Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Οικονομικών Επιστημών και Διοίκησης

Μεταπτυχιακό Πρόγραμμα *Διοίκηση, Τεχνολογία, Ποιότητα*

Μεταπτυχιακή Διατριβή

Η εφαρμογή του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR) στο Πλαίσιο της Λειτουργίας Ενός Εκπαιδευτικού Οργανισμού.

Τότσικας Αθανάσιος

Επιβλέπουσα Καθηγήτρια
Ευανθία Βόρρια

Νοέμβριος 2019

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Οικονομικών Επιστημών και Διοίκησης

Μεταπτυχιακό Πρόγραμμα Σπουδών *Διοίκηση, Τεχνολογία, Ποιότητα*

Μεταπτυχιακή Διατριβή

Η εφαρμογή του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR) στο Πλαίσιο της Λειτουργίας Ενός Εκπαιδευτικού Οργανισμού.

Τότσικας Αθανάσιος

Επιβλέπων Καθηγητής
Ευανθία Βόρρια

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών στη Διοίκηση, Τεχνολογία, Ποιότητα από τη Σχολή Οικονομικών Επιστημών και Διοίκησης του Ανοικτού Πανεπιστημίου Κύπρου.

Νοέμβριος 2019

Περίληψη

Ο Κανονισμός 2016/679 του Ευρωπαϊκού Κοινοβουλίου, γενικότερα γνωστός ως Γενικός Κανονισμός Προστασίας Δεδομένων ή GDPR κατά το Αγγλικό General Data Protection Regulation, είναι σε υποχρεωτική ισχύ από τις 25 Μαΐου 2018 και πρέπει να εφαρμόζεται από το σύνολο των επιχειρήσεων σε ευρωπαϊκό επίπεδο. Προκειμένου να είναι συμβατές με τον GDPR οι επιχειρήσεις είναι απαραίτητο να δημιουργήσουν ένα Σύστημα Διαχείρισης Προσωπικών Δεδομένων. Σε πολλές περιπτώσεις, ένα Σύστημα Διαχείρισης Προσωπικών Δεδομένων αφορά τη διαχείριση προσωπικών πληροφοριών που ήδη διατηρούνται ενδοεταιρικά σε ένα ευρύ φάσμα των λειτουργικών μονάδων και συστημάτων εφαρμογών. Συχνά αυτές οι προσωπικές πληροφορίες ενδέχεται να εμπίπτουν παράλληλα και στο πεδίο εφαρμογής άλλων συστημάτων διαχείρισης που εφαρμόζει ένας οργανισμός π.χ. διαχείριση ποιότητας κατά ISO 9001, ασφάλεια πληροφοριακών συστημάτων κατά ISO27000 κλπ. Όμως, τα εν λόγω πρότυπα (ISO09001, ISO27000) επειδή έχουν εκδοθεί πριν την ημερομηνία δημοσίευσης του GDPR, δεν είναι σήμερα συμβατά με τις απαιτήσεις του GDPR, έως ότου επικαιροποιηθούν, συνεπώς απαιτείται προσαρμογή των υπαρχόντων Συστημάτων Ποιότητας στις απαιτήσεις του GDPR.

Η παρούσα διατριβή ασχολείται με την εφαρμογή των επιταγών του GDPR στη λειτουργία ενός εκπαιδευτικού οργανισμού, που εκ των πραγμάτων προχωρά σε επεξεργασία προσωπικών δεδομένων μεγάλης κλίμακας, και στην ενσωμάτωσή του GDPR σε υπάρχοντα συστήματα ποιότητας που ήδη αυτός εφαρμόζει. Η ορθή εφαρμογή του GDPR στο ευρύτερο πλαίσιο λειτουργίας του οργανισμού θα του επιτρέψει αφενός να είναι νομικά κατοχυρωμένος και αφετέρου να συνεχίσει την απρόσκοπτη λειτουργία του μέσω της προσθήκης μόνο των διαδικασιών εκείνων που είναι απαραίτητοι για τη συμμόρφωσή του.

Συγκεκριμένα παρουσιάζεται συνοπτικά ο GDPR, αναλύονται οι απαιτήσεις του, δημιουργούνται πρότυπα αρχεία για την ανάλυση ελλείψεων (gap analysis) με σκοπό την οριστικοποίηση των απαραίτητων βημάτων για τη συμμόρφωση του οργανισμού. Πρακτικά η παρούσα διατριβή μπορεί να θεωρηθεί ένας ενδεικτικός οδηγός προσαρμογής στις απαιτήσεις του GDPR για έναν εκπαιδευτικό οργανισμό.

Summary

The EU 2016/679 Regulation, more commonly known as the General Data Protection Regulation or GDPR under the English General Data Protection Regulation, is in force since 25 May 2018 and must be applied by all businesses at European level. In order to be GDPR compliant, businesses need to create a Personal Data Management System. In many cases, a Personal Data Management System relates to the management of personal information already held in-company across a wide range of operating systems and application systems. Often this personal information may also fall under the scope of other management systems implemented by an organization eg. ISO 9001, ISO27000 etc. However, these standards (ISO09001, ISO27000) are not yet compliant with the GDPR requirements, because they were issued before the date of publication of the GDPR. Therefore existing Quality Systems need to be adopted to GDPR requirements.

This dissertation deals with the application of GDPR requirements to the operation of an educational organization, which de facto processes large-scale personal data, and the integration of GDPR into existing quality systems. The proper implementation of GDPR in the broader context of the organization will result in being both legally regulated and to continue operating smoothly by adding only the procedures necessary to comply.

More specifically, this dissertation summarizes the GDPR, analyzes its requirements, and creates templates for gap analysis in order to finalize the necessary steps of an organization for GDPR compliance. In practice this dissertation can be considered as an indicative guide for an educational organization to adapt to the GDPR requirements.

Περιεχόμενα

Κεφάλαιο 1
Εισαγωγή

Η συστηματική συλλογή Προσωπικών Δεδομένων είναι μια διαδικασία που έχει ξεκινήσει τα τελευταία χρόνια. Ανέκαθεν οι επιχειρήσεις αρχειοθετούσαν τα δεδομένα των υπαρχόντων και δυνητικών πελατών τους προκειμένου να μπορέσουν να επιτύχουν τους εταιρικούς τους στόχους. Η συλλογή των Προσωπικών Δεδομένων δεν γίνεται μόνο για λόγους επιχειρηματικούς. Η έννοια της διατήρησης ιστορικού σε πολλούς τομείς της καθημερινότητας (όπως η ιατρική, η οικονομική κλπ) επιβάλλουν τη διατήρηση συγκεκριμένων στοιχείων – προσωπικών δεδομένων για το κάθε πρόσωπο. Ειδικά με τη συνεχή και ταχύτατη ενσωμάτωση των νέων τεχνολογιών, η συλλογή των δεδομένων προσωπικού χαρακτήρα αποκτά μια ιδιαίτερη διάσταση, προκειμένου να διασφαλιστεί ότι τα δεδομένα που συλλέγονται, τηρούνται μόνο για τους σκοπούς για τους οποίους συλλέγονται, με τη σύμφωνη πάντα γνώμη του προσώπου – ιδιοκτήτη των δεδομένων. Είναι χαρακτηριστικό ότι το 2019 υπολογίστηκε ότι υπάρχουν ενεργοί 4,5 δισεκατομμύρια χρήστες του ίντερνετ[1]. Άρα «*η ανεξέλεγκτη επεξεργασία δεδομένων που συμβαίνει σε όλο τον κόσμο με τη χρήση όλο και περισσότερων παραγωγικών ψηφιακών συσκευές, μετατρέπουν τον κόσμο σε ένα ψηφιακό χωριό*[2]», γεγονός που επιβάλλει την ορθή αποθήκευση, επεξεργασία και χρήση των προσωπικών δεδομένων που κατέχει ένας οργανισμός, μόνο για τους σκοπούς που απαιτούνται και όχι για δόλιους σκοπούς. Για να κατανοήσουμε το μέγεθος των προσωπικών δεδομένων που συλλέγονται και επεξεργάζονται, σύμφωνα με τη Eurostat αυτή τη στιγμή υπολογίζεται ότι διαμένουν στην ΕΕ 510 εκ πολίτες[3]. Άρα μπορεί εύκολα να γίνει κατανοητό το μέγεθος και η έκταση των προσωπικών δεδομένων που επεξεργάζονται και πόσο κρίσιμο είναι να υπάρχει ορθή επεξεργασία με σκοπό την προστασία των πολιτών αυτών σε σχέση με τα προσωπικά τους δεδομένα.

Στο παρελθόν παρατηρήθηκαν πολλές περιπτώσεις όπου η συλλογή των δεδομένων προσωπικού χαρακτήρα από έναν οργανισμό αποτέλεσε πεδίο κερδοσκοπίας, με την «μεταβίβαση» δεδομένων από έναν οργανισμό σε έναν άλλο έναντι χρηματικής ή άλλου είδους αμοιβής. Πόσες φορές άλλωστε δεν λάβαμε μια κλήση, ένα sms ή ένα email από μια εταιρεία την οποία δεν γνωρίζαμε καν? Επίσης, δεν υπήρχαν πουθενά καταγεγραμμένα τα δικαιώματα των προσώπων απέναντι στη συλλογή των

[1] World Internet Users and 2019 Population Stats, 2018
[2] IMPACT OF EU GENERAL DATA PROTECTION REGULATION ON THE MANAGEMENT OF EDUCATION Antoņina Jemeljanenko, University of Latvia
[3] General Data Protection Regulation: No silver bullet for small and medium-sized enterprises. Authors: Wilkinson, Gerard, Source: Journal of Payments Strategy & Systems. Summer2018, Vol. 12 Issue 2, p139-149. 11p.

προσωπικών δεδομένων τους. Παράλληλα, δεν υπήρχαν τεκμηριωμένες και καταγεγραμμένες οι συνέπειες από μια αθέμιτη επεξεργασία προσωπικών δεδομένων. Επίσης, υπάρχουν πολλά παραδείγματα όπου Προσωπικά Δεδομένα διέρρευσαν ακούσια σε μη εξουσιοδοτημένα άτομα. Χαρακτηριστικό παράδειγμα το σκάνδαλο Equifax το 2017, που άφησε 144,5 εκατομμύρια χρήστες ψηφιακά ευάλωτους στην κλοπή ταυτότητας και σε μελλοντικά ατυχήματα[4]. Άλλο χαρακτηριστικό παράδειγμα είναι η υπόθεση της Cambridge Analytica, που επέτρεψε την κλοπή προσωπικών πληροφοριών περίπου 87 εκατομμυρίων χρηστών του Facebook[5].

Δεν είναι όμως μόνο η διαρροή προσωπικών δεδομένων που γέννησε την ανάγκη ενός πιο συνεκτική πλαισίου για την επεξεργασία τους. Το Ευρωπαϊκό Δικαστήριο της ΕΕ με τον λεγόμενο κανόνα Google Spain, εισήγαγε πρώτο το δικαίωμα της λήθης (rule to be forgotten), απαιτώντας από την Google να ικανοποιήσει το αίτημα του φυσικού προσώπου να αποκλείσει ορισμένα αποτελέσματα αναζήτησης που τον αφορούν και δε επιθυμεί να εμφανίζονται[6].

Για τους λόγους αυτούς, η Ευρωπαϊκή Επιτροπή οδηγήθηκε μετά από πολύχρονες συζητήσεις στη σύνταξη μια ευρωπαϊκής οδηγίας, που να καθορίζει το πλαίσιο μέσα στο οποίο θα πρέπει να κινούνται άπαντες σχετικά με τα προσωπικά δεδομένα και την επεξεργασία τους. Ψηφίστηκε λοιπόν στις 27 Απριλίου 2016 ο Κανονισμού 2016/679 του Ευρωπαϊκού Κοινοβουλίου για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών, ο οποίος είναι γενικότερα γνωστός ως Γενικός Κανονισμός για την Προστασία Δεδομένων ή ΓΚΠΔ ή General Data Protection Regulation ή GDPR. Ο GDPR αντικατέστησε την οδηγία Data Protection Directive 95/46/EC (Directive) που ήταν σε ισχύ από τον Δεκέμβριο του 1995[7]. Επειδή ο GDPR είναι Κανονισμός και όχι Οδηγία, αυτό σημαίνει ότι πρέπει να εφαρμόζεται υποχρεωτικά από όλα τα κράτη μέλη της Ευρωπαϊκής Ένωσης[8].

Στόχος του Κανονισμού είναι η εναρμόνιση της προστασίας των δεδομένων προσωπικού χαρακτήρα σε επίπεδο ΕΕ, η μεγαλύτερη έκταση ελέγχου για τα πρόσωπα που επεξεργάζονται τα δεδομένα

[4] "The internet is not pleased": twitter and the 2017 Equifax data breach. Novak, Alison N., Vilceanu, M. Olguta, Source: Communication Review. Jul-Sep2019, Vol. 22 Issue 3, p196-221. 26p. 3 Charts.
[5] The European General Data Protection Regulation: An instrument for the globalization of privacy standards? Colin J. Bennett Department of Political Science, University of Victoria, Victoria, BC, V8W 3P5, Canada
[6] The Right Tools: Europe's Intermediary Liability Laws and the EU 2016 General Data Protection Regulation, Authors: Keller, Daphne, Source: 33 Berkeley Tech. L.J. 287 (2018) / Berkeley Technology Law Journal, Vol. 33, Issue 1 pp. 287-364 Publication Year: 2018
[7] EU's General Data Protection Regulation (GDPR): Key Provisions and Best Practices. By: Schildhaus, Aaron, International Law News, 00470813, Winter2018, Vol. 46, Issue 2
[8] EU's General Data Protection Regulation (GDPR): Key Provisions and Best Practices. By: Schildhaus, Aaron, International Law News, 00470813, Winter2018, Vol. 46, Issue 2

(υποκείμενα των δεδομένων) και η βελτιωμένη διαχείριση των σύγχρονων κινδύνους στον τομέα αυτό[9].

Με την εισαγωγή του Κανονισμού 2016/679 του Ευρωπαϊκού Κοινοβουλίου, ο οποίος θέτει νέες προδιαγραφές για τον τρόπο με τον οποίο θα πρέπει να συλλέγονται, επεξεργάζονται και τηρούνται τα Προσωπικά Δεδομένα, όλες οι επιχειρήσεις θα πρέπει να αναπροσαρμόσουν τις διαδικασίες συλλογής, τήρησης και επεξεργασίας των Προσωπικών Δεδομένων, προκειμένου να είναι σύννομες. Παράλληλα, ο GDPR εισάγει και συγκεκριμενοποιεί τα δικαιώματα που έχει το φυσικό πρόσωπο, απέναντι στη συλλογή των προσωπικών του δεδομένων από τις επιχειρήσεις με τις οποίες έχει έρθει σε επαφή, όπως ένας εκπαιδευτικός οργανισμός.

Εξυπακούεται ότι ο GDPR είναι η πρώτη προσπάθεια δημιουργίας ενός πλαισίου για την προστασία των προσωπικών δεδομένων. Όσο ατελής και να είναι αυτή τη στιγμή, είναι το πρωταρχικό όπλο στον αγώνα για να εξουδετερωθούν οι άνθρωποι (hackers) που επιθυμούν να εκμεταλλευτούν οικονομικά τόσο επιχειρήσεις όσο και φυσικά πρόσωπα[10]. Η εφαρμογή του Κανονισμού είναι ένα δύσκολο εγχείρημα με πολλές προσκλήσεις, γιατί ουσιαστικά απαιτεί από τις επιχειρήσεις να αναπροσαρμόσουν τις λειτουργίες τους. Όμως η ανταγωνιστικότητα των επιχειρήσεων αυτών θα εξαρτηθεί από το πόσο επιτυχημένα θα μπορέσουν να υπερβούν αυτές τις προκλήσεις και να ενσωματώσουν τις επιταγές του Κανονισμού στην επιχειρηματική τους λειτουργία[11].

Ο GDPR ακουμπά όλες τις πτυχές των προσωπικών δεδομένων που επεξεργάζονται στην καθημερινή ζωή των πολιτών, όπως για παράδειγμα τα θέματα των προσωπικών δεδομένων Ιατρικής Φύσης. Το γεγονός αυτό είναι μια πρόκληση από μόνο του, αφού θα πρέπει να υπάρξει μια ενδελεχής μελέτη για το πώς τα Ιατρικά προσωπικά θα μπορούν να χρησιμοποιηθούν για Ιατρικούς Σκοπούς χωρίς παράλληλα να αίρονται τα δικαιώματα των Φυσικών Προσώπων[12].

Αντίστοιχη πρόκληση είναι και η επεξεργασία των Προσωπικών Δεδομένων για τραπεζικούς και οικονομικούς σκοπούς. Οι τράπεζες και οι φορολογικές αρχές, διατηρούν και επεξεργάζονται προσωπικά δεδομένα πολιτών για αυτούς τους λόγους[13]. Άρα πλέον, με την εισαγωγή του GDPR και

[9] GDPR: A new challenge for personal data protection, Academic Journal, By: Mraznica Erne. In: Bankarstvo, Vol 46, Iss 4, Pp 166-177 (2017); Association of Serbian Banks, 2017. Language: English; Serbian, Database: Directory of Open Access Journals

[10] GDPR and global data privacy - The future, Source: IQ: The RIM Quarterly, Date: May 1, 2019

[11] The European General Data Protection Regulation and Competitiveness of Firms. Authors: Bandyopadhyay, Soumava, Bandyopadhyay, Kakoli, Source: Competition Forum 2018, Vol. 16 Issue 1, p50 6p.

[12] GDPR and Health Personal Data; Tricks and Traps of Compliance. Authors: Orel A; Marand d.o.o. Ljubljana, Slovenia. Bernik I; University of Maribor, Faculty of Criminal Sciences and Security, Ljubljana, Slovenia., Source: Studies In Health Technology And Informatics [Stud Health Technol Inform] 2018; Vol. 255, pp. 155-159.Publication Type: Journal Article; Review

[13] Fighting Unfair Classifications in Credit Reporting: Should the United States Adopt GDPR-Inspired Rights in Regulating Consumer Credit ,Authors: Hertza, Vlad A. Source: 93 N.Y.U. L. Rev. 1707 (2018) / New York University Law Review, Vol. 93, Issue 6 (December 2018), pp. 1707-1741 Publication Year: 2018

την υποχρεωτικότητα που τον διακρίνει, θα πρέπει να προσαρμοστούν και να επιτρέψουν μέσα από τις λειτουργίες τους τις κατάλληλες εναλλακτικές, ώστε αφενός να μπορούν να συνεχίσουν οι ίδιες απρόσκοπτα τη λειτουργία τους με μεγαλύτερη διαφάνεια και αυξημένη ασφάλεια και αφετέρου να επιτρέψουν στα φυσικά πρόσωπα να προστατεύσουν τα δικαιώματά τους από τις ενδεχόμενες αθέμιτες πρακτικές που μπορεί ακούσια να εφαρμόζουν[14].

Ακόμα, ο GDPR έρχεται να θέσει όρους και στον τρόπο που επεξεργάζονται τα προσωπικά δεδομένα από εργολάβους (vendors) των επιχειρήσεων. Μπορεί μια επιχείρηση να είναι πλήρως συμβατή με τον GDPR, αλλά ένα μέρος του έργου που παράγει να το έχει αναθέσει σε μια Τρίτη επιχειρηματική οντότητα, η οποία να μην είναι συμβατή με τον GDPR. Πλέον ο GDPR θέτει την επιχείρηση υπεύθυνη και για τον τρόπο που επεξεργάζονται οι υπεργολάβοι της τα προσωπικά δεδομένα των πελατών της[15].

Επιπλέον, με την εισαγωγή των νέων τεχνολογιών υψηλής τεχνογνωσίας όπως το machine learning και η τεχνητή νοημοσύνη, δημιουργούνται όλο και περισσότερα συστήματα αυτοματοποιημένης επεξεργασίας και δημιουργίας προφίλ, που πιθανά να δημιουργήσουν κινδύνους για τα προσωπικά δεδομένα των πολιτών. Ο GDPR έρχεται και εδώ να θέσει όρους σε αυτές τις περιπτώσεις με πρωταρχικό του μέλημα να προστατέψει τα προσωπικά δεδομένα των πολιτών[16].

Ακόμα πιο απαιτητική είναι η περίπτωση της επεξεργασίας προσωπικών δεδομένων πολιτών της ΕΕ (όπου ουσιαστικά απευθύνεται ο GDPR) από τις εταιρείες που δραστηριοποιούνται παγκοσμίως. Υπάρχει αυτή τη στιγμή μια μεγάλη συζήτηση για την ασυμβατότητα του GDPR με τους αντίστοιχους νόμους προστασίας δεδομένων άλλων κρατών. Αυτή η ασυμβατότητα μπορεί να αποτελέσει τη δικαιολογία για την αθέμιτη επεξεργασία προσωπικών δεδομένων. Ο GDPR, όμως έχει λάβει υπόψη του αυτό το πλαίσιο και προσπαθεί να βάλει τάξη και σε αυτό το φαινόμενο[17].

Όπως λοιπόν έγινε κατανοητό, η επεξεργασία των προσωπικών δεδομένων των φυσικών προσώπων γίνεται σε όλες θα λέγαμε τις πτυχές της καθημερινότητας. Ειδικότερα στο πλαίσιο της παρούσας διατριβής, γίνεται συγκεκριμένη αναφορά στη λειτουργία ενός εκπαιδευτικού οργανισμού, όπου απαιτεί τη συλλογή προσωπικών δεδομένων, προκειμένου να μπορεί να τεκμηριώνεται η συμμετοχή

[14] Can consumers bank on financial services being secure with GDPR? Authors: Sydekum, Ralf, Affiliation: F5 Networks, Source: In Computer Fraud & Security June 2018 2018(6):11-13, Publisher: Elsevier Ltd

[15] GDPR puts vendor contracts in the security spotlight, Authors: Brook, David, Affiliation: Turnstone Services, Source: In Computer Fraud & Security April 2018 2018(4):5-7, Publisher: Elsevier Ltd

[16] Regulation of automated individual decision-making and artificially intelligent algorithmic systems: is the gdpr a powerful enough mechanism to protect data subjects? Authors: Ljungholm, Doina Popescu, Source: Analysis and Metaphysics. Annual, 2018, Vol. 17, p116, 6 p. Publisher Information: Addleton Academic Publishers, Publication Year: 2018

[17] The General Data Protection Regulation: What U.S.-Based Companies Need to Know, Authors: Ducich, Stefan, Fischer, Jordan L., Source: 74 Bus. Law. 205 (2018-2019) / Business Lawyer, Vol. 74, Issue 74 (Winter 2018-2019), pp. 205-216, Publication Year: 2018

ενός προσώπου σε εκπαιδευτικές δράσεις, οι οποίες πολλές φορές απαιτούνται από το νομοθετικό πλαίσιο (πχ Τεχνικός Ασφαλείας). Φυσικά, το είδος των προσωπικών δεδομένων που συλλέγονται και τηρούνται ποικίλλουν ανάλογα με το είδος της εκπαιδευτικής διαδικασίας στην οποία συμμετέχει ένα πρόσωπο. Τα δεδομένα που διατηρεί ένας εκπαιδευτικός οργανισμός τηρούνται από τη στιγμή της εγγραφής ενός μαθητή, έως τη λήξη της φοίτησής του ή ακόμα και αργότερα[18]. Εκτός από τους λόγους που αναφέρθηκαν παραπάνω, προσωπικά δεδομένα διατηρούνται και επεξεργάζονται και για λόγους επιστημονικούς και ερευνητικούς, όπως για παράδειγμα σε ιατρικές έρευνες[19]. Συνεπώς η ορθή εφαρμογή του GDPR είναι απαραίτητη ώστε να μην επηρεάζεται η επιστημονική ανάπτυξη.

Σκοπός της παρούσας εργασίας είναι να παρουσιάσει τον GDPR, να εξηγήσει τις απαιτήσεις του και να καταδείξει τη σχέση του με άλλα συστήματα ποιότητας που διατηρεί ενδεχομένως ένα εκπαιδευτικός οργανισμός. Τέλος, επιχειρεί να οριοθετήσει τα βήματα που πρέπει να κάνει ο εκπαιδευτικός οργανισμός προκειμένου η λειτουργία του - όσον αφορά τη συλλογή, επεξεργασία και τήρηση των προσωπικών δεδομένων – να είναι συμβατός με τις απαιτήσεις του GDPR.

[18] TEM Journal. Volume 8, Issue 1, Pages 150-156, ISSN 2217-8309, DOI: 10.18421/TEM81-21, February 2019, Preparing Students for the Era of the General Data Protection Regulation (GDPR), Maja Gligora Marković, , Sandra Debeljak, Nikola Kadoić

[19] The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era Currents in Contemporary Bioethics Edward S. Dove

Κεφάλαιο 2
Συνοπτική παρουσίαση του Γενικού Κανονισμού για την Προστασία Δεδομένων (GDPR)

2.1 Τι είναι ο Γενικός Κανονισμός για την Προστασία Δεδομένων(GDPR)

Ο Ευρωπαϊκός Κανονισμός GDPR 679/2016 αντικαθιστά την Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών. Τίθεται σε υποχρεωτική εφαρμογή για όλα τα κράτη μέλη της Ευρωπαϊκής Ένωσης, χωρίς την ανάγκη ψήφισης τοπικής εθνικής νομοθεσίας καταργώντας υφιστάμενους κανονισμούς και νομοθεσίες. Σύμφωνα με τον Κανονισμό 2016/679 κάθε φυσικό ή νομικό πρόσωπο (συνεπώς και τα εκπαιδευτικά ιδρύματα) που επεξεργάζεται προσωπικά δεδομένα έχει την υποχρέωση εφαρμογής του Κανονισμού ο οποίος έχει τεθεί σε υποχρεωτική ισχύ από την 25/05/2018. Κάθε υπόχρεος φορέας οφείλει να προσαρμόσει τις δραστηριότητες του στο ανανεωμένο και πιο αυστηρό θεσμικό πλαίσιο, διότι σε διαφορετική περίπτωση υφίστανται ιδιαίτερα υψηλά διοικητικά πρόστιμα.

Ο GDPR έχει σχεδιαστεί για να επιτρέπει στα μεμονωμένα άτομα να έχουν μεγαλύτερο έλεγχο των προσωπικών τους δεδομένων και επιβάλλει νέες υποχρεώσεις σε οργανισμούς που συλλέγουν, διαχειρίζονται ή αναλύουν τέτοιου είδους δεδομένα. Συνεπώς απαιτείται για όλους τους φορείς στην Ευρώπη μια ολοκληρωμένη διαδικασία εσωτερικής προετοιμασίας και προσαρμογής η οποία θα καταλήξει σε θετική δήλωση συμμόρφωσης σε σχέση με τη διαχείριση δεδομένων προσωπικού χαρακτήρα.

Κάθε χώρα οφείλει να ορίσει μια ανεξάρτητη Εθνική Αρχή, η οποία θα εποπτεύει τη λειτουργία των οργανισμών και επιχειρήσεων, σε σχέση με τις επιταγές του GDPR. Για την Ελλάδα η αρμόδια εποπτεύουσα αρχή είναι η ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

2.2 Ποιες είναι οι βασικές αλλαγές που προκύπτουν από την εφαρμογή του GDPR

2.2.1 Ατομικές ελευθερίες & προσωπικό απόρρητο

Όλα τα φυσικά πρόσωπα, τα «υποκείμενα» στα οποία ανήκουν δηλαδή τα δεδομένα, έχουν ολοκληρωμένα δικαιώματα διαχείρισης στα προσωπικά τους δεδομένα[20]. Συγκεκριμένα:

1. Δικαίωμα ενημέρωσης και πρόσβασης στα δεδομένα
2. Δικαίωμα διόρθωσης
3. Δικαίωμα περιορισμού της επεξεργασίας
4. Δικαίωμα εναντίωσης στην επεξεργασία
5. Δικαίωμα στη λήθη
6. Δικαίωμα στη φορητότητα των δεδομένων

2.2.2. Νεωτερισμοί του Κανονισμού

- Ενισχύεται η νομική θέση των πολιτών, με τη θέσπιση συγκεκριμένων δικαιωμάτων
- Επιβάλλονται νέες υποχρεώσεις στους υπεύθυνους επεξεργασίας της κάθε εταιρείας
- Θεσπίζονται νέα μοντέλα όπως privacy by design και privacy by default
- Εισάγεται η υποχρέωση γνωστοποίησης των παραβιάσεων δεδομένων
- Στο άρθρο 83 προβλέπονται βαρύτατες κυρώσεις για τους παραβάτες και υψηλότατα πρόστιμα (έως €20.000.000 ή έως το 4% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους μιας επιχείρησης, ανάλογα με το ποιο είναι υψηλότερο).
- Υπάρχει ειδική μνεία για τον τρόπο επεξεργασίας των Προσωπικών Δεδομένων ανήλικων ατόμων[21]

2.2.3. Διαφάνεια, γνωστοποιήσεις & συμμόρφωση

Όλοι οι οργανισμοί, οι εταιρείες και οι ελεύθεροι επαγγελματίες θα πρέπει να εφαρμόζουν πολιτικές & διαδικασίες σύμφωνα με τις οποίες:

- θα λαμβάνουν την συγκατάθεση για τη συλλογή και την επεξεργασία προσωπικών δεδομένων.

[20] www.dpa.gr

[21] Looking for needles in a haystack: Key issues affecting children's rights in the General Data Protection Regulation., Computer Law & Security Review. Apr2018, Vol. 34 Issue 2, p269-278. 10p., Lievens, Eva, Verdoodt, Valerie

- θα παρέχουν σαφή γνωστοποίηση για τη συλλογή και την επεξεργασία δεδομένων φυσικών προσώπων.
- θα περιγράφουν τους λόγους και τις περιπτώσεις επεξεργασίας των προσωπικών δεδομένων.
- θα τηρούν αρχεία που θα παρέχουν αναλυτικές πληροφορίες για τις διαδικασίες επεξεργασίας των δεδομένων.
- θα προστατεύουν τα προσωπικά δεδομένα λαμβάνοντας κατάλληλα μέτρα ασφαλείας στο εσωτερικό τους και στις επικοινωνίες τους με τρίτους.
- θα ορίζουν τις πολιτικές αποθήκευσης, διατήρησης, ασφαλούς φύλαξης και δια-γραφής δεδομένων τα οποία έχουν στην κατοχή τους, σε έντυπη και σε ηλεκτρονική μορφή.
- θα γνωστοποιούν εντός 72 ωρών στις Αρχές και στους ενδιαφερόμενους, τις παραβιάσεις προσωπικών δεδομένων.

2.2.4. Οι διαφορετικοί ρόλοι του GDPR

Ο προσδιορισμός της ιδιότητας του προσώπου που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα ως υπεύθυνου επεξεργασίας ή εκτελούντα την επεξεργασία είναι απαραίτητος για τον καθορισμό των υποχρεώσεών του.

Η υποχρέωση συμμόρφωσης με τις αρχές νόμιμης επεξεργασίας και η υποχρέωση τήρησης των διαδικασιών γνωστοποίησης στην τοπική εποπτική αρχή βαρύνουν πρωτίστως τον υπεύθυνο επεξεργασίας και όχι τον εκτελούντα την επεξεργασία.

Προκειμένου να γίνουν κατανοητά τα παραπάνω, κρίνεται απαραίτητο σε αυτό το σημείο να γίνει μια επεξήγηση των παραπάνω εννοιών:

Υπεύθυνος Επεξεργασίας: Το φυσικό ή νομικό πρόσωπο ή δημόσια αρχή που μόνο ή από κοινού καθορίζουν τους σκοπούς και τον τρόπο επεξεργασίας . Όταν αυτά καθορίζονται από το δίκαιο της Ε.Ε. ή το εθνικό δίκαιο ο υπεύθυνος επεξεργασίας ή τα κριτήρια ορισμού του μπορούν να καθορίζονται από το νομοθετικό πλαίσιο.

Εκτελών την Επεξεργασία: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας

Υπεύθυνος προστασίας δεδομένων: Προβλέπεται, υπό προϋποθέσεις, ο ορισμός «υπευθύνου προστασίας δεδομένων» (ΥΠΔ), ο οποίος έχει εχέγγυα ανεξαρτησίας και παρακολουθεί τη συμμόρφωση με τον νόμο αποτελώντας, συγχρόνως, το σημείο επαφής με την εθνική εποπτική αρχή.

Υποχρεωτικός είναι ο διορισμός υπεύθυνου επεξεργασίας όταν η επεξεργασία διενεργείται από δημόσια αρχή ή φορέα. Ο ΥΠΔ ενημερώνει τον υπεύθυνο επεξεργασίας για τις υποχρεώσεις του, παρακολουθεί τη συμμόρφωση με τον κανονισμό, παρέχει συμβουλές όσον αφορά την εκτίμηση αντικτύπου, συνεργάζεται με την εποπτική αρχή και ενεργεί ως σημείο επικοινωνίας για αυτήν, για ζητήματα που αφορούν την επεξεργασία.

Επεξεργασία δεδομένων: θεωρείται κάθε πράξη που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων ηλεκτρονικών μέσων, σε προσωπικά και ευαίσθητα προσωπικά δεδομένα. Επομένως η συλλογή, η οργάνωση, η αποθήκευση, η προσαρμογή, η χρήση, η διάδοση και η διαγραφή δεδομένων θεωρείται επεξεργασία δεδομένων.

2.2.5. Τι θεωρείται Προσωπικό Δεδομένο;

Κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»). Το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν τη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου

Προσωπικά δεδομένα ορίζονται όλα εκείνα τα στοιχεία που χαρακτηρίζουν ένα φυσικό πρόσωπο, όπως:

- Ονοματεπώνυμο
- Επάγγελμα
- Οικογενειακή κατάσταση
- Ηλικία
- Διεύθυνση κατοικίας
- Διεύθυνση ηλεκτρονικού ταχυδρομείου (email)
- Στοιχεία τραπεζικού λογαριασμού
- Διεύθυνση IP του ηλεκτρονικού υπολογιστή

Ειδικά (ευαίσθητα) προσωπικά δεδομένα ορίζονται τα δεδομένα που αφορούν:

- Ιατρικό ιστορικό (Διαγνώσεις, συνταγές, παραπομπές, παραπεμπτικά γνωματεύσεις, αποτελέσματα εργαστηριακών και απεικονιστικών εξετάσεων)
- φυλετική προέλευση
- εθνική προέλευση,

- πολιτικά φρονήματα και θρησκευτικές πεποιθήσεις,
- πληροφορίες σχετικές με την ερωτική ζωή,
- ποινικές διώξεις ή καταδίκες.

2.2.6. Βασική Ορολογία

Προσωπικά Δεδομένα

Ως «προσωπικά δεδομένα» ορίζονται η κάθε πληροφορία που αναφέρεται στο πρόσωπό του κάθε ατόμου, για παράδειγμα, το όνομα και το επάγγελμά του ατόμου, η οικογενειακή του κατάσταση, η ηλικία του, ο τόπος κατοικίας, η φυλετική του προέλευση, τα πολιτικά του φρονήματα, η θρησκεία που πιστεύει και ασκεί, οι φιλοσοφικές του απόψεις, η συνδικαλιστική του δράση, η υγεία του, η ερωτική του ζωή και οι τυχόν ποινικές του διώξεις και καταδίκες.

Ευαίσθητα δεδομένα

Τα δεδομένα που αφορούν στη φυλετική ή εθνική προέλευση, στα πολιτικά φρονήματα, στις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, στη συμμετοχή σε συνδικαλιστικές οργανώσεις, στην υγεία, στην κοινωνική πρόνοια και στην ερωτική ζωή, στα σχετικά με ποινικές διώξεις ή καταδίκες, καθώς και στη συμμετοχή σε συναφείς με τα ανωτέρω ενώσεις προσώπων. (άρθρο 2 Ν. 2472/1997)

Υποκείμενο δεδομένων

Φυσικό πρόσωπο στο οποίο αναφέρονται τα δεδομένα, και του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί (προσδιοριστεί) άμεσα ή έμμεσα πχ ΑΔΤ, ΑΦΜ, ΑΜΚΑ, Αρ. Διαβατηρίου, Αρ. πράσινης Κάρτας, Α.Μ. Ασφαλισμένου (ΕΦΚΑ) κλπ

Επεξεργασία

Κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων όπως η συλλογή, η οργάνωση, η αποθήκευση, η προσαρμογή, η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η κοινολόγηση με διαβίβαση, η διάδοση, η διαγραφή, η καταστροφή κλπ.

Υπεύθυνος Επεξεργασίας

Το φυσικό ή νομικό πρόσωπο ή δημόσια αρχή που μόνο ή από κοινού καθορίζουν τους σκοπούς και τον τρόπο επεξεργασίας . Όταν αυτά καθορίζονται από το δίκαιο της Ε.Ε. ή το εθνικό δίκαιο ο υπεύθυνος επεξεργασίας ή τα κριτήρια διορισμού του μπορούν να καθορίζονται από το νομοθετικό πλαίσιο.

Επομένως, εάν η διοίκηση του Οργανισμού αποφασίζει «γιατί» και «πώς» τα δεδομένα προσωπικού χαρακτήρα πρέπει να υποβάλλονται σε επεξεργασία, θεωρείται ο υπεύθυνος επεξεργασίας. Οι εργαζόμενοι που επεξεργάζονται δεδομένα προσωπικού χαρακτήρα εντός του Οργανισμού το κάνουν για να εκπληρώσουν τα καθήκοντα του Οργανισμού ως υπεύθυνου επεξεργασίας.

Εκτελών την επεξεργασία

Το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας

Τρίτος

Οποιοδήποτε φυσικό ή νομικό πρόσωπο, δημόσια αρχή, υπηρεσία ή φορέας, με εξαίρεση το υποκείμενο των δεδομένων, τον υπεύθυνο επεξεργασίας, τον εκτελούντα την επεξεργασία και τα πρόσωπα τα οποία, υπό την άμεση εποπτεία του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα

Αποδέκτης

Το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας, στα οποία κοινολογούνται τα δεδομένα προσωπικού χαρακτήρα, είτε πρόκειται για τρίτο είτε όχι.

Ωστόσο, οι δημόσιες αρχές που ενδέχεται να λάβουν δεδομένα προσωπικού χαρακτήρα στο πλαίσιο συγκεκριμένης έρευνας σύμφωνα με το δίκαιο της Ένωσης ή κράτους μέλους δεν θεωρούνται ως αποδέκτες· η επεξεργασία των δεδομένων αυτών από τις εν λόγω δημόσιες αρχές πραγματοποιείται σύμφωνα με τους ισχύοντες κανόνες προστασίας των δεδομένων ανάλογα με τους σκοπούς της επεξεργασίας

Συγκατάθεση

Κάθε ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, ρητή και εν πλήρη επίγνωση, με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν,

Σύστημα αρχειοθέτησης ή αρχείο δεδομένων

Κάθε διαρθρωμένο σύνολο δεδομένων τα οποία είναι προσβάσιμα με γνώμονα συγκεκριμένα κριτήρια είτε το σύνολο αυτό είναι συγκεντρωμένο είτε αποκεντρωμένο είτε κατανεμημένο ανά λειτουργική ή γεωγραφική βάση.

Ψευδωνυμοποίηση

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο ώστε τα δεδομένα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρωματικές πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλιστεί ότι δεν μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο.

Παραβίαση δεδομένων προσωπικού χαρακτήρα

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.

Γενετικά δεδομένα

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

Βιομετρικά δεδομένα

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

Δεδομένα που αφορούν την υγεία

Δεδομένα προσωπικού χαρακτήρα τα οποία σχετίζονται με τη σωματική ή ψυχική υγεία ενός φυσικού προσώπου, περιλαμβανομένης της παροχής υπηρεσιών υγειονομικής φροντίδας, και τα οποία αποκαλύπτουν πληροφορίες σχετικά με την κατάσταση της υγείας του.

Αρχεία των δραστηριοτήτων επεξεργασίας

Κάθε υπεύθυνος επεξεργασίας και, κατά περίπτωση, ο εκπρόσωπός του, τηρεί αρχείο των δραστηριοτήτων επεξεργασίας για τις οποίες είναι υπεύθυνος.

Εκτίμηση Αντικτύπου

Όταν ένα είδος επεξεργασίας, ιδίως με τη χρήση νέων τεχνολογιών και συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας ενδέχεται να επιφέρει υψηλό

κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας διενεργεί, πριν από την επεξεργασία, εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία των δεδομένων.

Υπεύθυνος Προστασίας Δεδομένων

Ο Υπεύθυνος Προστασίας Δεδομένων (ΥΠΔ) μεριμνά, με ανεξάρτητο τρόπο, για την ορθή εφαρμογή από τον φορέα του (νομικό πρόσωπο δημόσιου ή ιδιωτικού δικαίου, δημόσιος οργανισμός, εταιρεία κλπ.) της νομοθεσίας περί προστασίας των προσωπικών δεδομένων. Ο Υπεύθυνος Προστασίας Δεδομένων τηρεί μητρώο όπου καταγράφονται όλες οι πράξεις επεξεργασίας προσωπικών δεδομένων από τον φορέα του[22].

[22] Κανονισμός 2016/679 του Ευρωπαϊκού Κοινοβουλίου

Κεφάλαιο 3
Αναλυτική παρουσίαση των Γενικών Διατάξεων του GDPR

Στο παρόν τμήμα της διπλωματικής εργασίας αποτυπώνεται η διάρθρωση του GDPR. Στην αρχή κάθε κεφαλαίου παρατίθεται πληροφορίες για τον αριθμό των άρθρων που περιλαμβάνει το κάθε κεφάλαιο καθώς και μια σύντομη περίληψη των όσων περιγράφονται στα άρθρα που αποτελούν το κάθε κεφάλαιο.

