Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών

«Προηγμένα Συστήματα Πληροφορικής»

κατεύθυνση

Τεχνολογίες Διαχείρισης Ασφάλειας (ΤεΔΑ)

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	Πλαίσιο προετοιμασίας για το νέο κανονισμό της ΕΕ (2016/679) για την προστασία των προσωπικών δεδομένων. **Framework of preparation with the new EU regulation (2016/679) for the protection of personal data.**
Ονοματεπώνυμο Φοιτητή	ΠΡΟΚΟΠΙΟΣ ΣΤΑΜΑΤΙΟΥ
Πατρώνυμο	ΛΑΖΑΡΟΣ
Αριθμός Μητρώου	ΜΠΣΠ15082
Επιβλέπων	Χ. Δουληγέρης, Καθηγητής
Συνεπιβλέπων ερευνητής	Δρ. Εμμανουήλ Γεωργακάκης

Ημερομηνία Παράδοσης 2018

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Δουληγέρης Χρήστος Καθηγητής	Κοτζανικολάου Παναγιώτης Επίκουρος Καθηγητής	Ψαράκης Μιχαήλ Επίκουρος Καθηγητής

Περίληψη

Η εποχή των “big data” έχει αδιαμφισβήτητα φτάσει. Κάθε μέρα, πληθώρα προσωπικών πληροφοριών δημιουργείται και διαμοιράζεται από τα άτομα μέσω των συσκευών τους. Προσωπικά δεδομένα όπως η διεύθυνση τους, ο τηλεφωνικός τους αριθμός, οι πολιτικές τους απόψεις, οι πληροφορίες για την σεξουαλική τους ζωή, η εθνική ή φυλετική τους καταγωγή, ιατρικές πληροφορίες καθώς και πληροφορίες για τις τραπεζικές τους συναλλαγές μοιράζονται με οργανισμούς, στις περισσότερες των περιπτώσεων με τη συναίνεση των ατόμων. Οι οργανισμοί μπορούν να χρησιμοποιήσουν αυτά τα δεδομένα μόνο για ξεκάθαρους, νόμιμους και προσυμφωνημένους σκοπούς.

Παρ' όλα αυτά, σε πολλές περιπτώσεις, τα προσωπικά δεδομένα δεν χρησιμοποιούνται για τον σκοπό τον οποίο έχουν συλλεχθεί και για αυτόν τον λόγο η προστασία των προσωπικών δεδομένων είναι πλέον θέμα ζωτικής σημασίας.

Για την αντιμετώπιση αυτού του ζητήματος, το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο της Ευρωπαϊκής Ένωσης και η Ευρωπαϊκή Επιτροπή συνέταξαν τον γενικό κανονισμό για την προστασία των προσωπικών δεδομένων (2016/679) με σκοπό να ενδυναμώσουν και να ενοποιήσουν τις ενέργειες σχετικά με την προστασία των προσωπικών δεδομένων για όλα τα άτομα εντός της Ευρωπαϊκής Ένωσης.

Η παρούσα μεταπτυχιακή διατριβή ασχολείται με τις προκλήσεις που αντιμετωπίζει η ΕΕ όπως τα θέματα προστασίας των προσωπικών δεδομένων και οι παραβιάσεις αυτών, την σύγκριση του νέου κανονισμού 2016/679 με την προηγούμενη Ευρωπαϊκή οδηγία 95/46/EC και, επίσης, τη δημιουργία ενός πλαισίου προετοιμασίας το οποίο περιγράφει όλες τις απαραίτητες διαδικασίες που οι οργανισμοί χρειάζεται να εφαρμόσουν έτσι ώστε να επιτευχθεί η συμμόρφωση με το νέο κανονισμό.

Αυτό το πλαίσιο προετοιμασίας θα βοηθήσει τους οργανισμούς, έτσι ώστε να:

- ❏ Κατανοήσουν τους νέους κανόνες.
- ❏ Ενημερωθούν για τα σχετικά πρόστιμα σε περίπτωση μη συμμόρφωσης με τον νέο κανονισμό.
- ❏ Σχεδιάσουν τις απαραίτητες ενέργειες που χρειάζεται να εκτελεστούν έτσι ώστε ο οργανισμός να είναι συμμορφωμένος με το νέο κανονισμό.
- ❏ Εκτελέσουν τις παραπάνω ενέργειες μέσω ενός λεπτομερούς πλάνου εργασιών και ξεκάθαρων οδηγιών.

Στο τέλος αυτής της διαδικασίας ο εκάστοτε οργανισμός θα έχει επιτύχει τη συμμόρφωση με το νέο κανονισμό 2016/679, έχοντας εξοικονομήσει σημαντικό χρόνο και προσπάθεια.

Abstract

The “big data” future has undoubtedly arrived. Everyday a vast amount of information about a person’s life is created and made available through the use of their devices. Personal data such as their address, phone number, political opinions, sex life, racial or ethnic origin and medical or banking details are made available to persons and corporations, with consent in most of the cases. Those entities can use the personal data for specified and lawful purposes.

In many cases though, personal data can be misused and for that reason data protection has become a matter of vital importance.

To address this matter, the European Parliament, the Council of the European Union and the European Commission joined forces and compiled the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) in order to strengthen and unify data protection for all individuals within the European Union.

This master’s thesis deals with the challenges that the EU faces to address as data privacy issues and data breaches, the comparison between the GDPR 2016/679 and the previous EU Directive 95/46/EC and also the creation of a preparation framework that describes all the necessary processes that need to be implemented from an entity so that it is compliant with this new regulation.

The aforementioned preparation framework will help the institutions to:

- ❏ Understand the new rules.
- ❏ Get informed on the regulatory fines if they fail to comply with the new regulation.
- ❏ Plan the necessary actions to be performed so that the institution is compliant with the new regulation.
- ❏ Execute these actions through a detailed work plan/road map and clear guidelines.

At the end of this process, the institution will be compliant to the GDPR 2016/679 having saved a lot of time and effort.

1. Εισαγωγή

Στο παρόν κεφάλαιο αναφέρονται κάποιες βασικές έννοιες και ορισμοί που αφορούν τα δεδομένα προσωπικού χαρακτήρα και την προστασία τους, τις αυξανόμενες προκλήσεις στο κομμάτι της ασφάλειας των προσωπικών δεδομένων λόγο της ραγδαίας εξέλιξης της τεχνολογίας και παραδείγματα διαρροών προσωπικών δεδομένων λόγο της αποτυχίας να διαφυλαχθεί η ασφάλεια αυτών. Επίσης, στο κεφάλαιο αυτό περιγράφεται η υπάρχουσα οδηγία 95/46/ΕΚ της Ευρωπαϊκής ένωσης για την προστασία δεδομένων. Τέλος, παρουσιάζεται συνοπτικά το περιεχόμενο των υπόλοιπων κεφαλαίων, τα κίνητρα και οι στόχοι της παρούσας μεταπτυχιακής διατριβής.

1.1 Ορισμοί

«δεδομένα προσωπικού χαρακτήρα»: κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»)· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε κάποιο αναγνωριστικό στοιχείο ταυτότητας, όπως σε όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου [1]

«επεξεργασία»: κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή [1]

«περιορισμός της επεξεργασίας»: η επισήμανση αποθηκευμένων δεδομένων προσωπικού χαρακτήρα με στόχο τον περιορισμό της επεξεργασίας τους στο μέλλον [1]

«κατάρτιση προφίλ»: οποιαδήποτε μορφή αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα που συνίσταται στη χρήση δεδομένων προσωπικού χαρακτήρα για την αξιολόγηση ορισμένων προσωπικών πτυχών ενός φυσικού προσώπου, ιδίως για την ανάλυση ή την πρόβλεψη πτυχών που αφορούν την απόδοση στην εργασία, την οικονομική κατάσταση, την υγεία, τις προσωπικές προτιμήσεις, τα ενδιαφέροντα, την αξιοπιστία, τη συμπεριφορά, τη θέση ή τις μετακινήσεις του εν λόγω φυσικού προσώπου [1]

«ψευδωνυμοποίηση»: η επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο ώστε τα δεδομένα να μην μπορεί πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρωματικές πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλιστεί ότι δεν μπορεί να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο [1]

«σύστημα αρχειοθέτησης»: κάθε διαρθρωμένο σύνολο δεδομένων προσωπικού χαρακτήρα τα οποία είναι προσβάσιμα με γνώμονα συγκεκριμένα κριτήρια, είτε το σύνολο αυτό είναι συγκεντρωμένο είτε αποκεντρωμένο είτε κατανεμημένο σε λειτουργική ή γεωγραφική βάση [1]

«υπεύθυνος επεξεργασίας»: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα· όταν οι σκοποί και ο τρόπος της επεξεργασίας αυτής καθορίζονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια για τον διορισμό του μπορούν να προβλέπονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους [1]

«εκτελών την επεξεργασία»: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας [1]

«αποδέκτης»: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας, στα οποία

κοινολογούνται τα δεδομένα προσωπικού χαρακτήρα, είτε πρόκειται για τρίτον είτε όχι. [1]

1.2 Προκλήσεις

Η ιδιωτικότητα της πληροφορίας, ή των προσωπικών δεδομένων (ή η προστασία των δεδομένων) είναι η σχέση μεταξύ της συλλογής και διάδοσης των δεδομένων, της τεχνολογίας, της δημόσιας προσδοκίας για την ιδιωτικότητα και τα νομικά και πολιτικά θέματα γύρω από αυτά. Ανησυχίες για την ιδιωτικότητα υπάρχουν σε κάθε περίπτωση όπου προσωπικές αναγνωρίσιμες πληροφορίες ή άλλες ευαίσθητες πληροφορίες συλλέγονται, αποθηκεύονται, χρησιμοποιούνται και τελικά καταστρέφονται ή διαγράφονται - σε ψηφιακή ή μη μορφή. Ο λανθασμένος ή ανύπαρκτος έλεγχος για την αποκάλυψη ή τη γνωστοποίηση αυτών μπορεί να γίνει αιτία για θέματα ιδιωτικότητας. Θέματα ιδιωτικότητας μπορεί να προκύψουν σε πληροφορίες από μια ευρεία γκάμα πηγών, όπως:

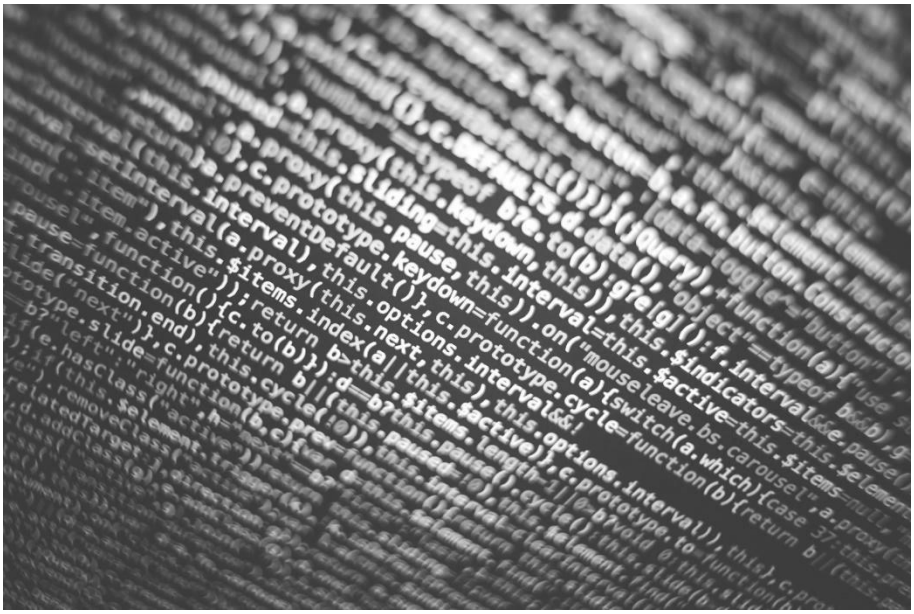
- Φάκελοι υγείας ασθενών
- Ποινικές έρευνες και τα αποτελέσματα τους
- Χρηματοπιστωτικά ιδρύματα και συναλλαγές
- Βιολογικά χαρακτηριστικά όπως γενετικό υλικό
- Κατοικία και γεωγραφικές πληροφορίες
- Παραβίαση της ιδιωτικής ζωής
- Υπηρεσίες που λειτουργούν με βάση την τοποθεσία
- Συμπεριφορά περιήγησης στο διαδίκτυο και προτιμήσεις χρηστών

Η πρόκληση της προστασίας των ιδιωτικών δεδομένων είναι η αξιοποίηση των δεδομένων, με ταυτόχρονη προστασία της ιδιωτικότητας και των προσωπικών στοιχείων κάθε ατόμου. Οι τομείς της ασφάλειας των υπολογιστών, της ασφάλειας των δεδομένων και της ασφάλειας της πληροφορίας σχεδιάζουν και χρησιμοποιούν λογισμικό, υλικό και ανθρώπινο δυναμικό έτσι ώστε να αντιμετωπίσουν αυτό το ζήτημα. Καθώς οι νόμοι και οι κανονισμοί σχετικά με την ιδιωτική ζωή και την προστασία των δεδομένων συνεχώς αλλάζουν, είναι πολύ σημαντικό να υπάρχει συνεχής ενημέρωση για τις εκάστοτε αλλαγές στην νομοθεσία. Επίσης πρέπει να επαναξιολογείται η συμμόρφωση με το απόρρητο των δεδομένων και τους κανονισμούς ασφαλείας.

1.3 Παραδείγματα διαρροών δεδομένων

Πηγαίνοντας πίσω στο χρόνο η διαρροή των προσωπικών δεδομένων ήταν πάντοτε ένα υπαρκτό φαινόμενο και σε γενικές γραμμές πρακτικά αδύνατον να αποφευχθεί ή καλύτερα να εξαλειφθεί 100%. Ωστόσο, με την εξέλιξη της τεχνολογίας ο όγκος των δεδομένων, η συχνότητα της ανταλλαγής των δεδομένων, της επεξεργασίας και της αποθήκευσής τους έχει μεγαλώσει σε υπερθετικό βαθμό. Αν σκεφτούμε μόνο ότι παλαιότερα τα προσωπικά δεδομένα ενός φυσικού προσώπου τα οποία αποθηκεύονταν από τρίτους, ιδιωτικές εταιρίες, δημόσιες υπηρεσίες, ήταν μόνο για σημαντικά γεγονότα της ζωής τους ενώ πλέον τα ίδια αυτά προσωπικά δεδομένα αποθηκεύονται, προσπελάζονται και επεξεργάζονται σε πιο απλές καθημερινές συνήθειες της ζωής μας, για παράδειγμα τις μεταφορές, τις ηλεκτρονικές παραγγελίες, ακόμα και τις διαφημίσεις. Μπορούμε, λοιπόν, εύκολα να συμπεράνουμε τον πολλαπλάσιο όγκο προσωπικών δεδομένων που διακινούνται καθημερινά στο διαδίκτυο. Ως εκ τούτου, είναι ξεκάθαρη η ανάγκη προστασίας των προσωπικών στοιχείων κάθε ατόμου, η ανάγκη μιας ασφαλούς διαδικασίας κατά την επεξεργασία των δεδομένων και η διασφάλιση ότι αυτά τα δεδομένα θα παραμείνουν ιδιωτικά και δεν θα αποκαλυφθούν.

Εικόνα 1



Παρακάτω αναφέρονται κάποιες γνωστές διαρροές προσωπικών δεδομένων [2]. Θα παρατηρήσουμε ότι οι διαρροές αυτές δεν είναι πάντα αποτέλεσμα μιας κακόβουλης πράξης ενός τρίτου προσώπου άλλα και αποτέλεσμα κακής διαχείρισης και συμμόρφωσης των οργανισμών με τους κανονισμούς της προστασίας των προσωπικών δεδομένων.

Πίνακας 1 - Γνωστές διαρροές προσωπικών δεδομένων από επιθέσεις ή ανθρώπινη αμέλεια

#1	**Περιγραφή συμβάντος:** Μια βάση δεδομένων με 191 εκατομμύρια ψηφοφόρους εκτέθηκε στο διαδίκτυο λόγω εσφαλμένης ρύθμισης στις παραμέτρους της βάσης δεδομένων. Η βάση δεδομένων περιελάμβανε ονόματα, διευθύνσεις, ημερομηνίες γέννησης, κομματική ένταξη, αριθμούς τηλεφώνου και διευθύνσεις ηλεκτρονικού ταχυδρομείου των ψηφοφόρων σε όλες τις πολιτείες των ΗΠΑ. **Οργανισμός/εταιρία:** NationBuilder **Όγκος δεδομένων:** προσωπικές πληροφορίες ~191.000.000 Αμερικανών ψηφοφόρων **Μέθοδος διαρροής:** εσφαλμένη ρύθμιση παραμέτρων της βάσης δεδομένων
#2	**Περιγραφή συμβάντος:** Οι δυο επιθέσεις στην Yahoo τα έτη 2013 και 2014 αποκάλυψαν προσωπικά δεδομένα περίπου 1,5 δισεκατομμυρίου χρηστών. Μεταξύ των πληροφοριών που εκτέθηκαν ήταν ονόματα, αριθμοί τηλεφώνων, ημερομηνίες γέννησης, κρυπτογραφημένοι κωδικοί πρόσβασης και ερωτήσεις ασφαλείας χωρίς κρυπτογράφηση. Ερωτήσεις που θα μπορούσαν να χρησιμοποιηθούν για να επαναφέρουν, οι επιτιθέμενοι, τους κωδικούς πρόσβασης. **Οργανισμός/εταιρία:** Yahoo **Όγκος δεδομένων:** ~ 1,5 δισεκατομμύρια λογαριασμοί χρηστών **Μέθοδος διαρροής:** κακόβουλη επίθεση

#3	**Περιγραφή συμβάντος:** Ένας πραγματικά μεγάλος αριθμός κωδικών πρόσβασης χρηστών της εταιρίας MySpace βρέθηκε να πωλείται στο διαδίκτυο. Το σχετικό αρχείο περιελάμβανε για κάθε εγγραφή μια διεύθυνση ηλεκτρονικού ταχυδρομείου, ένα όνομα χρήστη, έναν κωδικό πρόσβασης και σε ορισμένες περιπτώσεις και ένα δεύτερο κωδικό πρόσβασης. **Οργανισμός/εταιρία:** MySpace **Όγκος δεδομένων:** ~ 427.000.000 κωδικοί πρόσβασης χρηστών **Μέθοδος διαρροής:** Η μέθοδος της διαρροής δεν επιβεβαιώθηκε
#4	**Περιγραφή συμβάντος:** Νότιος Κορέα - Εκλάπησαν προσωπικά δεδομένα τουλάχιστον 20 εκατομμυρίων χρηστών τραπεζών και πιστωτικών καρτών. Ένας εργαζόμενος συνελήφθη και κατηγορήθηκε για την κλοπή των δεδομένων από τους πελάτες των τριών εταιρειών πιστωτικών καρτών. Τα προσωπικά δεδομένα τα όποια εκλάπησαν περιλάμβαναν τα ονόματα των πελατών, αριθμούς κοινωνικής ασφάλισης, αριθμούς τηλεφώνων, αριθμούς πιστωτικών καρτών και ημερομηνίες λήξης των πιστωτικών καρτών **Οργανισμός/εταιρία:** KB Kookmin Card, Lotte Card and NH Nonghyup Card **Όγκος δεδομένων:** ~20.000.000 χρήστες του πιστοληπτικού συστήματος της Νότιας Κορέας **Μέθοδος διαρροής:** Κλοπή δεδομένων εκ' των έσω

1.4 Υπάρχουσα οδηγία 95/46/ΕΚ

Η 95/46/ΕΚ [3] είναι μια οδηγία που εγκρίθηκε από την Ευρωπαϊκή Ένωση με σκοπό την προστασία της ιδιωτικής ζωής και την προστασία όλων των προσωπικών δεδομένων που συλλέγονται και είναι σχετικά με τους πολίτες της ΕΕ. Πιο συγκεκριμένα, στοχεύει στην προστασία των δεδομένων κατά την επεξεργασία, τη χρήση ή την ανταλλαγή αυτών Η οδηγία 95/46/ΕΚ, περιλαμβάνει όλα τα βασικά στοιχεία από το άρθρο 8 της Ευρωπαϊκής Σύμβασης για τα Ανθρώπινα Δικαιώματα το οποίο πρακτικά ορίζει των σεβασμό στα δικαιώματα της ιδιωτικής ζωής, προσωπικής και/ή οικογενειακής, καθώς και στην προσωπική αλληλογραφία Η οδηγία βασίζεται στις κατευθυντήριες γραμμές για την προστασία της ιδιωτικής ζωής και τις διασυνοριακές ροές δεδομένων προσωπικού χαρακτήρα όπως αυτές διατυπώθηκαν από τον Οργανισμό Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ) το 1980.

Οι κατευθυντήριες γραμμές/συστάσεις βασίζονται σε επτά αρχές οι οποίες κατοχυρώνονται στην οδηγία 94/46/ΕΚ της ΕΕ:

- **Σημείωση**: άτομα των οποίων τα δεδομένα συλλέγονται, θα πρέπει να ειδοποιούνται για την συλλογή των προσωπικών τους δεδομένων.
- **Σκοπός**: τα δεδομένα που συλλέγονται θα πρέπει να χρησιμοποιούνται μόνο για συγκεκριμένους δηλωμένους σκοπούς και για κανέναν άλλο σκοπό.
- **Συγκατάθεση**: τα προσωπικά δεδομένα δεν θα πρέπει να γνωστοποιούνται ή να μοιράζονται σε τρίτους χωρίς την συγκατάθεση του ατόμου στο οποίο ανήκουν τα δεδομένα.
- **Ασφάλεια**: τα προσωπικά δεδομένα που συλλέγονται θα πρέπει να διατηρούνται ασφαλή από πιθανή κατάχρηση, κλοπή ή απώλεια.
- **Αποκάλυψη**: τα άτομα των οποίων τα προσωπικά δεδομένα συλλέγονται, θα πρέπει να ενημερώνονται ως προς το ποιος(-οί) συλλέγουν τα δεδομένα.
- **Πρόσβαση**: τα άτομα των οποίων τα προσωπικά δεδομένα συλλέγονται, θα πρέπει να έχουν πρόσβαση στα προσωπικά τους δεδομένα και το δικαίωμα να τα διορθώσουν εάν υπάρχει τυχόν

ανακρίβεια.

- **Λογοδοσία**: τα άτομα των οποίων τα προσωπικά δεδομένα συλλέγονται, θα πρέπει να είναι σε θέση να θεωρήσουν τους συλλέκτες των προσωπικών τους δεδομένων υπόλογους για την μη τήρηση όλων των επτά αυτών των αρχών.

1.5 Κίνητρα και στόχοι

Στόχος της παρούσας μεταπτυχιακής διατριβής είναι η δημιουργία ενός πλαισίου για την προετοιμασία των οργανισμών με τον νέο κανονισμό της ευρωπαϊκής κοινότητας για την προστασία και επεξεργασία των προσωπικών δεδομένων. Για την υλοποίηση του πλαισίου θα γίνει μελέτη της τρέχουσας οδηγίας και του νέου κανονισμού και θα εντοπιστούν οι βασικές διάφορες μεταξύ τους. Η υλοποίηση του πλαισίου θα επικεντρωθεί στο κομμάτι των απαραίτητων διαδικασιών για την επίτευξη της εναρμόνισης των οργανισμών με τον νέο κανονισμό και στις απαραίτητες τεχνικές εφαρμογές και ρυθμίσεις. Το πλαίσιο προετοιμασίας θα συνοδεύεται από ένα πλάνο εργασιών για την ταχύτερη και ορθότερη υλοποίηση των απαραίτητων ενεργειών από την αρχή μέχρι και το τέλος

2. Ο νέος κανονισμός 2016/679

Εικόνα 2

Ο νέος Ευρωπαϊκός Κανονισμός 2016/679 ψηφίστηκε στις 27 Απριλίου του 2016 και θα τεθεί σε υποχρεωτική εφαρμογή για όλα τα κράτη μέλη της Ευρωπαϊκής Ένωσης στις 25 Μαΐου του 2018. Ο 2016/679 δεν πρόκειται για μια νέα ευρωπαϊκή οδηγία άλλα για κανονισμό της Ευρωπαϊκής Ένωσης. Με την εφαρμογή του 2016/679 έρχεται και η κατάργηση των υφιστάμενων κανονισμών και νομοθεσιών αφού δεν υπάρχει πλέον η ανάγκη της ψήφισης τοπικής εθνικής νομοθεσίας από την εκάστοτε χώρα της Ευρωπαϊκής Ένωσης. Δυο σημαντικά χαρακτηριστικά του 2016/679 είναι ότι αυξάνει σημαντικά τις απαιτήσεις που τίθενται στους οργανισμούς που επεξεργάζονται προσωπικά δεδομένα καθώς επίσης και το μέγεθος των κυρώσεων στις περιπτώσεις μη συμμόρφωσης των οργανισμών με τον κανονισμό.

Το αντικείμενο του 2016/679 είναι η διαμόρφωση ενός ενιαίου νομικού πλαισίου για την επεξεργασία προσωπικών δεδομένων στα κράτη μέλη της Ευρωπαϊκής Ένωσης, θέτοντας μία σειρά περιορισμών και νέων υποχρεώσεων στις επιχειρήσεις σχετικά με:

- την επεξεργασία των προσωπικών δεδομένων σε όλο τον κύκλο ζωής τους, από τη συλλογή έως και την καταστροφή τους,
- τη δυνατότητα μεταφοράς τους σε άλλες χώρες,
- την προστασία των δικαιωμάτων των φυσικών προσώπων,
- την ασφάλεια (εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα) των προσωπικών δεδομένων,
- τις ενέργειες γνωστοποίησης που οφείλει να κάνει η επιχείρηση σε περίπτωση παραβίασης.

Αξιοσημείωτο χαρακτηριστικό του νέου κανονισμού είναι τα σημαντικά αυξημένα πρόστιμα, τα οποία μπορεί να φτάσουν μέχρι και τα 20 εκατομμύρια ευρώ ή το 4% του παγκόσμιου ετήσιου τζίρου μιας επιχείρησης.

