ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ (Π.Μ.Σ.)
ΤΕΧΝΟΟΙΚΟΝΟΜΙΚΗ ΔΙΟΙΚΗΣΗ ΚΑΙ ΑΣΦΑΛΕΙΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Μεταπτυχιακή διπλωματική εργασία

«ΕΠΙΧΕΙΡΗΣΙΑΚΕΣ ΕΠΙΠΤΩΣΕΙΣ ΤΟΥ ΝΕΟΥ ΓΕΝΙΚΟΥ ΚΑΝΟΝΙΣΜΟΥ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ - GENERAL DATA PROTECTION REGULATION 2016/697 (ΓΚΠΔ/GDPR)»

Θεοδωράκης Ευάγγελος

Επιβλέπων
Δρ. Κανέλλος Λεωνίδας

Πειραιάς, Φεβρουάριος 2018

Η σελίδα αυτή αφήνεται σκόπιμα κενή

UNIVERSITY OF PIRAEUS

DEPARTMENT OF DIGITAL SYSTEMS

POSTGRADUATE STUDIES PROGRAM

TECHNO-ECONOMIC MANAGEMENT & SECURITY OF DIGITAL SYSTEMS

Master Dissertation

«OPERATIONAL IMPACT OF THE NEW GENERAL DATA PROTECTION REGULATION 2016/679 (GDPR) »

Theodorakis Evangelos

Supervisor

Dr. Kanellos Leonidas

Piraeus, February 2018

Ευχαριστίες

Η εργασία αυτή είναι απόσταγμα εμπειριών και γνώσεων που έχω διδαχθεί εντός και εκτός αιθουσών διδασκαλίας τόσο αυτού όσο και άλλων προγραμμάτων σπουδών. Αισθάνομαι την ανάγκη να εκφράσω τις θερμές μου ευχαριστίες σε αυτούς που η συμβολή και η συμπαράσταση τους ήταν πολύτιμη και καθοριστική στην εκπόνηση αυτής της διπλωματικής εργασίας.

Ξεκινώντας, να ευχαριστήσω τον καθηγητή και επιβλέποντα κ. Κανέλλο Λεωνίδα για την καθοδήγηση του με κατάλληλες επιστημονικές πρακτικές και άμεσες συμβουλές επί της οργάνωσης, της δομής και του περιεχομένου της παρούσας εργασίας.

Κρίνω απαραίτητο να εκφράσω εκ των προτέρων τις ευχαριστίες μου στα υπόλοιπα μέλη της εξεταστικής επιτροπής κ. Ρούσκα Άγγελο και κ. Τσαγκάρη Κωσταντίνο για τη συμβολή τους στην αξιολόγηση της εργασίας αυτής.

Ευχαριστώ επίσης τους συναδέλφους και φίλους του μεταπτυχιακού προγράμματος για την αλληλοσυμπαράσταση και υποστήριξη καθ' όλη τη διάρκεια της κοινής μας εκπαιδευτικής εμπειρίας.

Δεν μπορώ να παραλείψω να αναφερθώ στους ανθρώπους που ήταν κοντά μου με κατανόηση ανοχή και υπομονή σε όλο το διάστημα εκπόνησης της διπλωματικής μου εργασίας. Ιδιαιτέρως ευχαριστώ τον Μπάμπη και την Ευγενία που με την έμπρακτη υποστήριξη τους, τις επισημάνσεις και τις παροτρύνσεις τους, με ενθάρρυναν καθημερινά συμβάλλοντας με ξεχωριστό τρόπο στην ολοκλήρωση της συγγραφής.

Το ευχαριστώ προς την οικογένεια μου δεν μπορεί επίσης να λείπει από εδώ. Τους ευγνωμονώ για τα διδάγματα, την υπομονή και υποστήριξη τους στέκοντας δίπλα μου σε κάθε μου βήμα, δίνοντας μου ελπίδα και δύναμη να συνεχίσω για το καλύτερο.

Κλείνοντας, ευχαριστώ και ευγνωμονώ τους, για λίγο ή για πολύ, συνοδοιπόρους στο μονοπάτι που λέγεται ζωή...

Πειραιάς, Φεβρουάριος 2018

Ευάγγελος Θεοδωράκης

Η σελίδα αυτή αφήνεται σκόπιμα κενή

…σε όλα αυτά που

συνθέτουν το

« Είμαι » …

Περιεχόμενα

Κατάλογος πινάκων

Κατάλογος διαγραμμάτων

Περίληψη

Η παρούσα εργασία πραγματοποιήθηκε στο πλαίσιο συγγραφής της διπλωματικής εργασίας του προγράμματος μεταπτυχιακών σπουδών «Τεχνοοικονομική Διοίκηση και Ασφάλεια Ψηφιακών Συστημάτων» του τμήματος Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιώς. Το θέμα της διπλωματικής είναι: «Επιχειρησιακές επιπτώσεις του νέου Γενικού Κανονισμού Προστασίας Δεδομένων - General Data Protection Regulation 2016/679 (ΓΚΠΔ/GDPR)». Ο Ευρωπαϊκός κανονισμός είναι μια νομική πράξη της Ευρωπαϊκής Ένωσης που είναι δεσμευτική ως προς όλα τα μέρη του και ισχύει σε όλες τις χώρες μέλη της Ευρωπαϊκής Ένωσης. Ο ΓΚΠΔ/GDPR αφορά την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και την ελεύθερη κυκλοφορία των δεδομένων αυτών και πρόκειται να αντικαταστήσει την Οδηγία του Ευρωπαϊκού Κοινοβουλίου 95/46/ΕΚ (24/10/1995) «για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών». Ο ΓΚΠΔ έχει κάποια χαρακτηριστικά Οδηγίας στο μέτρο που επιτρέπει στα κράτη μέλη εθνικές ρυθμίσεις για ορισμένες περιπτώσεις, όπως π.χ. για την ελάχιστη ηλικία συναίνεσης των ανηλίκων (που τίθεται στα 15 χρόνια στο ελληνικό νομοσχέδιο που τέθηκε σε διαβούλευση και στα 13 χρόνια από το αντίστοιχο κυπριακό που θα δημοσιοποιηθεί προσεχώς).

Η ψήφιση του ΓΚΠΔ/GDPR έγινε στις 27 Απριλίου 2016 και η εφαρμογή του θα γίνει στις 25 Μαΐου 2018. Οι επιχειρήσεις - οργανισμοί θα πρέπει να συμμορφωθούν μέχρι την ημερομηνία εφαρμογής του κανονισμού. Στην εργασία αυτή μελετήθηκε η δημιουργία πρακτικού οδηγού, βήμα προς βήμα, συμμόρφωσης ενός οργανισμού με το νέο κανονισμό. Μέσα σε αυτήν αναλύεται η μεθοδολογία που ακολουθήθηκε για την δόμηση του οδηγού και η παρουσίαση αυτού.

Πιο συγκεκριμένα, στο πρώτο κεφάλαιο, γίνεται συνοπτική αναφορά στο περιεχόμενο του ΓΚΠΔ/GDPR. Δίνεται μια περιγραφή του νομικού πλαισίου που καθορίζει τους κανόνες για όλους τους εμπλεκομένους. Αναλύονται οι αρμοδιότητες, τα δικαιώματα και οι υποχρεώσεις του καθενός.
Στη συνέχεια, στο δεύτερο κεφάλαιο, παρουσιάζεται το πρακτικό μέρος της παρούσας εργασίας. Εδώ περιλαμβάνεται η μεθοδολογία δημιουργίας του οδηγού. Αναλύονται τα στάδια που οδήγησαν στην τελική μορφή του οδηγού και τα εργαλεία που δημιουργήθηκαν για αυτόν.

Στο επόμενο κεφάλαιο, τρίτο κατά σειρά, παρουσιάζεται ο οδηγός με τα έξι βήματα που οδηγούν έναν οργανισμό - επιχείρηση στη συμμόρφωση με τον κανονισμό. Τα βήματα περιλαμβάνουν τον τρόπο δράσης από την αρχική κατάσταση του οργανισμού μέχρι και τη μέγιστη δυνατή συμμόρφωση

Στο τέταρτο κεφάλαιο προκύπτουν τα συμπεράσματα από την εμπειρία δημιουργίας του οδηγού. Αναφέρονται τα δυνατά και τα αδύνατα του σημεία καθώς και οι προτάσεις για μελλοντική βελτίωση.

Λέξεις κλειδιά:
Γενικός Κανονισμός Προστασίας Δεδομένων, ΓΚΠΔ, General Data Protection Regulation , GDPR, 2016/679, προστασία δεδομένων προσωπικού χαρακτήρα, συμμόρφωση με τον γενικό κανονισμό προστασίας δεδομένων, εναρμόνιση με τον γενικό κανονισμό προστασίας δεδομένων, πρακτικός οδηγός συμμόρφωσης με το γενικό κανονισμό προστασίας δεδομένων, επιχείρηση, οργανισμός, επιπτώσεις κανονισμού προστασίας δεδομένων.

Abstract

The present assignment was carried out in the framework of the master Dissertation of the postgraduate program "Techno - economic Management & Security of Digital Systems" of the Department of Digital Systems of the University of Piraeus. The dissertation title is: "Operational impact of the new General Data Protection Regulation 2016/679 (GDPR)". The European Regulation is a European Union's legal act that is binding in its entirety and directly applicable in all Member States of the European Union. The GDPR concerns the protection of individuals with regard to the processing of personal data and the free movement of such data and is intended to replace Directive 95/46 / EC of the European Parliament (24/10/1995) "on the protection of individuals with regard to the processing of personal data persons with regard to the processing of personal data and the free movement of such data". The GDPR has some features of a Directive insofar as it allows member states to regulate national situations in certain cases e.g. The minimum age of consent of underage's (set at the age of 15 in the Greek draft law which has been consulted and 13 years since the corresponding Cypriot law that will be published shortly).

The GDPR adopted on April 27th, 2016 and will be enforced on May 25th, 2018. Businesses - organizations will have to comply by the regulation's date of application. In this work, a step-by-step practical guide was developed to help an organization comply with the new regulation. The structuring methodology of the practical guide and the actual guide, are described here.

More specifically, in the first chapter, a brief reference is made to the content of the GDPR. A description of the legal framework that sets the rules for all the parts involved, is presented, and their responsibilities, rights and obligations are analyzed.
In the second chapter, the practical part of this work is presented. This includes the methodology for creating the guide and its representation. The stages that led to the final form of the guide and the tools that were created, are analyzed in detail.
In the third chapter, the six-step guide that leads a company - organization to comply with the regulation, is displayed. It is included in steps the way of implementation from the initial organization's status to maximum possible compliance.
In the fourth and last chapter the conclusions drawn from the experience of creating and testing the guide, are shown. Its strengths and weaknesses as well as suggestions for future improvement are mentioned.

Keywords:
General Data Protection Regulation, GDPR, 2016/679, personal data protection, compliance with the General Data Protection Regulation, harmonization in the General Data Protection Regulation, practical guide for GDPR compliance, enterprise, organization, impact of the data protection regulation.

Συντομογραφίες - Ορισμοί

άρ. Άρθρο

§ Παράγραφος

Καν. Κανονισμός

Ν. Νόμος

α.σ. Αιτιολογικές σκέψεις κανονισμού. Είναι το μέρος μιας νομικής πράξης που περιέχει την αιτιολόγησή της και περιλαμβάνεται μεταξύ των σημείων αναφοράς και του διατακτικού της πράξης.

ΔΠΧ **Δεδομένα Προσωπικού Χαρακτήρα** ή

ΠΔ **Προσωπικά Δεδομένα**

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

ΔΠΧΕΚ **Δεδομένα Προσωπικού Χαρακτήρα Ειδικών Κατηγοριών**

Δεδομένα προσωπικού χαρακτήρα που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και η επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένων που αφορούν την υγεία ή δεδομένων που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή το γενετήσιο προσανατολισμό.

ΥΔ **Υποκείμενο Δεδομένων**

Το φυσικό πρόσωπο στο οποίο αναφέρονται τα δεδομένα και του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί, δηλαδή μπορεί να προσδιορισθεί αμέσως ή εμμέσως, ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός ή περισσότερων συγκεκριμένων

στοιχείων που χαρακτηρίζουν την υπόστασή του από άποψη φυσική, βιολογική, ψυχική, οικονομική, πολιτιστική, πολιτική ή κοινωνική.

ΥΠΕ **Υπεύθυνος Επεξεργασίας**

Το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα· όταν οι σκοποί και ο τρόπος της επεξεργασίας αυτής καθορίζονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια για το διορισμό του μπορούν να προβλέπονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους.

ΕΚΕ **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.

ΕΕ **Ευρωπαϊκή Ένωση**

EU **European Union**

Οικονομική και πολιτική ένωση είκοσι οκτώ ευρωπαϊκών κρατών. Η Ελλάδα περιλαμβάνεται μέσα σε αυτά, το Ηνωμένο Βασίλειο έχει ξεκινήσει τις διαδικασίες αποχώρησης από την ένωση αυτή (Τελευταία ενημέρωση 20/01/2018).

ΕΕΠ **Ευρωπαϊκή Επιτροπή**

EC **European Commission**

Η Ευρωπαϊκή Επιτροπή είναι το πολιτικά ανεξάρτητο εκτελεστικό όργανο της ΕΕ. Είναι το μόνο αρμόδιο όργανο για την κατάρτιση προτάσεων για νέα ευρωπαϊκή νομοθεσία, και εφαρμόζει τις αποφάσεις του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της ΕΕ.

ΕΟΧ **Ευρωπαϊκός Οικονομικός Χώρος**

ΕΕΑ **European Economic Area**

Συμφωνία (1/1/1994) μεταξύ της Ευρωπαϊκής Ζώνης Ελευθέρων Συναλλαγών (ΕΖΕΣ) και της Ευρωπαϊκής Οικονομικής Κοινότητας (ΕΟΚ) που επιτρέπει στις χώρες Ισλανδία,

Λίχτενσταϊν και Νορβηγία να συμμετέχουν στην Ευρωπαϊκή Κοινή Αγορά χωρίς να χρειαστεί να γίνουν μέλη της ΕΟΚ.

ΑΠΔΠΧ Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

Συνταγματικά κατοχυρωμένη ανεξάρτητη διοικητική αρχή που ιδρύθηκε με το Νόμο 2472/1997 «για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα», ο οποίος ενσωματώνει στο ελληνικό δίκαιο την ευρωπαϊκή οδηγία 95/46/ΕΚ.

ΕΑΠΔ Εκτίμηση Αντικτύπου Προστασίας Δεδομένων

DPIA Data Privacy Impact Assessment

Μελέτη που εκτιμά την πιθανότητα και τη σοβαρότητα των κινδύνων σχετικά με την προστασία δεδομένων ΔΠΧ σε έναν οργανισμό - επιχείρηση.

ΓΚΠΔ Γενικός Κανονισμός Προστασίας Δεδομένων

GDPR General Data Protection Regulation

Κανονισμός που σχετίζεται με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών. Αντικαθιστά την οδηγία 95/46/ΕΚ, που είναι για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών. Ψηφίστηκε στις 25 Απριλίου 2016 και τίθεται σε ισχύ στις 25 Μαΐου 2018.

ΥΠΔ Υπεύθυνος Προστασίας Δεδομένων

DPO Data Protection Officer

Φυσικό πρόσωπο, μέρος του προσωπικού του ΥΠΕ / ΕΚΕ ή εκτός αυτού με σύμβαση παροχής υπηρεσιών, που μεριμνά με ανεξάρτητο τρόπο, για την ορθή εφαρμογή του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ / GDPR) στον οργανισμό - επιχείρηση.

ΕΣΠΔ **Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων**

EDPB **European Data Protection Board**

Όργανο της Ευρωπαϊκής Ένωσης με νομική προσωπικότητα που με την εφαρμογή του ΓΚΠΔ/GDPR πρόκειται να αντικαταστήσει την ομάδα εργασίας του άρθρου 29 (ΟΕ29 / WP29).

ΕΕΠΔ **Ευρωπαίος Επόπτης Προστασίας Δεδομένων**

EDPS **European Data Protection Supervisor**

Ανεξάρτητη ευρωπαϊκή αρχή που σκοπό έχει να διασφαλίζει ότι κατά την επεξεργασία προσωπικών δεδομένων, τα όργανα και οι οργανισμοί της ΕΕ σέβονται το δικαίωμα των πολιτών για προστασία της ιδιωτικής ζωής.

Οργανισμός

Στην κοινωνική ορολογία, οργανισμός είναι μια ομάδα ανθρώπων με έναν ή περισσότερους κοινούς στόχους, τους οποίους επιδιώκει να υλοποιήσει μέσω επίσημα καθορισμένων αρχών και θεσμών. Είναι κάθε νομικό πρόσωπο που έχει δραστηριότητες οικονομικής, πολιτικής, κοινωνικής φύσεως. Οργανισμός θεωρείται ένας δημόσιος φορέας, μια επιχείρηση, ένας σύλλογος κτλ. Για την παρούσα εργασία όπου αναφέρεται οργανισμός εννοούνται όλες οι παραπάνω έννοιες.

Ευαίσθητα Προσωπικά Δεδομένα

Ο όρος ευαίσθητα προσωπικά δεδομένα στον ΓΚΠΔ / GDPR αντικαθίσταται από τον όρο Δεδομένα Προσωπικού Χαρακτήρα Ειδικών Κατηγοριών (ΔΠΧΕΚ).

Επεξεργασία

Κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή.

Περιορισμός της επεξεργασίας

Η επισήμανση αποθηκευμένων δεδομένων προσωπικού χαρακτήρα με στόχο τον περιορισμό της επεξεργασίας τους στο μέλλον. Όταν ισχύει ο περιορισμός της επεξεργασίας επιτρέπεται η αποθήκευση των δεδομένων όχι όμως η περαιτέρω επεξεργασία τους.

Κατάρτιση προφίλ

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

Ψευδωνυμοποίηση

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

Σύστημα αρχειοθέτησης

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

Αποδέκτης

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

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.

Συγκατάθεση του υποκειμένου των δεδομένων
Κάθε ένδειξη βούλησης, ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει, με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν.

Παραβίαση δεδομένων προσωπικού χαρακτήρα
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.

Εκπρόσωπος

Φυσικό ή νομικό πρόσωπο εγκατεστημένο στην Ευρωπαϊκή Ένωση, το οποίο ορίζεται εγγράφως από τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία βάσει του άρθρου 27 και εκπροσωπεί τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία ως προς τις αντίστοιχες υποχρεώσεις τους δυνάμει του παρόντος κανονισμού.

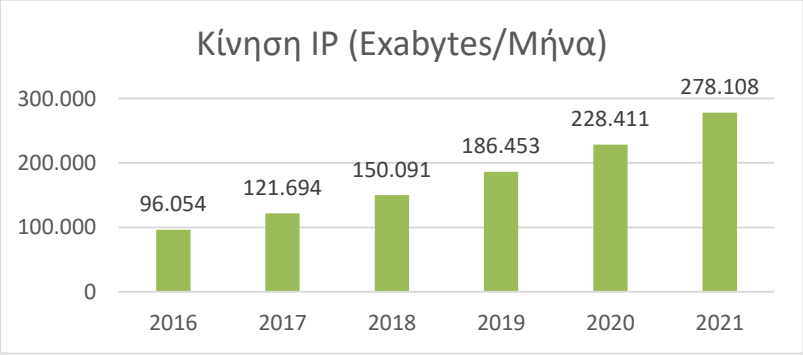
Επιχείρηση

Φυσικό ή νομικό πρόσωπο που ασκεί οικονομική δραστηριότητα, ανεξάρτητα από τη νομική του μορφή, περιλαμβανομένων των προσωπικών εταιρειών ή των ενώσεων που ασκούν τακτικά οικονομική δραστηριότητα.

1 Νομικό πλαίσιο

1.1 Εισαγωγή

Η αλματώδης εξέλιξη και σύγκλιση των τεχνολογιών έχουν διαμορφώσει την εποχή που η πρόσβαση σε δεδομένα και πληροφορίες είναι εύκολη και γρήγορη όσο ποτέ άλλοτε. Εκτιμάται ότι το 2017 η ποσότητα της κίνησης των δεδομένων μέσω Διαδικτύου ανέρχεται σε 121 EB (Exabytes) / Μήνα[1] και μέχρι το 2021 αναμένεται να ξεπεράσει τα 278 EB/μήνα. Το διαδίκτυο και οι ψηφιακές τεχνολογίες μεταβάλλουν τον τρόπο διαβίωσης μας σε ατομικό, κοινωνικό και επιχειρηματικό επίπεδο, καθώς όλοι οι τομείς της κοινωνίας και της οικονομίας μας ενοποιούνται σε ολοένα και μεγαλύτερο βαθμό.



Διάγραμμα 1. Στατιστικά κίνησης δεδομένων μέσω διαδικτύου[1]

Η Ευρωπαϊκή Επιτροπή (ΕΕΠ), ως εκτελεστικό όργανο της Ευρωπαϊκής Ένωσης (ΕΕ), σε μια προσπάθεια αξιοποίησης της ψηφιακής τεχνολογίας, το Μάιο του 2015 προσδιόρισε τη στρατηγική για την Ψηφιακή Ενιαία Αγορά - Digital Single Market (DSM) της Ευρώπης. Μέσα στους πυλώνες της στρατηγικής προσδιορίζει μια σειρά από νομοθετικές αλλαγές με σκοπό την ενίσχυση της ψηφιακής οικονομίας και της ελεύθερης διακίνησης αγαθών και υπηρεσιών ενισχύοντας την εμπιστοσύνη των καταναλωτών και των ελευθεριών του ατόμου. Οι

1 "Cisco Visual Networking Index: Forecast and Methodology, 2016–2021" 6 Ιουνίου 2017. http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.pdf "Global IP traffic growth, 2016–2021" σ.6 (Τελευταία πρόσβαση 08/02/2018)

Πολλαπλάσια του byte:

1KB=2^{10} bytes, 1MB=2^{20} bytes, 1GB=2^{30} bytes, 1TB=2^{40} bytes, 1PB=2^{50} bytes, 1EB=2^{60} bytes, 1ZB=2^{80} bytes, YB=2^{90} bytes

νομοθετικές αλλαγές περιλαμβάνουν Ευρωπαϊκές οδηγίες και κανονισμούς που προσδιορίζουν τους κανόνες της ΕΕ στην Ευρωπαϊκή και παγκόσμια ψηφιακή αγορά. Μεταξύ άλλων, η οδηγία NIS (2016/1148) αφορά μέτρα για κοινό υψηλό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση, ο κανονισμός EIDAS (2014/910) ασχολείται με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά και την κατάργηση της οδηγίας 1999/93/ΕΚ και ο κανονισμός GDPR/ΓΚΠΔ (2016/679) σχετίζεται με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ.

Στο κεφάλαιο αυτό θα γίνει συνοπτική αναφορά των βασικών σημείων του κανονισμού ΓΚΠΔ / GDPR ώστε ο αναγνώστης να κατανοήσει τα κύρια χαρακτηριστικά του νέου κανονιστικού ρυθμιστικού πλαισίου.

1.2 Ο Γενικός Κανονισμός Προστασίας Δεδομένων ΓΚΠΔ / GDPR

1.2.1 Στόχος του κανονισμού

Ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ / GDPR) έχει ως στόχο:

α) να θεσπίσει κανόνες για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα που αφορούν την ελεύθερη κυκλοφορία δεδομένων προσωπικού χαρακτήρα (ΔΠΧ),

β) να προστατεύσει τα θεμελιώδη δικαιώματα και τις ελευθερίες των φυσικών προσώπων,

γ) να προάγει την ελεύθερη κυκλοφορία δεδομένων προσωπικού χαρακτήρα (ΔΠΧ) εντός της Ευρωπαϊκής Ένωσης.

1.2.2 Πεδίο εφαρμογής

Ο κανονισμός εφαρμόζεται στην εν όλω ή εν μέρει, αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα (ΔΠΧ) καθώς και στη μη αυτοματοποιημένη επεξεργασία τέτοιων δεδομένων τα οποία περιλαμβάνονται ή πρόκειται να περιληφθούν σε σύστημα αρχειοθέτησης. Οι κανόνες για την επεξεργασία ΔΠΧ θα πρέπει να εφαρμοστούν από οργανισμούς:

α) που είναι εγκατεστημένοι εντός της ΕΕ ή του ΕΟΧ,
β) που δεν είναι εγκατεστημένοι στα γεωγραφικά όρια της ΕΕ ή του ΕΟΧ αλλά επεξεργάζονται ΔΠΧ υποκείμενων δεδομένων (ΥΔ) που βρίσκονται στην ΕΕ.

1.2.3 Αρχές επεξεργασίας ΔΠΧ

Πριν αναλυθούν οι αρχές της επεξεργασίας είναι απαραίτητο να επεξηγηθεί ο όρος «επεξεργασία δεδομένων προσωπικού χαρακτήρα (ΔΠΧ)» σύμφωνα με τον κανονισμό: είναι κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα (ΔΠΧ) ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή.

Όλες οι παραπάνω πράξεις (επεξεργασία ΔΠΧ) θα πρέπει να διέπονται από δέκα (10) αρχές (άρ.5). Πιο συγκεκριμένα από την:

1. **αρχή της νομιμότητας**: δηλαδή η επεξεργασία να είναι σύννομη,
2. **αρχή της αντικειμενικότητας**: δηλαδή η επεξεργασία να είναι θεμιτή,
3. **αρχή της διαφάνειας**: δηλαδή η επεξεργασία να είναι διαφανής,
4. **αρχή του σκοπού** (και περιορισμού αυτού): δηλαδή τα ΔΠΧ να συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και να μην υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς· η περαιτέρω επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς θεωρείται συμβατή με τους αρχικούς σκοπούς.
5. **αρχή της ελαχιστοποίησης των δεδομένων**: δηλαδή τα ΔΠΧ να είναι κατάλληλα, συναφή και να περιορίζονται στο αναγκαίο για τους σκοπούς που υποβάλλονται σε επεξεργασία,
6. **αρχή της ακρίβειας**: δηλαδή τα ΔΠΧ να είναι ακριβή σε όλα τα είδη επεξεργασίας διαφορετικά να επικαιροποιούνται ή να διαγράφονται,
7. **αρχή του περιορισμού της περιόδου αποθήκευσης**: δηλαδή τα ΔΠΧ να διατηρούνται μόνο για το διάστημα που απαιτείται για τους σκοπούς που έχουν συλλεχθεί· επιτρέπεται η αποθήκευση τους για μεγαλύτερα διαστήματα εφόσον τα ΔΠΧ θα υποβάλλονται σε επεξεργασία μόνο για τους σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για τους σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς και εφόσον εφαρμόζονται τα κατάλληλα τεχνικά και οργανωτικά μέτρα,

8. **αρχή της ακεραιότητας**: δηλαδή τα ΔΠΧ να μην τροποποιούνται από μη εξουσιοδοτημένες οντότητες (συστήματα, ανθρώπους κτλ.),
9. **αρχή της εμπιστευτικότητας**: δηλαδή τα ΔΠΧ να μην αποκαλύπτονται σε μη εξουσιοδοτημένες οντότητες (συστήματα, ανθρώπους κτλ.),
10. **αρχή της λογοδοσίας**: δηλαδή ο υπεύθυνος επεξεργασίας (ΥΠΕ) φέρει ευθύνη για την τήρηση όλων των παραπάνω αρχών και θα πρέπει να είναι σε θέση να το αποδείξει.

1.2.4 Νομιμότητα επεξεργασίας ΔΠΧ

Η νομιμότητα της επεξεργασίας ΔΠΧ καθορίζεται από συγκεκριμένες προϋποθέσεις και πρέπει να ισχύει τουλάχιστον μια από αυτές (άρ.6,10,11):

1. Συναίνεση (consent) (άρ.6§1α) : το υποκείμενο δεδομένων θα πρέπει να έχει συναινέσει - συγκαταθέσει για την επεξεργασία των ΔΠΧ.
2. Έννομη υποχρέωση (legal obligation) (άρ.6§1γ): όταν η επεξεργασία είναι απαραίτητη για να συμμορφωθεί ο υπεύθυνος επεξεργασίας με έννομη υποχρέωση.
3. Ζωτικού συμφέροντος (vital Interests) (άρ.6§1δ): όταν η επεξεργασία είναι απαραίτητη για την διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου.
4. Εκτέλεση σύμβασης (contract) (άρ.6§1β): όταν η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή για να ληφθούν μέτρα κατ' αίτηση του υποκειμένου δεδομένων πριν από τη σύναψη σύμβασης.
5. Δημόσια εξουσία (public function) (άρ.6§1ε): όταν η επεξεργασία είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας. Ειδική μνεία γίνεται για την επεξεργασία από ποινικές καταδίκες και αδικήματα η οποία επιτρέπεται μόνο υπό έλεγχο επίσημης αρχής (άρ.10).
6. Έννομα συμφέροντα (legitimate interests) (άρ.6§1στ): όταν η επεξεργασία είναι απαραίτητη για σκοπούς έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος. Εξαίρεση αποτελεί αν καταπατούνται θεμελιώδη δικαιώματα και ελευθερίες φυσικού προσώπου και ιδιαίτερα αν είναι παιδί.
7. Ανέφικτη εξακρίβωση ταυτότητας (unable identification) (άρ.11): όταν η επεξεργασία γίνεται σε δεδομένα που είναι ανέφικτη η εξακρίβωση ταυτότητας των υποκείμενων δεδομένων.

8. Σκοποί αρχειοθέτησης (archiving purposes) (άρ.89 §1,2): όταν η επεξεργασία γίνεται για σκοπούς αρχειοθέτησης για το δημόσιο συμφέρον, επιστημονικής ή ιστορικής έρευνας, στατιστικούς σκοπούς.

Δεδομένα Προσωπικού Χαρακτήρα Ειδικών Κατηγοριών (ΔΠΧΕΚ)

Τα ΔΠΧ έχουν μια υποκατηγορία που ονομάζονται Δεδομένα Προσωπικού Χαρακτήρα Ειδικών Κατηγοριών (ΔΠΧΕΚ). Σε παλαιότερους νόμους η κατηγορία των δεδομένων αυτών αναφέρονται ως ευαίσθητα ΔΠΧ. Η επεξεργασία ΔΠΧΕΚ κατά κανόνα απαγορεύεται. Κατ' εξαίρεση επιτρέπεται στις παρακάτω περιπτώσεις (άρ.9):

1. Ρητή συγκατάθεση (explicit consent) (άρ.9§2α): το υποκείμενο δεδομένων θα πρέπει να παρέχει ρητή συγκατάθεση, όχι απλή συγκατάθεση όπως είναι στα ΔΠΧ.
2. Έννομη υποχρέωση (legal obligation) (άρ.9§2β): όταν η επεξεργασία είναι απαραίτητη για την εκτέλεση των υποχρεώσεων και την άσκηση συγκεκριμένων δικαιωμάτων του υπευθύνου επεξεργασίας ή του υποκειμένου των δεδομένων στον τομέα του εργατικού δικαίου και του δικαίου κοινωνικής ασφάλισης και κοινωνικής προστασίας, εφόσον επιτρέπεται από το δίκαιο της Ένωσης ή κράτους μέλους ή από συλλογική συμφωνία σύμφωνα με το εθνικό δίκαιο παρέχοντας κατάλληλες εγγυήσεις για τα θεμελιώδη δικαιώματα και τα συμφέροντα του υποκειμένου των δεδομένων.
3. Ζωτικού συμφέροντος (vital interests) (άρ.9§2γ): όταν η επεξεργασία είναι απαραίτητη για την προστασία των ζωτικών συμφερόντων του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου, εάν το υποκείμενο των δεδομένων είναι σωματικά ή νομικά ανίκανο να συγκατατεθεί.
4. Μέλη φορέα (organization members) (άρ.9§2δ): όταν η επεξεργασία διενεργείται, με κατάλληλες εγγυήσεις, στο πλαίσιο των νόμιμων δραστηριοτήτων ιδρύματος, οργάνωσης ή άλλου μη κερδοσκοπικού φορέα με πολιτικό, φιλοσοφικό, θρησκευτικό ή συνδικαλιστικό στόχο και υπό την προϋπόθεση ότι η επεξεργασία αφορά αποκλειστικά τα μέλη ή τα πρώην μέλη του φορέα ή πρόσωπα τα οποία έχουν τακτική επικοινωνία μαζί του σε σχέση με τους σκοπούς του και ότι τα δεδομένα προσωπικού χαρακτήρα δεν κοινοποιούνται εκτός του συγκεκριμένου φορέα χωρίς τη συγκατάθεση των υποκειμένων των δεδομένων.
5. Προδήλως δημοσιοποιημένα (manifestly public) (άρ.9§2ε): όταν το υποκείμενο δεδομένων έχει προδήλως δημοσιοποιήσει ΔΠΧΕΚ
6. Υποστήριξη νομικών αξιώσεων (legal claims establishment) (άρ.9§2στ): όταν η επεξεργασία είναι απαραίτητη για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων ή όταν τα δικαστήρια ενεργούν υπό τη δικαιοδοτική τους ιδιότητα.

7. Δημόσιο συμφέρον (public interest) (άρ.9§2ζ): όταν η επεξεργασία είναι απαραίτητη για λόγους ουσιαστικού δημόσιου συμφέροντος της ΕΕ ή κράτους μέλους.
8. Προληπτική ή επαγγελματική ιατρική (preventive or occupational medicine) (άρ.9§2η): όταν η επεξεργασία είναι απαραίτητη για σκοπούς προληπτικής ή επαγγελματικής ιατρικής
9. Δημόσιο συμφέρον δημόσιας υγείας (public health interest) (άρ.9§2θ): όταν η επεξεργασία είναι απαραίτητη για λόγους δημόσιου συμφέροντος στον τομέα της δημόσιας υγείας
10. Αρχειοθέτηση για δημόσιο συμφέρον (public interest archiving purposes) (άρ.9§2ι, άρ.89§1,2): όταν η επεξεργασία είναι απαραίτητη για λόγους δημόσιου συμφέροντος στον τομέα της δημόσιας υγείας

Πίνακας 1. Περιπτώσεις νομιμότητας επεξεργασίας ΔΠΧ

Επιτρεπόμενες περιπτώσεις επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (ΔΠΧ) (άρ.6,9 -11)	
Δεδομένα προσωπικά	**Δεδομένα ειδικών κατηγοριών (εξαιρέσεις)**
Συναίνεση (consent) (άρ.6§1α)	Συναίνεση – Ρητή συγκατάθεση (explicit consent) (άρ.9§2α)
Έννομη υποχρέωση (legal obligation) (άρ.6§1γ)	Έννομη υποχρέωση (legal obligation) (άρ.9§2β)
Ζωτικού συμφέροντος (vital Interests) (άρ.6§1δ)	Ζωτικού συμφέροντος (vital interests) (άρ.9§2γ)
Εκτέλεση σύμβασης (contract) (άρ.6§1β)	Μέλη φορέα (organization members) (άρ.9§2δ)
Δημόσια εξουσία (public function) (άρ.6§1ε) (επεξεργασία από ποινικές καταδίκες και αδικήματα – μόνο υπο έλεγχο επίσημης αρχής ή από νομοθεσία) (άρ.10)	Προδήλως δημοσιοποιημένα (manifestly public) (άρ.9§2ε)
Έννομα συμφέροντα (legitimate interests) (άρ.6§1στ)	Υποστήριξη νομικών αξιώσεων (legal claims establishment) (άρ.9§2στ)
Ανέφικτη εξακρίβωση ταυτότητας (unable identification) (άρ.11)	Δημόσιο συμφέρον (public interest) (άρ.9§2ζ)
Αρχειοθέτηση για δημόσιο συμφέρον συμφέρον (public interest archiving purposes), επιστημονική ή ιστορική έρευνα, στατιστικούς σκοπούς (άρ.89 §1,2)	Προληπτική επαγγελματική ιατρική (preventive or occupational medicine) (άρ.9§2η)
	Δημόσιο συμφέρον δημόσιας υγείας (public health interest) (άρ.9§2θ)
	Αρχειοθέτηση για δημόσιο συμφέρον (public interest archiving purposes), επιστημονική ή ιστορική έρευνα, στατιστικούς σκοπούς (άρ.9§2ι, άρ.89 §1,2)

1.2.4.2 Συγκατάθεση

Η συγκατάθεση είναι πρωταρχική προϋπόθεση λήψης, απόκτησης και επεξεργασίας ΔΠΧ. Ο κανονισμός δίνει υψηλή σημασία στον τρόπο λήψης της συγκατάθεσης του οργανισμού από το

υποκείμενο δεδομένων (ΥΔ). Για τα ΔΠΧ ο κανονισμός προϋποθέτει «συναίνεση» ενώ για τα ΔΠΧΕΚ «Ρητή συγκατάθεση».

Ο υπεύθυνος επεξεργασίας (ΥΠΕ) θα πρέπει να είναι σε θέση να αποδείξει ότι το υποκείμενο δεδομένων συγκατατέθεσε και ότι η συγκατάθεση περιλαμβάνει :

1. Σαφή και απλή διατύπωση (άρ.7§2),
2. Διακριτό μέρος για τη συγκατάθεση (άρ.7§2),
3. Σαφή θετική ενέργεια (α.σ.32): η αδράνεια δεν θα πρέπει να εκλαμβάνεται ως συγκατάθεση
4. Συγκατάθεση για όλους τους σκοπούς επεξεργασίας (α.σ.32): να αναφέρονται όλοι οι σχετικοί σκοποί επεξεργασίας για κάθε ένα από τα δεδομένα που συλλέγονται π.χ. χρήση δεδομένων για συγκεκριμένη αγορά και χρήση των δεδομένων για τηλεφωνικές πωλήσεις,
5. Όχι καταχρηστικές ρήτρες σε περίπτωση άρνησης (α.σ.42): η συγκατάθεση δεν θεωρείτε ότι δόθηκε ελεύθερα αν το υποκείμενο δεδομένων δεν έχει αληθινή επιλογή ή δεν είναι σε θέση να αρνηθεί ή να αποσύρει τη συγκατάθεση του χωρίς να ζημιωθεί,
6. Ανισότητα μεταξύ ΥΔ και ΥΠΕ - Δημόσιου φορέα (α.σ.43): η νομική βάση του δημόσιου φορέα για επεξεργασία δεδομένων δεν συνεπάγεται με ελεύθερη συγκατάθεση για όλες τις περιστάσεις επεξεργασίας ΔΠΧ,
7. Μη αναγκαία επεξεργασία ΔΠΧ λόγω σύμβασης (άρ.7§4): συγκατάθεση που είναι μέσα σε ένα συμβόλαιο, ελεύθερη για περιπτώσεις που δεν είναι αναγκαίες και άνευ όρων,
8. Δυνατότητα ανάκλησης ανά πάσα στιγμή (άρ.7§3).

Η συγκατάθεση πρέπει να είναι «ΡΗΤΗ» σε περιπτώσεις:

1. επεξεργασίας ΔΠΧΕΚ ή
2. διαβίβασης ΔΠΧ σε χώρες εκτός ΕΕ - ΕΟΧ

Αυτό απαιτεί παραπάνω προσοχή στη λήψη της σε σχέση με την απλή συγκατάθεση, δεν μπορεί να είναι ένα απλό κουτί επιλογής (tick box) που το ΥΔ επιλέγει. Επίσης δεν είναι αποδεκτό να εξασφαλισθεί από συμπεριφορά όπως π.χ. «Η παραμονή σας στο δικτυακό τόπο δηλώνει τη ρητή συγκατάθεση σας για την επεξεργασία των ΔΠΧ» .

1.2.4.3 Συναίνεση σε ΔΠΧ παιδιών

Ο κανονισμός κάνει ιδιαίτερη μνεία στις προϋποθέσεις συγκατάθεσης παιδιού. Για παιδιά 16 ετών και άνω μπορεί να ζητείται απευθείας συγκατάθεση από αυτό. Για παιδιά 13 έως 16 θα πρέπει να ζητηθεί συγκατάθεση από το πρόσωπο που έχει τη γονική μέριμνα.

Επιπροσθέτως, ο κανονισμός αναφέρει (α.σ. 38,58,71,65) ότι:

- τα παιδιά απαιτούν ειδική προστασία όσον αφορά τα ΔΠΧ καθώς, μπορεί να έχουν μικρότερη επίγνωση των σχετικών κινδύνων, συνεπειών, εγγυήσεων και των δικαιωμάτων τους (α.σ.38),
- η ενημέρωση των παιδιών θα πρέπει να διατυπώνεται σε σαφή και απλή γλώσσα την οποία το παιδί μπορεί να κατανοήσει εύκολα (α.σ.58),
- η επεξεργασία που περιλαμβάνει κατάρτιση προφίλ και αυτόματες αποφάσεις δεν πρέπει να εφαρμόζεται σε παιδιά (α.σ.71),
- το δικαίωμα διόρθωσης και διαγραφής ΔΠΧ που έχουν συλλέγει από συγκατάθεση, εφαρμόζεται ιδιαίτερα όταν πρόκειται για παιδί ανεξάρτητα αν πλέον δεν είναι παιδί (α.σ.65).

Ο κανονισμός προβλέπει τη δυνατότητα εθνικής ρύθμισης της ελάχιστης ηλικίας συναίνεσης. Στο υπό διαβούλευση Ελληνικό νομοσχέδιο τίθεται στα 15 χρόνια ενώ στο Κυπριακό πρόκειται να τεθεί προσεχώς στα 13.

1.2.5 Δικαιώματα Υποκείμενου Δεδομένων (ΥΔ)

Ο κανονισμός προσδιορίζει οκτώ (8) δικαιώματα του υποκειμένου δεδομένων[2].

1. Δικαίωμα ενημέρωσης

Είναι το δικαίωμα ενημέρωσης του υποκειμένου δεδομένων (ΥΔ) σχετικά με την επεξεργασία των ΔΠΧ. Το ΥΔ θα πρέπει να ενημερώνεται από τον υπεύθυνο επεξεργασίας (ΥΠΕ) σχετικά με την επεξεργασία των δεδομένων του και θα πρέπει να περιλαμβάνει πληροφορίες όπως: ταυτότητα και στοιχεία επικοινωνίας του ΥΠΕ / ΕΚΕ και ΥΠΔ, τους σκοπούς της επεξεργασίας, την νομική βάση αυτών, τους αποδέκτες κ.α..

Οι πληροφορίες που παρέχονται πρέπει να είναι :

- σε συνοπτική, διαφανή, κατανοητή και εύκολα προσβάσιμη μορφή,
- με σαφή και απλή διατύπωση, ιδίως εάν απευθύνεται σε παιδί και
- δωρεάν

Ο τρόπος ενημέρωσης γίνεται συνήθως μέσω μιας δήλωσης γραπτά ή προφορικά με ποικίλες ονομασίες όπως «Δήλωση προστασίας προσωπικών δεδομένων», «Πολιτική προστασίας

[2] Ερμηνείες του κανονισμού σχετικά με τα δικαιώματα ΥΔ έχουν βασιστεί στην Αγγλική αρχή προστασίας δεδομένων - Information Commissioner's Office (ICO), " Guide to the General Data Protection Regulation (GDPR)" https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/ (τελευταία πρόσβαση 05/02/2018)

προσωπικών δεδομένων» «Πολιτική απορρήτου» «Δήλωση ιδιωτικότητας», «Προστασία ιδιωτικότητας» κ.α.

[Δείτε περισσότερα στα άρ.12§1, §5, §7, 13, 14 και α.σ. 58-62 του κανονισμού, γνωμοδότηση της ΟΕ29 "Guidelines on transparency under Regulation 2016/679", (WP260)]

2. Δικαίωμα πρόσβασης

Είναι το δικαίωμα του ΥΔ να έχει πρόσβαση σε ΔΠΧ και άλλες πληροφορίες που το αφορούν, προκειμένου να έχει επίγνωση και να επαληθεύει τη νομιμότητα της επεξεργασίας. Πιο συγκεκριμένα το ΥΔ έχει δικαίωμα να λάβει:

- επιβεβαίωση για την επεξεργασία των δικών του ΔΠΧ,
- πρόσβαση στα δικά του ΔΠΧ,
- αντίγραφο των δικών του ΔΠΧ,
- άλλες συμπληρωματικές πληροφορίες όπως:
  - τους σκοπούς επεξεργασίας,
  - τις κατηγορίες δεδομένων ΔΠΧ που επεξεργάζονται,
  - τους αποδέκτες των ΔΠΧ,
  - το χρονικό διάστημα αποθήκευσης,
  - την ύπαρξη δικαιώματος υποβολής αιτήματος (διόρθωση, διαγραφή, περιορισμού της επεξεργασίας και εναντίωσης),
  - το δικαίωμα υποβολής καταγγελίας,
  - την προέλευση των ΔΠΧ,
  - τη λογική που ακολουθείται στην αυτοματοποιημένη λήψη αποφάσεων, ένα υπάρχει, και τις πιθανές συνέπειες της επεξεργασίας αυτής στο ΥΔ. Στην αυτοματοποιημένη λήψη αποφάσεων περιλαμβάνεται και η κατάρτιση προφίλ,
  - τις πιθανές διαβιβάσεις των ΔΠΧ σε τρίτες χώρες και τις εγγυήσεις αυτών.

