμένων των δεδομένων ή των εκπροσώπων τους για τη σχεδιαζόμενη επεξεργασία και ομοίως, διαπίστωσε ότι πραγματοποιούνται διαβιβάσεις δεδομένων από το Υ.ΠΑΙ.Θ. ως υπεύθυνου επεξεργασίας προς την εδρεύουσα στις ΗΠΑ Cisco, χωρίς να διασφαλίζεται επαρκές επίπεδο προστασίας των προσωπικών δεδομένων. Για όλα αυτά η Εποπτική Αρχή απηύθυνε επιπλήξεις στο Υπουργείο Παιδείας και Θρησκευμάτων δίνοντας νέα εντολή για συμμόρφωση σε ορισμένη προθεσμία.

Πρόσφατα, η Αρχή ενεργώντας πάλι αυτεπάγγελτα, με τη με αριθμό 61/2022 απόφασή της[193], έκρινε τελικά ότι το Υπουργείο προέβη στις κατάλληλες ενέργειες

[193] Βλ. https://www.dpa.gr/el/enimerwtiko/prakseisArxis?field_year_from=2022&field_year_to=2022&field_category=239&field_thematic=All&field_protocol_number=61&field_keywords=

ώστε να είναι συμμορφωμένο με τις επιταγές του ΓΚΠΔ και ότι δεν απαιτείται κάποιο νέο διορθωτικό μέτρο σχετικά.

## Κεφάλαιο 6 – Επικύρωση της ΕΑΠΔ

### 6.1 Έλεγχος πληρότητας – Τελική αξιολόγηση

Στο τελευταίο στάδιο της εκπόνησης της εκτίμησης αντικτύπου παρουσιάζονται συνοπτικά τα πορίσματα και αποτελέσματα της μελέτης με σκοπό την τελική εξέτασή της για την πιθανή λήψη απόφαση αποδοχής της ή όχι. Από τον υπεύθυνο επεξεργασίας, με τη βοήθεια των αρμόδιων συμβούλων και την καίρια συμμετοχή και συμβολή του υπεύθυνου προστασίας προσωπικών δεδομένων, πραγματοποιείται επισταμένη και λεπτομερής αξιολόγηση των κινδύνων με στόχο την πρόβλεψη και αποφυγή πιθανού περιστατικού παραβίασης. Αξιολογούνται οι κίνδυνοι παράνομης πρόσβασης στα δεδομένα, ανεπιθύμητης τροποποίησης και καταστροφής των δεδομένων και γίνεται αποτίμηση του κατά πόσο τα υφιστάμενα ή προβλεπόμενα μέτρα μειώνουν επαρκώς τους κινδύνους[194]. Με τον τρόπο αυτό προκύπτει και τυχόν ανάγκη για καθορισμό και λήψη επιπλέον πρόσθετων μέτρων. Ακόμη, επιμελείται η πρόβλεψη οδηγών διαχείρισης συμβάντων ώστε ο οργανισμός να είναι σε ετοιμότητα και να δύναται να ακολουθήσει σχεδιασμένα βήματα προστασίας, ανίχνευσης του κινδύνου, αντίδρασης σε αυτόν και ανάκτησης των δεδομένων[195].

Κατά το στάδιο αυτό της προετοιμασίας των στοιχείων για την επικύρωση των αποτελεσμάτων, παρουσιάζονται τα συμπεράσματα της μελέτης με καλά σχεδιασμένους, ευανάγνωστους και σχηματικούς τρόπους παρουσίασης, όπως καταγραφές σε πίνακες, στους οποίους αποτυπώνονται τα μέτρα που επιλέχθηκαν να εφαρμόζονται στις συγκεκριμένες επεξεργασίες προς διασφάλιση της συμμόρφωσης με τις διατάξεις του Κανονισμού και τις θεμελιώδεις αρχές του, τα μέτρα που επιφέρουν το καλύτερο δυνατό αποτέλεσμα για την ασφάλεια των δεδομένων, καθώς και τους αναγνωρισμένους κινδύνους που ενέχει η κάθε επεξεργασία σε συνάρτηση με τη σοβαρότητα και την πιθανότητα επέλευσης[196].