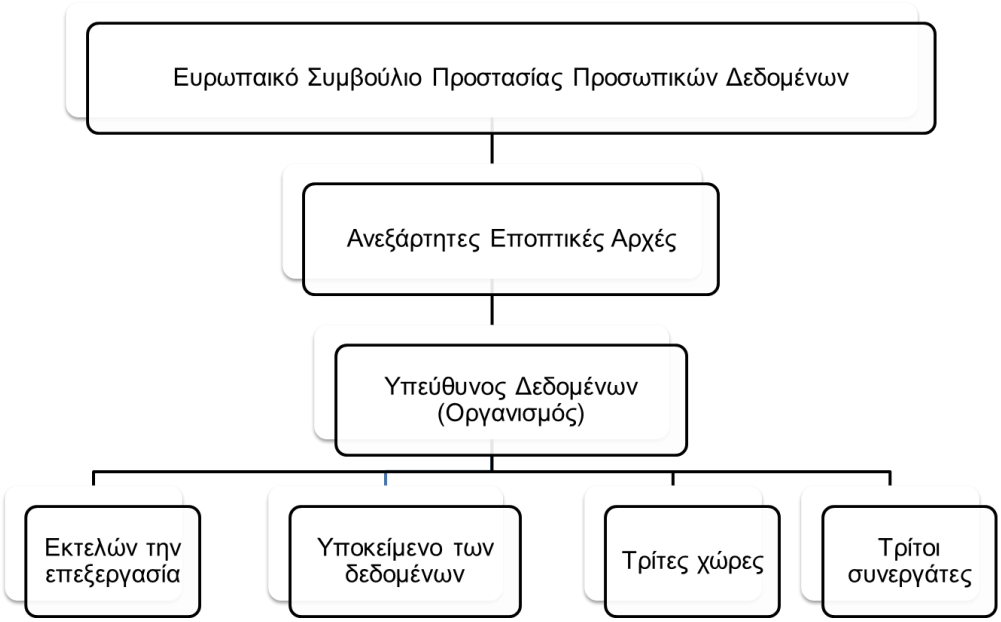
Ο 2016/679 αφορά όλες τις ιδιωτικές και δημόσιες επιχειρήσεις, καθώς και τις κρατικές αρχές που με οποιοδήποτε τρόπο διαχειρίζονται δεδομένα προσωπικού χαρακτήρα πελατών, πελατών των πελατών τους, εργαζομένων, συνεργατών ή άλλων φυσικών προσώπων. Ως εκ τούτου, ο 2016/679 αφορά

πρακτικά όλες τις επιχειρήσεις, εντός και εκτός Ευρωπαϊκής Ένωσης, εφόσον τα δεδομένα αφορούν Ευρωπαίους πολίτες.

Τα απαιτούμενα από τον 2016/679 μέτρα, πολιτικές και διαδικασίες ασφάλειας δεδομένων και επιχειρησιακής συνέχειας καθορίζονται από τα εξής διεθνή πρότυπα και οδηγίες:

- ISO 27001, το βασικό διεθνές πρότυπο για την ασφάλεια πληροφοριών
- ISO 22301, το διεθνές πρότυπο για την επιχειρησιακή συνέχεια
- PCI, το διεθνές πρότυπο για τις επιχειρήσεις που διαχειρίζονται δεδομένα καρτών πληρωμών
- ISO 27018, οδηγία για την προστασία των προσωπικών δεδομένων στο υπολογιστικό νέφος
- ISO 27017, οδηγία για την ασφάλεια των δεδομένων στην παροχή υπηρεσιών μέσω υπολογιστικού νέφους
- ISO 27799, οδηγία για την ασφάλεια των δεδομένων υγείας
- ISO 27011, οδηγία για την ασφάλεια των δεδομένων στους τηλεπικοινωνιακούς οργανισμούς
- ISO 27015, οδηγία για την ασφάλεια δεδομένων στις οικονομικές υπηρεσίες.

Εικόνα 3 – Δομή των νέων εποπτικών αρχών μέχρι και τους οργανισμούς με βάση τον νέο κανονισμό



2.1 Τα δικαιώματα του υποκειμένου των δεδομένων

Με τον 2016/679 και τα άρθρα 12 έως 23, τα όποια περιλαμβάνονται σε αυτόν, περιγράφονται τα δικαιώματα του υποκειμένου των δεδομένων. Το υποκείμενο των δεδομένων δικαιούται να γνωρίζει με πλήρη διαφάνεια εάν τα προσωπικά του δεδομένα συλλέγονται ή όχι από κάποιο μέσο. Εφόσον τα δεδομένα του υποκειμένου συλλέγονται πρέπει το υποκείμενο να διατηρεί το δικαίωμα πρόσβασης στα δεδομένα του όπως επίσης το δικαίωμα στον περιορισμό της επεξεργασίας αυτών, την διόρθωση και την διαγραφή τους. Επιπροσθέτως, εφόσον τα δεδομένα του υποκειμένου συλλέγονται, το υποκείμενο δικαιούται να διατηρεί το δικαίωμα στη φορητότητα των δεδομένων του καθώς και της αυτοματοποιημένης ατομικής λήψης αποφάσεων γι'αυτά τα δεδομένα, περιλαμβανομένης της κατάρτισης προφίλ.

2.1.1 Διαφάνεια και ρυθμίσεις

Για να είναι σε θέση το υποκείμενο των δεδομένων να ασκήσει τα δικαιώματά του, ο υπεύθυνος επεξεργασίας θα πρέπει:

- ❑ Να διαθέτει στο υποκείμενο των δεδομένων κάθε πληροφορία σχετικά με την επεξεργασία των προσωπικών του δεδομένων
- ❑ Να διαθέτει στο υποκείμενο των δεδομένων κάθε δικαίωμα πρόσβασης, διόρθωσης, διαγραφής, περιορισμού της επεξεργασίας, φορητότητας των δεδομένων και εναντίωσης.
- ❑ Να διευκολύνει την άσκηση των δικαιωμάτων του υποκειμένου των δεδομένων και να μην αρνείται να ενεργήσει κατόπιν αιτήσεως του υποκειμένου των δεδομένων εκτός και αν δεν είναι σε θέση να εξακριβώσει την ταυτότητά του.
- ❑ Να παρέχει στο υποκείμενο των δεδομένων πληροφορίες για τα αιτήματά του, χωρίς καθυστέρηση, μέσα σε ένα μήνα από την παραλαβή του αιτήματος. Η προθεσμία αυτή μπορεί να παραταθεί κατά 2 ακόμη μήνες, εφόσον λαμβάνεται υπόψη η πολυπλοκότητα του αιτήματος και ο αριθμός των αιτημάτων.
- ❑ Να παρέχει δωρεάν τις πληροφορίες προς το υποκείμενο των δεδομένων για τα αιτήματά του. Στην περίπτωση που τα αιτήματα είναι αβάσιμα ή υπερβολικά τότε ο υπεύθυνος επεξεργασίας έχει δικαίωμα να επιβάλει την καταβολή εύλογου τέλους ή να αρνηθεί να δώσει συνέχεια στο αίτημα.

Οι πληροφορίες που πρέπει να παρέχονται στα υποκείμενα των δεδομένων, θα πρέπει να είναι σαφώς διατυπωμένες ιδίως όταν απευθύνονται σε παιδιά και να παρέχονται γραπτώς ή με άλλα μέσα.

Αν ο υπεύθυνος επεξεργασίας έχει εύλογες αμφιβολίες σχετικά με την ταυτότητα του φυσικού προσώπου που υποβάλλει το αίτημα, μπορεί να ζητήσει την παροχή πρόσθετων πληροφοριών για την επιβεβαίωση της ταυτότητας του υποκειμένου των δεδομένων. Ο υπεύθυνος επεξεργασίας παρέχει τις πληροφορίες το αργότερο εντός ενός μηνός.

2.1.2 Ενημέρωση και πρόσβαση σε δεδομένα προσωπικού χαρακτήρα

2.1.2.1 Συλλογή δεδομένων κατευθείαν από το υποκείμενο των δεδομένων

Το υποκείμενο των δεδομένων δικαιούται να λαμβάνει από τον υπεύθυνο επεξεργασίας τις παρακάτω πληροφορίες για τα δεδομένα προσωπικού χαρακτήρα που συλλέγονται κατευθείαν από τον ίδιο:

- ❑ Την ταυτότητα και τα στοιχεία επικοινωνίας του υπευθύνου επεξεργασίας
- ❑ Τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων.

- ❑ Οι σκοποί της επεξεργασίας για τους οποίους προορίζονται τα δεδομένα προσωπικού χαρακτήρα.
- ❑ Εάν η επεξεργασία είναι σύννομη, τα έννομα συμφέροντα που επιδιώκονται από τον υπεύθυνο επεξεργασίας ή από τρίτο.
- ❑ Τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων προσωπικού χαρακτήρα, εάν υπάρχουν.
- ❑ Κατά περίπτωση, την πρόθεση του υπευθύνου επεξεργασίας να διαβιβάσει δεδομένα προσωπικού χαρακτήρα σε τρίτη χώρα ή διεθνή οργανισμό και την ύπαρξη ή την απουσία απόφασης επάρκειας της Επιτροπής.

Επιπροσθέτως, ο υπεύθυνος επεξεργασίας, υποχρεούται να παρέχει στο υποκείμενο των δεδομένων τις εξής επιπλέον πληροφορίες για την εξασφάλιση θεμιτής και διαφανούς επεξεργασίας:

- ❑ Το χρονικό διάστημα για το οποίο θα αποθηκευτούν τα δεδομένα προσωπικού χαρακτήρα.
- ❑ Την ύπαρξη δικαιώματος υποβολής αιτήματος στον υπεύθυνο επεξεργασίας για πρόσβαση και διόρθωση ή διαγραφή των δεδομένων προσωπικού χαρακτήρα ή περιορισμό της επεξεργασίας που αφορούν το υποκείμενο των δεδομένων ή δικαιώματος αντίταξης στην επεξεργασία, καθώς και δικαιώματος στη φορητότητα των δεδομένων.
- ❑ Την ύπαρξη δικαιώματος να ανακαλέσει τη συγκατάθεσή του οποτεδήποτε, χωρίς να θιγεί η νομιμότητα της επεξεργασίας που βασίστηκε στη συγκατάθεση πριν από την ανάκλησή της,
- ❑ Το δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή.
- ❑ Κατά πόσο η παροχή δεδομένων προσωπικού χαρακτήρα αποτελεί νομική ή συμβατική υποχρέωση ή απαίτηση για τη σύναψη σύμβασης, καθώς και κατά πόσο το υποκείμενο των δεδομένων υποχρεούται να παρέχει τα δεδομένα προσωπικού χαρακτήρα και ποιες ενδεχόμενες συνέπειες θα είχε η μη παροχή των δεδομένων αυτών.
- ❑ Την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ καθώς και τη σημασία και τις προβλεπόμενες συνέπειες της εν λόγω επεξεργασίας για το υποκείμενο των δεδομένων.

Όταν ο υπεύθυνος επεξεργασίας προτίθεται να επεξεργαστεί περαιτέρω τα δεδομένα προσωπικού χαρακτήρα για άλλο σκοπό από εκείνο για τον οποίο συλλέχθηκαν τα δεδομένα προσωπικού χαρακτήρα, υποχρεούται να παρέχει στο υποκείμενο των δεδομένων πληροφορίες για τον σκοπό αυτόν.

2.1.2.2 Έμμεση συλλογή δεδομένων από το υποκείμενο των δεδομένων

Το υποκείμενο των δεδομένων δικαιούται να λαμβάνει από τον υπεύθυνο επεξεργασίας τις παρακάτω πληροφορίες για τα δεδομένα προσωπικού χαρακτήρα που δεν συλλέγονται κατευθείαν από τον ίδιο:

- ❑ Την ταυτότητα και τα στοιχεία επικοινωνίας του υπευθύνου επεξεργασίας.
- ❑ Τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων.
- ❑ Τους σκοπούς της επεξεργασίας για τους οποίους προορίζονται τα δεδομένα προσωπικού χαρακτήρα.
- ❑ Τις σχετικές κατηγορίες δεδομένων προσωπικού χαρακτήρα.
- ❑ Τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων προσωπικού χαρακτήρα.
- ❑ Κατά περίπτωση, ότι ο υπεύθυνος επεξεργασίας προτίθεται να διαβιβάσει δεδομένα προσωπικού χαρακτήρα σε αποδέκτη σε τρίτη χώρα ή διεθνή οργανισμό και την ύπαρξη ή την απουσία απόφασης επάρκειας της Επιτροπής.

Επιπροσθέτως, ο υπεύθυνος επεξεργασίας, υποχρεούται να παρέχει στο υποκείμενο των δεδομένων τις εξής επιπλέον πληροφορίες για την εξασφάλιση θεμιτής και διαφανούς επεξεργασίας:

- Το χρονικό διάστημα για το οποίο θα αποθηκευτούν τα δεδομένα προσωπικού χαρακτήρα.
- Εάν η επεξεργασία είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας.
- Την ύπαρξη δικαιώματος υποβολής αιτήματος στον υπεύθυνο επεξεργασίας για πρόσβαση και διόρθωση ή διαγραφή των δεδομένων προσωπικού χαρακτήρα ή περιορισμό της επεξεργασίας που αφορούν το υποκείμενο των δεδομένων ή δικαιώματος αντίταξης στην επεξεργασία, καθώς και δικαιώματος στη φορητότητα των δεδομένων.
- Την ύπαρξη του δικαιώματος να ανακαλέσει τη συγκατάθεσή του οποτεδήποτε, χωρίς να θιγεί η νομιμότητα της επεξεργασίας που βασίστηκε στη συγκατάθεση πριν από την ανάκλησή της.
- Το δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή.
- Την πηγή από την οποία προέρχονται τα δεδομένα προσωπικού χαρακτήρα και, ανάλογα με την περίπτωση, εάν τα δεδομένα προήλθαν από πηγές στις οποίες έχει πρόσβαση το κοινό.
- Την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ, καθώς και τη σημασία και τις προβλεπόμενες συνέπειές της εν λόγω επεξεργασίας για το υποκείμενο των δεδομένων.

Όταν ο υπεύθυνος επεξεργασίας προτίθεται να επεξεργαστεί περαιτέρω τα δεδομένα προσωπικού χαρακτήρα για άλλο σκοπό από εκείνο για τον οποίο συλλέχθηκαν τα δεδομένα προσωπικού χαρακτήρα, υποχρεούται να παρέχει στο υποκείμενο των δεδομένων πληροφορίες για τον σκοπό αυτόν.

Το υποκείμενο των δεδομένων δεν δικαιούται την παροχή πληροφοριών στις παρακάτω περιπτώσεις:

- Το υποκείμενο των δεδομένων διαθέτει ήδη τις πληροφορίες.
- Η παροχή τέτοιων πληροφοριών αποδεικνύεται αδύνατη ή χρειάζεται δυσανάλογη προσπάθεια, ιδίως όσον αφορά επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς.
- Η απόκτηση ή η κοινολόγηση προβλέπεται ρητώς από το δίκαιο της Ένωσης ή του κράτους μέλους στο οποίο υπόκειται ο υπεύθυνος επεξεργασίας και το οποίο παρέχει τα κατάλληλα μέτρα για την προστασία των έννομων συμφερόντων του υποκειμένου των δεδομένων.
- Εάν τα δεδομένα προσωπικού χαρακτήρα πρέπει να παραμείνουν εμπιστευτικά λόγω επαγγελματικού απορρήτου που ρυθμίζεται από το δίκαιο της Ένωσης ή κράτους μέλους, συμπεριλαμβανομένης της εκ του νόμου υποχρέωσης τήρησης απορρήτου.

2.1.2.3 Επεξεργασία των δεδομένων και διαβίβαση σε τρίτες χώρες

Το υποκείμενο των δεδομένων έχει το δικαίωμα να λαμβάνει από τον υπεύθυνο επεξεργασίας επιβεβαίωση για την επεξεργασία ή μη των δεδομένων προσωπικού χαρακτήρα που το αφορούν. Εφόσον, τα δεδομένα προσωπικού χαρακτήρα υφίστανται επεξεργασία το υποκείμενο των δεδομένων έχει το δικαίωμα πρόσβασης σε αυτά τα δεδομένα και στις ακόλουθες πληροφορίες:

- Τους σκοπούς της επεξεργασίας.
- Τις σχετικές κατηγορίες δεδομένων προσωπικού χαρακτήρα.
- Όταν δεδομένα προσωπικού χαρακτήρα διαβιβάζονται σε τρίτη χώρα ή σε διεθνή οργανισμό, το υποκείμενο των δεδομένων έχει το δικαίωμα να ενημερώνεται για τις κατάλληλες εγγυήσεις.
- Τους αποδέκτες στους οποίους κοινοποιήθηκαν ή πρόκειται να κοινοποιηθούν τα δεδομένα προσωπικού χαρακτήρα, ιδίως τους αποδέκτες σε τρίτες χώρες ή διεθνείς οργανισμούς.
- Εάν είναι δυνατόν, το χρονικό διάστημα για το οποίο θα αποθηκευτούν τα δεδομένα προσωπικού χαρακτήρα.
- Την ύπαρξη δικαιώματος υποβολής αιτήματος στον υπεύθυνο επεξεργασίας για διόρθωση ή διαγραφή δεδομένων προσωπικού χαρακτήρα ή περιορισμό της επεξεργασίας των δεδομένων

προσωπικού χαρακτήρα που αφορά το υποκείμενο των δεδομένων ή δικαιώματος αντίταξης στην εν λόγω επεξεργασία.
- ❑ Το δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή.
- ❑ Όταν τα δεδομένα προσωπικού χαρακτήρα δεν συλλέγονται από το υποκείμενο των δεδομένων, κάθε διαθέσιμη πληροφορία σχετικά με την προέλευσή τους.
- ❑ Την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ, καθώς και τη σημασία και τις προβλεπόμενες συνέπειες της εν λόγω επεξεργασίας για το υποκείμενο των δεδομένων.
- ❑ Το δικαίωμα λήψης αντιγράφου όπου δεν επηρεάζει δυσμενώς τα δικαιώματα και τις ελευθερίες άλλων.

2.1.3 Διόρθωση και διαγραφή

Το υποκείμενο των δεδομένων έχει το δικαίωμα να απαιτήσει από τον υπεύθυνο επεξεργασίας χωρίς καθυστέρηση τη διόρθωση ή και την διαγραφή ανακριβών δεδομένων προσωπικού χαρακτήρα που το αφορούν.

Ο υπεύθυνος επεξεργασίας υποχρεούται να διόρθωση ή να διαγράψει τα δεδομένα προσωπικού χαρακτήρα χωρίς αδικαιολόγητη καθυστέρηση, εάν ισχύει ένας από τους ακόλουθους λόγους:

- ❑ Τα δεδομένα προσωπικού χαρακτήρα δεν είναι πλέον απαραίτητα σε σχέση με τους σκοπούς για τους οποίους συλλέχθηκαν.
- ❑ Το υποκείμενο των δεδομένων ανακαλεί τη συγκατάθεση επί της οποίας βασίζεται η επεξεργασία.
- ❑ Το υποκείμενο των δεδομένων αντιτίθεται στην επεξεργασία και δεν υπάρχουν επιτακτικοί και νόμιμοι λόγοι για την επεξεργασία.
- ❑ Τα δεδομένα προσωπικού χαρακτήρα υποβλήθηκαν σε επεξεργασία παράνομα.
- ❑ Τα δεδομένα προσωπικού χαρακτήρα πρέπει να διαγραφούν, ώστε να τηρηθεί κάποια νομική υποχρέωση,
- ❑ Τα δεδομένα προσωπικού χαρακτήρα έχουν συλλεχθεί σε σχέση με την προσφορά υπηρεσιών της κοινωνίας της πληροφορίας.

Το υποκείμενο των δεδομένων δικαιούται να εξασφαλίζει από τον υπεύθυνο επεξεργασίας τον περιορισμό της επεξεργασίας, όταν:

- ❑ Η ακρίβεια των δεδομένων προσωπικού χαρακτήρα αμφισβητείται από το υποκείμενο των δεδομένων, για χρονικό διάστημα που επιτρέπει στον υπεύθυνο επεξεργασίας να επαληθεύσει την ακρίβεια των δεδομένων προσωπικού χαρακτήρα.
- ❑ Η επεξεργασία είναι παράνομη και το υποκείμενο των δεδομένων αντιτάσσεται στη διαγραφή των δεδομένων προσωπικού χαρακτήρα και ζητεί, αντ'αυτής, τον περιορισμό της χρήσης τους.
- ❑ Ο υπεύθυνος επεξεργασίας δεν χρειάζεται πλέον τα δεδομένα προσωπικού χαρακτήρα για τους σκοπούς της επεξεργασίας, αλλά τα δεδομένα αυτά απαιτούνται από το υποκείμενο των δεδομένων για τη θεμελίωση, την άσκηση ή την υποστήριξη νομικών αξιώσεων.
- ❑ Το υποκείμενο των δεδομένων έχει αντιρρήσεις για την επεξεργασία εν αναμονή της επαλήθευσης του κατά πόσον οι νόμιμοι λόγοι του υπευθύνου επεξεργασίας υπερισχύουν έναντι των λόγων του υποκειμένου των δεδομένων.

Όταν η επεξεργασία έχει περιοριστεί, δεδομένα που δεν έχουν ήδη αποθηκευτεί, μπορεί να επεξεργαστούν μόνο με τη συγκατάθεση του υποκειμένου των δεδομένων ή για την προστασία των δικαιωμάτων άλλου φυσικού ή νομικού προσώπου ή για λόγους σημαντικού δημοσίου συμφέροντος της

Ένωσης ή κράτους μέλους.

Το υποκείμενο των δεδομένων το οποίο έχει εξασφαλίσει τον περιορισμό της επεξεργασίας ενημερώνεται από τον υπεύθυνο επεξεργασίας πριν από την άρση του περιορισμού επεξεργασίας.

Υποχρέωση γνωστοποίησης όσον αφορά τη διόρθωση ή τη διαγραφή δεδομένων προσωπικού χαρακτήρα ή τον περιορισμό της επεξεργασίας: κατά την άσκηση του δικαιώματος φορητότητας των δεδομένων, το υποκείμενο των δεδομένων έχει το δικαίωμα να ζητά την απευθείας διαβίβαση των δεδομένων προσωπικού χαρακτήρα από έναν υπεύθυνο επεξεργασίας σε άλλον, σε περίπτωση που αυτό είναι τεχνικά εφικτό. Το δικαίωμα αυτό δεν ισχύει για την επεξεργασία που είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας ή δεν επηρεάζει δυσμενώς τα δικαιώματα και τις ελευθερίες άλλων.

2.1.4 Δικαίωμα εναντίωσης και αυτοματοποιημένη ατομική λήψη αποφάσεων

Το υποκείμενο των δεδομένων δικαιούται να αντιτάσσεται, ανά πάσα στιγμή και για λόγους που σχετίζονται με την ιδιαίτερη κατάστασή του, στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που το αφορούν.

Όταν τα δεδομένα προσωπικού χαρακτήρα υφίστανται επεξεργασία για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς ή για σκοπούς απευθείας εμπορικής προώθησης και το υποκείμενο των δεδομένων αντιτίθενται στην επεξεργασία αυτών, τότε ο υπεύθυνος επεξεργασίας δεν έχει πλέον το δικαίωμα της επεξεργασίας των δεδομένων. Εξαίρεση αποτελεί όταν η επεξεργασία των δεδομένων χαρακτηρίζεται απαραίτητη για την εκτέλεση καθήκοντος που ασκείται για λόγους δημόσιου συμφέροντος.

Το υποκείμενο των δεδομένων έχει το δικαίωμα να μην υπόκειται σε απόφαση που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας, συμπεριλαμβανομένης της κατάρτισης προφίλ, η οποία παράγει έννομα αποτελέσματα που το αφορούν ή το επηρεάζει σημαντικά με παρόμοιο τρόπο.

Αυτό δεν εφαρμόζεται όταν η απόφαση:

- Είναι αναγκαία για τη σύναψη ή την εκτέλεση σύμβασης μεταξύ του υποκειμένου των δεδομένων και του υπευθύνου επεξεργασίας των δεδομένων.
- Επιτρέπεται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους στο οποίο υπόκειται ο υπεύθυνος επεξεργασίας και το οποίο προβλέπει επίσης κατάλληλα μέτρα για την προστασία των δικαιωμάτων, των ελευθεριών και των έννομων συμφερόντων του υποκειμένου των δεδομένων.
- Βασίζεται στη ρητή συγκατάθεση του υποκειμένου των δεδομένων.

Σε αυτήν την περίπτωση ο υπεύθυνος επεξεργασίας εφαρμόζει κατάλληλα μέτρα για την προστασία των δικαιωμάτων και των έννομων συμφερόντων του υποκειμένου των δεδομένων.

2.1.5 Περιορισμοί

Το δίκαιο της Ένωσης ή του κράτους μέλους στο οποίο υπόκειται ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία των δεδομένων μπορεί να περιορίζει μέσω νομοθετικού μέτρου το πεδίο εφαρμογής των υποχρεώσεων και των δικαιωμάτων που προβλέπονται, όταν ένας τέτοιος περιορισμός σέβεται την ουσία των θεμελιωδών δικαιωμάτων και ελευθεριών και συνιστά αναγκαίο και αναλογικό μέτρο σε μια δημοκρατική κοινωνία για τη διασφάλιση:

- Της ασφάλειας του κράτους.
- Της εθνικής άμυνας.
- Της δημόσιας ασφάλειας.
- Της πρόληψης, της διερεύνησης, της ανίχνευσης ή της δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων, συμπεριλαμβανομένης της προστασίας από απειλές κατά της δημόσιας ασφάλειας και της πρόληψης αυτών.
- Άλλων σημαντικών στόχων γενικού δημόσιου συμφέροντος της Ένωσης ή κράτους μέλους, ιδίως σημαντικού οικονομικού ή χρηματοοικονομικού συμφέροντος της Ένωσης ή κράτους μέλους, συμπεριλαμβανομένων των νομισματικών, δημοσιο-νομικών και φορολογικών θεμάτων, της δημόσιας υγείας και της κοινωνικής ασφάλισης.
- Της προστασίας της ανεξαρτησίας της δικαιοσύνης και των δικαστικών διαδικασιών.
- Της πρόληψης, της διερεύνησης, της ανίχνευσης και της δίωξης παραβάσεων δεοντολογίας σε νομοθετικά κατοχυρωμένα επαγγέλματα.
- Της παρακολούθησης, της επιθεώρησης ή της κανονιστικής λειτουργίας που συνδέεται, έστω περιστασιακά, με την άσκηση δημόσιας εξουσίας.
- Της προστασίας του υποκειμένου των δεδομένων ή των δικαιωμάτων και των ελευθεριών τρίτων.
- Της εκτέλεσης αστικών αξιώσεων.