Ο ΥΠΕ παρέχει στο ΥΔ τα παραπάνω χωρίς καθυστέρηση εντός μηνός από την παραλαβή του αιτήματος. Η εν λόγω προθεσμία μπορεί να παραταθεί, έως δύο μήνες, σε περιπτώσεις πολυπλοκότητας του αιτήματος ή μεγάλου όγκου αιτημάτων έχοντας ενημερώσει, εντός μηνός, το ΥΔ για τους λόγους της καθυστέρησης.

Η παροχή των παραπάνω πληροφοριών γίνεται δωρεάν και προβλέπεται ότι δύναται να παρέχεται εξ αποστάσεως σε ασφαλές σύστημα. Σε περιπτώσεις που το αίτημα του ΥΔ είναι προδήλως αβάσιμο ή υπερβολικό ο ΥΠΕ μπορεί να επιβάλει εύλογο τέλος λαμβάνοντας υπόψη τα σχετικά διοικητικά έξοδα ή να αρνηθεί να δώσει συνέχεια στο αίτημα αφού ενημερώσει το ΥΔ.

[Δείτε περισσότερα στα άρ.12,15 και α.σ.65 του κανονισμού]

3. Δικαίωμα διόρθωσης

Είναι το δικαίωμα του υποκειμένου δεδομένων (ΥΔ) να απαιτήσει από τον υπεύθυνο επεξεργασίας (ΥΠΕ) χωρίς αδικαιολόγητη καθυστέρηση τη διόρθωση ανακριβών δεδομένων προσωπικού χαρακτήρα που το αφορούν. Έχοντας υπόψη τους σκοπούς της επεξεργασίας, το ΥΔ έχει το δικαίωμα να απαιτήσει τη συμπλήρωση ελλιπών δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων μέσω συμπληρωματικής δήλωσης.

[Δείτε περισσότερα στα άρ.12,16 και 19 του κανονισμού]

4. Δικαίωμα διαγραφής (δικαίωμα στη λήθη)

Είναι το δικαίωμα του υποκειμένου δεδομένων (ΥΔ) να ζητήσει από τον υπεύθυνο επεξεργασίας τη διαγραφή δεδομένων προσωπικού χαρακτήρα που το αφορούν χαρακτήρα χωρίς αδικαιολόγητη καθυστέρηση, εάν ισχύουν κάποιοι από τους παρακάτω λόγους:

- τα ΔΠΧ δεν είναι πλέον απαραίτητα σε σχέση με τους σκοπούς που συλλέχθηκαν / υποβλήθηκαν σε επεξεργασία,
- το ΥΔ ανακαλεί τη συγκατάθεση του για την επεξεργασία ΔΠΧ,
- ο ΥΔ αντιτίθεται στην επεξεργασία και δεν υπάρχει κανένα υπερισχύον έννομο συμφέρον για τη συνέχιση της επεξεργασίας,
- Το ΥΔ αντιτίθεται στην επεξεργασία σύμφωνα με το δικαίωμα εναντίωσης (άρ.21§2) για σκοπούς απευθείας εμπορικής προώθησης,
- τα ΔΠΧ υποβλήθηκαν σε επεξεργασία παράνομα,
- τα ΔΠΧ πρέπει να διαγραφούν, ώστε να τηρηθεί νομική υποχρέωση,
- τα ΔΠΧ έχουν συλλεχθεί σε σχέση με την προσφορά υπηρεσιών της κοινωνίας των πληροφοριών σε παιδί.

Σε περιπτώσεις που τα ΔΠΧ έχουν κοινοποιηθεί σε τρίτους, ο ΥΠΕ θα πρέπει να τους ενημερώσει για το αίτημα διαγραφής ΔΠΧ (αντιγράφων, συνδέσμων σε αυτά ή αναπαραγωγών αυτών) του ΥΔ.

Τα παραπάνω εξαιρούνται :

- για την άσκηση του δικαιώματος ελευθερίας της έκφρασης και του δικαιώματος στην ενημέρωση,
- για την τήρηση νομικής υποχρέωσης εκπλήρωση καθήκοντος δημόσιου συμφέροντος ή άσκηση δημόσιας εξουσίας,
- για λόγους δημόσιου συμφέροντος στον τομέα της δημόσιας υγείας,

- για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς,
- για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων.

Ο κανονισμός ενισχύει το δικαίωμα διαγραφής διευκρινίζοντας ότι οι οργανισμοί που δημοσιεύουν ΔΠΧ θα πρέπει να ενημερώνουν τους άλλους οργανισμούς που κάνουν επεξεργασία δεδομένων να διαγράψουν τα αντίγραφα, τους συνδέσμους ή αναπαράγωγα των εν λόγω ΔΠΧ. Βεβαία όπως αναφέρθηκε ήδη, υπάρχουν περιπτώσεις στις οποίες οι οργανισμοί που επεξεργάζονται ΔΠΧ εξαιρούνται από την υποχρέωση του δικαιώματος της διαγραφής ΔΠΧ.

Παράδειγμα[3]: Μια μηχανή αναζήτησης ενημερώνει τον εκδότη ενός μέσου ότι διαγράφει τα αποτελέσματα αναζήτησης που συνδέονται με μια δική του είδηση λόγω αιτήματος διαγραφής από ένα άτομο. Εάν η δημοσίευση του άρθρου προστατεύεται από την ελευθερία έκφρασης, τότε ο εκδότης δεν υποχρεούται να διαγράψει το άρθρο.
[Δείτε περισσότερα στα άρ.17,19 και α.σ.65,66 του κανονισμού]

5. Δικαίωμα περιορισμού της επεξεργασίας

Είναι το δικαίωμα του υποκειμένου δεδομένων (ΥΔ) να περιοριστεί η επεξεργασία δεδομένων όταν ισχύουν κάποιες προϋποθέσεις. Όταν ισχύει ο περιορισμός της επεξεργασίας επιτρέπεται η αποθήκευση των δεδομένων όχι όμως η περαιτέρω επεξεργασία τους.
Ο περιορισμός επεξεργασίας μπορεί να ασκηθεί όταν ισχύει ένα από τα ακόλουθα:

- η ακρίβεια των ΔΠΧ αμφισβητείται από το ΥΔ, έως ότου ο ΥΠΕ επαληθεύσει την ακρίβεια των ΔΠΧ,
- η επεξεργασία είναι παράνομη και το ΥΔ αντιτάσσεται στη διαγραφή των δεδομένων προσωπικού χαρακτήρα και ζητεί, αντ' αυτής, τον περιορισμό της χρήσης τους,
- ο υπεύθυνος επεξεργασίας δεν χρειάζεται πλέον τα ΔΠΧ για τους σκοπούς της επεξεργασίας, αλλά τα δεδομένα αυτά απαιτούνται από το ΥΔ για τη θεμελίωση, την άσκηση ή την υποστήριξη νομικών αξιώσεων,
- το ΥΔ έχει αντιρρήσεις για την επεξεργασία (δικαίωμα εναντίωσης) και αναμένεται η επαλήθευση του κατά πόσον οι νόμιμοι λόγοι του ΥΠΕ υπερισχύουν έναντι των λόγων του ΥΔ.

[3] Παράδειγμα από την Αγγλική αρχή προστασίας δεδομένων (ICO): Right to erasuse https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/ (τελευταία πρόσβαση 12/02/2018)

Η άρση του περιορισμού της επεξεργασίας επιτρέπεται μόνο με τη συγκατάθεση του ΥΔ ή λόγω νομικών αξιώσεων ή για την προστασία άλλου νομικού ή φυσικού προσώπου ή για λόγους δημοσίου συμφέροντος.

Οι οργανισμοί πιθανόν να χρειαστεί να αναθεωρήσουν τις διαδικασίες τους για να μπορούν να προσδιορίσουν τις περιπτώσεις πού μπορεί να ζητηθεί ο περιορισμός της επεξεργασίας των προσωπικών δεδομένων.

Σε περιπτώσεις δημοσιοποίησης ή κοινοποίησης ΔΠΧ σε τρίτους θα πρέπει να γίνει ενημέρωση σε αυτούς για τον εν λόγω περιορισμό της επεξεργασίας των ΔΠΧ εκτός αν αυτό αποδειχθεί αδύνατο. Το ΥΔ θα πρέπει να ενημερώνεται σε κάθε περίπτωση καθώς επίσης και πριν από την άρση του περιορισμού της επεξεργασίας.

[Δείτε περισσότερα στα άρ.18, 19 και α.σ. 67 του κανονισμού]

6. Δικαίωμα φορητότητας

Είναι το δικαίωμα του υποκειμένου δεδομένων (ΥΔ) να λαμβάνει τα ΔΠΧ που το αφορούν σε μορφότυπο κοινώς αναγνώσιμο όταν:

- η επεξεργασία βασίζεται σε συγκατάθεση και
- η επεξεργασία διενεργείται με αυτοματοποιημένα μέσα.

Σε περιπτώσεις που είναι τεχνικά εφικτό, ο ΥΔ μπορεί να ζητήσει την απευθείας διαβίβαση των ΔΠΧ από τον ένα στον άλλο ΥΠΕ. Μορφότυπος κοινός αναγνώσιμος θεωρείται π.χ. ο τύπος αρχείων CSV. Οι πληροφορίες πρέπει να παρέχονται δωρεάν. Εάν τα προσωπικά δεδομένα αφορούν περισσότερα από ένα άτομα, πρέπει να εξετασθεί κατά πόσο η παροχή των πληροφοριών θίγει τα δικαιώματα οποιουδήποτε άλλου ατόμου.

[Δείτε περισσότερα στα άρ.12,20, α.σ.68 του κανονισμού και στην γνωμοδότηση της ΟΕ29 «Κατευθυντήριες γραμμές σχετικά με το δικαίωμα στη φορητότητα των δεδομένων», (WP 242 rev.01)]

7. Δικαίωμα εναντίωσης

Είναι το δικαίωμα του υποκειμένου δεδομένων (ΥΔ) να αντιτάσσεται ανά πάσα στιγμή στην επεξεργασία των ΔΠΧ που το αφορούν. Πιο συγκεκριμένα έχει δικαίωμα να εναντιωθεί σε:

- επεξεργασία με βάση νόμιμα συμφέροντα ή εκπλήρωση καθήκοντος προς το δημόσιο συμφέρον / άσκηση δημόσιας εξουσίας (συμπεριλαμβανομένης της κατάρτισης προφίλ),
- επεξεργασία για σκοπούς απευθείας εμπορικής προώθησης (συμπεριλαμβανομένης της κατάρτισης προφίλ)· και

- επεξεργασία για επιστημονική / ιστορική έρευνα και στατιστικές εκτός εάν η επεξεργασία είναι απαραίτητη για λόγους δημόσιου συμφέροντος.

[Δείτε περισσότερα στα άρ.12,21 και α.σ. 69,70 του κανονισμού]

8. Δικαίωμα σχετικά με την αυτοματοποιημένη λήψη αποφάσεων και κατάρτιση προφίλ

Είναι το δικαίωμα του ΥΔ να μην υπόκειται σε απόφαση που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας, συμπεριλαμβανομένης της κατάρτισης προφίλ, η οποία παράγει έννομα αποτελέσματα που το αφορούν ή το επηρεάζει σημαντικά με παρόμοιο τρόπο. Η αυτοματοποιημένη ατομική λήψη αποφάσεων είναι μια απόφαση που γίνεται με αυτοματοποιημένα μέσα χωρίς ανθρώπινη εμπλοκή. Τέτοια παραδείγματα είναι :

- σύστημα online που λαμβάνει απόφαση χορήγησης δανείου,
- τεστ αξιολόγησης που λαμβάνει απόφαση για την πραγματοποίηση πρόσληψης

Η αυτοματοποιημένη ατομική λήψη αποφάσεων δεν προϋποθέτει τη δημιουργία προφίλ, συνήθως όμως συσχετίζεται με αυτή. Εξαιρούνται από το παραπάνω δικαίωμα όταν η απόφαση:

α) είναι αναγκαία για τη σύναψη ή την εκτέλεση σύμβασης μεταξύ του υποκειμένου των δεδομένων και του υπευθύνου επεξεργασίας των δεδομένων,

β) επιτρέπεται από το Εθνικό ή Ενωσιακό δίκαιο,

γ) βασίζεται στη ρητή συγκατάθεση του υποκειμένου των δεδομένων.

[Δείτε περισσότερα στα άρ. 4§4, 9, 12, 13, 14, 15, 21, 22, 35§1§321,22 του κανονισμού και στη γνώμοδότηση της ΟΕ29 “Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679», (WP 251 αναθ.01) 06/02/2018]

Πίνακας 2. Δικαιώματα Υποκείμενων Δεδομένων (ΥΔ)

Πίνακας δικαιωμάτων Υποκειμένων Δεδομένων (ΥΔ)						
Περιπτώσεις νομιμότητας επεξεργασίας ΔΠΧ	Δικαιώματα ΥΔ					
	1. Ενημέρωση 2. Πρόσβαση 3. Διόρθωση	**4. Διαγραφή**	**5. Περιορισμός επεξεργασίας**	**6. Φορητότητα**	**7. Εναντίωση**	**8. Ένσταση σε αυτοματοποιημένες αποφάσεις**
Συναίνεση (consent) άρ.6§1α	ΝΑΙ	ΝΑΙ άρ.17§1β	ΝΑΙ	ΝΑΙ άρ.20§1α	ΝΑΙ άρ.7§3	ΝΑΙ άρ.2m2§2γ
Εκτέλεση σύμβασης (contract) άρ.6§1β	ΝΑΙ	ΟΧΙ	ΟΧΙ	ΝΑΙ άρ.20§1α	ΟΧΙ	ΟΧΙ άρ.22§ 2α
Έννομη υποχρέωση (legal obligation) άρ.6§1γ	ΝΑΙ	ΟΧΙ άρ.17§3β	ΟΧΙ	ΟΧΙ	ΟΧΙ	ΟΧΙ άρ.22§ 2β
Ζωτικού συμφέροντος (vital interests) άρ.6§1δ	ΝΑΙ	ΟΧΙ	ΟΧΙ	ΟΧΙ	ΟΧΙ	Πιθανόν
Δημόσια εξουσία (public function) άρ.6§1ε	ΝΑΙ	ΟΧΙ άρ.17§3β	ΝΑΙ άρ.21§1	ΟΧΙ	ΝΑΙ άρ.21§1	ΝΑΙ
Έννομα συμφέροντα (legitimate interests) άρ.6§1στ	ΝΑΙ	ΟΧΙ άρ.17§3β	ΝΑΙ άρ.21§1	ΟΧΙ	ΝΑΙ άρ.21§1	Πιθανόν
Ανέφικτη εξακρίβωση ταυτότητας (unable identification) (άρ.11)	ΟΧΙ	ΟΧΙ	ΟΧΙ	ΟΧΙ	ΟΧΙ	ΟΧΙ
Αρχειοθέτηση για δημόσιο συμφέρον συμφέρον (public interest archiving purposes), (άρ.89 §1,2)	1. ΝΑΙ 2,3. ΟΧΙ	ΟΧΙ	ΟΧΙ	ΟΧΙ	ΟΧΙ	ΟΧΙ

1.2.6 Υποχρεώσεις οργανισμών - Λογοδοσία (ΥΠΕ / ΕΚΕ)

Ο κάθε οργανισμός που επεξεργάζεται ΔΠΧ έχει, ή αν δεν έχει πρέπει να ορίσει, έναν υπεύθυνο επεξεργασίας (ΥΠΕ).

Υπεύθυνος επεξεργασίας (ΥΠΕ) είναι το φυσικό ή νομικό πρόσωπο που καθορίζει τους σκοπούς και τον τρόπο επεξεργασίας ΔΠΧ.

Εκτελών την επεξεργασία (ΕΚΕ) είναι το φυσικό ή νομικό πρόσωπο που ορίζεται από τον υπεύθυνο επεξεργασίας (ΥΠΕ) να επεξεργάζεται για λογαριασμό του τα ΔΠΧ.

Ο διαχωρισμός του ΥΠΕ από τον ΕΚΕ πρέπει να είναι σαφής. Είναι σημαντικό να καθορίζεται το αντικείμενο επεξεργασίας, οι υποχρεώσεις και οι ευθύνες του καθένα.

Παράδειγμα: Μια τράπεζα (ΥΠΕ) συλλέγει δεδομένα των πελατών της όταν ανοίγουν λογαριασμό, ένας άλλος οργανισμός (ΕΚΕ) όμως ψηφιοποιεί και αποθηκεύει όλες τις πληροφορίες που καταγράφονται σε χαρτί για λογαριασμό της τράπεζας. Ο οργανισμός αυτός

μπορεί να είναι εταιρίες κέντρα αποθήκευσης (Data Centers) ή εταιρίες διαχείρισης εγγράφων. Και τα δυο αυτά πρόσωπα έχουν ευθύνη για τη διαχείριση των ΔΠΧ των πελατών της τράπεζας.

1.2.6.1 Υπεύθυνος επεξεργασίας (ΥΠΕ)

Ο ΥΠΕ έχει την ευθύνη για την επεξεργασία ΔΠΧ και για όλα όσα συνεπάγονται με αυτό (άρ.24). Θα πρέπει δηλαδή λαμβάνοντας υπόψη:

- τους σκοπούς επεξεργασίας
- τη φύση και το πεδίο εφαρμογής της,
- τους πιθανούς κινδύνους για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων.

Να μπορεί να:

α) εφαρμόζει τα κατάλληλα τεχνικά και οργανωτικά μέτρα και

β) αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τον κανονισμό (λογοδοσία).

Ο ΥΠΕ μπορεί να είναι ένα η πολλά φυσικά πρόσωπα εντός του οργανισμού.

[Δείτε περισσότερα στα άρ. 24-27 και 30 του κανονισμού]

1.2.6.2 Εκτελών την επεξεργασία (ΕΚΕ)

Ο εκτελών την επεξεργασία δεν απαλλάσσεται της ευθύνης της επεξεργασίας (άρ.28). Ο κανονισμός δίνει ιδιαίτερη μνεία στις υποχρεώσεις του, οι οποίες είναι οι εξής:

1. Ορίζει εκπρόσωπο αν δεν είναι εγκατεστημένος στη ΕΕ.
2. Περιλαμβάνει τις υποχρεώσεις στη σύμβαση με τον ΥΠΕ.
3. Δεν μπορεί να προσλάβει άλλον εκτελούντα αν δεν υπάρχει γραπτή άδεια από τον ΥΠΕ.
4. Δεσμεύεται ότι κάθε πρόσωπο που έχει πρόσβαση στα ΔΠΧ και εκτελεί την επεξεργασία ενεργεί υπό την εποπτεία του.
5. Διατηρεί αρχείο δραστηριοτήτων εκ μέρους του ΥΠΕ.
6. Συνεργάζεται με τις εποπτικές αρχές.
7. Υλοποιεί κατάλληλα τεχνικά και οργανωτικά μέτρα για την ασφάλεια της επεξεργασίας.
8. Ενημερώνει τον ΥΠΕ αμελλητί για την παραβίαση ΔΠΧ.
9. Ορίζει ΥΠΔ όπου κρίνεται αναγκαίο λόγω της επεξεργασίας.
10. Συμμορφώνεται με τους κανόνες διαβίβασης ΔΠΧ εκτός ΕΕ.

[Δείτε περισσότερα στα άρ.28-30 του κανονισμού]

1.2.6.3 Αρχείο δραστηριοτήτων επεξεργασίας

Ο ΥΠΕ και ΕΚΕ είναι υποχρεωμένοι να διατηρούν αρχείο δραστηριοτήτων επεξεργασίας αν ισχύει κάτι από τα παρακάτω[4]:

α) απασχολεί πάνω από 250 άτομα,

β) η επεξεργασία του ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες ΥΔ,

γ) η επεξεργασία δεν είναι περιστασιακή,

δ) εκτελείται επεξεργασία ΔΠΧ ειδικών κατηγοριών.

Στον κανονισμό προσδιορίζονται συγκεκριμένες πληροφορίες που θα πρέπει να περιλαμβάνονται στο αρχείο δραστηριοτήτων επεξεργασίας συγκεκριμένα για τον ΥΠΕ και για τον ΕΚΕ.

[Δείτε περισσότερα στα άρ.30 και α.σ.82 του κανονισμού]

1.2.6.4 Προστασία δεδομένων από σχεδίαση κ εξ 'ορισμού

Ο ΥΠΕ έχει την ευθύνη της προστασίας των δεδομένων από τη σχεδίαση (by design) και εξ' ορισμού (by default) κατά τη στιγμή του καθορισμού των μέσων επεξεργασίας όσο και κατά την επεξεργασία. Η χρήση εγκεκριμένων πιστοποιήσεων είναι στοιχεία που μπορούν να αποδεικνύουν τις συμμορφώσεις στις απαιτήσεις αυτές (άρ. 25).

1.2.6.5 Γνωστοποίηση παραβίασης ΔΠΧ

Σε περίπτωση παραβίασης ΔΠΧ, ο ΥΠΕ εκτιμώντας ότι η παραβίαση ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων θα πρέπει (άρ. 33,34):

α) να το γνωστοποιήσει στην ΑΠΔΠΧ εντός 72 ωρών από τη στιγμή της παραβίασης. Η γνωστοποίηση θα περιλαμβάνει στοιχεία σχετικά με την παραβίαση, τα στοιχεία επικοινωνίας ΥΠΕ, τις συνέπειες, τα ληφθέντα και προτεινόμενα μέτρα.

β) να το γνωστοποιήσει στο υποκείμενο δεδομένων (ΥΔ). Η γνωστοποίηση θα περιλαμβάνει τα στοιχεία επικοινωνίας ΥΠΕ, τις συνέπειες, τα ληφθέντα και προτεινόμενα μέτρα.

[Δείτε περισσότερα στα άρ.33,34,58,83 και α.σ.75,78-88 του κανονισμού]

[4] «Υποχρεώσεις συμμόρφωσης στον Γενικό Κανονισμό Προσωπικών Δεδομένων (GDPR) και ο ρόλος του Υπευθύνου Προστασίας Δεδομένων (DPO)» Γρηγόρης Τσόλιας Μέλος (αν.) της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα 29/03/2017 σ.21 www.infocomsecurity.gr/presentations/2017/day1/tsolias.pdf 7ο INFOCOM SECURITY CONFERENCE 2017 (τελευταία πρόσβαση 09/07/2017)

1.2.6.6 Εκτίμηση Αντικτύπου Προστασίας Δεδομένων (ΕΑΠΔ/DPIA)

Ένα από τα κυριότερα εργαλεία προστασίας της επεξεργασίας ΔΠΧ και της απόδειξης συμμόρφωσης με τον κανονισμό είναι η διενέργεια Εκτίμηση Αντικτύπου Προστασίας Δεδομένων (ΕΑΠΔ / DPIA) (άρ.35,36). Η εκτίμηση αυτή απαιτείται στις περιπτώσεις που ενέχονται υψηλοί κίνδυνοι για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Τέτοιοι είναι:

α) συστηματική επεξεργασία ΔΠΧ που επηρεάζουν το φυσικό πρόσωπο,

β) μεγάλης κλίμακα επεξεργασία ΔΠΧΕΚ,

γ) συστηματική παρακολούθηση δημόσιου χώρου σε μεγάλη κλίμακα π.χ. κάμερες.

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) πρόκειται να δημοσιοποιήσει πλήρη σχετικό κατάλογο με είδη πράξεων που δεν απαιτείται ΕΑΠΔ.

Άλλα σημεία άξια αναφοράς είναι ότι :

- Ο ΥΠΕ ζητά τη γνώμη του ΥΠΔ σχετικά με τη διενέργεια εκτίμησης αντικτύπου,
- Ο ΥΠΕ ζητά τη γνώμη της ΑΠΔΠΧ (διαβούλευση) όταν η ΕΑΠΔ υποδεικνύει υψηλό κίνδυνο που δεν μπορεί να μετριαστεί με μέτρα από τον ΥΠΕ. Το αίτημα της διαβούλευσης με την ΑΠΔΠΧ θα πρέπει να απαντηθεί το πολύ εντός 14 εβδομάδων.

[Δείτε περισσότερα στα άρ.35,36,83, α.σ.84,89-96 του κανονισμού , και στη γνωμοδότηση της ΟΕ29 « Κατευθυντήριες γραμμές για την εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) και καθορισμός του κατά πόσον η επεξεργασία «ενδέχεται να επιφέρει υψηλό κίνδυνο» για τους σκοπούς του κανονισμού 2016/679.», (WP 248 αναθ.01) 04/10/2017]

1.2.6.7 Κώδικες δεοντολογίας

Ο ΥΠΕ και ΕΚΕ ενδείκνυται να ακολουθούν εγκεκριμένους κώδικες δεοντολογίας που έχουν στόχο να συμβάλουν στην ορθή εφαρμογή του κανονισμού. Οι εγκεκριμένοι κώδικες δεοντολογίας προκύπτουν από ενώσεις ή άλλους φορείς που εκπροσωπούν κατηγορίες ΥΠΕ ή ΕΚΕ αφού υποβάλουν στην ΑΠΔΠΧ το σχέδιο ώστε να ελεγχθεί, διορθωθεί και τέλος εγκριθεί.

Σε περίπτωση που το σχέδιο κώδικα δεοντολογίας αναφέρεται σε επεξεργασία σε άλλα κράτη μέλη η ΑΠΔΠΧ το υποβάλλει προς γνωμοδότηση στο Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων -European Data Protection Board (ΕΣΠΔ / EDPB). Εάν η γνωμοδότηση επιβεβαιώνει ότι είναι σύμφωνη με τον κανονισμό, το ΕΣΠΔ διαβιβάζει τη γνώμη του στην Ευρωπαϊκή Επιτροπή - European Commission (ΕΕΠ / EC). Αυτή με τη σειρά της έχει τη δυνατότητα, μέσω εκτελεστικών πράξεων να ορίσει τη γενική ισχύ του κώδικα εντός της ΕΕ.

[Δείτε περισσότερα στα άρ.40-43 α.σ.98-100,148,150,151 του κανονισμού]

1.2.6.8 Πιστοποίηση

Ο κανονισμός, μέσω των κρατών μελών, τις εποπτικές αρχές, το συμβούλιο προστασίας δεδομένων (EDPB / ΕΣΠΔ) και την Ευρωπαϊκή Επιτροπή, παροτρύνει τη θέσπιση μηχανισμών πιστοποίησης. Η πιστοποίηση είναι εθελοντική και διαθέσιμη μέσω διαφανούς διαδικασίας. Είναι ένα ακόμα εργαλείο, για τον ΥΠΕ και ΕΚΕ, απόδειξης συμμόρφωσης με τον κανονισμό αλλά δεν περιορίζει τις ευθύνες τους σχετικά με τη συμμόρφωση. Η πιστοποίηση χορηγείται για μέγιστη περίοδο τριών ετών και μπορεί να ανανεωθεί με τους ίδιους όρους με την προϋπόθεση ότι εξακολουθούν να πληρούνται οι σχετικές απαιτήσεις. Πιστοποίηση χορηγεί η ΑΠΔΠΧ ή το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (EDPB / ΕΣΠΔ) ή φορέας πιστοποίησης ο οποίος έχει πρώτα εγκριθεί από την ΑΠΔΠΧ ή και, από τον εθνικό οργανισμό διαπίστευσης (για την Ελλάδα Εθνικό Σύστημα Διαπίστευσης Ε.ΣΥ.Δ.) σύμφωνα με το EN ISO/IEC 17065:2012. Η Ευρωπαϊκή Επιτροπή ορίζει τα τεχνικά πρότυπα για τους μηχανισμούς πιστοποίησης, σφραγίδες και σήματα προστασίας δεδομένων (άρ.42,43).

[Δείτε περισσότερα στα άρ.40-43 α.σ.98-100,148,150,151 του κανονισμού]

1.2.6.9 Διαβιβάσεις σε τρίτες χώρες

Ο ΥΠΕ ή ΕΚΕ βάσει του κανονισμού μπορεί να διαβιβάσει δεδομένα εντός της ΕΕ. Για τις διαβιβάσεις εκτός ΕΕ υπάρχουν επιτρεπόμενες περιπτώσεις. Συνολικά όλες οι περιπτώσεις διαβιβάσεων δεδομένων εκτός χώρας αναφέρονται αναλυτικά στον παρακάτω πίνακα.

[Δείτε περισσότερα στα άρ.49 και α.σ.113 του κανονισμού]

Πίνακας 3. Επιτρεπόμενοι τρόποι διαβιβάσεων δεδομένων εκτός ΕΕ ή ΕΟΧ

Επιτρεπόμενοι τρόποι διαβιβάσεων δεδομένων (άρ. 44-50)			
α/α	**Διαβίβαση βάσει**	**Χώρα**	**Παρατηρήσεις**
1	Παρόντος κανονισμού (ΓΚΠΔ/GDPR)	Κράτη μέλη Ευρωπαϊκής Ένωσης – Ευρωπαϊκού Οικονομικού Χώρου (Ισλανδία, Λίχτενσταϊν Νορβηγία)	
2	Ασπίδα Προστασίας ΕΕ-ΗΠΑ για την ιδιωτικότητα (Privacy Shield)	ΗΠΑ	Ευθύνη εταιιών να συμμορφωθούν με υποχρεώσεις και εγγυήσεις του

			μηχανισμού “Privacy Shield”
3	Αποφάσεις Επάρκειας Ευρωπαϊκής Επιτροπής (Τελευταία ενημέρωση: 06/02/2018) (Commission Adequacy Decisions)	AD – Ανδόρα AR – Αργεντινή CA – Καναδάς CH – Ελβετία FO – Νήσοι Φερόες GG - Γκέρνσεϊ IL - Ισραήλ IM – Νήσος του Μάν JE - Τζέρσεϊ NZ - Νέα Ζηλανδία UY - Ανατολική Δημοκρατία της Ουρουγουάης JP - Ιαπωνία	Η Ευρωπαϊκή επιτροπή αποφασίζει αν η χώρα που θα διαβιβασθούν τα ΔΠΧ πληροί τις προϋποθέσεις
4	Νομικό δεσμευτικό εκτελεστό μέσο μεταξύ δημόσιων αρχών ή φορέων (άρ.46§2α)	Οποιαδήποτε χώρα	Δε χρειάζεται άδεια από την ΑΠΔΠΧ. Κατά περίπτωση δεσμευτικοί κανόνες
5	Εταιρικοί Δεσμευτικοί Κανόνες (Binding Corporate Rules - BCR) (άρ.47)	Οποιαδήποτε χώρα	Δε χρειάζεται άδεια από την ΑΠΔΠΧ
6	Πρότυπες Συμβατικές Ρήτρες της Επιτροπής (Standard Contractual Clauses) (άρ.46§2γ)	Οποιαδήποτε χώρα	Δε χρειάζεται άδεια από την ΑΠΔΠΧ
7	Πρότυπες Συμβατικές Ρήτρες της ΑΠΔΠΧ (Standard Contractual Clauses) (άρ.46§2δ)	Οποιαδήποτε χώρα	Δε χρειάζεται άδεια από την ΑΠΔΠΧ
8	Εγκεκριμένος κώδικας δεοντολογίας (άρ.46§2ε)	Οποιαδήποτε χώρα	Δε χρειάζεται άδεια από την ΑΠΔΠΧ
9	Εγκεκριμένος μηχανισμός πιστοποίησης (άρ.46§2στ)	Οποιαδήποτε χώρα	Με την επιφύλαξη της άδειας από την ΑΠΔΠΧ
10	Συμβατικές ρήτρες μεταξύ ΥΠΕ η ΕΚΕ ή αποδέκτη ΔΠΧ τρίτης χώρας ή διεθνή οργανισμό (άρ.46§3α)	Οποιαδήποτε χώρα	Με την επιφύλαξη της άδειας από την ΑΠΔΠΧ
11	Διατάξεων σε διοικητικές ρυθμίσεις μεταξύ δημόσιων αρχών ή φορέων	Οποιαδήποτε χώρα	-
12	Ρητή συγκατάθεση του ΥΔ για διαβίβαση στη συγκεκριμένη χώρα	Οποιαδήποτε χώρα	-
13	Εκτέλεση σύμβασης (ή προσυμβατικά μέτρα) μεταξύ ΥΔ και ΥΠΕ	Οποιαδήποτε χώρα	-

14	Εκτέλεση σύμβασης προς όφελος του ΥΔ μεταξύ ΥΠΕ και άλλου φυσικού/νομικού προσώπου	Οποιαδήποτε χώρα	-
15	Σημαντικούς λόγους Δημόσιου Συμφέροντος	Οποιαδήποτε χώρα	
16	Θεμελίωση , άσκηση ή υποστήριξη νομικών αξιώσεων	Οποιαδήποτε χώρα	-
17	Προστασία ζωτικών συμφερόντων του ΥΔ	Οποιαδήποτε χώρα	-

1.2.7 Άλλοι εμπλεκόμενοι φορείς

1.2.7.1 Υπεύθυνος Προστασίας Δεδομένων (ΥΠΔ / DPO)

Ο ΥΠΕ και ΕΚΕ θα πρέπει να ορίσουν Υπεύθυνο Προστασίας Δεδομένων - Data Protection Officer (ΥΠΔ / DPO) εάν η επεξεργασία διενεργείται (άρ 37):

α) από δημόσια αρχή ή δημόσιο φορέα
(συμπεριλαμβανομένων και φυσικών ή νομικών προσώπων δημοσίου ή ιδιωτικού δικαίου που ασκούν δημόσια εξουσία). Εξαιρούνται τα δικαστήρια όταν ενεργούν υπό τη δικαιοδοτική τους αρμοδιότητα,

β) με τακτική και συστηματική παρακολούθηση υποκειμένων των δεδομένων σε μεγάλη κλίμακα
(π.χ. ασφαλιστικές ή τραπεζικές υπηρεσίες, υπηρεσίες τηλεφωνίας ή διαδικτύου, παροχή υπηρεσιών ασφαλείας, όλες οι μορφές παρακολούθησης και διαμόρφωσης «προφίλ» στο διαδίκτυο, όπως για σκοπούς συμπεριφορικής διαφήμισης),

γ) σε ΔΠΧΕΚ σε μεγάλη κλίμακα
(π.χ. στο πλαίσιο παροχής υπηρεσιών υγείας από νοσοκομεία),

δ) σε ΔΠΧ που αφορούν ποινικές καταδίκες και αδικήματα.

«Τακτική και συστηματική παρακολούθηση υποκειμένων» θεωρείται π.χ. διαδικτυακή έρευνα συμπεριφοράς, profiling, εντοπισμός θέσης μέσω δεδομένων κινητού τηλεφώνου, κάρτες «επιβράβευσης πίστης» (“loyaltycards”) κτλ.

Για τον προσδιορισμό της «μεγάλης κλίμακας» επεξεργασίας πρέπει να λαμβάνονται υπόψη: α) ο αριθμός των εμπλεκομένων υποκειμένων, είτε ως συγκεκριμένος αριθμός είτε ως ποσοστό επί του πληθυσμού, β) ο όγκος και το εύρος των δεδομένων, γ) η διάρκεια ή ο μόνιμος χαρακτήρας της επεξεργασίας, δ) η γεωγραφική έκταση της επεξεργασίας.

Παραδείγματα που δεν συνιστούν επεξεργασία μεγάλης κλίμακας είναι, μεταξύ άλλων, η επεξεργασία δεδομένων ασθενών από ιδιώτη ιατρό και η επεξεργασία δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα από ιδιώτη δικηγόρο.

Ο ΥΠΔ μπορεί να είναι μέλος του προσωπικού του ΥΠΕ ή ΕΚΕ ή να ασκεί τα καθήκοντα του βάσει σύμβασης παροχής υπηρεσιών. Ο ΥΠΕ και ΕΚΕ διασφαλίζουν τους απαραίτητους πόρους στον ΥΠΔ για την άσκηση των εν λόγω καθηκόντων του. Ο ΥΠΔ λειτουργεί ανεξάρτητα και δεν απολύεται ούτε υφίσταται κύρωση από τον ΥΠΕ / ΕΚΕ σχετικά με την επιτέλεση των καθηκόντων του, αναφέρεται - λογοδοτεί απευθείας στο ανώτερο επίπεδο διοίκησης του οργανισμού (π.χ. Διοικητικό επίπεδο) και δεσμεύεται για την τήρηση απορρήτου ή της εμπιστευτικότητας σχετικά με την εκτέλεση των καθηκόντων του.

Τα καθήκοντα του ΥΠΔ είναι να:

α) ενημερώνει και να συμβουλεύει τον ΥΠΕ ή ΕΚΕ και τους υπαλλήλους που επεξεργάζονται ΔΠΧ για τις υποχρεώσεις τους που απορρέουν από τον κανονισμό και από άλλες σχετικές διατάξεις για την προστασία δεδομένων,

β) παρακολουθεί τη συμμόρφωση με τον κανονισμό και με τις πολιτικές του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία σε σχέση με την προστασία των δεδομένων προσωπικού χαρακτήρα,

γ) παρέχει συμβουλές, όταν ζητείται, όσον αφορά την εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων και παρακολουθεί την υλοποίησή της,

δ) συνεργάζεται με την εποπτική αρχή και ενεργεί ως σημείο επικοινωνίας για ζητήματα που σχετίζονται με την επεξεργασία ΔΠΧ,

ε) ενεργεί ως σημείο επικοινωνίας για τα ΥΔ των οποίον έχει γίνει επεξεργασία των προσωπικών τους δεδομένων (πελάτες, εργαζόμενοι κτλ.),

στ) συντάσσει ετήσια έκθεση δραστηριοτήτων του ΥΠΕ και την υποβάλει στο ανώτερο διοικητικό επίπεδο του οργανισμού.

[Δείτε περισσότερα στα άρ.37-39,83, α.σ.97 του κανονισμού και γνωμοδότηση της ΟΕ29 «Κατευθυντήριες γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων»(WP 243 αναθ.01) 05/04/2017]

1.2.7.2 Φορέας πιστοποίησης

Φορέας πιστοποίησης είναι ο οργανισμός που διαθέτει το ενδεδειγμένο επίπεδο εμπειρογνωμοσύνης σε σχέση με την προστασία των δεδομένων. Η διαπίστευση των φορέων

πιστοποίησης μπορεί να γίνει από την ΑΠΔΠΧ ή και από τον εθνικό οργανισμό διαπίστευσης σύμφωνα με το EN ISO/IEC 17065:2012 και έχει μέγιστη περίοδο πέντε έτη με δυνατότητα ανανέωσης (άρ.43).

Ο φορέας πιστοποίησης θα πρέπει:

α) να έχει αποδείξει την ανεξαρτησία και την εμπειρογνωμοσύνη του σε σχέση με το αντικείμενο του κώδικα κατά την κρίση της ΑΠΔΠΧ,

β) να έχει δεσμευτεί στην τήρηση των κριτηρίων της πιστοποίησης,

γ) να έχει θεσπίσει διαδικασίες για την έκδοση, επανεξέταση και ανάκληση πιστοποιητικών σφραγίδων και σημάτων προστασίας δεδομένων,

δ) να έχει θεσπίσει διαδικασίες και δομές για την αντιμετώπιση καταγγελιών περί παραβάσεων του κώδικα ή περί του τρόπου με τον οποίον ο κώδικας έχει εφαρμοστεί ή εφαρμόζεται από έναν υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία, καθώς και για να καταστούν οι διαδικασίες και οι δομές αυτές διαφανείς στα υποκείμενα των δεδομένων και στο ευρύ κοινό,

ε) να αποδεικνύει, κατά την κρίση της αρμόδιας εποπτικής αρχής, ότι τα καθήκοντα και οι υποχρεώσεις του δεν συνεπάγονται σύγκρουση συμφερόντων.

Στην Ελλάδα, δεν υπάρχουν διαπιστευμένοι φορείς για να πιστοποιούν επαγγελματικά προσόντα / δεξιότητες ή συμμόρφωση στον ΓΚΔΠ/GDPR (τελευταία επίσημη ενημέρωση 09/08/2017)[5].

[Δείτε περισσότερα στο άρ.43 του κανονισμού]

1.2.7.3 Φορέας παρακολούθησης κωδίκων δεοντολογίας

Ο φορέας παρακολούθησης των εγκεκριμένων κωδίκων δεοντολογίας διαθέτει το ενδεδειγμένο επίπεδο εμπειρογνωμοσύνης σε σχέση με το αντικείμενο του κώδικα και είναι διαπιστευμένος για το σκοπό αυτό από την αρμόδια εποπτική αρχή. Για την Ελλάδα η αρμόδια εποπτική αρχή είναι η ΑΠΔΠΧ.

Ο φορέας παρακολούθησης κωδίκων δεοντολογίας θα πρέπει:

α) να έχει αποδείξει την ανεξαρτησία και την εμπειρογνωμοσύνη του σε σχέση με το αντικείμενο του κώδικα κατά την κρίση της ΑΠΔΠΧ,

[5] *Ανακοίνωσή της ΑΠΧΠΧ Αρ. πρωτ.: Γ/ΕΞ/6007 09/08/2017 http://www.dpa.gr/APDPXPortlets/htdocs/documentSDisplay.jsp?docid=81,138,99,231,213,1,187,76* (τελευταία πρόσβαση 12/01/2018)

β) να έχει καθιερώσει διαδικασίες που του επιτρέπουν την εκτίμηση της επιλεξιμότητας των σχετικών υπευθύνων επεξεργασίας (ΥΠΕ) και των εκτελούντων την επεξεργασία (ΕΚΕ) προκειμένου να εφαρμόσουν τον κώδικα, την παρακολούθηση της συμμόρφωσής τους με τις διατάξεις του και την περιοδική επανεξέταση της λειτουργίας του,

γ) να έχει θεσπίσει διαδικασίες και δομές για την αντιμετώπιση καταγγελιών περί παραβάσεων του κώδικα ή περί του τρόπου με τον οποίον ο κώδικας έχει εφαρμοστεί ή εφαρμόζεται από έναν υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία, καθώς και για να καταστούν οι διαδικασίες και οι δομές αυτές διαφανείς στα υποκείμενα των δεδομένων και στο ευρύ κοινό και

δ) να αποδεικνύει, κατά την κρίση της αρμόδιας εποπτικής αρχής, ότι τα καθήκοντα και οι υποχρεώσεις του δεν συνεπάγονται σε σύγκρουση συμφερόντων.

[Δείτε περισσότερα στο άρ.41 του κανονισμού]

1.2.7.4 Ανεξάρτητη εποπτική αρχή Ελλάδας - Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ)

Η εποπτική αρχή - ανεξάρτητη δημόσια αρχή - για την Ελλάδα είναι η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ). Είναι συνταγματικά κατοχυρωμένη ανεξάρτητη αρχή και ιδρύθηκε με το νόμο 2472/1997.

Τα καθήκοντα της αρχής είναι:

1. η παρακολούθηση και επιβολή του κανονισμού,
2. η προώθηση της ευαισθητοποίησης του κοινού σχετικά με τα ΔΠΧ,
3. η συμβουλευτική στα όργανα του κράτους σχετικά με την προστασία δικαιωμάτων και ελευθεριών των φυσικών προσώπων,
4. η προώθηση ευαισθητοποίησης ΥΠΕ και ΕΚΕ,
5. η παροχή πληροφοριών στα ΥΔ σχετικά με τα δικαιώματα τους,
6. να χειρίζεται και να διευκολύνει τις καταγγελίες,
7. να συνεργάζεται με άλλες εποπτικές αρχές,
8. οι έρευνες για την εφαρμογή του κανονισμού,
9. η παρακολούθηση των εξελίξεων σχετικά με την προστασία ΔΠΧ,
10. να θεσπίζει ρήτρες σχετικά με ΕΚΕ και διαβιβάσεις δεδομένων,
11. να καταρτίζει κατάλογο για την απαίτηση διενέργειας ΕΑΠΔ/DPIA,
12. να παρέχει συμβουλές σχετικά με ΕΑΠΔ/DPIA – Διαβούλευση,
13. να ενθαρρύνει και να εγκρίνει κώδικες δεοντολογίας,

14. να ενθαρρύνει και να εγκρίνει μηχανισμούς πιστοποιήσεων ΔΠΧ και κριτήρια αυτών,
15. να διενεργεί επανεξέταση πιστοποιήσεων,
16. να σχεδιάζει και να δημοσιεύει κριτήρια διαπίστευσης φορέα για την παρακολούθηση κωδίκων δεοντολογίας,
17. να διενεργεί τη διαπίστευση φορέα για την παρακολούθηση κωδίκων δεοντολογίας,
18. να επιτρέπει συμβατικές ρήτρες για διαβιβάσεις δεδομένων εκτός ΕΕ,
19. να εγκρίνει δεσμευτικούς εταιρικούς κανόνες,
20. να συμβάλει στις δραστηριότητες του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων (ΕΣΠΔ/EDPB),
21. να τηρεί εσωτερικά αρχεία των παραβιάσεων του κανονισμού και των μέτρων που λήφθηκαν,
22. να εκπληρώνει κάθε άλλο καθήκον σχετικό με την προστασία ΔΠΧ.

Οι εξουσίες που διαθέτει κάθε αρχή είναι σε τρεις κατηγορίες:

α) Έρευνας: διεξάγει έρευνες σχετικά με τη συμμόρφωση στον κανονισμό.
β) Διορθωτικές: απευθύνει προειδοποιήσεις - επιπλήξεις - εντολές συμμόρφωσης - διόρθωσης - διαγραφής και διοικητικά πρόστιμα.
γ) Συμβουλευτικές: παρέχει συμβουλές σχετικά με το κανονισμό.

