ΧΑΡΟΚΟΠΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

Σχολή Ψηφιακής Τεχνολογίας

Τμήμα Πληροφορικής και Τηλεματικής

ΠΜΣ «Πληροφορική και Τηλεματική»

Πληροφοριακά Συστήματα στη Διοίκηση Επιχειρήσεων

Η πιστοποίηση στο GDPR (άρθρα 42-43) και η σχέση του με το ISO 27001

Διπλωματική Εργασία

Παναγιώτης Ζαβογιάννης

Αθήνα, 2020

ΧΑΡΟΚΟΠΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

Σχολή Ψηφιακής Τεχνολογίας

Τμήμα Πληροφορικής και Τηλεματικής

ΠΜΣ «Πληροφορική και Τηλεματική»

Πληροφοριακά Συστήματα στη Διοίκηση Επιχειρήσεων

Τριμελής Εξεταστική Επιτροπή

Ευαγγελία Μήτρου (Επιβλέπουσα)
Καθηγήτρια, Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων, Πανεπιστήμιο Αιγαίου

Παναγιώτης Ριζομυλιώτης
Επίκουρος Καθηγητής, Πληροφορικής και Τηλεματικής, Χαροκόπειο Πανεπιστήμιο

Χρήστος Μιχαλακέλης
Επίκουρος Καθηγητής, Πληροφορικής και Τηλεματικής, Χαροκόπειο Πανεπιστήμιο

Ο Παναγιώτης Ζαβογιάννης

δηλώνω υπεύθυνα ότι:

1) Είμαι ο κάτοχος των πνευματικών δικαιωμάτων της πρωτότυπης αυτής εργασίας και από όσο γνωρίζω η εργασία μου δε συκοφαντεί πρόσωπα, ούτε προσβάλει τα πνευματικά δικαιώματα τρίτων.

2) Αποδέχομαι ότι η ΒΚΠ μπορεί, χωρίς να αλλάξει το περιεχόμενο της εργασίας μου, να τη διαθέσει σε ηλεκτρονική μορφή μέσα από τη ψηφιακή Βιβλιοθήκη της, να την αντιγράψει σε οποιοδήποτε μέσο ή/και σε οποιοδήποτε μορφότυπο καθώς και να κρατά περισσότερα από ένα αντίγραφα για λόγους συντήρησης και ασφάλειας.

Αφιερώνεται σε όλους όσους με στήριξαν κατά τη διάρκεια των σπουδών μου και ειδικότερα στην οικογένειά μου, την αγαπημένη μου σύζυγο Ελένη και το αγαπημένο μου παιδί Σωτήρη!

«Όσο περισσότερα στοιχεία για εμάς καταγράφουν οι βάσεις δεδομένων, τόσο λιγότερο υπάρχουμε»

(Μάρσαλ Μακ Λούαν 1911 – 1980,
Καναδός Επικοινωνιολόγος)

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω ιδιαίτερα την επιβλέπουσα καθηγήτρια της εργασίας μου κυρία Ευαγγελία Μήτρου, για την εμπιστοσύνη που μου έδειξε αναθέτοντάς μου αυτή την εργασία, για την πολύτιμη βοήθεια και καθοδήγησή της, καθ' όλη τη διάρκειά της, και κυρίως για την ευκαιρία που μου έδωσε να ασχοληθώ με ένα πολύ ενδιαφέρον αντικείμενο.
Τέλος θα ήθελα να ευχαριστήσω τη σύζυγό μου Ελένη, Φιλόλογος και μελλοντική Ψυχολόγος, για την συντακτική επιμέλεια του κειμένου καθώς οι διορθώσεις της ήταν σημαντικές.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Περίληψη

Στοχεύοντας στη βελτίωση της διαφάνειας και της συμμόρφωσης προς τον Γενικό Κανονισμό για την Προστασία Δεδομένων - ΓΚΠΔ, παροτρύνεται (άρθρο 42 του ΓΚΠΔ) η θέσπιση μηχανισμών πιστοποίησης, σφραγίδων και σημάτων προστασίας των δεδομένων καθώς επίσης και η διαπίστευση φορέων πιστοποίησης (άρθρο 43 του ΓΚΠΔ). Σκοπός αυτής τη διπλωματικής εργασίας είναι να εξεταστεί το ζήτημα της πιστοποίησης στο GDPR όπως αναφέρεται στα άρθρα 42 και 43 του ΓΚΠΔ καθώς επίσης και στο άρθρο 37 του Νόμου 4624/2019. Στη συνέχεια, διερευνάται η όποια σχέση του ΓΚΠΔ ή δυνατότητα συνδυασμού του με το διεθνές πρότυπο για την ασφάλεια πληροφοριών ISO 27001. Η πιστοποίηση έχει σαν σκοπό την απόδειξη της συμμόρφωσης, προς τον ΓΚΠΔ, των πράξεων επεξεργασίας από τους Υπεύθυνους Επεξεργασίας και τους Εκτελούντες την επεξεργασία, χωρίς να περιορίζεται η ευθύνη τους για τη συμμόρφωσή τους προς τον ΓΚΠΔ και τον εθνικό νόμο 4624/2019 και χωρίς να θίγονται τα καθήκοντα και οι αρμοδιότητες της εποπτικής αρχής. Η πιστοποίηση αυτή δύναται να χορηγηθεί είτε από διαπιστευμένο φορέα πιστοποίησης, είτε από αρμόδια εποπτική αρχή, είτε από το Συμβούλιο Προστασίας Δεδομένων. Τα βήματα σχετικά με τη διαδικασία θέσπισης μηχανισμού πιστοποίησης προστασίας δεδομένων είναι: Καθορισμός κριτηρίων από τον φορέα πιστοποίησης – Έγκριση των κριτηρίων από την αρμόδια εποπτική αρχή – Διαπίστευση φορέα πιστοποίησης – Πιστοποίηση – Συγκέντρωση και δημοσιοποίηση μηχανισμών πιστοποίησης, σφραγίδων και σημάτων από Συμβούλιο Προστασίας Δεδομένων. Τα στάδια πιστοποίησης συνοπτικά είναι: Αίτηση για πιστοποίηση – Ανασκόπηση της αίτησης και αρχείο διαδικασίας πιστοποίησης – Προ αξιολόγηση – Αξιολόγηση – Επικύρωση αποτελεσμάτων – Ενημέρωση αρμόδιας εποπτικής Αρχής - Έκδοση και χορήγηση πιστοποίησης – Περιοδική ανασκόπηση πιστοποίησης (επιτήρηση) – Ανανέωση / Απόρριψη πιστοποίησης. Οι υπάρχουσες πιστοποιήσεις έχουν ήδη θεσπίσει μηχανισμούς, μεθοδολογίες αξιολόγησης, συμβατικές ρυθμίσεις και επιθεωρητές που μπορούν και πρέπει να χρησιμοποιηθούν για τη δημιουργία των μηχανισμών προστασίας δεδομένων ΓΚΠΔ. Από την έρευνα προέκυψε ότι ακολουθούν τρία μοντέλα: το ρυθμιστικό μοντέλο, το μοντέλο προτύπων και το συνδυασμένο μοντέλο. Μέχρι σήμερα, κανένα δημοσιευμένο πρότυπο δεν περιγράφει τον τρόπο διεξαγωγής της διαδικασίας σχετικά με την εκτίμηση των κινδύνων και του αντικτύπου για την ζωή των υποκειμένων των δεδομένων ώστε να αντιμετωπιστούν με ανάλογο τρόπο. Επομένως, η ανάπτυξη ενός συνεκτικού και επαρκούς συνόλου ευρωπαϊκών προτύπων πλήρως εναρμονισμένων με τις αρχές και τους μηχανισμούς του ΓΚΠΔ χρειάζεται ακόμη σημαντικές προσπάθειες. Η διατήρηση ενός πιστοποιημένου Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών με βάση το ISO 27001 πλέον απαιτείται όλο και περισσότερο από οργανισμούς, ανεξάρτητα από τον τύπο τους, το μέγεθός τους ή τη φύση τους, και έχει σαν σκοπό τη διατήρηση της εμπιστευτικότητας, της ακεραιότητας και διαθεσιμότητας των πληροφοριακών αγαθών τους. Η εφαρμογή του ISO 27001 καλύπτει τις περισσότερες από τις απαιτήσεις του ΓΚΠΔ. Ωστόσο, ορισμένα στοιχεία ελέγχου πρέπει να προσαρμοστούν ώστε να περιλαμβάνουν και προσωπικά δεδομένα. Εάν ο οργανισμός έχει ήδη εφαρμόσει το πρότυπο, είναι τουλάχιστον στη μέση της διασφάλισης της προστασίας των προσωπικών δεδομένων και της ελαχιστοποίησης του κινδύνου διαρροής.

Λέξεις κλειδιά: Πιστοποίηση, ΓΚΠΔ, Ασφάλεια, ISO 27001, Διαπίστευση

Abstract

Aiming to improve transparency and compliance with the General Data Protection Regulation - GDPR, it is urged (Article 42 of the GDPR) to establish data protection certification mechanisms, seals and marks as well as accreditation of certification bodies (Article 43 of the GDPR). The purpose of this dissertation is to examine the issue of GDPR certification as referred to in Articles 42 and 43 of the GDPR as well as Article 37 of Law 4624/2019. Subsequently, any relationship of the GDPR or the possibility of combining it with the international standard for information security ISO 27001 is investigated. The certification aims to prove compliance with the GDPR, the processing operations by the Controllers and the Processors, without limiting their responsibility for their compliance with the GDPR and national law 4624/2019 and without the duties and responsibilities of the supervisory authority are affected. This certification may be granted either by an accredited certification body, or by a competent supervisory authority, or by the European Data Protection Board (EDPB). The steps related to the process of establishing a data protection certification mechanism are: Defining criteria by the certification body - Approving the criteria by the competent supervisory authority - Accreditation of a certification body - Certification - Concentration and publication of certification mechanisms, seals and marks by EDPB. The certification stages are summarized as follows: Application for certification - Review of the application and file of certification process - Pre-evaluation - Evaluation - Validation of results - Information of the competent supervisory authority - Issuance and certification - Periodic certification Review / Certification - review (supervision). Existing certifications have already established mechanisms, evaluation methodologies, conventional regulations and auditors that can and should be used to create GDPR data protection mechanisms. The research revealed that three models follow: the regulatory model, the standards model and the combined model. To date, no published standard describes how the process is conducted to assess the risks and countermeasures of data subjects' lives so that they can be addressed in a similar manner. Therefore, the development of a coherent and adequate set of European standards fully harmonized with the principles and mechanisms of the GDPR still requires significant efforts. Maintaining a certified Information Security Management System (ISMS) based on ISO 27001 is now increasingly required by organizations, regardless of their type, size or nature, and aims to maintain the confidentiality, integrity and availability of their information. The implementation of ISO 27001 covers most of the requirements of the GDPR. However, some controls need to be adjusted to include personal data. If the organization has already implemented an ISMS based on ISO 27001, it is at least in the middle of ensuring the protection of personal data and minimizing the risk of leakage.

Keywords: Certification, GDPR, Security, ISO 27001, Accreditation

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

CBPR	Cross-Border Privacy Rules framework
COPPA	Children's Online Privacy Protection Act
DPA	Data Protection Authority
DPIA	Data Protection Impact Assessment (Εκτίμηση Αντικτύπου Προστασίας Δεδομένων)
EDPB	European Data Protection Board
GDPR	General Data Protection Regulation
IAB	Interactive Advertising Bureau Europe
IAF	International Accreditation Forum Inc.
IEC	International Electrotechnical Commission
ISDP	International scheme for the protection of personal data
ISMS	Information Security Management System
ISO	International Organization for Standardization
JIPDEC	Japan Institute for Promotion of Digital Economy and Community
PII	Personally Identifiable Information
SME	Small and medium-sized enterprise
ΑΠΔΠΧ	Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
ΓΚΠΔ	Γενικός Κανονισμός για την Προστασία Δεδομένων
ΕΣΥΔ	Εθνικό Σύστημα Διαπίστευσης
ΜΜΕ	Μικρές και Μεσαίου μεγέθους Επιχειρήσεις
ΣΔΑΠ	Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών
ΣΛΕΕ	Συνθήκη για τη Λειτουργία της Ευρωπαϊκής Ένωσης

ΕΙΣΑΓΩΓΗ

Στη σύγχρονη εποχή μας η εξέλιξη της τεχνολογίας σε επίπεδο υλικού (hardware) αλλά και σε επίπεδο λογισμικού (software) έχει δώσει τη δυνατότητα για ευκολότερη και ταχύτερη συλλογή, αποθήκευση, διακίνηση και επεξεργασία ολοένα και μεγαλύτερου όγκου δεδομένων. Τα δεδομένα αυτά αφορούν εκτός των άλλων και προσωπικά στοιχεία ανθρώπων, ευαίσθητα και μη, που η συλλογή τους, η επεξεργασία τους και η διακίνησή τους μπορεί να γίνεται είτε εις γνώση τους, είτε εν αγνοία τους.

Κατά το παρελθόν είχαν γίνει αρκετές προσπάθειες, προκειμένου να προστατευθούν τα προσωπικά δεδομένα (ευαίσθητα και μη), που στο σύνολο τους αδυνατούσαν όχι μόνο να εξαλείψουν αλλά και να περιορίσουν δραστικά το φαινόμενο της μη εξουσιοδοτημένης, και κάποιες φορές παράνομης, συλλογής, επεξεργασίας και διακίνησης αυτών. Τα τελευταία χρόνια και πιο συγκεκριμένα από τις 27 Απριλίου 2016, από τα κράτη μέλη της Ευρώπης Ένωσης ψηφίστηκε ο Κανονισμός 2016/679 της Ευρωπαϊκής Ένωσης, ευρύτερα γνωστός ως Γενικός Κανονισμός για την Προστασία Δεδομένων - ΓΚΠΔ (και στα αγγλικά General Data Protection Regulation - GDPR) ο οποίος εφαρμόστηκε υποχρεωτικά για όλα τα κράτη μέλη της Ευρωπαϊκής Ένωσης στις 25 Μαΐου 2018. Βασικός στόχος του Κανονισμού αυτού αποτελεί η διασφάλιση συνεκτικής και υψηλού επιπέδου προστασίας των φυσικών προσώπων και η άρση των εμποδίων στις ροές δεδομένων προσωπικού χαρακτήρα εντός της Ένωσης, διατηρώντας έτσι το επίπεδο προστασίας των δικαιωμάτων και των ελευθεριών των φυσικών προσώπων, σε σχέση με την επεξεργασία των εν λόγω δεδομένων, ισοδύναμο σε όλα τα κράτη μέλη. Επίσης, διασφαλίζεται συνεκτική και ομοιόμορφη εφαρμογή των κανόνων για την προστασία των θεμελιωδών δικαιωμάτων και των ελευθεριών των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα σε ολόκληρη την Ένωση.

Στοχεύοντας στη βελτίωση της διαφάνειας και της συμμόρφωσης προς τον Γενικό Κανονισμό για την Προστασία Δεδομένων - ΓΚΠΔ, παροτρύνεται (άρθρο 42 του ΓΚΠΔ) η θέσπιση μηχανισμών πιστοποίησης και σφραγίδων και σημάτων προστασίας των δεδομένων καθώς επίσης και φορέων πιστοποίησης (άρθρο 43 του ΓΚΠΔ). Παράλληλα προκειμένου να ενισχυθεί η ασφάλεια των δεδομένων αλλά και να διασφαλιστεί η τήρηση των απαιτήσεων του Κανονισμού, στο Κεφάλαιο IV του Κανονισμού, στο Τμήμα 2 – Ασφάλεια δεδομένων προσωπικού χαρακτήρα, στο άρθρο 32 γίνεται αναφορά για τη λήψη κατάλληλων τεχνικών και οργανωτικών μέτρων για την ασφάλεια, ανάλογο προς τους κινδύνους, συμπεριλαμβανομένων

της χρήσης ψευδωνύμου και της κρυπτογράφησης δεδομένων προσωπικού χαρακτήρα, τις διαδικασίες διαχείρισης περιστατικών και τη διαδικασία για την αξιολόγηση της αποτελεσματικότητας των μέτρων. Τέλος λαμβάνονται υπόψη οι κίνδυνοι που απορρέουν από την επεξεργασία, ιδίως από τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, άνευ αδείας κοινολόγηση ή προσπέλαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία.

Σημαντικό βήμα προς την ενίσχυση της προστασίας δεδομένων αποτελεί και η πρόσφατη ψήφιση και εφαρμογή του νόμου 4624/2019. Αυτός έχει ως σκοπό την ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την 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. Επίσης στοχεύει στην κατάργηση της απόφασης - πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου, τη λήψη μέτρων εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών. Τέλος αποβλέπει και στην κατάργηση της Οδηγίας 95/46/ΕΚ και την αντικατάσταση του νομοθετικού πλαισίου που ρυθμίζει τη συγκρότηση και λειτουργία της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

Ταυτόχρονα λόγω της τεχνολογικής εξέλιξης η ασφάλεια των πληροφοριακών αγαθών αποτελεί πλέον μείζονος σημασίας τόσο σε ατομικό όσο και σε εταιρικό επίπεδο. Η πληροφορία είναι αποφασιστικής σημασίας θέμα για τη λειτουργία και πιθανόν την επιβίωση ενός οργανισμού δημόσιου ή ιδιωτικού. Στο μεγαλύτερο ποσοστό η πληροφορία πηγάζει από την επεξεργασία ψηφιακά αποθηκευμένων δεδομένων σε πληροφοριακά συστήματα, στα οποία μπορούν να έχουν πρόσβαση πολλοί χρήστες από διάφορες γεωγραφικές περιοχές. Σε ένα τέτοιο λειτουργικό περιβάλλον εισάγονται κίνδυνοι μη εξουσιοδοτημένης πρόσβασης ή αποκάλυψης πληροφοριών, εισαγωγής λανθασμένων δεδομένων, καθώς και αλλοίωσης ή / και καταστροφής των πληροφοριών.

Η ασφάλεια πληροφοριών αποτελεί μία συνεχή και επαναλαμβανόμενη διαδικασία, με κεντρικό σημείο τη διαχείριση των σχετικών κινδύνων καθώς και τη λήψη απαιτούμενων και κατάλληλων μέτρων πρόληψης και αντιμετώπισης τους. Προκειμένου να βοηθηθεί και να ενισχυθεί η

διαδικασία ασφάλειας πληροφοριών υπάρχουν τεχνικά πρότυπα που συμβάλλουν προς αυτή την κατεύθυνση. Ένα από αυτά είναι το ISO/IEC 27001 που είναι το μόνο διεθνές πρότυπο που μπορεί να επιθεωρηθεί και το οποίο καθορίζει τις απαιτήσεις για ένα Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ-ISMS). Το πρότυπο αυτό είναι σχεδιασμένο έτσι ώστε να διασφαλίζει την επιλογή επαρκών και ισορροπημένων ελέγχων ασφάλειας. Αυτή η επιλογή βοηθά ένα οργανισμό να προστατεύσει τα περιουσιακά του στοιχεία πληροφοριών και να τον εμπιστεύονται τα ενδιαφερόμενα μέρη.

Σκοπός αυτής τη διπλωματικής εργασίας είναι να εξεταστεί το ζήτημα της πιστοποίησης στο GDPR όπως αναφέρεται στα άρθρα 42 και 43 του ΓΚΠΔ καθώς επίσης και στο άρθρο 37 του Νόμου 4624/2019. Στη συνέχεια θα διερευνηθεί η όποια σχέση του ΓΚΠΔ ή δυνατότητα συνδυασμού του με το διεθνές πρότυπο για την ασφάλεια πληροφοριών ISO 27001.

Στο Κεφάλαιο 1 γίνεται αναφορά σε ορισμούς βασικών εννοιών που χρησιμοποιούνται στη διπλωματική μελέτη. Στο Κεφάλαιο 2 γίνεται προσπάθεια εξέτασης της προτροπής για πιστοποίηση GDPR με αναφορές στην ανάγκη ύπαρξης πιστοποίησης, τα πλεονεκτήματα αυτής, τους μηχανισμούς, τα στάδια της διαδικασίας πιστοποίησης και τη διαπίστευση των φορέων πιστοποίησης. Στο Κεφάλαιο 3 εξετάζονται τα βασικά σημεία του διεθνούς προτύπου ISO 27001, οι απαιτήσεις και η συμβολή του στην ασφάλεια πληροφοριών. Στο Κεφάλαιο 4 διερευνάται η δυνατότητα συνδυασμού των απαιτήσεων πιστοποίησης στον ΓΚΠΔ βάσει των άρθρων 42 και 43, με τις απαιτήσεις του προτύπου 27001 για την ασφάλεια πληροφοριών. Τέλος στο Κεφάλαιο 5 εξάγονται συμπεράσματα και γίνονται προτάσεις για μελλοντικές ενέργειες προς την κατεύθυνση της πιστοποίησης της προστασίας δεδομένων.

ΚΕΦ.1: Βασικοί Ορισμοί

Στο κεφάλαιο αυτό δίνονται οι ορισμοί βασικών εννοιών που χρησιμοποιούνται κατά την εκπόνηση αυτής της διπλωματικής εργασίας και συμβάλλουν στην κατανόηση βασικών όρων και του πεδίου εφαρμογής της πιστοποίησης σύμφωνα με τον Γενικό Κανονισμό για την Προστασία Δεδομένων.

- **GDPR – ΓΚΠΔ**

  General Data Protection Regulation (GDPR) - Γενικός Κανονισμός για την Προστασία Δεδομένων (ΓΚΠΔ). Αποτελείται από τον Κανονισμό για την προστασία προσωπικών δεδομένων και την οδηγία σχετικά με την επεξεργασία προσωπικών δεδομένων για δικαστικούς σκοπούς και την πρόληψη παραβατικών συμπεριφορών. Πρόκειται για ένα νέο, ενιαίο και άμεσα εφαρμόσιμο νομικό πλαίσιο, το οποίο ρυθμίζει την επεξεργασία δεδομένων προσωπικού χαρακτήρα ατόμων που βρίσκονται στην Ευρωπαϊκή Ένωση, από άλλα άτομα, εταιρείες ή οργανισμούς. Ο Κανονισμός δεν αφορά στην επεξεργασία δεδομένων προσωπικού χαρακτήρα προσώπων που δεν βρίσκονται στη ζωή ή νομικών προσώπων, όπως, για παράδειγμα, εταιρειών. Επίσης, ο GDPR δεν εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα από φυσικό πρόσωπο στο πλαίσιο αποκλειστικά προσωπικής ή οικιακής δραστηριότητας και, ως εκ τούτου, χωρίς σύνδεση με κάποια επαγγελματική ή εμπορική δραστηριότητα. Με αυτόν τον Κανονισμό ενισχύονται τα δικαιώματα των υποκειμένων των δεδομένων, αυξάνονται, ποσοτικά και ποιοτικά, οι υποχρεώσεις των υπεύθυνων και εκτελούντων την επεξεργασία και γενικώς ενισχύεται σημαντικά η προστασία των προσωπικών δεδομένων των πολιτών της ΕΕ.

- **Δεδομένα προσωπικού χαρακτήρα**

  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

- **Ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα**

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 τον γενετήσιο προσανατολισμό.

- **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.

- **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

- **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 τον διορισμό του μπορούν να προβλέπονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους.

- **Εκτελών την επεξεργασία**

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

- **Τρίτος**

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

- **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.

- **Εποπτική αρχή**

  Ανεξάρτητη δημόσια αρχή που συγκροτείται από κράτος μέλος σύμφωνα με το άρθρο 51.

- **Ασφάλεια πληροφοριών**[1]

  Η έννοια της Ασφάλειας Πληροφοριών προσδιορίζεται από τρεις (3) συνιστώσες:

  - Εμπιστευτικότητα – Απόκρυψη εμπιστευτικών πληροφοριών από μη εξουσιοδοτημένους χρήστες, ακόμα και μέσα στον ίδιο τον Οργανισμό. Η εμπιστευτικότητα των δεδομένων επιτυγχάνεται με την επιβολή ειδικών μηχανισμών και συγκεκριμένων διαδικασιών.

[1] https://www.itsecuritypro.gr/diachirisi-asfalias-pliroforion-sygchroni-epichirisiaki-anagkeotita-2/ - *Tag: IT issue 5*

- Ακεραιότητα – Εξασφάλιση της Πληρότητας, Ακρίβειας και Εγκυρότητας των επιχειρησιακών πληροφοριών. Μηχανισμοί και διαδικασίες εξασφαλίζουν την προστασία τους από πιθανή τροποποίηση, που προέρχεται από μη εξουσιοδοτημένους χρήστες.
- Διαθεσιμότητα – Οι επιχειρησιακές πληροφορίες – και κατ' επέκταση τα συστήματα και οι υπηρεσίες που προσφέρονται μέσω αυτών – πρέπει να είναι πάντα διαθέσιμες για χρήση. Εξασφαλίζεται έτσι η συνεχής και γρήγορη διανομή των πληροφοριών, καθώς και η συνεχής και γρήγορη απόκριση των πληροφοριακών συστημάτων. Αυτό επιτυγχάνεται με διαδικασίες και μηχανισμούς, που αυξάνουν τη διαθεσιμότητα των πληροφοριακών πόρων και προβλέπουν ανάκτηση των πληροφοριών σε περιπτώσεις όπου τα πληροφοριακά συστήματα υποστούν σοβαρές βλάβες.

- **Πιστοποίηση**

  Πιστοποίηση είναι η επιβεβαίωση από τρίτο ανεξάρτητο φορέα ότι προϊόντα, διεργασίες, συστήματα ή πρόσωπα συμμορφώνονται με τις απαιτήσεις συγκεκριμένων τυποποιητικών εγγράφων[2].

  Η πιστοποίηση είναι διαδικασία εξωτερικής αξιολόγησης με βάση συγκεκριμένα, προκαθορισμένα, αποδεκτά, είτε διεθνώς, είτε σε εθνικό επίπεδο είτε σε Ενωσιακό επίπεδο, και εκ των προτέρων δημοσιοποιημένα ποσοτικά και ποιοτικά κριτήρια και δείκτες, εναρμονισμένα με Αρχές και Κατευθυντήριες Οδηγίες. Αποτελεί μια αδιάβλητη διαδικασία που διενεργείται με όρους διαφάνειας και αξιοκρατίας από μια αναγνωρισμένη ανεξάρτητη Αρχή

  Σύμφωνα με το ISO 17000 η Πιστοποίηση (certification) είναι επιβεβαίωση τρίτου μέρους που αναφέρεται σε Προϊόντα, Διεργασίες, Συστήματα, Άτομα. Η έννοια της πιστοποίησης καλύπτει όλα τα αντικείμενα της αξιολόγησης της συμμόρφωσης, εκτός από τους ίδιους τους φορείς αξιολόγησης της συμμόρφωσης, για τους οποίους ισχύει η διαπίστευση[3].

  Στο πλαίσιο της πιστοποίησης με βάση τα άρθρα 42 και 43 του ΓΚΠΔ, η πιστοποίηση αναφέρεται στην επιβεβαίωση τρίτου μέρους αναφορικά με πράξεις επεξεργασίας υπευθύνων επεξεργασίας και εκτελούντων την επεξεργασία.

- **Διαπίστευση και Φορέας Διαπίστευσης**

[2] http://www.elot.gr/34_ELL_HTML.aspx
[3] Πρότυπο ISO/IEC 17000:2004 παράγραφος 5.5

Η Διαπίστευση (accreditation), σύμφωνα με το πρότυπο ISO/IEC 17000:2004 παράγραφος 5.6, είναι η επιβεβαίωση τρίτου μέρους που αναφέρεται στο φορέα αξιολόγησης συμμόρφωσης, προσδίδοντας επίσημη τεκμηρίωση της ικανότητάς του να διεξάγει καθορισμένους ρόλους (tasks) αξιολόγησης συμμόρφωσης.

Φορέας Διαπίστευσης), σύμφωνα με το πρότυπο ISO/IEC 17000:2004 παράγραφος 2.6, είναι εξουσιοδοτημένος φορέας που διενεργεί διαπίστευση

Στην Ελλάδα Φορέας (Οργανισμός) Διαπίστευσης είναι το Εθνικό Σύστημα Διαπίστευσης Α.Ε. (Ε.ΣΥ.Δ.), που αποτελεί, με βάση την ορολογία του ISO 17000, αρχή αναγνώρισης (designating authority), δηλαδή είναι φορέας που έχει ιδρυθεί ή υποστηρίζεται από το κράτος, ώστε να αναγνωρίζει, μεταξύ άλλων, φορείς αξιολόγησης συμμόρφωσης (πιστοποίησης) και κατέχει το δικαίωμα να άρει προσωρινά, να κωλύει ή και να παύει οριστικά την οποιαδήποτε αναγνώριση παρέχει.

Σύμφωνα με τον πρόσφατο νόμο 4624/2019, που έχει σαν σκοπό την ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016, ορίζεται με το άρθρο 37 ότι η διαπίστευση των φορέων που χορηγούν πιστοποιήσεις σύμφωνα με το άρθρο 42 του ΓΚΠΔ, πραγματοποιείται από το Εθνικό Σύστημα Διαπίστευσης, με διακριτικό τίτλο «Ε.ΣΥ.Δ», το οποίο αποτελεί σύμφωνα με το άρθρο 1 παρ. 3 του ν. 4468/2017 (Α΄61) τον Εθνικό Οργανισμό Διαπίστευσης κατά την έννοια των διατάξεων του Κανονισμού (ΕΚ) αριθμ. 765/2008 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 9ης Ιουλίου 2008 (L 218/30), με βάση το πρότυπο EN-ISO/IEC 17065:2012 και σύμφωνα με συμπληρωματικές απαιτήσεις που έχουν οριστεί από την Αρχή.

- **Πρότυπο**

  Πρότυπο είναι το τυποποιητικό έγγραφο που έχει καθιερωθεί με συναίνεση, έχει εγκριθεί από έναν αναγνωρισμένο φορέα σε μια κοινότητα εφαρμογής. Τα πρότυπα είναι προαιρετικής εφαρμογής εκτός εάν κανονιστικές διατάξεις επιβάλλουν την εφαρμογή τους. Παράδειγμα: Το εθνικό πρότυπο (π.χ. πρότυπο ΕΛΟΤ) έχει εκπονηθεί με συναίνεση όλων των ενδιαφερομένων, σε εθνική κλίμακα, και έχει εγκριθεί από αναγνωρισμένο εθνικό οργανισμό τυποποίησης[4]

[4] http://www.elot.gr/194_ELL_HTML.aspx

ΚΕΦ.2: Πιστοποίηση GDPR

Ο Γενικός Κανονισμός για την Προστασία των Δεδομένων παρέχει ένα σύγχρονο πλαίσιο για τη συμμόρφωση με τη λογοδοσία και τα θεμελιώδη δικαιώματα για την προστασία των δεδομένων στην περιοχή της Ευρώπης. Η διευκόλυνση της συμμόρφωσης με τις διατάξεις του Γενικού Κανονισμού για την Προστασία των Δεδομένων, εφεξής ΓΚΠΔ, εξασφαλίζεται με μία σειρά μέτρων, από τα οποία άλλα περιλαμβάνουν υποχρεωτικές απαιτήσεις σε ειδικές συνθήκες (πχ: ορισμός Υπευθύνου Προστασίας Δεδομένων, διενέργεια εκτίμησης των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας (DPIA) και διάφορα άλλα) και άλλα αποτελούν εθελοντικά μέτρα όπως η εφαρμογή κώδικα δεοντολογίας και μηχανισμών πιστοποίησης τη συμμόρφωσης.

Σύμφωνα με τον ΓΚΠΔ άρθρο 42 παράγραφος 1, η θέσπιση μηχανισμών πιστοποίησης προστασίας δεδομένων και σφραγίδων και σημάτων προστασία δεδομένων έχουν σκοπό την απόδειξη της συμμόρφωσης, προς τον ΓΚΠΔ, των πράξεων επεξεργασίας από τους Υπεύθυνους Επεξεργασίας και τους Εκτελούντες την επεξεργασία. Στο πλαίσιο αυτό χρειάζεται να ληφθούν σοβαρά υπόψη οι ειδικές ανάγκες των πολύ μικρών, μικρών και μεσαίων επιχειρήσεων, ώστε η πιστοποίηση να είναι προσιτή και εφαρμόσιμη από αυτές. Σύμφωνα με το ίδιο άρθρο, στην παράγραφο 3, η πιστοποίηση είναι εθελοντική, διαθέσιμη μέσω διαφανούς διαδικασίας, και όχι δικαίωμα ή υποχρέωση. Ειδικότερα στην παράγραφο 1 αναφέρεται ότι τα κράτη μέλη, οι εποπτικές αρχές, το Συμβούλιο Προστασίας Δεδομένων και η Ευρωπαϊκή Επιτροπή παροτρύνουν, ιδίως σε επίπεδο Ευρωπαϊκής Ένωσης, τη θέσπιση μηχανισμών πιστοποίησης προστασίας δεδομένων και σφραγίδων και σημάτων προστασίας δεδομένων προς αυτή την κατεύθυνση. Στο σημείο αυτό διευκρινίζεται ότι η πιστοποίηση με βάση το άρθρο 42 του ΓΚΠΔ σε καμία περίπτωση δεν περιορίζει την ευθύνη του Υπευθύνου επεξεργασίας ή του Εκτελούντος την επεξεργασία σχετικά με την συμμόρφωσή τους προς τον ΓΚΠΔ, τον εθνικό νόμο 4624/2019 και δεν θίγει τα καθήκοντα και τις αρμοδιότητες της εποπτικής αρχής που είναι αρμόδια σύμφωνα με το άρθρο 55 ή 56.

Η πιστοποίηση δύναται να χορηγηθεί είτε από διαπιστευμένο φορέα πιστοποίησης όπως αναφέρεται στο άρθρο 43, ο οποίος θα κατέχει και την ανάλογη εμπειρία και τεχνογνωσία σε θέματα προστασίας και ασφάλειας δεδομένων, είτε από αρμόδια εποπτική αρχή, με βάση τα κριτήρια που έχει εγκρίνει δυνάμει του άρθρου 58 παράγραφος 3, είτε από το Συμβούλιο

Προστασίας Δεδομένων. Η τελευταία περίπτωση οδηγεί σε κοινή πιστοποίηση, την Ευρωπαϊκή Σφραγίδα Προστασίας των Δεδομένων.

Σύμφωνα με το άρθρο 42 η πιστοποίηση αναφέρεται στην επιβεβαίωση τρίτου μέρους, που μπορεί να είναι και κάποιος φορέας πιστοποίησης. Συγκεκριμένα, η πιστοποίηση συνεπάγεται την παροχή αξιολόγησης και αμερόληπτης βεβαίωσης τρίτου ότι έχει αποδειχθεί η εκπλήρωση συγκεκριμένων απαιτήσεων, που στην περίπτωση της προστασίας των προσωπικών δεδομένων ο ΓΚΠΔ παρέχει το κανονιστικό πλαίσιο ως βάση αξιολόγησης αυτών. Αυτοί οι φορείς πιστοποίησης εκτός από την αποδεδειγμένη εμπειρογνωμοσύνη τους, σε σχέση με την προστασία των δεδομένων και την ασφάλεια των πληροφοριών, θα πρέπει να είναι διαπιστευμένοι. Ο ΓΚΠΔ, με βάση το άρθρο 43, επιτρέπει στα κράτη μέλη να επιλέξουν το μοντέλο διαπίστευσης που θα ακολουθήσουν, επιλέγοντας ένα από τα παρακάτω:

1) Διαπίστευση από την εποπτική αρχή που είναι αρμόδια δυνάμει των άρθρων 55 ή 56, που στην περίπτωση της Ελλάδας είναι η Αρχή Προστασίας Προσωπικών Δεδομένων (ΑΠΔΠΧ),

2) Διαπίστευση από τον εθνικό οργανισμό διαπίστευσης που ορίζεται σύμφωνα με τον κανονισμό (ΕΚ) αριθ. 765/2008 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[5], σύμφωνα με το πρότυπο EN-ISO/IEC 17065/2012 και σύμφωνα με τις συμπληρωματικές απαιτήσεις που έχουν οριστεί από την εποπτική αρχή που είναι αρμόδια δυνάμει του άρθρου 55 ή 56.

3) Διαπίστευση με συνδυασμό των (1) και (2), δηλαδή με συνεργασία της εποπτικής αρχής και του εθνικού οργανισμού διαπίστευσης.

2.1. Σκοπός – Ανάγκη Πιστοποίησης

Σκοπός της πιστοποίησης, όπως αυτή περιγράφεται στα άρθρα 42 και 43 του ΓΚΠΔ, είναι η απόδειξη της συμμόρφωσης προς τον ΓΚΠΔ των πράξεων επεξεργασίας από τους Υπευθύνους επεξεργασίας και τους Εκτελούντες την επεξεργασία είτε αυτοί υπόκεινται στον ΓΚΠΔ είτε όχι. Αυτό σημαίνει ότι οι μηχανισμοί πιστοποίησης της προστασίας δεδομένων και οι σφραγίδες και τα σήματα προστασίας δεδομένων που εγκρίνονται βάσει της παραγράφου 5 του άρθρου 42, μπορούν να θεσπίζονται και για τον σκοπό της απόδειξης ότι παρέχονται κατάλληλες εγγυήσεις

[5] Κανονισμός (ΕΚ) αριθ. 765/2008 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 9ης Ιουλίου 2008, για τον καθορισμό των απαιτήσεων διαπίστευσης και εποπτείας της αγοράς όσον αφορά την εμπορία των προϊόντων και για την κατάργηση του κανονισμού (ΕΟΚ) αριθ. 339/93 του Συμβουλίου (ΕΕ L 218 της 13.8.2008, σ. 30)

από τους Υπευθύνους επεξεργασίας και τους Εκτελούντες την επεξεργασία που δεν υπόκεινται στον ΓΚΠΔ, σύμφωνα με το άρθρο 3, στο πλαίσιο των διαβιβάσεων δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες ή διεθνείς οργανισμούς, σύμφωνα με τους όρους που αναφέρονται στο άρθρο 46 παράγραφος 2 στοιχείο στ[6].

Επιπρόσθετα, η πιστοποίηση μπορεί να ικανοποιήσει και την ανάγκη των υποκειμένων των δεδομένων, των οποίων τα δεδομένα συλλέγονται και επεξεργάζονται, για γρήγορη και αξιόπιστη αξιολόγηση του επιπέδου προστασίας των δεδομένων και των υπηρεσιών επεξεργασίας που παρέχουν οι Υπεύθυνοι επεξεργασίας και οι Εκτελούντες την επεξεργασία. Αυτό συμβάλλει και στην ενίσχυση της διαφάνειας των εργασιών επεξεργασίας των δεδομένων σύμφωνα και με την αιτιολογική σκέψη (100) η οποία εκφράζει την παρότρυνση για θέσπιση μηχανισμών πιστοποίησης και σφραγίδων και σημάτων προστασίας των δεδομένων, όπως αναφέρεται στο άρθρο 42 παράγραφος 1.

Σε άμεση συνάρτηση με τα παραπάνω, σκοπός των μηχανισμών πιστοποίησης αποτελεί και η διευκόλυνση της μετάβασης από «την εκ των προτέρων στην εκ των υστέρων» προσέγγιση εφαρμογής, που είχε υιοθετήσει το προηγούμενο σύστημα προστασίας δεδομένων, προς ένα σύστημα υπευθυνότητας και ισχυρότερης εφαρμογής που είναι η προσέγγιση του ΓΚΠΔ.

Επιπλέον, σύμφωνα και με τις κατευθυντήριες γραμμές 1/2018[7], οι εγκεκριμένοι μηχανισμοί πιστοποίησης μπορούν να χρησιμοποιηθούν ως στοιχείο που αποδεικνύει τη συμμόρφωση με τις υποχρεώσεις των Υπευθύνων επεξεργασίας και των Εκτελούντων της επεξεργασίας αναφορικά με:

- την εφαρμογή και την απόδειξη κατάλληλων τεχνικών και οργανωτικών μέτρων (άρθρο 24 παράγραφος 1 και 3, άρθρο 25, άρθρο 32 παράγραφος 1 και 3).
- τις επαρκείς διαβεβαιώσεις (άρθρο 28 παράγραφος 1), του Εκτελούντος την επεξεργασία προς τον Υπεύθυνο επεξεργασίας.
- τις επαρκείς διαβεβαιώσεις (άρθρο 28 παράγραφος 4), του άλλου Εκτελούντος την επεξεργασία προς τον Εκτελούντα την επεξεργασία, που αφορά τις περιπτώσεις που ο

[6] 2. Οι κατάλληλες εγγυήσεις που αναφέρονται στην παράγραφο 1 μπορούν να προβλέπονται, χωρίς να απαιτείται ειδική άδεια εποπτικής αρχής, μέσω: … στ) εγκεκριμένου μηχανισμού πιστοποίησης, σύμφωνα με το άρθρο 42, από κοινού με δεσμευτικές και εκτελεστές υποχρεώσεις του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία στην τρίτη χώρα να εφαρμόζει τις κατάλληλες εγγυήσεις, μεταξύ άλλων όσον αφορά τα δικαιώματα των υποκειμένων των δεδομένων

[7] Κατευθυντήριες γραμμές 1/2018 σχετικά με την πιστοποίηση και τον προσδιορισμό κριτηρίων πιστοποίησης σύμφωνα με τα άρθρα 42 και 43 του κανονισμού 2016/679 (έκδοση 3 – 04/06/2019)

Εκτελών την επεξεργασία αναθέτει την επεξεργασία των δεδομένων, είτε μέρος αυτών είτε στο σύνολό τους, σε άλλο Εκτελούντα.

2.2. Πλεονεκτήματα Πιστοποίησης

Η διαδικασία πιστοποίησης μπορεί να αποτελέσει χρήσιμο τεστ για τους Υπευθύνους επεξεργασίας και τους Εκτελούντες την επεξεργασία με το οποίο θα μπορούν πιο εύκολα και αποτελεσματικά να ελέγξουν τη συμμόρφωσή τους, ιδίως στην αρχική φάση του νέου ρυθμιστικού πλαισίου, όπου οι Υπεύθυνοι επεξεργασίας και οι Εκτελούντες θα αντιμετωπίσουν και θα πρέπει να προσαρμοστούν σε ένα νέο νομικό περιβάλλον, παρέχοντάς τους περισσότερη βεβαιότητα για το επίπεδο συμμόρφωσης προς τον ΓΚΠΔ.

Επιπρόσθετα, προσφέρει ένα σημαντικό ανταγωνιστικό πλεονέκτημα τόσο στις εταιρείες παραγωγής λογισμικού, το οποίο υλοποιεί επεξεργασία δεδομένων με τέτοιο τρόπο ώστε να υφίσταται συμμόρφωση με τις απαιτήσεις του ΓΚΠΔ, πχ: προστασία δεδομένων από τον σχεδιασμό και εξ' ορισμού – άρθρο 25, όσο και στις εταιρείες που χρησιμοποιούν τέτοιου είδους τεχνολογικά εργαλεία για την επεξεργασία δεδομένων.

Ένα άλλο ακόμη πλεονέκτημα της πιστοποίησης προστασίας δεδομένων και σφραγίδων και σημάτων προστασίας δεδομένων, είναι ότι θα μπορούσαν να χρησιμοποιηθούν ως μία αρχική ένδειξη – απόδειξη, είτε προς το υποκείμενο των δεδομένων είτε προς ένα οργανισμό, που πρόκειται να αναθέσει την επεξεργασία δεδομένων προς έναν άλλο οργανισμό, ότι ο τελευταίος έχει προβεί στις απαιτούμενες ενέργειες για την αρχική συμμόρφωσή του, αλλά και τη διατήρηση αυτής προς τον ΓΚΠΔ. Ταυτόχρονα, θα μπορούσε να αποτελεί ένα σημαντικό κριτήριο επιλογής – μέτρο σύγκρισης μεταξύ των διάφορων Υπευθύνων Επεξεργασίας δεδομένων ή / και των διαφόρων Εκτελούντων την επεξεργασία, είτε στο πλαίσιο της αξιολόγησης και κατάταξης αυτών είτε στο πλαίσιο σύναψης συνεργασίας ή ανάθεσης έργου σχετικών με την επεξεργασία δεδομένων και την προστασία αυτών.