Ειδικότερα, κάθε νομοθετικό μέτρο περιέχει συγκεκριμένες διατάξεις τουλάχιστον, ανάλογα με την περίπτωση, όσον αφορά:

- Τους σκοπούς της επεξεργασίας ή τις κατηγορίες επεξεργασίας,
- Τις κατηγορίες δεδομένων προσωπικού χαρακτήρα.
- Το πεδίο εφαρμογής των περιορισμών που επιβλήθηκαν.
- Τις εγγυήσεις για την πρόληψη καταχρήσεων ή παράνομης πρόσβασης ή διαβίβασης.
- Την ειδική περιγραφή του υπευθύνου επεξεργασίας ή των κατηγοριών των υπευθύνων επεξεργασίας.
- Τις περιόδους αποθήκευσης και τις ισχύουσες εγγυήσεις, λαμβάνοντας υπόψη τη φύση, το πεδίο εφαρμογής και τους σκοπούς της επεξεργασίας ή τις κατηγορίες επεξεργασίας.
- Τους κινδύνους για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων.
- Το δικαίωμα των υποκειμένων των δεδομένων να ενημερώνονται σχετικά με τον περιορισμό, εκτός εάν αυτό μπορεί να αποβεί επιζήμιο για τους σκοπούς του περιορισμού.

2.2 Ο υπεύθυνος και ο εκτελών την επεξεργασία

Με τον 2016/679 και τα άρθρα 24 έως 43, τα όποια περιλαμβάνονται σε αυτόν, περιγράφονται οι υποχρεώσεις του υπεύθυνου και εκτελών την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Ο υπεύθυνος και εκτελών την επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι υπεύθυνος για την προστασία των δεδομένων. Ο τρόπος συλλογής, η αποθήκευση, η επεξεργασία, η φορητότητα και η διαγραφή των δεδομένων είναι ευθύνη του εκτελούντος την επεξεργασία δεδομένων

2.2.1 Γενικές υποχρεώσεις

Λαμβάνοντας υπόψη τις τελευταίες εξελίξεις, το κόστος εφαρμογής, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία υποχρεούνται να τηρούν τα παρακάτω με βάση τον παρόντα κανονισμό.

Ο υπεύθυνος επεξεργασίας υποχρεούται να εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τον παρόντα κανονισμό. Τα εν λόγω μέτρα επανεξετάζονται και επικαιροποιούνται όταν κρίνεται απαραίτητο. Τα μέτρα που εφαρμόζονται περιλαμβάνουν την εφαρμογή κατάλληλων πολιτικών και διαδικασιών για την προστασία των δεδομένων από τον υπεύθυνο επεξεργασίας.

Ο υπεύθυνος επεξεργασίας υποχρεούται να εφαρμόζει αποτελεσματικά, τόσο κατά τη στιγμή του καθορισμού των μέσων επεξεργασίας όσο και κατά τη στιγμή της επεξεργασίας, κατάλληλα τεχνικά και οργανωτικά μέτρα, όπως η ψευδωνυμοποίηση, σχεδιασμένα για την εφαρμογή αρχών προστασίας των δεδομένων, όπως η ελαχιστοποίηση των δεδομένων, και η ενσωμάτωση των απαραίτητων εγγυήσεων στην επεξεργασία κατά τρόπο ώστε να πληρούνται οι απαιτήσεις του παρόντος κανονισμού.

Επιπροσθέτως, ο υπεύθυνος επεξεργασίας υποχρεούται να εφαρμόζει τα κατάλληλα τεχνικά και οργανωτικά μέτρα για να διασφαλίζει ότι, εξ ορισμού, υφίστανται επεξεργασία μόνο τα δεδομένα προσωπικού χαρακτήρα που είναι απαραίτητα για τον εκάστοτε σκοπό της επεξεργασίας.

Για όλα τα παραπάνω, η τήρηση εγκεκριμένων κωδίκων δεοντολογίας ή εγκεκριμένου μηχανισμού πιστοποίησης ISO μπορεί να χρησιμοποιηθεί ως στοιχείο απόδειξης της συμμόρφωσης με τις υποχρεώσεις του υπευθύνου επεξεργασίας.

Στην περίπτωση που δύο ή περισσότεροι υπεύθυνοι επεξεργασίας καθορίζουν από κοινού τους σκοπούς και τα μέσα της επεξεργασίας, αποτελούν από κοινού τους υπευθύνους επεξεργασίας. Αυτοί καθορίζουν με διαφανή τρόπο τις αντίστοιχες ευθύνες τους για συμμόρφωση προς τις υποχρεώσεις τους με τον παρόντα κανονισμό Σε αυτήν την περίπτωση συντάσσεται συμφωνία μεταξύ των υπευθύνων επεξεργασίας όπου ορίζονται ξεκάθαρα των από κοινού υπευθύνων επεξεργασίας έναντι των υποκειμένων των δεδομένων. Η ουσία της συμφωνίας τίθεται στη διάθεση του υποκειμένου των δεδομένων.

Ο υπεύθυνος επεξεργασίας υποχρεούται να χρησιμοποιεί μόνο εκτελούντες την επεξεργασία που παρέχουν επαρκείς διαβεβαιώσεις για την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων, κατά τρόπο ώστε η επεξεργασία να πληροί τις απαιτήσεις του παρόντος κανονισμού και να διασφαλίζεται η προστασία των δικαιωμάτων του υποκειμένου των δεδομένων.

Για να ενεργήσει ο εκτελών την επεξεργασία πρέπει πρώτα να υπάρχει σύμβαση υπαγόμενη στο δίκαιο της Ένωσης, που να δεσμεύει τον εκτελούντα την επεξεργασία σε σχέση με τον υπεύθυνο επεξεργασίας και να καθορίζει το αντικείμενο και τη διάρκεια της επεξεργασίας, τον σκοπό της επεξεργασίας, το είδος των δεδομένων προσωπικού χαρακτήρα, τις κατηγορίες των υποκειμένων των δεδομένων και τις υποχρεώσεις και τα δικαιώματα του υπευθύνου επεξεργασίας.

Η εν λόγω σύμβαση προβλέπει ότι ο εκτελών την επεξεργασία υποχρεούται να:

- επεξεργάζεται τα δεδομένα προσωπικού χαρακτήρα μόνο βάσει καταγεγραμμένων εντολών του υπευθύνου επεξεργασίας
- διασφαλίζει ότι τα πρόσωπα που είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα έχουν αναλάβει δέσμευση τήρησης εμπιστευτικότητας,
- λαμβάνει όλα τα απαιτούμενα μέτρα για την σωστή τήρηση των πολιτικών και των διαδικασιών,
- λαμβάνει υπόψη τη φύση της επεξεργασίας και επικουρεί τον υπεύθυνο επεξεργασίας με τα κατάλληλα τεχνικά και οργανωτικά μέτρα, στον βαθμό που αυτό είναι δυνατό,
- απαντά σε αιτήματα για άσκηση των προβλεπόμενων δικαιωμάτων του υποκειμένου των δεδομένων,
- συνδράμει τον υπεύθυνο επεξεργασίας στη διασφάλιση της συμμόρφωσης λαμβάνοντας υπόψη τη φύση της επεξεργασίας και τις πληροφορίες που διαθέτει ο εκτελών την επεξεργασία,
- κατ' επιλογή του υπευθύνου επεξεργασίας, διαγράφει ή επιστρέφει όλα τα δεδομένα προσωπικού χαρακτήρα στον υπεύθυνο επεξεργασίας μετά το πέρας της παροχής υπηρεσιών επεξεργασίας και διαγράφει τα υφιστάμενα αντίγραφα, και
- θέτει στη διάθεση του υπευθύνου επεξεργασίας κάθε απαραίτητη πληροφορία προς απόδειξη της συμμόρφωσης προς τις υποχρεώσεις που θεσπίζονται στο παρόν άρθρο και επιτρέπει και διευκολύνει τους ελέγχους, περιλαμβανομένων των επιθεωρήσεων

Όταν ο εκτελών την επεξεργασία προσλαμβάνει άλλον εκτελούντα για τη διενέργεια συγκεκριμένων δραστηριοτήτων επεξεργασίας για λογαριασμό του υπευθύνου επεξεργασίας, οι ίδιες υποχρεώσεις όσον αφορά την προστασία των δεδομένων που προβλέπονται στη σύμβαση ή στην άλλη νομική πράξη μεταξύ υπευθύνου επεξεργασίας και εκτελούντος την επεξεργασία επιβάλλονται στον άλλον εκτελούντα μέσω σύμβασης σύμφωνα με το δίκαιο της Ένωσης, ιδίως ώστε να παρέχονται επαρκείς διαβεβαιώσεις ότι πληρούνται οι απαιτήσεις του παρόντος κανονισμού. Όταν ο άλλος εκτελών την επεξεργασία αδυνατεί να ανταποκριθεί στις σχετικές με την προστασία των δεδομένων υποχρεώσεις του, ο αρχικός εκτελών παραμένει πλήρως υπόλογος έναντι του υπευθύνου επεξεργασίας για την εκπλήρωση των υποχρεώσεων του άλλου εκτελούντος την επεξεργασία.

Ο εκτελών την επεξεργασία και κάθε πρόσωπο που ενεργεί υπό την εποπτεία του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, το οποίο έχει πρόσβαση σε δεδομένα προσωπικού χαρακτήρα, υποχρεούται να επεξεργάζεται τα εν λόγω δεδομένα μόνον κατ' εντολή του υπευθύνου επεξεργασίας, εκτός εάν υποχρεούται προς τούτο από το δίκαιο της Ένωσης ή του κράτους μέλους.

Κάθε υπεύθυνος επεξεργασίας ή ο εκπρόσωπός του υποχρεούται να τηρεί αρχείο των δραστηριοτήτων επεξεργασίας για τις οποίες είναι υπεύθυνος.

Το εν λόγω αρχείο περιλαμβάνει όλες τις ακόλουθες πληροφορίες:

- το όνομα και τα στοιχεία επικοινωνίας του υπευθύνου επεξεργασίας και, κατά περίπτωση, του από κοινού υπευθύνου επεξεργασίας, του εκπροσώπου του υπευθύνου επεξεργασίας και του υπευθύνου προστασίας δεδομένων,
- τους σκοπούς της επεξεργασίας,
- περιγραφή των κατηγοριών υποκειμένων των δεδομένων και των κατηγοριών δεδομένων προσωπικού χαρακτήρα,
- τις κατηγορίες αποδεκτών στους οποίους πρόκειται να γνωστοποιηθούν ή γνωστοποιήθηκαν τα δεδομένα προσωπικού χαρακτήρα, συμπεριλαμβανομένων των αποδεκτών σε τρίτες χώρες ή διεθνείς οργανισμούς,
- όπου είναι δυνατό, τις προβλεπόμενες προθεσμίες διαγραφής των διάφορων κατηγοριών δεδομένων, και
- όπου είναι δυνατό, μία γενική περιγραφή των τεχνικών και οργανωτικών μέτρων ασφάλειας.

Κάθε εκτελών την επεξεργασία ή ο εκπρόσωπος του εκτελούντος την επεξεργασία υποχρεούται να τηρεί αρχείο όλων των δραστηριοτήτων επεξεργασίας που διεξάγονται εκ μέρους του υπευθύνου επεξεργασίας, το οποίο περιλαμβάνει τα εξής:

- ❑ το όνομα και τα στοιχεία επικοινωνίας του εκτελούντος ή των εκτελούντων την επεξεργασία και των υπευθύνων επεξεργασίας εκ μέρους των οποίων ενεργεί ο εκτελών και, κατά περίπτωση, του εκπροσώπου του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, καθώς και του υπευθύνου προστασίας δεδομένων,
- ❑ τις κατηγορίες επεξεργασιών που διεξάγονται εκ μέρους κάθε υπευθύνου επεξεργασίας,
- ❑ όπου είναι δυνατό, γενική περιγραφή των τεχνικών και οργανωτικών μέτρων ασφάλειας

Τα παραπάνω αρχεία υφίστανται τόσο γραπτώς όσο και σε ηλεκτρονική μορφή.

Ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία ή ο εκπρόσωπος του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία θέτουν το αρχείο στη διάθεση της εποπτικής αρχής κατόπιν αιτήματος.

Τέλος, λαμβάνοντας υπόψη τις τελευταίες εξελίξεις, το κόστος εφαρμογής και τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων από την επεξεργασία ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία ή οι εκπρόσωποί τους υποχρεούνται να συνεργάζονται με την εποπτική αρχή για την άσκηση των καθηκόντων της.

2.2.2 Ασφάλεια δεδομένων προσωπικού χαρακτήρα

Εικόνα 4

Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία υποχρεούνται να εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων, περιλαμβανομένων, μεταξύ άλλων, κατά περίπτωση:

- ❑ της ψευδωνυμοποίησης και της κρυπτογράφησης δεδομένων προσωπικού χαρακτήρα,
- ❑ της δυνατότητας διασφάλισης του απορρήτου, της ακεραιότητας, της διαθεσιμότητας και της

αξιοπιστίας των συστημάτων και των υπηρεσιών επεξεργασίας σε συνεχή βάση,
- ❑ της δυνατότητας αποκατάστασης της διαθεσιμότητας και της πρόσβασης σε δεδομένα προσωπικού χαρακτήρα σε εύθετο χρόνο σε περίπτωση φυσικού ή τεχνικού συμβάντος, και
- ❑ της διαδικασίας για την τακτική δοκιμή, εκτίμηση και αξιολόγηση της αποτελεσματικότητας των τεχνικών και των οργανωτικών μέτρων για τη διασφάλιση της ασφάλειας της επεξεργασίας.

Κατά την εκτίμηση του ενδεδειγμένου επιπέδου ασφάλειας λαμβάνονται ιδίως υπόψη οι κίνδυνοι που απορρέουν από την επεξεργασία από τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, άνευ αδείας κοινολόγηση ή προσπέλαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία.

Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία υποχρεούνται να λαμβάνουν μέτρα ώστε να διασφαλίζεται ότι κάθε φυσικό πρόσωπο που ενεργεί υπό την εποπτεία του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, το οποίο έχει πρόσβαση σε δεδομένα προσωπικού χαρακτήρα, μπορεί να τα επεξεργάζεται μόνο κατ' εντολή του υπευθύνου επεξεργασίας, εκτός εάν υποχρεούται προς τούτο από το δίκαιο της Ένωσης ή του κράτους μέλους.

Σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα, ο υπεύθυνος επεξεργασίας υποχρεούται να γνωστοποιήσει το συντομότερο, και αν είναι δυνατό, εντός 72 ωρών από τη στιγμή που αποκτά γνώση του γεγονότος, την παραβίαση των δεδομένων προσωπικού χαρακτήρα στην εποπτική αρχή που είναι αρμόδια εκτός εάν η παραβίαση δεδομένων προσωπικού χαρακτήρα δεν ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Όταν η γνωστοποίηση στην εποπτική αρχή δεν πραγματοποιείται εντός 72 ωρών, συνοδεύεται από αιτιολόγηση για την καθυστέρηση.

Ο εκτελών την επεξεργασία ενημερώνει τον υπεύθυνο επεξεργασίας άμεσα, μόλις αντιληφθεί παραβίαση δεδομένων προσωπικού χαρακτήρα.

Η γνωστοποίηση περιλαμβάνει κατ’ ελάχιστο:

- ❑ μια περιγραφή της παραβίασης δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων, όπου είναι δυνατό, των κατηγοριών και του κατά προσέγγιση αριθμού των επηρεαζόμενων υποκειμένων των δεδομένων, καθώς και των κατηγοριών και του κατά προσέγγιση αριθμού των επηρεαζόμενων αρχείων δεδομένων προσωπικού χαρακτήρα,
- ❑ το όνομα και τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων ή άλλου σημείου επικοινωνίας από το οποίο μπορεί να ληφθούν περισσότερες πληροφορίες,
- ❑ τις ενδεχόμενες συνέπειες της παραβίασης των δεδομένων προσωπικού χαρακτήρα, και
- ❑ περιγράφει τα ληφθέντα ή τα προτεινόμενα προς λήψη μέτρα από τον υπεύθυνο επεξεργασίας για την αντιμετώπιση της παραβίασης των δεδομένων προσωπικού χαρακτήρα, καθώς και, όπου ενδείκνυται, μέτρα για την άμβλυνση ενδεχόμενων δυσμενών συνεπειών της.

Σε περίπτωση που και εφόσον δεν είναι δυνατόν να παρασχεθούν οι πληροφορίες ταυτόχρονα, μπορεί να παρέχονται σταδιακά χωρίς αδικαιολόγητη καθυστέρηση. Ο υπεύθυνος επεξεργασίας τεκμηριώνει κάθε παραβίαση δεδομένων προσωπικού χαρακτήρα, που συνίστανται στα πραγματικά περιστατικά που αφορούν την παραβίαση δεδομένων προσωπικού χαρακτήρα, τις συνέπειες και τα ληφθέντα διορθωτικά μέτρα. Όταν η παραβίαση δεδομένων προσωπικού χαρακτήρα ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας ανακοινώνει αμελλητί την παραβίαση των δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων.

Η ανακοίνωση στο υποκείμενο των δεδομένων περιγράφει με σαφήνεια την φύση της παραβίασης των δεδομένων προσωπικού χαρακτήρα και περιέχονται τουλάχιστον οι πληροφορίες για επικοινωνία καθώς και τα μέτρα για την αποφυγή μελλοντικής παραβίασης

Ο υπεύθυνος επεξεργασίας δεν υποχρεούται να ενημερώσει το υποκείμενο των δεδομένων εάν πληρείται οποιαδήποτε από τις ακόλουθες προϋποθέσεις:

- ο υπεύθυνος επεξεργασίας εφάρμοσε κατάλληλα τεχνικά και οργανωτικά μέτρα προστασίας και τα μέτρα αυτά εφαρμόστηκαν στα επηρεαζόμενα από την παραβίαση δεδομένα προσωπικού χαρακτήρα, κυρίως μέτρα που καθιστούν μη κατανοητά τα δεδομένα προσωπικού χαρακτήρα σε όσους δεν διαθέτουν άδεια πρόσβασης σε αυτά, όπως η κρυπτογράφηση,
- ο υπεύθυνος επεξεργασίας έλαβε στη συνέχεια μέτρα που διασφαλίζουν ότι δεν είναι πλέον πιθανό να προκύψει υψηλός κίνδυνος για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων,
- προϋποθέτει δυσανάλογες προσπάθειες. Στην περίπτωση αυτή, γίνεται αντί αυτής δημόσια ανακοίνωση ή υπάρχει παρόμοιο μέτρο με το οποίο τα υποκείμενα των δεδομένων ενημερώνονται με εξίσου αποτελεσματικό τρόπο.

Εάν ο υπεύθυνος επεξεργασίας δεν έχει ήδη ανακοινώσει την παραβίαση των δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων, η εποπτική αρχή μπορεί, έχοντας εξετάσει την πιθανότητα επέλευσης υψηλού κινδύνου από την παραβίαση των δεδομένων προσωπικού χαρακτήρα, να του ζητήσει να το πράξει ή μπορεί να αποφασίσει ότι πληρούνται οποιεσδήποτε από τις προϋποθέσεις που αναφέρονται παραπάνω.

2.2.3 Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων και προηγούμενη διαβούλευση

Όταν ένα είδος επεξεργασίας, ιδίως με χρήση νέων τεχνολογιών και συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας διενεργεί, πριν από την επεξεργασία, εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα. Σε μία εκτίμηση μπορεί να εξετάζεται ένα σύνολο παρόμοιων πράξεων επεξεργασίας οι οποίες ενέχουν παρόμοιους υψηλούς κινδύνους.

Ο υπεύθυνος επεξεργασίας ζητεί τη γνώμη του υπευθύνου προστασίας δεδομένων, εφόσον έχει οριστεί, κατά τη διενέργεια εκτίμησης αντίκτυπου σχετικά με την προστασία δεδομένων.

Η εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων απαιτείται ιδίως στις παρακάτω περιπτώσεις:

- συστηματικής και εκτενούς αξιολόγησης προσωπικών πτυχών σχετικά με φυσικά πρόσωπα, η οποία βασίζεται σε αυτοματοποιημένη επεξεργασία, περιλαμβανομένης της κατάρτισης προφίλ, και στην οποία βασίζονται αποφάσεις που παράγουν έννομα αποτελέσματα σχετικά με το φυσικό πρόσωπο ή ομοίως επηρεάζουν σημαντικά το φυσικό πρόσωπο,
- μεγάλης κλίμακας επεξεργασίας των ειδικών κατηγοριών δεδομένων ή δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα, και
- συστηματικής παρακολούθησης δημοσίως προσβάσιμους χώρους σε μεγάλη κλίμακα.

Η εποπτική αρχή καταρτίζει και δημοσιοποιεί κατάλογο με τα είδη των πράξεων επεξεργασίας που υπόκεινται στην απαίτηση για διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία των δεδομένων. Η εποπτική αρχή ανακοινώνει τον εν λόγω κατάλογο στο Συμβούλιο Προστασίας Δεδομένων. Η εποπτική αρχή δύναται επίσης να καταρτίζει και να δημοσιοποιεί κατάλογο με τα είδη των πράξεων επεξεργασίας για τα οποία δεν απαιτείται εκτίμηση αντικτύπου σχετικά με την προστασία

των δεδομένων.

Πριν από την έκδοση αυτών των καταλόγων, η αρμόδια εποπτική αρχή εφαρμόζει τον μηχανισμό συνεκτικότητας εάν οι εν λόγω κατάλογοι περιλαμβάνουν δραστηριότητες επεξεργασίας οι οποίες σχετίζονται με την προσφορά αγαθών ή υπηρεσιών σε υποκείμενα των δεδομένων ή με την παρακολούθηση της συμπεριφοράς τους σε περισσότερα του ενός κράτη μέλη ή οι οποίες ενδέχεται να επηρεάζουν σημαντικά την ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα στην Ένωση.

Η εκτίμηση περιέχει τουλάχιστον:

- συστηματική περιγραφή των προβλεπόμενων πράξεων επεξεργασίας και των σκοπών της επεξεργασίας, περιλαμβανομένου, κατά περίπτωση, του έννομου συμφέροντος που επιδιώκει ο υπεύθυνος επεξεργασίας,
- εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας σε συνάρτηση με τους σκοπούς,
- εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων, και
- τα προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων, περιλαμβανομένων των εγγυήσεων, των μέτρων και μηχανισμών ασφάλειας, ώστε να διασφαλίζεται η προστασία των δεδομένων προσωπικού χαρακτήρα και να αποδεικνύεται η συμμόρφωση προς τον παρόντα κανονισμό, λαμβάνοντας υπόψη τα δικαιώματα και τα έννομα συμφέροντα των υποκειμένων των δεδομένων και άλλων ενδιαφερόμενων προσώπων.

Η συμμόρφωση με εγκεκριμένους κώδικες δεοντολογίας από τους σχετικούς υπευθύνους επεξεργασίας ή από εκτελούντες την επεξεργασία λαμβάνεται δεόντως υπόψη κατά την εκτίμηση του αντικτύπου των πράξεων επεξεργασίας που εκτελούνται από τους εν λόγω υπευθύνους ή από τους εκτελούντες την επεξεργασία, ιδίως για τους σκοπούς εκτίμησης του αντικτύπου σχετικά με την προστασία δεδομένων.

Όπου ενδείκνυται, ο υπεύθυνος επεξεργασίας ζητεί τη γνώμη των υποκειμένων των δεδομένων για τη σχεδιαζόμενη επεξεργασία, με την επιφύλαξη της προστασίας εμπορικών ή δημοσίων συμφερόντων ή της ασφάλειας των πράξεων επεξεργασίας.

Όταν η επεξεργασία έχει νομική βάση στο δίκαιο της Ένωσης ή στο δίκαιο του κράτους μέλους στο οποίο υπόκειται ο υπεύθυνος επεξεργασίας, το εν λόγω δίκαιο ρυθμίζει την εκάστοτε συγκεκριμένη πράξη επεξεργασίας ή σειρά πράξεων και έχει διενεργηθεί ήδη εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων ως μέρος γενικής εκτίμησης αντικτύπου στο πλαίσιο της έγκρισης της εν λόγω νομικής βάσης.

Όπου απαιτείται, ο υπεύθυνος επεξεργασίας προβαίνει σε επανεξέταση για να εκτιμήσει εάν η επεξεργασία των δεδομένων προσωπικού χαρακτήρα διενεργείται σύμφωνα με την εκτίμηση αντικτύπου στην προστασία δεδομένων τουλάχιστον όταν μεταβάλλεται ο κίνδυνος που θέτουν οι πράξεις επεξεργασίας.

Ο υπεύθυνος επεξεργασίας ζητεί τη γνώμη της εποπτικής αρχής πριν από την επεξεργασία, όταν η δυνάμει του άρθρου 35 εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων υποδεικνύει ότι η επεξεργασία θα προκαλούσε υψηλό κίνδυνο ελλείψει μέτρων μετριασμού του κινδύνου από τον υπεύθυνο επεξεργασίας.