---

[194] Βλ. CNIL, Privacy Impact Assessment (PIA) Templates, 2018, σελ. 20.
[195] Βλ. National Cyber Security Centre, Incident management, σε https://www.ncsc.gov.uk/collection/incident-management ,
[196] Βλ. CNIL, Privacy Impact Assessment (PIA) Μεθοδολογία, 2018, σελ. 8.

Τέλος, καταγράφεται ένα πλάνο δράσεων και ενεργειών και ταυτόχρονα επίβλεψης της εφαρμογής του. Σε αυτό γίνεται αποτίμηση της δυσκολίας εκτέλεσης και εφαρμογής (μικρή, μέτρια, υψηλή), του οικονομικού κόστους εφαρμογής των μέτρων (μηδενικό, μέτριο, υψηλό), του χρόνου εκτέλεσης (μήνες, ένα έτος, τρία έτη) και της εξέλιξής του (δεν ξεκίνησε, σε εξέλιξη, ολοκληρώθηκε). Παράλληλα, σημειώνονται επίσημα οι τεκμηριωμένες προτάσεις και οι σκέψεις του υπεύθυνου προστασίας δεδομένων, των εμπλεκόμενων στο έργο συμβούλων και των υποκειμένων των δεδομένων ή των εκπροσώπων τους[197].

## 6.2 Επίσημη επικύρωση

Το τελικό στάδιο είναι εκείνο της απόφασης για την έγκριση της επεξεργασίας ή της αρνητικής γνωμοδότησης. Στην περίπτωση που αποφασιστεί ότι οι αναγνωριζόμενοι κίνδυνοι αντιμετωπίζονται επαρκώς με τα αντίμετρα που προτείνονται με τη μελέτη, ο υπεύθυνος επεξεργασίας αποδέχεται αιτιολογημένα την μελέτη εκτίμησης αντικτύπου και αυτή θεωρείται επικυρωμένη. Στην αντίθετη περίπτωση που αξιολογηθεί ότι οι κίνδυνοι δεν αποτρέπονται επαρκώς, είτε επανεξετάζονται τα στάδια αυτά της μελέτης και αναζητείται ή συνιστάται εφαρμογή πρόσθετων ή διαφορετικών μέτρων ασφαλείας και συνεπώς βελτίωση της ΕΑΠΔ, είτε -εάν κριθεί ότι δεν διασφαλίζεται αποδεκτό επίπεδο ασφάλειας των δεδομένων- η μελέτη απορρίπτεται. Σε περίπτωση που η επεξεργασία θα προκαλούσε υψηλό κίνδυνο που δεν δύναται να προβλεφθεί με αντίμετρα η αποφυγή του, τότε πραγματοποιείται διαβούλευση με την αρμόδια Εποπτική Αρχή.

## Κεφάλαιο 7 – Επίλογος - Συμπεράσματα

Η παρούσα διπλωματική εργασία πραγματεύτηκε τη διαδικασία εκπόνησης μελέτης εκτίμησης αντικτύπου ως ένα χρήσιμο εργαλείο αξιολόγησης των ενδεχόμενων κινδύνων για την προστασία των δεδομένων προσωπικού χαρακτήρα των φυσικών προσώπων μέσα σε έναν οργανισμό ή επιχείρηση, ταυτόχρονα με την εφαρμογή κατάλληλων μέτρων περιορισμού των κινδύνων ή πρόληψης των αρνητικών συνεπειών σύμφωνα με τις επιταγές του Κανονισμού. Η ΕΑΠΔ ανεξαρτήτως της

[197] Βλ. άρθρο 35 παρ. 2 και 9 ΓΚΠΔ.