Εν συνεχεία υπάρχει μια αναλυτική καταγραφή των τίτλων των άρθρων του κάθε κεφαλαίου, μαζί με μια συνοπτική περίληψη του περιεχομένου του κάθε άρθρου. Κατά αυτό τον τρόπο μπορεί κάποιος να δει συνοπτικά τη διάρθρωση του GDPR και σύντομες πληροφορίες για το τι περιλαμβάνει το κάθε άρθρο, ώστε εν συνεχεία να ανατρέξει στο πλήρες κείμενο του κανονισμού για τις αναλυτικές πληροφορίες.

Στο τέλος του κεφαλαίου γίνεται μια αποτίμηση των κεφαλαίων και άρθρων σχετικά με τη σημαντικότητα του κάθε ενός.

Ο GDPR περιλαμβάνει 11 γενικά κεφάλαια, τα οποία χωρίζονται σε 99 ειδικά άρθρα. Κάθε άρθρο ουσιαστικά ορίζει τις επιμέρους αρχές του GDPR, έτσι ώστε στο σύνολό του ο GDPR να είναι πλήρες και να καλύπτει το σύνολο των απαιτήσεων για το πώς η Επιτροπή θεωρεί ότι θα πρέπει να προστατεύονται τα Προσωπικά Δεδομένα.

Συγκεκριμένα:

ΚΕΦΑΛΑΙΟ 1: ΓΕΝΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Το κεφάλαιο αυτό, που αποτελείται από 4 άρθρα, παρουσιάζει τον GDPR, που αυτός εφαρμόζεται καθώς και περιγράφει και συγκεκριμενοποιεί τους ορισμούς που χρησιμοποιούνται στον Κανονισμό. Συγκεκριμένα:

Άρθρο 1. Αντικείμενο και στόχοι

Το άρθρο αυτό περιγράφει το γενικό αντικείμενο και τους στόχους του Κανονισμού

Άρθρο 2. Ουσιαστικό πεδίο εφαρμογής

Το άρθρο αυτό παρουσιάζει τις περιπτώσεις εκείνες για τις οποίες ο Κανονισμός θα πρέπει να εφαρμόζεται. Επίσης, κάνει ειδική αναφορά για τις περιπτώσεις όπου ο Κανονισμός δεν έχει υποχρεωτική εφαρμογή.

Άρθρο 3. Εδαφικό πεδίο εφαρμογής

Το παρόν άρθρο επεξηγεί τις περιπτώσεις που ο Κανονισμός έχει εφαρμογή σε σχέση με τη Γεωγραφική Περιοχή της Ευρωπαϊκής Ένωσης.

Άρθρο 4. Ορισμοί

Το παρόν άρθρο εξηγεί τους ορισμούς των εννοιών που χρησιμοποιούνται στον Κανονισμό.

ΚΕΦΑΛΑΙΟ 2: ΑΡΧΕΣ

Το κεφάλαιο αυτό, που αποτελείται από 7 άρθρα, παρουσιάζει τις βασικές αρχές που διέπουν τον Κανονισμό, τις προϋποθέσεις που πρέπει να τηρούνται για να αποδεικνύεται η συγκατάθεση του φυσικού προσώπου για την επεξεργασία των δεδομένων του, καθώς και οι ειδικές κατηγορίες επεξεργασίας προσωπικών δεδομένων[23]. Συγκεκριμένα:

Άρθρο 5. Αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα

Επεξηγούνται οι αρχές πάνω στις οποίες βασίζεται η ορθή κατά τον Κανονισμό επεξεργασία των προσωπικών δεδομένων

Άρθρο 6. Νομιμότητα της επεξεργασίας

Ορίζονται οι προϋποθέσεις κατά τις οποίες η επεξεργασία των προσωπικών δεδομένων είναι νόμιμη.

Άρθρο 7. Προϋποθέσεις για συγκατάθεση

Ορίζονται οι προϋποθέσεις που πρέπει να τηρούνται ώστε να αποδεικνύεται η συγκατάθεση του φυσικού προσώπου για την επεξεργασία των δεδομένων του.

Άρθρο 8. Προϋποθέσεις που ισχύουν για τη συγκατάθεση παιδιού σε σχέση με τις υπηρεσίες της κοινωνίας των πληροφοριών

Γίνεται ειδική αναφορά στις περιπτώσεις συγκατάθεσης για ανήλικους.

Άρθρο 9. Επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα

[23] GDPR: A new challenge for personal data protection, Authors: Mraznica Erne, Source: Bankarstvo, Vol 46, Iss 4, Pp 166-177 (2017)

Συγκεκριμενοποιούνται οι κατηγορίες προσωπικών δεδομένων που απαγορεύεται να επεξεργάζονται και οι περιπτώσεις που αυτές οι κατηγορίες είναι εφικτό να επεξεργάζονται.

Άρθρο 10. Επεξεργασία δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα

Ορίζονται οι προϋποθέσεις επεξεργασίας δεδομένων για ποινικούς σκοπούς.

Άρθρο 11. Επεξεργασία η οποία δεν απαιτεί εξακρίβωση ταυτότητας

Ορίζονται οι διαδικασίες επεξεργασίας δεδομένων που δεν είναι απαραίτητη η εξακρίβωση στοιχείων.

ΚΕΦΑΛΑΙΟ 3: ΔΙΚΑΙΩΜΑΤΑ ΤΟΥ ΥΠΟΚΕΙΜΕΝΟΥ ΤΩΝ ΔΕΔΟΜΕΝΩΝ

Στο κεφάλαιο αυτό, που αποτελείται από 12 άρθρα, παρουσιάζει τα βασικά δικαιώματα των φυσικών προσώπων σχετικά με τα προσωπικά τους δεδομένα (όπως το δικαίωμα πρόσβασης, διόρθωσης, διαγραφής και περιορισμού), καθώς και τις υποχρεώσεις των φυσικών προσώπων που προβαίνουν σε επεξεργασία Προσωπικών Δεδομένων[24]. Συγκεκριμένα:

Άρθρο 12. Διαφανής ενημέρωση, ανακοίνωση και ρυθμίσεις για την άσκηση των δικαιωμάτων του υποκειμένου των δεδομένων

Ορίζονται οι υποχρεώσεις που έχει όποιος επεξεργάζεται προσωπικά δεδομένα σχετικά με την ενημέρωση του φυσικού προσώπου για την επεξεργασία των δεδομένων του

Άρθρο 13. Πληροφορίες που παρέχονται εάν τα δεδομένα προσωπικού χαρακτήρα συλλέγονται από το υποκείμενο των δεδομένων

Ορίζονται οι προδιαγραφές που πρέπει να πληρούνται σε σχέση με την ενημέρωση του φυσικού προσώπου που αυτοβούλως έχει παράσχει προς επεξεργασία, σχετικά με τον τρόπο με τον οποίο επεξεργάζονται τα προσωπικά δεδομένα.

Άρθρο 14. Πληροφορίες που παρέχονται εάν τα δεδομένα προσωπικού χαρακτήρα δεν έχουν συλλεγεί από το υποκείμενο των δεδομένων

Ορίζονται οι πληροφορίες που πρέπει να παρέχονται σε ένα φυσικό πρόσωπο που δεν έχει παράσχει τα προσωπικά του δεδομένα

[24] A partial overview of the data subjects' control over their personal data under the general data protection regulation. Authors: BÂRSAN, Maria-Magdalena, Source: Bulletin of the Transilvania University of Brasov. Series VII: Social Sciences. Law. 2018, Vol. 11 Issue 2, p129-134. 6p.).

Άρθρο 15. Δικαίωμα πρόσβασης του υποκειμένου των δεδομένων

Ορίζονται οι πληροφορίες που πρέπει να είναι διαθέσιμες στον ιδιοκτήτη των προσωπικών δεδομένων σχετικά με το δικαίωμα πρόσβασης.

Άρθρο 16. Δικαίωμα διόρθωσης

Ορίζονται οι πληροφορίες που πρέπει να είναι διαθέσιμες στον ιδιοκτήτη των προσωπικών δεδομένων σχετικά με το δικαίωμα διόρθωσης.

Άρθρο 17. Δικαίωμα διαγραφής («δικαίωμα στη λήθη»)

Ορίζονται οι πληροφορίες που πρέπει να είναι διαθέσιμες στον ιδιοκτήτη των προσωπικών δεδομένων σχετικά με το δικαίωμα διαγραφής.

Άρθρο 18. Δικαίωμα περιορισμού της επεξεργασίας

Ορίζονται οι πληροφορίες που πρέπει να είναι διαθέσιμες στον ιδιοκτήτη των προσωπικών δεδομένων σχετικά με το δικαίωμα περιορισμού της επεξεργασίας των δεδομένων.

Άρθρο 19. Υποχρέωση γνωστοποίησης όσον αφορά τη διόρθωση ή τη διαγραφή δεδομένων προσωπικού χαρακτήρα ή τον περιορισμό της επεξεργασίας

Εισάγεται η έννοια της υποχρέωσης γνωστοποίησης διόρθωσης και διαγραφής στους αποδέκτες και τον ιδιοκτήτη των δεδομένων.

Άρθρο 20. Δικαίωμα στη φορητότητα των δεδομένων

Εισάγεται το δικαίωμα της φορητότητας των δεδομένων που έχει συλλέξει ένας οργανισμός σε έναν άλλο κατόπιν εντολής του ιδιοκτήτη των δεδομένων

Άρθρο 21. Δικαίωμα εναντίωσης

Εισάγονται οι προϋποθέσεις και τα δικαιώματα που έχει ένας ιδιοκτήτης δεδομένων, σχετικά με την άρνησή του στην επεξεργασία τους.

Άρθρο 22. Αυτοματοποιημένη ατομική λήψη αποφάσεων, περιλαμβανομένης της κατάρτισης προφίλ

Συγκεκριμενοποιούνται περιπτώσεις και περιορισμοί που έχουν να κάνουν με την αυτοματοποιημένη επεξεργασία και κατάρτιση προφίλ

Άρθρο 23. Περιορισμοί

Περιγράφονται οι περιορισμοί στα προηγούμενα άρθρα που αφορούν την εναντίωσης και αυτοματοποιημένη ατομική λήψη αποφάσεων

ΚΕΦΑΛΑΙΟ 4: ΥΠΕΥΘΥΝΟΣ ΕΠΕΞΕΡΓΑΣΙΑΣ ΚΑΙ ΕΚΤΕΛΩΝ ΤΗΝ ΕΠΕΞΕΡΓΑΣΙΑ

Στο κεφάλαιο αυτό, που αποτελείται από 20 άρθρα, είναι ένα πολύ σημαντικό κεφάλαιο γιατί εισάγει και συγκεκριμενοποιεί νέους υποχρεωτικούς ρόλους και όρους (όπως ο Υπεύθυνος Επεξεργασίας, ο εκτελών την επεξεργασία, η από κοινού επεξεργασία). Παράλληλα, συγκεκριμενοποιεί την τεκμηρίωση που πρέπει να κρατείται, τους τρόπους συνεργασίας με τις αρμόδιες αρχές και τις υποχρεώσεις σε περίπτωση παραβίασης προσωπικών δεδομένων. Ορίζεται σαφώς ο ρόλος του Υπεύθυνου Προστασίας σε κάθε επιχείρηση καθώς και οι τρόπου πιστοποίησης του[25]. Συγκεκριμένα:

Άρθρο 24. Ευθύνη του υπευθύνου επεξεργασίας

Περιγράφονται οι ευθύνες του Υπευθύνου Επεξεργασίας

Άρθρο 25. Προστασία των δεδομένων ήδη από το σχεδιασμό και εξ ορισμού

Περιγράφονται τα μέτρα που πρέπει να λαμβάνονται κατά το σχεδιασμό της διαδικασίας επεξεργασίας προσωπικών δεδομένων.

Άρθρο 26. Από κοινού υπεύθυνοι επεξεργασίας

Ορίζεται η έννοια της από κοινού επεξεργασίας

Άρθρο 27. Εκπρόσωποι υπευθύνων επεξεργασίας ή εκτελούντων την επεξεργασία μη εγκατεστημένων στην Ένωση

Ορίζονται τα απαιτούμενα μέτρα στην περίπτωση που η επεξεργασία γίνεται εκτός Ευρωπαϊκής Ένωσης.

Άρθρο 28. Εκτελών την επεξεργασία

Ορίζεται η έννοια και τα μέτρα που πρέπει να λαμβάνει ο Εκτελών την Επεξεργασία.

Άρθρο 29. Επεξεργασία υπό την εποπτεία του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία

Ορίζεται το πότε μπορεί να γίνεται επεξεργασία.

Άρθρο 30. Αρχεία των δραστηριοτήτων επεξεργασίας

[25] EU GDPR : A Pocket Guide, Authors: Calder, Alan, Publication Information: Ely : IT Governance Publishing. 2016

Ορίζονται τα αρχεία που πρέπει να τηρούνται για την επεξεργασία προσωπικών δεδομένων.

Άρθρο 31. Συνεργασία με την εποπτική αρχή

Γίνεται σαφής η υποχρεωτικότητα της συνεργασίας με την εποπτική αρχή.

Άρθρο 32. Ασφάλεια επεξεργασίας

Ορίζονται τα μέτρα που πρέπει να λαμβάνονται προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων

Άρθρο 33. Γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα στην εποπτική αρχή

Εισάγεται η υποχρέωση ενημέρωσης της εποπτικής αρχής σε περιπτώσεις παραβίασης προσωπικών δεδομένων

Άρθρο 34. Ανακοίνωση παραβίασης δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων

Εισάγεται η υποχρέωση ενημέρωσης των ιδιοκτητών των προσωπικών δεδομένων σε περιπτώσεις παραβίασης προσωπικών δεδομένων

Άρθρο 35. Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων

Περιγράφεται η διαδικασία και οι προδιαγραφές της Εκτίμησης Αντικτύπου που πρέπει να κάνει ο οργανισμός.

Άρθρο 36. Προηγούμενη διαβούλευση

Ορίζεται η διαδικασία συνεργασίας με την Εποπτική Αρχή για τη δημιουργία της Εκτίμησης Αντικτύπου.

Άρθρο 37. Ορισμός του υπευθύνου προστασίας δεδομένων

Εισάγεται η έννοια και οι δεξιότητες που πρέπει να κατέχει ο υπεύθυνος προστασίας δεδομένων

Άρθρο 38. Θέση του υπευθύνου προστασίας δεδομένων

Περιγράφεται ο τρόπος συνεργασίας του υπεύθυνου προστασίας δεδομένων με τα υπόλοιπα στελέχη που εμπλέκονται κατά την επεξεργασία των προσωπικών δεδομένων.

Άρθρο 39. Καθήκοντα του υπευθύνου προστασίας δεδομένων

Ορίζονται τα κατ' ελάχιστο καθήκοντα του υπευθύνου προστασίας δεδομένων

Άρθρο 40. Κώδικες δεοντολογίας

Ορίζονται οι προδιαγραφές και ο τρόπος δημιουργίας του Κώδικα Δεοντολογίας για όσους εμπλέκονται κατά την επεξεργασία των προσωπικών δεδομένων

Άρθρο 41. Παρακολούθηση των εγκεκριμένων κωδίκων δεοντολογίας

Ορίζεται ο τρόπος παρακολούθησης των εγκεκριμένων κωδίκων δεοντολογίας από τις αρμόδιες εποπτικές αρχές

Άρθρο 42. Πιστοποίηση

Ορίζονται οι έννοιες και οι βασικές απαιτήσεις για τη δημιουργία μηχανισμών πιστοποίησης σχετικά με τη συμμόρφωση της προστασίας Προσωπικών Δεδομένων.

Άρθρο 43. Φορείς πιστοποίησης

Ορίζονται οι έννοιες και οι βασικές απαιτήσεις για τη δημιουργία φορέων πιστοποίησης που χορηγούν πιστοποιήσεις σχετικά με τη συμμόρφωση της προστασίας Προσωπικών Δεδομένων.

ΚΕΦΑΛΑΙΟ 5: ΔΙΑΒΙΒΑΣΕΙΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ ΠΡΟΣ ΤΡΙΤΕΣ ΧΩΡΕΣ Η ΔΙΕΘΝΕΙΣ ΟΡΓΑΝΙΣΜΟΥΣ

Το κεφάλαιο αυτό, που αποτελείται από 7 άρθρα, συγκεκριμενοποιεί τις προϋποθέσεις υπό τις οποίες επιτρέπεται η διαβίβαση Προσωπικών Δεδομένων εκτός Ευρωπαϊκής Ένωσης[26]. Συγκεκριμένα:

Άρθρο 44. Γενικές αρχές για διαβιβάσεις

Εισάγονται οι βασικές αρχές που διέπουν τις διαβιβάσεις προσωπικών δεδομένων εκτός Ευρωπαϊκής Ένωσης.

Άρθρο 45. Διαβιβάσεις βάσει απόφαση επάρκειας

Ορίζονται οι προϋποθέσεις επάρκειας προκειμένου να μην απαιτείται ειδική άδεια διαβίβασης προσωπικών δεδομένων εκτός Ευρωπαϊκής Ένωσης.

Άρθρο 46. Διαβιβάσεις που υπόκεινται σε κατάλληλες εγγυήσεις

Ορίζονται οι προϋποθέσεις εγγυήσεων που πρέπει να παρέχονται προκειμένου να μην απαιτείται ειδική άδεια διαβίβασης προσωπικών δεδομένων εκτός Ευρωπαϊκής Ένωσης

[26] The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection?, Authors: Wagner, Julian, Source: International Data Privacy Law. Nov 2018, Vol. 8 Issue 4, p318, 20 p., Publisher Information: Oxford University Press, Publication Year: 2018

Άρθρο 47. Δεσμευτικοί εταιρικοί κανόνες

Ορίζονται και περιγράφονται οι όροι και οι προδιαγραφές για τους δεσμευτικούς εταιρικούς κανόνες που εγκρίνει η εποπτική αρχή

Άρθρο 48. Διαβιβάσεις ή κοινοποιήσεις που δεν επιτρέπονται από το δίκαιο της Ένωσης

Ορίζονται οι διαβιβάσεις ή κοινοποιήσεις προσωπικών δεδομένων που δεν επιτρέπονται από το δίκαιο της Ένωσης

Άρθρο 49. Παρεκκλίσεις για ειδικές καταστάσεις

Περιγράφονται ειδικές περιπτώσεις για τις διαβιβάσεις προσωπικών δεδομένων εκτός Ευρωπαϊκής Ένωσης.

Άρθρο 50. Διεθνής συνεργασία για την προστασία δεδομένων προσωπικού χαρακτήρα

Ορίζεται η υποχρέωση συνεργασίας με τρίτες χώρες και διεθνείς οργανισμούς σχετικά με τις διαβιβάσεις προσωπικών δεδομένων.

ΚΕΦΑΛΑΙΟ 6: ΑΝΕΞΑΡΤΗΤΕΣ ΕΠΟΠΤΙΚΕΣ ΑΡΧΕΣ

Το κεφάλαιο αυτό, που αποτελείται από 9 άρθρα, περιγράφει το ρόλο των Εποπτικών Αρχών που πρέπει να υπάρχουν σε κάθε χώρα της Ευρωπαϊκής Ένωσης καθώς και τους τρόπους λειτουργίας τους. Συγκεκριμένα:

Άρθρο 51. Εποπτική αρχή

Εισάγεται και περιγράφεται η έννοια της εποπτικής αρχής.

Άρθρο 52. Ανεξαρτησία

Ορίζεται σαφώς η ανεξαρτησία της εκάστοτε Εποπτικής Αρχής.

Άρθρο 53. Γενικές προϋποθέσεις για τα μέλη της εποπτικής αρχής

Περιγράφονται οι προδιαγραφές των μελών της εκάστοτε Εποπτικής Αρχής

Άρθρο 54. Κανόνες για τη σύσταση της εποπτικής αρχής

Εισάγονται οι κανόνες δημιουργίας και λειτουργίας της εκάστοτε Εποπτικής Αρχής

Άρθρο 55. Αρμοδιότητα

Εισάγονται οι αρμοδιότητες της Εποπτικής Αρχής

Άρθρο 56. Αρμοδιότητα της επικεφαλής εποπτικής αρχής

Εισάγονται οι αρμοδιότητες της της επικεφαλής εποπτικής αρχής

Άρθρο 57. Καθήκοντα

Ορίζονται τα καθήκοντα της εκάστοτε εποπτικής αρχής

Άρθρο 58. Εξουσίες

Ορίζονται οι εξουσίες της εκάστοτε εποπτικής αρχής

Άρθρο 59. Εκθέσεις δραστηριοτήτων

Ορίζεται η υποχρέωση ετήσιας έκθεσης δραστηριοτήτων της εκάστοτε εποπτικής αρχής

ΚΕΦΑΛΑΙΟ 7: ΣΥΝΕΡΓΑΣΙΑ ΚΑΙ ΣΥΝΕΚΤΙΚΟΤΗΤΑ

Το κεφάλαιο αυτό, που περιέχει 17 άρθρα, παρουσιάζει τους τρόπους συνεργασίας της επικεφαλής εποπτικής αρχής με τις επιμέρους εποπτικές αρχές και ορίζεται το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων και ο τρόπος λειτουργίας του. Συγκεκριμένα:

Άρθρο 60. Συνεργασία μεταξύ της επικεφαλής εποπτικής αρχής και των άλλων ενδιαφερόμενων εποπτικών αρχών

Ορίζεται η διαδικασία συνεργασίας της επικεφαλής εποπτικής αρχής και πιθανών άλλων εποπτικών αρχών.

Άρθρο 61. Αμοιβαία συνδρομή

Ορίζεται η υποχρεωτικότητα συνεργασίας και αμοιβαίας συνδρομής των εποπτικών αρχών

Άρθρο 62. Κοινές επιχειρήσεις αρχών ελέγχου

Προσδιορίζονται οι προϋποθέσεις για τη διενέργεια κοινών επιχειρήσεων ελέγχου από διαφορετικές εποπτικές αρχές.

Άρθρο 63. Μηχανισμός συνεκτικότητας

Εισάγεται η έννοια του μηχανισμού συνεκτικότητας

Άρθρο 64. Γνώμη του Συμβουλίου

Ορίζονται οι προϋποθέσεις και η διαδικασία για τη χορήγηση γνώμης του Συμβουλίου Προστασίας Δεδομένων

Άρθρο 65. Επίλυση διαφορών από το Συμβούλιο Προστασίας Δεδομένων

Ορίζονται οι περιπτώσεις και η διαδικασία όπου το Συμβούλιο Προστασίας Δεδομένων εκδίδει δεσμευτική απόφαση για την επίλυση τυχόν διαφορών

Άρθρο 66. Επείγουσα διαδικασία

Ορίζεται η διαδικασία λήψης έκτακτων μέτρων και επείγουσας απόφασης από το Συμβούλιο Προστασίας Δεδομένων

Άρθρο 67. Ανταλλαγή πληροφοριών

Εισάγεται η δυνατότητα της επιτροπής να εκδίδει εκτελεστικές πράξεις γενικής εμβέλειας

Άρθρο 68. Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων

Εισάγεται και περιγράφεται η έννοια του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων.

Άρθρο 69. Ανεξαρτησία

Ορίζεται η ανεξαρτησία του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων

Άρθρο 70. Καθήκοντα του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων

Ορίζονται και περιγράφονται τα καθήκοντα του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων

Άρθρο 71. Εκθέσεις

Ορίζεται η υποχρέωση του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων για τη δημοσιοποίηση ετήσιας έκθεσης

Άρθρο 72. Διαδικασία

Περιγράφεται ο τρόπος λήψης αποφάσεων και έγκρισης του Εσωτερικού Κανονισμού του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων

Άρθρο 73. Πρόεδρος

Ορίζεται η θέση του Προέδρου του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων

Άρθρο 74. Καθήκοντα του Προέδρου

Περιγράφονται τα καθήκοντα του Προέδρου του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων

Άρθρο 75. Γραμματεία

Ορίζεται και περιγράφεται η θέση και οι αρμοδιότητες της Γραμματείας του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων

Άρθρο 76. Εμπιστευτικότητα

Προσδιορίζεται η τήρηση της εμπιστευτικότητας για τις εργασίες του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων

ΚΕΦΑΛΑΙΟ 8: ΠΡΟΣΦΥΓΕΣ, ΕΥΘΥΝΗ ΚΑΙ ΚΥΡΩΣΕΙΣ

Το κεφάλαιο αυτό, που περιέχει 8 άρθρα, περιγράφει τις διαδικασίες προσφυγής και κυρώσεων σε και εναντίον Εποπτικών Αρχών και Υπευθύνων Επεξεργασίας. Το πιο σημαντικό όμως μέρος του κεφαλαίου αυτού είναι ότι για πρώτη φορά συγκεκριμενοποιούνται τα χρηματικά και δικαιωματικά πρόστιμα για περιπτώσεις παραβίασης του εν λόγω κανονισμού[27]. Συγκεκριμένα:

Άρθρο 77. Δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή

Ορίζεται το δικαίωμα υποβολής καταγγελίας για παραβάσεις του Κανονισμού

Άρθρο 78. Δικαίωμα πραγματικής δικαστικής προσφυγής κατά αρχής ελέγχου

Ορίζεται το δικαίωμα και οι διαδικασίες δικαστικής προσφυγής κατά εποπτικής αρχής ελέγχου για παραβάσεις του Κανονισμού

Άρθρο 79. Δικαίωμα πραγματικής δικαστικής προσφυγής κατά υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία

Ορίζεται το δικαίωμα και οι διαδικασίες δικαστικής προσφυγής κατά υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία για παραβάσεις του Κανονισμού

Άρθρο 80. Εκπροσώπηση υποκειμένων των δεδομένων

Ορίζεται ο τρόπος εκπροσώπησης των ιδιοκτητών των προσωπικών δεδομένων σε περιπτώσεις καταγγελίας

Άρθρο 81. Αναστολή των διαδικασιών

Ορίζονται οι προϋποθέσεις αναστολής δικαιοδοσίας δικαστηρίου για περιπτώσεις κοινών υποθέσεων

Άρθρο 82. Δικαίωμα αποζημίωσης και ευθύνη

Ορίζεται το δικαίωμα αποζημίωσης σε όποιον έχει δημιουργηθεί ζημία από την επεξεργασία προσωπικών δεδομένων.

[27] GDPR: Does Coverage Exist for Fines and Penalties for Noncompliance? Authors: Reetz, Margaret, Source: TortSource. Spring2019, Vol. 21 Issue 3, p8-10. 3p.

Άρθρο 83. Γενικοί όροι επιβολής διοικητικών προστίμων

Ορίζονται οι όροι, οι προϋποθέσεις και το ύψος των διοικητικών προστίμων για παραβάσεις του Κανονισμού.

Άρθρο 84. Κυρώσεις

Ορίζεται η διαδικασία επιβολής κυρώσεων για παραβάσεις του Κανονισμού

ΚΕΦΑΛΑΙΟ 9: ΔΙΑΤΑΞΕΙΣ ΠΟΥ ΑΦΟΡΟΥΝ ΕΙΔΙΚΕΣ ΠΕΡΙΠΤΩΣΕΙΣ ΕΠΕΞΕΡΓΑΣΙΑΣ

Στο κεφάλαιο αυτό, που αποτελείται από 7 άρθρα, συγκεκριμενοποιούνται οι όροι επεξεργασίας προσωπικών δεδομένων για ειδικές κατηγορίες, όπως η έρευνα, τα επίσημα κρατικά έγγραφα και η θρησκευτική πίστη. Συγκεκριμένα:

Άρθρο 85. Επεξεργασία και ελευθερία έκφρασης και πληροφόρησης

Περιγράφεται η διαδικασία διαφύλαξης της ελεύθερης έκφρασης και πληροφόρησης για δημοσιογραφικούς σκοπούς ή για σκοπούς ακαδημαϊκής, καλλιτεχνικής ή λογοτεχνικής έκφρασης

Άρθρο 86. Επεξεργασία και πρόσβαση του κοινού σε επίσημα έγγραφα

Περιγράφεται η διαδικασία κοινοποίησης προσωπικών δεδομένων για λόγους δημοσίου συμφέροντος.

Άρθρο 87. Επεξεργασία του εθνικού αριθμού ταυτότητας

Ορίζεται ο όρος και η προδιαγραφές χρήσης του εθνικού αριθμού ταυτότητας

Άρθρο 88. Επεξεργασία στο πλαίσιο της απασχόλησης

Ορίζεται η υποχρέωση θέσπισης κανόνων για την επεξεργασία προσωπικών δεδομένων στο ευρύτερο πλαίσιο της απασχόλησης.

Άρθρο 89. Διασφαλίσεις και παρεκκλίσεις σχετικά με την επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς

Ορίζονται οι εγγυήσεις, οι παρεκκλίσεις και η διαδικασία επεξεργασίας για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή επιστημονικής, ιστορικής έρευνας ή στατιστικούς σκοπούς

Άρθρο 90. Υποχρεώσεις τήρησης απορρήτου

Ορίζεται η υποχρέωση τήρησης του επαγγελματικού απορρήτου για να συμβιβαστεί το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα με την υποχρέωση τήρησης του απορρήτου.

Άρθρο 91. Υφιστάμενοι κανόνες προστασίας των δεδομένων εκκλησιών και θρησκευτικών ενώσεων

Περιγράφεται η υποχρέωση εναρμόνισης υπαρχόντων διαδικασιών προστασίας των δεδομένων εκκλησιών και θρησκευτικών ενώσεων με τον Κανονισμό.

ΚΕΦΑΛΑΙΟ 10: ΚΑΤ' ΕΞΟΥΣΙΟΔΟΤΗΣΗ ΠΡΑΞΕΙΣ ΚΑΙ ΕΚΤΕΛΕΣΤΙΚΕΣ ΠΡΑΞΕΙΣ

Στο κεφάλαιο αυτό, που αποτελείται από 2 άρθρα, περιγράφονται τον τρόπο λειτουργίας της επιτροπής για το δικαίωμα της εξουσιοδότησης. Συγκεκριμένα:

Άρθρο 92. Άσκηση της εξουσιοδότησης

Ορίζονται οι προϋποθέσεις και η διαδικασία που αναθέτει το δικαίωμα εξουσιοδότησης στην Επιτροπή.

Άρθρο 93. Διαδικασία επιτροπής

Ορίζεται η δημιουργία και οι όροι λειτουργίας ειδικής επιτροπής που επικουρεί την Ευρωπαϊκή Επιτροπή για την άσκηση του δικαιώματος εξουσιοδότησης.

ΚΕΦΑΛΑΙΟ 11: ΤΕΛΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Το τελευταίο κεφάλαιο, που αποτελείται από 6 άρθρα, είναι ένα τυπικό κεφάλαιο που ουσιαστικά ενεργοποιεί τον GDPR και καταργεί όλες τις υπόλοιπες σχετικές διατάξεις. Συγκεκριμένα:

Άρθρο 94. Κατάργηση της οδηγίας 95/46/ΕΚ

Ορίζεται η κατάργηση της οδηγίας 95/46/ΕΚ

Άρθρο 95. Σχέση με την οδηγία 2002/58/ΕΚ

Ορίζεται η σχέση του Κανονισμού με την οδηγία 2002/58/ΕΚ

Άρθρο 96. Σχέση με συμφωνίες που έχουν συναφθεί παλαιότερα

Ορίζεται η σχέση του Κανονισμού με συμφωνίες που έχουν συναφθεί παλαιότερα

Άρθρο 97. Εκθέσεις της Επιτροπής

Ορίζεται η περιοδικότητα και η διαδικασία δημοσιοποίησης των Εκθέσεων της Επιτροπής.

Άρθρο 98. Επισκόπηση άλλων νομικών πράξεων της Ένωσης για την προστασία των δεδομένων

Ορίζεται το δικαίωμα της επιτροπής να υποβάλλει νομοθετικές προτάσεις για την τροποποίηση άλλων νομικών πράξεων της Ένωσης σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα

Άρθρο 99. Έναρξη ισχύος και εφαρμογή

Ορίζεται η έναρξη ισχύος του Κανονισμού.

Από την παραπάνω περίληψη των Κεφαλαίων και των Άρθρων του Κανονισμού διαφαίνεται ότι το κεφάλαιο 3 είναι ένα από τα πιο σημαντικά κεφάλαια του Κανονισμού, διότι ορίζει τα βασικά δικαιώματα των Φυσικών Προσώπων, σε σχέση με τον τρόπο που αυτά επιθυμούν να διαχειρίζονται οι διάφοροι οργανισμοί τα Προσωπικά τους δεδομένα. Πλέον ο οποιοσδήποτε γνωρίζει τι δικαιώματα έχει και μπορεί να απαιτήσει όταν δεν γίνεται ορθή επεξεργασία των προσωπικών του Δεδομένων. Παραδείγματος χάριν, το άρθρο 17 μιλά για το δικαίωμα λήθης. Αυτό σημαίνει ότι ένα φυσικό πρόσωπο που εν γνώσει του έδωσε τα προσωπικά του δεδομένα σε έναν οργανισμό για να τα επεξεργαστεί στο πλαίσιο των υπηρεσιών που προσέφερε, πλέον έχει το δικαίωμα να ζητήσει από τον οργανισμό αυτό να διαγράψει τα προσωπικά του δεδομένα, αφού δεν λαμβάνει πλέον τις υπηρεσίες του οργανισμού. Έτσι, ο οργανισμός αυτός δεν θα μπορεί να χρησιμοποιήσει αυτά τα δεδομένα για λόγους διαφήμισης/marketing στο μέλλον χωρίς την εκ νέου έγκριση του φυσικού προσώπου. Παράλληλα, το κεφάλαιο αυτό εισάγει και συγκεκριμενοποιεί για πρώτη φορά τις υποχρεώσεις των ατόμων που επεξεργάζονται Προσωπικά Δεδομένα στο πλαίσιο των εταιρικών τους καθηκόντων. Συνεπώς όσοι επεξεργάζονται Προσωπικά Δεδομένα έχουν πλέον το πλαίσιο στο οποίο πρέπει να κινούνται, ώστε η εργασία τους να είναι συμβατή με τον Κανονισμό.

Επίσης, το κεφάλαιο 4 είναι ένα εξίσου σημαντικό κεφάλαιο γιατί θεσπίζει νέους ρόλους που θα πρέπει να διαθέτουν οι οργανισμοί, όπως ο Υπεύθυνος Προστασίας, ο Υπεύθυνος Επεξεργασίας, ο εκτελών την επεξεργασία. Εκτός από τον ορισμό των παραπάνω ρόλων, ο Κανονισμός συγκεκριμενοποιεί την τεκμηρίωση που θα πρέπει να διαθέτει ένας οργανισμός, για να αποδεικνύει ότι τηρεί τις επιταγές του Κανονισμού. Επίσης εισάγει για πρώτη φορά τις υποχρεώσεις που ενός οργανισμού σε περίπτωση παραβίασης προσωπικών δεδομένων. Συνεπώς, το κεφάλαιο αυτό θέτει πρακτικά το εταιρικό πλαίσιο λειτουργίας ενός οργανισμού για τη ορθή επεξεργασία των προσωπικών δεδομένων στην οποία προβαίνει λόγω των επιχειρηματικών του δραστηριοτήτων, με σκοπό την προστασία των Φυσικών Προσώπων.

Το κεφάλαιο 6 από την άλλη μεριά είναι περισσότερο σημαντικό σε θεσμικό επίπεδο, αφού ορίζει την υποχρέωση κάθε χώρας να διαθέτει εποπτικές αρχές που να διαχειρίζονται και να ελέγχουν τον τρόπο με τον οποίο οι οργανισμοί υιοθετούν τον GDPR.

Τέλος, το Κεφάλαιο 8 είναι ιδιαίτερα σημαντικό. Εκτός από τις διαδικασίες προσφυγών που ούτως ή άλλως πιθανά να υπήρχαν στο δικονομικό σύστημα κάθε χώρας, για πρώτη φορά συγκεκριμενοποιούνται τα χρηματικά πρόστιμα για περιπτώσεις παραβίασης του εν λόγω κανονισμού. Το ύψος μάλιστα των προστίμων που προβλέπει ο Κανονισμός είναι ιδιαίτερα υψηλό, γεγονός που σίγουρα θα λειτουργήσει υπέρ του Κανονισμού, υπό την έννοια ότι οι οργανισμοί θα μπορέσουν να συγκρίνουν το κόστος συμμόρφωσης και μη συμμόρφωσης με τον Κανονισμό. Έμμεσα λοιπόν οι οργανισμοί, σε περίπτωση που δεν κατανοούν τη θεωρητική σημασία του GDPR, θα «αναγκαστούν» να επωμιστούν το κόστος συμμόρφωσής τους με το GDPR, διότι το κόστος Μη συμμόρφωσής τους θα είναι πολλαπλάσιο[28].

[28] Κανονισμός 2016/679 του Ευρωπαϊκού Κοινοβουλίου

Κεφάλαιο 4
Σύνδεση GDPR με Συστήματα Διαχείρισης Ποιότητας

Σε πολλές περιπτώσεις οι οργανισμοί διαθέτουν ήδη Συστήματα Διαχείρισης Ποιότητας τα οποία πληρούν τις απαιτήσεις διεθνών προτύπων, όπως το ISO9001[29] και ISO27001[30]. Τα Συστήματα αυτά καλύπτουν μεν ένα μέρος των απαιτήσεων του GDPR, αλλά όχι το σύνολό του. Αυτό συμβαίνει διότι η ισχύουσα έκδοσή τους δημιουργήθηκε πριν την δημοσίευση του GDPR. Χαρακτηριστικά η ισχύουσα έκδοση του ISO9001 είναι αυτή του 2015, ενώ του ISO27001 είναι αυτή του 2013.

Πιο συγκεκριμένα, η εφαρμογή του προτύπου ISO27001 περί της ασφάλειας πληροφοριακών συστημάτων, διευκολύνει την εφαρμογή μιας ισχυρής και συστηματικής προσέγγισης για τη διαχείριση των πληροφοριών – άρα και των προσωπικών δεδομένων που τηρεί ένας οργανισμός. Συγκεκριμένα, Το ISO 27001 μπορεί να βοηθήσει εταιρείες με τις απαιτήσεις του GDPR υπό το πρίσμα:

- Της διασφάλισης της ακρίβειας και της πληρότητας των περιουσιακών στοιχείων.
- Της εξασφάλισης ότι οι πληροφορίες δεν διατίθενται ή αποκαλύπτονται σε μη εξουσιοδοτημένα άτομα, οντότητες ή διαδικασίες.
- Της προσβασιμότητας και χρήσης δεδομένων κατόπιν αιτήματος από εξουσιοδοτημένο φορέα[31]

Οι ειδικοί ισχυρίζονται ότι μια εταιρεία που έχει εφαρμόσει το ISO 27001 έχει ήδη κάνει τουλάχιστον το ήμισυ της εργασίας για την επίτευξη της συμμόρφωσης με το GDPR με την ελαχιστοποίηση του κινδύνου παραβίασης, δεδομένου ότι ένα Σύστημα Ποιότητας κατά ISO / IEC 27001 εντοπίζει πιθανούς κινδύνους για τα δεδομένα πελατών και ενδιαφερομένων (δηλαδή και προσωπικά δεδομένα) και διασφαλίζει ότι οι οργανισμοί εφαρμόζουν τους σχετικούς ελέγχους για να τους μετριάσουν[32].

[29] International Organization for Standardization. (2015). *Quality management systems — Requirements* (ISO Standard No. 9001)
[30] International Organization for Standardization. (2013). *Information technology — Security techniques — Information security management systems — Requirements* (ISO Standard No. 27001)
[31] https://www.pegasuslegalregister.com/2019/01/18/general-data-protection-regulation/
[32] https://iecetech.org/index.php/Technology-Focus/2018-02/International-Standards-provide-toolkit-for-GDPR-compliance

Παραδείγματος χάριν, το άρθρο 32 του GDPR απαιτεί οι κίνδυνοι "από τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, μη εξουσιοδοτημένη αποκάλυψη ή πρόσβαση σε προσωπικά δεδομένα" να εντοπίζονται και να μετριάζονται. Ένα Σύστημα Ποιότητας κατά ISO / IEC 27001 πληροί την παραπάνω απαίτηση[33].

Άλλο παράδειγμα αποτελεί το σημείο ελέγχου Α.10.1, που αναφέρει ότι οι κρυπτογραφικοί μηχανισμοί και οι σχετικές τεχνολογίες μπορούν να χρησιμοποιηθούν για την προστασία προσωπικών πληροφοριών είτε αυτές βρίσκονται αποθηκευμένες είτε κατά την μεταφορά τους σε δίκτυα[34]. Το σημείο αυτό λοιπόν μπορεί να υποστηρίξει τη συμμόρφωση με το GDPR, όπως αυτό αναφέρεται στο άρθρο 32, και απαιτεί την ψευδωνυμοποίηση και την κρυπτογράφηση δεδομένων προσωπικού χαρακτήρα. Η ψευδωνυμοποίηση ειδικά είναι απαιτητή στις περιπτώσεις που η επεξεργασία γίνεται μέσω των δημοφιλών και πλήρως εξατομικευμένων συσκευών όπως τα κινητά τηλέφωνα και τα tablets[35].