Εκτός από τα παραπάνω, η πιστοποίηση προσφέρει σημαντικά και στην εύρεση, αξιολόγηση και έλεγχο του βαθμού συμμόρφωσης ενός Εκτελούντα την επεξεργασία που δεν ανήκει στην Ευρωπαϊκή Ένωση και συνεπώς δεν υπόκεινται στον ΓΚΠΔ. Συνεπώς, αποτελεί κατάλληλο μέσο για ασφαλέστερη και ευκολότερη διαβίβαση των προς επεξεργασία δεδομένων σε οργανισμό που εδρεύει σε τρίτη χώρα. Η πιστοποίηση σε τέτοιους οργανισμούς θα είναι μια αξιοσημείωτη πρώτη ένδειξη - απόδειξη συμμόρφωσης προς τον ΓΚΠΔ.

Δεδομένου της υποχρεωτικής συμμόρφωσης για όλους του οργανισμούς των Κρατών Μελών, αλλά και για εκείνους που είναι εγκατεστημένοι εκτός Ευρωπαϊκής Ένωσης και οι οποίοι λειτουργούν εντός αυτής, προς τον ΓΚΠΔ, καθώς επίσης και των εξαιρετικά υψηλών κυρώσεων, που ειδικά για τους Μικρούς και Μεσαίους Οργανισμούς θα μπορούσαμε να τις χαρακτηρίσουμε και ως «εξοντωτικές», η βιωσιμότητα αυτών των οργανισμών, εξαρτάται, μακροπρόθεσμα, από τον βαθμό συμμόρφωσή τους προς τον ΓΚΠΔ. Στην υιοθέτηση, διατήρηση και συνεχή βελτίωση ενός υψηλού επιπέδου συμμόρφωσης προς τον ΓΚΠΔ συμβάλλει και η πιστοποίηση των οργανισμών που έχουν το ρόλο του Υπευθύνου Επεξεργασίας δεδομένων ή/και του Εκτελούντα την επεξεργασία, για την αύξηση του οποίου ένα σημαντικό μέτρο αποτελεί και η πιστοποίησή τους.

Στη συνέχεια, λαμβάνοντας υπόψη ότι ο ΓΚΠΔ επιβάλλει την ύπαρξη των κατάλληλων διαδικασιών σε κάθε οργανισμό για την προστασία των δεδομένων και την διασφάλιση των δικαιωμάτων των φυσικών προσώπων καθώς και την απόδειξη της συμμόρφωσης τους, αποτελεί ξεκάθαρο γεγονός ότι εισάγει την αρχή της λογοδοσίας αφού πλέον μεταφέρει το βάρος για την απόδειξη της συμμόρφωσης από τον ρυθμιστή / ελεγκτή στον ρυθμιζόμενο / ελεγχόμενο. Αυτό συνεπάγεται ότι οι Υπεύθυνοι Επεξεργασίας δεδομένων και οι Εκτελούντες την επεξεργασία είναι εκείνοι που πρέπει να είναι σε θέση να αποδείξουν ότι έχουν λάβει όλα τα απαραίτητα μέτρα για την προστασία των προσωπικών δεδομένων, με την εποπτική Αρχή να αναλαμβάνει ρόλο και δράση σε δεύτερο χρόνο. Τα παραπάνω και σε συνδυασμό με το γεγονός ότι δεν υπάρχει προηγούμενη εμπειρία σε σχέση με αντίστοιχες απαιτήσεις συμμόρφωσης, εργαλεία που πρέπει να χρησιμοποιηθούν, ενέργειες που χρειάζεται να γίνουν προς την κατεύθυνση της συμμόρφωσης, αυξάνουν σε μεγάλο βαθμό τον κίνδυνο να συμβεί περιστατικό που να παραβιάζει την προστασία των δεδομένων, αναδεικνύοντας και τα κενά στο δομημένο σύστημα προστασίας των δεδομένων που εφαρμόζουν, και κατά συνέπεια οι οργανισμοί αυτοί να βρεθούν αντιμέτωποι με προσφυγές Φυσικών προσώπων. Στο σημείο αυτό η διαδικασία της πιστοποίησης, που περιλαμβάνει την επιθεώρηση, τον έλεγχο των οργανισμών καθώς και την τακτική επιτήρηση τους, διασφαλίζει σε αρκετά μεγάλο βαθμό την υψηλού επιπέδου συμμόρφωση του οργανισμού στις απαιτήσεις του ΓΚΠΔ καθώς και την εφαρμογή των κατάλληλων μέτρων προσαρμογής του προς αυτή την κατεύθυνση, σύμφωνα με το αντικείμενο του οργανισμού που αφορά την επεξεργασία των δεδομένων.

2.3. Μηχανισμός Πιστοποίησης

Ο ΓΚΠΔ δεν ορίζει τους «μηχανισμούς πιστοποίησης, τις σφραγίδες ή τα σήματα» και χρησιμοποιεί τους όρους συλλογικά. Χαρακτηριστικά παρουσιάζει το πλαίσιο στο οποίο μπορούν να χρησιμοποιηθούν εγκεκριμένοι μηχανισμοί πιστοποίησης ως στοιχείο που αποδεικνύει τη συμμόρφωση με τις υποχρεώσεις των Υπευθύνων επεξεργασίας και των Εκτελούντων την επεξεργασία σχετικά με:

- την εφαρμογή και την απόδειξη κατάλληλων τεχνικών και οργανωτικών μέτρων όπως αναφέρεται στο άρθρο 24 παράγραφοι 1 και 3, στο άρθρο 25 και στο άρθρο 32 παράγραφοι 1 και 3
- τις επαρκείς διαβεβαιώσεις που αναφέρονται στο άρθρο 28 παράγραφος 1 (ο Εκτελών την επεξεργασία στον Υπεύθυνο επεξεργασίας) και παράγραφος 4 (ο άλλος Εκτελών την επεξεργασία στον Εκτελούντα την επεξεργασία)

Το πιστοποιητικό είναι μια δήλωση συμμόρφωσης. Η απόδειξη της συμμόρφωσης απαιτεί δικαιολογητικά έγγραφα, ειδικότερα γραπτές εκθέσεις που όχι μόνο επαναλαμβάνουν, αλλά περιγράφουν πώς πληρούνται τα κριτήρια και, αν δεν πληρούνταν αρχικά, περιγράφουν τις διορθώσεις, τις διορθωτικές δράσεις και την καταλληλότητά τους, παρέχοντας έτσι τους λόγους χορήγησης και διατήρησης της πιστοποίησης. Αυτό περιλαμβάνει την περιγραφή κάθε απόφασης χορήγησης, ανανέωσης ή ανάκλησης πιστοποιητικού και κατ' επέκταση θα πρέπει να παρέχει τους λόγους, τα επιχειρήματα και τις αποδείξεις που προκύπτουν από την εφαρμογή των κριτηρίων, καθώς και τα συμπεράσματα, τις αποφάσεις ή τα συμπερασματικά στοιχεία από πραγματικά περιστατικά ή παραδοχές που συγκεντρώθηκαν κατά τη διάρκεια της πιστοποίησης.

Η σφραγίδα ή το σήμα μπορούν να χρησιμοποιηθούν για να σημάνουν την επιτυχή ολοκλήρωση της διαδικασίας πιστοποίησης. Η σφραγίδα ή το σήμα αναφέρονται συνήθως στο λογότυπο ή στο σύμβολο του οποίου η παρουσία (επιπλέον του πιστοποιητικού) υποδεικνύει ότι το αντικείμενο της πιστοποίησης έχει αξιολογηθεί ανεξάρτητα στο πλαίσιο διαδικασίας πιστοποίησης και συμμορφώνεται με συγκεκριμένες απαιτήσεις που αναφέρονται σε κανονιστικά έγγραφα όπως κανονισμούς, πρότυπα ή τεχνικές προδιαγραφές. Οι απαιτήσεις αυτές, στο πλαίσιο της πιστοποίησης σύμφωνα με τον ΓΚΠΔ, περιέχονται στις πρόσθετες απαιτήσεις που συμπληρώνουν τους κανόνες διαπίστευσης των φορέων πιστοποίησης στο πρότυπο EN-ISO/IEC 17065/2012 και στα κριτήρια πιστοποίησης που έχει εγκρίνει η αρμόδια εποπτική αρχή ή το Συμβούλιο Προστασίας Δεδομένων.

Οι μηχανισμοί πιστοποίησης, συμπεριλαμβανομένων των σφραγίδων και των σημάτων προστασίας δεδομένων, όπως περιγράφονται στα άρθρα 42 και 43, μπορούν να θεωρηθούν ως πιστοποίηση προσανατολισμένη στο στόχο, σε αντίθεση με τις πιστοποιήσεις βάσει των προτύπων διαχείρισης, όπως το ISO / IEC 27001, EN ISO 9001 κλπ, που μπορεί να στοχεύουν είτε σε μια συγκεκριμένη επιχειρηματική διαδικασία, είτε σε μία συγκεκριμένη υπηρεσία είτε σε στο σύνολο των επιχειρηματικών διαδικασιών ενός οργανισμού. Συνεπώς, το επίκεντρο της πιστοποίησης στον ΓΚΠΔ δεν αφορά μόνο τη θέσπιση απαιτούμενων μέτρων, αλλά και σε ποιο βαθμό τα μέτρα αυτά επαρκούν για τη διασφάλιση της συμμόρφωσης.

Σύμφωνα με την ορολογία που έχει προταθεί από τον ISO και την IEC, μια απαίτηση πιστοποίησης αποτελεί απαίτηση «που εκπληρώνει ο πελάτης ως προϋπόθεση για την καθιέρωση ή τη διατήρηση της πιστοποίησης». Ο όρος απαίτηση περιλαμβάνει τόσο τις ουσιαστικές απαιτήσεις (που και αλλιώς ονομάζονται απαιτήσεις προϊόντος / διεργασίας / ατόμου) όσο και τις διαδικαστικές απαιτήσεις. Οι ουσιαστικές απαιτήσεις απορρέουν από την κανονιστική βάση. Στην περίπτωση του ΓΚΠΔ τα δικαιώματα των υποκειμένων στα οποία αναφέρονται τα δεδομένα (άρθρα 15 – 22), η ασφάλεια δεδομένων (άρθρο 32), η προστασία δεδομένων από το σχεδιασμό (άρθρο 25 παράγραφος 1) και από προεπιλογή (άρθρο 25 παράγραφος 2) , για παράδειγμα, αποτελούν μια κανονιστική βάση που μπορεί περαιτέρω να προσδιοριστεί σε ουσιαστικές απαιτήσεις πιστοποίησης. Οι διαδικαστικές απαιτήσεις αποτελούν, επίσης, μέρος ενός συστήματος πιστοποίησης και πρέπει να πληρούνται από το μέρος που ζητεί πιστοποίηση. Τέτοιες διαδικαστικές απαιτήσεις θα διευκρινίζουν, για παράδειγμα, υπό ποιες προϋποθέσεις ο Υπεύθυνος επεξεργασίας μπορεί να χρησιμοποιήσει το αποκτηθέν πιστοποιητικό, ποιες είναι οι περίοδοι επιτήρησης και διάφορες άλλες. Ορισμένες από τις διαδικαστικές πτυχές διευκρινίζονται ήδη από τον ΓΚΠΔ, όπως το χρονικό διάστημα ισχύος της πιστοποίησης, που είναι τρία έτη (άρθρο 42 παράγραφος 7).

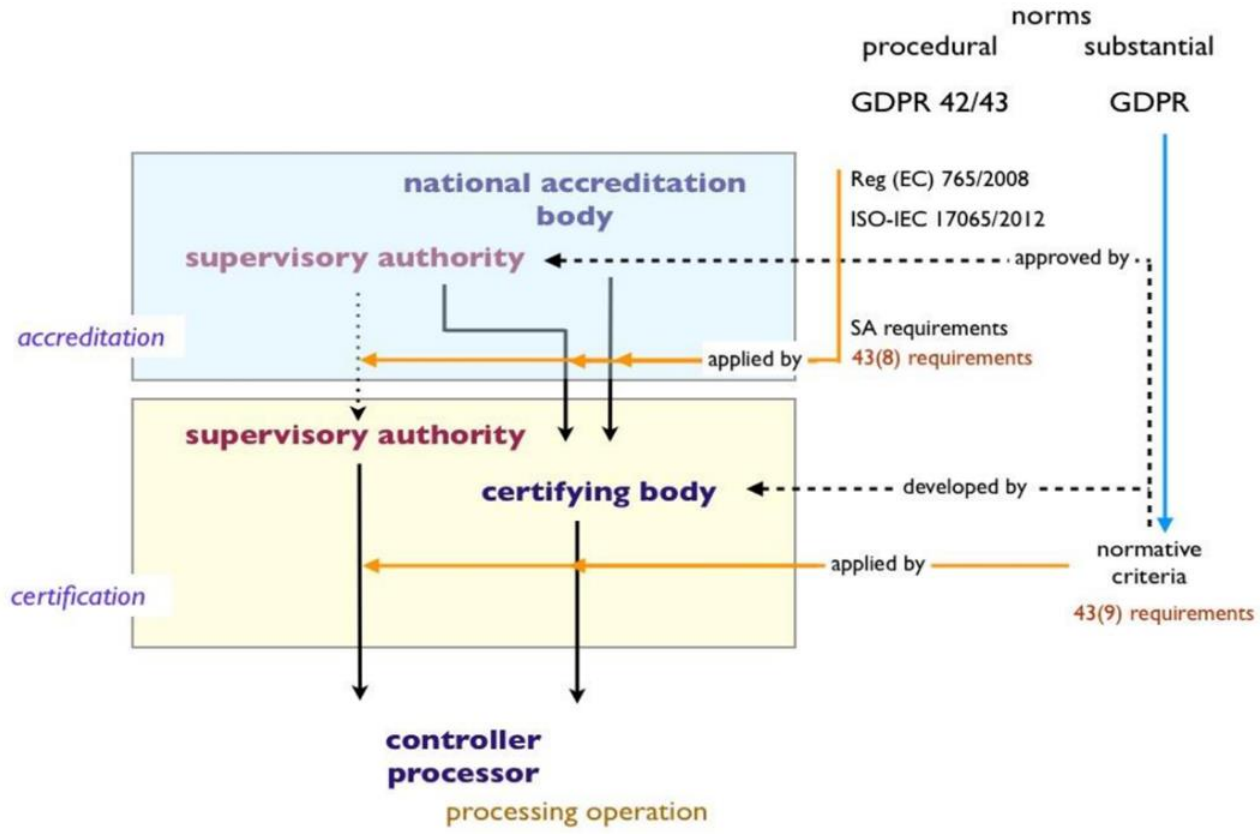
Γενικά ένας μηχανισμός πιστοποίησης θα πρέπει να περιλαμβάνει :

- Διαφανείς διαδικασίες και διαφάνεια σχετικά με το κόστος του συστήματος πιστοποίησης.
- Περιληπτικές αναφορές για τις πιστοποιήσεις που θα πρέπει να είναι προσβάσιμες από όλους.
- Δημοσιοποίηση των κριτηρίων, των απαιτήσεων και των μεθόδων αξιολόγησης.
- Επιτόπιες επιθεωρήσεις σε συνδυασμό με ανασκοπήσεις τεκμηρίωσης.

- Τακτικές επιτηρήσεις μετά την πιστοποίηση καθώς και επικαιροποίηση πιστοποίησης (επιθεώρηση επαναπιστοποίησης), όταν κρίνεται απαραίτητη.
- Διαφανή μηχανισμό παραπόνων – καταγγελιών.
- Ικανότητες - αρμοδιότητες επιθεωρητών / ελεγκτών.

Τα κριτήρια αποτελούν αναπόσπαστο μέρος του μηχανισμού πιστοποίησης και μπορεί να βασίζονται είτε σε τεχνικά πρότυπα είτε σε νόμους. Στη δεύτερη περίπτωση θα χρειαστεί να γίνει κατάλληλη διαμόρφωση των νομικών απαιτήσεων σε κριτήρια συμμόρφωσης. Σύμφωνα με το ΓΚΠΔ τα κριτήρια πιστοποίησης μπορούν να καθοριστούν είτε από τον διαπιστευμένο φορέα πιστοποίησης με την προϋπόθεση ότι πρώτα αυτά θα έχουν εγκριθεί από την αρμόδια εποπτεύουσα αρχή είτε από την ίδια την εποπτεύουσα αρχή.

Όπως περιγράφεται από τον ΓΚΠΔ, μια επισκόπηση της πιστοποίησης σύμφωνα με τα άρθρα 42 και 43 αποτελεί η παρακάτω εικόνα:



Εικ.1. Επισκόπηση πιστοποίησης με βάση τα άρθρα 42 και 43 του ΓΚΠΔ[8]

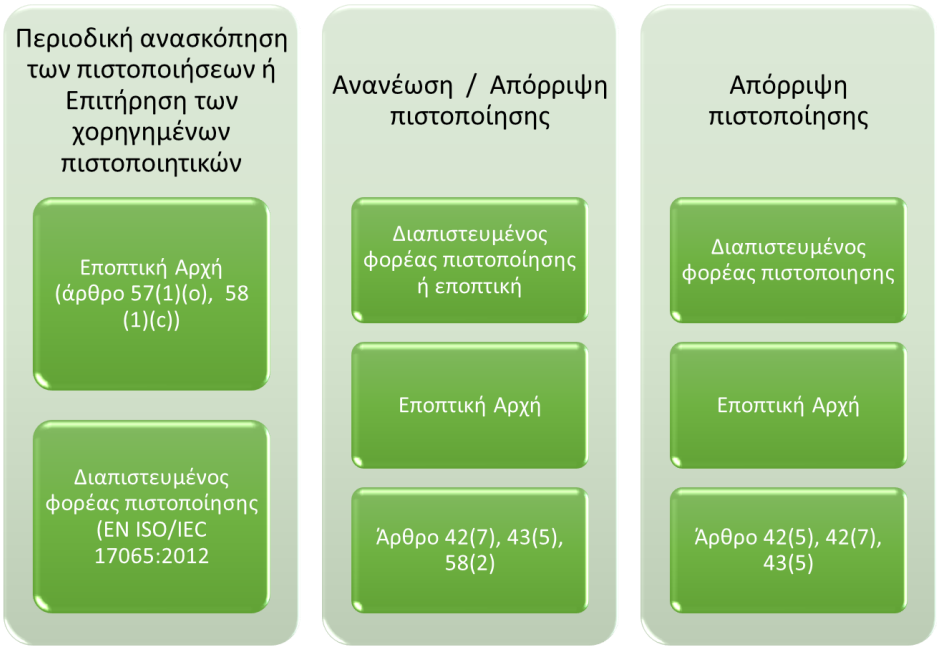
[8] Data Protection Certification Mechanisms - Study on Articles 42 and 43 of the Regulation (EU) 2016/679 - Final Report - (Authors: Irene Kamara, Ronald Leenes, Eric Lachaud, Kees Stuurman (TILT), Marc van Lieshout, Gabriela Bodea (TNO))

Σύμφωνα με το παραπάνω οι εθνικοί οργανισμοί διαπίστευσης εκτελούν τις δραστηριότητές τους σύμφωνα με το πρότυπο EN-ISO / IEC 17065:2012, τον κανονισμό (ΕΚ) 765/2008 και τις πρόσθετες απαιτήσεις που καθορίζονται από την αρμόδια εποπτική αρχή, ενώ οι εποπτικές αρχές θα ασκήσουν τις δραστηριότητές τους ως φορείς διαπίστευσης βάσει των απαιτήσεων που καθορίζονται από τις ίδιες.

Η διαδικασία πιστοποίησης διεξάγεται είτε από διαπιστευμένο φορέα πιστοποίησης είτε από εποπτική αρχή. Ο ΓΚΠΔ δεν προβλέπει όρους για τις εποπτικές αρχές που ενεργούν ως φορείς πιστοποίησης. Η επιλογή αφήνεται ανοιχτή στα κράτη μέλη για να προσδιορίσουν το μοντέλο που ταιριάζει καλύτερα στις εθνικές τους ανάγκες στην αγορά. Όταν ανατίθεται σε έναν φορέα πιστοποίησης η εξουσία πιστοποίησης σύμφωνα με το άρθρο 42, η αρχή προστασίας δεδομένων έχει εποπτικό ρόλο με ενισχυμένες εξουσίες για ανάκληση πιστοποιητικών ή για εντολή προς τον οργανισμό πιστοποίησης να μην εκδώσει πιστοποίηση.

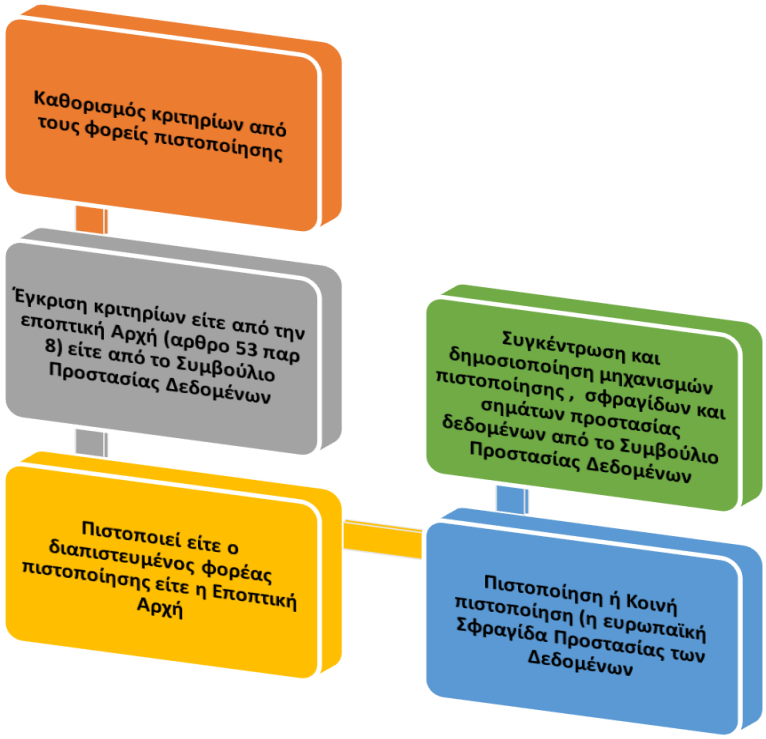
Επίσης, ο ΓΚΠΔ παρέχει την ανάπτυξη μιας κοινής πιστοποίησης, η οποία λειτουργεί παράλληλα με τις εθνικές ή διακρατικές πιστοποιήσεις εντός της Ευρωπαϊκής Ένωσης. Η κοινή πιστοποίηση, που ονομάζεται Ευρωπαϊκή Σφραγίδα Προστασίας Δεδομένων, απαιτεί ένα σύνολο κριτηρίων εγκεκριμένων από το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων.

Συνοπτικά τα στάδια πιστοποίησης, μαζί με τους αρμόδιους που συμμετέχουν και τα σχετικά άρθρα, όπως αυτά περιγράφονται στον ΓΚΠΔ είναι τα παρακάτω:



Εικ.2. Επισκόπηση των σταδίων πιστοποίησης με βάση τα άρθρα 42 και 43 του ΓΚΠΔ[9]

Τα βήματα σχετικά με τη διαδικασία θέσπισης πιστοποίησης προστασίας δεδομένων, σύμφωνα με το άρθρο 42 του ΓΚΠΔ, είναι τα αναφερόμενα στην παρακάτω εικόνα:



Εικ.3. Βήματα διαδικασίας θέσπισης πιστοποίησης (άρθρο 42 ΓΚΠΔ)

[9] Data Protection Certification Mechanisms - Study on Articles 42 and 43 of the Regulation (EU) 2016/679 - Final Report - (Authors: Irene Kamara, Ronald Leenes, Eric Lachaud, Kees Stuurman (TILT), Marc van Lieshout, Gabriela Bodea (TNO))

Έγκριση κριτηρίων και έκδοση πιστοποίησης

Η πιστοποίηση εκδίδεται είτε από την Αρμόδια Εποπτική Αρχή, η οποία έχει και την εξουσία να την αποσύρει, είτε από διαπιστευμένο φορέα πιστοποίησης. Στην δεύτερη περίπτωση η Εποπτική Αρχή έχει την διορθωτική εξουσία να διατάξει τον φορέα πιστοποίησης είτε να αποσύρει πιστοποίηση, που έχει εκδώσει με βάση τα άρθρα 42 και 43, είτε να μην εκδώσει πιστοποίηση στην περίπτωση που δεν ικανοποιήθηκαν οι απαιτήσεις ή δεν ικανοποιούνται πλέον. Γενικά πιστοποιητικό, σφραγίδα ή σήμα σύμφωνα με τον ΓΚΠΔ μπορεί να χορηγηθεί μόνο κατόπιν της ανεξάρτητης αξιολόγησης των αποδείξεων από διαπιστευμένο φορέα πιστοποίησης ή από την αρμόδια εποπτική αρχή, που θα αναφέρει ότι τα κριτήρια πιστοποίησης έχουν εκπληρωθεί.

Προκειμένου να εγκριθεί ή να επανεξεταστεί ένα μηχανισμός πιστοποίησης, με βάση τα άρθρα 42 και 43 του ΓΚΠΔ, προηγείται η έγκριση των κριτηρίων πιστοποίησης, η βάση των οποίων πρέπει να προέρχεται από τις αρχές και τους κανόνες του ΓΚΠΔ και να βοηθά στην παροχή βεβαιότητας ότι τα κριτήρια αυτά πληρούνται. Η έγκριση αυτή δίνεται είτε από την αρμόδια εποπτική αρχή είτε από το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων.

Έγκριση απαιτείται επίσης και για επικαιροποιημένα ή πρόσθετα συστήματα ή σύνολα κριτηρίων σύμφωνα με το πρότυπο ISO 17065 από τον ίδιο φορέα πιστοποίησης πριν από τη χρήση των τροποποιημένων μηχανισμών πιστοποίησης (άρθρο 42 παράγραφος 5 και άρθρο 43 παράγραφος 2 στοιχείο β).

Οι εποπτικές αρχές θα πρέπει να αντιμετωπίζουν όλα τα αιτήματα έγκρισης κριτηρίων πιστοποίησης με δίκαιο τρόπο και χωρίς διακρίσεις, σύμφωνα με μια δημόσια διαθέσιμη διαδικασία η οποία θα προσδιορίζει τις γενικές προϋποθέσεις που πρέπει να πληρούνται και θα περιγράφει τη διαδικασία έγκρισης.

Στην περίπτωση αυτή, των εποπτικών αρχών, χρειάζεται να γίνει έλεγχος για το αν είναι αρμόδια η εποπτική αρχή στην οποία έχουν κατατεθεί τα κριτήρια αυτά. Ο έλεγχος αυτός περιλαμβάνει τόσο την εδαφική – γεωγραφική αρμοδιότητα όσο και την ουσιαστική.

Σε εθνικού επιπέδου πιστοποίηση αρμόδια είναι η εθνική εποπτική αρχή. Σε πιστοποίηση επιπέδου Ευρωπαϊκής Ένωσης αρμόδιο είναι το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. Σε επίπεδο διακρατικής πιστοποίησης, που αφορά πιστοποίηση σε περισσότερα από ένα Κράτη Μέλη αλλά όχι για όλα, χρειάζεται να καθοριστεί ποια είναι η επικεφαλής εποπτική αρχή και σε

συνεργασία με τις άλλες ενδιαφερόμενες εποπτικές αρχές να προβεί στην έγκριση ή αναθεώρηση των κριτηρίων πιστοποίησης.

Εκτός από την εδαφική αρμοδιότητα, χρειάζεται να εξεταστεί και η ουσιαστική αρμοδιότητα της εποπτικής αρχής, η οποία αφορά τόσο στις απαιτήσεις, στο σύνολό τους, και το πεδίο εφαρμογής του ΓΚΠΔ όσο και στο πεδίο εφαρμογής της πιστοποίησης για την προστασία των δεδομένων σύμφωνα με τα άρθρα 42 και 43. Οι πιστοποιήσεις μπορεί να βασίζονται σε περισσότερες από μία κανονιστικές πηγές. Οι πηγές αυτές μπορεί να αποτελούν είτε νομικά μέσα είτε μη νομικά μέσα, όπως είναι τα τεχνικά πρότυπα. Στην περίπτωση των κριτηρίων που σχετίζονται με τον ΓΚΠΔ και των μη νομικών μέσων, ο σκοπός της πιστοποίησης είναι καθοριστικός για τον προσδιορισμό της αρμοδιότητας της εποπτικής αρχής. Παρόλο που η εποπτική αρχή δεν είναι εξουσιοδοτημένη αλλά ούτε και αρμόδια να αναθεωρεί κριτήρια πιστοποίησης με βάση τα τεχνικά πρότυπα, θα πρέπει να το πράξει εάν ο σκοπός της υπό έγκρισης πιστοποίησης είναι να αποδείξει τη συμμόρφωση προς τον ΓΚΠΔ με βάση τα άρθρα 42 και 43. Συνεπώς, τα πρότυπα ως κανονιστική πηγή τέτοιων πιστοποιήσεων θα πρέπει να θεωρούνται ως μέσο επίτευξης ενός στόχου (ανάπτυξη κριτηρίων που αντιστοιχούν στις υποχρεώσεις ΓΚΠΔ) και επομένως να εμπίπτουν στην αρμοδιότητα της εκάστοτε εποπτικής αρχής.

Στην περίπτωση που η πιστοποίηση βασίζεται σε πολλαπλά νομικά μέσα, η εποπτική αρχή είναι αρμόδια μόνο για το τμήμα που σχετίζεται με τον ΓΚΠΔ. Ακόμη και σε αυτές τι περιπτώσεις, ο σκοπός της πιστοποίησης αποτελεί σημαντικό παράγοντας. Αν ο σκοπός αυτός είναι να αποδειχθεί η συμμόρφωση προς τις απαιτήσεις του ΓΚΠΔ και τα πρόσθετα νομικά μέσα συντελούν στην ενίσχυση των κριτηρίων, τότε η εποπτική αρχή είναι αρμόδια για την έγκριση των κριτηρίων. Στην περίπτωση, όμως, που ο σκοπός είναι η παροχή μιας συνδυασμένης πιστοποίησης αποδεικνύοντας συμμόρφωση βάσει του ΓΚΠΔ αλλά και πρόσθετων κανονισμών, στους οποίους η εποπτική αρχή δεν είναι αρμόδια, τότε ο ρόλος περιορίζεται μόνο στο τμήμα που αφορά τον ΓΚΠΔ. Σε κάθε περίπτωση η εποπτική αρχή θα πρέπει να είναι σε θέση να συνεργαστεί και με άλλες αρμόδιες αρχές προκειμένου να εξασφαλιστεί ενότητα και συνέπεια τόσο των διαδικασιών όσο και των αποτελεσμάτων.

Σε όλα τα παραπάνω προστίθεται και το γεγονός ότι ο ΓΚΠΔ προβλέπει συγκεκριμένες προϋποθέσεις σχετικά με τους μηχανισμούς πιστοποίησης της προστασίας δεδομένων. Ακόμα και στην περίπτωση που η εποπτική αρχή εγκρίνει κριτήρια, η διαδικασία έγκρισης δεν μπορεί να αποσυνδεθεί από το γενικό στόχο και το πεδίο εφαρμογής του μηχανισμού πιστοποίησης

όπως αυτά ορίζονται στα άρθρα 42 και 43. Συνεπώς, η εποπτική αρχή θα πρέπει να αποδείξει ότι πληρούνται οι όροι των εν λόγω άρθρων και πιο συγκεκριμένα ότι πληρούνται σε σχέση με το αντικείμενο πιστοποίησης (δραστηριότητα επεξεργασίας), τον αιτούντα οργανισμό (Υπεύθυνο επεξεργασίας ή Εκτελούντα την επεξεργασία δεδομένων), τον εθελοντικό χαρακτήρα της προτεινόμενης πιστοποίησης, τη λειτουργία της πιστοποίησης από διαπιστευμένο οργανισμό πιστοποίησης (άρθρο 43). Επιπλέον, πρέπει να καθοριστεί και ποιο θα είναι το πεδίο πιστοποίησης (πλήρης ή σε ένα μόνο τομέα του ΓΚΠΔ / γενικό ή ειδικό) ώστε να είναι εφικτή η αξιολόγηση των προτεινόμενων κριτηρίων.

Τα κριτήρια πιστοποίησης παρέχουν τις ονομαστικές απαιτήσεις έναντι των οποίων αξιολογείται η πραγματική πράξη επεξεργασίας που ορίζεται στο αντικείμενο αξιολόγησης. Η θέσπιση τους θα πρέπει να εστιάζει στην επαληθευσιμότητα, στη βαρύτητα και στην καταλληλόλητά τους για την απόδειξη της συμμόρφωσης με τον κανονισμό. Η διατύπωση των κριτηρίων οφείλει να είναι τέτοια ώστε αυτά να είναι σαφή και κατανοητά και ταυτόχρονα να καθίσταται δυνατή η πρακτική εφαρμογή τους.

Τα παρακάτω θέματα αποτελούν σημαντική καθοδήγηση για την αξιολόγηση κριτηρίων πιστοποίησης και αποτελούν ζητήματα που από τη μία πλευρά η εποπτική αρχή προστασίας δεδομένων και το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων θα εξετάσουν και θα εφαρμόσουν για τον σκοπό της έγκρισης των κριτηρίων πιστοποίησης ενός μηχανισμού πιστοποίησης και από την άλλη θα χρειαστεί να λαμβάνονται υπόψη από τους οργανισμούς πιστοποίησης και τους ιδιοκτήτες των συστημάτων που επιθυμούν να καταρτίσουν και να υποβάλουν κριτήρια προς έγκριση.

Η ακόλουθη λίστα προφανώς και δεν είναι εξαντλητική αλλά παρουσιάζει βασικά θέματα που θα πρέπει να εξεταστούν[10].

1. Πεδίο εφαρμογής μηχανισμού πιστοποίησης και στόχος της αξιολόγησης.

   Το πεδίο εφαρμογής θα πρέπει να περιγράφεται με σαφήνεια και να αντικατοπτρίζονται σε αυτό όλες οι σχετικές πτυχές των πράξεων επεξεργασίας. Επίσης απαιτείται να διευκρινίζεται αν καλύπτει την επεξεργασία μόνο στη χώρα εφαρμογής ή καλύπτει και τη διασυνοριακή επεξεργασία ή/και τη διαβίβαση δεδομένων.

[10] Κατευθυντήριες γραμμές 1/2018 (έκδοση 3 – 04/06/2019)

Όσον αφορά τους στόχους της αξιολόγησης, τα κριτήρια που έχουν δοθεί θα πρέπει να εξασφαλίζουν ότι αυτοί είναι κατανοητοί προς τους ενδιαφερόμενους συμπεριλαμβανομένων και των υποκειμένων των δεδομένων.

2. Γενικές απαιτήσεις.

   Στο σύνολο των κριτηρίων θα πρέπει να προσδιορίζονται, επεξηγούνται και να περιγράφονται όλοι οι σχετικοί όροι καθώς και να προσδιορίζονται και οι κανονιστικές παραπομπές. Επιπλέον στα κριτήρια θα πρέπει να περιλαμβάνεται ο ορισμός των αρμοδιοτήτων, των διαδικασιών και της επεξεργασίας για την προστασία των δεδομένων που καλύπτονται από το πεδίο εφαρμογής.

3. Πράξεις Επεξεργασίας (άρθρο 42 παράγραφος 1).

   Όσον αφορά το πεδίο εφαρμογής του μηχανισμού πιστοποίησης (γενικό ή ειδικό), τα κριτήρια θα πρέπει να καλύπτουν όλα τα σχετικά στοιχεία των πράξεων επεξεργασίας (δεδομένα, συστήματα και διαδικασίες). Επιπρόσθετα τα κριτήρια χρειάζεται να προσδιορίζουν, με βάση το στόχο αξιολόγησης, όλες τις έγκυρες νομικές βάσεις της επεξεργασίας.

   Όσον αφορά το στόχο της αξιολόγησης, τα κριτήρια χρειάζεται να προσδιορίζουν τα στάδια επεξεργασίας και τον πλήρη κύκλο ζωής των δεδομένων, συμπεριλαμβανομένων της διαγραφής ή/και της ανωνυμοποίησης. Σημαντικό είναι να προσδιορίζονται ειδικές κατηγορίες δεδομένων (για παράδειγμα ιατρικά δεδομένα) καθώς επίσης και να αποτυπώνουν ειδικούς τύπους πράξεων επεξεργασίας (για παράδειγμα της αυτοματοποιημένης λήψης αποφάσεων ή της κατάρτισης προφίλ). Τέλος, χρειάζεται να λαμβάνουν επαρκώς υπόψη τους κινδύνους για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων

4. Νομιμότητα της επεξεργασίας.

   Είναι αναγκαίο να περιλαμβάνεται έλεγχος της νομιμότητας της επεξεργασίας για επιμέρους πράξεις επεξεργασίας όσον αφορά τον σκοπό και την αναγκαιότητα της επεξεργασίας καθώς επίσης και όλων των απαιτήσεων μιας νομικής βάσης για επιμέρους πράξεις επεξεργασίας.

5. Αρχές που διέπουν την επεξεργασία προσωπικών δεδομένων (άρθρο 5).

   Τα κριτήρια θα πρέπει να καλύπτουν επαρκώς όλες τις αρχές προστασίας των δεδομένων και παράλληλα να εξασφαλίζεται η ελαχιστοποίηση των δεδομένων.

6. Γενικές υποχρεώσεις των Υπευθύνων επεξεργασίας και των Εκτελούντων την επεξεργασία.

   Στα κριτήρια θα πρέπει να προσδιορίζονται οι υποχρεώσεις των Υπευθύνων και των Εκτελούντων την επεξεργασία καθώς και να απαιτούνται η επανεξέταση των τεχνικών και οργανωτικών μέτρων που έχουν ληφθεί από αυτούς. Επίσης, σε περίπτωση που ο Υπεύθυνος και ο Εκτελών την επεξεργασία είναι διαφορετικοί, στα κριτήρια θα πρέπει να γίνεται αναφορά στα αποδεικτικά στοιχεία σχετικά με την μεταξύ τους συμφωνία καθώς και στην αξιολόγηση αυτής.

   Παράλληλα τα κριτήρια θα πρέπει να συμβάλουν προς την κατεύθυνση της επαλήθευσης για το αν ο οργανισμός που θα αιτηθεί να πιστοποιηθεί από τον φορέα πιστοποίησης, έχει εκτιμήσει το κατά πόσο θα πρέπει να διαθέτει Υπεύθυνο Προστασίας Δεδομένων (σύμφωνα με τα άρθρα 37, 38 και 39)

7. Δικαιώματα των υποκειμένων των δεδομένων.

   Βασικός παράγοντας που θα πρέπει να ικανοποιείται από τα κριτήρια είναι το αν διασφαλίζεται το δικαίωμα της ενημέρωσης, πρόσβασης, ελέγχου των δεδομένων από τα αντίστοιχα υποκείμενα και των μέτρων που έχουν ληφθεί προκειμένου να ικανοποιούνται και τα δικαιώματα για διόρθωση, διαγραφή ή περιορισμό.

8. Κίνδυνοι για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων.

   Σημαντικό είναι τα κριτήρια που θα τεθούν να συμβάλλουν προς την αξιολόγηση του κινδύνου καθώς και της μεθοδολογίας που ακολουθήθηκε, για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Επιπρόσθετα, θα πρέπει να απαιτούν και την αξιολόγηση του κατά πόσο έχει διενεργηθεί εκτίμηση αντικτύπου, των πράξεων επεξεργασίας, σχετικά με την προστασία των δεδομένων.

9. Τεχνικά και οργανωτικά μέτρα που εγγυώνται την προστασία.

   Τα κριτήρια χρειάζεται να καθιστούν αναγκαία όχι μόνο την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων για τη διασφάλιση της ακεραιότητας – διαθεσιμότητας – εμπιστευτικότητας των δεδομένων, της λογοδοσίας, των δικαιωμάτων των υποκειμένων, της προστασίας εξ’ ορισμού και ήδη από τον σχεδιασμό των δεδομένων, της ελαχιστοποίησης, εφαρμογής διαδικασιών αντιμετώπισης συμβάντων και κοινοποίησης παραβίασης των δεδομένων προσωπικού χαρακτήρα, αλλά και την αξιολόγηση και επαναπροσδιορισμό αυτών.

10. Κριτήρια με σκοπό την απόδειξη της ύπαρξης κατάλληλων εγγυήσεων για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα.

    Τα κριτήρια αυτά χρειάζεται να εξασφαλίζουν ότι γίνεται αξιολόγηση των αποδεικτικών στοιχείων για τις συμβάσεις συνεργασίας καθώς και της διαδικασίας που ακολουθήθηκε προκειμένου να εξασφαλιστεί ο οργανισμός που ανήκει εκτός Ευρωπαϊκής ένωσης θα συμμορφώνεται με τις απαιτήσεις του ΓΚΠΔ.

11. Πρόσθετα κριτήρια για την Ευρωπαϊκή Σφραγίδα Προστασίας δεδομένων.

    Τα κριτήρια θα πρέπει να καλύπτουν όλα τα Κράτη Μέλη και να έχουν λάβε υπόψη την νομοθεσία τους για την προστασία δεδομένων. Τέλος θα πρέπει να απαιτούν οι πληροφορίες που θα δίνονται από τον Υπεύθυνο και των Εκτελούντα την επεξεργασία να είναι προσαρμοσμένες στη γλώσσα του κράτους μέλους που απευθύνονται.

12. Συνολική αξιολόγηση κριτηρίων.

    Τα κριτήρια θα πρέπει να καλύπτουν ολόκληρο το πεδίο εφαρμογής του μηχανισμού πιστοποίησης προκειμένου η πιστοποίηση να είναι αξιόπιστη. Επίσης, θα πρέπει να είναι κατάλληλα ώστε να ανταποκρίνονται στο εύρος και του κινδύνους της επεξεργασίας καθώς επίσης και στο είδος των δεδομένων. (για παράδειγμα ευαίσθητα προσωπικά δεδομένα)

Γενικά ένα από τα βασικά χαρακτηριστικά των κριτηρίων είναι η αξιοπιστία τους μέσα στο χρόνο. Για το λόγο αυτό χρειάζεται να αναθεωρούνται ανά τακτά χρονικά διαστήματα και ειδικότερα όταν υπάρχουν τροποποιήσεις στο νομικό πλαίσιο, αποφάσεις του Ευρωπαϊκού Δικαστηρίου που ερμηνεύουν όρους και διατάξεις, καθώς επίσης και όταν εξελίσσεται η τεχνολογία.

Στάδιο μετά την πιστοποίηση – Επιτήρηση πιστοποιημένου οργανισμού

Η αξιοπιστία της πιστοποίησης συνδέεται άμεσα με το αν και κατά πόσο το χορηγημένο πιστοποιητικό ανταποκρίνεται στους όρους με βάση τους οποίους χορηγήθηκε η πιστοποίηση. Για το λόγο αυτό πραγματοποιούνται περιοδικοί έλεγχοι δηλαδή επιθεωρήσεις επιτήρησης με σκοπό την διασφάλιση της αξιοπιστίας.

Σύμφωνα με τον ΓΚΠΔ αρμόδιοι για την υλοποίηση περιοδικών ελέγχων των πιστοποιήσεων που έχουν χορηγηθεί είναι:

- Η εποπτική αρχή (άρθρο 57 – παράγραφος 1 στοιχείο ιε και άρθρο 58 – παράγραφος 1 στοιχείο β) ή
- Διαπιστευμένος φορέας πιστοποίησης ο οποίος θα πρέπει να έχει θεσπίσει διαδικασία περιοδικής επανεξέτασης (επιθεωρήσεις επιτήρησης), άρθρο 43 παράγραφος 2 στοιχείο γ. Αν και ο ΓΚΠΔ δεν καθορίζει λεπτομέρειες για τέτοιου είδους ελέγχους, παρ' όλα αυτά το πρότυπο ISO/IEC 17065:2012, που εφαρμόζεται από τους διαπιστευμένους φορείς πιστοποίησης, παρέχει ένα πλαίσιο για τέτοιου είδους ελέγχους.

