ΕΝΟΠΟΙΗΣΗ GDPR & ISO

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΓΙΑΝΝΑΚΟΠΟΥΛΟΣ ΣΩΤΗΡΙΟΣ ΜΤΕ1707
GIANNA.KO@SSL-UNIPI.GR

Πίνακας περιεχομένων

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

ΣΥΝΤΟΜΕΥΣΕΙΣ

ΕΕ = Ευρωπαϊκή Ένωση

GDPR = General Data Protection Regulation

ISO = International Organization for Standardization

CIA = Confidentiality Integrity Availability (Εμπιστευτικότητα, Ιδιωτικότητα Διαθεσιμότητα)

ISMS = Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών

IEC = International Electrotechnical Commission

ΠΕΡΙΛΗΨΗ

Ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων αντιλήφθηκε την ανάγκη για μεταρρύθμιση των κανόνων της Ευρωπαϊκής Ένωσης (ΕΕ) σχετικά με την προστασία των δεδομένων, κανόνες που είχαν θεσπιστεί σε ευρωπαϊκό επίπεδο για πρώτη φορά το 1995. Η ανάγκη αυτή αποσκοπεί στην ενίσχυση κυρίως των δικαιωμάτων της διαδικτυακής ιδιωτικότητας, εξαιτίας του ότι η ραγδαία ανάπτυξη της τεχνολογίας από το 1995 και ύστερα δεν μπορεί να θεωρηθεί ανάλογη με τις μεταρρυθμίσεις που έλαβαν χώρα για την προστασία των Ευρωπαίων πολιτών.

Συγκεκριμένα, η οδηγία που δημιουργούσε το νομικό πλαίσιο γύρω από την προστασία των προσωπικών δεδομένων, δεν είχε δεχτεί κάποια τροποποίηση, με αποτέλεσμα οι διάφοροι ενδιαφερόμενοι να επιδίδονται στην απόκτηση προσωπικών πληροφοριών χωρίς τη συγκατάθεση των ιδιωτών. Με τον τρόπο αυτό παραβίαζαν συστηματικά τη σφαίρα ιδιωτικότητας των πολιτών, χωρίς να δίνεται στους τελευταίους είτε η επιλογή άρνησης παραχώρησης των προσωπικών τους πληροφοριών είτε η νομική προστασία τους από τις διαρροές αυτές.

Προκειμένου ο ευρωπαίος νομοθέτης να προστατέψει τους πολίτες των χωρών της ΕΕ, δημιούργησε ένα νέο σύγχρονο νομικό πλαίσιο μέσω της εφαρμογής του Κανονισμού 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου «για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και την ελεύθερη κυκλοφορία των δεδομένων αυτών», γνωστός με το ακρωνύμιο GDPR. (General Data Protection Regulation). Από το χρονικό σημείο έναρξης της εφαρμογής του, όλες οι εταιρείες, οι οποίες δραστηριοποιούνται στην ευρωπαϊκή επικράτεια, θα πρέπει να τον τηρούν.

Έτσι, παρουσιάστηκε η ανάγκη να δημιουργηθεί κάποιο πρότυπο, από την εφαρμογή του οποίου οι εταιρείες θα δύνανται να πιστοποιηθούν, ώστε να καλύψουν μεγάλο εύρος από τα απαιτούμενα που θέτει ο Κανονισμός. Ένα τέτοιο πρότυπο είναι η πιστοποίηση ISO 27001. Με βάση την πιστοποίηση αυτή, οι εταιρείες μπορούν να έχουν ένα αρκετά ικανοποιητικό επίπεδο ασφαλείας, όσον αφορά τα διάφορα προσωπικά δεδομένα που έχουν στην κατοχή τους.

Στόχος της συγκεκριμένης έρευνας είναι να καταδείξει τα σημεία, στα οποία τέμνονται ο Κανονισμός της ΕΕ με τις διαδικασίες για την απόκτηση της πιστοποίησης ISO 27001.

1. ΠΛΗΡΟΦΟΡΙΕΣ

Ένα σημαντικό στοιχείο σε μια διαδικασία επικοινωνίας δύο ή περισσοτέρων ατόμων είναι η ανταλλαγή πληροφοριών που γίνεται με ένα μήνυμα το οποίο περιέχει νέα στοιχεία σε σύγκριση με αυτά που γνώριζε προηγουμένως ο χρήστης, σχετικά με το χαρακτηρισμό μίας συγκεκριμένης κατάστασης ή κάποιων φαινόμενων ή ορισμένων γεγονότων ή κάποιων οικονομικών διαδικασιών.

Οι πληροφορίες μπορούν να αποθηκευτούν με διαφορετικούς τρόπους, συμπεριλαμβανομένων των εξής: με ψηφιακή μορφή (αρχεία δεδομένων αποθηκευμένα σε οπτική ή ηλεκτρονική αποθήκευση) ή με μορφή υλικού (π.χ. χαρτί). Επίσης υπάρχουν και πληροφορίες που δεν μπορούν να αποθηκευτούν κάπου αλλά βασίζονται στις γνώσεις των εργαζομένων.

Επίσης και η μετάδοση των πληροφοριών μπορεί να πραγματοποιηθεί με διάφορες μεθόδους, οι οποίες είναι : με υπηρεσία ταχυμεταφορών, με ηλεκτρονική επικοινωνία ή προφορικά. Επιπλέον είναι υποχρεωτικό να ταξινομούνται όλες οι πληροφορίες, ανεξάρτητα στο πού χρησιμοποιούνται. Στην ΕΕ, οι πληροφορίες ταξινομούνται με τους παρακάτω τρόπους: ως αυστηρά μυστικές, μυστικές, εμπιστευτικές και περιορισμένες. Επίσης υπάρχει και μια ευρύτερη ταξινόμηση για τις πληροφορίες, που τις διαχωρίζει σε υποκειμενικές πληροφορίες και αντικειμενικές πληροφορίες. Στο πρότυπο ISO 27001 δεν αναφέρεται ότι οι πληροφορίες ταξινομούνται με συγκεκριμένο τρόπο, αλλά αντίθετα επιτρέπεται σε όλες τις εταιρείες να εφαρμόσουν την δική τους ταξινόμηση. Τα συστήματα ταξινόμησης πρέπει να εξετάζουν τα ουσιώδη χαρακτηριστικά των πληροφοριών: εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα. Οι περισσότερες μέθοδοι που χρησιμοποιούνται έχουν 4 επίπεδα ασφαλείας:

- Δημόσιες ή μη περιορισμένες πληροφορίες
- Εσωτερικές ή προστατευμένες πληροφορίες
- Εμπιστευτικές πληροφορίες
- Μυστικές ή περιορισμένες πληροφορίες

Αυτό το μοντέλο μπορεί να βελτιωθεί σύμφωνα με τις αντικειμενικές ανάγκες της εταιρείας. Αξίζει να αναφέρουμε ότι μέσα σε ένα μοντέλο ταξινόμησης, η τοποθέτηση πληροφοριών σε μια κατηγορία ταξινόμησης δεν είναι τελική αλλά

μπορεί να υποστεί αλλαγές σύμφωνα με τις πολιτικές που ακολουθεί η εταιρεία. Γι' αυτό οι πληροφορίες πρέπει να ταξινομηθούν σύμφωνα με την αξία, τις νομικές απαιτήσεις και το επίπεδο οργάνωσης της εταιρείας. Το πρότυπο ISO 27002 συνιστά τα ακόλουθα για την ταξινόμηση των πληροφοριών:

- Η ταξινόμηση των πληροφοριών μπορεί να γίνει με βάση τις αντικειμενικές ανάγκες προστασίας, δηλαδή με τις πληροφορίες που προκύπτουν από το πεδίο δραστηριότητας της εταιρείας και τον αντίκτυπο που έχει η αποκάλυψή τους, η μη εξουσιοδοτημένη χρήση τους ή ακόμη και η κατά-στροφή οποιουδήποτε είδους πληροφορίας που μπορεί να συμβεί στην Εταιρεία.
- Το επίπεδο προστασίας των πληροφοριών πρέπει να αναλυθεί στο πλαίσιο της CIA (Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα).
- Οι κανόνες για τη χρήση και τον έλεγχο των πληροφοριών πρέπει να βασίζονται στην ταξινόμηση των πληροφοριών.
- Η διοίκηση της εταιρείας πρέπει να επανεξετάζει περιοδικά την ταξινόμηση των πληροφοριών σύμφωνα με τις πολιτικές πρόσβασης που έχουν αποφασιστεί.
- Η ευθύνη για τη διάθεση των πληροφοριών σε μια συγκεκριμένη κατηγορία και για την αναθεώρησή της ανήκει στον κάτοχο των πληροφοριών.
- Όταν οι πληροφορίες μοιράζονται με τρίτους, θα πρέπει να επιλέξουν τα μέτρα που μπορούν να εξαλείψουν τυχόν διαφωνίες που σχετίζονται με την χρήση.
- Οι ιδιοκτήτες των πληροφοριών πρέπει να εποπτεύουν τη χρήση των πληροφοριών από κάθε κατηγορία ταξινόμησης και πρέπει να λάβουν υπόψη τους ακόλουθους τύπους επεξεργασίας: δημιουργία, τροποποίηση, αντιγραφή, αποθήκευση μετάδοση μέσω ταχυδρομείου, φαξ, ηλεκτρονικού ταχυδρομείου, προφορικά, μέσω τηλεφώνου, φωνητικού ταχυδρομείου και τηλεφωνητή.

1.1 Ασφάλεια πληροφοριών

Η ασφάλεια των πληροφοριών όπως έχουμε αναφέρει και προηγουμένως αποτελείται από τρεις σημαντικές πτυχές: εμπιστευτικότητα, διαθεσιμότητα και ακεραιότητα . Για να υπάρξει επιτυχία στην επιχείρηση, συνέχεια αυτής και ελαχιστοποίηση των επιπτώσεων των πληροφοριών είναι απαραίτητα κατάλληλα μέτρα ασφαλείας στη χρήση και τη διαχείριση πληροφοριών γιατί υπάρχει μεγάλος αριθμός απειλών. Η ασφάλεια των πληροφοριών πετυχαίνετε με την εφαρμογή μιας σειράς ελέγχων και είναι απαραίτητη η λήψη μέτρων για τη διαχείριση κινδύνου επεξεργασίας με τη χρήση ενός ISMS το οποίο περιλαμβάνει πολιτικές, διαδικασίες, οργανωτικές δομές, λογισμικό και κατάλληλο υλικό, προκειμένου να προστατευτούν οι αναγνωρισμένοι πληροφοριακοί πόροι.

1.2 Κίνδυνοι και προσεγγίσεις όσον αφορά ασφάλεια των πληροφοριών

Η σημερινή κοινωνία αντιμετωπίζει σε μόνιμη βάση μια μεγάλη ποικιλία κινδύνων: φυσικοί κίνδυνοι, επαγγελματικοί κίνδυνοι στην υγεία, κίνδυνοι στην ασφάλεια των πληροφοριών, κίνδυνοι για το φυσικό περιβάλλον. Όλα αυτά έχουν τις αρνητικές επιπτώσεις στις μελλοντικές γενιές και η επίδραση τους είναι πιθανό να είναι μόνιμη.

Ένας από τους πολυάριθμους ορισμούς του κινδύνου είναι η πιθανότητα εμφάνισης απειλής και χαρακτηρίζεται από την μια πλευρά από τη σοβαρότητα των συνεπειών και από την άλλη από την πιθανότητα εμφάνισής του. Ένας οργανισμός που θέλει την εφαρμογή και πιστοποίηση ενός συστήματος διαχείρισης ασφάλειας πληροφοριών, θα πρέπει να ορίζει και να εφαρμόζει μια διαδικασία που ακολουθεί τα παρακάτω βήματα:

- Δημιουργία και διατήρηση της ασφάλειας των πληροφοριών με βάση τα κριτήρια κινδύνου ασφαλείας, αποδοχής κινδύνου και αξιολόγησης κινδύνου.
- Επιβεβαίωση ότι η αξιολόγηση κινδύνου είναι συνεχής και επαναλαμβανόμενη και μπορεί να παράγει συνεπή, έγκυρα και συγκρίσιμα αποτελέσματα .

- Αναγνώριση κινδύνων, δηλαδή κινδύνων που σχετίζονται με εμπιστευτικότητα πληροφοριών, ακεραιότητα και απώλεια διαθεσιμότητας και προσδιορίζουν τους ιδιοκτήτες των πληροφοριών που είναι υπεύθυνοι για αυτούς τους κινδύνους.
- Ανάλυση κινδύνου, σε περίπτωση εμφάνισης του εντοπισμένου κινδύνου, πραγματική πιθανότητα εμφάνισης του προσδιορισμένου κινδύνου και προσδιορισμός του επιπέδου κινδύνου.
- Εκτίμηση κινδύνων.

2 ΚΕΦΑΛΑΙΟ

2.1 ISO 27001

Η σειρά ISO 27000, αναπτύσσεται και δημοσιεύεται από τον ISO και τον IEC για την παροχή ενός παγκοσμίως αναγνωρισμένου πλαισίου για βέλτιστη πρακτική διαχείριση της ασφάλειας των πληροφοριών.

Αυτά τα πρότυπα ασφαλείας βοηθούν τους οργανισμούς να διατηρούν ασφαλή τα πληροφοριακά τους στοιχεία, όπως οι οικονομικές τους πληροφορίες, τα στοιχεία των εργαζομένων και η πνευματική τους ιδιοκτησία. Ο πυλώνας της σειράς ISO 27000 είναι το ISO / IEC 27001: 2013 (επίσης γνωστός ως ISO 27001). Το ISO / IEC 27001, είναι ένα πρότυπο ασφαλείας που περιγράφει τις προτεινόμενες απαιτήσεις για την κατασκευή, την παρακολούθηση και τη βελτίωση ενός ISMS. Το ISMS είναι ένα πλαίσιο πολιτικών και διαδικασιών που περιλαμβάνει τους νομικούς, τεχνικούς και φυσικούς ελέγχους που εμπλέκονται στις διαδικασίες διαχείρισης κινδύνων μιας εταιρείας. Παράγοντες που επηρεάζουν την εφαρμογή του ISMS περιλαμβάνουν τους στόχους του οργανισμού, τις απαιτήσεις ασφάλειας, το μέγεθος και τη δομή. Το ISO 27001 παρέχει ένα αποδεδειγμένο πλαίσιο που βοηθά τους οργανισμούς να προστατεύουν τις πληροφορίες τους μέσω αποτελεσματικών πρακτικών τεχνολογίας, ελέγχου και δοκιμών, οργανωτικών διαδικασιών και προγραμμάτων ευαισθητοποίησης του προσωπικού.

2.2 GDPR

Ο GDPR αφορά στην διαμόρφωση ενός ενιαίου νομοθετικού πλαισίου για την επεξεργασία προσωπικών δεδομένων στα κράτη μέλη της ΕΕ. Το GDPR εγκρίθηκε από το κοινοβούλιο της ΕΕ στις 14 Απριλίου 2016 και τέθηκε σε ισχύ στις 25 Μαΐου 2018 και αντικαθιστά την οδηγία της ΕΕ για την προστασία των δεδομένων του 1995. Η νέα οδηγία εστιάζεται στη διατήρηση της διαφάνειας των επιχειρήσεων και στην επέκταση των δικαιωμάτων της ιδιωτικής ζωής των υποκειμένων των δεδομένων. Οι οδηγίες στον κανονισμό γενικής προστασίας δεδομένων ισχύουν για όλα τα δεδομένα που παράγουν οι πολίτες της ΕΕ, ανεξάρτητα από το αν η εταιρεία που συλλέγει τα εν λόγω δεδομένα βρίσκεται

στην ΕΕ, καθώς και όλα τα άτομα των οποίων τα δεδομένα αποθηκεύονται εντός της ΕΕ, είτε αυτά είναι είτε όχι στην πραγματικότητα πολίτες της ΕΕ.

2.3 Λίγα λόγια για ISO 27001 & GDPR

Οι συνεχώς αυξανόμενες επιθέσεις στον κυβερνοχώρο δείχνουν την ανάγκη στους οργανισμούς (ανεξαρτήτους του μεγέθους τους) να αρχίσουν να λαμβάνουν σοβαρά υπόψη την ασφάλεια των δεδομένων και να περιορίζουν πολύ πιο αποτελεσματικά τον κίνδυνο. Για τον παραπάνω λόγο κρίνεται απαραίτητο το νομικό πλαίσιο να συμβαδίσει με αυτές τις απειλές. Ο εγκεκριμένος κανονισμός της ΕΕ για την γενική προστασία δεδομένων (GDPR)[1] οδηγεί στην αποτελεσματική αντιμετώπιση μερικών κενών που υπήρχαν, με αποτέλεσμα την μείωση των επιθέσεων στο κυβερνοχώρο.

Όλοι αυτοί οι οργανισμοί που χειρίζονται τα προσωπικά δεδομένα των Ευρωπαίων πολιτών θα πρέπει να υιοθετήσουν τις απαιτήσεις του GDPR. Ο κανονισμός εισάγει αυστηρές κυρώσεις για τη μη συμμόρφωση σε αυτόν, ενώ οι οργανισμοί που τον παραβιάζουν αντιμετωπίζουν πρόστιμα μέχρι 4% του ετήσιου παγκόσμιου κύκλου εργασιών ή 20 εκατ. Ευρώ (όποιο πρόστιμο από τα δυο είναι μεγαλύτερο).

Ένας τρόπος που μπορεί να οδηγήσει τις επιχειρήσεις να συμμορφωθούν με αυτόν τον κανονισμό, είναι να πετύχουν την συμμόρφωση με το διεθνές πρότυπο για την ασφάλεια των πληροφοριών ISO 27001.

Το Πρότυπο καλύπτει τρεις βασικές πτυχές της ασφάλειας των πληροφοριών:

- τους ανθρώπους
- τις διαδικασίες
- την τεχνολογία

Με την υιοθέτηση μέτρων για την προστασία της πληροφορίας με βάση την τριπλή αυτή προσέγγιση, ο οργανισμός μπορεί να υπερασπιστεί όχι μόνο τους κινδύνους που οφείλονται στην τεχνολογία αλλά και άλλους πιο κοινούς κινδύνους, όπως το ανεπαρκώς ενημερωμένο προσωπικό ή τις αναποτελεσματικές διαδικασίες που μπορεί να ακολουθεί.

[1]ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2016/679 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 27ης Απριλίου 2016

Με την εφαρμογή του ISO 27001, ο οργανισμός έχει την δυνατότητα να αναπτύξει ένα ISMS: όταν το σύστημα αυτό υποστηρίζεται από την ηγεσία, ενσωματώνεται στην κουλτούρα και τη στρατηγική του οργανισμού ενώ ταυτόχρονα παρακολουθείται, ενημερώνεται και ελέγχεται συνεχώς. Χρησιμοποιώντας μια διαδικασία συνεχούς βελτίωσης, ο οργανισμός είναι σε θέση να διασφαλίσει ότι το ISMS προσαρμόζεται στις αλλαγές (τόσο στο περιβάλλον όσο και εντός του οργανισμού) ώστε να εντοπίζει συνεχώς και να μειώνει τους κινδύνους.