Όταν η εποπτική αρχή θεωρήσει ότι η σχεδιαζόμενη επεξεργασία που αναφέρεται παραβαίνει τον παρόντα κανονισμό, ιδίως εάν ο υπεύθυνος επεξεργασίας δεν έχει προσδιορίσει ή μετριάσει επαρκώς τον κίνδυνο, η εποπτική αρχή παρέχει γραπτώς συμβουλές στον υπεύθυνο επεξεργασίας εντός προθεσμίας μέχρι οκτώ εβδομάδων από την παραλαβή του αιτήματος διαβούλευσης, και, όπου απαιτείται, στον εκτελούντα την επεξεργασία. Η εν λόγω προθεσμία μπορεί να παραταθεί κατά έξι εβδομάδες, λόγω της πολυπλοκότητας που χαρακτηρίζει τη σχεδιαζόμενη επεξεργασία. Η εποπτική αρχή ενημερώνει τον υπεύθυνο επεξεργασίας και, όπου απαιτείται, τον εκτελούντα την επεξεργασία για την εν λόγω

παράταση εντός ενός μηνός από την παραλαβή του αιτήματος διαβούλευσης, καθώς και για τους λόγους της καθυστέρησης Οι εν λόγω προθεσμίες μπορούν να αναστέλλονται έως ότου η εποπτική αρχή λάβει τις πληροφορίες που ζήτησε για τους σκοπούς της διαβούλευσης

Κατά τη διαβούλευση με την εποπτική αρχή, ο υπεύθυνος επεξεργασίας παρέχει στην εποπτική αρχή:

- κατά περίπτωση, τις αντίστοιχες αρμοδιότητες του υπευθύνου επεξεργασίας, των από κοινού υπευθύνων επεξεργασίας και των εκτελούντων την επεξεργασία που συμμετέχουν στις εργασίες, ιδίως όσον αφορά επεξεργασία ενός ομίλου επιχειρήσεων,
- τους σκοπούς και τα μέσα της σχεδιαζόμενης επεξεργασίας,
- τα μέτρα και τις εγγυήσεις για την προστασία των δικαιωμάτων και των ελευθεριών των υποκειμένων των δεδομένων σύμφωνα με τον παρόντα κανονισμό,
- κατά περίπτωση, τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων,
- την εκτίμηση του αντικτύπου σχετικά με την προστασία των δεδομένων, και
- κάθε άλλη πληροφορία που ζητεί η εποπτική αρχή.

Τα κράτη μέλη ζητούν τη γνώμη της εποπτικής αρχής κατά την εκπόνηση προτάσεων νομοθετικών μέτρων προς θέσπιση από τα εθνικά κοινοβούλια ή κανονιστικών μέτρων που βασίζονται σε τέτοια νομοθετικά μέτρα τα οποία αφορούν την επεξεργασία.

2.2.4 Υπεύθυνος προστασίας δεδομένων

Εικόνα 5

2.2.4.1 Ορισμός υπευθύνου προστασίας δεδομένων

Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία ορίζουν υπεύθυνο προστασίας δεδομένων σε κάθε περίπτωση στην οποία:

- η επεξεργασία διενεργείται από δημόσια αρχή ή φορέα, εκτός από δικαστήρια που ενεργούν στο πλαίσιο της δικαιοδοτικής τους αρμοδιότητας,
- οι βασικές δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν πράξεις επεξεργασίας οι οποίες, λόγω της φύσης, του πεδίου εφαρμογής και/ή των σκοπών τους, απαιτούν τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε μεγάλη κλίμακα,
- οι βασικές δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα και δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα

Ένας όμιλος επιχειρήσεων μπορεί να διορίσει ένα μόνο υπεύθυνο προστασίας δεδομένων, υπό την προϋπόθεση ότι κάθε εγκατάσταση έχει εύκολη πρόσβαση στον υπεύθυνο προστασίας δεδομένων.

Εάν ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία είναι δημόσια αρχή ή δημόσιος φορέας, ένας μόνο υπεύθυνος προστασίας δεδομένων μπορεί να ορίζεται για πολλές τέτοιες αρχές ή πολλούς τέτοιους φορείς, λαμβάνοντας υπόψη την οργανωτική τους δομή και το μέγεθός τους.

Σε άλλες περιπτώσεις, ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία ή ενώσεις και άλλοι φορείς που εκπροσωπούν κατηγορίες υπευθύνων επεξεργασίας ή εκτελούντων την επεξεργασία μπορούν να ορίζουν υπεύθυνο προστασίας δεδομένων όπου απαιτείται από το δίκαιο της Ένωσης ή του κράτους μέλους.

Ο υπεύθυνος προστασίας δεδομένων διορίζεται βάσει επαγγελματικών προσόντων και ιδίως βάσει της εμπειρίας που διαθέτει στον τομέα του δικαίου και των πρακτικών περί προστασίας δεδομένων, καθώς και βάσει της ικανότητας εκπλήρωσης των καθηκόντων που αναφέρονται στο άρθρο 39.

Ο υπεύθυνος προστασίας δεδομένων μπορεί να είναι μέλος του προσωπικού του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία ή να ασκεί τα καθήκοντά του βάσει σύμβασης παροχής υπηρεσιών.

Ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία δημοσιεύουν τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων και τα ανακοινώνουν στην εποπτική αρχή.

2.2.4.2 Η θέση του υπευθύνου προστασίας δεδομένων

Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία διασφαλίζουν ότι ο υπεύθυνος προστασίας δεδομένων συμμετέχει, δεόντως και εγκαίρως, σε όλα τα ζητήματα τα οποία σχετίζονται με την προστασία δεδομένων προσωπικού χαρακτήρα. Επίσης, στηρίζουν τον υπεύθυνο προστασίας δεδομένων στην άσκηση των καθηκόντων που αναφέρονται στο άρθρο 39 παρέχοντας τους απαραίτητους πόρους για την άσκηση των εν λόγω καθηκόντων και πρόσβαση σε δεδομένα προσωπικού χαρακτήρα και σε πράξεις επεξεργασίας, καθώς και πόρους απαραίτητους για τη διατήρηση της εμπειρίας του.

Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία διασφαλίζουν ότι ο υπεύθυνος προστασίας δεδομένων δεν λαμβάνει εντολές για την άσκηση των εν λόγω καθηκόντων. Δεν απολύεται ούτε υφίσταται κυρώσεις από τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία επειδή επιτέλεσε τα καθήκοντά του. Ο υπεύθυνος προστασίας δεδομένων λογοδοτεί απευθείας στο ανώτατο διοικητικό επίπεδο του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία.

Τα υποκείμενα των δεδομένων μπορούν να επικοινωνούν με τον υπεύθυνο προστασίας δεδομένων για κάθε ζήτημα σχετικό με την επεξεργασία των δεδομένων τους προσωπικού χαρακτήρα και με την άσκηση των δικαιωμάτων τους δυνάμει του παρόντος κανονισμού.

Ο υπεύθυνος προστασίας δεδομένων δεσμεύεται από την τήρηση του απορρήτου ή της εμπιστευτικότητας σχετικά με την εκτέλεση των καθηκόντων του, σύμφωνα με το δίκαιο της Ένωσης ή του κράτους μέλους. Μπορεί να επιτελεί και άλλα καθήκοντα και υποχρεώσεις. Ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία διασφαλίζει ότι τα εν λόγω καθήκοντα και υποχρεώσεις δεν συνεπάγονται σύγκρουση συμφερόντων.

2.2.4.3 Καθήκοντα του υπευθύνου προστασίας δεδομένων

Ο υπεύθυνος προστασίας δεδομένων έχει τουλάχιστον τα ακόλουθα καθήκοντα:

- ενημερώνει και συμβουλεύει τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία και τους υπαλλήλους που επεξεργάζονται τις υποχρεώσεις τους που απορρέουν από τον παρόντα κανονισμό και από άλλες διατάξεις της Ένωσης ή του κράτους μέλους σχετικά με την προστασία δεδομένων,
- παρακολουθεί τη συμμόρφωση με τον παρόντα κανονισμό, με άλλες διατάξεις της Ένωσης ή του κράτους μέλους σχετικά με την προστασία δεδομένων και με τις πολιτικές του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία σε σχέση με την προστασία των δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων της ανάθεσης αρμοδιοτήτων, της ευαισθητοποίησης και της κατάρτισης των υπαλλήλων που συμμετέχουν στις πράξεις επεξεργασίας, και των σχετικών ελέγχων,
- παρέχει συμβουλές, όταν ζητείται, όσον αφορά την εκτίμηση του αντικτύπου σχετικά με την προστασία των δεδομένων και παρακολουθεί την υλοποίησή της,
- συνεργάζεται με την εποπτική αρχή, και
- ενεργεί ως σημείο επικοινωνίας για την εποπτική αρχή για ζητήματα που σχετίζονται με την επεξεργασία

Κατά την εκτέλεση των καθηκόντων του, ο υπεύθυνος προστασίας δεδομένων λαμβάνει δεόντως υπόψη τον κίνδυνο που συνδέεται με τις πράξεις επεξεργασίας, συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας.

2.2.5 Κώδικες δεοντολογίας και πιστοποίηση

Εικόνα 6

2.2.5.1 Κώδικες δεοντολογίας

Τα κράτη μέλη, οι εποπτικές αρχές, το Συμβούλιο Προστασίας Δεδομένων και η Επιτροπή ενθαρρύνουν την εκπόνηση κωδίκων δεοντολογίας που έχουν ως στόχο να συμβάλουν στην ορθή εφαρμογή του παρόντος κανονισμού, λαμβάνοντας υπόψη τα ειδικά χαρακτηριστικά των διάφορων τομέων επεξεργασίας και τις ειδικές ανάγκες των πολύ μικρών, των μικρών και των μεσαίων επιχειρήσεων.

Ενώσεις και άλλοι φορείς που εκπροσωπούν κατηγορίες υπευθύνων επεξεργασίας ή εκτελούντων την επεξεργασία μπορούν να εκπονούν κώδικες δεοντολογίας ή να τροποποιούν ή να επεκτείνουν υφιστάμενους κώδικες δεοντολογίας, προκειμένου να προσδιορίσουν την εφαρμογή του παρόντος κανονισμού, όπως όσον αφορά:

- τη θεμιτή και με διαφάνεια επεξεργασία,
- τα έννομα συμφέροντα που επιδιώκουν οι υπεύθυνοι επεξεργασίας σε συγκεκριμένα πλαίσια,
- τη συλλογή δεδομένων προσωπικού χαρακτήρα,
- την ψευδωνυμοποίηση δεδομένων προσωπικού χαρακτήρα,
- την ενημέρωση του κοινού και των υποκειμένων των δεδομένων,
- την άσκηση των δικαιωμάτων των υποκειμένων των δεδομένων,
- την ενημέρωση και την προστασία των παιδιών και τον τρόπο απόκτησης της συγκατάθεσης του ασκούντος τη γονική μέριμνα του παιδιού,
- τα μέτρα και τις πολίτικες και διαδικασίες για τη διασφάλιση της ασφάλειας της επεξεργασίας
- τη γνωστοποίηση παραβιάσεων δεδομένων προσωπικού χαρακτήρα στις εποπτικές αρχές και στα υποκείμενα των δεδομένων,
- τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες ή διεθνείς οργανισμούς,
- τις εξωδικαστικές διαδικασίες και άλλες διαδικασίες επίλυσης διαφορών για την επίλυση διαφορών μεταξύ υπευθύνων επεξεργασίας και υποκειμένων των δεδομένων

Οι κώδικες δεοντολογίας περιέχουν μηχανισμούς που επιτρέπουν στον φορέα να διενεργεί την υποχρεωτική παρακολούθηση της συμμόρφωσης προς τις διατάξεις του από τους υπευθύνους επεξεργασίας ή από τους εκτελούντες την επεξεργασία που έχουν αναλάβει να τον εφαρμόζουν, με την επιφύλαξη των καθηκόντων και των αρμοδιοτήτων των εποπτικών αρχών.

Ενώσεις και άλλοι φορείς μπορούν να εκπονήσουν κώδικα δεοντολογίας ή να τροποποιήσουν ή να επεκτείνουν υφιστάμενο κώδικα και να υποβάλλουν το νέο σχέδιο κώδικα στην εποπτική αρχή.

Η εποπτική αρχή γνωμοδοτεί ως προς τη συμμόρφωση του σχεδίου κώδικα προς τον παρόντα κανονισμό και εγκρίνει το εν λόγω σχέδιο κώδικα εάν κρίνει ότι παρέχει επαρκείς κατάλληλες εγγυήσεις. Όταν το σχέδιο κώδικα εγκρίνεται και ο σχετικός κώδικας δεοντολογίας δεν έχει σχέση με δραστηριότητες επεξεργασίας σε περισσότερα του ενός κράτη μέλη, η εποπτική αρχή καταχωρεί και δημοσιεύει τον κώδικα.

Σε περίπτωση που το σχέδιο κώδικα δεοντολογίας αναφέρεται σε δραστηριότητες σε διάφορα κράτη μέλη, η εποπτική αρχή το υποβάλλει στο Συμβούλιο Προστασίας Δεδομένων, το οποίο γνωμοδοτεί ως προς τη συμμόρφωση του σχεδίου κώδικα προς τον παρόντα κανονισμό. Όταν η γνωμοδότηση επιβεβαιώνει ότι ο κώδικας είναι σύμφωνα με τον παρόντα κανονισμό, το Συμβούλιο Προστασίας Δεδομένων διαβιβάζει τη γνώμη του στην Επιτροπή.

Τέλος, η Επιτροπή μέσω εκτελεστικών πράξεων, αποφασίζει εάν ο κώδικας δεοντολογίας που της υποβλήθηκε έχει γενική ισχύ εντός της Ένωσης.

Η Επιτροπή διασφαλίζει τη δέουσα δημοσιότητα για τους εγκεκριμένους κώδικες για τους οποίους αποφάσισε ότι έχουν γενική ισχύ και το Συμβούλιο Προστασίας Δεδομένων συγκεντρώνει όλους τους εγκεκριμένους κώδικες δεοντολογίας, τις τροποποιήσεις και τις επεκτάσεις σε μητρώο και τους καθιστά διαθέσιμους στο κοινό με κάθε κατάλληλο μέσο.

2.2.5.2 Παρακολούθηση των εγκεκριμένων κωδίκων δεοντολογίας

Με την επιφύλαξη των καθηκόντων και των αρμοδιοτήτων της αρμόδιας εποπτικής αρχής η παρακολούθηση της συμμόρφωσης με κώδικα δεοντολογίας μπορεί να διεξάγεται από φορέα που διαθέτει το ενδεδειγμένο επίπεδο εμπειρογνωμοσύνης σε σχέση με το αντικείμενο του κώδικα και είναι διαπιστευμένος για τον σκοπό αυτόν από την αρμόδια εποπτική αρχή.

Ο φορέας μπορεί να είναι διαπιστευμένος για την παρακολούθηση της συμμόρφωσης με κώδικα δεοντολογίας, εφόσον ο εν λόγω φορέας:

- έχει αποδείξει την ανεξαρτησία και την εμπειρογνωμοσύνη του σε σχέση με το αντικείμενο του κώδικα κατά την κρίση της αρμόδιας εποπτικής αρχής,
- έχει καθιερώσει διαδικασίες που του επιτρέπουν την εκτίμηση της επιλεξιμότητας των σχετικών υπευθύνων επεξεργασίας και των εκτελούντων την επεξεργασία προκειμένου να εφαρμόσουν τον κώδικα, την παρακολούθηση της συμμόρφωσής τους με τις διατάξεις του και την περιοδική επανεξέταση της λειτουργίας του,
- έχει θεσπίσει διαδικασίες και δομές για την αντιμετώπιση καταγγελιών περί παραβάσεων του κώδικα ή περί του τρόπου με τον οποίον ο κώδικας έχει εφαρμοστεί ή εφαρμόζεται από έναν υπεύθυνο επεξεργασίας ή από τον εκτελούντα την επεξεργασία, καθώς και για να καταστούν οι διαδικασίες και οι δομές αυτές διαφανείς στα υποκείμενα των δεδομένων και στο ευρύ κοινό,
- αποδεικνύει, κατά την κρίση της αρμόδιας εποπτικής αρχής, ότι τα καθήκοντα και οι υποχρεώσεις του δεν συνεπάγονται σύγκρουση συμφερόντων.

Η αρμόδια εποπτική αρχή υποβάλλει τα σχέδια κριτηρίων πιστοποίησης του φορέα στο Συμβούλιο Προστασίας Δεδομένων.

Με την επιφύλαξη των καθηκόντων και των αρμοδιοτήτων της αρμόδιας εποπτικής αρχής, ο φορέας αναλαμβάνει, με την επιφύλαξη κατάλληλων εγγυήσεων, κατάλληλη δράση σε περίπτωση παράβασης του κώδικα από τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία, περιλαμβανομένης της αναστολής άσκησης καθηκόντων ή της εξαίρεσης του οικείου υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία από τον κώδικα. Ενημερώνει την αρμόδια εποπτική αρχή για τις δράσεις αυτές και για τους λόγους ανάληψής τους.

Η αρμόδια εποπτική αρχή ανακαλεί την πιστοποίηση φορέα εάν οι προϋποθέσεις πιστοποίησης δεν πληρούνται ή δεν πληρούνται πλέον ή οι ενέργειες που αναλήφθηκαν από τον φορέα παραβαίνουν τον παρόντα κανονισμό.

2.2.5.3 Πιστοποιήσεις

Τα κράτη μέλη, οι εποπτικές αρχές, το Συμβούλιο Προστασίας Δεδομένων και η Επιτροπή παροτρύνουν τη θέσπιση μηχανισμών πιστοποίησης προστασίας δεδομένων και σφραγίδων και σημάτων προστασίας δεδομένων με σκοπό την απόδειξη της συμμόρφωσης προς τον παρόντα κανονισμό των πράξεων επεξεργασίας από τους υπευθύνους επεξεργασίας και τους εκτελούντες την επεξεργασία. Λαμβάνονται υπόψη οι ειδικές ανάγκες των πολύ μικρών, των μικρών και των μεσαίων επιχειρήσεων. Η πιστοποίηση χορηγείται από τους φορείς πιστοποίησης ή από την αρμόδια εποπτική αρχή.

Πέραν της εφαρμογής τους από τους υπευθύνους επεξεργασίας ή από τους εκτελούντες την επεξεργασία που υπόκεινται στον παρόντα κανονισμό, οι μηχανισμοί πιστοποίησης της προστασίας δεδομένων και οι σφραγίδες και τα σήματα προστασίας δεδομένων που εγκρίνονται μπορούν να θεσπίζονται για τον σκοπό της απόδειξης ότι παρέχονται κατάλληλες εγγυήσεις από τους υπευθύνους επεξεργασίας ή τους εκτελούντες την επεξεργασία στο πλαίσιο των διαβιβάσεων δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες ή διεθνείς οργανισμούς

Η πιστοποίηση είναι εθελοντική και διαθέσιμη μέσω διαφανούς διαδικασίας και δεν περιορίζει την ευθύνη του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία για συμμόρφωση προς τον παρόντα κανονισμό. Ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία που υποβάλλει την επεξεργασία του στον μηχανισμό πιστοποίησης παρέχει στον φορέα πιστοποίησης κάθε πληροφορία και πρόσβαση στις δραστηριότητες επεξεργασίας που απαιτείται για τη διεξαγωγή της διαδικασίας πιστοποίησης. Η πιστοποίηση χορηγείται στον υπεύθυνο επεξεργασίας ή στον εκτελούντα την επεξεργασία για μέγιστη περίοδο τριών ετών και μπορεί να ανανεωθεί με τους ίδιους όρους, υπό την προϋπόθεση ότι εξακολουθούν να πληρούνται οι σχετικές απαιτήσεις. Η πιστοποίηση ανακαλείται, ανάλογα με την περίπτωση όταν δεν πληρούνται πλέον οι απαιτήσεις για την πιστοποίηση.

Το Συμβούλιο Προστασίας Δεδομένων συγκεντρώνει όλους τους μηχανισμούς πιστοποίησης

και τις σφραγίδες και τα σήματα προστασίας δεδομένων σε μητρώο και τα καθιστά διαθέσιμα στο κοινό με κάθε κατάλληλο μέσο.

2.2.5.4 Φορείς πιστοποίησης

Οι φορείς πιστοποίησης που διαθέτουν το ενδεδειγμένο επίπεδο εμπειρογνωμοσύνης σε σχέση με την προστασία των δεδομένων, αφού ενημερώσουν την εποπτική αρχή προκειμένου να μπορέσει να ασκήσει τις αρμοδιότητές της μπορούν πλέον να χορηγούν και να ανανεώνουν πιστοποιήσεις. Το κράτος μέλος διασφαλίζει ότι η διαπίστευση των εν λόγω φορέων πιστοποίησης πραγματοποιείται από ένα ή αμφότερα τα ακόλουθα:

- την εποπτική αρχή που είναι αρμόδια, και
- τον εθνικό οργανισμό διαπίστευσης που ορίζεται σύμφωνα με τον κανονισμό (ΕΚ) αριθ. 765/2008 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (1), σύμφωνα με το πρότυπο EN-ISO/IEC 17065/2012

Οι φορείς πιστοποίησης είναι διαπιστευμένοι σύμφωνα με την εν λόγω παράγραφο, μόνο εφόσον:

- έχουν αποδείξει την ανεξαρτησία και την εμπειρογνωμοσύνη τους σε σχέση με το αντικείμενο της πιστοποίησης κατά την κρίση της αρμόδιας εποπτικής αρχής,
- έχουν δεσμευτεί να σέβονται τα κριτήρια που αναφέρονται στο άρθρο 42 παράγραφος 5 και τα οποία έχουν εγκριθεί από την εποπτική αρχή που είναι αρμόδια δυνάμει του άρθρου 55 ή 56 ή από το Συμβούλιο Προστασίας Δεδομένων δυνάμει του άρθρου 63,
- έχουν θεσπίσει διαδικασίες για την έκδοση, την περιοδική επανεξέταση και την ανάκληση πιστοποιητικών, σφραγίδων και σημάτων προστασίας των δεδομένων,
- έχουν θεσπίσει διαδικασίες και δομές για τη διαχείριση καταγγελιών περί παραβάσεων της πιστοποίησης ή περί του τρόπου με τον οποίο η πιστοποίηση έχει εφαρμοστεί ή εφαρμόζεται από τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία, καθώς και για να καταστούν οι διαδικασίες και οι δομές αυτές διαφανείς στα υποκείμενα των δεδομένων και στο ευρύ κοινό,
- αποδεικνύουν, κατά την κρίση της αρμόδιας εποπτικής αρχής, ότι τα καθήκοντα και οι υποχρεώσεις τους δεν συνεπάγονται σύγκρουση συμφερόντων.

Η διαπίστευση των φορέων πιστοποίησης πραγματοποιείται βάσει των κριτηρίων που έχουν εγκριθεί από την εποπτική αρχή που είναι αρμόδια ή από το Συμβούλιο Προστασίας Δεδομένων.

Οι φορείς πιστοποίησης είναι υπεύθυνοι για την ορθή εκτίμηση που οδηγεί στην πιστοποίηση ή την ανάκληση της πιστοποίησης, με την επιφύλαξη της ευθύνης του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία για συμμόρφωση προς τον παρόντα κανονισμό. Η διαπίστευση χορηγείται για μέγιστη περίοδο πέντε ετών και μπορεί να ανανεωθεί με τους ίδιους όρους, υπό την προϋπόθεση ότι ο φορέας πιστοποίησης πληροί τις απαιτήσεις του παρόντος άρθρου.

Οι φορείς πιστοποίησης παρέχουν στις αρμόδιες εποπτικές αρχές τους λόγους χορήγησης ή ανάκλησης της αιτηθείσας πιστοποίησης

Το Συμβούλιο Προστασίας Δεδομένων συγκεντρώνει όλους τους μηχανισμούς πιστοποίησης και τις σφραγίδες προστασίας δεδομένων σε μητρώο και τα καθιστά διαθέσιμα στο κοινό με κάθε κατάλληλο μέσο.

Η αρμόδια εποπτική αρχή ή ο εθνικός οργανισμός διαπίστευσης ανακαλεί διαπίστευση σε φορέα πιστοποίησης εφόσον οι προϋποθέσεις πιστοποίησης δεν πληρούνται ή δεν πληρούνται πλέον ή εφόσον οι ενέργειες του φορέα πιστοποίησης παραβαίνουν τον παρόντα κανονισμό.

Η Επιτροπή μπορεί να εκδίδει εκτελεστικές πράξεις σχετικά με τη θέσπιση τεχνικών προτύπων για μηχανισμούς πιστοποίησης, σφραγίδες και σήματα προστασίας δεδομένων, καθώς και μηχανισμούς για την προώθηση και την αναγνώριση των εν λόγω μηχανισμών πιστοποίησης, σφραγίδων και σημάτων.

2.3 Προσφυγές, ευθύνη, κυρώσεις

Εικόνα 7

2.3.1 Προσφυγές

Με τον 2016/679 και τα άρθρα 77 έως 84, τα όποια περιλαμβάνονται σε αυτόν, περιγράφονται τα δικαιώματα του υποκείμενου δεδομένων στην χρήση κάθε νόμιμου μέσου, υποβολής καταγγελίας, προσφυγή στα δικαστήρια όταν θεωρεί/κρίνει ότι η αποθήκευση, επεξεργασία και διαγραφή των προσωπικών του δεδομένων δεν πραγματοποιήθηκε με βάση τον παρόντα κανονισμό. Με τον 2016/679 ορίζονται οι ευθύνες του υπευθύνου επεξεργασίας καθώς και οι προβλεπόμενες κυρώσεις εφόσον κριθεί ένοχος για σχετικές παραβάσεις.

Κάθε υποκείμενο δεδομένων έχει το δικαίωμα υποβολής καταγγελίας όταν θεωρεί ότι ο τρόπος με τον οποίο γίνεται η επεξεργασία των δεδομένων που το αφορά παραβαίνει τον παρόντα κανονισμό. Το υποκείμενο των δεδομένων έχει το δικαίωμα α) να υποβάλει καταγγελία σε εποπτική αρχή (ιδίως στο κράτος μέλος στο οποίο έχει τη συνήθη διαμονή του ή τον τόπο εργασίας του ή τον τόπο της εικαζόμενης παράβασης σε εποπτική αρχή) ή β) στον υπεύθυνο επεξεργασίας που εκτελεί την επεξεργασία.

α) Στην πρώτη περίπτωση, η εποπτική αρχή στην οποία έχει υποβληθεί η καταγγελία ενημερώνει τον καταγγέλλοντα για την πρόοδο και για την έκβαση της καταγγελίας, καθώς και για τη δυνατότητα άσκησης δικαστικής προσφυγής. Το υποκείμενο των δεδομένων έχει δικαίωμα δικαστικής προσφυγής, εφόσον η εποπτική αρχή που είναι αρμόδια δεν εξετάσει την καταγγελία ή δεν ενημερώσει το υποκείμενο των δεδομένων εντός τριών μηνών για την πρόοδο ή την έκβαση της καταγγελίας. Οι

διαδικασίες κατά της εποπτικής αρχής κινούνται ενώπιον των δικαστηρίων του κράτους μέλους στο οποίο είναι εγκατεστημένη η εποπτική αρχή. Το φυσικό ή νομικό πρόσωπο έχει το δικαίωμα δικαστικής προσφυγής κατά νομικά δεσμευτικής απόφασης της εποπτικής αρχής που το αφορά ή εάν θεωρεί ότι παραβιάστηκαν τα δικαιώματά του.