Εκτελεστικές εξουσίες Ευρωπαϊκής Επιτροπής

Ο ΓΚΠΔ εξουσιοδοτεί την Επιτροπή να εκδίδει πράξεις σχετικά με τους μηχανισμούς πιστοποίησης της προστασίας των δεδομένων και οι οποίες αφορούν:

- Έκδοση κατ' εξουσιοδότηση πράξεων, σύμφωνα με το άρθρο 92, με σκοπό τον καθορισμό των απαιτήσεων που πρέπει να ληφθούν υπόψη για τους μηχανισμούς πιστοποίησης προστασίας δεδομένων (άρθρο 42 παράγραφος 1).

  Σύμφωνα με την αιτιολογική σκέψη 166 του ΓΚΠΔ, για την εκπλήρωση των στόχων του ΓΚΠΔ, θα πρέπει να ανατεθεί στην Επιτροπή η εξουσία έκδοσης πράξεων σύμφωνα με το άρθρο 290 ΣΛΕΕ (Συνθήκη για τη Λειτουργία της Ευρωπαϊκής Ένωσης). Οι πράξεις αυτές αποσκοπούν στην συμπλήρωση του ΓΚΠΔ, όσον αφορά τους μηχανισμούς πιστοποίησης της προστασίας δεδομένων, καθορίζοντας όλες τις απαιτήσεις οι οποίες δεν προσδιορίζονται στον ΓΚΠΔ.

  Βάσει του άρθρου 290 ΣΛΕΕ και σε σχέση με τις κατά εξουσιοδότηση πράξεις χρειάζεται να ληφθούν υπόψη τα παρακάτω:

  - Το περιεχόμενο των πράξεων αυτών θα πρέπει να συμμορφώνεται με τον ΓΚΠΔ στο σύνολό του και η έγκριση των κανόνων αυτής να εμπίπτει στο κανονιστικό πλαίσιο όπως αυτό ορίζεται από τον ΓΚΠΔ.
  - Οι πράξεις αυτές θα πρέπει να αναφέρονται σε μη ουσιώδη στοιχεία της νομοθεσίας, τα οποία δεν έχει προσδιορίσει ο ΓΚΠΔ.
  - Οι πράξεις πρέπει να είναι γενικής εφαρμογής και κατά συνέπεια αποκλείεται η δυνατότητα κάλυψης μεμονωμένων μέτρων.

- Τη θέσπιση τεχνικών προτύπων για μηχανισμούς πιστοποίησης, σφραγίδες και σήματα προστασίας δεδομένων, καθώς και μηχανισμών για την προώθηση και την αναγνώριση αυτών. (άρθρο 93 παράγραφος 2).

  Όπως αναφέρεται στην αιτιολογική σκέψη 167 του ΓΚΠΔ και περαιτέρω στο άρθρο 291 ΣΛΕΕ, σκοπός των εκτελεστικών πράξεων είναι να εξασφαλιστούν ενιαίες προϋποθέσεις εφαρμογής του Κανονισμού. Αυτές αποτελούν μέσο για την εξασφάλιση επαρκών επιπέδων ομοιομορφίας της νομοθεσίας και στη συγκεκριμένη περίπτωση του ΓΚΠΔ. Συνεπώς σκοπός της παραπομπής σε τεχνικά πρότυπα για τους μηχανισμούς πιστοποίησης είναι να εξασφαλιστεί η ομοιομορφία στην εφαρμογή του ΓΚΠΔ.

  Παράλληλα, η Επιτροπή εξουσιοδοτείται να ασχοληθεί με την προώθηση και αναγνώριση των μηχανισμών πιστοποίησης προστασία δεδομένων, των σφραγίδων και των σημάτων. Σε αυτό το πλαίσιο η αναγνώριση θα μπορούσε να σημαίνει την επίσημη αναγνώριση / αποδοχή των διασυνοριακών πιστοποιήσεων ή την οπτική διάκριση των πιστοποιήσεων, των σφραγίδων και των σημάτων από άλλες σφραγίδες και σήματα.

  Η προώθηση αυτή θα πρέπει να γίνεται στο πλαίσιο του γενικού σκοπού του άρθρου 42 – παράγραφος 1 και ταυτόχρονα να καθοριστούν ειδικά μέτρα για τις ΜΜΕ (Μικρές και Μεσαίου μεγέθους εταιρείες).

2.4. Πεδίο εφαρμογής Πιστοποίησης

Η πιστοποίηση στο πλαίσιο του ΓΚΠΔ, συνδέεται με την αρχή της ευθύνης, μπορεί να αιτηθεί μόνο από Υπεύθυνους επεξεργασίας ή Εκτελούντες την επεξεργασία των προσωπικών δεδομένων (άρθρο 42 παράγραφος 7) και όπως περιγράφεται αφορά την διαδικασία επεξεργασίας των προσωπικών δεδομένων, η οποία μπορεί να διεξάγεται στο πλαίσιο ενός προϊόντος ή ενός συστήματος ή μιας υπηρεσίας. Η πιστοποίηση θα πρέπει να χορηγείται σε σχέση με τις δραστηριότητες που αφορούν την επεξεργασία των δεδομένων και σε σχέση με το προϊόν ή την υπηρεσία ή το σύστημα που αφορά αυτή η επεξεργασία.

Κατά την αξιολόγηση μία πράξης επεξεργασίας, στο πλαίσιο της συμμόρφωσή της με τον ΓΚΠΔ, πρέπει να λαμβάνονται υπόψη, σε βαθμό ανάλογο με το αντικείμενο πιστοποίησης, τα παρακάτω:

- Τα προσωπικά δεδομένα.
- Η τεχνολογική υποδομή (λογισμικό και υλικό) που χρησιμοποιείται για την επεξεργασία.

- Οι διαδικασίες που σχετίζονται με την επεξεργασία των δεδομένων.

τα οποία και επηρεάζουν σημαντικά και το σχεδιασμό των κριτηρίων και των διαδικασιών πιστοποίησης. Στα παραπάνω στοιχεία έχουν επίδραση οι ακόλουθοι σημαντικοί παράγοντες:

- Η οργάνωση και το νομικό πλαίσιο του Υπευθύνου επεξεργασίας ή του εκτελούντα την επεξεργασία.
- Το τμήμα, το περιβάλλον και τα άτομα που εμπλέκονται στην επεξεργασία των δεδομένων.
- Η τεχνική περιγραφή των στοιχείων προς αξιολόγηση.
- Οι υποδομές Τεχνολογίας της Πληροφορίας που υποστηρίζουν την πράξη της επεξεργασίας όπως τα λειτουργικά συστήματα, οι βάσεις δεδομένων, τα συστήματα αποθήκευσης, τα συστήματα ελέγχου ταυτότητας και εξουσιοδότησης, οι υποδομές επικοινωνίας και πρόσβασης στο διαδίκτυο και άλλα.

Ο μηχανισμός πιστοποίησης μπορεί να ορίσει το πεδίο εφαρμογής του είτε γενικά είτε σε σχέση με ένα συγκεκριμένο είδος ή τομέα πράξεων επεξεργασίας και ως εκ τούτου μπορεί να προσδιορίσει τα αντικείμενα της πιστοποίησης που εμπίπτουν στο πεδίο εφαρμογής του μηχανισμού πιστοποίησης (για παράδειγμα ασφαλής αποθήκευση και προστασία των προσωπικών δεδομένων που περιέχονται σε ψηφιακό θησαυροφυλάκιο).

Τα άρθρα 42 και 43 προσφέρουν ένα γενικό πλαίσιο για πιστοποίηση βάσει του ΓΚΠΔ. Ωστόσο άλλα άρθρα του ΓΚΠΔ επισημαίνουν πιο συγκεκριμένα θέματα πιστοποίησης υπό την αιγίδα των άρθρων 42 και 43. Για παράδειγμα, στο άρθρο 25 παράγραφος 3 αναφέρεται σε «εγκεκριμένους μηχανισμούς πιστοποίησης με τους οποίους ένας Υπεύθυνος επεξεργασίας μπορεί να δείξει συμμόρφωση όσον αφορά την προστασία δεδομένων από το σχεδιασμό (άρθρο 25 παράγραφος 1) και από προεπιλεγμένη (άρθρο 25 παράγραφος 2). Επίσης πεδίο εφαρμογής πιστοποίησης προκύπτει και από τα παρακάτω άρθρα:

- Άρθρο 24 – Ευθύνη του Υπευθύνου επεξεργασίας, όπου στην παράγραφο 3 γίνεται αναφορά για εγκεκριμένο μηχανισμό πιστοποίησης, βάσει άρθρου 42, ο οποίος μπορεί να χρησιμοποιηθεί ως στοιχείο για την απόδειξη της συμμόρφωσης με τις υποχρεώσεις του Υπευθύνου.
- Άρθρο 28 – Εκτελών την επεξεργασία, όπου στην παράγραφο 5 αναφέρεται ότι η τήρηση εκ μέρους του εκτελούντος την επεξεργασία εγκεκριμένου μηχανισμού πιστοποίησης όπως αναφέρεται στο άρθρο 42 δύναται να χρησιμοποιηθεί ως στοιχείο για να

αποδειχθεί ότι παρέχει επαρκείς διαβεβαιώσεις σύμφωνα με τις παραγράφους 1 και 4 στου άρθρου 28. Επίσης, στην παράγραφο 6 αναφέρεται ότι, με την επιφύλαξη ατομικής σύμβασης μεταξύ του υπευθύνου επεξεργασίας και του εκτελούντος την επεξεργασία, η σύμβαση ή η άλλη νομική πράξη που αναφέρεται στις παραγράφους 3 και 4 του εν λόγω άρθρου μπορεί να βασίζεται, εν όλω ή εν μέρει, σε τυποποιημένες συμβατικές ρήτρες που αναφέρονται στις παραγράφους 7 και 8 του άρθρου 28, μεταξύ άλλων όταν αποτελούν μέρος πιστοποίησης που χορηγείται στον υπεύθυνο επεξεργασίας ή στον εκτελούντα την επεξεργασία σύμφωνα με τα άρθρα 42 και 43.

- Άρθρο 32 – Ασφάλεια επεξεργασίας, όπου στην παράγραφο 3 γίνεται αναφορά για εγκεκριμένο μηχανισμό πιστοποίησης, βάσει άρθρου 42, ο οποίος μπορεί να χρησιμοποιηθεί ως στοιχείο για την απόδειξη της συμμόρφωσης με τις απαιτήσεις της παραγράφου 1 του άρθρου 32.
- Άρθρο 46 – Διαβιβάσεις που υπόκεινται σε κατάλληλες εγγυήσεις όπου στην παράγραφο 2 αναφέρεται ότι οι κατάλληλες εγγυήσεις που αναφέρονται στην παράγραφο 1 του αν λόγω άρθρου μπορούν να προβλέπονται, χωρίς να απαιτείται ειδική άδεια εποπτικής αρχής, μεταξύ άλλων και μέσω εγκεκριμένου μηχανισμού πιστοποίησης, σύμφωνα με το άρθρο 42, από κοινού με δεσμευτικές και εκτελεστές υποχρεώσεις του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία στην τρίτη χώρα να εφαρμόζει τις κατάλληλες εγγυήσεις, μεταξύ άλλων όσον αφορά τα δικαιώματα των υποκειμένων των δεδομένων (σημείο στ).

Επιπρόσθετα, υπάρχει περιθώριο για συστήματα πιστοποίησης και σε άλλα πεδία όπως τα Δικαιώματα των υποκειμένων στα οποία αναφέρονται τα δεδομένα (άρθρα 15 μέχρι και 22) και στη συγκατάθεση παιδιών (άρθρο 8 – Προϋποθέσεις που ισχύουν για τη συγκατάθεση παιδιού σε σχέση με τις υπηρεσίες της κοινωνίας των πληροφοριών)

Συμπερασματικά, μπορούμε να διακρίνουμε τα ολοκληρωμένα συστήματα πιστοποίησης ΓΚΠΔ που καλύπτουν το πλήρες εύρος των απαιτήσεων του ΓΚΠΔ και τα συστήματα πιστοποίησης μεμονωμένων θεμάτων – σκοπού, όπως για παράδειγμα πιστοποίηση προστασίας δεδομένων από το σχεδιασμό, τα οποία επικεντρώνονται σε συγκεκριμένο θέμα του ΓΚΠΔ.

Το ουσιαστικό πεδίο εφαρμογής των ολοκληρωμένων συστημάτων πιστοποίησης μπορεί να καθοριστεί από το σύνολο των απαιτήσεων του ΓΚΠΔ αφαιρώντας διαδικαστικές διατάξεις, τις διατάξεις που αφορούν το πεδίο εφαρμογής καθώς και εκείνες που αφορούν άλλες οντότητες εκτός από τους Υπευθύνους και τους Εκτελούντες την επεξεργασία (για παράδειγμα εκτός

μπορεί να είναι τα άρθρα 1 έως και 3, το 23 και το 51 καθώς δεν περιλαμβάνουν υποχρεώσεις για τους Υπευθύνους και τους Εκτελούντες την επεξεργασία). Ο παρακάτω πίνακας περιέχει μία επισκόπηση του «πεδίου εφαρμογής» όλων των διατάξεων του ΓΚΠΔ όπου η στήλη «Σχετικό με τη συμμόρφωση» δείχνει τα άρθρα των οποίων οι απαιτήσεις χρειάζεται να αποτελούν μέρος ενός ολοκληρωμένου συστήματος πιστοποίησης.

ΑΡΘΡΟ	ΠΕΡΙΓΡΑΦΗ	ΑΝΑΦΕΡΕΙ ΠΙΣΤΟΠΟΙΗΣΗ	ΣΧΕΤΙΚΟ ΜΕ ΤΗ ΣΥΜΜΟΡΦΩΣΗ
ΚΕΦ I	Γενικές διατάξεις		
1	Αντικείμενο και στόχοι		
2	Ουσιαστικό πεδίο εφαρμογής		
3	Εδαφικό πεδίο εφαρμογής		
4	Ορισμοί		X
ΚΕΦ II	Αρχές		
5	Αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα		X
6	Νομιμότητα της επεξεργασίας		X
7	Προϋποθέσεις για συγκατάθεση		X
8	Προϋποθέσεις που ισχύουν για τη συγκατάθεση παιδιού σε σχέση με τις υπηρεσίες της κοινωνίας των πληροφοριών		X
9	Επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα		X
10	Επεξεργασία δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα		X
11	Επεξεργασία η οποία δεν απαιτεί εξακρίβωση ταυτότητας		X
ΚΕΦ III	Δικαιώματα του υποκειμένου των δεδομένων		
ΤΜΗΜΑ 1	Διαφάνεια και ρυθμίσεις		

ΑΡΘΡΟ	ΠΕΡΙΓΡΑΦΗ	ΑΝΑΦΕΡΕΙ ΠΙΣΤΟΠΟΙΗΣΗ	ΣΧΕΤΙΚΟ ΜΕ ΤΗ ΣΥΜΜΟΡΦΩΣΗ
12	Διαφανής ενημέρωση, ανακοίνωση και ρυθμίσεις για την άσκηση των δικαιωμάτων του υποκειμένου των δεδομένων		**X**
ΤΜΗΜΑ 2	Ενημέρωση και πρόσβαση σε δεδομένα προσωπικού χαρακτήρα		
13	Πληροφορίες που παρέχονται εάν τα δεδομένα προσωπικού χαρακτήρα συλλέγονται από το υποκείμενο των δεδομένων		**X**
14	Πληροφορίες που παρέχονται εάν τα δεδομένα προσωπικού χαρακτήρα δεν έχουν συλλεγεί από το υποκείμενο των δεδομένων		**X**
15	Δικαίωμα πρόσβασης του υποκειμένου των δεδομένων		**X**
ΤΜΗΜΑ 3	Διόρθωση και διαγραφή		**X**
16	Δικαίωμα διόρθωσης		**X**
17	Δικαίωμα διαγραφής («δικαίωμα στη λήθη»)		**X**
18	Δικαίωμα περιορισμού της επεξεργασίας		**X**
19	Υποχρέωση γνωστοποίησης όσον αφορά τη διόρθωση ή τη διαγραφή δεδομένων προσωπικού χαρακτήρα ή τον περιορισμό της επεξεργασίας		**X**
20	Δικαίωμα στη φορητότητα των δεδομένων		**X**
ΤΜΗΜΑ 4	Δικαίωμα εναντίωσης και αυτοματοποιημένη ατομική λήψη αποφάσεων		
21	Δικαίωμα εναντίωσης		**X**
22	Αυτοματοποιημένη ατομική λήψη αποφάσεων, περιλαμβανομένης της κατάρτισης προφίλ		**X**

ΑΡΘΡΟ	ΠΕΡΙΓΡΑΦΗ	ΑΝΑΦΕΡΕΙ ΠΙΣΤΟΠΟΙΗΣΗ	ΣΧΕΤΙΚΟ ΜΕ ΤΗ ΣΥΜΜΟΡΦΩΣΗ
ΚΕΦ IV	Υπεύθυνος επεξεργασίας αι εκτελών την επεξεργασία		
ΤΜΗΜΑ 1	Γενικές Υποχρεώσεις		
24	Ευθύνη του υπευθύνου επεξεργασίας	X	X
25	Προστασία των δεδομένων ήδη από το σχεδιασμό και εξ ορισμού	X	X
26	Από κοινού υπεύθυνοι επεξεργασίας		X
27	Εκπρόσωποι υπευθύνων επεξεργασίας ή εκτελούντων την επεξεργασία μη εγκατεστημένων στην Ένωση		X
28	Εκτελών την επεξεργασία	X	X
29	Επεξεργασία υπό την εποπτεία του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία		X
30	Αρχεία των δραστηριοτήτων επεξεργασίας		X
31	Συνεργασία με την εποπτική αρχή		
ΤΜΗΜΑ 2	ασφάλεια δεδομένων προσωπικού χαρακτήρα		
32	Ασφάλεια επεξεργασίας		X
33	Γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα στην εποπτική αρχή		X
34	Ανακοίνωση παραβίασης δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων		X
ΤΜΗΜΑ 3	Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων και προηγούμενη διαβούλευση		
35	Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων		X
36	Προηγούμενη διαβούλευση		X
ΤΜΗΜΑ 4	Υπεύθυνος προστασίας δεδομένων		

ΑΡΘΡΟ	ΠΕΡΙΓΡΑΦΗ	ΑΝΑΦΕΡΕΙ ΠΙΣΤΟΠΟΙΗΣΗ	ΣΧΕΤΙΚΟ ΜΕ ΤΗ ΣΥΜΜΟΡΦΩΣΗ
37	Ορισμός του υπευθύνου προστασίας δεδομένων		**X**
42	Πιστοποίηση	**X**	
43	Φορείς πιστοποίησης	**X**	
ΚΕΦ V	Διαβίβαση δεδομένων προσωπικού χαρακτήρα προς τρίτες χώρες ή διεθνείς οργανισμούς		
44	Γενικές αρχές για διαβιβάσεις		**X**
45	Διαβιβάσεις βάσει απόφαση επάρκειας		
46	Διαβιβάσεις που υπόκεινται σε κατάλληλες εγγυήσεις	**X**	**X**
47	Δεσμευτικοί εταιρικοί κανόνες		**X**
87	Επεξεργασία του εθνικού αριθμού ταυτότητας		**X**
88	Επεξεργασία στο πλαίσιο της απασχόλησης		**X**

Πίν.1: Πεδίο εφαρμογής ολοκληρωμένων συστημάτων πιστοποίησης ΓΚΠΔ

Το πεδίο εφαρμογής των συστημάτων πιστοποίησης μεμονωμένων θεμάτων – σκοπού μπορεί να είναι οποιοδήποτε θέμα του ΓΚΠΔ (για παράδειγμα η επεξεργασία δεδομένων σχετικά με τα παιδιά, η διατήρηση των δεδομένων, η ασφάλεια των δεδομένων και άλλα) με την προϋπόθεση ότι πληρούνται οι απαιτήσεις των άρθρων 42 και 43. Αξίζει να σημειωθεί ότι αυτής της κατηγορίας οι πιστοποιήσεις πιθανόν να μπορούν να συνδυαστούν και με τεχνικά πρότυπα (όπως το ISO 27001) τα οποία συμπληρώνουν τις διατάξεις του ΓΚΠΔ.

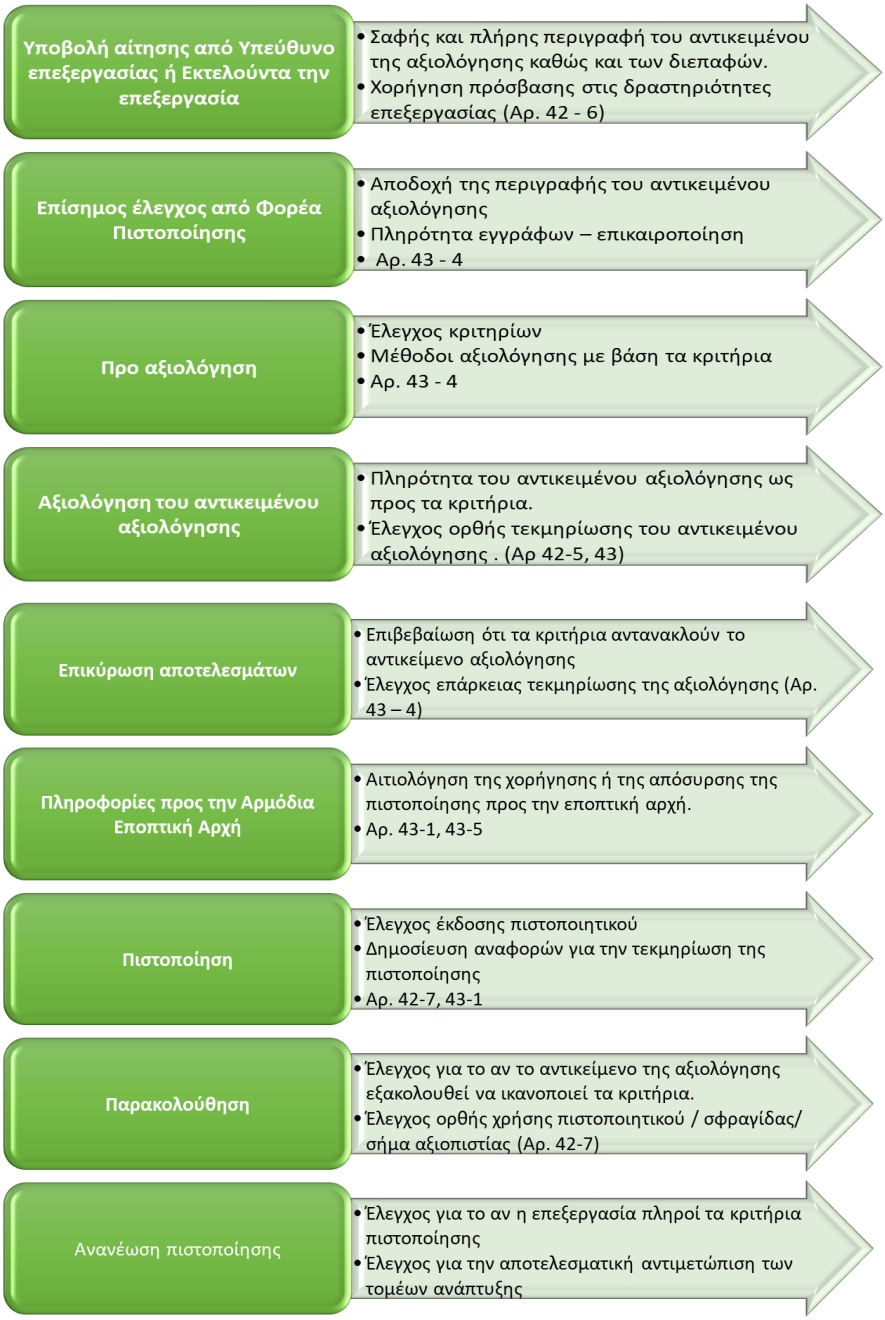
Σε κάθε περίπτωση, αξιόπιστη και ουσιαστική αξιολόγηση συμμόρφωσης μπορεί να γίνει μόνο αν κάθε αντικείμενο ενός έργου πιστοποίησης περιγραφεί με ακρίβεια. Για το λόγο αυτό πρέπει να προσδιοριστούν με σαφήνεια ποιες πράξεις επεξεργασίας περιλαμβάνονται στο αντικείμενο της πιστοποίησης και στη συνέχεια να περιγραφούν τα βασικά στοιχεία, δηλαδή, ποια δεδομένα, διαδικασίες και τεχνικές υποδομές θα αξιολογηθούν και ποια όχι. Σε αυτά συμπεριλαμβάνονται και οι διεπαφές προς άλλες διαδικασίες που πρέπει πάντα να λαμβάνονται υπόψη καθώς και να περιγράφονται. Είναι αντιληπτό πως οτιδήποτε δεν είναι

γνωστό δεν μπορεί και να αποτελεί μέρος της αξιολόγησης και κατά συνέπεια δεν γίνεται να πιστοποιηθεί. Σε κάθε περίπτωση, το επιμέρους αντικείμενο της πιστοποίησης πρέπει να είναι κατανοητό ως προς το μήνυμα ή τους ισχυρισμούς που διατυπώνεται/-νται στην/από την πιστοποίηση και δεν θα πρέπει να παραπλανά τον χρήστη, τον πελάτη ή τον καταναλωτή.

2.5. Στάδια Διαδικασίας Πιστοποίησης

Η διαδικασία πιστοποίησης είναι τα βήματα που χρειάζεται να ολοκληρωθούν με επιτυχία από τον Υπεύθυνο επεξεργασίας ή τον Εκτελούντα την επεξεργασία που έχει υποβάλει αίτηση για πιστοποίηση.

Συνοπτικά τα βήματα για την διαδικασία πιστοποίησης είναι τα ακόλουθα:



Εικ.4. Τυπικά βήματα διαδικασίας πιστοποίησης Υπευθύνου ή Εκτελούντα την επεξεργασία

Κατά τη διαδικασία πιστοποίησης θα πρέπει να ληφθούν υπόψη τα παρακάτω:

- Στις περιπτώσεις που αφορούν αίτηση αρχικής πιστοποίησης ή ανανέωσης πιστοποίησης ή οποιασδήποτε τροποποίησή της (για παράδειγμα επέκταση ή περιορισμός του πεδίου εφαρμογής της) θα πρέπει να διατεθούν στον φορέα πιστοποίησης και να του δοθεί πρόσβαση σε όλες τις απαιτούμενες πληροφορίες.
- Ο φορέας πιστοποίησης θα πρέπει να διαθέτει κατάλληλη διαδικασία και απαραίτητη εμπειρογνωμοσύνη για :
  - την επανεξέταση των αιτήσεων στο πλαίσιο των υφιστάμενων μηχανισμών πιστοποίησης
  - την αναθεώρηση νέων μηχανισμών πιστοποίησης ή νέων τύπων επεξεργασίας δεδομένων
  - την αξιολόγηση των δραστηριοτήτων επεξεργασίας δεδομένων
  - την αναθεώρηση των αποτελεσμάτων της διαδικασίας αξιολόγησης
  - την εκτέλεση διαφόρων δραστηριοτήτων παρακολούθησης, που απαιτείται μετά από μια θετική απόφαση πιστοποίησης. Τέτοιες δραστηριότητες θα μπορούσαν να περιλαμβάνουν την επιτήρηση, τις αλλαγές στο πεδίο της πιστοποίησης, τις αλλαγές στον τύπο και το εύρος των δραστηριοτήτων επεξεργασίας δεδομένων που πραγματοποίησε ο πιστοποιημένος οργανισμός, την αναστολή, την απόσυρση, την αποκατάσταση ή τον τερματισμό των πιστοποιήσεων
  - την παραλαβή, την αξιολόγηση και την παρακολούθηση των καταγγελιών και των προσφυγών που σχετίζονται με τις δραστηριότητες πιστοποίησης
- Η αξιολόγηση που διεξάγεται από τον οργανισμό πιστοποίησης θα πρέπει να τεκμηριωθεί και στην περίπτωση που υπάρξουν μη συμμορφώσεις, αυτές να κοινοποιηθούν στον προς πιστοποίηση οργανισμό. Μετά την κοινοποίηση, ο υποψήφιος οργανισμός αποφασίζει εάν θέλει να αντιμετωπίσει ενδεχόμενες μη συμμορφώσεις και να συνεχίσει τη διαδικασία πιστοποίησης.
- Οι δραστηριότητες αξιολόγησης και απόφασης να είναι ξεχωριστές και να εκτελούνται από διαφορετικούς εμπειρογνώμονες. Όλες οι δραστηριότητες και τα αποτελέσματά

τους θα πρέπει να είναι τεκμηριωμένα και τα αποτελέσματα να διατηρούνται εμπιστευτικά.

- Οι αποφάσεις πιστοποίησης να τεκμηριώνονται πλήρως και επισήμως, καθώς επίσης και να εγγράφονται σε δημόσιο κατάλογο που περιλαμβάνει τις πιστοποιημένες επεξεργασίες δεδομένων.

Τα στάδια της διαδικασίας πιστοποίησης, όπως παραπάνω προσδιορίζονται από τον ΓΚΠΔ, μπορούν να συμπληρωθούν από τα στάδια που προσδιορίζονται στο πρότυπο EN ISO/IEC 17065:2012. Σημαντική βοήθεια προς την κατεύθυνσης της εφαρμογής κατάλληλης και αξιόπιστης διαδικασίας πιστοποίησης προστασίας δεδομένων αποτελεί και η μελέτη των υφιστάμενων πιστοποιήσεων για τον προσδιορισμό των βέλτιστων πρακτικών. Ενδεικτικά αναφέρονται τα παρακάτω:

- Αξιολόγηση της συμμόρφωσης

  Η διαδικασία αξιολόγησης της συμμόρφωσης αντιπροσωπεύει ένα υποσύνολο της διαδικασίας πιστοποίησης με στόχο να αποδειχθεί εάν έχουν εκπληρωθεί συγκεκριμένες απαιτήσεις σχετικά με ένα προϊόν, μια διαδικασία, μια υπηρεσία, ένα σύστημα, ένα πρόσωπο ή ένα σώμα. Η πλειονότητα των πιστοποιητικών απαιτεί, εκτός από την εξέταση των εγγράφων, και επιτόπιο έλεγχο. Όσον αφορά τους επιθεωρητές μπορεί να είναι είτε εσωτερικοί (που να ανήκουν στο φορέα πιστοποίησης) είτε εξωτερικοί. Στην περίπτωση των εξωτερικών επιθεωρητών, αυτοί οφείλουν να καθορίζονται, από τον ιδιοκτήτη του συστήματος. Οι εξωτερικοί ελεγκτές διενεργούν τον έλεγχο και οφείλουν να υποβάλουν αναφορά στον υποψήφιο οργανισμό προς πιστοποίηση στο τέλος της διαδικασίας αξιολόγησης της συμμόρφωσης. Στη συνέχεια, η αναφορά αυτή υποβάλλεται προς τον φορέα πιστοποίησης για έγκριση και εφόσον κριθεί από αυτόν ότι ικανοποιούνται τα κριτήρια, εκδίδεται η πιστοποίηση.

- Έκδοση πιστοποίησης

  Μια πιστοποίηση συνήθως συναντάται ως γραπτή βεβαίωση που εκδίδεται από τον φορέα που είναι υπεύθυνος για την αξιολόγηση της συμμόρφωσης. Η γραπτή βεβαίωση συχνά συνοδεύεται, αλλά όχι πάντα, από ένα οπτικό σύμβολο που ονομάζεται σφραγίδα, ετικέτα, σήμα ή πιστοποίηση. Ο κάτοχος του συστήματος έχει το δικαίωμα να επιτρέπει στον πιστοποιημένο οργανισμό να χρησιμοποιεί τη σφραγίδα, ο οποίος μπορεί να τη τοποθετήσει στα προϊόντα και τα δικαιολογητικά του, υπό την προϋπόθεση ότι ο

πιστοποιημένος οργανισμός διατηρεί τη συμμόρφωσή του κατά τη διάρκεια της περιόδου ισχύος του πιστοποιητικού.

Όλα τα συστήματα περιλαμβάνουν ένα στάδιο εξέτασης της έκθεσης ελέγχου πριν από την έκδοση της πιστοποίησης, όπως προβλέπεται επίσης στο πρότυπο ISO / IEC 17065. Αυτό οφείλεται, επίσης, στο γεγονός ότι ένας σημαντικός αριθμός συστημάτων πιστοποίησης μεταβιβάζει τη διαδικασία ελέγχου σε εξωτερικούς ελεγκτές. Οι διαδικασίες αξιολόγησης και έκδοσης ελέγχονται στη συνέχεια από διαφορετικές οντότητες.

Η περίοδος ισχύος της πιστοποίησης μπορεί να εκτείνεται σε οποιαδήποτε περίοδο, από ένα έως τρία έτη, ενώ στην περίπτωση του ΓΚΠΔ η πιστοποίηση χορηγείται για μέγιστη περίοδο τριών ετών (άρθρο 42 παράγραφος 7).

Στις περιπτώσεις που ο φορέας πιστοποίησης είναι δημόσια αρχή, η αρχή εκδίδει πιστοποίηση που αποτελεί απόφαση δημόσιας διοίκησης. Η έκδοση της πιστοποίησης (ή η απόρριψή της) μπορεί να αμφισβητηθεί στα διοικητικά δικαστήρια.

- Παρακολούθηση (επιτήρηση)

Η πιστοποίηση εξαρτάται από την διατήρηση της συμμόρφωσης προς τις απαιτήσεις και τα κριτήρια κατά τη διάρκεια της περιόδου ισχύος αυτής. Ο φορέας που εκδίδει την πιστοποίηση, που έχει συμμόρφωση με το πρότυπο EN ISO / IEC 17065, θα πρέπει να παρακολουθεί τη συμμόρφωση των πιστοποιημένων οργανισμών προκειμένου να διατηρηθεί η πιστοποίηση αυτών αλλά και η εμπιστοσύνη στο σύστημα.

Μέχρι σήμερα και με βάση των υφιστάμενων πιστοποιήσεων υπάρχουν δύο βασικά μοντέλα επιτήρησης:

Α) Επιτήρηση από τον ιδιοκτήτη του συστήματος πιστοποίησης

Α.1) Το μεγαλύτερο ποσοστό διενεργεί τακτικές επιθεωρήσεις επιτήρησης, συνήθως ετήσιες.

Α.2) Ένα μικρό ποσοστό διενεργεί και τυχαίους ελέγχους εκτός από τις τακτικές επιθεωρήσεις επιτήρησης

Β) Επιτήρηση από τρίτο μέρος.

Η επιτήρηση μπορεί να γίνει είτε από τρίτο μέρος είτε από την Αρχή Προστασίας Δεδομένων, είτε από την εποπτική αρχή είτε και από τους εξωτερικού επιθεωρητές που έκαναν την αξιολόγηση της συμμόρφωσης.

- Ανανέωση

Η πιστοποίηση χορηγείται για περιορισμένο χρονικό διάστημα και είναι ανανεώσιμη, με την προϋπόθεση ότι ο πιστοποιημένος οργανισμός διατηρεί τη συμμόρφωσή του με τα κριτήρια και τις απαιτήσεις της πιστοποίησης. Η διαδικασία ανανέωσης είναι προαιρετική και πρέπει να ζητηθεί από τον πιστοποιημένο οργανισμό πριν από τη λήξη της περιόδου ισχύος. Ο φορέας πιστοποίησης μπορεί να απαιτήσει πλήρη ή μερική επανεκτίμηση (είναι ελάχιστες αυτές οι περιπτώσεις), ελέγχοντας μόνο, στη δεύτερη περίπτωση, τις αλλαγές στη συμμόρφωση του πιστοποιημένου οργανισμού κατά την περίοδο ισχύος.

- Πολιτική κυρώσεων

Η πολιτική κυρώσεων οργανώνει τις διάφορες κυρώσεις που ο φορέας μπορεί να επιβάλει σε ένα πιστοποιημένο οργανισμό που πλέον δεν συμμορφώνεται με τους όρους σύμφωνα με τους οποίους έχει εκδοθεί η πιστοποίηση. Οι πολιτικές αυτές ορίζουν μια σταδιακή διαδικασία επιβολής κυρώσεων η οποία ξεκινά με αναστολή της πιστοποίησης, που σε ορισμένες περιπτώσεις δημοσιοποιείται, και μπορεί να καταλήξει στην απόσυρση της πιστοποίησης, που θα συμβεί στην περίπτωση που ο μη συμμορφούμενος πιστοποιημένος οργανισμός δεν λάβει μέτρα για τον πλήρη μετριασμό της μη συμμόρφωσης εντός προκαθορισμένου χρονικού διαστήματος.

Σύμφωνα με την υφιστάμενη κατάσταση αρκετά συστήματα πιστοποίησης έχουν καθορίσει ένα χρονικό όριο, το οποίο κυμαίνεται ανάμεσα σε τρεις έως και έξι μήνες, εντός του οποίου οι πιστοποιημένοι οργανισμοί θα πρέπει να έχουν προβεί στις απαιτούμενες διαδικασίες για τη διόρθωση των μη συμμορφώσεων, προτού ενεργοποιηθεί η διαδικασία απόσυρσης του πιστοποιητικού.

- Καταγγελίες και επίλυση διαφορών

Χρειάζεται να υπάρχει κατάλληλη διαδικασία σχετικά με την υποβολή καταγγελιών και την διευθέτησή τους. Ο χειρισμός τους συνήθως γίνεται εσωτερικά και κάποιοι φορείς προσφέρουν, μέσω του διαδικτυακού τους τόπου, μια ηλεκτρονική φόρμα για την υποβολή παραπόνων. Η διαδικασία επίλυσης διαφορών περιλαμβάνει τις διαδικασίες

που χρησιμοποιούνται για την επίλυση διαφοράς μεταξύ του ιδιοκτήτη του συστήματος πιστοποίησης, του πιστοποιημένου οργανισμού και του τελικού χρήστη.

Οι τύποι διαδικασιών επίλυσης διαφορών συνήθως είναι δύο: δικαστικές και εξώδικες διαδικασίες. Οι δικαστικές διαδικασίες, με δίκες και διαιτησία, επιτρέπουν στο δικαστήριο να καθορίσει το αποτέλεσμα. Οι εξωδικαστικές διαδικασίες, που επίσης ονομάζονται και συναινετικές διαδικασίες, περιλαμβάνουν τη διαμεσολάβηση, τη συνδιαλλαγή ή τη διαπραγμάτευση μεταξύ των μερών. Το μεγαλύτερο ποσοστό από τις υφιστάμενες πιστοποιήσεις διαχειρίζεται εσωτερικά την επίλυση διαφορών και στην περίπτωση που δεν υπάρξει αποτέλεσμα γίνεται χρήση δικαστικής διαδικασίας, στην οποία απ' ευθείας καταφεύγει μόνο ένα μικρό ποσοστό.

2.6. Φορείς Πιστοποίησης – Διαπίστευση

Ο ρόλος του φορέα πιστοποίησης είναι να εκδίδει, να επανεξετάζει, να ανανεώνει και να ανακαλεί πιστοποιήσεις (άρθρο 42 παράγραφοι 5 και 7) βάσει ενός μηχανισμού πιστοποίησης και εγκεκριμένων κριτηρίων (άρθρο 43 παράγραφος 1). Αυτό απαιτεί από τον φορέα πιστοποίησης ή τον ιδιοκτήτη του συστήματος πιστοποίησης να δημιουργήσει και να καθορίσει κριτήρια πιστοποίησης, η ύπαρξη των οποίων είναι απαραίτητη προκειμένου να επιτευχθεί η διαπίστευσή του σύμφωνα με το άρθρο 43, και διαδικασίες πιστοποίησης, περιλαμβανομένων διαδικασιών για την παρακολούθηση της τήρησης, την επανεξέταση, τη διαχείριση καταγγελιών και την ανάκληση. Τα κριτήρια πιστοποίησης επανεξετάζονται στο πλαίσιο της διαδικασίας διαπίστευσης, η οποία λαμβάνει υπόψη τους κανόνες και τις διαδικασίες βάσει των οποίων εκδίδονται πιστοποιήσεις, σφραγίδες ή σήματα (άρθρο 43 παράγραφος 2 στοιχείο γ).

Σημαντική επίδραση στις ενέργειες του φορέα πιστοποίησης έχει το πεδίο εφαρμογής και το είδος των κριτηρίων πιστοποίησης που έχουν αντίκτυπο στις διαδικασίες πιστοποίησης και αντίστροφα. Συγκεκριμένα κριτήρια μπορεί, για παράδειγμα, να απαιτούν συγκεκριμένες μεθόδους αξιολόγησης, όπως επιτόπιες επιθεωρήσεις.

Ο ΓΚΠΔ προβλέπει ότι αρμόδιοι για την έκδοση, την ανάκληση ή την απόσυρση πιστοποίησης είναι είτε οι διαπιστευμένοι φορείς πιστοποίησης είτε η αρμόδια Εποπτική Αρχή. Ανεξάρτητα τελικά από το ποιος είναι αρμόδιος και οι δύο θα πρέπει:

- Να έχουν υλοποιήσει μία αξιολόγηση για το αν ο οργανισμός που έχει υποβάλει αίτηση πιστοποίησης ικανοποιεί τα κριτήρια πιστοποίησης (στάδιο αξιολόγησης)

- Να κάνει ανασκόπηση των απαραίτητων πληροφοριών και των αποτελεσμάτων της αξιολόγησης (στάδιο ανασκόπησης αποτελεσμάτων)
- Να πάρουν μία απόφαση σχετικά με την αίτηση η οποία θα βασίζεται στις πληροφορίες που έχουν συλλέξει καθώς και στην αναφορά του σταδίου αξιολόγησης.

Στην περίπτωση του διαπιστευμένου φορέα πιστοποίησης, αυτός είναι υποχρεωμένος (άρθρο 43 παράγραφος 5) να παρέχει ενημέρωση, σχετικά με τους λόγους που χορηγείται / ανανεώνεται ή ανακαλείται η πιστοποίηση, στην αρμόδια εποπτική αρχή ώστε αυτή με τη σειρά της να μπορέσει να ασκήσει τις διορθωτικές εξουσίες της, με την προϋπόθεση ότι είναι απαραίτητο, σύμφωνα με το άρθρο 58 παράγραφος 2 στοιχείο η. Οι πληροφορίες αυτές θα πρέπει να παρέχονται πριν την έκδοση και χορήγηση ή την ανανέωση της πιστοποίησης.

Αν και ο ΓΚΠΔ δίνει τη δυνατότητα στις εποπτικές αρχές να καθορίσουν τον τρόπο λήψης, επιβεβαίωσης, επανεξέτασης και διαχείρισης αυτών των πληροφοριών σε επιχειρησιακό επίπεδο (για παράδειγμα, αυτό θα μπορούσε να περιλαμβάνει τεχνολογικές λύσεις για την υποβολή εκθέσεων από τους φορείς πιστοποίησης), ο φορέας πιστοποίησης μπορεί να θέσει σε εφαρμογή μια διαδικασία και κριτήρια επεξεργασίας των πληροφοριών και των εκθέσεων που υποβάλλονται σε κάθε επιτυχές έργο πιστοποίησης σύμφωνα με το άρθρο 43 παράγραφος 1. Βάσει αυτών των πληροφοριών, η εποπτική αρχή μπορεί να ασκεί την εξουσία της να διατάσσει τον φορέα πιστοποίησης να αποσύρει ή να μην εκδώσει πιστοποίηση και να παρακολουθεί και να επιβάλλει την εφαρμογή των απαιτήσεων και των κριτηρίων πιστοποίησης σύμφωνα με τον ΓΚΠΔ άρθρο 57 παράγραφος 1 στοιχείο α και άρθρο 58 παράγραφος 2 στοιχείο η. Αυτό θα έχει σαν αποτέλεσμα την ενίσχυση της εναρμονισμένης προσέγγισης και της συγκρισιμότητας, περίπτωση πιστοποίησης από διαφορετικούς φορείς πιστοποίησης, καθώς και την γνώση εκ μέρους των εποπτικών αρχών των πληροφοριών για την κατάσταση πιστοποίησης ενός οργανισμού.