υποχρεωτικότητάς της, αποτελεί μία πολύτιμη έκθεση «αυτοελέγχου» ενός οργανισμού ή επιχείρησης που αποσκοπεί μέσα από τη διασφάλιση της συμμόρφωσης του υπεύθυνου επεξεργασίας, στην πρωτίστως προστασία και διασφάλιση των δικαιωμάτων των υποκειμένων των δεδομένων.

Η παρούσα εργασία προσέγγισε και ανέπτυξε βήμα προς βήμα όλα τα στάδια που ακολουθούνται για την ορθή εκπόνηση μιας εκτίμησης αντικτύπου, βασισμένη στη μεθοδολογία της Γαλλικής Αρχής CNIL, με αναφορές σε παραδείγματα και νομολογία. Αναλύθηκε εκτενώς ότι μια σύννομη ΕΑΠΔ πρέπει να περιέχει οπωσδήποτε αξιολογήσεις στους άξονες της σοβαρότητας και της πιθανότητας ενός κινδύνου πιθανού να προκύψει, ενώ παράλληλα αναδείχθηκε η αξία της ΕΑΠΔ και του ρόλου όλων των εμπλεκομένων σε αυτή.

Ως κατάληξη, παρατίθεται ο προβληματισμός ότι στη χώρα μας φαίνεται μάλλον έως σήμερα να μην έχει αναγνωριστεί η αξία της μελέτης εκτίμησης αντικτύπου και να μην της έχει αποδοθεί η δέουσα σημασία. Συχνά δείχνει να αντιμετωπίζεται από τους υπεύθυνους επεξεργασίας είτε ως άσκοπο εργαλείο είτε ως μία διαδικασία που μάλλον επιβαρύνει τον οικονομικό προϋπολογισμό τους παρά τους οφελεί. Ίσως να χρειαστεί ακόμη πρόσθετος χρόνος ωριμότητας των εκπροσώπων των επιχειρήσεων και φορέων στον τομέα αυτό ώστε να πεισθούν για την αξία της επένδυσης σε μία μελέτη εκτίμησης της νομιμότητας των επεξεργασιών τους, της εφαρμογής των θεμελιωδών αρχών, της διασφάλισης των δικαιωμάτων των υποκειμένων, της διαχείρισης των κινδύνων και της αξιολόγησης των μέτρων ασφάλειας.

**ΒΙΒΛΙΟΓΡΑΦΙΑ**

**Ελληνική**


*Ε. Αλεξανδροπούλου-Αιγυπτιάδου*, Προσωπικά δεδομένα, εκδ. Νομ. Βιβλιοθήκη 2016

*Ι. Ιγγλεζάκης,* Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων, Interactive Books, 2018

*Ι. Ιγγλεζάκης,* Η εκτίμηση αντικτύπου στην προστασία προσωπικών δεδομένων (Data Protection Impact Assessment). Δικαιοπολιτική θεώρηση ενός καινοτόμου εργαλείου προστασίας της ιδιωτικότητας στον 21ο αιώνα, Επιθεώρηση Δικαίου Πληροφορικής, Τομ. 1, Τεύχ. 1, 2020

*Λ. Κανέλλος*, The GDPR Handbook, Εκδ. Νομική Βιβλιοθήκη, 2020

*Σ. Κάτσικας, Στ. Γκρίτζαλης, Κ. Λαμπρινουδάκης*, Ασφάλεια Πληροφοριών και Συστημάτων στον Κυβερνοχώρο, εκδ. Νέων Τεχνολογιών 2021

*Κ. Κόμνιος*, Γενικός κανονισμός για την προστασία δεδομένων, Εκδ. Σάκκουλα, 2020

*Λ. Κοτσαλής*, Προσωπικά δεδομένα, Ανάλυση – Σχόλια - Εφαρμογή, εκδ. Νομ. Βιβλιοθήκη 2016