Η κάθε αρχή συνεργάζεται με τις άλλες ενδιαφερόμενες εποπτικές αρχές ανταλλάσσοντας κάθε συναφή πληροφορία και διεξάγοντας κοινές επιχειρήσεις και έρευνες.
[Δείτε περισσότερα στο άρ.51-59 του κανονισμού]

Εξυπηρέτηση μιας στάσης και μηχανισμός συνεκτικότητας

Ο οργανισμός - επιχείρηση που δραστηριοποιείται σε περισσότερα του ενός κράτους μέλους εποπτεύεται από μια εποπτική αρχή, ονομαζόμενη ως επικεφαλής εποπτική αρχή (Lead authority). Έτσι δε χρειάζεται να απευθύνεται σε όλες τις εποπτικές αρχές των χωρών κρατών μελών που έχει δραστηριότητες (εξυπηρέτηση μιας στάσης - One stop shop).

Για να υπάρχει συνεκτική εφαρμογή του κανονισμού οι εποπτικές αρχές συνεργάζονται μεταξύ τους με γνωμοδοτικό και συντονιστικό ρόλο να έχει το «Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων» (European Data Protection Board) ΕΣΠΔ / EDPB). Όλες οι διαδικασίες αυτές ονομάζονται μηχανισμός συνεκτικότητας (consistency mechanism).

1.2.7.5 Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (ΕΣΠΔ / EDPB) και η Ομάδα Εργασίας του άρθρου 29 (ΟΕ29 / WP29)

Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων -European Data Protection Board (ΕΣΠΔ / EDPB) συστήνεται ως όργανο της Ευρωπαϊκής Ένωσης και διαθέτει νομική προσωπικότητα. Πρόκειται να αντικαταστήσει την «Ομάδα Εργασίας του άρθρου 29» - Working Party by article 29 (ΟΕ29 / WP29). Η ομάδα εργασίας του άρθρου 29 είναι ένα ανεξάρτητο συμβουλευτικό σώμα που ασχολείται με την προστασία των δεδομένων προσωπικού χαρακτήρα και την ιδιωτικότητα στην Ευρωπαϊκή Ένωση. Συστάθηκε με βάση το άρθρο 29 της Οδηγίας 95/46/ΕΚ.

Το ΕΣΠΔ εκπροσωπείται από τον πρόεδρό του και απαρτίζεται από:

- τον προϊστάμενο της εποπτικής αρχής κάθε κράτους μέλους
- τον Ευρωπαίο Επόπτη Προστασίας Δεδομένων - European Data Protection Supervisor (ΕΕΠΔ / EDPS) με δικαίωμα ψήφου μόνο για τις αποφάσεις που αφορούν τις αρχές και τους κανόνες για τα θεσμικά όργανα, τους φορείς, τις υπηρεσίες και τους οργανισμούς της Ευρωπαϊκής Ένωσης. Ο ΕΕΠΔ διασφαλίζει ότι κατά την επεξεργασία προσωπικών δεδομένων, τα όργανα και οι οργανισμοί της ΕΕ σέβονται το δικαίωμα των πολιτών για προστασία της ιδιωτικής ζωής.
- Εκπρόσωπο της Ευρωπαϊκής Επιτροπής χωρίς δικαίωμα ψήφου στις δραστηριότητες και στις συνεδριάσεις του Συμβουλίου Προστασίας Δεδομένων.

Πίνακας 4. Σύνθεση του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων (ΕΣΠΔ / EDPB)

Μέλη Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων (ΕΣΠΔ / EDPB)	Αριθμός μελών
Προϊστάμενοι αρχών	28
Ευρωπαίος Επόπτης Προστασίας Δεδομένων (ΕΕΠΔ / EDPS)	1
Εκπρόσωπος της Ευρωπαϊκής Επιτροπής	1
Σύνολο	**30**

Ο πρόεδρος μαζί με δυο αναπληρωτές εκλέγονται από τα μέλη του ΕΣΠΔ , έχει πενταετή θητεία και ανανέωση άπαξ.

Το ΕΣΠΔ έχει τα εξής κύρια καθήκοντα:

α) συντονιστικό ρόλο μεταξύ των αρχών των κρατών μελών ώστε να διασφαλίζεται η ορθή και συνεκτική εφαρμογή του κανονισμού (μηχανισμός συνεκτικότητας),

β) συμβουλευτικό ρόλο προς την Ευρωπαϊκή επιτροπή,

γ) εκδίδει κατευθυντήριες γραμμές, συστάσεις και βέλτιστες πρακτικές για την καλύτερη εφαρμογή του κανονισμού,

δ) γνωμοδοτεί στην Ευρωπαϊκή Επιτροπή για θέματα σχετικά με τον κανονισμό,

ε) εκπονεί ετήσια έκθεση για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας στην Ένωση.

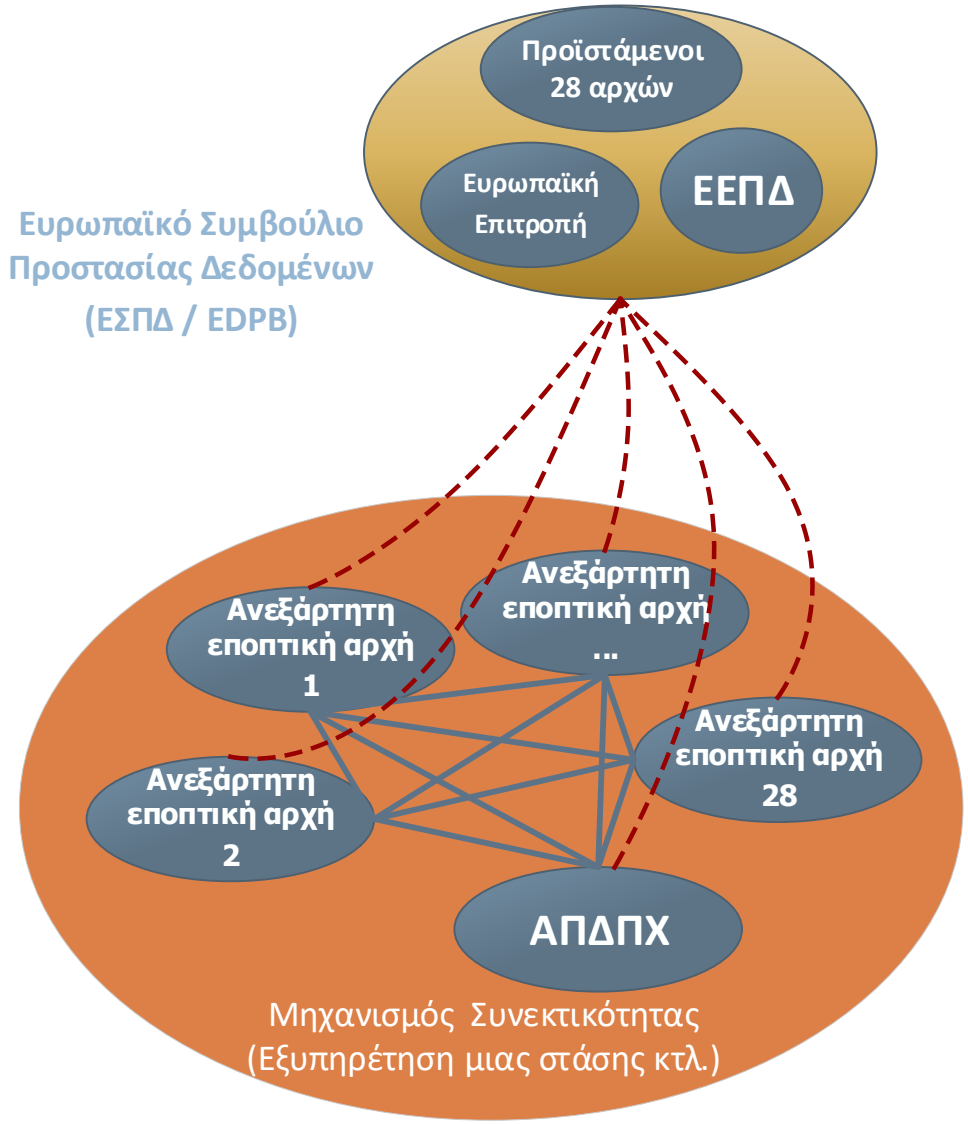
[Δείτε περισσότερα στα άρ.68-76 του κανονισμού]

Η ομάδα εργασίας εκδίδει κατευθυντήριες γραμμές σχετικά με συστάσεις και βέλτιστες πρακτικές για την καλύτερη εφαρμογή του κανονισμού. Έχει εκδώσει συνολικά εννιά κατευθυντήριες γραμμές (τελευταία ενημέρωση 15/02/2018)

Πίνακας 5. Κατευθυντήριες γραμμές της Ομάδα Εργασίας του άρθρου 29 (OE29 / WP29)

	Αριθμός εγγράφου	Ημερομηνία	Θέμα
1	WP 244 αναθ.01	05/04/2017	Επικεφαλής εποπτική αρχή, Κατευθυντήριες γραμμές για τον προσδιορισμό της επικεφαλής εποπτικής αρχής των υπευθύνων επεξεργασίας ή των εκτελούντων την επεξεργασία
2	WP242 αναθ.01	5/04/2017	Δικαίωμα φορητότητας δεδομένων, Κατευθυντήριες γραμμές σχετικά με το δικαίωμα στη φορητότητα των δεδομένων
3	WP243 αναθ.01	5/04/2017	Υπεύθυνοι Προστασίας Δεδομένων ('DPOs'), Κατευθυντήριες γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων
4	WP250	03/10/2017	Γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα Guidelines on Personal data breach notification under Regulation 2016/679
5	WP253	03/10/2017	Εφαρμογή και καθορισμός διοικητικών προστίμων Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679
6	WP248 αναθ.01	4/10/2017	Εκτίμηση επιπτώσεων στην προστασία δεδομένων, Κατευθυντήριες γραμμές για την εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) και καθορισμός του κατά

			πόσον η επεξεργασία «ενδέχεται να επιφέρει υψηλό κίνδυνο» για τους σκοπούς του κανονισμού 2016/679
7	WP251 αναθ.01	06/02/2018	Αυτοματοποιημένη ατομική λήψη αποφάσεων και κατάρτιση προφίλ, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679
8	WP259	-	Συγκατάθεση (σε διαβούλευση έως 23/01/2018), Guidelines on Consent under Regulation 2016/679
3	WP260	-	Διαφάνεια (σε διαβούλευση έως 23/01/2018), Guidelines on transparency under Regulation 2016/679



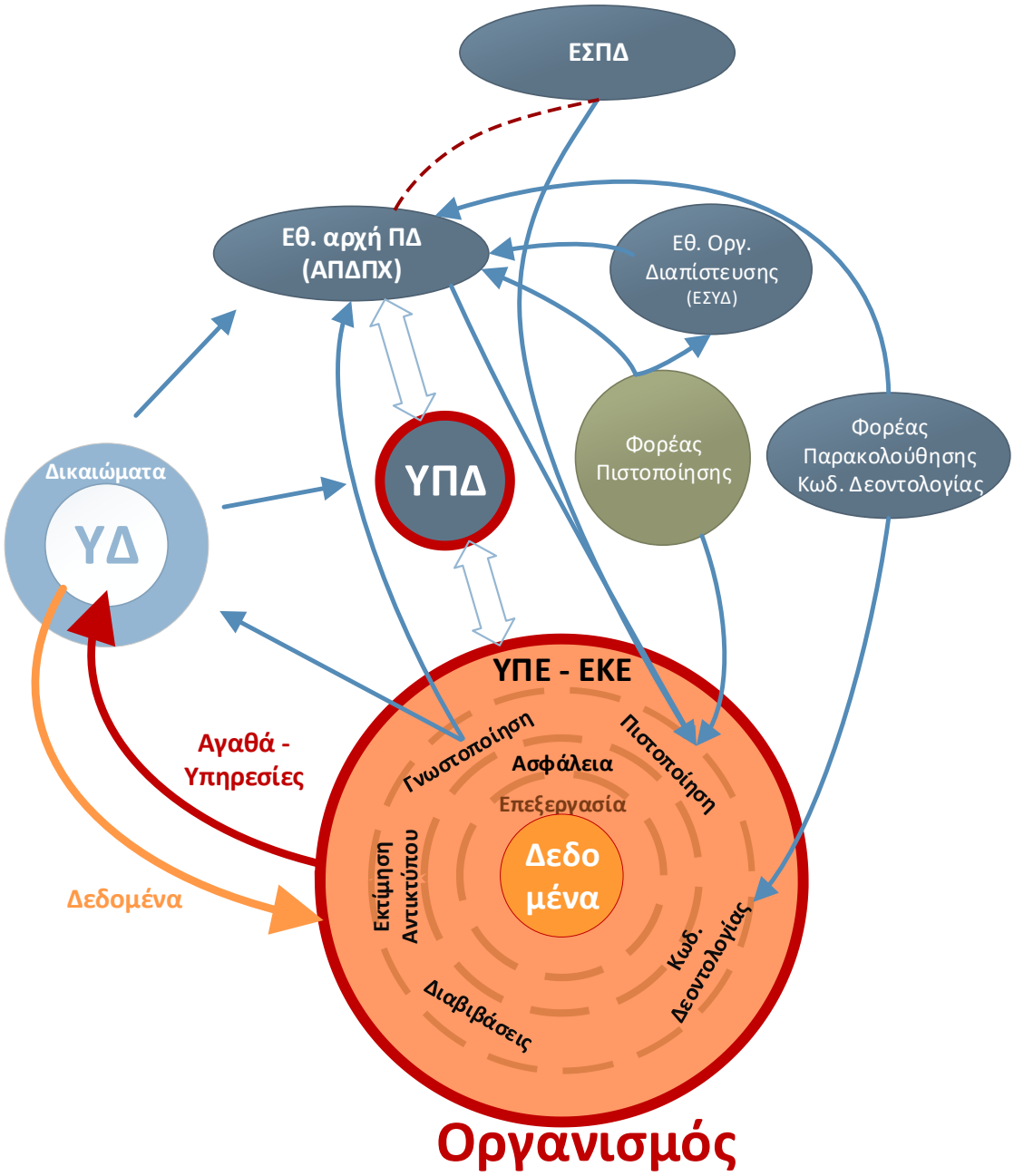
Διάγραμμα 2. Απεικόνιση μηχανισμού συνεκτικότητας και Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων (ΕΣΠΔ / EDPB)

1.2.7.6 Ευρωπαϊκή Επιτροπή (ΕΕΠ / EC)

Η Ευρωπαϊκή Επιτροπή - European Commission (ΕΕΠ / EC) έως τις 25 Μαΐου 2020 και κάθε τέσσερα χρόνια υποβάλλει εκθέσεις σχετικά με την αξιολόγηση και την αναθεώρηση του κανονισμού στο Ευρωπαϊκό Κοινοβούλιο. Η επιτροπή εξετάζει:

α) Την εφαρμογή και λειτουργία περί μεταφοράς ΔΠΧ προς τρίτες χώρες,

β) Την εφαρμογή και λειτουργία της συνεργασίας και συνεκτικότητας.



Διάγραμμα 3. Απεικόνιση εμπλεκόμενων φορέων στον ΓΚΠΔ

1.2.8 Κυρώσεις

Η εποπτική αρχή μεριμνά ώστε η επιβολή διοικητικών προστίμων έναντι παραβάσεων του κανονισμού να είναι μεμονωμένη περίπτωση, αποτελεσματική, αναλογική και αποτρεπτική.

Τα διοικητικά πρόστιμα επιβάλλονται επιπλέον ή αντί των διορθωτικών μέτρων. Κατά τη λήψη απόφασης του προστίμου λαμβάνονται υπόψη όλοι οι παράγοντες που έχουν σχέση με την παραβίαση. Τέτοιοι είναι η φύση, η βαρύτητα, η διάρκεια της παραβίασης, πιθανός δόλος ή αμέλεια, διορθωτικές κινήσεις που έγιναν, ιστορικό παραβιάσεων αν υπάρχει, κατηγορίες δεδομένων που επηρεάστηκαν κ.α.

Υπάρχουν δυο βαθμίδες διοικητικών προστίμων .

α) Παραβάσεις που έχουν σχέση με:

1. Υποχρεώσεις Υπευθύνου Επεξεργασίας (ΥΠΕ)
2. Υποχρεώσεις του φορέα πιστοποίησης
3. Φορέα παρακολούθησης

Με διοικητικά πρόστιμα έως 10.000.000 € ή 2% του παγκόσμιου τζίρου της επιχείρησης του προηγούμενου έτους.

β) Παραβάσεις που έχουν σχέση με:

1. Αρχές επεξεργασίας
2. Δικαιώματα Υποκείμενου Δεδομένων (ΥΔ)
3. Διαβιβάσεις Δεδομένων προσωπικού χαρακτήρα
4. Άλλες εθνικές υποχρεώσεις του κράτους μέλους
5. Μη συμμορφώσεις σε εντολές εποπτικής αρχής

Με διοικητικά πρόστιμα έως 20.000.000 € ή 4% του παγκόσμιου τζίρου της επιχείρησης του προηγούμενου έτους.

[Δείτε περισσότερα στα άρ.83,84 του κανονισμού]

Διάγραμμα 4. Είδη κυρώσεων[6]

[6] Διάγραμμα από το δικτυακό τόπο της Ευρωπαϊκής Επιτροπής σχετικά με την ενημέρωση των μικρομεσαίων επιχειρήσεων για τον ΓΚΠΔ http://ec.europa.eu/justice/newsroom/data-protection/infographic/2017/index_el .htm (τελευταία πρόσβαση 24/01/2018)

2 Μεθοδολογία δόμησης του οδηγού συμμόρφωσης με τον ΓΚΠΔ /GDPR

Κύριος στόχος της μελέτης αυτής, όπως ειπώθηκε και παραπάνω είναι η δημιουργία πρακτικού οδηγού, βήμα προς βήμα, συμμόρφωσης ενός οργανισμού με τον Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ / GDPR). Προϋποθέσεις του στόχου αυτού είναι ο οδηγός να έχει τα εξής χαρακτηριστικά:

- **απλός**: να χρησιμοποιεί, όσο αυτό είναι εφικτό, απλή γλώσσα αποφεύγοντας τις σύνθετες νομικές ορολογίες και τεχνικούς όρους,
- **κατανοητός**: να είναι σαφής και να μην αφήνει περιθώρια λανθασμένης ερμηνείας,
- **πρακτικός**: να έχει πρακτική χροιά, εστιάζοντας σε πρακτικά ζητήματα συμμόρφωσης ενός οργανισμού με τον ΓΚΠΔ / GDPR,
- **αποτελεσματικός**: να μπορεί να προτείνει ενέργειες που να είναι άμεσες με όσο το δυνατόν λιγότερους πόρους αλλά με το μέγιστο αποτέλεσμα,
- **ενιαίος**: να μπορεί να χρησιμοποιηθεί, όσο αυτό είναι εφικτό, σε όλους τους οργανισμούς που θέλουν να συμμορφωθούν με τον ΓΚΠΔ / GDPR. Να περιλαμβάνει όλες τις δυνατές περιπτώσεις και να δίνει τη δυνατότητα στο χρήστη να μπορεί να ανατρέξει, αν χρειαστεί, σε μέρος του κανονισμού,
- **ακριβής**: να δίνει με ακρίβεια οδηγίες για τις ενέργειες που θα πρέπει να γίνουν.
- **διαφανείς**: να είναι ξεκάθαρος ο τρόπος λήψης οδηγιών – προτάσεων,
- **τεκμηριωμένος**: να δίνει τη δυνατότητα στον χρήστη να ανατρέξει ανά πάσα στιγμή στον κανονισμό και σε άλλες σχετικές νομικές διατάξεις.

Ακολουθεί η περιγραφή της μεθοδολογίας δόμησης του οδηγού μέσα από τρία στάδια. Τα στάδια αυτά είναι: α) η μελέτη και καταγραφή απαιτήσεων, β) η κατασκευή εργαλείων αποτύπωσης και ενεργειών και γ) ο προσδιορισμός των τελικών βημάτων του οδηγού. Στον πίνακα που ακολουθεί φαίνονται τα στάδια και οι επιμέρους εργασίες ολοκλήρωσης του πρακτικού οδηγού συμμόρφωσης.

Πίνακας 6. Μεθοδολογία δόμησης πρακτικού οδηγού συμμόρφωσης με τον ΓΚΠΔ / GDPR

Μεθοδολογία δόμησης πρακτικού οδηγού συμμόρφωσης με τον ΓΚΠΔ / GDPR	
Στάδιο	**Εργασίες**
Στάδιο 1 Μελέτη και καταγραφή απαιτήσεων	α. Διερεύνηση του υπάρχοντος θεσμικού πλαισίου β. Μελέτη του νέου θεσμικού πλαισίου
Στάδιο 2 Κατασκευή εργαλείων αποτύπωσης και ενεργειών	Εγχειρίδιο αποτύπωσης α. Προσαρμογή ερωτημάτων σε κλειστού τύπου β. Ομαδοποίηση ερωτημάτων και δημιουργία παραρτήματος γ. Προσθήκη βοηθητικών πληροφοριών δ. Διαμόρφωση του εγχειριδίου αποτύπωσης Εγχειρίδιο ενεργειών α. Καταχώρηση προτεινόμενων ενεργειών β. Χρήση διευκρινίσεων γ. Προσθήκη βοηθητικών πληροφοριών δ. Δημιουργία πρότυπου εντύπου προτεινόμενων ενεργειών ε. Διαμόρφωση του εγχειριδίου ενεργειών στ. Δοκιμαστική χρήση εγχειριδίων και ανατροφοδότηση
Στάδιο 3 Προσδιορισμός βημάτων	Πίνακας βημάτων οδηγού συμμόρφωσης

2.1 Στάδιο 1: Μελέτη και καταγραφή απαιτήσεων του κανονισμού

Το πρώτο στάδιο περιλαμβάνει εργασίες κατανόησης, συλλογής και καταγραφής των στοιχειών, όρων και μηχανισμών που σχετίζονται με την προστασία δεδομένων. Διερευνήθηκε το υπάρχον και μελετήθηκε το νέο θεσμικό πλαίσιο.

α. Διερεύνηση του υπάρχοντος θεσμικού πλαισίου

Αρχικά έγινε διερεύνηση του ισχύοντος θεσμικού πλαισίου για την προστασία των δεδομένων προσωπικού χαρακτήρα (ΔΠΧ) στην Ελλάδα. Η διερεύνηση αυτή περιλάμβανε χρόνο εξοικείωσης με νομικά κείμενα, ορολογίες και ορισμούς. Έγινε κυρίως η μελέτη του νόμου

2472/1997 «Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα» ο οποίος ενσωματώνει την ευρωπαϊκή οδηγία 95/46/ΕΚ στο Ελληνικό δίκαιο. Συμπληρωματικά μελετήθηκαν οι νεότερες αλλαγές που έγιναν με τους:

α) Ν.3471/2006 «Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν. 2472/1997»

β) Ν.3783/2009 «Ταυτοποίηση των κατόχων και χρηστών εξοπλισμού και υπηρεσιών κινητής τηλεφωνίας και άλλες διατάξεις»,

γ) Ν.3917/2011 «Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις.»,

δ) Ν.4070/2012 «Ρυθμίσεις Ηλεκτρονικών Επικοινωνιών, Μεταφορών, Δημοσίων Έργων και άλλες διατάξεις.».

β. Μελέτη του νέου θεσμικού πλαισίου

Μετά την εισαγωγή στο υπάρχον θεσμικό πλαίσιο μελετήθηκε το κείμενο του ΓΚΠΔ / GDPR. Ο κανονισμός αποτελείται από δυο μέρη, το προοίμιο και το διατακτικό. Το προοίμιο περιέχει 173 αιτιολογικές σκέψεις. Οι αιτιολογικές σκέψεις είναι η αιτιολόγηση του νομικού κειμένου που ακολουθεί με στόχο να γνωστοποιηθούν οι περιστάσεις υπό τις οποίες εκδόθηκε η νομοθετική πράξη[7]. Το διατακτικό μέρος είναι το κανονιστικό τμήμα μιας νομοθετικής πράξης, δηλαδή το κύριο μέρος του νομικού κειμένου. Ο κανονισμός περιλαμβάνει 99 άρθρα. Σημαντικό μέρος για τη μελέτη και την κατανόηση του κανονισμού είναι οι κατευθυντήριες γραμμές που σταδιακά εκδίδονται από την ομάδα εργασίας του άρθρου 29 - Working Party by article 29 (OE29 / WP29) που έχει αναλάβει αυτό το ρόλο. Έως τον Φεβρουάριο του 2018 έχουν εκδοθεί συνολικά εννιά κατευθυντήριες γραμμές.

Λαμβάνοντας υπόψη όλα τα παραπάνω έγινε λεπτομερής επεξεργασία του κάθε άρθρου ώστε να καταγραφεί η απαίτηση, ως προς τους οργανισμούς, που προκύπτει από αυτό. Η απαίτηση αυτή μετασχηματίστηκε σε μορφή ερωτήματος ή ερωτημάτων. Μαζί με τα ερωτήματα καταγράφηκαν και οι ενέργειες που απαιτούνται ώστε να ικανοποιηθεί η κάθε απαίτηση. Η

[7] «Κοινός πρακτικός οδηγός του Ευρωπαϊκού Κοινοβουλίου, του Συμβουλίου και της Επιτροπής για τα πρόσωπα που συμβάλλουν στη σύνταξη των νομοθετικών κειμένων της Ευρωπαϊκής Ένωσης» σ.30 18 Αυγούστου 2016 https://publications.europa.eu/en/publication-detail/-/publication/3879747d-7a3c-411b-a3a0-55c14e2ba732/language-el (Τελευταία πρόσβαση 06/02/2018)

καταγραφή όλων των ερωτημάτων αποτελεί το σύνολο των σημείων ελέγχου για τη συμμόρφωση με τον κανονισμό.

Διάγραμμα 5. Διαδικασία καταγραφής απαιτήσεων - ρυθμίσεων του κανονισμού

Η συγκέντρωση όλων των παραπάνω σε μια οργανωμένη μορφή οδήγησε στην ακόλουθη μορφή ενός πίνακα καταγραφής απαιτήσεων.

Πίνακας 7. Αρχική μορφή καταγραφής απαιτήσεων του κανονισμού

Άρθρο	Παράγραφος	Ερώτημα	Ενέργειες	Διευκρινίσεις
…	…..	….	…..	……
8	1	Ζητάτε συγκατάθεση από παιδιά κάτω των 16 ετών για την επεξεργασία των ΔΠΧ τους;	Αν όχι [Καμία ενέργεια] Αν ναι: μεριμνήστε για τη συγκατάθεση από το άτομο που έχει τη γονική μέριμνα (άρ.8$1,2)	Ο ΥΠΕ θα πρέπει να καταβάλει εύλογες προσπάθειες για την επαλήθευση της συγκατάθεσης
…	…..	….	…..	……

2.2 Στάδιο 2: Κατασκευή εργαλείων αποτύπωσης και ενεργειών

Στο δεύτερο στάδιο έγινε η περαιτέρω επεξεργασία του πίνακα καταγραφής των απαιτήσεων. Βάσει αυτού κατασκευάστηκαν δυο εγχειρίδια που είναι τα βασικά εργαλεία του οδηγού συμμόρφωσης.

α) Το πρώτο ονομάστηκε «***εγχειρίδιο αποτύπωσης***» το οποίο είναι ένα ερωτηματολόγιο που σκοπό έχει να χρησιμοποιηθεί για την αποτύπωση - χαρτογράφηση της κατάστασης του οργανισμού.

β) Το δεύτερο ονομάστηκε «***εγχειρίδιο ενεργειών***» το οποίο περιέχει το σύνολο των προτεινόμενων ενεργειών στον οργανισμό για να συμμορφωθεί με τον κανονισμό. Οι

ενέργειες αυτές προκύπτουν από τις απαντήσεις του εγχειριδίου αποτύπωσης (ερωτηματολόγιο). Σκοπός αυτού είναι, με εύκολο τρόπο, να γίνεται ένα είδος αποκρυπτογράφησης των απαντήσεων του ερωτηματολογίου και ανάδειξης των προτεινόμενων ενεργειών προσαρμοσμένες στον κάθε οργανισμό. Η διαφορά της παρούσας με την επιθυμητή κατάσταση είναι η «απόκλιση» - “gap” της συμμόρφωσης του οργανισμού με τον κανονισμό.

2.2.1 Εγχειρίδιο αποτύπωσης

Για την δημιουργία του εγχειριδίου αποτύπωσης χρειάστηκαν οι ακόλουθες εργασίες.

α. Προσαρμογή ερωτημάτων σε κλειστού τύπου

Τα ερωτήματα που είχαν καταγραφεί αρχικώς, ανασυντάχθηκαν λαμβάνοντας υπόψη ότι το κάθε ερώτημα θα πρέπει να έχει τα εξής χαρακτηριστικά:

- να έχει απαντήσεις κλειστού τύπου,
- οι απαντήσεις να είναι της μορφής «ναι» / «όχι» για όλες τις περιπτώσεις,
- να είναι σαφές και σύντομο,
- να μην έχει αρνητικές ερωτήσεις,
- να μην έχει διπλά ερωτήματα - έννοιες,
- να μην έχει καθοδηγούμενες ερωτήσεις,
- να αποφεύγονται οι ειδικοί τεχνικοί όροι ή δυσνόητες λέξεις.

Η μορφή των απαντήσεων των ερωτημάτων κλειστού τύπου επιλέχθηκε να έχει τις επιλογές «Ναι», «Όχι», «Άγνωστο» και «Δεν αφορά». Αυτό διευκολύνει τόσο τη συμπλήρωση του ερωτηματολογίου όσο την κωδικοποίηση και επεξεργασία των απαντήσεων. Ωστόσο, παραμονεύει ο κίνδυνος να χαθεί χρήσιμη πληροφορία του χρήστη ή αδυναμία δήλωσης λεπτομερειών ειδικών περιπτώσεων. Αυτό εξασφαλίστηκε με την προσθήκη ενός ελεύθερου προς συμπλήρωση πεδίου «Σχόλια ερωτώντος» σε κάθε ερώτηση.
Τέλος στις περιπτώσεις που ένα ερώτημα εμπεριείχε άλλα πολλαπλά, διαχωρίζονταν σε υποερωτήματα ώστε να είναι κατανοητά και σαφή.

β. Ομαδοποίηση ερωτημάτων και δημιουργία παραρτήματος

Μετά την προσαρμογή των ερωτημάτων σε κλειστού τύπου και την απλούστευση αυτών, ακολούθησε η οργάνωση τους σε δυο επίπεδα. Το πρώτο ήταν η ομαδοποίηση των ερωτήσεων σε πέντε κύριες θεματικές ενότητες:

- Εδαφικός προσδιορισμός - Διαβιβάσεις δεδομένων
- Νομιμότητα Επεξεργασίας Προσωπικών Δεδομένων (ΠΔ)
- Δικαιώματα Υποκειμένων Δεδομένων (ΥΔ)
- Υπεύθυνος επεξεργασίας, εκτελών, υπεύθυνος προστασίας δεδομένων
- Θέματα ασφάλειας

Το δεύτερο ήταν ο διαχωρισμός των ερωτημάτων σε κύρια και δευτερεύοντα. Τα περισσότερα υποερωτήματα αποσπάστηκαν, ως δευτερεύοντα, από το κύριο ερωτηματολόγιο και μεταφέρθηκαν στο παράρτημα. Σκοπός των ομαδοποιήσεων ήταν η απλοποίηση και η ευχρηστία της συμπλήρωσης.

γ. Προσθήκη βοηθητικών πληροφοριών

Ολοκληρώνοντας το ερωτηματολόγιο προστέθηκαν τρία επιπλέον πεδία. Το «Α/Α» για να υπάρχει ένας αύξων αριθμός των ερωτημάτων, το «ID» που είναι μια μορφή κωδικοποίησης - συσχέτισης του ερωτήματος με το άρθρο του κανονισμού ώστε να υπάρχει δυνατότητα άμεσης παραπομπής στο σχετικό άρθρο του κανονισμού και το «Επεξήγηση ερώτησης» για να περιγράφεται η παραπομπή στο παράρτημα που έχει τα δευτερεύοντα ερωτήματα ή η επεξήγηση ερωτήματος. Συνοψίζοντας, τα πεδία του ερωτηματολογίου περιγράφονται στον παρακάτω πίνακα.

Πίνακας 8. Πεδία ερωτηματολογίου (εγχειρίδιο αποτύπωσης)

Πεδίο		Περιγραφή
Α/Α		Αύξων αριθμός
ID		Κωδικοποίηση ερωτήματος που συνδέει το ερώτημα με το άρθρο του κανονισμού (π.χ. 11-1 είναι άρθρο 11, παράγραφος 1)
Ερώτηση		Το ερώτημα που έχει προκύψει από το άρθρο του κανονισμού
Απάντηση	**Ναι**	Επιλογή απάντησης «Ναι» στο ερώτημα
	Όχι	Επιλογή απάντησης «Όχι» στο ερώτημα
	Άγνωστο	Επιλογή απάντησης σε περιπτώσεις που δεν είναι ξεκάθαρή ή είναι άγνωστη η απάντηση. Δηλαδή δεν υπάρχει επαρκής πληροφόρηση ώστε να απαντηθεί
	Δεν αφορά	Επιλογή απάντησης σε περιπτώσεις που το ερώτημα δεν αφορά το συγκεκριμένο τμήμα. (π.χ. εξειδικευμένα τεχνικά θέματα ασφάλειας πληροφορικής σε τμήμα μάρκετινγκ)
Επεξήγηση ερώτησης		Πεδίο που χρησιμοποιείται: α) για να δοθεί παραπομπή στο παράρτημα του ερωτηματολογίου β) για να δοθεί διευκρίνιση για το ερώτημα
Σχόλια ερωτώντος		Ελεύθερος χώρος προς συμπλήρωση σχολίων πληροφοριών σχετικών με το ερώτημα

δ. Διαμόρφωση του εγχειριδίου αποτύπωσης

Ολοκληρώνοντας προστέθηκαν οδηγίες χρήσης και έγινε η τελική μορφοποίηση αυτών. Στην τελική του μορφή το εγχειρίδιο αποτύπωσης αποτελείται από τρία μέρη:

α) Οδηγίες: που είναι οι οδηγίες συμπλήρωσης του ερωτηματολογίου,

β) Ερωτηματολόγιο: που είναι το κύριο μέρος του εγχειριδίου με 28 κύρια ερωτήματα,

γ) Παράρτημα (ΠΑ): που είναι 20 επιμέρους ερωτήματα του κύριου ερωτηματολογίου.

Πίνακας 9. Απόσπασμα ερωτηματολογίου (εγχειρίδιο αποτύπωσης)

Α/Α	ID	Ερώτηση	Απάντηση				Επεξήγηση ερώτησης	Σχόλια ερωτώντος
			Ναι	Όχι	Άγνωστο	Δεν αφορά		
Εδαφικός προσδιορισμός - Διαβιβάσεις δεδομένων								
1	03-2 (I)	Οι εγκαταστάσεις του οργανισμού σας είναι εκτός ΕΕ ή ΕΟΧ (Ευρωπαϊκής Ένωσης - Ευρωπαϊκού Οικονομικού Χώρου);						
1.1	- 0	Αν ναι, έχετε ορίσει γραπτώς εκπρόσωπο στην ΕΕ ;						
2	44- (V)	Τα ΔΠΧ που επεξεργάζεστε μένουν εντός της ΕΕ ή του ΕΟΧ;						
2.1	27-1 (IV)	Αν όχι, προσδιορίστε σε ποιες χώρες και με ποια νόμιμη διαδικασία.					Συμπληρώστε το σχετικό πίνακα στο παράρτημα ΠΑ-§2.1.	
Νομιμότητα Επεξεργασίας Προσωπικών Δεδομένων (ΠΔ)								
3	06-1 (II)	Είναι σύννομη η επεξεργασία ΔΠΧ;					Συμπληρώστε το σχετικό πίνακα στο παράρτημα ΠΑ-§3.	
3.1	8-1 (II)	Ζητάτε συγκατάθεση από παιδιά κάτω των 16 ετών για την επεξεργασία των ΔΠΧ τους;						
3.2	9-3 (II)	Τα ΔΠΧ χρησιμοποιούνται για σκοπούς προληπτικής ιατρικής;						

Πίνακας 10. Απόσπασμα παραρτήματος ερωτηματολογίου (ΠΑ) (εγχειρίδιο αποτύπωσης)

ΠΑ-§6.1 Δικαίωμα ενημέρωσης

Επιλέξτε τι ισχύει από τα παρακάτω σχετικά με το δικαίωμα τους ενημέρωσης του ΥΔ για τα προσωπικά του δεδομένα.

Α. Μορφή παρεχόμενων πληροφοριών στο Υδ (άρ.13,14)						
	Οι πληροφορίες που παρέχετε σχετικά με την επεξεργασία των ΔΠΧ:	**ΝΑΙ**	**ΤΟΥΣ**	**ΑΓΝΩΣΤΟ**	**ΔΕΝ ΑΦΟΡΑ**	**Αν ναι Προσδιορίστε σχετικά**
1.	είναι σε συνοπτική, διαφανή και κατανοητή μορφή;					----------
2.	είναι εύκολα προσβάσιμες; (αν ναι προσδιορίστε)					
3.	είναι με σαφή και απλή διατύπωση;					----------
4.	σε περιπτώσεις που απευθύνεστε σε παιδί, είναι προσεγμένες ιδιαιτέρως για τη σαφή και απλή διατύπωση τους; (αν ναι προσδιορίστε τον τρόπο)					Γραπτά (έντυπα) Γραπτά (Ηλεκτρονικά) Προφορικά Άλλο: .....
5.	είναι δωρεάν η διάθεση τους;					----------
Β. Τρόπος διάθεσης πληροφοριών στο Υδ						
	Έντυπα (π.χ. μέσω πολιτικής ιδιωτικότητας)					
	Ηλεκτρονικά					
	Προφορικά					
	Άλλο:					

2.2.2 Εγχειρίδιο ενεργειών

Το εγχειρίδιο ενεργειών είναι η συνέχεια του εγχειριδίου αποτύπωσης. Σε κάθε ερώτημα προστέθηκε η προτεινόμενη ενέργεια ανά περίπτωση. Αυτό προέκυψε μετά τις ακόλουθες ενέργειες.

α. Καταχώρηση προτεινόμενων ενεργειών

Για κάθε απάντηση («ΝΑΙ» ή «ΟΧΙ») του ερωτήματος καταγράφηκε η αντίστοιχη προτεινόμενη ενέργεια. Αυτό υλοποιήθηκε με την προσθήκη δυο στηλών «αν Ναι» και «αν Όχι». Για τις περιπτώσεις απάντησης «Άγνωστο», προτείνεται η περαιτέρω διερεύνηση ώστε να απαντηθεί το ερώτημα. Για τις περιπτώσεις απάντησης «Δεν αφορά» προτείνεται να γίνει επιβεβαίωση ότι όντως το ερώτημα δεν αφορά το συγκεκριμένο τμήμα/ διεύθυνση/ οργανισμό και στη συνέχεια παραλείπεται.

β. Χρήση διευκρινίσεων

Σε αρκετές περιπτώσεις οι προτάσεις ενεργειών των ερωτημάτων χρίζουν περισσότερων πληροφοριών. Για το λόγο αυτό προτέθηκε στήλη με το όνομα «Διευκρινίσεις». Στις περιπτώσεις που το κείμενο ήταν μεγάλο, δημιουργήθηκε παράρτημα εγχειριδίου (ΠΕ) προσθέτοντας στις διευκρινίσεις την αντίστοιχη παραπομπή.

γ. Προσθήκη βοηθητικών πληροφοριών

Συμπληρωματικά, ως προσπάθεια ομαδοποίησης των προτεινόμενων ενεργειών προστέθηκαν τα παρακάτω:

α) Υποχρέωση διατήρησης στοιχείων

Μέσα από τον κανονισμό, στα πλαίσια της λογοδοσίας των ΥΠΕ - ΕΚΕ, προκύπτουν άμεσα ή έμμεσα υποχρεώσεις διατήρησης στοιχείων π.χ. Αρχείο δραστηριοτήτων επεξεργασίας του ΥΠΕ - ΕΚΕ. Για τη διευκόλυνση αυτού προστέθηκε στήλη που καταγράφει σε ποιες περιπτώσεις υποχρεούται η διατήρηση στοιχείων.

β) Χρήση εγγράφου ως τεκμηρίωση

Η στήλη αυτή προστέθηκε για να επισημάνει τις περιπτώσεις που ενδείκνυται η χρήση εγγράφων ως τεκμηρίωση συμμόρφωσης με τον κανονισμό. Στα πλαίσια λογοδοσίας του ΥΠΕ / ΕΚΕ αυτά τα έγγραφα είναι ενδεικνυόμενα για συλλογή και διατήρηση τους ως απόδειξη συμμόρφωσης.

γ) Κατηγοριοποίηση προτεινόμενων ενεργειών (πολιτική, διαδικασία, τεχνικό)

Οι προτεινόμενες ενέργειες απαιτούν αλλαγές σε πολιτικές, διαδικασίες ή και τεχνικά θέματα. Για λόγους καλύτερης οργάνωσης των πληροφοριών αυτών προστέθηκαν τρεις στήλες ώστε να καταγραφεί για κάθε ερώτημα το είδος της παρεμβάσεις που χρειάζεται στον οργανισμό. Εν τούτοις οι εκτιμήσεις αυτές είναι ενδεικτικές και κάθε οργανισμός θα πρέπει να τις αναθεωρεί βάσει των δικών του αναγκών.

Με βάση όλα τα παραπάνω προκύπτουν τα πεδία του πίνακα ενεργειών και περιγράφονται στον ακόλουθο πίνακα.

Πίνακας 11. Πεδία πίνακα ενεργειών (εγχειρίδιο ενεργειών)

Πεδίο		Περιγραφή
Α/Α		Αύξων αριθμός
ID		Κωδικοποίηση ερωτήματος που συνδέει το ερώτημα με το άρθρο του κανονισμού (π.χ. 11-1 είναι άρθρο 11, παράγραφος 1)
Ερώτηση		Το ερώτημα που έχει προκύψει από το άρθρο του κανονισμού
§ παραρτήματος αποτύπωσης		Σχετιζόμενη παράγραφος στο παράρτημα του εγχειριδίου αποτύπωσης (ΠΑ)
Προτεινόμενες ενέργειες	**Αν Ναι**	Προτεινόμενες ενέργειες σε περίπτωση που η απάντηση είναι «Ναι»
	Αν Όχι	Προτεινόμενες ενέργειες σε περίπτωση που η απάντηση είναι «Όχι»
	Διευκρίνιση	Διευκρινίσεις προτεινόμενων ενεργειών και παραπομπές στο παράρτημα (ΠΕ) για περαιτέρω διευκρινίσεις
Βοηθητικές πληροφορίες	**Υποχρέωση διατήρησης στοιχειών**	Περιγράφει τις περιπτώσεις που υποχρεούται ο οργανισμός να διατηρεί στοιχεία βάσει του κανονισμού
	Έγγραφο ως τεκμηρίωση	Δηλώνει τις ενδεικνυόμενες περιπτώσεις χρησιμοποίησης εγγράφων ως τεκμηρίωση συμμόρφωσης στον κανονισμό
	Πολιτική	Δηλώνει τις αλλαγές σε πολιτικές του οργανισμού
	Διαδικασία	Δηλώνει τις αλλαγές σε διαδικασίες του οργανισμού
	Τεχνικό	Δηλώνει τις αλλαγές σε τεχνικά θέματα στον οργανισμό

δ. Δημιουργία πρότυπου εντύπου προτεινόμενων ενεργειών

Για τη διευκόλυνση συλλογής των ενεργειών δημιουργήθηκε ένα υπόδειγμα ώστε να συλλέγονται οι προτεινόμενες ενέργειες που προκύπτουν από τον πίνακα ενεργειών. Η μορφή του εντύπου φαίνεται παρακάτω.

Πίνακας 12. Μορφή υποδείγματος προτεινόμενων ενεργειών (εγχειρίδιο ενεργειών)

Προτεινόμενες ενέργειες

για τη συμμόρφωση με τον Ευρωπαϊκό Κανονισμό Προστασίας Προσωπικών δεδομένων (ΓΚΠΔ/GDPR) 2016/679

Οργανισμός - Διεύθυνση - Τμήμα: **Ημερομηνία:**

Αριθμός Ερωτήματος	Προτεινόμενη ενέργεια	Βοηθητικές πληροφορίες: Υποχρέωση διατήρησης στοιχείων	Έγγραφο ως τεκμηρίωση	Πολιτική	Διαδικασία	Τεχνικό	Παρατηρήσεις
Εδαφικός προσδιορισμός - Διαβιβάσεις δεδομένων							
1							
1.1			v				
2							
2.1			v				
Νομιμότητα Επεξεργασίας Προσωπικών Δεδομένων (ΠΔ)							
3		1.Λίστα ΔΠΧ που γίνεται επεξεργασία 2.Απόδειξη συναίνεσης του ΥΔ	v	v	v	v	

ε. Διαμόρφωση του εγχειριδίου ενεργειών

Ολοκληρώνοντας το εγχειρίδιο προστέθηκαν οδηγίες χρήσης και έγινε η τελική μορφοποίηση αυτού. Στην τελική του μορφή το εγχειρίδιο ενεργειών αποτελείται από τέσσερα μέρη:

α) Οδηγίες: που είναι οι οδηγίες χρήσης του πίνακα ενεργειών,

β) Έντυπο προτεινόμενων ενεργειών: που είναι το υπόδειγμα εντύπου για την καταγραφή των προτεινόμενων ενεργειών για τον υπό μελέτη οργανισμό,

γ) Πίνακας ενεργειών: που είναι το κύριο μέρος του εργαλείου με τις προτεινόμενες ενέργειες ανά απάντηση ερωτήματος,

δ) Παράρτημα (ΠΕ): που είναι οι συμπληρωματικές πληροφορίες των προτεινόμενων ενεργειών (άρθρα, παραπομπές κτλ.).