Επιπρόσθετα, ο υποψήφιος φορέας πιστοποίησης, για να είναι διαπιστευμένος, πρώτα θα πρέπει να:

- έχει αποδείξει την ανεξαρτησία και την εμπειρογνωμοσύνη του σε σχέση με το αντικείμενο της πιστοποίησης κατά την κρίση της αρμόδιας εποπτικής αρχής,
- έχει δεσμευτεί να σέβεται τα κριτήρια που αναφέρονται στο άρθρο 42 παράγραφος 5 και τα οποία έχουν εγκριθεί από την εποπτική αρχή που είναι αρμόδια δυνάμει του άρθρου 55 ή 56 ή από το Συμβούλιο Προστασίας Δεδομένων δυνάμει του άρθρου 63,

- έχει θεσπίσει διαδικασίες και δομές για τη διαχείριση καταγγελιών περί παραβάσεων της πιστοποίησης ή περί του τρόπου με τον οποίο η πιστοποίηση έχει εφαρμοστεί ή εφαρμόζεται από τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία, καθώς και για να καταστούν οι διαδικασίες και οι δομές αυτές διαφανείς στα υποκείμενα των δεδομένων και στο ευρύ κοινό,
- αποδεικνύει, κατά την κρίση της αρμόδιας εποπτικής αρχής, ότι τα καθήκοντα και οι υποχρεώσεις του δεν συνεπάγονται σύγκρουση συμφερόντων

Στην περίπτωση όπου η εποπτική αρχή έχει επιλεγεί για τη διενέργεια πιστοποίησης, θα πρέπει να αξιολογήσει προσεκτικά τον ρόλο της αναφορικά με τα καθήκοντα που της έχουν ανατεθεί σύμφωνα με τον ΓΚΠΔ. Ο ρόλος της θα πρέπει να είναι διαφανής κατά την άσκηση των αρμοδιοτήτων της. Θα χρειαστεί να προσέξει ειδικότερα τη διάκριση εξουσιών που αφορούν τις έρευνες και την επιβολή προκειμένου να αποφύγει οποιεσδήποτε πιθανές συγκρούσεις συμφερόντων.

Η εποπτική αρχή ενεργώντας ως φορέας πιστοποίησης θα πρέπει να διασφαλίσει την κατάλληλη δημιουργία ενός μηχανισμού πιστοποίησης και να αναπτύξει δικά της κριτήρια πιστοποίησης ή να υιοθετήσει άλλα. Επιπλέον, έχει το καθήκον να επανεξετάζει περιοδικά τις πιστοποιήσεις που εκδίδει (άρθρο 57 παράγραφος 1 στοιχείο ιε) και την εξουσία να τις αποσύρει εφόσον οι απαιτήσεις πιστοποίησης δεν πληρούνται ή δεν πληρούνται πλέον (άρθρο 58 παράγραφος 2 στοιχείο η). Για την εκπλήρωση αυτών των απαιτήσεων, είναι χρήσιμο να δημιουργηθούν μια διαδικασία πιστοποίησης και απαιτήσεις της διαδικασίας αυτής, και, αν δεν ορίζεται διαφορετικά π.χ. από την εθνική νομοθεσία, να τεθεί σε εφαρμογή μια νομικά εκτελεστή σύμβαση με κάθε αιτούντα οργανισμό για την παροχή δραστηριοτήτων πιστοποίησης. Θα πρέπει να διασφαλιστεί ότι η εν λόγω σύμβαση πιστοποίησης απαιτεί από τον αιτούντα να συμμορφώνεται τουλάχιστον με τα κριτήρια πιστοποίησης, περιλαμβανομένων των απαραίτητων ρυθμίσεων για τη διενέργεια της αξιολόγησης, την παρακολούθηση της τήρησης των κριτηρίων και την περιοδική επανεξέταση, περιλαμβανομένης της πρόσβασης σε πληροφορίες και/ή εγκαταστάσεις, της τεκμηρίωσης και της δημοσίευσης εκθέσεων και αποτελεσμάτων, και της διερεύνησης καταγγελιών. Τέλος, η εποπτική αρχή θα πρέπει να τηρεί τις απαιτήσεις στις κατευθυντήριες γραμμές για τη διαπίστευση των φορέων πιστοποίησης επιπλέον των απαιτήσεων σύμφωνα με το άρθρο 43 παράγραφος 2.

<u>Διαπίστευση φορέων πιστοποίησης</u>

Σύμφωνα με τα αποτελέσματα έρευνας που πραγματοποίησε ο παγκόσμιος οργανισμός για την Αξιολόγηση της Συμμόρφωσης των Φορέων Διαπίστευσης (IAF), έγινε φανερό ότι οι επιχειρήσεις έχουν σημαντικά οφέλη από την διαπιστευμένη πιστοποίηση. Σε αυτά συμπεριλαμβάνονται η βελτίωση των εσωτερικών διαδικασιών ενός οργανισμού, η κανονιστική συμμόρφωση και η θετική επίδραση στα έσοδα.[11]

Ο ΓΚΠΔ ορίζει υποχρεωτική τη διαπίστευση των φορέων πιστοποίησης, οι οποίοι μπορούν να χορηγούν και να ανανεώνουν πιστοποιήσεις σε Υπευθύνους επεξεργασίας και Εκτελούντες την επεξεργασία υπό την προϋπόθεση ότι έχουν προηγουμένως:

Α) διαπιστευθεί ότι διαθέτουν το ενδεδειγμένο επίπεδο εμπειρογνωμοσύνης σε σχέση με την προστασία προσωπικών δεδομένων, και

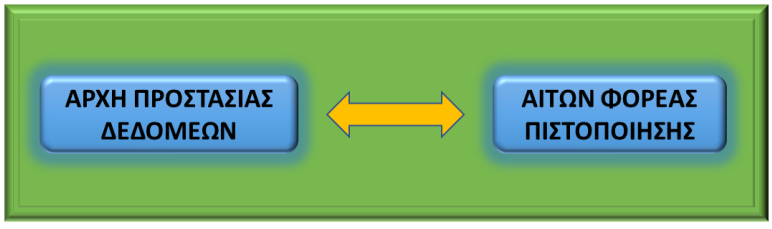
Β) ενημερώσει σχετικά την αρμόδια εποπτική αρχή.

Επίσης, ο ΓΚΠΔ προβλέπει ότι η διαπίστευση ισχύει για πέντε έτη (άρθρο 43 παράγραφος 4) και μπορεί να ανανεωθεί υπό την προϋπόθεση ότι ο φορέας πιστοποίησης εξακολουθεί να πληροί τις απαιτήσεις διαπίστευσης.

Στο άρθρο 43 παράγραφος 1, αναφέρεται ότι τα Κράτη Μέλη εξασφαλίζουν ότι οι φορείς πιστοποίησης είναι διαπιστευμένοι και ότι είναι στη δικαιοδοσία του Μέλους να επιλέξει έναν από τους διαθέσιμους τρόπους με τον οποίο θα γίνεται η διαπίστευση. Αυτοί οι διαθέσιμοι τρόποι είναι:

I. <u>Διαπίστευση από την αρμόδια Αρχή Προστασία Δεδομένων</u> (DPA).

   Η εποπτική αρχή δίνει διαπίστευση στον αιτούντα φορέα πιστοποίησης εφόσον αυτός πληροί τις αναγκαίες προϋποθέσεις.



Εικ.5. Συμμετέχοντες στον πρώτο τρόπο διαπίστευσης

   Η αρμοδιότητα της Αρχής Προστασίας Δεδομένων έχει καθοριστεί στη βάση των άρθρων 55 ή 56 του ΓΚΠΔ[12]. Στην περίπτωση της Ευρωπαϊκής Σφραγίδας, την έγκριση των

[11] International Accreditation Forum, 'The value of accredited certification. Survey Report' (May 2012)
[12] Το άρθρο 55 αναφέρεται στην αρμοδιότητα της εποπτικής αρχής και το άρθρο 56 στην αρμοδιότητα της επικεφαλής εποπτικής αρχής.

απαιτήσεων που αναφέρονται στο άρθρο 43 παράγραφος 3, αναλαμβάνει το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων, υπό το πρίσμα της διαπίστευσης των φορέων πιστοποίησης που αναφέρονται στο άρθρο 43.(άρθρο 70 παράγραφος 1 στοιχείο ιστ)

Ένας φορέας πιστοποίησης που επιθυμεί να παρέχει υπηρεσίες σε μηχανισμούς πιστοποίησης με βάση τον ΓΚΠΔ οφείλει να υποβάλει αίτηση στην αρμόδια εποπτική Αρχή προκειμένου να διαπιστευτεί. Η εποπτική Αρχή είναι αρμόδια για το έδαφος του κράτους μέλους της, όπου ο οργανισμός πιστοποίησης έχει την κύρια ή την ενιαία του εγκατάσταση (άρθρο 43 – παράγραφος 1). Όταν ο φορέας πιστοποίησης σκοπεύει να προσφέρει υπηρεσίες σε περισσότερα του ενός Κράτη Μέλη, τότε εφαρμόζονται οι απαιτήσεις του άρθρου 56 του ΓΚΠΔ προκειμένου να προσδιοριστεί η επικεφαλής εποπτική Αρχή.

Η εποπτική Αρχή σε εθνικό επίπεδο έχει δύο κύριες αρμοδιότητες:

- Η πρώτη είναι να καταρτίζει και να δημοσιεύει κριτήρια για τη διαπίστευσης του φορέα πιστοποίησης. (άρθρο 57 ΓΚΠΔ)

  Στην περίπτωση της ευρωπαϊκής σφραγίδας προστασίας δεδομένων, οι αιτούντες οργανισμοί πιστοποίησης είναι διαπιστευμένοι βάσει των απαιτήσεων διαπίστευσης που έχουν εγκριθεί από το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων.

- Η δεύτερη είναι η διεξαγωγή της διαδικασίας διαπίστευσης του αιτούντος φορέα πιστοποίησης. (άρθρο 57 – παράγραφος 1 σημείο ιζ και άρθρο 58 – παράγραφος 3 σημείο ε)

Ο ΓΚΠΔ αν και δεν παρέχει λεπτομέρειες σχετικά με τη διαδικασία διαπίστευσης όταν διενεργείται από εποπτική Αρχή, ωστόσο παρέχει ορισμένες εγγυήσεις και απαιτήσεις διαπίστευσης που πρέπει να τηρούνται από τον αιτούντα φορέα πιστοποίησης. Οι διασφαλίσεις αφορούν τόσο τα διαδικαστικά όσο και τα οργανωτικά ζητήματα του αιτούντος φορέα πιστοποίησης, συμπεριλαμβανομένης της ακεραιότητάς του και της εμπειρογνωμοσύνης του.

Ο αιτών φορέας πιστοποίησης, πριν υποβάλει αίτηση για διαπίστευση στην αρμόδια εποπτική αρχή, πρέπει να έχει θεσπίσει διαδικασίες για την έκδοση πιστοποιητικών, σφραγίδων και σημάτων, να διενεργεί περιοδική επανεξέταση και απόσυρση των πιστοποιητικών προστασίας δεδομένων καθώς επίσης και να διαθέτει μηχανισμούς

υποβολής καταγγελιών. Ο υποψήφιος φορέας πρέπει να δημοσιοποιήσει αυτές τις διαδικασίες στο υποκείμενο που αναφέρονται τα δεδομένα με διαφανή τρόπο.

Βασικό χαρακτηριστικό του υποψήφιου φορέα πιστοποίησης είναι η ανεξαρτησία του από τους Υπεύθυνους επεξεργασίας και τους Εκτελούντες την επεξεργασία που υποβάλλουν αίτηση πιστοποίησης. Η ανεξαρτησία του πρέπει να αποδεικνύεται, γεγονός που συνεπάγεται ότι ο υποψήφιος φορέας έχει καλή ιστορία αξιόπιστων πιστοποιήσεων πριν από την αίτηση διαπίστευσης. Επίσης οι εργασίες και τα καθήκοντα του αιτούντος φορέα πιστοποίησης δεν πρέπει να οδηγήσουν σε σύγκρουση συμφερόντων (άρθρο 43 παράγραφος 2 στοιχείο ε). Το άρθρο 43 παράγραφος 2 προβλέπει ότι αυτές οι ιδιότητες πρέπει να αποδεικνύονται κατά τρόπο ικανοποιητικό για την εποπτική αρχή χωρίς να δίνει πληροφορίες για το πώς θα γίνει αυτό σε ικανοποιητικό επίπεδο. Επιπρόσθετα, ο αιτών φορέας πιστοποίησης πρέπει να δεσμευτεί να τηρήσει τα εγκεκριμένα κριτήρια πιστοποίησης, σύμφωνα με το άρθρο 42 – παράγραφος 5 του ΓΚΠΔ.

Τέλος, ο αιτών οργανισμός πιστοποίησης πρέπει να έχει αποδείξει την εμπειρία του στο θέμα της πιστοποίησης. Η εμπειρογνωμοσύνη σε σχέση με το θέμα είναι κρίσιμη για την επιτυχία των μηχανισμών πιστοποίησης της προστασίας δεδομένων: ο φορέας πιστοποίησης είναι αυτός που εξετάζει κατά πόσον ένας Υπεύθυνος επεξεργασίας ή Εκτελών την επεξεργασία, επεξεργάζεται δεδομένα προσωπικού χαρακτήρα σύμφωνα με τα εγκεκριμένα κριτήρια πιστοποίησης. Οι φορείς πιστοποίησης οφείλουν να έχουν αποδεδειγμένο ιστορικό εμπειρίας και εμπειρογνωμοσύνης στον τομέα της προστασίας των δεδομένων γενικά, αλλά και στον ειδικό τομέα ή τομέα εφαρμογής όπου ο Υπεύθυνος επεξεργασίας ή ο Εκτελών είναι ενεργός. Αυτό σημαίνει ότι εάν ένας φορέας πιστοποίησης επιθυμεί να παρέχει υπηρεσίες σε Υπεύθυνους επεξεργασίας και Εκτελούντες την επεξεργασία που δραστηριοποιούνται στον τομέα της υγειονομικής περίθαλψης, ο φορέας αυτός είναι αναγκαίο να διαπιστευθεί ότι διαθέτει επαρκή εμπειρία στην επεξεργασία προσωπικών δεδομένων στον συγκεκριμένο τομέα.

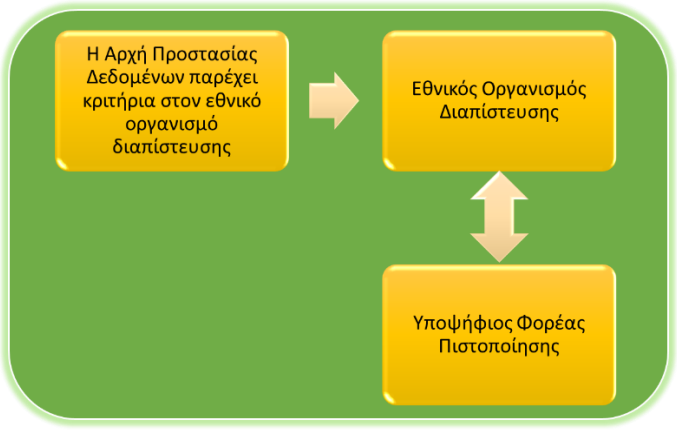
Η εποπτική Αρχή έχει την εξουσία να προβεί σε ανάκληση της διαπίστευσης στις περιπτώσεις που δεν πληρούνται ή δεν πληρούνται πλέον οι προϋποθέσεις για τη χορήγηση της διαπίστευσης καθώς επίσης και όταν οι ενέργειες ενός φορέα πιστοποίησης παραβιάζουν τον ΓΚΠΔ. Για το λόγο αυτό η εποπτική αρχή απαιτείται να εποπτεύει στενά τους διαπιστευμένους φορείς και να διενεργεί επιτόπιους ελέγχους ή

δειγματοληπτική εξέταση των πιστοποιήσεων που έχουν εκδοθεί από τον διαπιστευμένο φορέα πιστοποίησης. Παράλληλα, ένας φορέας πιστοποίησης πρέπει να αποτελεί καλό παράδειγμα, προτού να είναι σε θέση να πιστοποιήσει σε άλλους ότι επεξεργάζονται δεδομένα σύμφωνα με τα κριτήρια που βασίζονται στο ΓΚΠΔ.

Η χορήγηση πιστοποιητικού διαπίστευσης από την Αρχή Προστασίας Δεδομένων αποτελεί διοικητική πράξη με δεσμευτική νομική ισχύ που όμως θα μπορούσε να αμφισβητηθεί ενώπιον των αρμόδιων εθνικών δικαστηρίων

II. <u>Διαπίστευση από τον Εθνικό Οργανισμό Διαπίστευσης με την υποστήριξη της Αρχής Προστασίας Δεδομένων</u>.

Ο εθνικός φορέας διαπίστευσης κάθε κράτους μέλους παρέχει διαπίστευση σε φορείς πιστοποίησης σύμφωνα με το πρότυπο αξιολόγησης της συμμόρφωσης EN ISO / IEC 17065: 2012 και τις πρόσθετες απαιτήσεις που παρέχονται από την αρμόδια εποπτική αρχή ή την Ευρωπαϊκή Επιτροπή για την Προστασία των Δεδομένων (άρθρο 43 – παράγραφος 1 στοιχείο β, άρθρο 43 – παράγραφος 3, άρθρο 63).



Εικ.6. Συμμετέχοντες στον δεύτερο τρόπο διαπίστευσης

Οι κυριότεροι παράγοντες είναι ο Εθνικός Οργανισμός Διαπίστευσης, που κάθε Κράτος Μέλος διαθέτει, η Αρχή Προστασία Δεδομένων (αρμόδια εποπτική αρχή) και ο αιτών φορέας πιστοποίησης.

Η αρμόδια εποπτική (Αρχή Προστασίας Δεδομένων) δεν συμμετέχει άμεσα στη διαδικασία διαπίστευσης, αλλά παρέχει στον Εθνικό Οργανισμό Διαπίστευσης πρόσθετες απαιτήσεις, τις οποίες θα πρέπει να λάβει υπόψη του στην αξιολόγηση.

Κάθε φορέας πιστοποίησης που ενδιαφέρεται να προσφέρει υπηρεσίες με μηχανισμούς πιστοποίησης με βάση τα άρθρα 42 και 43 του ΓΚΠΔ, πρέπει να υποβάλει αίτηση για διαπίστευση στο Εθνικό Φορέα Διαπίστευσης, ο οποίος έχει συσταθεί σύμφωνα με τον Κανονισμό 765/2008. Ο κανονισμός για τη διαπίστευση χρησιμοποιεί το κριτήριο εγκατάστασης, προκειμένου να καθορίσει ποιο εθνικό όργανο διαπίστευσης είναι αρμόδιο.

Από το 2010 ισχύει και στην Ελλάδα ο Ευρωπαϊκός Κανονισμός (ΕΚ) αριθ. 765/2008 που αναφέρεται, ανάμεσα σε άλλα, στον καθορισμό των απαιτήσεων διαπίστευσης και εποπτείας της αγοράς, με τον οποίο καθιερώνεται το νομικό πλαίσιο για τη διαπίστευση στην Ευρώπη. Σύμφωνα με τον Κανονισμό αυτό, διαπίστευση είναι «η βεβαίωση από εθνικό οργανισμό διαπίστευσης ότι ένας οργανισμός αξιολόγησης της συμμόρφωσης πληροί τις απαιτήσεις που έχουν τεθεί με εναρμονισμένα πρότυπα και, όπου είναι εφαρμοστέο, τις τυχόν πρόσθετες απαιτήσεις, συμπεριλαμβανομένων αυτών που καθορίζονται στα αντίστοιχα τομεακά συστήματα, για να εκτελεί μια συγκεκριμένη δραστηριότητα αξιολόγησης της συμμόρφωσης» και ως εθνικός οργανισμός διαπίστευσης νοείται «ο μόνος οργανισμός κράτους μέλους που εκτελεί τη διαπίστευση επί τη βάσει εξουσίας που του παρέχει το κράτος αυτό»

Οι θεμελιώδεις αρχές επί των οποίων βασίζεται ο θεσμός της διαπίστευσης σύμφωνα με τον Κανονισμό 765/2008 είναι οι εξής:

- κάθε κράτος μέλος ορίζει έναν και μόνο εθνικό οργανισμό διαπίστευσης (άρθρο 4 – παράγραφος 1),
- η διαπίστευση συνιστά άσκηση δημόσιας εξουσίας (άρθρο 4 – παράγραφος 5),
- ο εθνικός οργανισμός διαπίστευσης λειτουργεί σε μη κερδοσκοπική βάση (άρθρο 4 – παράγραφος 7),
- ο εθνικός οργανισμός διαπίστευσης συγκροτεί και διατηρεί κατάλληλες δομές στην οργανωτική του διάρθρωση για τη διασφάλιση της αποτελεσματικής και ισόρροπης συμμετοχής όλων των ενδιαφερομένων (άρθρο 4 – παράγραφος 11),
- ο εθνικός οργανισμός διαπίστευσης δεν ανταγωνίζεται τους οργανισμούς αξιολόγησης της συμμόρφωσης (άρθρο 6 – παράγραφος 1),
- διαπίστευση χορηγείται μόνον σε νομικά πρόσωπα - οντότητες, και όχι σε φυσικά πρόσωπα (άρθρο 2 – παράγραφος 10 και 13).

Εκτός από τις απαιτήσεις που επιβάλλονται στο Εθνικό Οργανισμό Διαπίστευσης από τον Κανονισμό 765/2008, το ΓΚΠΔ προβλέπει ότι ο Εθνικός Οργανισμός Διαπίστευσης πρέπει να τηρεί τις απαιτήσεις ενός τεχνικού προτύπου αξιολόγησης της συμμόρφωσης. Το πρότυπο ISO / IEC 17065:2012 παρέχει ένα ευρύ φάσμα απαιτήσεων σε θέματα όπως:

- Νομικά και συμβατικά θέματα, συμπεριλαμβανομένης της ευθύνης
- Αμεροληψία, μη διακριτική μεταχείριση, εμπιστευτικότητα
- Οργανωτικά και διαρθρωτικά θέματα
- Διαδικασία αξιολόγησης, απόφασης, τεκμηρίωσης και επιτήρησης
- Παραπόνων και προσφυγών

Το πρότυπο ISO IEC 17065:2012 εφαρμόζεται στην πιστοποίηση προϊόντων, διαδικασιών και υπηρεσιών, αλλά στην περίπτωση των μηχανισμών πιστοποίησης προστασίας δεδομένων ΓΚΠΔ, το αντικείμενο της πιστοποίησης θα πρέπει να θεωρείται ως «επεξεργασία», όπως ορίζεται στο άρθρο 2 του ΓΚΠΔ.

Όσον αφορά τις διασφαλίσεις, διατάξεις του άρθρου 43 – παράγραφος 2 σχετικά με την ανεξαρτησία, την εμπειρογνωμοσύνη και άλλα, ισχύουν και για αυτό τον τρόπο διαπίστευσης όπως και στον πρώτο. Επιπλέον, η διαδικασία διαπίστευσης και οι διασφαλίσεις επιβάλλονται από τον κανονισμό 765/2008 στον οποίο υπόκεινται οι εθνικοί φορείς διαπίστευσης.

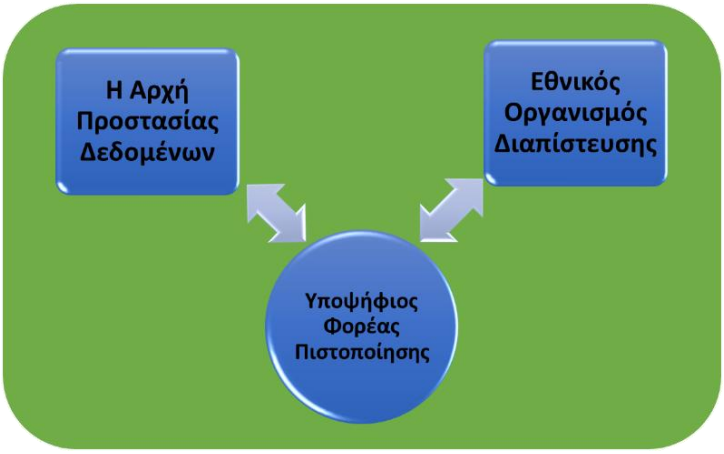
Οι εθνικοί φορείς διαπίστευσης αξιολογούν τις αιτήσεις των φορέων πιστοποίησης και αξιολογούν εάν ο φορέας αξιολόγησης της συμμόρφωσης είναι αρμόδιος για τη διεξαγωγή συγκεκριμένης δραστηριότητας αξιολόγησης της συμμόρφωσης. Στην περίπτωση του ΓΚΠΔ, η δραστηριότητα αξιολόγησης της συμμόρφωσης αναφέρεται στην πιστοποίηση Υπευθύνων και Εκτελούντων την Επεξεργασία βάσει εγκεκριμένων κριτηρίων πιστοποίησης. Η επιτυχής αξιολόγηση οδηγεί στην έκδοση πιστοποιητικού διαπίστευσης από τον εθνικό φορέα διαπίστευσης, το οποίο ισχύει για μέγιστο διάστημα πέντε ετών και μπορεί να ανανεωθεί.

Εκτός από τη διαδικασία αξιολόγησης, ο Εθνικός Οργανισμός Διαπίστευσης έχει την αρμοδιότητα και της επιτήρησης των διαπιστευμένων οργανισμών πιστοποίησης. Στις περιπτώσεις που ένας διαπιστευμένος οργανισμός πιστοποίησης δεν είναι πλέον αρμόδιος για την εκτέλεση της πιστοποίησης για την οποία έλαβε το πιστοποιητικό διαπίστευσης, ο Εθνικός Οργανισμός Διαπίστευσης οφείλει να λάβει τα κατάλληλα

μέτρα για τον περιορισμό, την αναστολή ή την ανάκληση της διαπίστευσης[13]. Αυτά τα μέτρα μπορούν επίσης να επιβληθούν και στην περίπτωση που ο οργανισμός πιστοποίησης έχει διαπράξει σοβαρή παράβαση των υποχρεώσεών του ή / και παραβιάζει τον ΓΚΠΔ. Συνήθως, οι υποχρεώσεις του διαπιστευμένου οργανισμού πιστοποίησης καθορίζονται σε συμβατική συμφωνία μεταξύ του Εθνικού Οργανισμού Διαπίστευσης και του οργανισμού πιστοποίησης.

III. <u>Διαπίστευση με συνδυασμό και του εθνικού Οργανισμού διαπίστευσης και της Αρχής Προστασίας Δεδομένων</u>.

Σε αυτόν τον τρόπο διαπίστευσης, τόσο ο Εθνικός Φορέας Διαπίστευσης όσο και η αρμόδια εποπτική αρχή διεξάγουν τη διαδικασία διαπίστευσης, πιθανότατα καθένας από αυτούς στο πεδίο αρμοδιοτήτων και εμπειρογνωμοσύνης τους. Ο τρόπος αυτός προκύπτει από τη διατύπωση « αμφότερα τα ακόλουθα »[14]



Εικ.7. Συμμετέχοντες στον τρίτο τρόπο διαπίστευσης

Στην περίπτωση αυτή έχουμε μια κοινή διαδικασία διαπίστευσης. Δεδομένου ότι τόσο ο Εθνικός Φορέας Διαπίστευσης όσο και η αρμόδια εποπτική αρχή διεξάγουν ένα μέρος της διαδικασίας διαπίστευσης. Η εποπτική αρχή θα καθορίσει τις διαδικασίες συνεργασίας και καθοδήγησης προς τους αιτούντες σχετικά με θέματα όπως το πού να υποβάλουν αίτηση, ποιος παρέχει το πιστοποιητικό διαπίστευσης και ποιος επιτηρεί και ανανεώνει τη διαπίστευση που κανένα από αυτά δεν ρυθμίζεται στο ΓΚΠΔ. Όσον αφορά στην αξιολόγηση από τον Εθνικό Οργανισμό Διαπίστευσης θα ήταν λογικό να

[13] Άρθρο 5 – παράγραφος 4 του ΕΚ 765/2008
[14] Άρθρο 43 – παράγραφος 1 του ΓΚΠΔ σελ 182

επικεντρωθεί στις απαιτήσεις διαδικαστικής, οργανωτικής και ακεραιότητας, όπως ορίζει ο Κανονισμός Διαπίστευσης και το πρότυπο ISO / IEC 17065: 2012. Στη συνέχεια

ακολουθεί η αξιολόγηση από την Αρχή Προστασίας Δεδομένων, η οποία να επικεντρώνεται μόνο στην αρμοδιότητα προστασίας των δεδομένων και την εμπειρογνωμοσύνη του αιτούντος φορέα πιστοποίησης.

Σχετικά με τις διαδικασίες και τις διασφαλίσεις, όλοι οι όροι του άρθρου 43 – παράγραφος 2 του ΓΚΠΔ σε συνδυασμό με τον κανονισμό διαπίστευσης και το τεχνικό πρότυπο ISO / IEC 17065: 2012 θα ισχύουν.

Σχέση του ΓΚΠΔ με τον Ευρωπαϊκό Κανονισμό Διαπίστευσης 765/2008

Όπως έχει ήδη αναφερθεί ο ΓΚΠΔ παρέχει ειδικούς κανόνες για τη διαπίστευση των φορέων πιστοποίησης που επιθυμούν να παρέχουν υπηρεσίες σύμφωνα με τους εγκεκριμένους μηχανισμούς πιστοποίησης της προστασίας δεδομένων του άρθρου. 42. Ταυτόχρονα, σε επίπεδο ΕΕ, ο κανονισμός διαπίστευσης ισχύει ήδη από το 2008 και εφαρμόζεται από το 2010 στα κράτη μέλη της ΕΕ. Το πεδίο εφαρμογής του κανονισμού για τη διαπίστευση δεν είναι ταυτόσημο με το πεδίο εφαρμογής των διατάξεων σχετικά με τη διαπίστευση του ΓΚΠΔ. Στόχος του κανονισμού είναι να θεσπίσει κανόνες για την οργάνωση της διαπίστευσης των φορέων διαπίστωσης της συμμόρφωσης που εκτελούν δραστηριότητες αξιολόγησης της συμμόρφωσης προϊόντων, διαδικασιών, υπηρεσιών, συστημάτων, προσώπων ή φορέων. Οι απαιτήσεις διαπίστευσης και αξιολόγησης της συμμόρφωσης αναφέρονται στην επεξεργασία των προσωπικών δεδομένων είναι πιο περιορισμένες σε σχέση με τον ευρωπαϊκό κανονισμό διαπίστευσης.

Όλες αυτές οι διαδικασίες και διασφαλίσεις, που αναφέρονται στο κανονισμό διαπίστευσης, εγγυώνται ότι ο φορέας διαπίστευσης μπορεί να παράσχει αξιόπιστες εκτιμήσεις σχετικά με το αν ένας υποψήφιος φορέας πιστοποίησης διαθέτει εκτός από την εμπειρογνωμοσύνη για την παροχή υπηρεσιών πιστοποίησης σε συγκεκριμένο τομέα, αλλά και αν παρέχει επίσης εγγυήσεις από άποψη της διαχείρισης, των πόρων, της ευθύνης, της εμπιστευτικότητας και άλλων θεμάτων.

Πρόσθετες απαιτήσεις διαπίστευσης – άρθρο 43 παράγραφος 1 σημείο β του ΓΚΠΔ

Θα μπορούσαμε να διακρίνουμε τρεις κύριες κατηγορίες πρόσθετων απαιτήσεων πέραν του κανονισμού περί διαπίστευσης και του προτύπου EN ISO / IEC 17065.

- Συμπληρωματικές απαιτήσεις σχετικά με τον οργανισμό πιστοποίησης και την εμπειρογνωμοσύνη των επιθεωρητών του στον τομέα της προστασίας δεδομένων.

  Η Αρχή Προστασίας Δεδομένων πρέπει να παρέχει συγκεκριμένες απαιτήσεις σχετικά με την εξειδίκευση και τις γνώσεις που απαιτούνται από τους φορείς πιστοποίησης στον τομέα της προστασίας δεδομένων και το ειδικό πεδίο εφαρμογής της συστήματος πιστοποίησης. Τόσο η επαγγελματική πείρα όσο και το εκπαιδευτικό υπόβαθρο στον νόμο περί προστασίας δεδομένων και στην ασφάλεια των πληροφοριών είναι απαραίτητες ικανότητες για τους επιθεωρητές που εργάζονται για διαπιστευμένους φορείς πιστοποίησης. Οι ίδιοι οι επιθεωρητές θα μπορούσαν επίσης να πιστοποιούνται ως εμπειρογνώμονες στον τομέα της προστασίας δεδομένων.

  Επομένως απαιτήσεις σε Γνώση και Εξειδίκευση σχετικά με:

  - τον ΓΚΠΔ και ενδεχομένως πιστοποιημένη. Για παράδειγμα, συγκεκριμένα κριτήρια αξιολόγησης της Αρχής Προστασίας Δεδομένων, ειδικό πλαίσιο αξιολόγησης και εργαλεία σχετικά με τεχνικά και οργανωτικά μέτρα ασφαλείας.
  - τη νομοθεσία για την προστασία της ιδιωτικής ζωής στον τομέα του ηλεκτρονικού χρήματος (ePrivacy), Αξιολογήσεις επιπτώσεων για την προστασία δεδομένων, ανωνυμοποίηση.

  και επιπρόσθετα πρακτική εμπειρία σε επιθεωρήσεις συστημάτων διαχείρισης ασφάλειας πληροφοριών.

- Πρόσθετες απαιτήσεις σχετικά με τον φορέα πιστοποίησης και την ικανότητα των επιθεωρητών του να διενεργούν επιθεωρήσεις.

  Εκτός από την εξειδίκευση στον τομέα που σχετίζεται με το πεδίο πιστοποίησης, ο φορέας πιστοποίησης και οι επιθεωρητές του πρέπει να έχουν κατάρτιση και δεξιότητες για τη διενέργεια επιθεωρήσεων. Η εμπειρία ως νομικός εμπειρογνώμονας ή ειδικός στον τομέα της ασφάλειας των πληροφοριών δεν συνεπάγεται ότι κάποιος γνωρίζει πώς να διενεργεί ελέγχους, πού να αναζητά τις απαραίτητες πληροφορίες, πώς να προσδιορίζει τις κατάλληλες μεθόδους για κάθε περίπτωση και άλλες δεξιότητες.

  - Εμπειρία και ικανότητα ως επιθεωρητής

- Γνώση και ειδίκευση στην επιχειρησιακή λογική ή στις διαδικασίες που σχετίζονται με διάφορους τομείς δραστηριότητας κ.λπ.

- Πρόσθετες απαιτήσεις σχετικά με την ακεραιότητα των επιθεωρητών και του φορέα πιστοποίησης.

  Η εποπτική αρχή θα χρειαστεί να παρέχει πρόσθετες απαιτήσεις στους φορείς διαπίστευσης σχετικά με την ακεραιότητα και την ανεξαρτησία τους. Οι απαιτήσεις θα πρέπει να βασίζονται στις γνώσεις και τις πρακτικές των Εθνικών Οργανισμών Διαπίστευσης για την αξιολόγηση της ακεραιότητας και της αμεροληψίας. Επίσης, οφείλουν να προσδιορίζουν συγκεκριμένα παραδείγματα σχετικά με τον τρόπο εφαρμογής αυτών των απαιτήσεων στο πλαίσιο της προστασίας δεδομένων, λαμβάνοντας υπόψη τις σχέσεις των μερών (Υπεύθυνοι επεξεργασίας, Εκτελούντες την επεξεργασία, φορείς πιστοποίησης), τις δραστηριότητες επεξεργασίας, την άσκηση των δικαιωμάτων των υποκειμένων των δεδομένων και τη φύση των δεδομένων.

  - Καταλληλότητα στο πλαίσιο των δικαιωμάτων των πληροφοριών
  - Επάρκεια και συνάφεια των πόρων
  - Ανεξαρτησία
  - Απαιτήσεις αμεροληψίας και σύγκρουσης συμφερόντων

<u>Διαπίστευση σε φορείς πιστοποίησης που δραστηριοποιούνται σε πολλές χώρες</u>

Ειδική περίπτωση αποτελεί η διαπίστευση φορέων πιστοποίησης που είναι εγκατεστημένοι σε πολλές χώρες και ειδικά στην περίπτωση της πιστοποίησης για μεταφορά δεδομένων οπού θα πρέπει να ληφθεί υπόψη η γεωγραφική θέση του φορέα πιστοποίησης. Ο ΓΚΠΔ δεν διευκρινίζει εάν ο φορέας πιστοποίησης θα μπορούσε να εγκατασταθεί σε τρίτη χώρα και εάν θα μπορούσε να αναθέσει σε τοπικούς συνεργάτες των οργανισμών πιστοποίησης τμημάτων της διαδικασίας πιστοποίησης (όπως προ-αξιολόγηση και συλλογή τεκμηρίωσης). Ενώ απαιτείται ειδική καθοδήγηση από το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων για το συγκεκριμένο ζήτημα ειδικά σε σχέση με τους μηχανισμούς πιστοποίησης της προστασίας δεδομένων με βάση τον ΓΚΠΔ, υπάρχει ήδη σημαντική εμπειρία από τις πρακτικές διαπίστευσης σε άλλους τομείς, η οποία ενσωματώνεται στην καθοδήγηση του Παγκόσμιου Οργανισμός για την Αξιολόγηση της Συμμόρφωσης των Φορέων Διαπίστευσης (IAF).

Ο IAF έχει εκδώσει καθοδήγηση σχετικά με την αρμοδιότητα των αξιολογητών του φορέα διαπίστευσης σύμφωνα με το πρότυπο ISO / IEC 17011. Οι αρμοδιότητες των αξιολογητών καλύπτουν γενικά θέματα διαπίστευσης (όπως δομές νομικών οντοτήτων, πρότυπα διαπίστευσης, τεχνικοί όροι που σχετίζονται με τη διαπίστευση), σχεδιασμού και προγραμματισμού (όπως η ιεράρχηση των αξιολογήσεων ανά περιοχές κινδύνου, η προετοιμασία των σχεδίων αξιολόγησης, οι πόροι που απαιτούνται κατά την αξιολόγηση και άλλα), αναθεώρησης εγγράφων, επιτόπιας αξιολόγησης και δραστηριότητες υποβολής εκθέσεων. Επιπλέον, ο IAF περιγράφει δεξιότητες ηγεσίας, συμπεριφοράς και οργάνωσης και προβλέπει ότι ο φορέας διαπίστευσης φέρει ευθύνη να διασφαλίσει ότι όλες οι δραστηριότητες του υπό αξιολόγηση φορέα πιστοποίησης είναι σύμφωνες με τα σχετικά πρότυπα, ανεξάρτητα από τον ή τους τόπους στους οποίους εκτελούνται αυτές οι δραστηριότητες[15]. Υπάρχουν περιπτώσεις που οι δραστηριότητες αξιολόγησης της συμμόρφωσης εκτελούνται από προσωπικό, απομακρυσμένα, το οποίο χρησιμοποιεί κατάλληλο σύστημα πληροφορικής. Το όργανο διαπίστευσης πρέπει να εκπονήσει πρόγραμμα αξιολόγησης που να του επιτρέπει να επιβεβαιώνει τη συμμόρφωση των δραστηριοτήτων του φορέα πιστοποίησης στο πλαίσιο της διαπίστευσης. Στοιχεία ενός τέτοιου προγράμματος αξιολόγησης περιλαμβάνουν την αποτελεσματικότητα των ελέγχων διαχείρισης του φορέα πιστοποίησης, εάν ο οργανισμός πιστοποίησης είναι διαπιστευμένος από τον Εθνικό του Φορέα Διαπίστευσης, τις βασικές δραστηριότητες που εκτελούνται από το προσωπικό που είναι εγκατεστημένο σε μια ξένη χώρα και άλλα. Η αξιολόγηση πρέπει να πραγματοποιηθεί όχι μόνο στην αρχική φάση της αίτησης διαπίστευσης αλλά και σε μεταγενέστερο στάδιο μετά από μια περίοδο επιτήρησης που ακολουθεί την έκδοση του πιστοποιητικού διαπίστευσης.

<u>Πιστοποίηση ως μέσο μεταφοράς δεδομένων</u>

Σχετικά με τη μεταφορά δεδομένων σε Υπευθύνους και Εκτελούντες την επεξεργασία που ανήκουν σε χώρες εκτός Ευρωπαϊκής Ένωσης, ο ΓΚΠΔ δεν αφήνει περιθώρια για «εκπτώσεις» στην προστασία των προσωπικών δεδομένων. Επιπρόσθετα παρέχει άλλες νομικές βάσεις για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες ή σε διεθνείς οργανισμούς μέσω κατάλληλων διασφαλίσεων. Στην περίπτωση αυτή ο υποψήφιος οργανισμός για πιστοποίηση (άρθρο 42 – παράγραφος 2) είναι ο εισαγωγέας δεδομένων, Υπεύθυνος

[15] IAF, Accreditation Assessment of Conformity Assessment Bodies with Activities in Multiple Countries, Issue 2, 2016

επεξεργασίας / Εκτελών την επεξεργασία, που είναι εγκατεστημένος σε τρίτη χώρα και δεν υπόκεινται στον ΓΚΠΔ. Ειδικότερα ο Υπεύθυνος επεξεργασίας / Εκτελών την επεξεργασία, που είναι εγκατεστημένοι σε τρίτες χώρες ή στους διεθνείς οργανισμούς (παραλήπτες / εισαγωγείς δεδομένων), μπορούν, μέσω της τήρησης ενός μηχανισμού πιστοποίησης προστασίας δεδομένων, να αποδείξουν την ύπαρξη κατάλληλων διασφαλίσεων, ότι επεξεργάζονται τα δεδομένα με τρόπο συμβατό προς τον ΓΚΠΔ, για τον Υπεύθυνο επεξεργασίας / Εκτελών την επεξεργασία που υπόκεινται στον ΓΚΠΔ και επιθυμούν να εξάγουν προσωπικά δεδομένα (εξαγωγείς δεδομένων).

Αντικείμενο της πιστοποίησης, με σκοπό την απόδειξη ύπαρξης των κατάλληλων διασφαλίσεων του άρθρου 42 – παράγραφος 2, είναι μια διαδικασία επεξεργασίας ή ένα σύνολο εργασιών επεξεργασίας ενός Υπευθύνου ή Εκτελούντος την επεξεργασία. Λαμβάνοντας υπόψη τους περιορισμούς της εδαφικής αρμοδιότητας των εποπτικών αρχών της Ευρωπαϊκής Ένωσης σε συνδυασμό με τις πρακτικές δυσκολίες που συνεπάγεται η πιστοποίηση ενός εισαγωγέα δεδομένων σε μια τρίτη χώρα, είναι πολύ πιθανό ότι οι διαπιστευμένοι φορείς πιστοποίησης θα πραγματοποιούν πιστοποίηση στην περίπτωση του άρθρου 42 παράγραφος 2. Είναι αντιληπτό ότι η θέση του Υπευθύνου / Εκτελών την επεξεργασία σε μια τρίτη χώρα συνεπάγεται διοικητικές επιβαρύνσεις και επιβαρύνσεις πόρων, καθώς ο διαπιστευμένος φορέας πιστοποίησης πρέπει να έχει τη δυνατότητα να διεξάγει τη διαδικασία πιστοποίησης και να παρακολουθεί αποτελεσματικά την πιστοποίηση που εκδόθηκε. Παράλληλα η αρμόδια εποπτική αρχή ή ο Εθνικός Οργανισμός Διαπίστευσης θα πρέπει να εξασφαλίσουν ότι ο φορέας πιστοποίησης είναι σε θέση να επιτηρεί τον Υπεύθυνο / Εκτελών την επεξεργασία στην Τρίτη χώρα.