Αυτή η προσέγγιση βοηθά τους οργανισμούς να ανταποκριθούν στις νέες νομικές υποχρεώσεις του GDPR ενώ ταυτόχρονα εξορθολογεί τις διαδικασίες ασφάλειας στον κυβερνοχώρο, αυξάνοντας την αποδοτικότητα των επιχειρήσεων και μειώνοντας την απειλή μιας επίθεσης σε αυτόν.

Σύμφωνα με τον κανονισμό υπάρχουν πολλές αναφορές σε συστήματα πιστοποίησης όπου το GDPR ενθαρρύνει τη χρήση αυτών όπως το ISO 27001. Δίνοντας την δυνατότητα στον οργανισμό να επιδείξει ότι διαχειρίζεται ενεργά την ασφάλεια των δεδομένων του σύμφωνα με τις διεθνείς βέλτιστες πρακτικές.

Με βάση όλα τα παραπάνω προκύπτει ότι το GDPR και το ISO 27001 είναι δύο σημαντικά πρότυπα συμμόρφωσης που έχουν πολλά κοινά σημεία μεταξύ τους ,αν και προέρχονται από διαφορετικές αντιλήψεις. Το ISO 27001 και το GDPR έχουν στο επίκεντρο τους την μείωση του κινδύνου για τους ανθρώπους και τους οργανισμούς που προκαλείται από την κακή χρήση των προσωπικών δεδομένων. Και τα δύο έχουν ως στόχο την ενίσχυση της ασφάλειας των δεδομένων και την άμβλυνση του κινδύνου παραβίασης αυτών. Επίσης απαιτούν από τους οργανισμούς να διασφαλίζουν την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα (CIA) των ευαίσθητων δεδομένων.

Αρχικά, το ISO 27001 επικεντρώνεται στη μείωση των κινδύνων για την ασφάλεια των πληροφοριών, αναγκάζοντας τους οργανισμούς να παράγουν συστήματα διαχείρισης της ασφάλειας των πληροφοριών που διατηρούνται και βελτιώνονται συνεχώς. Από την άλλη πλευρά, το GPDR επικεντρώνεται στη μείωση των κινδύνων για τα πρόσωπα στα οποία αναφέρονται τα δεδομένα, παρέχοντας σε αυτούς δικαιώματα, θέτοντας σαφείς ευθύνες για την προστασία προσωπικών δεδομένων σε οργανισμούς που επεξεργάζονται προσωπικά

δεδομένα και τους κρατά υπόλογους μέσω νομικών και διοικητικών μηχανισμών επιβολής.

Τόσο το GDPR όσο και το ISO 27001 καλούν τους οργανισμούς να επενδύσουν σε ηγεσίες που έχουν την απαιτούμενη μόρφωση και την ανάπτυξη της ευαισθητοποίησης εντός του οργανισμού για την προστασία και την ασφάλεια των δεδομένων. Το ISO 27001 απαιτεί από τους οργανισμούς να υιοθετούν μια ολιστική προσέγγιση στην ασφάλεια των δεδομένων, αναπτύσσοντας σαφείς και περιεκτικές πολιτικές και διαδικασίες, βασισμένες σε οργανωτικό πεδίο (συμπεριλαμβανομένης της φύσης και της ποσότητας των επεξεργασμένων δεδομένων) που πρέπει να διατηρούνται μέσω ανασκοπήσεων και ελέγχων. Μία από τις θεμελιώδεις απαιτήσεις του ISO 27001 είναι ο καθορισμός ηγεσίας με προβλεπόμενες ευθύνες για τη διαχείριση της ασφάλειας των πληροφοριών. Ομοίως, το GPDR απαιτεί από πολλούς οργανισμούς να διορίζουν αξιωματούχους προστασίας δεδομένων με εξειδικευμένες γνώσεις του κανονισμού και επαρκή εξουσία εντός του οργανισμού, προκειμένου να υποστηρίζουν τα δικαιώματα των υποκειμένων των δεδομένων, καθώς και να εφαρμόζουν και να εποπτεύουν ολοκληρωμένες πολιτικές απορρήτου και ασφάλειας.

3 ΑΞΟΝΕΣ GDPR-ISO 27000

3.1 Γενικές Διατάξεις

Ο κανονισμός του GDPR ξεκινάει με τον ορισμό κάποιων γενικών διατάξεων οι οποίες σκοπό έχουν να αποσαφηνίσουν κάποιους βασικούς τομείς στους οποίους θα αναπτυχθεί στην συνέχεια σχετικά με την προστασία έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα.

Ο κανονισμός του GDPR στο άρθρο 1 αφορά την προστασία και την ελεύθερη κυκλοφορία των "δεδομένων προσωπικού χαρακτήρα"[2] για τα άτομα που βρίσκονται στην Ευρωπαϊκή Ένωση, είτε πρόκειται για επεξεργασία αυτών των δεδομένων στην ΕΕ είτε αλλού (που αναφέρεται και στο άρθρο 3). Κάθε οργανισμός που αλληλοεπιδρά με τους ανθρώπους στην Ευρωπαϊκή Ένωση μπορεί να εμπίπτει στον GDPR, ιδιαίτερα βέβαια αν συλλέγει προσωπικές πληροφορίες. Ένα αναγνωρίσιμο φυσικό πρόσωπο είναι αυτό που μπορεί να ταυτοποιηθεί, άμεσα ή έμμεσα, ιδίως με αναφορά σε κάποιο στοιχείο αναγνώρισης, όπως όνομα, αναγνωριστικό αριθμό, δεδομένα θέσης, διαδικτυακό αναγνωριστικό ή σε έναν ή περισσότερους παράγοντες που αφορούν συγκεκριμένα τη σωματική, γενετική, πνευματική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του φυσικού αυτού προσώπου. Τα πρότυπα ISO 27000 αφορούν τους κινδύνους πληροφόρησης, ιδίως τη διαχείριση των ελέγχων ασφάλειας πληροφοριών που μετριάζουν τους κινδύνους για τις πληροφορίες των οργανισμών. Επιπροσθέτως η εφαρμογή του τυγχάνει παγκόσμιας εμβέλειας. Στο πλαίσιο του GDPR, η ιδιωτικότητα είναι σε μεγάλο βαθμό θέμα διασφάλισης των προσωπικών πληροφοριών των ανθρώπων, ιδιαίτερα ευαίσθητων δεδομένων του υπολογιστή. Τα πρότυπα ISO27000 αναφέρουν συγκεκριμένα τις υποχρεώσεις συμμόρφωσης που σχετίζονται με την ιδιωτικότητα και την προστασία των προσωπικών πληροφοριών (πιο επισήμως γνωστές ως προσωπικά αναγνωρίσιμες πληροφορίες σε ορισμένες χώρες) και μπορούν να ικανοποιήσουν αυτήν την ανάγκη που διαμορφώνεται ακολουθώντας τις οδηγίες που βρίσκονται στο παράρτημα του προτύπου (A 18.1.4).

[2]που ορίζονται στο **άρθρο 4** ως "οποιαδήποτε πληροφορία σχετικά με ταυτοποιήσιμο ή αναγνωρίσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»).

Ο GDPR αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα εν όλων ή εν μέρει με αυτοματοποιημένα μέσα,(ουσιαστικά, συστήματα πληροφορικής, εφαρμογές και δίκτυα) και σε ένα επιχειρηματικό ή εταιρικό/οργανωτικό περιβάλλον (οι ιδιωτικές οικιακές χρήσεις δεν βρίσκονται στο πεδίο εφαρμογής).

Ο ISO 27000 αφορά πληροφορίες γενικά και όχι μόνο δεδομένα υπολογιστή, συστήματα, εφαρμογές και δίκτυα. Πρόκειται για ένα ευρύ πλαίσιο, που βασίζεται σε ένα «σύστημα διαχείρισης». Αντιμετωπίζει τους κινδύνους και τους ελέγχους των πληροφοριών σε όλο το σύνολο του οργανισμού, συμπεριλαμβανομένων πέραν των πτυχών της ιδιωτικής ζωής και της συμμόρφωσης. Λόγω αυτού του εύρους που καταλαμβάνει μπορεί εύκολα να καλύψει τις απαιτήσεις του Άρθρου 2 που μας ορίζει το ουσιαστικό πεδίο εφαρμογής του κανονισμού.

Στο τελευταίο κομμάτι αυτού του κεφαλαίου του κανονισμού ορίζονται οι ορισμοί που αφορούν το GDPR. Κάθε οργανισμός ορίζει τους δικούς του ορισμούς όπως και τα πρότυπα έχουν και αυτά τους δικούς τους. Έτσι και το ISO/IEC 27000 ορίζει τους δικούς του ορισμούς που θα πρέπει να αναλύονται ώστε να μην έρχονται σε σύγκρουση με αυτών του GDPR.

GDPR	ISO 27001
1-4	**Παράγραφος:** 3 **Παράρτημα:** A. 18.1.4

Πίνακας 1

3.2 Αρχές

Ιδιαίτερης σημασίας θεωρείται το άρθρο 5 του Κανονισμού. Τα δεδομένα προσωπικού χαρακτήρα πρέπει: α) να επεξεργάζονται νόμιμα, δίκαια και με διαφάνεια, β) να συλλέγονται αποκλειστικά για καθορισμένους, σαφείς και νόμιμους σκοπούς, γ) να είναι επαρκή, συναφή και περιορισμένα, δ) να είναι ακριβή, ε) να μην διατηρούνται περισσότερο από όσο χρειάζεται και στ) να επεξεργάζονται με ασφάλεια, για την εξασφάλιση της ακεραιότητας και της εμπιστευτικότητας.

Ένα μεγάλο μέρος του προτύπου (ISO 27000) έχει αναπτυχθεί, ώστε να καλυφθούν οι παραπάνω ανάγκες. Για το λόγο αυτό οι επιχειρηματικές

διαδικασίες και οι εφαρμογές, τα συστήματα και τα δίκτυα, πρέπει αφενός να εξασφαλίζουν επαρκώς τις προσωπικές πληροφορίες, απαιτώντας μια ολοκληρωμένη επιλογή τεχνολογικών, διαδικαστικών, φυσικών και άλλων ελέγχων και αφετέρου να υπάρχει μία αξιολόγηση των σχετικών κινδύνων των πληροφοριών. Για να ικανοποιηθούν αυτές οι απαιτήσεις, οι οργανισμοί πρέπει να γνωρίζουν που βρίσκονται τα προσωπικά στοιχεία, να τα ταξινομούν και να εφαρμόζουν τα κατάλληλα μέτρα για την αντιμετώπιση των στοιχείων που αναφέρθηκαν παραπάνω.

Επίσης, σύμφωνα με τον νέο κανονισμό, ο "ελεγκτής" είναι υπόλογος για όλες τις ενέργειες που αναφέρθηκαν, ενώ πρέπει να είναι σε θέση να αποδείξει, καθώς σε αυτόν ανατίθεται η συγκεκριμένη αρμοδιότητα της συμμόρφωσης με τις ενέργειες και τις ανάγκες που θέτει ο Κανονισμός. Παρά το γεγονός ότι δεν αναφέρεται με ξεκάθαρο τρόπο, η έννοια της λογοδοσίας καταλαμβάνει περίοπτη θέση στο τμήμα «ηγεσία» του ISO/IEC 27001.

Εφάμιλλης σημασίας θεωρείται το άρθρο 6, που ορίζει ότι για τη νόμιμη επεξεργασία των δεδομένων[3] πρέπει: α) να συναινεί το υποκείμενο για τον εκάστοτε σκοπό, β) να προβλέπεται από τη σύμβαση, γ) να είναι απαραίτητη για λόγους συμμόρφωσης, δ) να είναι αναγκαία για την προστασία των ζωτικών συμφερόντων του ιδιώτη, ε) να επιβάλλεται λόγω δημοσίου συμφέροντος ή κατόπιν απαίτησης από επίσημη αρχή και στ) να μετριάζεται, εάν το υποκείμενο είναι ανήλικος. Σε όλα τα παραπάνω δίνεται η δυνατότητα στα κράτη μέλη της ΕΕ να μπορούν να επιβάλλουν πρόσθετους κανόνες.

Επιπλέον, η επεξεργασία των δεδομένων θα πρέπει να καλύπτεται από την αξιολόγηση και την αντιμετώπιση των κινδύνων πληροφόρησης. Θα πρέπει να τονιστεί ότι η επεξεργασία δεδομένων επηρεάζει το σχεδιασμό των επιχειρηματικών διεργασιών και δραστηριοτήτων, των εφαρμογών, των συστημάτων (λ.χ. μπορεί να είναι απαραίτητο να προσδιοριστεί η ηλικία κάποιου πριν προχωρήσει η επιχείρηση στη συλλογή και στη χρήση των προσωπικών του πληροφοριών).

Επομένως, αυτές χαρακτηρίζονται ως επιχειρηματικές απαιτήσεις, απαραίτητες για τον περιορισμό και την προστασία των προσωπικών πληροφοριών. Στην πραγματικότητα απαιτούνται αρκετοί έλεγχοι ασφαλείας, ώστε να μετριαστούν οι

[3]Υπάρχουν αρκετές λεπτομερείς και ρητές απαιτήσεις σχετικά με τη νόμιμη επεξεργασία-βλέπε GDPR!

κίνδυνοι αναφορικά με τις προσωπικές πληροφορίες, εξαιτίας της φύσης του προβλήματος.

Μια ακόμα σημαντική παράμετρος διατυπώνεται στο άρθρο 7 του κανονισμού και αφορά στη συγκατάθεση του υποκειμένου των δεδομένων, το οποίο πρέπει να ενημερώνεται. Η συγκατάθεση πρέπει να παρέχεται ελεύθερα, ενώ το υποκείμενο θα πρέπει να έχει τη δυνατότητα να μπορεί να την αποσύρει εύκολα και οποιαδήποτε στιγμή θελήσει. Παρατηρούνται ωστόσο, ειδικοί περιορισμοί α) στη συγκατάθεση από τα παιδιά (GDPR 8) και β) στα ιδιαίτερα ευαίσθητα δεδομένα σχετικά με τη φυλή, τις πολιτικές γνώμες, τη θρησκεία, τη σεξουαλικότητα, τις γενετικές πληροφορίες , βιομετρικά στοιχεία κλπ. Η επεξεργασία των πληροφοριών αυτών απαγορεύεται από προεπιλογή, εκτός εάν δοθεί συγκατάθεση ή εάν η επεξεργασία είναι απαραίτητη (όπως ορίζεται στο άρθρο). Ειδικοί περιορισμοί ισχύουν επίσης για τα δεδομένα προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα.

Με την ίδια λογική και στα πρότυπα του ISO 27001 υπάρχει η απαίτηση να ζητείται η συγκατάθεση, κατόπιν ενημέρωσης, για την επεξεργασία των δεδομένων, ενώ είναι απαραίτητο ο κάτοχος αυτών να είναι σε θέση να αποδείξει ότι έχει στην κατοχή του την συγκατάθεση. Με την ίδια λογική έχει προνοηθεί και αναφέρεται στους ειδικούς περιορισμούς (Άρθρο 7 ISO 27001) που ισχύουν για τα παιδιά, όπως η λήψη συγκατάθεσης από τον γονέα.

Όπως προαναφέρθηκε, είναι σημαντικό να προσδιοριστεί σε ποιες περιπτώσεις μπορούν να υποβληθούν σε επεξεργασία τα ευαίσθητα δεδομένα, πότε αυτό είναι «απαραίτητο» στην πραγματικότητα και πότε πρέπει να ληφθεί ρητή συναίνεση (παράγοντες που πρέπει να εξεταστούν στο σχεδιασμό συστημάτων, εφαρμογών και επιχειρηματικών διαδικασιών). Οποιαδήποτε χρήση αυτών των πληροφοριών θα πρέπει να προσδιορίζεται και να υποβάλλεται σε επεξεργασία μόνο υπό συγκεκριμένες συνθήκες. Οι πληροφορίες αυτές θα πρέπει κατά προτίμηση να μην διατηρούνται (με εξαίρεση τις επίσημες αρχές, καθώς ενδέχεται να χρειαστούν για ελέγχους ιστορικού, αναγνώριση κινδύνου για πίστωση/απάτη κ.λπ.). Οι διαδικασίες πρέπει να έχουν τεθεί σε εφαρμογή, ενώ τα αρχεία που αποδεικνύουν τη συγκατάθεση, πρέπει να προστατεύονται και να διατηρούνται. Η ανάκληση της συγκατάθεσης συνεπάγεται τη δυνατότητα εντοπισμού των προσωπικών πληροφοριών και την κατάργηση αυτών, ίσως κατά τη διάρκεια της επεξεργασίας τους και ίσως και από αντίγραφα ασφαλείας και

αρχεία, καθώς και από επιχειρηματικές διαδικασίες για τον έλεγχο και τον χειρισμό των αιτημάτων.

Πέρα από όλα αυτά, στον κανονισμό και στα πρότυπα διατυπώνεται ότι ορισμένοι περιορισμοί δεν ισχύουν, εάν ένα άτομο δεν μπορεί να αναγνωριστεί από τα δεδομένα που διατηρούνται. Ακολουθώντας την παραπάνω διαδικασία (με το να μην γνωρίζει ο οργανισμός ποιοι είναι τα υποκείμενα) είναι μια καλή επιλογή που μπορεί να τις προστατεύσει από κινδύνους που μπορούν να εμφανιστούν σε περιπτώσεις απώλειας δεδομένων. Για να εφαρμοστεί το μέτρο αυτό θα πρέπει ο οργανισμός να είναι σε θέση να απαντήσει αν χρειάζεται πραγματικά να γνωρίζει την ταυτότητα του ατόμου ή απλά την καλύπτει να συγκεντρώνει πληροφορίες και στατιστικά τα οποία δεν προσωποποιούνται.

GDPR	ISO 27001
5-11	**Παράγραφος:** 5, 6.1.2, 7 **Παράρτημα:** Για να καλυφθεί πλήρως θα πρέπει να υλοποιηθεί το μεγαλύτερο μέρος του παραρτήματος

Πίνακας 2

3.3 Δικαιώματά του υποκειμένου των δεδομένων

3.3.1 Διαφάνεια και ρυθμίσεις - Ενημέρωση και πρόσβαση σε δεδομένα προσωπικού χαρακτήρα

Οι επικοινωνίες με τα υποκείμενα των δεδομένων πρέπει να είναι διαφανείς, ξεκάθαρες και εύκολα κατανοητές. Για τον λόγο αυτό όταν συλλέγονται προσωπικά δεδομένα, πρέπει να δίνονται (ή να διαθέτουν ήδη) συγκεκριμένα στοιχεία πληροφοριών, όπως λεπτομέρειες του "υπευθύνου επεξεργασίας" και του "υπεύθυνου προστασίας δεδομένων", εάν οι πληροφορίες τους θα εξάγονται (ιδίως εκτός ΕΕ), πόσο καιρό θα τηρούνται, τα δικαιώματά τους και ο τρόπος με τον οποίο τους δίνετε η δυνατότητα να ρωτήσουν ή να παραπονεθούν.