Πίνακας 13. Απόσπασμα πίνακα ενεργειών (εγχειρίδιο ενεργειών)

Α/Α	ID	Ερώτηση	Παραπομπές Αναπόδειξης	Προτεινόμενες ενέργειες			Βοηθητικές πληροφορίες			
				Αν ΝΑΙ	Αν 'ΟΧΙ	Διευκρίνιση	Υποχρέωση διατήρησης αποδείξεων	Έγγραφα ως τεκμηρίωση	Πολιτική	Διαδικασία	Τεχνικό
Ειδικοί προσδιορισμοί - Διαβάθμιση δεδομένων											
1		Οι εγκαταστάσεις του οργανισμού σας είναι εντός ΕΕ ή ΕΟΧ (Ευρωπαϊκής Ένωσης - Ευρωπαϊκού Οικονομικού Χώρου);		-	[κανένα ενέργεια]						
1.1		Αν ναι, έχετε ορίσει υπεύθυνο επιφόρτισης εντός της ΕΕ;		[κανένα ενέργεια]	Υποχρεούστε να ορίσετε υπεύθυνο επιφόρτισης στην ΕΕ.			✓			
2		Τα ΔΠΣ που επεξεργάζεστε μένουν εντός της ΕΕ ή του ΕΟΧ;		[κανένα ενέργεια]	Επιβεβαιώστε ότι είναι νόμιμη η διαβίβαση δεδομένων εκτός ΕΕ- ΕΟΧ.		-				
2.1		Αν όχι, προσδιορίστε σε ποιες χώρες και με ποια νόμιμη διαδικασία	ΠΑ-§2.1	-	-	Παρακάτω πληροφορίες στο παράρτημα ΠΕ-§2.1.		✓			
Νομιμότητα Επεξεργασίας Προσωπικών Δεδομένων											
3		Είναι σύννομη η επεξεργασία ΔΠΣ;	ΠΑ-§3	-	-	Επιβεβαιώστε ότι υπάρχει σύννομη απόδειξη για κάθε ΔΠΣ που επεξεργάζεστε. Περισσότερες πληροφορίες στο παράρτημα ΠΕ-§3.	1. Λίστα ΔΠΣ που γίνεται επεξεργασία 2. απόδειξη συναίνεσης του Υπ.	✓	✓	✓	✓
3.1		Ζητάτε συγκατάθεση από παιδιά κάτω των 16 ετών για την επεξεργασία των ΔΠΣ τους;		Παρμένετε, για τις περιπτώσεις συγκατάθεσης κάτω των 16 ετών, να λάβετε συγκατάθεση από το άτομο που έχει τη γονική μέριμνα (άρ.§8.2)	[κανένα ενέργεια]	Ο ΥΠΕ θα πρέπει να καταβάλει εύλογες προσπάθειες για την επαλήθευση της συγκατάθεσης.		✓			
3.2		Τα ΔΠΣ χρησιμοποιούνται για σκοπούς προώθησης;		Υποχρεούστε, ως επεξεργαστής υγείας, στην τήρηση αποτελεσματικού αποχρατου	[κανένα ενέργεια]			✓			
3.3		Επιλέξτε τι περιλαμβάνεται στην υπάρχουσα πολιτική ιδιωτικότητας	ΠΑ-§3.3	-	-	Επιβεβαιώστε - ενεργείστε ώστε να περιλαμβάνονται στην πολιτική ιδιωτικότητας σας όλα όσα αναφέρονται στον πίνακα στο παράρτημα ΠΕ-§3.3.		✓			

στ. Δοκιμαστική χρήση εγχειριδίων και ανατροφοδότηση

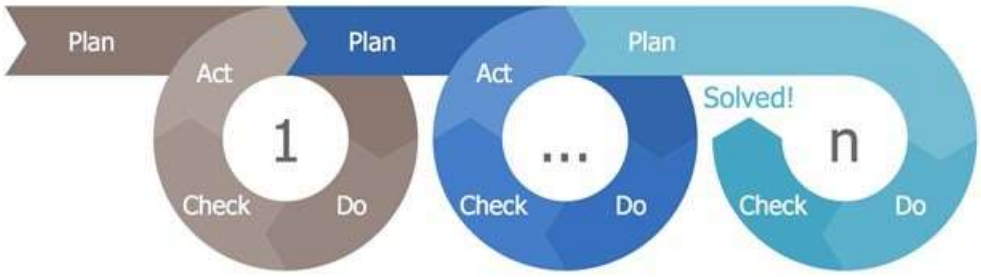
Στα πλαίσια δοκιμής και βελτίωσης των εργαλείων αποτύπωσης και ενεργειών, επιχειρήθηκε η συμπλήρωση αυτών με στελέχη τριών διαφορετικών οργανισμών μέσω της προσωπικής συνέντευξης. Μέσα από αυτές τι δοκιμές προέκυψαν εποικοδομητικά σχόλια και εύστοχες παρατηρήσεις για τα εγχειρίδια σχετικά με το περιεχόμενο (θέματα σχετικά με σύνταξη ερωτήσεων, προτάσεις ενεργειών, απλοποίηση ερωτημάτων και προσθήκη νέων) και τη δομή (οδηγίες, μέρη εγχειριδίου, μορφή πινάκων κτλ.). Οι ανατροφοδοτήσεις αυτές αφού μελετήθηκαν και αξιολογήθηκαν ενσωματώθηκαν ήδη στα εγχειρίδια που παρουσιάστηκαν παραπάνω.

2.3 Στάδιο 3: Προσδιορισμός βημάτων

Μετά την ολοκλήρωση των βασικών εργαλείων του οδηγού ακολουθήθηκε η ενσωμάτωση τους σε μια σειρά βημάτων. Ο προσδιορισμός αυτών έγινε λαμβάνοντας υπόψη: α) τις αρχές διαχείρισης έργων, β) τις αρχές διαχείρισης ολικής ποιότητας και γ) τα καθιερωμένα διεθνή πρότυπα διασφάλισης ποιότητας και ασφάλειας πληροφοριών (ISO900x, ISO2700x). Αναγνωρίζοντας ότι η συμμόρφωση με τον ΓΚΠΔ / GDPR είναι μια διαδικασία συνεχούς βελτίωσης της προστασίας των δεδομένων, υιοθετήθηκε το μοντέλο PDCA (Plan Do Check Act) ή αλλιώς “Shewhart cycle” που δημιουργός του ήταν ο Walter A. Shewhart (1939), παρόλα αυτά

δημοφιλές έγινε από τον W. Edwards Deming[8] (1950-51), επομένως στη βιβλιογραφία συναντάται με διάφορες εκδοχές (Deming Cycle, Shewhart Cycle κτλ.).

Το μοντέλο PDCA είναι μια μέθοδος διοίκησης για τον έλεγχο της συνεχούς βελτίωσης διαδικασιών – προϊόντων και αποτελείται από τέσσερις επαναλαμβανόμενες φάσεις. Η πρώτη φάση περιγράφει το σχεδιασμό για μια αλλαγή (Plan), η δεύτερη φάση είναι η υλοποίηση της σχεδίασης (Do), η τρίτη περιλαμβάνει τον έλεγχο των αλλαγών που έγιναν (Check) και τέλος η τέταρτη περιέχει τις εργασίες διόρθωσης και διατήρησής της κατάστασης (Act) δίνοντας έναυσμα για την επανεκκίνηση των φάσεων. Με βάση τις τέσσερις αυτές φάσεις διαμορφώθηκαν τα βήματα του οδηγού συμμόρφωσης.



Διάγραμμα 6. Επαναλαμβανόμενες φάσεις του μοντέλου PDCA του Walter A. Shewhart [9]

Στη φάση σχεδίασης (plan) περιλήφθηκαν όλες οι εργασίες που σχετίζονται με την προετοιμασία της αλλαγής. Για λόγους απλοποίησης η σχεδίαση επιμερίστηκε σε τρία μικρότερα βήματα, την αφύπνιση, την αποτύπωση και την πρόταση. Οι υπόλοιπες τρεις φάσεις (Do - Check - Act) χρησιμοποιήθηκαν χωρίς τροποποιήσεις. Επομένως τα βήματα συμμόρφωσης διαμορφώθηκαν σε έξι. Ακολουθεί σύντομη περιγραφή προσδιορισμού των βημάτων αυτών ενώ η πλήρης ανάλυση τους γίνεται στο επόμενο κεφάλαιο. Στα πλαίσια της λογοδοσίας που προωθεί ο κανονισμός και για την απόδειξη συμμόρφωσης του κρίθηκε απαραίτητο να μπορεί να υπάρχει ένδειξη προόδου εργασιών σε κάθε βήμα. Γι’ αυτό προσδιορίστηκαν παραδοτέα ανά βήμα, τα οποία χρησιμοποιούνται ως σημεία αναφοράς προόδου συμμόρφωσης.

[8] Moen, Ronald D.; Norman, Clifford L. (2010). "Circling back: Clearing up myths about the Deming cycle and seeing how it keeps evolving". Quality Progress. 43 (11): 21–28.

[9] Πηγή: Wikimedia commons από Christoph Roser στο AllAboutLean.com, ανακτήθηκε απο https://commons.wikimedia.org/wiki/File:PDCA-Multi-Loop.png (Τελευταία πρόσβαση 15/02/2018)

Βήμα 1:Αφύπνιση

Στο αρχικό βήμα του οδηγού, την αφύπνιση, εντάχθηκαν οι εργασίες που απαιτούνται για την προετοιμασία των ανθρώπινων πόρων για την έναρξη της διαδικασίας της συμμόρφωσης. Είναι το βασικότερο βήμα που καθορίζει την επιτυχία του έργου της συμμόρφωσης με τον ΓΚΠΔ. Ο ανθρώπινος παράγοντας είναι ο κυριότερος συντελεστής σε όλη τη διαδικασία του οδηγού. Οι εργασίες που συμπεριλήφθηκαν στο βήμα αυτό είναι:

α) Δέσμευση της διοίκησης

β) Ορισμός ομάδας διοίκησης έργου (ΟΔΕ)

γ) Ορισμός Υπεύθυνου Προστασίας Δεδομένων (ΥΠΔ / DPO)

δ) Ενημέρωση ΟΔΕ και ΥΠΔ

ε) Ενημέρωση εμπλεκομένων

Βήμα 2: Αποτύπωση

Το δεύτερο βήμα, της αποτύπωσης, αφιερώθηκε για όλες τις ενέργειες που συμβάλουν στη συλλογή στοιχείων για την βέλτιστη αποτύπωση της πραγματικότητας του οργανισμού σχετικά με την επεξεργασία ΔΠΧ. Αποκλειστικότητα του βήματος αυτού είναι η χρήση του εγχειριδίου αποτύπωσής μέσα από συνεντεύξεις σε όλα τα μέρη (τμήματα / διευθύνσεις) του οργανισμού. Παραδοτέο του βήματος της αποτύπωσης είναι όλα τα συμπληρωμένα ερωτηματολόγια τα οποία περιλαμβάνουν πλήρως το σύνολο των ΔΠΧ που επεξεργάζεται ο οργανισμός και τις διαδικασίες που σχετίζονται με αυτά (εσωτερικές ροές).

Βήμα 3: Πρόταση

Η φάση της σχεδίασης ολοκληρώνεται με το τρίτο βήμα που ονομάστηκε πρόταση. Εδώ ενσωματώθηκαν όλες οι εργασίες μελέτης του τρόπου ελαχιστοποίησης της απόκλισης μεταξύ υπάρχουσας και υποχρεούμενης κατάστασης “Gap analysis”. Συλλέγονται οι προτεινόμενες ενέργειες βάσει του εγχειριδίου ενεργειών, ομαδοποιούνται, ιεραρχούνται και τέλος οριστικοποιούνται σε ένα πλάνο συμμόρφωσης του οργανισμού. Οι εργασίες αυτές χωρίστηκαν ως εξής:

α) Χρήση εγχειριδίου ενεργειών

β) Ομαδοποίηση προτεινόμενων ενεργειών

γ) Ιεράρχηση προτεινόμενων ενεργειών

δ) Οριστικοποίηση πλάνου συμμόρφωσης

Το οριστικό πλάνο συμμόρφωσης του οργανισμού είναι το παραδοτέο του τρίτου βήματος.

Βήμα 4: Δράση

Το τέταρτο βήμα, φάση δεύτερη του μοντέλου PDCA, ονομάστηκε δράση, εδώ είναι το κύριο μέρος των πρακτικών αλλαγών που θα εφαρμοστούν στον οργανισμό. Προσδιορίστηκε να δοθεί βάρος στον συντονισμό και παρακολούθηση της εξέλιξης των αλλαγών σε όλο τον οργανισμό αποφεύγοντας τις αποσπασματικές και τμηματικές διορθωτικές κινήσεις.

Το ποσοστό προόδου των προγραμματισμένων δράσεων είναι το παραδοτέο του βήματος αυτού.

Βήμα 5: Έλεγχος

Ακολουθεί το βήμα ελέγχου των αλλαγών με στόχο την αξιολόγηση αυτών και το ποσοστό ικανοποίησης των αρχικών στόχων που ήταν να εκμηδενίσουν την απόκλιση συμμόρφωσης με τον κανονισμό.

Παραδοτέο αυτού ο πίνακας ελέγχου των αρχικών στόχων των δράσεων και η πρόοδος διόρθωσης του.

Βήμα 6: Διόρθωση

Το τελευταίο βήμα περιλαμβάνει την εφαρμογή των τελευταίων διορθωτικών αλλαγών που ο έλεγχος ανέδειξε και την ενσωμάτωση της διαδικασίας συμμόρφωσης στις πολιτικές συνεχούς βελτίωσης του οργανισμού.

Παραδοτέα του τελευταίου βήματος είναι ο πίνακας διορθωτικών δράσεων και εργασιών διατήρησης της συμμόρφωσης

Ο πίνακας που ακολουθεί συνοψίζει όλα τα παραπάνω αποτυπώνοντας το μοντέλο PDCA στα βήματα συμμόρφωσης του οδηγού. Συμπληρωματικά περιγράφονται οι επιμέρους εργασίες ανά βήμα και τα σχετικά τους παραδοτέα.

Πίνακας 14. Τα έξι βήματα του οδηγού συμμόρφωσης

Βήματα οδηγού συμμόρφωσης				
Φάση		**Βήμα**	**Επιμέρους εργασίες**	**Παραδοτέα**
Κύκλος ποιότητας Shewhart PDCA	**Σχεδίαση (Plan)**	Βήμα 1: Αφύπνιση	α. Δέσμευση της διοίκησης β. Ορισμός ομάδας διοίκησης έργου (ΟΔΕ) γ. Ορισμός Υπεύθυνου Προστασίας Δεδομένων (ΥΠΔ / DPO) δ. Ενημέρωση ΟΔΕ και ΥΠΔ ε. Ενημέρωση εμπλεκομένων	-
		Βήμα 2: Αποτύπωση	Χρήση εγχειριδίου χαρτογράφησης	Συμπληρωμένα ερωτηματολόγια
		Βήμα 3: Πρόταση	α. Χρήση εγχειριδίου ενεργειών β. Ομαδοποίηση προτεινόμενων ενεργειών γ. Ιεράρχηση προτεινόμενων ενεργειών δ. Οριστικοποίηση πλάνου συμμόρφωσης	Πίνακας οριστικοποιημένων ενεργειών (Πλάνο συμμόρφωσης)
	Υλοποίηση (Do)	Βήμα 4: Δράση	α. Συντονισμός δράσεων β. Παρακολούθηση υλοποίησης δράσεων	Πίνακας υλοποιημένων ενεργειών
	Έλεγχος (Check)	Βήμα 5: Έλεγχος	Έλεγχος των υλοποιημένων δράσεων	Πίνακας ελέγχου απόδοσης υλοποιημένων δράσεων
	Διόρθωση (Act)	Βήμα 6: Διόρθωση	α. Εφαρμογή διορθωτικών κινήσεων β. Εργασίες διατήρησης	Πίνακας διορθωτικών δράσεων Πίνακας εργασιών διατήρησης

Στο κεφάλαιο που ακολουθεί γίνεται αναλυτική περιγραφή των βημάτων του οδηγού συμμόρφωσης. Έχει γίνει η βέλτιστη δυνατή προσπάθεια ώστε να είναι αυτοτελές και να μπορεί ο αναγνώστης να ανατρέξει απευθείας σε αυτό.

3 Πρακτικός οδηγός συμμόρφωσης του οργανισμού με τον ΓΚΠΔ / GDPR

Η ενότητα αυτή παρουσιάζει τον πρακτικό οδηγό συμμόρφωσης ενός οργανισμού με τον Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ/GDPR). Εδώ περιγράφονται οι οδηγίες, βήμα προς βήμα, για τη συμμόρφωση με τον Ευρωπαϊκό κανονισμό ενώ σε κάθε βήμα αναλύονται οι εργασίες που προτείνεται να πραγματοποιηθούν.

Ο οδηγός μπορεί να χρησιμοποιηθεί από ανθρώπους ανεξαρτήτως γνωστικού υπόβαθρου. Έχει γίνει η βέλτιστη προσπάθεια να είναι όσο πιο απλός, κατανοητός, πρακτικός, αποτελεσματικός ενιαίος, ακριβής, διαφανής και τεκμηριωμένος είναι εφικτό. Εντούτοις, αν και δεν είναι επιβεβλημένη, ενθαρρύνεται η γνώση θεμάτων νομικής και πληροφορικής φύσεως. Στόχος είναι να μπορεί μια μεσαίου μεγέθους επιχείρηση - οργανισμός να ακολουθήσει τα βήματα και μέσα από αυτά να κατανοήσει τη διαδικασία ώστε να φτάσει στη μέγιστη δυνατή συμμόρφωση με τον ΓΚΠΔ. Για τις περιπτώσεις οργανισμών με ειδικά κανονιστικά και θεσμικά πλαίσια είναι απαραίτητη η εμπλοκή ανθρώπων καταρτισμένων σε νομικά και θέματα πληροφορικής. Ο οδηγός έχει κατασκευαστεί για να μπορεί να χρησιμοποιηθεί σε ανεξαρτήτου μεγέθους οργανισμό. Εν τούτοις, σημείο αναφοράς έχει καθοριστεί ένας οργανισμός μεσαίου μεγέθους που η εσωτερική του δομή περιλαμβάνει τμήμα πληροφορικής, διοικητικής και νομικής υποστήριξης.

Η φιλοσοφία του κανονισμού είναι να δημιουργήσει μια κουλτούρα προστασίας ΔΠΧ σε ευρωπαϊκό επίπεδο με κοινούς κανόνες. Η συμμόρφωση είναι μια επαναλαμβανόμενη διαδικασία συνεχούς βελτίωσης. Ο οδηγός υιοθετεί το μοντέλο ποιότητας Shewhart (PDCA) που περιλαμβάνει τέσσερις επαναλαμβανόμενες φάσεις:

α) Plan : Σχεδίαση
β) Do: Υλοποίηση
γ) Check: Έλεγχος
δ) Act: Διόρθωση

Για λόγους απλοποίησης η πρώτη φάση, η σχεδίαση, επιμερίστηκε σε τρία μέρη (αφύπνιση, αποτύπωση, πρόταση) αυξάνοντας τα επαναλαμβανόμενα βήματα σε έξι.

Διάγραμμα 7. Το μοντέλο ποιότητας Shewhart (PDCA) στον οδηγό συμμόρφωσης

Στον πίνακα που ακολουθεί φαίνονται αναλυτικά οι φάσεις του μοντέλου PDCA, τα βήματα, οι επιμέρους εργασίες και τα σχετικά παραδοτέα. Ο ρόλος των παραδοτέων είναι τριπλός: α) για ένδειξη ολοκλήρωσης βήματος, β) για χρήση αυτών ως αξιολόγηση – βελτίωση γ) για απόδειξη συμμόρφωσης προς τον κανονισμό (λογοδοσία).

Πίνακας 15. Τα έξι βήματα του οδηγού συμμόρφωσης

Βήματα οδηγού συμμόρφωσης				
Φάση		**Βήμα**	**Επιμέρους εργασίες**	**Παραδοτέα**
Κύκλος ποιότητας Shewhart - PDCA	**Σχεδίαση (Plan)**	Βήμα 1: Αφύπνιση	α. Δέσμευση της διοίκησης β. Ορισμός ομάδας διοίκησης έργου (ΟΔΕ) γ. Ορισμός Υπεύθυνου Προστασίας Δεδομένων (ΥΠΔ / DPO) δ. Ενημέρωση ΟΔΕ και ΥΠΔ ε. Ενημέρωση εμπλεκομένων	-
		Βήμα 2: Αποτύπωση	Χρήση εγχειριδίου αποτύπωσης	Συμπληρωμένα ερωτηματολόγια
		Βήμα 3: Πρόταση	α. Χρήση εγχειριδίου ενεργειών β. Ομαδοποίηση προτεινόμενων ενεργειών γ. Ιεράρχηση προτεινόμενων ενεργειών δ. Οριστικοποίηση πλάνου συμμόρφωσης	Πίνακας οριστικοποιημένων ενεργειών (Πλάνο συμμόρφωσης)
	Υλοποίηση (Do)	Βήμα 4: Δράση	α. Συντονισμός δράσεων β. Παρακολούθηση υλοποίησης δράσεων	Πίνακας υλοποιημένων ενεργειών
	Έλεγχος (Check)	Βήμα 5: Έλεγχος	Έλεγχος των υλοποιημένων δράσεων	Πίνακας ελέγχου απόδοσης υλοποιημένων δράσεων
	Διόρθωση (Act)	Βήμα 6: Διόρθωση	α. Εφαρμογή διορθωτικών κινήσεων β. Εργασίες διατήρησης	Πίνακας διορθωτικών δράσεων Πίνακας εργασιών διατήρησης

3.1 Βήμα 1: Αφύπνιση

Στο πρώτο και καθοριστικό βήμα είναι απαραίτητο να προσδιοριστούν οι άνθρωποι που θα ασχοληθούν με τη συμμόρφωση του οργανισμού με τον κανονισμό. Ανεξαρτήτως μεγέθους, πολυπλοκότητας, σύνθεσης, τεχνολογίας και άλλων παραγόντων, οι άνθρωποι του οργανισμού

είναι αυτοί που θα έχουν τον πρώτο και τελευταίο λόγο στην ασφαλή επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα (ΔΠΧ).

Το βήμα αυτό ασχολείται με τη διαδικασία επαγρύπνησης του ανθρώπινου δυναμικού που εμπλέκεται στην επεξεργασία ΔΠΧ και στις αλλαγές που θα φέρει ο κανονισμός. Ακολουθούν οι ενδεικνυόμενες εργασίες.

α. Δέσμευση της διοίκησης

Πρώτο μέλημα είναι να ενημερωθεί η διοίκηση για την υποχρέωση συμμόρφωσης, τα βήματα που πρέπει να ακολουθηθούν και για τις κυρώσεις σε περίπτωση μη συμμόρφωσης. Είναι καθοριστικό η διοίκηση να δεσμευτεί ότι θα υποστηρίξει τη διαδικασία συμμόρφωσης του οργανισμού και να διαθέσει του αντίστοιχους πόρους για αυτή. Οι πόροι αυτοί περιλαμβάνουν ανθρώπινα και τεχνικά μέσα που θα χρειαστούν σε όλη τη δομή του οργανισμού για όλα τα βήματα της συμμόρφωσης. Αρχικώς η διοίκηση θα πρέπει να ορίσει την ομάδα (ομάδα διοίκησης έργου - ΟΔΕ) που θα επιφορτιστεί με το έργο συμμόρφωσης και θα αναλάβει το ρόλο του συντονιστή μέσα στον οργανισμό. Δευτερευόντως θα πρέπει η διοίκηση να ορίσει τον υπεύθυνο προστασίας δεδομένων (ΥΠΔ) ώστε να έχει ενεργό συμβουλευτικό ρόλο στη διαδικασία της συμμόρφωσης.

β. Ορισμός ομάδας διοίκησης έργου (ΟΔΕ)

Προτείνεται να οριστεί μια ομάδα, εντός του οργανισμού, που θα αναλάβει την οργανωτική και τεχνική υποστήριξη της συμμόρφωσης του οργανισμού με τον κανονισμό. Όπως αναφέρθηκε και προηγουμένως η συμμόρφωση θα πρέπει να παρακολουθείται συνεχώς και να βελτιώνεται. Ιδανικά, η ομάδα αυτή θα πρέπει να συντίθεται από ανθρώπους με γνώσεις νομικής, πληροφορικής και διοικητικών διαδικασιών. Έτσι θα υπάρχει η βέλτιστη ευελιξία στη διαχείριση θεμάτων που θα προκύπτουν στη διαδικασία της συμμόρφωσης.

Ο ορισμός της ΟΔΕ είναι απόφαση της διοίκησης και θα πρέπει να περιλαμβάνονται οι απαραίτητοι πόροι για την εκτέλεση των καθηκόντων της (υλικοτεχνική υποδομή, ανθρώπινοι πόροι κτλ.).

γ. Ορισμός υπεύθυνου προστασίας δεδομένων (ΥΠΔ / DPO)

Ο ορισμός υπεύθυνου προστασίας δεδομένων (ΥΠΔ) ανεξαρτήτως αν ορίζεται υποχρεωτικά ή προαιρετικά, βάσει του άρθρου 37, ενδείκνυται να γίνει στην αρχή της διαδικασίας συμμόρφωσης ώστε να έχει ενεργό συμμετοχή σε αυτή. Ο ρόλος του είναι ενημερωτικός και

συμβουλευτικός για τη συμμόρφωση του οργανισμού παράλληλα συνεργάζεται και ενεργεί ως σύνδεσμος επικοινωνίας με την εποπτική αρχή.

Υπενθυμίζεται ότι υποχρέωση ορισμού ΥΠΔ έχουν οι οργανισμοί που η επεξεργασία διενεργείται (άρ. 37):

α) από δημόσια αρχή,

β) με τακτική και συστηματική παρακολούθηση υποκειμένων των δεδομένων σε μεγάλη κλίμακα,

γ) σε Δεδομένα Προσωπικού Χαρακτήρα Ειδικών κατηγοριών (ΔΠΧΕΚ) σε μεγάλη κλίμακα,

δ) σε ΔΠΧ που αφορούν ποινικές καταδίκες.

Άξιο αναφοράς είναι ότι ο κανονισμός ενθαρρύνει τον προαιρετικό διορισμό ΥΠΔ όταν δεν υπάρχει υποχρέωση. Ο ΥΠΔ είναι φυσικό πρόσωπο, είτε μέλος του προσωπικού του οργανισμού χωρίς όμως να υπάρχει σύγκρουση συμφερόντων της κανονικής του θέσης με την θέση του ΥΠΔ, είτε εξωτερικός συνεργάτης βάσει σύμβασης παροχής υπηρεσιών. Σε κάθε περίπτωση μπορεί να συνεπικουρείται από ομάδα ανθρώπων, εάν το απαιτεί ο φόρτος εργασίας, όμως ένας θα είναι ο επικεφαλής επικοινωνίας[10].

Ο ορισμός του ΥΠΔ είναι απόφαση της διοίκησης και θα πρέπει να περιλαμβάνει τους απαραίτητους πόρους για την εκτέλεση των καθηκόντων του (υλικοτεχνική υποδομή, ανθρώπινοι πόροι κτλ.).

δ. Ενημέρωση ΟΔΕ και ΥΠΔ

Η ΟΔΕ και ο ΥΠΔ θα πρέπει να ενημερωθούν πλήρως για το θεσμικό πλαίσιο προστασίας των ΔΠΧ που περιλαμβάνει τους ρόλους των εμπλεκομένων, τις απαιτήσεις, τις υποχρεώσεις και τις κυρώσεις. Ενδείκνυται αρχικά η μελέτη του πρώτου κεφαλαίου της παρούσας εργασίας για μια συνοπτική και περιεκτική εισαγωγή των βασικών στοιχείων του κανονισμού. Δευτερευόντως για ειδικές και συγκεκριμένες περιπτώσεις θα χρειαστεί περαιτέρω ενημέρωση - εκπαίδευση από εξιδεικευμένους στο θέμα. Ο ΥΠΔ θα πρέπει να ενημερωθεί για τα καθήκοντα του και για το ρόλο του στη συμμόρφωση του οργανισμού. Η ΟΔΕ έχοντας πλέον εμπεριστατωμένη γνώση μπορεί να ξεκινήσει τη διαδικασία συμμόρφωσης.

[10] «Κατευθυντήριες γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων», Γνωμοδότηση WP 243/2017 αναθ.01 (05/04/2017), σ.29, http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048 (Τελευταία πρόσβαση 21/01/2018)

ε. Ενημέρωση εμπλεκομένων

Το πρώτο βήμα του οδηγού ολοκληρώνεται με την ενημέρωση όλων των εμπλεκομένων για τη διαδικασία των βημάτων που θα ακολουθηθούν ώστε να προετοιμαστούν για τις ενέργειες στις οποίες θα εμπλακούν. Ενδείκνυται η ενημέρωση όλων των διευθύνσεων του οργανισμού, ανεξαρτήτως αν εμφανώς δεν υπάρχει εμπλοκή των τμημάτων στην επεξεργασία ΔΠΧ. Κατά την ενημέρωση θα πρέπει να τονισθεί η σημαντικότητα και η σοβαρότητα των εργασιών που θα ακολουθήσουν.

3.2 Βήμα 2: Αποτύπωση

Το δεύτερο βήμα περιλαμβάνει όλες εκείνες τις εργασίες που θα βοηθήσουν να διαφανεί και να καταγραφεί η παρούσα κατάσταση του οργανισμού σχετικά με την προστασία προσωπικών δεδομένων. Αυτό θα γίνει με τη βοήθεια του εγχειριδίου αποτύπωσης.

Χρήση εγχειριδίου αποτύπωσης

Το εγχειρίδιο αποτύπωσης (βλ. Παράρτημα Π1) αποτελείται από τις οδηγίες, το ερωτηματολόγιο και το παράρτημα (ΠΑ). Το ερωτηματολόγιο του εγχειριδίου ενδείκνυται να συμπληρώνεται για κάθε διεύθυνση του οργανισμού. Είναι απαραίτητο η συμπλήρωση να είναι πλήρης και για λογαριασμό ολόκληρης της διεύθυνσης. Η ΟΔΕ θα κρίνει την αναγκαιότητα συνεντεύξεων ώστε να συμπληρωθεί το ερωτηματολόγιο του εγχειριδίου πετυχαίνοντας τη βέλτιστη αποτύπωση της πραγματικότητας.

Το δυσκολότερο και ουσιαστικότερο μέρος του ερωτηματολογίου, είναι η πλήρης καταγραφή των αγαθών - δεδομένων που διαχειρίζεται ο οργανισμός. Αυτό επιχειρείται μέσα από το ερωτηματολόγιο με την οπτική της καταγραφής προσωπικών δεδομένων ανά παρεχόμενη ή λαμβανόμενη υπηρεσία. Ουσιαστικά θα πρέπει να διερευνηθεί κάθε ΠΔ που είναι εισερχόμενο εξερχόμενο η δημιουργείται εντός του οργανισμού. Η διαδικασία αυτή είναι επίπονη και χρειάζεται μέθοδο, ανάλυση και χρόνο.

Τα συμπληρωμένα ερωτηματολόγια του οργανισμού, που είναι και παραδοτέα, ολοκληρώνουν το δεύτερο βήμα.

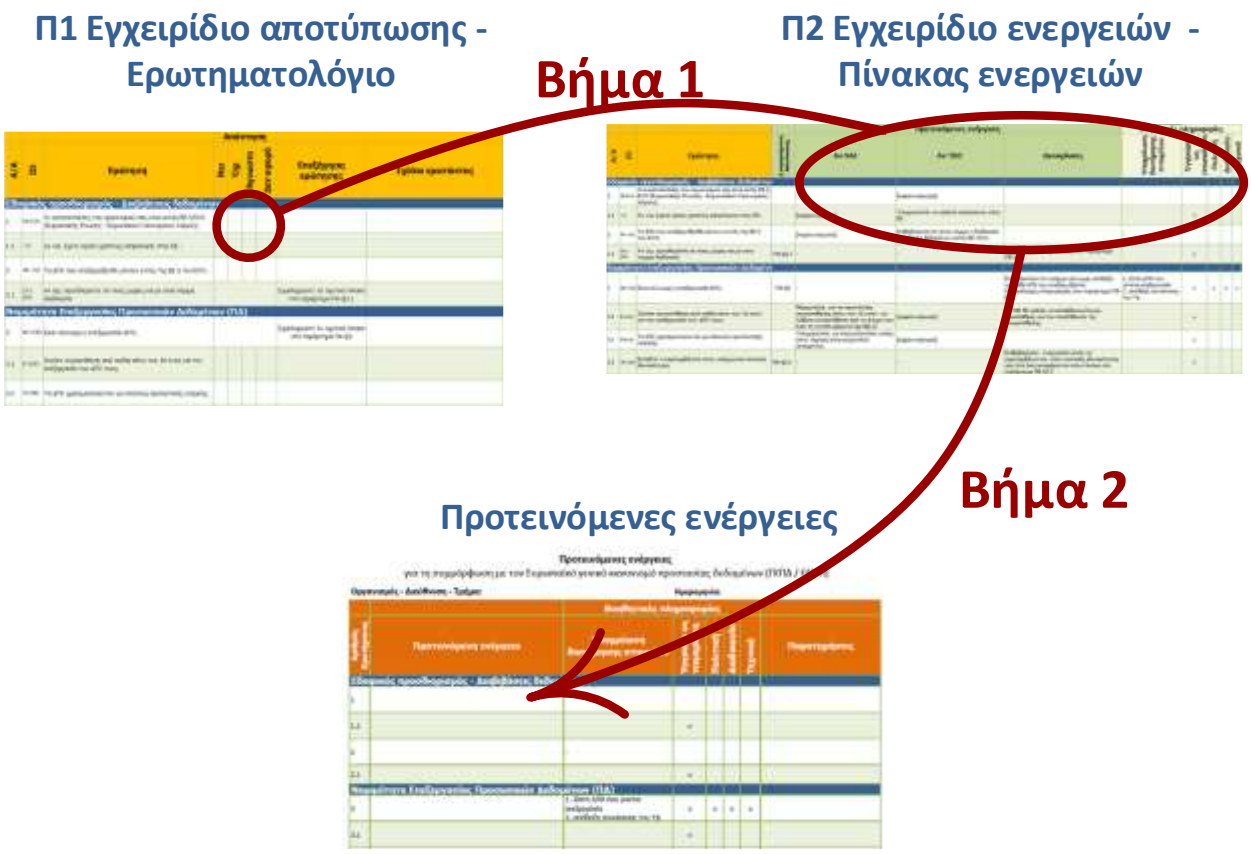
3.3 Βήμα 3: Πρόταση

Στόχος του τρίτου βήματος είναι να διαμορφωθεί μια δομημένη πρόταση ενεργειών στον οργανισμό, ώστε να φτάσει στη μέγιστη δυνατή συμμόρφωση με τον ΓΚΠΔ. Αυτό προϋποθέτει να γίνει η επεξεργασία των απαντήσεων από τις οποίες θα προκύψουν προτεινόμενες ενέργειες που θα συναρτηθούν – ομαδοποιηθούν και ιεραρχηθούν ώστε να προκύψει το πλάνο συμμόρφωσης. Το πλάνο συμμόρφωσης είναι το αποτέλεσμα ανάλυσης αποκλίσεων (Gap Analysis) της επιθυμητής με την παρούσα κατάσταση συμμόρφωσης του κανονισμού. Ακολουθεί αναλυτική περιγραφή των προτεινόμενων εργασιών.

Διάγραμμα 8. Διαδικασία διαμόρφωσης πρότασης ενεργειών (πλάνο συμμόρφωσης)

α. Χρήση εγχειριδίου ενεργειών ανά ερωτηματολόγιο

Το εγχειρίδιο ενεργειών (βλ. Παράρτημα Π2) αποτελείται από τέσσερα μέρη. Τις οδηγίες χρήσης, το «Υπόδειγμα προτεινόμενων ενεργειών», τον «Πίνακα ενεργειών» και το «Παράρτημα (ΠΕ)». Ανάλογα τις απαντήσεις του ερωτηματολογίου του εγχειριδίου αποτύπωσης (Π1) και έχοντας ως οδηγό τον πίνακα ενεργειών (Π2), προκύπτει μια λίστα ενεργειών. Αυτό επαναλαμβάνεται για όλα τα απαντημένα ερωτηματολόγια. Το «Υπόδειγμα προτεινόμενων ενεργειών», θα βοηθήσει στη συγκέντρωση των προτεινόμενων ενεργειών.



Διάγραμμα 9. Βήματα χρήσης του εγχειριδίου ενεργειών

β. Ομαδοποίηση προτεινόμενων ενεργειών

Χρησιμοποιώντας τη λίστα των προτεινόμενων ενεργειών ανά διεύθυνση, γίνεται ομαδοποίηση τους σε δυο επίπεδα. Το ένα είναι να συγκεντρωθούν όλες οι ενέργειες που θα πρέπει να γίνουν καθολικά σε όλο τον οργασμό (οριζόντιες) και το άλλο είναι να ξεχωρίσουν οι ενέργειες που θα πρέπει να γίνουν σε μεμονωμένες διευθύνσεις (κάθετες) π.χ. η κρυπτογράφηση των προσωπικών δεδομένων των πελατών μιας επιχείρησης είναι οριζόντια ενέργεια που σχετίζεται με τμήμα πωλήσεων, μάρκετινγκ, υποστήριξης. Ενώ κάθετη ενέργεια είναι η διαγραφή του πεδίου θρησκεύματος από την αίτηση πρόσληψης των υπαλλήλων στο τμήμα ανθρώπινου δυναμικού.

Αυτός ο τρόπος ομαδοποίησης των ενεργειών είναι βοηθητικός στο να φανεί γενικά και ειδικά το σύνολο των δράσεων που πρέπει να υλοποιηθούν.

γ. Ιεράρχηση προτεινόμενων ενεργειών

Η ομάδα διοίκησης έργου (ΟΔΕ) έχοντας καταγεγραμμένες οριζόντιες και κάθετες προτεινόμενες ενέργειες για όλο τον οργανισμό τις αξιολογεί και τις ιεραρχεί. Το σημείο αυτό είναι επίσης σημαντικό διότι για κάθε αλλαγή θα πρέπει να συνεκτιμηθούν αρκετές συνιστώσες όπως η αναγκαιότητα (υποχρέωση), το κόστος, ο χρόνος, το ρίσκο, το όφελος και το εύρος αυτής.

Εδώ να σημειωθεί ότι η ανάλυση των κινδύνων που περιλαμβάνεται σε μια εκτίμηση αντικτύπου προσωπικών δεδομένων (ΕΑΠΔ / DPIA) είναι εξαιρετικά βοηθητική στην τεκμηρίωση ιεράρχησης ενεργειών. Βάσει αυτής προκύπτουν εύκολα οι προτεραιότητες λαμβάνοντας υπόψη το ρίσκο. Στην ιεράρχηση αυτή θα κληθεί να γνωμοδοτήσει και ο ΥΠΔ / DPO.

Η ΟΔΕ ολοκληρώνοντας αυτό το μέρος εργασιών έχει ιεραρχημένες τις προτεινόμενες ενέργειες με εναλλακτικά σενάρια για να προτείνει στη διοίκηση και να οριστικοποιηθεί το πλάνο συμμόρφωση.

δ. Οριστικοποίηση πλάνου συμμόρφωσης

Ως τελευταίο μέρος του τρίτου βήματος είναι η παρουσίαση των προτεινόμενων ενεργειών με τις εναλλακτικές επιλογές ανά περίπτωση και με ανάλυση των απαιτούμενων πόρων αυτών (ανθρώπινους, εξοπλισμό, κτήρια, χρήματα κτλ.) για την υλοποίηση τους στη διοίκηση του οργανισμού. Μετά τη σύμφωνη γνώμη αυτής οριστικοποιείται το πλάνο συμμόρφωσης (compliance plan) και ξεκινάει η ΟΔΕ ως συντονιστής την υλοποίηση των ενεργειών.

Το τρίτο βήμα έχει παραδοτέο το εγκεκριμένο από την διοίκηση πλάνο συμμόρφωσης το οποίο περιέχει πίνακα οριστικοποιημένων ενεργειών.

3.4 Βήμα 4: Δράση

Το βήμα αυτό ασχολείται με τη διαχείριση της αλλαγής. Εδώ περιλαμβάνονται όλες οι εργασίες για την υλοποίηση των προτεινόμενων ενεργειών που έχουν εγκριθεί από την διοίκηση. Η ΟΔΕ αναλαμβάνει το ρόλο συντονισμού, προγραμματισμού και παρακολούθησης της υλοποίησης των ενεργειών. Ο συντονισμός των οριζόντιων δράσεων εμπλέκει διευθύνσεις του οργανισμού και είναι απαιτητικός. Οι κάθετες δράσεις είναι λιγότερο απαιτητικές, όλες όμως χρειάζεται να συντονιστούν ώστε να μην επικαλύπτονται ή να δημιουργήσουν προβλήματα εφαρμογής. Τρείς

είναι οι στόχοι της αλλαγής, η βέλτιστη επίδοση στο σωστό χρόνο και με το λιγότερο δυνατό κόστος. Οι εργασίες που θα ακολουθηθούν περιγράφονται παρακάτω.

α. Συντονισμός δράσεων

Επιβάλλεται αναλυτική ενημέρωση - επικοινωνία με όλες τις εμπλεκόμενες διευθύνσεις - τμήματα για τις αλλαγές που πρόκειται να γίνουν. Αρχικά, θα διερευνηθούν τα θέματα πολιτικής, έπειτα τα θέματα διαδικασιών και τέλος τα τεχνικά. Το χρονοδιάγραμμα υλοποίησης αυτών είναι βασική παράμετρος επιτυχίας των αλλαγών.

Δεν πρέπει να παραληφθεί η σημαντικότητα της ενημέρωσης και εκπαίδευσης των εμπλεκομένων στα νέα δεδομένα. Η υποστήριξη του προσωπικού είναι σημείο κλειδί στην επιτυχία των αλλαγών. Ενδείκνυται η εκπαίδευση θεωρητική και πρακτική - πάνω στην εργασία (on the job training) - για την βέλτιστη κατανόηση των υποχρεώσεων του καθένα απέναντι στον κανονισμό.

β. Παρακολούθηση υλοποίησης δράσεων

Η κάθε διεύθυνση θα αναλάβει την υλοποίηση των ενεργειών που είναι εντός των αρμοδιοτήτων της είτε η δράση είναι οριζόντια είτε κάθετη. Η ΟΔΕ παρακολουθεί την εξέλιξη όλων ώστε να υπάρχει συνολική εικόνα προόδου εναρμόνισης με τον κανονισμό. Μέσα στις παρακολούθηση των δράσεων περιλαμβάνεται η επιβεβαίωση δημιουργίας και τήρησης αρχείων καθώς και η συλλογή των εγγράφων που πρόκειται να χρησιμοποιηθούν ως τεκμηρίωση συμμόρφωσης.

Ολοκληρώνοντας τις δράσεις έχει υλοποιηθεί το κυριότερο μέρος συμμόρφωσης του κανονισμού, μένει η αξιολόγηση των αλλαγών αυτών και οι διορθωτικές κινήσεις για τη βελτιστοποίηση αυτών.

Παραδοτέο του τέταρτου βήματος είναι ο πίνακας υλοποιημένων ενεργειών που δείχνει το επίπεδο ολοκλήρωσης των ενεργειών.

3.5 Βήμα 5: Έλεγχος

Στο βήμα αυτό θα γίνει ο έλεγχος των υλοποιημένων δράσεων του προηγούμενου βήματος με στόχο την αξιολόγηση των ενεργειών που προτάθηκαν και του τρόπου υλοποίησης τους. Αυτό θα γίνει αξιολογώντας:

α) την επίτευξη των αρχικών στόχων,

β) την επίτευξη αποτελεσματικότητα τους και
γ) τις πιθανές διορθωτικές κινήσεις.

Παραδοτέο του βήματος αυτού είναι ο πίνακας ελέγχου των αρχικών στόχων των δράσεων και τα σημεία διόρθωσης.

3.6 Βήμα 6: Διόρθωση

Το τελευταίο βήμα αποτελείται από δυο εργασίες. Τις εργασίες διόρθωσης και διατήρησης.