*Λ. Κοτσαλής – Κ. Μενουδάκος*, Γενικός Κανονισμός για την προστασία των προσωπικών δεδομένων (GDPR), Νομική διάσταση και πρακτική εφαρμογή, εκδ. Νομ. Βιβλιοθήκη 2021

*Κ. Λαμπρινουδάκης, Λ. Μήτρου, Στ. Γκρίτζαλης, Σ. Κάτσικας*, Προστασία της Ιδιωτικότητας, Τεχνολογίες Πληροφορικής και Επικοινωνιών, Τεχνικά και Νομικά Θέματα, εκδ. Παπασωτηρίου 2010

*Λ. Μήτρου*, Ο γενικός κανονισμός προστασίας προσωπικών δεδομένων, νέο δίκαιο – νέες υποχρεώσεις- νέα δικαιώματα, Εκδ. Σάκκουλα, 2017

*ΟΕ 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

*ΟΕ 29*, Κατευθυντήριες γραμμές για την αυτοματοποιημένη λήψη αποφάσεων και την κατάρτιση προφίλ για τους σκοπούς του κανονισμού 2016/679

*ΟΕ 29*, Κατευθυντήριες γραμμές σχετικά με τη διαφάνεια βάσει του κανονισμού 2016/679

*ΟΕ 29*, Κατευθυντήριες γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων
*ΟΕ 29*, Γνώμη 1/2010 σχετικά με τις έννοιες του «υπεύθυνου της επεξεργασίας» και του «εκτελούντος την επεξεργασία»
*ΟΕ 29*, Γνώμη 3/2013 σχετικά με τον περιορισμό του σκοπού
*Β. Σωτηρόπουλος*, Υπεύθυνος Προστασίας Δεδομένων, Εκδ. Σάκκουλα, 2019
*FRA,* Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων, έκδοση 2018
*Δ. Τζέλλης, Μ. Μυλώση,* Εκτίμηση Αντικτύπου στην προστασία προσωπικών δεδομένων, Εκδ. Νομική Βιβλιοθήκη, 2022
*Κ. Χριστοδούλου*, Δίκαιο Προσωπικών Δεδομένων, εκδ. Νομ. Βιβλιοθήκη 2020

**Ξενόγλωσση**

*A. Askarov, R. Hansen, W. Rafnsson,* Secure IT Systems, Springer, 2019
*CNIL,* Privacy Impact Assessment (PIA) Methology, 2018
*CNIL*, Privacy Impact Assessment (PIA) Knowledge Bases, 2018
*CNIL*, Privacy Impact Assessment (PIA) Templates, 2018
*CNIL*, Security of personal data, 2018
*CNIL*, Practical Guide GDPR, DPO, 2021
*ENISA*, Handbook on security of Personal Data Processing, December 2017
*EDPB*, Opinion 7/2018 on the draft list of the competent supervisory authority of Greece regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR)
*EDPB*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR
*M. Hansen, E. Kosta, Ig. Nai-Fovino, S. Fischer-Hübner*, Privacy and Identity Management, Springer, 2017
D. Solove, Nothing to Hide, Yale University Press, 2011

**Άρθρα σε περιοδικά**

*Ε. Αλεξανδροπούλου-Αιγυπτιάδου*, Ηλεκτρονική επεξεργασία προσωπικών δεδομένων και το δικαίωμα αντίρρησης του υποκειμένου τους, Αρμ. ΝΘ΄(2005) 137-142

*Ε. Αλεξανδροπούλου-Αιγυπτιάδου – Ι. Μαυρίδης*, Η προστασία των προσωπικών δεδομένων ενόψει της εφαρμογής της νέας τεχνολογίας της ταυτοποίησης με ραδιοσυχνότητες, Αρμ. ΞΑ΄(2007) 493-504

*Δ. Γεωργόπουλος,* Σχέδιο αντιμετώπισης περιστατικών παραβίασης δεδομένων προσωπικού χαρακτήρα, Συνήγορος 122/2017