Παρόμοιες απαιτήσεις γνωστοποίησης στο άρθρο 13 εφαρμόζονται εάν τα προσωπικά στοιχεία λαμβάνονται έμμεσα (π.χ. μια εμπορική λίστα αλληλογραφίας;). Οι άνθρωποι πρέπει να ενημερώνονται εντός ενός μηνός. Τα υποκείμενα έχουν το δικαίωμα να μάθουν αν ο οργανισμός διατηρεί τις

προσωπικές τους πληροφορίες, τι χρησιμοποιείται από αυτές, σε ποιον μπορεί να γνωστοποιηθούν κ.α. Επίσης πρέπει να ενημερωθούν ότι έχουν το δικαίωμα να τις διορθώσουν αλλά και να τις διαγράψουν.

Όλα τα παραπάνω σε μεγάλο βαθμό εμπίπτουν σε κατηγορίες που χρήζουν υλοποίησης για να λάβει ένας οργανισμός την πιστοποίηση του ISO 27001. Αρχικά πρέπει να δημιουργηθούν σωστά διατυπωμένες φόρμες στην ιστοσελίδα του κάθε οργανισμού και ειδοποιήσεων όπως επίσης και να καθιστούν σαφής οι διαδικασίες. Χρειάζεται επίσης να υπάρχουν οι διαδικασίες με τη διαχείριση περιστατικών δηλαδή μηχανισμών που επιτρέπουν στους ανθρώπους να ερωτούν ή να παραπονεθούν σε σχέση με τις προσωπικές τους πληροφορίες (που συνεπάγονται ένα μέσο για την ταυτοποίηση και την εξακρίβωση της ταυτότητάς τους), για την έγκαιρη ανταπόκρισή τους και για τη διατήρηση αρχείων αυτών των επικοινωνιών (π.χ. για τον περιορισμό ή τη φόρτιση για υπερβολικές αιτήσεις)

Επιπροσθέτως πρέπει να καθοριστούν και να υλοποιηθούν οι διαδικασίες για την παροχή δίκαιων πληροφοριών επεξεργασίας, πληροφοριών σχετικά με τον υπεύθυνο επεξεργασίας δεδομένων και τους σκοπούς επεξεργασίας των δεδομένων. Αυτό βασίζεται εν μέρει στον εντοπισμό των προσωπικών πληροφοριών που χρησιμοποιούνται. Επίσης η εταιρεία θα πρέπει να έχει την δυνατότητα να παρέχει ένα αντίγραφο των προσωπικών τους πληροφοριών αφού είναι δικαίωμα των υποκειμένων να το ζητήσουν και στην συνέχεια ο οργανισμός να τους το παραδώσει.

Τα δικαιώματα των υποκείμενων περιλαμβάνουν τη δυνατότητα απόκτησης αντιγράφου των δικών τους πληροφοριών (υπονοώντας ξανά την ανάγκη αναγνώρισης και εξακρίβωσης της γνησιότητας πριν από την υποβολή της αίτησης), αποκαλύπτοντας τη φύση της επεξεργασίας και τις συνέπειες αυτής αλλά και πληροφορίες σχετικά με τα στοιχεία ελέγχου, εάν εξάγονται τα δεδομένα τους. Μπορεί επίσης να επηρεάσει αντίγραφα ασφαλείας και αρχειοθέτησης αντιγράφων.

GDPR	ISO 27001
12-15	**Παράγραφος:** - **Παράρτημα:**A 8.1.1, A 8.2.1, A. 8.2.3, A. 12.1.1, A. 13.2.1, A. 14.1, A. 14.1.1, A. 16

Πίνακας 3

3.3.2 Διόρθωση και διαγραφή

Σε αυτό το σημείο ο κανονισμός αναλύει τα δικαιώματα που έχει ο καθένας για τα δεδομένα του σε περίπτωση που κάποια ή και όλα από αυτά χρήζουν διόρθωσης ή και διαγραφής.

Πιο αναλυτικά δίνεται τα δικαίωμα στο υποκείμενο να αιτείται να διορθώνονται, να συμπληρώνονται, να αποσαφηνίζονται τα προσωπικά τους στοιχεία. Ένα ακόμα σημαντικό στοιχείο που υπάρχει στον νέο κανονισμό είναι το δικαίωμα στην λήθη που ορίζεται ως το δικαίωμα του υποκειμένου των δεδομένων να ζητήσει από τον υπεύθυνο επεξεργασίας τη διαγραφή δεδομένων προσωπικού χαρακτήρα που το αφορούν εφόσον συντρέχουν κάποιες προϋποθέσεις η οποίες ορίζονται στο άρθρο 17 του κανονισμού. Επίσης δίνεται η δυνατότητα να ζητείται ο περιορισμός της επεξεργασίας των προσωπικών τους πληροφοριών αλλά και να γνωρίζουν το αποτέλεσμα των αιτημάτων τους για να διορθωθούν, να ολοκληρωθούν, να διαγραφούν και να περιοριστούν τα προσωπικά τους στοιχεία. Τέλος πολύ σημαντικό κομμάτι είναι ότι μπορεί το υποκείμενο να λάβει ένα χρησιμοποιούμενο «φορητό» ηλεκτρονικό αντίγραφο των προσωπικών τους δεδομένων το οποίο να διαβιβάζει τα εν λόγω δεδομένα σε άλλον υπεύθυνο επεξεργασίας χωρίς αντίρρηση από τον υπεύθυνο επεξεργασίας στον οποίο παρασχέθηκαν τα δεδομένα προσωπικού χαρακτήρα

Για την εφαρμογή όλων αυτών που ορίζονται στο συγκεκριμένο τμήμα (3ο) του κανονισμού μπορούν να ακολουθηθούν κάποιες ενέργειες μέσα από το πρότυπο (ISO 27001) που μπορούν να φέρουν τον συλλέκτη των πληροφοριών σε ένα ικανοποιητικό επίπεδο απέναντι στον κανονισμό. Για τον λόγο αυτών χρειάζονται λειτουργικές απαιτήσεις για τον έλεγχο, την επεξεργασία και την επέκταση αποθηκευμένων πληροφοριών, με διάφορους ελέγχους σχετικά με την ταυτοποίηση, την πιστοποίηση, την πρόσβαση και την επικύρωση. Μπορεί επίσης να επηρεάσει αντίγραφα ασφαλείας και αρχειοθέτηση αντιγράφων. Το πρότυπο μπορεί να μην εμπεριέχει τον όρο του δικαιώματος στην λήθη αλλά πρόκειται για μια μορφή ανάκλησης της συγκατάθεσης. Υπονοεί ότι το σύστημα πρέπει να επεξεργάζεται λειτουργικές απαιτήσεις για να είναι σε θέση να διαγράψει συγκεκριμένες αποθηκευμένες

πληροφορίες, με διάφορους ελέγχους σχετικά με την ταυτοποίηση, την πιστοποίηση, την πρόσβαση και την επικύρωση. Μπορεί επίσης να εμφανίζεται η ανάγκη να προσδιορίσουν τα συγκεκριμένα δεδομένα που πρόκειται να περιοριστούν και να εφαρμόσουν νέους κανόνες χειρισμού/ επεξεργασίας. Μπορεί επίσης να επηρεάσει αντίγραφα ασφαλείας και αρχειοθέτηση αντιγράφων. Γίνεται επίσης αναφορά στην ενημέρωση του μεταβιβάζοντος που είναι ένα συμβατικό μέρος της διαδικασίας διαχείρισης συμβάντων, αλλά μπορεί να υπάρχει μια χωριστή ή παράλληλη διαδικασία ειδικά για καταγγελίες προστασίας της ιδιωτικής ζωής και αιτήματα δεδομένου ότι οι δημιουργοί εδώ δεν είναι συνήθως υπάλληλοι/κάτοχοι. Τέλος τα εξαγόμενα δεδομένα πρέπει να περιορίζονται στο ταυτοποιημένο και επικυρωμένο πρόσωπο και πρέπει να κοινοποιούνται με ασφάλεια όπως να είναι και κρυπτογραφημένα. Μπορεί επίσης να συνεπάγεται με τη διαγραφή ή τον περιορισμό των δεδομένων και την επιβεβαίωση της παρούσας (άρθρα 17, 18 και 19). Όπως γίνεται αντιληπτό, σημαντικό σε αυτό το τελευταίο σκέλος είναι η ταυτοποίηση του υποκειμένου για να αποφευχθούν τυχόν ενέργειες από επιτήδειους που σκοπό έχουν να βλάψουν τον οργανισμό.

GDPR	ISO 27001
16-20	**Παράγραφος:** 6.1.2 **Παράρτημα:**A 8.2.1,A. 8.3 A. 9, A 8.2.1, A. 8.2.3,A. 10, A. 12.1.1, A. 13.2.1, A. 14.1, A. 14.1.1, A. 16, A. 18.1.1

Πίνακας 4

3.3.3 Δικαίωμα εναντίωσης - Αυτοματοποιημένη ατομική λήψη αποφάσεων και περιορισμοί

Οι άνθρωποι έχουν το δικαίωμα να αντιταχθούν στις πληροφορίες που χρησιμοποιούνται για σκοπούς κατάρτισης προφίλ και μάρκετινγκ, όπως επίσης και στις αποφάσεις που προκύπτουν από την αυτόματη επεξεργασία των προσωπικών τους πληροφοριών. Έτσι προκύπτει η ανάγκη να χρειάζονται τρόποι για να προσδιορίσουν τα συγκεκριμένα δεδομένα που δεν πρέπει να υποβληθούν σε επεξεργασία ή να εφαρμοστούν νέοι κανόνες χειρισμού και επεξεργασίας που οι παραπάνω τρόποι αναφέρονται στο πρότυπο του ISO 27000. Αναφορά γίνεται στην κατάρτιση προφίλ και τα συστήματα

υποστήριξης αποφάσεων που περιλαμβάνουν προσωπικές πληροφορίες και πρέπει να επιτρέπουν την μη αυτόματη αναθεώρηση αλλά και παρακάμψεις, με την κατάλληλη εξουσιοδότηση, πρόσβαση και έλεγχο ακεραιότητας

Σημαντικό κομμάτι είναι και το τελευταίο μέρος του κεφαλαίου 3 του κανονισμού το οποίο αναφέρεται στους περιορισμούς που μπορεί να υπάρξουν. Δίνεται η δυνατότητα στους εθνικούς νόμους να μπορούν να τροποποιήσουν ή να παρακάμψουν διάφορα δικαιώματα και περιορισμούς για την εθνική ασφάλεια και άλλους σκοπούς που μπορεί να παρουσιαστούν. Το πρότυπο αναφέρεται στον προσδιορισμό της εφαρμοστέας νομοθεσίας και συμβατικών απαιτήσεων που δύναται να προκύψουν (A 18.1.1). Όλες οι σχετικές νομοθετικές, κανονιστικές, συμβατικές απαιτήσεις και η προσέγγιση του οργανισμού για την εκπλήρωση αυτών των απαιτήσεων πρέπει να προσδιορίζονται ρητά, να τεκμηριώνονται και να ενημερώνονται για κάθε σύστημα πληροφοριών και τον οργανισμό. Αυτό βρίσκει εφαρμογή κυρίως σε δημόσιους φορείς και στα συστήματα τους ωστόσο μπορεί ορισμένες φορές να επηρεάσει και ιδιωτικούς ή εμπορικούς οργανισμούς.

GDPR	ISO 27001
21-23	**Παράγραφος:** 6.1.2 **Παράρτημα:**A. 12.1.1, A 12.3, A. 14.1.1, A. 16, A. 18.1.1

Πίνακας 5

3.4 Υπεύθυνος επεξεργασίας και εκτελών την επεξεργασία

Το συγκεκριμένο κεφάλαιο του κανονισμού αφορά τον Υπεύθυνο επεξεργασίας και τον εκτελών την επεξεργασία. Για κάθε οργανισμό αυτό αποτελεί ένα σημαντικό κομμάτι και θα πρέπει να συμμορφώνεται με τον κανονισμό.

3.4.1 Γενικές υποχρεώσεις

Ο "ελεγκτής" (γενικά ο οργανισμός που κατέχει και επωφελείται από την επεξεργασία προσωπικών πληροφοριών) είναι υπεύθυνος για την εφαρμογή των κατάλληλων ελέγχων προστασίας της ιδιωτικής ζωής

(συμπεριλαμβανομένων των πολιτικών και των κωδίκων δεοντολογίας) λαμβάνοντας υπόψη τους κινδύνους, τα δικαιώματα και άλλες απαιτήσεις εντός και ίσως πέραν του GDPR. Σημαντικό κριτήριο που πρέπει να λαμβάνει υπόψη του είναι οι κίνδυνοι, το κόστος και τα οφέλη, γι' αυτό θα πρέπει να υπάρχει επαρκής προστασία των προσωπικών πληροφοριών και αυτό να εφαρμόζεται από τον σχεδιασμό τους.

Σε περίπτωση που δύο ή περισσότεροι υπεύθυνοι επεξεργασίας καθορίζουν από κοινού τους σκοπούς και τα μέσα της επεξεργασίας, αποτελούν από κοινού υπευθύνους επεξεργασίας. Αυτοί θα πρέπει να καθορίζουν με διαφανή τρόπο τις αντίστοιχες ευθύνες τους για συμμόρφωση προς τις υποχρεώσεις που απορρέουν από τον παρόντα κανονισμό. Οι οργανισμοί εκτός Ευρώπης καλούνται επίσης να ορίσουν επισήμως εκπροσώπους υπευθύνων επεξεργασίας ή εκτελούντων την επεξεργασία εντός της Ευρώπης, σε περίπτωση που πληρούν ορισμένες προϋποθέσεις (π.χ. να προμηθεύουν αγαθά και υπηρεσίες σε Ευρωπαίους πολίτες). Ο ρόλος των «επεξεργαστών» είναι να επεξεργάζονται προσωπικές πληροφορίες σύμφωνα με τις οδηγίες του υπευθύνου επεξεργασίας και της ισχύουσας νομοθεσίας και να μην παρεκκλίνουν σε κανέναν βαθμό πέρα από αυτής. Προσοχή θα πρέπει να δίνεται και στο ιστορικό των αρχείων που θα πρέπει να υπάρχουν. Οι ελεγκτές πρέπει να διατηρούν αρχεία των δραστηριοτήτων επεξεργασίας για τις οποίες είναι υπεύθυνοι π.χ. τους σκοπούς για τους οποίους συγκεντρώνονται και επεξεργάζονται προσωπικές πληροφορίες, «κατηγορίες» υποκειμένων των δεδομένων και προσωπικά δεδομένα κ.α. Εάν ένας οργανισμός χρησιμοποιεί ένα ή περισσότερα τρίτα μέρη για να επεξεργαστεί προσωπικές πληροφορίες («μεταποιητές»), πρέπει να διασφαλίσει ότι και αυτοί συμμορφώνονται με τον GDPR. Ο υπεύθυνος επεξεργασίας του οργανισμού θα πρέπει να συνεργάζεται με την εποπτική αρχή (π.χ. τους διαμεσολαβητές) για την προστασία της ιδιωτικής ζωής ή της προστασίας δεδομένων. Επισημαίνεται ότι για να πραγματοποιηθεί η μεταξύ τους επικοινωνία πρέπει να ακολουθείται μια συγκεκριμένη διαδικασία η οποία είναι κατόπιν αιτήματος, με την εποπτική αρχή για την άσκηση των καθηκόντων της.

Πρόκειται για μια επίσημη υπενθύμιση ότι πρέπει να εφαρμοστεί ένα κατάλληλο, ολοκληρωμένο πλέγμα ελέγχων προστασίας της ιδιωτικής ζωής,

συμπεριλαμβανομένων πολιτικών και διαδικασιών, καθώς και τεχνικών, φυσικών και άλλων ελέγχων που αφορούν τους κινδύνους πληροφόρησης και τις υποχρεώσεις συμμόρφωσης. Η κλίμακα αυτή συνήθως απαιτεί μια δομημένη, συστηματική προσέγγιση της ιδιωτικής ζωής. Δεδομένων των επικαλύψεων, είναι συνήθως λογικό να ενσωματώνετε ή τουλάχιστον να ευθυγραμμίζετε και να συντονίζετε η ιδιωτικότητα με το πρότυπο ISO 27001 και άλλες πτυχές όπως η συμμόρφωση και η διαχείριση επιχειρηματικής συνέχειας συμπερασματικά πρόκειται για ένα ζήτημα διακυβέρνησης.

Υπάρχουν επιχειρηματικοί λόγοι για την κατάλληλη επένδυση στην ιδιωτικότητα, συμπεριλαμβανομένων των κινδύνων πληροφόρησης και των επιταγών συμμόρφωσης, καθώς και των επιλογών εφαρμογής με διάφορες δαπάνες και οφέλη: η εκπόνηση αυτών των στοιχείων αποτελεί έναν καλό τρόπο για την εξασφάλιση της διαχείρισης στήριξης και συμμετοχής, συν τη διάθεση της χρηματοδότησης και των πόρων που απαιτούνται για τον σχεδιασμό, την υλοποίηση, την εφαρμογή και τη διατήρηση των ρυθμίσεων προστασίας της ιδιωτικής ζωής. Η ιδιωτικότητα ανά σχεδιασμό και από προεπιλογή είναι παραδείγματα αρχών προστασίας της ιδιωτικής ζωής που στηρίζουν τις προδιαγραφές, το σχεδιασμό, την ανάπτυξη, τη λειτουργία και τη συντήρηση των συστημάτων και διεργασιών πληροφορικής που σχετίζονται με την προστασία της ιδιωτικής ζωής, συμπεριλαμβανομένων των σχέσεων και των συμβάσεων με τρίτα μέρη , π.χ. ISP και ΚΕΕ.

Οι οργανισμοί πρέπει να διαχειρίζονται τις σχέσεις με τους επιχειρηματικούς εταίρους, διασφαλίζοντας ότι η ιδιωτικότητα και άλλες πτυχές της ασφάλειας των πληροφοριών δεν πέφτουν μεταξύ των ρωγμών. Αυτό περιλαμβάνει, για παράδειγμα, από κοινού διερεύνηση και επίλυση περιστατικών προστασίας της ιδιωτικής ζωής, παραβιάσεων ή αιτημάτων πρόσβασης, την επίτευξη και τη διατήρηση ενός εξασφαλισμένο επιπέδου συμμόρφωσης του GDPR, και την τήρηση συναινούσα σκοπών για τους οποίους οι προσωπικές πληροφορίες ήταν αρχικά να συγκεντρωθούν, ανεξάρτητα από το πού καταλήγουν.