α. Εφαρμογή διορθωτικών κινήσεων

Εδώ ενδείκνυται να γίνουν οι τελευταίες ενέργειες που έχουν διαπιστωθεί ως διορθωτικές. Είναι οι εργασίες που μπορούν διορθώσουν πιθανά κενά που έχουν προκύψει από τις αλλαγές. Ο χαρακτήρας τον ενεργειών είναι συμπληρωματικός και δεν αποσκοπούν σε διαθρωτικές παρεμβάσεις.

β. Εργασίες διατήρησης

Τα βήματα του οδηγού ολοκληρώνονται εδώ, η διαδικασία της συμμόρφωσης όμως δε σταματά και ενδείκνυται να ενσωματωθεί στην πολιτική της συνεχούς βελτίωσης του οργανισμού για την προστασία ΔΠΧ. Προτείνεται η συνέχιση της λειτουργίας της ΟΔΕ και η καθιέρωσή της στον οργανισμό.
Σε κάθε περίπτωση η ΟΔΕ παραδίδει όλο το υλικό (παραδοτέα ανά βήμα, σημειώσεις τηρούμενων αρχείων, έγγραφα απόδειξης συμμόρφωσης) στον υπεύθυνο επεξεργασίας (ΥΠΕ) και τον υπεύθυνο προστασίας Δεδομένων (DPO) με την σημείωση της υποχρέωσης συνεχούς παρακολούθησης, διατήρησης και βελτίωσης του οργανισμού στη συμμόρφωση με τον κανονισμό.

Παραδοτέο του τελευταίο βήματος είναι ο πίνακας των δράσεων που διορθώθηκαν και πίνακας των προτεινόμενων εργασιών συντήρησης. Έτσι η διαδικασία επανέναρξης των βημάτων είναι έτοιμη για την διατήρηση και βελτίωση του επιπέδου προστασίας προσωπικών δεδομένων και συμμόρφωσης με τον κανονισμό.

4 Συμπεράσματα

Σύντομη αναδρομή

Η παρούσα εργασία εστιάζοντας στις επιχειρησιακές επιπτώσεις του νέου Γενικού Κανονισμού Προστασίας Δεδομένων - General Data Protection Regulation (ΓΚΠΔ / GDPR), προσπάθησε να αναδείξει μια σειρά βημάτων στο θολό μονοπάτι της συμμόρφωσης με το ανανεωμένο ρυθμιστικό πλαίσιο. Ιεραρχεί τις παρεμβάσεις που απαιτούνται ώστε να υπάρξει η βέλτιστη δυνατή συμμόρφωση με τον ΓΚΠΔ / GDPR.

Η διαμόρφωση των βημάτων προέκυψε από αναλυτική μελέτη και καταγραφή απαιτήσεων των άρθρων του κανονισμού. Δεδομένου ότι το γνωστικό υπόβαθρο του μελετητή δεν ήταν νομικό, αύξησε την δυσκολία των εργασιών αυτών. Σε δεύτερη φάση διαμορφώθηκε ένας τρόπος αποτύπωσης - χαρτογράφησης της υφιστάμενης κατάστασης ενός οργανισμού μέσω ενός εύκολου και κατανοητού ερωτηματολογίου. Στη συνέχεια διαμορφώθηκε ένας τρόπος ανάδειξης των προτεινόμενων ενεργειών βάσει της υφιστάμενης κατάστασης του οργανισμού. Όλα τα παραπάνω εντάχθηκαν σε μια σειρά επιχειρησιακών βημάτων με συγκεκριμένες εργασίες ώστε να είναι άμεσα, πρακτικά και αποτελεσματικά.

Καινοτομία και περιορισμοί

Το κίνητρο εκπόνησης της εργασίας αυτής είναι η διαμόρφωση ενός απλού, πρακτικού και τεκμηριωμένου οδηγού συμμόρφωσης με δυνατότητα προσαρμογής του στην ιδιομορφία κάθε οργανισμού - επιχείρησης αποφεύγοντας την πολύπλοκη νομική ορολογία. Από την μοντελοποίηση των απαιτήσεων του κανονισμού δομήθηκε μια γραμμική μορφή εξατομικευμένων παρεμβάσεων που συμμορφώνουν τον οργανισμό με την νομοθεσία. Ξεκινώντας ως δεδομένο το μηδενικό υπόβαθρο του «χρήστη» που θα αναλάβει να ανιχνεύσει τα βήματα της συμμόρφωσης του οργανισμού του δίνει οδηγίες και βήματα που ακολουθώντας τα καταλήγουν στις προτεινόμενες ενέργειες για την βέλτιστη συμμόρφωση με τον κανονισμό. Αυτοί είναι οι στόχοι και η καινοτομία της παρούσας εργασίας.

Στον αντίποδα, υπήρχαν αρκετές δυσκολίες αυτού του εγχειρήματος. Η ανάλυση και καταγραφή των απαιτήσεων έγινε από μελετητή που το γνωστικό του υπόβαθρο δεν είναι νομικό, αυξάνοντας την πιθανότητα λάθους σε ερμηνείες νομικών κειμένων και ορολογιών με κίνδυνο η μοντελοποίηση των απαιτήσεων να απέχει από την πραγματικότητα των απαιτήσεων του κανονισμού. Η απόκλισή αυτή πιθανόν να επιφέρει εσφαλμένες προτάσεις ενεργειών για τον οργανισμό. Στο μέτρο του δυνατού, αυτό περιορίστηκε με την καθοδήγηση του επιβλέποντα

καθηγητή, την μελέτη γνωμοδοτήσεων - καθοδηγήσεων των αρχών προστασίας δεδομένων και γνωμοδοτήσεων της «Ομάδας Εργασίας του άρθρου 29» -Working Party by article 29 (OE29 / WP29). Εντούτοις δεν είναι εφικτό να υπάρξει πλήρη εγγύηση σε αυτό. Η τελική πρακτική χρήση του οδηγού, η επιβεβαίωση των προτάσεων και η διόρθωση του, θα συνθέσουν ένα οδηγό με τα ελάχιστα ή μηδενικά σφάλματα. Ο παραπάνω περιορισμός ήταν από τις αρχικές παραδοχές της ερευνητικής εργασίας και έγιναν όλες οι δυνατές προσπάθειες ελαχιστοποίησης του.

Προτάσεις

α) Ηλεκτρονικός οδηγός συμμόρφωσης

Η παρούσα εργασία μπορεί να είναι η βάση της ανάλυσης απαιτήσεων για την ανάπτυξη ηλεκτρονικής έκδοσης του οδηγού συμμόρφωσης. Η υλοποίηση ενός πληροφοριακού συστήματος που καταγράφει και καθοδηγεί αναλυτικά τα βήματα συμμόρφωσης του οδηγού θα διευκολύνει την ευχρηστία, αμεσότητα και αποτελεσματικότητά του. Μηχανογραφώντας το σύστημα αυτό θα μπορεί να έχει συγκεντρωμένες και δομημένες όλες τις ενέργειες του οργανισμού για τη συμμόρφωση. Έτσι θα είναι εφικτό να παρέχει άμεσα πλήρη εικόνα για τη διαδικασία συμμόρφωσης, τον τρόπο ελέγχου και τα σημεία βελτίωσης. Τέλος, μεγάλο πλεονέκτημα του ηλεκτρονικού οδηγού θα είναι η ευκολία λογοδοσίας για τη συμμόρφωση αφού οι ενέργειες και η πληροφορία θα είναι δομημένες και άμεσες.

β) Χρήση του οδηγού σε (με) άλλα εργαλεία

Τα εργαλεία του οδηγού μπορούν να χρησιμοποιηθούν συνδυαστικά ή βοηθητικά σε άλλα εργαλεία συμμόρφωσης στον κανονισμό. Η καταγραφή του μητρώο αγαθών (assets inventory), η εκτίμηση αντικτύπου προστασίας δεδομένων (ΕΠΑΔ/DPIA), η πολιτική ασφάλειας και η διάρθρωση του αρχείου δραστηριοτήτων είναι εργασίες που μπορούν να τροφοδοτηθούν ή να τροφοδοτήσουν στοιχεία στο εγχειρίδια αποτύπωσης και ενεργειών. Η συνδυαστική χρήση αυτών θα δώσει ολιστικές και σε βάθος προτάσεις συμμόρφωσης.

γ) Προσθήκη ποσοτικοποίησης συμμόρφωσης και κοστολόγησης

Μια ακόμα πρόταση εξέλιξης της παρούσας έρευνας είναι να προστεθούν συντελεστές που θα εκτιμούν το ποσοστό συμμόρφωσης. Να μπορεί δηλαδή ο οδηγός μετά το βήμα της αποτύπωσης να δώσει ένα ποσοστό (επι τις εκατό) συμμόρφωσης με τον κανονισμό, στοιχείο

που θα αναθεωρείται μετά από τις ανάλογες διορθωτικές κινήσεις. Η υλοποίησή του θεωρητικά είναι απλή, στην πράξη όμως υπάρχουν αρκετές δυσκολίες. Η μεγαλύτερη είναι ότι υπάρχει δυσκολία στην αξιολόγηση της βαρύτητας της κάθε ενέργειάς του οργανισμού, δεδομένου ότι το επίπεδο και ή έκταση προστασίας δεδομένων είναι ανόμοιες σε κάθε περίπτωση.
Παράλληλα με αυτή την ιδέα, με λιγότερα ίσως πρακτικά προβλήματα είναι η προσθήκη εκτίμησης κόστους της συμμόρφωσης με βάση την αποτύπωση του οργανισμού. Ο οργανισμός να μπορεί να έχει μια εκτίμηση κοστολόγησης των παρεμβάσεων που απαιτούνται σε ανθρώπινους και υλικούς πόρους προσεγγίζοντας ένα εύρος τιμών (βέλτιστο, μέσο, χείριστο σενάριο) ώστε να φτάσει σε ικανοποιητικά επίπεδα συμμόρφωσης.

δ) Δοκιμή σε πραγματικές συνθήκες
Ο οδηγός παρόλο που έχει μελετηθεί εξαντλητικά λαμβάνοντας υπόψη όλες τις δυνατές συνιστώσες και συνθήκες παραμένει να είναι ένα «εργαστηριακό πείραμα». Η χρήση του σε πραγματικό περιβάλλον θα δείξει την πρακτικότητα και αποτελεσματικότητα του. Εκεί θα αναδειχθούν οι αδυναμίες και κενά που θα οδηγήσουν στην βελτιστοποίηση του.
Ως πρόταση εξέλιξης λοιπόν είναι η δοκιμή του σε πραγματικές συνθήκες με σκοπό να βελτιστοποιηθεί και να χρησιμοποιηθεί στην πράξη από οργανισμούς που θέλουν να αναλάβουν την αυτό-συμμόρφωση τους με τον κανονισμό.

Αντί επιλόγου

Ο Γενικός κανονισμός προστασίας δεδομένων είναι ένα καινοτόμο παγκόσμιο νομοθετικό εγχείρημα αύξησης της προστασίας των Δεδομένων Προσωπικού Χαρακτήρα του ατόμου. Η παρούσα εργασία προσπάθησε να πλησιάσει τις υποχρεώσεις συμμόρφωσης με το πραγματικό επιχειρησιακό περιβάλλον.
Πιθανόν η πρακτική προσέγγιση να υστερεί σε νομοθετικές ερμηνείες του κανονισμού όμως ο θεωρώ ότι διακρίνεται για την απλότητα, την ανάλυση του σε βάθος και πρακτικότητα της. Αισιοδοξώ μέσα από την επιστημονική ανάλυση νομικής πληροφορικής να προέκυψε μια άλλη οπτική που μικραίνει την απόσταση νομοθετικών κειμένων και πρακτικότητας.
Ολοκληρώνοντας ελπίζω η εργασία αυτή να είναι ένα ακόμα λιθαράκι στην διευκόλυνση προσαρμογής των οργανισμών στο νέο κανονιστικό πλαίσιο με αύξηση εμπιστοσύνης του ατόμου (πολίτη, πελάτη) προς την επιχείρηση και τη βελτίωση σεβασμού της ιδιωτικότητας και της ατομικής ελευθερίας.

Βιβλιογραφικές παραπομπές

Ελληνική νομοθεσία για την προστασία προσωπικών δεδομένων

[1] Νόμος 2472/1997, *Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.* (με ενσωματωμένες και τις τελευταίες τροποποιήσεις βάσει του Ν. 4139/2013). Ανακτήθηκε από http://www.dpa.gr/pls/portal/url/ITEM/E3BC3C1B7FC83BA6E040A8C07D24022A.

[2] Νόμος 3471/2006, *Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του Ν. 2472/97*. (με ενσωματωμένες και τις τελευταίες τροποποιήσεις βάσει των Ν. 3783/2009, Ν. 3917/2011 και Ν. 4070/2012). Ανακτήθηκε από http://www.dpa.gr/pls/portal/url/ITEM/DEF1C46F2229C66FE040A8C07C246917 .

[3] Νόμος 3783/2009, *Ταυτοποίηση των κατόχων και χρηστών εξοπλισμού και υπηρεσιών κινητής τηλεφωνίας και άλλες διατάξεις*. Ανακτήθηκε από http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/LAW/NOMOTHESIA%20PROSOPIKA%20DEDOMENA/FILES/%CE%9D.3783_2009.PDF .

[4] Νόμος 3917/2011, *Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις*. Ανακτήθηκε από: http://www.dpa.gr/pls/portal/url/ITEM/E3BCAB5DD0CCC28AE040A8C07D243B29.

[5] Νόμος 4070/2012, *Ρυθμίσεις Ηλεκτρονικών Επικοινωνιών, Μεταφορών, Δημοσίων Έργων και άλλες διατάξεις* Ανακτήθηκε από http://www.dpa.gr/pls/portal/url/ITEM/C49ECABDABE13F46E040A8C07C247802.

Ευρωπαϊκή νομοθεσία για την προστασία προσωπικών δεδομένων

[1] Οδηγία 95/46/ΕΚ (1995), *Προστασία των φυσικών προσώπων έναντι της επεξεργασία δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών.*

[2] Οδηγία 2002/58/ΕΚ (2002), Επεξεργασία *των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών.*

[3] Οδηγία 2006/24/ΕΚ, *Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίων δικτύων επικοινωνιών και για την τροποποίηση της οδηγίας 2002/58/ΕΚ.*

[4] Οδηγία 2009/136/ΕΚ, *Τροποποίηση της οδηγίας 2002/22/ΕΚ για την καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών, της οδηγίας 2002/58/ΕΚ σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και του κανονισμού (ΕΚ) αριθ. 2006/2004 για τη συνεργασία μεταξύ των εθνικών αρχών που είναι αρμόδιες για την επιβολή της νομοθεσίας για την προστασία των καταναλωτών.*

[5] Κανονισμός (ΕΕ) 2016/679, *Προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων)* http://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32016R0679 .

[6] Οδηγία (ΕΕ) 2016/680, *Προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της απόφασης-πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου.*

[7] Οδηγία (ΕΕ) 2016/681, *Χρήση των δεδομένων που περιέχονται στις καταστάσεις ονομάτων επιβατών (PNR) για την πρόληψη, ανίχνευση, διερεύνηση και δίωξη τρομοκρατικών και σοβαρών εγκλημάτων.*

Κατευθυντήριες γραμμές της Ομάδας εργασίας του άρθρου 29 (ΟΕ29/WP29) και Ευρωπαϊκής Επιτροπής (ΕΕΠ/ΕC)

(Τελευταία ενημέρωση 15/02/2018)

[1] Ευρωπαϊκή επιτροπή (2018), *Ανακοίνωση της επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο (Ισχυρότερη προστασία, νέες ευκαιρίες - Κατευθυντήριες γραμμές της Επιτροπής σχετικά με την άμεση εφαρμογή του γενικού κανονισμού για την προστασία δεδομένων από την 25η Μαΐου 2018),* (24-01/2018), ανακτήθκε από http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:43:FIN (Τελευταία πρόσβαση 09/02/2018).

[2] Ευρωπαϊκή επιτροπή (2018), *Διαδικτυακή εργαλειοθήκη καθοδήγησης για τους πολίτες, τις επιχειρήσεις (ιδίως τις ΜΜΕ) και τους άλλους οργανισμούς, σχετικά με τον ΓΚΠΔ/GDPR* (24-01/2018) https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_el (Τελευταία πρόσβαση 09/02/2018).

[3] Ομάδα εργασίας του άρθρου 29 (2017) - Γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα , *Guidelines on Personal data breach notification under Regulation 2016/679*, (WP250) 03/10/2017.

[4] Ομάδα εργασίας του άρθρου 29 (2017) - Διαφάνεια (σε διαβούλευση έως 23/01/201), Guidelines on transparency under Regulation 2016/679, (WP260).

[5]Ομάδα εργασίας του άρθρου 29 (2017) - Δικαίωμα φορητότητας δεδομένων, *Κατευθυντήριες γραμμές σχετικά με το δικαίωμα στη φορητότητα των δεδομένων,* έκδοση:01 (WP242 αναθ.01) 13/12/2016, αναθεωρήθηκε 5/04/2017.

[6] Ομάδα εργασίας του άρθρου 29 (2017) - Εκτίμηση επιπτώσεων στην προστασία δεδομένων,*Κατευθυντήριες γραμμές για την εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) και καθορισμός του κατά πόσον η επεξεργασία «ενδέχεται να επιφέρει υψηλό κίνδυνο» για τους σκοπούς του κανονισμού 2016/679,* έκδοση:01 (WP248 αναθ.01) 04/04/2017, αναθεωρήθηκε 4/10/2017.

[7] Ομάδα εργασίας του άρθρου 29 (2017) - Επικεφαλής εποπτική αρχή, *Κατευθυντήριες γραμμές για τον προσδιορισμό της επικεφαλής εποπτικής αρχής των υπευθύνων επεξεργασίας ή των εκτελούντων την επεξεργασία,* έκδοση:01 (WP244 αναθ.01) 13/12/2016, αναθεωρήθηκε 5/04/2017.

[8] Ομάδα εργασίας του άρθρου 29 (2017) - Εφαρμογή και καθορισμός διοικητικών προστίμων Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, (WP253) 03/10/2017.

[9] Ομάδα εργασίας του άρθρου 29 (2017) – Συγκατάθεση (σε διαβούλευση έως 23/01/201), Guidelines on Consent under Regulation 2016/679, (WP259) 28/11/2017.

[10] Ομάδα εργασίας του άρθρου 29 (2017) - Υπεύθυνοι Προστασίας Δεδομένων ('DPOs') *Κατευθυντήριες γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων* έκδοση:01 (WP243 αναθ.01) 13/12/2016, αναθεωρήθηκε 5/04/2017.

[11] Ομάδα εργασίας του άρθρου 29 (2018) - Αυτοματοποιημένη ατομική λήψη αποφάσεων και κατάρτιση προφίλ, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679,* (WP251 αναθ.01) 06/02/2018.

Εποπτικές αρχές – Ευρωπαϊκοί οργανισμοί

[1] CNIL (2015), *General Data Protection Regulation: a guide to assist processors,* (27/11/2017). Ανακτήθηκε από https://www.cnil.fr/en/general-data-protection-regulation-guide-assist-processors (Τελευταία πρόσβαση 02/02/2018)

[2] CNIL (2015), *Privacy Impact Assessments: the CNIL publishes its PIA manual*, (10/07/2015). Ανακτήθηκε από https://www.cnil.fr/fr/node/15798 (Τελευταία πρόσβαση 02/02/2018)

[3] ENISA (2016), *ENISA's Position on the General Data Protection Regulation (GDPR,* (01/ 2016). Ανακτήθηκε από https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/ enisa2019s-position-on-the-general-data-protection-regulation-gdpr/ (Τελευταία πρόσβαση 06/02/2018)

[4] ENISA (2016), Guidelines for SMEs on the security of personal data processing, (12/2016). Ανακτήθηκε από https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing/at_download/fullReport (Τελευταία πρόσβαση 06/02/2018).

[5] ENISA (2017), *Recommendations on European Data Protection Certification*, (27/11/2017). Ανακτήθηκε από https://www.enisa.europa.eu/publications/recommendations-on-

european-data-protection-certification/at_download/fullReport (Τελευταία πρόσβαση 06/02/2018)

[6] ICO (2017), *Guide to the General Data Protection Regulation (GDPR)*. Ανακτήθηκε από https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/ (Τελευταία πρόσβαση 02/02/2018)

[7] ICO (2017), *Preparing for the General Data Protection Regulation (GDPR): 12 steps to take now,* (25/05/2017). Ανακτήθηκε από https://ico.org.uk/media/for-organisations/ documents/1624219/ preparing-for-the-gdpr-12-steps.pdf (Τελευταία πρόσβαση 02/02/2018)

[8] ICO (2018), *Guide to the General Data Protection Regulation (GDPR)*. Ανακτήθηκε από https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf (Τελευταία πρόσβαση 09/02/2018)

[9] ΑΠΔΠΧ (2018), *Γενικός Κανονισμός για την Προστασία των Δεδομένων*. Ανακτήθηκε από http://www.dpa.gr/portal/page?_pageid=33,311094&_dad=portal&_schema=PORTAL (Τελευταία πρόσβαση 02/02/2018)

[10] ΑΠΔΠΧ - Τσόλιας Γ. (2017), *Υποχρεώσεις συμμόρφωσης στον Γενικό Κανονισμό Προσωπικών Δεδομένων (GDPR) και ο ρόλος του Υπευθύνου Προστασίας Δεδομένων (DPO)*, (03/04/2017). Ανακτήθηκε από http://www.infocomsecurity.gr/presentations/2017/day1/tsolias.pdf & https://www.youtube.com/watch?v=y5tZTes4p0M, Παρουσίαση στο 7ο Infocom Security 2017 (Τελευταία πρόσβαση 06/02/2018)

Άλλες πηγές

[1] Alan M, (2016), *GDPR: Evolutionary or revolutionary?*, (13/09/2016). DOI:10.1057/s41263-016-0006-9 Ανακτήθηκε από https://link.springer.com/article/10.1057/s41263-016-0006-9 (Τελευταία πρόσβαση 19/02/2018).

[2] Bastiaan van Loenen , Stefan Kulk, Hendrik Ploeger (2016), *Data protection legislation: A very hungry caterpillar: The case of mapping data in the European Union*, (30/04/2016). DOI:10.1016/j.giq.2016.04.002 Ανακτήθηκε από https://www.sciencedirect.com/science/article/pii/S0740624X16300326 (Τελευταία πρόσβαση 19/02/2018).

[3] Colin Tankard – Digital Pathways (2016), *What the GDPR means for business*. DOI:10.1016/S1353-4858(16)30056-3 Ανακτήθηκε από https://www.sciencedirect.com/science/article/pii/S1353485816300563 (Τελευταία πρόσβαση 19/02/2018).

[4] Eric Lachaud (2016), *Why the certification process defined in the General Data Protection Regulation cannot be successful*, (02/08/2016). DOI: 10.1016/j.clsr.2016.07.001 Ανακτήθηκε από https://www.sciencedirect.com/science/article/pii/S0267364916301157 (Τελευταία πρόσβαση 19/02/2018).

[5] EricLachaud (2016) *Why the certification process defined in the General Data Protection Regulation cannot be successful*. DOI: 10.1016/j.clsr.2016.07.001 Ανακτήθηκε από https://linkinghub.elsevier.com/retrieve/pii/S0267364916301157 (Τελευταία πρόσβαση 19/02/2018).

[6] Ernst & Young (EY) LLP (2017), *EU general data protection regulation: are you ready?,* (03/2017). Ανακτήθηκε από http://www.ey.com/Publication/vwLUAssets/EY-EU-general-data-protection-regulation-are-you-ready-mar-2017/$FILE/EY-EU-general-data-protection-regulation-are-you-ready-mar-2017.pdf (Τελευταία πρόσβαση 06/02/2018).

[7] IAPP - *International Association of Privacy Professionals (2016) The Top 10 Operational Impacts of the EU's General Data Protection Regulation*. Ανακτήθηκε από https://iapp.org/resources/article/top-10-operational-impacts-of-the-gdpr-e-book/ (Τελευταία πρόσβαση 06/02/2018).

[8] IAPP & EY (2017), *IAPP-EY Annual Privacy Governance Report 2017*, https://iapp.org/media/pdf/resource_center/IAPP-EY-Governance-Report-2017.pdf (Τελευταία πρόσβαση 06/02/2018).

[9] IAPP & EY, (2017), *IAPP-EY Annual Privacy Governance Report 2016*. Ανακτήθηκε από https://iapp.org/media/pdf/resource_center/IAPP%202016%20GOVERNANCE%20SURVEY-FINAL3.pdf (Τελευταία πρόσβαση 06/02/2018).

[10] IAPP Nymity (2016*), Preparing for the GDPR: Attaining and Demonstrating Compliance*, (09/2016). Ανακτήθηκε από https://iapp.org/media/presentations/PSR_2016/PSR_2016/Preparing_for_the_GDPR_Attaining_and_Demonstrating_Compliance_PPT.pdf.

[11] IAPP, TRUSTe (2016), *Preparing for the GDPR: DPOs, PIAs, and Data Mapping*. Ανακτήθηκε από https://iapp.org/resources/article/preparing-for-the-gdpr-dpos-pias-and-data-mapping/ (Τελευταία πρόσβαση 06/02/2018).

[12] ISACA (2017), *GDPR data protection impact assessments*. Ανάκτηση από http://www.isaca.org/Knowledge-Center/Research/Documents/GDPR_res_eng_0917.pdf (Τελευταία πρόσβαση 06/02/2018).

[13] Kadenic V - Luleå University of Technology (2015), *Compliance of Data Lake Enterprise Architecture Model with the General Data Protection Regulation (GDPR)* [πτυχιακή εργασία]

[14] Karyda M & Mitrou L (2016), *Data Breach Notification: Issues and Challenges for Security Management*. Ανακτήθηκε από https://aisel.aisnet.org/mcis2016/60 MCIS 2016 Proceedings. 60.

[15] Linklatters (2016), *The GDPR at a glance, and a "to do" list to help you prepare for it* ,(07/2016). Ανακτήθηκε από https://lpscdn.linklaters.com/-/media/files/linklaters/pdf/mkt/london/ general_data-protection_regulationgdpr_brochure_web_final_spreads4.ashx?rev=eb50f 7f4-0634-4f11-9ce5-11e9983deaaa&la=en&hash=122CA9CAEDA66921605321EF2906916FEA210C82 (Τελευταία πρόσβαση 02/02/2018).

[16] Mark Hall, Redcentric (2016), *Why people are key to cyber-security* DOI: 10.1016/S1353-4858(16)30057-5 Ανακτήθηκε από

https://www.sciencedirect.com/science/article/pii/S1353485816300575 (Τελευταία πρόσβαση 19/02/2018).

[17] Nymity, www.nymity.com/GDPR-Toolkit (Τελευταία πρόσβαση 06/02/2018).

[18] Paul Lambert (2016) *The Data Protection Officer: Profession, Rules, and Role*, CRC Press, ISBN 9781138031937 (12/2016)

[19] Peter Church – Linklatters (2016), *The General Data Protection Regulation A survival guide*, (10/2016). Ανακτήθηκε από https://lpscdn.linklaters.com/-/media/files/linklaters/pdf/mkt/ london/tmt_data_ protection_survival_guide_singles.ashx?la=en&rev=5ef6afd7-f614-4423-9145 0a9d0a60a452&hash=95E65AFC95091DE3CE114A19B104E5BD27D9AAFD (Τελευταία πρόσβαση 02/02/2018)

[20] Ralph O'Brien (2016), *Privacy and security The new European data protection regulation and it's data breach notification requirements,* (08/06/2016). DOI: 10.1177/0266382116650297 Ανακτήθηκε από http://journals.sagepub.com/doi/10.1177/0266382116650297 (Τελευταία πρόσβαση 19/02/2018).

[21] Rowena Rodrigues, David Barnard-Wills, Paul De Hert & Vagelis Papakonstantinou (2016), *The future of privacy certification in Europe: an exploration of options under article 42 of the GDPR, International Review of Law, Computers & Technology*, 30:3, 248-270, DOI: 10.1080/13600869.2016.1189737 Ανακτήθηκε από http://www.tandfonline.com/doi/full/10.1080/13600869.2016.1189737 (Τελευταία πρόσβαση 19/02/2018).

[22] Srouji J., Veillon M (2016), *The brave new world of fines, myths and Reality, a French regulator Perspective*, (09/2016). Ανακτήθηκε από https://www.sroujiavocats.com/app/download/9522654/J+Srouji-ACC+Docket+September+2016+np.pdf (Τελευταία πρόσβαση 06/02/2018)

[23] Μήτρου Λ. (2016), *Ο Γενικός κανονισμός προστασίας προσωπικών δεδομένων (2016/697) νέο δίκαιο, Νέες προκλήσεις*, Παρουσίαση στο 2ο Ετήσιο Συνέδριο Ασφάλειας Ψηφιακών Συστημάτων "ICT Security World", 25/5/2016.

[24] Μήτρου Λ. (2017), *Προστασία Προσωπικών Δεδομένων*. Παρουσίαση στο 3ο Ετήσιο Συνέδριο Ασφάλειας Ψηφιακών Συστημάτων «ICT SECURITY WORLD» (8/06/2017).

Ανακτήθηκε από https://www.dropbox.com/sh/yyymk60cuc8izvr/AABfzYX20UMnP8VzryET_mM5a/Παρουσιάσεις/Ασφάλεια%20Πληροφοριών%20-%20Προστασία%20Υποδομών%20-%20Προστασία%20Δεδομένων.%20Πολιτικές%20-%20Στρατηγικές%20-%20Κανονισμοί/Στρατηγικές%20και%20Κανονιστικές%20Παρεμβάσεις/MITROU%20LILIAN.ppt?dl=0 (Τελευταία πρόσβαση 19/02/2018).

[25] Ντούσκας Θ. (2017), *ΓΚΠΔ: ΜΕΘΟΔΟΛΟΓΙΑ ΠΡΑΚΤΙΚΗΣ ΕΝΑΡΜΟΝΙΣΗΣ.* Παρουσίαση στο 3ο Ετήσιο Συνέδριο Ασφάλειας Ψηφιακών Συστημάτων «ICT SECURITY WORLD», (8/06/2017). Ανακτήθηκε από https://www.dropbox.com/sh/yyymk60cuc8izvr/AACvfqFwe4dtWvMTGCY1wjEfa/Παρουσιάσεις/Ασφάλεια Πληροφοριών - Προστασία Υποδομών - Προστασία Δεδομένων. Πολιτικές - Στρατηγικές - Κανονισμοί/Στρατηγικές και Κανονιστικές Παρεμβάσεις/DOUSKAS THEODOROS - AUEB.pdf?dl=0 (Τελευταία πρόσβαση 19/02/2018).

Η σελίδα αυτή αφήνεται σκόπιμα κενή

Παράρτημα

Εργαλεία οδηγού συμμόρφωσης

Η σελίδα αυτή αφήνεται σκόπιμα κενή

Παράρτημα

Π1 Εγχειρίδιο αποτύπωσης

για τη συμμόρφωση με τον Ευρωπαϊκό Γενικό Κανονισμό Προστασίας Δεδομένων - General Data Protection Regulation (ΓΚΠΔ/GDPR) 2016/679

Οργανισμός - Επιχείρηση

Τμήμα

Ημερομηνία Συμπλήρωσης :

Έκδοση: 1.4

Οδηγίες χρήσης του εγχειριδίου

Εισαγωγή

Το παρόν εγχειρίδιο έχει σκοπό τη συλλογή όλων των πληροφοριών, μέσω ερωτήσεων, για την αποτύπωση της κατάστασης του οργανισμού - επιχείρησης σχετικά με την προστασία δεδομένων φυσικών προσώπων. Μετά την αποτύπωση της κατάστασης θα ακολουθήσει επεξεργασία και έκδοση αναφοράς με τις προτεινόμενες ενέργειες, ώστε ο οργανισμός να συμμορφωθεί με τον Ευρωπαϊκό Γενικό Κανονισμό Προστασίας Δεδομένων - General Data Protection Regulation (ΓΚΠΔ/GDPR) 2016/679.

Το ερωτηματολόγιο είναι δομημένο ώστε να μπορεί να συμπληρωθεί από οποιοδήποτε οργανισμό. Ενδείκνυται η συμπλήρωση του από όλες τις διευθύνσεις του οργανισμού ανεξαρτήτως αν εμφανώς δεν υπάρχει επεξεργασία δεδομένων προσωπικού χαρακτήρα. Η συλλογή των απαντήσεων όλων των ερωτηματολογίων θα αποτελέσει την αποτύπωση - χαρτογράφηση της κατάστασης του οργανισμού στην προστασία δεδομένων προσωπικού χαρακτήρα. Η συμπλήρωση να γίνεται με ευθύνη του προϊσταμένου της διεύθυνσης – τμήματος.

Πεδίο εφαρμογής

Ο κανονισμός εφαρμόζεται σε οργανισμούς που επεξεργάζονται Δεδομένα Προσωπικού Χαρακτήρα (ΔΠΧ) φυσικών προσώπων της Ευρωπαϊκής Ένωσης ανεξαρτήτως που βρίσκονται οι εγκαταστάσεις του (άρ.3). Εξαιρούνται όσοι επεξεργάζονται δεδομένα που δεν είναι εφικτό να εξακριβωθεί η ταυτότητα των φυσικών προσώπων (αρ.11).

Παρουσίαση

Το εγχειρίδιο αποτύπωσης αποτελείται από τρία μέρη. Τις παρούσες οδηγίες, το «ερωτηματολόγιο» και το «παράρτημα».

Το ερωτηματολόγιο περιλαμβάνει 28 ερωτήσεις που κάθε μια έχει:

α) την «**Απάντηση**» που είναι κλειστού ή ανοιχτού τύπου και έχει επιλογές (Ναι, Όχι, Άγνωστο, Δεν αφορά),

β) την «**Επεξήγηση ερώτησης**» που είναι επεξήγηση της ερώτησης ή παραπομπή στο παράρτημα για πληροφορίες ή περαιτέρω ερωτήσεις και

γ) τα «**Σχόλια ερωτώντος**» που είναι ελεύθερο κείμενο προς συμπλήρωση.

Το παράρτημα περιέχει δευτερεύουσες ερωτήσεις - πίνακες προς συμπλήρωση με σχετικές οδηγίες ανά περίπτωση. Σε κάποιες περιπτώσεις δίνονται περισσότερες πληροφορίες για το ερώτημα.

Στο ερωτηματολόγιο και το παράρτημα υπάρχουν παραπομπές στα άρθρα και τις παραγράφους του Ευρωπαϊκού Κανονισμού. Οι παραπομπές αυτές είναι της μορφής

(άρ.xx§xx). Το κείμενο του Κανονισμού (2016/679) βρίσκεται στην επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης «EUR-Lex» στον ακόλουθο σύνδεσμο: http://eur-lex.europa.eu/eli/reg/2016/679/oj

Οδηγίες χρήσης

Συμπληρώστε το ερωτηματολόγιο ανά διεύθυνση με ευθύνη του προϊσταμένου.
Στο πεδίο «απάντηση» που έχει απαντήσεις κλειστού τύπου συμπληρώστε «✓» στην ανάλογη επιλογή (Ναι, Όχι, Άγνωστο, Δεν αφορά). Στις απατήσεις ανοιχτού τύπου απαντήστε με ελεύθερο κείμενο. Επιλέξτε μόνο αν είστε απόλυτα σίγουρος για την απάντηση σας. Διαφορετικά επιλέξτε άγνωστο ώστε να διερευνηθεί περαιτέρω η απάντηση της ερώτησης. Η επιλογή «δεν αφορά» να επιλέγεται αν εκτιμάται ότι το ερώτημα δεν έχει σχέση με τη συγκεκριμένη διεύθυνση.

Στο πεδίο «Επεξήγηση ερώτησης» θα βρείτε επεξηγηματικές πληροφορίες ή παραπομπή στο παράρτημα (ΠΑ) για να συμπληρώσετε περαιτέρω ερωτήσεις.
Στο πεδίο «Σχόλια ερωτώντος» προσθέστε αν επιθυμείτε να δηλώσετε κάτι περαιτέρω σχετικά με την ερώτηση.

Συντομογραφίες - Ορισμοί

άρ.	Άρθρο
§	Παράγραφος
Καν.	Κανονισμός
Ν.	Νόμος
α.σ.	Αιτιολογικές σκέψεις κανονισμού. Είναι το μέρος μιας νομικής πράξης που περιέχει την αιτιολόγησή της και περιλαμβάνεται μεταξύ των σημείων αναφοράς και του διατακτικού της πράξης.

ΔΠΧ **Δεδομένα Προσωπικού Χαρακτήρα** ή

ΠΔ **Προσωπικά Δεδομένα**

Κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»). Το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους

παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου.

ΔΠΧΕΚ Δεδομένα Προσωπικού Χαρακτήρα Ειδικών Κατηγοριών

Δεδομένα προσωπικού χαρακτήρα που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και η επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένων που αφορούν την υγεία ή δεδομένων που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή το γενετήσιο προσανατολισμό.

ΥΔ Υποκείμενο Δεδομένων

Το φυσικό πρόσωπο στο οποίο αναφέρονται τα δεδομένα και του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί, δηλαδή μπορεί να προσδιορισθεί αμέσως ή εμμέσως, ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός ή περισσότερων συγκεκριμένων στοιχείων που χαρακτηρίζουν την υπόστασή του από άποψη φυσική, βιολογική, ψυχική, οικονομική, πολιτιστική, πολιτική ή κοινωνική.

ΥΠΕ Υπεύθυνος Επεξεργασίας

Το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα· όταν οι σκοποί και ο τρόπος της επεξεργασίας αυτής καθορίζονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια για το διορισμό του μπορούν να προβλέπονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους.

ΕΚΕ 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.

ΕΕ Ευρωπαϊκή Ένωση

EU European Union

Οικονομική και πολιτική ένωση είκοσι οκτώ ευρωπαϊκών κρατών. Η Ελλάδα περιλαμβάνεται μέσα σε αυτά, το Ηνωμένο Βασίλειο έχει ξεκινήσει τις διαδικασίες αποχώρησης από την ένωση αυτή (Τελευταία ενημέρωση 20/01/2018).

ΕΕΠ Ευρωπαϊκή Επιτροπή

EC European Commission

Η Ευρωπαϊκή Επιτροπή είναι το πολιτικά ανεξάρτητο εκτελεστικό όργανο της ΕΕ. Είναι το μόνο αρμόδιο όργανο για την κατάρτιση προτάσεων για νέα ευρωπαϊκή νομοθεσία, και εφαρμόζει τις αποφάσεις του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της ΕΕ.

ΕΟΧ Ευρωπαϊκός Οικονομικός Χώρος

EEA European Economic Area

Συμφωνία (1/1/1994) μεταξύ της Ευρωπαϊκής Ζώνης Ελευθέρων Συναλλαγών (ΕΖΕΣ) και της Ευρωπαϊκής Οικονομικής Κοινότητας που επιτρέπει στις χώρες Ισλανδία, Λίχτενσταϊν και Νορβηγία να συμμετέχουν στην Ευρωπαϊκή Κοινή Αγορά χωρίς να χρειαστεί να γίνουν μέλη της ΕΟΚ.

ΑΠΔΠΧ Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

Συνταγματικά κατοχυρωμένη ανεξάρτητη διοικητική αρχή που ιδρύθηκε με το Νόμο 2472/1997 «για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα», ο οποίος ενσωματώνει στο ελληνικό δίκαιο την ευρωπαϊκή οδηγία 95/46/ΕΚ.

ΕΑΠΔ Εκτίμηση Αντικτύπου Προστασίας Δεδομένων

DPIA Data Privacy Impact Assessment

Μελέτη που εκτιμά την πιθανότητα και τη σοβαρότητα των κινδύνων σχετικά με την προστασία δεδομένων ΔΠΧ σε έναν οργανισμό - επιχείρηση.

ΓΚΠΔ Γενικός Κανονισμός Προστασίας Δεδομένων

GDPR General Data Protection Regulation

Κανονισμός που σχετίζεται με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών. Αντικαθιστά την οδηγία 95/46/ΕΚ, που είναι για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών. Ψηφίστηκε στις 25 Απριλίου 2016 και τίθεται σε ισχύ στις 25 Μαΐου 2018.

ΥΠΔ Υπεύθυνος Προστασίας Δεδομένων

DPO Data Protection Officer

Φυσικό πρόσωπο, μέρος του προσωπικού του ΥΠΕ / ΕΚΕ ή εκτός αυτού με σύμβαση παροχής υπηρεσιών, που μεριμνά με ανεξάρτητο τρόπο, για την ορθή εφαρμογή του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ / GDPR) στον οργανισμό - επιχείρηση.

ΕΣΠΔ **Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων**

EDPB **European Data Protection Board**

Όργανο της Ευρωπαϊκής Ένωσης με νομική προσωπικότητα που με την εφαρμογή του ΓΚΠΔ/GDPR πρόκειται να αντικαταστήσει την ομάδα εργασίας του άρθρου 29 (ΟΕ29 / WP29).

ΕΕΠΔ **Ευρωπαίος Επόπτης Προστασίας Δεδομένων**

EDPS **European Data Protection Supervisor**

Ανεξάρτητη ευρωπαϊκή αρχή που σκοπό έχει να διασφαλίζει ότι κατά την επεξεργασία προσωπικών δεδομένων, τα όργανα και οι οργανισμοί της ΕΕ σέβονται το δικαίωμα των πολιτών για προστασία της ιδιωτικής ζωής.

Οργανισμός

Στην κοινωνική ορολογία, οργανισμός είναι μια ομάδα ανθρώπων με έναν ή περισσότερους κοινούς στόχους, τους οποίους επιδιώκει να υλοποιήσει μέσω επίσημα καθορισμένων αρχών και θεσμών. Είναι κάθε νομικό πρόσωπο που έχει δραστηριότητες οικονομικής, πολιτικής, κοινωνικής φύσεως. Οργανισμός θεωρείται ένας δημόσιος φορέας, μια επιχείρηση, ένας σύλλογος κτλ. Για την παρούσα εργασία όπου αναφέρεται οργανισμός εννοούνται όλες οι παραπάνω έννοιες.

Ευαίσθητα Προσωπικά Δεδομένα

Ο όρος ευαίσθητα προσωπικά δεδομένα στον ΓΚΠΔ / GDPR αντικαθίσταται από τον όρο Δεδομένα Προσωπικού Χαρακτήρα Ειδικών Κατηγοριών (ΔΠΧΕΚ).

Επεξεργασία

Κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή.

Περιορισμός της επεξεργασίας

Η επισήμανση αποθηκευμένων δεδομένων προσωπικού χαρακτήρα με στόχο τον περιορισμό της επεξεργασίας τους στο μέλλον. Όταν ισχύει ο περιορισμός της επεξεργασίας επιτρέπεται η αποθήκευση των δεδομένων όχι όμως η περαιτέρω επεξεργασία τους.

Κατάρτιση προφίλ

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

Ψευδωνυμοποίηση

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

Σύστημα αρχειοθέτησης

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

Αποδέκτης

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

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.

Συγκατάθεση του υποκειμένου των δεδομένων
Κάθε ένδειξη βούλησης, ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει, με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν.

Παραβίαση δεδομένων προσωπικού χαρακτήρα
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.

Εκπρόσωπος
Φυσικό ή νομικό πρόσωπο εγκατεστημένο στην Ευρωπαϊκή Ένωση, το οποίο ορίζεται εγγράφως από τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία βάσει του άρθρου 27 και

εκπροσωπεί τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία ως προς τις αντίστοιχες υποχρεώσεις τους δυνάμει του παρόντος κανονισμού.

Επιχείρηση

Φυσικό ή νομικό πρόσωπο που ασκεί οικονομική δραστηριότητα, ανεξάρτητα από τη νομική του μορφή, περιλαμβανομένων των προσωπικών εταιρειών ή των ενώσεων που ασκούν τακτικά οικονομική δραστηριότητα.

Δικαιώματα υποκειμένου δεδομένων ΥΔ

Ο κανονισμός προσδιορίζει οκτώ (8) δικαιώματα του υποκειμένου δεδομένων[1].

1. Δικαίωμα ενημέρωσης

Είναι το δικαίωμα ενημέρωσης του υποκειμένου δεδομένων (ΥΔ) σχετικά με την επεξεργασία των ΔΠΧ. Το ΥΔ θα πρέπει να ενημερώνεται από τον υπεύθυνο επεξεργασίας (ΥΠΕ) σχετικά με την επεξεργασία των δεδομένων του και θα πρέπει να περιλαμβάνει πληροφορίες όπως: ταυτότητα και στοιχεία επικοινωνίας του ΥΠΕ/ΕΚΕ και ΥΠΔ, τους σκοπούς της επεξεργασίας, την νομική βάση αυτών, τους αποδέκτες κ.α..

Οι πληροφορίες που παρέχονται πρέπει να είναι :

- σε συνοπτική, διαφανή, κατανοητή και εύκολα προσβάσιμη μορφή,
- με σαφή και απλή διατύπωση, ιδίως εάν απευθύνεται σε παιδί και
- δωρεάν

Ο τρόπος ενημέρωσης γίνεται συνήθως μέσω μιας δήλωσης γραπτά ή προφορικά με ποικίλες ονομασίες όπως «Δήλωση απορρήτου», «Δήλωση προστασίας ιδιωτικού απορρήτου», «Δήλωση προστασίας προσωπικών δεδομένων», «Πολιτική απορρήτου» κ.α.