Σχετικά με τον διαπιστευμένο φορέα πιστοποίησης είναι δυνατά τα ακόλουθα σενάρια:

I. <u>Ο διαπιστευμένος οργανισμός πιστοποίησης είναι εγκατεστημένος στην ΕΕ και παρέχει διασυνοριακή πιστοποίηση στην τρίτη χώρα</u>

   Ο φορέας πιστοποίησης πρέπει να διασφαλίζει ότι είναι σε θέση να ασκεί αποτελεσματικά το έργο του στην τρίτη χώρα. Συνήθως, αυτό είναι δυνατό με τη συνεργασία ενός τοπικού οργανισμού πιστοποίησης στην τρίτη χώρα. Ο τοπικός οργανισμός πιστοποίησης (υπεργολάβος) εκτελεί τις δραστηριότητές εκ μέρους του διαπιστευμένου φορέα πιστοποίησης και αποτελεί ξεχωριστή νομική οντότητα και οργάνωση. Κατά την καθιέρωση συνεργασίας με έναν τοπικό φορέα πιστοποίησης, ο φορέας πιστοποίησης που είναι εγκατεστημένος στην Ευρωπαϊκή Ένωση θα πρέπει να

ζητήσει εγγυήσεις ότι ο τοπικός συνεργάτης θα ανταποκριθεί στα υψηλά πρότυπα των απαιτήσεων διαπίστευσης του άρθρου 43 του ΓΚΠΔ, στις απαιτήσεις του κανονισμού 765/2008 και του ISO / IEC 17011. Επιπλέον, ο τοπικός φορέας πιστοποίησης θα πρέπει να είναι σε θέση να παρέχει πιστοποίηση με βάση το πρότυπο ISO / IEC 17065. Ένας ασφαλής τρόπος διασφάλισης του υψηλού επιπέδου είναι η διαπίστευση του τοπικού φορέα πιστοποίησης (στην τρίτη χώρα) από τον Εθνικό Οργανισμό Διαπίστευσης της εν λόγω χώρας που συμμετέχει στο Διεθνές Φόρουμ Διαπίστευσης (IAF).

Συνεπώς κατά τη διαπίστευση του φορέα πιστοποίησης που είναι εγκατεστημένος στην Ευρωπαϊκή Ένωση πρέπει να εξεταστεί, μεταξύ άλλων θεμάτων, ο τρόπος με τον οποίο ο φορέας πιστοποίησης, που έχει συσταθεί στην Ευρωπαϊκή Ένωση, θα διεξάγει και θα διαχειρίζεται τις δραστηριότητές του στην τρίτη χώρα.

II. <u>Ο διαπιστευμένος οργανισμός πιστοποίησης έχει εγκαταστάσεις στην Ευρωπαϊκή Ένωση ή / και σε τρίτη χώρα</u>

Υπάρχουν δύο δυνατότητες για τον διαπιστευμένο φορέα πιστοποίησης που προσφέρει υπηρεσίες πιστοποίησης πολλαπλών τοποθεσιών:

A. Έχει την κύρια εγκατάστασή του σε τρίτη χώρα ή / και εγκατάσταση ή υποκατάστημα σε κράτος μέλος της Ευρωπαϊκής Ένωσης, ή

B. Η κύρια εγκατάστασή του βρίσκεται στην Ευρωπαϊκή Ένωση και επιχειρησιακά υποκαταστήματα σε μία ή περισσότερες τρίτες χώρες (όπου βρίσκονται οι εισαγωγείς δεδομένων).

Σύμφωνα με τον IAF, ένας σημαντικός παράγοντας για τη διαδικασία διαπίστευσης είναι η «κρίσιμη θέση (-ες)», η οποία είναι ο τόπος ή οι τόποι όπου ο οργανισμός πιστοποίησης εκτελεί τις κύριες δραστηριότητές του. Συνήθως, η κεντρική υπηρεσία λαμβάνει το πιστοποιητικό διαπίστευσης και οι τοπικοί χώροι πραγματοποιούν διαπίστευση στο πλαίσιο του χορηγούμενου πιστοποιητικού.

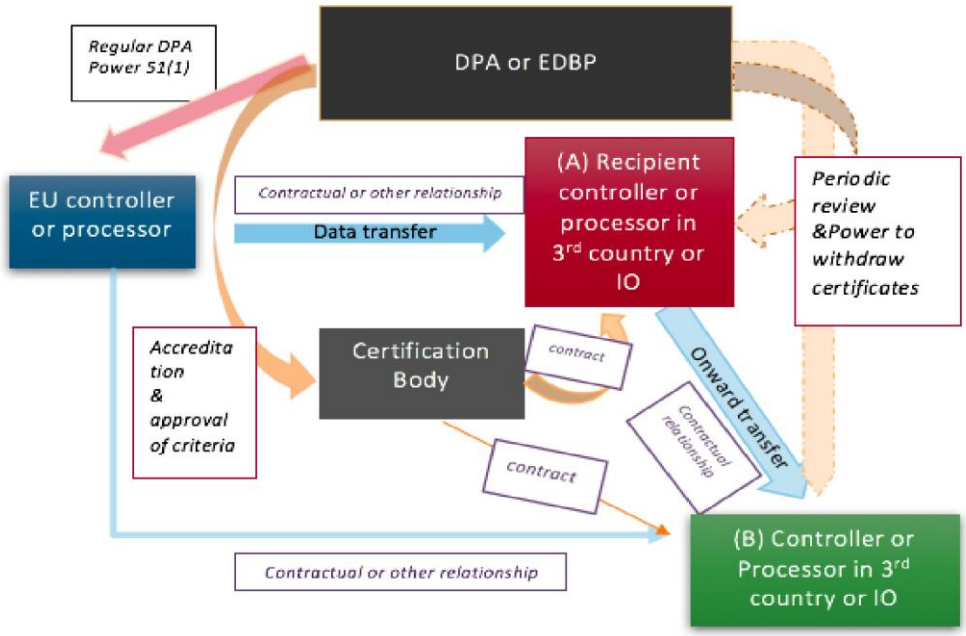
Στην περίπτωση φορέα πιστοποίησης, διαπιστευμένου σύμφωνα με το άρθρο. 43 του ΓΚΠΔ, ο οποίος έχει την κύρια εγκατάστασή του στην τρίτη χώρα, η διαδικασία πιστοποίησης και η επιτήρηση της χορηγούμενης πιστοποίησης είναι ευκολότερες. Σε κάθε περίπτωση μπορεί να προκύψουν δυσκολίες όσον αφορά το πώς η διαπίστευση και ο συντονισμός με τις εποπτικές αρχές της Ευρωπαϊκής Ένωσης είναι οργανωμένα.

Υπάρχει τεκμήριο ότι, μόλις εγκριθεί ένας μηχανισμός πιστοποίησης προστασίας δεδομένων από μια εποπτική αρχή σε ένα κράτος μέλος ή από το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων, σύμφωνα με το άρθρο 5 του ΓΚΠΔ, ο Υπεύθυνος επεξεργασίας ή ο Εκτελών την επεξεργασία, που τηρεί τον εν λόγω μηχανισμό πιστοποίησης, παρέχει τις διασφαλίσεις που απαιτούνται για τη διαβίβαση δεδομένων σύμφωνα με το άρθρο. 46. Κατ' αυτόν τον τρόπο, η διαδικασία πιστοποίησης πρέπει να είναι διεξοδική, δεδομένου ότι η χορήγηση της πιστοποίησης συνεπάγεται ότι ο εισαγωγέας δεδομένων πληροί καταρχήν την παραλαβή και επεξεργασία δεδομένων προσωπικού χαρακτήρα από έναν εξαγωγέα δεδομένων της Ευρωπαϊκής Ένωσης.

Το τεκμήριο ύπαρξης διασφαλίσεων που προσφέρονται από την τήρηση ενός εγκεκριμένου μηχανισμού πιστοποίησης μετατοπίζει σημαντικό βάρος τόσο στις εποπτικές αρχές όσο και στους φορείς πιστοποίησης. Η έγκριση των κριτηρίων πιστοποίησης προστασίας δεδομένων από τις εποπτικές αρχές ή το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων καθορίζει εάν ένας μηχανισμός πιστοποίησης παρέχει όλα τα απαραίτητα κριτήρια για να διασφαλίσει ότι ο πιστοποιημένος Υπεύθυνος επεξεργασίας ή Εκτελών την επεξεργασία μπορεί καταρχήν να παρέχει τις κατάλληλες διασφαλίσεις για τις μεταφορές δεδομένων. Ο φορέας πιστοποίησης έχει την ευθύνη να εφαρμόσει τα κριτήρια και να καθορίσει εάν ο αιτών εισαγωγέας δεδομένων είναι συμμορφωμένος σε αυτά και τα τηρεί.

Ο Υπεύθυνος επεξεργασίας – εξαγωγέας, ο οποίος υπάγεται στον ΓΚΠΔ, παραμένει υπεύθυνος, έναντι των αρμόδιων εποπτικών αρχών της Ευρωπαϊκής Ένωσης, να αποδείξει την ύπαρξη διασφαλίσεων που παρέχονται από τον εισαγωγέα Υπεύθυνο επεξεργασίας ή Εκτελών την επεξεργασία, συμπεριλαμβανομένης της απαγόρευσης, της ανάκλησης ή της απόσυρσης της πιστοποίησης κατά τη διάρκεια της επεξεργασίας των μεταβιβασμένων προσωπικών δεδομένων.

Η παρακάτω εικόνα προσδιορίζει το σενάριο μιας ενιαίας μεταφοράς δεδομένων σε χώρα εκτός της Ευρωπαϊκής Ένωσης και μιας μετάβασης σε άλλη χώρα εκτός Ευρωπαϊκής Ένωσης (Η πιστοποίηση χορηγείται από διαπιστευμένο οργανισμό πιστοποίησης).



Εικ.8. Επισκόπηση των νομικών σχέσεων στις μεταβιβάσεις δεδομένων σε πιστοποιημένους υπεύθυνους επεξεργασίας / επεξεργασίας σε τρίτες χώρες.[16]

Στην παραπάνω εικόνα προσδιορίζονται οι ακόλουθες σχέσεις:

- Υπεύθυνος Επεξεργασίας / Εκτελών την επεξεργασία εγκατεστημένος στην Ευρωπαϊκή Ένωση (Εξαγωγέας) και Υπεύθυνος Επεξεργασίας / Εκτελών την επεξεργασία εγκατεστημένος σε τρίτη χώρα (Παραλήπτης / Εισαγωγέας): Αυτή αποτελεί τον κεντρικό άξονα της μεταφοράς δεδομένων. Μια συμβατική σχέση πιθανότατα, αλλά όχι απαραίτητα, να καθιερωθεί.
- Υπεύθυνος Επεξεργασίας / Εκτελών την επεξεργασία (Εισαγωγέας) και φορέας πιστοποίησης που χορηγεί πιστοποίηση σύμφωνα με τις απαιτήσεις του ΓΚΠΔ. Ο Υπεύθυνος επεξεργασίας ή ο Εκτελών την επεξεργασία στην τρίτη χώρα ή τον Διεθνή Οργανισμό πρέπει να πιστοποιηθεί σύμφωνα με το άρθρο. 42 και 43 προτού ξεκινήσει την επεξεργασία των προσωπικών δεδομένων.

  Ο Εισαγωγέας δεδομένων είναι σημαντικό να παρέχει νομικές και εκτελεστικές δεσμεύσεις. Συνήθως, ο φορέας πιστοποίησης και ο αιτών πιστοποίησης συνάπτουν συμβατική συμφωνία που περιγράφει τους όρους χορήγησης της πιστοποίησης, τις υποχρεώσεις και των δύο μερών και άλλα συναφή θέματα σχετικά με την πιστοποίηση.

[16] Data Protection Certification Mechanisms - Study on Articles 42 and 43 of the Regulation (EU) 2016/679 – Final Report, σελ 185

- Αρχή Προστασίας Δεδομένων / Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων και Υπεύθυνος Επεξεργασίας / Εκτελών την επεξεργασία εγκατεστημένος στην Ευρωπαϊκή Ένωση (Εξαγωγέας). Ο Εξαγωγέας δεδομένων υπόκειται στις εξουσίες έρευνας της αρμόδιας εποπτικής αρχής όσον αφορά την επεξεργασία δεδομένων που πραγματοποιεί ο ίδιος ο Εξαγωγέας και οι Εκτελούντες την επεξεργασία δεδομένων που επεξεργάζονται δεδομένα για λογαριασμό του Εξαγωγέα δεδομένων ή σε συνεργασία με τον Εξαγωγέα δεδομένων.
- Αρχή Προστασίας Δεδομένων / Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων και Φορέας Πιστοποίησης. Ένας φορέας πιστοποίησης πρέπει να διαπιστευθεί από την αρμόδια εποπτική αρχή ή από τον Εθνικό Οργανισμό Διαπίστευσης. Η Αρχή Προστασίας Δεδομένων έχει την εξουσία να ανακαλέσει τη διαπίστευση όταν οι όροι για τους οποίους χορηγήθηκε δεν πληρούνται πλέον και επίσης εγκρίνει τα κριτήρια πιστοποίησης.
- Υπεύθυνος Επεξεργασίας / Εκτελών την επεξεργασία (Εισαγωγέας) και αρμόδια Αρχή Προστασίας Δεδομένων ή Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. Πρόκειται για έμμεση σχέση, που δεν έχει θεσπιστεί επίσημα στον ΓΚΠΔ, δεδομένου ότι Υπεύθυνος Επεξεργασίας / Εκτελών την επεξεργασία, παραλήπτης στην τρίτη χώρα, δεν εμπίπτει στη δικαιοδοσία της Αρχής Προστασίας Δεδομένων. Η Αρχή Προστασίας Δεδομένων είναι αρμόδια για την επίβλεψη της μεταφοράς δεδομένων, η οποία αποτελεί δραστηριότητα επεξεργασίας. Ωστόσο, όσον αφορά την πιστοποίηση που έχει απονεμηθεί, η Αρχή Προστασίας Δεδομένων έχει το καθήκον και την εξουσία να διεξάγει (περιοδικές) αναθεωρήσεις των πιστοποιητικών που έχουν εκδοθεί και να διατάξει τον φορέα πιστοποίησης να αποσύρει πιστοποίηση όταν δεν πληρούνται πλέον οι όροι έκδοσης. Οι εξουσίες αυτές της Αρχή Προστασίας Δεδομένων συνεπάγονται ότι, τουλάχιστον για την χορηγούμενη πιστοποίηση, ο παραλήπτης πιστοποιημένος Υπεύθυνος Επεξεργασίας / Εκτελών την επεξεργασία υπόκειται στην εποπτεία μίας Αρχή Προστασίας Δεδομένων της Ευρωπαϊκής Ένωσης.
- Υπεύθυνος Επεξεργασίας / Εκτελών την επεξεργασία του παραλήπτη (Εισαγωγέας) (Α) και επόμενος Υπεύθυνος Επεξεργασίας / Εκτελών την επεξεργασία (Β). Ο επόμενος Υπεύθυνος Επεξεργασίας / Εκτελών την επεξεργασία πρέπει να συμμορφώνεται με τους όρους μεταβίβασης (άρθρο 44 του ΓΚΠΔ). Εάν η χώρα του Υπεύθυνου Επεξεργασίας / Εκτελούντα την επεξεργασία προσφέρει επαρκές επίπεδο της προστασίας, όπως

αποφασίστηκε από την Επιτροπή με μια Απόφαση Επάρκειας, δεν υπάρχει ανάγκη πιστοποίησης του επόμενου Υπεύθυνου Επεξεργασίας / Εκτελούντα την επεξεργασία. Ωστόσο, εάν αυτή η τρίτη χώρα δεν εξασφαλίζει επαρκές επίπεδο προστασίας, μία από τις διασφαλίσεις του άρθρου 46 πρέπει να προβλεφθεί.

- Επόμενος Υπεύθυνος Επεξεργασίας / Εκτελών την επεξεργασία και αρμόδια Αρχή Προστασίας Δεδομένων ή Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. Ισχύει ό,τι και για τη σχέση μεταξύ Υπεύθυνού Επεξεργασίας / Εκτελούντα την επεξεργασία και Αρχής Προστασίας Δεδομένων ενός κράτους μέλους.
- Επόμενος Υπεύθυνος Επεξεργασίας / Εκτελών την επεξεργασία και Υπεύθυνος Επεξεργασίας / Εκτελών την επεξεργασία εγκατεστημένος στην Ευρωπαϊκή Ένωση (Εξαγωγέας). Η σχέση αυτή μπορεί να επισημοποιηθεί με διμερή σύμβαση ή να καλύπτεται από εξουσιοδότηση του Υπεύθυνου επεξεργασίας δεδομένων της Ευρωπαϊκής Ένωσης προς τον παραλήπτη Εκτελούντα την επεξεργασία. Σε κάθε περίπτωση, δεδομένου ότι ο επόμενος Εκτελών επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του Υπευθύνου της Ευρωπαϊκής Ένωσης, ο τελευταίος είναι υπεύθυνος για τυχόν παραβιάσεις του ΓΚΠΔ.

2.7. Υφιστάμενη κατάσταση

Παρά την καινοτομία των μηχανισμών προστασίας δεδομένων του ΓΚΠΔ, μπορούν να αντληθούν πολύτιμα διδάγματα από την ανάλυση των υφιστάμενων πιστοποιήσεων. Οι υπάρχουσες πιστοποιήσεις έχουν ήδη θεσπίσει μηχανισμούς, μεθοδολογίες αξιολόγησης, συμβατικές ρυθμίσεις και επιθεωρητές που μπορούν και πρέπει να χρησιμοποιηθούν για τη δημιουργία των μηχανισμών προστασίας δεδομένων ΓΚΠΔ. Από έρευνες που έχουν γίνει εντοπίστηκαν μοντέλα πιστοποιήσεων με ποικίλο βαθμό συμμετοχής των δημόσιων αρχών, από ιδιωτικά συστήματα πιστοποίησης έως πιστοποιήσεις που ανήκουν σε δημόσιες αρχές.

Σκοπός αυτού του κεφαλαίου είναι να δοθούν πληροφορίες για τον τρόπο λειτουργίας της αγοράς πιστοποίησης προστασίας των δεδομένων και να προσφερθούν «ιδέες» και καλές πρακτικές στους μηχανισμούς πιστοποίησης προστασίας δεδομένων με βάση τα άρθρα 42 και 43 του ΓΚΠΔ. Εξετάζεται το υφιστάμενο περιβάλλον πιστοποίησης στην Ευρωπαϊκή Ένωση και εκτός της Ευρωπαϊκή Ένωση, με στόχο να αντληθεί εμπειρία από την αγορά.

Τα στοιχεία που αναφέρονται έχουν αντληθεί από το κεφάλαιο 3 του «Data Protection Certification Mechanisms - Study on Articles 42 and 43 of the Regulation (EU) 2016/679 – Final Report» και του κεφαλαίου 4 του «Recommendations on European Data Protection Certification VERSION 1.0 NOVEMBER 2017»

Τα αποτελέσματα έχουν προκύψει από την ανάλυση των παρακάτω πιστοποιήσεων:

1. BS 10012 Personal Information Management System Certification (UK)

   Είναι πιστοποίηση που βασίζεται στο βρετανικό τεχνικό πρότυπο BS 10012: Προστασία Προσωπικών Δεδομένων 2009 - Προδιαγραφή για ένα Σύστημα Διαχείρισης Προσωπικών Πληροφοριών: μια Μεθοδολογία Εφαρμογής. Στόχος της είναι η βελτίωση της συμμόρφωσης με τη νομοθεσία για την προστασία των δεδομένων και την αναγνωρισμένη βέλτιστη πρακτική και περιλαμβάνει απαιτήσεις που αντιπροσωπεύουν τις αρχές προστασίας δεδομένων, συμπεριλαμβανομένης ειδικής έκδοσης προσαρμοσμένης στις Μικρές και Μεσαίου μεγέθους Επιχειρήσεις. Η πιστοποίηση αυτή επικεντρώνεται στις διαδικασίες διαχείρισης πληροφοριών.[17]

2. TÜV Italia ISO/IEC 27001 Information Security Management Certification

   Είναι ένα συστήματα πιστοποίησης που βασίζεται στο ευρέως υιοθετημένο πρότυπο για τα Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών που έχει εκδοθεί από τον Διεθνή Οργανισμό Τυποποίησης. Παρέχει μια συστηματική προσέγγιση όσον αφορά τη διαχείριση και προστασία υπολογιστών, κέντρων δεδομένων και δεδομένων και συνεπώς αφορά την προστασία των δεδομένων.

3. BSI ISO/IEC 27018 Information technology. Security techniques. Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors Certification (UK)

   Είναι μια πιστοποίηση για το Cloud που απευθύνεται σε δημόσιους παρόχους υπηρεσιών cloud που λειτουργούν ως επεξεργαστές αναγνωρίσιμων προσωπικών πληροφοριών (PII). Βασίζεται στο πρότυπο ISO / IEC 27018 Τεχνολογία Πληροφοριών - Κώδικας πρακτικής για την προστασία αναγνωρίσιμων προσωπικών πληροφοριών (PII) σε δημόσια νέφη που λειτουργούν ως επεξεργαστές PII. Βασίζεται στους γενικούς ελέγχους που περιγράφονται στο ISO / IEC 27002 και είναι κατάλληλο για κάθε

[17] The British Standards Institution, 'Personal Information Management',(Bsigroup) <https://www.bsigroup.com/en-GB/BS-10012-Personal-information-management/>

οργανισμό που επεξεργάζεται προσωπικά δεδομένα. Επιπλέον, χρησιμοποιείται σε συνδυασμό με το ISO / IEC 27001 (δηλ. Ο υποψήφιος οργανισμός θα χρειαστεί πρώτα πιστοποίηση σύμφωνα με το πρότυπο ISO / IEC 27001 για να μπορέσει να λάβει πιστοποίηση σύμφωνα με το BSI ISO / IEC 27018.)

4. Certificazione ISDP 10003:2015 Data protection (IT)

   Είναι ένα σύστημα πιστοποίησης σύμφωνο με το πρότυπο ISO / IEC 17065:2012 και βασίζεται στο πρότυπο ISDP 10003: 2015. Το πρότυπο ISDP καθορίζει απαιτήσεις σχετικά με τις αρχές προστασίας δεδομένων του κανονισμού για την προστασία των δεδομένων. Επίσης, περιγράφει τις απαιτήσεις ασφαλείας και τους ελέγχους ώστε τα δεδομένα να ανταποκρίνονται στην ακρίβεια, επικαιρότητα, συνέπεια, πληρότητα, αξιοπιστία και τα επίπεδα ενημέρωσης που απαιτούνται από τους ισχύοντες κανονισμούς προστασίας προσωπικών δεδομένων, με ιδιαίτερη προσοχή στις αρχές της ποιότητας και της ασφάλειας των δεδομένων. Το σύστημα ανήκει στην INVEO και η πιστοποίηση διενεργείται από εξωτερικούς φορείς πιστοποίησης.[18]

5. Datenschutzaudit beim ULD (DE)

   Είναι μια πιστοποίηση που απευθύνεται σε δημόσιους φορείς. Πιστοποιεί βάσει του νόμου περί προστασίας δεδομένων του Schleswig-Holstein (LDSG). Η πιστοποίηση αξιολογεί ολόκληρες διαδικασίες επεξεργασίας δεδομένων, ξεχωριστά μέρη τους και διαδικασίες ατομικής επεξεργασίας δεδομένων. Περίπου 15 δημόσιοι οργανισμοί έχουν πιστοποιηθεί από το 2007 σύμφωνα με το δημόσιο μητρώο της ULD. Η επιθεώρηση πραγματοποιείται από το ULD (DPA Schleswig-Holstein)[19]

6. E-privacy app (DE)[20]

   Είναι ένα σύστημα πιστοποίησης αφιερωμένο στην αντιμετώπιση εφαρμογών κινητής τηλεφωνίας για την αξιολόγηση της συμμόρφωσης με τον ΓΚΠΔ, το IAB Europe Online Behavioral Advertising Framework - Πλαίσιο Διαφήμισης με Ανάλυση Συμπεριφοράς (που διέπει την αυτορρύθμιση από τον κλάδο της ψηφιακής διαφήμισης) και τη Γερμανική νομοθεσία προστασίας δεδομένων. Το E-privacy app προσφέρει δύο

[18] InVeo, 'ISDP 10003:2015 Data Protection Certification' (InVeo Accredited Certification Body) <https://www.in-veo.com/en/certification/isdp-10003-2015-data-protection>
[19] ULD, ' Datenschutzaudit beim ULD' (ULD, 2018) <https://www.datenschutzzentrum.de/audit/ >
[20] E- Privacy seal<https://www.eprivacy.eu/en/privacy-seals/eprivacyseal/>

επίπεδα ωριμότητας πιστοποίησης ανάλογα με την ευαισθησία των δεδομένων που επεξεργάζονται στις εφαρμογές.

7. EuroPrise - the European Privacy Seal (DE)

   Είναι ένα πανευρωπαϊκό σύστημα πιστοποίησης που αναπτύχθηκε για προϊόντα και υπηρεσίες βασισμένα σε τεχνολογίες πληροφορικής, από το 2007 έως το 2009, για να πιστοποιήσει ως προς τη νομοθεσία προστασίας δεδομένων σε επίπεδο Ευρωπαϊκής Ένωσης (DPD). Από τον Ιανουάριο του 2017 το σύστημα καλύπτει τον ΓΚΠΔ. Στην ανάπτυξη της πιστοποίησης συνέβαλε και η ULD (DPA of Germany) και σήμερα λειτουργεί από ιδιωτικό φορέα (EuroPrise GmbH). Από το 2008 έως τον Οκτώβριο του 2017 χορηγήθηκαν περίπου 35 πιστοποιητικά.[21]

8. IkeepSafe Coppa Safe Harbor[22] (US)

   Σκοπός του συστήματος είναι να διασφαλίσει ότι οι πρακτικές που αφορούν τη συλλογή, τη χρήση, τη συντήρηση και η αποκάλυψη προσωπικών πληροφοριών από παιδιά ηλικίας κάτω των 13 ετών συνάδει με τις αρχές και τις απαιτήσεις του νόμου για την προστασία της ιδιωτικής ζωής των παιδιών στο Διαδίκτυο (COPPA) των ΗΠΑ. Έχει πιστοποιήσει περίπου 10 εφαρμογές, λύσεις cloud και υπηρεσίες ιστού σύμφωνα με το δημόσιο μητρώο του συστήματος και ανήκει σε μη κερδοσκοπική οργάνωση.[23]

9. Label CNIL digital safe boxes (FR)

   Είναι πιστοποίηση που προβλέπεται από το άρθρο 11(3) και (3) (γ) του τροποποιημένου γαλλικού νόμου περί προστασίας δεδομένων της 6ης Ιανουαρίου 1978 και βασίζεται στο πρότυπο CNIL's[24]. Το CNIL πιστοποιεί τη συμμόρφωση των ψηφιακών θόλων που είναι, σύμφωνα με το CNIL, «αποθηκευτικοί χώροι, δεδομένου ότι τα δεδομένα που αποθηκεύονται εκεί (έγγραφα και μεταδεδομένα) είναι προσβάσιμα μόνο στον κάτοχο της χώρου» σύμφωνα με τους κανόνες του Γαλλικού νόμου περί προστασίας δεδομένων μεταφρασμένο σε απαιτήσεις.

10. Health Personal Data Storage Agreement (FR)

[21] EuroPrise, 'European Privacy Seal' (European Privacy Seal for IT Products and IT-Based Services) <https://www.european-privacy-seal.eu/EPS-en/Home >
[22] Safe harbor αναφέρεται σε οποιοδήποτε μέρος ή τοποθεσία που προσφέρει προστασία και ασφάλεια.
[23] ikeepsafe, 'About the iKeepSafe COPPA Safe Harbor Certification' (COPPA Safe Harbor) <https://ikeepsafe.org/certification/coppa/>
[24] CNIL, 'Data Protection' (CNIL) <https://www.cnil.fr/fr/labels>

Το Γαλλικό Υπουργείο Υγείας απαιτεί από τους επεξεργαστές, που αποθηκεύουν προσωπικά δεδομένα σχετικά με την υγεία για λογαριασμό των Υπευθύνων επεξεργασίας δεδομένων, να υποβάλλονται σε διαδικασία προηγούμενης έγκρισης υπό την καθοδήγηση του CNIL.

11. Myobi Privacy Seal (NL)

Είναι ένα σύστημα πιστοποίησης που αποσκοπεί στην πιστοποίηση της συμμόρφωσης προϊόντων και υπηρεσιών σε σχέση με τον Ολλανδικό νόμο περί προστασίας δεδομένων (Wet bescherming persoonsgegevens), την εφαρμογή της Ολλανδικής οδηγίας για την προστασία των δεδομένων. Η αξιολόγηση γίνεται από επιθεωρητές που παρακολούθησαν την εκπαίδευση στην Ακαδημία Duthler. Το σύστημα αποτιμά το επίπεδο συμμόρφωσης του οργανισμού σε επίπεδα «ωριμότητας» και έχει πιστοποιήσει περίπου 60 οργανισμούς σύμφωνα με το δημόσιο μητρώο των ιδιοκτητών του.[25]

12. Norea Privacy-Audit-Proof (NL)

Είναι μια εθνική πιστοποίηση βασισμένη στη συμμόρφωση με την Ολλανδική εφαρμογή της οδηγίας 95/46 / EC για την προστασία των δεδομένων.[26] Το σύστημα ανήκει στην ένωση των IT-Auditors στην Ολλανδία. Η αξιολόγηση των εργασιών επεξεργασίας δεδομένων πραγματοποιείται από εγκεκριμένους επιθεωρητές. Σύμφωνα με το δημόσιο μητρώο της NOREA, υπάρχουν λίγες πιστοποιήσεις που χορηγούνται μέσω αυτού του συστήματος, αλλά αυτές που έχουν χορηγηθεί αφορούν πολύ μεγάλα συστήματα (π.χ. το Ολλανδικό σύστημα καταχώρισης αδειών οχημάτων).[27]

13. PrivacyMark System (JP)

Είναι μια πιστοποίηση που παρέχεται από το JIPDEC και αξιολογεί τη συμμόρφωση με τον Ιαπωνικό νόμο για την προστασία των προσωπικών πληροφοριών (APPI) και συμμορφώνεται με το Ιαπωνικό Βιομηχανικό Πρότυπο JIS Q 15001: 2006 για το Σύστημα Διαχείρισης Προστασίας Προσωπικών Πληροφοριών (PMS). Το σύστημα δημιουργήθηκε το 1998 και έχει εκδώσει περισσότερα από 31.000 πιστοποιητικά. Το Ιαπωνικό Ινστιτούτο για την Προώθηση της Ψηφιακής Οικονομίας και της Κοινότητας (JIPDEC) είναι ένα μη κερδοσκοπικό ίδρυμα για την ανάπτυξη βασικών τεχνολογιών και πολιτικών

[25] MYOBI, 'Controle krijgen over uw eigen bedrijfsinformatie' (MYOBI, 2018) <https://www.myobi.eu/ >
[26] Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens)
[27] NOREA, 'Privacy audit proof' (NOREA) <https://www.privacy-audit-proof.nl/ >

πληροφορικής. Το σύστημα απευθύνεται σε ιδιωτικές επιχειρήσεις και εκδίδει ένα πιστοποιητικό ανά επιχείρηση.[28]

14. Privacy by Design Certification Ryerson (CA)

    Η πιστοποίηση αυτή παρέχεται από το Πανεπιστήμιο Ryerson και τη Deloitte, πιστοποιεί τη συμμόρφωση με μια σειρά κριτηρίων που βασίζονται στις 7 από τον σχεδιασμό αρχές Προστασίας Προσωπικών Δεδομένων του πρώην Επίτροπου προστασίας της ιδιωτικής ζωής του Οντάριο, Ann Cavoukian. Το σύστημα αξιολογεί συστήματα πληροφορικής, υπεύθυνες επιχειρηματικές πρακτικές και δικτυωμένες υποδομές. Η αξιολόγηση τρίτου μέρους γίνεται από τη Deloitte. Έχει χορηγήσει 7 πιστοποιητικά το 2017 σύμφωνα με το δημόσιο μητρώο του Ryerson. Το σύστημα ανήκει στο Πανεπιστήμιο Ryerson.[29]

15. TrustArc APEC CBPR certification (US)

    Η Οικονομική Συνεργασία Ασίας-Ειρηνικού, με τις 21 χώρες μέλη της, συμπεριλαμβανομένων των ΗΠΑ, είναι μια σημαντική οικονομική περιοχή. Έχει θεσπίσει ένα πλαίσιο διασυνοριακών κανόνων απορρήτου (CBPR) με Υπεύθυνους λογοδοσίας πιστοποιώντας τις πρακτικές μεταφοράς δεδομένων. Μέχρι στιγμής, μόνο οι ΗΠΑ και η Ιαπωνία έχουν διαπιστευμένους Υπεύθυνους λογοδοσίας. Το TrustArc είναι ο Υπεύθυνος λογοδοσίας στις ΗΠΑ. Προσφέρει πολλαπλές πιστοποιήσεις και ως εκ τούτου έχει μεγάλη εμπειρία στον τομέα της πιστοποίησης.[30]

Τα κριτήρια που χρησιμοποιήθηκαν για την επιλογή τους, λαμβάνοντας υπόψη και τα αναφερόμενα του ΓΚΠΔ, είναι: η ωριμότητα, η περιεκτικότητα, η προστασία των δεδομένων από τον σχεδιασμό και από προεπιλογή, η ασφάλεια των δεδομένων, η μεταφορά δεδομένων, νέα θέματα (όπως η συγκατάθεση των ανηλίκων), η εδαφικότητα της κανονιστικής βάσης (κανονισμοί Ευρωπαϊκής Ένωσης, εθνικές ρυθμίσεις εκτός Ευρωπαϊκής Ένωσης, περιφερειακές ρυθμίσεις εκτός Ευρωπαϊκής Ένωσης), η οντότητα πιστοποίησης (Υπεύθυνος επεξεργασίας, Εκτελών την επεξεργασία), ο τομέας που απευθύνεται (ουδέτερος ή εξειδικευμένος).

Τα πορίσματα που έχουν προκύψει αναφέρονται στους παρακάτω πίνακες:

Πιστοποίηση όλων των διαδικασιών ή σε αποκλειστικές διαδικασίες

[28] JIPDEC, 'PrivacyMark' (PrivacyMark System) <https://privacymark.org/ >
[29] Ryerson university, 'Privacy by Design Certification' (Privacy by Design Centre of Excellence, 2018) <http://www.ryerson.ca/pbdce/certification/ >
[30] TrustArc, 'Extend your privacy commitment with the APEC Cross Border Privacy Certification' (TrustArc, 2018)<https://www.trustarc.com/products/apec-certification/ >

Πεδίο Πιστοποίησης	
Συστήματα που εφαρμόζονται σε όλους τους τύπους των διαδικασιών	EuroPriSe, ISDP 10003:2015, JIPDEC PrivacyMark, Privacy by design certification Ryerson, Privacy-Audit-Proof, Privacy Seal MYOBI
Συστήματα που εφαρμόζονται σε αποκλειστικές διαδικασίες	SI-BS 10012 (management systems) BSI- ISO/IEC 27018 (cloud processes) CNIL - ASIP Santé (Health data storage) Datenschutzaudit beim ULD (public processes) ePrivacy App (mobile app processes) TRUSTArc APEC CBPR (data transfers) TUV Italia - ISO/IEC 27001 certification (information security)

Πίν.2: Επισκόπηση πιστοποιήσεων: όλες οι διαδικασίες – αποκλειστικές διαδικασίες

Κάποια συστήματα πιστοποίησης υποστηρίζουν πολυτομεακή κάλυψη, προσφέροντας πιστοποίηση διαδικασιών σε όλες τις επιχειρηματικές δραστηριότητες, ενώ άλλα επικεντρώνονται σε συγκεκριμένες επιχειρηματικές δραστηριότητες.

Πεδίο Πιστοποίησης	
Πολυτομεακό **Η πιστοποίηση εφαρμόζεται σε όλες τις επιχειρηματικές δραστηριότητες**	EuroPriSe, ISDP 10003:2015, JIPDEC PrivacyMark, Privacy by design certification Ryerson, Privacy-Audit-Proof, Privacy Seal MYOBI, TRUSTArc APEC CBPR, TUV Italia - ISO/IEC 27001 certification
Ένας μόνο τομέας **Η πιστοποίηση εφαρμόζεται σε μία συγκεκριμένη επιχειρηματική δραστηριότητα.**	BSI- ISO/IEC 27018 CNIL Safebox, CNIL - ASIP Santé Datenschutzaudit beim ULD E-Privacy App IKeepSafe

Πίν.3: Επισκόπηση πολυτομεακών – συγκεκριμένου τομέα πιστοποιήσεις

Ορισμένες πιστοποιήσεις, χωρίς να επικεντρώνονται στις μικρές και μεσαίες επιχειρήσεις (ΜΜΕ), έχουν ειδική προσφορά για τις ΜΜΕ. Κάποιες εφαρμόζουν μια πολιτική τιμολόγησης προσαρμοσμένη στο μέγεθος του οργανισμού, ενώ άλλες εφαρμόζουν μια πολιτική δωρεάν ή έκπτωσης σε όλους τους υποψήφιους πιστοποίησης.

Πεδίο Πιστοποίησης	
Ειδική προσφορά για μικρές και μεσαίες επιχειρήσεις	NIL Safebox (Δωρεάν) CNIL - ASIP Santé (Δωρεάν) IKeepSafe, (πολιτική έκπτωσης) JIPDEC PrivacyMark (πολιτική έκπτωσης)

Πίν.4: Επισκόπηση πιστοποιήσεων φιλικών προς τις ΜΜΕ

Μερικά συστήματα έχουν διεθνές πεδίο εφαρμογής υπό την έννοια ότι προσφέρουν την πιστοποίηση οργανισμών εγκατεστημένων εντός και εκτός της Ευρωπαϊκής Ένωσης, ενώ άλλα πιστοποιούν οργανισμούς που είναι καταχωρημένοι στο εθνικό έδαφος του διαχειριστή του συστήματος.

Πεδίο Πιστοποίησης	
Εθνικό **Η πιστοποίηση εφαρμόζεται σε εθνικό επίπεδο**	CNIL Safebox, CNIL - ASIP Santé, Datenschutzaudit beim ULD, IKeepSafe, (USA) JIPDEC PrivacyMark, (Japan) Privacy-Audit-Proof, TRUSTe APEC CBPR (USA)
Ευρωπαϊκής Ένωσης **Η πιστοποίηση εφαρμόζεται σε όλα τα Κράτη Μέλη**	BSI-BS 10012, BSI- ISO/IEC 27018, EuroPriSe, ISDP 10003:2015, Privacy by design certification Ryerson, TUV Italia - ISO/IEC 27001 certification.
Διεθνές **Η πιστοποίηση εφαρμόζεται σε διεθνές επίπεδο ή τουλάχιστον εντός και εκτός Ευρωπαϊκής Ένωσης**	BSI-BS 10012, BSI- ISO/IEC 27018, EuroPriSe, ISDP 10003:2015, Privacy by design certification Ryerson, TUV Italia - ISO/IEC 27001 certification.

Πίν.5: Επισκόπηση πιστοποιήσεων σε εθνικό – διεθνές επίπεδο

Το ρυθμιστικό πλαίσιο αποκαλύπτει δύο αντίθετα μοντέλα. Ένα ολοκληρωμένο μοντέλο που περιλαμβάνει πιστοποιήσεις που πιστοποιούν τη συντριπτική πλειοψηφία των απαιτήσεων που περιλαμβάνονται στον ΓΚΠΔ ή άλλους νόμους περί προστασίας δεδομένων και ένα μοντέλο πιστοποίησης σε ένα μόνο θέμα περιλαμβάνει τα συστήματα που πιστοποιούν τη συμμόρφωση σε ένα μόνο ή σε περιορισμένο αριθμό νομικών υποχρεώσεων στον κανονισμό.

Οι πιστοποιήσεις που βασίζονται σε διεθνή πρότυπα φαίνεται να ακολουθούν την προσέγγιση του ISO / IEC που ενθαρρύνει μια αποκλειστική / τομεακή προσέγγιση, ενώ τα ευρωπαϊκά συστήματα φαίνεται να προτιμούν ένα γενικότερο, που όλα τα συμπεριλαμβάνει, μοντέλο.

Πεδίο Πιστοποίησης	
Μοντέλο σε συγκεκριμένο θέμα – απαίτηση του ΓΚΠΔ **Το σύστημα αποδεικνύει συμμόρφωση σε συγκεκριμένες απαιτήσεις του ΓΚΠΔ**	BSI - ISO/IEC 27018 (Article 28) CNIL - SafeBox (Article 28) CNIL - ASIP Santé (Article 28) Privacy by design certification Ryerson (Article 25) TUV Italia - ISO/IEC 27001 certification (Article 32)
Μοντέλο «Συνολικής» Πιστοποίησης **Το σύστημα βοηθά να αποδειχθεί συμμόρφωση στην πλειοψηφία των απαιτήσεων του ΓΚΠΔ**	BSI - BS 10012 Datenschutzaudit beim ULD E-Privacy App EuroPriSe ISDP 10003:2015

Πίν.6: Επισκόπηση πιστοποιήσεων ενός θέματος - Συνολική

Με βάση τα κανονιστικά κριτήρια προκύπτει η κατάταξη του παρακάτω πίνακα:

Κανονιστικά κριτήρια	
Κανονιστική βάση: νομοθεσία Νομικό πλαίσιο (Ευρωπαϊκής Ένωσης ή μη)	CNIL Safebox, CNIL - ASIP Santé, Datenschutzaudit beim ULD E-Privacy App, EuroPriSe, IKeepSafe (US) ISDP 10003:2015, Privacy by design certification Ryerson, Privacy Seal MYOBI, Privacy-Audit-Proof
Τομεακός Κανονισμός Η πιστοποίηση αναφέρεται στον ΕΚΠΔ ή σε άλλο με Ευρωπαϊκής Ένωσης Κανονισμό	BSI- BS 10012 EuroPriSe, ISDP 10003:2015, Privacy by design certification Ryerson

Κανονιστικά κριτήρια	
Εθνικός Κανονισμός	CNIL Safebox, CNIL - ASIP Santé, E-Privacy App, IKeepSafe (US) Privacy-Audit-Proof
Διάφοροι κανονισμοί **Το σύστημα αναφέρεται στις απαιτήσεις διάφορων κανονισμών**	EuroPrise (GDPR + e-Privacy)
Μοντέλο Τεχνικών Προτύπων **Το σύστημα βασίζεται σε πρότυπο που έχει εκδοθεί από εθνικό ή διεθνή οργανισμό τυποποίησης**	BSI -BS 10012, BSI- ISO/IEC 27018, JIPDEC PrivacyMark, TUV Italia - ISO/IEC 27001 certification

Πίν.7: Επισκόπηση πιστοποιήσεων με βάση τα κανονιστικά κριτήρια

Η πλειοψηφία των συστημάτων που βασίζονται στον κανονισμό έχουν μετατρέψει τις νομικές διατάξεις σε ελεγκτικά πρότυπα. Δύο συστήματα χρησιμοποιούν ήδη τις άμεσες διατάξεις του νόμου, ως απαιτήσεις. Τα περισσότερα από τα συστήματα έχουν συντάξει τα κριτήρια τους σύμφωνα με τις συστάσεις σύνταξης που περιλαμβάνονται στο πρότυπο ISO / IEC 17007 χωρίς πάντως να τις αναφέρουν πάντοτε.

Το συνδυασμένο μοντέλο περιλαμβάνει τις πιστοποιήσεις που αναφέρονται τόσο σε κανονιστικό πλαίσιο όσο και σε τεχνικά πρότυπα, προκειμένου να διασφαλιστεί ότι οι απαιτήσεις δεν έρχονται σε αντίθεση με τους κανόνες και τις έννοιες που υπάρχουν στις διάφορες πηγές.