Για τους παρόχους υπηρεσιών Διαδικτύου και τις υπηρεσίες ISP, τα κέντρα δεδομένων που ανατίθενται σε τρίτους, καθώς και άλλες εμπορικές υπηρεσίες στις οποίες ο οργανισμός μεταβιβάζει προσωπικές πληροφορίες σε τρίτα μέρη και εμπεριέχονται σε αυτά πληροφορίες για πολίτες της ΕΕ.

Επίσης οι πάροχοι υπηρεσιών μπορούν να αναμένουν ότι θα υπάρχει αμφισβήτηση σχετικά με την κατάσταση συμμόρφωσης με το GDPR, λόγω όλων αυτό το πρότυπο προτείνει την δημιουργία πολιτικών απορρήτου, άλλων ελέγχων και να έχουν όρους συμμόρφωσης, διασφάλισης και υποχρεώσεων που περιλαμβάνονται σε συμβάσεις και συμφωνίες. Οι κίνδυνοι πληροφόρησης πρέπει να εντοπίζονται, να αξιολογούνται και να αντιμετωπίζονται με τον συνήθη τρόπο, και από τις δύο πλευρές.

Τέλος ο υπεύθυνος απορρήτου (ή υπεύθυνος προστασίας δεδομένων) θα πρέπει να είναι υπόλογος για να βεβαιωθεί ότι όλες οι διαδικασίες και οι ενέργειες που χρειάζονται γίνονται σωστά. Οι επεξεργαστές πρέπει να είναι σε θέση να συγκρατούν και να ελέγχουν τις προσωπικές πληροφορίες με τον ίδιο τρόπο όπως και οι ελεγκτές.

GDPR	ISO 27001
24-31	Εδώ αναφέρονται σχεδόν όλα τα μέρη του προτύπου που θα πρέπει να υλοποιηθούν για να καλυφθούν τα συγκεκριμένα κομμάτια του κανονισμού.

Πίνακας 6

3.4.2 Ασφάλεια δεδομένων προσωπικού χαρακτήρα

Ο κανονισμός του GDPR αναφέρεται στους οργανισμούς που πρέπει να υλοποιούν, να διαχειρίζονται και να διατηρούν μέσω κατάλληλων τεχνικών και οργανωτικών μέτρων ασφάλειας για τις προσωπικές πληροφορίες, καταφέρνοντας να αντιμετωπίσουν τους κινδύνους που μπορεί να παρουσιαστούν. Ένα μεγάλο μέρος του παραρτήματος του GDPR αναφέρει μερικά παραδείγματα χρησιμοποίησης κατάλληλων μέτρων απέναντι στους πιθανούς κινδύνους που μπορεί να παρουσιαστούν (όπως κρυπτογράφηση, ανωνυμοποίηση κ.α.) που καλύπτουν τα δεδομένα εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας, καθώς και μέτρα διασφάλισης και συμμόρφωσης των εργαζομένων (που συνεπάγονται με πολιτικές και ευαισθητοποίησης/κατάρτισης αλλά και συμμόρφωσης/ενίσχυσης). Το ISO 27000 παρέχει ένα συνεκτικό και ολοκληρωμένο πλαίσιο για τη διαχείριση της ιδιωτικής ζωής παράλληλα με άλλους ελέγχους των κινδύνων και της ασφάλειας της πληροφορίας.

Ωστόσο η χρησιμοποίηση των κατάλληλων μέτρων δεν μπορεί να μας διασφαλίσει στην σημερινή εποχή που ζούμε την απόλυτη βεβαιότητα ότι δεν θα μπορεί να υπάρξει κάποια παράβαση του απορρήτου των πληροφοριών. Στην συγκεκριμένη περίπτωση απαιτείται από τον κανονισμό να κοινοποιούνται στις αρχές αμέσως η διαρροή4 των πληροφοριών. Οι παραβιάσεις θα αντιμετωπίζονται κανονικά ως συμβάντα εντός της διαδικασίας διαχείρισης περιστατικών, αλλά οι υποχρεώσεις που αφορούν τον GDPR (όπως η προθεσμία των 3 ημερών για την κοινοποίηση των αρχών) πρέπει να πληρούνται.

Επίσης πέρα από την κοινοποίηση στις αρχές των παραβάσεων όπως αναφέρθηκε και παραπάνω θα πρέπει οι παραβάσεις του ιδιωτικού απορρήτου που έχουν εκθέσει ή βλάψει προσωπικά στοιχεία και, ως εκ τούτου, είναι πιθανό να βλάψουν τα συμφέροντά των ανθρώπων των οποίων αφορούσαν πρέπει να κοινοποιούνται σε αυτούς που επηρεάζονται «χωρίς αδικαιολόγητη καθυστέρηση». Εκτός από τις νομικές και δεοντολογικές εκτιμήσεις και την κατεύθυνση από τις αρχές προστασίας προσωπικών δεδομένων, υπάρχουν προφανώς σημαντικά επιχειρηματικά ζητήματα σχετικά με το χρονοδιάγραμμα και τη φύση της γνωστοποίησης. Αυτό αποτελεί συνήθως μέρος της διαδικασίας διαχείρισης συμβάντων για σοβαρά ή σημαντικά περιστατικά, με τη συμμετοχή ανώτερων διευθυντικών στελεχών καθώς και ειδικών συμβούλων. Για την αποφυγή ακριβώς αυτής της κατάστασης, η ιδιωτικότητα αποτελεί μια εταιρική επιτακτική ανάγκη όπως και η επένδυση σε κατάλληλα προληπτικά μέτρα.

GDPR	ISO 27001
32-34	**Παράγραφος:**8.2,8.3 **Παράρτημα:**A. 16, A. 18.1.4

Πίνακας 7

3.4.3 Εκτίμηση αντίκτυπου σχετικά με την προστασία δεδομένων και προηγούμενη διαβούλευση

Οι κίνδυνοι προστασίας της ιδιωτικής ζωής, συμπεριλαμβανομένων των δυνητικών επιπτώσεων, πρέπει να αξιολογούνται, ιδίως όταν εξετάζονται νέες

[4]εντός 3 ημερών από την γνώση τους, εκτός εάν δικαιολογούνται καθυστερήσεις.

τεχνολογίες, συστήματα και ρυθμίσεις ή διαφορετικά όταν οι κίνδυνοι ενδέχεται να είναι σημαντικοί[5].

Επιπλέον οι κίνδυνοι απορρήτου που αξιολογούνται ως «υψηλοί κίνδυνοι» θα πρέπει να κοινοποιούνται στις αρχές, δίνοντάς την ευκαιρία στις αρχές να κρίνουν και αυτές ανάλογα.

Και πάλι, υπάρχουν υγιείς επιχειρηματικοί και δεοντολογικοί λόγοι για τον εντοπισμό, την αξιολόγηση και τη αντιμετώπιση των κινδύνων (συμπεριλαμβανομένων των κινδύνων ιδιωτικότητας και συμμόρφωσης), εκτός από τις υποχρεώσεις του GDPR. Οι κίνδυνοι που σχετίζονται με την προστασία της ιδιωτικής ζωής θα πρέπει πιθανώς να συμπεριληφθούν σε μητρώα επιχειρηματικών κινδύνων μαζί με διάφορους άλλους κινδύνους. Ο GDPR προβάλλει επίσης υποδείξεις για την ενσωμάτωση της αξιολόγησης των κινδύνων για την προστασία της ιδιωτικής ζωής στο πλαίσιο των συνήθων δραστηριοτήτων εκτίμησης κινδύνου για έργα αλλαγής επιχειρήσεων, νέες εξελίξεις συστημάτων πληροφορικής κ.α.

Η απαίτηση GDPR είναι καλή αλλά ασαφής: αυτό μπορεί να καλυφθεί σε εταιρικές πολιτικές που αφορούν τον ακριβή ορισμό των "υψηλών" κινδύνων προστασίας της ιδιωτικής ζωής ακολουθώντας οδηγίες οι οποίες δίνονται σε πρότυπα όπως το ISO 27000.

GDPR	ISO 27001
35-36	**Παράγραφος:**6.1.2 **Παράρτημα:**A. 6.1.3, A 8.2.1

Πίνακας 8

3.4.4 Υπεύθυνος προστασίας δεδομένων

Ο υπεύθυνος προστασίας δεδομένων πρέπει να ορίζεται επισήμως υπό συγκεκριμένες συνθήκες, π.χ. δημόσιοι φορείς, οργανισμοί που παρακολουθούν τακτικά και συστηματικά τους ανθρώπους σε μεγάλη κλίμακα ή εκείνοι που πραγματοποιούν μεγάλης κλίμακας επεξεργασία ευαίσθητων

[5]Σημαντικά επικίνδυνες καταστάσεις" πρέπει να καθοριστούν από τις εθνικές αρχές προστασίας της ιδιωτικής ζωής.

προσωπικές πληροφορίες σχετικά με τα ποινικά μητρώα. Σε περιπτώσεις που ο υπεύθυνος προστασίας δεδομένων έχει οριστεί επισήμως θα πρέπει να υποστηρίζεται από τον οργανισμό και να ασχολείται με όλα τα ζητήματα τα οποία σχετίζονται με την προστασία δεδομένων προσωπικού χαρακτήρα. Επίσης θα πρέπει να παρέχει συμβουλές σχετικά με θέματα όπως ενημέρωσης και συμβουλής οποιουδήποτε επεξεργάζεται πληροφορίες σχετικά με τις διατάξεις των προσωπικών δεδομένων, να παρακολουθεί τη συμμόρφωση, να επικοινωνεί με τις αρχές, να ενεργεί ως σημείο επαφής, να αντιμετωπίζει κινδύνους για το απόρρητο κ.α.

Εκτός από την υποχρέωση του GDPR, ο ρόλος του υπεύθυνος προστασίας είναι πολύ ευρύτερα εφαρμόσιμος και πολύτιμος. Αναφέρεται και στο πρότυπο του ISO 27001 όπου γίνεται και εκεί μια περιγραφή των καθηκόντων του αλλά και τις εκτιμήσεως που θα πρέπει να τον διακατέχει από τα υψηλόβαθμα στελέχη και την διοίκηση σε έναν οργανισμό. Σε περίπτωση που δεν χαίρει αυτής της εκτιμήσεως και ταυτόχρονα υπάρχει και εμπλοκή αυτών των προσώπων στα θέματα της προστασίας των δεδομένων τότε καθίσταται σαφές ότι ο ρόλος του είναι ανίσχυρος και ανούσιος. Υπάρχουν σαφώς πολλές οπτικές γωνίες ωστόσο ένα καθορισμένο εταιρικό σημείο εστίασης για την ιδιωτικότητα έχει νόημα για σχεδόν όλους τους οργανισμούς.

GDPR	ISO 27001
37-39	**Παράγραφος:**5.3 **Παράρτημα:**A. 6.1.1, A18.1.4

Πίνακας 9

3.4.5 Κώδικες δεοντολογίας και πιστοποίηση

Η Ευρωπαϊκή Επιτροπή ενθαρρύνει την εκπόνηση κωδίκων δεοντολογίας που έχουν ως στόχο να συμβάλουν στην ορθή εφαρμογή του GDPR. Διάφορες αρχές, ενώσεις και φορείς του κλάδου αναμένεται να καταρτίσουν κώδικες δεοντολογίας που να επεξεργάζονται τον GDPR και να προσφέρουν επίσημη έγκριση (με απροσδιόριστο μηχανισμό) και (όπου ενδείκνυται) να εφαρμόσουν τη δική τους συμμόρφωση (μέλος) μηχανισμών.

Για τον λόγο αυτό οι οργανισμοί που βρίσκονται πίσω από κώδικες δεοντολογίας υποχρεούνται να παρακολουθούν τη συμμόρφωση (από τα μέλη τους), ανεξάρτητα και με την επιφύλαξη της νομικής και κανονιστικής παρακολούθησης της συμμόρφωσης που διενεργούν οι εθνικές αρχές. Επίσης τα εθελοντικά συστήματα πιστοποίησης της προστασίας των δεδομένων που προσφέρουν σφραγίδες και σήματα συμμόρφωσης (ισχύουν για 3 έτη) πρέπει να αναπτυχθούν και να καταχωρούνται. Τέλος οι οργανισμοί πιστοποίησης που αναθέτουν σφραγίδες και σήματα συμμόρφωσης θα πρέπει να είναι αρμόδιοι και διαπιστευμένοι για το σκοπό αυτό. Η Ευρωπαϊκή Επιτροπή μπορεί να επιβάλει τεχνικά πρότυπα για τα συστήματα πιστοποίησης.

Η ηθική υποχρέωση είναι σαφής: η ιδιωτικότητα είναι κάτι περισσότερο από ένα θέμα αυστηρής τήρησης των επίσημων, νομικών υποχρεώσεων. Οι κώδικες δεοντολογίας και τα πρότυπα όπως το ISO 27001 μπορούν να προσφέρουν καθοδήγηση ορθής πρακτικής και συμμόρφωσης με τον κανονισμό.

GDPR	ISO 27001
40-43	**Παράγραφος:**5.3 **Παράρτημα:**A. 6.1.1, A18.1.4

Πίνακας 10

3.5 Μεταφορές δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες ή διεθνείς οργανισμούς

Ο κανονισμός ξεκινάει καθιστώντας σαφές ότι οι διεθνείς διαβιβάσεις και η επεξεργασία προσωπικών πληροφοριών πρέπει να πληρούν τις απαιτήσεις που θα ορίζονται στα επόμενα άρθρα και θα αναφερθούν παρακάτω.

Οι διαβιβάσεις δεδομένων σε χώρες των οποίων οι ρυθμίσεις προστασίας της ιδιωτικής ζωής (νόμοι, κανονισμοί, επίσημοι μηχανισμοί συμμόρφωσης) κρίνονται επαρκείς από την Ευρωπαϊκή Επιτροπή (δηλαδή συμμόρφωση με τον GDPR) δεν απαιτούν επίσημη άδεια ή ειδικές πρόσθετες διασφαλίσεις. Σε αντίθεση σε χώρες στις οποίες δεν κρίνονται επαρκείς από την Ευρωπαϊκή Επιτροπή αλλά μπορούν να πληρούν ορισμένα άλλα κριτήρια απαιτούν πρόσθετες διασφαλίσεις. Για τον

λόγο αυτό ο οργανισμός πρέπει να εφαρμόσει και να διασφαλίσει την επάρκεια των ελέγχων προστασίας της ιδιωτικής ζωής πριν από τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τέτοιες χώρες. Επίσης οι περισσότερες διατυπώσεις πρέπει να διεκπεραιώνονται από την Επιτροπή. Η συμμόρφωση συνεπάγεται με την αποφυγή μεταβιβάσεων σε άλλες χώρες, την παρακολούθηση των επίσημων καταλόγων για αλλαγές και τη διασφάλιση της τήρησης των κατάλληλων συμβάσεων/συμφωνιών και άλλων ελέγχων προστασίας της ιδιωτικής ζωής, όπως και με άλλες διαβιβάσεις δεδομένων τρίτων μερών (άρθρο 28 ιδιαίτερα). Επιπλέον οι εθνικές αρχές μπορούν να εγκρίνουν νομικά δεσμευτικούς κανόνες προστασίας της ιδιωτικής ζωής που επιτρέπουν μεταφορές σε μη εγκεκριμένες χώρες. Οι διατυπώσεις μπορούν να επηρεάσουν συμβατικούς όρους, ρυθμίσεις συμμόρφωσης και υποχρεώσεις .

Σημαντική απαίτηση του κανονισμού είναι ότι οι απαιτήσεις για τους ευρωπαϊκούς οργανισμούς από αρχές εκτός Ευρώπης για την αποκάλυψη προσωπικών δεδομένων μπορεί να είναι άκυρες, εκτός εάν καλύπτονται από διεθνείς συμφωνίες ή συνθήκες. Αυτές οι καταστάσεις κανονικά θα αντιμετωπίζονται από νομικούς και κανονισμούς κανονιστικής συμμόρφωσης-αλλά μπορεί να ξεκινούν ως συμβάντα. Αντίθετα, ισχύουν περισσότεροι όροι για τη μεταφορά προσωπικών πληροφοριών σε μη εγκεκριμένες χώρες, π.χ. ρητή συγκατάθεση των υποκειμένων των δεδομένων. Η Επιτροπή το καθιστά σκόπιμα δύσκολο, ή μάλλον λαμβάνει μεγάλη μέριμνα, δεδομένου ότι οι κίνδυνοι για την ιδιωτικότητα είναι υψηλότεροι. Τέλος καθίσταται σαφές ότι οι διεθνείς αρχές θα συνεργαστούν για την προστασία της ιδιωτικής ζωής.

GDPR	ISO 27001
44-50	**Παράγραφος:**- **Παράρτημα:**A. 16, A18.1.4

Πίνακας 11

3.6 Ἐνδικα μέσα, ευθύνη και ποινές

Στα πρώτα κομμάτια του κεφαλαίου VIII του κανονισμού γίνεται αναφορά στους τρόπους που οι εποπτικές αρχές μπορούν να αντιμετωπίσουν παράπονα για την προστασία της ιδιωτικής ζωής και γίνεται αναφορά ότι όποιος υποστεί ζημιές από παραβάσεις του GDPR, έχει δικαίωμα αποζημίωσης από τον υπεύθυνο επεξεργασίας ή τον επεξεργαστή. Στην συνέχεια γίνεται προσδιορισμός των

διοικητικών προστίμων που επιβάλλονται από τις εποπτικές αρχές πρέπει να είναι «αποτελεσματικά, αναλογικά και αποτρεπτικά». Για τον λόγο αυτόν ορίζονται διάφορα κριτήρια, ανάλογα με τις παραβάσεις και τις περιστάσεις, τα πρόστιμα μπορούν να φθάσουν τα 20.000.000 ευρώ ή έως το 4% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών για το προηγούμενο έτος , εάν το πρόστιμο είναι μεγαλύτερο.

Τέτοια τεράστια πρόστιμα προορίζονται σαφώς να αποτελέσουν ισχυρό αποτρεπτικό παράγοντα, που αντιπροσωπεύει σημαντικό μέρος του δυνητικού αντίκτυπου των παραβιάσεων της ιδιωτικής ζωής στην αξιολόγηση από την οργάνωση της συμμόρφωσης με τον GDPR και άλλων κινδύνων προστασίας της ιδιωτικής ζωής. Μπορεί να επιβληθούν και άλλες κυρώσεις οι οποίες θα πρέπει να είναι και αυτές "αποτελεσματικές, αναλογικές και αποτρεπτικές".