Πιο αναλυτικά, σχετικά με ISO27001 μπορούμε να δούμε τη συσχέτισή του με το GDPR στον παρακάτω πίνακα, όπου αναφέρονται τα άρθρα του GDPR με αντιπαραβολή των σημείων που καλύπτονται μερικώς ή ολικώς από το ISO27001:

Άρθρα GDPR	**Κεφάλαια & Σημεία Ελέγχου ISO27001**
Άρθρο 1 Αντικείμενο και στόχοι	
Άρθρο 2 Ουσιαστικό πεδίο εφαρμογής	
Άρθρο 3 Εδαφικό πεδίο εφαρμογής	
Άρθρο 4 Ορισμοί	3: Terms And Definitions

[33] https://www.itgovernance.co.uk/gdpr-and-iso-27001

[34] https://www.epixeiro.gr/article/76053

[35] GDPR principles in Data protection encourage pseudonymization through most popular and full-personalized devices - mobile phones, Authors: Štarchoň, Peter, Pikulík, Tomáš, Affiliation: Faculty of Management, Comenius University in Bratislava, Odbojárov 10, 820 05 Bratislava 25, Slovakia, Source: In The 10th International Conference on Ambient Systems, Networks and Technologies (ANT 2019) / The 2nd International Conference on Emerging Data and Industry 4.0 (EDI40 2019) / Affiliated Workshops, Procedia Computer Science 2019 151:303-312

Άρθρο 5 - Αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα	A.8.1.1: Inventory Of Assets A.8.2: Information Classification A.8.3: Media Handling A.9.1.1: Access Control Policy A.9.4.1: Information Access Restriction A.10: Cryptography A.13.2: Information Transfer A.14.1.1: Information Security Requirements Analysis And Specification A.15: Supplier Relationships A.17: Information Security Aspects Of Business Continuity Management A.18: Compliance
Άρθρο 6 - Νομιμότητα της επεξεργασίας	6.1.2 : Information Security Risk Assessment A.14.1.1: Information Security Requirements Analysis And Specification A.18.1.1: Identification Of Applicable Legislation And Contractual Requirements
Άρθρο 7 - Προϋποθέσεις συγκατάθεσης	A.8.2.3: Handling Of Assets A.12.1.1: Documented Operating Procedures A.18.1.3: Protection Of Records 6.1.2 : Information Security Risk Assessment A.14.1.1: Information Security Requirements Analysis And Specification A.8.3.2: Disposal Of Media A.13.2: Information Transfer
Άρθρο 8 - Όροι που ισχύουν για τη συγκατάθεση του παιδιού σε σχέση με τις υπηρεσίες της κοινωνίας της πληροφορίας	A.8.2.3: Handling Of Assets A.12.1.1: Documented Operating Procedures A.18.1.3: Protection Of Records 6.1.2 : Information Security Risk Assessment A.14.1.1: Information Security Requirements Analysis And Specification A.8.3.2: Disposal Of Media A.13.2: Information Transfer
Άρθρο 9 - Επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα	A.8.2.1: Classification Of Information A.8.2.3: Handling Of Assets A.14.1.1: Information Security Requirements Analysis And Specification
Άρθρο 10 - Επεξεργασία δεδομένων προσωπικού χαρακτήρα σχετικά με ποινικές καταδίκες και αδικήματα	A.7.1: Prior To Employment A.8.2.1: Classification Of Information A.8.2.3: Handling Of Assets 6.1.2: Information Security Risk Assessment A.14.1.1: Information Security Requirements Analysis And Specification

Άρθρο 11 - Επεξεργασία που δεν απαιτεί εξακρίβωση ταυτότητας	A.8.2.1: Classification Of Information A.8.2.3: Handling Of Assets 6.1.2 : Information Security Risk Assessment A.14.1.1: Information Security Requirements Analysis And Specification
Άρθρο 12 - Διαφανής ενημέρωση, ανακοίνωση και ρυθμίσεις για την άσκηση των δικαιωμάτων του υποκειμένου των δεδομένων	A.12.1.1: Documented Operating Procedures A.14.1.1: Information Security Requirements Analysis And Specification A.16: Information Security Incident Management
Άρθρο 13 - Πληροφορίες που παρέχονται εάν τα δεδομένα προσωπικού χαρακτήρα συλλέγονται από το υποκείμενο των δεδομένων	A.8.2.1: Classification Of Information A.8.2.3: Handling Of Assets A.12.1.1: Documented Operating Procedures A.14.1.1: Information Security Requirements Analysis And Specification A.16: Information Security Incident Management
Άρθρο 14 - Πληροφορίες που παρέχονται εάν τα δεδομένα προσωπικού χαρακτήρα δεν έχουν συλλεγεί από το υποκείμενο των δεδομένων	A.8.2.1: Classification Of Information A.8.2.3: Handling Of Assets A.12.1.1: Documented Operating Procedures A.14.1: Security Requirements Of Information Systems A.16: Information Security Incident Management
Άρθρο 15 - Δικαίωμα πρόσβασης του υποκειμένου των δεδομένων	A.8.1.1: Inventory Of Assets A.8.2.1: Classification Of Information A.12.1.1: Documented Operating Procedures A.13.2.1: Information Transfer Policies And Procedures A.14.1.1: Information Security Requirements Analysis And Specification
Άρθρο 16 - Δικαίωμα διόρθωσης	A.12.1.1: Documented Operating Procedures A.14.1: Security Requirements Of Information Systems A.9: Access Control A.16 : Information Security Incident Management A.12.3: Backup A.18.1.3: Protection Of Records
Άρθρο 17 - Δικαίωμα διαγραφής («δικαίωμα στη λήθη»)	6.1.2 : Information Security Risk Assessment A.14.1.1: Information Security Requirements Analysis And Specification A.9: Access Control A.16 : Information Security Incident Management A.12.3: Backup A.8.3.2: Disposal Of Media

Άρθρο 18 - Δικαίωμα περιορισμού της επεξεργασίας	6.1.2 : Information Security Risk Assessment A.8.2.1: Classification Of Information A.8.2.3: Handling Of Assets A.12.1.1: Documented Operating Procedures A.14.1.1: Information Security Requirements Analysis And Specification A.16 : Information Security Incident Management A.12.3: Backup A.18.1.1: Identification Of Applicable Legislation And Contractual Requirements
Άρθρο 19 -Υποχρέωση γνωστοποίησης όσον αφορά τη διόρθωση ή τη διαγραφή δεδομένων προσωπικού χαρακτήρα ή τον περιορισμό της επεξεργασίας	A.12.1.1: Documented Operating Procedures 6.1.2 : Information Security Risk Assessment A.14.1.1: Information Security Requirements Analysis And Specification A.16: Information Security Incident Management
Άρθρο 20 - Δικαίωμα στη φορητότητα των δεδομένων	6.1.2: Information Security Risk Assessment A.13: Communications Security A.14.1.1: Information Security Requirements Analysis And Specification A.8.3: Media Handling A.10: Cryptography A.18.1.3: Protection Of Records
Άρθρο 21 - Δικαίωμα εναντίωσης	6.1.2: Information Security Risk Assessment A.12.1.1: Documented Operating Procedures A.14.1.1: Information Security Requirements Analysis And Specification A.16 : Information Security Incident Management A.12.3: Backup
Άρθρο 22 - Αυτοματοποιημένη ατομική λήψη αποφάσεων, περιλαμβανομένης της κατάρτισης προφίλ	6.1.2 : Information Security Risk Assessment A.12.1.1: Documented Operating Procedures A.14.1.1: Information Security Requirements Analysis And Specification A.16 : Information Security Incident Management
Άρθρο 23 - Περιορισμοί	A.18.1.1: Identification Of Applicable Legislation And Contractual Requirements
Άρθρο 24 -Ευθύνη του υπευθύνου επεξεργασίας	4: Context Of The Organization 5: Leadership, 6: Planning 7: Support 8: Operation 9: Performance Evaluation 10: Improvement
Άρθρο 25 - Προστασία των δεδομένων ήδη από το σχεδιασμό και εξ ορισμού	6: Planning

Άρθρο 26 - Από κοινού υπεύθυνοι επεξεργασίας	5.3: Organizational Roles, Responsibilities And Authorities 9.1: Monitoring, Measurement, Analysis And Evaluation A.13.2: Information Transfer A.15: Supplier Relationships A.16 : Information Security Incident Management A.18.1: Compliance With Legal And Contractual Requirements
Άρθρο 27 -Εκπρόσωποι υπευθύνων επεξεργασίας ή εκτελούντων την επεξεργασία μη εγκατεστημένων στην Ένωση	5.3: Organizational Roles, Responsibilities And Authorities 7.5.1: General A.15: Supplier Relationships A.18.1.4: Privacy And Protection Of Personally Identifiable
Άρθρο 28 - Εκτελών την επεξεργασία	8.2: Information Security Risk Assessment 9.1: Monitoring, Measurement, Analysis And Evaluation A.15: Supplier Relationships A.18.1.1: Identification Of Applicable Legislation And Contractual Requirements A.18.1.3: Protection Of Records A.18.1.4: Privacy And Protection Of Personally Identifiable
Άρθρο 29 - Επεξεργασία υπό την εποπτεία του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία	
Άρθρο 30 - Αρχεία των δραστηριοτήτων επεξεργασίας	7.5: Documented Information
Άρθρο 31 - Συνεργασία με την εποπτική αρχή	A.6.1.3: Contact With Authorities
Άρθρο 32 - Ασφάλεια της επεξεργασίας	8.2: Information Security Risk Assessment 8.3: Information Security Risk Treatment
Άρθρο 33 - Κοινοποίηση της παραβίασης των προσωπικών δεδομένων στην εποπτική αρχή	A.16 : Information Security Incident Management A.18.1.4: Privacy And Protection Of Personally Identifiable
Άρθρο 34 - Αναγγελία παραβίασης των προσωπικών δεδομένων στο υποκείμενο των δεδομένων	A.16 : Information Security Incident Management A.18.1.4: Privacy And Protection Of Personally Identifiable
Άρθρο 35 - Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων	6.1.2: Information Security Risk Assessment A.6.1.3: Contact With Authorities A.8.2.1: Classification Of Information
Άρθρο 36 -Προηγούμενη διαβούλευση	6.1.2: Information Security Risk Assessment A.6.1.3: Contact With Authorities A.8.2.1: Classification Of Information

Άρθρο 37 - Καθορισμός του υπευθύνου προστασίας δεδομένων	5.3: Organizational Roles, Responsibilities And Authorities A.6.1.1: Information Security Roles And Responsibilities A.18.1.4: Privacy And Protection Of Personally Identifiable
Άρθρο 38 - Θέση του υπευθύνου προστασίας δεδομένων	5.3: Organizational Roles, Responsibilities And Authorities A.6.1.1: Information Security Roles And Responsibilities A.18.1.4: Privacy And Protection Of Personally Identifiable
Άρθρο 39 - Καθήκοντα του υπευθύνου προστασίας δεδομένων	5.3: Organizational Roles, Responsibilities And Authorities A.6.1.1: Information Security Roles And Responsibilities A.18.1.4: Privacy And Protection Of Personally Identifiable
Άρθρο 40 - Κώδικες δεοντολογίας	5.3: Organizational Roles, Responsibilities And Authorities, A.6.1.1: Information Security Roles And Responsibilities A.18.1.4: Privacy And Protection Of Personally Identifiable
Άρθρο 41 - Παρακολούθηση εγκεκριμένων κωδίκων δεοντολογίας	5.3: Organizational Roles, Responsibilities And Authorities A.6.1.1: Information Security Roles And Responsibilities A.18.1.4: Privacy And Protection Of Personally Identifiable
Άρθρο 42 - Πιστοποίηση	5.3: Organizational Roles, Responsibilities And Authorities A.6.1.1: Information Security Roles And Responsibilities A.18.1.4: Privacy And Protection Of Personally Identifiable
Άρθρο 43 - Φορείς πιστοποίησης	5.3: Organizational Roles, Responsibilities And Authorities A.6.1.1: Information Security Roles And Responsibilities A.18.1.4: Privacy And Protection Of Personally Identifiable
Άρθρο 44 - Γενική αρχή για διαβιβάσεις	
Άρθρο 45 - Διαβιβάσεις βάσει απόφασης επάρκειας	A.18.1.4: Privacy And Protection Of Personally Identifiable
Άρθρο 46 -Διαβιβάσεις που υπόκεινται σε κατάλληλες εγγυήσεις	A.18.1.4: Privacy And Protection Of Personally Identifiable
Άρθρο 47 - Δεσμευτικοί εταιρικοί κανόνες	A.18.1.4: Privacy And Protection Of Personally Identifiable
Άρθρο 48 - Διαβιβάσεις ή κοινοποιήσεις που δεν επιτρέπονται από το δίκαιο της Ένωσης	A.18.1.4: Privacy And Protection Of Personally Identifiable, A.16 : Information Security Incident Management
Άρθρο 49 - Παρεκκλίσεις για ειδικές καταστάσεις	A.18.1.4: Privacy And Protection Of Personally Identifiable
Άρθρο 50 - Διεθνής συνεργασία για την προστασία των δεδομένων προσωπικού χαρακτήρα	
Άρθρο 51 - Εποπτική αρχή	
Άρθρο 52 - Ανεξαρτησία	

Άρθρο 53 - Γενικές προϋποθέσεις για τα μέλη της εποπτικής αρχής .	
Άρθρο 54 - Κανόνες για τη σύσταση της εποπτικής αρχής	
Άρθρο 55 - Αρμοδιότητα	
Άρθρο 56 - Άρθρο 56. Αρμοδιότητα της επικεφαλής εποπτικής αρχής	
Άρθρο 57 - Καθήκοντα	
Άρθρο 58 - Εξουσίες	
Άρθρο 59 - Εκθέσεις δραστηριοτήτων	
Άρθρο 60 - Συνεργασία μεταξύ της επικεφαλής εποπτικής αρχής και των άλλων ενδιαφερόμενων εποπτικών αρχών	
Άρθρο 61 - Αμοιβαία συνδρομή	
Άρθρο 62 - Κοινές επιχειρήσεις αρχών ελέγχου	
Άρθρο 63 - Μηχανισμός συνεκτικότητας	
Άρθρο 64 - Γνώμη του συμβουλίου	
Άρθρο 65 - Επίλυση διαφορών από το Συμβούλιο Προστασίας Δεδομένων	
Άρθρο 66 -Επείγουσα διαδικασία	
Άρθρο 67 - Ανταλλαγή πληροφοριών	
Άρθρο 68 - Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων	
Άρθρο 69 - Ανεξαρτησία	
Άρθρο 70 - Καθήκοντα του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων	
Άρθρο 71 - Εκθέσεις	
Άρθρο 72 - Διαδικασία	
Άρθρο 73 - Πρόεδρος	
Άρθρο 74 - Καθήκοντα του προέδρου	
Άρθρο 75 - Γραμματεία	

Άρθρο 76 - Εμπιστευτικότητα	
Άρθρο 77 - Δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή	
Άρθρο 78 - Δικαίωμα πραγματικής δικαστικής προσφυγής κατά αρχής ελέγχου	
Άρθρο 79 - Δικαίωμα πραγματικής δικαστικής προσφυγής κατά υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία	
Άρθρο 80 - Εκπροσώπηση υποκειμένων των δεδομένων	
Άρθρο 81 - Αναστολή των διαδικασιών	
Άρθρο 82 - Δικαίωμα αποζημίωσης και ευθύνη	A.18.1.4: Privacy And Protection Of Personally Identifiable
Άρθρο 83 - Γενικοί όροι επιβολής διοικητικών προστίμων	A.18.1.4: Privacy And Protection Of Personally Identifiable
Άρθρο 84 - Κυρώσεις	A.18.1.4: Privacy And Protection Of Personally Identifiable
Άρθρο 85 - Επεξεργασία και ελευθερία έκφρασης και πληροφόρησης	A.18.1.1: Identification Of Applicable Legislation And Contractual Requirements A.18.1.4: Privacy And Protection Of Personally Identifiable
Άρθρο 86 - Επεξεργασία και πρόσβαση του κοινού στα επίσημα έγγραφα	A.18.1.1: Identification Of Applicable Legislation And Contractual Requirements A.18.1.4: Privacy And Protection Of Personally Identifiable
Άρθρο 87 - Επεξεργασία του εθνικού αριθμού ταυτότητας	A.18.1.1: Identification Of Applicable Legislation And Contractual Requirements A.18.1.4: Privacy And Protection Of Personally Identifiable
Άρθρο 88 - Επεξεργασία στο πλαίσιο της απασχόλησης	A.18.1.1: Identification Of Applicable Legislation And Contractual Requirements A.18.1.4: Privacy And Protection Of Personally Identifiable
Άρθρο 89 - Διασφαλίσεις και παρεκκλίσεις σχετικά με την επεξεργασία για σκοπούς αρχειοθέτησης	A.18.1.4: Privacy And Protection Of Personally Identifiable

προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς	
Άρθρο 90 - Υποχρεώσεις τήρησης απορρήτου	A.18.1.1: Identification Of Applicable Legislation And Contractual Requirements A.18.1.4: Privacy And Protection Of Personally Identifiable
Άρθρο 91 - Υφιστάμενοι κανόνες προστασίας των εκκλησιών και των θρησκευτικών ενώσεων	A.18.1.4: Privacy And Protection Of Personally Identifiable
Άρθρο 92 - Άσκηση της εξουσιοδότησης	
Άρθρο 93 - Διαδικασία επιτροπής	
Άρθρο 94 - Κατάργηση της οδηγίας 95/46 / ΕΚ	
Άρθρο 95 - Σχέση με την οδηγία 2002/58 / ΕΚ	
Άρθρο 96 - Σχέση με συμφωνίες που έχουν συναφθεί παλαιότερα	
Άρθρο 97 - Εκθέσεις της Επιτροπής	
Άρθρο 98 - Επισκόπηση άλλων νομικών πράξεων της Ένωσης για την προστασία των δεδομένων	
Άρθρο 99 - Έναρξη ισχύος και εφαρμογή	

Όπως διαφαίνεται παραπάνω, ο GDPR εισάγει ένα σύνολο από κανόνες, οι οποίοι απαιτούν από τους οργανισμούς να εφαρμόζουν ελέγχους και η εφαρμογή του ISO 27001 θα βοηθήσει τους οργανισμούς να ανταποκριθούν σε αυτές τις απαιτήσεις[36].

Από την έρευνα που έγινε, δεν εντοπίστηκε ότι το πρότυπο ISO9001 έχει μεγάλη συσχέτιση με τον GDPR, εκτός αν το πεδίο του Συστήματος Διαχείρισης Ποιότητας αφορά αποκλειστικά τη διαχείριση προσωπικών δεδομένων. Παράλληλα, υπάρχουν Συστήματα Διαχείρισης Ποιότητας που είναι συμβατά και με το ISO9001 και με το ISO27001.

Με δεδομένο όμως ότι ο GDPR δημοσιεύτηκε το 2016 είναι εμφανές ότι η ύπαρξη συστημάτων ποιότητας που πληρούν τις προδιαγραφές των προαναφερόμενων προτύπων, δεν συνεπάγεται την

[36] How ISO 27001 Can Help Achieve GDPR Compliance Contributors: Lopes, Isabel Maria Guarda, Teresa, Oliveira, Pedro, Source: 2019 14th Iberian Conference on Information Systems and Technologies (CISTI) Information Systems and Technologies (CISTI), 2019 14th Iberian Conference on. :1-6 Jun, 2019

πλήρωση όλων των προδιαγραφών του GDPR, απαιτείται λοιπόν προσαρμογή τους. Συγκεκριμένα το τρέχον πρότυπο ISO9001 είναι έκδοσης 2015, ενώ το ISO27001 είναι έκδοσης 2013. Άρα, δεν θα ήταν εφικτό να έχουν προβλεφθεί οι απαιτήσεις του GDPR με ημερομηνία 2016 στις παραπάνω εκδόσεις των 2 προτύπων που εξετάστηκαν.

Ένα από τα ελάχιστα πρότυπα που καλύπτει σε πολύ μεγάλο βαθμό τον GDPR είναι το British Standard 10012[37] με τίτλο "Data protection – Specification for a personal information management system." Αυτό συμβαίνει επειδή η ισχύουσα έκδοση του British Standard 10012 είναι του 2017, ημερομηνίας μεταγενέστερης της δημοσίευσης του GDPR (2016). Παράλληλα, το BS10012 πραγματεύεται το ίδιο αντικείμενο με τον GDPR, δηλαδή τα προσωπικά δεδομένα και την επεξεργασία τους. Με δεδομένα ότι το BS10012 επικαιροποιήθηκε το 2017, δηλαδή μετά την δημοσιοποίηση του GDPR, και ότι πραγματεύεται το ίδιο θέμα με το GDPR, σημαίνει ότι είναι συμβατό με τον GDPR[38]. Όπως αναφέρει και το Βρετανικός Οργανισμός Τυποποίησης British Standards Institution «*Το πρότυπο BS 10012 παρέχει ένα πλαίσιο βέλτιστης πρακτικής για ένα σύστημα διαχείρισης προσωπικών πληροφοριών που ευθυγραμμίζεται με τις αρχές του GDPR της ΕΕ*»[39].

Στο Παράρτημα Α της παρούσας εργασίας φαίνονται οι απαιτήσεις ενός συστήματος διαχείρισης ποιότητας, σύμφωνα με το British Standard 10012. Από την ενδελεχή μελέτη, φαίνεται ξεκάθαρα ότι όλες οι απαιτήσεις του προτύπου είναι απόλυτα συμβατές με τον GDPR. Στην παρούσα εργασία δεν μπορεί να γίνει mapping του British Standard 10012 με το κάθε άρθρο του GDPR όπως έγινε για το ISO27001 διότι κάθε σημείο ελέγχου του BS10012 αντιστοιχίζεται σε πολλαπλά άρθρα του GDPR. Με δεδομένο ότι ο ίδιος ο British Standards Institution ρητά αναφέρει ότι το BS10012 είναι πλήρως συμβατό με τις επιταγές του GDPR, θεωρείται σίγουρο ότι η αντίστοιχη διαδικασία αντιπαραβολής έχει γίνει από την τεχνική επιτροπή που συνέταξε το BS10012.

Λαμβάνοντας υπόψη όλα τα παραπάνω, η προσαρμογή ενός οργανισμού στις απαιτήσεις του British Standard 10012, θεωρητικά σημαίνει και την προσαρμογή του οργανισμού σε πολλές από τις απαιτήσεις του GDPR. Φυσικά, η προσαρμογή στις επιταγές του BS10012, σε συνδυασμό με τη χρήση άλλων προτύπων όπως το ISO27001, μπορεί να θεωρηθεί ο ενδεδειγμένος τρόπος για έναν οργανισμό να προσαρμοστεί στον GDPR[40].

[37] British Standards Institution, (2017). *Personal Information Management System*. (BS Standard Number 10012)
[38] https://www.lr.org/en-gb/gdpr/bs-10012
[39] https://www.bsigroup.com/en-GB/BS-10012-Personal-information-management/
[40] https://www.itgovernance.co.uk/blog/gdpr-compliance-why-you-should-consider-bs-10012-certification

Κεφάλαιο 5

Βήματα για την εναρμόνιση ενός εκπαιδευτικού οργανισμού στον GDPR

Όπως αναλύθηκε παραπάνω, ο GDPR είναι ένας κανονισμός που εισάγει αρκετούς νεοτερισμούς. Συνεπώς η εφαρμογή του στο πλαίσιο της λειτουργίας των οργανισμών είναι μια απαιτητική διαδικασία, που απαιτεί εξειδικευμένη γνώση τόσο θεμάτων που άπτονται νομικών γνώσεων όσο και γνώσεων πληροφορικής. Η γνώση πληροφορικής κρίνεται απαραίτητη διότι πλέον η επεξεργασία δεδομένων πραγματοποιείται από το σύνολο σχεδόν των οργανισμών μέσω εργαλείων πληροφορικής. Προκειμένου λοιπόν να βοηθηθούν οι οργανισμοί, ο ΣΕΒ προχώρησε σε σχετική μελέτη[41] προκειμένου να βοηθήσει το έργο της συμμόρφωσης ενός οργανισμού στον GDPR. Τα προτεινόμενα αυτά βήματα απεικονίζονται στο παρακάτω διάγραμμα:

1. Σύσταση ομάδας εργασίας
2. Ορισμός ΥΠΔ
3. Καταγραφή Υπάρχουσας Κατάστασης
4. Εντοπισμός & ανάλυση ελλείψεων
5. Μελέτη Εκτίμησης Αντικτύπου
6. Υλοποίηση Διορθωτικών Ενεργειών
7. Αξιοποίηση εργαλείων πληροφορικής
8. Ανάπτυξη διαδικασιών γνωστοποίησης
9. Δοκιμαστικοί έλεγχοι
10. Διαρκής παρακολούθηση και επικαιροποίηση

Πιο αναλυτικά, τα βήματα της παραπάνω μελέτης έχουν ως εξής:

[41] ΣΕΒ, Ο νέος Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR) Εφαρμογή και προκλήσεις για τις επιχειρήσεις στην εποχή της ψηφιοποίησης, Οκτώβριος 2018

ΒΗΜΑ 1: Σύσταση Ομάδας Εργασίας

Το απαραίτητο βήμα για την έναρξη της διαδικασίας προσαρμογής ενός οργανισμού στις απαιτήσεις του GDPR είναι η ενημέρωση της Διοίκησης σχετικά με το τι είναι ο GDPR, τι σημαίνει η εφαρμογή του για τη λειτουργία του οργανισμού, ποια είναι τα βασικά βήματα που απαιτούνται και ποια θα είναι η εμπλοκή του οργανισμού και των στελεχών στην όλη διαδικασία. Όταν η Διοίκηση κατανοήσει την ανάγκη και την υποχρεωτικότητα της όλης διαδικασίας θα πρέπει να δεσμεύσει τους πόρους (ανθρώπινους και χρηματοοικονομικούς) που απαιτούνται για την ολοκλήρωση της διαδικασίας. Θα λέγαμε ότι η διαδικασία προσαρμογής ενός οργανισμού στο GDPR θα μπορούσε να παρουσιαστεί σαν ένα συγκεκριμένο project. Μέσα λοιπόν από την ενημέρωση της Διοίκησης αναζητούμε το Project Charter, τη δέσμευση δηλαδή του ότι θα παρασχεθούν όλοι οι απαραίτητοι πόροι για την υλοποίηση της συμμόρφωσης. Με τη δέσμευση της Διοίκησης, ουσιαστικά συστήνεται η Ομάδα Εργασίας που θα αναλάβει το project της προσαρμογής του Οργανισμού στα δεδομένα του GDPR.

ΒΗΜΑ 2: Ορισμός Υπεύθυνου Προστασίας Δεδομένων (ΥΠΔ)

Σύμφωνα με το άρθρο 37 του Κανονισμού, είτε ο Εκτελών την Επεξεργασία είτε ο Υπεύθυνος επεξεργασίας (δηλαδή ο ίδιος ο οργανισμός) πρέπει να ορίσει έναν Υπεύθυνο Προστασίας Δεδομένων (ΥΠΔ ή DPO). Ο ΥΠΔ είναι ουσιαστικά η ανεξάρτητη φωνή του οργανισμού σε θέματα που άπτονται με την επεξεργασία προσωπικών δεδομένων. Ένας εκπαιδευτικός οργανισμός, που εκ των πραγμάτων, πραγματοποιεί επεξεργασία προσωπικών δεδομένων μεγάλης κλίμακας, δεν συμπεριλαμβάνεται στους οργανισμούς που εξαιρούνται από την υποχρεωτικότητα ορισμού ΥΠΔ. Έτσι, ο ΥΠΔ θα πρέπει σύμφωνα με το άρθρο 39 του κανονισμού να ενημερώνει, να συμβουλεύει και να παρακολουθεί τη συμμόρφωσή του οργανισμού με τον GDPR, ενώ παράλληλα θα πρέπει να συνεργάζεται και να επικοινωνεί με την Εθνική Εποπτική Αρχή όταν παρατηρεί την αδυναμία και απροθυμία του Οργανισμού να προσαρμοστεί στον GDPR. Άρα, ο ΥΠΔ θα πρέπει να είναι ένα στέλεχος κατάλληλα καταρτισμένο, με τις απαραίτητες γνώσεις και δεξιότητες που απαιτεί η θέση, ενώ παράλληλα θα πρέπει να λειτουργεί ανεξάρτητα και αμερόληπτα.

ΒΗΜΑ 3: Καταγραφή υπάρχουσας κατάστασης - Καταγραφή πράξεων επεξεργασίας (Data Mapping)

Το επόμενο βήμα είναι η δημιουργία ενός Αρχείου Δραστηριοτήτων Επεξεργασίας, σύμφωνα με το άρθρο 30 του Κανονισμού. Για να γίνει αυτό θα πρέπει ο Οργανισμός να χαρτογραφήσει τα προσωπικά δεδομένα που τηρεί και τον τρόπο που αυτά χρησιμοποιούνται. Με την ολοκλήρωση αυτής της διαδικασίας, ο οργανισμός θα μπορέσει να αποτυπώσει την υπάρχουσα κατάσταση της, που θα την βοηθήσει στα επόμενα βήματα.

Ένα απαραίτητο στοιχείο του βήματος του Data Mapping είναι τα Στοιχεία Υπευθύνου Επεξεργασίας. Ενδεικτικά, τα στοιχεία του Υπευθύνου Επεξεργασίας που έχει ορίσει ο Οργανισμός θα πρέπει να είναι της μορφής:

1. Όνομα και στοιχεία επικοινωνίας Υπεύθυνου Επεξεργασίας	
Επωνυμία/Ονοματεπώνυμο	
Αριθμός ΓΕΜΗ (αν υπάρχει)	
ΑΦΜ	
Ηλεκτρονική Διεύθυνση	
Τηλέφωνο	
Ταχυδρομική Διεύθυνση	

2. Όνομα και στοιχεία επικοινωνίας Εκπροσώπου του Υπευθύνου Επεξεργασίας	
Επωνυμία/Ονοματεπώνυμο	
ΑΦΜ	
Ηλεκτρονική Διεύθυνση	
Τηλέφωνο	
Ταχυδρομική Διεύθυνση	

3. Όνομα και στοιχεία επικοινωνίας Υπευθύνου Προστασίας Δεδομένων	
Ονοματεπώνυμο	
Ηλεκτρονική Διεύθυνση	
Τηλέφωνο	
Ταχυδρομική Διεύθυνση	

4. Όνομα και στοιχεία επικοινωνίας από κοινού Υπευθύνου Επεξεργασίας	
Από κοινού Δραστηριότητες επεξεργασίας	
Επωνυμία/Ονοματεπώνυμο	
Αριθμός ΓΕΜΗ (αν υπάρχει)	
ΑΦΜ	
Ηλεκτρονική Διεύθυνση	
Τηλέφωνο	
Ταχυδρομική Διεύθυνση	

Εν συνεχεία, προκειμένου να δημιουργηθεί το αρχείο δραστηριοτήτων, θα πρέπει να ελεγχθούν όλα τα στοιχεία του Κανονισμού και να καταγραφούν. Ακολουθεί ενδεικτικό αρχείο Data Mapping:

	Α/Α Δραστηριότητας	**1**	**2**	**…**	**Χ**
Βασικά χαρακτηριστικά της επεξεργασίας	επεξεργασία (όνομα και περιγραφή δραστηριότητας)				
	είδος αρχείου (φυσικό/ηλεκτρονικό) /φύση επεξεργασίας				
	κύρια ή παρεπόμενη δραστηριότητα				

	Τμήμα επιχείρησης				
	Σκοπός επεξεργασίας				
	Σύνδεσμος στο αρχείο συμφωνίας "Από Κοινού Υπευθύνων Επεξεργασίας" (αν υπάρχει)				
	Πηγές των δεδομένων				
	Κατηγορίες υποκειμένων των δεδομένων				
	Κατηγορίες δεδομένων προσωπικού χαρακτήρα				
	Ειδικής κατηγορίας δεδομένα				
	Κατηγορίες αποδεκτών				
	Προβλεπόμενες προθεσμίες διαγραφής (όπου είναι δυνατό)				
Στοιχεία Υπευθύνου επεξεργασίας	λειτουργεί ως ΥΕ η ως ΕΤΕ				
	Όνομα και στοιχεία επικοινωνίας υπευθύνου επεξεργασίας/ και εκπροσώπου του (εάν υπάρχει)				
Στοιχεία αναθέτοντος εκτελούντος την επεξεργασία (εάν υπάρχει)	Όνομα και στοιχεία επικοινωνίας αναθέτοντος εκτελούντος την επεξεργασία (αν υπάρχει)/ και εκπροσώπου του (εάν υπάρχει)				
	Σύνδεσμος στο αρχείο σύμβασης με τον αναθέτοντα εκτελούντα την επεξεργασία				
	Σύνδεσμος στο αρχείο σύμβασης με τον υπεύθυνο επεξεργασίας (ισχύει αν λειτουργεί ως ΕΤΕ)				
Διαβιβάσεις σε χώρες/οργανισμούς εκτός Ε.Ε.	Τρίτες χώρες ή διεθνείς οργανισμοί στους οποίους θα διαβιβαστούν τα δεδομένα (εφόσον υπάρχουν)				
	Νομική Βάση για τη διαβίβαση (σύμφωνα με άρθρα 45-49 του Κανονισμού) και τεκμηρίωση αν ισχύει το άρθρο άρ. 49 παρ. 1 β' εδαφ				
Μέτρα Ασφαλείας	Τόπος ή πληροφοριακό σύστημα τήρησης των δεδομένων προσωπικού χαρακτήρα				
	Γενική περιγραφή οργανωτικών και τεχνικών μέτρων ασφάλειας (όπου είναι δυνατό)				
Νομιμότητα της Επεξεργασίας	Βάση για τη νομιμότητα της επεξεργασίας, σύμφωνα με το άρ. 6 και 9 του Κανονισμού				

Εκτίμηση αντικτύπου στην προστασία δεδομένων προσωπικού χαρακτήρα	Απαιτείται η διενέργεια εκτίμησης αντικτύπου στην προστασία προσωπικών δεδομένων (ΕΑΠΔ);				
Περιστατικά παραβίασης δεδομένων προσωπικού χαρακτήρα	Έχει λάβει χώρα περιστατικό παραβίασης δεδομένων προσωπικού χαρακτήρα; (περιγράψτε τις λεπτομέρειες)				
Ενημέρωση	Με ποιόν τρόπο ενημερώνονται τα υποκείμενα των δεδομένων για την επεξεργασία;				

Στο παραπάνω template, τα κελιά που είναι γραμμοσκιασμένα με πράσινο χρώμα, υποδηλώνουν πεδία που είναι υποχρεωτικό να συμπληρωθούν. Αντίθετα, τα γαλάζια γραμμοσκιασμένα κελιά υποδηλώνουν πεδία προαιρετικής συμπλήρωσης. Το χρώμα του κάθε κελιού, άρα ουσιαστικά η υποχρεωτικότητα ή όχι συμπλήρωσης, ορίζεται στο άρθρο 30 του GDPR.

Τα παραπάνω template προτείνεται να έχουν την παραπάνω μορφή, ώστε αφενός να είναι εύκολη η αντιπαραβολή τους με τα αντίστοιχα κεφάλαια του GDPR και αφετέρου η πληροφορία που συγκεντρώνεται να είναι εύκολα ιχνηλατίσιμη. Παραδείγματος χάριν, οι πίνακες που αφορούν τα προσωπικά στοιχεία του Υπεύθυνου Επεξεργασίας καλύπτουν την απαίτηση του Άρθρου 13, 14 και 30. Παράλληλα, οι πληροφορίες είναι έτσι ταξινομημένες ώστε να υπάρχει εύκολη ιχνηλασιμότητα και σε περίπτωση ελέγχου από την Εποπτική Αρχή.

Βήμα 4: Εντοπισμός και ανάλυση κινδύνων και ελλείψεων

Έχοντας ολοκληρώσει το παραπάνω βήμα, ο οργανισμός είναι πλέον σε θέση να κάνει μια αναλυτική εκτίμηση των σημείων στα οποία ήδη είναι συμβατός με τις επιταγές του GDPR και των σημείων στα οποία υπάρχουν ελλείψεις και άρα σχετικός κίνδυνος. Θα πρέπει δηλαδή να προχωρήσει σε μια gap analysis, ώστε να εντοπίσει τις δραστηριότητες που εντοπίστηκαν με ελλείψεις, την προτεραιοποίησή τους με βάση τον κίνδυνο που ενέχουν και τις προτεινόμενες ενέργειες για την αντιμετώπισή τους, για να καλύπτει όλες τις απαιτήσεις του Κανονισμού. Προκειμένου να διενεργηθεί μια σωστή GAP Analysis, θα πρέπει να ληφθούν υπόψη όλα τα άρθρα του Κανονισμού και να ελεγχθεί κατά πόσο ο Οργανισμός είναι ήδη συμβατός ή όχι. Ενδεικτικό παράδειγμα ακολουθεί παρακάτω:

ΑΠΑΊΤΗΣΗ GDPR	ΕΥΡΗΜΑ	ΑΠΟΤΈΛΕΣΜΑ
Αναγνώριση Νομικής Οντότητας	ΝΠΔΔ λειτουργεί σύμφωνα με την κείμενη νομοθεσία	Πλήρης Συμμόρφωση

Χώρες συλλογής προσωπικών δεδομένων	Εντός Ε.Ε	Πλήρης Συμμόρφωση
Χώρες όπου αποθηκεύονται ή υποβάλλονται σε επεξεργασία τα προσωπικά δεδομένα	Εντός Ε.Ε	Πλήρης Συμμόρφωση
Έχουν αναγνωριστεί όλες οι οργανώσεις τρίτων, οι εταίροι και οι οντότητες στις οποίες ενδέχεται να κοινοποιούνται τα δεδομένα	Η οντότητα γνωρίζει εν γένει τους αποδέκτες των δεδομένων χωρίς να έχει καταρτιστεί ποτέ σχετική λίστα απαρίθμησης ή/και να έχει υιοθετήσει διαδικασίες εντοπισμού τους	Μερική Συμμόρφωση
Έχουν αναγνωριστεί οι πάροχοι υπηρεσιώνCloud; (Λίστα σε σημειώσεις)	Έχει γίνει αναγνώριση των παρόχων μέσα από τη διαδικασία συνεντεύξεων, εντούτοις δεν τηρείται σχετική λίστα	Πλήρης Συμμόρφωση
Έχουν τεθεί σε ισχύ συμβατικά κείμενα που καλύπτουν δεόντως τις επεξεργασίες δεδομένων μέσω παρόχων υπηρεσιών cloud	Δεν υπάρχουν ενδείξεις συμμόρφωσης	Μη Συμμόρφωση
Η οντότητα γνωρίζει τα cookies που εγκαθίστανται μέσω της πλοήγησης στον ιστότοπό του	Δε γνωρίζει την ύπαρξηcookies	Μη Συμμόρφωση
Ο ιστότοπος διαθέτει Πολιτική cookies	Δε διαθέτει πολιτική	Μη Συμμόρφωση
Η συγκατάθεση του χρήστη για τα cookies δίδεται μέσω της ιστοσελίδας του παρόχου υπηρεσίας του διαδικτύου με χρήση κατάλληλων μηχανισμών (π.χ. με αναδυόμενα παράθυρα)	Δεν υπάρχει Pop-up window	Μη Συμμόρφωση
Η ενημέρωση για τα cookies αναρτάται σε εμφανές σημείο στην ιστοσελίδα και είναι ειδική για κάθε περίπτωση	Δε γίνεται καμία ενημέρωση χρηστών	Μη Συμμόρφωση

Με την ολοκλήρωση ενός τέτοιου αρχείου, ο Οργανισμός είναι σε θέση να γνωρίζει σε ποια ακριβώς σημεία του GDPR δεν είναι πλήρως εναρμονισμένος. Άρα, όπως αναφέρθηκε παραπάνω, θα πρέπει τώρα να προβεί σε μια καταγραφή των μη συμμορφώσεων, να εντοπίσει τους πιθανούς κινδύνους και καταγράψει τα προτεινόμενα μέτρα για την άρση των Μη συμμορφώσεων. Σε σχέση λοιπόν με το παραπάνω παράδειγμα ακολουθεί το προτεινόμενο template:

Εντοπισμός Απόκλισης	Κίνδυνος	Διορθωτική Ενέργεια
Χρήση εφαρμογών cloud χωρίς να υπάρχει σχετική τεκμηριωμένη πολιτική/διαδικασία	Κίνδυνος Διαμοιρασμού Προσωπικών δεδομένων πιθανώς σε Τρίτη χώρα	Σύνταξη Σχετικής Πολιτικής

Δεν υπάρχει συγκατάθεση κατά την εγκατάσταση cookies (marketing&statistics) στην Ιστοσελίδα καθώς και δεν υπάρχει ενημέρωση για τα cookies τα οποία είναι απαραίτητα για την περιήγηση στις συγκεκριμένες Ιστοσελίδες. Επίσης, δεν υπάρχει ενημέρωση για τα cookies τρίτων.	Επεξεργασία προσωπικών δεδομένων χωρίς την συγκατάθεση του υποκειμένου.	Δημιουργία popup παραθύρου κατά την έναρξη περιήγησης στην ιστοσελίδα με τεχνολογίες που επιτρέπουν την ελεύθερη συγκατάθεση και ενημερώνουν ορθά το υποκείμενο.