β) Στην δεύτερη περίπτωση, η διαδικασία κατά του υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία κινείται ενώπιον των δικαστηρίων του κράτους μέλους στο οποίο ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία έχουν εγκατάσταση. Εναλλακτικά, η εν λόγω διαδικασία μπορεί να κινηθεί ενώπιον των δικαστηρίων του κράτους μέλους στο οποίο το υποκείμενο των δεδομένων έχει τη συνήθη διαμονή του, εκτός εάν ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία είναι δημόσια αρχή κράτους μέλους.

Κατά την διάρκεια των δικαστικών διαδικασιών ο υπεύθυνος επεξεργασίας μπορεί να απαλλαχθεί από την ευθύνη εάν αποδείξει ότι δεν φέρει καμία ευθύνη για την παράβαση για την οποία διώκεται. Εάν περισσότεροι του ενός υπεύθυνοι επεξεργασίας εμπλέκονται στην ίδια επεξεργασία και εν δυνάμει είναι υπεύθυνοι για τυχόν ζημία που προκάλεσε η επεξεργασία, κάθε υπεύθυνος επεξεργασίας ευθύνεται για τη συνολική ζημία έτσι ώστε να διασφαλιστεί η αποτελεσματική αποζημίωση του υποκειμένου των δεδομένων.

Σε αντίθετη περίπτωση και εφόσον αποδειχθεί ότι το υποκείμενο δεδομένων υπέστη υλική ή μη υλική ζημία ως αποτέλεσμα παραβίασης του παρόντος κανονισμού, τότε το υποκείμενο δεδομένων δικαιούται αποζημίωση από τον υπεύθυνο επεξεργασίας για τη ζημία που υπέστη. Κάθε υπεύθυνος επεξεργασίας που συμμετέχει στην επεξεργασία είναι υπεύθυνος για τη ζημία που προκάλεσε η εκ μέρους του επεξεργασία που παραβαίνει τον παρόντα κανονισμό. Ο εκτελών την επεξεργασία ευθύνεται για τη ζημία που προκάλεσε η επεξεργασία μόνο εφόσον δεν ανταποκρίθηκε στις υποχρεώσεις του παρόντος κανονισμού που αφορούν ειδικότερα τους εκτελούντες την επεξεργασία ή υπερέβη ή ενήργησε αντίθετα προς τις νόμιμες εντολές του υπευθύνου επεξεργασίας. Εάν ο υπεύθυνος επεξεργασίας έχει καταβάλει, πλήρη αποζημίωση για τη ζημία που προκάλεσε, ο εν λόγω υπεύθυνος δικαιούται να ζητήσει από τους άλλους υπευθύνους επεξεργασίας που εμπλέκονται στην ίδια επεξεργασία την ανάκτηση μέρους της αποζημίωσης που αντιστοιχεί στο μέρος της ευθύνης τους λόγω της ζημίας που προκλήθηκε.

2.3.2 Κυρώσεις

Κάθε εποπτική αρχή είναι υπεύθυνη ώστε η επιβολή των διοικητικών προστίμων για κάθε περίπτωση να είναι αποτελεσματική, αναλογική και αποτρεπτική. Τα διοικητικά πρόστιμα είναι διαφορετικά για κάθε περίσταση και επιβάλλονται επιπρόσθετα ή αντί των μέτρων που αναφέρονται στον παρόντα κανονισμό.

Κατά τη λήψη μιας απόφασης σχετικά με την επιβολή και το ύψος ενός διοικητικού προστίμου, λαμβάνονται υπόψη τα ακόλουθα:

- η φύση, η βαρύτητα και η διάρκεια της παράβασης,
- ο δόλος ή η αμέλεια που προκάλεσε την παράβαση,
- οι ενέργειες στις οποίες προέβη ο υπεύθυνος επεξεργασίας για να μετριάσει τη ζημία,
- ο βαθμός ευθύνης του υπευθύνου επεξεργασίας λαμβάνοντας υπόψη τα τεχνικά και οργανωτικά μέτρα,
- τυχόν σχετικές προηγούμενες παραβάσεις του υπευθύνου επεξεργασίας,
- ο βαθμός συνεργασίας με την αρχή ελέγχου για την επανόρθωση της παράβασης και τον περιορισμό των πιθανών δυσμενών επιπτώσεών της,
- οι κατηγορίες δεδομένων προσωπικού χαρακτήρα που επηρεάζει η παράβαση,
- ο τρόπος με τον οποίο η εποπτική αρχή πληροφορήθηκε την παράβαση,
- σε περίπτωση που διατάχθηκε προηγουμένως η λήψη μέτρων κατά του εμπλεκόμενου υπευθύνου επεξεργασίας σχετικά με το ίδιο αντικείμενο, η συμμόρφωση με τα εν λόγω μέτρα,
- η τήρηση εγκεκριμένων κωδίκων δεοντολογίας σύμφωνα με τον παρόν κανονισμό,
- κάθε άλλο επιβαρυντικό ή ελαφρυντικό στοιχείο που προκύπτει από τις περιστάσεις της συγκεκριμένης περίπτωσης, όπως τα οικονομικά οφέλη που αποκομίσθηκαν ή των ζημιών που

αποφεύχθηκαν, άμεσα ή έμμεσα, από την παράβαση.

Ανάλογα με το είδος των παραβάσεων επισύρονται διαφορετικά διοικητικά πρόστιμα. Το ύψος των διοικητικών προστίμων ορίζεται μέσα στα άρθρα του παρόντος κανονισμού. Στην περίπτωση που ο υπεύθυνος επεξεργασίας παραβιάζει αρκετές διατάξεις του παρόντος κανονισμού, το συνολικό ύψος του διοικητικού προστίμου δεν υπερβαίνει το ποσό που ορίζεται για τη βαρύτερη από τις παραβάσεις.

Το μέγιστο των διοικητικών προστίμων που μπορεί να επιβληθούν βάσει των άρθρων του παρόντος κανονισμού είναι έως είκοσι εκατομμύρια ευρώ ή σε περίπτωση επιχειρήσεων έως το 4% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους, ανάλογα με το ποιο είναι υψηλότερο.

Όσον αφορά κυρώσεις οι οποίες δεν αποτελούν διοικητικά πρόστιμα τα κράτη μέλη θεσπίζουν τους κανόνες. Τα κράτη μέλη υλοποιούν όλα τα αναγκαία μέτρα ώστε οι κυρώσεις αυτές να εφαρμόζονται. Οι εν λόγω κυρώσεις πρέπει να είναι αποτελεσματικές, αναλογικές και αποτρεπτικές. Κάθε κράτος μέλος κοινοποιεί στην Επιτροπή τις διατάξεις που θεσπίζει χωρίς καθυστέρηση καθώς και κάθε επακολουθούσα τροποποίησή τους.

2.4 Σύγκριση του νέου κανονισμού 2016/679 με την οδηγία 95/46/ΕΚ

Εικόνα 8

Ο 2016/679 αποτελεί κανονισμό της Ευρωπαϊκής ένωσης ο όποιος καταργεί την οδηγία 95/46/ΕΚ και συνεπώς και τοπική διάταξη που δημιουργήθηκε για τις ανάγκες του. Οι παραπομπές στην καταργούμενη οδηγία θεωρούνται παραπομπές στον παρόντα κανονισμό. Ο 2016/679 σε σχέση με την 95/46/ΕΚ, αλλάζει ριζικά τον τρόπο με τον οποίο η Ευρωπαϊκή Ένωση:

- θεσπίζει και ανανεώνει τους κανόνες που αφορούν την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και τους κανόνες που αφορούν την ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα,
- προστατεύει τα θεμελιώδη δικαιώματα και ελευθερίες των φυσικών προσώπων και ειδικότερα το δικαίωμά τους στην προστασία των δεδομένων προσωπικού χαρακτήρα,

- ελέγχει και παρακολουθεί την τήρηση αυτών των κανόνων

Γενικότερα, ο 2016/679 είναι μια εκτεταμένη έκδοση της τρέχουσας οδηγίας. Η ανανέωσή του σε σχέση με την τρέχουσα οδηγία έχει να κάνει τόσο στην προσθήκη νέων σημείων που δεν καλύπτονταν στο παρελθόν, όσο και στην επέκταση και την λεπτομερή ανάλυση σημείων που ήδη υπάρχουν στην οδηγία, ώστε να μπορεί να θεσμοθετήσουν έναν ολοκληρωμένο κανονισμό.

Τα σημεία τα οποία προστέθηκαν έχουν να κάνουν με τεχνικούς όρους και μη, οι οποίοι δεν υπήρχαν παλαιότερα. Έχουν να κάνουν με καινούρια όργανα, ρόλους και διαδικασίες οι οποίες δημιουργήθηκαν με την εξέλιξη της τεχνολογίας και τις νέες ανάγκες που δημιουργούνται από αυτήν την εξέλιξη αυτή.

Ο 2016/679 εισάγει και καθιερώνει νέους ορισμούς, όρους και ορολογίες, οι οποίες δεν υπήρχαν παλαιότερα και οι οποίες φυσικά δεν συμπεριλαμβάνονται στον τρέχοντα κανονισμό, παραδείγματα όπως η «ψευδωνυμοποίηση», η «κατάρτιση προφίλ», τα «γενετικά δεδομένα», τα «βιομετρικά δεδομένα», η «υπηρεσία της κοινωνίας των πληροφοριών» και άλλους.

Με τον 2016/679, δημιουργείται το Ευρωπαϊκό Συμβούλιο Προστασίας Προσωπικών δεδομένων ως το όργανο ελέγχου των εποπτικών αρχών των κρατών μελών.

Στο κομμάτι του κώδικα δεοντολογίας καθιερώνονται οι φορείς παρακολούθησης καθώς και οι φορείς πιστοποίησης. Οι φορείς παρακολούθησης θα διεξάγουν την παρακολούθηση της συμμόρφωσης με τον κώδικα δεοντολογίας. Οι φορείς πιστοποίησης αφού ενημερώσουν την εποπτική αρχή προκειμένου να μπορέσει να ασκήσει τις αρμοδιότητές της μπορούν πλέον να χορηγούν, να ανανεώνουν και να ανακαλούν πιστοποιήσεις.

Σημαντική διαφοροποίηση μεταξύ των δύο είναι στο κομμάτι των διοικητικών κυρώσεων όπου εκεί οι κυρώσεις γίνονται αναλογικές των συμβάντων και μεγάλες σε κόστος για τους οργανισμούς οι οποίοι δεν συμμορφώνονται. Είναι χαρακτηριστικό ότι με τον 2016/679 τα διοικητικά πρόστιμα μπορεί να φτάσουν τα είκοσι εκατομμύρια ευρώ ή σε περίπτωση επιχειρήσεων έως το 4% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους, ανάλογα με το ποιο είναι υψηλότερο.

Ο 2016/679 επεκτείνει και συγκεκριμενοποιεί τα δικαιώματα και όλα αυτά που αφορούν το υποκείμενο των δεδομένων, κάτι που ήταν πιο γενικό και όχι τόσο ξεκάθαρο στην υπάρχουσα οδηγία και άφηνε τις λεπτομέρειες να νομοθετούνται από το εκάστοτε κράτος μέλος.

Πολύ σημαντικό επίσης είναι ότι ο 2016/679 επεκτείνει και δίνει κατευθύνσεις για συγκεκριμένες υλοποιήσεις που αφορούν τον υπεύθυνο προστασίας των προσωπικών δεδομένων και σε όλους τους νέους ρόλους που χρειάζονται για την σωστή διαχείριση των προσωπικών δεδομένων από έναν οργανισμό.

3. Πλαίσιο προετοιμασίας για το νέο κανονισμό 2016/679

Σε αυτό το κεφάλαιο παρουσιάζεται μια σειρά από βήματα, στάδια/φάσεις και προτεινόμενες λύσεις/προιόντα για την υλοποίηση των εργασιών τα οποία θα βοηθήσουν τους οργανισμούς και τις ομάδες ασφάλειας τους να κατανοήσουν και να αναγνωρίσουν πιο γρήγορα και εύκολα τις απαραίτητες ενέργειες που θα πρέπει να πραγματοποιηθούν ώστε να επιτευχθεί η συμμόρφωση με τον 2016/679. Οι ομάδες ασφάλειας ακολουθώντας τα παρακάτω βήματα, λαμβάνοντας υπόψιν τις παρακάτω αναφορές και φυσικά μαζί με τους άλλους πόρους που προσφέρουν οι εποπτικές αρχές, θα μπορέσουν να προετοιμαστούν κατάλληλα για τον 2016/679.

Ένας οργανισμός είναι απαραίτητο να σχεδιάσει από τώρα την προσέγγιση για τη συμμόρφωση με τον 2016/679 ώστε να επιτύχει όσο το δυνατό γρηγορότερα την ενημέρωση των βασικών ανθρώπων του οργανισμού, οι οποίοι πιθανόν θα αναλάβουν μελλοντικά τους αντίστοιχους ρόλους στην ομάδα ασφαλείας.

Πολλές από τις βασικές έννοιες και αρχές του 2016/679 είναι παρόμοιες με εκείνες της τρέχουσας οδηγίας. Εφόσον, ένας οργανισμός συμμορφώνεται ήδη με την τρέχουσα οδηγία, τότε το μεγαλύτερο μέρος της προσέγγισης στην συμμόρφωση, θα παραμείνει έγκυρη στο πλαίσιο του 2016/679.
Ορισμένα τμήματα του 2016/679 θα έχουν μεγαλύτερο αντίκτυπο σε ορισμένους οργανισμούς από ό,τι σε άλλους.

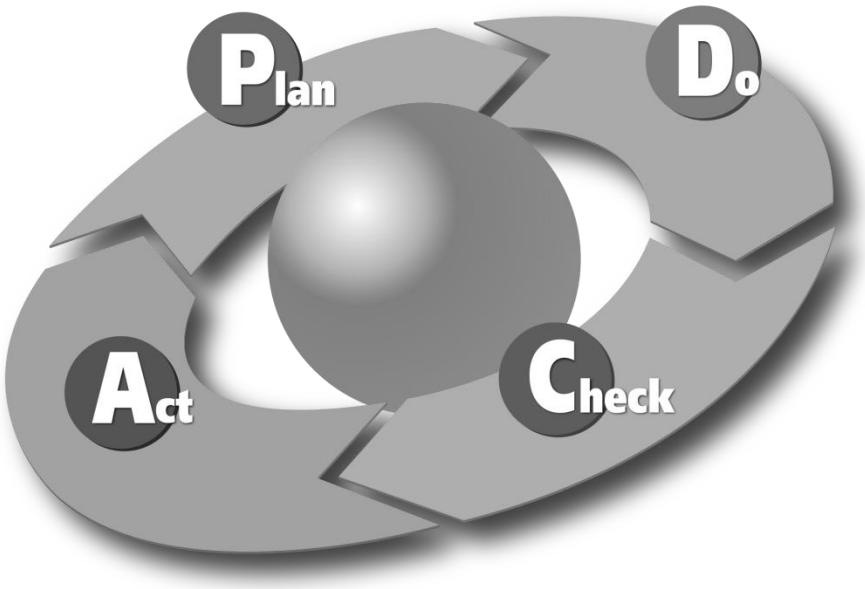
Ωστόσο, υπάρχουν νέα στοιχεία και σημαντικές βελτιώσεις που έρχονται μαζί με τον 2016/679. Υπό αυτήν την εννοια σε κάποια σημεία θα χρειαστεί, σίγουρα, υλοποίηση από την αρχή καθώς επίσης και κάποια σχετική ανανέωση σε κάποια άλλα σημεία

Θα χρειαστεί να τεθούν σε εφαρμογή νέες διαδικασίες για την αντιμετώπιση των νέων διατάξεων διαφάνειας και των δικαιωμάτων των πολιτών με βάση των 2016/679. Σε έναν μεγάλο ή πολύπλοκο οργανισμό, αυτό θα μπορούσε να έχει σημαντικές επιπτώσεις στον προϋπολογισμό, στο κομμάτι του IT, στην διεύθυνση προσωπικού και στις επικοινωνίες.

Ο 2016/679 δίνει μεγαλύτερη έμφαση στην τεκμηρίωση που πρέπει να τηρούν οι ελεγκτές δεδομένων για να αποδείξουν την ευθύνη τους. Η συμμόρφωση με όλες τις περιοχές που αναφέρονται στο παρόν έγγραφο απαιτεί από τους οργανισμούς να αναθεωρήσουν την προσέγγισή τους στη διακυβέρνηση και τον τρόπο με τον οποίο διαχειρίζονται την προστασία δεδομένων ως εταιρικό ζήτημα.

3.1 Φάσεις υλοποίησης της προετοιμασίας επί του 2016/679

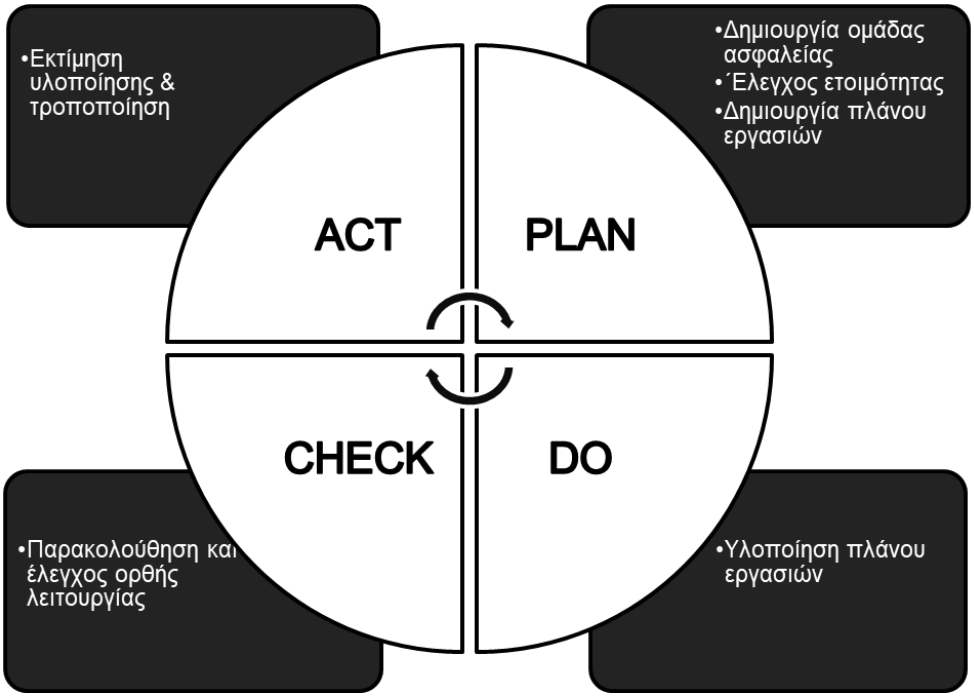
Εικόνα 8 [18] - Κύκλος του Deming



Καλό θα ήταν για την ομάδα ασφάλειας, για να επιτύχει το συντομότερο δυνατό και με μεγαλύτερη επιτυχία την συμμόρφωση με τον νέο κανονισμό, να ακολουθήσει την μέθοδο του Deming ή αλλιώς γνωστή ως κύκλος του Deming [18]. Η συγκεκριμένη μέθοδος προτείνεται λόγω της επαναληπτικής της μορφής η οποία βοηθάει πολύ στον έλεγχο και στην συνεχή βελτίωση των διαδικασιών ενός οργανισμού. Η συγκεκριμένη μέθοδος διαχείρισης είναι χωρισμένη σε τέσσερις φάσεις: PDCA (plan-do-check-act) όπου σε κάθε φάση εκτελούνται συγκεκριμένες εργασίες.

Είναι χαρακτηριστικό ότι η συγκεκριμένη μέθοδος ακολουθείται από τις ομάδες ασφάλειας και στα πλαίσια πιστοποίησης ενός οργανισμού στο σύστημα διαχείρισης της ασφάλειας των πληροφοριών, γνωστά ως ISO27001 ή PCI.

Εικόνα 9 – Βήματα εργασιών ανά φάση υλοποίησης



3.1.1 PLAN

Η φάση αυτή αποτελεί το στρατηγικό σχεδιασμό της συμμόρφωσης με τον νέο κανονισμό. Σε αυτήν την φάση γίνεται ο καθορισμός των γενικών κατευθύνσεων για τη συμμόρφωση του οργανισμού με τον 2016/679. Υπό προϋποθέσεις, εάν και εφόσον δεν υφίσταται ομάδα ασφάλειας, καλό είναι να γίνει σύσταση της ομάδας ώστε να είναι ξεκάθαροι οι ρόλοι και πιο αποτελεσματική η εφαρμογή των απαραίτητων ενεργειών για την επίτευξη του στόχου του οργανισμού που είναι η συμμόρφωση με τον νέο κανονισμό. Είναι περιττό να αναφέρουμε ότι αποτελεί την πιο σημαντική φάση.

Σε αυτή την φάση ο οργανισμός καλείται να εκτελέσει τα εξής βήματα:

- ❏ Δημιουργία ομάδας ασφαλείας
- ❏ Έλεγχος ετοιμότητας
- ❏ Δημιουργία πλάνου εργασιών

Παρακάτω θα αναλυθούν λεπτομερώς τα βήματα αυτά.

3.1.2 DO

Σε αυτήν την φάση υλοποιούνται οι εργασίες που αποφασίστηκαν στην προηγούμενη φάση. Οι εργασίες υλοποιούνται βάσει του πλάνου εργασιών που εκπονήθηκε στην προηγούμενη φάση.
Αυτές οι εργασίες μπορεί να είναι τόσο στο επιχειρησιακό κομμάτι του οργανισμού όσο και στο υλικοτεχνικό του κομμάτι.

3.1.3 CHECK

Σε αυτή την φάση γίνεται η παρακολούθηση των όσων υλοποιήθηκαν από το παραπάνω βήμα για τυχόν ανίχνευση παραλείψεων ή λαθών στα συστήματα, στις εφαρμογές ακόμα και στο κομμάτι των πολιτικών και των διαδικασιών.

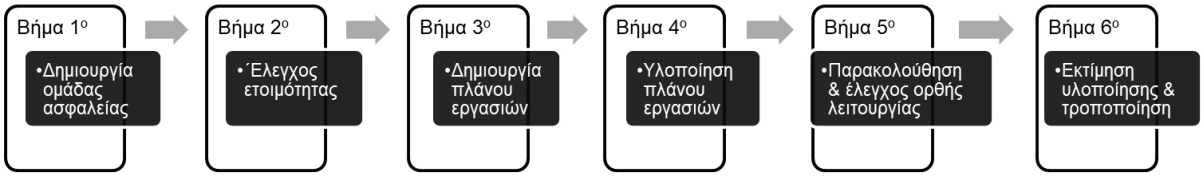
3.1.4 ACT

Σε αυτή τη φάση πραγματοποιούνται έλεγχοι για την διασφάλιση της ορθής εφαρμογής των επιλεγμένων μέτρων και της αποτελεσματικότητας των μέτρων να αντιμετωπίσουν τα πραγματικά και πιθανώς μεταβαλλόμενα προβλήματα ασφάλειας.

Οι έλεγχοι αυτοί μπορεί να είναι εσωτερικοί ή εξωτερικοί έλεγχοι από ανεξάρτητους φορείς. Ανάλογα με τα αποτελέσματα των ελέγχων ενδέχεται να προκύψει η ανάγκη για αναθεώρηση. Ο έλεγχος της αναθεώρησης θα πρέπει να πραγματοποιείται ανεξάρτητα από το εάν θα γίνουν τελικά οι αλλαγές ή όχι.

3.2 Τα βήματα για μια επιτυχημένη προετοιμασία

Εικόνα 10 – Τα 6 βήματα για την επίτευξη της συμμόρφωσης



3.2.1 Βήμα 1ο Δημιουργία ομάδας ασφαλείας

Σε αυτό το βήμα, ο οργανισμός θα πρέπει να δημιουργήσει τον προσανατολισμό και να ορίσει τους στόχους τους οποίους θα πρέπει να εκπληρώσει ώστε να επιτύχει τη συμμόρφωσή του με τον 2016/679. Ο οργανισμός σε αυτό το βήμα θα πρέπει να εντοπίσει όλα τα ενδιαφερόμενα μέρη και εφόσον δεν υπάρχει ήδη ομάδα ασφάλειας, να την καταρτίσει. Η ομάδα ασφάλειας θα πρέπει να εκπληρώσει τους στόχους για την συμμόρφωση με τον 2016/679. Επίσης, βάσει του 2016/79 θα πρέπει να οριστούν οι νέοι ρόλοι μέσα στην ομάδα, με προτεραιότητα αυτή του υπευθύνου προστασίας των δεδομένων η οποία είναι υποχρεωτική και πάρα πολύ σημαντική λόγω καθηκόντων.

Σε αυτό το βήμα, όπως είναι λογικό ο οργανισμός θα πρέπει να διαθέσει τους απαραίτητους πόρους και να ορίσει τον προϋπολογισμό ώστε να επιτύχει την συμμόρφωση με τον 2016/679. Επειδή προαναφέραμε, στον 2016/679 τα μεγέθη όσον αφορά τις κυρώσεις και τα πρόστιμα είναι μεγάλα.

3.2.2 Βήμα 2ο Έλεγχος ετοιμότητας

Σε αυτό το βήμα η ομάδα ασφάλειας θα πρέπει να ελέγξει την ετοιμότητα στην οποία βρίσκεται ο οργανισμός σε σχέση με τον 2016/679 για την προστασία και την επεξεργασία των προσωπικών δεδομένων. Βασική προϋπόθεση είναι η ομάδα ασφάλειας να γνωρίζει την αλλαγή του νόμου και να έχει μελετήσει τον νέο κανονισμό. Η ομάδα ασφάλειας σε αυτό το βήμα θα πρέπει να αξιολογήσει τους κινδύνους με βάση τον νέο κανονισμό και την υπάρχουσα πολιτική ασφάλειας που εφαρμόζει ο οργανισμός και να ορίσει τις απαραίτητες ενέργειες για την συμμόρφωση με τον νέο κανονισμό. Η υπάρχουσα πολιτική ασφάλειας θα ακολουθεί και συμμορφώνεται με την υπάρχουσα ευρωπαϊκή οδηγία

η οποία θα θεωρείται παρωχημένη. Η ομάδα ασφάλειας θα πρέπει να ευαισθητοποιηθεί και να αναλύσει την ροή των προσωπικών δεδομένων, να διεξαγάγει απογραφή των δεδομένων και να κάνει εκτίμηση του κινδύνου εντοπίζοντας τα κενά μεταξύ της υπάρχουσας πολιτικής ασφαλείας της και του νέου κανονισμού.