Για να μπορεί ένας οργανισμός να καλυφθεί από τα παραπάνω πρόστιμα που το μέγεθός τους μπορεί να αποδειχθεί μοιραίο για την εύρυθμη λειτουργία του οργανισμού μέσω του προτύπου ISO 27001 μπορεί να θωρακίσει σε έναν πολύ μεγάλο βαθμό ακολουθώντας κάποια κομμάτια που αναφέρονται μέσα στο πρότυπο(π.χ. A.18.1.4).

GDPR	ISO 27001
77-84	**Παράγραφος:**6 **Παράρτημα:**A18.1.4

Πίνακας 12

3.7 Διατάξεις σχετικά με ειδικές καταστάσεις επεξεργασίας

Στο συγκεκριμένο κομμάτι του κανονισμού γίνεται σαφές εκ των προτέρων ότι μπορεί να παρουσιαστεί η ανάγκη η νομοθεσία να τέμνεται με τον κανονισμό GDPR.Εδώ και ανάλογα με την περίπτωση όπως θα δούμε παρακάτω μπορεί η νομοθεσία να υπερβαίνει του κανονισμού ή ακόμα να μπορεί να επικρατήσουν διφορούμενες απόψεις που θα οδηγήσουν σε πολυπλοκότητα της κατάστασης χωρίς να προκύπτει και η λύση στα συγκεκριμένα θέματα.

Αρχικά οι χώρες πρέπει να εξισορροπήσουν τα δικαιώματα απορρήτου/προστασίας δεδομένων έναντι της ελευθερίας της έκφρασης, της

δημοσιογραφίας, της ακαδημαϊκής έρευνας κλπ. μέσω κατάλληλων νόμων. Τα ζητήματα που προβλέπονται στο παρόν άρθρο ενδέχεται να αποτελέσουν αντικείμενο διαφορετικών νομικών ερμηνειών στο δικαστήριο, επομένως και πάλι υπάρχουν κίνδυνοι για την αναγνώριση, την αξιολόγηση και την επεξεργασία των πληροφοριών, όπου εμπλέκονται προσωπικές πληροφορίες. Τα δεδομένα προσωπικού χαρακτήρα σε επίσημα έγγραφα μπορούν να γνωστοποιούνται εάν τα έγγραφα υποχρεούνται επισήμως να γνωστοποιούνται στο πλαίσιο της νομοθεσίας περί «ελευθερίας πληροφορείται».

Επιπροσθέτως οι χώρες μπορούν να επιβάλλουν περαιτέρω ελέγχους προστασίας της ιδιωτικής ζωής για τους αριθμούς ταυτότητας. Οι αριθμοί ταυτότητας μπορούν να χρησιμοποιηθούν μυστικά για την απόδειξη της «γνησιότητας» ενός προσώπου, οπότε πρέπει να παραμείνουν εμπιστευτικοί για να μειώσουν τον κίνδυνο κάποιας κλοπής ταυτότητας. Στην πραγματικότητα είναι ευαίσθητες προσωπικές πληροφορίες, που υποδηλώνουν την ανάγκη για κρυπτογράφηση και άλλους ελέγχους ασφάλειας/απορρήτου.

Οι χώρες μπορούν να επιβάλλουν περαιτέρω περιορισμούς στην εταιρική επεξεργασία και τη χρήση προσωπικών πληροφοριών σχετικά με τους εργαζομένους, π.χ. για τη διαφύλαξη της ανθρώπινης αξιοπρέπειας και των θεμελιωδών δικαιωμάτων. Οι νόμοι για την απασχόληση μπορούν να τέμνονται με τον GDPR και την ιδιωτικότητα. Έτσι περιπλέκουν περαιτέρω τη συμμόρφωση και αλλάζοντας τους κινδύνους πληροφόρησης σε αυτόν τον τομέα.

Όταν τα δεδομένα προσωπικού χαρακτήρα πρέπει να αρχειοθετούνται π.χ. για ερευνητικούς και στατιστικούς σκοπούς, οι κίνδυνοι για την προστασία της ιδιωτικής ζωής θα πρέπει να αντιμετωπίζεται μέσω κατάλληλων ελέγχων, όπως η ψευδωνυμοποίηση και η ελαχιστοποίηση των δεδομένων, όπου είναι εφικτό. Οι ανησυχίες για την ιδιωτικότητα παραμένουν εφόσον τα υποκείμενα των δεδομένων είναι ζωντανά (ίσως περισσότερο αν οι οικογένειές τους ή οι κοινότητές τους ενδέχεται να επηρεαστούν από παραβάσεις). Λαμβανομένων υπόψη των ανωτέρω, οι κίνδυνοι πληροφόρησης θα πρέπει να εντοπίζονται, να αξιολογούνται και να αντιμετωπίζονται καταλλήλως κατά τον συνήθη τρόπο.

Τέλος οι χώρες μπορούν να θεσπίσουν πρόσθετους νόμους σχετικά με το απόρρητο και τις υποχρεώσεις απορρήτου των εργαζομένων. Η νομοθεσία για την

απασχόληση ή το απόρρητο μπορεί να τέμνει τον GDPR και την ιδιωτικότητα, δυσχεραίνοντας ακόμη περισσότερο τη συμμόρφωση και τροποποιώντας τους κινδύνους πληροφόρησης σε αυτόν τον τομέα.

GDPR	ISO 27001
85-91	**Παράγραφος:**6 **Παράρτημα:**A18.1.1, A18.1.4

Πίνακας 13

4. Ασφάλεια και Ιδιωτικότητα σε τεμνόμενα σημεία

Υπάρχει σημαντικός κοινός λόγος μεταξύ του GDPR και των απαιτήσεων ISO 27001. Αν και προέρχονται από διαφορετικές οπτικές γωνίες, το ISO 27001 και ο κανονισμός του GDPR ο πυρήνας τους είναι σε πολλά σημεία κοινός και αφορά την μείωση του κινδύνου για τους ανθρώπους και τις οργανώσεις που προκαλούνται από την κατάχρηση των προσωπικών δεδομένων. Από τη μία πλευρά, το πρότυπο ISO 27001 επικεντρώνεται στη μείωση των κινδύνων για την ασφάλεια των πληροφοριών από οργανισμούς για την παραγωγή συστημάτων διαχείρισης της ασφάλειας πληροφοριών που διατηρούνται και βελτιώνονται συνεχώς. Από την άλλη πλευρά, ο κανονισμός επικεντρώνεται στη μείωση των κινδύνων για τα υποκείμενα των δεδομένων, παρέχοντάς τους δικαιώματα και θέτοντας σαφείς ευθύνες σχετικά με την προστασία της ιδιωτικής ζωής στους οργανισμούς που επεξεργάζονται δεδομένα προσωπικού χαρακτήρα.

Τόσο ο κανονισμός GDPR όσο και το ISO 27001 καλούν τους οργανισμούς να αναπτύξουν την ευαισθητοποίηση τους για την προστασία των δεδομένων και την ασφάλεια αυτών. Το ISO 27001 απαιτεί από τους οργανισμούς να λαμβάνουν μια ολιστική προσέγγιση στην ασφάλεια των δεδομένων, αναπτύσσοντας σαφείς και ολοκληρωμένες πολιτικές και διαδικασίες που βασίζονται σε θέματα οργανογράμματος (συμπεριλαμβανομένης της φύσης και της ποσότητας των δεδομένων που υποβάλλονται σε επεξεργασία) που πρέπει να διατηρηθούν μέσω κριτικών και ελέγχων. Μία από τις θεμελιώδεις απαιτήσεις του ISO 27001 είναι ο ορισμός υπεύθυνου με καθορισμένες αρμοδιότητες για τη διαχείριση της ασφάλειας των πληροφοριών. Ομοίως, και το GDPR απαιτεί από πολλούς οργανισμούς να ορίσουν υπεύθυνο για την προστασία των δεδομένων με εξειδικευμένες γνώσεις του κανονισμού και επαρκή εξουσία εντός αυτού για να υποστηρίζει τα δικαιώματα του υποκειμένου των δεδομένων. Επίσης να έχει την δυνατότητα να εφαρμόζει και να επιβλέπει τις ολοκληρωμένες Πολιτικές απορρήτου και ασφάλειας.

Παρακάτω θα παρουσιαστεί ο τρόπος με τον οποίο το πλαίσιο διαχείρισης ασφάλειας πληροφοριών ISO 27001 συσχετίζεται με τους στόχους, ακόμη και τις ειδικές απαιτήσεις του GDPR.

Συγκεκριμένα, θα προσδιοριστούν έξι κρίσιμοι τομείς κοινών σημείων μεταξύ του ISO 27001 και του GPDR:

- Ασφάλειας
- Ειδοποίηση παραβίασης
- Διαχείριση προμηθευτών
- Λόγοι αρχειοθέτησης
- Ιδιωτικότητα ανά σχεδιασμό
- Δικαιώματα υποκειμένου των δεδομένων

Για κάθε θέμα, θα εντοπιστεί η επικάλυψη μεταξύ των δύο συστημάτων και θα αναφερθεί ο τρόπος με τον οποίο οι υπεύθυνοι ασφαλείας των δεδομένων μπορούν να εργαστούν πιο αποτελεσματικά με τους υπεύθυνους του απορρήτου για τη συμμόρφωση με τον κανονισμό του GDPR.

4.1 Ασφάλεια

ISO 27001

Το ISO 27001 δημιουργεί έναν οδηγό για την ανάπτυξη, την υλοποίηση και τη συντήρηση ενός ολοκληρωμένου προγράμματος ασφάλειας πληροφοριών. Ξεκινώντας από την παράγραφο 4, οι οδηγίες ISO 27001 απαιτούν οι οργανισμοί να καθορίσουν τόσο τα εσωτερικά όσο και τα εξωτερικά ζητήματα που ενδέχεται να επηρεάσουν τα προγράμματα ασφάλειας τους. Η διαπίστωση αυτή πρέπει να περιλαμβάνει την εξέταση πιθανών ζητημάτων που αφορούν τρίτα μέρη και θα πρέπει να προσδιοριστεί το πεδίο εφαρμογής και τους περιορισμούς του προγράμματος ασφαλείας.

Στη συνέχεια, η παράγραφος 6 απαιτεί από τους οργανισμούς να σχεδιάζουν και να δομούν ένα πρόγραμμα ασφάλειας που μπορεί να επιτύχει τους στόχους και να ταιριάζει με το πεδίο που προσδιορίζεται στην παράγραφο 4. Ζητάει επίσης τη δημιουργία μιας μεθοδολογίας εκτίμησης των κινδύνων για την ασφάλεια των πληροφοριών, η οποία θα περιλαμβάνει τον προσδιορισμό του επιπέδου του κινδύνου και την αποδοχή αυτών, την εκχώρηση ευθυνών, τα σχέδια για την αντιμετώπιση των εντοπισμένων κινδύνων για την ασφάλεια, και τον καθορισμό των στόχων ασφαλείας.

Τέλος, η παράγραφος 8 απαιτεί την εφαρμογή των διαδικασιών που δημιουργήθηκαν με τη παράγραφο 6 και θέτει πρότυπα για τη συνεχή συντήρηση του προγράμματος. Επικεντρώνεται σε μεγάλο βαθμό στην τεκμηρίωση της αξιολόγησης των κινδύνων, της επίλυση αυτών και των λειτουργιών του προγράμματος ασφαλείας γενικά, ώστε να αποδεικνύεται η συμμόρφωση με τους κανονισμούς. Τέλος ζητάει την περιοδική επανεξέταση, προκειμένου να διασφαλιστεί ότι θα σημειωθεί πρόοδος όσον αφορά τους στόχους ασφάλειας που προβλέπει η παράγραφος 6.

GDPR

Το άρθρο 5 του GDPR καθορίζει τις θεμελιώδεις αρχές του κανονισμού που διέπουν την επεξεργασία δεδομένων, συμπεριλαμβανομένης της διασφάλισης "κατάλληλης ασφάλειας των δεδομένων προσωπικού χαρακτήρα" και την προστασία από "μη εξουσιοδοτημένη ή παράνομη επεξεργασία και κατά τυχαίας απώλειας, καταστροφή ή φθορά, με τη χρήση κατάλληλων τεχνικών ή οργανωτικών μέτρων". [6] Τα μέτρα αυτά περιλαμβάνουν την ψευδωνυμοποίηση και την κρυπτογράφηση των δεδομένων προσωπικού χαρακτήρα της CIA (διασφαλίζοντας την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των δεδομένων) , την ικανότητα επαναφοράς της πρόσβασης των προσωπικών δεδομένων λίγο μετά από ένα φυσικό ή τεχνικό περιστατικό και μια διαδικασία για "τακτικές δοκιμές, αξιολόγηση και αξιολόγηση της αποτελεσματικότητας" των τεχνικών και οργανωτικών μέτρων ασφαλείας.

Το άρθρο 32 απαιτεί επίσης τη χρήση περιορισμών πρόσβασης σε προσωπικά δεδομένα που εμποδίζουν τους εργαζομένους και τους υπεύθυνους να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε αυτά. Σχετικά με τις υποχρεώσεις ασφάλειας του άρθρου 32 είναι οι αρμοδιότητες που έχουν οι υπεύθυνοι για την προστασία των δεδομένων σύμφωνα με το άρθρο 39 για να ενημερώνουν και να συμβουλεύουν τον οργανισμό σχετικά με τις υποχρεώσεις του GDPR (συμπεριλαμβανομένης της ασφάλειας) και την παρακολούθηση της συμμόρφωσης του οργανισμού με τις διατάξεις για την επεξεργασία δεδομένων του GDPR.

[6]Πρόσθετες οδηγίες σχετικά με τα κατάλληλα "τεχνικά και οργανωτικά μέτρα" βρίσκονται στο άρθρο 32, το οποίο απαιτεί από τους οργανισμούς "να εξασφαλίζουν επίπεδο ασφάλειας κατάλληλο για τον κίνδυνο" των δεδομένων που διατηρούνται και υποβάλλονται σε επεξεργασία

ISO 27001	GDPR	Τεμνόμενα Σημεία
Παράγραφος 5.1: η Διαχείριση διασφαλίζει ότι οι πολιτικές και οι στόχοι για την ασφάλεια των πληροφοριών καθορίζονται, ενσωματώνονται και συμβιβάζονται με τη στρατηγική κατεύθυνση του οργανισμού και επιτυγχάνουν τα επιθυμητά αποτελέσματα. **Παράγραφος 6.1.2:** ο οργανισμός προσδιορίζει τον κίνδυνο που συνδέεται με την απώλεια της «εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας» των πληροφοριών, προσδιορίζει τους ιδιοκτήτες κινδύνου (RiskOwners) και καθορίζει τα επίπεδα κινδύνου. **Παράγραφος 6.2:** ο οργανισμός θεσπίζει στόχους για την ασφάλεια των πληροφοριών που προκύπτουν από τις εκτιμήσεις κινδύνου **Παράγραφος 8:** ο οργανισμός επιβλέπει και διαχειρίζεται την εφαρμογή των διάφορων πτυχών του προγράμματος ασφάλειας σε ένα σχέδιο και επανεκτιμά συστηματικά τον κίνδυνο. **Έλεγχος Α. 10:** οι πολιτικές θα πρέπει να αναπτυχθούν και να υλοποιηθούν για τη χρήση κρυπτογραφικών στοιχείων ελέγχου και την προστασία των κρυπτογραφικών κλειδιών.	**Άρθρο 5 παράγραφος 1 στοιχείο στ) &Άρθρο 32:** οι ελεγκτές δεδομένων και οι επεξεργαστές εφαρμόζουν τεχνικά και οργανωτικά μέτρα για να διασφαλίσουν ένα επίπεδο ασφάλειας κατάλληλο για τον κίνδυνο. **Άρθρο 32:** για την αξιολόγηση του κατάλληλου επιπέδου ασφάλειας, λαμβάνονται υπόψη οι κίνδυνοι που παρουσιάζονται από την επεξεργασία, ιδίως από ακούσια ή παράνομη καταστροφή, απώλεια, αλλοίωση, μη εξουσιοδοτημένη αποκάλυψη ή πρόσβαση σε δεδομένα προσωπικού χαρακτήρα ενώ αυτά διαβιβάζονται, αποθηκεύονται ή υποβάλλονται σε επεξεργασία. **Άρθρο 32:** η ασφάλεια που ενδείκνυται για τον κίνδυνο μπορεί να περιλαμβάνει: Ψευδωνυμοποίηση και κρυπτογράφηση προσωπικών δεδομένων. Ικανότητα διασφάλισης συνεχούς εμπιστευτικότητας, ακεραιότητας, διαθεσιμότητας και ανθεκτικότητας των συστημάτων και υπηρεσιών επεξεργασίας. Δυνατότητα έγκαιρης επαναφοράς της διαθεσιμότητας και της πρόσβασης σε προσωπικά δεδομένα σε περίπτωση φυσικού ή τεχνικού περιστατικού. Διαδικασία για την τακτική δοκιμή και αξιολόγηση της αποτελεσματικότητας των τεχνικών και οργανωτικών μέτρων για την εξασφάλιση της ασφάλειας της επεξεργασίας. **Άρθρο 39:** ο υπεύθυνος προστασίας δεδομένων ενημερώνει και συμβουλεύει	Η συμμόρφωση με το ISO 27001 παρέχει ισχυρές ενδείξεις συμμόρφωσης με τις απαιτήσεις ασφάλειας του άρθρου 32 του GDPR. Αμφότερα επικεντρώνονται στον κίνδυνο που συνδέεται με την απώλεια εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας προστατευόμενων δεδομένων. Και τα δύο καθεστώτα απαιτούν η εσωτερική ηγεσία να συνεργαστεί με άλλους υπεύθυνους σε όλο τον οργανισμό για να χαρτογραφήσει τις δραστηριότητες επεξεργασίας δεδομένων και να αξιολογήσει τον κίνδυνο για την οργάνωση – και τα υποκείμενα των δεδομένων – κατανοώντας την ευαισθησία των πληροφοριών. Οι υπεύθυνοι ασφάλειας θα συνεργαστούν στενά με την ομάδα απορρήτου για να παράσχουν τεκμηρίωση ότι τα συστήματα ασφάλειας είναι στα κατάλληλα επίπεδα.

	τον υπεύθυνο επεξεργασίας ή τον εκτελούντα της επεξεργασίας και τους εργαζομένους του σχετικά με τις υποχρεώσεις τους βάσει του GDPR και παρακολουθεί τη συμμόρφωση με τον κανονισμό, συμπεριλαμβανομένης της ανάθεσης αρμοδιοτήτων, ευαισθητοποίησης και κατάρτισης του προσωπικού και των συναφών ελέγχων. **Άρθρο 32:** ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία λαμβάνουν μέτρα για να διασφαλίσουν ότι κάθε φυσικό πρόσωπο που ενεργεί υπό την εξουσία του και έχει πρόσβαση σε δεδομένα προσωπικού χαρακτήρα δεν επεξεργάζεται τα δεδομένα για σκοπούς που δεν έχουν σχέση με τις αρμοδιότητες του.	