ΒΗΜΑ 5: Μελέτη Εκτίμησης Αντικτύπου (Data Privacy Impact Assessment)

Το επόμενο βήμα που θα πρέπει να ακολουθήσει ο Οργανισμός είναι η Εκτίμηση του Αντικτύπου που έχει η επεξεργασία των Προσωπικών Δεδομένων. Εφόσον στο προηγούμενο στάδιο έχουν εντοπιστεί κίνδυνοι πολύ υψηλοί για την προστασία της ιδιωτικής ζωής των φυσικών προσώπων, τότε αυτό το βήμα είναι υποχρεωτικό. Κατηγοριοποιεί τους κινδύνους που έχουν εντοπιστεί και επανεξετάζει τις διαδικασίες και τα απαιτούμενα μέτρα. Η εκτίμηση Αντικτύπου θα πρέπει να γίνει υποχρεωτικά πριν την επεξεργασία των Προσωπικών Δεδομένων. Ενδεικτικά η Εκτίμηση αντικτύπου θα πρέπει να είναι της παρακάτω μορφής:

Α.α	Περιγραφή κινδύνου	Διαχειριστής (κινδύνου)	Επίπεδο κινδύνου	Τρόπος διαχείρισης κινδύνου	Μέτρα που πρέπει να εφαρμοστούν	Υπεύθυνος εφαρμογής μέτρων	Χρονοδιάγραμμα	Επίπεδο υπολειπόμενου κινδύνου
1.								
2.								

Η Εκτίμηση Αντικτύπου είναι μια πολύ εξειδικευμένη και απαιτητική διαδικασία. Ανάλυση για τον τρόπο που υλοποιείται δεν μπορεί να γίνει στην παρούσα εργασία. Η προτεινόμενη μεθοδολογία της Εθνικής Επιτροπής Πληροφορικής και Ελευθεριών[42] για την εκπόνηση ΕΑ βρίσκεται εδώ:

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf

ΒΗΜΑ 6: Υλοποίηση Διορθωτικών Ενεργειών

Έχοντας ολοκληρώσει την εύρεση των πεδίων που χρήζουν προσοχής και ενεργειών, προκειμένου οι λειτουργίες του Οργανισμού να είναι συμβατές με τον GDPR, ακολουθεί η διαδικασία της υλοποίησης των διορθωτικών ενεργειών. Εκεί ο οργανισμός θα πρέπει είτε να βελτιώσει τις ήδη υπάρχουσες διαδικασίες του στα σημεία που εντοπίστηκαν αποκλίσεις είτε να δημιουργήσει νέες διαδικασίες για

[42] Commission Nationale de l'Informatique et des Libertés - CNIL

σημεία που έως σήμερα δεν είχε λάβει υπόψη του και αφορούν τη επεξεργασία των Προσωπικών Δεδομένων σύμφωνα με τον GDPR.

ΒΗΜΑ 7: Αξιοποίηση των εργαλείων πληροφορικής

Ανάλογα με το μέγεθος και τις δυνατότητές του, κάθε εκπαιδευτικός οργανισμός θα πρέπει να εξετάσει αν μπορεί να εκμεταλλευτεί τις δυνατότητες που του παρέχουν οι Νέες Τεχνολογίες για να ασφαλίσει και να διαχειρίζεται καλύτερα τα προσωπικά δεδομένα. Η επιστήμη της πληροφορικής δίνει ήδη και θα δώσει στο μέλλον ακόμα περισσότερα εργαλεία που μπορούν να βοηθήσουν σε αυτή την κατεύθυνση. Τέτοια εργαλεία είναι η κρυπτογράφηση και η ψευδονυμοποίηση. Τα εργαλεία αυτά θα μπορέσουν αφενός να βελτιώσουν τις υπάρχουσες διαδικασίες προστασίας των προσωπικών δεδομένων και αφετέρου να τις κάνουν ακόμα ασφαλέστερες.

ΒΗΜΑ 8: Ανάπτυξη διαδικασιών γνωστοποίησης εποπτικής Αρχής και ανακοίνωσης υποκειμένου

Οι 2 αυτές διαδικασίες είναι κρίσιμης σημασίας σύμφωνα με τα όσα ορίζονται στο GDPR. Αφορούν την υποχρέωση του οργανισμού να ενημερώνει άμεσα τόσο την Εθνική Εποπτεύουσα Αρχή όσο και τα ίδια τα Φυσικά Πρόσωπα σε περίπτωση που ο οργανισμός εντοπίσει Παραβίαση Προσωπικών Δεδομένων. Μάλιστα ο Κανονισμός υποχρεώνει τον οργανισμό να ενημερώσει εντός 3 ημερών την εποπτεύουσα Αρχή για τέτοιες περιπτώσεις, γεγονός που καθιστά απαραίτητο να υπάρχει πλήρης σχετική διαδικασία, ώστε να μην παρεκλίνει από το χρονικό αυτό όριο. Αντίστοιχα, εφόσον τα δεδομένα του φυσικού προσώπου που παραβιάστηκαν ενδέχεται να προκαλέσουν μεγάλο κίνδυνο στα δικαιώματα και τις ελευθερίες του, ο Οργανισμός είναι υποχρεωμένος να ενημερώνει αναλυτικά και το ίδιο το φυσικό πρόσωπο.

ΒΗΜΑ 9: Δοκιμαστικοί έλεγχοι συστημάτων και διαδικασιών

Έχοντας υλοποιήσει όλα τα παραπάνω βήματα σε θεωρητικό επίπεδο, είναι κρίσιμο οι αλλαγές και το νέο σύστημα να δοκιμαστεί στην πράξη. Πολλές φορές τα σχέδια επί χάρτου δεν είναι το ίδιο αποτελεσματικά στην πραγματική ροή. Έτσι, εφόσον παρατηρηθεί ότι κάποιες από τις νέες και αναπροσαρμοσμένες διαδικασίες πάσχουν στο κομμάτι της υλοποίησης, θα πρέπει να γίνουν οι απαραίτητες διορθωτικές ενέργειες.

ΒΗΜΑ 10: Διαρκής παρακολούθηση και επικαιροποίηση των διαδικασιών και των συστημάτων

Η υλοποίηση όλων των παραπάνω είναι υποχρεωτική, αλλά δεν σημαίνει ότι θα πρέπει να γίνεται μια φορά και εν συνεχεία να μην λαμβάνεται υπόψη. Όπως όλα τα Συστήματα Διαχείρισης Ποιότητας, έτσι και οι διαδικασίες που αναφέρονται στη Διαχείριση των Προσωπικών Δεδομένων, θα πρέπει να παρακολουθούνται και να επικαιροποιούνται σε τακτά χρονικά διαστήματα. Νέου είδους

επεξεργασίες δεδομένων στον οργανισμό λόγω νέων προσφερόμενων υπηρεσιών, νέες τεχνολογικές εξελίξεις είναι μόνο 2 παραδείγματα αιτιών που απαιτούν τη συνεχή παρακολούθηση των διαδικασιών αυτών. Παράλληλα, ο Οργανισμός θα πρέπει να φροντίσει να αρχειοθετεί τη σχετική τεκμηρίωση, ώστε να μπορεί να τεκμηριώνει την προσαρμογή της λειτουργία του στα όσα απαιτεί ο GDPR.

Κεφάλαιο 6
Δημιουργία Συστήματος Διαχείρισης Προσωπικών Δεδομένων

Έχοντας λάβει υπόψη όλα τα παραπάνω κεφάλαια της παρούσας εργασίας, διαφαίνεται ότι ο ιδανικός τρόπος προκειμένου να είναι συμβατός ένας εκπαιδευτικός οργανισμός με τον GDPR είναι η δημιουργία ενός Συστήματος Διαχείρισης Προσωπικών Δεδομένων. Ένα τέτοιο σύστημα δεν είναι υποχρεωτικό να είναι ένα νέο σύστημα εξολοκλήρου, γιατί όπως φάνηκε και από το κεφάλαιο 4 της εργασίας, ο οργανισμός μπορεί να διαθέτει ήδη κάποιο σύστημα διαχείρισης ποιότητας που να πληροί κάποιες από τις απαιτήσεις του κανονισμού. Θα πρέπει να γίνει προσεκτική μελέτη των υπαρχόντων διαδικασιών και εντύπων των υπαρχόντων συστημάτων, που αυτά πληρούν τις απαιτήσεις του GDPR, και μετά να προστεθούν όσο χρειάζονται και να τροποποιηθούν όσα καλύπτουν μερικώς τις απαιτήσεις.

Επειδή κάθε εκπαιδευτικός οργανισμός έχει διαφορετικό πεδίο δραστηριότητας, όπως και επίσης διαφορετικές διαδικασίες, είναι πρακτικά αδύνατο να δημιουργηθούν διαδικασίες που είναι συμβατές οριζόντια με το σύνολο των εκπαιδευτικών οργανισμών. Ανάλογα με τον τρόπο που λειτουργεί ο καθένας, θα πρέπει να υπάρχει μια εξατομικευμένη παρέμβαση στα συστήματα του κάθε οργανισμού.

Παρόλα αυτά, υπάρχουν κάποιες πολιτικές και διαδικασίες που είναι απαραίτητες. Ενδεικτικά παρατίθενται παρακάτω απαραίτητες πολιτικές και διαδικασίες που δεν καλύπτονται από τα υπάρχοντα συστήματα σχετικά με τις απαιτήσεις του GDPR και θα μπορούσαν δυνητικά να χρησιμοποιηθούν από το σύνολο των εκπαιδευτικών οργανισμών. Οι διαδικασίες που αναφέρονται παρακάτω μπορούν, με μικρές εξατομικευμένες αλλαγές, να χρησιμοποιηθούν από κάθε εκπαιδευτικό οργανισμό είτε αυτός είναι παραδείγματος χάριν ένα Ιδιωτικό Σχολείο με 50 εργαζόμενους και 200 σπουδαστές είτε αυτός είναι ένα Κέντρο Δια Βίου Μάθησης με 10 εργαζόμενους, 1000 καταρτιζόμενους και 30 εξωτερικούς συνεργάτες. Προφανώς, ο κάθε οργανισμός θα πρέπει να προσαρμόσει αυτές τις διαδικασίες στον τρόπο που λειτουργεί, αλλά η γενική εικόνα είναι ότι θα πρέπει να διαθέτει κατ' ελάχιστον τα παρακάτω.

Οι παρακάτω διαδικασίες και πολιτικές, είναι απαραίτητο να ενσωματωθούν σε υπάρχοντα ή προς δημιουργία συστήματα. Μάλιστα, καλύπτουν τις πιο σημαντικές πτυχές του του GDPR. Συγκεκριμένα, η Πολιτική Ρόλων και Αρμοδιοτήτων καλύπτει το Κεφάλαιο 4 (άρθρα 24-39), η Διαδικασία Τήρησης

Αρχείων το άρθρο 30 του Κεφαλαίου 4, η διαδικασία Γνωστοποίησης Παραβίασης Προσωπικών Δεδομένων τα άρθρα 33-34, η διαδικασία Συγκατάθεσης και Ανάκλησης Συγκατάθεσης Υποκειμένου το άρθρο 2 του Κεφαλαίου 2 και το σύνολο των άρθρων του Κεφαλαίου 3 που αφορά τα δικαιώματα του Υποκειμένου, η διαδικασία Προστασίας των Δεδομένων των Εργαζομένων τα άρθρα 12, 13 και 15-21 του Κεφαλαίου 3 και το άρθρο 88 του Κεφαλαίου 9 και τέλος η διαδικασία Ασφάλειας των Πληροφοριών το Κεφάλαιο 5 (άρθρο 32). Σαφώς όμως, ανάλογα με το οργανόγραμμα και τη λειτουργία του κάθε οργανισμού, θα πρέπει τόσο να εμπλουτιστούν οι προτεινόμενες διαδικασίες όσο και να προστεθούν νέες διαδικασίες και πολιτικές, που να καλύπτουν το σύνολο των απαιτήσεων των κεφαλαίων του GDPR.

Στη συνέχεια του παρόντος κεφαλαίου, αποτυπώνονται οι προτεινόμενες πολιτικές και διαδικασίες ανά Κεφάλαιο του GDPR, που μπορούν να χρησιμοποιηθούν από έναν εκπαιδευτικό οργανισμό. Κάποια από τα κεφάλαια του κανονισμού δεν απαιτούν συγκεκριμένες πολιτικές, διότι περιλαμβάνουν άρθρα που αποτελούν τη θεωρητική βάση για την υλοποίηση πολιτικών άλλων κεφαλαίων, όπως το Κεφάλαιο 1 – Γενικές Διατάξεις και το Κεφάλαιο 11 – Τελικές Διατάξεις. Επίσης, κάποια κεφάλαια δεν έχουν εφαρμογή στο πλαίσιο λειτουργίας ενός εκπαιδευτικού οργανισμού σε οριζόντιο επίπεδο, όπως το Κεφάλαιο 6 – Ανεξάρτητες Εποπτικές Αρχές, το Κεφάλαιο 7 – Συνεργασία και συνεκτικότητα, το Κεφάλαιο 8 – Προσφυγές, Ευθύνες και Κυρώσεις και το Κεφάλαιο 10 – Εξουσιοδοτήσεις. Για όλα τα υπόλοιπα κεφάλαια, λαμβάνονται υπόψη οι απαιτήσεις του κάθε άρθρου και επιχειρείται η δημιουργία πρότυπων διαδικασιών, με επεξήγηση των απαραίτητων στοιχείων που θα πρέπει να περιλαμβάνουν, ώστε να θεωρούνται πλήρεις και συμβατές.

A. Κεφάλαιο 2 GDPR → Διαδικασία Τήρησης Αρχείων

Μια πολύ σημαντική διαδικασία, που θα πιθανά ήδη να διαθέτουν εκπαιδευτικοί οργανισμοί που εφαρμόζουν συστήματα ποιότητας είναι αυτή της τήρησης αρχείων. Η διαδικασία της τήρησης αρχείων είναι και αυτή προαπαιτούμενη σε Συστήματα Διαχείρισης Ποιότητας που πληρούν τις προδιαγραφές του ISO9001 και του ISO27001. Εφόσον υπάρχει θα πρέπει να προσαρμοστεί σχετικά, ώστε να περιλαμβάνει ένα αρχείο δραστηριοτήτων σύμφωνα με τις αρχές προστασίας προσωπικών δεδομένων και τις απαιτήσεις του GDPR. Αυτή η διαδικασία αναφέρεται στο Άρθρο 30 - Αρχεία των δραστηριοτήτων επεξεργασίας, στο ΚΕΦΑΛΑΙΟ ΙΙ- Αρχές και στο ΚΕΦΑΛΑΙΟ ΙV- Υπεύθυνος επεξεργασίας και εκτελών την επεξεργασία του GDPR. Οι περισσότεροι φορείς οφείλουν να τηρούν ένα αρχείο με την περιγραφή των δραστηριοτήτων επεξεργασίας προσωπικών δεδομένων. Το αρχείο αυτό δεν είναι σημαντικό μόνο γιατί αποτελεί υποχρέωση από το άρθρο 30 ΓΚΠΔ ως εργαλείο λογοδοσίας, αλλά και γιατί είναι χρήσιμο για τη σωστή οργάνωση των διαδικασιών χειρισμού των τηρούμενων προσωπικών δεδομένων. Υποχρέωση τήρησης του αρχείου έχουν οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία, με διαφορετικά στοιχεία για τον καθένα. Τα

υποχρεωτικά στοιχεία περιγράφονται αναλυτικά στο άρ. 30 παρ. 1 ΓΚΠΔ, όσον αφορά στους υπευθύνους επεξεργασίας και στο άρ. 30 παρ. 2 όσον αφορά στους εκτελούντες την επεξεργασία. Εκτός των υποχρεωτικών στοιχείων, μπορεί να συμπεριληφθούν και επιπλέον στοιχεία που ένας υπεύθυνος ή εκτελών θεωρεί ότι διευκολύνουν τη συμμόρφωσή του.

Η τήρηση του αρχείου δραστηριοτήτων εξυπηρετεί πολλαπλούς σκοπούς εντός μιας οντότητας. Καταρχήν, μια οντότητα έχει υποχρέωση να θέσει το Αρχείο Δραστηριοτήτων στη διάθεση της Αρμόδιας Εποπτικής Αρχής, αν αυτή το ζητήσει. Εν συνεχεία η σύνταξη και η τήρηση του αρχείου δραστηριοτήτων συντελεί στην γνώση του οργανωτικού πλαισίου λειτουργίας μιας οντότητας καθώς είναι ένα εργαλείο αυτογνωσίας και αυτό-αξιολόγησης για τη συμμόρφωση με τον Κανονισμό. Παράλληλα η συμπλήρωση του αρχείου δραστηριοτήτων βοηθά στη διαμόρφωση πολιτικών ή/και μηχανισμών για την άσκηση των δικαιωμάτων των υποκειμένων των δεδομένων (Άρθρο 12(1)) ή ακόμη και στην ενδεχόμενη υιοθέτηση πολιτικής προστασίας της ιδιωτικής ζωής. Τέλος η τήρηση του αρχείου δραστηριοτήτων, βοηθά μια οντότητα να συμμορφώνεται με τις Αρχές της Λογοδοσίας (Άρθρο 5(2)) και της Διαφάνειας (Άρθρο 5(1)(α)) όπως απαιτείται από τη νομοθεσία.

Η συμπλήρωση του Αρχείου Δραστηριοτήτων Επεξεργασίας δεν είναι στατική. Είναι μια συνεχής διαδικασία αφού, όταν διαφοροποιείται ή αλλάζει μια υφιστάμενη δραστηριότητα επεξεργασίας ή προστίθεται μια καινούργια, το Αρχείο πρέπει να επικαιροποιείται.

Ένας υπεύθυνος επεξεργασίας ή ο εκπρόσωπός του, έχει υποχρέωση να τηρεί τις πληροφορίες που αναφέρονται στο Άρθρο 30(1). Ωστόσο, τίποτε δεν τους εμποδίζει να τηρούν πρόσθετες πληροφορίες, για σκοπούς αυτογνωσίας, αυτό-αξιολόγησης, λογοδοσίας και διαφάνειας. Το αρχείο δραστηριοτήτων θα πρέπει να συμπληρώνεται, ανανεώνεται και αναθεωρείται με σεβασμό στην αρχή της αναλογικότητας και της αναγκαιότητας, ειδικά σε ό,τι αφορά το χρονικό διάστημα διατήρησης των αρχείων που αναγράφονται. Το αρχείο δραστηριοτήτων μπορεί να τηρείται σε οποιαδήποτε μορφή αν και συνίσταται ο ηλεκτρονικός τρόπος αποθήκευσης με τη λήψη όλων των κατάλληλων μέτρων ασφαλείας φυσικής και ψηφιακής πρόσβασης.

Β. Κεφάλαιο 3 GDPR → Διαδικασία Συγκατάθεσης και Ανάκλησης Συγκατάθεσης Υποκειμένου

Μια τέτοια διαδικασία θα πρέπει να περιγράφει πώς ο Εκπαιδευτικός Οργανισμός θα λάβει τη συγκατάθεση του υποκειμένου δεδομένων όπως αυτό καθορίζεται στον ΓΚΠΔ, σύμφωνα με τα όσα ορίζονται στο Άρθρο 7 και το Κεφάλαιο 3 του GDPR.

Η συγκατάθεση του υποκειμένου των δεδομένων ορίζεται από το ΓΚΠΔ ως « κάθε ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, ρητή και εν πλήρη επίγνωση, με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο

επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν». Συγκεκριμένα στον ΓΚΠΔ αναφέρεται ότι «Η συγκατάθεση θα πρέπει να παρέχεται με σαφή θετική ενέργεια η οποία να συνιστά ελεύθερη, συγκεκριμένη, ρητή και εν πλήρη επίγνωση ένδειξη της συμφωνίας του υποκειμένου των δεδομένων υπέρ της επεξεργασίας των δεδομένων που το αφορούν, για παράδειγμα με γραπτή δήλωση, μεταξύ άλλων με ηλεκτρονικά μέσα, ή με προφορική δήλωση. Αυτό θα μπορούσε να περιλαμβάνει τη συμπλήρωση ενός τετραγωνιδίου κατά την επίσκεψη σε διαδικτυακή ιστοσελίδα, την επιλογή των επιθυμητών τεχνικών ρυθμίσεων για υπηρεσίες της κοινωνίας των πληροφοριών ή μια δήλωση ή συμπεριφορά που δηλώνει σαφώς, στο συγκεκριμένο πλαίσιο, ότι το υποκείμενο των δεδομένων αποδέχεται την πρόταση επεξεργασίας των οικείων δεδομένων προσωπικού χαρακτήρα. Επομένως, η σιωπή, τα προσυμπληρωμένα checkboxes ή η αδράνεια δεν θα πρέπει να εκλαμβάνονται ως συγκατάθεση. Η συγκατάθεση θα πρέπει να καλύπτει το σύνολο των δραστηριοτήτων επεξεργασίας που διενεργείται για τον ίδιο σκοπό ή για τους ίδιους σκοπούς. Όταν η επεξεργασία έχει πολλαπλούς σκοπούς, θα πρέπει να δίνεται συγκατάθεση για όλους αυτούς τους σκοπούς. Εάν η συγκατάθεση του υποκειμένου των δεδομένων πρόκειται να δοθεί κατόπιν αιτήματος με ηλεκτρονικά μέσα, το αίτημα πρέπει να είναι σαφές, περιεκτικό και να μην διαταράσσει αδικαιολόγητα τη χρήση της υπηρεσίας για την οποία παρέχεται.»

Η συγκατάθεση του υποκειμένου των δεδομένων είναι ένας από τους όρους για την επεξεργασία των προσωπικών του δεδομένων και εμπίπτει στο πεδίο εφαρμογής της παρούσας διαδικασίας.

Ο Εκπαιδευτικός Οργανισμός θα πρέπει να λαμβάνει συγκατάθεση όταν δεν ισχύει άλλη νόμιμη βάση. Απαιτείται ρητή συγκατάθεση για την επεξεργασία ευαίσθητων προσωπικών δεδομένων. Ειδικοί όροι ισχύουν για την εγκυρότητα της συγκατάθεσης που δίνεται από τα παιδιά σε σχέση με τις υπηρεσίες της κοινωνίας της πληροφορίας, με απαιτήσεις για την απόκτηση και την επαλήθευση της γονικής συναίνεσης κάτω από ορισμένα όρια ηλικίας.

Εκτός από το θεωρητικό σκέλος, θα πρέπει να αναφέρονται αναλυτικά τα βήματα που πρέπει να γίνουν για να ληφθεί η Συγκατάθεση. Έτσι, ενδεικτικά θα πρέπει να αναφέρεται ότι:

1. Ο Εκπαιδευτικός Οργανισμός παρέχει μια σαφή Δήλωση Απορρήτου όπου συλλέγονται προσωπικά δεδομένα για να εξασφαλίζεται ότι η συγκατάθεση υφίσταται και ότι το υποκείμενο των δεδομένων ενημερώνεται για τα δικαιώματά του σε σχέση με τα προσωπικά του δεδομένα.

2. Ο Εκπαιδευτικός Οργανισμός καταδεικνύει τη συγκατάθεση του υποκείμενου των δεδομένων για την επεξεργασία των προσωπικών του δεδομένων ή τη ρητή συγκατάθεσή του για ευαίσθητα προσωπικά δεδομένα (έντυπο συναίνεσης του υποκειμένου των δεδομένων).

3. Ο Εκπαιδευτικός Οργανισμός καταδεικνύει τη συγκατάθεση του υποκείμενου των δεδομένων για την επεξεργασία των προσωπικών του δεδομένων για έναν ή περισσότερους συγκεκριμένους σκοπούς (έντυπο συναίνεσης του υποκειμένου των δεδομένων).

4. Ο Εκπαιδευτικός Οργανισμός καταδεικνύει ότι η συγκατάθεση του υποκείμενου των δεδομένων είναι σαφώς διακριτή από οποιοδήποτε άλλο θέμα σχετικά με το υποκείμενο των δεδομένων.

5. Ο Εκπαιδευτικός Οργανισμός καταδεικνύει ότι η συγκατάθεση του υποκείμενου των δεδομένων είναι κατανοητή και προσβάσιμη, χρησιμοποιώντας σαφή και απλή γλώσσα.

6. Ο Εκπαιδευτικός Οργανισμός αποδεκνύει ότι τα υποκείμενα των δεδομένων ενημερώνονται για το δικαίωμά τους να αποσύρουν τη συγκατάθεσή τους πριν δώσουν τη συγκατάθεσή τους (Διαδικασία Ανάκλησης συγκατάθεσης).

7. Ο Εκπαιδευτικός Οργανισμός αποδεικνύει ότι η επεξεργασία των δεδομένων περιορίζεται σε αυτή που αναφέρεται στη σύμβαση, η οποία δεσμεύεται από τη ρητή συγκατάθεση του υποκειμένου των δεδομένων.

Όταν η επεξεργασία αφορά ανήλικο κάτω των 14 ετών, ο Εκπαιδευτικός Οργανισμός θα πρέπει να αποδεικνύει ότι η συγκατάθεση έχει παρασχεθεί από το πρόσωπο που έχει τη γονική μέριμνα του ανηλίκου και να καταδεικνύει ότι έχουν γίνει εύλογες προσπάθειες για την επαλήθευση της ηλικίας του ανηλίκου και για τον καθορισμό της γνησιότητας της γονικής μέριμνας λαμβάνοντας υπόψη τη διαθέσιμη τεχνολογία.

Εκτός όμως από τη λήψη της συγκατάθεσης του Φυσικού Προσώπου, ο GDPR αναφέρει ότι θα πρέπει να υπάρχει ρητή πρόβλεψη και για την ανάκληση της συγκατάθεσης σε μεταγενέστερο χρόνο (Άρθρο 7, Κεφάλαιο 3). Η ανάκληση της συγκατάθεσης από το υποκείμενο των δεδομένων σημαίνει μια ξεκάθαρη ένδειξη της επιθυμίας του υποκειμένου των δεδομένων με την οποία αυτός ή αυτή, με δήλωση ή με σαφή καταφατική δράση, ανακαλεί τη συγκατάθεσης για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα που τον/την αφορούν. Η ανάκληση της συγκατάθεσης δεν επηρεάζει τη νομιμότητα της επεξεργασίας βάσει της προηγουμένως δοθείσας έγκυρης συγκατάθεσης πριν από την απόσυρσή της. Η ανάκληση της συγκατάθεσης καλύπτει όλες τις επεξεργασίες που πραγματοποιήθηκαν για τον ίδιο σκοπό ή σκοπούς για τους οποίους δόθηκε και αρχικά η συγκατάθεση. Προκειμένου να είναι σαφής η διαδικασία, θα πρέπει να καταγραφούν τα αναλυτικά βήματα. Ενδεικτικά τέτοια βήματα είναι:

1. Το υποκείμενο των δεδομένων υποβάλλει αίτημα μέσω μιας από πολλές μεθόδους, συμπεριλαμβανομένης της ηλεκτρονικής (μέσω ηλεκτρονικού ταχυδρομείου ή μέσω της ιστοσελίδας μας), με επιστολή ή μέσω τηλεφώνου. Αυτό μπορεί να ληφθεί από οποιοδήποτε υπάλληλο του οργανισμού, αλλά θα πρέπει ιδανικά να διοχετεύεται μέσω της εξυπηρέτησης πελατών. Για το σκοπό

αυτό είναι διαθέσιμες φόρμες για την άσκηση των δικαιωμάτων των υποκειμένων. Σε κάθε περίπτωση θα πρέπει να ενημερώνεται και ο Υπεύθυνος Προστασίας Δεδομένων εάν υπάρχει ώστε να επιβλέπει τη διαδικασία

2. Το γεγονός ότι έχει ληφθεί το αίτημα καταγράφεται στο Μητρώο Αιτημάτων Υποκειμένου Δεδομένων και καταγράφεται και η ημερομηνία του αιτήματος.

3. Η ταυτότητα του υποκειμένου δεδομένων επιβεβαιώνεται με εγκεκριμένη μέθοδο. Μπορεί να ζητηθούν περισσότερες πληροφορίες για την επιβεβαίωση της ταυτότητας, εάν απαιτείται. Εάν δεν είναι δυνατόν να επιβεβαιωθεί η ταυτότητα του υποκειμένου δεδομένων, το αίτημα απορρίπτεται και ο λόγος γι' αυτό κοινοποιείται στο υποκείμενο των δεδομένων.

4. Ελέγχεται αν το αίτημα είναι «προδήλως αβάσιμο ή υπερβολικό». Εάν ναι, αποφασίζεται εάν θα απορριφθεί το αίτημα ή θα επιβληθεί σχετική επιβάρυνση. Σε περίπτωση αιτήσεων για διόρθωση, διαγραφή, περιορισμό ή εναντίωση κατά της επεξεργασίας, λαμβάνεται επίσης απόφαση σχετικά με το αν το αίτημα είναι εύλογο και νόμιμο. Εάν όχι, απορρίπτεται το αίτημα και ενημερώνεται το υποκείμενο των δεδομένων για την απόφαση και το δικαίωμά του να υποβάλει καταγγελία στην εποπτική αρχή.

5. Εάν εφαρμόζεται χρέωση, το υποκείμενο των δεδομένων ενημερώνεται για την επιβάρυνση και έχει την ευκαιρία να αποφασίσει εάν θα συνεχίσει ή όχι. Εάν το υποκείμενο των δεδομένων αποφασίσει να μην προχωρήσει, η αίτηση απορρίπτεται και οι κοινοποιούνται οι λόγοι.

6. Οι σχετικές πληροφορίες συγκεντρώνονται σύμφωνα με τον τύπο αιτήματος. Αυτό μπορεί να περιλαμβάνει τον προγραμματισμό του τρόπου με τον οποίο ζητείται η ενέργεια, π.χ. διαγραφή ή περιορισμό της επεξεργασίας. Χορηγείται κατ' ανώτατο όριο προθεσμία ενός μήνα. Αν το αίτημα θα διαρκέσει περισσότερο από αυτό τότε επιτρέπονται κατ' ανώτατο όριο δύο επιπλέον μήνες και το υποκείμενο δεδομένων πρέπει να ενημερωθεί για την καθυστέρηση και τους λόγους της εντός ενός μηνός από την υποβολή της αίτησης.

7. Η ζητούμενη ενέργεια διεξάγεται (εάν ισχύει) και οι πληροφορίες που ζητούνται παρέχονται στο υποκείμενο των δεδομένων ηλεκτρονικά, εάν αυτή είναι η προτιμώμενη μέθοδος ή με άλλα μέσα.

8. Το γεγονός ότι το αίτημα έχει απαντηθεί καταχωρείται σε σχετικό Μητρώο Αιτημάτων Υποκειμένων Δεδομένων, μαζί με την ημερομηνία ολοκλήρωσης

Η ανάκληση της συγκατάθεσης από το υποκείμενο των δεδομένων υποδηλώνει την επιθυμία του υποκειμένου των δεδομένων για άρση της συγκατάθεσής του ως προς μια ή περισσότερες συγκεκριμένες επεξεργασίες δεδομένων που το αφορούν. Υπό αυτή την έννοια με την άρση της συγκατάθεσης και εφόσον δεν υφίσταται άλλη νόμιμη βάση επεξεργασίας όπως π.χ σύμβαση, ο

Υπεύθυνος Επεξεργασίας προφανώς θα πρέπει να παύσει την επεξεργασία των εν λόγω προσωπικών δεδομένων του υποκειμένου για την οποία δεν έχει πλέον νόμιμη βάση (οπότε και η συνέχισή της θα θεωρείται παράνομη). Ως εκ τούτου πριν από την εξαίρεση των προσωπικών δεδομένων του υποκειμένου από την επεξεργασία, πρέπει να επιβεβαιωθεί ότι η συναίνεση είναι πράγματι η βάση της επεξεργασίας (και δεν υφίσταται άλλη νόμιμη βάση). Εάν υφίσταται άλλη νόμιμη βάση διαφορετική από την συγκατάθεση με βάση το ΓΚΠΔ τότε το αίτημα μπορεί να απορριφθεί με την αιτιολογία ότι η επεξεργασία δεν απαιτεί τη συγκατάθεση του υποκειμένου των δεδομένων. Διαφορετικά, θα πρέπει να επιτρέπεται το αίτημα.

Σε πολλές περιπτώσεις, η παροχή και η απόσυρση της συγκατάθεσης θα είναι διαθέσιμη ηλεκτρονικά, δηλ. στο διαδίκτυο, και αυτή η διαδικασία ενδεχομένως να τροποποιείται στο βαθμό που απαιτείται ή δεν απαιτείται η εμπλοκή και ανταπόκριση του Υπεύθυνου Επεξεργασίας μέσω του προσωπικού του. Όταν η συναίνεση αφορά ένα παιδί, η παραχώρηση ή η απόσυρση πρέπει να επιτρέπεται μόνο από το νόμιμο κηδεμόνα του ανηλίκου.

C. Κεφάλαιο 4 GDPR → Πολιτική Ρόλων και Αρμοδιοτήτων

Το έγγραφο αυτό θα πρέπει να παρουσιάζει ορισμένους από τους κύριους ρόλους που μπορεί να εμπλέκονται στη συμμόρφωση με το ΓΚΠΔ, καθώς και τις σχετικές αρμοδιότητές τους. Σχετίζεται με το Κεφάλαιο IV– Υπεύθυνος επεξεργασίας και εκτελών την επεξεργασία και το Τμήμα 4. - Υπεύθυνος προστασίας δεδομένων του GDPR.

Η πολιτική αυτή θα πρέπει να περιλαμβάνει το οργανόγραμμα του Οργανισμού. Ένα τέτοιο έγγραφο σίγουρα υπάρχει, εφόσον ο οργανισμός διαθέτει και εφαρμόζει ήδη Συστήματα Διαχείρισης Ποιότητας βάσει άλλων προτύπων, αφού είναι προαπαιτούμενο τόσο στο ISO9001, όσο και στο ISO27001. Μέσα στο πλαίσιο προστασίας δεδομένων που σχετίζεται με τη συμμόρφωσή του Οργανισμού με το ΓΚΠΔ, στην ήδη υπάρχουσα πολιτική θα πρέπει να καθοριστούν, να διανεμηθούν και να προστεθούν οι ακόλουθοι σημαντικοί ρόλοι:

- Υπεύθυνος επεξεργασίας
- Εκτελών την επεξεργασία
- Υπεύθυνος ασφάλειας πληροφοριών
- Υπεύθυνος Προστασίας Δεδομένων
- Υπεύθυνος συμμόρφωσης με το ΓΚΠΔ

Μετά την οριοθέτηση και καταγραφή των ρόλων που έχουν εμπλοκή στη διαχείριση των Προσωπικών Δεδομένων, θα πρέπει να υπάρχει μια καταγραφή με το τι ακριβώς αρμοδιότητες έχει ο κάθε ρόλος.

Έτσι, ενδεικτικά θα μπορούσε να αναφερθεί ότι ο ΥΠΕΥΘΥΝΟΣ ΕΠΕΞΕΡΓΑΣΙΑΣ θα μπορούσε να έχει τις ακόλουθες αρμοδιότητές:

- Διασφαλίζει ότι τηρούνται οι αρχές σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα που περιγράφονται στο άρθρο 5 του ΓΚΠΔ και ότι είναι εφικτό να αποδειχθεί η συμμόρφωση του Εκπαιδευτικού Οργανισμού με αυτές. Εν ολίγοις, οι ακόλουθες προϋποθέσεις διασφαλίζουν ότι τα προσωπικά δεδομένα:
    - Τυγχάνουν επεξεργασίας νόμιμα, δίκαια και με διαφάνεια
    - Συλλέγονται για συγκεκριμένους, σαφείς και νόμιμους σκοπούς ο Είναι επαρκή, σχετικά και περιορισμένα σε ό, τι είναι απαραίτητο ο Είναι ακριβή και, όπου χρειάζεται, ενημερωμένα
    - Διατηρούνται σε μορφή που επιτρέπει τον εντοπισμό των υποκειμένων των δεδομένων για όχι περισσότερο χρονικό διάστημα από το αναγκαίο
    - Υποβάλλονται σε επεξεργασία με τρόπο που εξασφαλίζει την κατάλληλη ασφάλεια
- Εξασφαλίζει ότι η συγκατάθεση του υποκειμένου των δεδομένων στην επεξεργασία των προσωπικών δεδομένων λαμβάνεται, όπου ενδείκνυται, συμπεριλαμβανομένης της γονικής άδειας για ανηλίκους
- Παρέχει όλες τις πληροφορίες που απαιτούνται βάσει του ΓΚΠΔ στο υποκείμενο των δεδομένων με συνοπτική, διαφανή, κατανοητή και εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή γλώσσα
- Διευκολύνει την άσκηση των δικαιωμάτων των υποκειμένων των δεδομένων στο πλαίσιο του ΓΚΠΔ και ενημερώνει το υποκείμενο των δεδομένων για την πρόοδο του αιτήματός του
- Εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα για να εξασφαλίσει και να καταδείξει ότι η επεξεργασία πραγματοποιείται σύμφωνα με τις προϋποθέσεις του ΓΚΠΔ
- Εξασφαλίζει ότι χρησιμοποιούνται μόνο εκτελούντες την επεξεργασία που παρέχουν επαρκείς διαβεβαιώσεις για την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων κατά τρόπο ώστε η επεξεργασία να πληροί της απαιτήσεις του ΓΚΠΔ και να διασφαλίζεται η προστασία των δικαιωμάτων του υποκειμένου των δεδομένων.
- Διατηρεί αρχείο δραστηριοτήτων επεξεργασίας σχετικά με προσωπικά δεδομένα που εμπίπτουν στην ευθύνη του
- Συνεργάζεται, κατόπιν αιτήματος, με την εποπτική αρχή κατά την εκτέλεση των καθηκόντων της
- Εξασφαλίζει ότι κάθε πρόσωπο που ενεργεί υπό την εποπτεία του υπεύθυνου

επεξεργασίας που έχει πρόσβαση σε δεδομένα προσωπικού χαρακτήρα δεν τα επεξεργάζεται παρά μόνο με βάση τις οδηγίες του υπεύθυνου επεξεργασίας

- Διασφαλίζει ότι τα πρόσωπα που επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα έχουν αναλάβει δέσμευση τήρησης εμπιστευτικότητας ή τελούν υπό τη δέουσα κανονιστική υποχρέωση τήρησης εμπιστευτικότητας
- Ειδοποιεί το αρμόδιο γραφείο του Οργανισμού περί παραβίασης προσωπικών δεδομένων, εκτός εάν η παραβίαση προσωπικών δεδομένων είναι απίθανο να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, σύμφωνα με τις οργανωτικές διαδικασίες
- Καταγράφει τυχόν παραβιάσεις των προσωπικών δεδομένων, συμπεριλαμβανομένων των γεγονότων σχετικά με την παραβίαση των προσωπικών δεδομένων, των αποτελεσμάτων τους και των επανορθωτικών μέτρων που έχουν ληφθεί
- Όπου ενδείκνυται, κοινοποιεί ζητήματα παραβίασης των δεδομένων προσωπικού χαρακτήρα χωρίς αδικαιολόγητη καθυστέρηση
- Διεξάγει αξιολογήσεις επιπτώσεων για την προστασία των δεδομένων, κατά περίπτωση, σύμφωνα με τις διαδικασίες
- Ορίζει υπεύθυνο προστασίας δεδομένων, όπου απαιτείται από το ΓΚΠΔ, δημοσιεύει τα στοιχεία του και τα κοινοποιεί στην Αρμόδια Εποπτική Αρχή**.** Στηρίζει τον υπεύθυνο προστασίας δεδομένων στην άσκηση των καθηκόντων του παρέχοντας τους απαραίτητους πόρους για την άσκηση των εν λόγω καθηκόντων καθώς και πρόσβαση σε προσωπικά δεδομένα και πράξεις επεξεργασίας και πόρους απαραίτητους για τη διατήρηση της εμπειρογνωμοσύνης του.
- Διαβιβάζει δεδομένα προσωπικού χαρακτήρα σε Τρίτη χώρα ή διεθνή οργανισμό μόνο εάν ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία έχει παράσχει τις κατάλληλες εγγυήσεις και υπό την προϋπόθεση ότι υφίστανται εκτελεστά δικαιώματα και αποτελεσματικά ένδικα μέσα για τα υποκείμενα των δεδομένων

Ο ΕΚΤΕΛΩΝ ΤΗΝ ΕΠΕΞΕΡΓΑΣΙΑ θα μπορούσε να έχει τις παρακάτω αρμοδιότητες:

- Επεξεργάζεται τα δεδομένα προσωπικού χαρακτήρα μόνο βάσει καταγεγραμμένων εντολών του υπευθύνου επεξεργασίας, μεταξύ άλλων όσον αφορά τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε Τρίτη χώρα ή διεθνή οργανισμό, ο εκτελών την επεξεργασία ενημερώνει τον υπεύθυνο επεξεργασίας για την εν λόγω νομική απαίτηση πριν από την επεξεργασία, εκτός εάν το εκάστοτε δίκαιο απαγορεύει αυτού του είδους την ενημέρωση για σοβαρούς λόγους δημόσιου συμφέροντος,