Με βάση τον νέο κανονισμό, θα πρέπει να δοθεί ιδιαίτερη έμφαση στα παρακάτω χαρακτηριστικά ώστε η ομάδα ασφάλειας να καταφέρει να επιτύχει σύντομα την συμμόρφωση με τον νέο κανονισμό.

3.2.2.1 Προστασία των δεδομένων από τον σχεδιασμό και εκτίμηση των επιπτώσεων στην προστασία δεδομένων

Είναι καλή πρακτική η υιοθέτηση μιας προσέγγισης απορρήτου από το σχεδιασμό και η πραγματοποίηση μιας αξιολόγησης των επιπτώσεων στην ιδιωτική ζωή, ως μέρος αυτής. Ωστόσο, ο 2016/679 καθιστά την προστασία της ιδιωτικής ζωής από κατασκευής ρητή νομική απαίτηση, με τον όρο «προστασία δεδομένων από το σχεδιασμό και από προεπιλογή». Επίσης, καθιστά υποχρεωτικές τις Αξιολογήσεις Επιπτώσεων Προστασίας Δεδομένων» ή ΑΔΕΑ στις περιπτώσεις όπου η επεξεργασία δεδομένων ενδέχεται να έχει ως αποτέλεσμα υψηλό κίνδυνο για τα άτομα, για παράδειγμα:

- ❑ όπου αναπτύσσεται μια νέα τεχνολογία.
- ❑ όταν μια δραστηριότητα δημιουργίας προφίλ μπορεί να επηρεάσει σημαντικά τα άτομα
- ❑ όπου υπάρχει μεγάλης κλίμακας επεξεργασία των ειδικών κατηγοριών δεδομένων.

Εάν μια ΑΔΕΑ υποδεικνύει ότι η επεξεργασία των προσωπικών δεδομένων είναι υψηλού κινδύνου και δεν είναι δυνατόν να αντιμετωπίσει επαρκώς, ο οργανισμός θα πρέπει να συμβουλευτεί την τοπική εποπτική αρχή για να ζητήσει τη γνώμη της σχετικά με το εάν η επεξεργασία είναι σύμφωνη με το νέο κανονισμό.

Είναι φυσικό ότι ο οργανισμός να πρέπει να αξιολογήσει τις καταστάσεις στις οποίες θα χρειαστεί να πραγματοποιηθεί μια ΑΔΕΑ.

3.2.2.2 Υπεύθυνος προστασίας δεδομένων

Θα πρέπει να οριστεί κάποιος για να αναλάβει την ευθύνη για τη συμμόρφωση με την προστασία των δεδομένων. Θα πρέπει να εξεταστεί αν πρέπει να οριστεί επισήμως ένας υπεύθυνος προστασίας δεδομένων.

Πρέπει να οριστεί ένας υπεύθυνος προστασίας δεδομένων αν ο οργανισμός είναι:

- ❑ δημόσια αρχή (εκτός από τα δικαστήρια που ενεργούν υπό την ιδιότητά τους ως δικαστών),
- ❑ ένας οργανισμός που πραγματοποιεί την τακτική και συστηματική παρακολούθηση ατόμων σε μεγάλη κλίμακα, ή
- ❑ ένας οργανισμός που διεξάγει τη μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων, όπως τα αρχεία υγείας ή πληροφορίες σχετικά με ποινικές καταδίκες.

Είναι σημαντικό ότι κάποιος μέσα στον οργανισμό ή ένας εξωτερικός σύμβουλος προστασίας δεδομένων πρέπει να αναλάβει την ευθύνη για τη συμμόρφωση του οργανισμού για την προστασία των δεδομένων και να έχει τη γνώση, την υποστήριξη και την εξουσία να εκτελεί αποτελεσματικά τα καθήκοντά του με βάση τον ρόλο του.

3.2.2.3 Προσωπικά δεδομένα που κατέχει και επεξεργάζεται ο οργανισμός

Θα πρέπει ο οργανισμός να είναι σε θέση να τεκμηριώσει ποια προσωπικά δεδομένα κρατάει/συντηρεί στα συστήματά του, από πού προήλθαν αυτά τα δεδομένα και με ποιον τρίτο οργανισμό τα μοιράζεται. Θα χρειαστεί να πραγματοποιηθεί έλεγχος των πληροφοριών σε ολόκληρο τον οργανισμό ή σε συγκεκριμένους επιχειρηματικούς τομείς.

Ο 2016/679 απαιτεί να διατηρούνται αρχεία των δραστηριοτήτων επεξεργασίας των δεδομένων προσωπικού χαρακτήρα. Επίσης, απαιτεί την άμεση ανανέωση σε περίπτωση αλλαγής αυτών. Για παράδειγμα, εάν υπάρχουν ανακριβή προσωπικά δεδομένα τα οποία έχουν μοιραστεί με κάποιον άλλο οργανισμό, θα πρέπει ο άλλος οργανισμός να ενημερώνεται για την ανακρίβεια των στοιχείων ώστε να μπορέσει να διορθώσει τα δικά του αρχεία. Αυτό σαν διαδικασία δεν μπορεί να επιτευχθεί εάν ο οργανισμός δεν γνωρίζει ποια προσωπικά δεδομένα διατηρεί, από πού προέρχονται και με ποιον τα μοιράζεται. Το παραπάνω θα βοηθήσει τον οργανισμό να συμμορφωθεί με την αρχή της λογοδοσίας του 2016/679, η οποία απαιτεί από τους οργανισμούς να είναι σε θέση να δείξουν και να τεκμηριώσουν τον τρόπο με τον όποιο συμμορφώνονται Εδώ είναι απαραίτητη η δημιουργία και η εφαρμογή συγκεκριμένων πολιτικών και διαδικασιών.

3.2.2.4 Συγκατάθεση

Η συγκατάθεση πρέπει να παρέχεται ελεύθερα, να είναι συγκεκριμένη, ενημερωμένη και χωρίς αμφιβολία. Η συγκατάθεση πρέπει να είναι θετική και ξεχωριστή από άλλους όρους και προϋποθέσεις. Επίσης είναι απαραίτητο να υπάρχουν απλοί τρόποι για την απόσυρσή της από το υποκείμενο. Ο οργανισμός θα πρέπει να ελέγξει τον τρόπο που ζητείται, καταγράφεται και διαχειρίζεται τη συγκατάθεσή ενός υποκειμένου και αν πρέπει να κάνει τις απαραίτητες αλλαγές. Η συγκατάθεση πρέπει να είναι επαληθεύσιμη και τα άτομα γενικά να έχουν περισσότερα δικαιώματα, όταν αυτή βασίζεται στη συναίνεση για την επεξεργασία των δεδομένων τους.

3.2.2.5 Παιδιά

Θα πρέπει να γίνει ειδική μελέτη για το εάν πρέπει να εγκατασταθούν συστήματα για την επαλήθευση της ηλικίας των ατόμων και να λαμβάνεται η συγκατάθεση των γονέων ή των κηδεμόνων για οποιαδήποτε δραστηριότητα επεξεργασίας δεδομένων παιδιών.

Για πρώτη φορά, με τον νέο κανονισμό, θα υπάρξει ειδική προστασία για τα προσωπικά δεδομένα των παιδιών, ιδίως στο πλαίσιο των εμπορικών υπηρεσιών διαδικτύου όπως η κοινωνική δικτύωση. Εάν ο οργανισμός προσφέρει σε παιδιά ηλεκτρονικές υπηρεσίες («υπηρεσίες της κοινωνίας της πληροφορίας») και βασίζεται στη συγκατάθεσή τους για τη συλλογή πληροφοριών σχετικά με αυτές, τότε ίσως χρειαστεί η συγκατάθεση του γονέα ή του κηδεμόνα για τη νόμιμη επεξεργασία των προσωπικών δεδομένων τους. Ο νέος κανονισμός θέτει την ηλικία όπου ένα παιδί μπορεί να δώσει, το ίδιο, τη συγκατάθεσή του για την επεξεργασία των προσωπικών του δεδομένων στα 16 έτη. Για παιδιά μικρότερα από αυτήν την ηλικία θα χρειαστεί η συγκατάθεση του ατόμου που έχει την «γονική μέριμνα» του παιδιού.

Αυτό θα μπορούσε να έχει σημαντικές επιπτώσεις εάν ο οργανισμός προσφέρει επιγραμμικές/διαδικτυακές υπηρεσίες σε παιδιά και συλλέγει τα προσωπικά τους δεδομένα. Η συναίνεση πρέπει να είναι επαληθεύσιμη και η ειδοποίηση για την προστασία της ιδιωτικής ζωής πρέπει να είναι γραμμένη σε γλώσσα που τα παιδιά θα κατανοούν.

3.2.2.6 Κοινοποίηση πληροφοριών απορρήτου

Θα πρέπει να αναθεωρηθούν οι τρέχουσες ειδοποιήσεις απορρήτου και να δημιουργηθεί ένα σχέδιο για την πραγματοποίηση των απαραίτητων αλλαγών εγκαίρως με βάση τον 2016/679. Όταν γίνεται συλλογή προσωπικών δεδομένων, πρέπει να κοινοποιούνται στους χρήστες συγκεκριμένες πληροφορίες, όπως η ταυτότητα του οργανισμού και ο τρόπος με τον οποίο σκοπεύει ο οργανισμός να χρησιμοποιήσει τις πληροφορίες που ζητάει και συλλέγει από το υποκείμενο Αυτό γίνεται συνήθως μέσω της ειδοποίησης απορρήτου.

Με τον νέο κανονισμό, όμως, υπάρχουν μερικά επιπλέον πράγματα που θα πρέπει να κοινοποιούνται στα υποκείμενα των δεδομένων. Για παράδειγμα, θα πρέπει να εξηγείτε τη νόμιμη βάση σας για την επεξεργασία των δεδομένων, τις περιόδους αποθήκευσης δεδομένων σας και ότι τα άτομα

έχουν δικαίωμα να διαμαρτυρηθούν στις τοπικές εποπτικές αρχές εάν πιστεύουν ότι υπάρχει κάποιο πρόβλημα με τον τρόπο που χειρίζεστε τα δεδομένα τους. Με βάση τον 2016/679 απαιτείται όλες αυτές οι πληροφορίες να παρέχονται με συνοπτική, κατανοητή και σαφή γλώσσα.

3.2.2.7 Δικαιώματα των πολιτών

Η ομάδα ασφάλειας πρέπει να γνωρίζει όλα τα δικαιώματα των υποκειμένων των δεδομένων ώστε να είναι σε θέση να ελέγξει τις διαδικασίες του οργανισμού και να βεβαιωθεί ότι καλύπτουν όλα τα δικαιώματα, συμπεριλαμβανομένου του τρόπου με τον οποίο γίνεται η διαγραφή των προσωπικών δεδομένων ή του τρόπου με τον οποίο τα δεδομένα αυτά παρέχονται ηλεκτρονικά και μορφή που χρησιμοποιείται συνήθως.

Σε γενικές γραμμές, τα δικαιώματα του υποκειμένου των δεδομένων στον νέο κανονισμό είναι τα ίδια με εκείνα που απορρέουν από την «Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα», με κάποιες σημαντικές βελτιώσεις. Εάν ο οργανισμός είναι ήδη προσανατολισμένος με βάση την «Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα», τότε η μετάβαση στο νέο κανονισμό πρέπει να είναι σχετικά εύκολη.

Ο 2016/679 περιλαμβάνει τα ακόλουθα δικαιώματα για ιδιώτες:

- το δικαίωμα ενημέρωσης,
- το δικαίωμα πρόσβασης,
- το δικαίωμα διόρθωσης,
- το δικαίωμα διαγραφής,
- το δικαίωμα περιορισμού της επεξεργασίας,
- το δικαίωμα στη φορητότητα δεδομένων,
- το δικαίωμα ένστασης,
- το δικαίωμα να μην υπόκεινται σε αυτοματοποιημένη λήψη αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ.

Ιδιαίτερη προσοχή θα πρέπει να δοθεί στα παρακάτω, αφού με τον νέο κανονισμό γίνεται πολύ συγκεκριμένος και πλέον απαιτητικός ο τρόπος που ένας οργανισμός θα πρέπει να διαχειρίζεται τις αιτήσεις για την διαγραφή, την μεταφορά και την πρόσβαση στα δεδομένα, από το υποκείμενο.

Αιτήσεις διαγραφής

Ο οργανισμός θα πρέπει να ελέγξει τις διαδικασίες του και να σχεδιάσει τον τρόπο με τον όποιο θα αντιδρούσε εάν κάποιος του ζητούσε να διαγραφούν τα προσωπικά του δεδομένα. Για παράδειγμα, θα μπορούσαν τα υπάρχοντα συστήματα να βοηθήσουν ώστε να εντοπιστούν και να διαγραφούν τα δεδομένα αυτά; Ποιος θα πάρει τις αποφάσεις σχετικά με τη διαγραφή;

Το δικαίωμα μεταφοράς δεδομένων είναι κάτι νέο. Ισχύει μόνο:

- στα προσωπικά δεδομένα που έχει υποβάλει ένα άτομο σε υπεύθυνο επεξεργασίας.
- όταν η επεξεργασία βασίζεται στη συναίνεση του ατόμου ή στην εκτέλεση μιας σύμβασης
- όταν η επεξεργασία πραγματοποιείται με αυτοματοποιημένα μέσα.

Θα πρέπει να εξεταστούν και να ανανεωθούν οι σχετικές διαδικασίες. Τα προσωπικά δεδομένα θα πρέπει να παρέχονται σε δομημένη, ευρέως χρησιμοποιούμενη και μηχανικά αναγνώσιμη μορφή και οι πληροφορίες να παρέχονται δωρεάν.

Θέματα αιτήσεων πρόσβασης

Ο οργανισμός θα πρέπει να να ενημερώσει τις σχετικές διαδικασίες και να σχεδιάσει πώς θα χειρίζεται

τέτοιου είδους αιτήματα λαμβάνοντας υπόψη τους νέους κανόνες, όπως αυτοί εμφανίζονται παρακάτω:

- Στις περισσότερες περιπτώσεις δεν θα πρέπει να χρεώνεται η ικανοποίηση ενός αιτήματος.
- Θα πρέπει να ικανοποιηθεί το αίτημα μέσα σε ένα μήνα
- Μπορεί να υπάρξει άρνηση ή χρέωση για κάποιο αίτημα που είναι προδήλως αβάσιμο ή υπερβολικό.
- Εάν απορριφθεί ένα αίτημα, αυτό πρέπει να γίνει χωρίς αδικαιολόγητη καθυστέρηση και το αργότερο εντός ενός μηνός. Πρέπει να γνωστοποιηθεί στο άτομο ο λόγος και ότι ακολούθως έχει το δικαίωμα να υποβάλει καταγγελία στην τοπική εποπτική αρχή και σε ένδικα μέσα.

Εάν ο οργανισμός χειρίζεται μεγάλο αριθμό αιτήσεων πρόσβασης, θα πρέπει να εξεταστεί και η περίπτωση της αναβάθμισης της υλικοτεχνικής υποδομής με συνέπεια να είναι ταχύτερη η αντιμετώπιση των αιτημάτων.

3.2.2.8 Παραβιάσεις δεδομένων

Εικόνα 11

Θα πρέπει ο οργανισμός να εφαρμόσει τις κατάλληλες διαδικασίες για την ανίχνευση, την αναφορά και τη διερεύνηση μιας παραβίασης προσωπικών δεδομένων.

Ορισμένοι οργανισμοί υποχρεούνται ήδη να ενημερώνουν την τοπική εποπτική αρχή (και ενδεχομένως και άλλους φορείς) όταν υποστούν κάποια παραβίαση στην βάση των προσωπικών δεδομένων την οποία συντηρούν. Ο 2016/679 εισάγει το καθήκον σε όλους τους οργανισμούς να αναφέρουν ορισμένες παραβιάσεις δεδομένων στην τοπική εποπτική αρχή, και σε ορισμένες περιπτώσεις κατευθείαν και στα άτομα.

Όταν μια παραβίαση είναι πιθανό να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των ατόμων, όπως για παράδειγμα ζημιές στη φήμη, οικονομικές απώλειες, απώλεια εμπιστευτικότητας ή γενικά άλλου είδους οικονομικές ή κοινωνικές ζημιές, τότε θα πρέπει να ενημερώνεται η τοπική εποπτική αρχή.

Όταν μια παραβίαση ενδέχεται να οδηγήσει σε υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των ατόμων, θα πρέπει επίσης να ενημερώνονται και οι άμεσα ενδιαφερόμενοι.

Για τους λόγους αυτούς, θα πρέπει να τεθούν σε εφαρμογή διαδικασίες για την αποτελεσματική ανίχνευση, αναφορά και διερεύνηση της παραβίασης των προσωπικών δεδομένων. Θα βοηθήσει πολύ εάν στην φάση του σχεδιασμού, η ομάδα ασφαλείας αξιολογήσει τους τύπους των προσωπικών δεδομένων που κατέχει ο οργανισμός και ορίσει εξαρχής πότε θα πρέπει να ειδοποιηθεί η τοπική εποπτική αρχή ή τα θιγόμενα άτομα σε περίπτωση παραβίασης των προσωπικών τους δεδομένων. Θα χρειαστεί επίσης, να αναπτυχθούν πολιτικές και διαδικασίες για τη διαχείριση παραβιάσεων δεδομένων. Η παράλειψη δήλωσης μίας παραβίασης, όταν απαιτείται, θα μπορούσε να οδηγήσει σε πρόστιμο, καθώς και πρόστιμο για την παραβίαση.

3.2.2.9 Τρίτες χώρες

Εάν ο οργανισμός λειτουργεί σε περισσότερα από ένα κράτη μέλη της ΕΕ, πρέπει να οριστεί η εποπτική αρχή προστασίας δεδομένων κατόπιν τεκμηρίωσης.

Η κυρίαρχη αρχή είναι η εποπτική αρχή του κράτους όπου βρίσκεται η κύρια έδρα του οργανισμού. Η κύρια εγκατάσταση είναι η τοποθεσία στην οποία βρίσκεται η κεντρική διοίκηση στην ΕΕ ή αλλιώς ο τόπος όπου λαμβάνονται και εφαρμόζονται οι αποφάσεις σχετικά με τους σκοπούς και τα μέσα επεξεργασίας.

Αυτό ισχύει μόνο όταν διεξάγεται διασυνοριακή επεξεργασία - δηλαδή υπάρχουν εγκαταστάσεις σε περισσότερα από ένα κράτη μέλη της ΕΕ ή υπάρχει μια ενιαία εγκατάσταση στην ΕΕ που ασκεί επεξεργασία όπου επηρεάζει ουσιαστικά άτομα σε άλλα κράτη της ΕΕ.

Εάν αυτό ισχύει για έναν οργανισμό, θα πρέπει να γίνει ορισμός σε ποιο σημείο ο οργανισμός λαμβάνει τις πιο σημαντικές αποφάσεις σχετικά με τις δραστηριότητες επεξεργασίας του. Αυτό θα βοηθήσει να προσδιοριστεί η «κύρια εγκατάσταση» και επομένως η κύρια εποπτική αρχή του οργανισμού.

3.2.3 Βήμα 3ο - Δημιουργία πλάνου εργασιών

Σε αυτό το βήμα, η ομάδα εργασίας θα πρέπει να δημιουργήσει το πλάνο των απαραίτητων εργασιών οι οποίες πρέπει να εκτελεστούν για να επιτευχθεί η συμμόρφωση του οργανισμού με τον νέο κανονισμό.

Είναι σημαντικό οι εργασίες να ομαδοποιηθούν με ορθό τρόπο ώστε να γίνει καλύτερη χρήση του χρόνου. Η μείωση του απαιτουμένου χρόνου υλοποίησης των εργασιών συμβάλλει στην συντομότερη έκδοση νέων πολιτικών, διαδικασιών και φυσικά τεχνικών υλοποιήσεων σε πραγματικό περιβάλλον κάτι που βοηθάει σημαντικά στην παρακολούθηση και στον εντοπισμό πιθανών λαθών ή κενών κατά την υλοποίηση, ακόμα λαθών και κενών από την φάση της ανάλυσης της ετοιμότητας.

Προτείνεται λόγω των απαιτήσεων του 2016/679, η ομάδα ασφαλείας να ομαδοποιήσει της εργασίες σε δυο βασικές κατηγορίες Οι εργασίες των κατηγοριών αυτών μπορεί να εκτελούνται παράλληλα χωρίς να υπάρχει στις περισσότερες των περιπτώσεων εμπλοκή μεταξύ τους.

1η κατηγορία – Επιχειρησιακές αλλαγές: Εργασίες που αφορούν υλοποίηση σε επίπεδο πολιτικών, διαδικασιών και γενικών επιχειρηματικών διαδικασιών

Για παράδειγμα:

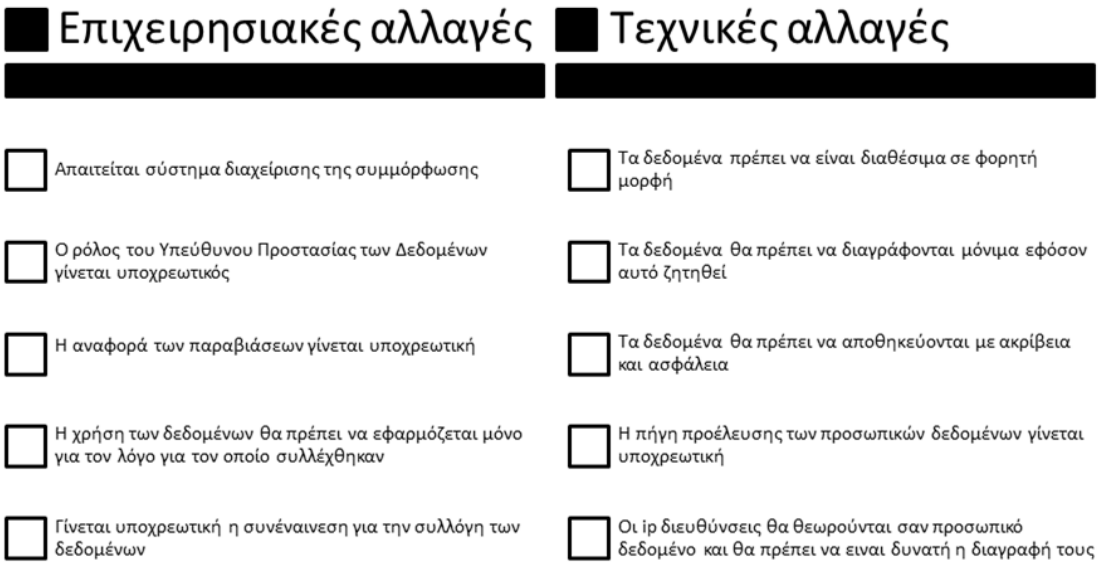
- Απαιτείται σύστημα διαχείρισης της συμμόρφωσης
- Ο ρόλος του Υπεύθυνου Προστασίας των Δεδομένων γίνεται υποχρεωτικός
- Η αναφορά των παραβιάσεων γίνεται υποχρεωτική
- Η χρήση των δεδομένων θα πρέπει να εφαρμόζεται μόνο για τον λόγο για τον οποίο συλλέχθηκαν
- Γίνεται υποχρεωτική η συναίνεση για την συλλογή των δεδομένων

2η κατηγορία – Τεχνικές αλλαγές: εργασίες που αφορούν αποκλειστικά το τεχνικο-υλικό κομμάτι του οργανισμού

Για παράδειγμα:

- ❏ Τα δεδομένα πρέπει να είναι διαθέσιμα σε φορητή μορφή
- ❏ Τα δεδομένα θα πρέπει να διαγράφονται μόνιμα εφόσον αυτό ζητηθεί
- ❏ Τα δεδομένα θα πρέπει να αποθηκεύονται με ακρίβεια και ασφάλεια
- ❏ Η πηγή προέλευσης των προσωπικών δεδομένων γίνεται υποχρεωτική
- ❏ Οι ip διευθύνσεις θα θεωρούνται σαν προσωπικό δεδομένο και θα πρέπει να είναι δυνατή η διαγραφή τους

Εικόνα 12 - Λίστα απαραίτητων επιχειρησιακών αλλαγών



3.2.4 Βήμα 4ο - Υλοποίηση πλάνου εργασιών

Σε αυτό το βήμα πραγματοποιείται η υλοποίηση όλων όσων έχουν αποφασιστεί και έχουν εισαχθεί στο πλάνο των εργασιών Η σωστή υλοποίηση και η κατανόηση των όσων πρέπει να υλοποιηθούν από όλα τα εμπλεκόμενα μέρη είναι πλέον σημαντική.

Στο βήμα αυτό, είναι απαραίτητο ο υπεύθυνος του έργου κατά την εκπόνηση των εργασιών να παρακολουθεί και να πραγματοποιεί συναντήσεις με όλα τα μέλη της ομάδας για να αποφευχθεί η περίπτωση λάθους κατά την υλοποίηση.