Συμπερασματικά προκύπτει με βάση την ανάλυση που έγινε ότι η εφαρμογή του προτύπου ISO 27001 είναι ένα ισχυρό μέσο για την απόδειξη της συμμόρφωσης με τις απαιτήσεις ασφάλειας του άρθρου 32 του GDPR. Φυσικά, ο τελικός έλεγχος στο πρότυπο ISO 27001 του παραρτήματος 1 απαιτεί από τους υπεύθυνους ασφάλειας να γνωρίζουν όλες τις σχετικές νομικές απαιτήσεις, να τεκμηριώνουν αυτές και να τις ενσωματώνουν σε σχέδια ασφάλειας, έτσι ώστε η συμμόρφωση με το ISO 27001 να απαιτεί την ενημέρωση σε πολιτικές και διαδικασίες που αντικατοπτρίζουν τις απαιτήσεις του GDPR.

4.2 Παραβίαση Δεδομένων

ISO 27001

Το ISO 27001 απαιτεί μηχανισμούς τόσο για τον γρήγορο εντοπισμό περιστατικών ασφαλείας όσο και για την αναφορά τους μέσω των απαραίτητων ενεργειών. Ο έλεγχος αυτός (Α. 16) έχει σχεδιαστεί για να εξασφαλίζει μια συνεπή και αποτελεσματική προσέγγιση στη διαχείριση περιστατικών ασφάλειας πληροφοριών,

συμπεριλαμβανομένης της επικοινωνίας σχετικά με συμβάντα ασφαλείας και αδυναμίες του συστήματος. Τα θεμελιώδη στοιχεία που στηρίζουν ένα σχέδιο ανταπόκρισης συμβατό με το ISO 27001 είναι μια σαφής αλυσίδα της διοίκησης, με τις καθιερωμένες διαδικασίες ταυτοποίησης και αναφοράς ή της αναφοράς οποιασδήποτε ασυνήθιστης δραστηριότητας ή συμβάντων από εργαζομένους και υπεύθυνους.

GDPR

Ο κανονισμός GDPR περιέχει δύο ξεχωριστές απαιτήσεις γνωστοποίησης παραβίασης δεδομένων. Πρώτα, στο άρθρο 33, απαιτεί από τους υπεύθυνους επεξεργασίας δεδομένων να παρέχουν ειδοποίηση για οποιαδήποτε παραβίαση δεδομένων "που ενδέχεται να οδηγήσει σε κίνδυνο για τα δικαιώματα και τις ελευθερίες ενός φυσικού προσώπου" στη σχετική εποπτική αρχή "χωρίς αδικαιολόγητη καθυστέρηση" και το αργότερο εντός 72 ωρών από τη στιγμή που έχει προηγηθεί η παραβίαση. Το άρθρο 33 απαιτεί επίσης από τους επεξεργαστές των δεδομένων να ενημερώνουν τους υπεύθυνους επεξεργασίας δεδομένων για τυχόν παραβιάσεις "*χωρίς αδικαιολόγητη καθυστέρηση*".

Ομοίως και ο κανονισμός του GDPR στο άρθρο 34 απαιτεί κοινοποίηση στα υποκείμενα των δεδομένων μετά από παραβίαση, αλλά μόνο όταν η παραβίαση θα οδηγήσει σε "υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων". Η κοινοποίηση πρέπει να περιλαμβάνει τα στοιχεία επικοινωνίας του ΥΠΔ, τις πιθανές συνέπειες της παραβίασης, καθώς και τα μέτρα που ελήφθησαν ή εξετάστηκαν για την αντιμετώπιση της παραβίασης . Το άρθρο 34 εξαιρεί τους ελεγκτές από την κοινοποίηση των υποκειμένων των δεδομένων όταν έχουν εφαρμόσει κατάλληλα τεχνικά και οργανωτικά μέτρα προστασίας που καθιστούν τα δεδομένα προσωπικού χαρακτήρα μη κατανοητά. Τέλος, το άρθρο 34 παρέχει στις αρχές προστασίας δεδομένων τη διακριτική ευχέρεια να υποχρεώνουν τους οργανισμούς να κοινοποιούν τα υποκείμενα των δεδομένων τα οποία επηρεάστηκαν από την παραβίαση.

ISO 27001	GDPR	Τεμνόμενα Σημεία
Έλεγχος Α. 16: τα συμβάντα ασφάλειας πληροφοριών πρέπει να αναφέρονται άμεσα μέσω των κατάλληλων	**Άρθρο 33:** ο υπεύθυνος επεξεργασίας πρέπει να ενημερώνει την εποπτική αρχή χωρίς αδικαιολόγητη καθυστέρηση , εφόσον είναι	Η οργανωτική δομή αναφοράς που δημιουργείται από τις απαιτήσεις ISO 27001 μπορεί να προσαρμοστεί για να

εσωτερικών ενεργειών, τα οποία αξιολογούνται για να προσδιοριστεί εάν είναι "συμβάντα" τεκμηριωμένα και στην συνέχεια ερευνώνται.	εφικτό, το αργότερο εντός 72 ωρών από τη στιγμή που έχει ενημερωθεί για την παραβίαση των δεδομένων προσωπικού χαρακτήρα, εκτός εάν η παραβίαση δεν είναι πιθανό να οδηγήσει σε κίνδυνο για τα δικαιώματα του φυσικού προσώπου. Η ανακοίνωση προς την εποπτική αρχή πρέπει να περιλαμβάνει, όταν είναι εφικτό: Την φύση της παραβίασης δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων των κατηγοριών και κατά προσέγγιση του αριθμού των ενδιαφερομένων προσώπων. Τα στοιχεία επικοινωνίας του ΥΠΔ του υπευθύνου επεξεργασίας. Τις πιθανές συνέπειες της παραβίασης. Σχέδιο αντίδρασης, συμπεριλαμβανομένων των μέτρων μετριασμού. **Άρθρο 34:** όταν η παραβίαση δεδομένων προσωπικού χαρακτήρα είναι πιθανό να οδηγήσει σε υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας κοινοποιεί την παραβίαση των δεδομένων προσωπικού χαρακτήρα στα θιγόμενα υποκείμενα των δεδομένων χωρίς αδικαιολόγητη καθυστέρηση. Η ειδοποίηση πρέπει να περιλαμβάνει, όταν είναι εφικτό: Τον αριθμό των υποκειμένων των δεδομένων. Τα στοιχεία επικοινωνίας του ΥΠΔ. Πιθανές συνέπειες της παραβίασης. Το σχέδιο απόκρισης του υπευθύνου επεξεργασίας,	ενσωματώσει την απαραίτητη αρχή προστασίας δεδομένων. Το προσωπικό ασφαλείας θα είναι συχνά το πρώτο που θα ανακαλύψει ένα περιστατικό παραβίασης. Οι κατάλληλες διαδικασίες για την αναφορά ενός συμβάντος ασφαλείας περιλαμβάνουν την κοινοποίηση του ΥΠΔ. Ο ΥΠΔ θα συμμετέχει επίσης στον προσδιορισμό του εάν το γεγονός επηρεάζει το επίπεδο παραβίασης δεδομένων προσωπικού χαρακτήρα. Οι ομάδες απορρήτου και ασφάλειας θα πρέπει επίσης να συνεργαστούν για την ανακοίνωση στην εποπτική αρχή και, εάν είναι απαραίτητο, στα υποκείμενα των δεδομένων. Η ανακοίνωση θα πρέπει να περιλαμβάνει πληροφορίες σχετικά με την παραβίαση δεδομένων προσωπικού χαρακτήρα που ανακαλύφθηκε κατά τη διάρκεια ερευνών , καθώς και σχέδια ασφάλειας για τον μετριασμό των βλαβών και την πρόληψη μελλοντικών πρόσθετων περιστατικών.

	συμπεριλαμβανομένων των μέτρων μετριασμού.	
Έλεγχος Α. 18: η Διαχείριση της ασφάλειας περιλαμβάνει τη συμμόρφωση με νομικές, κανονιστικές και συμβατικές υποχρεώσεις σχετικά με την ιδιωτικότητα των πληροφοριών	**Άρθρο 33:** οι μεταποιητές δεδομένων πρέπει να ενημερώνουν τους υπεύθυνους επεξεργασίας δεδομένων χωρίς αδικαιολόγητη καθυστέρηση για την παραβίαση των δεδομένων προσωπικού χαρακτήρα	Να υπάρχει προσδιορισμός των συμβάσεων που ενδέχεται να σχετίζονται με τα δεδομένα που επηρεάζονται από το περιστατικό ασφαλείας και την παροχή κατάλληλης ειδοποίησης σύμφωνα με τις εν λόγω συμφωνίες, ανάλογα με τις ανάγκες.

Οι απαιτήσεις του άρθρου 33 του GDPR και του άρθρου 34 είναι συμπληρωματικές των προτύπων ISO 27001. Μέσω του κατάλληλου σχεδιασμού, κατάρτισης και πρακτικής αντίδρασης σε συμβάντα, ένα περιστατικό ασφάλειας θα πρέπει να συνοδεύεται από επικοινωνία μεταξύ των υπευθύνων ασφάλειας και προστασίας της ιδιωτικής ζωής. Οι τρέχουσες πολιτικές θα πρέπει να περιλαμβάνουν τη σχετική δομή εκθέσεων και τις απογραφές κινδύνων προσωπικών δεδομένων, ώστε να μπορούν να διερευνηθούν τα συμβάντα, να αξιολογηθούν με βάση τον ορισμό της "παραβίασης δεδομένων προσωπικού χαρακτήρα" στο πλαίσιο του GDPR και να είναι σε ετοιμότητα ο οργανισμός για να κοινοποιηθεί η παραβίαση χωρίς καθυστέρηση.

4.3 Διαχείριση προμηθευτών

ISO 27001

Το ISO 27001 περιλαμβάνει την εποπτεία και τον έλεγχο των προμηθευτών ως κρίσιμα στοιχεία των κατάλληλων πρωτοκόλλων ασφάλειας δεδομένων. Η παράγραφος 8 απαιτεί από τους οργανισμούς να προσδιορίζουν τις ενέργειες επεξεργασίας που ανατίθενται εξωτερικά και να διασφαλίζουν ότι οι διαδικασίες αυτές αποτελούν ελεγχόμενο τμήμα του προγράμματος ασφάλειας. Επίσης απαιτείται από τους οργανισμούς να επανεξετάζουν, να τεκμηριώνουν και να διατηρούν την εποπτεία των προγραμμάτων ασφαλείας, τα οποία μπορεί να περιλαμβάνουν προγραμματισμένες αξιολογήσεις κινδύνου και ελέγχους για να επιβεβαιώσουν ότι τα δεδομένα των πελατών είναι ασφαλή. Πρόσθετες, πιο συγκεκριμένες κατευθύνσεις βρίσκονται στους ελέγχους Α. 15, που διέπουν τις «σχέσεις προμηθευτών» και Α.

18.1, που διέπουν τη συμμόρφωση με τις συμβατικές απαιτήσεις. Επιπλέον, ο έλεγχος Α. 15 αντιμετωπίζει ζητήματα ασφάλειας όπου ο οργανισμός είναι ευάλωτος στην πρόσβαση προμηθευτών ("προμηθευτής") σε προσωπικά δεδομένα. Απαιτεί την μείωση του κινδύνου περιορίζοντας την πρόσβαση στα δεδομένα και εισάγοντας συμφωνίες για την επιβολή ευθυνών ασφαλείας και την εκχώρηση ευθύνης. Τέλος, ο έλεγχος Α. 18 εξετάζει τη συμμόρφωση με τις συμφωνίες και ο οργανισμός ενεργεί ως προμηθευτής, απαιτώντας τη συμμόρφωση με τις απαιτήσεις ασφαλείας του πελάτη.

GDPR

Το άρθρο 28 του GDPR ορίζει λεπτομερείς απαιτήσεις για τη διαχείριση των προμηθευτών, θέτοντας σαφείς ευθύνες τόσο για τους υπεύθυνους επεξεργασίας δεδομένων όσο και για τους μεταποιητές που πρέπει να ενσωματώνονται στις συμβάσεις. Οι ελεγκτές περιορίζονται στη χρήση μόνο των επεξεργαστών που μπορούν να εγγυηθούν τεχνικές, διοικητικές και οργανωτικές διασφαλίσεις σε επίπεδα ίσα ή υπερβαίνοντας αυτά που απαιτούνται από τον GDPR. Ένα σημαντικό επίκεντρο του άρθρου 28 είναι η απαίτηση να εξασφαλίζουν οι ελεγκτές συμβατικούς όρους και διαβεβαιώσεις από τους μεταποιητές, δημιουργώντας μια μορφή συμφωνίας γνωστή ως "συμφωνία προστασίας δεδομένων". Το άρθρο 28 προτείνει τους τύπους ελέγχων που πρέπει να περιέχει η συμφωνία για την προστασία των δεδομένων

ISO 27001	GDPR	Τεμνόμενα Σημεία
Παράγραφος 8: έλεγχος και επίβλεψη των διαδικασιών που ανατίθενται σε τρίτους. **Παράγραφος 9:** αναθεώρηση του αντίκτυπου των συμβάσεων προμηθευτών και των επιδόσεων σε θέματα ασφάλειας. **Έλεγχος Α. 15:** άμβλυνση των κινδύνων για τον οργανισμό που παρουσιάζονται από προμηθευτές που έχουν πρόσβαση σε προσωπικά δεδομένα. Οι συμφωνίες προμηθευτών θα πρέπει να αντιμετωπίζουν τους κινδύνους για την ασφάλεια των πληροφοριών και να	**Άρθρο 28: οι** ελεγκτές χρησιμοποιούν μόνο τους μεταποιητές που εξασφαλίζουν τις κατάλληλες τεχνικές και οργανωτικές διασφαλίσεις. Η επεξεργασία πρέπει να διέπετε από συμβατή σύμβαση. **Άρθρο 28:** οι μεταποιητές δεν μπορούν να αναθέτουν υπεργολαβία σε άλλους μεταποιητές χωρίς την συγκατάθεση του υπευθύνου επεξεργασίας και την ύπαρξη της κατάλληλης σύμβασης. Οι μεταποιητές μοιράζονται την ευθύνη για τις απαιτήσεις ασφάλειας και πρόσβασης.	Επειδή το άρθρο 28 του GDPR επιβαρύνει τους ελεγκτές με την επιλογή επεξεργαστών που διαθέτουν κατάλληλα τεχνικά και οργανωτικά μέτρα ασφαλείας, γι' αυτό τον λόγο οι ομάδες προστασίας προσωπικών δεδομένων των ελεγκτών θα πρέπει να συνεργαστούν με τις ομάδες ασφάλειας για να ανταποκριθούν στις απαιτήσεις των ελεγκτών. Οι στόχοι του ISO 27001 όσον αφορά την ασφάλεια των προμηθευτών και τον σεβασμό των συμβατικών υποχρεώσεων είναι συμβατές με αυτούς τους στόχους.

επιβάλλουν ευθύνες για την ιδιωτικότητα και την ασφάλεια. **Έλεγχος Α. 18:** αποφυγή παραβιάσεων των συμβατικών ευθυνών για τη διατήρηση της ιδιωτικής ζωής και της ασφάλειας των προσωπικών πληροφοριών.		

Με το άρθρο 28 του GDPR να απαιτεί ρητώς από τους υπεύθυνους του απορρήτου να ενσωματώνουν διαβεβαιώσεις ασφαλείας σε συμβάσεις επεξεργασίας δεδομένων, η ικανότητα του προμηθευτή να επιδεικνύει συμμόρφωση με το ISO 27001 γίνεται ακόμη πιο συναφής. Επίσης ο κανονισμός του GDPR απαγορεύει στους ελεγκτές δεδομένων να μεταφέρουν δεδομένα σε μεταποιητές που δεν μπορούν να εγγυηθούν κατάλληλες τεχνικές και οργανωτικές διασφαλίσεις σε γραπτή συμφωνία. Οι συμβατικές απαιτήσεις του άρθρου 28 είναι επίσης κρίσιμες για τη διάρθρωση των σχέσεων μεταξύ υπευθύνων επεξεργασίας και μεταποιητών. Οι υπεύθυνοι ασφάλειας μπορεί να χρειαστεί να βοηθήσουν με πιθανούς προμηθευτές για να αξιολογήσουν τα καθεστώτα ασφαλείας των προμηθευτών και να ανταποκριθούν στα ερωτηματολόγια ασφαλείας των πελατών.

4.4 Τήρηση εγγράφων

ISO 27001

Ο στόχος του ISO 27001 στην παράγραφο 8 είναι η ανάπτυξη και η διατήρηση κατάλληλων διασφαλίσεων για οργανωτικά έγγραφα. Αυτό το πρωτόκολλο απογραφής περιλαμβάνει απαιτήσεις για σαφείς ορισμούς της ιδιοκτησίας και αποδεκτές χρήσεις για τα δεδομένα. Η παράγραφος 8.2 συνεχίζει με την απαίτηση ταξινόμησης, επισήμανσης και ελέγχου πρόσβασης δεδομένων με βάση τα επίπεδα ευαισθησίας. Τέλος η παράγραφος 9 περιλαμβάνει επίσης σχετικές κατευθύνσεις για τη δημιουργία και τη διατήρηση μιας πολιτικής ελέγχου της πρόσβασης.

GDPR

Ο κανονισμός του GDPR στο άρθρο 30 απαιτεί από τους ελεγκτές και τους μεταποιητές δεδομένων να διατηρούν αρχεία των δραστηριοτήτων επεξεργασίας

τους, προσδιορίζοντας τον τρόπο επεξεργασίας και διατήρησης διαφορετικών κατηγοριών δεδομένων από έναν οργανισμό. Για τους ελεγκτές, τα αρχεία αυτά πρέπει να περιέχουν: τις κατηγορίες των υποκειμένων των δεδομένων, τις κατηγορίες των συλλεγόμενων δεδομένων , τα είδη των δραστηριοτήτων επεξεργασίας που έχουν και είναι πιθανό να πραγματοποιηθούν, τον νομικό σκοπό ή τον λόγο της επεξεργασίας, δυνητικούς αποδέκτες γνωστοποιήσεων, πληροφορίες σχετικά με τη διασυνοριακή μεταφορά των δεδομένων, σχέδια διατήρησης και τους ελέγχους ασφάλειας. Για τους μεταποιητές, τα περιεχόμενα των εγγραφών είναι πιο περιορισμένα και περιλαμβάνουν: κατηγορίες δραστηριοτήτων επεξεργασίας, πληροφορίες σχετικά με τον υπεύθυνο επεξεργασίας δεδομένων, πληροφορίες σχετικά με τις διασφαλίσεις ασφάλειας και τις διασυνοριακές διαβιβάσεις δεδομένων.