- Διασφαλίζει ότι τα πρόσωπα που είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα έχουν αναλάβει δέσμευση τήρησης εμπιστευτικότητας ή τελούν υπό τη δέουσα κανονιστική υποχρέωση τήρησης εμπιστευτικότητας
- Λαμβάνει τα κατάλληλα τεχνικά και οργανωτικά μέτρα για τη διασφάλιση ενός επιπέδου ασφαλείας που να ανταποκρίνεται στον κίνδυνο που συνδέεται με την επεξεργασία των προσωπικών δεδομένων
- Δεν προσλαμβάνει άλλον εκτελούντα την επεξεργασία χωρίς προηγούμενη ειδική ή γενική γραπτή άδεια του υπευθύνου επεξεργασίας.
- Λαμβάνει υπόψη τη φύση της επεξεργασίας και επικουρεί τον υπεύθυνο επεξεργασίας με τα κατάλληλα τεχνικά και οργανωτικά μέτρα, στον βαθμό που αυτό είναι δυνατό, για την εκπλήρωση της υποχρέωσης του υπευθύνου επεξεργασίας να απαντά σε αιτήματα για άσκηση των δικαιωμάτων του υποκειμένου των δεδομένων,
- Κατ' επιλογή του υπευθύνου επεξεργασίας, διαγράφει ή επιστρέφει όλα τα δεδομένα προσωπικού χαρακτήρα στον υπεύθυνο επεξεργασίας μετά το πέρας της παροχής υπηρεσιών επεξεργασίας και διαγράφει τα υφιστάμενα αντίγραφα
- Θέτει στη διάθεση του υπευθύνου επεξεργασίας κάθε απαραίτητη πληροφορία προς απόδειξη της συμμόρφωσης προς τις υποχρεώσεις που θεσπίζονται στο παρόν άρθρο και επιτρέπει και διευκολύνει τους ελέγχους, συμπεριλαμβανομένων των επιθεωρήσεων, που διενεργούνται από τον υπεύθυνο επεξεργασίας ή από άλλον ελεγκτή εντεταλμένο από τον υπεύθυνο επεξεργασίας.
- Διατηρεί αρχείο όλων των κατηγοριών δραστηριοτήτων επεξεργασίας που εκτελούνται για λογαριασμό του υπευθύνου επεξεργασίας
- Συνεργάζεται κατόπιν αιτήματος, με την Αρμόδια Εποπτική Αρχή κατά την εκτέλεση των καθηκόντων του
- Λαμβάνει μέτρα ώστε να διασφαλίζεται ότι κάθε φυσικό πρόσωπο που ενεργεί υπό την εποπτεία του εκτελούντα την επεξεργασία που έχει πρόσβαση σε δεδομένα προσωπικού χαρακτήρα δεν τα επεξεργάζεται παρά μόνο με βάση τις οδηγίες του υπεύθυνου επεξεργασίας
- Ενημερώνει τον υπεύθυνο επεξεργασίας αμελλητί μόλις αντιληφθεί παραβίαση προσωπικών δεδομένων
- Ορίζει υπεύθυνο προστασίας δεδομένων, όπου απαιτείται από το ΓΚΠΔ, δημοσιεύει τα στοιχεία του και τα κοινοποιεί στην εποπτική αρχή
- Στηρίζει το υπεύθυνο προστασίας δεδομένων στην άσκηση των καθηκόντων του παρέχοντας τους απαραίτητους πόρους για την άσκηση των εν λόγω καθηκόντων και πρόσβαση σε προσωπικά δεδομένα και πράξεις επεξεργασίας και πόρους απαραίτητους για

τη διατήρηση της εμπειρογνωμοσύνης του

Ο ΥΠΕΥΘΥΝΟΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ θα μπορούσε να έχει τις παρακάτω αρμοδιότητες:

- Ενημερώνει και συμβουλεύει τον Εκπαιδευτικό Οργανισμό και τους υπαλλήλους του σχετικά με τις υποχρεώσεις τους που απορρέουν από τον Κανονισμό και άλλες διατάξεις περί προστασίας δεδομένων.
- Παρακολουθεί την εσωτερική συμμόρφωση με τον Κανονισμό και άλλες διατάξεις περί προστασίας δεδομένων (π.χ. προσδιορισμός και διαχείριση δραστηριοτήτων επεξεργασίας, εκπαίδευση προσωπικού, διενέργεια εσωτερικών ελέγχων).
- Παρέχει συμβουλές για την εκτίμηση αντικτύπου και παρακολουθεί την υλοποίησή της.
- Είναι το πρώτο σημείο επαφής για τις εποπτικές αρχές και τα υποκείμενα των δεδομένων (εργαζόμενοι, πελάτες κ.λπ.)
- Συνεργάζεται με την εποπτική αρχή.
- Ενεργεί ως σημείο επαφής των εποπτικών αρχών σε θέματα επεξεργασίας δεδομένων προσωπικού χαρακτήρα και διαβουλεύεται, κατά περίπτωση, σχετικά με οποιοδήποτε άλλο θέμα

Ο ΥΠΕΥΘΥΝΟΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ θα μπορούσε να έχει τις εξής αρμοδιότητες:

- Υποβάλλει εκθέσεις στη Διοίκηση για όλα τα θέματα που σχετίζονται με την ασφάλεια σε τακτική βάση και κατά περίπτωση, όταν απαιτείται
- Επικοινωνεί την πολιτική ασφάλειας των πληροφοριών σε όλα τα ενδιαφερόμενα μέρη, όπου ενδείκνυται, συμπεριλαμβανομένων των πελατών
- Εφαρμόζει την πολιτική ασφάλειας πληροφοριών
- Διαχειρίζεται κινδύνους που σχετίζονται με την πρόσβαση σε υπηρεσίες ή τα πληροφοριακά συστήματα
- Βεβαιώνει ότι έχουν τεθεί σε λειτουργία και έχουν τεκμηριωθεί οι έλεγχοι ασφαλείας
- Ποσοτικοποιεί και παρακολουθεί τους τύπους, τους όγκους και τις επιπτώσεις των συμβάντων και των δυσλειτουργιών ασφαλείας
- Καθορίζει σχέδια βελτίωσης και στόχους για το οικονομικό έτος
- Παρακολουθεί την επίτευξη των στόχων
- Προσδιορίζει και διαχειρίζεται τα περιστατικά ασφάλειας πληροφοριών σύμφωνα με μια διαδικασία

Ο ΥΠΕΥΘΥΝΟΣ ΣΥΜΜΟΡΦΩΣΗΣ ΜΕ ΤΟ ΓΚΠΔ θα μπορούσε να έχει αρμοδιότητες:

- Για την εφαρμογή του συστήματος συμμόρφωσης, διαχείρισης και προστασίας προσωπικών δεδομένων εντός της οντότητας και για άλλα ζητήματα όπως α) η επικοινωνία και ο συντονισμός με την ομάδα έργου συμμόρφωσης, β) η παρακολούθηση της αναθεώρησης και υπογραφής εγγράφων σχετικών με την προστασία προσωπικών δεδομένων, γ) η εισαγωγή ζητημάτων προς συζήτηση με την Διοίκηση, δ) η συνεργασία και η παρακολούθηση με τον ΥΠΔ κλπ.
- Τον έλεγχο και την ανάγκη έκτακτης αναθεώρησης ή/και προσαρμογής διαδικασιών και πολιτικών προστασίας με βάση τις νέες τεχνολογίες, πρακτικές, συμβατικές δεσμεύσεις και μεθόδους επεξεργασίας της οντότητας
- Για τη συμπλήρωση, φύλαξη και εισαγωγή προς έγκριση στη Διοίκηση εντύπων του συστήματος διαχείρισης και προστασίας προσωπικών δεδομένων.
- Για την κοινοποίηση των εντύπων στα ενδιαφερόμενα μέρη
- Για το συντονισμό των ενεργειών για την προστασία των προσωπικών δεδομένων εντός της οντότητας με βάση τις αρμοδιότητες κάθε ρόλου.

D. Κεφάλαιο 4: Διαδικασία Γνωστοποίησης Παραβίασης Προσωπικών Δεδομένων

Αυτή η διαδικασία ορίζει το πώς ένας εκπαιδευτικός Οργανισμός θα ικανοποιήσει, ως ελάχιστο, τις απαιτήσεις κοινοποίησης του ΓΚΠΔ σε περίπτωση παραβίασης προσωπικών δεδομένων (Άρθρο 33 και 34). Ο ΓΚΠΔ είναι συγκεκριμένος όσον αφορά τις πληροφορίες που πρέπει να παρέχονται στην εποπτική αρχή σε περίπτωση παραβίασης και τις προϋποθέσεις που πρέπει να πληρούνται εάν απαιτείται κοινοποίηση στα υποκείμενα των δεδομένων. Είναι σημαντικό να κατανοηθούν αυτές τις απαιτήσεις και ο οργανισμός να είναι σε θέση να λαμβάνει αποφάσεις σχετικά με την κοινοποίηση που δεν συμμορφώνεται μόνο με τον ΓΚΠΔ αλλά και με τις επιχειρηματικές και δεοντολογικές ανάγκες και τις φιλοδοξίες του Οργανισμού. Η Αναγνώριση παραβιάσεων δεδομένων και η καταγραφή τους ένα αρχείο καταγραφής παραβίασης δεδομένων είναι απαραίτητο. Ακριβώς όπως ένα βιβλίο ατυχημάτων, το αρχείο καταγραφής παραβίασης δεδομένων πρέπει να καταγράφει όλες τις παραβιάσεις, όσο ήσσονος σημασίας και αν είναι[43].

Σύμφωνα με τον ΓΚΠΔ τα περιστατικά που αφορούν δεδομένα προσωπικού χαρακτήρα και ενδέχεται να θέσουν σε κίνδυνο τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων πρέπει να αναφέρονται χωρίς καθυστέρηση στην εποπτική αρχή προστασίας δεδομένων, όπου είναι εφικτό,

[43] DEMYSTIFYING THE GENERAL DATA PROTECTION REGULATION (GDPR): SOME OF THE ISSUES RELEVANT TO THE COUNSELLING PROFESSIONS. Authors: MEMBREY, DAVID MITCHELS, BARBARA, Source: Healthcare Counselling & Psychotherapy Journal. Jan2019, Vol. 19 Issue 1, p16-21. 6p.

εντός 72 ωρών από τη στιγμή που λαμβάνουν γνώση. Σε περίπτωση που δεν επιτευχθεί ο στόχος των 72 ωρών, πρέπει να δοθούν λόγοι για την καθυστέρηση.

Όταν ένα περιστατικό αφορά δεδομένα προσωπικού χαρακτήρα, πρέπει να ληφθεί απόφαση σχετικά με την έκταση, το χρονοδιάγραμμα και το περιεχόμενο της επικοινωνίας με τα πρόσωπα στα οποία αναφέρονται τα δεδομένα. Ο ΓΚΠΔ απαιτεί η επικοινωνία να πραγματοποιείται «χωρίς αδικαιολόγητη καθυστέρηση» εάν η παραβίαση ενδέχεται να οδηγήσει σε «υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων».

Εφόσον διαπιστωθεί ότι έχει συμβεί παραβίαση προσωπικών δεδομένων, υπάρχουν δύο εμπλεκόμενα μέρη που πρέπει να λάβουν άμεσα ενημέρωση σύμφωνα με τον ΓΚΠΔ δηλαδή η αρμόδια εποπτική αρχή και τα υποκείμενα των δεδομένων που επηρεάστηκαν.

Η κοινοποίηση θα πρέπει να παρέχεται με τα κατάλληλα ασφαλή μέσα και να περιλαμβάνει τις παρακάτω πληροφορίες:

1. Η φύση της παραβίασης προσωπικών δεδομένων, συμπεριλαμβάνοντας τις κατηγορίες και κατά προσέγγιση αριθμό υποκειμένων τα οποία αφορά η παραβίαση και τις κατηγορίες και κατά προσέγγιση αριθμό αρχείων προσωπικών δεδομένων τα οποία αφορά

2. Όνομα και στοιχεία επικοινωνίας του υπεύθυνου προστασίας δεδομένων ή άλλο σημείο επαφής όπου μπορούν να αποκτηθούν περισσότερες πληροφορίες

3. Περιγραφή των πιθανών συνεπειών της παραβίασης προσωπικών δεδομένων

4. Περιγραφή των μέτρων που ελήφθησαν ή προτείνονται να ληφθούν για την αντιμετώπιση της παραβίασης των προσωπικών δεδομένων, συμπεριλαμβανομένων ενδεχομένως μέτρων για τον μετριασμό των πιθανών δυσμενών επιπτώσεών της και

5. Εάν η ειδοποίηση δεν εμπίπτει στο πλαίσιο των 72 ωρών, οι λόγοι για τους οποίους δεν υποβλήθηκε νωρίτερα

Απαιτείται γραπτή επιβεβαίωση από την Αρμόδια εποπτική αρχή ότι έχει παραληφθεί η κοινοποίηση παραβίασης προσωπικών δεδομένων, συμπεριλαμβανομένης της ημερομηνίας και της ώρας κατά την οποία ελήφθη η ειδοποίηση. Όπου είναι απαραίτητο, ο ΓΚΠΔ επιτρέπει την παροχή των πληροφοριών σε φάσεις χωρίς αδικαιολόγητη περαιτέρω καθυστέρηση.

Δεν συνάγεται εκ των προτέρων ότι η παραβίαση πρέπει να γνωστοποιηθεί. Αυτό εξαρτάται από την εκτίμηση του κινδύνου, αν δηλαδή η παραβίαση επηρεάζει «τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων» (Άρθρο 33 του ΓΚΠΔ).

Σε σχέση με τα Φυσικά Πρόσωπα ο ΓΚΠΔ αναφέρει ότι η παραβίαση προσωπικών δεδομένων πρέπει να κοινοποιείται στο υποκείμενο των δεδομένων "όταν η παραβίαση των προσωπικών δεδομένων είναι πιθανό να οδηγήσει σε υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων" (Άρθρο 34 του ΓΚΠΔ).

Η εκτίμηση κινδύνου που θα πρέπει να έχει διεξήχθη νωρίτερα θα έχει καθορίσει κατά πόσον ο κίνδυνος για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων είναι επαρκής ώστε να δικαιολογείται η κοινοποίησή τους. Ωστόσο, αν έχουν ληφθεί μεταγενέστερα μέτρα για τον μετριασμό του υψηλού κινδύνου για τα υποκείμενα των δεδομένων, έτσι ώστε να μην είναι πλέον πιθανό να συμβεί, τότε η επικοινωνία με τα υποκείμενα των δεδομένων δεν απαιτείται από τον ΓΚΠΔ.

Η κοινοποίηση στα επηρεαζόμενα υποκείμενα των δεδομένων δεν είναι επίσης επιτακτική από τον ΓΚΠΔ όπου «θα συνεπαγόταν δυσανάλογη προσπάθεια» (Άρθρο 34 του ΓΚΠΔ). Ωστόσο, σε αυτή την περίπτωση θα πρέπει να χρησιμοποιηθεί μια μορφή δημόσιας επικοινωνίας. Και πάλι, αυτό μπορεί να αλλάξει με βάση τις οδηγίες από την εποπτική αρχή.

Μόλις καθοριστεί ότι η παραβίαση δικαιολογεί την επικοινωνία με τα επηρεαζόμενα υποκείμενα δεδομένων, ο ΓΚΠΔ απαιτεί αυτό να γίνει χωρίς αδικαιολόγητη καθυστέρηση. Η ανακοίνωση στα επηρεαζόμενα υποκείμενα δεδομένων «περιγράφει με σαφήνεια τη φύση της παραβίασης των προσωπικών δεδομένων» (Άρθρο 34 του ΓΚΠΔ) και πρέπει επίσης να καλύπτει:

1. Όνομα και στοιχεία επικοινωνίας του υπεύθυνου προστασίας δεδομένων ή άλλου σημείου επαφής όπου μπορούν να αποκτηθούν περισσότερες πληροφορίες.

2. Περιγραφή των πιθανών συνεπειών της παραβίασης προσωπικών δεδομένων

3. Περιγραφή των μέτρων που ελήφθησαν ή προτείνεται να ληφθούν για την αντιμετώπιση της παραβίασης των προσωπικών δεδομένων, συμπεριλαμβανομένων, κατά περίπτωση, μέτρων για τον μετριασμό των πιθανών δυσμενών επιπτώσεών της

Πέραν των σημείων που απαιτούνται από τον ΓΚΠΔ, μπορεί να είναι σκόπιμο να παρέχονται συμβουλές στο υποκείμενο των δεδομένων σχετικά με τις ενέργειες που μπορεί να αναλάβει προκειμένου να μειώσει τους κινδύνους που συνδέονται με την παραβίαση των προσωπικών δεδομένων. Στις περισσότερες περιπτώσεις, θα ήταν σκόπιμο να ειδοποιηθούν τα επηρεαζόμενα υποκείμενα δεδομένων μέσω επιστολής ή ηλεκτρονικού ταχυδρομείου ή και των δύο, προκειμένου να διασφαλιστεί ότι το μήνυμα έχει ληφθεί και ότι έχουν την ευκαιρία να λάβουν τα απαιτούμενα μέτρα.

Ε. Κεφάλαιο 5 GDPR → Πολιτική Ασφαλείας Πληροφοριών

Μία από τις βασικές υποχρεώσεις για όλες τις επιχειρήσεις, ενεργώντας είτε ως Υπεύθυνοι είτε ως εκτελούντες, είναι η ασφάλεια της επεξεργασίας δεδομένων προσωπικού χαρακτήρα (Κεφάλαιο ΙΙ – Αρχές και Κεφάλαιο V-άρθρο 32).

Μολονότι η ασφάλεια των δεδομένων προσωπικού χαρακτήρα έχει ήδη αποτελέσει νομική υποχρέωση βάσει της οδηγίας για την προστασία των δεδομένων, ο Γ.Κ.Π.Δ. ενισχύει τις σχετικές διατάξεις (τόσο στην ουσία όσο και στο πλαίσιο), επεκτείνοντας ταυτόχρονα την ευθύνη αυτή άμεσα και στους εκτελούντες την επεξεργασία..

Ο κίνδυνος μη συμμόρφωσης με τη νομοθεσία για την προστασία δεδομένων πρέπει να αξιολογείται και να διαχειρίζεται ως μέρος του προγράμματος διαχείρισης κινδύνου. Οι συνέπειες της μη συμμόρφωσης με το νόμο ενδέχεται να περιλαμβάνουν βαριά πρόστιμα, οπότε αυτό πρέπει να αποτελεί βασικό πεδίο εστίασης για τον οργανισμό.

Σύμφωνα με τις προαναφερθείσες διατάξεις, ο Γ.Κ.Π.Δ. καλύπτει εξίσου την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα και θα πρέπει να εξετάζεται μετά από μια προσέγγιση βασισμένη στον κίνδυνο: όσο υψηλότερος είναι ο κίνδυνος (για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων), τόσο περισσότερο αυστηρά τα μέτρα που πρέπει να λάβει ο υπεύθυνος ή ο εκτελών την επεξεργασία (για τη διαχείριση του κινδύνου). Επιπλέον, η ασφάλεια της επεξεργασίας θα πρέπει να θεωρείται το πλαίσιο λογοδοσίας για την προστασία των δεδομένων, το οποίο βασίζεται επίσης στον κίνδυνο και στον αντίκτυπο αυτού και στοχεύει στην προσαρμογή στο συγκεκριμένο επιχειρησιακό πλαίσιο και τις πρακτικές ενός οργανισμού.

Αντικείμενο προστασίας μιας τέτοιας πολιτικής είναι οποιοδήποτε έγγραφο εμπεριέχει προσωπικά Δεδομένα και ιδιοκτήτης του είναι ο Εκπαιδευτικός Οργανισμός συμπεριλαμβανομένων καθώς και το σύνολο των εγκαταστάσεων. Αναλυτικά:

- το κεντρικό κτίριο στο οποίο στεγάζεται,
- η ιστοσελίδα και οι μεταπληροφορίες που συλλέγει,
- το σύνολο των πληροφορικών συστημάτων στο οποίο περιλαμβάνονται:
    - οι σταθεροί υπολογιστές
    - φορητοί υπολογιστές
    - το λογισμικό
    - οι διακομιστές (servers)
    - η κάμερα και το καταγραφικό αυτής
    - οι συσκευές για την υλοποίηση δικτύου (καλωδίωση, switch, modem, router κλπ.)
    - υπηρεσίες cloud

- το σύνολο του έγχαρτου αρχείου
- τα tablet που έχουν στην κατοχή τους οι εκπαιδευτικοί
- συσκευές ανίχνευσης τοποθεσίας οχημάτων

Η πολιτική ισχύει για όλους τους υπαλλήλους του Εκπαιδευτικού Οργανισμού. Εφαρμόζεται επίσης στους εξωτερικούς συνεργάτες, τους υπεργολάβους και τους επισκέπτες, οι οποίοι δεν απασχολούνται στον Εκπαιδευτικό Οργανισμό , αλλά συνεργάζονται με αυτόν ή έχουν πρόσβαση σε πληροφορίες υπαλλήλων, προμηθευτών ή οποιοδήποτε άλλου υποκειμένου τις πληροφορίες φέρει και επεξεργάζεται νομίμως ο Εκπαιδευτικός Οργανισμός (π.χ. εργολάβοι συντήρησης υπολογιστών) και σε οποιεσδήποτε εξωτερικά φιλοξενούμενες υπολογιστικές συσκευές (site & mail hosting, υπηρεσίες cloud).

Ο Εκπαιδευτικός Οργανισμός μεριμνά έτσι ώστε να θεσπίζονται κατάλληλες συμβάσεις και ρήτρες εμπιστευτικότητας με τους υπαλλήλους, τα μέλη ΔΣ και με του εξωτερικούς συνεργάτες πριν αποκτήσουν πρόσβαση σε οποιοδήποτε προσωπικό δεδομένο σε οποιαδήποτε μορφή.

Κανένα τρίτο μέρος δεν επιτρέπεται να έχει πρόσβαση σε προσωπικά δεδομένα που διατηρεί ο Εκπαιδευτικός Οργανισμός χωρίς να έχει προσχωρήσει πρώτα σε σύμβαση εμπιστευτικότητας για τα προσωπικά δεδομένα και η οποία επιβάλλει στο τρίτο μέρος υποχρεώσεις όχι λιγότερο επαχθείς από αυτές με τις οποίες δεσμεύεται ο Εκπαιδευτικός Οργανισμός ως υπεύθυνος επεξεργασίας.

Ο υπεύθυνος του εκάστοτε τμήματος του Εκπαιδευτικού Οργανισμού είναι υπεύθυνος για την διασφάλιση του διαμοιρασμού της πολιτικής αυτής καθώς και της πλήρους κατανόησης από όλο το προσωπικό.

Εάν διαπιστωθεί ότι ένας χρήστης/υπάλληλος παραβίασε την παρούσα πολιτική, ενδέχεται να υπόκειται στη διαδικασία αξιολόγησης και να υποστεί τις εκάστοτε συνέπιες. Σοβαρές παραβιάσεις της παρούσας πολιτικής θα μπορούσαν να θεωρηθούν ως σοβαρό παράπτωμα.

Κάθε επεξεργασία προσωπικών δεδομένων θα πρέπει να διενεργείται σύμφωνα με τις αρχές προστασίας των δεδομένων όπως ορίζονται στο Άρθρο 5 του ΓΚΠΔ. Οι πολιτικές και οι διαδικασίες του εκπαιδευτικού οργανισμού θα πρέπει να είναι σχεδιασμένες για να διασφαλίζουν τη συμμόρφωση με τις εν λόγω αρχές. Εξάλλου η ασφάλεια των προσωπικών δεδομένων αποτελεί πρωταρχική προτεραιότητα προκειμένου τα δεδομένα προσωπικού χαρακτήρα:

- να υποβάλλονται μόνο σε θεμιτή και νόμιμη επεξεργασία.
- να υπόκεινται σε επεξεργασία μόνο για έναν ή περισσότερους συγκεκριμένους και νόμιμους σκοπούς και να μην υποβάλλονται σε περαιτέρω επεξεργασία με οποιονδήποτε τρόπο ασυμβίβαστο προς τον σκοπό ή τους σκοπούς αυτούς.

- να είναι επαρκή, συναφή και όχι υπερβολικά σε σχέση με το σκοπό ή τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία.
- να είναι ακριβή και, όπου χρειάζεται, να ενημερώνονται.
- να μην υποβάλλονται σε επεξεργασία για οποιονδήποτε σκοπό ή σκοπούς και να μην φυλάσσονται για περισσότερο από το χρονικό διάστημα που είναι απαραίτητο για το σκοπό αυτό ή για τους σκοπούς αυτούς.
- να υποβάλλονται σε επεξεργασία σύμφωνα με τα δικαιώματα των προσώπων στα οποία αναφέρονται τα δεδομένα βάσει νόμου.
- να προστατεύονται με την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων κατά της μη εξουσιοδοτημένης ή παράνομης επεξεργασίας τους καθώς και κατά της τυχαίας απώλειας, καταστροφής ή ζημίας.
- να μη μεταφέρονται σε χώρα ή έδαφος εκτός της Ε.Ε, εκτός εάν εξασφαλίζεται επαρκές επίπεδο προστασίας των δικαιωμάτων και ελευθεριών των υποκειμένων των δεδομένων σε σχέση με την επεξεργασία σύμφωνα με τις ειδικές προϋποθέσεις που ορίζονται στον ΓΚΠΔ.

Ο εκπαιδευτικός Οργανισμός θα πρέπει να επιδείξει συμμόρφωση με τις αρχές προστασίας των προσωπικών δεδομένων εφαρμόζοντας πολιτικές για την προστασία των προσωπικών δεδομένων, τηρώντας τον ισχύοντα κώδικα δεοντολογίας, εφαρμόζοντας τεχνικά και οργανωτικά μέτρα, καθώς και θεσπίζοντας τεχνικές όπως η προστασία δεδομένων ήδη από τον σχεδιασμό, DPIAs, διαδικασίες για τη γνωστοποίηση παραβίασης προσωπικών δεδομένων και σχέδια παρέμβασης στα συμβάντα.

Μια τέτοια πολιτική θα πρέπει να ορίζει τα είδη προσωπικών δεδομένων που συλλέγει και επεξεργάζεται, όπως:

- στοιχεία επικοινωνίας, όπως ονοματεπώνυμο, διεύθυνση ηλεκτρονικού ταχυδρομείου, ταχυδρομική διεύθυνση οικείας, αριθμό τηλεφώνου και αριθμό κινητού τηλεφώνου, όνομα συζύγου, επάγγελμα συζύγου, αριθμός τέκνων, φωτογραφία, φύλο, ημερομηνία και τόπος γέννησης, αριθμός διαβατηρίου, ΑΔΤ, ημερομηνία εγγραφής, ημερομηνία απόφασης ΔΣ, κ.α.
- προσωπικές πληροφορίες πάσης φύσεως όπως συμβάσεις, υπεύθυνες δηλώσεις, πιστοποιητικά και άλλα δημόσια έγγραφα κ.α
- φορολογικά στοιχεία
- στοιχεία ασφάλισης όπως ΑΜΑ κ.α.
- μορφή επικοινωνίας που στέλνει εκούσια το υποκείμενο σε οποιαδήποτε μορφή όπως email, αλληλογραφία, fax, φόρμα επικοινωνίας ιστοσελίδας κ.α.

- στο πλαίσιο λειτουργίας της ιστοσελίδας του αν χρησιμοποιεί τεχνολογίες cookies που συλλέγουν δεδομένα με σκοπό την εύρυθμη και ταχεία λειτουργία της.

- Τέλος, ο εκπαιδευτικός οργανισμός ενδέχεται να παρακρατεί, σε ορισμένες περιπτώσεις, κάποιους τύπους προσωπικών δεδομένων, σύμφωνα με τις κατά περίπτωση ισχύουσες νομοθετικές απαιτήσεις.

Ακόμα, θα πρέπει να ορίζει την ακριβή διάρκεια που διατηρεί τα προσωπικά δεδομένα σύμφωνα με τον ΓΚΠΔ μόνο για όσο χρονικό διάστημα είναι απαραίτητο για τον σκοπό για τον οποίο συλλέχθηκαν, σύμφωνα με τις αρχές ελαχιστοποίησης των δεδομένων και περιορισμού της περιόδου αποθήκευσης ή εάν και εφόσον κάτι τέτοιο επιτρέπεται από το νόμο.

Η διάρκεια διατήρησης των δεδομένων σχετίζεται άμεσα με το χρονικό διάστημα της υποχρέωσής του εκπαιδευτικού Οργανισμού ως Ν.Π.Δ.Δ. ή ως εργοδότης να τηρεί τα δεδομένα προσωπικού χαρακτήρα.

Μετά το πέρας της ισχύος της έννομης διατήρησης των προσωπικών δεδομένων, το εκάστοτε υποκείμενο μπορεί να ζητήσει υπό προϋποθέσεις την επιστροφή του πλήρη φακέλου του καθώς και τη διαγραφή των δεδομένων του από την αποθήκευσή τους, σε ηλεκτρονικό υπολογιστή ή εξωτερικό δίσκο ή κάθε μέρους αποθήκευσης. Εάν δεν παραλάβει το φάκελό του σε αυτή την περίπτωση ο εκπαιδευτικός οργανισμός διατηρεί δικαίωμα καταστροφής του. Εντούτοις, σε ορισμένες περιπτώσεις, συγκεκριμένες προσωπικές πληροφορίες μπορεί να διατηρηθούν πέραν αυτού του χρονικού διαστήματος λόγω πιθανών νομικών υποχρεώσεων, έννομων συμφερόντων (π.χ έννομης υποχρέωσης, οικονομικής εκκρεμότητας κ.λπ.)

Τέλος, στην παρούσα πολιτική θα πρέπει να γίνει ρητή και αναλυτική αναφορά για τα παρακάτω θέματα, όπως η Ασφάλεια Τεχνολογιών Πληροφοριών & Εφαρμογών, η Διασυνοριακή ροή δεδομένων, τα Δικαιώματα υποκειμένων και τις περιπτώσεις Αναθεώρησης της ίδιας της πολιτικής ασφαλείας.

F. Κεφάλαιο 9 GDPR → Διαδικασία Προστασίας Δεδομένων Εργαζομένων

Ένας εκπαιδευτικός οργανισμός διατηρεί και προσωπικά δεδομένα των ίδιων των εργαζομένων του. Οπότε στο πλαίσιο της παραπάνω διαδικασίας θα πρέπει να λαμβάνεται μέριμνα και για τα προσωπικά δεδομένων των εργαζομένων. Έτσι, ο Εκπαιδευτικός Οργανισμός θα πρέπει να διαθέτει σχετική διαδικασία που να περιλαμβάνει ποια δεδομένα των εργαζομένων του διατηρεί, όπως:

- Στοιχεία που ταυτοποιούν τον Εργαζόμενο [όνομα, επώνυμο, όνομα και επώνυμο γονέων, ημερομηνία και τόπος γέννησης, φύλο, υπηκοότητα, ταυτότητα ή διαβατήριο ή άδεια διαμονής, αριθμός εγγράφου και εκδούσα αρχή, άδεια εργασίας, Επαγγελματικά στοιχεία (θέση, ρόλος),

υπογραφή]. Όταν ο Εργαζόμενος διορίζεται ως αρμόδιος για να εκπροσωπεί τον Οργανισμό ενώπιον αρχών, οργανισμών ή πιστωτικών ιδρυμάτων, συλλέγονται επιπλέον προσωπικά του στοιχεία (έγγραφα φορολογικών αρχών, αποδεικτικά διεύθυνσης οικίας, έγγραφα που πιστοποιούν την επαγγελματική εξειδίκευση του Εργαζομένου, πιστοποιήσεις, αντίγραφο ποινικού μητρώου)

- Στοιχεία επικοινωνίας (διεύθυνση, τηλέφωνο, email)

- Στοιχεία που είναι απαραίτητα για την εκπλήρωση υποχρεώσεων του Εκπαιδευτικού Οργανισμού ενώπιον φορολογικών αρχών, ταμείων κοινωνικής ασφάλισης και φορέων για την προστασία και τις παροχές σε εργαζόμενους και ανέργους (αριθμός φορολογικού μητρώου, αριθμός μητρώου κοινωνικής ασφάλισης, αριθμός μητρώου άλλων εθνικών αρχών και οργανισμών)

- Πληροφορίες σχετικά με την οικογενειακή κατάσταση του εργαζομένου (έγγαμος/άγαμος, όνομα και επώνυμο συζύγου, αριθμός τέκνων)

-Πληροφορίες απαραίτητες για την καταβολή των αποδοχών του εργαζομένου (τραπεζικός λογαριασμός, αριθμός ημερών και ωρών εργασίας/άδειας, λόγοι άδειας, ιατρικές βεβαιώσεις όταν πρόκειται για άδεια ασθενείας, εγκυμοσύνης ή λοχείας)

-Πληροφορίες σχετικά με την εκπαίδευση και την επαγγελματική εμπειρία του εργαζομένου (π.χ. προηγούμενη εργασιακή εμπειρία, έτη προϋπηρεσίας, ακαδημαϊκοί τίτλοι, πιστοποιήσεις, σεμινάρια, γνώση ξένων γλωσσών, γνώση προγραμμάτων Η/Υ)

- Στοιχεία ηλεκτρονικής ταυτοποίησης [email, ονόματα χρήστη σε λογαριασμούς, πληροφορίες χρόνου/διάρκειας σύνδεσης σε λογαριασμούς,

- Στοιχεία σχετικά με επαγγελματικά έξοδα των Εργαζομένων (επαγγελματικό κινητό τηλέφωνο, αριθμός πινακίδας επαγγελματικού αυτοκινήτου, όνομα τρίτου οδηγού επαγγελματικού οχήματος, δίπλωμα οδήγησης, επαγγελματικά έξοδα μεταφοράς/μετακίνησης, διαμονής, κτλ.)

- Στοιχεία σχετικά με την διαχείριση ανθρώπινου δυναμικού (αξιολόγηση απόδοσης, επίτευξη στόχων κλπ).

Επίσης, θα πρέπει να υπάρχει ρητή αποτύπωση των σκοπών επεξεργασίας των δεδομένων των εργαζομένων, όπως:

- Για να ολοκληρωθεί η διαδικασία πρόσληψης ανθρώπινου δυναμικού και για να κριθεί εάν συγκεκριμένος Εργαζόμενος είναι ικανός για συγκεκριμένη θέση εργασίας ή συγκεκριμένα καθήκοντα

- Για να εκτελεστούν οι υποχρεώσεις που προκύπτουν από τη σύμβαση εργασίας ή από τον νόμο, όπως η καταβολή μισθού, η παροχή ημερών αδείας, η παροχή επιδομάτων, η εξασφάλιση της υγείας και της ασφάλειας των εργαζομένων, η παροχή ωφελημάτων που προβλέπονται στη σύμβαση

εργασίας, η υποχρεωτική γνωστοποίηση των στοιχείων των εργαζομένων σε φορολογικές αρχές, οργανισμούς κοινωνικής ασφάλισης, οργανισμούς προστασίας εργαζομένων, κανονιστικές αρχές που ελέγχουν και ρυθμίζουν τη λειτουργία της Οντότητας.

- Για τη διαχείριση του ανθρώπινου δυναμικού, όπως τη διαχείριση των καθηκόντων κάθε θέσης, την αξιολόγηση της απόδοσης κατά την εργασία, το κόστος μισθών και παροχών, τη συμμετοχή των Εργαζομένων σε προγράμματα ομαδικής ασφάλισης ή τη συμμετοχή σε εκδηλώσεις που οργανώνουμε για τους Εργαζόμενους

- Για την διαχείριση των επαγγελματικών εξόδων του εκπαιδευτικού Οργανισμού, όπως τα έξοδα που σχετίζονται με επαγγελματικά ταξίδια, τη χρήση επαγγελματικών κινητών τηλεφώνων, τη χρήση επαγγελματικών οχημάτων, τα έξοδα μετακίνησης.

- Για την οργάνωση και εκτέλεση των εργασιών του εκπαιδευτικού Οργανισμού, όπως τη διενέργεια πληρωμών, τη διαχείριση των σχέσεων μας με πελάτες και μετόχους, πιθανούς ή μελλοντικούς

- Για την ασφάλεια των εργαζομένων και την ασφάλεια κρίσιμων εγκαταστάσεων του εκπαιδευτικού Οργανισμού.

- Για την παροχή εκπαίδευσης και ενημέρωσης

- Για την διαχείριση και την ασφάλεια των ηλεκτρονικών υποδομών του εκπαιδευτικού Οργανισμού και την αδιάλειπτη λειτουργία της

- Για σκοπούς ελέγχου των διαδικασιών του εκπαιδευτικού Οργανισμού από αρχές και τρίτα μέρη ή/και την εξασφάλιση πιστοποιήσεων

- Για να απαντηθούν επίσημα αιτήματα των αρχών και των Δημοσίων Φορέων

Εκτός των παραπάνω, θα πρέπει να γίνεται αναφορά στο ποιοι έχουν πρόσβαση και ποιοι επεξεργάζονται αυτά τα δεδομένα, καθώς και το διάστημα που αυτά διατηρούνται.

Τέλος, στο πλαίσιο μια τέτοιας διαδικασίας θα πρέπει να είναι εύκολα κατανοητά τα δικαιώματα των εργαζομένων σχετικά με τα προσωπικά τους δεδομένα. Προτείνεται η χρήση του παρακάτω πίνακα, σχετικά με τα δικαιώματα των εργαζομένων:

Έχετε τα παρακάτω δικαιώματα σχετικά με τα προσωπικά σας δεδομένα Δικαίωμα ενημέρωσης	
Δικαίωμα ενημέρωσης	Έχετε το δικαίωμα να ενημερώνεστε για τη συλλογή και χρήση των προσωπικών σας δεδομένων

Δικαίωμα πρόσβασης	Έχετε το δικαίωμα να λαμβάνετε από τον Εκπαιδευτικό Οργανισμό, επιβεβαίωση για το κατά πόσον ή όχι τα δεδομένα προσωπικού χαρακτήρα που σας αφορούν υφίστανται επεξεργασία και, εάν συμβαίνει τούτο, έχετε το δικαίωμα πρόσβασης στα δεδομένα προσωπικού χαρακτήρα σε σύντομη, κατανοητή, διαφανή και εύκολα προσβάσιμη μορφή.
Δικαίωμα διόρθωσης	Μπορείτε να ζητήσετε από τον Εκπαιδευτικό Οργανισμό ότι θα διασφαλίσει χωρίς αδικαιολόγητη καθυστέρηση ότι θα προβεί στη διόρθωση ανακριβών ή ελλιπών Προσωπικών Δεδομένων, μεταξύ άλλων μέσω συμπληρωματικής δήλωσης.
Δικαίωμα διαγραφής	Έχετε το δικαίωμα να ζητήσετε από τον Εκπαιδευτικό Οργανισμό τη διαγραφή των Προσωπικών Δεδομένων που σας αφορούν, χωρίς αδικαιολόγητη καθυστέρηση και ο Εκπαιδευτικός Οργανισμός υποχρεούται να προβεί στη διαγραφή, υπό τις προϋποθέσεις που ορίζει ο ΓΚΠΔ.
Δικαίωμα περιορισμού της επεξεργασίας	Έχετε το δικαίωμα να ζητήσετε από τον Εκπαιδευτικό Οργανισμό να περιορίσει τις δραστηριότητες επεξεργασίας μόνο σε συγκεκριμένους σκοπούς, υπό τις προϋποθέσεις που ορίζει ο νόμος.
Δικαίωμα εναντίωσης	Δικαιούστε να αντιτάσσεστε, ανά πάσα στιγμή και για λόγους που σχετίζονται με την ιδιαίτερη κατάστασή σας, στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που σας αφορούν. Ο Εκπαιδευτικός Οργανισμός δεν θα υποβάλλει πλέον τα δεδομένα προσωπικού χαρακτήρα σε επεξεργασία, εκτός εάν καταδείξει επιτακτικούς και νόμιμους λόγους για την επεξεργασία οι οποίοι υπερισχύουν των συμφερόντων, των δικαιωμάτων και των ελευθεριών σας ή για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων.
Δικαίωμα στη φορητότητα των δεδομένων	Έχετε το δικαίωμα να λαμβάνετε τα δεδομένα προσωπικού χαρακτήρα που σας αφορούν, και τα οποία έχει παράσχει ο Εκπαιδευτικός Οργανισμός, σε δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα μορφότυπο, καθώς και το δικαίωμα να ζητάτε τη διαβίβαση των λόγω

	δεδομένων σε άλλον υπεύθυνο επεξεργασίας χωρίς αντίρρηση από τον Εκπαιδευτικό Οργανισμό υπό τις προϋποθέσεις που ορίζει ο ΓΚΠΔ.
Δικαίωμα απόκτησης ανθρώπινης παρέμβασης	Έχετε το δικαίωμα να μην υπόκεισθε σε απόφαση που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας, συμπεριλαμβανομένης της κατάρτισης προφίλ, η οποία παράγει έννομα αποτελέσματα που σας αφορούν ή σας επηρεάζουν σημαντικά με παρόμοιο τρόπο.

Εκτός από τις παραπάνω ενδεικτικές πολιτικές και διαδικασίες, ο Εκπαιδευτικός Οργανισμός θα πρέπει να προσαρμόσει και τα αντίστοιχα έντυπα που χρησιμοποιεί, ώστε να είναι συμβατά τόσο με τα όσα περιγράφονται στις εν λόγω πολιτικές και διαδικασίες, όσο και με τα όσα απαιτούνται από τον Κανονισμό για να αποτελούν τεκμήριο συμμόρφωσης με τον Κανονισμό. Η διαδικασία αυτή απαιτεί εκτός από γνώση των διαδικασιών και λειτουργιών του οργανισμού και νομικές γνώσεις. Χαρακτηριστικό παράδειγμα αποτελεί η διαδικασία λήψης της συγκατάθεσης, που αναφέρθηκε παραπάνω. Πώς ένας οργανισμός θα μπορεί να τεκμηριώσει ότι έχει λάβει την συγκατάθεση του Φυσικού Προσώπου σχετικά με την επεξεργασία των προσωπικών του Δεδομένων?