Δημόσιες πιστοποιήσεις και ιδιόκτητες πιστοποιήσεις:

Διακανονισμοί Συστήματος	
Πιστοποίηση από Δημόσιες Αρχές **Το σύστημα διαχειρίζεται πλήρως από Δημόσια Αρχή**	CNIL Safebox, CNIL - ASIP Santé, Datenschutzaudit beim ULD

Διακανονισμοί Συστήματος	
Εποπτευόμενη **Μια Δημόσια Αρχή παίζει περιορισμένο αλλά ενεργό ρόλο (πχ Διαπίστευση)**	BSI -BS 10012 (Accreditation), BSI- ISO/IEC 27018 (Accreditation), IKeepSafe (Accreditation, Requirements drafting), ISDP 10003:2015 (Accreditation), TRUSTe APEC CBPR (Accreditation, Requirements drafting), TUV Italia - ISO/IEC 27001 certification (Accreditation)
Ιδιωτική **Το σύστημα διαχειρίζεται πλήρως από τον ιδιωτικό οργανισμό χωρίς την παρέμβαση Δημόσια Αρχής.**	E-Privacy App, EuroPriSe, JIPDEC PrivacyMark, Privacy by design certification Ryerson, Privacy Seal MYOBI, Privacy-Audit-Proof

Πίν.8: Επισκόπηση πιστοποιήσεων δημόσιων – ιδιωτικών που εποπτεύονται ή όχι

Σχετικά με την ανάθεση διαχείρισης διαδικασιών εσωτερικά ή εξωτερικά έχουμε την παρακάτω κατάταξη:

Διακανονισμοί Συστήματος	
Μοντέλο Εσωτερική διαχείρισης **Ο ιδιοκτήτης του συστήματος διαχειρίζεται όλες τις διαδικασίες πιστοποίησης**	BSI - BS 10012, BSI - ISO/IEC 27018, CNIL - SafeBox, CNIL - ASIP Santé, Datenschutzaudit beim ULD, IKeepSafe, Privacy Seal MYOBI, TRUSTe APEC CBPR, TUV Italia - ISO/IEC 27001 certification
Μοντέλο εξωτερική διαχείρισης Η διαδικασία πιστοποίησης έχει ανατεθεί ολόκληρη ή εν μέρη σε εξωτερικούς επιθεωρητές	E-Privacy App, EuroPriSe, ISDP 10003:2015, JIPDEC PrivacyMark System, Privacy by design certification Ryerson, Privacy-Audit-Proof

Πίν.9: Επισκόπηση πιστοποιήσεων εσωτερικής / εξωτερικής διαχείρισης

Κάθε επιλογή μπορεί να συνδέεται με τις συνθήκες της αγοράς, τις επιχειρηματικές ευκαιρίες ή την ανάγκη ευελιξίας.

Σύμφωνα με τις κανονιστικές πηγές και τα κριτήρια, οι αναλυόμενες πιστοποιήσεις ακολουθούν τρία μοντέλα: το ρυθμιστικό μοντέλο, το μοντέλο προτύπων και το συνδυασμένο μοντέλο. Οι πιστοποιήσεις που ακολουθούν το ρυθμιστικό μοντέλο χρησιμοποιούν ως κανονιστική βάση τη νομοθεσία. Πρόκειται για ένα μοντέλο κοντά στις πιστοποιήσεις προστασίας δεδομένων με βάση τον ΓΚΠΔ, οι οποίες υποδηλώνουν ότι οι πιστοποιήσεις σύμφωνα με το άρθρο 42 του ΓΚΠΔ σχετίζονται με μία ή περισσότερες διατάξεις του ΓΚΠΔ (συστήματα πιστοποίησης μεμονωμένων θεμάτων – σκοπού ή ολοκληρωμένα συστήματα πιστοποίησης ΓΚΠΔ).

Οι πιστοποιήσεις βάσει του ρυθμιστικού μοντέλου συνδυάζουν συχνά το ePrivacy με το ΓΚΠΔ, τον εθνικό νόμο που εφαρμόζει την προηγούμενη οδηγία για την προστασία δεδομένων ή άλλη νομοθεσία σχετικά με την προστασία των δεδομένων σε τοπικό επίπεδο. Από τη μία πλευρά, η πρακτική αυτή μειώνει σημαντικά τη γραφειοκρατία και το κόστος για τους αιτούντες, καθώς παρέχει μια ενιαία πιστοποίηση για διαφορετικές νομικές απαιτήσεις. Από την άλλη πλευρά, ο συνδυασμός νομικών μέσων ως βάση για την ίδια πιστοποίηση απαιτεί ιδιαίτερη προσοχή, καθώς ενδέχεται να προκύψουν κίνδυνοι ασυμβίβαστων στόχων ή κριτηρίων.

Πιστοποιήσεις βάσει διεθνών, Ευρωπαϊκών ή εθνικών προτύπων συνήθως δεν απαιτούν οποιαδήποτε σχέση με τη νομοθεσία. Τα διεθνή πρότυπα από το ISO και το IEC σχεδιάζονται με τέτοιο τρόπο ώστε να εξυπηρετούν οργανισμούς που είναι εγκατεστημένοι σε παγκόσμιο επίπεδο. Αυτό έχει σαν αποτέλεσμα να αποφεύγονται οι αναφορές σε εθνική ή περιφερειακή νομοθεσία. Ωστόσο συχνά στην πράξη χρησιμοποιούνται τέτοιες προδιαγραφές και οι συνεπαγόμενες πιστοποιήσεις τους σε σχέση με τις νομικές υποχρεώσεις. Πριν από την υποβολή αξίωσης ότι πιστοποίηση βάσει ISO / IEC χρησιμοποιείται για την απόδειξη της συμμόρφωσης με (ορισμένες) νομικές υποχρεώσεις του ΓΚΠΔ, πρέπει να ληφθούν αρκετά απαραίτητα μέτρα όπως η επανεξέταση της συμβατότητας της ορολογίας και η αντιστοίχιση του πεδίου εφαρμογής του προτύπου με τις απαιτήσεις για την εκπλήρωση της νομικής υποχρέωσης.

Τέλος σχετικά με το τρίτο μοντέλο που προσδιορίστηκε, ακολουθείται ο συνδυασμός των κανονιστικών πηγών, πρότυπα και νομοθεσία. Η προσέγγιση αυτού του μοντέλου προσφέρει το πλεονέκτημα του συνδυασμού της εμπειρίας από τα πρότυπα με τη νομοθεσία ως κανονιστική πηγή. Στο πλαίσιο αυτό οι μηχανισμοί πιστοποίησης οφείλουν να εξηγούν με σαφήνεια τη μεθοδολογία συνδυασμού των δύο διαφορετικών τύπων κανονιστικών πηγών και τον τρόπο με τον οποίο επιλύονται οι ασυμβατότητες.

Σύμφωνα με όλα τα παραπάνω εύκολα διαπιστώνεται ότι μόνο ένας σχετικά μικρός αριθμός συστημάτων πιστοποίησης μπορεί να θεωρηθεί ότι σχετίζεται, έως κάποιο βαθμό, με τον ΓΚΠΔ.

2.8. Η εθνική νομοθεσία για την πιστοποίηση

Στις 29/08/2020 δημοσιεύτηκε ο Νόμος 4624/2019 «Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις »[31]. Ο νόμος αυτός αφορά:

- την αντικατάσταση του νομοθετικού πλαισίου που ρυθμίζει τη συγκρότηση και λειτουργία της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα,
- τη λήψη μέτρων εφαρμογής του Κανονισμού 2016/679 (ΓΚΠΔ/GDPR)
- την ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 για την 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.[32]

Στο άρθρο 37 του νόμου γίνεται αναφορά για την διαπίστευση φορέων πιστοποίησης και την πιστοποίηση των Υπευθύνων επεξεργασίας και των Εκτελούντων την επεξεργασία. Σύμφωνα με αυτό, η επιλογή του εθνικού νομοθέτη σχετικά με τον οργανισμό διαπίστευσης των φορέων που χορηγούν πιστοποιήσεις, βάσει του άρθρου 42 του ΓΚΠΔ, είναι το Εθνικό Σύστημα Διαπίστευσης (Ε.ΣΥ.Δ.) με βάση το πρότυπο EN-ISO/IEC17065:2012 και σύμφωνα με συμπληρωματικές απαιτήσεις που έχουν οριστεί από την Αρχή. Το Ε.ΣΥ.Δ. έχει την δυνατότητα να ανακαλέσει διαπίστευση φορέα πιστοποίησης στις ακόλουθες περιπτώσεις:

- όταν ενημερωθεί από την Αρχή ότι δεν πληρούνται πλέον οι απαιτήσεις διαπίστευσης ή
- όταν ο φορέας πιστοποίησης παραβαίνει τον ΓΚΠΔ και τις διατάξεις του εθνικού νόμου 4624/2019

[31] Εφημερίδα της κυβερνήσεως της Ελληνικής Δημοκρατίας – 29/08/2020, Τεύχος Πρώτο, Αρ. Φύλλου 137
[32] GDPR: Δημοσιεύθηκε ο νόμος 4624/2019 για την προστασία προσωπικών δεδομένων - https://www.lawspot.gr/nomika-nea/gdpr-dimosieythike-o-nomos-4624-2019-gia-tin-prostasia-prosopikon-dedomenon

Όπως έχει ήδη αναφερθεί, προκειμένου να επιτευχθεί συμμόρφωση με τις απαιτήσεις του ΓΚΠΔ ένα μέτρο αποτελεί και η χρήση μηχανισμών πιστοποίησης. Σύμφωνα και με τον Επίκουρο Καθηγητής Νομικής Σχολής Πανεπιστημίου Αθηνών κ. Γ. Ν. Γιαννόπουλο, η χρήση των (εγκεκριμένων) μηχανισμών πιστοποίησης επιφέρει ορατά πλεονεκτήματα και ειδικότερα[33]:

- Αποδεικνύει τη συμμόρφωση του Υπεύθυνου επεξεργασίας γενικώς με τον ΓΚΠΔ (άρθρο 24 παράγραφος 3).
- Μπορεί να χρησιμοποιηθεί ως στοιχείο απόδειξης για την συμμόρφωση με τις προϋποθέσεις προστασίας κατά τον σχεδιασμό και εξ ορισμού (άρθρο 25 παράγραφος 3).
- Αποτελεί απόδειξη ότι παρέχονται οι κατάλληλες εγγυήσεις από Υπεύθυνο επεξεργασίας ή Εκτελούντα την επεξεργασία που δεν υπόκεινται στον ΓΚΠΔ, για την διαβίβαση των δεδομένων σε τρίτες χώρες (άρθρο 42 παράγραφος 2).
- Οι Εκτελούντες την επεξεργασία έχουν τη δυνατότητα να προσχωρήσουν σε μηχανισμούς πιστοποίησης και η προσχώρηση αυτή να αποτελέσει στοιχείο απόδειξης της δικής τους συμμόρφωσης με τις υποχρεώσεις του Υπεύθυνου Επεξεργασίας (αιτιολογική σκέψη 81).

Στο ίδιο άρθρο ο κ. Γιαννόπουλος κάνει αναφορά για τους κώδικες δεοντολογίας, που ενώ η Οδηγία 95/46 τους θεωρούσε (αιτιολογική σκέψη 26, 61, άρθρο 27)[34] ως «χρήσιμο μέσο» και ενθάρρυνε τους επαγγελματικούς κύκλους να τους καταρτίσουν προκειμένου να διευκολυνθεί η εφαρμογή της, παρόλα αυτά δεν απέκτησαν ιδιαίτερη απήχηση.

Σε αντίθεση με την τότε Οδηγία ο ΓΚΠΔ, υπερθεματίζοντας υιοθετεί ως πολύ σημαντικό «εργαλείο» την θέσπιση γενικών αρχών τις οποίες κατόπιν ακολουθούν οι ενδιαφερόμενοι υπό την μορφή Κωδίκων Δεοντολογίας και ενθαρρύνει την εκπόνησή τους. Κατά το σύστημα του ΓΚΠΔ η τήρηση Κώδικα Δεοντολογίας ή η προσχώρηση σε αυτόν, δεν παραμένει σε επίπεδο ευχολογίου, όπως έχει συμβεί σε άλλα νομοθετικά κείμενα, αλλά εξασφαλίζει συγκεκριμένα και σημαντικά πλεονεκτήματα. Τέλος, αναφέρει ότι η παρακολούθηση της συμμόρφωσης με τους Κώδικες Δεοντολογίας μπορεί να διεξάγεται από φορέα που έχει διαπιστευθεί από την αρμόδια Αρχή (άρθρο 41 παράγραφος 1) ή και από οργανισμό διαπίστευσης εφ' όσον τηρεί τις συγκεκριμένες προϋποθέσεις βάσει του άρθρου 43 – παράγραφος 2 – σημεία (α) έως (δ)[35].

[33] Υπό δημοσίευση άρθρο Επίκουρου Καθηγητή Νομικής Σχολής Πανεπιστημίου Αθηνών κ. Γ. Ν. Γιαννόπουλου
[34] Βλ. *Γ. Γιαννόπουλο*, Ροή πληροφοριών στο Διαδίκτυο, 2002, παρ. 5.4, σελ.118
[35] Υπό δημοσίευση άρθρο Επίκουρου Καθηγητή Νομικής Σχολής Πανεπιστημίου Αθηνών κ. Γ. Ν. Γιαννόπουλου

ΚΕΦ.3: ISO 27001 – Πρότυπο Διαχείρισης Ασφάλειας Πληροφοριών

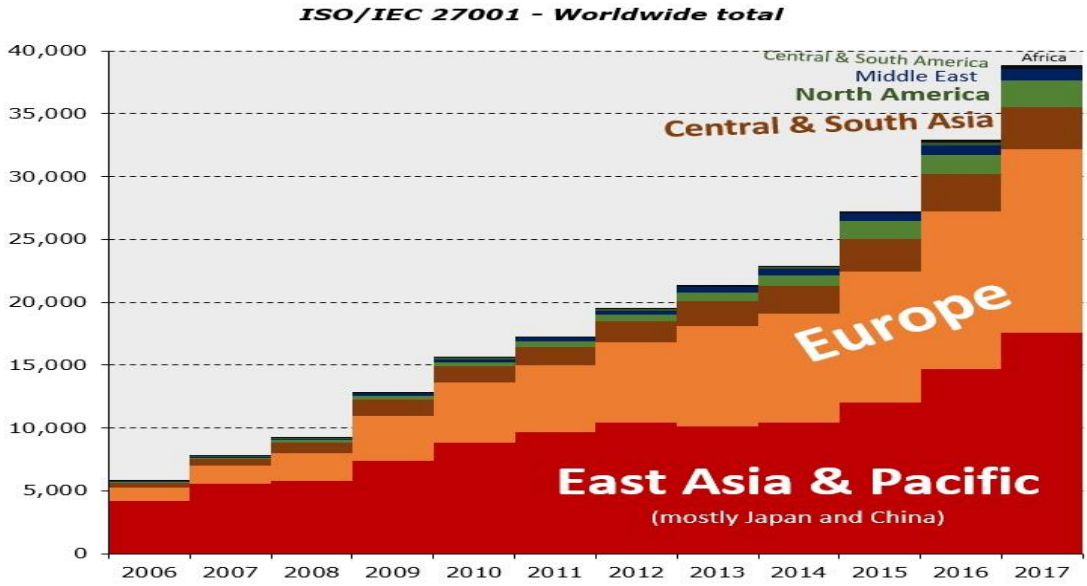
3.1. Γενικές πληροφορίες

Τα πληροφοριακά αγαθά ενός οργανισμού, στα οποία περιλαμβάνονται και τα δεδομένα – πληροφορίες του ίδιου του οργανισμού ή / και συνεργατών του, ή/και των πελατών του, είναι υψίστης σημαίας. Στη σύγχρονη ψηφιακή εποχή, πολλά από τα δεδομένα που διαθέτουν οι οργανισμοί, όπως χρηματοοικονομικές πληροφορίες και δεδομένα προσωπικού χαρακτήρα, καθίστανται ιδιαίτερα ευάλωτα καθώς μια πιθανή διαρροή πληροφοριών μπορεί να προκαλέσει σοβαρά προβλήματα, που να απειλήσουν, σε μεγάλο βαθμό, την λειτουργία του οργανισμού, αλλά και να προκαλέσουν την απώλεια της εμπιστοσύνης των πελατών και γενικότερα των ενδιαφερόμενων μερών.

Η πιστοποιημένη συμμόρφωση με το ISO / IEC 27001 από έναν διαπιστευμένο και αξιόπιστο οργανισμό πιστοποίησης μπορεί να είναι προαιρετική, αλλά πλέον απαιτείται όλο και περισσότερο από προμηθευτές και επιχειρηματικούς εταίρους και γενικότερα από οργανισμούς που ανησυχούν για την ασφάλεια των πληροφοριών τους και για την ασφάλεια των πληροφοριών σε όλη την εφοδιαστική αλυσίδα ή το δίκτυο διακίνησης, επεξεργασίας και φύλαξης αυτών.

Σύμφωνα με την έρευνα ISO για το 2017[36], υπάρχουν, από το 2006, περίπου 40.000 πιστοποιητικά ISO / IEC 27001 παγκοσμίως. Επίσης, σύμφωνα με τα αποτελέσματά της, καταγράφεται μια αξιοσημείωτη αυξητική τάση κατά περίπου 20% ετησίως.

[36] ISO Survey of certifications to management system standards - Full results
< https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1 >



Εικ.9. Παγκόσμιος ετήσιος αριθμός πιστοποιητικών ISO 27001 – (https://www.iso27001security.com/html/27001.html)

Σκοπός ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών, που ικανοποιεί τις απαιτήσεις του ISO 27001, είναι η διατήρηση της εμπιστευτικότητας, της ακεραιότητας και διαθεσιμότητας των πληροφοριακών αγαθών ενός οργανισμού.

- Εμπιστευτικότητα:

  Αφορά την προφύλαξη από μη εξουσιοδοτημένη πρόσβαση σε δεδομένα και πληροφορίες. Πρόσβαση σε αυτά έχουν μόνο όσοι κατέχουν τα απαιτούμενα δικαιώματα. Μπορεί να επιτευχθεί είτε με ελεγχόμενη πρόσβαση είτε με χρήση κρυπτογράφησης είτε και με συνδυασμό και των δύο.

- Ακεραιότητα:

  Αφορά την προστασία των δεδομένων και των πληροφοριών ως προς την πληρότητα και την ακρίβειά τους και των μεθόδων επεξεργασίας τους. Προστατεύει τα δεδομένα από μη εξουσιοδοτημένη τροποποίησή τους, στην οποία περιλαμβάνονται: εισαγωγή καινούργιων δεδομένων, τροποποίηση υφιστάμενων, διαγραφή του συνόλου ή μέρους αυτών. Μπορεί να επιτευχθεί με τη χρήση κατάλληλων μηχανισμών αυθεντικοποίησης, με χρήση ψηφιακών υπογραφών, και ειδικότερα προηγμένων, καθώς επίσης και με έλεγχο πρόσβασης.

- Διαθεσιμότητα:

Αφορά την εξασφάλιση ότι τα δεδομένα και οι πληροφορίες είναι πάντα διαθέσιμα, εντός εύλογου χρονικού διαστήματος, μόνο προς στους εξουσιοδοτημένους χρήστες και όποτε χρειάζεται. Εκτός από τα δεδομένα, η διαθεσιμότητα αφορά γενικότερα και τους πόρους ενός συστήματος.

Εικ.10. Θεμελιώδης Αρχές Ασφάλειας Πληροφοριών

Πλήγμα σε οποιοδήποτε από τα ανωτέρω, είτε από τυχαία είτε από εσκεμμένη ενέργεια, αποτελεί περιστατικό ασφάλειας για το οποίο πρέπει άμεσα να γίνουν οι κατάλληλες ενέργειες αντιμετώπισής του.

Επιπλέον, εφαρμόζει διαδικασία διαχείρισης κινδύνου, ικανοποιώντας τις απαιτήσεις του προτύπου για αξιολόγηση και αντιμετώπιση των κινδύνων που σχετίζονται με την ασφάλεια των πληροφοριακών αγαθών.

Το πρότυπο αυτό υιοθετεί τη δομή, Annex SL Appendix 2[37], που έχει αναπτυχθεί από τον ISO (International Organization for Standardization – Διεθνή Οργανισμό Τυποποίησης) για τη βελτίωση της συμβατότητας μεταξύ των Διεθνών προτύπων για τα συστήματα διαχείρισης. Σύμφωνα με αυτή την οδηγία όλα τα πρότυπα Συστημάτων Διαχείρισης θα έχουν ενιαία δομή, ταυτόσημο βασικό κείμενο και κοινούς όρους των βασικών εννοιών.

3.2. Απαιτήσεις

[37] ISO/IEC Directives, Part 1, Annex SL, Appendix 2 – HLS (2012)

Το ISO/IEC 27001 είναι ένα πρότυπο το οποίο καθορίζει τις απαιτήσεις που πρέπει να ικανοποιούνται για την καθιέρωση, την εφαρμογή, τη διατήρηση και τη συνεχή βελτίωση ενός Συστήματος Διαχείρισης Ασφάλειες Πληροφοριών (ΣΔΑΠ – ISMS (Information Security Management System)), ώστε να είναι αποτελεσματικό, αξιόπιστο και να ικανοποιεί, στο πλαίσιο ενός οργανισμού, τις απαιτήσεις των ενδιαφερόμενων μερών. Παράλληλα η απαίτησή του για εκπόνηση μελέτης διακινδύνευσης, παρέχει εμπιστοσύνη στα ενδιαφερόμενα μέρη ότι οι κίνδυνοι αντιμετωπίζονται επαρκώς.

Οι απαιτήσεις του Διεθνούς Προτύπου ISO 27001 είναι γενικές και είναι δυνατόν να εφαρμοστούν, από όλους τους οργανισμούς, ανεξάρτητα από τον τύπο τους, το μέγεθός τους ή τη φύση τους και σε κάθε εργασιακό χώρο. Ιδιαίτερη σημασία έχει το γεγονός ότι το πρότυπο αυτό είναι το μοναδικό με διεθνή αναγνώριση και το οποίο μπορεί να επιθεωρηθεί. Η επιθεώρηση υλοποιείται από διαπιστευμένο φορέα πιστοποίησης και η ισχύς του πιστοποιητικού είναι για τρία έτη, με την προϋπόθεση ότι οι απαιτήσεις διατήρησής του ικανοποιούνται.

Κατά την διάρκεια της τριετίας πραγματοποιούνται τουλάχιστον δύο ετήσιες επιθεωρήσεις επιτήρησης. Σκοπός αυτής της περιοδικής αξιολόγησης, σε διαστήματα και με μεθοδολογία που προβλέπεται από το σχήμα πιστοποίησης, είναι να διασφαλίζεται από τον Φορέα Πιστοποίησης ότι το προϊόν – διεργασία – υπηρεσία συνεχίζει να ικανοποιεί τις απαιτήσεις του σχήματος κατά τη διάρκεια ισχύος του πιστοποιητικού. Η συχνότητα διενέργειάς των επιθεωρήσεων επιτήρησης καθορίζεται, λαμβάνοντας υπόψη και τα ευρήματα προηγουμένων Επιθεωρήσεων του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών καθώς και την πολυπλοκότητα των δραστηριοτήτων του οργανισμού.

Το πρότυπο αποτελείται από τις παρακάτω ενότητες / κεφάλαια που υποχρεωτικά θα πρέπει να ικανοποιούνται από ένα πιστοποιημένο Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών:

Ενότητα	Υποενότητες
4 Πλαίσιο Λειτουργίας Οργανισμού	4.1 Κατανόηση του Οργανισμού και του πλαισίου Λειτουργίας του. 4.2 Κατανόηση των αναγκών και των προσδοκιών των ενδιαφερόμενων μερών. 4.3 Καθορισμός του πεδίου εφαρμογής του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ). 4.4. Σύστημα διαχείρισης ασφάλειας πληροφοριών και διεργασίες αυτών.
5 Ηγεσία	5.1 Ηγεσία και Δέσμευση. 5.2 Πολιτική. 5.3 Ρόλοι, υπευθυνότητες και αρμοδιότητες εντός του Οργανισμού.
6 Σχεδιασμός	6.1 Ενέργειες για την αντιμετώπιση απειλών και την αξιοποίηση ευκαιριών. 6.2 Στόχοι Ασφάλειας Πληροφοριών και σχεδιασμός για την επίτευξή τους.
7 Υποστήριξη	7.1 Πόροι 7.2 Επαγγελματική επάρκεια. 7.3 Ευαισθητοποίηση / Επίγνωση. 7.4 Επικοινωνία. 7.5 Τεκμηριωμένες πληροφορίες.
8 Λειτουργία	8.1 Επιχειρησιακός Προγραμματισμός και Έλεγχος Διεργασιών. 8.2 Εκτίμηση / Αξιολόγηση διακινδύνευσης (κινδύνων) στην ασφάλεια πληροφοριών (Information security risk assessment). 8.3 Αντιμετώπιση διακινδύνευσης στην ασφάλεια πληροφοριών (Information security risk treatment).

Ενότητα	Υποενότητες
9 Αξιολόγηση επιδόσεων	9.1 Παρακολούθηση, μέτρηση, ανάλυση και αξιολόγηση. 9.2 Εσωτερική επιθεώρηση. 9.3 Ανασκόπηση από τη Διοίκηση.
10 Βελτίωση	10.1 Μη συμμόρφωση και διορθωτικές ενέργειες. 10.3 Συνεχής βελτίωση.

Πίν.10: Κατάλογος υποχρεωτικών ενοτήτων προτύπου ISO 27001:2013

Επιπρόσθετα το πρότυπο ορίζει μία σειρά από ελέγχους (controls) στο Annex A ((normative) – Reference control objectives and controls), τα οποία προέρχονται άμεσα από και ευθυγραμμίζονται με εκείνα που περιλαμβάνονται στο ISO/IEC 27002:2013[38]

A/A	Περιγραφή
A.5	**Information security policies**
	5.1 Management direction for information security
A.6	**Organization of information security**
	6.1 Internal Organization
	6.2 Mobile devices and teleworking
A.7	**Human resource security**
	7.1 Prior to Employment
	7.2 During Employment
	7.3 Termination and change of employment
A.8	**Asset management**
	8.1 Responsibility for assets

[38] ISO / IEC 27002:2013, Information technology – Security Techniques – Code of practice for information security controls

A/A	Περιγραφή
	8.2 Information classification
	8.3 Media Handling
A.9	**Access control**
	9.1 Business requirement of access control
	9.2 User Access Management
	9.3 User Responsibilities
	9.4 System and application access control
A.10	**Cryptography**
	10.1 Cryptographic controls
A.11	**Physical and environmental security**
	11.1 Secure Areas
	11.2 Equipment
A.12	**Operations security**
	12.1 Operational Procedures and responsibilities
	12.2 Protection from malware
	12.3 Backup
	12.4 Logging and monitoring
	12.5 Control of operational software
	12.6 Technical vulnerability management
	12.7 Information system audit considerations
A.13	**Communications security**
	13.1 Network security management
	13.2 Information transfer
A.14	**System acquisition, development and maintenance**

A/A	Περιγραφή
	14.1 Security requirements of information systems
	14.2 Security in development and support processes
	14.3 Test data
A.15	**Supplier relationships**
	15.1 Information security in supplier relationships
	15.2 Supplier service delivery management
A.16	**Information security incident management**
	16.1 Management of Information Security Incidents and Improvements
A.17	**Information security aspects of business continuity management**
	17.1 Information security continuity
	17.2 Redundancies
A.18	**Compliance**
	18.1 Compliance with legal and contractual requirements
	18.2 Information security reviews

Πίν.11: Κατάλογος Controls Annex A - ISO 27001:2013

Σχετικά με τα Controlς του Annex A, στα οποία αντιστοιχούν και μερικά από τα παρακάτω έγγραφα και αρχεία καταγραφής, χρειάζεται να αναφερθεί ότι κάποια μπορεί να εξαιρεθούν στην περίπτωση που ένας οργανισμός καταλήξει στο συμπέρασμα ότι δεν υπάρχουν κίνδυνοι ή άλλες απαιτήσεις που θα καθιστούσαν αναγκαία την εφαρμογή τους.

Σύμφωνα με τις απαιτήσεις του προτύπου είναι υποχρεωτική η δημιουργία, εφαρμογή και τήρηση, τουλάχιστον, των παρακάτω εγγράφων και αρχείων:

A/A	Έγγραφο / Αρχείο καταγραφής
1	Scope of the ISMS

A/A	Έγγραφο / Αρχείο καταγραφής
2	Information security policy and objectives
3	Statement of Applicability
4	Risk assessment and risk treatment methodology
5	Risk treatment plan
6	Risk assessment and risk treatment report
7	Definition of security roles and responsibilities
8	Inventory of assets
9	Acceptable use of assets
10	Access control policy
11	Operating procedures for IT management
12	Secure system engineering principles
13	Supplier security policy
14	Incident management procedure
15	Business continuity procedures
16	Legal, regulatory, and contractual requirements
17	Records of training, skills, experience and qualifications
18	Monitoring and measurement results
19	Internal audit program
20	Results of internal audits
21	Results of corrective actions

A/A	Έγγραφο / Αρχείο καταγραφής
22	Logs of user activities, exceptions, and security events

Πίν.12: Κατάλογος υποχρεωτικών εγγράφων και καταγραφών – ISO 27001

Τα παρακάτω έγγραφα και αρχεία καταγραφών δεν είναι υποχρεωτικά από το πρότυπο, αλλά στην συντριπτική πλειοψηφία των περιπτώσεων τηρούνται.

A/A	Έγγραφο / Αρχείο καταγραφής (μη υποχρεωτικό από το πρότυπο)
1	Procedure for document control
2	Controls for managing records
3	Procedure for internal audit
4	Procedure for corrective action
5	Information classification policy
6	Password policy
7	Disposal and destruction policy
8	Procedures for working in secure areas
9	Clear desk and clear screen policy
10	Change management policy
11	Backup policy
12	Information transfer policy
13	Business impact analysis
14	Maintenance and review plan
15	Business continuity strategy

Πίν.13: Κατάλογος πρόσθετων εγγράφων και καταγραφών που συνήθως χρησιμοποιούνται – ISO 27001

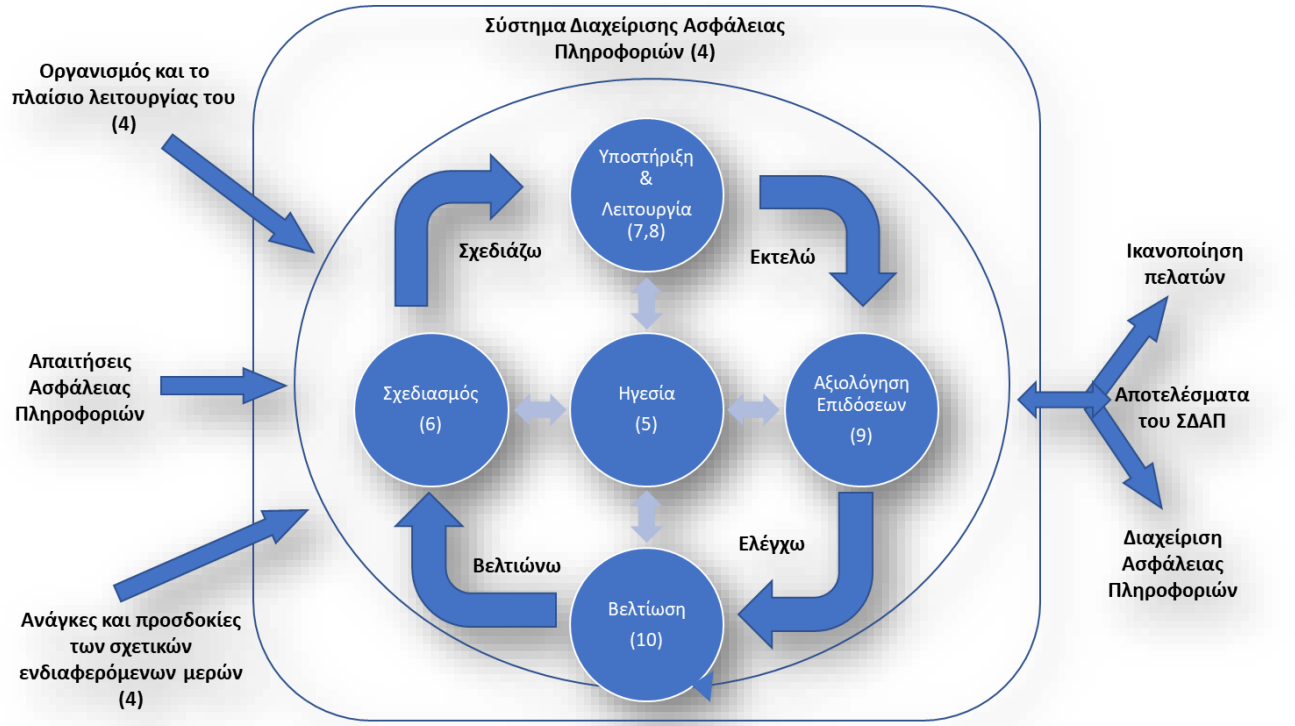
Αναφορικά και με τους δύο παραπάνω πίνακες (Πίν.12 και Πιν.13), δεν αποτελούν τη μοναδική λίστα εγγράφων και αρχείων, καθώς το πρότυπο επιτρέπει και την προσθήκη οποιωνδήποτε άλλων εγγράφων που θα συμβάλλουν στη βελτίωση του επιπέδου ασφάλειας των πληροφοριών.

Το πρότυπο είναι σχεδιασμένο έτσι ώστε να διασφαλίζει την επιλογή επαρκών και αναλογικών ελέγχων ασφάλειας και είναι βασισμένο στη διεργασιακή προσέγγιση, για την εδραίωση, εφαρμογή, λειτουργία, παρακολούθηση, ανασκόπηση, συντήρηση και βελτίωση ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών. Προς αυτή την κατεύθυνση συμβάλλουν καθοριστικά και η παροχή συστάσεων καλών πρακτικών για την διαχείριση της ασφάλειας πληροφοριών, των κινδύνων καθώς και τα αντίμετρα στο πλαίσιο εντός τέτοιου συστήματος.

Η κατανόηση και διαχείριση αλληλένδετων διεργασιών ως ένα ενιαίο σύστημα, καθορίζει σημαντικά την αποτελεσματικότητα και την αποδοτικότητα του οργανισμού. Η διεργασιακή προσέγγιση επιτρέπει τον έλεγχο των αλληλεξαρτήσεων και αλληλεπιδράσεων των διεργασιών συμβάλλοντας στη βελτίωση των επιδόσεων. Η προσέγγιση αυτή περιλαμβάνει το συστηματικό καθορισμό και διαχείριση των διεργασιών και των αλληλεπιδράσεών τους έτσι ώστε να επιτυγχάνονται τα επιδιωκόμενα αποτελέσματα σύμφωνα με την πολιτική ασφάλειας πληροφοριών και την στρατηγική του οργανισμού.

Επιπρόσθετα, η διεργασιακή προσέγγιση ενσωματώνει τη μεθοδολογία του κύκλου βελτίωσης η οποία είναι γνωστή ως κύκλος του Deming ή κύκλος PDCA (Plan-Do-Check-Act), Σχεδιάζω – Εκτελώ – Ελέγχω – Βελτιώνω.

Στην παρακάτω εικόνα παρουσιάζεται σχηματικά η αλληλεπίδραση των Διεργασιών σε συνδυασμό τις φάσεις του κύκλου του Deming:



Εικ.11. Αναπαράσταση της αλληλεπίδρασης των Διεργασιών και κύκλος του Deming

Η παραπάνω μεθοδολογία μπορεί να περιγραφεί ως ακολούθως:

- <u>Σχεδιάζω</u>

  Περιλαμβάνει την καθιέρωση των αντικειμενικών σκοπών και των διεργασιών που είναι απαραίτητες για να παραχθούν αποτελέσματα σε συμφωνία με τις απαιτήσεις των πελατών, των ενδιαφερόμενων μερών και τις πολιτικές του οργανισμού. Αποσκοπεί στο σχεδιασμό της βασικής οργάνωσης της ασφάλειας των πληροφοριών, στη θέσπιση στόχων για την ασφάλεια των πληροφοριών και στην επιλογή των κατάλληλων ελέγχων ασφαλείας.

- <u>Εκτελώ</u>

  Περιλαμβάνεται η εφαρμογή των διαδικασιών και γενικότερα οτιδήποτε έχει αποφασιστεί και εγκριθεί από την Διοίκηση του οργανισμού στη φάση του σχεδιασμού.

- <u>Ελέγχω</u>

  Γίνεται η παρακολούθηση του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών και η μέτρηση, όπου έχει εφαρμογή, των διαδικασιών και των παραγόμενων προϊόντων και

υπηρεσιών ως προς την πολιτική, τους στόχους, τις απαιτήσεις και τις προβλεπόμενες ενέργειες. Στο τέλος γίνεται εκτενής αναφορά των αποτελεσμάτων προς την Διοίκηση.

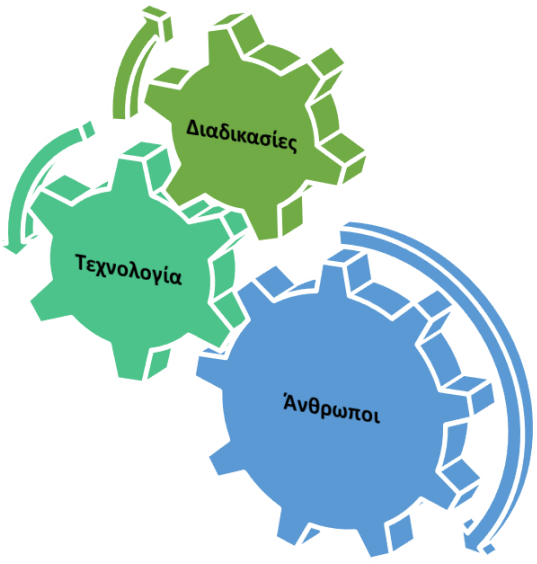
- Βελτιώνω

  Γίνονται ενέργειες για τη βελτίωση, όπου χρειάζεται, της αποτελεσματικότητας και ιδιαίτερα σε οτιδήποτε έχει χαρακτηριστεί ως μη συμβατό στη φάση του ελέγχου.

Το ISO/IEC 27001 είναι ιδιαίτερα κατάλληλο για οργανισμούς που η προστασία δεδομένων και της πληροφορίας είναι κρίσιμη, όπως σε χρηματοπιστωτικούς οργανισμούς, στις τηλεπικοινωνίες, στην υγεία, στο δημόσιο και στην πληροφορική. Επίσης, είναι κατάλληλο και για εταιρείες που διαχειρίζονται δεδομένα / πληροφορίες για λογαριασμό είτε δικός τους είτε άλλων, όπως εταιρείες παροχής υπηρεσιών πληροφορικής. Στις περιπτώσεις αυτές το πρότυπο αυτό μπορεί να λειτουργήσει ως εγγύηση ότι οι πληροφορίες των πελατών προστατεύονται επαρκώς καθώς και ότι έχουν σχεδιαστεί και εγκριθεί οι απαιτούμενες διαδικασίες τόσο για την πρόληψη όσο και για την άμεση και αποτελεσματική αντιμετώπιση συμβάντων ασφαλείας.

3.3. Πλεονεκτήματα

Το ISO 27001 είναι ένα πρότυπο ασφάλειας πληροφοριών που βοηθά τους οργανισμούς να συμμορφωθούν με τα διεθνή μοντέλα βέλτιστων πρακτικών. Το πρότυπο καλύπτει τρία βασικά στοιχεία της ασφάλειας δεδομένων : Άνθρωποι – Διαδικασίες – Τεχνολογία



Εικ.12. Αναπαράσταση των βασικών στοιχείων της ασφάλειας πληροφοριών

Όταν λαμβάνονται μέτρα για τη διασφάλιση δεδομένων λαμβάνοντας υπόψη αυτά τα τρία στοιχεία, οι οργανισμοί είναι καλύτερα εξοπλισμένοι για την προστασία των πληροφοριών, τον μετριασμό των κινδύνων και τη διόρθωση διαδικασιών που θεωρούνται αναποτελεσματικές.

Η εφαρμογή Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών, πιστοποιημένο με βάση τις απαιτήσεις του IEC/ISO 27001:2013, προσφέρει πολλά πλεονεκτήματα – οφέλη όχι μόνο στον οργανισμό που το εφαρμόζει, αλλά και γενικότερα σε όλα τα ενδιαφερόμενα μέρη, στο πλαίσιο της δραστηριότητάς του.

Ενδεικτικά μερικά από αυτά είναι:

- Προβάλλει την ύπαρξη ενός επίσημου, αποτελεσματικού και λειτουργικού Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών.
- Αποδεικνύει ότι οι απαιτήσεις για σωστή διακυβέρνηση και επιχειρησιακή συνέχεια ικανοποιούνται.
- Συμβάλλει στην εφαρμογή της σχετικής νομοθεσίας και των τυποποιητικών κανονισμών.
- Αποτελεί μέσω απόδειξης σχετικά με τη δέσμευση της ανώτατης διοίκησης του οργανισμού στο Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών.
- Διασφαλίζει ότι η ασφάλεια των πληροφοριών είναι εδραιωμένη στον οργανισμό, βελτιώνοντας και ενισχύοντας την εταιρική κουλτούρα σε θέματα ασφάλειας πληροφοριών.
- Αποδεικνύει μέσω ενός ανεξάρτητου διαπιστευμένου φορέα ότι τα οργανωτικά ρίσκα έχουν αναγνωριστεί, αξιολογηθεί και διαχειριστεί ικανοποιητικά και σωστά.
- Συμβάλλει στην καλύτερη παρακολούθηση, μέσω τακτικών αξιολογήσεων, της απόδοσης και κατ’ επέκταση στη συνεχή βελτίωση του οργανισμού σε θέματα ασφάλειας πληροφοριών.
- Αποτελεί απόδειξη για τους πελάτες και τα άλλα ενδιαφερόμενα μέρη ότι ο οργανισμός μεριμνά για την ασφάλεια των δεδομένων και των πληροφοριών τους.
- Δημιουργεί ανταγωνιστικό πλεονέκτημα στην ικανοποίηση των συμβατικών υποχρεώσεων και επεκτείνει τη φήμη του οργανισμού.
- Αποτελεί σημαντικό εργαλείο που βοηθά στην κατανόηση των δεδομένων και των πληροφοριών, στο να εντοπιστούν τα σημεία αποθήκευσης και επεξεργασίας αυτών και στον τρόπο που μπορούν να προστατευθούν.

- Βοηθά στη διαχείριση πληροφοριών σε όλες τις μορφές τους, συμπεριλαμβανομένων των ψηφιακών αρχείων, των φυσικών εγγράφων (χαρτόο αρχείο) και των προσωπικών πληροφοριών.
- Βοηθά έναν οργανισμό να αμυνθεί από κινδύνους που προέρχονται από την εξέλιξη της τεχνολογίας καθώς επίσης και από πιο κοινές απειλές, όπως το προσωπικό με ελλιπή κατάρτιση σε θέματα ασφάλειας και οι διαδικασίες με αδυναμίες στην κάλυψη της ασφάλειας πληροφοριών.

Το πρότυπο αυτό χρησιμοποιεί την αξιολόγηση των ρίσκων ώστε να δημιουργηθεί ένα σύστημα διαχείρισης που παρέχει:

- Μεγιστοποίηση της διαθεσιμότητας των συστημάτων, των δεδομένων και των πληροφοριών.
- Διαβεβαίωση ότι η ακεραιότητα των συστημάτων, των συστημάτων επεξεργασίας, των δεδομένων και της πληροφορίας συντηρείται.
- Επιβεβαίωση ότι η εμπιστευτικότητα των δεδομένων και της πληροφορίας διατηρείται.

ΚΕΦ.4: Σχέση ISO 27001 με GDPR – Δυνατότητα Συνδυασμού

4.1. Διερεύνηση σχέσης προτύπου ISO 27001 και ΓΚΠΔ

Ο ΓΚΠΔ έχει καθορίσει ένα νέο νομικό πλαίσιο για την διακυβέρνηση της επεξεργασίας αλλά και της ασφάλειας των προσωπικών δεδομένων για όλους τους οργανισμούς της Ευρωπαϊκής Ένωσης. Ο κανονισμός τυποποιεί τους κανόνες στην Ευρωπαϊκή Ένωση έχοντας ως στόχο να εξασφαλιστεί αυστηρότερος έλεγχος των οργανισμών που επεξεργάζονται δεδομένα προσωπικού χαρακτήρα, ενώ επιβάλλει αυστηρά πρόστιμα στις περιπτώσεις που εμφανίζεται μη συμμόρφωση.