[Δείτε περισσότερα στα άρ.12§1, §5, §7, 13, 14 και α.σ. 58-62 του κανονισμού, γνωμοδότηση της ΟΕ29 "Guidelines on transparency under Regulation 2016/679", (WP260)]

2. Δικαίωμα πρόσβασης

Είναι το δικαίωμα του ΥΔ να έχει πρόσβαση σε ΔΠΧ και άλλες πληροφορίες που το αφορούν, προκειμένου να έχει επίγνωση και να επαληθεύει τη νομιμότητα της επεξεργασίας. Πιο συγκεκριμένα το ΥΔ έχει δικαίωμα να λάβει:

- επιβεβαίωση για την επεξεργασία των δικών του ΔΠΧ,
- πρόσβαση στα δικά του ΔΠΧ,
- αντίγραφο των δικών του ΔΠΧ,
- άλλες συμπληρωματικές πληροφορίες όπως:
  - τους σκοπούς επεξεργασίας,
  - τις κατηγορίες δεδομένων ΔΠΧ που επεξεργάζονται,
  - τους αποδέκτες των ΔΠΧ,
  - το χρονικό διάστημα αποθήκευσης,
  - την ύπαρξη δικαιώματος υποβολής αιτήματος (διόρθωση, διαγραφή, περιορισμού της επεξεργασίας και εναντίωσης),

[1] Ερμηνείες του κανονισμού σχετικά με τα δικαιώματα ΥΔ έχουν βασιστεί στην Αγγλική αρχή προστασίας δεδομένων - Information Commissioner's Office (ICO), " Guide to the General Data Protection Regulation (GDPR)" https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/ (τελευταία πρόσβαση 05/02/2018)

- το δικαίωμα υποβολής καταγγελίας,
- την προέλευση των ΔΠΧ,
- τη λογική που ακολουθείται στην αυτοματοποιημένη λήψη αποφάσεων, ένα υπάρχει, και τις πιθανές συνέπειες της επεξεργασίας αυτής στο ΥΔ. Στην αυτοματοποιημένη λήψη αποφάσεων περιλαμβάνεται και η κατάρτιση προφίλ,
- τις πιθανές διαβιβάσεις των ΔΠΧ σε τρίτες χώρες και τις εγγυήσεις αυτών.

Ο ΥΠΕ παρέχει στο ΥΔ τα παραπάνω χωρίς καθυστέρηση εντός μηνός από την παραλαβή του αιτήματος. Η εν λόγω προθεσμία μπορεί να παραταθεί, έως δύο μήνες, σε περιπτώσεις πολυπλοκότητας του αιτήματος ή μεγάλου όγκου αιτημάτων έχοντας ενημερώσει, εντός μηνός, το ΥΔ για τους λόγους της καθυστέρησης.

Η παροχή των παραπάνω πληροφοριών γίνεται δωρεάν και προβλέπεται ότι δύναται να παρέχεται εξ αποστάσεως σε ασφαλές σύστημα. Σε περιπτώσεις που το αίτημα του ΥΔ είναι προδήλως αβάσιμο ή υπερβολικό ο ΥΠΕ μπορεί να επιβάλει εύλογο τέλος λαμβάνοντας υπόψη τα σχετικά διοικητικά έξοδα ή να αρνηθεί να δώσει συνέχεια στο αίτημα αφού τον ενημερώσει.

[Δείτε περισσότερα στα άρ.12,15 και α.σ.65 του κανονισμού]

3. Δικαίωμα διόρθωσης

Είναι το δικαίωμα του υποκειμένου δεδομένων (ΥΔ) να απαιτήσει από τον υπεύθυνο επεξεργασίας (ΥΠΕ) χωρίς αδικαιολόγητη καθυστέρηση τη διόρθωση ανακριβών δεδομένων προσωπικού χαρακτήρα που το αφορούν. Έχοντας υπόψη τους σκοπούς της επεξεργασίας, το ΥΔ έχει το δικαίωμα να απαιτήσει τη συμπλήρωση ελλιπών δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων μέσω συμπληρωματικής δήλωσης.

[Δείτε περισσότερα στα άρ.12,16 και 19 του κανονισμού]

4. Δικαίωμα διαγραφής (δικαίωμα στη λήθη)

Είναι το δικαίωμα του υποκειμένου δεδομένων (ΥΔ) να ζητήσει από τον υπεύθυνο επεξεργασίας τη διαγραφή δεδομένων προσωπικού χαρακτήρα που το αφορούν χαρακτήρα χωρίς αδικαιολόγητη καθυστέρηση, εάν ισχύουν κάποιοι από τους παρακάτω λόγους:

- τα ΔΠΧ δεν είναι πλέον απαραίτητα σε σχέση με τους σκοπούς που συλλέχθηκαν / υποβλήθηκαν σε επεξεργάσία,
- το ΥΔ ανακαλεί τη συγκατάθεση του για την επεξεργασία ΔΠΧ,
- ο ΥΔ αντιτίθεται στην επεξεργασία και δεν υπάρχει κανένα υπερισχύον έννομο συμφέρον για τη συνέχιση της επεξεργασίας,
- Το ΥΔ αντιτίθεται στην επεξεργασία σύμφωνα με το δικαίωμα εναντίωσης (άρ.21§2) για σκοπούς απευθείας εμπορικής προώθησης,
- τα ΔΠΧ υποβλήθηκαν σε επεξεργασία παράνομα,

- τα ΔΠΧ πρέπει να διαγραφούν, ώστε να τηρηθεί νομική υποχρέωση,
- τα ΔΠΧ έχουν συλλεχθεί σε σχέση με την προσφορά υπηρεσιών της κοινωνίας των πληροφοριών σε παιδί.

Σε περιπτώσεις που τα ΔΠΧ έχουν κοινοποιηθεί σε τρίτους, ο ΥΠΕ θα πρέπει να τους ενημερώσει για το αίτημα διαγραφής ΔΠΧ (αντιγράφων , συνδέσμων σε αυτά ή αναπαραγωγών αυτών) του ΥΔ.

Τα παραπάνω εξαιρούνται :

- για την άσκηση του δικαιώματος ελευθερίας της έκφρασης και του δικαιώματος στην ενημέρωση,
- για την τήρηση νομικής υποχρέωσης εκπλήρωση καθήκοντος δημόσιου συμφέροντος ή άσκηση δημόσιας εξουσίας,
- για λόγους δημόσιου συμφέροντος στον τομέα της δημόσιας υγείας,
- για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς,
- για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων.

Ο κανονισμός ενισχύει το δικαίωμα διαγραφής διευκρινίζοντας ότι οι οργανισμοί που δημοσιεύουν ΔΠΧ θα πρέπει να ενημερώνουν τους άλλους οργανισμούς που κάνουν επεξεργασία δεδομένων να διαγράψουν τα αντίγραφα, τους συνδέσμους ή αναπαράγωγα των εν λόγω ΔΠΧ. Βεβαία όπως αναφέρθηκε ήδη, υπάρχουν περιπτώσεις στις οποίες οι οργανισμοί που επεξεργάζονται ΔΠΧ εξαιρούνται από την υποχρέωση του δικαιώματος της διαγραφής ΔΠΧ.

Παράδειγμα[2]: Μια μηχανή αναζήτησης ενημερώνει τον εκδότη ενός μέσου ότι διαγράφει τα αποτελέσματα αναζήτησης που συνδέονται με μια δική του είδηση λόγω αιτήματος διαγραφής από ένα άτομο. Εάν η δημοσίευση του άρθρου προστατεύεται από την ελευθερία έκφρασης, τότε ο εκδότης δεν υποχρεούται να διαγράψει το άρθρο.

[Δείτε περισσότερα στα άρ.17,19 και α.σ.65,66 του κανονισμού]

5. Δικαίωμα περιορισμού της επεξεργασίας

Είναι το δικαίωμα του υποκειμένου δεδομένων (ΥΔ) να περιοριστεί η επεξεργασία δεδομένων όταν ισχύουν κάποιες προϋποθέσεις. Όταν ισχύει ο περιορισμός της επεξεργασίας επιτρέπεται η αποθήκευση των δεδομένων όχι όμως η περαιτέρω επεξεργασία τους.

[2] Παράδειγμα από την Αγγλική αρχή προστασίας δεδομένων (ICO): Right to erasuse https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/ (τελευταία πρόσβαση 12/02/2018)

Ο περιορισμός επεξεργασίας μπορεί να ασκηθεί όταν ισχύει ένα από τα ακόλουθα:

- η ακρίβεια των ΔΠΧ αμφισβητείται από το ΥΔ, έως ότου ο ΥΠΕ επαληθεύσει την ακρίβεια των ΔΠΧ,
- η επεξεργασία είναι παράνομη και το ΥΔ αντιτάσσεται στη διαγραφή των δεδομένων προσωπικού χαρακτήρα και ζητεί, αντ' αυτής, τον περιορισμό της χρήσης τους,
- ο υπεύθυνος επεξεργασίας δεν χρειάζεται πλέον τα ΔΠΧ για τους σκοπούς της επεξεργασίας, αλλά τα δεδομένα αυτά απαιτούνται από το ΥΔ για τη θεμελίωση, την άσκηση ή την υποστήριξη νομικών αξιώσεων,
- το ΥΔ έχει αντιρρήσεις για την επεξεργασία (δικαίωμα εναντίωσης) και αναμένεται η επαλήθευση του κατά πόσον οι νόμιμοι λόγοι του ΥΠΕ υπερισχύουν έναντι των λόγων του ΥΔ.

Η άρση του περιορισμού της επεξεργασίας επιτρέπεται μόνο με τη συγκατάθεση του ΥΔ ή λόγω νομικών αξιώσεων ή για την προστασία άλλου νομικού ή φυσικού προσώπου ή για λόγους δημοσίου συμφέροντος.

Οι οργανισμοί πιθανόν να χρειαστεί να αναθεωρήσουν τις διαδικασίες τους για να μπορούν να προσδιορίσουν τις περιπτώσεις πού μπορεί να ζητηθεί ο περιορισμός της επεξεργασίας των προσωπικών δεδομένων.

Σε περιπτώσεις δημοσιοποίησης ή κοινοποίησης ΔΠΧ σε τρίτους θα πρέπει να γίνει ενημέρωση σε αυτούς για τον εν λόγω περιορισμό της επεξεργασίας των ΔΠΧ εκτός αν αυτό αποδειχθεί αδύνατο. Το ΥΔ θα πρέπει να ενημερώνεται σε κάθε περίπτωση καθώς επίσης και πριν από την άρση του περιορισμού της επεξεργασίας.

[Δείτε περισσότερα στα άρ.18, 19 και α.σ. 67 του κανονισμού]

6. Δικαίωμα φορητότητας

Είναι το δικαίωμα του υποκειμένου δεδομένων (ΥΔ) να λαμβάνει τα ΔΠΧ που το αφορούν σε μορφότυπο κοινώς αναγνώσιμο όταν:

- η επεξεργασία βασίζεται σε συγκατάθεση και
- η επεξεργασία διενεργείται με αυτοματοποιημένα μέσα.

Σε περιπτώσεις που είναι τεχνικά εφικτό, ο ΥΔ μπορεί να ζητήσει την απευθείας διαβίβαση των ΔΠΧ από τον ένα στον άλλο ΥΠΕ. Μορφότυπος κοινός αναγνώσιμος θεωρείται π.χ. ο τύπος αρχείων CSV. Οι πληροφορίες πρέπει να παρέχονται δωρεάν. Εάν τα προσωπικά δεδομένα αφορούν περισσότερα από ένα άτομα, πρέπει να εξετασθεί κατά πόσο η παροχή των πληροφοριών θίγει τα δικαιώματα οποιουδήποτε άλλου ατόμου.

[Δείτε περισσότερα στα άρ.12,20, α.σ.68 του κανονισμού και στην γνωμοδότηση της ΟΕ29 «Κατευθυντήριες γραμμές σχετικά με το δικαίωμα στη φορητότητα των δεδομένων», (WP 242 rev.01)]

7. Δικαίωμα εναντίωσης

Είναι το δικαίωμα του υποκειμένου δεδομένων (ΥΔ) να αντιτάσσεται ανά πάσα στιγμή στην επεξεργασία των ΔΠΧ που το αφορούν. Πιο συγκεκριμένα έχει δικαίωμα να εναντιωθεί σε:

- επεξεργασία με βάση νόμιμα συμφέροντα ή εκπλήρωση καθήκοντος προς το δημόσιο συμφέρον / άσκηση δημόσιας εξουσίας (συμπεριλαμβανομένης της κατάρτισης προφίλ),
- επεξεργασία για σκοπούς απευθείας εμπορικής προώθησης (συμπεριλαμβανομένης της κατάρτισης προφίλ)· και
- επεξεργασία για επιστημονική / ιστορική έρευνα και στατιστικές εκτός εάν η επεξεργασία είναι απαραίτητη για λόγους δημόσιου συμφέροντος.

[Δείτε περισσότερα στα άρ.12,21 και α.σ. 69,70 του κανονισμού]

8. Δικαίωμα σχετικά με την αυτοματοποιημένη λήψη αποφάσεων και κατάρτιση προφίλ

Είναι το δικαίωμα του ΥΔ να μην υπόκειται σε απόφαση που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας, συμπεριλαμβανομένης της κατάρτισης προφίλ, η οποία παράγει έννομα αποτελέσματα που το αφορούν ή το επηρεάζει σημαντικά με παρόμοιο τρόπο.

Η αυτοματοποιημένη ατομική λήψη αποφάσεων είναι μια απόφαση που γίνεται με αυτοματοποιημένα μέσα χωρίς ανθρώπινη εμπλοκή. Τέτοια παραδείγματα είναι :

- σύστημα online που λαμβάνει απόφαση χορήγησης δανείου,
- τεστ αξιολόγησης που λαμβάνει απόφαση για την πραγματοποίηση πρόσληψης

Η αυτοματοποιημένη ατομική λήψη αποφάσεων δεν προϋποθέτει τη δημιουργία προφίλ, συνήθως όμως συσχετίζεται με αυτή.

Εξαιρούνται από το παραπάνω δικαίωμα όταν η απόφαση :

α) είναι αναγκαία για τη σύναψη ή την εκτέλεση σύμβασης μεταξύ του υποκειμένου των δεδομένων και του υπευθύνου επεξεργασίας των δεδομένων,

β) επιτρέπεται από το Εθνικό ή Ενωσιακό δίκαιο,

γ) βασίζεται στη ρητή συγκατάθεση του υποκειμένου των δεδομένων.

[Δείτε περισσότερα στα άρ. 4§4, 9, 12, 13, 14, 15, 21, 22, 35§1§321,22 του κανονισμού και στη γνώμοδότηση της ΟΕ29 “Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679», (WP 251 αναθ.01) 06/02/2018]

Ερωτηματολόγιο εγχειριδίου αποτύπωσης

για τη συμμόρφωση με τον Ευρωπαϊκό Γενικό Κανονισμό Προστασίας Δεδομένων - General Data Protection Regulation (ΓΚΠΔ/GDPR) 2016/679

Π1 Εγχειρίδιο αποτύπωσης - Ερωτηματολόγιο

για τη συμμόρφωση με τον Ευρωπαϊκό Κανονισμό Προστασίας Προσωπικών δεδομένων (ΓΚΠΔ / GDPR) 2016/679

			Απάντηση					
Α/Α	**ID**	**Ερώτηση**	**Ναι**	**Όχι**	**Άγνωστο**	**Δεν αφορά**	**Επεξήγηση ερώτησης**	**Σχόλια ερωτώντος**
Εδαφικός προσδιορισμός - Διαβιβάσεις δεδομένων								
1	03-2 (I)	Οι εγκαταστάσεις του οργανισμού σας είναι εκτός ΕΕ ή ΕΟΧ (Ευρωπαϊκής Ένωσης - Ευρωπαϊκού Οικονομικού Χώρου);						
1.1	- ()	Αν ναι, έχετε ορίσει γραπτώς εκπρόσωπο στην ΕΕ ;						
2	44-- (V)	Τα ΔΠΧ που επεξεργάζεστε μένουν εντός της ΕΕ ή του ΕΟΧ;						
2.1	27-1 (IV)	Αν όχι, προσδιορίστε σε ποιες χώρες και με ποια νόμιμη διαδικασία.					Συμπληρώστε το σχετικό πίνακα στο παράρτημα ΠΑ-§2.1.	
Νομιμότητα Επεξεργασίας Προσωπικών Δεδομένων (ΠΔ)								
3	06-1 (II)	Είναι σύννομη η επεξεργασία ΔΠΧ;					Συμπληρώστε το σχετικό πίνακα στο παράρτημα ΠΑ-§3.	
3.1	8-1 (II)	Ζητάτε συγκατάθεση από παιδιά κάτω των 16 ετών για την επεξεργασία των ΔΠΧ τους;						
3.2	9-3 (II)	Τα ΔΠΧ χρησιμοποιούνται για σκοπούς προληπτικής ιατρικής;						
4	06-4 (II)	Έχει η επεξεργασία άλλο σκοπό από αυτόν που αρχικά έχουν συλλεγεί τα δεδομένα;						

			Απάντηση					
Α/Α	**ID**	**Ερώτηση**	**Ναι**	**Όχι**	**Άγνωστο**	**Δεν αφορά**	**Επεξήγηση ερώτησης**	**Σχόλια ερωτώντος**
4.1	- ()	Αν ναι, προσδιορίστε σχετικά.						
5	10-- (II)	Επεξεργάζεστε ΔΠΧ από ποινικές καταδίκες;						
5.1	- ()	Αν ναι, εκτελείτε τις επεξεργασίες αυτές αποκλειστικά υπό τον έλεγχο επίσημης αρχής (δικαστήριο, εφετείο κτλ.);						
Δικαιώματα Υποκειμένων Δεδομένων (ΥΔ)								
6	12-- (III)	Υπάρχει το δικαίωμα ενημέρωσης του ΥΔ για τα προσωπικά του δεδομένα;						
6.1	- ()	Αν ναι, προσδιορίστε σχετικά.					Συμπληρώστε το σχετικό πίνακα στο παράρτημα ΠΑ-§6.1.	
7	15-1 (III)	Υπάρχει δικαίωμα πρόσβασης του ΥΔ στα προσωπικά του δεδομένα;						
7.1	- ()	Αν ναι, προσδιορίστε σχετικά.					Συμπληρώστε το σχετικό πίνακα στο παράρτημα ΠΑ-§7.1.	
8	16-- (III)	Υπάρχει το δικαίωμα διόρθωσης δεδομένων του ΥΔ;						

			Απάντηση					
Α/Α	**ID**	**Ερώτηση**	**Ναι**	**Όχι**	**Άγνωστο**	**Δεν αφορά**	**Επεξήγηση ερώτησης**	**Σχόλια ερωτώντος**
8.1	- ()	Αν ναι, προσδιορίστε σχετικά.					Συμπληρώστε το σχετικό πίνακα στο παράρτημα ΠΑ-§8.1.	
9	17-1 (III)	Υπάρχει το δικαίωμα διαγραφής δεδομένων του ΥΔ;						
9.1	- ()	Αν ναι επιλέξτε για ποιες περιπτώσεις μπορεί να ασκηθεί το δικαίωμα της διαγραφής.					Συμπληρώστε το σχετικό πίνακα στο παράρτημα ΠΑ-§9.1.	
10	18-1 (III)	Υπάρχει το δικαίωμα περιορισμού της επεξεργασίας από το ΥΔ;						
10.1	- ()	Αν ναι, προσδιορίστε σχετικά.					Συμπληρώστε τους σχετικούς πίνακες στο παράρτημα ΠΑ-§10.1.	
11	20-1 (III)	Υπάρχει το δικαίωμα φορητότητας των δεδομένων;					Περισσότερες πληροφορίες στο παράρτημα ΠΑ-§11.	
12	21-- (III)	Υπάρχει το δικαίωμα εναντίωσης σε επεξεργασία δεδομένων;						
12.1	- ()	Αν ναι, προσδιορίστε σχετικά.					Συμπληρώστε τους σχετικούς πίνακες στο παράρτημα ΠΑ-§12	

			Απάντηση					
Α/Α	**ID**	**Ερώτηση**	**Ναι**	**Όχι**	**Άγνωστο**	**Δεν αφορά**	**Επεξήγηση ερώτησης**	**Σχόλια ερωτώντος**
13	22-- (III)	Υπάρχει το δικαίωμα εναντίωσης στη λήψη αυτοματοποιημένων αποφάσεων;					Περισσότερες πληροφορίες στο παράρτημα ΠΑ-§13.	
Υπεύθυνος Επεξεργασίας, Εκτελών, Υπεύθυνος προστασίας								
14	26-1 (IV)	Οι σκοποί και τα μέσα επεξεργασίας καθορίζονται από ένα μοναδικό υπεύθυνο επεξεργασίας (ΥΠΕ);						
15	30-5 (IV)	Απασχολείτε περισσότερα από 250 άτομα στον οργανισμό σας;						
16	30-1 (IV)	Ως υπεύθυνος επεξεργασίας (ΥΠΕ) τηρείτε αρχείο δραστηριοτήτων επεξεργασίας;						
16.1	- ()	Αν ναι, προσδιορίστε σχετικά.					Συμπληρώστε το σχετικό πίνακα στο παράρτημα ΠΑ-§16.1.	
17	28-2 (IV)	Είστε ο μοναδικός εκτελών την επεξεργασία (ΕΚΕ) ΔΠΧ;						
18	30-2 (IV)	Ως εκτελών την επεξεργασία (ΕΚΕ) τηρείτε αρχείο δραστηριοτήτων επεξεργασίας;						

			Απάντηση					
Α/Α	**ID**	**Ερώτηση**	**Ναι**	**Όχι**	**Άγνωστο**	**Δεν αφορά**	**Επεξήγηση ερώτησης**	**Σχόλια ερωτώντος**
18.1	- ()	Αν ναι, προσδιορίστε σχετικά.					Συμπληρώστε το σχετικό πίνακα στο παράρτημα ΠΑ-§18.1.	`
Θέματα ασφαλείας								
19	24-1 (IV) 32-1 (IV)	Είναι τα τεχνικά και οργανωτικά μέτρα κατάλληλα προκειμένου να διασφαλιστεί το κατάλληλο επίπεδο ασφάλειας της επεξεργασίας δεδομένων;					Συμπληρώστε το σχετικό πίνακα στο παράρτημα ΠΑ-§19.	
20	25-1 (IV)	Λαμβάνετε μέτρα προστασίας ΔΠΧ κατά το σχεδιασμό (by design) και εξ' ορισμού (by default) (αφορά περιπτώσεις που σχεδιάζετε νέες εφαρμογές);						
20.1	- ()	Αν ναι, προσδιορίστε σχετικά.					Συμπληρώστε το σχετικό πίνακα στο παράρτημα ΠΑ-§20.1.	
21	32-2 (IV)	Ποιους κινδύνους λαμβάνετε υπόψη κατά την επεξεργασία ΔΠΧ;					Συμπληρώστε το σχετικό πίνακα στο παράρτημα ΠΑ-§21.	

Π1 Εγχειρίδιο αποτύπωσης - Ερωτηματολόγιο

για τη συμμόρφωση με τον Ευρωπαϊκό Κανονισμό Προστασίας Προσωπικών δεδομένων (ΓΚΠΔ / GDPR) 2016/679

			Απάντηση					
Α/Α	**ID**	**Ερώτηση**	**Ναι**	**Όχι**	**Άγνωστο**	**Δεν αφορά**	**Επεξήγηση ερώτησης**	**Σχόλια ερωτώντος**
22	32-3 (IV)	Τηρείτε εγκεκριμένο κώδικα δεοντολογίας;						
22.1	- ()	Αν ναι, προσδιορίστε σχετικά.						
23	32-4 (IV)	Είναι κάθε φυσικό πρόσωπο που έχει πρόσβαση στα ΠΔ υπό την εποπτεία του ΥΠΕ ή ΕΚΕ;						
24	33-1 (IV)	Έχετε διαδικασία γνωστοποίησης σε περίπτωση παραβίασης δεδομένων στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ);						
24.1	- ()	Αν ναι, προσδιορίστε σχετικά.					Συμπληρώστε το σχετικό πίνακα στο παράρτημα ΠΑ-§24.1.	
25	34-1 (IV)	Έχετε διαδικασία γνωστοποίησης σε περίπτωση παραβίασης δεδομένων στο ΥΔ;						
25.1	- ()	Αν ναι, προσδιορίστε σχετικά.					Συμπληρώστε το σχετικό πίνακα στο παράρτημα ΠΑ-§25.1.	

Π1 Εγχειρίδιο αποτύπωσης - Ερωτηματολόγιο

για τη συμμόρφωση με τον Ευρωπαϊκό Κανονισμό Προστασίας Προσωπικών δεδομένων (ΓΚΠΔ / GDPR) 2016/679

			Απάντηση					
Α/Α	**ID**	**Ερώτηση**	**Ναι**	**Όχι**	**Άγνωστο**	**Δεν αφορά**	**Επεξήγηση ερώτησης**	**Σχόλια ερωτώντος**
26	35-1 (IV)	Έχετε μελέτη εκτίμησης αντικτύπου προστασίας δεδομένων (ΕΑΠΔ/DPIA);						
26.1	- ()	Αν όχι, συμπληρώστε το σχετικό πίνακα.					Συμπληρώστε το σχετικό πίνακα στο παράρτημα ΠΑ-§26.1.	
26.2	- ()	Αν ναι, προσδιορίστε σχετικά.					Συμπληρώστε το σχετικό πίνακα στο παράρτημα ΠΑ-§26.2.	
27	37-1 (IV)	Έχετε ορίσει υπεύθυνο προστασίας δεδομένων (ΥΠΔ/DPO);						
28	43-1 (IV)	Έχετε κάποια πιστοποίηση για την προστασία δεδομένων;						
28.1	- ()	Αν ναι, προσδιορίστε σχετικά.					Συμπληρώστε το σχετικό πίνακα στο παράρτημα ΠΑ-§28.1.	

Παράρτημα (ΠΑ)
εγχειριδίου αποτύπωσης

για τη συμμόρφωση με τον Ευρωπαϊκό Γενικό Κανονισμό Προστασίας Δεδομένων - General Data Protection Regulation (ΓΚΠΔ/GDPR) 2016/679

Περιεχόμενα παραρτήματος

Εδαφικός προσδιορισμός – Διαβιβάσεις δεδομένων

ΠΑ-§2.1 Διαβιβάσεις δεδομένων

Επιλέξτε, βάσει του πίνακα που ακολουθεί, τις χώρες που διαβιβάζετε ΔΠΧ. Αναφέρετε σχετικές αποφάσεις που νομιμοποιούν τη διαβίβαση δεδομένων εκτός ΕΕ.

Επιτρεπόμενες χώρες/ τρόποι διαβίβασης δεδομένων (άρ. 44-50)				
Επιλογή	Χώρα	Διαβίβαση βάσει	Παρατηρήσεις	Σχόλια
☐	Κράτη μέλη Ευρωπαϊκής Ένωσης – Ευρωπαϊκού Οικονομικού Χώρου (Ισλανδία, Λίχτενσταϊν Νορβηγία)	ΕΕ - ΕΟΧ Ευρωπαϊκή Ένωση - Ευρωπαϊκός Οικονομικός Χώρος	Επιτρέπεται βάσει του παρόντος κανονισμού (ΓΚΠΔ/GDPR)	
☐	ΗΠΑ	Privacy Shield	Ευθύνη εταιρειών να συμμορφωθούν με υποχρεώσεις και εγγυήσεις του μηχανισμού “Privacy Shield”	
☐	AD – Ανδόρα	Αποφάσεις Επάρκειας Ευρωπαϊκής Επιτροπής (Τελευταία ενημέρωση: 06/02/2018) (Commission Adequacy Decisions)	Η Ευρωπαϊκή επιτροπή αποφασίζει αν η χώρα που θα διαβιβασθούν τα ΔΠΧ πληροί τις προϋποθέσεις	
☐	AR – Αργεντινή			
☐	CA – Καναδάς			
☐	CH – Ελβετία			
☐	FO – Νήσοι Φερόες			
☐	GG - Γκέρνσεϊ			
☐	IL - Ισραήλ			
☐	IM – Νήσος του Μάν			
☐	JE - Τζέρσεϊ			

☐	NZ - Νέα Ζηλανδία				
☐	UY - Ανατολική Δημοκρατία της Ουρουγουάης				
☐	JP - Ιαπωνία				
☐	Άλλη χώρα, Προσδιορίστε:……	☐	Νομικό δεσμευτικό εκτελεστό μέσο μεταξύ δημόσιων αρχών ή φορέων (άρ.46§2α) Προσδιορίστε: ……	Δε χρειάζεται άδεια από την ΑΠΔΠΧ	
		☐	Εταιρικοί Δεσμευτικοί Κανόνες (Binding Corporate Rules - BCR) (άρ.47) Προσδιορίστε: ……	Δε χρειάζεται άδεια από την ΑΠΔΠΧ. Κατά περίπτωση δεσμευτικοί κανόνες	
		☐	Πρότυπες Συμβατικές Ρήτρες της Επιτροπής (Standard Contractual Clauses) (άρ.46§2γ) Προσδιορίστε: ……	Δε χρειάζεται άδεια από την ΑΠΔΠΧ	
		☐	Πρότυπες Συμβατικές Ρήτρες της ΑΠΔΠΧ (Standard Contractual Clauses) (άρ.46§2δ) Προσδιορίστε: ……	Δε χρειάζεται άδεια από την ΑΠΔΠΧ	
		☐	Εγκεκριμένος κώδικας δεοντολογίας (άρ.46§2ε) Προσδιορίστε: ……	Δε χρειάζεται άδεια από την ΑΠΔΠΧ	
		☐	Εγκεκριμένος μηχανισμός πιστοποίησης (άρ.46§2στ) Προσδιορίστε: ……	Δε χρειάζεται άδεια από την ΑΠΔΠΧ	
		☐	Συμβατικές ρήτρες μεταξύ ΥΠΕ η ΕΚΕ ή αποδέκτη ΔΠΧ τρίτης χώρας ή διεθνή οργανισμό (άρ.46§3α) Προσδιορίστε: ……	Με την επιφύλαξη της άδειας από την ΑΠΔΠΧ	
		☐	Διατάξεων σε διοικητικές ρυθμίσεις μεταξύ δημόσιων αρχών ή φορέων Προσδιορίστε: ……	Με την επιφύλαξη της άδειας από την ΑΠΔΠΧ	

		☐	Ρητή συγκατάθεση του ΥΔ για διαβίβαση στη συγκεκριμένη χώρα		
		☐	Εκτέλεση σύμβασης (ή προσυμβατικά μέτρα) μεταξύ ΥΔ και ΥΠΕ		
		☐	Εκτέλεση σύμβασης προς όφελος του ΥΔ μεταξύ ΥΠΕ και άλλου φυσικού/νομικού προσώπου		
		☐	Σημαντικούς λόγους Δημόσιου Συμφέροντος Προσδιορίστε: ……		
		☐	Θεμελίωση , άσκηση ή υποστήριξη νομικών αξιώσεων Προσδιορίστε: ……		
		☐	Προστασία ζωτικών συμφερόντων του ΥΔ		
		☐	Άλλο, Προσδιορίστε: ……		

ΠΑ-§3 Σύννομη επεξεργασία δεδομένων

Ακολουθήστε τα παρακάτω βήματα ώστε να γίνει α) καταγραφή των ΔΠΧ που επεξεργάζεστε* και β) διερεύνηση της σύννομης επεξεργασίας αυτών.

1. Στον πίνακα που ακολουθεί καταγράψτε τα ΔΠΧ που επεξεργάζεστε ανά παροχή ή λήψη υπηρεσίας (Εισερχόμενα, Εξερχόμενα, Δημιουργημένα εντός).
   π.χ. δεδομένα πελάτη για παροχή υπηρεσίας αγοράς αγαθών.
   δεδομένα προμηθευτή(ή εργαζομένου) για λήψη υπηρεσίας καθαριότητας.

2. Στον ίδιο πίνακα, αιτιολογήστε ποια είναι η σύννομη προϋπόθεση για καθένα από αυτά. Λάβετε υπόψη τους πίνακες:
   α) «Ενδεικτική λίστα Δεδομένων Προσωπικού Χαρακτήρα (ΔΠΧ) (άρ.4,9)» σελίδα 9
   β) «Επιτρεπόμενες περιπτώσεις επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (ΔΠΧ) (άρ.6,9-11)» σελίδα 10
   γ) «Αρχές επεξεργασίας ΔΠΧ βάσει του κανονισμού (άρ.5§1)» σελίδα 11
   δ) «Συναίνεση – Ρητή συγκατάθεση» σελίδα 12

3. Επιβεβαιώστε ότι ισχύει τουλάχιστον μία από τις σύννομες προϋποθέσεις για κάθε ένα από τα ΔΠΧ που επεξεργάζεσθε

Χρησιμοποιήστε τον πίνακα όσες φορές χρειαστεί ώστε να γίνει η πλήρης καταγραφή των δεδομένων που χρησιμοποιούνται.

*Στον όρο επεξεργασία περιλαμβάνεται κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή.

Καταγραφή ΔΠΧ που υπόκεινται σε επεξεργασία																		
Υπηρεσία **(π.χ. Κάρτα μέλους πελατών)**:																		
Καταγραφή									**Αιτιολόγηση**									
Α/Α	**Δεδομένο**	**Πηγή**	**Μορφή**	**Αποθήκευση**	**Χρόνος διατήρησης**	**Πρόσβαση**	**Υπεύθυνος συλλογής**	**Διαμοιρασμός**	**Σύννομο βάσει**	**Αρχές επεξεργασίας**								
	Ποιο ΔΠΧ συλλέγετε.. Δείτε πίνακα: «Ενδεικτική λίστα Δεδομένων Προσωπικού Χαρακτήρα (ΔΠΧ) (άρ.4,9))»	Από πού συλλέγετε το ΔΠΧ π.χ. ΥΔ, πληροφοριακό σύστημα, άλλο οργανισμό κτλ.	Ποιά είναι η μορφή του δεδομένου πχ έντυπη, λογιστικό φύλλο, έγγραφο κειμένου, ΒΔ, Πληροφοριακό Σύστημα κτλ.	Ποιά είναι η φυσική αποθήκευση του ΔΠΧ π.χ. έντυπο, αφαιρούμενος / Τοπικός / δικτυακός / Cloud δίσκος, Διακομιστής	Πόσο καιρό διατηρείται το ΔΠΧ για τη συγκεκριμένη υπηρεσία.	Ποιές ομάδες υπαλλήλων έχουν πρόσβαση και ποιό το είδος πρόσβασης π.χ. τμ. Προσωπικού – Write, δντές - Read, τμ. πληροφορικής	Ποιός είναι ο υπεύθυνος συλλογής του ΔΠΧ	Πού διαμοιράζεται το ΔΠΧ εκτός του οργανισμού πχ. προμηθευτής, εταιρία λογιστηρίου κτλ	Αιτιολογείστε ποιά είναι η σύννομη προϋπόθεση βάσει του πίνακα «Επιτρεπόμενες περιπτώσεις επεξεργασίας ΔΠΧ (άρ.6,9-11)»	Επιλέξτε με ✓ τις αρχές που τηρείτε για το συγκεκριμένο δεδομένο							
										Αντικειμενικότητα	Διαφάνεια	Περιορισμός σκοπού	Ελαχιστοποίηση δεδομένων	Ακρίβεια	Περιορισμός περιόδου αποθήκευσης	Ακεραιότητα	Εμπιστευτικότητα
1																	
2																	
3																	
4																	
5																	
6																	
7																	
8																	

Καταγραφή ΔΠΧ που υπόκεινται σε επεξεργασία																		
Υπηρεσία **(π.χ. Κάρτα μέλους πελατών)**:																		
Καταγραφή									**Αιτιολόγηση**									
Α/Α	**Δεδομένο**	**Πηγή**	**Μορφή**	**Αποθήκευση**	**Χρόνος διατήρησης**	**Πρόσβαση**	**Υπεύθυνος συλλογής**	**Διαμοιρασμός**	**Σύννομο βάσει**	**Αρχές επεξεργασίας**								
	Ποιο ΔΠΧ συλλέγετε.. Δείτε πίνακα: «Ενδεικτική λίστα Δεδομένων Προσωπικού Χαρακτήρα (ΔΠΧ) (άρ.4,9))»	Από πού συλλέγετε το ΔΠΧ π.χ. ΥΔ, πληροφοριακό σύστημα, άλλο οργανισμό κτλ.	Ποιά είναι η μορφή του δεδομένου πχ έντυπη, λογιστικό φύλλο, έγγραφο κειμένου, ΒΔ, Πληροφοριακό Σύστημα κτλ.	Ποιά είναι η φυσική αποθήκευση του ΔΠΧ π.χ. έντυπο, αφαιρούμενος / Τοπικός / δικτυακός / Cloud δίσκος, Διακομιστής	Πόσο καιρό διατηρείται το ΔΠΧ για τη συγκεκριμένη υπηρεσία.	Ποιές ομάδες υπαλλήλων έχουν πρόσβαση και ποιό το είδος πρόσβασης π.χ. τμ. Προσωπικού – Write, δντές - Read, τμ. πληροφορικής	Ποιός είναι ο υπεύθυνος συλλογής του ΔΠΧ	Πού διαμοιράζεται το ΔΠΧ εκτός του οργανισμού πχ. προμηθευτής, εταιρία λογιστηρίου κτλ	Αιτιολογείστε ποιά είναι η σύννομη προϋπόθεση βάσει του πίνακα «Επιτρεπόμενες περιπτώσεις επεξεργασίας ΔΠΧ (άρ.6,9-11)»	Επιλέξτε με ✓ τις αρχές που τηρείτε για το συγκεκριμένο δεδομένο							
										Αντικειμενικότητα	Διαφάνεια	Περιορισμός σκοπού	Ελαχιστοποίηση δεδομένων	Ακρίβεια	Περιορισμός περιόδου αποθήκευσης	Ακεραιότητα	Εμπιστευτικότητα
9																	
10																	
11																	
12																	
13																	
14																	
15																	
Παρατηρήσεις:																		

Ενδεικτική λίστα Δεδομένων Προσωπικού Χαρακτήρα (ΔΠΧ) (άρ.4,9)			
Δεδομένα Προσωπικού Χαρακτήρα (άρ.4§1)		Δεδομένα Προσωπικού Χαρακτήρα Ειδικών Κατηγοριών (άρ.9§1)	
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:		Κάθε πληροφορία που αποκαλύπτει:	
1	Όνομα	1	Φυλετική ή εθνοτική καταγωγή
2	Επώνυμο	2	Πολιτικά φρονήματα
3	Αριθμός Ταυτότητας	3	Θρησκευτικές ή φιλοσοφικές πεποιθήσεις
4	Ηλικία	4	Συμμετοχή σε συνδικαλιστική οργάνωση
5	Κατοικία	5	Γενετικά - βιομετρικά δεδομένα
6	Επάγγελμα	6	Υγείας
7	Οικογενειακή κατάσταση	7	Σεξουαλική ζωή ή γενετήσιο προσανατολισμό
8	Φυσικά χαρακτηριστικά		
9	Εκπαίδευση		
10	Εργασία (προϋπηρεσία, εργασιακή συμπεριφορά κλπ)		
11	Οικονομική κατάσταση (έσοδα, περιουσιακά στοιχεία, οικονομική συμπεριφορά)		
12	Ενδιαφέροντα		
13	Δραστηριότητες		
14	Συνήθειες		
15	Δεδομένα θέσης		
16	…		

Επιτρεπόμενες περιπτώσεις επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (ΔΠΧ) (άρ.6,9 -11)	
Δεδομένα προσωπικά	Δεδομένα ειδικών κατηγοριών (εξαιρέσεις)
Συναίνεση (consent) (άρ.6§1α)	Συναίνεση – Ρητή συγκατάθεση (explicit consent) (άρ.9§2α)
Έννομη υποχρέωση (legal obligation) (άρ.6§1γ)	Έννομη υποχρέωση (legal obligation) (άρ.9§2β)
Ζωτικού συμφέροντος (vital Interests) (άρ.6§1δ)	Ζωτικού συμφέροντος (vital interests) (άρ.9§2γ)

Εκτέλεση σύμβασης (contract) (άρ.6§1β)	Μέλη φορέα (organization members) (άρ.9§2δ)
Δημόσια εξουσία (public function) (άρ.6§1ε) (επεξεργασία από ποινικές καταδίκες και αδικήματα – μόνο υπο έλεγχο επίσημης αρχής ή από νομοθεσία) (άρ.10)	Προδήλως δημοσιοποιημένα (manifestly public) (άρ.9§2ε)
Έννομα συμφέροντα (legitimate interests) (άρ.6§1στ)	Υποστήριξη νομικών αξιώσεων (legal claims establishment) (άρ.9§2στ)
Ανέφικτη εξακρίβωση ταυτότητας (unable identification) (άρ.11)	Δημόσιο συμφέρον (public interest) (άρ.9§2ζ)
Αρχειοθέτηση για δημόσιο συμφέρον συμφέρον (public interest archiving purposes), επιστημονική ή ιστορική έρευνα, στατιστικούς σκοπούς (άρ.89 §1,2)	Προληπτική επαγγελματική ιατρική (preventive or occupational medicine) (άρ.9§2η)
	Δημόσιο συμφέρον δημόσιας υγείας (public health interest) (άρ.9§2θ)
	Αρχειοθέτηση για δημόσιο συμφέρον (public interest archiving purposes), επιστημονική ή ιστορική έρευνα, στατιστικούς σκοπούς (άρ.9§2ι, άρ.89 §1,2)

Αρχές επεξεργασίας ΔΠΧ βάσει του κανονισμού (άρ.5§1)	
1	Νομιμότητα Τα ΔΠΧ να υποβάλλονται σε σύννομη επεξεργασία
2	Αντικειμενικότητα Η επεξεργασία ΔΠΧ να είναι θεμιτή
3	Διαφάνεια Η επεξεργασία ΔΠΧ να είναι διαφανής
4	Περιορισμός σκοπού Τα ΔΠΧ να συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και να μην υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς• η περαιτέρω επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς θεωρείται συμβατή με τους αρχικούς σκοπούς.
5	Ελαχιστοποίηση δεδομένων Τα ΔΠΧ να είναι κατάλληλα, συναφή και να περιορίζονται στο αναγκαίο για τους σκοπούς που υποβάλλονται σε επεξεργασία

6	Ακρίβεια Τα ΔΠΧ να είναι ακριβή, διαφορετικά να επικαιροποιούνται ή να διαγράφονται
7	Περιορισμός περιόδου αποθήκευσης Τα ΔΠΧ να διατηρούνται μόνο για το διάστημα που απαιτείται για τους σκοπούς που έχουν συλλεχθεί• επιτρέπεται η αποθήκευση τους για μεγαλύτερα διαστήματα εφόσον τα ΔΠΧ θα υποβάλλονται σε επεξεργασία μόνο για τους σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για τους σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς και εφόσον εφαρμόζονται τα κατάλληλα τεχνικά και οργανωτικά μέτρα
8	Ακεραιότητα Τα ΔΠΧ να μην τροποποιούνται από μη εξουσιοδοτημένες οντότητες (συστήματα, ανθρώπους κτλ.),
9	Εμπιστευτικότητα Τα ΔΠΧ να μην αποκαλύπτονται σε μη εξουσιοδοτημένες οντότητες (συστήματα, ανθρώπους κτλ.),
10	Λογοδοσία Ο υπεύθυνος επεξεργασίας (ΥΠΕ) φέρει ευθύνη για την τήρηση όλων των παραπάνω αρχών και θα πρέπει να είναι σε θέση να το αποδείξει

Συναίνεση – Ρητή συγκατάθεση	
Συναίνεση (Consent) (άρ.6§1α)	Συναίνεση – Ρητή συγκατάθεση (Explicit Consent) (άρ.9§2α)
«συγκατάθεση» του υποκειμένου των δεδομένων είναι 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 (αρ 4 §11)	Η ρητή συγκατάθεση είναι περιγραφή δήλωσης προκειμένου να αρθούν τους οι πιθανές αμφιβολίες και ενδεχόμενες ελλείψεις αποδεικτικών στοιχείων.
Για περισσότερες πληροφορίες ανατρέξτε: α) στη γνωμοδότηση WP 259 /2017 τους ομάδας Εργασίας του άρθρου 29 (WP29), «Guidelines on Consent under Regulation 2016/679» 28/11/2017 (τελευταία ενημέρωση 11/01/2018). Εκκρεμεί ανοιχτή διαβούλευση 23/01/2018 http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611232 β) στη γνωμοδότηση WP 187/2011 τους ομάδας Εργασίας του άρθρου 29 (WP29), «Γνώμη 15/201 σχετικά με τον ορισμό τους συγκατάθεσης» 13/07/2011.	

Δικαιώματα Υποκειμένων Δεδομένων (ΥΔ)

ΠΑ-§6.1 Δικαίωμα ενημέρωσης

Επιλέξτε τι ισχύει από τα παρακάτω σχετικά με το δικαίωμα τους ενημέρωσης του ΥΔ για τα προσωπικά του δεδομένα που επεξεργάζετε ή πρόκειται να επεξεργαστεί ο οργανισμός .