ISO 27001	GDPR	Τεμνόμενα Σημεία
Παράγραφος 8: ο οργανισμός τεκμηριώνει τις διαδικασίες ασφάλειάς του, καθώς και τα αποτελέσματα των αξιολογήσεων κινδύνου ασφάλειας και μείωσης του κινδύνου. **Έλεγχος Α. 8:** η απογραφή και η κατάταξη των στοιχείων να είναι διαβαθμισμένα. Επίσης οι κάτοχοι των περιουσιακών στοιχείων ανατίθενται με διαδικασίες που ορίζονται για την αποδεκτή χρήση των δεδομένων, την επισήμανση και τον χειρισμό. **Έλεγχος Α. 8.3:** η πρόληψη της μη εξουσιοδοτημένης γνωστοποίησης περιλαμβάνει την ασφαλή διάθεση των μέσων αποθήκευσης στα οποία αποθηκεύονται οι πληροφορίες όταν δεν είναι πλέον απαραίτητες. **Έλεγχος Α. 13.2** οι πληροφορίες που μεταφέρονται σε εξωτερικό σημείο να είναι με τα κατάλληλα μέτρα ασφάλειας και με την δημιουργία συμφωνιών που αφορούν την ασφάλεια και συνάδουν	**Άρθρο 30 παράγραφος 1:** ο υπεύθυνος επεξεργασίας τηρεί αρχείο των δραστηριοτήτων επεξεργασίας υπό την ευθύνη του, η οποία περιλαμβάνει: Το όνομα και τα στοιχεία επικοινωνίας του υπευθύνου επεξεργασίας και του ΥΠΔ. Τους σκοπούς της επεξεργασίας. Τις κατηγορίες υποκειμένων των δεδομένων και δεδομένων προσωπικού χαρακτήρα. Την μεταφορά δεδομένων προσωπικού χαρακτήρα σε οποιαδήποτε τρίτη χώρα και τεκμηρίωση κατάλληλων εγγυήσεων για τις εν λόγω μεταβιβάσεις. Τις προθεσμίες διαγραφής δεδομένων, πολιτικές και διατήρησης δεδομένων. Την γενική περιγραφή των τεχνικών και οργανωτικών μέτρων ασφάλειας που χρησιμοποιήθηκαν. **Άρθρο 30 παράγραφος 2:** ο εκτελών την επεξεργασία τηρεί αρχείο όλων των κατηγοριών των δραστηριοτήτων επεξεργασίας που	Η συμμόρφωση με τις απαιτήσεις τήρησης αρχείων του άρθρου 30 περιλαμβάνει σημαντική εσωτερική επικοινωνία. Η τεκμηρίωση της ομάδας ασφάλειας για τις διαδικασίες ασφάλειας και την κατάταξη των στοιχείων θα συμβάλει στην προσπάθεια αυτή. Αντιστρόφως, η κατηγοριοποίηση των υποκειμένων των δεδομένων και των προσωπικών δεδομένων από την ομάδα απορρήτου μπορεί να είναι σχετική με την ταξινόμηση πληροφοριών που τηρούνται από τους υπεύθυνους ασφάλειας. Οι υπεύθυνοι απορρήτου ασχολούνται επίσης με την απογραφή και την αντιστοίχιση δεδομένων, μια εργασία που θα βοηθηθεί από τον προσδιορισμό της ομάδας ασφαλείας για τη θέση και την ιδιοκτησία των στοιχείων. Οι τρέχοντες κατάλογοι αποδεκτών χρήσεων για πληροφορίες που απαιτούνται από το ISO 27001 θα παρέχουν επίσης στην ομάδα απορρήτου

με τυπικές πολιτικές, διαδικασίες και ελέγχους.	διενεργούνται για λογαριασμό του υπευθύνου επεξεργασίας, ο οποίος περιλαμβάνει: Όνομα και στοιχεία επικοινωνίας του μεταποιητή και κάθε υπευθύνου επεξεργασίας για λογαριασμό του οποίου ενεργεί ο εκτελών την επεξεργασία. Τις κατηγορίες επεξεργασίας που διενεργούνται για λογαριασμό κάθε υπευθύνου επεξεργασίας. Τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα σε τρίτη χώρα και τεκμηρίωση κατάλληλων εγγυήσεων. Την γενική περιγραφή των τεχνικών και οργανωτικών μέτρων ασφαλείας που χρησιμοποιήθηκαν. Τα αρχεία αυτά πρέπει να είναι γραπτώς, μεταξύ άλλων και σε ηλεκτρονική μορφή.	σημαντικές πληροφορίες για τη διατήρηση και την επεξεργασία των δεδομένων. Ο ορισμός της ασφάλειας για τις αποδεκτές χρήσεις των στοιχείων αντικατοπτρίζει τη συνολική τεχνική και οργανωτική ασφάλεια που υπάρχει για τα δεδομένα προσωπικού χαρακτήρα και μπορεί να ταιριάζει απόλυτα με τις απαιτήσεις των εγγραφών του άρθρου 30. Τέλος, παρόλο που οι διεθνείς μεταφορές δεδομένων αποτελούν ειδική περίπτωση στο πλαίσιο του GDPR, τα μέτρα που λαμβάνουν οι υπεύθυνοι ασφαλείας για να εντοπίσουν και να διασφαλίσουν την ασφάλεια των μεταβιβάσεων σε "εξωτερικά μέρη" μπορούν να βοηθήσουν την ομάδα απορρήτου με την καταγραφή των διασυνοριακών μεταβιβάσεων.

Η καταγραφή των υπαρχόντων δεδομένων και η χαρτογράφηση τους είναι τα πρώτα βήματα για την δημιουργία ενός προγράμματος προστασίας προσωπικών δεδομένων. Το άρθρο 30 απαιτεί να τηρούνται αρχεία ορισμένων πληροφοριών που αποκτώνται κατά τη διαδικασία απογραφής και χαρτογράφησης. Αυτή η δυνητικά περίπλοκη εργασία απαιτεί σημαντική προσπάθεια από όλους σε ολόκληρο τον οργανισμό και όχι μόνο από την ομάδα απορρήτου. Η ομάδα ασφαλείας μπορεί να έχει ήδη τεκμηριωμένες και διαβαθμισμένες τις πληροφορίες σύμφωνα με το ISO 27001 και έτσι μπορεί να είναι το πρώτο μέρος που θα ξεκινήσει την χαρτογράφηση και καταγραφή. Το άρθρο 30 μπορεί να μεταβάλει τον τρόπο με τον οποίο οι πληροφορίες κατηγοριοποιούνται, επισημαίνονται και διατηρούνται. Αυτές οι αλλαγές θα απαιτήσουν συνεργασία μεταξύ των ομάδων ασφάλειας και προστασίας προσωπικών δεδομένων. Παρά τις αλλαγές αυτές, τα υφιστάμενα πλαίσια απογραφής ISO 27001 είναι πιθανό να αποτελέσουν ισχυρό σημείο εκκίνησης για την επίτευξη της συμμόρφωσης με το άρθρο 30.

4.5 Προστασία προσωπικών δεδομένων μέσω του σχεδιασμού

ISO 27001

Οι παράγραφοι 5 και 6 περιέχουν πολλαπλές απαιτήσεις που έχουν σχεδιαστεί για την ανάπτυξη και τη διατήρηση ενός προσαρμοζόμενου πλαισίου ασφάλειας, ενώ ταυτόχρονα εντοπίζονται και μετριάζονται οι λειτουργικοί κίνδυνοι.

Πιο αναλυτικά, η παράγραφος 5 υιοθετεί μια διαρθρωτική προσέγγιση του θέματος, απαιτώντας την ανάπτυξη και την περιοδική αναθεώρηση των αναγκαίων πολιτικών ασφαλείας. Απαιτεί επίσης τον διορισμό όλων των απαραίτητων διευθυντικών στελεχών και τη σαφή ανάθεση των καθηκόντων και ευθυνών.

Η παράγραφος 6 τώρα απαιτεί από έναν οργανισμό να διεξάγει σε μόνιμη βάση αξιολογήσεις του κινδύνου για την ασφάλεια, σχεδιασμένες να εξασφαλίζουν την αποτελεσματικότητα του προγράμματος διαχείρισης ασφάλειας, όπως και τον εντοπισμό και πρόληψη του κινδύνου, καθώς και την κατάλληλη αντιμετώπιση των ζητημάτων ασφαλείας. Σε συνδυασμό, οι παράγραφοι αυτοί τονίζουν τη σημασία της θέσπισης ενός θεμελιώδους πλαισίου που θα επιτρέπει τη δοκιμή και τη διαφύλαξη των δράσεων επεξεργασίας.

GDPR

Όπως και τα πρότυπα ISO 27001, έτσι και το άρθρο 25 του GDPR ενθαρρύνει ένα σύστημα και μια πρακτική, που ενισχύεται από τις πολιτικές που εποπτεύονται από τη διοίκηση, την ενσωμάτωση των αρχών ασφάλειας και προστασίας της ιδιωτικής ζωής σε προϊόντα και διεργασίες από την αρχή και κατά τη διάρκεια της διαδικασίας. Ο GDPR αποκαλεί αυτό "προστασία δεδομένων από τη σχεδίαση και από προεπιλογή." Πρώτον, λαμβάνοντας υπόψη το κόστος, το πεδίο εφαρμογής και το περιεχόμενο της επεξεργασίας, ο υπεύθυνος επεξεργασίας πρέπει να παρέχει "κατάλληλες" διασφαλίσεις "τόσο κατά τον καθορισμό των μέσων επεξεργασίας όσο και κατά τον χρόνο της επεξεργασίας." Δεύτερον, το άρθρο 25 απαιτεί από τους οργανισμούς να συλλέγουν, να επεξεργάζονται και να διατηρούν μόνο δεδομένα που είναι απολύτως απαραίτητα, μειώνοντας έτσι τον όγκο και το εύρος των δεδομένων που θα μπορούσαν να χαθούν, και να προσδιορίσουν τους πιθανούς κινδύνους για την προστασία της ιδιωτικής ζωής που συνδέονται με μια συγκεκριμένη για την

εφαρμογή μέτρων μετριασμού των κινδύνων αυτών. Οι απαιτήσεις αυτές ενθαρρύνουν μια ολιστική άποψη της διαχείρισης δεδομένων, προσδιορίζοντας επακριβώς τα δεδομένα που απαιτούνται για κάθε βήμα της διαδικασίας και εξασφαλίζοντας ότι οι κατάλληλες διασφαλίσεις έχουν ήδη πραγματοποιηθεί ακόμη και πριν από τη συλλογή των δεδομένων.

ISO 27001	GDPR	Τεμνόμενα Σημεία
Παράγραφος 4: οι οργανισμοί κατανοούν το πεδίο εφαρμογής και το πλαίσιο των ήδη υπαρχόντων και επεξεργασμένων δεδομένων. **Παράγραφος 5:** πρέπει να οριστεί ο υπεύθυνος ασφάλειας και να δοθούν σαφώς καθορισμένες αρμοδιότητες. **Παράγραφος 6:** οι υπεύθυνοι ασφάλειας θα πρέπει να εκτελούν συστηματικά αναλύσεις κινδύνου για τον προσδιορισμό των απειλών ασφάλειας, της ανοχής κινδύνου και των στόχων ασφάλειας **Έλεγχος Α. 10:** οι πολιτικές θα πρέπει να αναπτυχθούν και να υλοποιηθούν κατάλληλα για τη χρήση κρυπτογραφικών στοιχείων ελέγχου και την προστασία αυτών των κρυπτογραφικών κλειδιών	**Άρθρο 25:** λαμβάνοντας υπόψη την κατάσταση της τεχνολογίας, το κόστος εφαρμογής, τη φύση και το πεδίο εφαρμογής της επεξεργασίας, καθώς και τους κινδύνους για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων, ο υπεύθυνος επεξεργασίας εφαρμόζει τα κατάλληλα τεχνικά και οργανωτικά μέτρα , όπως την ψευδωνυμοποίηση, τον σχεδιασμός για την εφαρμογή αρχών προστασίας δεδομένων, την ελαχιστοποίηση των δεδομένων και την ενσωμάτωση των διασφαλίσεων στην επεξεργασία. Ο υπεύθυνος επεξεργασίας εφαρμόζει τα κατάλληλα τεχνικά και οργανωτικά μέτρα για να διασφαλίσει ότι, εξ ορισμού, υφίστανται επεξεργασία μόνο τα δεδομένα προσωπικού χαρακτήρα που είναι απαραίτητα για κάθε συγκεκριμένο σκοπό της επεξεργασίας. Η συλλογή, η επεξεργασία και η διατήρηση περιορίζονται σε ό,τι είναι απαραίτητο.	Οι ομάδες προστασίας προσωπικών δεδομένων κατά πάσα πιθανότητα θα συμμετάσχουν στις ομάδες ασφάλειας αξιολογώντας τις υπάρχουσες πρακτικές συλλογής και επεξεργασίας για να καθορίσουν αν η αρχή του περιορισμού της συλλογής εξετάζεται δεόντως. Η ασφάλεια είναι ένα βασικό συστατικό από τον σχεδιασμό της για την προστασία της ιδιωτικής ζωής ως προς την σχεδίαση προϊόντων και συστημάτων.

Απαιτώντας από τους οργανισμούς να προσδιορίσουν το πεδίο εφαρμογής, το περιβάλλον και τη δομή διαχείρισης των προγραμμάτων ασφαλείας, το ISO 27001

ενθαρρύνει την προστασία δεδομένων μέσω σχεδιασμού. Η ελαχιστοποίηση των δεδομένων είναι ένα σημαντικό μέλημα που προστέθηκε από το άρθρο 25 του GDPR, το οποίο θα πρέπει να ενσωματωθεί στις υφιστάμενες πολιτικές ασφαλείας. Οι ομάδες προστασίας προσωπικών δεδομένων κατά πάσα πιθανότητα θα συμμετάσχουν στις ομάδες ασφάλειας αξιολογώντας τις υπάρχουσες πρακτικές συλλογής και επεξεργασίας για να καθορίσουν αν η αρχή του περιορισμού της συλλογής απαιτείται. Παρόλο που η προστασία των δεδομένων από τον σχεδιασμό και την προεπιλογή στοχεύει σε ομάδες προγραμματισμού, μάρκετινγκ και ανάπτυξης προϊόντων, η ασφάλεια είναι πάντα ένα κρίσιμο στοιχείο της ιδιωτικής ζωής, ιδίως στον σχεδιασμό προϊόντων και συστημάτων.

4.6 Κατηγοριοποίηση δεδομένων και απαιτήσεις ελέγχου πρόσβασης

ISO 27001

Το ISO 27001 δεν αντιμετωπίζει ρητά τα δικαιώματα του υποκειμένου των δεδομένων. Ο συνδυασμός της απογραφής των δεδομένων, της ταξινόμησης και των λειτουργικών απαιτήσεων από τον όρο 8 και τον έλεγχο Α. 8, ενισχύει την ασφάλεια με γνώση των κατηγοριών δεδομένων που συλλέγει ο οργανισμός σχετικά με τα υποκείμενα των δεδομένων. Επιπλέον, ο έλεγχος Α. 9 ορίζει διευθύνσεις ελέγχου πρόσβασης, που περιλαμβάνουν τον τρόπο ελέγχου ταυτότητας των υποκειμένων δεδομένων που αποκτούν πρόσβαση στα δικά τους δεδομένα μέσω πιστοποιημένης σύνδεσης.

GDPR

Ο κανονισμός GDPR αντιμετωπίζει τα δικαιώματα του υποκειμένου των δεδομένων στα άρθρα 13 έως 22, με κάθε άρθρο εστιάζοντας σε ένα συγκεκριμένο δικαίωμα. Τα υποκείμενα των δεδομένων δικαιούνται: διαφάνεια σχετικά με τα προσωπικά δεδομένα που συλλέγονται και τον τρόπο επεξεργασίας τους, το δικαίωμα πρόσβασης στα προσωπικά τους δεδομένα, το δικαίωμα να διορθώσει ανακριβή δεδομένα προσωπικού χαρακτήρα σχετικά με αυτά και να διαγράψει τις πληροφορίες του υπό ορισμένες συνθήκες, να περιορίσει την επεξεργασία των δεδομένων από τον υπεύθυνο επεξεργασίας και να είναι σε θέση να απαιτήσει από τον υπεύθυνο

επεξεργασίας να λάβει τα δεδομένα του σε άλλον υπεύθυνο επεξεργασίας σε ορισμένες περιπτώσεις. Επιπλέον, τα υποκείμενα των δεδομένων έχουν το δικαίωμα να γνωρίζουν εάν λαμβάνονται αποφάσεις σχετικά με αυτά μέσω αυτοματοποιημένων μέσων και να αντιτίθενται στην επεξεργασία, καθώς και στην άμεση εμπορική προώθηση των δεδομένων.