Ας πάρουμε ως δεδομένο, για λόγους κατανόησης, ότι κάθε δυνητικός μαθητής/σπουδαστής/καταρτιζόμενος συμπληρώνει μια σχετική αίτηση. Η αίτηση αυτή περιέχει μεταξύ άλλων και προσωπικά δεδομένα, όπως αναφέρθηκε παραπάνω. Δεν χρειάζεται να δημιουργηθεί ένα νέο έντυπο που να δηλώνει τη συγκατάθεση του υποψήφιου. Μπορεί στην υπάρχουσα αίτηση, να προστεθεί ένα κείμενο σαν το παρακάτω: «*Με την υπογραφή της παρούσας δηλώνω ότι παρέχω ρητώς τη συγκατάθεσή μου για την επεξεργασία των παραπάνω δεδομένων προσωπικού χαρακτήρα και ειδικών κατηγοριών δεδομένων που αναφέρονται ή/και συνοδεύουν την παρούσα αίτηση από τον ΕΚΠΑΙΔΕΥΤΙΚΟΣ ΟΡΓΑΝΙΣΜΟΣ που εδρεύει στην Αθήνα, οδός ΣΥΝΤΑΓΜΑ, αριθμ. 1 ΑΦΜ 99999999 και εκπροσωπείται νόμιμα, που είναι υπεύθυνος επεξεργασίας κατά το νόμο (Γενικός Κανονισμός ΕΕ 2016/679). Δηλώνω επίσης ότι ενημερώθηκα πλήρως για τα κάτωθι: Η επεξεργασία των εν λόγω δεδομένων είναι απαραίτητη για τους σκοπούς των εννόμων συμφερόντων που επιδιώκει ο υπεύθυνος προστασίας όπως είναι η απόδειξη της ύπαρξης ή της μη ύπαρξης αστικής ή ποινικής του ευθύνης ή/και η διασφάλιση καλής οργάνωσης των λειτουργιών του. Τα δεδομένα αυτά θα χρησιμοποιηθούν για την προώθηση και ολοκλήρωση των διαδικασιών εγγραφής μου στο ΕΚΠΑΙΔΕΥΤΙΚΟΣ ΟΡΓΑΝΙΣΜΟΣ καθώς και για τη σύναψη μελλοντικής σύμβασης μεταξύ μας και*

ενδέχεται για τους σκοπούς αυτούς τα δεδομένα μου να τύχουν επεξεργασίας από Συνεργαζόμενους φορείς του Εξωτερικού, να κοινοποιηθούν σε Δημόσιες Υπηρεσίες, συνεργάτες καθώς και άλλες εταιρίες του Ομίλου λόγω κοινών λειτουργικών τους μονάδων. Τα δεδομένα αυτά διατηρούνται για διάστημα δέκα ετών. Η νομιμότητα της επεξεργασίας βασίζεται μεταξύ άλλων στα άρθρα 6§1α , 6§1β, 6§1στ και 9§2α του Κανονισμού (ΕΕ) 2016/679. Έλαβα γνώση ότι η παροχή δεδομένων είναι απαραίτητη κατά το προσυμβατικό στάδιο και ότι αν δεν τα παρέχω η σύμβαση εν τέλει δεν θα καταρτιστεί και δεν θα είναι δυνατή η ολοκλήρωση των απαραίτητων διαδικασιών για την αίτηση εγγραφής μου στο ΕΚΠΑΙΔΕΥΤΙΚΟΣ ΟΡΓΑΝΙΣΜΟΣ. Επιπροσθέτως έλαβα γνώση του δικαιώματος υποβολής αιτήματος στον υπεύθυνο επεξεργασίας για την άσκηση των δικαιωμάτων μου ως υποκειμένου: δικαίωμα πρόσβασης και διόρθωσης ή διαγραφής ή περιορισμού της επεξεργασίας των δεδομένων που με αφορούν, το δικαίωμα αντίταξης στην επεξεργασία καθώς και το δικαίωμα στη φορητότητα. Τα δικαιώματα αυτά ασκούνται είτε με την αποστολή επιστολής στη διεύθυνση ΣΥΝΤΑΓΜΑ, Αθήνα, είτε με ηλεκτρονικό μήνυμα στη διεύθυνση: info@ΕΚΠΑΙΔΕΥΤΙΚΟΣ.ΟΡΓΑΝΙΣΜΟΣ.gr. Επίσης, έλαβα γνώση ότι για τυχόν καταγγελία έχω το δικαίωμα να απευθυνθώ στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Δνση: Κηφισίας 1-3, Τ.Κ. 115 23, Αθήνα) είτε σε ηλεκτρονική μορφή μέσω του ιστότοπου: www.dpa.gr.»

Η προσαρμογή του ήδη υπάρχοντος εντύπου με ένα κείμενο τέτοιου είδους, θα επιτρέψει στον Εκπαιδευτικό Οργανισμό να τεκμηριώσει ότι έχει λάβει τη συγκατάθεση του Φυσικού Προσώπου, σύμφωνα με τα όσα ορίζει ο GDPR. Αντίστοιχη διαδικασία, με την συνδρομή ατόμου που έχει και νομικές γνώσεις, θα πρέπει να γίνει για όλα τα σημεία και έντυπα που διαθέτει και εφαρμόζει ο Εκπαιδευτικός Οργανισμός.

Κεφάλαιο 7
Συμπεράσματα

Ανακεφαλαιώνοντας, με τη συνεχή συλλογή Προσωπικών Δεδομένων που πραγματοποιείται για την υποστήριξη των επιχειρησιακών λειτουργιών των επιχειρήσεων και οργανισμών, παρατηρείται ένας αυξανόμενος κίνδυνος για την προστασία της ιδιωτικότητας των πολιτών σε σχέση με τα Προσωπικά τους Δεδομένα. Η Ευρωπαϊκή Επιτροπή, έχοντας εντοπίσει τον παραπάνω κίνδυνο, προχώρησε σε μια πρώτη προσπάθεια δημιουργίας ενός κοινού πλαισίου προστασίας των πολιτών της σε σχέση με τα Προσωπικά τους Δεδομένα, μέσω της δημοσίευσης του Κανονισμού 2016/679 του Ευρωπαϊκού Κοινοβουλίου, που είναι πλέον ευρύτερα γνωστός ως GDPR. Μέσα στον όρο επιχειρήσεις και οργανισμούς, περιλαμβάνονται και όλοι οι εκπαιδευτικοί οργανισμοί, οι οποίοι εκ των πραγμάτων πραγματοποιούν συλλογή και επεξεργασία προσωπικών δεδομένων μεγάλης κλίμακας.

Όπως αναλύθηκε στο πλαίσιο της παρούσας εργασίας, ο GDPR θέτει ένα πολύ συγκεκριμένο μείγμα προαπαιτουμένων που θα πρέπει πλέον να λαμβάνουν υπόψη τους οι οργανισμοί, ώστε να θεωρούνται ότι επεξεργάζονται τα Προσωπικά Δεδομένα που συλλέγουν με γνώμονα την ασφάλεια της ελευθερίας των πολιτών.

Εν προκειμένω, παρουσιάστηκε ο GDPR ως προς τις αλλαγές και τους νεοτερισμούς που εισάγει. Αναλύθηκαν τα δικαιώματα που πλέον έχουν οι πολίτες σε σχέση με τα προσωπικά τους δεδομένα, οι νέοι ρόλοι που θα πρέπει να εντάξουν οι οργανισμοί καθώς και έγινε μια επεξήγηση της βασικής ορολογίας που χρησιμοποιεί η ΕΕ σε σχέση πάντα με τα προσωπικά δεδομένα. Παράλληλα, έγινε μια προσπάθεια σύνοψης των όλων των κεφαλαίων και άρθρων του Κανονισμού, ώστε να μπορεί ο οποιοσδήποτε να αποκτήσει μια περιεκτική άποψη του τι περιλαμβάνει.

Εν συνεχεία παρουσιάστηκε η σύνδεση και η συσχέτιση του GDPR με τα υπάρχοντα συστήματα διαχείρισης ποιότητας. Αναλύθηκε κυρίως η συσχέτιση με το πρότυπο ISO27001 περί ασφάλειας πληροφοριακών συστημάτων, δεδομένου ότι η επεξεργασία στις μέρες μας γίνεται μέσω των πληροφοριακών συστημάτων που χρησιμοποιούν όλοι οι οργανισμοί.

Στη συνέχεια παρουσιάστηκαν τα προτεινόμενα βήματα, σύμφωνα και με τη μελέτη του ΣΕΒ, που θα πρέπει ένας οργανισμός να ακολουθήσει ώστε να γίνει συμβατός με τον GDPR και αναλύθηκαν οι απαιτήσεις των διαδικασιών και πολιτικών που θα πρέπει ο οργανισμός να δημιουργήσει ή να προσαρμόσει, ώστε η συμβατότητα να έχει πρακτική εφαρμογή και τεκμηρίωση.

Μέσα από την έρευνα, παρατηρήθηκε ότι η προσαρμογή ενός εκπαιδευτικού οργανισμού στις απαιτήσεις του GDPR είναι μια πολύ σύνθετη διαδικασία. Απαιτεί την πολύ καλή γνώση θεμάτων νομικής φύσης, θεμάτων που έχουν να κάνουν με τη χρήση πληροφοριακών συστημάτων και φυσικά γνώση της λειτουργίας του κάθε οργανισμού.

Η πιθανή ύπαρξη άλλων συστημάτων ποιότητας που εφαρμόζει ο οργανισμός θα πρέπει να λαμβάνεται υπόψη, ώστε να μην υπάρχουν αλληλοεπικαλύψεις και αντιθέσεις μεταξύ των υπαρχόντων διαδικασιών και των διαδικασιών που θα δημιουργηθούν αποκλειστικά για το GDPR, με σκοπό τη δημιουργία ενός ευέλικτου συστήματος προστασίας προσωπικών δεδομένων. Δεν θα πρέπει να δημιουργηθεί ένα σύστημα το οποίο να αποτελεί τροχοπέδη στις επιχειρησιακές λειτουργίες κατά την εφαρμογή του.

Η σωστή κατανόηση των διατάξεων του Κανονισμού και παράλληλα η γνώση των λειτουργιών του οργανισμού, θα επιτρέψει στον οργανισμό και τα στελέχη του να λειτουργούν απρόσκοπτα, προστατεύοντας παράλληλα και τα προσωπικά δεδομένα που συλλέγουν και επεξεργάζονται.

Η παρούσα εργασία θα μπορούσε να αποτελέσει κίνητρο για επιπλέον έρευνα. Θα μπορούσε να υπάρξει μια μελέτη περίπτωσης ενός συγκεκριμένου εκπαιδευτικού οργανισμού, όπου μέσα από την ανάλυση όλων των επιχειρησιακών λειτουργιών που ήδη διαθέτει και των υπαρχόντων συστημάτων ποιότητας που εφαρμόζει, να δημιουργηθεί ένα εξατομικευμένο πλήρες Σύστημα Διαχείρισης απόλυτα συμβατό τόσο με τον GDPR όσο και με τα υπόλοιπα πρότυπα που εφαρμόζει.

Παραρτήματα Α

ΑΠΑΙΤΗΣΕΙΣ ΣΥΣΤΗΜΑΤΟΣ ΔΙΑΧΕΙΡΙΣΗΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΚΑΤΑ ΤΟ ΠΡΟΤΥΠΟ BS10012:2017

4 Πλαίσιο λειτουργίας του οργανισμού
4.1 Κατανόηση του οργανισμού και του πλαισίου λειτουργίας του
1. Έχει προσδιορίσει ο οργανισμός τυχόν εξωτερικές παραμέτρους που θα μπορούσαν να επηρεάσουν την ικανότητά του να επιτυγχάνει τα επιδιωκόμενα αποτελέσματα του ΣΔΠΔ (PIMS) του;
2. Έχει προσδιορίσει ο οργανισμός τυχόν εσωτερικές παραμέτρους που θα μπορούσαν να επηρεάσουν την ικανότητά του να επιτυγχάνει τα επιδιωκόμενα αποτελέσματα του ΣΔΠΔ (PIMS) του;
4.2 Κατανόηση των αναγκών και των προσδοκιών των ενδιαφερομένων μερών
1. Ο οργανισμός έχει προσδιορίσει:
α) τα ενδιαφερόμενα μέρη που σχετίζονται με το ΣΔΠΔ (PIMS);
β) τις απαιτήσεις των εν λόγω ενδιαφερομένων μερών που σχετίζονται με το ΣΔΠΔ (PIMS);
4.3 Καθορισμός του πεδίου εφαρμογής του συστήματος διαχείρισης πληροφοριών προσωπικού χαρακτήρα
1. Ο οργανισμός έχει καθορίσει τα όρια και τη δυνατότητα εφαρμογής του ΣΔΠΔ (PIMS) ώστε να ορίζει το πεδίο εφαρμογής του;
2. Ο οργανισμός έχει λάβει υπόψη:
α) τις εσωτερικές και εξωτερικές παραμέτρους; (4.1 παραπάνω)
β) τις απαιτήσεις των ενδιαφερομένων μερών; (4.2 παραπάνω)
γ) τους οργανωτικούς στόχους και υποχρεώσεις;
δ) την αποδεκτή στάθμη διακινδύνευσης του οργανισμού;
ε) τις εφαρμοστέες νομοθετικές, κανονιστικές, συμβατικές και/ή επαγγελματικές υποχρεώσεις;
2. Είναι το πεδίο εφαρμογής διαθέσιμο ως τεκμηριωμένη πληροφορία;
4.4 Σύστημα διαχείρισης πληροφοριών προσωπικού χαρακτήρα
1. Ο οργανισμός έχει καθιερώσει, εφαρμόσει, διατηρήσει ενήμερο και συνεχώς βελτιώσει το ΣΔΠΔ (PIMS), σύμφωνα με τις απαιτήσεις του Βρετανικού Προτύπου 10012:2017;
2. Αυτό συμπεριλαμβάνει τις αναγκαίες διεργασίες και τις αλληλεπιδράσεις τους στον οργανισμό;
3. Υπάρχει τυχόν αλληλοεπικάλυψη με άλλα συστήματα;
5 Ηγεσία
5.1 Ηγεσία και δέσμευση
1. Η ανώτατη Διοίκηση έχει ασκήσει τον ηγετικό ρόλο της και καταδεικνύει τη δέσμευσή της σε σχέση με το ΣΔΠΔ (PIMS) μέσω της:
α) καθιέρωσης πολιτικής και στόχων του ΣΔΠΔ (PIMS) που είναι συμβατοί με τον στρατηγικό προσανατολισμό του οργανισμού;
β) ενσωμάτωσης των απαιτήσεων του ΣΔΠΔ (PIMS) στις επιχειρησιακές διεργασίες του οργανισμού;
γ) διασφάλισης ότι οι πόροι που απαιτούνται για το ΣΔΠΔ (PIMS) διατίθενται;
δ) γνωστοποίησης της σημαντικότητας της αποτελεσματικής διαχείρισης των προσωπικών πληροφοριών και της συμμόρφωσης με τις απαιτήσεις του ΣΔΠΔ (PIMS);
ε) διασφάλισης ότι το ΣΔΠΔ (PIMS) επιτυγχάνει τα επιδιωκόμενα αποτελέσματα;

	στ) καθοδήγησης και υποστήριξης του προσωπικού ώστε να συμβάλλει στην αποτελεσματικότητα του ΣΔΠΔ (PIMS);
	ζ) προαγωγής της συνεχούς βελτίωσης;
	η) υποστήριξης των λοιπών διευθυντικών στελεχών του οργανισμού ώστε να αναλαμβάνουν ηγετικό ρόλο στους τομείς ευθύνης τους;
5.2 Πολιτική	
1.	Η ανώτατη Διοίκηση έχει καθιερώσει μια πολιτική ΣΔΠΔ (PIMS), η οποία:
	α) είναι κατάλληλη για τον σκοπό λειτουργίας του οργανισμού;
	β) παρέχει ένα πλαίσιο για τον καθορισμό των στόχων του ΣΔΠΔ (PIMS);
	γ) περιλαμβάνει δέσμευση για την ικανοποίηση των εφαρμοστέων απαιτήσεων;
	δ) περιλαμβάνει δέσμευση για συνεχή βελτίωση του συστήματος διαχείρισης ΣΔΠΔ (PIMS);
2.	Η πολιτική του ΣΔΠΔ (PIMS):
	α) είναι διαθέσιμη ως τεκμηριωμένη πληροφορία;
	β) γνωστοποιείται εντός του οργανισμού;
	γ) είναι στη διάθεση των ενδιαφερόμενων μερών;
3.	Η πολιτική του ΣΔΠΔ (PIMS) αναφέρει τη δέσμευση του οργανισμού να συμμορφώνεται με τις απαιτήσεις για την προστασία δεδομένων και τις ορθές πρακτικές, συμπεριλαμβανομένων:
	α) της επεξεργασίας προσωπικών δεδομένων μόνο όταν αυτό είναι απολύτως απαραίτητο για νομικούς και κανονιστικούς σκοπούς ή για νόμιμους οργανωτικούς σκοπούς;
	β) της επεξεργασίας μόνο των ελάχιστων προσωπικών πληροφοριών που απαιτούνται για αυτούς τους σκοπούς;
	γ) της παροχής σαφών πληροφοριών σε φυσικά πρόσωπα (συμπεριλαμβανομένων παιδιών) σχετικά με τον τρόπο με τον οποίο μπορούν να χρησιμοποιηθούν οι προσωπικές τους πληροφορίες και από ποιον;
	δ) της διασφάλισης ειδικών εγγυήσεων κατά τη συλλογή πληροφοριών απευθείας από παιδιά;
	ε) της επεξεργασίας μόνο συναφών και κατάλληλων προσωπικών πληροφοριών;
	στ) της θεμιτής και σύννομης επεξεργασίας προσωπικών πληροφοριών;
	ζ) της διατήρησης μιας τεκμηριωμένης καταγραφής με τις κατηγορίες των προσωπικών πληροφοριών που επεξεργάζεται ο οργανισμός;
	η) της διατήρησης της ακρίβειας των προσωπικών πληροφοριών και όταν είναι αναγκαίο να επικαιροποιούνται;
	θ) της διατήρησης προσωπικών πληροφοριών μόνο για όσο χρονικό διάστημα είναι απαραίτητο για νομικούς ή κανονιστικούς λόγους ή για νόμιμους οργανωτικούς σκοπούς και της διασφάλισης έγκαιρης και κατάλληλης καταστροφής;
	ι) του σεβασμού των δικαιωμάτων των φυσικών προσώπων σε σχέση με τις προσωπικές τους πληροφορίες;
	ια) της τήρησης της ασφάλειας όλων των προσωπικών πληροφοριών;
	ιβ) της διαβίβασης των προσωπικών πληροφοριών εκτός της ΕΕ μόνο σε περιπτώσεις όπου μπορούν να προστατευτούν επαρκώς;
	ιγ) όπου χρειάζεται, της στρατηγικής για την αντιμετώπιση των ρυθμιστικών αρχών σε ολόκληρη την ΕΕ, όπου τα προϊόντα και/ή οι υπηρεσίες προσφέρονται σε φυσικά πρόσωπα που κατοικούν σε άλλες χώρες της ΕΕ;
	ιδ) της εφαρμογής των διαφόρων εξαιρέσεων που επιτρέπονται από τη νομοθεσία για την προστασία δεδομένων;
	ιε) της ανάπτυξης και εφαρμογής ενός ΣΔΠΔ (PIMS) για να μπορεί να εφαρμόζεται η πολιτική του ΣΔΠΔ (PIMS);
	ιστ) του εντοπισμού των εσωτερικών και εξωτερικών ενδιαφερόμενων μερών και του βαθμού στον οποίο αυτά συμμετέχουν στη διακυβέρνηση του ΣΔΠΔ (PIMS) του οργανισμού; (4.1 παραπάνω)
	ιζ) του προσδιορισμού των εργαζομένων με ειδική υπευθυνότητα και υποχρέωση λογοδοσίας για το ΣΔΠΔ (PIMS);
	ιη) της διατήρησης αρχείων επεξεργασίας προσωπικών πληροφοριών;
4.	Η πολιτική του ΣΔΠΔ (PIMS) αναφέρει ότι καλύπτει είτε:
	α) ολόκληρο τον οργανισμό; ή
	β) ένα προσδιορισμένο τμήμα του οργανισμού;
5.3 Ρόλοι, υπευθυνότητες και αρμοδιότητες εντός του οργανισμού	
1.	Η ανώτατη Διοίκηση έχει αναθέσει υπευθυνότητες και αρμοδιότητες για τους σχετικούς ρόλους στον οργανισμό;
2.	Αυτή η πληροφορία έχει γνωστοποιηθεί εντός του οργανισμού;
3.	Η ανώτατη Διοίκηση έχει αναθέσει την ευθύνη και αρμοδιότητα για να:

	α) διασφαλίζεται ότι το ΣΔΠΔ (PIMS) συμμορφώνεται με τις απαιτήσεις του Βρετανικού Προτύπου 10012:2017;
	β) γίνονται οι αναφορές για τις επιδόσεις του ΣΔΠΔ (PIMS) στην ανώτατη Διοίκηση;
4.	Υπάρχει μέλος της ομάδας της ανώτατης Διοίκησης που είναι υπεύθυνο για τη διαχείριση των προσωπικών πληροφοριών εντός του οργανισμού, ώστε να μπορεί να αποδειχθεί η συμμόρφωση με τον ΓΚΠΔ;
5.	Αυτή η λογοδοσία περιλαμβάνει:
	α) την έγκριση της πολιτικής του ΣΔΠΔ (PIMS) από την ομάδα της ανώτατης Διοίκησης;
	β) την ανάπτυξη και εφαρμογή του ΣΔΠΔ (PIMS) όπως απαιτείται από την πολιτική του ΣΔΠΔ (PIMS);
	γ) τη διαχείριση ασφάλειας και τη διαχείριση διακινδύνευσης σε σχέση με τη συμμόρφωση με την πολιτική του ΣΔΠΔ;
6.	Έχουν διοριστεί ένας ή περισσότεροι κατάλληλα ειδικευμένοι ή έμπειροι εργαζόμενοι για να αναλάβουν την ευθύνη της συμμόρφωσης του οργανισμού σε καθημερινή βάση;
7.	Ο οργανισμός διασφαλίζει ότι το προσωπικό συμμορφώνεται με την πολιτική του ΣΔΠΔ (PIMS):
	α) με την εφαρμογή διεργασιών και διαδικασιών;
	β) με την εφαρμογή κυρώσεων;
	γ) με την κατάλληλη ανάπτυξη των εργαζομένων;
	δ) με διαδικασίες που εφαρμόζονται για την αντιμετώπιση τυχόν μη συμμορφώσεων;
5.4	**Ένταξη του ΣΔΠΔ (PIMS) στην κουλτούρα του οργανισμού**
1.	Διασφαλίζει ο οργανισμός ότι το ΣΔΠΔ (PIMS) είναι μέρος των βασικών αξιών του μέσω:
	α) της ευαισθητοποίησης και ενίσχυσης, δοκιμασίας και διατήρησης της ευαισθητοποίησης για το ΣΔΠΔ (PIMS) μέσω ενός διαρκούς προγράμματος εκπαίδευσης και ευαισθητοποίησης για το προσωπικό;
	β) της καθιέρωσης μιας διεργασίας για την αξιολόγηση της αποτελεσματικότητας του τρόπου που πραγματοποιείται η ευαισθητοποίηση για το ΣΔΠΔ (PIMS);
	γ) της γνωστοποίησης στους εργαζομένους της σημαντικότητας:
	i) της επίτευξης των στόχων του ΣΔΠΔ (PIMS);
	ii) της συμμόρφωσης με την πολιτική του ΣΔΠΔ (PIMS);
	iii) της συνεχούς βελτίωσης της πολιτικής του ΣΔΠΔ (PIMS);
	δ) της διασφάλισης ότι οι εργαζόμενοι έχουν επίγνωση της συμβολής τους στην επίτευξη των στόχων του ΣΔΠΔ (PIMS) του οργανισμού και των συνεπειών της μη συμμόρφωσης;
	ε) της διατήρησης τεκμηριωμένων πληροφοριών σχετικά με τις δραστηριότητες εκπαίδευσης και ευαισθητοποίησης και την αποτελεσματικότητά του;
6	**Σχεδιασμός**
6.1	**Ενέργειες για την αντιμετώπιση απειλών και την αξιοποίηση ευκαιριών**
6.1.1	**Γενικά**
1.	Ο οργανισμός έχει λάβει υπόψη τις παραμέτρους που αναφέρονται στο 4.1 και τις απαιτήσεις του 4.2 για να εντοπίζει τις απειλές και τις ευκαιρίες που πρέπει να αντιμετωπίζονται ώστε:
	α) να διασφαλίζεται ότι το ΣΔΠΔ (PIMS) μπορεί να επιτυγχάνει τα επιδιωκόμενα αποτελέσματα;
	β) να εξαλείφονται ή να μειώνονται οι ανεπιθύμητες επιδράσεις;
	γ) να επιτυγχάνεται η συνεχής βελτίωση;
2.	Ο οργανισμός έχει σχεδιάσει:
	α) τις ενέργειες για την αντιμετώπιση των εν λόγω απειλών και των ευκαιριών;
	β) τον τρόπο με τον οποίον:
	i) ενσωματώνει και εφαρμόζει τις εν λόγω ενέργειες στις διεργασίες του ΣΔΠΔ (PIMS);
	ii) αξιολογεί την αποτελεσματικότητα των εν λόγω ενεργειών;
6.1.2	**Καταγραφή δεδομένων και ροή δεδομένων**
1.	Ο οργανισμός έχει καθορίσει μια διεργασία για την καταγραφή δεδομένων και για την ανάλυση της ροής δεδομένων η οποία:
	α) καθιερώνει και διατηρεί ενήμερη μια καταγραφή δεδομένων και μια ανάλυση ροής δεδομένων που συμπεριλαμβάνει την αναγνώριση:
	i) των βασικών επιχειρησιακών διεργασιών που χρησιμοποιούν προσωπικές πληροφορίες;
	ii) των πηγών των προσωπικών πληροφοριών;

iii) των κατηγοριών των προσωπικών πληροφοριών που έχουν υποστεί επεξεργασία, συμπεριλαμβανομένης της αναγνώρισης των προσωπικών πληροφοριών υψηλού κινδύνου;
iv) των σκοπών για τους οποίους μπορούν να χρησιμοποιηθούν οι προσωπικές πληροφορίες, συμπεριλαμβανομένων των παρεπόμενων δευτερευόντων σκοπών πέραν του αρχικού σκοπού που συλλέχθηκαν;
v) των δυνητικών παραληπτών προσωπικών πληροφοριών, συμπεριλαμβανομένης της κοινολόγησης προσωπικών πληροφοριών σε τρίτους, σε εκτελούντες την επεξεργασία και σε προμηθευτές;
vi) των περιπτώσεων όπου ένας οργανισμός ενεργεί ως υπεύθυνος επεξεργασίας δεδομένων, ως εκτελών την επεξεργασία ή ως από κοινού υπεύθυνος επεξεργασίας δεδομένων;
vii) των βασικών συστημάτων και αποθηκών προσωπικών πληροφοριών;
viii) των περιπτώσεων όπου οι προσωπικές πληροφορίες μεταφέρονται εκτός των διεθνών συνόρων ή υπόκεινται σε διαφορετικούς νόμους, κανονισμούς, πρότυπα ή πλαίσια;
ix) των απαιτήσεων διατήρησης και καταστροφής προσωπικών πληροφοριών και των κριτηρίων για τις απαιτήσεις αυτές;
β) διασφαλίζει ότι οι επαναλαμβανόμενες καταγραφές δεδομένων παράγουν συνεπή, έγκυρα και συγκρίσιμα αποτελέσματα;
6.1.3 Νομική βάση
6.1.3.1 Επεξεργασία
1. Ο οργανισμός έχει προσδιορίσει, καθορίσει και τεκμηριώσει τη νομική βάση για την επεξεργασία όλων των προσωπικών πληροφοριών, η οποία πρέπει να επιλέγεται από μία ή περισσότερες από τις ακόλουθες:
α) την κατάλληλη απερίφραστη συγκατάθεση του φυσικού προσώπου για συγκεκριμένους σκοπούς;
β) απαραίτητη για την εκτέλεση σύμβασης της οποίας το φυσικό πρόσωπο είναι συμβαλλόμενο μέρος ή για να ληφθούν μέτρα πριν από τη σύναψη σύμβασης;
γ) απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση του οργανισμού;
δ) απαραίτητη για τη διαφύλαξη ζωτικών συμφερόντων του φυσικού προσώπου;
ε) απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον οργανισμό;
στ) απαραίτητη για τα έννομα συμφέροντα του υπεύθυνου επεξεργασίας δεδομένων ή τρίτου, εκτός εάν έναντι των συμφερόντων αυτών υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του φυσικού προσώπου; (δεν εφαρμόζεται στην επεξεργασία που διενεργείται από δημόσιες αρχές κατά την άσκηση των καθηκόντων τους)
ζ) πρόσθετες διατάξεις για κάποιο είδος επεξεργασίας που θεσπίστηκαν από εθνικές νομοθεσίες;
6.1.3.2 Ειδικές κατηγορίες
1. Ο οργανισμός έχει προσδιορίσει, καθορίσει και τεκμηριώσει τη νομική βάση για την επεξεργασία ειδικών κατηγοριών προσωπικών πληροφοριών, η οποία πρέπει να επιλέγεται από μία ή περισσότερες από τις ακόλουθες:
α) τη ρητή συγκατάθεση του φυσικού προσώπου για συγκεκριμένους σκοπούς;
β) απαραίτητη για εργασιακά δικαιώματα ή υποχρεώσεις;
γ) απαραίτητη για την προστασία των ζωτικών συμφερόντων του φυσικού προσώπου;
δ) απαραίτητη για νόμιμες δραστηριότητες ενός ιδρύματος, οργάνωσης ή άλλου μη κερδοσκοπικού φορέα με πολιτικό, φιλοσοφικό, θρησκευτικό ή συνδικαλιστικό στόχο, με κατάλληλες εγγυήσεις;
ε) πληροφορίες που έχουν σκόπιμα δημοσιοποιηθεί από το φυσικό πρόσωπο;
στ) απαραίτητη για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων;
ζ) αναγκαία για λόγους ουσιαστικού δημοσίου συμφέροντος;
η) απαραίτητη για την προληπτική ή επαγγελματική ιατρική, την εκτίμηση της ικανότητας προς εργασία ενός εργαζομένου, την ιατρική διάγνωση, την παροχή υγειονομικών και κοινωνικών συστημάτων και υπηρεσιών;
θ) απαραίτητη για λόγους δημόσιας υγείας ή επαγγελματικού απορρήτου;
ι) πρόσθετες διατάξεις για κάποιο είδος επεξεργασίας που θεσπίστηκαν από εθνικές νομοθεσίες, όσον αφορά την επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων ή δεδομένων που αφορούν την υγεία;
6.1.4 Εκτίμηση αντικτύπου για την προστασία της ιδιωτικής ζωής (PIA)
1. Ο οργανισμός έχει καθορίσει διεργασίες για την ΕΑΠΔ (PIA) σχετικά με την επεξεργασία προσωπικών πληροφοριών οι οποίες:
α) καθιερώνουν και διατηρούν κριτήρια διακινδύνευσης για την προστασία της ιδιωτικής ζωής, συμπεριλαμβανομένων:

i) των κριτηρίων αποδοχής διακινδύνευσης;
ii) των κριτηρίων για τη διενέργεια αξιολογήσεων διακινδύνευσης για την προστασία της ιδιωτικής ζωής (συμπεριλαμβανομένου και όταν απαιτείται εξωτερικά);
iii) της εφαρμογής των αρχών προστασίας δεδομένων στις ροές δεδομένων, προκειμένου να προσδιοριστούν οι κίνδυνοι για την προστασία της ιδιωτικής ζωής;
β) διασφαλίζουν ότι οι επαναλαμβανόμενες διεργασίες αξιολόγησης διακινδύνευσης για την προστασία της ιδιωτικής ζωής είναι συνεπείς, έγκυρες και συγκρίσιμες;
γ) προσδιορίζουν τους κινδύνους για την προστασία δεδομένων που σχετίζονται με τη διεργασία αξιολόγησης της διακινδύνευσης για την προστασία της ιδιωτικής ζωής προκειμένου να προσδιοριστούν οι κίνδυνοι που σχετίζονται με:
i) τους σχετικούς νόμους για την προστασία της ιδιωτικής ζωής, τα πρότυπα και τα πλαίσια;
ii) τον αντίκτυπο στα δικαιώματα και τις ελευθερίες των φυσικών προσώπων;
iii) οποιαδήποτε σωματική, υλική ή μη υλική βλάβη σε φυσικά πρόσωπα;
iv) τον αντίκτυπο στον οργανισμό (συμπεριλαμβανομένων, μεταξύ άλλων, της φήμης, της κανονιστικής ενέργειας, της οικονομικής απώλειας κ.λπ.);
δ) προσδιορίζουν τις προσωπικές πληροφορίες υψηλού κινδύνου και τις συναφείς διεργασίες που είναι υψηλού κινδύνου;
ε) προσδιορίζουν τους υπόλογους διαχείρισης διακινδύνευσης;
στ) αναλύουν τους κινδύνους για την προστασία της ιδιωτικής ζωής οι οποίοι:
i) αξιολογούν τις πιθανές συνέπειες που θα προέκυπταν εάν επέρχονταν οι κίνδυνοι που προσδιορίστηκαν στην αξιολόγηση διακινδύνευσης για την προστασία της ιδιωτικής ζωής;
ii) αξιολογούν τη ρεαλιστική πιθανότητα εμφάνισης των κινδύνων που προσδιορίστηκαν στην αξιολόγηση διακινδύνευσης για την προστασία της ιδιωτικής ζωής;
iii) καθορίζουν τη στάθμη διακινδύνευσης;
ζ) αποτιμούν τη διακινδύνευση για την προστασία της ιδιωτικής ζωής, συμπεριλαμβανομένων:
i) της σύγκρισης των αποτελεσμάτων της ανάλυσης διακινδύνευσης με τα κριτήρια διακινδύνευσης;
ii) της ιεράρχησης των αναλυμένων κινδύνων για την αντιμετώπιση διακινδύνευσης;
2. Ο οργανισμός διατηρεί τεκμηριωμένες πληροφορίες σχετικά με τη διεργασία εκτίμησης αντικτύπου για την προστασία της ιδιωτικής ζωής και τη διεργασία αξιολόγησης διακινδύνευσης;
6.1.5 Αντιμετώπιση διακινδύνευσης για την προστασία της ιδιωτικής ζωής
1. Ο οργανισμός έχει καθορίσει διεργασίες για την αντιμετώπιση διακινδύνευσης για την προστασία της ιδιωτικής ζωής ώστε:
α) να κάνει τις κατάλληλες επιλογές για την αντιμετώπιση διακινδύνευσης για την προστασία της ιδιωτικής ζωής, λαμβάνοντας υπόψη τα αποτελέσματα της αξιολόγησης της διακινδύνευσης;
β) να καθορίζει όλους τους ελέγχους που είναι απαραίτητοι για την εφαρμογή των επιλεγμένων προτάσεων αντιμετώπισης της διακινδύνευσης για την προστασία της ιδιωτικής ζωής;
γ) να διαμορφώνει ένα σχέδιο αντιμετώπισης διακινδύνευσης για την προστασία της ιδιωτικής ζωής;
δ) να λαμβάνει την έγκριση των υπόλογων διαχείρισης της διακινδύνευσης για το σχέδιο αντιμετώπισης διακινδύνευσης για την προστασία της προσωπικής ζωής και την αποδοχή της παραμένουσας διακινδύνευσης;
2. Ο οργανισμός διατηρεί τεκμηριωμένες πληροφορίες σχετικά με τη διεργασία αντιμετώπισης της διακινδύνευσης για την προστασία της ιδιωτικής ζωής;
6.1.6 Προηγούμενη διαβούλευση και έγκριση
1. Όταν οι κίνδυνοι για το φυσικό πρόσωπο από την επεξεργασία των προσωπικών πληροφοριών προσδιορίζονται από την ΕΑΠΔ να είναι υψηλοί και οι κίνδυνοι δεν μπορούν να μετριαστούν, ο οργανισμός έχει ζητήσει προηγούμενη διαβούλευση και εξουσιοδότηση από την εποπτική αρχή;
2. Ο οργανισμός διατηρεί τεκμηριωμένες πληροφορίες για τα κριτήρια και τις διαδικασίες σχετικά με την αλληλεπίδραση με τα κατάλληλα εποπτικά όργανα για την προηγούμενη διαβούλευση και έγκριση;
6.1.7 Προστασία της ιδιωτικής ζωής ήδη από τον σχεδιασμό και εξ ορισμού
1. Κατά τον σχεδιασμό ή την υλοποίηση σημαντικών αλλαγών σε συστήματα, προϊόντα και υπηρεσίες, ο οργανισμός διασφαλίζει ότι η επεξεργασία προσωπικών πληροφοριών:
α) ελαχιστοποιείται εξ ορισμού;
β) χρησιμοποιεί ανωνυμοποιημένες πληροφορίες όπου είναι δυνατόν;
γ) είναι διαφανής όσον αφορά τις λειτουργίες και την επεξεργασία των προσωπικών πληροφοριών;
2. Επιτυγχάνεται αυτό με τη λήψη κατάλληλων οργανωτικών και τεχνικών μέτρων:

α) τα οποία είναι κατάλληλα για τους προσδιοριζόμενους κινδύνους;
β) τα οποία διασφαλίζουν ότι οι προσδιορισμένοι έλεγχοι για την προστασία της ιδιωτικής ζωής εφαρμόζονται ως κατάλληλες προστασίες για προσωπικές πληροφορίες;
γ) τα οποία τηρούν κατάλληλες τεκμηριωμένες πληροφορίες σχετικά με τις δραστηριότητες και τα αποτελέσματα της προστασίας της ιδιωτικής ζωής ήδη από τον σχεδιασμό και τα αποτελέσματα;
6.2 Στόχοι του ΣΔΠΔ (PIMS) και σχεδιασμός για την επίτευξή τους
1. Ο οργανισμός έχει καθιερώσει τους στόχους του ΣΔΠΔ (PIMS) στις σχετικές λειτουργίες και βαθμίδες;
2. Είναι οι στόχοι του ΣΔΠΔ (PIMS):
α) συμβατοί με την πολιτική του ΣΔΠΔ (PIMS);
β) μετρήσιμοι;
γ) λαμβάνουν υπόψη τις εφαρμοστέες απαιτήσεις για την προστασία της ιδιωτικής ζωής και τα αποτελέσματα από τις αξιολογήσεις διακινδύνευσης και τις αντιμετωπίσεις διακινδύνευσης;
δ) παρακολουθούνται;
ε) γνωστοποιούνται;
στ) διατηρούνται ενήμεροι όπως ενδείκνυται;
3. Διατηρεί ο οργανισμός ενήμερες τεκμηριωμένες πληροφορίες για τους στόχους του ΣΔΠΔ (PIMS);
4. Κατά τη φάση σχεδιασμού της επίτευξης των στόχων του ΣΔΠΔ (PIMS), ο οργανισμός έχει καθορίσει:
α) τί πρόκειται να υλοποιηθεί;
β) ποιοί πόροι απαιτούνται;
γ) ποιός είναι υπεύθυνος;
δ) πότε θα ολοκληρώνεται;
ε) πώς θα αξιολογούνται τα αποτελέσματα;
7 Υποστήριξη
7.1 Πόροι
1. Ο οργανισμός έχει προσδιορίσει και παράσχει τους πόρους που απαιτούνται για την:
α) καθιέρωση του ΣΔΠΔ (PIMS);
β) εφαρμογή του ΣΔΠΔ (PIMS);
γ) διατήρηση ενήμερου του ΣΔΠΔ (PIMS);
δ) συνεχή βελτίωση του ΣΔΠΔ (PIMS);
7.2 Επαγγελματική επάρκεια
1. Ο οργανισμός έχει:
α) καθορίσει την απαραίτητη επαγγελματική επάρκεια του προσωπικού που εκτελεί εργασίες υπό τον έλεγχό του οι οποίες επηρεάζουν τις επιδόσεις του ΣΔΠΔ (PIMS);
β) διασφαλίσει ότι το εν λόγω προσωπικό διαθέτει την επαγγελματική επάρκεια βάσει της κατάλληλης μόρφωσης, κατάρτισης ή εμπειρίας;
γ) αναλάβει ενέργειες για την απόκτηση της απαραίτητης επαγγελματικής επάρκειας και έχει αξιολογήσει την αποτελεσματικότητα των ενεργειών αυτών;
2. Ο οργανισμός έχει τηρήσει τεκμηριωμένες πληροφορίες ως αποδεικτικά στοιχεία της επαγγελματικής επάρκειας;
7.3 Ευαισθητοποίηση
1. Έχει επίγνωση το προσωπικό που εκτελεί εργασίες υπό τον έλεγχο του οργανισμού:
α) της πολιτικής του ΣΔΠΔ (PIMS);
β) της συμβολής του στην αποτελεσματικότητα του ΣΔΠΔ (PIMS), συμπεριλαμβανομένων των ωφελημάτων από τη βελτίωση των επιδόσεων του ΣΔΠΔ (PIMS);
γ) των επιπτώσεων της μη συμμόρφωσης με τις απαιτήσεις του ΣΔΠΔ (PIMS);
7.4 Επικοινωνία
1. Ο οργανισμός έχει προσδιορίσει τις ανάγκες εσωτερικής και εξωτερικής επικοινωνίας σχετικά με το ΣΔΠΔ (PIMS), συμπεριλαμβανομένων:
α) για το τί γνωστοποιείται;
β) πότε γνωστοποιείται;
γ) σε ποιόν γνωστοποιείται;
δ) πώς γνωστοποιείται;
7.5 Τεκμηριωμένες πληροφορίες
7.5.1 Γενικά