Α. Μορφή παρεχόμενων πληροφοριών στο ΥΔ (άρ.13,14)						
	Οι πληροφορίες που παρέχετε σχετικά με την επεξεργασία των ΔΠΧ:	ΝΑΙ	ΟΧΙ	ΑΓΝΩΣΤΟ	ΔΕΝ ΑΦΟΡΑ	Αν ναι Προσδιορίστε σχετικά
1.	είναι σε συνοπτική, διαφανή και κατανοητή μορφή;					----------
2.	είναι εύκολα προσβάσιμες ; (αν ναι προσδιορίστε)					
3.	είναι με σαφή και απλή διατύπωση;					----------
4.	σε περιπτώσεις που απευθύνεστε σε παιδί, είναι προσεγμένες ιδιαιτέρως για τη σαφή και απλή διατύπωση τους ; (αν ναι προσδιορίστε τον τρόπο)					Γραπτά (έντυπα) Γραπτά (Ηλεκτρονικά) Προφορικά Άλλο: .....
5.	είναι δωρεάν η διάθεση τους;					----------
Β. Τρόπος διάθεση πληροφοριών στο ΥΔ						
	Εντυπα (π.χ. μέσω πολιτικής ιδιωτικότητας)					
	Ηλεκτρονικά					
	Προφορικά					
	Άλλο:					
Γ. Χρόνος διάθεσης πληροφοριών στο ΥΔ						
1.	*(Για τις περιπτώσεις που η λήψη γίνεται από το ΥΔ)* Η παροχή των πληροφοριών γίνεται κατά τη λήψη των ΔΠΧ;					----------

-	*(Για τις περιπτώσεις που η λήψη δε γίνεται από το ΥΔ)* Η παροχή των πληροφοριών γίνεται:					
1.	εντός μηνός					----------
2.	κατά την πρώτη επικοινωνία με το ΥΔ					----------
3.	κατά τη γνωστοποίηση σε άλλον αποδέκτη					----------

Επιλέξτε το είδος της πληροφορίας που περιλαμβάνετε στην ενημέρωση του ΥΔ (σε δήλωση ιδιωτικότητας ή άλλο)

Δ. Είδος παρεχόμενων πληροφοριών (άρ.13,14)					
	Πληροφορία	ΝΑΙ	ΟΧΙ	ΑΓΝΩΣΤΟ	ΔΕΝ ΑΦΟΡΑ
1.	Στοιχεία επικοινωνίας του υπευθύνου επεξεργασίας και, κατά περίπτωση, του εκπροσώπου του υπευθύνου επεξεργασίας				
2.	Στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων, κατά περίπτωση				
3.	Σκοπούς της επεξεργασίας για τους οποίους προορίζονται τα δεδομένα προσωπικού χαρακτήρα, καθώς και τη νομική βάση για την επεξεργασία				
4.	Εάν η επεξεργασία βασίζεται σε σκοπούς έννομων συμφερόντων (άρ.6§1), τα έννομα συμφέροντα που επιδιώκονται από τον υπεύθυνο επεξεργασίας ή από τρίτο				
5.	Τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων προσωπικού χαρακτήρα, εάν υπάρχουν				
6.	Διαβίβαση δεδομένων σε τρίτη χώρα, εάν υπάρχει				
7.	Το χρονικό διάστημα αποθήκευσης ή τα κριτήρια που καθορίζουν το εν λόγω διάστημα				
8.	Το δικαίωμα υποβολής αιτήματος για τα δικαιώματα του Υποκειμένου Δεδομένων (ΥΔ)				
9.	Το δικαίωμα ανακάλεσης της συναίνεσης / ρητής συγκατάθεσης				
10.	Το δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή				
11.	Την τυχόν υποχρέωση του ΥΔ να παρέχει ΔΠΧ με αναφορά στο λόγο (νομική - συμβατική υποχρέωση ή σύμβαση)				
12.	Τις συνέπειες μη παροχής ΔΠΧ όταν υπάρχει υποχρέωση λόγω νομικής ή συμβατικής υποχρέωσης ή σύμβασης				

13.	Την τυχόν ύπαρξη, αυτοματοποιημένης λήψης αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ, τη σημασία και τις προβλεπόμενες συνέπειες της εν λόγω επεξεργασίας για το ΥΔ				
14.	Την πηγή των δεδομένων (σε περιπτώσεις που δεν έχει γίνει συλλογή από το ΥΔ)				

ΠΑ-§7.1 Δικαίωμα πρόσβασης

Επιλέξτε τι ισχύει από τα παρακάτω σχετικά με το δικαίωμα της πρόσβασης του ΥΔ στα προσωπικά του δεδομένα.

Α. Πληροφορίες στο ΥΔ για το δικαίωμα πρόσβασης. (άρ.13,14)					
	Παρέχετε στο ΥΔ το δικαίωμα να :	ΝΑΙ	ΟΧΙ	ΑΓΝΩΣΤΟ	ΔΕΝ ΑΦΟΡΑ
1.	λάβει επιβεβαίωση για την επεξεργασία των δικών του ΔΠΧ				
2.	λάβει πρόσβαση στα δικά του ΔΠΧ				
3.	λάβει πληροφορίες για τους σκοπούς επεξεργασίας				
4.	λάβει πληροφορίες για τις κατηγορίες δεδομένων ΔΠΧ που επεξεργάζονται				
5.	λάβει πληροφορίες για τους αποδέκτες των ΔΠΧ				
6.	λάβει πληροφορίες για το χρονικό διάστημα αποθήκευσης				
7.	λάβει πληροφορίες για την ύπαρξη δικαιώματος υποβολής αιτήματος (διόρθωση , διαγραφή, περιορισμού της επεξεργασίας και εναντίωσης)				
8.	λάβει πληροφορίες για το δικαίωμα υποβολής καταγγελίας				
9.	λάβει πληροφορίες για την προέλευση των ΔΠΧ (αφορά τις περιπτώσεις που δε συλλέγονται από το ΥΔ)				
10.	λάβει πληροφορίες για τη λογική που ακολουθείται στην αυτοματοποιημένη λήψη αποφάσεων, ένα υπάρχει, και τις πιθανές συνέπειες της επεξεργασίας αυτής στο ΥΔ.				
11.	λάβει αντίγραφο δεδομένων του ΥΔ				

	Αν ναι προσδιορίστε :				
	Εντυπα				
	Ηλεκτρονικά				
	Άλλο: ……..				
12.	λάβει ενημέρωση για τυχόν διαβίβαση ΔΠΧ σε τρίτες χώρες				

Επιλέξτε πως ενημερώνετε το ΥΔ σχετικά με τη διαβίβαση ΔΠΧ του σε τρίτες χώρες .

Β. Τρόπος ενημέρωσης ΥΔ για διαβίβαση ΔΠΧ σε τρίτες χώρες (άρ.15§2,46)									
Τρόπος ενημέρωσης		Ενημέρωση για τη διαβίβαση				Ενημέρωση για τις εγγυήσεις			
		ΝΑΙ	ΟΧΙ	ΑΓΝΩΣΤΟ	ΔΕΝ ΑΦΟΡΑ	ΝΑΙ	ΟΧΙ	ΑΓΝΩΣΤΟ	ΔΕΝ ΑΦΟΡΑ
	Προφορικά								
	Γραπτά (έντυπο - δήλωση ιδιωτικότητας)								
	Γραπτά (έντυπο - προσδιορίστε: ……..)								
	Γραπτά (Ηλεκτρονικά - δήλωση ιδιωτικότητας)								
	Γραπτά (Ηλεκτρονικά - προσδιορίστε: ……..)								
	Άλλο: ……..								

ΠΑ-§8.1 Δικαίωμα διόρθωσης

Επιλέξτε πως παρέχετε στο ΥΔ τη δυνατότητα διόρθωσης των δεδομένων του .

Τρόπος διόρθωσης των δεδομένων του ΥΔ					
	Τρόπος	ΝΑΙ	ΟΧΙ	ΑΓΝΩΣΤΟ	ΔΕΝ ΑΦΟΡΑ
1	Εντυπα				
2	Ηλεκτρονικά				
3	Άλλο: ……..				

ΠΑ-§9.1 Δικαίωμα διαγραφής (δικαίωμα στη λήθη)

Συμπληρώστε τον παρακάτω πίνακα σχετικά με το δικαίωμα διαγραφής.

Α. Δικαίωμα διαγραφής					
	Επιλέξτε για ποιες από τις παρακάτω περιπτώσεις υπάρχει διαδικασία διαγραφής ΔΠΧ μετά από αίτημα του ΥΔ (άρ17)	ΝΑΙ	ΟΧΙ	ΑΓΝΩΣΤΟ	ΔΕΝ ΑΦΟΡΑ
1	Τα ΔΠΧ δεν είναι πλέον απαραίτητα σε σχέση με τους σκοπούς για τους οποίους συλλέχθηκαν / ή υποβλήθηκαν σε επεξεργασία				
2	Το ΥΔ ανακαλεί τη συγκατάθεση (συναίνεση ή ρητή - αρ.6§1α,9§2α) βάσει της οποίας γίνεται η επεξεργασία και δεν υπάρχει άλλη νομική βάση για την επεξεργασία				
3	Το ΥΔ αντιτίθεται στην επεξεργασία σύμφωνα με το δικαίωμα εναντίωσης (άρ.21§1) όταν δεν υπάρχουν λόγοι δημοσίου συμφέροντος – άσκηση δημόσιας εξουσίας ή έννομων συμφερόντων / θεμελιώδη δικαιώματα και ελευθερίες ΥΔ				
4	Το ΥΔ αντιτίθεται στην επεξεργασία σύμφωνα με το δικαίωμα εναντίωσης (άρ.21§2) για σκοπούς απευθείας εμπορικής προώθησης				

5	Τα ΔΠΧ υποβλήθηκαν σε επεξεργασία παράνομα				
6	Ως τήρηση νομικής υποχρέωσης βάσει του ενωσιακού δικαίου ή του δικαίου της Ελλάδος , στην οποία υπόκειται ο υπεύθυνος επεξεργασίας				
7	Τα ΔΠΧ έχουν συλλεχθεί σε σχέση με την προσφορά υπηρεσιών της κοινωνίας των πληροφοριών σε παιδί				
8	Άλλο, προσδιορίστε: ……				
Β. Δικαίωμα διαγραφής σε περίπτωση κοινοποίησης σε τρίτους					
	Σε περιπτώσεις που τα ΔΠΧ έχουν κοινοποιηθεί σε τρίτους, έχετε διαδικασία ενημέρωσης προς αυτούς για το αίτημα διαγραφής ΔΠΧ (αντιγράφων , συνδέσμων σε αυτά ή αναπαραγωγών αυτών) του ΥΔ.				
Γ. Εξαιρέσεις δικαιώματος διαγραφής					
Επιλέξτε ποιες περιπτώσεις λαμβάνετε υπόψη ως εξαιρέσεις στο δικαίωμα διαγραφής:					
1	την άσκηση του δικαιώματος ελευθερίας της έκφρασης και του δικαιώματος στην ενημέρωση				
2	την τήρηση νομικής υποχρέωσης εκπλήρωση καθήκοντος δημόσιου συμφέροντος ή άσκηση δημόσιας εξουσίας				
3	για λόγους δημόσιου συμφέροντος στον τομέα της δημόσιας υγείας				
4	για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς				
5	για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων				

.

ΠΑ-§10.1 Δικαίωμα περιορισμού της επεξεργασίας

Επιλέξτε για ποιες από τις παρακάτω περιπτώσεις μπορεί να ασκηθεί το δικαίωμα διαδικασίας περιορισμού της επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (ΔΠΧ), από το υποκείμενο δεδομένων (ΥΔ) και σε ποιες περιπτώσεις είναι εφικτή η άρση .

Περιπτώσεις περιορισμού της επεξεργασίας από το υποκείμενο δεδομένων (ΥΔ)(άρ.18§1)					
	Περίπτωση	ΝΑΙ	ΟΧΙ	ΑΓΝΩΣΤΟ	ΔΕΝ ΑΦΟΡΑ
1	Η ακρίβεια των δεδομένων προσωπικού χαρακτήρα αμφισβητείται από το υποκείμενο των δεδομένων, για χρονικό διάστημα που επιτρέπει στον υπεύθυνο επεξεργασίας να επαληθεύσει την ακρίβεια των δεδομένων προσωπικού χαρακτήρα,				
2	Η επεξεργασία είναι παράνομη και το υποκείμενο των δεδομένων αντιτάσσεται στη διαγραφή των δεδομένων προσωπικού χαρακτήρα και ζητεί, αντ' αυτής, τον περιορισμό της χρήσης τους,				
3	Ο υπεύθυνος επεξεργασίας δεν χρειάζεται πλέον τα δεδομένα προσωπικού χαρακτήρα για τους σκοπούς της επεξεργασίας, αλλά τα δεδομένα αυτά απαιτούνται από το υποκείμενο των δεδομένων για τη θεμελίωση, την άσκηση ή την υποστήριξη νομικών αξιώσεων,				
4	Το υποκείμενο των δεδομένων έχει αντιρρήσεις για την επεξεργασία όταν δεν υπάρχουν λόγοι δημοσίου συμφέροντος – άσκηση δημόσιας εξουσίας ή έννομών συμφερόντων / θεμελιώδη δικαιώματα και ελευθερίες ΥΔ				
5	Άλλο, προσδιορίστε: ……				

Περιπτώσεις άρσης περιορισμού της επεξεργασίας (άρ.18§2)					
	Περίπτωση	ΝΑΙ	ΟΧΙ	ΑΓΝΩΣΤΟ	ΔΕΝ ΑΦΟΡΑ
1	Συγκατάθεση του υποκειμένου των δεδομένων				
2	Για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων				
3	Για την προστασία των δικαιωμάτων άλλου φυσικού ή νομικού προσώπου				
4	Για λόγους σημαντικού δημόσιου συμφέροντος της Ευρωπαϊκής Ένωσης ή κράτους μέλους				
5	Άλλο, προσδιορίστε: ……				

ΠΑ-§11 Δικαίωμα φορητότητας

Ενημερωθείτε για τις περιπτώσεις του δικαιώματος φορητότητας δεδομένων.

Περιπτώσεις δικαιώματος φορητότητας δεδομένων (άρ.20§1)	
1	Η επεξεργασία βασίζεται σε συγκατάθεση (Συναίνεση ή ρητή - αρ.6§1α,9§2α) ή σε σύμβαση (άρ.6§1β)
2	Η επεξεργασία διενεργείται με αυτοματοποιημένα μέσα.

Περιπτώσεις εξαίρεσης φορητότητας δεδομένων (άρ.20§3,4)	
1	Το δικαίωμα στη φορητότητα δεν ισχύει στην επεξεργασία που είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας
2	Όταν επηρεάζει δυσμενώς τα δικαιώματα και ελευθερίες άλλων

ΠΑ-§12 Δικαίωμα εναντίωσης

Επιλέξτε ποιες περιπτώσεις λαμβάνετε υπόψη για το δικαίωμα εναντίωσης.

Περιπτώσεις που λαμβάνετε υπόψη το δικαίωμα εναντίωσης (άρ. 21,22,23)					
Το υποκείμενο των δεδομένων μπορεί να ασκήσει το δικαίωμα εναντίωσης σε:		ΝΑΙ	ΟΧΙ	ΑΓΝΩΣΤΟ	ΔΕΝ ΑΦΟΡΑ
1	επεξεργασία με βάση νόμιμα συμφέροντα ή εκπλήρωση καθήκοντος προς το δημόσιο συμφέρον / άσκηση δημόσιας εξουσίας (συμπεριλαμβανομένης της κατάρτισης προφίλ) ;				
2	επεξεργασία για σκοπούς απευθείας εμπορικής προώθησης (συμπεριλαμβανομένης της κατάρτισης προφίλ) ;				
3	επεξεργασία για επιστημονική / ιστορική έρευνα και στατιστικές εκτός εάν η επεξεργασία είναι απαραίτητη για λόγους δημόσιου συμφέροντος ;				
Ενημέρωση για το δικαίωμα της εναντίωσης (άρ. 21)					
4	Ενημερώνετε το ΥΔ, χωριστά από κάθε άλλη πληροφορία, για το δικαίωμα εναντίωσης του στις ανωτέρω περιπτώσεις;				

ΠΑ-§13 Δικαίωμα σχετικά με την αυτοματοποιημένη λήψη αποφάσεων και κατάρτιση προφίλ

Ενημερωθείτε για το δικαίωμα του ΥΔ σχετικά με την αυτοματοποιημένη λήψη αποφάσεων και κατάρτιση προφίλ.

Δικαίωμα σχετικά με την αυτοματοποιημένη λήψη αποφάσεων και κατάρτιση προφίλ (άρ.22)
Το ΥΔ έχει δικαίωμα να μην υπόκεινται σε αποφάσεις που λαμβάνονται αποκλειστικά από αυτοματοποιημένη επεξεργασία η οποία παράγει έννομα αποτελέσματα ή το επηρεάζει σημαντικά. Η αυτοματοποιημένη επεξεργασία δεν προϋποθέτει τη δημιουργία προφίλ, μπορεί όμως να την περιλαμβάνει.
Εξαιρέσεις στο δικαίωμα για την αυτοματοποιημένη λήψη αποφάσεων
Εξαιρέσεις στο παραπάνω δικαίωμα, όταν η απόφαση: α) είναι αναγκαία για τη σύναψη ή την εκτέλεση σύμβασης μεταξύ του ΥΔ και του ΥΠΕ, β) επιτρέπεται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους στο οποίο υπόκειται ο ΥΠΕ και το οποίο προβλέπει επίσης κατάλληλα μέτρα για την προστασία των δικαιωμάτων, των ελευθεριών και των έννομων συμφερόντων του υποκειμένου των δεδομένων γ) έχει προκύψει από επεξεργασία ΔΠΧΕΚ και δε βασίζεται στη ρητή συγκατάθεση του ΥΔ δ) έχει προκύψει από επεξεργασία ΔΠΧΕΚ και δε βασίζεται στους λόγους δημόσιου συμφέροντος (άρ.22§4)

ΠΑ-§16.1 Αρχείο δραστηριοτήτων του ΥΠΕ

Επιλέξτε ποιες πληροφορίες τηρείτε στο αρχείο δραστηριοτήτων ως Υπεύθυνος Επεξεργασίας (ΥΠΕ).

Περιλαμβανόμενες πληροφορίες για το αρχείο δραστηριοτήτων Υπεύθυνου Επεξεργασίας (ΥΠΕ) (άρ.30§1)					
	Πληροφορία	ΝΑΙ	ΟΧΙ	ΑΓΝΩΣΤΟ	ΔΕΝ ΑΦΟΡΑ
1	Το όνομα και τα στοιχεία επικοινωνίας του υπευθύνου επεξεργασίας και, κατά περίπτωση, του από κοινού υπευθύνου επεξεργασίας, του εκπροσώπου του υπευθύνου επεξεργασίας και του υπευθύνου προστασίας δεδομένων				
2	Τους σκοπούς της επεξεργασίας				
3	Περιγραφή των κατηγοριών υποκειμένων των δεδομένων και των κατηγοριών δεδομένων προσωπικού χαρακτήρα				
4	Τις κατηγορίες αποδεκτών στους οποίους πρόκειται να γνωστοποιηθούν ή γνωστοποιήθηκαν τα δεδομένα προσωπικού χαρακτήρα, περιλαμβανομένων των αποδεκτών σε τρίτες χώρες ή διεθνείς οργανισμούς				
5	Σε περιπτώσεις διαβίβασης ΔΠΧ σε τρίτη χώρα, αναφέρονται όλες οι πιθανές περιπτώσεις διαβίβασης και οι τεκμηριώσεις των κατάλληλων εγγυήσεων				
6	Όπου είναι δυνατό, τις προβλεπόμενες προθεσμίες διαγραφής των διάφορων κατηγοριών δεδομένων				
7	Γενική περιγραφή των τεχνικών και οργανωτικών μέτρων προστασίας ΔΠΧ του οργανισμού				

ΠΑ-§18.1 Αρχείο δραστηριοτήτων του ΕΚΕ

Επιλέξτε ποιες πληροφορίες τηρείτε στο αρχείο δραστηριοτήτων ως Εκτελών την Επεξεργασία (ΕΚΕ).

Περιλαμβανόμενες πληροφορίες για το αρχείο δραστηριοτήτων εκτελούντα την επεξεργασία (άρ.30§2)					
	Πληροφορία	ΝΑΙ	ΟΧΙ	ΑΓΝΩΣΤΟ	ΔΕΝ ΑΦΟΡΑ
1	Το όνομα και τα στοιχεία επικοινωνίας του εκτελούντος ή των εκτελούντων την επεξεργασία και των υπευθύνων επεξεργασίας εκ μέρους των οποίων ενεργεί ο εκτελών και, κατά περίπτωση, του εκπροσώπου του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, καθώς και του υπευθύνου προστασίας δεδομένων				
2	Τις κατηγορίες επεξεργασιών που διεξάγονται εκ μέρους κάθε υπευθύνου επεξεργασίας				
3	Σε περιπτώσεις διαβίβασης ΔΠΧ σε τρίτη χώρα, αναφέρονται όλες οι πιθανές περιπτώσεις διαβίβασης και οι τεκμηριώσεις των κατάλληλων εγγυήσεων				
4	Γενική περιγραφή των τεχνικών και οργανωτικών μέτρων προστασίας ΔΠΧ του οργανισμού				

Θέματα ασφαλείας

ΠΑ-§19 Τεχνικά και οργανωτικά μέτρα ασφάλειας δεδομένων

Ως υπεύθυνος επεξεργασίας ή εκτελών την επεξεργασία, επιλέξτε ποια τεχνικά και οργανωτικά μέτρα εφαρμόζετε προκειμένου να διασφαλίζετε το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων. Λάβετε υπόψη τα παρακάτω:

- τις τελευταίες εξελίξεις,
- το κόστος εφαρμογής και τη φύση,
- το πεδίο εφαρμογής,
- το πλαίσιο και τους σκοπούς της επεξεργασίας,
- τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων.

Τεχνικά και οργανωτικά μέτρα ασφάλειας ΔΠΧ (άρ.32§1)							
Υπηρεσία:							
	Είδος τεχνικού και οργανωτικού μέτρου	ΝΑΙ	ΟΧΙ	ΑΓΝΩΣΤΟ	ΔΕΝ ΑΦΟΡΑ	Αν ναι Προσδιορίστε σχετικά	
Οργανωτικά και τεχνικά μέτρα (εκτός από πληροφορική)							
1	Διαδικασία (ες) με διαβαθμισμένα επίπεδα πρόσβασης σε ΔΠΧ						
2	Διαδικασία για την τακτική δοκιμή, εκτίμηση και αξιολόγηση της αποτελεσματικότητας των τεχνικών και των οργανωτικών μέτρων για τη διασφάλιση της ασφάλειας της επεξεργασίας						
3	Ελεγχόμενη προσβασιμότητα (Φυσικά) (Χώροι ελεγχόμενης πρόσβασης –ντουλάπες, δωμάτια κτλ.) Αν ναι, προσδιορίστε :						
4	Άλλο, Προσδιορίστε :						
5	Άλλο, Προσδιορίστε :						
6	Άλλο, Προσδιορίστε :						
7	Άλλο, Προσδιορίστε :						
8	Άλλο, Προσδιορίστε :						
Οργανωτικά και τεχνικά μέτρα (Πληροφορικής)							
9	Ψευδωνυμοποίηση ΔΠΧ (Pseudonymization)						
10	Κρυπτογράφηση ΔΠΧ (Cryptography)						Φυσικών μέσων (Δίσκου) Φυσικών μέσων (αφαιρούμενων δίσκων)

							Εικονικών μέσων (Δίσκων δικτύου/ Cloud)
							Ηλεκτρονικής επικοινωνίας
							Άλλο:……
11	Ανωνυμοποίηση ΔΠΧ (Anonymization)						
12	Αξιοπιστία συστημάτων και υπηρεσιών επεξεργασίας ΔΠΧ σε συνεχή βάση (Confidentiality)						
13	Ακεραιότητα ΔΠΧ (Integrity)						
14	Διαθεσιμότητα ΔΠΧ (Availability)						
15	Διασφάλιση απορρήτου ΔΠΧ (Privacy)						
16	Δυνατότητα αποκατάστασης της διαθεσιμότητας και της πρόσβασης σε ΔΠΧ σε εύθετο χρόνο σε περίπτωση φυσικού ή τεχνικού συμβάντος						
17	Εφαρμοσμένη πολιτική ασφάλειας						
18	Ελεγχόμενη προσβασιμότητα (Ηλεκτρονικά) Αν ναι, προσδιορίστε : ……..						
19	Χρήση εγκεκριμένου μηχανισμού πιστοποίησης (άρ.42) Αν ναι, προσδιορίστε : ……..						
20	Λογισμικό προστασίας από ιούς						
21	Λογισμικό προστασίας από κακόβουλο λογισμικό						
22	Λογισμικό προστασίας από ιούς στο ηλεκτρονικού ταχυδρομείο.						
23	Προστασία του εταιρικού δικτύου από τείχος προστασίας (firewall)						
24	Σύστημα εντοπισμού διαρροών δεδομένων για την προστασία ευαίσθητων/προσωπικών δεδομένων						

25	Σύστημα Παρακολούθησης, ανίχνευσης, ανάλυσης και αναφοράς περιστατικών ασφάλειας (IDS/IPS)					
26	Τακτική λήψη αντιγράφων ασφαλείας (backup) των ΔΠΧ					
27	Τακτική δοκιμή επανάκτησης δεδομένων (restore) των ΔΠΧ					
28	Προστασία εταιρικού δικτύου και wifi με κωδικό πρόσβασης					
29	Απομακρυσμένη πρόσβαση στο εταιρικό δίκτυο αποκλειστικά μέσω εικονικού ιδιωτικού δικτύου (VPN)					
30	Έλεγχος πρόσβασης σε ΔΠΧ μόνο σε εξουσιοδοτημένα άτομα					
31	Ελεγχόμενη πρόσβαση χρηστών σε πόρους (υπολογιστές)					
32	Ελεγχόμενη πρόσβαση χρηστών σε πόρους (Δικτυακούς πόρους)					
33	Ελεγχόμενη πρόσβαση χρηστών σε πόρους (Εφαρμογή ΔΠΧ)					
34	Ελεγχόμενη φυσική πρόσβαση σε δωμάτια εξυπηρετητών					
35	Ελεγχόμενη φυσική πρόσβαση σε κατανεμητές					
36	Άλλο, Προσδιορίστε : ……..					
37	Άλλο, Προσδιορίστε : ……..					
38	Άλλο, Προσδιορίστε : ……..					
39	Άλλο, Προσδιορίστε : ……..					

ΠΑ-§20.1 Τεχνικά και οργανωτικά μέτρα στο σχεδιασμό εξ ορισμού

Σε περιπτώσεις που σχεδιάζετε νέες εφαρμογές που θα περιλαμβάνουν επεξεργασία ΔΠΧ, επιλέξτε ποια από τα παρακάτω μέτρα λαμβάνετε.

Τεχνικά και οργανωτικά μέτρα για την προστασία δεδομένων από το σχεδιασμό εξ ορισμού (άρ.25)							
	Είδος τεχνικού και οργανωτικού μέτρου	ΝΑΙ	ΟΧΙ	ΑΓΝΩΣΤΟ	ΔΕΝ ΑΦΟΡΑ	Αν ναι Προσδιορίστε σχετικά	
1	Τήρηση των δέκα αρχών (νομιμότητα, αντικειμενικότητα, διαφάνεια, περιορισμός σκοπού, ελαχιστοποίηση των δεδομένων, ακρίβεια, περιορισμός της περιόδου αποθήκευσης, ακεραιότητα, εμπιστευτικότητα και λογοδοσία)						
2	Ψευδωνυμοποίηση ΔΠΧ (Pseudonymization)						
3	Κρυπτογράφηση ΔΠΧ (Cryptography)						Φυσικών μέσων (Δίσκου)
							Φυσικών μέσων (αφαιρούμενων δίσκων)
							Εικονικών μέσων (Δίσκων δικτύου/ Cloud)
							Ηλεκτρονικής επικοινωνίας
							Άλλο:……
4	Ανωνυμοποίηση ΔΠΧ (Anonymization)						
5	Αξιοπιστία συστημάτων και υπηρεσιών επεξεργασίας ΔΠΧ σε συνεχή βάση (Confidentiality)						
6	Ακεραιότητα ΔΠΧ (Integrity)						
7	Διαθεσιμότητα ΔΠΧ (Availability)						
8	Διασφάλιση απορρήτου ΔΠΧ (Privacy)						
9	Δυνατότητα αποκατάστασης της διαθεσιμότητας και της πρόσβασης σε ΔΠΧ σε εύθετο χρόνο σε περίπτωση φυσικού ή τεχνικού συμβάντος						
10	Ελεγχόμενη προσβασιμότητα (Φυσικά) Αν ναι, προσδιορίστε : ……..						

11	Ελεγχόμενη προσβασιμότητα (Ηλεκτρονικά) Αν ναι, προσδιορίστε :					
12	Χρήση εγκεκριμένου μηχανισμού πιστοποίησης (άρ.42) Αν ναι, προσδιορίστε :					
13	Τήρηση κωδίκων δεοντολογίας Αν ναι, προσδιορίστε :					
14	Σύστημα Opt in (το ΥΔ αιτείται να επιλεγεί π.χ. τηλεφωνικός κατάλογος) Αν ναι, προσδιορίστε περιπτώσεις :					
15	Σύστημα Opt out (το ΥΔ αιτείται να εξαιρεθεί π.χ. τηλεφωνικός κατάλογος) Αν ναι, προσδιορίστε περιπτώσεις :					
16	Άλλο, Προσδιορίστε :					

ΠΑ-§21 Μέτρα περιορισμού κινδύνων από την επεξεργασία ΔΠΧ

Επιλέξτε τους κινδύνους και τα μέτρα προστασίας που λαμβάνετε, για αυτούς, από την επεξεργασία ΔΠΧ

Τρόποι λήψης μέτρων για τους κίνδυνους που απορρέουν από την επεξεργασία ΔΠΧ (άρ.32§3)						
	Κίνδυνος	ΝΑΙ	ΟΧΙ	ΑΓΝΩΣΤΟ	ΔΕΝ ΑΦΟΡΑ	Αν ναι Προσδιορίστε σχετικό μέτρο αποφυγής κινδύνου
1	Κατά την ίδια την επεξεργασία					
2	Τυχαία ή παράνομη καταστροφή					
3	Απώλεια					
4	Αλλοίωση					
5	Άνευ άδειας κοινολόγηση					
6	Προσπέλαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία.					
7	Άλλο, Προσδιορίστε :					

ΠΑ-§24.1 Γνωστοποίηση παραβίασης στην Αρχή

Επιλέξτε ποια στοιχεία περιλαμβάνετε στη διαδικασία γνωστοποίησης σε περίπτωση παραβίασης δεδομένων στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ).

Περιλαμβανόμενα στοιχεία της γνωστοποίησης στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) (άρ.33§3)					
	Πληροφορία	ΝΑΙ	ΟΧΙ	ΑΓΝΩΣΤΟ	ΔΕΝ ΑΦΟΡΑ
1	Γνωστοποίηση παραβίασης εντός 72 ωρών ή αιτιολόγηση πέρα του χρονικού ορίου αυτού, από τη στιγμή που αποκτά γνώση του γεγονότος της παραβίασης				
2	Τη φύση - είδος της παραβίασης ΔΠΧ				
3	Τις κατηγορίες / αριθμό των επηρεαζόμενων ΥΔ (κατά προσέγγιση)				
4	Τις κατηγορίες /αριθμό επηρεαζόμενων αρχείων ΔΠΧ (κατά προσέγγιση)				
5	Τα στοιχεία επικοινωνίας του ΥΠΕ ή άλλου σημείου επικοινωνίας από το οποίο μπορούν να ληφθούν περισσότερες πληροφορίες				
6	Συνέπειες της παραβίασης των ΔΠΧ				
7	Μέτρα, ληφθέντα/προτεινόμενα, για την αντιμετώπιση της παραβίασης των ΔΠΧ				
8	Μέτρα, ληφθέντα/προτεινόμενα, για την άμβλυνση ενδεχόμενων δυσμενών συνεπειών της παραβίασης ΔΠΧ				

ΠΑ-§25.1 Γνωστοποίηση παραβίασης στο ΥΔ

Επιλέξτε ποια στοιχεία περιλαμβάνετε στη διαδικασία γνωστοποίησης σε περίπτωση παραβίασης δεδομένων στο Υποκείμενο Δεδομένων (ΥΔ).

Περιλαμβανόμενα στοιχεία στη γνωστοποίηση στο ΥΔ (άρ.34§2)					
	Ενέργειες – Πληροφορίες	ΝΑΙ	ΟΧΙ	ΑΓΝΩΣΤΟ	ΔΕΝ ΑΦΟΡΑ
1	Τη φύση - είδος της παραβίασης ΔΠΧ				
2	Τα στοιχεία επικοινωνίας του ΥΠΕ ή άλλου σημείου επικοινωνίας από το οποίο μπορούν να ληφθούν περισσότερες πληροφορίες				
3	Συνέπειες της παραβίασης των ΔΠΧ				
4	Μέτρα, ληφθέντα/προτεινόμενα, για την αντιμετώπιση της παραβίασης των ΔΠΧ				
5	Μέτρα, ληφθέντα/προτεινόμενα, για την άμβλυνση ενδεχόμενων δυσμενών συνεπειών της παραβίασης ΔΠΧ				

Εξαιρέσεις υποχρέωσης γνωστοποίησης στο ΥΔ (άρ.34§3)	
	Εξαιρέσεις
1	Όταν έχουν ληφθεί μέτρα ώστε τα ΔΠΧ να μην είναι κατανοητά (π.χ. Κρυπτογράφηση)
2	Όταν ο ΥΠΕ έλαβε μέτρα που δε θέτουν σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες των ΥΔ
3	Όταν προϋποθέτει δυσανάλογες προσπάθειες. Στην περίπτωση αυτή, γίνεται αντ' αυτής δημόσια ανακοίνωση ή υπάρχει παρόμοιο μέτρο με το οποίο τα υποκείμενα των δεδομένων ενημερώνονται με εξίσου αποτελεσματικό τρόπο.

ΠΑ-§26.1 Απαίτηση εκτίμησης αντικτύπου προστασίας δεδομένων – Data privacy impact assessment (ΕΑΠΔ/DPIA)

Απαντήστε αν ο οργανισμός σας ανήκει σε κάποιες από τις περιπτώσεις που αναφέρονται παρακάτω.

Περιπτώσεις απαίτησης μελέτης εκτίμησης αντικτύπου προστασίας δεδομένων – Data privacy impact assessment (ΕΑΠΔ/DPIA) (άρ.35§3)					
Περίπτωση		ΝΑΙ	ΟΧΙ	ΑΓΝΩΣΤΟ	ΔΕΝ ΑΦΟΡΑ
1	Το είδος επεξεργασίας ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων;				
2	Εκτελείτε συστηματική και εκτενούς αξιολόγηση προσωπικών πτυχών σχετικά με φυσικά πρόσωπα, η οποία βασίζεται σε αυτοματοποιημένη επεξεργασία, περιλαμβανομένης της κατάρτισης προφίλ, και στην οποία βασίζονται αποφάσεις που παράγουν έννομα αποτελέσματα σχετικά με το φυσικό πρόσωπο ή ομοίως επηρεάζουν σημαντικά το φυσικό πρόσωπο;				
3	Εκτελείτε μεγάλης κλίμακας επεξεργασία σε ΔΠΧΕΚ ή ΔΠΧ που αφορούν ποινικές καταδίκες και αδικήματα;				
4	Πραγματοποιείτε συστηματική παρακολούθηση δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα;				

ΠΑ-§26.2 Στοιχεία μελέτης αντικτύπου

Επιλέξτε τι περιλαμβάνει η μελέτη εκτίμησης αντικτύπου προστασίας δεδομένων (ΕΑΠΔ/DPIA).

Περιλαμβανόμενα στοιχεία στη Μελέτη Εκτίμησης Αντικτύπου προστασίας δεδομένων (άρ.35§7)					
Περιγραφή στοιχείου		ΝΑΙ	ΟΧΙ	ΑΓΝΩΣΤΟ	ΔΕΝ ΑΦΟΡΑ
1	Συστηματική περιγραφή των προβλεπόμενων πράξεων επεξεργασίας και των σκοπών της επεξεργασίας περιλαμβανομένου κατά περίπτωση, του έννομου συμφέροντος που επιδιώκει ο υπεύθυνος επεξεργασίας				
2	Εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας σε συνάρτηση με τους σκοπούς,				
3	Εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων κατά την επεξεργασία				
4	Τα προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων, περιλαμβανομένων των εγγυήσεων, των μέτρων και μηχανισμών ασφάλειας, ώστε να διασφαλίζεται η προστασία των δεδομένων προσωπικού χαρακτήρα και να αποδεικνύεται η συμμόρφωση προς τον παρόντα κανονισμό, λαμβάνοντας υπόψη τα δικαιώματα και τα έννομα συμφέροντα των υποκειμένων των δεδομένων και άλλων ενδιαφερόμενων προσώπων.				

ΠΑ-§28 Πιστοποιήσεις

Συμπληρώστε ποιές πιστοποιήσεις για την προστασία ΔΠΧ έχετε στον οργανισμό σας.

Πιστοποιήσεις για την προστασία ΔΠΧ του οργανισμού				
	Όνομα Πιστοποίησης	Ημερομηνία απόκτησης	Φορέας	Ισχύ έως
1				
2				
3				
4				
5				

Π2 Εγχειρίδιο ενεργειών

για τη συμμόρφωση με τον Ευρωπαϊκό Γενικό Κανονισμό Προστασίας Δεδομένων - General Data Protection Regulation (ΓΚΠΔ/GDPR) 2016/679

Οργανισμός - Επιχείρηση

Τμήμα

Έκδοση: 1.0

Οδηγίες χρήσης του εγχειριδίου

Εισαγωγή

Το εγχειρίδιο ενεργειών έχει σκοπό την ανάλυση της απόκλισης (gap analysis) μεταξύ της παρούσας και επιθυμητής κατάστασης. Αυτό θα γίνει με την επεξεργασία των απαντημένων ερωτηματολογίων του εγχειριδίου αποτύπωσης (παρούσα κατάσταση) και την ανάδειξη των προτεινόμενων ενεργειών ώστε να φτάσει στην μέγιστη δυνατή συμμόρφωση (επιθυμητή κατάσταση) με τον Ευρωπαϊκό Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ) - General Data Protection Regulation (GDPR). Το κάθε ερωτηματολόγιο θα πρέπει να εξετασθεί ξεχωριστά. Το σύνολο των ενεργειών που θα προκύψει από κάθε ερωτηματολόγιο συνθέτει τις προτεινόμενες ενέργειες για όλο τον οργανισμό. Η καταγραφή, ομαδοποίηση και ιεράρχηση τους θα οδηγήσουν στο τελικό πλάνο συμμόρφωσης του οργανισμού στον ΓΚΠΔ.

Παρουσίαση

Το εγχειρίδιο ενεργειών αποτελείται από τέσσερα μέρη. Τις παρούσες οδηγίες, το «Υπόδειγμα προτεινόμενων ενεργειών», τον «Πίνακα ενεργειών» και το «Παράρτημα (ΠΕ)».

Το υπόδειγμα προτεινόμενων ενεργειών θα χρησιμοποιηθεί για να καταγραφούν οι προτεινόμενες ενέργειες που θα προκύψουν από την επεξεργασία των εγχειριδίων αποτύπωσης με τη βοήθεια του εγχειριδίου ενεργειών.

Ο πίνακας ενεργειών στηρίζεται στις 28 ερωτήσεις του ερωτηματολογίου, του εγχειριδίου αποτύπωσης και περιλαμβάνει ενδεικνυόμενες ενέργειες ανά απάντηση. Για κάθε ερώτημα υπάρχει:

α) η «**§ απάντησης παραρτήματος**» που δείχνει ποια είναι η σχετιζόμενη παράγραφος στο παράρτημα του εγχειριδίου αποτύπωσης. Χρησιμοποιείται για να διευκολύνει τον αναγνώστη στο να ανατρέχει στις απαντήσεις του παραρτήματος,

β) οι «**Προτεινόμενες ενέργειες**» που περιλαμβάνει τις προτεινόμενες ενέργειες ανά απάντηση ερώτησης οι οποίες κατηγοριοποιούνται σε :

- «**αν Ναι**» που έχει τις προτεινόμενες ενέργειες για τις θετικές απαντήσεις
- «**αν Όχι**» που έχει τις προτεινόμενες ενέργειες για τις αρνητικές απαντήσεις
- «**Διευκρίνηση**» που έχει διευκρινήσεις για κάθε άλλη απάντηση («άγνωστο», «δεν αφορά», ελεύθερο κείμενο κτλ.) ή συμπληρωματικές οδηγίες για την κάθε περίπτωση ή παραπομπή για περισσότερες πληροφορίες,

γ) οι «**Βοηθητικές πληροφορίες**» που διευκολύνουν στην οργάνωση των ενεργειών και κατηγοριοποιούνται σε στήλες με τίτλο:

- «**Υποχρέωση διατήρησης στοιχείων**» που καταγράφει τις περιπτώσεις υποχρέωσης του οργανισμού να διατηρήσει στοιχεία ως απαίτηση του κανονισμού
- «**Έγγραφο ως τεκμηρίωση**» που καταγράφει τις περιπτώσεις χρήσης εγγράφου ως απόδειξη τεκμηρίωσης σε απαιτήσεις του οργανισμού
- «**Πολιτική**» που καταγράφει τις περιπτώσεις οι οποίες άπτονται σε αλλαγές πολιτικές του οργανισμού

- «**Διαδικασία**» που καταγράφει τις περιπτώσεις οι οποίες άπτονται σε αλλαγές διαδικασιών του οργανισμού
- «**Τεχνικό**» που καταγράφει τις περιπτώσεις που χρίζουν αλλαγές σε τεχνικά θέματα του οργανισμού

Οι βοηθητικές πληροφορίες είναι ενδεικτικές και κάθε οργανισμός βάσει των δικών του ιδιαιτεροτήτων και αναγκών επιβεβαιώνει και αναθεωρεί τις πληροφορίες αυτές. Το παράρτημα περιέχει συμπληρωματικές πληροφορίες προτεινόμενων ενεργειών, άρθρα, παραπομπές, διευκρινίσεις κτλ.

Το παράρτημα (ΠΕ) περιέχει πληροφορίες – διευκρινήσεις για συγκεκριμένα ερωτήματα καθώς και οδηγίες – παραπομπές σε επίσημους δικτυακούς τόπους (Ευρωπαϊκές αρχές ΠΔ, ΟΕ29 κτλ.)

Βήματα χρήσης

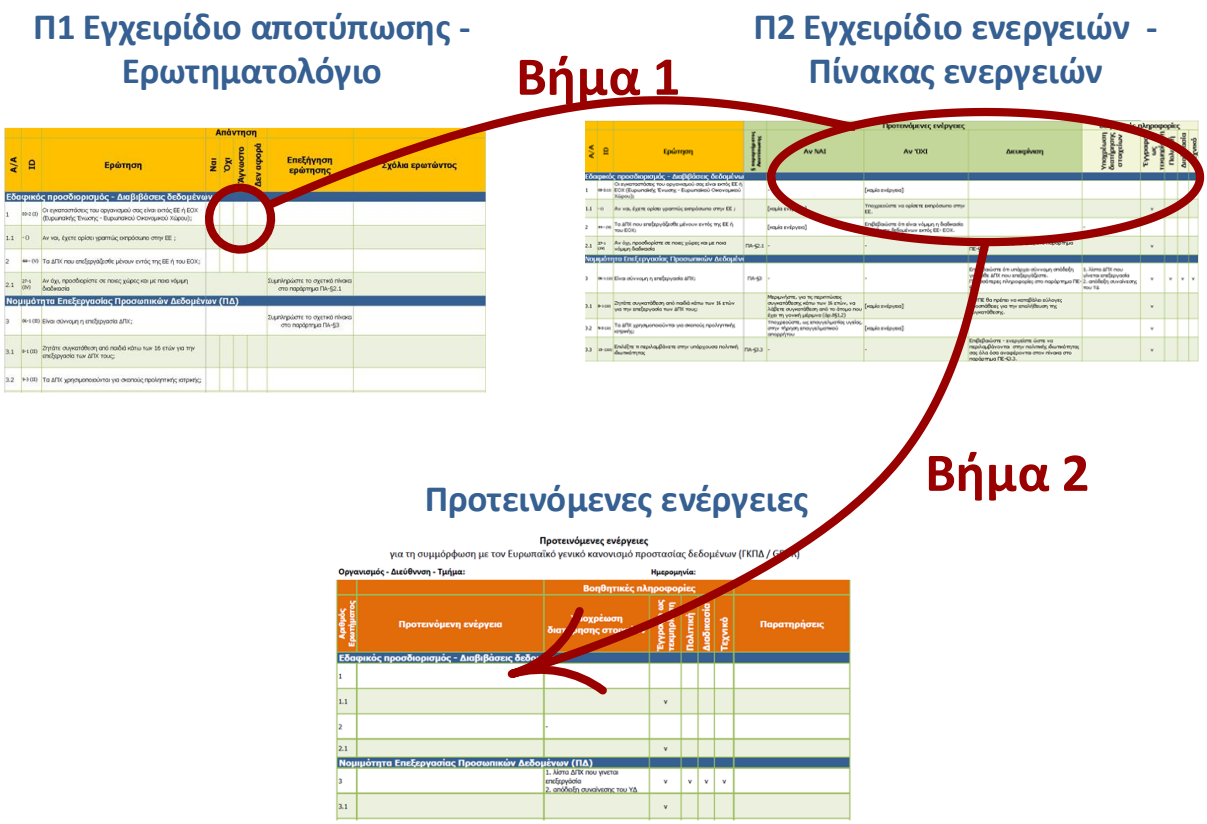
Χρησιμοποιήστε το «υπόδειγμα προτεινόμενες ενέργειες» που βρίσκεται στο παρόν εγχειρίδιο για να καταγράψετε τις προτεινόμενες ενέργειες για το συγκεκριμένο ερωτηματολόγιο, ακολουθώντας τα παρακάτω βήματα.