Το πρότυπο ISO 27001:2013 ασχολείται με την ασφάλεια της πληροφορίας και έχει αρκετά κοινά σημεία με τον ΓΚΠΔ. Το πρότυπο αυτό έχει ως σκοπό την ασφάλεια όλης της πληροφορίας ενός οργανισμού, διασφαλίζοντας τα συμφέροντα των ενδιαφερόμενων μερών, ενώ ο ΓΚΠΔ μεταξύ άλλων, αφορά την ασφάλεια των προσωπικών δεδομένων, τα οποία αποτελούν κρίσιμες πληροφορίες που πρέπει να προστατεύσουν όλοι οι οργανισμοί με σκοπό την προστασία των ελευθεριών και των δικαιωμάτων των φυσικών προσώπων. Δεδομένου ότι τα προσωπικά δεδομένα είναι υποσύνολα της συνολικής πληροφορίας ενός οργανισμού, το πρότυπο έχει ευρύτερο πεδίο εφαρμογής καθώς ένα Συστήμα Διαχείρισης Ασφάλειας Πληροφοριών, πιστοποιημένο με βάση το πρότυπο ISO 27001, δύναται να προσδιορίσει τα προσωπικά δεδομένα ως πληροφοριακό περιουσιακό στοιχείο ασφάλειας πληροφοριών. Επίσης είναι σχεδιασμένο με τέτοιο τρόπο ώστε μπορεί να συμβάλλει στην επίτευξη της συμμόρφωσης με τον ΓΚΠΔ σε αρκετά σημεία καθώς και το πρότυπο ISO 27001 και ο ΓΚΠΔ έχουν σαν βασικό στόχο την ακεραιότητα, διαθεσιμότητα και εμπιστευτικότητα των δεδομένων – πληροφοριών.

Τα βασικά σημεία που η επιτυγχάνεται η συμβολή του προτύπου στη συμμόρφωση με απαιτήσεις του ΓΚΠΔ είναι:

- <u>Κρυπτογράφηση</u>

  Οι κρυπτογραφικοί μηχανισμοί που αναφέρει το πρότυπο (A.10.1) και οι σχετικές τεχνολογίες μπορούν να χρησιμοποιηθούν για την προστασία προσωπικών πληροφοριών που βρίσκονται αποθηκευμένες ή μεταφέρονται σε δίκτυα. Η χρήση της κρυπτογράφησης σε συνδυασμό με τεχνικές ψευδωνυμοποίησης σε μεγάλες βάσεις δεδομένων μπορεί να εξασφαλίσει την εμπιστευτικότητα των προσωπικών δεδομένων ικανοποιώντας τις απαιτήσεις του ΓΚΠΔ (άρθρο 32). Τεχνικές κρυπτογράφησης ήδη

ενσωματώνονται σε τεχνολογίες μεταφοράς δεδομένων όπως VPN, SSL, ακόμη και σε διακομιστές ηλεκτρονικού ταχυδρομείου.

- Προστασία δεδομένων από τον σχεδιασμό και εξ' ορισμού

  Το άρθρο 25 του ΓΚΠΔ ορίζει ότι οι οργανισμοί πρέπει να εφαρμόσουν τεχνικά και οργανωτικά μέτρα κατά το στάδιο σχεδιασμού όλων των έργων, ώστε να μπορούν να διασφαλίσουν την ιδιωτικότητα των δεδομένων από την αρχή («προστασία δεδομένων από το σχεδιασμό»). Επιπλέον, οι οργανισμοί θα πρέπει να προστατεύουν το απόρρητο των δεδομένων από προεπιλογή και να διασφαλίζουν ότι χρησιμοποιούνται μόνο οι πληροφορίες που είναι απαραίτητες για κάθε συγκεκριμένο σκοπό της επεξεργασίας («προστασία δεδομένων από προεπιλογή»).

  Στο ISO 27001, παρόμοιες απαιτήσεις περιγράφονται στα κεφάλαια 4 και 6. Το Κεφάλαιο 4 απαιτεί από τους οργανισμούς να κατανοήσουν το εύρος και το πλαίσιο των δεδομένων που συλλέγουν και επεξεργάζονται, ενώ το Κεφάλαιο 6 συνιστά να πραγματοποιούν τακτικές αξιολογήσεις κινδύνων ασφαλείας για να διασφαλίζουν την αποτελεσματικότητα της διαχείρισης ασφάλειας των πληροφοριών.

  Επιπρόσθετα η υιοθέτηση της προστασίας από τον σχεδιασμό, απαίτηση του ΓΚΠΔ, είναι πλέον υποχρεωτική και στην ανάπτυξη προϊόντων και συστημάτων. Στο πρότυπο ISO 27001 το σημείο ελέγχου A.14 (System acquisition, development and maintenance) διασφαλίζει ότι η ασφάλεια πληροφοριών αποτελεί αναπόσπαστο μέρος των συστημάτων πληροφοριών σε ολόκληρο τον κύκλο ζωής.

- Σχέσεις με τους προμηθευτές

  Ο ΓΚΠΔ απαιτεί από τους Υπεύθυνους επεξεργασίας να χρησιμοποιούν μόνο Εκτελούντες την επεξεργασία που παρέχουν επαρκείς εγγυήσεις για την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων για την ικανοποίηση των απαιτήσεων του ΓΚΠΔ (άρθρο 24 και 26 έως 29). Η Συμφωνία Επεξεργασίας Δεδομένων Προμηθευτή έχει σκοπό να διασφαλίσει ότι οι Υπεύθυνοι και οι Εκτελούντες την επεξεργασία έχουν δεσμευτικούς κανόνες σε ισχύ για τη ρύθμιση του τρόπου επεξεργασίας των δεδομένων από τον Εκτελούντα την επεξεργασία για λογαριασμό του Υπευθύνου επεξεργασίας. Το πρότυπο ISO 27001 εστιάζει στην διαχείριση προμηθευτών και τρίτων (σημείο ελέγχου A.15 (Suppliers relationship)). Με την αξιολόγηση των Εκτελούντων την επεξεργασία ή μια εγκεκριμένη πιστοποίησή τους, οι Υπεύθυνοι επεξεργασίας δεδομένων μπορούν να

υποστηρίξουν την κανονιστική συμμόρφωση, μέσα από συμφωνίες / συμβάσεις μεταξύ των δύο μερών.

- Εκτίμηση κινδύνου (Risk Assessment)

  Εξαιτίας των υψηλών προστίμων που ορίζονται στον ΓΚΠΔ και των σημαντικών οικονομικών επιπτώσεων σε οργανισμούς, είναι αναμενόμενο ότι ο κίνδυνος που θα εντοπιστεί κατά την αξιολόγηση του κινδύνου σχετικά με τα προσωπικά δεδομένα είναι πολύ υψηλός για να μην αντιμετωπιστεί. Επίσης μία από τις απαιτήσεις του ΓΚΠΔ είναι και η υλοποίηση εκτιμήσεων αντικτύπου για την προστασία δεδομένων (DPIA), όπου οι οργανισμοί θα πρέπει πρώτα να αναλύσουν τους κινδύνους για το απόρρητό τους, όπως το ίδιο απαιτείται και από το ISO 27001. Κατά την εφαρμογή Συστήματος Διαχείρισης Ασφάλειας πληροφοριών σύμφωνο με το πρότυπο ISO 27001, τα προσωπικά δεδομένα πρέπει να ταξινομηθούν ως πάρα πολύ κρίσιμα και υψηλού κινδύνου. Άλλωστε σύμφωνα με το στοιχείο ελέγχου A.8.2 (Information classification), οι πληροφορίες πρέπει να ταξινομούνται ως προς τις νομικές απαιτήσεις, την αξία, την κριτική και ευαισθησία σε μη εξουσιοδοτημένη αποκάλυψη ή τροποποίηση. Επίσης συμμόρφωση προς το Κεφάλαιο 6, ενότητα 6.1.2 (information security risk assessment), και προς το κεφάλαιο 8, ενότητα 8.2 (information security risk assessment), σημαίνει ότι ένας οργανισμός πρέπει να προβεί σε ολοκληρωμένες και τακτικές αξιολογήσεις κινδύνων για τον εντοπισμό απειλών και τρωτών σημείων που θα μπορούσαν να επηρεάσουν τα δεδομένα και εν συνεχεία να ληφθούν τα κατάλληλα μέτρα για την προστασία του απορρήτου, της προσβασιμότητας και της ακεραιότητας αυτών των πληροφοριών.

- Συμμόρφωση (Compliance)

  Σύμφωνα με το σημείο ελέγχου A.18.1 (Compliance with legal and contractual requirements) του ISO 27001, το οποίο αφορά τον προσδιορισμό της ισχύουσας νομοθεσίας και των συμβατικών απαιτήσεων, ένας οργανισμός πρέπει να απαριθμεί όλες τις νομοθετικές, κανονιστικές και συμβατικές απαιτήσεις. Εάν ένας οργανισμός απαιτείται να συμμορφωθεί με τον ΓΚΠΔ, αυτό πρέπει να αναφέρεται ως μία από τις κανονιστικές απαιτήσεις. Ακόμη και χωρίς το δίκαιο της Ευρωπαϊκής Ένωσης, το σημείο ελέγχου A.18.1.4 οδηγεί τους οργανισμούς, που συμμορφώνονται με το πρότυπο, στην εφαρμογή μιας πολιτικής δεδομένων και την προστασία των αναγνωρίσιμων προσωπικών πληροφοριών.

- Παραβίαση και Ειδοποίηση παραβίασης (Breach & Breach notification)

Στο άρθρο 4 παράγραφος 12 του ΓΚΠΔ αναφέρεται : «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. Προκειμένου να αποφευχθεί μια τέτοιου είδους παραβίαση ένα μέτρο μπορεί να είναι και το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών, πιστοποιημένο με βάση το πρότυπο ISO 27001. Αυτό θα συμβάλει στη μείωση της πιθανότητας παραβίασης και στην απόδειξη εφαρμογής των κατάλληλων ελέγχων που έχουν υιοθετηθεί, προκειμένου να μειωθούν οι πιθανές επιπτώσεις αυτών των κινδύνων ασφαλείας, και επιπρόσθετα θα δώσει τη δυνατότητα για πιο άμεση, γρήγορη και έγκαιρη αντίδραση

Σύμφωνα με τα άρθρα 33 και 34 του ΓΚΠΔ, οι οργανισμοί πρέπει να ενημερώσουν τις αρμόδιες αρχές εντός 72 ωρών από την ανακάλυψη παραβίασης προσωπικών δεδομένων. Τα υποκείμενα των δεδομένων πρέπει επίσης να ειδοποιούνται χωρίς αδικαιολόγητη καθυστέρηση, αλλά μόνο εάν τα δεδομένα ενέχουν υψηλό κίνδυνο για τα δικαιώματα και την ελευθερία των υποκειμένων των δεδομένων.

Το σημείο ελέγχου Α.16 (Management of information security incidents and improvements) του ISO 27001, που αναφέρεται στους ελέγχους διαχείρισης συμβάντων ασφαλείας πληροφοριών, δεν καθορίζει ένα ακριβές χρονικό πλαίσιο για την ειδοποίηση παραβίασης δεδομένων, αλλά αναφέρει ότι οι οργανισμοί πρέπει να αναφέρουν άμεσα συμβάντα ασφαλείας και να τα κοινοποιούν με τέτοιο τρόπο που να επιτρέπει να ληφθούν έγκαιρα διορθωτικά μέτρα.

- <u>Διαχείριση πληροφοριακών αγαθών (Asset management)</u>

  Οι οργανισμοί πρέπει να προσδιορίσουν τα πληροφοριακά περιουσιακά τους στοιχεία και να καθορίσουν το κατάλληλο επίπεδο προστασίας που απαιτείται για το καθένα. Αυτό αντιμετωπίζεται με το σημείο ελέγχου Α.8 (Asset management) του προτύπου ISO 27001, το οποίο οδηγεί στη συμπερίληψη προσωπικών δεδομένων ως περιουσιακών στοιχείων ασφάλειας πληροφοριών και επιτρέπει στους οργανισμούς να κατανοήσουν ποια προσωπικά δεδομένα εμπλέκονται, πού να τα αποθηκεύσουν και για πόσο καιρό, την προέλευσή τους και ποιος έχει πρόσβαση σε αυτά, τα οποία είναι και απαιτήσεις του ΓΚΠΔ.

- <u>Επιχειρησιακή Συνέχεια</u>

Το πρότυπο ISO 27001 καλύπτει τη διαχείριση της επιχειρησιακής συνέχειας. Σε αυτό περιγράφονται τα βασικά στοιχεία της συνέχειας στη διαχείριση επιχειρήσεων, όπου τα στοιχεία του σημείου ελέγχου A.17 (Information security aspects of business continuity management) εφαρμόζονται κατάλληλα προκειμένου να βοηθήσουν έναν οργανισμό να διατηρήσει τα δεδομένα (προσωπικά ή μη) και γενικότερα τις πληροφορίες άμεσα διαθέσιμες σε περίπτωση διακοπής του συστήματος. Αυτά τα ίδια πρωτόκολλα μπορούν να βοηθήσουν τον οργανισμό στη γρήγορη ανάκαμψή του από αυτό που διαφορετικά θα ήταν μια μακρά και δαπανηρή διακοπή. Συνεπώς υπάρχει η δυνατότητα επαναφοράς της διαθεσιμότητας και της πρόσβασης σε προσωπικά δεδομένα εγκαίρως σε περίπτωση φυσικού ή τεχνικού συμβάντος, ικανοποιώντας έτσι και τις απαιτήσεις του ΓΚΠΔ – άρθρο 32 – παράγραφος 1.

- Συνεχής Βελτίωση και διαρκείς Έλεγχοι – Επιθεωρήσεις

  Το ISO 27001 απαιτεί ότι το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών των οργανισμών, κεφάλαιο 10 ενότητα 2, παρακολουθείται συνεχώς, ενημερώνεται και ελέγχεται. Αυτό συνεπάγεται ότι το Σύστημα Διαχείρισης εξελίσσεται χρησιμοποιώντας μια διαδικασία συνεχούς βελτίωσης καθώς επίσης και ότι θα προσαρμοστεί σε αλλαγές που μπορεί να οφείλονται τόσο σε εσωτερικούς παράγοντες όσο και σε εξωτερικούς. Συνεπώς οι πιστοποιημένοι οργανισμοί με βάση το πρότυπο ISO 27001 διενεργούν τακτικές εσωτερικές επιθεωρήσεις (Κεφάλαιο 9 ενότητα 2) και παράλληλα λαμβάνουν τακτικούς ελέγχους από διαπιστευμένο οργανισμό πιστοποίησης, ώστε να διασφαλιστεί συνεχώς η συμμόρφωσή τους με το πρότυπο. Η επίτευξη διαπιστευμένης πιστοποίησης σύμφωνα με το πρότυπο ISO 27001 παρέχει μια ανεξάρτητη και εξειδικευμένη αξιολόγηση για το αν έχουν εφαρμοστεί τα κατάλληλα μέτρα για την προστασία των δεδομένων και ταυτόχρονα διασφαλίζεται ότι το Σύστημα Διαχείρισης πληροί τις απαιτήσεις του Προτύπου.

  Ο ΓΚΠΔ αναφέρεται σε: «τακτικές δοκιμές, αξιολόγηση και αξιολόγηση της αποτελεσματικότητας τεχνικών και οργανωτικών μέτρων για τη διασφάλιση της ασφάλειας της επεξεργασίας» (άρθρο 32). Προκειμένου να υλοποιηθούν αυτά, πρέπει να εντοπίζονται αδυναμίες ή αστοχίες στα μέτρα προστασίας των δεδομένων και να γίνεται η κατάλληλη προσαρμογή στις νέες απειλές που προκύπτουν. Αυτό σημαίνει ότι θα πρέπει να διασφαλίζεται η συνεχής βελτίωση. Επομένως, το πρότυπο ISO 27001

παρέχει συνεχώς απόδειξη βέλτιστων πρακτικών και συμβάλλει στη συμμόρφωση με τον ΓΚΠΔ.

- Εκπαίδευση προσωπικού - ευαισθητοποίηση

  Το πρότυπο ISO 27001 περιλαμβάνει απαιτήσεις σχετικά με την κατάρτιση και την ευαισθητοποίηση του προσωπικού σε θέματα ασφάλειας πληροφοριών. (Κεφάλαιο 7.2 και 7.3 – σημείο ελέγχου A.7.2.2.(Information security awareness, education and training)).

  Όλοι οι εμπλεκόμενοι πρέπει να λάβουν κατάλληλη εκπαίδευση και κατάρτιση ώστε να κάνουν τη δουλειά τους καλά και με ασφάλεια. Χρειάζεται να λαμβάνουν τακτικές ενημερώσεις σχετικά με τις οργανωτικές πολιτικές και διαδικασίες, και ειδικότερα όταν αυτές αλλάζουν. Επιπρόσθετα χρειάζεται να έχουν κατανοήσει σε άριστο βαθμό της απαιτήσεις της ισχύουσας νομοθεσίας οι οποίες σχετίζονται με τις αρμοδιότητές τους. Το πρότυπο απαιτεί να γίνονται αξιολογήσεις δεξιοτήτων, γνώσεων, ικανοτήτων και να σχεδιάζεται και να εφαρμόζεται ένα πρόγραμμα ευαισθητοποίησης, εκπαίδευσης και κατάρτισης. Ο οργανισμός πρέπει πάντα να είναι σε θέση να αποδείξει ότι συμμορφώνεται με αυτή την απαίτηση καθώς και ότι οι αντίστοιχες διαδικασίες γίνονται με τρόπο αποδοτικό και παράλληλα με έγκυρο και επικαιροποιημένο περιεχόμενο.

  Με βάση τον ΓΚΠΔ ένα από τα καθήκοντα του Υπεύθυνου Προστασίας Δεδομένων είναι να παρακολουθεί τη συμμόρφωση του οργανισμού με το σύνολο της νομοθεσίας που αφορά την προστασία δεδομένων και τις αντίστοιχες δραστηριότητες που αφορούν την ευαισθητοποίηση και την κατάρτιση του προσωπικού που συμμετέχει στις πράξεις επεξεργασίας (άρθρο 39 – παράγραφος β). Συνεπώς το ISO 27001 συμβάλλει στην εκπλήρωση ενός μέρους των καθηκόντων του Υπεύθυνου Προστασίας Δεδομένων για τη συμμόρφωση με τον ΓΚΠΔ.

- Τήρηση αρχείων

  Το άρθρο 30 του ΓΚΠΔ απαιτεί από τους οργανισμούς να τηρούν αρχεία των δραστηριοτήτων επεξεργασίας τους, συμπεριλαμβανομένων των κατηγοριών δεδομένων, του σκοπού της επεξεργασίας και μιας γενικής περιγραφής των σχετικών τεχνικών και οργανωτικών μέτρων ασφαλείας. Ομοίως, το πρότυπο ISO 27001 αναφέρει ότι οι οργανισμοί πρέπει να τεκμηριώσουν τις διαδικασίες ασφαλείας τους, καθώς και τα αποτελέσματα των εκτιμήσεων κινδύνου ασφάλειας και της αντιμετώπισης κινδύνων

(Κεφάλαιο 8). Επίσης σύμφωνα με το σημείο ελέγχου Α.8 (Asset Management), τα πληροφοριακά περιουσιακά στοιχεία πρέπει να απογραφούν και να ταξινομηθούν. Ταυτόχρονα τα στοιχεία αυτά χρειάζεται να ανατεθούν στους αρμόδιους ιδιοκτήτες και είναι αναγκαίο να καθοριστούν οι κατάλληλες διαδικασίες για την αποδεκτή χρήση τους.

Παρακάτω ακολουθεί ένας συνοπτικός πίνακας τρόπου συσχέτισης ΓΚΠΔ και προτύπου ISO 27001:

ΓΚΠΔ		**ISO 27001**	
Άρθρο	**Συνοπτική αναφορά**	**Κεφ. (#.#) ή control (A.#.#)**	**Περιγραφή**
ΚΕΦΑΛΑΙΟ Ι – ΓΕΝΙΚΕΣ ΔΙΑΤΑΞΕΙΣ			
1	Ο ΓΚΠΔ αφορά την προστασία και την ελεύθερη κυκλοφορία «προσωπικών δεδομένων», που ορίζονται στο άρθρο 4 ως «οποιεσδήποτε πληροφορίες σχετικά με ταυτοποίηση ή αναγνώριση φυσικού προσώπου («υποκείμενο δεδομένων»). Ένα αναγνωρίσιμο φυσικό πρόσωπο είναι αυτό που μπορεί να αναγνωριστεί, άμεσα ή έμμεσα, ιδίως με αναφορά σε κάποιο αναγνωριστικό όπως το όνομα, ο αριθμός ταυτότητας, δεδομένα τοποθεσίας, ηλεκτρονικό αναγνωριστικό ή ένας ή περισσότεροι παράγοντες ειδικοί για τη φυσική, φυσιολογική, γενετική, διανοητική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα αυτού του φυσικού προσώπου.	Α.18.1.4	Το πρότυπο ISO 27001 αφορά τους κινδύνους στις πληροφορίες, ιδίως τη διαχείριση των ελέγχων ασφάλειας πληροφοριών, μετριάζοντας τους μη αποδεκτούς κινδύνους για τις πληροφορίες ενός οργανισμού. Στο πλαίσιο του ΓΚΠΔ, το απόρρητο είναι σε μεγάλο βαθμό θέμα της ασφάλειας των προσωπικών δεδομένων των υποκειμένων και ιδιαίτερα των ευαίσθητων. Το πρότυπο αναφέρει συγκεκριμένα τις υποχρεώσεις συμμόρφωσης που σχετίζονται με το απόρρητο και την προστασία των προσωπικών πληροφοριών (γνωστές ως Αναγνωρίσιμες Προσωπικές Πληροφορίες - PII) στο control Α.18.1.4.
2	Στον ΓΚΠΔ αναφέρεται: «.. επεξεργασία προσωπικών δεδομένων εν όλω ή εν μέρει με αυτοματοποιημένα μέσα ....» (Συστήματα πληροφορικής, εφαρμογές και δίκτυα) και σε επιχειρηματικό ή εταιρικό / οργανωτικό πλαίσιο (δεν αφορά ιδιωτική χρήση).	Αναφορές σε διάφορα κεφαλαία και controls	Το πρότυπο αφορά γενικά πληροφορίες, όχι μόνο δεδομένα υπολογιστών, συστήματα, εφαρμογές και δίκτυα. Είναι ένα ευρύ πλαίσιο, χτισμένο γύρω από ένα «σύστημα διαχείρισης». Το ISO 27001 αντιμετωπίζει συστηματικά τους κινδύνους και τους ελέγχους πληροφοριών σε ολόκληρο τον οργανισμό, συμπεριλαμβανομένων εκτός των άλλων και των θεμάτων απορρήτου και συμμόρφωσης.

3	Ο ΓΚΠΔ αφορά προσωπικά δεδομένα για άτομα στην Ευρωπαϊκή Ένωση, είτε τα δεδομένα αυτά υποβάλλονται σε επεξεργασία στην Ευρωπαϊκή Ένωση είτε αλλού.	ISO 27001 – Introduction, 1 – Scope A.18.1.4	Το ISO 27001 έχει παγκόσμιο πεδίο εφαρμογής. Οποιοσδήποτε οργανισμός που αλληλεπιδρά με άτομα στην Ευρωπαϊκή Ένωση ενδέχεται να εμπίπτει στον ΓΚΠΔ και ειδικά όταν συλλέγει προσωπικά δεδομένα.
4	Δίνονται επίσημοι ορισμοί εννοιών που αναφέρονται στον ΓΚΠΔ.	3	Το ISO / IEC 27000 ορίζει τους περισσότερους όρους για το πρότυπο ISO 27001 συμπεριλαμβανομένων ορισμένων όρων που αφορούν το απόρρητου. Θα πρέπει να γίνει έλεγχος για το αν μπορεί να υπάρξει διένεξη μεταξύ των εταιρικών ορισμών και αυτών που δίνονται στον ΓΚΠΔ, καθώς αρκετοί οργανισμοί, στο πλαίσιο της εταιρικής διακυβέρνησης, δίνουν τους δικούς τους.
ΚΕΦΑΛΑΙΟ ΙΙ - ΑΡΧΕΣ			
5	Τα προσωπικά δεδομένα πρέπει: (α) να υποβάλλονται σε επεξεργασία νόμιμα, δίκαια και με διαφανή τρόπο, (β) να συλλέγονται μόνο για καθορισμένους, ρητούς και νόμιμους σκοπούς, (γ) να είναι επαρκή, σχετικά και περιορισμένα, (δ) να είναι ακριβή,· (ε) να διατηρούνται όχι περισσότερο από όσο χρειάζεται, (στ) να επεξεργάζονται με ασφάλεια για να διασφαλιστεί η ακεραιότητα και η εμπιστευτικότητά τους.	6.1.2, A.5, A6, A.8.1.1, A.8.2, A.8.3, A.9.1.1, A.9.4.1, A.10, A.13.2, A.14.1.1, A.15, A.16, A.17, A.18	Οι επιχειρηματικές διαδικασίες και εφαρμογές, τα συστήματα και τα δίκτυα πρέπει να διασφαλίζουν επαρκώς τα προσωπικά δεδομένα, απαιτώντας μια ολοκληρωμένη σειρά τεχνολογικών, διαδικαστικών, φυσικών και άλλων ελέγχων, ξεκινώντας από την αξιολόγηση των σχετικών κινδύνων πληροφοριών. Προκειμένου οι οργανισμοί να ικανοποιήσουν αυτές τις απαιτήσεις, πρέπει να γνωρίζουν που βρίσκονται τα προσωπικά δεδομένα, να τα ταξινομήσουν και να εφαρμόσουν τα κατάλληλα μέτρα για την συμμόρφωση στις απαιτήσεις του ΓΚΠΔ.
6	Σχετικά με τη νόμιμη επεξεργασία πρέπει: (α) το υποκείμενο να συναινέσει για τον δηλωμένο σκοπό, (β) να υπάρχει αντίστοιχη σύμβαση, (γ) να είναι απαραίτητο για άλλους λόγους συμμόρφωσης,	6.1.2, A.14.1.1, A.18.1.1	Αυτό χρειάζεται να καλύπτεται από την διαδικασία αξιολόγησης και αντιμετώπισης των κινδύνων. Είναι αναμενόμενο να επηρεαστεί ο σχεδιασμός επιχειρηματικών διαδικασιών / δραστηριοτήτων, εφαρμογών, συστημάτων κ.λπ. (για παράδειγμα. μπορεί να είναι απαραίτητο να

	(δ) να είναι απαραίτητο για την προστασία των ζωτικών συμφερόντων, (ε) να απαιτείται για δημόσιο συμφέρον ή επίσημη αρχή και / ή (στ) να περιορίζεται εάν το υποκείμενο είναι παιδί.		προσδιοριστεί η ηλικία κάποιου πριν προχωρήσει στη συλλογή και χρήση των προσωπικών του δεδομένων). Αποτελούν επιχειρηματικές απαιτήσεις για τον περιορισμό και την προστασία των προσωπικών δεδομένων. Στην πράξη απαιτούνται πολλοί έλεγχοι ασφαλείας για τον μετριασμό των μη αποδεκτών κινδύνων οι οποίοι δεν μπορούν να αποφευχθούν ή χρειάζεται να ληφθούν από κοινού (περίπτωση που τμήμα της συλλογής ή της επεξεργασίας γίνεται από τρίτο.
7	Η συγκατάθεση του υποκειμένου των δεδομένων πρέπει να είναι ενήμερη, να δίνεται ελεύθερα και να μπορεί να ανακληθεί εύκολα οποιαδήποτε χρονική στιγμή.	6.1.2 A.8.2.3, A.12.1.1, A.13.2.4, A.18.1.3, A.14.1.1, A.8.3.2, A.13.2	Απαιτείται συγκατάθεση του υποκειμένου και να μπορεί να αποδειχθεί. Πρέπει να υπάρχουν διαδικασίες για αυτό και αρχεία που αποδεικνύουν τη συγκατάθεση τα οποία θα πρέπει να προστατεύονται και να διατηρούνται. Η ανάκληση συναίνεσης συνεπάγεται τη δυνατότητα εντοπισμού και αφαίρεσης των προσωπικών δεδομένων, ίσως κατά τη διάρκεια της επεξεργασίας τους καθώς επίσης και από αντίγραφα ασφαλείας και αρχεία. Επιπρόσθετα χρειάζεται να σχεδιαστούν και να ενεργοποιηθούν επιχειρηματικές διαδικασίες για τον έλεγχο και τον χειρισμό των αιτημάτων.
8	Ειδικοί περιορισμοί ισχύουν για τη συγκατάθεση που αφορά ανήλικα άτομα (παιδιά)	6.1.2 A.8.2.3, A.12.1.1, A.13.2.4, A.18.1.3, A.14.1.1, A.8.3.2, A.13.2	Αυτοί οι ειδικοί περιορισμοί ισχύουν κυρίως κατά τη στιγμή της συλλογής των δεδομένων (π.χ. λήψη της συγκατάθεσης ενός γονέα).
9	Ειδικοί περιορισμοί ισχύουν για ιδιαίτερα ευαίσθητα δεδομένα σχετικά με τη φυλετική καταγωγή, τις πολιτικές πεποιθήσεις, τη θρησκεία, τη	A.8.2.1, A.8.2.3, A.14.1.1	Είναι σημαντικό να προσδιοριστεί πού μπορούν να υποβληθούν σε επεξεργασία ευαίσθητα δεδομένα, αν αυτό είναι απαραίτητο στην πραγματικότητα, και να

	σεξουαλικότητα, τις γενετικές πληροφορίες και άλλα βιομετρικά στοιχεία. Η επεξεργασία τέτοιων πληροφοριών απαγορεύεται από προεπιλογή, εκτός εάν δοθεί συναίνεση και απαιτείται επεξεργασία (όπως ορίζεται στο άρθρο).		ληφθεί ρητή συγκατάθεση - παράγοντες που πρέπει να λαμβάνονται σοβαρά υπόψη στο σχεδιασμό συστημάτων, εφαρμογών και επιχειρηματικών διαδικασιών.
10	Ειδικοί περιορισμοί ισχύουν για προσωπικά δεδομένα σχετικά με ποινικές καταδίκες και αδικήματα	6.1.2, A.7.1, A.8.2.1, A.8.2.3, A.14.1.1	Οποιαδήποτε χρήση αυτών των πληροφοριών πρέπει να προσδιοριστεί και να υποβληθεί σε επεξεργασία μόνο σε συγκεκριμένες περιπτώσεις. Τέτοιες μπορεί να απαιτούνται για ελέγχους ιστορικού, κινδύνου απάτης κλπ.
11	Διαδικασίες που δεν απαιτείται ταυτοποίηση. Ορισμένοι περιορισμοί πιθανότατα να μην χρειάζονται στην περίπτωση που τα δεδομένα τα οποία διατηρούνται δεν «οδηγούν» σε ταυτοποίηση υποκειμένου.	6.1.2 A.8.2.1, A.8.2.3, A.14.1.1	Στις περιπτώσεις που είναι εφικτό αποτελεί καλή στρατηγική να μην είναι γνωστή η ταυτότητα του υποκειμένου, με την προϋπόθεση ότι τα υπόλοιπα στοιχεία αρκούν, με σκοπό την αποφυγή του κινδύνου.
ΚΕΦΑΛΑΙΟ ΙΙΙ – ΔΙΚΑΙΩΜΑΤΑ ΤΟΥ ΥΠΟΚΕΙΜΕΝΟΥ ΤΩΝ ΔΕΔΟΜΕΝΩΝ			
ΤΜΗΜΑ 1 – ΔΙΑΦΑΝΕΙΑ ΚΑΙ ΡΥΘΜΙΣΕΙΣ			
12	Η επικοινωνία με το υποκείμενο για την ενημέρωσή του και την άσκηση των δικαιωμάτων του θα πρέπει να είναι διαφανής, σαφής, εύκολη και κατανοητή.	A.12.1.1, A.14.1.1, A.16	Αυτό επηρεάζει τη διαμόρφωση των ηλεκτρονικών φορμών επικοινωνίας και ειδοποιήσεων καθώς και των διαδικασιών. Σχετίζεται με τη διαχείριση συμβάντων, δηλαδή μηχανισμούς που επιτρέπουν στα υποκείμενα να διερευνούν ή να διαμαρτύρονται σχετικά με τα προσωπικά τους δεδομένα, την άμεση ανταπόκριση και την τήρηση αρχείων τέτοιων επικοινωνιών.
ΤΜΗΜΑ 2 – ΕΝΗΜΕΡΩΣΗ ΚΑΙ ΠΡΟΣΒΑΣΗ ΣΕ ΔΕΔΟΜΕΝΑ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ			
13	Όταν συλλέγονται προσωπικά δεδομένα, το υποκείμενο πρέπει να έχει πληροφόρηση για τα στοιχεία του Υπεύθυνου επεξεργασίας, του	A.8.2., A.8.2.3, A.12.1.1, A.14.1.1, A.16	Οι διαδικασίες για την παροχή νόμιμης επεξεργασίας πληροφοριών, πληροφοριών σχετικά με τον Υπεύθυνο επεξεργασίας και το/τους σκοπούς

	Υπεύθυνου Προστασίας Δεδομένων, για πόσο καιρό τα δεδομένα του θα διατηρηθούν, τα δικαιώματά του και πώς θα επικοινωνήσει ή θα παραπονεθεί.		επεξεργασίας των δεδομένων πρέπει να καθοριστούν και να εφαρμοστούν. Αυτό εξαρτάται εν μέρει από τον προσδιορισμό του πού χρησιμοποιούνται προσωπικά δεδομένα.
14	Παρόμοιες απαιτήσεις κοινοποίησης με το άρθρο 13 ισχύουν στην περίπτωση που τα προσωπικά στοιχεία λαμβάνονται έμμεσα (π.χ. μια εμπορική λίστα αλληλογραφίας;): τα υποκείμενα πρέπει να ενημερώνονται εντός ενός μήνα και για την πρώτη επικοινωνία μαζί τους	A.8.2.1, A.8.2.3, A.12.1.1, A.14.1, A.16,	Οι διαδικασίες για την παροχή νόμιμης επεξεργασίας πληροφοριών, πληροφοριών σχετικά με τον Υπεύθυνο επεξεργασίας και τον/τους σκοπούς επεξεργασίας των δεδομένων πρέπει να καθοριστούν και να εφαρμοστούν. Αυτό εξαρτάται εν μέρει από τον προσδιορισμό του πού χρησιμοποιούνται προσωπικά δεδομένα.
15	Το υποκείμενο έχει το δικαίωμα να μάθει αν ο οργανισμός διατηρεί τα προσωπικά του στοιχεία, για ποιον σκοπό, σε ποιον μπορεί να αποκαλυφθούν και να ενημερωθεί για το δικαίωμα καταγγελίας, της διόρθωσης, της διαγραφή κ.λπ. Τα υποκείμενα έχουν δικαίωμα να αποκτήσουν αντίγραφο των προσωπικών τους δεδομένων.	A.8.1.1, A.8.2.1, A.12.1.1, A.13.2.1, A.14.1.1	Στα δικαιώματα των υποκειμένων περιλαμβάνονται η δυνατότητα λήψης αντιγράφου των δικών τους πληροφοριών (συνεπώς υπάρχει ανάγκη ταυτοποίησης και ελέγχου πριν την ικανοποίηση τέτοιων αιτημάτων), η ενημέρωση σχετικά με τη φύση της επεξεργασίας (για παράδειγμα τη λογική και τις συνέπειες του «προφίλ») καθώς και πληροφορίες σχετικά με τους ελέγχους και την ασφάλεια στην περίπτωση που τα δεδομένα τους πρόκειται να εξαχθούν. Επηρεάζεται η διαδικασία σχετικά με τα αντίγραφα ασφαλείας και της αντιγραφής αρχείων. Επίσης επηρεάζει και τη διαδικασία σχετικά με την ανάκληση της συγκατάθεσης.
ΤΜΗΜΑ 3 – ΔΙΟΡΘΩΣΗ ΚΑΙ ΔΙΑΓΡΑΦΗ			
16	Τα υποκείμενα έχουν το δικαίωμα να διορθώσουν, να συμπληρώσουν, να διευκρινίσουν τα προσωπικά τους δεδομένα.	A.12.1.1, A.14.1, A.9, A.16, A.12.3, A.18.1.3	Εφαρμόζονται λειτουργικές απαιτήσεις για έλεγχο, επεξεργασία και επέκταση των αποθηκευμένων πληροφοριών, με διάφορα στοιχεία ελέγχου σχετικά με την ταυτοποίηση, την αυθεντικοποίηση και τον έλεγχο πρόσβασης, την επικύρωση κλπ. Επηρεάζεται η διαδικασία σχετικά με

			τα αντίγραφα ασφαλείας και της αντιγραφής αρχείων.
17	Τα υποκείμενα έχουν το δικαίωμα στη λήθη, δηλαδή να διαγράψουν τα προσωπικά τους δεδομένα προκειμένου αυτά να μην χρησιμοποιούνται πλέον.	6.1.2, A.14.1.1, A.9, A.16, A.12.3, A.8.3.2	Αποτελεί μια μορφή ανάκλησης της συγκατάθεσης. Υπονοεί λειτουργικές απαιτήσεις συστήματος και διεργασίας για τη διαγραφή συγκεκριμένων αποθηκευμένων πληροφοριών, με διάφορα στοιχεία ελέγχου σχετικά με την αναγνώριση, τον έλεγχο ταυτότητας, την πρόσβαση, την επικύρωση κ.λπ. Επηρεάζεται η διαδικασία σχετικά με τα αντίγραφα ασφαλείας και της αντιγραφής αρχείων.
18	Τα υποκείμενα έχουν το δικαίωμα να περιορίζουν την επεξεργασία των προσωπικών τους δεδομένων.	6.1.2, A.8.2.1, A.8.2.3, A.12.1.1, A.14.1.1, A.16, A.12.3, A.18.1.1	Θα χρειαστεί διαδικασία για τον προσδιορισμό των συγκεκριμένων δεδομένων που πρόκειται να περιοριστούν και την εφαρμογή νέων κανόνων χειρισμού / επεξεργασίας. Επηρεάζεται η διαδικασία σχετικά με τα αντίγραφα ασφαλείας και της αντιγραφής αρχείων.
19	Τα υποκείμενα έχουν το δικαίωμα να γνωρίζουν το αποτέλεσμα των αιτημάτων διόρθωσης, ολοκλήρωσης, διαγραφής, περιορισμού κ.λπ. των προσωπικών τους δεδομένων.	6.1.2, A.12.1.1, A.14.1.1, A.16	Η πληροφόρηση / ενημέρωση των υποκειμένων αποτελεί συμβατικό μέρος της διαδικασίας διαχείρισης συμβάντων.
20	Τα υποκείμενα έχουν το δικαίωμα να αποκτήσουν ένα έγκυρο ηλεκτρονικό αντίγραφο των προσωπικών τους δεδομένων για να τα διαβιβάσουν σε διαφορετικό Υπεύθυνο επεξεργασίας.	6.1.2, A.13, A.14.1.1, A.8.3, A.10, A.18.1.3	Τα εξαγόμενα δεδομένα πρέπει να περιορίζονται στα ενδιαφερόμενα υποκείμενα που έχουν ταυτοποιηθεί και επικυρωθεί και πρέπει να κοινοποιούνται με ασφάλεια (κρυπτογραφημένα). Μπορεί επίσης να συνεπάγεται διαγραφή ή περιορισμό των δεδομένων και επιβεβαίωση ολοκλήρωσης αυτής της διαδικασίας.
ΤΜΗΜΑ 4 – ΔΙΚΑΙΩΜΑ ΕΝΑΝΤΙΩΣΗΣ ΚΑΙ ΑΥΤΟΜΑΤΟΠΟΙΗΜΈΝΗ ΑΤΟΜΙΚΗ ΛΗΨΗ ΑΠΟΦΑΣΕΩΝ			

21	Τα υποκείμενα έχουν το δικαίωμα να εναντιωθούν στη χρήση των δεδομένων τους για σκοπούς προφίλ και μάρκετινγκ.	6.1.2, A.12.1.1, A.14.1.1, A.16, A.12.3	Μπορεί να χρειάζονται τρόποι για τον προσδιορισμό των συγκεκριμένων δεδομένων που δεν πρόκειται να υποβληθούν σε επεξεργασία και να εφαρμοστούν νέοι κανόνες χειρισμού / επεξεργασίας.
22	Τα υποκείμενα έχουν το δικαίωμα να αναθεωρούν / επανεξετάζουν αποφάσεις που προκύπτουν από την αυτόματη επεξεργασία των προσωπικών τους δεδομένων.	6.1.2, A.12.1.1, A.14.1.1, A.16	Τα συστήματα προφίλ και υποστήριξης λήψης αποφάσεων που περιλαμβάνουν προσωπικά δεδομένα πρέπει να επιτρέπουν εξωτερικό έλεγχο, εκτός συστήματος, και παράκαμψη, με την κατάλληλη εξουσιοδότηση, του ελέγχου πρόσβασης και ακεραιότητας.
ΤΜΗΜΑ 5 – ΠΕΡΙΟΡΙΣΜΟΙ			
23	Οι εθνικοί νόμοι μπορούν να τροποποιήσουν ή να παρακάμψουν διάφορα δικαιώματα και περιορισμούς για την εθνική ασφάλεια και άλλους σκοπούς	A.18.1.1	Αυτό αφορά κυρίως τις αρχές / τους δημόσιους φορείς, αλλά μπορεί να επηρεάσει ορισμένους ιδιωτικούς / εμπορικούς οργανισμούς, είτε τακτικά είτε κατ' εξαίρεση.
ΚΕΦΑΛΑΙΟ IV – ΥΠΕΥΘΥΝΟΣ ΕΠΕΞΕΡΓΑΣΙΑΣ ΚΑΙ ΕΚΤΕΛΩΝ ΤΗΝ ΕΠΕΞΕΡΓΑΣΙΑ			
ΤΜΗΜΑ 1 – ΓΕΝΙΚΕΣ ΥΠΟΧΡΕΩΣΕΙΣ			
24	Ο Υπεύθυνος επεξεργασίας είναι αρμόδιος για την εφαρμογή κατάλληλων ελέγχων απορρήτου (συμπεριλαμβανομένων πολιτικών και κωδικών δεοντολογίας) λαμβάνοντας υπόψη τους κινδύνους, τα δικαιώματα και άλλες απαιτήσεις εντός και ίσως πέραν του ΓΚΠΔ	4, 5, 6, 7, 8, 9, 10, Τα περισσότερα control στο Annex A	Είναι αναγκαίο να εφαρμοστεί ένα κατάλληλο, ολοκληρωμένο πλέγμα ελέγχων απορρήτου, συμπεριλαμβανομένων πολιτικών και διαδικασιών, καθώς και τεχνικών, φυσικών και άλλων ελέγχων που αντιμετωπίζουν τους κινδύνους πληροφόρησης και τις υποχρεώσεις συμμόρφωσης. Η κλίμακα αυτού απαιτεί συνήθως μια δομημένη, συστηματική προσέγγιση της ιδιωτικότητας. Λαμβάνοντας υπόψη τις αλληλεπικαλύψεις, είναι αναμενόμενο να ενσωματωθεί και να ευθυγραμμιστεί το απόρρητο με το σύστημα διαχείρισης ασφάλειας πληροφοριών, βάσει του προτύπου ISO 27001, καθώς και με τη συμμόρφωση διαχείρισης της

			επιχειρησιακής συνέχειας. Γενικά αφορά τη διακυβέρνηση στο σύνολό της.
25	Λαμβάνοντας υπόψη τους κινδύνους, το κόστος και τα οφέλη, θα πρέπει να υπάρχει επαρκής προστασία για τα προσωπικά δεδομένα από το σχεδιασμό και από προεπιλογή.	6 , Τα περισσότερα control στο Annex A	Υπάρχουν επιχειρηματικοί λόγοι για την κατάλληλη επένδυση στην προστασία της ιδιωτικής ζωής, συμπεριλαμβανομένων των κινδύνων σχετικά με την ασφάλεια των πληροφοριών και των απαιτήσεων συμμόρφωσης, καθώς και επιλογές εφαρμογής με διάφορα κόστη και οφέλη. Η συνεργασία αυτών είναι ένας καλός τρόπος για να εξασφαλιστεί η υποστήριξη και η συμμετοχή της διοίκησης, καθώς και η κατανομή της χρηματοδότησης και των πόρων που απαιτούνται για να σχεδιαστούν, να παραδοθούν, να εφαρμοστούν και να διατηρηθούν οι ρυθμίσεις απορρήτου. Το απόρρητο από το σχεδιασμό και από προεπιλογή αποτελεί παράδειγμα αρχών απορρήτου που υποστηρίζουν την προδιαγραφή, το σχεδιασμό, την ανάπτυξη, τη λειτουργία και τη συντήρηση συστημάτων και διαδικασιών πληροφορικής που σχετίζονται με την προστασία της ιδιωτικής ζωής, συμπεριλαμβανομένων των σχέσεων και των συμβάσεων με τρίτα μέρη.
26	Όταν οι οργανισμοί είναι από κοινού υπεύθυνοι για τον καθορισμό και την εκπλήρωση των απαιτήσεων απορρήτου χρειάζεται να προσδιοριστούν οι ρόλοι και οι υπευθυνότητες που αντιστοιχούν στο κάθε ένα.	5.3, 9.1 A.13.2, A.15, A.16, A.18.1	Οι οργανισμοί πρέπει να διαχειρίζονται σχέσεις με επιχειρηματικούς εταίρους, διασφαλίζοντας το ότι απόρρητο και άλλες πτυχές ασφάλειας πληροφοριών ικανοποιούνται. Αυτό περιλαμβάνει από κοινού διερεύνηση και επίλυση περιστατικών απορρήτου, παραβιάσεων ή αιτημάτων πρόσβασης, επίτευξη και διατήρηση ενός εγγυημένου επιπέδου συμμόρφωσης με τον ΓΚΠΔ και σεβασμό στο σκοπό για τον οποίο συλλέχθηκαν τα προσωπικά δεδομένα.