1. Περιλαμβάνει το ΣΔΠΔ (PIMS):
α) τις τεκμηριωμένες πληροφορίες που απαιτούνται από το Βρετανικό Πρότυπο 10012:2017;
β) τις τεκμηριωμένες πληροφορίες που ο οργανισμός προσδιορίζει ως απαραίτητες για την αποτελεσματικότητα του ΣΔΠΔ (PIMS);
7.5.2 Γενικά
1. Κατά τη δημιουργία και επικαιροποίηση των τεκμηριωμένων πληροφοριών, ο οργανισμός διασφαλίζει:
α) ταυτοποίηση και περιγραφή (π.χ. τίτλος, ημερομηνία, συντάκτης ή αριθμός αναφοράς);
β) μορφή (π.χ. γλώσσα, έκδοση λογισμικού, γραφικά) και μέσα εγγραφής (π.χ. χαρτί, ηλεκτρονικά);
γ) ανασκόπηση και έγκριση ως προς την καταλληλότητα και επάρκεια;
7.5.3 Δημιουργία και επικαιροποίηση
1. Οι τεκμηριωμένες πληροφορίες που απαιτούνται από το ΣΔΠΔ (PIMS) ελέγχονται ώστε να διασφαλίζεται ότι:
α) είναι διαθέσιμες και κατάλληλες για χρήση, όπου και όταν χρειάζεται;
β) προστατεύονται επαρκώς; (π.χ. έναντι απώλειας της εμπιστευτικότητας, αθέμιτης χρήσης ή απώλειας της ακεραιότητας)
2. Για τον έλεγχο των τεκμηριωμένων πληροφοριών, ο οργανισμός υλοποιεί τις ακόλουθες δραστηριότητες:
α) τη διανομή, πρόσβαση, ανάκτηση και χρήση;
β) την αποθήκευση και διαφύλαξη;
γ) τον έλεγχο των αλλαγών (π.χ. έλεγχος έκδοσης);
δ) την τήρηση και τελική διάθεση;
3. Προσδιορίζονται και ελέγχονται από τον οργανισμό οι τεκμηριωμένες πληροφορίες σχετικά με το ΣΔΠΔ (PIMS) εξωτερικής προέλευσης;
8 Λειτουργία
8.1 Σχεδιασμός, λειτουργία και έλεγχος των διεργασιών
1. Ο οργανισμός έχει σχεδιάσει, υλοποιήσει και ελέγξει τις διεργασίες που απαιτούνται ώστε να ανταποκρίνεται στις απαιτήσεις καθώς και για την υλοποίηση των ενεργειών που καθορίζονται στο 6.1 (απειλές και ευκαιρίες) με:
α) τον καθορισμό των απαιτήσεων για τις διεργασίες;
β) τη διενέργεια ελέγχων των διεργασιών σύμφωνα με τα κριτήρια;
γ) την τήρηση τεκμηριωμένων πληροφοριών στον βαθμό που είναι αναγκαίο για την παροχή εμπιστοσύνης ως προς το ότι οι διεργασίες λειτουργούν σύμφωνα με τα προβλεπόμενα;
2. Ο οργανισμός ελέγχει τις σχεδιαζόμενες αλλαγές και ανασκοπεί τις συνέπειες των ακούσιων αλλαγών αναλαμβάνοντας ενέργειες για τον περιορισμό των αρνητικών επιπτώσεων;
3. Οι διεργασίες που έχουν ανατεθεί σε εξωτερικά μέρη ελέγχονται;
8.2 Εφαρμογή του ΣΔΠΔ (PIMS)
8.2.1 Βασικές αναθέσεις
8.2.1.1 Ανώτατη Διοίκηση
1. Υπάρχει μέλος της ανώτατης Διοίκησης που να έχει καθοριστεί υπόλογο για τη διαχείριση των προσωπικών πληροφοριών εντός του οργανισμού;
8.2.1.2 Υπεύθυνος προστασίας δεδομένων (ΥΠΔ) (DPO)
1. Ο οργανισμός υποχρεώνεται να διορίσει ΥΠΔ (DPO);
2. Εάν ναι, έχει διοριστεί ένας εργαζόμενος με τα κατάλληλα προσόντα για την εκπλήρωση αυτού του ρόλου;
3. Έχουν υποβληθεί τα στοιχεία επικοινωνίας του ΥΠΔ (DPO) στην αρμόδια εποπτική αρχή;
4. Ο ΥΠΔ (DPO) διασφαλίζει ότι η πολιτική του ΣΔΠΔ (PIMS) συμμορφώνεται με τους εφαρμοστέους νόμους, τους κανονισμούς και τις επιχειρησιακές απαιτήσεις;
5. Ο ΥΠΔ (DPO) διασφαλίζει ότι διεξάγονται οι ενδεδειγμένες εκτιμήσεις αντίκτυπου για την προστασία της ιδιωτικής ζωής και οι αξιολογήσεις διακινδύνευσης, όπου αυτό είναι αναγκαίο;
6. Ο ΥΠΔ (DPO) διασφαλίζει ότι διεξάγονται τυχόν κοινοποιήσεις προς την εποπτική αρχή, όπου αυτό είναι αναγκαίο;
7. Ο οργανισμός διασφαλίζει ότι ο ΥΠΔ (DPO) συμμετέχει έγκαιρα σε όλα τα ζητήματα που αφορούν την επεξεργασία προσωπικών δεδομένων;
8.2.1.3 Ευθύνη για συμμόρφωση με την πολιτική του ΣΔΠΔ (PIMS) σε καθημερινή βάση

1. Υπάρχει ένας ή περισσότεροι εργαζόμενοι με τα κατάλληλα προσόντα ή έμπειροι που να έχουν οριστεί ως υπεύθυνοι για τη συμμόρφωση με την πολιτική του ΣΔΠΔ (PIMS) σε καθημερινή βάση;
2. Όπου χρειάζεται, αυτοί οι διορισμένοι δίνουν αναφορά στον ΥΠΔ (DPO);
3. Αυτοί οι διορισμένοι έχουν τις ακόλουθες αρμοδιότητες:
α) συνολική ευθύνη για την παρακολούθηση της συμμόρφωσης με την πολιτική του ΣΔΠΔ (PIMS);
β) ανάπτυξη και ανασκόπηση της πολιτικής του ΣΔΠΔ (PIMS);
γ) διασφάλιση της εφαρμογής της πολιτικής του ΣΔΠΔ (PIMS);
δ) ανασκόπησης της διαχείρισης της πολιτικής του ΣΔΠΔ (PIMS);
ε) εκπαίδευση και συνεχή ευαισθητοποίηση όπως απαιτείται από την πολιτική του ΣΔΠΠ (PIMS);
στ) έγκριση των διαδικασιών όταν επεξεργάζονται προσωπικές πληροφορίες όπως:
i) διαχείριση και γνωστοποίηση των πληροφοριών για την προστασία της ιδιωτικής ζωής;
ii) διαχείριση αιτημάτων από φυσικά πρόσωπα;
iii) συλλογή και διαχείριση των προσωπικών πληροφοριών;
iv) διαχείριση παραπόνων;
v) διαχείριση των παραβιάσεων της ασφάλειας;
vi) εξωτερική ανάθεση εργασιών και δημιουργία υπεράκτιων εταιριών;
ζ) σύνδεση με τους υπεύθυνους για τη διαχείριση διακινδύνευσης, για τις παραμέτρους ασφάλειας και για τις λειτουργίες επιθεώρησης εντός του οργανισμού;
η) παροχή εμπειρογνωμοσύνης, συμβουλών και καθοδήγησης σε παραμέτρους για την προστασία δεδομένων;
θ) ερμηνεία και εφαρμογή των διαφόρων εξαιρέσεων που εφαρμόζονται στην επεξεργασία προσωπικών πληροφοριών;
ι) παροχή συμβουλών σε σχέση με εργασίες ανταλλαγής δεδομένων (συμπεριλαμβανομένων των παραμέτρων ασφάλειας όταν τα δεδομένα είναι εκτός της κύριας εγκατάστασης της επιχείρησης;
ια) διασφάλιση ότι ο οργανισμός έχει πρόσβαση σε νομοθετικές ενημερώσεις και κατάλληλη καθοδήγηση σχετικά με τις απαιτήσεις για την προστασία δεδομένων και ότι η πολιτική του ΣΔΠΔ (PIMS) ανασκοπείται διαρκώς ώστε να συμμορφώνεται με τις νομοθετικές ενημερώσεις;
ιβ) εφαρμογή όπως ενδείκνυται των πρακτικών που σχετίζονται με την επεξεργασία των προσωπικών πληροφοριών οι οποίες περιγράφονται σε όλους τους υποχρεωτικούς ή συμβουλευτικούς τομεακούς κώδικες που ισχύουν για τον οργανισμό;
8.2.1.4 Εκπρόσωποι για την προστασία δεδομένων
1. Ο οργανισμός έχει καθορίσει αν θα ήταν σκόπιμο να δημιουργηθεί ένα δίκτυο εκπροσώπων για την προστασία δεδομένων σε διάφορα τμήματα ή συστήματα που επεξεργάζονται προσωπικές πληροφορίες;
2. Εάν ναι, το δίκτυο εκπροσώπων για την προστασία δεδομένων:
α) εκπροσωπεί τμήματα ή συστήματα τα οποία αναγνωρίζονται ως υψηλού κινδύνου σε σχέση με τη διαχείριση των προσωπικών πληροφοριών;
β) βοηθά τους εργαζόμενους με την καθημερινή ευθύνη για συμμόρφωση με την πολιτική του ΣΔΠΔ (PIMS);
8.2.2 Προσδιορισμός και καταγραφή χρήσεων των προσωπικών πληροφοριών
8.2.2.1 Καταγραφή
1. Διατηρείται ένας κατάλογος των κατηγοριών των προσωπικών πληροφοριών που επεξεργάζεται ο οργανισμός;
2. Ο κατάλογος αυτός τεκμηριώνει τους σκοπούς για τους οποίους χρησιμοποιείται κάθε κατηγορία προσωπικών πληροφοριών;
3. Ο οργανισμός τεκμηριώνει τη ροή των προσωπικών πληροφοριών σε όλες τις διεργασίες του οργανισμού;
8.2.2.2 Προσωπικές πληροφορίες υψηλού κινδύνου
1. Η καταγραφή επιτρέπει τον σαφή προσδιορισμό και την τεκμηρίωση των κατηγοριών προσωπικών πληροφοριών υψηλού κινδύνου που επεξεργάζονται από τον οργανισμό;
8.2.3 Αξιολόγηση και αντιμετώπιση διακινδύνευσης
1. Ο οργανισμός αξιολογεί τη στάθμη διακινδύνευσης για τα φυσικά πρόσωπα που σχετίζεται με την επεξεργασία των προσωπικών τους πληροφοριών, με την εφαρμογή της ΕΑΠΔ (PIA);
2. Ο οργανισμός έχει εφαρμόσει σχέδιο αντιμετώπισης διακινδύνευσης για τη διαχείριση τυχόν κινδύνων που προσδιορίζονται στην αξιολόγηση διακινδύνευσης προκειμένου να μειωθεί η πιθανότητα μη συμμόρφωσης με την πολιτική του ΣΔΠΔ (PIMS);

3. Η διεργασία αξιολόγησης της διακινδύνευσης περιλαμβάνει διαδικασίες με τις οποίες οποιαδήποτε επεξεργασία προσωπικών πληροφοριών που θα μπορούσε να προκαλέσει βλάβη και/ή αγωνία στα φυσικά πρόσωπα να μπορεί να κλιμακωθεί για ανασκόπηση από τους υπεύθυνους και υπόλογους για τη διαχείριση των προσωπικών πληροφοριών;
8.2.4 Εκπαίδευση και ευαισθητοποίηση
1. Ο οργανισμός διασφαλίζει ότι ο εργαζόμενος με καθημερινή ευθύνη για την απόδειξη της συμμόρφωσης με τις απαιτήσεις για την προστασία δεδομένων:
α) είναι σε θέση να αποδεικνύει επάρκεια στην κατανόηση των απαιτήσεων για την προστασία δεδομένων και στον τρόπο με τον οποίο θα πρέπει να εφαρμόζεται αυτό εντός του οργανισμού;
β) παραμένει ενήμερος για παραμέτρους που σχετίζονται με τη διαχείριση των προσωπικών πληροφοριών, όπου χρειάζεται, μέσω επαφής με εξωτερικούς φορείς;
2. Ο οργανισμός είναι σε θέση να αποδεικνύει ότι οι εργαζόμενοι κατανοούν την ευθύνη τους να διασφαλίζουν ότι οι προσωπικές πληροφορίες προστατεύονται και επεξεργάζονται σύμφωνα με τις εφαρμοστέες διαδικασίες;
3. Σε αυτό, λαμβάνονται υπόψη οι σχετικές απαιτήσεις ασφάλειας;
4. Οι εργαζόμενοι λαμβάνουν εκπαίδευση για να μπορούν να επεξεργάζονται προσωπικές πληροφορίες σύμφωνα με τις εφαρμοστέες διαδικασίες;
5. Η εκπαίδευση αυτή πρέπει να είναι συναφής με τον ρόλο του κάθε εργαζομένου στον οργανισμό;
6. Η εκπαίδευση αναφέρεται στις διαδικασίες ασφάλειας πληροφοριών;
8.2.5 Επικαιροποίηση του ΣΔΠΔ (PIMS)
1. Το προσωπικό με καθημερινή ευθύνη για τη συμμόρφωση με την πολιτική του ΣΔΠΔ (PIMS) αξιολογεί σε προγραμματισμένα χρονικά διαστήματα εάν το ΣΔΠΔ (PIMS) επιτρέπει και θα συνεχίσει να επιτρέπει την απόδειξη συμμόρφωσης με τις απαιτήσεις για την προστασία δεδομένων;
2. Αυτή η αξιολόγηση περιλαμβάνει την ανασκόπηση του ΣΔΠΔ (PIMS), όταν συμβαίνουν αλλαγές στις απαιτήσεις και/ή στην τεχνολογία του οργανισμού;
8.2.6 Θεμιτή, σύννομη και διαφανής επεξεργασία
8.2.6.1 Συλλογή και επεξεργασία προσωπικών πληροφοριών
1. Διασφαλίζει το ΣΔΠΔ (PIMS) ότι:
α) ο οργανισμός επεξεργάζεται προσωπικές πληροφορίες θεμιτά και σύννομα;
β) ο οργανισμός επεξεργάζεται προσωπικές πληροφορίες μόνο εφόσον αυτό δικαιολογείται;
γ) ο οργανισμός επεξεργάζεται προσωπικές πληροφορίες υψηλού κινδύνου μόνο όταν αυτό είναι απαραίτητο για τους σκοπούς του οργανισμού;
δ) ο οργανισμός παρέχει στα φυσικά πρόσωπα πληροφορίες σε κατάλληλο μορφότυπο, οι οποίες γνωστοποιούν με σαφήνεια:
i) την ταυτότητα του οργανισμού και των εκπροσώπων του, όπου εφαρμόζεται;
ii) τους σκοπούς για τους οποίους μπορούν να επεξεργαστούν οι προσωπικές πληροφορίες;
iii) τα έννομα συμφέροντα του οργανισμού ή την επεξεργασία, εφόσον αυτή είναι η νομική βάση που χρησιμοποιήθηκε;
iv) τα είδη των προσωπικών πληροφοριών που συλλέγονται;
v) την πηγή των προσωπικών πληροφοριών και κατά πόσον προέρχονται από πηγές στις οποίες έχει πρόσβαση το κοινό;
vi) πληροφορίες σχετικά με την κοινολόγηση προσωπικών πληροφοριών σε τρίτους;
vii) εάν οι προσωπικές πληροφορίες διαβιβάζονται εκτός του ΕΟΧ και παρέχουν επεξηγήσεις σχετικά με τις εγγυήσεις που εφαρμόζονται και με τον τρόπο απόκτησης αντιγράφου αυτών των εγγυήσεων;
viii) όπου ο οργανισμός εδρεύει εκτός της ΕΕ και το φυσικό πρόσωπο βρίσκεται στην ΕΕ, την ταυτότητα του εκπροσώπου με έδρα την ΕΕ, όπου αυτό απαιτείται;
ix) λεπτομέρειες σχετικά με όλες τις τεχνολογίες, όπως cookies, που χρησιμοποιούνται σε έναν ιστότοπο για τη συλλογή προσωπικών πληροφοριών σχετικά με τα φυσικά πρόσωπα;
x) άλλες πληροφορίες που καθιστούν την επεξεργασία θεμιτή και διαφανή:
i) το χρονικό διάστημα διατήρησης ή τα κριτήρια που χρησιμοποιούνται για τον καθορισμό της διατήρησης;

ii) οι πληροφορίες που αφορούν τα δικαιώματα του φυσικού προσώπου για πρόσβαση, διόρθωση, διαγραφή και περιορισμό των προσωπικών πληροφοριών, καθώς και το δικαίωμα στη φορητότητα των δεδομένων;
iii) το δικαίωμα υποβολής καταγγελίας στην εποπτική αρχή;
iv) όταν η επεξεργασία βασίζεται σε συγκατάθεση, το δικαίωμα ανάκλησης της συγκατάθεσης;
v) όταν η παροχή πληροφοριών αποτελεί νομική ή συμβατική απαίτηση, η ενημέρωση του φυσικού προσώπου για τους λόγους που καθιστούν απαραίτητη την παροχή πληροφοριών και ποιές είναι οι συνέπειες της μη παροχής των πληροφοριών;
vi) πληροφορίες σχετικά με τυχόν αυτοματοποιημένη λήψη αποφάσεων και/ή την κατάρτιση προφίλ που θα μπορούσαν να χρησιμοποιηθούν οι πληροφορίες;
2. Όταν τα προσωπικά στοιχεία συλλέγονται για σκοπούς εμπορικής προώθησης ή ενδέχεται να χρησιμοποιηθούν στο μέλλον για σκοπούς εμπορικής προώθησης, το ΣΔΠΔ (PIMS) διασφαλίζει ότι το φυσικό πρόσωπο ενημερώνεται για τον τρόπο με τον οποίον μπορεί να αντιταχθεί;
3. Όταν χρησιμοποιείται η κατάρτιση προφίλ με αυτοματοποιημένα μέσα για σκοπούς εμπορικής προώθησης, το ΣΔΠΔ (PIMS) διασφαλίζει ότι το δικαίωμα αντίταξης και ο μηχανισμός με τον οποίο ένα φυσικό πρόσωπο μπορεί να αντιταχθεί σε τέτοιες διαδικασίες εξηγείται σαφώς στο εν λόγω φυσικό πρόσωπο;
4. Όταν η επεξεργασία βασίζεται στη συγκατάθεση, διατηρούνται τα αρχεία της συγκατάθεσης;
5. Όταν ανακαλείται η συγκατάθεση, διατηρούνται τα αρχεία της ανάκλησης της συγκατάθεσης;
6. Για άλλες τομεακές απαιτήσεις ή νομοθεσία που απαιτούν ρητή συγκατάθεση για την εμπορική προώθηση συλλέγεται η συγκατάθεση;
7. Όταν συλλέγονται προσωπικές πληροφορίες υψηλού κινδύνου αναφέρονται ρητά ο σκοπός/οι σκοποί για τους οποίους χρησιμοποιούνται οι πληροφορίες υψηλού κινδύνου ή πρόκειται να χρησιμοποιηθούν;
8. Οι νέες μέθοδοι συλλογής ανασκοπούνται και υπογράφονται από έναν εργαζόμενο με τα κατάλληλα προσόντα ή έναν έμπειρο εργαζόμενο;
8.2.6.2 Αρχεία πληροφοριών ιδιωτικού απορρήτου (όπως ειδοποιήσεις και δηλώσεις)
1. Διατηρούνται αρχεία των πληροφοριών ιδιωτικού απορρήτου που παρέχονται σε φυσικά πρόσωπα; (πχ. ειδοποιήσεις ιδιωτικού απορρήτου και επιγραμμικές δηλώσεις ιδιωτικού απορρήτου)
2. Τα αρχεία αυτά διατηρούνται τουλάχιστον για όσο χρονικό διάστημα διατηρούνται οι προσωπικές πληροφορίες στις οποίες αναφέρονται;
3. Διατηρεί ο οργανισμός πληροφορίες σχετικά με το πότε ίσχυε μια συγκεκριμένη ειδοποίηση ιδιωτικού απορρήτου (ή έκδοση ειδοποίησης ιδιωτικού απορρήτου);
8.2.6.3 Χρονικά σημεία παροχής/διάθεσης των πληροφοριών ιδιωτικού απορρήτου
1. Παρέχετε στα φυσικά πρόσωπα τυχόν πληροφορίες όταν συλλέγετε δεδομένα;
2. Εάν ναι, όταν συλλέγετε προσωπικές πληροφορίες απευθείας από το φυσικό πρόσωπο, παρέχετε αυτές τις πληροφορίες πριν από την απόκτηση προσωπικών πληροφοριών;
3. Εάν οι προσωπικές πληροφορίες δεν λαμβάνονται απευθείας από το φυσικό πρόσωπο, αυτές οι απαιτούμενες πληροφορίες παρέχονται μετά τη λήψη των πληροφοριών ή:
α) το αργότερο εντός ενός μηνός, λαμβάνοντας υπόψη τις ειδικές συνθήκες υπό τις οποίες οι πληροφορίες υποβάλλονται σε επεξεργασία;
β) εάν οι πληροφορίες χρησιμοποιούνται για επικοινωνία με το φυσικό πρόσωπο, τότε κατά την πρώτη επικοινωνία;
γ) εάν οι πληροφορίες προορίζονται να γνωστοποιηθούν σε άλλον παραλήπτη, τότε το αργότερο όταν οι πληροφορίες γνωστοποιούνται για πρώτη φορά;
8.2.6.4 Προσβασιμότητα των πληροφοριών ιδιωτικού απορρήτου
1. Οι τυχόν πληροφορίες που παρουσιάζονται σε φυσικά πρόσωπα παρουσιάζονται με τρόπο που επιτρέπει την εύκολη πρόσβαση και κατανόηση των πληροφοριών, συμπεριλαμβανομένων να είναι εύκολα κατανοητές από παιδιά και ευάλωτους ενήλικες;
8.2.6.5 Συλλογή από τρίτους
1. Οι προσωπικές πληροφορίες που συλλέγονται από τρίτους, συλλέγονται θεμιτά και σύννομα;
2. Τα φυσικά πρόσωπα των οποίων οι προσωπικές πληροφορίες έχουν συλλεχθεί από τρίτους λαμβάνουν τις πληροφορίες που ορίζονται στο 8.2.6.1 (δ);

3. Αυτές οι πληροφορίες παρέχονται στα φυσικά πρόσωπα εντός ενός μηνός από τη συλλογή από τον τρίτο;
8.2.7 Επεξεργασία για καθορισμένους νόμιμους σκοπούς
8.2.7.1 Λόγοι επεξεργασίας
1. Οι προσωπικές πληροφορίες αποκτώνται μόνο για έναν ή για περισσότερους καθορισμένους σκοπούς και δεν υποβάλλονται σε περαιτέρω επεξεργασία με κανέναν τρόπο ασύμβατο με τον εν λόγω σκοπό ή τους εν λόγω σκοπούς;
2. Διασφαλίζει το ΣΔΠΔ (PIMS) ότι η επεξεργασία προσωπικών πληροφοριών δεν πραγματοποιείται κατά τρόπο που παραβιάζει ή ενδεχομένως παραβιάζει τυχόν νομικές υποχρεώσεις, συμπεριλαμβανομένων των κανονιστικών διατάξεων, του κοινού δικαίου ή των συμβατικών όρων;
3. Διασφαλίζει το ΣΔΠΔ (PIMS) ότι οι προσωπικές πληροφορίες που συλλέγονται για καθορισμένους σκοπούς δεν χρησιμοποιούνται για άλλον ασύμβατο σκοπό, εκτός εάν:
α) εφαρμόζεται σχετική εξαίρεση από τη νομοθεσία;
β) τα φυσικά πρόσωπα των οποίων οι προσωπικές πληροφορίες πρόκειται να υποβληθούν σε επεξεργασία για τον νέο σκοπό, έχουν συγκατατεθεί στην επεξεργασία για τον εν λόγω νέο σκοπό;
4. Όταν πρόκειται να χρησιμοποιηθούν προσωπικές πληροφορίες υψηλού κινδύνου για έναν ασύμβατο νέο σκοπό, παρέχεται η ρητή συγκατάθεση του φυσικού προσώπου για τον σκοπό αυτό πριν από την επεξεργασία;
8.2.7.2 Συγκατάθεση για ασύμβατους σκοπούς
1. Είναι οποιαδήποτε επεξεργασία συμβατή με τον αρχικό σκοπό, ή αν υπάρχει χρήση για πρόσθετο σκοπό, διασφαλίζεται ότι η νέα χρήση δεν είναι απροσδόκητη και ότι είναι θεμιτή;
2. Παρέχεται η συγκατάθεση για κάθε ασυμβίβαστο σκοπό ελεύθερα και εν επιγνώσει;
3. Το ΣΔΠΔ (PIMS) διασφαλίζει ότι:
α) αποκτώνται θετικές ενδείξεις για τη συγκατάθεση ενός φυσικού προσώπου σχετικά με τη χρήση των προσωπικών του πληροφοριών για κάποιο σκοπό;
β) διατηρούνται τα αρχεία της συγκατάθεσης που αποκτήθηκε για έναν νέο σκοπό;
8.2.7.3 Επεξεργασία πληροφοριών παιδιών
1. Επεξεργάζεστε προσωπικές πληροφορίες που αφορούν παιδιά;
2. Εάν ναι, υπάρχει μηχανισμός για τη λήψη της συγκατάθεσης του προσώπου που έχει τη γονική μέριμνα;
3. Αυτό επεκτείνεται στην κατάρτιση προφίλ και στις δραστηριότητες εμπορικής προώθησης;
8.2.7.4 Ανταλλαγή δεδομένων
1. Μοιράζεστε προσωπικές πληροφορίες με άλλον οργανισμό;
2. Εάν ναι, οι ευθύνες και των δύο μερών όσον αφορά τις προσωπικές πληροφορίες τεκμηριώνονται επισήμως με συμφωνητικό έγγραφο ή σύμβαση;
3. Εάν ο άλλος οργανισμός χρησιμοποιεί τις προσωπικές πληροφορίες για δικούς του σκοπούς υπάρχει:
α) έγγραφο συμφωνητικό ή η σύμβαση που να περιγράφει τόσο τους σκοπούς για τους οποίους μπορούν να χρησιμοποιηθούν οι πληροφορίες όσο και τους τυχόν περιορισμούς για την περαιτέρω χρήση των προσωπικών πληροφοριών για άλλους σκοπούς;
β) απόδειξη ότι ο άλλος οργανισμός δεσμεύεται να επεξεργάζεται τις πληροφορίες κατά τρόπο που δεν αντιβαίνει στη νομοθεσία για την προστασία δεδομένων;
4. Όπου είναι δυνατόν, οποιαδήποτε νέα επεξεργασία που συνεπάγεται την ανταλλαγή προσωπικών πληροφοριών με τρίτους είναι συμβατή με τους όρους των πληροφοριών που παρέχονται στο φυσικό πρόσωπο όπως απαιτείται στο 8.2.6.1 του Προτύπου;
5. Εάν αυτό δεν είναι δυνατό, ο οργανισμός:
α) έχει μια νομική βάση για την ανταλλαγή δεδομένων;
β) παρέχει κατάλληλη ειδοποίηση για την ανταλλαγή στο φυσικό πρόσωπο;
γ) αξιολογεί τη συμμόρφωση σύμφωνα με την αρχή του «περιορισμού του σκοπού»;
δ) εάν απαιτείται, έχει τη συγκατάθεση του φυσικού προσώπου για την ανταλλαγή δεδομένων;

6. Εάν επιτρέπεται η ανταλλαγή δεδομένων με τρίτους χωρίς τη συγκατάθεση του φυσικού προσώπου, υπάρχει ένα ελεγχόμενο αρχείο των πρωτοκόλλων και των ελέγχων για την εν λόγω ανταλλαγή δεδομένων;
7. Αυτό τεκμηριώνεται;
8. Όπου απαιτείται η ανταλλαγή δεδομένων με τρίτους (π.χ. από τον νόμο), τεκμηριώνονται τα πρωτόκολλα και οι έλεγχοι για την ανταλλαγή δεδομένων;
8.2.7.5 Ανοιχτά δεδομένα
1. Δημοσιεύονται προσωπικές πληροφορίες στο πλαίσιο μιας πρωτοβουλίας «ανοιχτών δεδομένων»;
2. Εάν ναι, ανωνυμοποιούνται οι προσωπικές πληροφορίες ώστε τα φυσικά πρόσωπα να μην είναι ταυτοποιήσιμα;
3. Ο οργανισμός, λαμβάνει υπόψη όλα τα εύλογα μέσα που μπορούν να χρησιμοποιηθούν για να επανα-ταυτοποιήσουν το φυσικό πρόσωπο;
8.2.7.6 Συνδυασμός δεδομένων
1. Οι προσωπικές πληροφορίες συνδυάζονται με άλλες προσωπικές πληροφορίες;
2. Εάν ναι, οι συνδυασμένες προσωπικές πληροφορίες χρησιμοποιούνται μόνο:
α) για γνωστοποιημένους και συμβατούς σκοπούς;
β) όπως απαιτείται από τον νόμο;
γ) όταν έχει αποκτηθεί συναίνεση;
3. Όταν ο συνδυασμός δεδομένων σχετίζεται με προσωπικές πληροφορίες για παιδιά, περιλαμβάνονται συγκεκριμένα μέτρα προστασίας εντός του ΣΔΠΔ (PIMS);
4. Αυτά τα μέτρα λαμβάνουν υπόψη:
α) τους πιθανούς κινδύνους και τις συνέπειες;
β) τις απαιτήσεις για εγγυήσεις;
γ) τα συγκεκριμένα δικαιώματα των παιδιών;
8.2.8 Κατάλληλες, συναφείς και σύμφωνες με τις αρχές ελαχιστοποίησης των δεδομένων
8.2.8.1 Καταλληλότητα
1. Είναι οι προσωπικές πληροφορίες που συλλέγει ο οργανισμός κατάλληλες για τους σκοπούς του οργανισμού;
2. Διεξάγονται τακτικές ανασκοπήσεις (π.χ. ετήσια) της τεχνολογίας και των διεργασιών που αφορούν την επεξεργασία προσωπικών πληροφοριών, ώστε να διασφαλίζεται ότι οι προσωπικές πληροφορίες εξακολουθούν να είναι κατάλληλες για τους σκοπούς αυτούς;
8.2.8.2 Συναφείς και όχι υπερβολικές
1. Το ΣΔΠΔ (PIMS) διασφαλίζει ότι:
α) ο οργανισμός επεξεργάζεται την ελάχιστη ποσότητα προσωπικών πληροφοριών που απαιτούνται για την εκπλήρωση των νόμιμων σκοπών του;
β) πρόσθετες προσωπικές πληροφορίες που δεν είναι σχετικές ή είναι υπερβολικές για τους δηλωμένους σκοπούς δεν υποβάλλονται σε επεξεργασία, εκτός εάν η παροχή των πληροφοριών αυτών είναι προαιρετική και επεξεργάζονται μόνο με τη συγκατάθεση του φυσικού προσώπου;
γ) ανασκοπούνται νέα συστήματα και διεργασίες που αφορούν την επεξεργασία προσωπικών πληροφοριών, ώστε να διασφαλίζεται ότι οι πληροφορίες που υποβάλλονται σε επεξεργασία είναι σχετικές και όχι υπερβολικές;
2. Όταν δεν είναι σχετικό ή απαραίτητο να υποβληθούν σε επεξεργασία προσωπικές πληροφορίες για τους σκοπούς του οργανισμού, το ΣΔΠΔ (PIMS) διασφαλίζει ότι οι προσωπικές πληροφορίες δεν θα υποστούν επεξεργασία;
8.2.9 Ακρίβεια
8.2.9.1 Ακριβείς και επικαιροποιημένες
1. Διατηρείται η ακεραιότητα και η ακρίβεια των προσωπικών πληροφοριών που υποβάλλονται σε επεξεργασία;
2. Είναι τα φυσικά πρόσωπα σε θέση να αμφισβητούν την ακρίβεια των προσωπικών πληροφοριών τους και να ζητούνε τη διόρθωσή τους όταν είναι αναγκαίο;
3. Αυτό τεκμηριώνεται;
4. Υπάρχει μια εγκεκριμένη και τεκμηριωμένη διεργασία για να ελέγχεται κατά πόσον οι υποτιθέμενες ανακρίβειες είναι όντως ανακριβείς;
5. Εάν κατά τον έλεγχο της αναφοράς των ανακριβών πληροφοριών, ο οργανισμός καθορίσει ότι

η παραπάνω υπόθεση είναι εσφαλμένη και τα δεδομένα στην πραγματικότητα είναι ακριβή, διατηρούνται αποδεικτικά στοιχεία;
6. Ενημερώνεται το προσωπικό για τη σημαντικότητα που έχει η ακριβής καταγραφή των προσωπικών πληροφοριών και η χρήση μόνο επικαιροποιημένων προσωπικών πληροφοριών για τη λήψη σημαντικών αποφάσεων σχετικά με τα φυσικά πρόσωπα;
7. Το ΣΔΠΔ (PIMS):
α) ενημερώνει κάθε τρίτο με τον οποίο ο οργανισμός έχει μοιραστεί ανακριβείς ή παρωχημένες προσωπικές πληροφορίες ότι οι πληροφορίες είναι ανακριβείς και/ή παρωχημένες και δεν πρέπει να χρησιμοποιούνται για την ενημέρωση των αποφάσεων σχετικά με τα φυσικά πρόσωπα;
β) μοιράζεται τυχόν διορθώσεις των προσωπικών πληροφοριών με τον τρίτο, όταν αυτό απαιτείται;
8. Ανασκοπούνται τα νέα συστήματα και οι διεργασίες που αφορούν την επεξεργασία προσωπικών πληροφοριών προκειμένου να:
α) επιβεβαιώνεται ότι αυτά τα συστήματα ή οι διεργασίες αποτρέπουν όσο το δυνατόν περισσότερο την καταγραφή ανακριβών ή παρωχημένων προσωπικών πληροφοριών;
β) επιτρέπονται οι διορθώσεις σε ανακριβείς ή παρωχημένες προσωπικές πληροφορίες;
8.2.10 Διατήρηση και καταστροφή
8.2.10.1 Χρονοδιαγράμματα διατήρησης
1. Γίνεται παραπομπή σε χρονοδιαγράμματα διατήρησης για τον προσδιορισμό των χρονικών διαστημάτων διατήρησης προσωπικών πληροφοριών;
2. Τα χρονοδιαγράμματα:
α) περιλαμβάνουν όλα τα ελάχιστα χρονικά διαστήματα διατήρησης που απαιτούνται από το νόμο, καθώς και τα διαστήματα διατήρησης που καθορίζονται από τον οργανισμό;
β) διευκρινίζουν και τεκμηριώνουν την αιτιολόγηση και τη βάση των διαστημάτων διατήρησης;
3. Καταστρέφονται όλα τα αντίγραφα των προσωπικών πληροφοριών που δεν απαιτούνται πλέον από τον οργανισμό με αναφορά στις διαδικασίες καταστροφής οι οποίες διαχειρίζονται:
α) χρησιμοποιώντας εγκεκριμένες διεργασίες;
β) με επίπεδο ασφάλειας ανάλογο με την ευαισθησία των προσωπικών πληροφοριών;
γ) σύμφωνα με την αξιολόγηση διακινδύνευσης της ασφάλειας των πληροφοριών του οργανισμού;
4. Εφαρμόζονται και γνωστοποιούνται τα χρονοδιαγράμματα διατήρησης σε όλους τους σχετικούς εργαζόμενους;
5. Διασφαλίζει το ΣΔΠΔ (PIMS) την εφαρμογή και γνωστοποίηση των χρονοδιαγραμμάτων διατήρησης σε όλους τους σχετικούς εργαζόμενους;
6. Μεταφέρονται προσωπικές πληροφορίες για μακροπρόθεσμη διατήρηση;
7. Εάν ναι, εφαρμόζονται τα κατάλληλα τεχνικά και οργανωτικά μέτρα;
8.2.11 Παράμετροι ασφάλειας
8.2.11.1 Μέτρα ασφάλειας
1. Προσδιορίζονται τα κατάλληλα μέτρα ασφάλειας, λαμβάνοντας υπόψη τις τελευταίες εξελίξεις, το κόστος εφαρμογής και τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας των προσωπικών πληροφοριών;
8.2.11.2 Έλεγχοι ασφάλειας
1. Εφαρμόζει το ΣΔΠΔ (PIMS) τα κατάλληλα μέτρα ασφάλειας με τον καθορισμό και την εφαρμογή ελέγχων ασφάλειας, όπως ενδείκνυται:
α) στον τύπο των προσωπικών πληροφοριών που υποβάλλονται σε επεξεργασία;
β) στον κίνδυνο βλάβης ή αγωνίας για τα φυσικά πρόσωπα, εάν οι πληροφορίες έχουν υπονομευτεί;
γ) στον κίνδυνο λειτουργικής βλάβης και βλάβης της φήμης στον οργανισμό;
2. Όταν προσωπικές πληροφορίες υψηλού κινδύνου υποβάλλονται σε επεξεργασία, οι έλεγχοι ασφάλειας που καθορίζονται και εφαρμόζονται είναι κατάλληλοι για τους εκτιμώμενους κινδύνους;
8.2.11.3 Αποθήκευση και διαχείριση
1. Οι προσωπικές πληροφορίες αποθηκεύονται και διαχειρίζονται με ασφάλεια, με προφυλάξεις κατάλληλες για την εμπιστευτικότητα και την ευαισθησία τους;
2. Δίνεται ιδιαίτερη προσοχή στην αποθήκευση προσωπικών πληροφοριών σε αφαιρούμενα μέσα, σε φορητές συσκευές και σε συστήματα αποθήκευσης τρίτων;
8.2.11.4 Διαβίβαση