*Δ. Ζωγραφόπουλος*, Η υποχρέωση διενέργειας εκτίμησης αντικτύπου στον Γενικό Κανονισμό για την Προστασία Δεδομένων, Συνήγορος, 120/2017

*Ι. Ιγγλεζάκης*, Η εκτίμηση αντικτύπου στην προστασία προσωπικών δεδομένων. Δικαιοπολιτική θεώρηση ενός καινοτόμου εργαλείου προστασίας της ιδιωτικότητας στον 21ο αιώνα, Επιθεώρηση Δικαίου Πληροφορικής, Τομ. 1, τεύχ. 1, 2020

*Ν. Λουκάς*, Τεχνικά μέτρα του Γενικού Κανονισμού για την προστασία δεδομένων, Κρυπτογράφηση και Ψευδωνυμοποίηση, Συνήγορος 123/2017

*Ν. Λουκάς*, Η έννοια και η διαχείριση του «Κινδύνου» στον ΓΚΠΔ, ΔΙΜΕΕ 4/2017

*Λ. Μήτρου*, Privacy by design, Η τεχνολογική διάσταση της προστασίας προσωπικών δεδομένων, ΔΙΜΕΕ 1/2013

*Ε. Σμυρνάκη*, Υπολογιστικό Νέφος (Cloud) και Προσωπικά Δεδομένα – Γενικός Κανονισμός Προστασίας Δεδομένων 679/2016, Pro Justitia, 2016, 254 επ.

*Γ. Ψαράκης*, GDPR και Μελέτη Εκτίμησης Αντικτύπου (DPIA): Better safe than sorry?, Lawspot https://www.lawspot.gr/nomika-blogs/giannis_psarakis/gdpr-kai-meleti-ektimisis-antiktypoy-dpia-better-safe-sorry

*F. Bieker, M. Friedewald, M. Hansen, H. Obersteller, M. Rost*, A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation, Springer 2016, 21-37

*I. Borocz,* Risk to the Right to the Protection of Personal Data, EDPL 4/2016, 467

*R. Clarke*, Privacy impact assessment: Its origins and development, Elsevier, Computer Law & Security review 25 (2009), 123-135

*N. Dirjk, R. Gellert, K. Rommetveit*, A risk to a right? Beyond data protection risk assessments, Elsevier, Computer Law & Security review 32 (2016), 286-306

J. Sarrat, R. Brun, DPIA: How to Carry Out One of the Key Principles of Accountability, Springer 2018, 172-182

*O. Tene, J. Polonetsky*, Big Data for All: Privacy and User Control in the Age of Analytics, Northwestern Journal of Technology and Intellectual Property, vol. 11, issue 5, 2013, σελ. 240 και επ.

*A. Warren, R. Bayley, C. Bennett, A. Charlesworth, R. Clarke, C. Oppenheim*, Privacy Impact Assessments: International experience as a basis for UK Guidance, Elsevier, Computer Law & Security report 24 (2008), 233-242

*D. Wright*, The state of the art in privacy impact assessment, Elsevier, Computer Law & Security review 28 (2012), 54-61

*D. Wright*, *R. Finn, R. Rodrigues*, A Comparative Analysis of Privacy Impact Assessment in Six Countries, Journal of Contemporary European Research, Volume 9, Issue 1 (2013)

**Ιστοσελίδες**

*Κ. Κόμνιος*, GDPR: Η σύμβαση με τον εκτελούντα την επεξεργασία, https://www.capital.gr/me-apopsi/3288247/gdpr-i-sumbasi-me-ton-ektelounta-tin-epexergasia#0

*Ιστότοπος ΑΠΔΠΧ, www.dpa.gr*

*Ιστότοπος CNIL*, https://www.cnil.fr

*ISO/IEC 29134:2017* «Information technology — Security techniques — Guidelines for privacy impact assessment», https://www.iso.org/obp/ui/#iso:std:iso-iec:29134:ed-1:v1:en

*CNIL Software* https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assessment