27	Οργανισμοί εκτός Ευρωπαϊκής Ένωσης πρέπει να ορίσουν επίσημα νόμιμους εκπροσώπους της ιδιωτικότητας εντός της Ένωσης.	5.3, 7.5.1, A.15, A.18.1.4	Αυτή είναι μία από τις πολλές διατυπώσεις συμμόρφωσης: ο Υπεύθυνος Προστασίας Δεδομένων πρέπει να είναι υπεύθυνος για να βεβαιωθεί ότι αυτό γίνεται σωστά.
28	Σε περίπτωση που ένας οργανισμός χρησιμοποιεί ένα ή περισσότερα τρίτα μέρη για την επεξεργασία προσωπικών δεδομένων (Εκτελούντες την επεξεργασία), πρέπει να διασφαλίσει ότι και αυτοί συμμορφώνονται με τον ΓΚΠΔ.	8.2, 9.1, A.15, A.18.1.1, A.18.1.3, A.18.1.4	Αυτό ισχύει για κέντρα δεδομένων εξωτερικής ανάθεσης καθώς και για άλλες εμπορικές υπηρεσίες όπου ο οργανισμός διαβιβάζει προσωπικά στοιχεία σε τρίτους, π.χ. για μάρκετινγκ και HR, μισθοδοσία και ιατρικές υπηρεσίες για υπαλλήλους. Εφαρμόζεται επίσης στο τέλος παραλαβής υπηρεσιών όπου οι πάροχοι υπηρεσιών μπορεί να ερωτηθούν σχετικά με την κατάσταση συμμόρφωσής τους με το ΓΚΠΔ, τις πολιτικές απορρήτου και άλλους ελέγχους και να συμπεριληφθούν ρήτρες συμμόρφωσης και διασφάλισης / όροι και υποχρεώσεις στις συμβάσεις και στις συμφωνίες. Οι κίνδυνοι για την ασφάλεια πληροφοριών πρέπει να αναγνωριστούν, να αξιολογηθούν και να αντιμετωπίζονται και από τις δύο πλευρές.
29	Οι Εκτελούντες την επεξεργασία μπορούν να επεξεργάζονται προσωπικά δεδομένα μόνο σύμφωνα με τις οδηγίες του Υπευθύνου και της ισχύουσας νομοθεσίας.		Οι εκτελούντες την επεξεργασία πρέπει να προστατεύουν και να ελέγχουν τα προσωπικά δεδομένα με τον ίδιο τρόπο όπως οι Υπεύθυνοι. Χρειάζεται να έχουν στη διάθεσή τους όλες τις απαραίτητες ρυθμίσεις απορρήτου.
30	Οι Υπεύθυνοι επεξεργασίας πρέπει να διατηρούν τεκμηρίωση σχετικά με το απόρρητο, όπως για παράδειγμα τους σκοπούς για τους οποίους συλλέγονται και υποβάλλονται σε επεξεργασία προσωπικά δεδομένα, «κατηγορίες» υποκειμένων δεδομένων και προσωπικών δεδομένων.	7.5	Τεκμηριωμένες πληροφορίες.

31	Οι οργανισμοί πρέπει να συνεργάζονται με τις αρχές.	A.6.1.3	Επικοινωνία με τις αρχές.
ΤΜΗΜΑ 2 – ΑΣΦΑΛΕΙΑ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ.			
32	Οι οργανισμοί είναι αναγκαίο να εφαρμόζουν, να λειτουργούν και να διατηρούν κατάλληλα τεχνικά και οργανωτικά μέτρα ασφαλείας για τα προσωπικά δεδομένα, αντιμετωπίζοντας τους κινδύνους που σχετίζονται με την ασφάλεια πληροφοριών.	8.2, 8.3 Τα περισσότερα control στο Annex A	Ο ΓΚΠΔ αναφέρει μερικά παραδείγματα ελέγχου (όπως κρυπτογράφηση, ανωνυμοποίηση) που καλύπτουν στοιχεία εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας, καθώς και μέτρα ελέγχου / διασφάλισης και συμμόρφωση των εργαζομένων (πολιτικές και διαδικασίες, ευαισθητοποίηση / εκπαίδευση και επιβολή συμμόρφωσης / ενίσχυση). Ένα Σύστημα διαχείρισης Ασφάλειας Πληροφοριών, με βάση το πρότυπο ISO 27001, παρέχει ένα συνεκτικό, ολοκληρωμένο και δομημένο πλαίσιο για τη διαχείριση της προσωπικών δεδομένων μαζί με άλλους κινδύνους ασφάλειας πληροφοριών, ελέγχους, συμμόρφωση κλπ.
33	Οι παραβιάσεις απορρήτου που έχουν αποκαλύψει ή βλάψει προσωπικά δεδομένα πρέπει να κοινοποιούνται αμέσως στις αρχές (εντός 3 ημερών από την ημερομηνία που έγινε κάτι τέτοιο αντιληπτό, εκτός εάν δικαιολογούνται καθυστερήσεις).	A.16, A.18.1.4	Οι παραβιάσεις αντιμετωπίζονται ως περιστατικά στο πλαίσιο της διαδικασίας διαχείρισης συμβάντων του συστήματος διαχείρισης Ασφάλειας Πληροφοριών και ταυτόχρονα θα πρέπει να εκπληρωθούν οι ειδικές υποχρεώσεις προς τον ΓΚΠΔ (όπως η προθεσμία 3 ημερών για την κοινοποίηση στις αρχές).
34	Οι παραβιάσεις απορρήτου που έχουν εκθέσει ή βλάψει προσωπικά δεδομένα και κριθούν ως σημαντικές με σοβαρές συνέπειες, πρέπει να κοινοποιηθούν στα υποκείμενα που επηρεάζονται χωρίς αδικαιολόγητη καθυστέρηση.	A.16, A.18.1.4	Εκτός από τις νομικές και ηθικές εκτιμήσεις και την κατεύθυνση / καθοδήγηση από τις αρχές απορρήτου, υπάρχουν προφανώς σημαντικά επιχειρηματικά ζητήματα σχετικά με το χρονοδιάγραμμα και τη φύση της αποκάλυψης. Αυτό θα πρέπει να αποτελεί μέρος της διαδικασίας διαχείρισης συμβάντων για σοβαρά περιστατικά, με τη συμμετοχή ανώτερων στελεχών, ειδικών και συμβούλων.

ΤΜΗΜΑ 3 – ΕΚΤΙΜΗΣΗ ΑΝΤΙΚΤΥΠΟΥ ΣΧΕΤΙΚΑ ΜΕ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΠΡΟΗΓΟΥΜΕΝΗ ΔΙΑΒΟΥΛΕΥΣΗ			
35	Οι κίνδυνοι απορρήτου, συμπεριλαμβανομένων πιθανών επιπτώσεων, πρέπει να αξιολογούνται, ιδίως όταν εξετάζονται νέες τεχνολογίες / συστήματα / ρυθμίσεις ή όπου οι κίνδυνοι ενδέχεται να είναι σημαντικοί (π.χ. «προφίλ»).	6.1.2, A.6.1.3, A.8.2.1	Υπάρχουν επιχειρηματικοί και ηθικοί λόγοι για τον εντοπισμό, την αξιολόγηση και την αντιμετώπιση κινδύνων πληροφοριών (συμπεριλαμβανομένων των κινδύνων απορρήτου και της συμμόρφωσης), εκτός από τις υποχρεώσεις του ΓΚΠΔ. Οι κίνδυνοι που σχετίζονται με το απόρρητο θα πρέπει πιθανώς να περιλαμβάνονται στα μητρώα εταιρικών κινδύνων μαζί με διάφορους άλλους κινδύνους. Ο ΓΚΠΔ υποστηρίζει την ενσωμάτωση της εκτίμησης των κινδύνων απορρήτου ως μέρος των συνήθων δραστηριοτήτων εκτίμησης διακινδύνευσης για έργα επιχειρηματικών αλλαγών, νέων εξελίξεων συστημάτων πληροφορικής κλπ.
36	Οι κίνδυνοι απορρήτου που αξιολογούνται ως «υψηλοί» πρέπει να κοινοποιούνται στις αρχές, δίνοντάς τους την ευκαιρία να τοποθετηθούν.	6.1.2, A.6.1.3, A.8.2.1	Η απαίτηση του ΓΚΠΔ είναι εύλογη αλλά αόριστη: αυτό μπορεί να καλύπτεται από εταιρικές πολιτικές σχετικά με τον ακριβή ορισμό των «υψηλών» κινδύνων απορρήτου. Από την άλλη πλευρά, ρητές πληροφορίες από τις αρχές μπορεί να είναι χρήσιμες όσον αφορά μια επίσημη θέση σχετικά με την καταλληλότητα και επάρκεια των προτεινόμενων ελέγχων.
ΤΜΗΜΑ 4 – ΥΠΕΥΘΥΝΟΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ			
37	Ο Υπεύθυνος Προστασίας Δεδομένων πρέπει να αναγνωρίζεται επίσημα υπό συγκεκριμένες συνθήκες π.χ. δημόσιοι φορείς, οργανισμοί που εκτελούν μεγάλης κλίμακας επεξεργασία ευαίσθητων προσωπικών δεδομένων κλπ.	5.3, A.6.1.1, A.18.1.4	Εκτός από την απαίτηση του ΓΚΠΔ, ο ρόλος Υπεύθυνος Προστασίας Δεδομένων είναι ευρύτερα εφαρμόσιμος και πολύτιμος. Αυτό αποτελεί ζήτημα της Διοίκησης του Οργανισμού εκτός αν προκύπτει υποχρέωση με βάση τις απαιτήσεις του ΓΚΠΔ.
38	Ο Υπεύθυνος Προστασίας Δεδομένων χρειάζεται να υποστηρίζεται από τον	5.3,	Χωρίς υποστήριξη από τη Διοίκηση και εμπλοκή με τον οργανισμό, ένας

	οργανισμό και να ασχολείται με θέματα προστασίας δεδομένων.	Α.6.1.1, Α.18.1.4	Υπεύθυνος Προστασίας Δεδομένων είναι αδύναμος και άσκοπος
39	Ο Υπεύθυνος Προστασίας Δεδομένων πρέπει να παρέχει συμβουλές για θέματα απορρήτου, να παρακολουθεί τη συμμόρφωση, να έρχεται σε επαφή με τις αρχές, να ενεργεί ως σημείο επαφής, να αντιμετωπίζει τους κινδύνους απορρήτου κλπ.	5.3, Α.6.1.1, Α.18.1.4	Οι απαιτήσεις του ΓΚΠΔ θα αποτελούσαν τη βάση μιας περιγραφής ρόλου του Υπεύθυνου Προστασίας Δεδομένων.
ΤΜΗΜΑ 5 – ΚΩΔΙΚΕΣ ΔΕΟΝΤΟΛΟΓΙΑΣ ΚΑΙ ΠΙΣΤΟΠΟΙΗΣΗ			
40	Ο κώδικας δεοντολογίας βάσει του ΓΚΠΔ θα πρέπει να εγκριθεί επίσημα από αρμόδια αρχή	5.3, Α.6.1.1, Α.18.1.4	Η προστασία των προσωπικών δεδομένων δεν είναι απλώς θέμα αυστηρής συμμόρφωσης με τις επίσημες, νομικές υποχρεώσεις. Εκτός από αυτό ο κώδικας δεοντολογίας και τα σε συνεργασία με το πρότυπο 27001, προσφέρουν καθοδήγηση ορθής πρακτικής. Επομένως η συμμόρφωση μπορεί να δημιουργήσει εμπορικά πλεονεκτήματα.
41	Οι φορείς πίσω από τους κώδικες δεοντολογίας υποχρεούνται να παρακολουθούν τη συμμόρφωση, ανεξάρτητα από και με την επιφύλαξη της νομικής και κανονιστικής παρακολούθησης της συμμόρφωσης που διεξάγουν οι εθνικές αρχές.	5.3, Α.6.1.1, Α.18.1.4	Η προστασία των προσωπικών δεδομένων δεν είναι απλώς θέμα αυστηρής συμμόρφωσης με τις επίσημες, νομικές υποχρεώσεις. Εκτός από αυτό ο κώδικας δεοντολογίας και τα σε συνεργασία με το πρότυπο 27001, προσφέρουν καθοδήγηση ορθής πρακτικής. Επομένως η συμμόρφωση μπορεί να δημιουργήσει εμπορικά πλεονεκτήματα.
42	Παροτρύνεται να αναπτυχθούν και να καταχωρηθούν συστήματα πιστοποίησης προστασίας δεδομένων που παρέχουν σφραγίδες και σήματα συμμόρφωσης (ισχύς για 3 χρόνια).	5.3, Α.6.1.1, Α.18.1.4	Με βάση την τρέχουσα κατάσταση υπάρχουν σχήματα πιστοποίησης που καλύπτουν μέρη του ΓΚΠΔ.
43	Οι οργανισμοί πιστοποίησης που απονέμουν πιστοποιητικά, σφραγίδες και σήματα συμμόρφωσης πρέπει να είναι αρμόδιοι και διαπιστευμένοι για το σκοπό αυτό.	5.3, Α.6.1.1, Α.18.1.4	Αυτό θα βελτιώσει την αξιοπιστία και το νόημα των πιστοποιητικών, των σφραγίδων και των σημάτων προστασίας των δεδομένων.

ΚΕΦΑΛΑΙΟ V – ΔΙΑΒΙΒΑΣΗ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ ΠΡΟΣ ΤΡΙΤΕΣ ΧΩΡΕΣ Η΄ ΔΙΕΘΝΕΙΣ ΟΡΓΑΝΙΣΜΟΥΣ.			
44	Οι διεθνείς μεταφορές και επεξεργασία προσωπικών δεδομένων πρέπει να πληρούν τις προϋποθέσεις που ορίζονται στα επόμενα άρθρα		
45	Οι διαβιβάσεις δεδομένων σε χώρες των οποίων οι ρυθμίσεις απορρήτου (νόμοι, κανονισμοί, επίσημοι μηχανισμοί συμμόρφωσης κλπ) θεωρούνται επαρκείς από την Ευρωπαϊκή Επιτροπή (δηλαδή συμμορφώνονται με τον GDPR) και δεν απαιτούν επίσημη εξουσιοδότηση ή συγκεκριμένες πρόσθετες διασφαλίσεις	Α.18.1.4	Η συμμόρφωση συνεπάγεται την αποφυγή μεταβιβάσεων σε άλλες χώρες, την παρακολούθηση των επίσημων καταλόγων για αλλαγές και τη διασφάλιση ότι εφαρμόζονται κατάλληλες συμβάσεις / συμφωνίες και άλλοι έλεγχοι απορρήτου όπως και με άλλες μεταφορές δεδομένων τρίτων
46	Η μεταφορά δεδομένων σε χώρες των οποίων οι ρυθμίσεις απορρήτου (νόμοι, κανονισμοί, επίσημοι μηχανισμοί συμμόρφωσης κλπ) δεν θεωρούνται επαρκείς από την Ευρωπαϊκή Επιτροπή (δηλαδή δεν συμμορφώνονται με τον GDPR) αλλά πληρούν ορισμένα άλλα κριτήρια και συνεπώς απαιτούν πρόσθετες διασφαλίσεις.	Α.18.1.4	Ουσιαστικά, ο οργανισμός πρέπει να εφαρμόσει και να διασφαλίσει την επάρκεια των ελέγχων απορρήτου και πριν από τη μεταφορά προσωπικών δεδομένων σε τέτοιες χώρες αλλά και στη συνέχεια με κατάλληλες συμβατικές ρήτρες και δραστηριότητες συμμόρφωσης.
47	Οι εθνικές αρχές μπορούν να εγκρίνουν νομικά δεσμευτικούς κανόνες απορρήτου που επιτρέπουν τη μεταφορά σε μη εγκεκριμένες χώρες.	Α.18.1.4	Οι διατυπώσεις σε αυτούς τους κανόνες ενδέχεται να επηρεάσουν τους συμβατικούς όρους, τις ρυθμίσεις συμμόρφωσης, τις υποχρεώσεις κλπ.
48	Οι απαιτήσεις σε ευρωπαϊκούς οργανισμούς από αρχές εκτός Ευρωπαϊκής Ένωσης για την αποκάλυψη προσωπικών δεδομένων ενδέχεται να είναι άκυρες εκτός εάν καλύπτονται από διεθνείς συμφωνίες ή συνθήκες.	Α.18.1.4, Α.16	Τέτοιες καταστάσεις αντιμετωπίζονται συνήθως από ειδικούς σε θέματα νομικής και κανονιστικής συμμόρφωσης - αλλά μπορεί να ξεκινούν και ως περιστατικά.
49	Ακόμη περισσότερες προϋποθέσεις και όροι πρέπει να εφαρμόζονται σε περιπτώσεις που αφορούν μεταφορά προσωπικών δεδομένων σε χώρες εκτός	Α.18.1.4	Η Επιτροπή δυσκολεύει σκόπιμα, ή μάλλον μεριμνά ιδιαίτερα, καθώς οι

	Ευρωπαϊκής Ένωσης, όπως ρητή συγκατάθεση από τα υποκείμενα των δεδομένων.		κίνδυνοι προστασίας των δεδομένων είναι υψηλότεροι.
50 - 76		N/A	N/A
ΚΕΦΑΛΑΙΟ VIII – ΠΡΟΣΦΥΓΕΣ – ΕΥΘΥΝΗ ΚΑΙ ΚΥΡΩΣΕΙΣ			
77 - 81		N/A	N/A
82	Όποιος έχει υποστεί ζημιά λόγω παραβιάσεων του ΓΚΠΔ έχει δικαίωμα αποζημίωσης από τον Υπεύθυνο ή τον Εκτελών την επεξεργασία	A.18.1.4	Απόρρητο και προστασία αναγνωρίσιμων προσωπικών πληροφοριών.
83	Τα διοικητικά πρόστιμα που επιβάλλονται από τις εποπτικές αρχές είναι αποτελεσματικά, αναλογικά και αποτρεπτικά. Ορίζονται διάφορα κριτήρια. Ανάλογα με τις παραβάσεις και τις περιστάσεις, τα πρόστιμα μπορεί να φτάσουν τα 20 εκατομμύρια ευρώ ή έως και το 4% του συνολικού ετήσιου κύκλου εργασιών παγκοσμίως για το προηγούμενο έτος, όπου θα εφαρμοστεί το μεγαλύτερο από τα δύο.	6, A.18.1.4	Τέτοια τεράστια πρόστιμα προορίζονται σαφώς να αποτελέσουν ισχυρό αποτρεπτικό παράγοντα, που αντιπροσωπεύει σημαντικό μέρος του ενδεχόμενου αντίκτυπου των παραβιάσεων των προσωπικών δεδομένων, στην αξιολόγηση του οργανισμού σχετικά με τη συμμόρφωση με τον ΓΚΠΔ και άλλους κινδύνους απορρήτου.
84	Μπορεί να επιβληθούν και άλλες κυρώσεις. Πρέπει επίσης να είναι «αποτελεσματικοί, αναλογικοί και αποτρεπτικοί»	6, A.18.1.4	Τεράστια πρόστιμα προορίζονται σαφώς να αποτελέσουν ισχυρό αποτρεπτικό παράγοντα, που αντιπροσωπεύει σημαντικό μέρος του ενδεχόμενου αντίκτυπου των παραβιάσεων των προσωπικών δεδομένων, στην αξιολόγηση του οργανισμού σχετικά με τη συμμόρφωση με τον ΓΚΠΔ και άλλους κινδύνους απορρήτου
ΚΕΦΑΛΑΙΟ IX – ΔΙΑΤΑΞΕΙΣ ΠΟΥ ΑΦΟΡΟΥΝ ΕΙΔΙΚΕΣ ΠΕΡΙΠΤΩΣΕΙΣ ΕΠΕΞΕΡΓΑΣΙΑΣ			
85	Οι χώρες πρέπει να εξισορροπήσουν τα δικαιώματα προστασίας προσωπικών δεδομένων έναντι της ελευθερίας της	6, A.18.1.1, A.18.1.4	Τα ζητήματα βάσει αυτού του άρθρου ενδέχεται να καταλήξουν σε διαφορετικές νομικές ερμηνείες στο δικαστήριο,

	έκφρασης, της δημοσιογραφίας, της ακαδημαϊκής έρευνας κλπ μέσω κατάλληλων νόμων		επομένως και πάλι υπάρχουν κίνδυνοι για την ασφάλεια πληροφοριών που πρέπει να εντοπιστούν, να αξιολογηθούν και να αντιμετωπιστούν όταν εμπλέκονται προσωπικά δεδομένα.
86	Τα προσωπικά δεδομένα σε επίσημα έγγραφα ενδέχεται να αποκαλυφθούν στην περίπτωση που απαιτείται επίσημα να αποκαλυφθούν βάσει νομοθεσίας.	6, A.18.1.1, A.18.1.4	Μπορεί να είναι εφικτό να δημοσιευθούν προσωπικά ή άλλα ευαίσθητα στοιχεία.
87	Οι χώρες μπορούν να επιβάλουν περαιτέρω ελέγχους απορρήτου για εθνικούς αριθμούς ταυτότητας	6, A.18.1.1, A.18.1.4	Οι εθνικοί αριθμοί ταυτότητας μπορούν να χρησιμοποιηθούν ως μυστικοί προσωπικοί επικυρωτές, οπότε πρέπει να παραμείνουν εμπιστευτικοί για να μειώσουν τον κίνδυνο κλοπής ταυτότητας. Στην ουσία είναι ευαίσθητα προσωπικά στοιχεία, που υποδηλώνουν την ανάγκη για κρυπτογράφηση και άλλους ελέγχους ασφάλειας / απορρήτου
88	Οι χώρες ενδέχεται να επιβάλουν περαιτέρω περιορισμούς στην εταιρική επεξεργασία και τη χρήση προσωπικών δεδομένων σχετικά με τους υπαλλήλους, π.χ. για την προστασία της ανθρώπινης αξιοπρέπειας και των θεμελιωδών δικαιωμάτων.	6, A.18.1.1, A.18.1.4	Οι νόμοι για την απασχόληση ενδέχεται να συγκρούονται με τον ΓΚΠΔ και το απόρρητο, περιπλέκοντας περαιτέρω τη συμμόρφωση και αλλάζοντας τους κινδύνους για την ασφάλεια των πληροφοριών σε αυτόν τον τομέα.
89	Όπου προσωπικά δεδομένα πρόκειται να αρχειοθετηθούν π.χ. για ερευνητικούς και στατιστικούς σκοπούς, οι κίνδυνοι προστασίας της ιδιωτικής τους πρέπει να αντιμετωπιστούν μέσω κατάλληλων ελέγχων όπως ψευδώνυμοποιηση και ελαχιστοποίηση δεδομένων, όπου αυτό είναι εφικτό.	6, A.18.1.4	Οι απαιτήσεις για την ιδιωτικότητα παραμένουν όσο τα υποκείμενα των δεδομένων είναι ζωντανά (ίσως περισσότερο εάν οι οικογένειες ενδέχεται να επηρεαστούν από παραβιάσεις). Λαμβάνοντας υπόψη αυτό, οι κίνδυνοι για την ασφάλεια πληροφοριών πρέπει να εντοπίζονται, να αξιολογούνται και να αντιμετωπίζονται κατάλληλα.
90	Οι χώρες μπορούν να θεσπίσουν πρόσθετους νόμους σχετικά με την τήρηση απορρήτου και τις υποχρεώσεις για την ιδιωτικότητα των εργαζομένων.	6, A.18.1.1, A.18.1.4	Οι νόμοι για την απασχόληση ή το απόρρητο ενδέχεται να συγκρούονται με τον ΓΚΠΔ και το απόρρητο, περιπλέκοντας ακόμη περισσότερο τη συμμόρφωση και αλλάζοντας τους κινδύνους για την

			ασφάλεια πληροφοριών σε αυτόν τον τομέα.
91	Οι υφιστάμενοι κανόνες απορρήτου για εκκλησίες και θρησκευτικούς συλλόγους ενδέχεται να συνεχιστούν, υπό τον όρο ότι θα ευθυγραμμιστούν με τον ΓΚΠΔ.	Α.18.1.4	Απόρρητο και προστασία αναγνωρίσιμων προσωπικών πληροφοριών.
ΚΕΦΑΛΑΙΟ Χ – ΚΑΤ' ΕΞΟΥΣΙΟΔΟΤΗΣΗ ΠΡΑΞΗΣ ΚΑΙ ΕΚΤΕΛΕΣΤΙΚΕΣ ΠΡΑΞΕΙΣ			
92 - 99	Πώς θεσπίζεται ο ΓΚΠΔ από την Ευρωπαϊκή Ένωση.	Α.18.1.1	Δεν σχετίζεται με τις ρυθμίσεις απορρήτου ενός οργανισμού, εκτός εάν χρειάζεται να συμμορφώνονται με τους ισχύοντες νόμους και κανονισμούς.

Πίν.14: Πίνακας συσχετίσεων άρθρων του ΓΚΠΔ με το πρότυπο ISO 27001

4.2. Συμπέρασμα

Το ISO / IEC 27001 και ο ΓΚΠΔ στο πυρήνα τους έχουν από κοινού τη δέσμευση να επεξεργάζονται και να αποθηκεύουν σωστά τα ευαίσθητα και εμπιστευτικά δεδομένα. Επομένως, η εφαρμογή του ολοκληρωμένου πλαισίου ISO / IEC 27001 καθοδηγεί τη συμμόρφωση με τον ΓΚΠΔ, δεδομένου ότι πολλές από τις απαιτήσεις του κανονισμού καλύπτονται από το ISO / IEC 27001. Ωστόσο, πρέπει να προσαρμοστούν συγκεκριμένοι έλεγχοι για την αντιμετώπιση της προστασίας των προσωπικών δεδομένων εντός του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών.

Συμπερασματικά η εφαρμογή του προτύπου ISO 27001 είναι σε θέση να αποδείξει στις ρυθμιστικές αρχές ότι ο οργανισμός, που εφαρμόζει το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών, σε συμμόρφωση με τις απαιτήσεις του προτύπου, λαμβάνει την ασφάλεια των πληροφοριών σοβαρά υπόψη του και εφόσον έχει εντοπίσει τους κινδύνους, έχει κάνει οτιδήποτε είναι λογικά και τεχνικά δυνατό για να αντιμετωπιστούν. Εντούτοις, υπάρχουν ορισμένες απαιτήσεις του ΓΚΠΔ οι οποίες δεν καλύπτονται άμεσα από το ISO 27001, όπως η υποστήριξη των δικαιωμάτων των υποκειμένων των δεδομένων προσωπικού χαρακτήρα (για παράδειγμα το δικαίωμα ενημέρωσης και το δικαίωμα διαγραφής των δεδομένων τους), η φορητότητα των προσωπικών δεδομένων, καθώς και οι ιδιαιτερότητες της προστασίας της ιδιωτικής ζωής, όπως οι επιπτώσεις στα άτομα.

ΚΕΦ.5: Συμπεράσματα – Προτάσεις

Η συμμόρφωση με τις «επιταγές» του ΓΚΠΔ δεν είναι ένα εφάπαξ έργο που τερματίζεται όταν ολοκληρωθεί η διαδικασία. Αντίθετα, είναι διαρκές και συνεχίζεται για όσο τα δεδομένα προσωπικού χαρακτήρα κυκλοφορούν και υφίστανται επεξεργασία. Προκειμένου να επιτευχθεί και να διατηρηθεί η συμμόρφωση, θα πρέπει να υπάρξουν διαδικασίες που να ελέγχουν, να αναθεωρούν τα κριτήρια και να προτείνουν διορθώσεις. Η πιστοποίηση από μόνη της είναι κενή περιεχομένου εάν οι Υπεύθυνοι επεξεργασίας και οι Εκτελούντες την επεξεργασία δεν είναι σε θέση να αποδείξουν τη συμμόρφωση.

Μια επίσημη σύσταση ενός συγκεκριμένου προτύπου απαιτεί προσεκτική εξέταση της καταλληλότητας και της ποιότητάς του και θα πρέπει να συμπεριληφθούν, μεταξύ άλλων, οι ακόλουθες πτυχές:

- Το πρότυπο πρέπει να είναι αρκετά πλούσιο σε αυτό που καλύπτει ώστε να αποφευχθεί η προώθηση μιας σειράς προτύπων τα οποία ασχολούνται με υπό – θέματα.
- Το πρότυπο πρέπει να είναι συνεπές με τον ΓΚΠΔ ώστε να αποφευχθεί η προώθηση προτύπων που αντιβαίνουν στις νομικές αρχές που περιλαμβάνονται στο ευρωπαϊκό πλαίσιο προστασίας δεδομένων.
- Το πρότυπο θα πρέπει να είναι αρκετά ώριμο, δεδομένου ότι η πιθανότητα να ξεπεραστεί από ένα άλλο πιο ώριμο πρότυπο να μπορεί να θεωρηθεί χαμηλή.
- Το πρότυπο δεν θα πρέπει να είναι διφορούμενο σε οτιδήποτε επιδιώκει, προωθώντας ευρέως κοινούς και σαφείς σκοπούς.
- Στο πλαίσιο ενός διεθνούς προτύπου, όχι μόνο ευρωπαϊκό, θα μπορούσαν επίσης να ληφθούν υπόψη τα κριτήρια του Annex II του Κανονισμού 1025/2012 (Requirements for the identification of ICT technical specifications). Τα κριτήρια αυτά καλύπτουν την πηγή, τη διαδικασία και το περιεχόμενο ενός προτύπου. Βάσει του Κανονισμού 1025/2012, ο εκδότης προτύπων πρέπει να είναι μη κερδοσκοπικός οργανισμός (πχ επαγγελματική ένωση, βιομηχανικός ή επαγγελματικός σύνδεσμος κλπ). Όσον αφορά τις διαδικαστικές πτυχές, η διαδικασία σύνταξης πρέπει να συμβαδίζει με ανοικτά τύπου πρότυπα, τη συναίνεση και τη διαφάνεια. Σχετικά με το περιεχόμενο των βασικών προδιαγραφών, τα κριτήρια είναι η διατήρηση, η διαθεσιμότητα, τα δικαιώματα πνευματικής ιδιοκτησίας, η συνάφεια, η ουδετερότητα, η σταθερότητα καθώς επίσης και η ποιότητα.

Βάσει της τρέχουσας κατάστασης υπάρχει ένα σημαντικό σύνολο προτύπων σχετικά με τους μηχανισμούς πιστοποίησης, η βάση των οποίων κυριαρχείται σαφώς από τα διεθνή πρότυπα, ιδίως από το ISO και το IEC. Ορισμένα από τα πρότυπα ISO και IEC έχουν εγκριθεί ως ευρωπαϊκά πρότυπα ενώ άλλα είναι διαθέσιμα μόνο ως διεθνή πρότυπα.

Εξακολουθεί να υπάρχει σημαντικός αριθμός πρωτοβουλιών τυποποίησης που βρίσκονται σε εξέλιξη, με στόχο την ενίσχυση του συνόλου των προτύπων που σχετίζονται με την προστασία δεδομένων και των προτύπων που σχετίζονται ειδικότερα με τον ΓΚΠΔ. Παρ' όλα αυτά, μέχρι σήμερα, κανένα δημοσιευμένο πρότυπο δεν περιγράφει τον τρόπο διεξαγωγής της διαδικασίας σχετικά με την εκτίμηση των κινδύνων και του αντικτύπου για την ζωή των υποκειμένων των δεδομένων ώστε να αντιμετωπιστούν με ανάλογο τρόπο. Επομένως, η ανάπτυξη ενός συνεκτικού και επαρκούς συνόλου ευρωπαϊκών προτύπων πλήρως εναρμονισμένων με τις αρχές και τους μηχανισμούς του ΓΚΠΔ χρειάζεται ακόμη σημαντικές προσπάθειες.

Προώθηση πιστοποίησης

Στο πλαίσιο του ΓΚΠΔ, οι εγκεκριμένες πιστοποιήσεις θεωρούνται σημαντικό μέσο για την παροχή καθοδήγησης σχετικά με την εφαρμογή των κατάλληλων μέτρων καθώς και για την απόδειξη της συμμόρφωσης από τον Υπεύθυνο επεξεργασίας ή τον Εκτελών την επεξεργασία.

Τα πιθανά μέτρα που μπορούν να χρησιμοποιηθούν για την προώθηση και αναγνώριση των μηχανισμών πιστοποίησης της προστασίας δεδομένων βάσει του ΓΚΠΔ μπορεί να είναι αρκετά διαφορετικά και μπορούν να κατηγοριοποιηθούν με διάφορους τρόπους όπως αναφορικά με τους αποδέκτες:

- τα συμβαλλόμενα μέρη που προσφέρουν και εφαρμόζουν πιστοποιήσεις προστασίας δεδομένων (νομικοί εμπειρογνώμονες, σύμβουλοι, επιθεωρητές, φορείς πιστοποίησης, φορείς διαπίστευσης)
- Κοινοτικοί και Εθνικοί νομοθέτες και αρμόδιες Αρχές
- Υπεύθυνοι και Εκτελούντες την επεξεργασία δεδομένων, συμπεριλαμβανομένων των Μικρών και Μεσαίων Επιχειρήσεων.

Λαμβάνοντας υπόψη την εξουσία που παρέχεται στην Επιτροπή, στο πλαίσιο του ΓΚΠΔ, μια άλλη σημαντική διάκριση είναι αυτή μεταξύ νομοθετικών (μορφών ρύθμισης και επιβολής) και μη νομοθετικών μέτρων. Η πρώτη κατηγορία περιλαμβάνει την επιβολή σε επίπεδο Ευρωπαϊκής Ένωσης και σε εθνικό επίπεδο, παρέχοντας νομική σαφήνεια ως προς το καθεστώς των πιστοποιήσεων που σχετίζονται με τον ΓΚΠΔ, αύξηση του νομικού προστατευτικού

αποτελέσματος της πιστοποίησης, εξασφάλιση της αμοιβαίας αναγνώρισης κλπ. Τα μη νομοθετικά καλύπτουν επίσης ένα ευρύ φάσμα μέτρων, όπως η ευαισθητοποίηση, η πληροφόρηση, η κατάρτιση και η οικονομική στήριξη συμπεριλαμβανομένων των φορολογικών κινήτρων και επιδοτήσεων. Επιπλέον, σε αυτά θα μπορούσαν να ενταχθούν οι δημόσιες συμβάσεις, η στήριξη της ανάπτυξης και της πρόσβασης σε σχετικά πρότυπα, η εκτίμηση των επιπτώσεων αλλά και η παρακολούθηση του κόστους συμμόρφωσης των επιχειρήσεων.

Από τα παραπάνω γίνεται αντιληπτό πως η δημιουργία ενός ολοκληρωμένου Συστήματος Διαχείρισης της Ασφάλειας των Πληροφοριών, το οποίο συμμορφώνεται με τις απαιτήσεις του προτύπου ISO 27001, επιτρέπει στους οργανισμούς που επεξεργάζονται δεδομένα προσωπικού χαρακτήρα, να αποδεικνύουν ότι οι κίνδυνοι για τα προσωπικά δεδομένα επανεξετάζονται (άρθρο 32 παράγραφος 1 - σημείο δ και παράγραφος 2), και οι σχετικές διαδικασίες ενημερώνονται και βελτιώνονται συνεχώς. Ένα εδραιωμένο Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών είναι το ιδανικό πλαίσιο για τη διαχείριση των κινδύνων για όλα τα πληροφοριακά περιουσιακά στοιχεία του οργανισμού, στα οποία συμπεριλαμβάνονται και τα προσωπικά δεδομένα, και μπορεί να παρέχει τη συνεχή διαβεβαίωση ότι ο οργανισμός λαμβάνει σοβαρά υπόψη τις προδιαγραφές ασφάλειας ISO 27001 αλλά και αυτές του ΓΚΠΔ (άρθρο 32).

Η εφαρμογή του ISO 27001 καλύπτει τις περισσότερες από τις απαιτήσεις του ΓΚΠΔ. Ωστόσο, ορισμένα στοιχεία ελέγχου πρέπει να προσαρμοστούν ώστε να περιλαμβάνουν και προσωπικά δεδομένα στο Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών. Εκτός από αυτό που έχει προγραμματιστεί για την εφαρμογή του ISO 27001, ορισμένα μέτρα είναι αναγκαίο να συμπεριληφθούν προκειμένου ένας οργανισμός, είτε ως Υπεύθυνος επεξεργασίας είτε ως Εκτελών την επεξεργασία, να διασφαλίσει τη συμμόρφωση με τον ΓΚΠΔ. Ειδικότερα, χρειάζεται να σχεδιαστούν διαδικασίες με σκοπό την εξασφάλιση της άσκησης των δικαιωμάτων των υποκειμένων των δεδομένων καθώς και μηχανισμοί για τη μεταφορά δεδομένων εκτός Ευρωπαϊκής Ένωσης στοχεύοντας στην ισορροπία μεταξύ της ελεύθερης διακίνησης των προσωπικών δεδομένων και της προστασίας της ελευθερίας και των δικαιωμάτων των φυσικών προσώπων. Παράλληλα, σε αυτά μπορούν να προστεθούν η εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων καθώς και οι διαδικασίες που πρέπει να ακολουθούνται σε περίπτωση παραβίασής τους. Όλοι αυτοί οι έλεγχοι μπορούν να ενσωματωθούν στο Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών, ως εγγύηση της νομικής συμμόρφωσης και της συνεχούς βελτίωσης, ακόμη περισσότερο όταν το Σύστημα και ο ΓΚΠΔ ευθυγραμμίζονται.

Το πρότυπο ISO 27001 είναι ένα εξαιρετικό πλαίσιο για την ασφάλεια των πληροφοριών. Εάν ο οργανισμός έχει ήδη εφαρμόσει το πρότυπο, είναι τουλάχιστον στη μέση της διασφάλισης της προστασίας των προσωπικών δεδομένων και της ελαχιστοποίησης του κινδύνου διαρροής, από την οποία οι ηθικές και κυρίως οι οικονομικές επιπτώσεις θα μπορούσαν να είναι καταστροφικές για τον οργανισμό.

ΒΙΒΛΙΟΓΡΑΦΙΑ

- Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών. – Γενικός Κανονισμός για την Προστασία Δεδομένων – ΓΚΠΔ
- ΝΟΜΟΣ ΥΠ' ΑΡΙΘΜ. 4624 – Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις ΑF
- Κατευθυντήριες γραμμές 1/2018 σχετικά με την πιστοποίηση και τον προσδιορισμό κριτηρίων πιστοποίησης σύμφωνα με τα άρθρα 42 και 43 του κανονισμού 2016/679 (Έκδοση 3.0 – 4 Ιουνίου 2019)
- Data Protection Certification Mechanisms - Study on Articles 42 and 43 of the Regulation (EU) 2016/679 – Final Report (Authors: Irene Kamara, Ronald Leenes, Eric Lachaud, Kees Stuurman (TILT), Marc van Lieshout, Gabriela Bodea (TNO). Contributors: Camille Salinier, Kris Best (CIVIC Consulting), Mirell Piir, Magdalena Brewczyńska (TILT))
- Data Protection Certification Mechanisms – Study on Articles 42 and 43 of the Regulation (EU) 2016/679 – Final Report – ANNEXES
- Recommendations on European Data Protection Certification VERSION 1.0 NOVEMBER 2017 (© European Union Agency for Network and Information Security (ENISA), 2017 – ISBN 978-92-9204-238-7, DOI 10.2824/787306)
- ISO / IEC 27002:2013,Information technology – Security Techniques – Code of practice for information security controls
- ΕΝΟΠΟΙΗΜΕΝΗ ΑΠΟΔΟΣΗ ΤΗΣ ΣΥΝΘΗΚΗΣ ΓΙΑ ΤΗΝ ΕΥΡΩΠΑΪΚΗ ΕΝΩΣΗ ΚΑΙ ΤΗΣ ΣΥΝΘΗΚΗΣ ΓΙΑ ΤΗ ΛΕΙΤΟΥΡΓΙΑ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ (2016/C 202/01).
- International Accreditation Forum, 'The value of accredited certification. Survey Report' (May 2012)

- Γ. Γιαννόπουλος, Ροή Πληροφοριών στο Διαδίκτυο, 2002
- Υπό δημοσίευση άρθρο Επίκουρου Καθηγητή Νομικής Σχολής Πανεπιστημίου Αθηνών κ. Γ. Ν. Γιαννόπουλου, «V. Κώδικες δεοντολογίας και πιστοποίηση»
- Lawspot GDPR - https://www.lawspot.gr/gdpr
- Certification – Trust, Accountability, Liability – editor : Peter Rott (University of Kassel) - Volume 16 - ISBN 978-3-030-02498-7
- Adhering to GDPR codes of conduct: A possible option for SMEs to GDPR certification - Eric Lachaud - TILT, the Tilburg Institute for Law, Technology, and Society, Tilburg University, The Netherlands
- The General Data Protection Regulation and the rise of certification as a regulatory instrument - Eric Lachaud - Tilburg Institute for Law, Technology, and Society (TILT), Tilburg Law School, The Netherlands
- The future of privacy certification in Europe: an exploration of options under article 42 of the GDPR. (28/06/2016) - Rowena Rodrigues, David Barnard-Wills, Paul De Hert & Vagelis Papakonstantinou - http://dx.doi.org/10.1080/13600869.2016.1189737
- https://www.itsecuritypro.gr/diachirisi-asfalias-pliroforion-sygchroni-epichirisiaki-anagkeotita-2/ - Tag: IT issue 5
- http://www.elot.gr
- ISO/IEC 17000:2004
- Κανονισμός (ΕΚ) αριθ. 765/2008 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 9ης Ιουλίου 2008
- IAF, Accreditation Assessment of Conformity Assessment Bodies with Activities in Multiple Countries, Issue 2, 2016
- The British Standards Institution, 'Personal Information Management',(Bsigroup) https://www.bsigroup.com/en-GB/BS-10012-Personal-information-management/
- InVeo, 'ISDP 10003:2015 Data Protection Certification' (InVeo Accredited Certification Body) https://www.in-veo.com/en/certification/isdp-10003-2015-data-protection
- ULD, ' Datenschutzaudit beim ULD' (ULD, 2018) https://www.datenschutzzentrum.de/audit/
- E- Privacy sealhttps://www.eprivacy.eu/en/privacy-seals/eprivacyseal/

- EuroPrise, 'European Privacy Seal' (European Privacy Seal for IT Products and IT-Based Services) <https://www.european-privacy-seal.eu/EPS-en/Home >
- CNIL, 'Data Protection' (CNIL) https://www.cnil.fr/fr/labels
- JIPDEC, 'PrivacyMark' (PrivacyMark System) https://privacymark.org/
- Ryerson university, 'Privacy by Design Certification' (Privacy by Design Centre of Excellence, 2018) http://www.ryerson.ca/pbdce/certification/
- TrustArc, 'Extend your privacy commitment with the APEC Cross Border Privacy Certification' (TrustArc, 2018)https://www.trustarc.com/products/apec-certification/
- ISO/IEC Directives, Part 1, Annex SL, Appendix 2 – HLS (2012)