Σε αυτό το βήμα εφόσον οι εργασίες έχουν κατάλληλα χωριστεί ανάλογα με το ύφος των εργασιών:

- ❏ Σύνταξη ή ανανέωση της Πολιτικής Ασφάλειας με βάση των 2016/679
- ❏ Σύνταξη ή ανανέωση διαφόρων διαδικασιών με βάση των 2016/679
- ❏ Δημιουργία ή ανανέωση φορμών και εγγράφων που θα ακολουθούν τις παραπάνω διαδικασίες
- ❏ Θέσπιση καινούριων ρόλων ασφάλειας, όπως είναι αυτή του Υπευθύνου προστασίας

προσωπικών δεδομένων, πλέον υποχρεωτική από τον 2016/679

- ❑ Σχεδιασμός τεχνικών ή άλλων λύσεων που απαιτούνται για την τεχνική υλοποίηση των απαιτήσεων. Κωδικοποίηση των προσωπικών δεδομένων, φορητότητα, μόνιμη διαγραφή εφόσον ζητηθεί και άλλα
- ❑ Υλοποίηση, εγκατάσταση και λειτουργία του απαιτούμενου εξοπλισμού ασφάλειας (υλικού και λογισμικού)
- ❑ Παραμετροποίηση των συστημάτων και των εφαρμογών

3.2.5 Βήμα 5ο - Παρακολούθηση & έλεγχος ορθής λειτουργίας

Είναι καλό για τον οργανισμό να έχει ολοκληρώσει τις εργασίες και να ενεργεί με βάση τον νέο κανονισμό, ακόμα και πριν την ημερομηνία της ενεργοποίησής του. Με αυτόν τον τρόπο είναι δυνατόν να εντοπιστούν προβλήματα ή κενά, τα οποία εάν και εφόσον εντοπίζονταν την περίοδο όπου ο νέος κανονισμός είναι ενεργός πιθανότατα να δημιουργούσαν ή να απαιτούσαν διαφορετική προσέγγιση στο κομμάτι της διαχείρισης για την επίλυσή τους ή ακόμα επιπλέον χρόνο και κόπο.

Σε αυτό το βήμα περιλαμβάνονται εργασίες όπως:

- ❑ η καθημερινή παρακολούθηση της ορθής λειτουργίας των συστημάτων π.χ. αρχεία καταγραφής, εφαρμογές
- ❑ η τακτική ενημέρωση/ επικαιροποίηση των εφαρμογών και συστημάτων ασφάλειας
- ❑ η παρακολούθηση των εξειδικευμένων μηχανισμών εντοπισμού πιθανών προβλημάτων ασφάλειας, και
- ❑ ασκήσεις σε πιθανά σενάρια που είναι πολύ πιθανό να προκύψουν στο οργανισμό

3.2.6 Βήμα 6ο - Εκτίμηση υλοποίησης και τροποποίηση

Στο βήμα αυτό πραγματοποιούνται έλεγχοι για την διασφάλιση της πλήρους και ορθής εφαρμογής των επιλεγμένων μέτρων και της αποτελεσματικότητας των μέτρων να αντιμετωπίσουν τα πραγματικά και πιθανώς μεταβαλλόμενα προβλήματα ασφάλειας.

Οι έλεγχοι αυτοί μπορεί να είναι εσωτερικοί (internal audits) ή εξωτερικοί έλεγχοι από ανεξάρτητους φορείς (external or independent audits). Η διεξαγωγή των ελέγχων μπορεί να στηρίζεται σε ερωτηματολόγια ελέγχου διαδικασιών (checklists), δοκιμές διείσδυσης και άλλα. Ανάλογα με τα αποτελέσματα των ελέγχων, ενδέχεται να προκύψει η ανάγκη για αναθεώρηση. Ο έλεγχος της αναθεώρησης θα πρέπει να πραγματοποιείται ανεξάρτητα από το εάν θα γίνουν τελικά οι αλλαγές ή όχι.

3.3 Μέθοδοι, τεχνικές λύσεις και προτεινόμενα εργαλεία για την υλοποίηση των απαιτήσεων

Όπως περιγράψαμε μέχρι τώρα, από τα πιο σημαντικά βήματα στην προετοιμασία ενός οργανισμού για τον νέο κανονισμό είναι ο έλεγχος της ετοιμότητάς του σε σχέση με τον νέο κανονισμό και η δημιουργία του πλάνου των εργασιών για την επίτευξη της συμμόρφωσής του με αυτόν.

Σε αυτήν την ενότητα προτείνουμε μεθόδους που θα βοηθήσουν την ομάδα ασφαλείας ενός οργανισμού να αποφασίσει ποιες θα είναι οι επιχειρησιακές και τεχνικές αλλαγές για τον οργανισμό και σε τι επίπεδο θα πρέπει αυτές να εφαρμοστούν ώστε να καταφέρει ο οργανισμός να επιτύχει συμμόρφωση με τον νέο κανονισμό. Σαν συνέχεια, προτείνουμε διάφορες τεχνικές λύσεις και εργαλεία τα οποία ο οργανισμός μπορεί να χρησιμοποιήσει και να εφαρμόσει κατά την υλοποίηση του πλάνου των εργασιών.

Όπως έχουμε αναφέρει και παραπάνω, το άρθρο 32 του νέου κανονισμού απαιτεί από τον υπεύθυνο επεξεργασίας και από τον εκτελούντα την επεξεργασία σε ένα οργανισμό να εφαρμόσει τα κατάλληλα τεχνικά και οργανωτικά μέτρα για να εξασφαλίσει ένα επίπεδο ασφαλείας κατάλληλο για:

- την ψευδωνυμοποίηση και την κρυπτογράφηση δεδομένων προσωπικού χαρακτήρα,
- την ικανότητα να εξασφαλίζεται η συνεχής εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα και ανθεκτικότητα των συστημάτων και υπηρεσιών επεξεργασίας,
- την ικανότητα έγκαιρης αποκατάστασης της διαθεσιμότητας και της πρόσβασης σε προσωπικά δεδομένα σε περίπτωση φυσικού ή τεχνικού συμβάντος, και
- τη διαδικασία τακτικού ελέγχου, αξιολόγησης και αξιολόγησης της αποτελεσματικότητας των τεχνικών και οργανωτικών μέτρων για την εξασφάλιση της ασφάλειας της επεξεργασίας.

Βάσει των παραπάνω, ταξινομήσαμε τις προτεινόμενες μεθόδους και τα εργαλεία για την επίτευξη της συμμόρφωσης με τον νέο κανονισμό σε τέσσερις βασικούς πυλώνες.

- στην θωράκιση των συστημάτων του οργανισμού,
- στην πρόληψη πιθανών απωλειών δεδομένων από τον οργανισμό,
- στο τρόπο αποθήκευσης των δεδομένων, και
- στην παρακολούθηση των συστημάτων του οργανισμού

3.3.1 Θωράκιση των συστημάτων

Εικόνα 13

Για την θωράκιση των συστημάτων του οργανισμού προτείνουμε την εφαρμογή της διαδικασίας Hardening [5]. Το Hardening είναι η διαδικασία διασφάλισης ενός συστήματος με στόχο την μείωση της ευπάθειάς του. Μεγαλώνοντας η πολυπλοκότητα των συστημάτων ενός οργανισμού και/ή μεγαλώνοντας το πλήθος των πολλαπλών χρήσεων των συστημάτων τόσο αυξάνεται η πιθανότητα ευπάθειας του.

Οι βασικές ενέργειες του hardening περιλαμβάνουν:

- Την διατήρηση και ενημέρωση των λογισμικών ασφαλείας
- Την εγκατάσταση τείχους προστασίας
- Την διακοπή πρόσβασης σε ορισμένες θύρες
- Την αποτροπή της κοινής χρήσης αρχείων μεταξύ προγραμμάτων
- Την εγκατάσταση λογισμικού προστασίας από ιούς
- Την δημιουργία ισχυρών κωδικών πρόσβασης
- Την δημιουργία συχνών αντιγράφων ασφαλείας
- Την απενεργοποίηση των cookies
- Την χρησιμοποίηση κρυπτογράφησης όταν είναι δυνατόν

Προτεινόμενα εργαλεία που θα μπορούσαν να βοηθήσουν την ομάδα εργασίας τόσο στην εκτίμηση της ευπάθειας των συστημάτων του οργανισμού όσο και στην πραγματοποίηση του hardening είναι τα εξής: το Lynis για λογισμικά Unix και Linux καθώς και το Attack Surface Analyzer για συστήματα Windows.

Lynis [6]: Το εργαλείο αυτό εκτελεί έλεγχο ασφάλειας του συστήματος και καθορίζει πόσο ευπαθές είναι το σύστημα Τα τυχόν ζητήματα ασφάλειας παρέχονται υπό μορφή πρότασης ή προειδοποίησης στο τέλος του ελέγχου. Εκτός από τις πληροφορίες που σχετίζονται με την ασφάλεια, το Lynis εξετάζει επίσης τις γενικές πληροφορίες του συστήματος, τα εγκατεστημένα πακέτα και πιθανά σφάλματα διαμόρφωσης. Το Lynis βοηθάει στο κομμάτι του αυτοματοποιημένου ελέγχου, στο

hardening, στη διαχείριση των ενημερώσεων του λογισμικού και στην ανίχνευση κακόβουλου λογισμικού.

Εικόνα 14 [6] – Στιγμιότυπο κονσόλας Lynis

Attack Surface Analyzer [7] της Microsoft, το οποίο αναφέρεται σε λογισμικό Windows. Το εργαλείο αυτό είναι παρόμοιο με το Lynis με την διαφορά ότι βοηθάει στην ανάλυση συστημάτων που τρέχουν σε Windows.

Εικόνα 15 [7] Στιγμιότυπο από Attack Surface Analyzer

Κάποια άλλα εργαλεία που μπορούν να αναλύσουν ένα σύστημα και έμμεσα να δώσουν βοήθεια στην ομάδα ασφαλείας στο κομμάτι του σχεδιασμού του hardening είναι τα Nessus, openVAS και nmap.

Φυσικά, υπάρχουν πολλά ακόμα εργαλεία που μπορούν να πουν πολλά για τις ευπάθειες ενός συστήματος. Εργαλεία που ανήκουν στην κατηγορία των εργαλείων διείσδυσης είναι τα ZAP (Zed Attack Proxy), IronWASP και Metasploit.

3.3.2 Πρόληψη απωλειών δεδομένων

Εικόνα 16

Η πρόληψη της απώλειας δεδομένων (Data Loss Prevention) [8] είναι πολύ σημαντική στρατηγική που χρησιμοποιείται για να διασφαλιστεί ότι τα ευαίσθητα δεδομένα δεν θα χαθούν, δεν θα χρησιμοποιηθούν κατά λάθος ή δεν θα είναι προσβάσιμα από μη εξουσιοδοτημένους χρήστες. Σκοπός της στρατηγικής αυτής είναι να προστατεύουν εμπιστευτικές και κρίσιμες πληροφορίες ώστε να αποτρέψουν τους τελικούς χρήστες από μία τυχαία ή μία κακόβουλη διανομή δεδομένων. Το λογισμικό και τα εργαλεία πρόληψης απώλειας δεδομένων παρακολουθούν και ελέγχουν τις δραστηριότητες και τις ροές δεδομένων σε εταιρικά δίκτυα και προστατεύουν τα δεδομένα καθώς αυτά μετακινούνται.

Παρακάτω, παρατίθενται, κάποια εργαλεία τα οποία ψηφίστηκαν το 2017 ως τα πιο πλήρη στην πρόληψη απώλειας δεδομένων [9]

- Symantec Data Loss Prevention,
- Trustwave Data Loss Prevention,
- McAfee Total Protection for Data Loss Prevention,
- Check Point Data Loss Prevention, και
- Digital Guardian Endpoint DLP

Πολλές από τις εταιρείες που έχουν αναπτύξει τα παραπάνω εργαλεία, διαφημίζουν ότι τα προϊόντα τους είναι έτοιμα για τον νέο κανονισμό. Πιο συγκεκριμένα, ο τρόπος με τον οποίο το κάνουν είναι προωθώντας πως τα προϊόντα τους έχουν έτοιμες ρυθμίσεις και σύνολα από κανόνες βασισμένα στα πρότυπα του νέου κανονισμού. Οι ρυθμίσεις αυτές μπορεί να ενεργοποιηθούν/απενεργοποιηθούν/παραμετροποιηθούν κατά παραγγελία.

Φυσικά, κάποια από τα εργαλεία αναφέρονται σε μεγάλα συστήματα και οργανισμούς ενώ κάποια άλλα σε μέτριους ή πιο μικρούς οργανισμούς Ωστόσο, η παραπάνω λίστα κάνει γρήγορη την εύρεση του κατάλληλου εργαλείου για την πρόληψη της απώλειας δεδομένων περιορίζοντάς τα στα πέντε.

Σημαντικό ρόλο στην αποτροπή της απώλειας των δεδομένων άλλα και στην αποτροπή εξωγενών παραγόντων στην προσβασιμότητα των δεδομένων ενός οργανισμού είναι και τα τείχη προστασίας Προτείνεται η χρηση τειχών προστασίας τεχνολογίας επόμενης γενιάς (Next Generation Firewalls) [14]. Τα τείχη προστασίας επόμενης γενιάς λειτουργούν όπως τα παραδοσιακά τείχη προστασίας ωστόσο έχουν και άλλες λειτουργίες οι όποιες βοηθάνε στην άμυνα των συστημάτων ενός οργανισμού.

Παρακάτω, παρατίθενται, κάποια τείχη προστασίας επόμενης γενιάς [14]

- Sophos XG Firewall
- Barracuda F-Series
- Juniper Networks SRX
- Fortinet FortiGate
- Forcepoint NGFW
- SonicWall SuperMassive
- Palo Alto Networks PA Series
- Cisco Firepower NGFW
- Huawei USG
- Check Point Advanced Threat Protection

3.3.3 Αποθήκευση των δεδομένων

Η αποθήκευση των δεδομένων είναι ένα πολύ σημαντικό κομμάτι του νέου κανονισμού. Ο τρόπος αποθήκευσης των δεδομένων θα πρέπει να αντιπροσωπεύει έναν ουσιαστικό μέσο για την καθιέρωση της εμπιστευτικότητας και της ακεραιότητας των δεδομένων. Ανεξαρτήτως εάν τα δεδομένα αποθηκεύονται σε εσωτερική υποδομή ή στο σύννεφο, για να επιτευχθεί η συμμόρφωση του οργανισμού με το νέο κανονισμό ενδέχεται αυτός να χρειαστεί να χρησιμοποιήσει μία ή περισσότερες διαφορετικές μεθόδους κρυπτογράφησης. Η κρυπτογράφηση δεδομένων μεταφράζει δεδομένα σε μια άλλη μορφή, έτσι ώστε μόνο τα άτομα που έχουν πρόσβαση σε ένα μυστικό κλειδί να μπορούν να διαβάσουν τα δεδομένα. Ο νέος κανονισμός, συνιστά τόσο την χρηση της τεχνικής της ανωνυμοποίησης των δεδομένων όσο και αυτής της ψευδωνυμοποίησης.

Η ανωνυμοποίηση δεδομένων [15] είναι μια τεχνική η οποία έχει στόχο την προστασία της ιδιωτικής ζωής. Είναι η διαδικασία κρυπτογράφησης ή αφαίρεσης πληροφοριών προσωπικής ταυτοποίησης από σύνολα δεδομένων, έτσι ώστε οι άνθρωποι που περιγράφουν τα δεδομένα να παραμένουν ανώνυμοι και να μην μπορούν να τακτοποιηθούν πότε μέσα από τα δεδομένα

Η ψευδωνυμοποίηση [16] είναι μια τεχνική όπου η επεξεργασία των δεδομένων προσωπικού χαρακτήρα γίνεται με τέτοιο τρόπο ώστε τα δεδομένα να μην μπορεί να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών.

Η απόφαση για το ποια τεχνική θα χρησιμοποιηθεί είναι καθαρά επιλογή του οργανισμού οποίος θα πρέπει να έχει σαν γνώμονα την ελαχιστοποίηση του κινδύνου.

Παρακάτω παρατίθενται διάφορες μέθοδοι [15] για την ανωνυμοποίηση των δεδομένων. Πάλι η επιλογή της μεθόδου θα εξαρτηθεί από το βαθμό κινδύνου και την προοριζόμενη χρήση των δεδομένων.

- Directory replacement
- Scrambling
- Masking
- Personalized anonymization
- Blurrin

Κάποια προτεινόμενα εργαλεία που βοηθούν στην κρυπτογράφηση των δεδομένων είναι τα εξής [10]:

- VeraCrypt
- AxCrypt
- bitlocker
- CryptoExpert 8
- CertainSafe

3.3.4 Παρακολούθηση των συστημάτων

Ανάλογα με τον οργανισμό, ένας άλλος σημαντικός παράγοντας για την συμμόρφωση με τον νέο κανονισμό είναι ο συνεχόμενος έλεγχος των συστημάτων του. Με τον νέο κανονισμό, θα πρέπει να κοινοποιείται, το συντομότερο δυνατό, η όποια απώλεια προσωπικών δεδομένων. Ως συνέπεια προκύπτει η παρακολούθηση των δικτύων του οργανισμού για την καταγραφή πιθανών επιθέσεων αλλά και για τον εντοπισμό παραβάσεων.

Για την καλύτερη παρακολούθηση των συστημάτων αλλά και γενικότερα για την καλύτερη επιχειρησιακή λειτουργία του οργανισμού στον τομέα αυτό, προτείνεται η χρήση λύσεων/προϊόντων που χρησιμοποιούν την τεχνολογία security information and event management (SIEM) [17] και όχι απλά προϊόντα παρακολούθησης συστημάτων. Τα συστήματα ασφάλειας πληροφοριών και διαχείρισης συμβάντων (SIEM) απορροφούν και παρακολουθούν δεδομένα από πολλαπλά σημεία εισόδου, υλικό αλλά και λογισμικό, και από πολλαπλές πηγές ασφαλείας για να αποτρέψουν επιθέσεις, και επιτόπιες επιδρομές στο δίκτυο ενός οργανισμού και να ανιχνεύσουν αμυντικές αδυναμίες σε περίπτωση παραβίασης. Τα συστήματα SIEM περιέχουν ένα ευρύ φάσμα εργαλείων ασφαλείας όπως τείχη προστασίας, ασφάλεια παραμέτρων, πρόληψη εισβολών, απειλή πληροφοριών και μπορεί να αποτελέσουν ένα σημαντικό κομμάτι για την βέλτιστη επιχειρησιακή λειτουργία ενός οργανισμού

Τα κύρια χαρακτηριστικά ενός SIEM συστήματος είναι τα εξής:

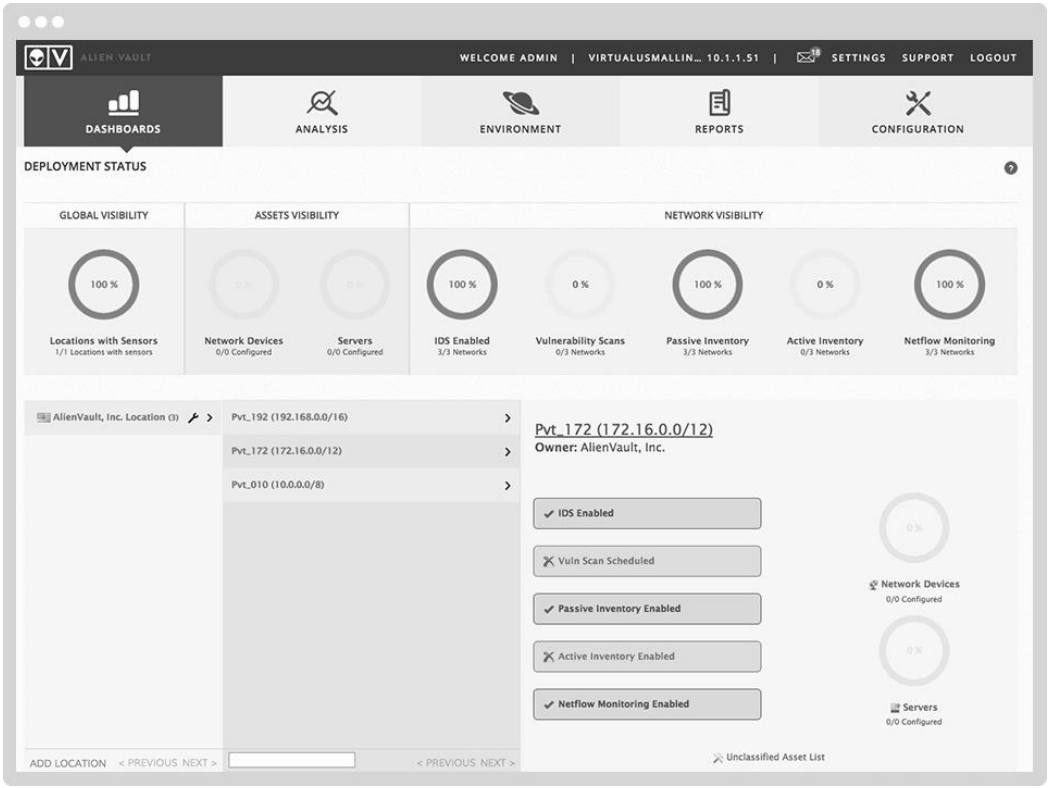
- εισροή δεδομένων από πολλαπλές πηγές
- ερμηνεία των δεδομένων
- ενσωμάτωση και συσχέτιση όλων των πληροφοριών από διάφορες απειλές ή συναγερμούς
- ανάλυση των στοιχείων και δημιουργία προτύπων συμπεριφορών, δημιουργία αυτοματοποιημένων λύσεων στις πιθανές απειλές

Με απλά λόγια, η χρήση ενός SIEM συστήματος αντικαθιστά την χειροκίνητη διαδικασία ενός διαχειριστή ασφαλείας ο οποίος πρέπει να ανοίξει πολλές εφαρμογές και να προσπαθήσει να συνδέσει/συσχετίσει διαφορετικές ειδοποιήσεις. Ένα SIEM σύστημα παρέχει αυτοματοποιημένα σε μεγάλο βαθμό τη διαχείριση, την ολοκλήρωση, τη συσχέτιση και την ανάλυση των δεδομένων.

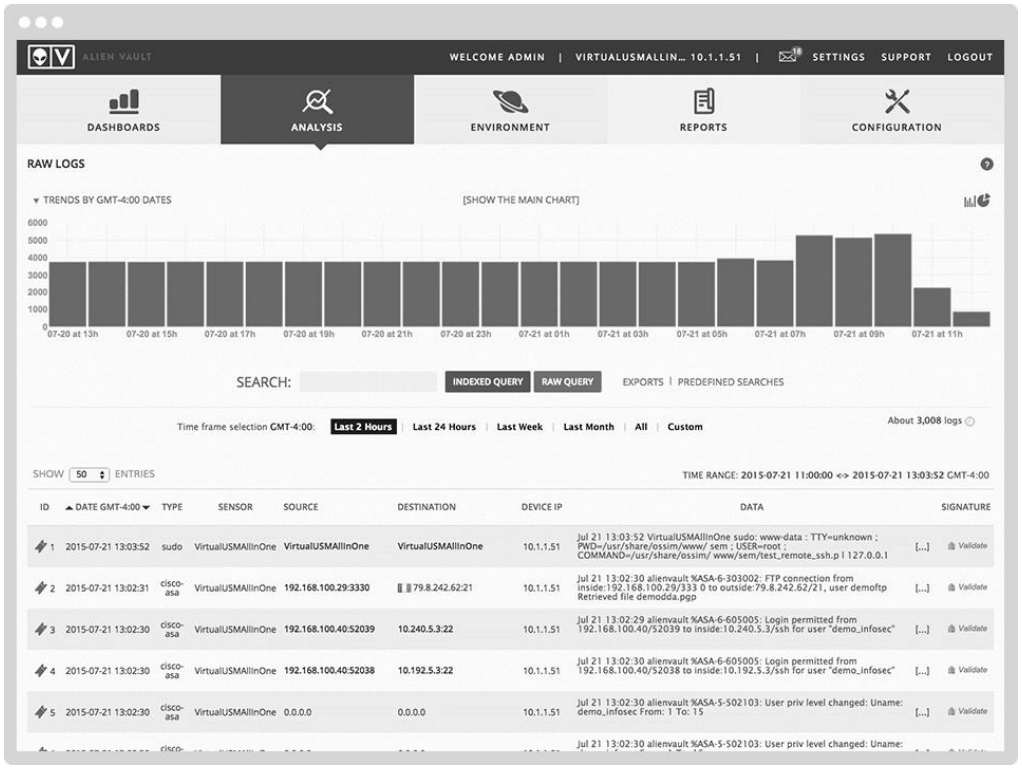
Τα παρακάτω εργαλεία προτείνονται όχι μόνο διότι προσφέρουν αυτές τις δυνατότητες στον οργανισμό αλλά για τον τρόπο και την ευκολία με την οποία μπορεί να παραμετροποιηθούν και να χρησιμοποιηθούν από την ομάδα ασφαλείας.

OSSIM (open-source SIM) [13]: Το OSSIM είναι από τις πλέον διαδεδομένες ελεύθερες λύσεις τεχνολογίας SIEM. Προσφέρεται από την AlienVault, αν και ελεύθερο λογισμικό παρέχει πολλές λύσεις για τους οργανισμούς. Διατίθεται και σε εμπορική έκδοση για οργανισμούς με μεγάλο όγκο δεδομένων και πληροφοριών γενικότερα.