1. Διασφαλίζεται η διαβίβαση προσωπικών πληροφοριών με τα κατάλληλα μέσα, όπως καθορίζονται από τον οργανισμό, προκειμένου να διαφυλάσσονται οι πληροφορίες κατά τη διάρκεια της διαβίβασης;
8.2.11.5 Έλεγχοι πρόσβασης
1. Περιορίζεται η πρόσβαση σε εκείνους τους εργαζόμενους που απαιτούν τέτοια πρόσβαση ως μέρος του ρόλου τους;
2. Διευκρινίζεται στους εργαζόμενους ότι, όταν η πρόσβαση παρέχεται νόμιμα, αυτό ισχύει μόνο για λόγους εργασίας και ότι οι πληροφορίες θα είναι προσπελάσιμες μόνο για νόμιμους σκοπούς;
3. Υπάρχουν έλεγχοι πρόσβασης που αντανακλούν την ευαισθησία των πληροφοριών υψηλού κινδύνου;
4. Η πρόσβαση σε προσωπικές πληροφορίες παρακολουθείται και αξιολογείται σύμφωνα με την αξιολόγηση διακινδύνευσης της ασφάλειας των πληροφοριών του οργανισμού;
8.2.11.6 Αξιολογήσεις ασφάλειας
1. Οι αξιολογήσεις ασφάλειας διεξάγονται με συστηματικό τρόπο;
2. Καθορίζουν οι αξιολογήσεις κατά πόσον οι υφιστάμενοι έλεγχοι ασφάλειας είναι κατάλληλοι και διατυπώνουν οι αξιολογήσεις συστάσεις για βελτιώσεις;
3. Αυτές οι αξιολογήσεις λαμβάνουν υπόψη τον κίνδυνο ζημίας, βλάβης και/ή αγωνίας για τα φυσικά πρόσωπα σε περίπτωση παραβίασης της ασφάλειας;
8.2.11.7 Διαχείριση παραβιάσεων ασφάλειας
1. Το ΣΔΠΔ (PIMS):
α) αξιολογεί, διαχειρίζεται και τεκμηριώνει τις παραβιάσεις ασφάλειας που αφορούν προσωπικές πληροφορίες, συμπεριλαμβανομένων των διαδικασιών για τον μετριασμό της βλάβης που προκλήθηκε από τυχόν παραβίαση ασφάλειας;
β) γνωστοποιεί στην εποπτική αρχή τυχόν παραβιάσεις ασφάλειας που αφορούν προσωπικές πληροφορίες εντός 72 ωρών από τη στιγμή που αποκτάται γνώση της παραβίασης;
Οι γνωστοποιήσεις αυτές περιλαμβάνουν:
i) μια περιγραφή των προσωπικών πληροφοριών που εμπλέκονται;
ii) λεπτομέρειες των κατηγοριών των προσωπικών πληροφοριών και του κατά προσέγγιση αριθμού των επηρεαζόμενων αρχείων;
iii) τα στοιχεία επικοινωνίας του ΥΠΔ (DPO) ή άλλου σημείου επικοινωνίας εντός του οργανισμού;
iv) μια περιγραφή των ενδεχόμενων συνεπειών της παραβίασης;
v) μια περιγραφή των ληφθέντων ή των προτεινόμενων προς λήψη μέτρων για την αντιμετώπιση της παραβίασης και της άμβλυνσης ενδεχόμενων δυσμενών συνεπειών της;
γ) γνωστοποιεί χωρίς αδικαιολόγητη καθυστέρηση στα ενδιαφερόμενα φυσικά πρόσωπα:
i) την παραβίαση της ασφάλειας;
ii) τη φύση της παραβίασης;
iii) τυχόν συστάσεις για τις ενέργειές τους σχετικά με τον μετριασμό τυχόν δυσμενών κινδύνων;
δ) τεκμηριώνει κάθε παραβίαση ασφάλειας, συμπεριλαμβανομένης της αξιολόγησης του τρόπου με τον οποίο σημειώθηκε η παραβίαση, των διορθωτικών ενεργειών που έγιναν και της συμπερασμάτων που συνήχθησαν από την παραβίαση;
ε) λαμβάνει αποφάσεις σχετικά με το εάν μία παραβίαση ασφάλειας αναφέρεται ή όχι σε κάποια σχετική ρυθμιστική αρχή [π.χ. τη Βρετανική Αρχή Οικονομικής Συμπεριφοράς (FCA)];
στ) τηρεί αρχεία των τυχόν γνωστοποιήσεων που έχουν εκδοθεί;
8.2.11.8 Διαβίβαση προσωπικών πληροφοριών εκτός της ΕΕ
1. Διαβιβάζονται προσωπικές πληροφορίες εκτός της ΕΕ;
2. Εάν ναι, προστατεύονται τα δικαιώματα των φυσικών προσώπων:
α) κατά τον χρόνο της διαβίβασης, η χώρα ή το έδαφος έχει εκτιμηθεί από την Ευρωπαϊκή Επιτροπή ότι παρέχει επαρκή προστασία;
β) με τη συμπερίληψη στα συμβόλαια ειδικών όρων που διασφαλίζουν την προστασία των προσωπικών πληροφοριών και την επεξεργασία, π.χ. με τη χρήση, στήριξη ή πλήρη αποδοχή καθιερωμένων τυποποιημένων ρητρών ή υποδειγμάτων συμβάσεων;
γ) με την εφαρμογή εσωτερικών δεσμευτικών εταιρικών κανόνων (BCR), όταν η διαβίβαση γίνεται προς άλλη οντότητα εντός του ίδιου οργανισμού;
δ) με τη συμμόρφωση με εγκεκριμένο κώδικα δεοντολογίας ή εγκεκριμένο μηχανισμό πιστοποίησης από κοινού με δεσμευτικές και εκτελεστές υποχρεώσεις για τον οργανισμό του προορισμού;
ε) για τους δημόσιους φορείς, με τη συμμόρφωση με νομικά δεσμευτικό και εκτελεστό μέσο ή διοικητική ρύθμιση;

στ) με τη διαβίβαση σύμφωνα με εφαρμοστέα απόκλιση;

3. Η ανώτατη Διοίκηση και οι εργαζόμενοι που είναι υπεύθυνοι και υπόλογοι για τη συμμόρφωση με τις απαιτήσεις για την προστασία δεδομένων και τις ορθές πρακτικές εξετάζουν όλες τις νέες πρωτοβουλίες που αφορούν τη διαβίβαση προσωπικών πληροφοριών εκτός της ΕΕ;

4. Καθορίζει η εν λόγω ανασκόπηση εάν παρέχεται επαρκής προστασία για τέτοιου είδους διαβιβάσεις;

5. Οι εκτελούντες την επεξεργασία και οι τυχόν υπο-εκτελούντες την επεξεργασία που εδρεύουν εκτός της ΕΕ και επεξεργάζονται προσωπικές πληροφορίες για λογαριασμό του οργανισμού, λειτουργούν σύμφωνα με τους κατάλληλους συμβατικούς όρους; (π.χ. τυποποιημένες ρήτρες ή πρότυπα συμβάσεων, όπως αυτά που έχει εγκρίνει η Ευρωπαϊκή Επιτροπή για τη διασφάλιση επαρκούς προστασίας των προσωπικών πληροφοριών)

8.2.11.9 Γνωστοποίηση σε αιτήματα τρίτων

1. Οι τρίτοι προσκομίζουν αποδεικτικά στοιχεία σχετικά με:

α) το δικαίωμά τους να ζητούν αντίγραφο των καθορισμένων προσωπικών πληροφοριών;

β) όταν είναι αναγκαίο, την ταυτότητά τους;

2. Γίνεται έλεγχος για να διασφαλίζεται ότι υπάρχουν νομικοί λόγοι για τη γνωστοποίηση τα τυχόν πληροφοριών σε τρίτους;

3. Γνωστοποιούνται σε τρίτους μόνο οι ελάχιστες αναγκαίες προσωπικές πληροφορίες;

4. Τηρούνται αρχεία γνωστοποιήσεων προσωπικών πληροφοριών και διατηρούνται αυτά τα αρχεία ενήμερα;

5. Αποδεικνύουν τα εν λόγω αρχεία ότι η γνωστοποίηση ήταν νόμιμη;

6. Είναι ο οργανισμός σε θέση να παρακολουθεί πού γνωστοποιήθηκαν οι προσωπικές πληροφορίες;

8.2.11.10 Επεξεργασία πληροφοριών από υπεργολάβους

1. Όταν υποβάλλονται σε επεξεργασία προσωπικές πληροφορίες για λογαριασμό του οργανισμού από άλλον οργανισμό, διασφαλίζει το ΣΔΠΔ (PIMS) ότι:

α) επιλέγονται μόνο οι οργανισμοί που ενεργούν ως εκτελούντες την επεξεργασία οι οποίοι μπορούν να παρέχουν τεχνική, φυσική και οργανωτική ασφάλεια και που ανταποκρίνονται στις απαιτήσεις του οργανισμού για όλες τις προσωπικές πληροφορίες που επεξεργάζονται για λογαριασμό του οργανισμού;

β) πριν εμπλακεί ένας οργανισμός που ενεργεί ως εκτελών την επεξεργασία, διενεργείται με τη δέουσα επιμέλεια αξιολόγηση της κατάλληλης ασφάλειας και εάν κρίνεται αναγκαίο λόγω της φύσης των προσωπικών πληροφοριών που πρέπει να υποβληθούν σε επεξεργασία ή λόγω των ιδιαίτερων συνθηκών της επεξεργασίας, πραγματοποιείται έλεγχος των ρυθμίσεων ασφάλειας του οργανισμού που ενεργεί ως εκτελών την επεξεργασία πριν αυτός συνάψει τη σύμβαση;

γ) τηρείται η δέουσα επιμέλεια στον οργανισμό που ενεργεί ως εκτελών την επεξεργασία;

δ) αφού έχει επιλεγεί ο οργανισμός που ενεργεί ως εκτελών την επεξεργασία, ο οργανισμός δημιουργεί δεσμευτικό έγγραφο συμφωνητικό ή σύμβαση που:

i) ορίζει το αντικείμενο και τη διάρκεια της επεξεργασίας, τη φύση και τον σκοπό της επεξεργασίας, το είδος των προσωπικών πληροφοριών και τις κατηγορίες φυσικών προσώπων, καθώς και τις υποχρεώσεις και τα δικαιώματα του οργανισμού;

ii) ορίζει ότι ο οργανισμός που ενεργεί ως εκτελών την επεξεργασία πρέπει να επεξεργάζεται προσωπικές πληροφορίες μόνο με τεκμηριωμένες οδηγίες;

iii) ορίζει ότι ο οργανισμός που ενεργεί ως εκτελών την επεξεργασία πρέπει να ενημερώνει τον οργανισμό για κάθε νόμιμη απαίτηση πριν από την επεξεργασία;

iv) διασφαλίζει ότι οι εργαζόμενοι που είναι εξουσιοδοτημένοι να επεξεργάζονται τις προσωπικές πληροφορίες έχουν δεσμευτεί για εμπιστευτικότητα ή ότι έχουν την κατάλληλη νομική υποχρέωση εμπιστευτικότητας;

v) απαιτεί από τον οργανισμό που ενεργεί ως εκτελών την επεξεργασία να βοηθήσει τον οργανισμό να συμμορφωθεί με τα δικαιώματα των φυσικών προσώπων;

vi) καθορίζει τη συμμόρφωση με τις νομικές απαιτήσεις για τη γνωστοποίηση στον οργανισμό τυχόν παραβιάσεων της ασφάλειας χωρίς αδικαιολόγητη καθυστέρηση;

vii) απαιτεί από τον οργανισμό που ενεργεί ως εκτελών την επεξεργασία να παρέχει την κατάλληλη ασφάλεια για τις προσωπικές πληροφορίες που θα επεξεργάζεται;

viii) επιτρέπει τακτικούς ελέγχους των ρυθμίσεων ασφάλειας του οργανισμού που ενεργεί ως εκτελών την επεξεργασία κατά τη διάρκεια της περιόδου που ο οργανισμός ο οποίος ενεργεί ως εκτελών την επεξεργασία έχει πρόσβαση στις προσωπικές πληροφορίες;

ix) απαιτεί από τον οργανισμό που ενεργεί ως εκτελών την επεξεργασία να αποκτήσει την άδεια του οργανισμού να χρησιμοποιήσει και άλλους υπεργολάβους για να επεξεργαστεί τις προσωπικές πληροφορίες;

x) απαιτεί οι συμβάσεις με τους υπεργολάβους του οργανισμού που ενεργεί ως εκτελών την επεξεργασία, να απαιτούν από τους υπεργολάβους να συμμορφώνονται τουλάχιστον με τις ίδιες διατάξεις ασφάλειας και με άλλες διατάξεις όπως ο οργανισμός που ενεργεί ως εκτελών την επεξεργασία;
xi) απαιτεί οι συμβάσεις με τον οργανισμό που ενεργεί ως εκτελών την επεξεργασία (οι οποίες δεσμεύουν τυχόν υπεργολάβους) να διευκρινίζουν ότι, όταν λήξει η σύμβαση, οι σχετικές προσωπικές πληροφορίες είτε θα καταστραφούν είτε θα διαβιβαστούν στον οργανισμό ή σε άλλον οργανισμό που θα ενεργεί ως εκτελών την επεξεργασία όπως καθορίζεται από τον οργανισμό;
xii) απαιτεί από τον οργανισμό που ενεργεί ως εκτελών την επεξεργασία να θέσει στη διάθεση του οργανισμού αποδεικτικά στοιχεία συμμόρφωσης προς το συμφωνητικό/σύμβαση;
8.2.12 Δικαιώματα των φυσικών προσώπων
8.2.12.1 Απάντηση σε δικαιώματα
1. Υπάρχουν διαδικασίες που διασφαλίζουν ότι τα δικαιώματα των φυσικών προσώπων σε σχέση με τις προσωπικές τους πληροφορίες είναι σεβαστά και ότι τα αιτήματα για την άσκηση αυτών των δικαιωμάτων διεκπεραιώνονται χωρίς αδικαιολόγητη καθυστέρηση;
2. Αυτό διεκπεραιώνεται εντός ενός μηνός από την παραλαβή του αιτήματος από το φυσικό πρόσωπο;
3. Τα φυσικά πρόσωπα ενημερώνονται σε περίπτωση επέκτασης του χρονικού διαστήματος του ενός μηνός;
4. Σε περίπτωση που ο οργανισμός απαιτεί επέκταση του χρονικού διαστήματος του ενός μηνός, διασφαλίζεται ότι αυτή η παράταση δεν υπερβαίνει τους επιπλέον δύο μήνες;
5. Οι διαδικασίες περιλαμβάνουν εξέταση του ενδεχόμενου να ισχύουν τυχόν παρεκκλίσεις ή εξαιρέσεις;
8.2.12.2 Πρόσβαση στις πληροφορίες
1. Μπορεί το φυσικό πρόσωπο, να λαμβάνει επιβεβαίωση για το κατά πόσον ή όχι οι προσωπικές πληροφορίες που το αφορούν υφίστανται επεξεργασία;
2. Εάν συμβαίνει αυτό, μπορεί το φυσικό πρόσωπο να έχει πρόσβαση στις προσωπικές πληροφορίες, να λαμβάνει αντίγραφο των προσωπικών πληροφοριών και να λαμβάνει πληροφορίες για τα ακόλουθα:
α) τους σκοπούς της επεξεργασίας;
β) τις σχετικές κατηγορίες προσωπικών πληροφοριών;
γ) τους αποδέκτες ή τις κατηγορίες αποδεκτών στους οποίους κοινολογήθηκαν ή πρόκειται να κοινολογηθούν οι προσωπικές πληροφορίες, ιδίως τους αποδέκτες σε τρίτες χώρες ή διεθνείς οργανισμούς;
δ) εάν είναι δυνατόν, το χρονικό διάστημα για το οποίο θα αποθηκευτούν οι προσωπικές πληροφορίες ή, όταν αυτό είναι αδύνατο, τα κριτήρια που καθορίζουν το εν λόγω διάστημα;
ε) την ύπαρξη δικαιώματος υποβολής αιτήματος για διόρθωση ή διαγραφή προσωπικών πληροφοριών ή περιορισμό της επεξεργασίας των προσωπικών πληροφοριών που αφορά το φυσικό πρόσωπο ή δικαιώματος αντίταξης στην εν λόγω επεξεργασία;
στ) την ύπαρξη του δικαιώματος υποβολής καταγγελίας σε εποπτική αρχή;
ζ) όταν οι προσωπικές πληροφορίες δεν έχουν συλλεχθεί από το υποκείμενο των δεδομένων, κάθε διαθέσιμη πληροφορία σχετικά με την προέλευσή τους;
η) την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ και σημαντικών πληροφοριών σχετικά με τη λογική που ακολουθείται, καθώς και τη σημασία και τις συνέπειες της εν λόγω επεξεργασίας για το υποκείμενο των δεδομένων;
θ) όταν προσωπικές πληροφορίες διαβιβάζονται σε τρίτη χώρα ή σε διεθνή οργανισμό, ποιές είναι οι κατάλληλες εγγυήσεις που εφαρμόζονται;
8.2.12.3 Διόρθωση
1. Μπορεί το φυσικό πρόσωπο να απαιτήσει τη διόρθωση ανακριβών προσωπικών πληροφοριών που το αφορούν; (σύμφωνα με το εδάφιο 8.2.9 του προτύπου για την «ακρίβεια»)
2. Είναι αυτό διαθέσιμο στο φυσικό πρόσωπο χωρίς αδικαιολόγητη καθυστέρηση;
3. Οι εν λόγω διαδικασίες για διόρθωση επιτρέπουν στο φυσικό πρόσωπο να απαιτήσει τη συμπλήρωση ελλιπών προσωπικών πληροφοριών;
8.2.12.4 Διαγραφή
1. Διεκπεραιώνονται κατάλληλα τα αιτήματα φυσικών προσώπων σύμφωνα με την αρχή «δικαίωμα διαγραφής»;

2.	Μπορεί το φυσικό πρόσωπο να ασκήσει το δικαίωμά του να ζητήσει τη διαγραφή των προσωπικών του πληροφοριών χωρίς αδικαιολόγητη καθυστέρηση όταν:
	α) οι προσωπικές πληροφορίες δεν είναι πλέον απαραίτητες σε σχέση με τους σκοπούς για τους οποίους συλλέχθηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία;
	β) το φυσικό πρόσωπο ανακαλεί τη συγκατάθεση επί της οποίας βασίστηκε η επεξεργασία και δεν υπάρχει άλλη νομική βάση για τη συνέχιση της επεξεργασίας των πληροφοριών;
	γ) το φυσικό πρόσωπο έχει αντιταχθεί στην εν λόγω επεξεργασία και δεν υπάρχουν επιτακτικοί και νόμιμοι λόγοι για την επεξεργασία ή το φυσικό πρόσωπο έχει αντιταχθεί στην εμπορική προώθηση;
	δ) οι προσωπικές πληροφορίες υποβλήθηκαν σε επεξεργασία παράνομα;
	ε) οι προσωπικές πληροφορίες πρέπει να διαγραφούν ώστε να τηρηθεί νομική υποχρέωση;
	στ) οι προσωπικές πληροφορίες έχουν συλλεχθεί για την προσφορά υπηρεσιών της κοινωνίας των πληροφοριών;
3.	Όταν οι πληροφορίες έχουν δημοσιοποιηθεί, λαμβάνονται τα κατάλληλα μέτρα για την ενημέρωση άλλων οργανισμών που ενδέχεται να επεξεργάζονται τις προσωπικές πληροφορίες των οποίων τη διαγραφή έχει ζητήσει το φυσικό πρόσωπο;
8.2.12.5	**Περιορισμός της επεξεργασίας**
1.	Έχει το φυσικό πρόσωπο το δικαίωμα να εξασφαλίζει τον περιορισμό της επεξεργασίας των προσωπικών πληροφοριών του όταν:
	α) η ακρίβεια των προσωπικών πληροφοριών αμφισβητείται από το φυσικό πρόσωπο, για χρονικό διάστημα που επιτρέπει στον οργανισμό να επαληθεύσει την ακρίβεια των προσωπικών πληροφοριών;
	β) η επεξεργασία είναι παράνομη και το φυσικό πρόσωπο αντιτάσσεται στη διαγραφή των προσωπικών πληροφοριών και ζητεί, αντ' αυτής, τον περιορισμό της χρήσης τους;
	γ) ο οργανισμός δεν χρειάζεται πλέον τις προσωπικές πληροφορίες για τους σκοπούς της επεξεργασίας, αλλά οι προσωπικές πληροφορίες αυτές απαιτούνται από το φυσικό πρόσωπο για τη θεμελίωση, την άσκηση ή την υποστήριξη νομικών αξιώσεων;
	δ) το φυσικό πρόσωπο έχει αντιρρήσεις για την επεξεργασία, εν αναμονή της επαλήθευσης του κατά πόσον οι νόμιμοι λόγοι του οργανισμού υπερισχύουν έναντι των λόγων του φυσικού προσώπου;
2.	Όταν ένας περιορισμός πρόκειται να αρθεί, το φυσικό πρόσωπο ενημερώνεται πριν από αυτό;
8.2.12.6	**Φορητότητα δεδομένων**
1.	Όταν το φυσικό πρόσωπο έχει δικαίωμα στη φορητότητα δεδομένων και η επεξεργασία των πληροφοριών διενεργείται με αυτοματοποιημένα μέσα, το φυσικό πρόσωπο μπορεί να διαβιβάζει τα εν λόγω δεδομένα σε αυτούς ή σε άλλον οργανισμό που αυτοί ορίζουν;
2.	Είναι αυτή η υπηρεσία δωρεάν και παρέχονται οι προσωπικές πληροφορίες σε δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα μορφότυπο;
8.2.12.7	**Αντιρρήσεις**
1.	Υπάρχουν διαδικασίες για την εξέταση και απάντηση σε αιτήματα φυσικού προσώπου που αντιτάσσεται στην επεξεργασία προσωπικών πληροφοριών;
2.	Όταν ένα φυσικό πρόσωπο αντιτάσσεται στην επεξεργασία προσωπικών πληροφοριών για σκοπούς απευθείας εμπορικής προώθησης, παύει για το φυσικό αυτό πρόσωπο η επεξεργασία;
8.2.12.8	**Αυτοματοποιημένη λήψη αποφάσεων, περιλαμβανομένης της κατάρτισης προφίλ**
1.	Υπάρχουν διαδικασίες που προσδιορίζουν πότε η επεξεργασία των προσωπικών πληροφοριών απορρέει από την αυτοματοποιημένη λήψη αποφάσεων; (συμπεριλαμβανομένης της κατάρτισης προφίλ, η οποία μπορεί να επηρεάσει σημαντικά ένα φυσικό πρόσωπο)
2.	Το ΣΔΠΔ (PIMS) διασφαλίζει ότι κάθε αυτοματοποιημένη απόφαση μπορεί να περιλαμβάνει ανθρώπινη παρέμβαση όταν αυτό ζητηθεί από το φυσικό πρόσωπο;
8.2.12.9	**Παράπονα και προσφυγές**
1.	Υπάρχει μια διαδικασία παραπόνων που να διασφαλίζει ότι τα παράπονα σχετικά με την επεξεργασία των προσωπικών πληροφοριών διαχειρίζονται σωστά;
2.	Περιλαμβάνει αυτό διαδικασίες για την εξέταση των προσφυγών φυσικών προσώπων σχετικά με τον τρόπο που αντιμετωπιστήκανε τα παράπονά τους;
8.2.13	**Συντήρηση**
1.	Συντηρούνται οι διαδικασίες και τα τεχνολογικά εξαρτήματα έτσι ώστε να διασφαλίζεται η σωστή και κατάλληλη λειτουργία τους;
2.	Είναι αυτή η συντήρηση προγραμματισμένη και εκτελείται σε τακτική, προγραμματισμένη βάση;
3.	Είναι αυτή η συντήρηση μέρος των διαδικασιών;

9 Αξιολόγηση επιδόσεων
9.1 Παρακολούθηση, μέτρηση, ανάλυση και αξιολόγηση
1. Ο οργανισμός έχει προσδιορίσει:
α) τί χρειάζεται να παρακολουθείται και να μετρείται;
β) τις μεθόδους παρακολούθησης, μέτρησης, ανάλυσης και αξιολόγησης, όπου έχει εφαρμογή, για να διασφαλίζονται έγκυρα αποτελέσματα;
γ) πότε πρέπει να διενεργείται η παρακολούθηση και η μέτρηση;
δ) πότε πρέπει να αναλύονται και να αξιολογούνται τα αποτελέσματα παρακολούθησης και μέτρησης;
2. Τηρεί ο οργανισμός κατάλληλες τεκμηριωμένες πληροφορίες;
3. Ο οργανισμός αξιολογεί τις επιδόσεις και την αποτελεσματικότητα του ΣΔΠΔ (PIMS);
9.2 Εσωτερική επιθεώρηση
1. Διεξάγει ο οργανισμός σε προγραμματισμένα χρονικά διαστήματα εσωτερικές επιθεωρήσεις, και όταν πραγματοποιούνται σημαντικές αλλαγές, ώστε να παρέχονται πληροφορίες σχετικά με το κατά πόσον το ΣΔΠΔ (PIMS):
α) συμμορφώνεται:
i) με τις απαιτήσεις του ίδιου του οργανισμού για το ΣΔΠΔ (PIMS) του;
ii) με τις απαιτήσεις του Βρετανικού Προτύπου 10012:2017;
β) εφαρμόζεται αποτελεσματικά και διατηρείται ενήμερο;
2. Ο οργανισμός:
α) σχεδιάζει, καθιερώνει, υλοποιεί και διατηρεί ενήμερο πρόγραμμα επιθεώρησης;
β) καθορίζει τα κριτήρια και το πεδίο εφαρμογής κάθε επιθεώρησης;
γ) επιλέγει επιθεωρητές και διενεργεί επιθεωρήσεις για να διασφαλίζεται η αντικειμενικότητα και η αμεροληψία της επιθεώρησης;
δ) διασφαλίζει ότι τα αποτελέσματα των επιθεωρήσεων αναφέρονται στη σχετική βαθμίδα Διοίκησης;
ε) τηρεί τεκμηριωμένες πληροφορίες ως τεκμήριο της υλοποίησης του προγράμματος επιθεώρησης και των αποτελεσμάτων επιθεώρησης;
2. Το πρόγραμμα επιθεώρησης περιλαμβάνει επεξεργασία προσωπικών πληροφοριών υψηλού κινδύνου;
3. Το πρόγραμμα επιθεώρησης περιλαμβάνει επεξεργασία προσωπικών πληροφοριών από υπεργολάβους;
4. Οι εκθέσεις επιθεώρησης περιγράφουν κάθε σημαντική απόκκλιση από την πολιτική του ΣΔΠΔ (PIMS) και/ή οι καθιερωμένες διαδικασίες;
5. Αυτές οι εκθέσεις επιθεώρησης παρέχονται στη Διοίκηση;
6. Οι εκθέσεις επιθεώρησης προσδιορίζουν παραμέτρους σχετικά με την τεχνολογία ή διεργασίες που θα μπορούσαν να επηρεάσουν τη συμμόρφωση με την πολιτική του ΣΔΠΔ (PIMS);
9.3 Ανασκόπηση από τη Διοίκηση
1. Η ανώτατη Διοίκηση ανασκοπεί το ΣΔΠΔ (PIMS) του οργανισμού σε προγραμματισμένα χρονικά διαστήματα, ώστε να διασφαλίζεται:
α) η συνεχιζόμενη καταλληλότητα;
β) η επάρκεια;
γ) η αποτελεσματικότητα;
2. Η ανασκόπηση από τη Διοίκηση λαμβάνει υπόψη:
α) την πρόοδο υλοποίησης ενεργειών από προηγούμενες ανασκοπήσεις της Διοίκησης;
β) τις αλλαγές σε εξωτερικές και εσωτερικές παραμέτρους που αφορούν το ΣΔΠΔ (PIMS);
γ) τις πληροφορίες σχετικά με τις επιδόσεις του ΣΔΠΔ (PIMS), συμπεριλαμβανομένων και των τάσεων:
i) των μη συμμορφώσεων και των διορθωτικών ενεργειών;
ii) των αποτελεσμάτων της παρακολούθησης και μέτρησης;
iii) των αποτελεσμάτων επιθεώρησης;
δ) τις ευκαιρίες για συνεχή βελτίωση;
ε) την αναπληροφόρηση από τους χρήστες του ΣΔΠΔ (PIMS);
στ) τους προσδιορισμένους κινδύνους που κλιμακώνονται από τους εργαζομένους;
ζ) αρχεία διαδικαστικών ανασκοπήσεων;

	η) αποτελέσματα αναβαθμίσεων της τεχνολογίας και/ή αντικαταστάσεων;
	θ) επίσημα αιτήματα για αξιολόγηση από ρυθμιστικούς φορείς;
	ι) τον χειρισμό παραπόνων;
	ια) παραβιάσεις ασφάλειας/συμβάντα ασφάλειας που έχουν σημειωθεί;
3.	Τα αποτελέσματα της ανασκόπησης από τη Διοίκηση περιλαμβάνουν αποφάσεις που σχετίζονται με τις ευκαιρίες συνεχούς βελτίωσης και οποιαδήποτε ανάγκη για αλλαγές στο ΣΔΠΔ (PIMS); (π.χ. με τον προσδιορισμό τροποποιήσεων στην πολιτική, στις διεργασίες και/ή στην τεχνολογία του ΣΔΠΔ (PIMS) που ενδέχεται να επηρεάσουν τη συμμόρφωση)
4.	Ο οργανισμός τηρεί τεκμηριωμένες πληροφορίες ως αποδεικτικό στοιχείο των αποτελεσμάτων των ανασκοπήσεων από τη Διοίκηση;
5.	Όταν εφαρμόζονται σημαντικές αλλαγές στο ΣΔΠΔ (PIMS), η επιθεώρηση ολοκληρώνεται το συντομότερο δυνατό μετά την εφαρμογή;
10	**Βελτίωση**
10.1	**Μη συμμόρφωση και διορθωτικές ενέργειες**
1.	Ο οργανισμός:
	α) ανταποκρίνεται στη μη συμμόρφωση και, όπως έχει εφαρμογή:
	i) ενεργεί για να την ελέγχει και να τη διορθώνει;
	ii) αντιμετωπίζει τις συνέπειες;
	β) αξιολογεί την ανάγκη για ενέργειες εξάλειψης των αιτίων της μη συμμόρφωσης, ώστε να μην επανεμφανίζεται ή να μην εμφανίζεται αλλού, μέσω:
	i) της ανασκόπησης της μη συμμόρφωσης;
	ii) του προσδιορισμού των αιτιών της μη συμμόρφωσης;
	iii) του προσδιορισμού κατά πόσον υφίστανται παρόμοιες μη συμμορφώσεις;
	γ) υλοποιεί οποιαδήποτε αναγκαία ενέργεια;
	δ) ανασκοπεί την αποτελεσματικότητα των διορθωτικών ενεργειών που υλοποιήθηκαν;
	ε) προβαίνει σε αλλαγές στο ΣΔΠΔ (PIMS), εφόσον είναι απαραίτητο;
2.	Είναι οι διορθωτικές ενέργειες κατάλληλες ανάλογα με τις επιπτώσεις των μη συμμορφώσεων;
3.	Η αξιολόγηση της διακινδύνευσης διεξάγεται σε τακτά χρονικά διαστήματα;
4.	Αξιολογούνται όλοι οι νέοι κίνδυνοι που έχουν προσδιοριστεί για τις προσωπικές πληροφορίες (είτε εντός του οργανισμού είτε από την ευρύτερη εθνική προοπτική), χρησιμοποιώντας προληπτικές διαδικασίες όπως οι εκτιμήσεις αντικτύπου για την προστασία της ιδιωτικής ζωής (PIAs);
5.	Όλες οι προτεινόμενες αλλαγές και/ή βελτιώσεις αξιολογούνται πριν από την εφαρμογή, προκειμένου να διασφαλίζεται ότι πληρούνται οι απαιτήσεις της πολιτικής του ΣΔΠΔ (PIMS);
6.	Οι αλλαγές που θα μπορούσαν να επηρεάσουν τη δυνατότητα απόδειξης της συμμόρφωσης με τις απαιτήσεις για την προστασία δεδομένων και τις ορθές πρακτικές (όπως η μετατροπή προσωπικών πληροφοριών σε νέα μορφή αρχείου αποθήκευσης) ανασκοπούνται για να καθορίζεται το κατά πόσον επηρεάζουν τη συμμόρφωση;
7.	Οι αλλαγές που προκύπτουν από προληπτικές και διορθωτικές ενέργειες τεκμηριώνονται και διατηρούνται σύμφωνα με χρονοδιάγραμμα διατήρησης;
8.	Ο οργανισμός διατηρεί τεκμηριωμένες πληροφορίες ως αποδεικτικά στοιχεία για:
	α) τη φύση των μη συμμορφώσεων και την υλοποίηση τυχόν ενεργειών που ακολούθησαν;
	β) τα αποτελέσματα οποιασδήποτε διορθωτικής ενέργειας;
10.2	**Προληπτικές ενέργειες**
1.	Ο οργανισμός λαμβάνει μέτρα έναντι ενδεχόμενων μη συμμορφώσεων με σκοπό να αποφευχθεί η εμφάνισή τους;
2.	Έχει καθιερωθεί διαδικασία για:
	α) τον προσδιορισμό δυνητικών μη συμμορφώσεων και των αιτίων τους;
	β) τον καθορισμό και την εφαρμογή τυχόν αναγκαίων προληπτικών μέτρων;
	γ) την καταγραφή των αποτελεσμάτων και της ανασκόπησης των ενεργειών που υλοποιήθηκαν;
	δ) τον προσδιορισμό των μεταβληθέντων κινδύνων;
	ε) τη διασφάλιση ότι ενημερώνονται όλοι όσοι πρέπει να γνωρίζουν, για τη δυνητική μη συμμόρφωση και τις προληπτικές ενέργειες που εφαρμόζονται;
10.3	**Συνεχής βελτίωση**

1. Ο οργανισμός βελτιώνει συνεχώς την καταλληλότητα, την επάρκεια και την αποτελεσματικότητα του ΣΔΠΔ (PIMS) μέσω των αποτελεσμάτων της επιθεώρησης, των προληπτικών και διορθωτικών ενεργειών και της ανασκόπησης από τη Διοίκηση;
2. Τα παράπονα, οι παραβιάσεις της ασφάλειας, τα αιτήματα πρόσβασης του υποκειμένου των δεδομένων, οι τεχνολογικές πρόοδοι και άλλες παράμετροι χρησιμοποιούνται επικουρικά για τη βελτίωση της αποτελεσματικότητας του ΣΔΠΔ (PIMS);

Βιβλιογραφία

- Antoņina Jemeļjanenko, 2018, 'Impact of EU general data protection regulation on the management of education', University of Latvia, *Proceedings of the International Scientific Conference of Daugavpils University / Daugavpils Universitates Starptautiskas Zinatniskas Konferences Materiali*. 2018, Issue 60, p169-177. 9p.
- Bandyopadhyay, Soumava, Bandyopadhyay, Kakoli, 2018, 'The European General Data Protection Regulation and Competitiveness of Firms'. Source: *Competition Forum 2018*, Vol. 16 Issue 1, p50 6p
- BÂRSAN, Maria-Magdalena, 2018, 'A partial overview of the data subjects' control over their personal data under the general data protection regulation'. Source: *Bulletin of the Transilvania University of Brasov. Series VII: Social Sciences. Law.* 2018, Vol. 11 Issue 2, p129-134. 6p.
- Bennett, Colin J.; Chun, Soon Ae; Adam, Nabil R.; Noveck, Beth, 2018, 'The European General Data Protection Regulation: An instrument for the globalization of privacy standards?' *The International Journal of Government & Democracy in the Information Age. 2018*, Vol. 23 Issue 2, p239-246. 8p
- Brook, David, 2018, 'GDPR puts vendor contracts in the security spotlight', Affiliation: Turnstone Services, Source: *In Computer Fraud & Security April 2018* 2018(4):5-7, Publisher: Elsevier Ltd
- Calder, Alan, 2016, 'EU GDPR: A Pocket Guide', Publication Information: Ely*: IT Governance Publishing.*
- Dove, Edward S., 2018, 'The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era', *Journal of Law, Medicine & Ethics*. Winter2018, Vol. 46 Issue 4, p1013-1030. 18p. 1 Chart.
- Ducich, Stefan, Fischer, Jordan L., 2018, 'The General Data Protection Regulation: What U.S.-Based Companies Need to Know', Source: *74 Bus. Law. 205 (2018-2019) / Business Lawyer, Vol. 74, Issue 74* (Winter 2018-2019), pp. 205-216, Publication Year: 2018
- Hertza, Vlad A., 2018, 'Fighting Unfair Classifications in Credit Reporting: Should the United States Adopt GDPR-Inspired Rights in Regulating Consumer Credit', Source: *93 N.Y.U. L. Rev. 1707 (2018) / New York University Law Review, Vol. 93, Issue 6* (December 2018), pp. 1707-1741 Publication Year: 2018

- Keller, Daphne, 2018, 'The Right Tools: Europe's Intermediary Liability Laws and the EU 2016 General Data Protection Regulation', Source: *33 Berkeley Tech. L.J. 287 (2018) / Berkeley Technology Law Journal, Vol. 33, Issue 1* pp. 287-364 Publication Year: 2018
- Lievens, Eva, Verdoodt, Valerie, 2018 'Looking for needles in a haystack: Key issues affecting children's rights in the General Data Protection Regulation.', *Computer Law & Security Review*. Apr2018, Vol. 34 Issue 2, p269-278. 10p.,
- Ljungholm, Doina Popescu, 2018, 'Regulation of automated individual decision-making and artificially intelligent algorithmic systems: is the GDPR a powerful enough mechanism to protect data subjects?' Source: *Analysis and Metaphysics. Annual, 2018*, Vol. 17, p116, 6 p. Publisher Information: Addleton Academic Publishers, Publication Year: 2018
- Lopes, Isabel Maria Guarda, Teresa, Oliveira, Pedro, 2019, 'How ISO 27001 Can Help Achieve GDPR Compliance' Source: *2019 14th Iberian Conference on Information Systems and Technologies (CISTI) Information Systems and Technologies (CISTI)*, 2019 14th Iberian Conference on. :1-6 Jun, 2019
- Maja Gligora Marković, Sandra Debeljak, Nikola Kadoić, 2019, 'Preparing Students for the Era of the General Data Protection Regulation (GDPR)', *TEM Journal. Volume 8, Issue 1*, Pages 150-156, ISSN 2217-8309, DOI: 10.18421/TEM81-21, February 2019, ,
- Membrey, David Mitchels, Barbara, 2019, 'Demystifying the general data protection regulation (gdpr): some of the issues relevant to the counselling professions.' Source: *Healthcare Counselling & Psychotherapy Journal. Jan2019*, Vol. 19 Issue 1, p16-21. 6p
- Mraznica Erne, 2017, 'GDPR: A new challenge for personal data protection', Source: *Bankarstvo, Vol 46, Iss 4*, Pp 166-177 (2017).
- Mraznica Erne., 2017, 'GDPR: A new challenge for personal data protection', *Academic Journal, In: Bankarstvo, Vol 46, Iss 4,* Pp 166-177 (2017); Association of Serbian Banks, 2017. Database: Directory of Open Access Journals
- Novak, Alison N., Vilceanu, M. Olguta, 2019, 'The internet is not pleased: twitter and the 2017 Equifax data breach', Source: *Communication Review. Jul-Sep2019*, Vol. 22 Issue 3, p196-221. 26p. 3 Chart
- Orel A; Marand, Bernik I., 2018, 'GDPR and Health Personal Data; Tricks and Traps of Compliance.', Source: *Studies In Health Technology And Informatics [Stud Health Technol Inform] 2018*; Vol. 255, pp. 155-159.Publication Type: Journal Article; Review
- Reetz, Margaret, 2019, 'GDPR: Does Coverage Exist for Fines and Penalties for Noncompliance?' Source: *TortSource. Spring2019, Vol. 21* Issue 3, p8-10. 3p
- Schildhaus, Aaron, 2018, 'EU's General Data Protection Regulation (GDPR): Key Provisions and Best Practices.' *International Law News*, 00470813, Winter2018, Vol. 46, Issue 2

- Štarchoň, Peter, Pikulík, Tomáš, 2019, 'GDPR principles in Data protection encourage pseudonymization through most popular and full-personalized devices - mobile phones', Affiliation: Faculty of Management, Comenius University in Bratislava, Odbojárov 10, 820 05 Bratislava 25, Slovakia, Source: *In The 10th International Conference on Ambient Systems, Networks and Technologies (ANT 2019) / The 2nd International Conference on Emerging Data and Industry 4.0 (EDI40 2019)* / Affiliated Workshops, Procedia Computer Science 2019 151:303-312
- Sydekum, Ralf, 2018, 'Can consumers bank on financial services being secure with GDPR?' Affiliation: F5 Networks, Source: *In Computer Fraud & Security June 2018* 2018(6):11-13, Publisher: Elsevier Ltd
- Tombs, Ken, 2019, 'GDPR and global data privacy - The future', *IQ: The RIM Quarterly*, Date: May 1, 2019
- Wagner, Julian, 2018, 'The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection?' Source: *International Data Privacy Law.* Nov 2018, Vol. 8 Issue 4, p318, 20 p., Publisher Information: Oxford University Press, Publication Year: 2018
- Wilkinson, Gerard, 2018, 'General Data Protection Regulation: No silver bullet for small and medium-sized enterprises.' Source: *Journal of Payments Strategy & Systems*. Summer2018, Vol. 12 Issue 2, p139-149. 11p
- British Standards Institution, (2017). Personal Information Management System. (BS Standard Number 10012)
- International Organization for Standardization. (2015). Quality management systems — Requirements (ISO Standard No. 9001),
- International Organization for Standardization. (2013). Information technology — Security techniques — Information security management systems — Requirements (ISO Standard No. 27001)
- EUROLEX, 2016, Κανονισμός 2016/679 του Ευρωπαϊκού Κοινοβουλίου, available from: < https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32016R0679>
- Σύνδεσμος Επιχειρήσεων και Βιομηχανιών - ΣΕΒ, Ο νέος Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR). Εφαρμογή και προκλήσεις για τις επιχειρήσεις στην εποχή της ψηφιοποίησης, Οκτώβριος 2018

Websites

- Dutton Julia, 2019, GDPR compliance: why you should consider BS 10012 certification, available from: <https://www.itgovernance.co.uk/blog/gdpr-compliance-why-you-should-consider-bs-10012-certification>
- Mullane Michael A., 2018, *International Standards provide toolkit for GDPR compliance*, available from: <https://iecetech.org/index.php/Technology-Focus/2018-02/International-Standards-provide-toolkit-for-GDPR-compliance>
- Κόζιαρης Χρίστος, 2018, *Η Σχέση του ISO 27001 με τον GDPR* available from: <https://www.epixeiro.gr/article/76053>
- World Internet Users and 2019 Population Stats, 2019, available from: <https://www.internetworldstats.com/stats.htm >
- How ISO 27001 can help you comply with the GDPR, available from: <https://www.itgovernance.co.uk/gdpr-and-iso-27001>
- Personal information management with GDPR., available from: <https://www.lr.org/en-gb/gdpr/bs-10012/>
- The General Data Protection Regulation (GDPR) in the Context of ISO 27001, 2018, available from: <https://www.pegasuslegalregister.com/2019/01/18/general-data-protection-regulation/>
- BS 10012 Personal Information Management System, available from: <https://www.bsigroup.com/en-GB/BS-10012-Personal-information-management/>
- Αρχή Προστασίας Δεδομένων, available from: <https://www.dpa.gr>
- Commission Nationale de l'Informatique et des Libertés - CNIL (Εθνικής Επιτροπής Πληροφορικής και Ελευθεριών, available from: < https://www.cnil.fr/en/home >