Βήμα 1: Για κάθε απάντηση του ερωτηματολογίου (εγχειρίδιο αποτύπωσης) ανατρέξτε στην αντίστοιχη γραμμή του πίνακα ενεργειών (εγχειρίδιο ενεργειών).

Βήμα 2: Καταγράψτε ανάλογα την απάντηση, τις προτεινόμενες ενέργειες, τυχόν διευκρινίσεις και το σύνολο των βοηθητικών στηλών.

Σε περιπτώσεις που έχει επιλεγεί το «Άγνωστο», θα χρειαστεί να διερευνηθεί η απάντηση από ειδικούς (νομικό, πληροφορικό ή άλλο).

Σε περιπτώσεις που έχει επιλεγεί το «Δεν αφορά», επιβεβαιώστε ότι όντως η ερώτηση δεν αφορά τη συγκεκριμένη διεύθυνση – τμήμα.



Διάγραμμα 1. Βήματα χρήσης του εγχειριδίου ενεργειών

Οι προτεινόμενες ενέργειες έχουν τις εξής μορφές:

- Ενημέρωσης π.χ. για απαλλαγή, υποχρέωση
- Επιβεβαίωσης - ελέγχου σε τεχνικά και οργανωτικά θέματα
- Ενεργειών σε τεχνικά και οργανωτικά θέματα

Ολοκληρώνοντας την καταγραφή έχετε συλλέξει το σύνολο των προτεινόμενων ενεργειών για τη διεύθυνση - τμήμα του οργανισμού.

Προτεινόμενες ενέργειες

για τη συμμόρφωση με τον Ευρωπαϊκό Κανονισμό Προστασίας Προσωπικών δεδομένων (ΓΚΠΔ/GDPR) 2016/679

Οργανισμός - Διεύθυνση - Τμήμα: **Ημερομηνία:**

		Βοηθητικές πληροφορίες					
Αριθμός Ερωτήματος	Προτεινόμενη ενέργεια	Υποχρέωση διατήρησης στοιχείων	Έγγραφο ως τεκμηρίωση	Πολιτική	Διαδικασία	Τεχνικό	Παρατηρήσεις
Εδαφικός προσδιορισμός - Διαβιβάσεις δεδομένων							
1							
1.1			v				
2							
2.1			v				
Νομιμότητα Επεξεργασίας Προσωπικών Δεδομένων (ΠΔ)							
3		1.Λίστα ΔΠΧ που γίνεται επεξεργασία 2.Απόδειξη συναίνεσης του ΥΔ	v	v	v	v	
3.1			v				
3.2			v				
4				v	v		
4.1							
5			v		v		
5.1							
Δικαιώματα Υποκείμενων Δεδομένων (ΥΔ)							
6		Τρόπος, τόπος, χρόνος ενημέρωσης ΥΔ	v	v	v	v	
6.1							
7		1.Μορφή αντιγράφου ΔΠΧ ΥΔ 2.Εγγυήσεις για διαβιβάσεις εκτός ΕΕ - ΕΟΧ (άρ.46)	v	v	v	v	
7.1							
8			v	v	v	v	
8.1							
9			v	v	v	v	
9.1							
10			v	v	v	v	
10.1							
11			v	v	v	v	
12							

Προτεινόμενες ενέργειες

για τη συμμόρφωση με τον Ευρωπαϊκό Κανονισμό Προστασίας Προσωπικών δεδομένων (ΓΚΠΔ/GDPR) 2016/679

Οργανισμός - Διεύθυνση - Τμήμα: **Ημερομηνία:**

		Βοηθητικές πληροφορίες					
Αριθμός Ερωτήματος	Προτεινόμενη ενέργεια	Υποχρέωση διατήρησης στοιχείων	Έγγραφο ως τεκμηρίωση	Πολιτική	Διαδικασία	Τεχνικό	Παρατηρήσεις
12.1							
13			v	v	v	v	
Υπεύθυνος Επεξεργασίας, Εκτελών, Υπεύθυνος Προστασίας							
14			v	v	v		
15			v				
16		Αρχείο δραστηριοτήτων επεξεργασίας	v	v	v	v	
16.1							
17			v				
18		Αρχείο δραστηριοτήτων επεξεργασίας	v	v	v	v	
18.1							
Θέματα ασφαλείας							
19		Έκθεση αναφοράς τεχνικών μέτρων	v	v	v	v	
20		Έκθεση αναφοράς τεχνικών μέτρων	v	v	v	v	
20.1							
21		Έκθεση αναφοράς λήψης μέτρων για κινδύνους	v	v	v	v	
22			v	v	v	v	
22.1							
23			v	v	v	v	
24			v	v	v	v	
24.1							
25			v	v	v	v	
25.1							
26			v	v	v		
26.1							
26.2							
27			v	v	v		
28			v	v	v	v	
28.1							

Πίνακας ενεργειών εγχειριδίου ενεργειών

για τη συμμόρφωση με τον Ευρωπαϊκό Γενικό Κανονισμό Προστασίας Δεδομένων - General Data Protection Regulation (ΓΚΠΔ/GDPR) 2016/679

Π1.1 Εγχειρίδιο αποτύπωσης - Ερωτηματολόγιο

για τη συμμόρφωση με τον Ευρωπαϊκό Κανονισμό Προστασίας Προσωπικών δεδομένων (ΓΚΠΔ / GDPR) 2016/679

				Προτεινόμενες ενέργειες			Βοηθητικές πληροφορίες				
Α/Α	**ID**	**Ερώτηση**	**§ παραρτήματος Αποτύπωσης**	**Αν ΝΑΙ**	**Αν ΟΧΙ**	**Διευκρίνιση**	**Υποχρέωση διατήρησης στοιχείων**	**Έγγραφο ως τεκμηρίωση**	**Πολιτική**	**Διαδικασία**	**Τεχνικό**
Εδαφικός προσδιορισμός - Διαβιβάσεις δεδομένων											
1	03-2 (I)	Οι εγκαταστάσεις του οργανισμού σας είναι εκτός ΕΕ ή ΕΟΧ (Ευρωπαϊκής Ένωσης - Ευρωπαϊκού Οικονομικού Χώρου);		-	[καμία ενέργεια]						
1.1	- ()	Αν ναι, έχετε ορίσει γραπτώς εκπρόσωπο στην ΕΕ ;		[καμία ενέργεια]	Υποχρεούστε να ορίσετε εκπρόσωπο στην ΕΕ.			v			
2	44-- (V)	Τα ΔΠΧ που επεξεργάζεστε μένουν εντός της ΕΕ ή του ΕΟΧ;		[καμία ενέργεια]	Επιβεβαιώστε ότι είναι νόμιμη η διαδικασία μετάβασης δεδομένων εκτός ΕΕ- ΕΟΧ.						
2.1	27-1 (IV)	Αν όχι, προσδιορίστε σε ποιες χώρες και με ποια νόμιμη διαδικασία.	ΠΑ-§2.1	-	-	Περισσότερες πληροφορίες στο παράρτημα ΠΕ-§2.1.		v			
Νομιμότητα Επεξεργασίας Προσωπικών Δεδομένων (ΠΔ)											
3	06-1 (II)	Είναι σύννομη η επεξεργασία ΔΠΧ;	ΠΑ-§3	-	-	Επιβεβαιώστε ότι υπάρχει σύννομη σπόδειξη για κάθε ΔΠΧ που επεξεργάζεστε. Περισσότερες πληροφορίες στο παράρτημα ΠΕ-§3.	1. Λίστα ΔΙΧ που γίνεται επεξεργασία 2. Απόδειξη συναίνεσης του ΥΔ	v	v	v	v
3.1	8-1 (II)	Ζητάτε συγκατάθεση από παιδιά κάτω των 16 ετών για την επεξεργασία των ΔΠΧ τους;		Μεριμνήστε, για τις περιπτώσεις συγκατάθεσης κάτω των 16 ετών, να λάβετε συγκατάθεση από το άτομο που έχει τη γονική μέριμνα (άρ.8§1,2)	[καμία ενέργεια]	Ο ΥΠΕ θα πρέπει να καταβάλει εύλογες προσπάθειες για την επαλήθευση της συγκατάθεσης.		v	v	v	v
3.2	9-3 (II)	Τα ΔΠΧ χρησιμοποιούνται για σκοπούς προληπτικής ιατρικής;		Υποχρεούστε, ως επαγγελματίας υγείας, στην τήρηση επαγγελματικού απορρήτου	[καμία ενέργεια]			v	v	v	
4	06-4 (II)	Έχει η επεξεργασία άλλο σκοπό από αυτόν που αρχικά έχουν συλλεγεί τα δεδομένα;		Επιβεβαιώστε αν είναι νόμιμος - συμβατός ο άλλος σκοπός της επεξεργασίας και αναλόγως να γίνει ενημέρωση στο ΥΔ.	[καμία ενέργεια]				v	v	
4.1	- ()	Αν ναι, προσδιορίστε σχετικά.		-	-						
5	10-- (II)	Επεξεργάζεστε ΔΠΧ από ποινικές καταδίκες;		Επιβεβαιώστε ότι επεξεργάζεστε ΔΠΧ ΜΟΝΟ υπό τον έλεγχο επίσημης αρχής	[καμία ενέργεια]			v		v	
5.1	- ()	Αν ναι, εκτελείτε τις επεξεργασίες αυτές αποκλειστικά υπό τον έλεγχο επίσημης αρχής (δικαστήριο, εφετείο κτλ.);		-	Δεν επιτρέπεται να επεξεργάζεστε ΔΠΧ από ποινικές καταδίκες εκτός εάν εκτελείτε αποκλειστικά υπό τον έλεγχο επίσημης αρχής. Ενεργείστε σχετικά.						

				Προτεινόμενες ενέργειες			Βοηθητικές πληροφορίες				
Α/Α	**ID**	**Ερώτηση**	**§ παραρτήματος Αποτύπωσης**	**Αν ΝΑΙ**	**Αν ΌΧΙ**	**Διευκρίνιση**	**Υποχρέωση διατήρησης στοιχείων**	**Έγγραφο ως τεκμηρίωση**	**Πολιτική**	**Διαδικασία**	**Τεχνικό**
Δικαιώματα Υποκειμένων Δεδομένων (ΥΔ)											
6	12-- (III)	Υπάρχει το δικαίωμα ενημέρωσης του ΥΔ για τα προσωπικά του δεδομένα;		Επιβεβαιώστε ότι παρέχετε το δικαίωμα της ενημέρωσης στο ΥΔ.	Ορίστε διαδικασίες για το δικαίωμα ενημέρωσης του ΥΔ.	Περισσότερες πληροφορίες στο παράρτημα ΠΕ-§6.	Τρόπος, τόπος, χρόνος ενημέρωσης ΥΔ	v	v	v	v
6.1	- ()	Αν ναι, προσδιορίστε σχετικά.	ΠΑ-§6.1								
7	15-1 (III)	Υπάρχει δικαίωμα πρόσβασης του ΥΔ στα προσωπικά του δεδομένα;		Επιβεβαιώστε ότι παρέχετε το δικαίωμα της πρόσβασης στο ΥΔ σε όλα του τα δεδομένα.	Ορίστε διαδικασίες για το δικαίωμα πρόσβασης του ΥΔ.	Περισσότερες πληροφορίες στο παράρτημα ΠΕ-§7.	1.Μορφη αντιγράφου ΔΠΧ ΥΔ 2.Εγγυήσεις για διαβιβάσεις εκτός ΕΕ - ΕΟΧ (άρ.46)	v	v	v	v
7.1	- ()	Αν ναι, προσδιορίστε σχετικά.	ΠΑ-§7.1								
8	16-- (III)	Υπάρχει το δικαίωμα διόρθωσης δεδομένων του ΥΔ;		Επιβεβαιώστε ότι παρέχετε διόρθωση δεδομένων σε όλα τα δεδομένα του ΥΔ.	Ορίστε διαδικασίες για το δικαίωμα διόρθωσης δεδομένων του ΥΔ.			v	v	v	v
8.1	- ()	Αν ναι, προσδιορίστε σχετικά.	ΠΑ-§8.1	-	-						
9	17-1 (III)	Υπάρχει το δικαίωμα διαγραφής δεδομένων του ΥΔ;		Επιβεβαιώστε ότι ισχύουν οι περιπτώσεις άσκησης δικαιώματος διαγραφής.	Ελέγξτε αν υποχρεούστε να εφαρμόσετε το δικαίωμα διαγραφής του ΥΔ. Αν ναι ορίστε διαδικασίες σχετικά.	Περισσότερες πληροφορίες στο παράρτημα ΠΕ-§9.		v	v	v	v
9.1	- ()	Αν ναι επιλέξτε για ποιες περιπτώσεις μπορεί να ασκηθεί το δικαίωμα της διαγραφής.	ΠΑ-§9.1	-	-						
10	18-1 (III)	Υπάρχει το δικαίωμα περιορισμού της επεξεργασίας από το ΥΔ;		Επιβεβαιώστε ότι ισχύουν οι περιπτώσεις περιορισμού της επεξεργασίας, άρσης περιορισμού, ενημέρωσης του ΥΔ.	Ελέγξτε αν υποχρεούστε να εφαρμόσετε το δικαίωμα περιορισμού της επεξεργασίας ΔΠΧ του ΥΔ. Αν ναι ορίστε διαδικασίες σχετικά.	Περισσότερες πληροφορίες στο παράρτημα ΠΕ-§10.		v	v	v	v
10.1	- ()	Αν ναι, προσδιορίστε σχετικά.	ΠΑ-§10.1	-	-						
11	20-1 (III)	Υπάρχει το δικαίωμα φορητότητας των δεδομένων;	ΠΑ-§11	Επιβεβαιώστε ότι ισχύουν οι περιπτώσεις δικαιώματος φορητότητας και εξαιρέσεις αυτών.	Ελέγξτε αν υποχρεούστε να εφαρμόσετε το δικαίωμα φορητότητας δεδομένων του ΥΔ. Αν ναι ορίστε διαδικασίες σχετικά.	Περισσότερες πληροφορίες στο παράρτημα ΠΕ-§11.		v	v	v	v

				Προτεινόμενες ενέργειες			Βοηθητικές πληροφορίες				
Α/Α	**ID**	**Ερώτηση**	**§ παραρτήματος Αποτύπωσης**	**Αν ΝΑΙ**	**Αν ΌΧΙ**	**Διευκρίνιση**	**Υποχρέωση διατήρησης στοιχείων**	**Έγγραφο ως τεκμηρίωση**	**Πολιτική**	**Διαδικασία**	**Τεχνικό**
12	21-- (III)	Υπάρχει το δικαίωμα εναντίωσης σε επεξεργασία δεδομένων;		Επιβεβαιώστε ότι ισχύουν οι περιπτώσεις δικαιώματος εναντίωσης του ΥΔ.	Ελέγξτε αν υποχρεούστε να εφαρμόσετε το δικαίωμα εναντίωσης του ΥΔ και ορίστε διαδικασίες σχετικά.	Περισσότερες πληροφορίες στο παράρτημα ΠΕ-§12.					
12.1	- ()	Αν ναι, προσδιορίστε σχετικά.	ΠΑ-§12								
13	22-- (III)	Υπάρχει το δικαίωμα εναντίωσης στη λήψη αυτοματοποιημένων αποφάσεων;	ΠΑ-§13	Επιβεβαιώστε ότι ισχύουν οι περιπτώσεις δικαιώματος εναντίωσης στη λήψη αυτοματοποιημένων αποφάσεων και εξαιρέσεις αυτών	Ελέγξτε αν υποχρεούστε να εφαρμόσετε το δικαίωμα εναντίωσης στη λήψη αυτοματοποιημένων αποφάσεων του ΥΔ και ορίστε διαδικασίες σχετικά.	Περισσότερες πληροφορίες στο παράρτημα ΠΕ-§13.		v	v	v	v
Υπεύθυνος Επεξεργασίας, Εκτελών, Υπεύθυνος προστασίας											
14	26-1 (IV)	Οι σκοποί και τα μέσα επεξεργασίας καθορίζονται από ένα μοναδικό υπεύθυνο επεξεργασίας (ΥΠΕ);		Τεκμηριώστε ότι τα μέσα επεξεργασίας καθορίζονται από ένα μοναδικό υπεύθυνο επεξεργασίας (ΥΠΕ).	Ενεργείστε ώστε να είναι ξεκάθαρο εγγράφως, ποιες αρμοδιότητες - ευθύνες έχει ο καθένας ΥΠΕ.	Περισσότερες πληροφορίες στο παράρτημα ΠΕ-§14.		v	v	v	
15	30-5 (IV)	Απασχολείτε περισσότερα από 250 άτομα στον οργανισμό σας;		Υποχρεούστε της διατήρησης αρχείου δραστηριοτήτων επεξεργασίας ως ΥΠΕ ή ΕΚΕ.	Απαλλάσσεστε από την υποχρέωση διατήρησης αρχείου δραστηριοτήτων επεξεργασίας ως ΥΠΕ ή ΕΚΕ. Εξαιρέσεις αρ.30§5.			v			
16	30-1 (IV)	Ως υπεύθυνος επεξεργασίας (ΥΠΕ) τηρείτε αρχείο δραστηριοτήτων επεξεργασίας;		Επιβεβαιώστε ότι το αρχείο δραστηριοτήτων επεξεργασίας, ως ΥΠΕ, έχει όλες τις πληροφορίες που αναφέρονται στον πίνακα παραρτήματος ΠΑ-§16.1.	Ορίστε διαδικασία διατήρησης αρχείου δραστηριοτήτων επεξεργασίας, ως ΥΠΕ, που να περιέχει όλες τις πληροφορίες που αναφέρονται στον πίνακα παραρτήματος ΠΑ-§16.1.		Αρχείο δραστηριοτήτων επεξεργασίας	v	v	v	v
16.1	- ()	Αν ναι, προσδιορίστε σχετικά.	ΠΑ-§16.1	-	-						
17	28-2 (IV)	Είστε ο μοναδικός εκτελών την επεξεργασία (ΕΚΕ) ΔΠΧ;		[καμία ενέργεια]	Εκδώστε γραπτή άδεια του υπεύθυνου επεξεργασίας (ΥΠΕ) για καθένα από τους εκλελώντες την επεξεργασία (ΕΚΕ). Ελέγξτε τη συμμόρφωση τους με τον ΓΚΠΔ/GDPR.			v			
18	30-2 (IV)	Ως εκτελών την επεξεργασία (ΕΚΕ) τηρείτε αρχείο δραστηριοτήτων επεξεργασίας;		Επιβεβαιώστε ότι τηρείτε αρχείο δραστηριοτήτων επεξεργασίας σε γραπτή ή ηλεκτρονική μορφή ως εκτελών την επεξεργασία (ΕΚΕ) (άρ.30§3)	Ορίστε διαδικασία διατήρησης αρχείου δραστηριοτήτων επεξεργασίας σε γραπτή ή ηλεκτρονική μορφή ως εκτελών την επεξεργασία (ΕΚΕ) (άρ.30§3).	Επιβεβαιώστε ότι τηρείτε όλα όσα αναφέρονται στον σχετικό πίνακα.	Αρχείο δραστηριοτήτων επεξεργασίας	v	v	v	v
18.1	- ()	Αν ναι, προσδιορίστε σχετικά.	ΠΑ-§18.1	-	-						

				Προτεινόμενες ενέργειες			Βοηθητικές πληροφορίες				
Α/Α	**ID**	**Ερώτηση**	**§ παραρτήματος Αποτύπωσης**	**Αν ΝΑΙ**	**Αν ΌΧΙ**	**Διευκρίνιση**	**Υποχρέωση διατήρησης στοιχείων**	**Έγγραφο ως τεκμηρίωση**	**Πολιτική**	**Διαδικασία**	**Τεχνικό**
Θέματα ασφαλείας											
19	24-1 (IV) 32-1 (IV)	Είναι τα τεχνικά και οργανωτικά μέτρα κατάλληλα προκειμένου να διασφαλιστεί το κατάλληλο επίπεδο ασφάλειας της επεξεργασίας δεδομένων;	ΠΑ-§19	-	-	Επιβεβαιώστε και τεκμηριώστε ότι ισχύουν τα κατάλληλα οργανωτικά μέτρα ασφαλείας στην επεξεργασία των δεδομένων. Περισσότερες πληροφορίες στο παράρτημα ΠΕ-§19.	Έκθεση αναφοράς τεχνικών μέτρων	v	v	v	v
20	25-1 (IV)	Λαμβάνετε μέτρα προστασίας ΔΠΧ κατά το σχεδιασμό (by design) και εξ' ορισμού (by default) (αφορά περιπτώσεις που σχεδιάζετε νέες εφαρμογές);		-	-	Επιβεβαιώστε και τεκμηριώστε ότι λαμβάνετε τα κατάλληλα οργανωτικά μέτρα ασφαλείας κατά τον σχεδιασμό και εξ' ορισμού σε νέες εφαρμογές για την επεξεργασία των δεδομένων. Περισσότερες πληροφορίες στο παράρτημα ΠΕ-§20.	Έκθεση αναφοράς τεχνικών μέτρων	v	v	v	v
20.1	- ()	Αν ναι, προσδιορίστε σχετικά.	ΠΑ-§20.1	-	-						
21	32-2 (IV)	Ποιους κινδύνους λαμβάνετε υπόψη κατά την επεξεργασία ΔΠΧ;	ΠΑ-§21	-	-	Επιβεβαιώστε - ενεργείστε ώστε να λαμβάνονται υπόψη όλοι οι κίνδυνοι που είναι στον πίνακα του παραρτήματος ΠΕ-§21.	Έκθεση αναφοράς λήψης μέτρων για κινδύνους	v	v	v	v
22	32-3 (IV)	Τηρείτε εγκεκριμένο κώδικα δεοντολογίας;		Επιβεβαιώστε ότι ο κώδικά δεοντολογίας τηρείτε και είναι εγκεκριμένος.	Ενδείκνυται να τηρήσετε εγκεκριμένο κώδικα δεοντολογίας.	Περισσότερες πληροφορίες στο παράρτημα ΠΕ-§21.		v	v	v	v
22.1	- ()	Αν ναι, προσδιορίστε σχετικά.		-	-						
23	32-4 (IV)	Είναι κάθε φυσικό πρόσωπο που έχει πρόσβαση στα ΠΔ υπό την εποπτεία του ΥΠΕ ή ΕΚΕ;		Επιβεβαιώστε ότι κάθε φυσικό πρόσωπο που έχει πρόσβαση στα ΠΔ είναι υπό την εποπτεία του ΥΠΕ ή ΕΚΕ	Μεριμνήστε ώστε κάθε φυσικό πρόσωπο που έχει πρόσβαση στα ΠΔ να ενεργεί υπό την εποπτεία του ΥΠΕ ή ΕΚΕ.			v	v	v	v
24	33-1 (IV)	Έχετε διαδικασία γνωστοποίησης σε περίπτωση παραβίασης δεδομένων στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ);		Επιβεβαιώστε ότι η γνωστοποίηση παραβίασης δεδομένων στην ΑΠΔΠΧ περιλαμβάνει όλα όσα αναφέρονται στον πίνακα στο παράρτημα ΠΑ-§24.1.	Ορίστε διαδικασία γνωστοποίησης παραβίασης δεδομένων στην ΑΠΔΠΧ περιλαμβάνοντας όλα όσα αναφέρονται στον πίνακα στο παράρτημα ΠΑ-§24.1.			v	v	v	v
24.1	- ()	Αν ναι, προσδιορίστε σχετικά.	ΠΑ-§24.1	-	-						

				Προτεινόμενες ενέργειες			Βοηθητικές πληροφορίες				
Α/Α	ID	Ερώτηση	§ παραρτήματος Αποτύπωσης	Αν ΝΑΙ	Αν ΌΧΙ	Διευκρίνιση	Υποχρέωση διατήρησης στοιχείων	Έγγραφο ως τεκμηρίωση	Πολιτική	Διαδικασία	Τεχνικό
25	34-1 (IV)	Έχετε διαδικασία γνωστοποίησης σε περίπτωση παραβίασης δεδομένων στο ΥΔ;		Επιβεβαιώστε ότι η γνωστοποίηση παραβίασης δεδομένων στο ΥΔ περιλαμβάνει όλα όσα αναφέρονται στον πίνακα στο παράρτημα ΠΑ-§25.1.	Ορίστε διαδικασία γνωστοποίησης παραβίασης δεδομένων στο ΥΔ περιλαμβάνοντας όλα όσα αναφέρονται στον πίνακα στο παράρτημα ΠΑ-§25.1.			v	v	v	v
25.1	- ()	Αν ναι, προσδιορίστε σχετικά.	ΠΑ-§25.1								
26	35-1 (IV)	Έχετε μελέτη εκτίμησης αντικτύπου προστασίας δεδομένων (ΕΑΠΔ/DPIA);		Επιβεβαιώστε ότι η ΕΑΠΔ/DPIA περιλαμβάνει όλα όσα αναφέρονται στον πίνακα στο παράρτημα ΠΑ-§26.2	Ελέγξτε εάν περιλαμβάνεστε στις περιπτώσεις που απαιτείται η διενέργεια ΕΑΠΔ/DPIA στον πίνακα του παραρτήματος ΠΑ-§26.2. Αν όχι είναι προαιρετική η διενέργεια ΕΑΠΔ/DPIA.	Περισσότερες πληροφορίες στο παράρτημα ΠΕ-§16.		v	v	v	
26.1	- ()	Αν όχι, συμπληρώστε το σχετικό πίνακα.	ΠΑ-§26.1	-	-						
26.2	- ()	Αν ναι, προσδιορίστε σχετικά.	ΠΑ-§26.2	-	-						
27	37-1 (IV)	Έχετε ορίσει υπεύθυνο προστασίας δεδομένων (ΥΠΔ/DPO);		Επιβεβαιώστε ότι ο ΥΠΔ έχει τα προβλεπόμενα καθήκοντα.	Ελέγξτε αν υποχρεούστε να ορίσετε ΥΠΔ/DPO.	Περισσότερες πληροφορίες στο παράρτημα ΠΕ-§27.		v	v	v	v
28	43-1 (IV)	Έχετε κάποια πιστοποίηση για την προστασία δεδομένων;		Επιβεβαιώστε ότι πιστοποίηση(εις) που έχετε μπορεί να χρησιμοποιηθούν ως απόδειξη συμμόρφωσης στον Κανονισμό.	Ενθαρρύνεται η χρήση πιστοποιήσεων από τον Κανονισμό ως απόδειξη συμμόρφωσης σε αυτόν.	Σχετικές πιστοποιήσεις μπορούν να χρησιμοποιηθούν ως απόδειξη συμμόρφωσης στον κανονισμό. Επίσημα δεν έχουν οριστεί εγκεκριμένες σχετικές πιστοποιήσεις τελ. ενημέρωση 11/01/2018. (αρ.42,43).		v	v	v	v
28.1	- ()	Αν ναι, προσδιορίστε σχετικά.	ΠΑ-§28.1	-	-						

Παράρτημα (ΠΕ)
εγχειριδίου ενεργειών

για τη συμμόρφωση με τον Ευρωπαϊκό Γενικό Κανονισμό Προστασίας Δεδομένων - General Data Protection Regulation (ΓΚΠΔ/GDPR) 2016/679

Περιεχόμενα παραρτήματος

Εδαφικός προσδιορισμός – Διαβιβάσεις δεδομένων

ΠΕ-§2.1 Διαβιβάσεις δεδομένων

Στον πίνακα «Επιτρεπόμενες χώρες / τρόποι διαβίβασης δεδομένων (άρ. 44-50)» του παραρτήματος, του εγχειριδίου αποτύπωσης, αναφέρονται οι περισσότερες δυνατές περιπτώσεις επιτρεπόμενων διαβιβάσεων δεδομένων εκτός ΕΕ. Επιβεβαιώστε με το νομικό σας σύμβουλο την ισχύ της νομιμότητας σας.

[Σχετικά άρθρα του κανονισμού: 44-50]

ΠΕ-§3 Σύννομη επεξεργασία δεδομένων

Για να αποδειχθεί η νομιμότητα της επεξεργασίας θα πρέπει για κάθε ΔΠΧ που επεξεργάζεστε να υπάρχει σύννομη απόδειξή του. Η εργασία αυτή είναι η πιο σημαντική και χρονοβόρα σε όλο τον οδηγό συμμόρφωσης. Επιβεβαιώσετε ότι:

1. Έχει γίνει πλήρης καταγραφή των ΔΠΧ και των επεξεργασιών αυτών (Εισερχόμενα ΠΔ, Εξερχόμενα ΠΔ, παραγόμενα εντός ΠΔ) (φυσικό αρχείο, φυσικούς - εικονικούς δίσκους, ηλεκτρονική αλληλογραφία κτλ.)
2. Ισχύει η νομιμότητα κάθε ΔΠΧ και ΔΠΧΕΚ (συγκατάθεση , σύμβαση κτλ.)
3. Σε περιπτώσεις που διαμοιράζονται δεδομένα, να ελεγχθεί ότι είναι σύννομο βάσει του πίνακα που έχετε συμπληρώσει στο ερώτημα2.1.

[Σχετικά άρθρα του κανονισμού: 6, 9-11,13]

Τήρηση αρχείου για:

α) τα ΔΠΧ που υπόκεινται επεξεργασία,

β) απόδειξη συγκατάθεσης του ΥΔ για ΔΠΧ και ρητής συγκατάθεσης για ΔΠΧΕΚ.

Νομιμότητα Επεξεργασίας Προσωπικών Δεδομένων (ΠΔ)

Δικαιώματα Υποκειμένων Δεδομένων (ΥΔ)

ΠΕ-§6 Δικαίωμα ενημέρωσης

Ελέγξτε τις απαντήσεις του ΠΑ-§6.1, επιβεβαιώστε ότι έχουν απαντηθεί καταφατικά και ισχύουν οι πίνακες :

«Α. Μορφή παρεχόμενων πληροφοριών στο ΥΔ (άρ.13,14)»

«Γ. Χρόνος διάθεσης πληροφοριών στο ΥΔ»

«Δ. Είδος παρεχόμενων πληροφοριών (άρ.13,14)»

Στην ενημέρωση περιλαμβάνεται και η δήλωση ιδιωτικότητας σας (ή πολιτική ιδιωτικότητας ή δήλωση απορρήτου κτλ.). Επιβεβαιώστε ότι περιλαμβάνονται όλα όσα αναφέρονται στο ΠΑ-§6.1 πίνακας «Δ. Είδος παρεχόμενων πληροφοριών (άρ.13,14)».

Επιβεβαιώστε ότι, ισχύει κατ΄ ελάχιστο μια από τις υπάρχουσες επιλογές του πίνακα «Β. Τρόπος διάθεση πληροφοριών στο ΥΔ» (έντυπα ή ηλεκτρονικά ή προφορικά).

[Σχετικά άρθρα του κανονισμού: 12§1, §5, §7, 13, 14, α.σ. 58-62 και
γνωμοδότηση της ΟΕ29 “Guidelines on transparency under Regulation 2016/679”, (WP260)]

ΠΕ-§7 Δικαίωμα πρόσβασης

Επιβεβαιώστε ότι:

α) Ισχύουν όλα όσα αναφέρονται στον πίνακα Α. Πληροφορίες στο ΥΔ για το δικαίωμα πρόσβασης. (άρ.13,14).

β) Σε περίπτωση που κάνετε διαβιβάσεις δεδομένων εκτός ΕΕ- ΕΟΧ, επιβεβαιώστε ότι ισχύει κάτι από τις υπάρχουσες επιλογές

Υποχρεούστε να διατηρείτε αρχεία

1.Μορφή αντιγράφου ΔΠΧ ΥΔ

2.Εγγυήσεις για διαβιβάσεις εκτός ΕΕ - ΕΟΧ (άρ.46)

[Σχετικά άρθρα του κανονισμού: 12,15 και α.σ.65]

ΠΕ-§9 Δικαίωμα διαγραφής (δικαίωμα στη λήθη)

Το δικαίωμα διαγραφής δεδομένων ισχύει υπο περιπτώσεις. Ελέγξτε εάν ο οργανισμός σας εμπίπτει σε κάποιους από του λόγους υποχρέωσης διαγραφής δεδομένων. Οι λόγοι είναι αυτοί που αναφέρονται στον αντίστοιχο πίνακα ΠΑ-§9.1 Δικαίωμα διαγραφής (δικαίωμα στη λήθη) Δώστε προσοχή και στις εξαιρέσεις του δικαιώματος διαγραφής (άρ.17$3). Αν υποχρεούστε ορίστε διαδικασία διαγραφής ΔΠΧ .

[Σχετικά άρθρα του κανονισμού: 17,19 και α.σ.65,66]

ΠΕ-§10 Δικαίωμα περιορισμού της επεξεργασίας

Το δικαίωμα περιορισμού της επεξεργασίας ασκείται αν ισχύει κάποια από τις προϋποθέσεις που αναφέρονται στο ΠΑ-§10.1 πίνακα «Περιπτώσεις περιορισμού της επεξεργασίας από το υποκείμενο δεδομένων (ΥΔ)(άρ.18§1)». Σε αυτή την περίπτωση θα πρέπει να οριστούν:

1. Διαδικασίες άρσης του περιορισμού επεξεργασίας (άρ.18$2) λαμβάνοντας υπόψη τον πίνακα «Περιπτώσεις άρσης περιορισμού της επεξεργασίας (άρ.18§2)»,
2. Διαδικασία ενημέρωσης πριν την άρση περιορισμού επεξεργασίας (άρ.18$3),
3. Διαδικασία γνωστοποίησης - διόρθωσης - διαγραφής - περιορισμού σε κάθε αποδέκτη που γνωστοποιήθηκαν δεδομένα (άρ.19).

[Σχετικά άρθρα του κανονισμού: 18, 19 και α.σ. 67]

ΠΕ-§11 Δικαίωμα φορητότητας

Το δικαίωμα φορτητότητας δεδομένων ισχύει υπό περιπτώσεις. Ελέγξτε εάν ο οργανισμός σας εμπίπτει σε κάποιους από του λόγους υποχρέωσης διαγραφής δεδομένων. Ενημερωθείτε για τις περιπτώσεις του δικαιώματος φορητότητας δεδομένων.

Περιπτώσεις δικαιώματος φορητότητας δεδομένων (άρ.20§1)	
1	Η επεξεργασία βασίζεται σε συγκατάθεση (Συναίνεση ή ρητή - αρ.6§1α,9§2α) ή σε σύμβαση (άρ.6§1β)
2	Η επεξεργασία διενεργείται με αυτοματοποιημένα μέσα.

Περιπτώσεις εξαίρεσης φορητότητας δεδομένων (άρ.20§3,4)	
1	Το δικαίωμα στη φορητότητα δεν ισχύει για την επεξεργασία που είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας
2	Όταν επηρεάζει δυσμενώς τα δικαιώματα και τις ελευθερίες άλλων

[Σχετικά άρθρα του κανονισμού: άρ.12,20, α.σ.68 και
γνωμοδότηση της ΟΕ29 «Κατευθυντήριες γραμμές σχετικά με το δικαίωμα στη φορητότητα των δεδομένων», (WP 242 rev.01)]

ΠΕ-§12 Δικαίωμα εναντίωσης

Επιβεβαιώστε ότι λαμβάνετε υπόψη όλες τις περιπτώσεις που επιτρέπεται το δικαίωμα της εναντίωσης. Δώστε προσοχή στον τρόπο ενημέρωσης του ΥΔ για αυτό.

[Σχετικά άρθρα του κανονισμού: άρ.12,21 και α.σ. 69,70]

ΠΕ-§13 Δικαίωμα εναντίωσης στη λήψη αυτοματοποιημένων αποφάσεων

Επιβεβαιώστε ότι λαμβάνετε υπόψη τις περιπτώσεις που επιτρέπεται/ εξαιρείται η αυτοματοποιημένη λήψη αποφάσεων και κατάρτιση προφίλ (άρ.22) .

Σχετικά άρθρα του κανονισμού: άρ. 4§4, 9, 12, 13, 14, 15, 21, 22, 35§1§321,22 και
γνωμοδότηση της ΟΕ29 “Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679», (WP 251 αναθ.01) 06/02/2018]

Υπεύθυνος Επεξεργασίας, Εκτελών, Υπεύθυνος προστασίας

ΠΕ-§14 Πολλοί ΥΠΕ

Στην περίπτωση που υπάρχουν παραπάνω από ένας υπεύθυνοι επεξεργασίας (ΥΠΕ) θα πρέπει να γίνουν τα εξής:

1. Γραπτή συμφωνία μεταξύ των δυο, ή παραπάνω, ΥΠΕ και καθορισμός του σημείου επικοινωνίας στο υποκείμενο δεδομένων ΥΔ.
2. Η συμφωνία να είναι διαθέσιμη στο ΥΔ.

Επίσης να γίνει γνωστό ότι το ΥΔ μπορεί να ασκήσει δικαιώματα σε όλους τους ΥΠΕ ανεξάρτητα από τους όρους της μεταξύ τους συμφωνίας (άρ.26$2).

ΠΕ-§15-18 Υπεύθυνος επεξεργασίας ΥΠΕ – Εκτελών την επεξεργασία ΕΚΕ

Περιγραφή των ΥΠΕ - ΕΚΕ

Ο κάθε οργανισμός που επεξεργάζεται ΔΠΧ έχει, ή αν δεν έχει πρέπει να ορίσει, έναν υπεύθυνο επεξεργασίας (ΥΠΕ). Υπεύθυνος επεξεργασίας (ΥΠΕ) είναι το φυσικό ή νομικό αυτό πρόσωπο που καθορίζει τους σκοπούς και τον τρόπο επεξεργασίας ΔΠΧ.

Εκτελών την επεξεργασία (ΕΚΕ) είναι το φυσικό ή νομικό πρόσωπο που ορίζεται από τον υπεύθυνο επεξεργασίας (ΥΠΕ) να επεξεργάζεται για λογαριασμό του τα ΔΠΧ.

Ο διαχωρισμός του ΥΠΕ από τον ΕΚΕ πρέπει να είναι σαφής ώστε να καθορίζεται το αντικείμενο επεξεργασίας και ο ορισμός των υποχρεώσεων. Αυτό είναι σημαντικό για το διαχωρισμό των ευθυνών.

Παράδειγμα:

Μια τράπεζα (ΥΠΕ) συλλέγει δεδομένα των πελατών της όταν ανοίγουν λογαριασμό, ένας άλλος οργανισμός (ΕΚΕ) όμως ψηφιοποιεί και αποθηκεύει όλες τις πληροφορίες που καταγράφονται σε χαρτί για λογαριασμό της τράπεζας. Ο οργανισμός αυτός μπορεί να είναι εταιρίες κέντρα αποθήκευσης (Data Centers) ή εταιρίες διαχείρισης εγγράφων. Και τα δυο αυτά πρόσωπα έχουν ευθύνη για τη διαχείριση των ΔΠΧ των πελατών της τράπεζας.

[Σχετικά άρθρα του κανονισμού: 29-31]

ΠΕ-§19- 20 Κατάλληλα τεχνικά και οργανωτικά μέτρα

Ο κανονισμός δεν ορίζει συγκεκριμένα μέτρα ασφάλειας που πρέπει να εφαρμοστούν σε κάθε οργανισμό. Αναφέρει (α.σ.83) ότι… «Για τη διατήρηση της ασφάλειας και την αποφυγή της επεξεργασίας κατά παράβαση του παρόντος κανονισμού, ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία θα πρέπει να (α) αξιολογεί τους κινδύνους που ενέχει η επεξεργασία και (β) να εφαρμόζει μέτρα για τον μετριασμό των εν λόγω κινδύνων, όπως για παράδειγμα μέσω κρυπτογράφησης….»

Τα εν λόγω μέτρα θα πρέπει να διασφαλίζουν κατάλληλο επίπεδο ασφάλειας, πράγμα που περιλαμβάνει και την εμπιστευτικότητα, λαμβάνοντας υπόψη τις τελευταίες εξελίξεις και το κόστος της εφαρμογής σε σχέση με τους κινδύνους και τη φύση των δεδομένων προσωπικού χαρακτήρα που πρέπει να προστατευθούν.

Κατά την εκτίμηση του κινδύνου για την ασφάλεια των δεδομένων θα πρέπει να δίνεται προσοχή στους κινδύνους που προκύπτουν από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, όπως :

α) η τυχαία ή παράνομη καταστροφή,

β) η απώλεια,

γ) η μεταβολή,

δ) η άνευ αδείας κοινολόγηση ή προσπέλαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία η οποία θα μπορούσε να οδηγήσει σε σωματική, υλική ή μη υλική βλάβη.»

Συνεπώς ο υπεύθυνος επεξεργασίας έχοντας αξιολογήσει τους κινδύνους, έχει την ευθύνη να εφαρμόσει τα κατάλληλα τεχνικά και οργανωτικά μέτρα για το μετριασμό αυτών. Αυτό μπορεί να αναλυθεί σε μια μελέτη εκτίμησης αντικτύπου προστασίας δεδομένων - data privacy impact assessment (ΜΕΑΠΔ - DPIA) - ή μελέτη ανάλυσης και διαχείρισης κινδύνου - Risk assessment and management analysis - για την ασφάλεια των δεδομένων. Μέσα από αυτές τις αναλύσεις κατατάσσονται διαβαθμισμένοι κίνδυνοι. Ο ΥΠΕ ορίζει το όριο του αποδεκτού κινδύνου και για τους σοβαρότερους λαμβάνει μέτρα αντιμετώπισης. Τα ανάλογα ισχύουν και για τις περιπτώσεις σχεδιασμού συστημάτων.

Ο πίνακας των τεχνικών και οργανωτικών μέτρων που είναι προς συμπλήρωση έχει ως στόχο την αποτύπωση της κατάστασης που υπάρχει στον οργανισμό. Για μεγάλους οργανισμούς ενδείκνυται η εκπόνηση σχετικής μελέτης που αναφέρθηκε παραπάνω.

Ενδεικτικά μέτρα ασφάλειας σε τεχνολογίες πληροφορικής μπορείτε να βρείτε στον ιστότοπο της Αγγλικής αρχής προστασίας δεδομένων - International Commissioner Office ICO με τίτλο «IT security top tips» στο σύνδεσμο:

https://ico.org.uk/for-organisations/guide-to-data-protection/it-security-top-tips/

ΠΕ-§21 Εγκεκριμένοι κώδικες δεοντολογίας

Ο κανονισμός ενθαρρύνει την τήρηση εγκεκριμένων κωδίκων δεοντολογίας. Λάβετε υπόψη τα εξής:

1. Η τήρηση κώδικα δεοντολογίας μπορεί να χρησιμοποιηθεί ως απόδειξη συμμόρφωσης.
2. Δεν υπάρχουν προς το παρόν(11/01/2018) εγκεκριμένοι κώδικες δεοντολογίας από επίσημες αρχές ΑΠΔΠΧ κτλ.

[Σχετικά άρθρα του κανονισμού: 40,41]

ΠΕ-§26 Μελέτη εκτίμησης αντικτύπου προστασίας δεδομένων – Data privacy impact assessment (ΕΑΠΔ/DPIA)

Η ΜΕΑ / PIA ενθαρρύνεται από τον κανονισμό ως εργαλείο ανάλυσης και αντιμετώπισης κινδύνων. Οι οργανισμοί που διενεργούν μελέτη εκτίμησης αντικτύπου έχουν κατά μεγάλο ποσοστό οργανωμένη την πληροφορία που απαιτείται για την αποτύπωση της υφιστάμενης κατάστασης καθώς και τρόπους βελτίωσης.

[Σχετικά άρθρα του κανονισμού: 35 και
γνωμοδότηση ΟΕ29, «Κατευθυντήριες γραμμές για την εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) και καθορισμός του κατά πόσον η επεξεργασία «ενδέχεται να επιφέρει υψηλό κίνδυνο» για τους σκοπούς του κανονισμού 2016/679.» WP 248 αναθ. 01 04/10/2017]

ΠΕ-§27 Υπεύθυνος προστασίας δεδομένων ΥΠΔ /PDO

Για περισσότερες πληροφορίες σχετικά με τον ΥΠΔ λάβετε υπόψη τα παρακάτω:

1. Περιπτώσεις που ορίζεται ΥΠΔ (άρ.37)
2. Δικαιώματα ΥΠΔ (άρ.38)
3. Καθήκοντα ΥΠΔ (άρ.39)
4. Γνωμοδότηση WP 243 αναθ. 01, «Κατευθυντήριες γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων» της Ομάδα Εργασίας του άρθρου 29 (WP29). 05/04/2017 (τελευταία ενημέρωση 11/01/2018)