Εικόνα 17 [13] Στιγμιότυπο του προγράμματος OSSIM

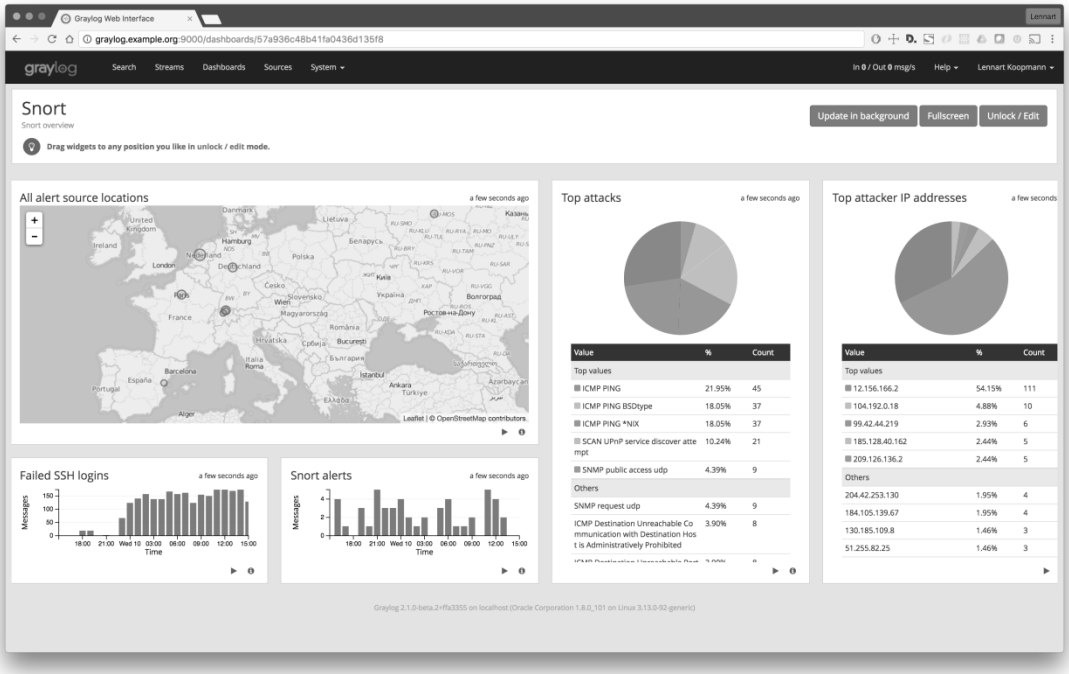


Εικόνα 18 [13] Στιγμιότυπο του προγράμματος OSSIM

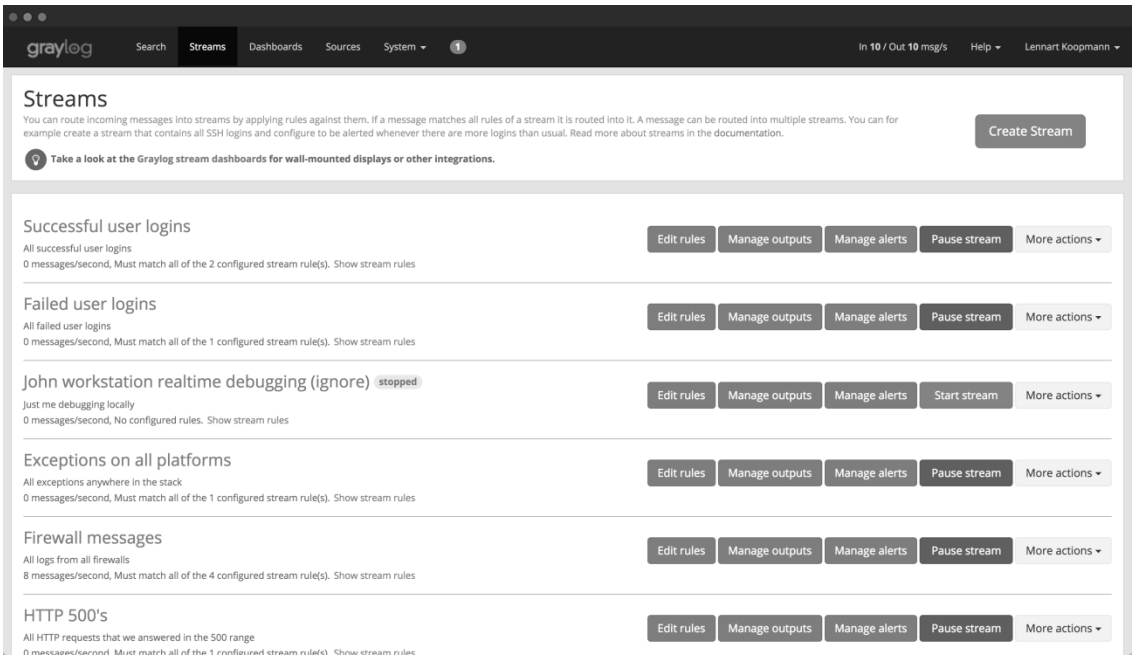


Graylog [11]: Το Graylog είναι ένα εργαλείο με το οποίο ο οργανισμός μπορεί να συλλέξει και να επεξεργαστεί όλα τα δεδομένα και τα γεγονότα που βρίσκονται εντός του οργανισμού ή προσπαθούν να εισχωρήσουν στο εσωτερικό του. Με το Graylog, είναι δυνατή η γρήγορη αναζήτηση σε αυτά τα δεδομένα και η ανάλυσή τους ώστε να μπορέσουν να εφαρμοστούν μηχανισμοί ειδοποίησης σε ανάλογες περιπτώσεις. Όλα αυτά ακολουθούνται από ένα πλήρως απλό και εύκολο στον χρήστη γραφικό περιβάλλον με πλούσιες αναφορές.

Εικόνα 19 [11] Στιγμιότυπο του προγράμματος Graylog

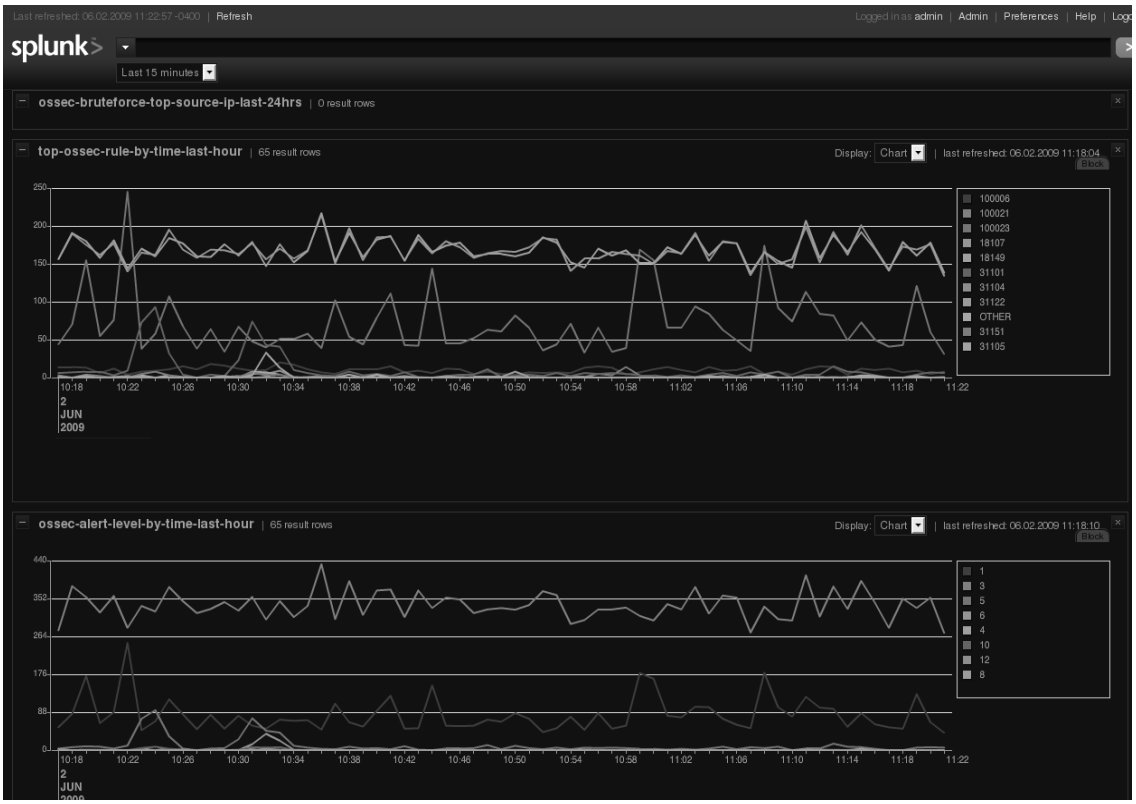


Εικόνα 20 [11] Στιγμιότυπο του προγράμματος Graylog



Splunk [12]: Το Splunk είναι παρόμοιο εργαλείο με το graylog. Στόχος και του Splunk είναι η παρακολούθηση, η αναζήτηση, η ανάλυση, η οπτικοποίηση και η λειτουργία σε ογκώδεις ροές δεδομένων σε πραγματικό χρόνο. Το splunk σε σχέση με το Graylog έχει ευρεία εφαρμογή και χρησιμοποιείται σε πολλές διαφορετικές βιομηχανίες.

Εικόνα 21 [12] Στιγμιότυπο του προγράμματος Splunk



Εικόνα 22 [12]

3.3.5 Πίνακας ιχνηλασιμότητας

Στον παρακάτω πίνακα συνοψίζονται οι στόχοι, οι ενέργειες και τα προτεινόμενα εργαλεία ανα φάση στο πλαίσιο προετοιμασίας ενός οργανισμού με τον νέο κανονισμό

Πίνακας 2

Φάση	Βήμα	Στόχος	Ενέργειες	Προτεινόμενα εργαλεία / μεθόδοι
PLAN	1ο	Δημιουργία ομάδας ασφαλείας	- Ορισμός στόχων για την συμμόρφωση με τον 2016/679. - Κατάρτιση ομάδας ασφάλειας - Ορισμός ρόλων. π.χ. υπευθύνος προστασίας δεδομένων. - Διάθεση απαραίτητων πόρων και καθορισμός προϋπολογισμού	
	2ο	Έλεγχος ετοιμότητας	- Μελέτη του νέου κανονισμού.Έμφαση σε: συγκατάθεση, παιδιά, κοινοποίηση πληροφοριών απορρήτου, δικαιώματα των πολιτών, παραβιάσεις δεδομένων, τρίτες χώρες. - Αναγνώριση των προσωπικών δεδομένων που κατέχει και επεξεργάζεται ο οργανισμός - Εκτίμηση των επιπτώσεων στην προστασία δεδομένων	
	3ο	Δημιουργία πλάνου εργασιών	- Ορισμός εργασιών - Κατηγοριοποίηση εργασιων (Επιχειρησιακές αλλαγές, Τεχνικές αλλαγές) - Ορισμός χρόνου εκτέλεσης και ολοκλήρωσης των εργασιών	Εφαρμογή/χρήση της μεθόδου Hardening. Εφαρμογή/χρήση εργαλείων Lynis, Attack Surface Analyzer, Nessus, openVAS, nmap
DO	4ο	Υλοποίηση πλάνου εργασιών	- Υλοποίηση επιχειρησιακών αλλαγών(δημιουργία πολιτικών ασφάλειας, διαδικασιών, θέσπιση νέων ρόλων) - Υλοποίηση τεχνικών αλλαγών(πρόληψη απωλειών δεδομένων, αποθήκευση των δεδομένων, παρακολούθηση των συστημάτων)	Εφαρμογή/χρήση εργαλείων Symantec Data Loss Prevention, Trustwave Data Loss Prevention, Barracuda F-Series. Bitlocker, VeraCrypt OSSIM, Graylog, Splunk

CHECK	5ο	Παρακολούθηση και έλεγχος ορθής λειτουργίας	- Παρακολούθηση της ορθής λειτουργίας των συστημάτων - Παρακολούθηση των εξειδικευμένων μηχανισμών εντοπισμού πιθανών προβλημάτων ασφάλειας. - Ασκήσεις σεναρίων που είναι πιθανό να προκύψουν στην πραγματικότητα	Εφαρμογή/χρήση των εργαλείων με τα οποία έγινε η υλοποίηση των εργασιών
ACT	6ο	Εκτίμηση λειτουργίας και τροποποίηση	έλεγχοι διασφάλισης: - της πλήρους και ορθής εφαρμογής των επιλεγμένων μέτρων, - της αποτελεσματικότητας των μέτρων να αντιμετωπίσουν τα πραγματικά και πιθανώς μεταβαλλόμενα προβλήματα ασφάλειας. Έλεγχος για πιθανή ανάγκη αναθεώρησης.	

4. Συμπεράσματα

Τα προσωπικά δεδομένα που διαμοιράζονται από τα άτομα μέσω των ηλεκτρονικών συσκευών έχουν αυξηθεί σε υπερθετικό βαθμό και η ανάγκη προστασίας τους είναι πλέον επιτακτική.

Έως τώρα, για την προστασία των προσωπικών δεδομένων, υπάρχει μόνο η οδηγία 95/46/ΕΚ η οποία είχε εγκριθεί από την Ευρωπαϊκή Ένωση με σκοπό την προστασία της ιδιωτικής ζωής και την προστασία όλων των προσωπικών δεδομένων που συλλέγονται και αφορούν τους πολίτες της. Η οδηγία στόχευε στην προστασία των δεδομένων κατά την επεξεργασία, τη χρήση ή την ανταλλαγή αυτών. Καθώς οι εξελίξεις στην τεχνολογία είναι μεγάλες, η οδηγία 95/46/ΕΚ πλέον δεν είναι επαρκής.

Τα τελευταία χρόνια υπήρξαν πολλά συμβάντα διαρροών προσωπικών δεδομένων - σε πολλές περιπτώσεις δεδομένα εκατομμυρίων χρηστών εκτέθηκαν στο διαδίκτυο. Οι διαρροές αυτές δεν ήταν πάντα αποτέλεσμα μιας κακόβουλης πράξης ενός τρίτου προσώπου, αλλά περισσότερο, αποτέλεσμα κακής διαχείρισης και μη συμμόρφωσης των οργανισμών με τους κανονισμούς της προστασίας των προσωπικών δεδομένων.

Για να αντιμετωπιστούν οι προκλήσεις σχετικά με την προστασία των προσωπικών δεδομένων, ψηφίστηκε ο νέος Ευρωπαϊκός Κανονισμός 2016/679 ο οποίος θα τεθεί σε εφαρμογή, στις 25 Μαΐου του 2018. Τα δύο πιο σημαντικά χαρακτηριστικά του 2016/679, είναι ότι αυξάνονται σημαντικά οι απαιτήσεις που τίθενται στους οργανισμούς που επεξεργάζονται προσωπικά δεδομένα καθώς επίσης και το μέγεθος των κυρώσεων στις περιπτώσεις μη συμμόρφωσης των οργανισμών με τον κανονισμό.

Με βασικά του στοιχεία, την εναρμόνιση μέσα και πέρα από την Ευρωπαϊκή Ένωση, τις νέες έννοιες των ελεγκτών και των εκτελούντων την επεξεργασία, τα πρόστιμα και τις κυρώσεις, την διαχείριση του απορρήτου, τη συγκατάθεση, τις πληροφορίες που παρέχονται κατά τη συλλογή των δεδομένων, την κατάρτιση προφίλ, το κομμάτι της παραβίασης και της ειδοποίησης, τα αιτήματα πρόσβασης στα προσωπικά δεδομένα, το δικαίωμα στη φορητότητα των δεδομένων, τη διατήρηση και το δικαίωμα διαγραφής. Ο νέος κανονισμός για την προστασία των προσωπικών δεδομένων έχει σχεδιαστεί για να επιτρέπει στα άτομα να ελέγχουν καλύτερα τα προσωπικά τους δεδομένα, ελπίζοντας παράλληλα ότι αυτοί οι εκσυγχρονισμένοι και ενοποιημένοι κανόνες θα επιτρέψουν στις επιχειρήσεις να αξιοποιήσουν στο έπακρο τις ευκαιρίες της ψηφιακής ενιαίας αγοράς, μειώνοντας τη νομοθεσία και επωφελούμενοι από την ενισχυμένη εμπιστοσύνη των καταναλωτών.

Η δικαιοσύνη πλέον θα μπορεί να εξασφαλίσει ότι τα δεδομένα των θυμάτων, των μαρτύρων και των υπόπτων εγκλημάτων θα προστατεύονται δεόντως στο πλαίσιο ποινικής έρευνας ή δράσης επιβολής του νόμου. Συγχρόνως, οι πιο εναρμονισμένοι νόμοι θα διευκολύνουν τη διασυνοριακή συνεργασία των αστυνομικών και των εισαγγελέων για την αποτελεσματικότερη καταπολέμηση της εγκληματικότητας και της τρομοκρατίας σε ολόκληρη την Ευρώπη.

Στο πλαίσιο της προετοιμασίας με το νέο κανονισμό 2016/679, στην παρούσα μεταπτυχιακή διατριβή, παρουσιάστηκαν μια σειρά από βήματα και στάδια/φάσεις των εργασιών τα οποία έχουν ως σκοπό να βοηθήσουν τους οργανισμούς και τις ομάδες ασφάλειας τους να κατανοήσουν και να αναγνωρίσουν πιο γρήγορα και εύκολα τις απαραίτητες ενέργειες που θα πρέπει να πραγματοποιηθούν ώστε να επιτευχθεί η συμμόρφωση με τον 2016/679.

Για να επιτευχθεί το συντομότερο δυνατό και με μεγαλύτερη επιτυχία η συμμόρφωση με τον νέο κανονισμό, προτείνεται η ομάδα ασφαλείας να ακολουθήσει την μέθοδο του Deming η οποία είναι χωρισμένη σε τέσσερις φάσεις PDCA (plan-do-check-act), όπου σε κάθε φάση εκτελούνται συγκεκριμένες εργασίες οι οποίες και περιγράφονται αναλυτικά, στο αντίστοιχο κεφάλαιο. Η μέθοδος αυτή δεν επιλέχθηκε τυχαία καθώς ήδη ακολουθείται από ομάδες ασφαλείας στα πλαίσια πιστοποίησης ενός οργανισμού στο ISO27001 ή PCI.

Για να μπορέσει η ομάδα ασφαλείας να εξυπηρετήσει των όγκο των αλλαγών, προτείνεται να τις ομαδοποιήσει σε “Επιχειρησιακές” και “Τεχνικές”. Οι επιχειρησιακές αλλαγές αφορούν υλοποίηση σε επίπεδο πολιτικών και διαδικασιών ενώ οι τεχνικές έχουν να κάνουν αποκλειστικά με το τεχνικό-υλικό κομμάτι του οργανισμού.

Και για τις δύο υπάρχει εκτενής αναφορά στα βήματα που πρέπει ο οργανισμός να ακολουθήσει ώστε να αποφασίσει ποιες θα είναι οι αλλαγές που θα κάνει σε κάθε επίπεδο, για να επιτύχει την

πολυπόθητη συμμόρφωση με τον κανονισμό. Επίσης, προτείνονται διάφορα εργαλεία και τεχνικές λύσεις τις οποίες ο οργανισμός μπορεί να χρησιμοποιήσει στην υλοποίηση του πλάνου εργασιών.

Οι τεχνικές αυτές λύσεις που θα βοηθήσουν τον οργανισμό να συμμορφωθεί με το νέο κανονισμό ταξινομούνται σε τέσσερις βασικούς πυλώνες, τη θωράκιση των συστημάτων του, την πρόληψη πιθανών απωλειών δεδομένων, τον τρόπο με τον οποίο αποθηκεύονται τα δεδομένα και την παρακολούθηση των συστημάτων του.

Για την θωράκιση των συστημάτων προτείνεται η εφαρμογή της διαδικασίας Hardening ο σκοπός της οποίας είναι να μειώσει τις ευπάθειές τους. Μέσω του hardening, κάποιες από τις ενέργειες που μπορεί να κάνει η ομάδα ασφαλείας του οργανισμού είναι ενδεικτικά η διατήρηση και ενημέρωση των λογισμικών ασφαλείας, η εγκατάσταση τείχους ασφαλείας, η δημιουργία συχνών αντιγράφων ασφαλείας και η διακοπή της πρόσβασης σε πολλές θύρες. Τα εργαλεία που χρειάζεται ο οργανισμός για να εφαρμόσει την διαδικασία hardening στα συστήματά του αναλύονται εκτενώς στο αντίστοιχο κεφάλαιο.

Όσον αφορά την πρόληψη πιθανών απωλειών δεδομένων, ο σκοπός της ομάδας ασφαλείας είναι να διασφαλίσει πως ευαίσθητα δεδομένα δεν θα χαθούν, δεν θα χρησιμοποιηθούν κατά λάθος ή δεν θα είναι προσβάσιμα από μη εξουσιοδοτημένους χρήστες. Για να το επιτύχουν αυτό, προτείνεται να εγκαταστήσουν κάποιο από τα εργαλεία πρόληψης δεδομένων που αναφέρονται αναλυτικά στο αντίστοιχο κεφάλαιο.

Η αποθήκευση των δεδομένων είναι και αυτή με τη σειρά της ένα πολύ σημαντικό κομμάτι του νέου κανονισμού. Ανεξαρτήτως του τρόπου αποθήκευσης των δεδομένων αυτών, είτε σε εσωτερική υποδομή ή στο σύννεφο, θα πρέπει ο οργανισμός να χρησιμοποιήσει μία ή περισσότερες διαφορετικές μεθόδους κρυπτογράφησης. Επίσης, συνιστάται η χρήση της τεχνικής της ανωνυμοποίησης και ψευδωνυμοποίησης των δεδομένων. Τα εργαλεία που μπορεί να χρησιμοποιήσει ο οργανισμός για να εφαρμόσει τις παραπάνω μεθόδους και τεχνικές περιγράφονται αναλυτικά στο αντίστοιχο κεφάλαιο.

Ο σκοπός της παρακολούθησης των συστημάτων είναι ο συνεχόμενος έλεγχος τους έτσι ώστε να κοινοποιείται το συντομότερο δυνατόν μία ενδεχόμενη απώλεια προσωπικών δεδομένων. Για να επιτευχθεί αυτό, οι έλεγχοι που γίνονται αφορούν στην παρακολούθηση των δικτύων του οργανισμού για την καταγραφή πιθανών επιθέσεων αλλά και στον εντοπισμό πιθανών παραβάσεων. Τα εργαλεία με τα οποία μπορεί ο οργανισμός να παρακολουθήσει με επιτυχία τα συστήματά του, αναφέρονται αναλυτικά στο αντίστοιχο κεφάλαιο.

Καλό είναι οι οργανισμοί να σχεδιάσουν από τώρα την προσέγγισή τους για τη συμμόρφωσή τους με τον 2016/679 ώστε να ενημερωθούν όσο το δυνατόν γρηγορότερα οι αρμόδιοι υπάλληλοι του οργανισμού, οι οποίοι πιθανόν θα αναλάβουν μελλοντικά τους αντίστοιχους ρόλους στην ομάδα ασφαλείας, ιδιαίτερα εάν μέχρι τώρα δεν υπήρχαν διαδικασίες στον οργανισμό οι οποίες να αφορούν θέματα ασφαλείας.

Μια πιθανή μετεξέλιξη/συνέχεια της παρούσας διατριβής θα ήταν η συγκεκριμενοποίηση και σε βάθος ανάλυση των απαραίτητων “Επιχειρησιακών” και “Τεχνικών” αλλαγών ενός οργανισμού. Για να επιτευχθεί αυτό, θα πρέπει να υπάρξει η ενασχόληση με ένα και μονό συγκεκριμένο τομέα/αντικείμενοστο οποιο δραστηριοποιείται ένας οργανισμός. Χαρακτηριστικά παραδείγματα θα μπορούσαν να είναι οι μεταφορές(εναέριες ή επίγειες), η ναυτιλία, η υγεία και άλλα.

Με την επιλογή συγκεκριμένου τομέα, στο σκέλος των επιχειρησιακών αλλαγών θα ήταν δυνατή η ανάπτυξη συγκεκριμένων πολιτικών ασφαλείας που θα πρέπει να έχει ένας οργανισμός ο οποίος διαχειρίζεται προσωπικά δεδομένα. Παράλληλα με την πολιτική ασφαλείας θα ήταν δυνατή και η ανάπτυξη συγκεκριμένων διαδικασιών και των αντίστοιχων φορμών για τις διαδικασίες. Στο κομμάτι των τεχνικών αλλαγών, θα ήταν η παρουσίαση συγκεκριμένων πλέον προτάσεων, λύσεων και προϊόντων για την υλοποίηση των απαραιτήτων τεχνικών αλλαγών που θα χρειαστεί να προβεί ένας οργανισμός για την συμμόρφωση με τον νέο κανονισμό.

Βιβλιογραφία

[1] Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ), http://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32016R0679 , ανασύρθηκε στις 20 Δεκεμβριου 2016.

[2] Information is beautiful, World's Biggest Data Breaches, press reports/research: Miriam Quick, Ella Hollowood, Christian Miles, Dan Hampson, http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/ διαβάστηκε στις 21 Ιανουαριου 2017.

[3] Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046 , ανασύρθηκε στις 20 Δεκεμβριου 2016.

[4] INTERNATIONAL STANDARD, ISO/IEC 27001, Second edition, https://www.iso.org/standard/54534.html , ανασύρθηκε στις 3 Απριλιου 2017.

[5] Ορισμός Hardening, https://www.techopedia.com/definition/24833/hardening , διαβάστηκε στις 2 Νοεμβρίου 2017.

[6] Lynis, εφαρμογή hardening, https://cisofy.com/lynis/ , διαβάστηκε στις 2 Νοεμβρίου 2017.

[7] Attack Surface Analyzer, εφαρμογή hardening, https://www.microsoft.com/en-in/download/details.aspx?id=24487 , διαβάστηκε στις 2 Νοεμβρίου 2017.

[8] Ορισμός «πρόληψη της απώλειας δεδομένων (DLP)», http://whatis.techtarget.com/definition/data-loss-prevention-DLP , διαβάστηκε στις 4 Νοεμβρίου 2017.

[9] Εργαλεία για «πρόληψη της απώλειας δεδομένων (DLP)», http://www.techradar.com/news/top-5-best-data-loss-prevention-services , διαβάστηκε στις 4 Νοεμβρίου 2017.

[10] Top 5 best encryption software tools of 2017, http://www.techradar.com/news/top-5-best-encryption-tools , διαβάστηκε στις 11 Νοεμβρίου 2017

[11] graylog εφαρμογή SIEM παρακολούθησης συστημάτων, https://www.graylog.org , διαβάστηκε στις 11 Νοεμβρίου 2017

[12] splunk εφαρμογή SIEM παρακολούθησης συστημάτων, https://www.splunk.com/ , διαβάστηκε στις 11 Νοεμβρίου 2017

[13] OSSIM εφαρμογή SIEM παρακολούθησης συστημάτων, https://www.alienvault.com/ , διαβάστηκε στις 30 Δεκεμβρίου 2017

[14] Ten Top Next-Generation Firewall (NGFW), https://www.esecurityplanet.com/products/top-ngfw-vendors.html , διαβάστηκε στις 5 Ιανουάριου 2018

[15] Owasp anonymization definition, https://www.owasp.org/index.php/Anonymization#Definition , διαβάστηκε στις 2 Νοεμβρίου 2017

[16] Pseudonymization, https://en.wikipedia.org/wiki/Pseudonymization , διαβάστηκε στις 2 Νοεμβρίου 2017

[17] Security information and event management, http://searchsecurity...security-information-and-event-management-SIEM , διαβάστηκε στις 30 Δεκεμβρίου 2017

[18] Εικόνα PDCA, https://en.wikipedia.org/wiki/PDCA , ανασύρθηκε στις 3 Νοεμβριου 2017.