ISO 27001	GDPR	Τεμνόμενα Σημεία
Έλεγχος Α. 8: τα στοιχεία πληροφοριών πρέπει να είναι ταξινομημένα. Επίσης να ταξινομούνται οι κάτοχοι περιουσιακών στοιχείων, με διαδικασίες που ορίζονται για την αποδεκτή χρήση των δεδομένων, την επισήμανση και το χειρισμό τους. Η κυριότητα των περιουσιακών στοιχείων πρέπει να προσδιορίζεται σαφώς. **Έλεγχος Α. 9.2:**οι οργανισμοί πρέπει να διαθέτουν τυπικά συστήματα για την καταχώριση και την αποταξινόμηση των χρηστών, ώστε να επιτρέπουν την εκχώρηση δικαιώματος πρόσβασης. Να έχουν διαδικασίες για την πιστοποίηση των χρηστών και την ανάκληση της πρόσβασης τους όπου οι εργαζόμενοι και τα εξωτερικά μέρη να χάνουν τα δικαιώματα πρόσβασης που είχαν κατά τον τερματισμό της σχέσης. **Έλεγχος Α. 9.4:** οι ασφαλείς διαδικασίες σύνδεσης πρέπει να χρησιμοποιούνται για τον έλεγχο της πρόσβασης των χρηστών σε συστήματα πληροφοριών και εφαρμογών. **Έλεγχος Α. 12:** οι λειτουργικές διαδικασίες πρέπει να τεκμηριώνονται. **Έλεγχος Α. 13:** το προσωπικό ασφαλείας πρέπει να έχει επίγνωση και κατάλληλους ελέγχους για	**Άρθρο 12:** οι ελεγκτές πρέπει να είναι διαφανείς όσον αφορά τις δραστηριότητες της επεξεργασίας και να παρέχουν σαφώς κατανοητές πληροφορίες όταν τα υποκείμενα των δεδομένων ασκούν τα δικαιώματά τους. **Άρθρο 13:** οι ελεγκτές ανταλλάσσουν ορισμένες πληροφορίες με τα υποκείμενα των δεδομένων κατά τη στιγμή της συλλογής, συμπεριλαμβανομένων: Τα στοιχεία επικοινωνίας του ελεγκτή και του ΥΠΔ. Τον σκοπό και τις νομικές βάσεις για την επεξεργασία προσωπικών δεδομένων. Τρίτους αποδέκτες των προσωπικών δεδομένων. Πληροφορίες σχετικά με τυχόν διεθνείς διαβιβάσεις των δεδομένων. Την Περίοδο διατήρησης των δεδομένων. Την ύπαρξη των δικαιωμάτων του υποκειμένου των δεδομένων. **Άρθρο 14:** τα υποκείμενα των δεδομένων δικαιούνται να λαμβάνουν ορισμένες κοινοποιήσεις όταν τα δεδομένα τους λαμβάνονται από τρίτα μέρη. **Άρθρο 15:** τα υποκείμενα των δεδομένων δικαιούνται να λαμβάνουν ορισμένες πληροφορίες κατόπιν αιτήματος, συμπεριλαμβανομένων: Τους σκοπούς των δραστηριοτήτων επεξεργασίας του υπευθύνου	Για τους υπεύθυνους της ασφάλειας, η ανταλλαγή πληροφοριών σχετικά με την επεξεργασία δεδομένων με τους καταναλωτές είναι πιθανόν να είναι αντίθετη στην εκπαίδευσή τους για την ασφάλεια των πληροφοριών. Ωστόσο, ο GDPR ορίζει ότι οι ελεγκτές είναι ανοικτοί και διαφανείς σχετικά με τις πρακτικές επεξεργασίας δεδομένων τους και επιτρέπουν ακόμη και στα υποκείμενα των δεδομένων τη δυνατότητα να αποκτούν πρόσβαση στα δεδομένα τους μέσω ασφαλών αυτοματοποιημένων μέσων, εάν είναι εφικτό. Οι ομάδες απορρήτου θα πρέπει να συνεργαστούν στενά με τους υπεύθυνους ασφαλείας για να κατανοήσουν τις κατηγορίες των δεδομένων που συλλέγονται και αποθηκεύονται, καθώς και τις αντίστοιχες πολιτικές διατήρησης. Θα χρειαστούν επίσης βοήθεια για την καταγραφή των εξωτερικών μερών με τα οποία κοινοποιούνται τα δεδομένα, συμπεριλαμβανομένης οποιασδήποτε μεταφοράς και αποθήκευσης εκτός της ΕΕ. Οι πολιτικές επεξεργασίας που απαιτούνται από το ISO 27001 είναι κρίσιμες για την παροχή στις

την ασφάλεια των πληροφοριών που διαβιβάζονται εκτός του οργανισμού.	επεξεργασίας. Τις κατηγορίες των δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία. Τους αποδέκτες των δεδομένων, συμπεριλαμβανομένων των τρίτων. Την περίοδο διατήρησης δεδομένων. Την ύπαρξη των δικαιωμάτων του υποκειμένου των δεδομένων. Πληροφορίες σχετικά με την αρχική προέλευση των δεδομένων, αν όχι ο ελεγκτής. Την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων. Ο υπεύθυνος επεξεργασίας παρέχει αντίγραφο των δεδομένων που υποβάλλονται σε επεξεργασία. **Άρθρο 16:** τα υποκείμενα των δεδομένων έχουν το δικαίωμα να διορθώσουν ανακριβή προσωπικά δεδομένα σχετικά με αυτά. **Άρθρο 17:** τα δεδομένα των υποκειμένων θα πρέπει να διαγράφονται χωρίς αδικαιολόγητη καθυστέρηση όταν τα δεδομένα δεν είναι πλέον απαραίτητα για τον σκοπό για τον οποίο συλλέχθηκαν ή όταν ανακαλείται η συγκατάθεση για μεταποίηση ή το υποκείμενο των δεδομένων αντιτίθεται στην επεξεργασία για ορισμένους λόγους ή όταν τα δεδομένα έχουν υποστεί παράνομη επεξεργασία. **Άρθρο 18: τα** υποκείμενα των δεδομένων έχουν το δικαίωμα να υποχρεώνουν τον υπεύθυνο επεξεργασίας να περιορίζει την επεξεργασία των δεδομένων του υπό συγκεκριμένες συνθήκες. **Άρθρο 19:** ο υπεύθυνος επεξεργασίας πρέπει να παρέχει ειδοποίηση στα υποκείμενα των δεδομένων σε περίπτωση διόρθωσης,	πληροφορίες των υποκειμένων των δεδομένων ακριβών πληροφοριών σχετικά με τις δραστηριότητες επεξεργασίας. Οι υπεύθυνοι ασφαλείας μπορούν να παράσχουν σημαντική υποστήριξη στην ομάδα απορρήτου για να ανταποκριθούν στα υποκείμενα των δεδομένων που ζητούν πρόσβαση, διόρθωση, διαγραφή ή ακόμα και φορητότητα των προσωπικών τους δεδομένων. Οι δραστηριότητες αυτές παρουσιάζουν εγγενώς κινδύνους για την ασφάλεια των συστημάτων πληροφοριών, εάν δεν αντιμετωπίζονται προσεκτικά. Έτσι, η ομάδα απορρήτου θα πρέπει να συνεργαστεί με την ομάδα ασφαλείας για τα συστήματα δόμησης για την ανταπόκριση σε αιτήματα υποκειμένων δεδομένων με τρόπο που να πιστοποιεί το υποκείμενο των δεδομένων – ο GDPR φυσικά απαιτεί από τα υποκείμενα των δεδομένων να μπορούν να βλέπουν μόνο τα δικά τους δεδομένα και να εξακριβώνεται η ταυτότητά τους σε περίπτωση υποβολής αιτήματος. Η ομάδα απορρήτου θα πρέπει επίσης να βασιστεί σε προγραμματιστές και υπεύθυνους ασφαλείας που θα διευκολύνουν την αυτοματοποιημένη πρόσβαση, διόρθωση και ίσως ακόμη και διαγραφή των δεδομένων. Η ομάδα ασφαλείας μπορεί επίσης να βοηθήσει με τη δημιουργία αρχείων αυτών των αιτημάτων για την έγκαιρη ανταπόκριση. Οι ομάδες ασφαλείας που ακολουθούν την

	διαγραφής ή περιορισμού. **Άρθρο 20:** τα υποκείμενα των δεδομένων μπορούν να ζητήσουν τη διαβίβαση δεδομένων προσωπικού χαρακτήρα μεταξύ ελεγκτών όταν αυτό είναι εφικτό. **Άρθρο 21:** τα υποκείμενα των δεδομένων μπορούν να αντιταχθούν στη γενική επεξεργασία των προσωπικών τους δεδομένων, συμπεριλαμβανομένης της κατάρτισης προφίλ και του μάρκετινγκ. **Άρθρο 22:** τα υποκείμενα των δεδομένων έχουν το δικαίωμα να μην υπόκεινται σε αυτοματοποιημένη λήψη αποφάσεων.	ταξινόμηση και τις λειτουργικές διαδικασίες ISO 27001 πρέπει να είναι καλά τοποθετημένες για να βοηθήσουν σε αυτές τις προσπάθειες. Ωστόσο, η ταξινόμηση, τα δικαιώματα πρόσβασης και οι λειτουργικές διαδικασίες ενδέχεται να χρειαστεί να αναθεωρηθούν με την ομάδα απορρήτου και να ενημερωθούν όσο είναι απαραίτητο για να εξασφαλιστεί ότι οι κατάλληλες πληροφορίες παρέχονται στα υποκείμενα των δεδομένων κατά τη στιγμή της συλλογής και κατόπιν αιτήματος.

Οι οργανισμοί που θα έχουν στην κατοχή τους το ISO 27001 και πολιτικές θα μπορούν να έχουν μια βάση για την εξασφάλιση πιο αποτελεσματικών απαντήσεων στα δικαιώματα του υποκειμένου των δεδομένων στο πλαίσιο του GDPR. Οι απαιτήσεις απογραφής και ταξινόμησης του ISO 27001 θα επιτρέψουν στις ομάδες ασφαλείας να υποστηρίξουν τους υπεύθυνους του ιδιωτικού απορρήτου στην αντιστοίχιση και απογραφή δεδομένων και στην περιγραφή στα υποκείμενα των δεδομένων τις κατηγορίες πληροφοριών σχετικά με αυτά και τον τρόπο επεξεργασίας τους, καθώς και σε αυτούς στους οποίους μεταφέρεται. Οι υπεύθυνοι ασφαλείας θα είναι απαραίτητοι για τη διαχείριση των στοιχείων διασφαλίζοντας ότι χρησιμοποιούνται τα κατάλληλα δικαιώματα και εφαρμόζονται πολιτικές προειδοποίησης και αναθεώρησης.

4.7 Λογικό διάγραμμα

Στον παρακάτω πίνακα εμφανίζεται ένα διάγραμμα που αποτυπώνει την αλληλοκάλυψη που υπάρχει μεταξύ του ISO 27001 και GDPRκαι τους τομείς που στους οποίους πραγματοποιείται.

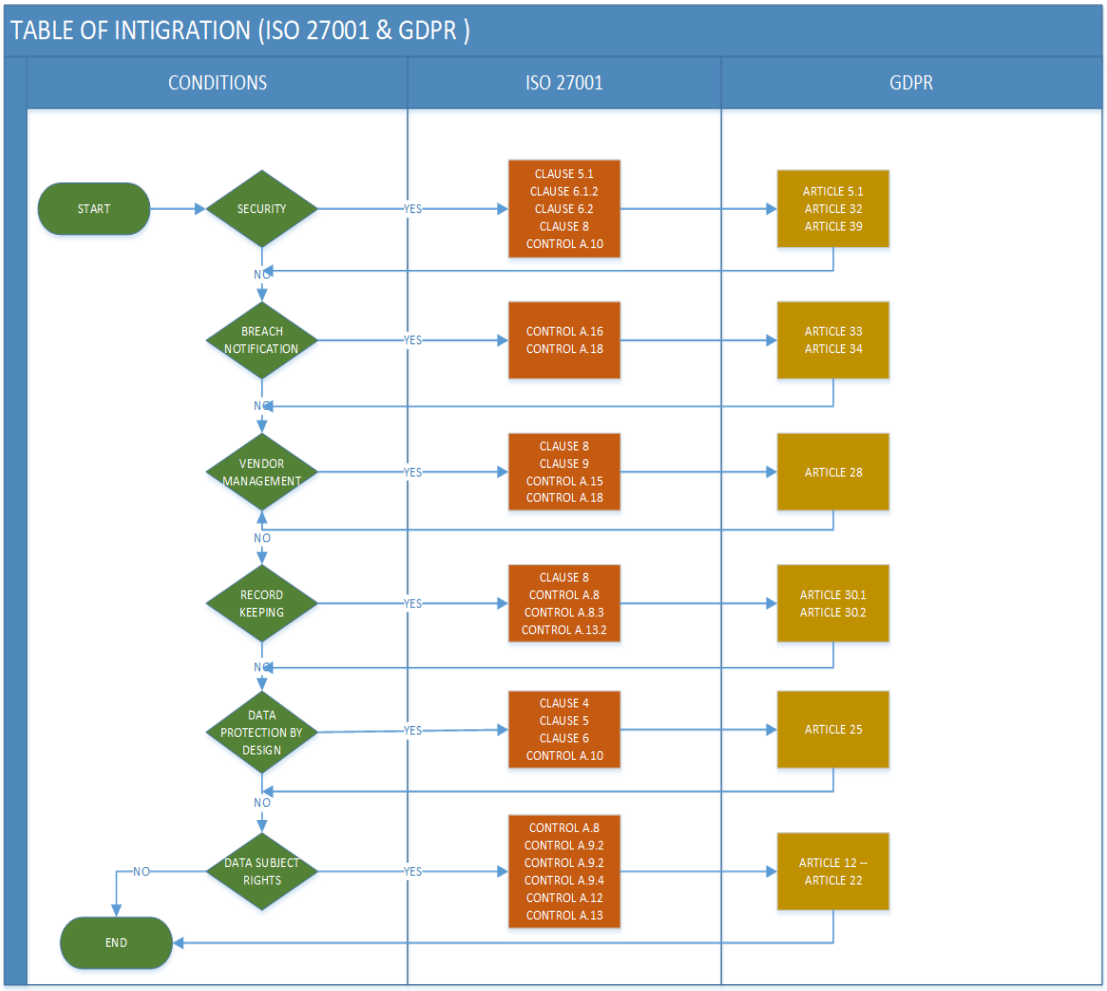
TABLE OF INTIGRATION (ISO 27001 & GDPR)
CONDITIONS
ISO 27001
GDPR
START
SECURITY
YES
CLAUSE 5.1
CLAUSE 6.1.2
CLAUSE 6.2
CLAUSE 8
CONTROL A.10
ARTICLE 5.1
ARTICLE 32
ARTICLE 39
NO
BREACH NOTIFICATION
YES
CONTROL A.16
CONTROL A.18
ARTICLE 33
ARTICLE 34
NO
VENDOR MANAGEMENT
YES
CLAUSE 8
CLAUSE 9
CONTROL A.15
CONTROL A.18
ARTICLE 28
NO
RECORD KEEPING
YES
CLAUSE 8
CONTROL A.8
CONTROL A.8.3
CONTROL A.13.2
ARTICLE 30.1
ARTICLE 30.2
NO
DATA PROTECTION BY DESIGN
YES
CLAUSE 4
CLAUSE 5
CLAUSE 6
CONTROL A.10
ARTICLE 25
NO
DATA SUBJECT RIGHTS
YES
CONTROL A.8
CONTROL A.9.2
CONTROL A.9.2
CONTROL A.9.4
CONTROL A.12
CONTROL A.13
ARTICLE 12 -- ARTICLE 22
NO
END

Πίνακας 14

5. ΣΥΜΠΕΡΑΣΜΑ

Εκτός από τους εγκεκριμένους τεχνικούς ελέγχους, τη δομημένη τεκμηρίωση, την παρακολούθηση και τη συνεχή βελτίωση, η εφαρμογή του ISO 27001 προωθεί μια κουλτούρα καθώς και την συνειδητοποίηση των συμβάντων ασφάλειας σε οργανισμούς. Οι υπάλληλοι αυτών των οργανισμών μέσω του ISO 27001 είναι σε θέση να έχουν μεγαλύτερη επίγνωση και περισσότερες γνώσεις για να μπορούν να ανιχνεύουν και να αναφέρουν τα συμβάντα ασφάλειας. Επίσης, στα πλαίσια και τις πολιτικές που έχουν ήδη αναπτυχθεί και υλοποιηθεί από ομάδες ασφαλείας μπορούν να εξορθολογήσουν και να απλοποιήσουν σημαντικά την ανάπτυξη νέων διαδικασιών προστασίας της ιδιωτικής ζωής που συμμορφώνονται με τον GDPR. Η ασφάλεια των πληροφοριών δεν αφορά μόνο την τεχνολογία, αλλά αφορά τους ανθρώπους και τις διαδικασίες.

Επίσης, σχεδόν οποιαδήποτε εταιρεία που δραστηριοποιείται σε διεθνές επίπεδο θα πρέπει να συμμορφωθεί με το πρότυπο του ISO 27001. Αυτό θα ωφελήσει τον οργανισμό σε δυο βασικούς της άξονες. Πρώτον , οι υπεύθυνοι ασφαλείας που είναι εξοικειωμένοι με το ISO 27001 πρέπει να βρίσκονται σε ένα ικανοποιητικό επίπεδο για να κατανοήσουν και να προσθέσουν αξία στα προγράμματα GDPR της ομάδας απορρήτου — και αντίστροφα. Δεύτερον το ISO 27001 αναγνωρίζεται διεθνώς και εφαρμόζεται σε όλο τον κόσμο και ίσως να αποτελεί την καλύτερη επιλογή για να συμμορφωθεί ένας οργανισμός με το GDPR της ΕΕ.

Τέλος με βάση όλη την παραπάνω ανάλυση γίνεται αντιληπτό ότι η ασφάλεια και η ιδιωτικότητα ενώ μπορεί να αναλύονται και να εμφανίζονται σε διαφορετικές παραγράφους και άρθρα είναι πολλές φορές αλληλένδετες και η επιτυχία της μίας είναι εξαρτώμενη από την άλλη.

6. ΒΙΒΛΙΟΓΡΑΦΙΑ

Advisera Expert Solutions Ltd. "Diagram of EU GDPR & ISO 27001 Integrated Implementation | Thank You." *ISO 9001, 13485, 14001, 45001, 20000, 27001, AS9100, IATF 16949 and ITIL Implementation*, info.advisera.com/eugdpracademy/free-download/diagram-of-eu-gdpr-and-iso-27001-integrated-implementation/thank-you?submissionGuid=11df447d-dc0d-4dfe-9231-ee7f3252a99c.

"Lex Access to European Union Law." *EUR*, eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32016R0679.

Department. "Guide to Undertaking Privacy Impact Assessments - Office of the Australian Information Commissioner (OAIC)." *OAIC*, Office of the Australian Information Commissioner, 5 Mar. 2018, www.oaic.gov.au/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments.

"Look for ISO 27001 Certification – The Gold Standard in Data Processing, IT & Communications." *ABP TECH*, www.abptech.com/look-iso-27001-certification-%E2%80%93-gold-standard-data-processing-it-communications.

"Τι Είναι Το GDPR;" *Techpress.gr*, www.techpress.gr/index.php/archives/96912.

"What Is General Data Protection Regulation (GDPR) - Definition from WhatIs.com." *WhatIs.com*, whatis.techtarget.com/definition/General-Data-Protection-Regulation-GDPR.

Graham, Annabelle. "What Is the ISO 27000 Series of Standards?" *IT Governance Blog*, 28 Mar. 2019, www.itgovernance.co.uk/blog/what-is-the-iso-27000-series-of-standards.

"Similarities and Differences between GDPR, ISO 27001 and Other Data Protection Regulations ." *YASH Technologies*, www.yash.com/blog/differences-between-gdpr-and-other-data-protection/.

"Free Guide: Achieve GDPR Compliance with ISO 27001." *IT Governance*, www.itgovernanceusa.com/free-download-gdpr-compliance-iso-27001.

"ISO 27001 v GDPR - Mapping." *Blog - ISO 27001 v GDPR - Mapping*, www.nqa.com/en-gb/resources/blog/november-2018/iso-27001-gdpr.

"How to Comply with the GDPR If You're Already ISO 27001-Compliant." *ManageEngine Blog*, 22 Jan. 2019, blogs.manageengine.com/it-security/2018/01/30/comply-gdpr-youre-already-iso-27001-compliant.html.