Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών &
Μηχανικών Ηλεκτρονικών Υπολογιστών

Πανεπιστήμιο Πειραιά
Τμήμα Βιομηχανικής Διοίκησης&
Τεχνολογίας

ΔΙΑΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

«ΤΕΧΝΟ-ΟΙΚΟΝΟΜΙΚΑ ΣΥΣΤΗΜΑΤΑ»

GDPR ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΕΣ ΕΦΑΡΜΟΓΕΣ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ (eGOVERMENT)

Αλεξοπούλου Αργυρώ

Επιβλέποντες :

Δρ. Κωνσταντίνος Σιασιάκος
Επιστημονικός Συνεργάτης Ε.Μ.Π

Δημήτριος Ασκούνης
Καθηγητής Ε.Μ.Π

Αθήνα, Ιούνιος 2019

Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών &
Μηχανικών Ηλεκτρονικών Υπολογιστών

Πανεπιστήμιο Πειραιά
Τμήμα Βιομηχανικής Διοίκησης&
Τεχνολογίας

«GDPR ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΕΣ ΕΦΑΡΜΟΓΕΣ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ (eGoverment)»

Αλεξοπούλου Αργυρώ

Εγκρίθηκε από την τριμελή επιτροπή την 14η Ιουνίου 2019.

.....	.....	.....
Ιωάννης Ψαρράς	Δημήτριος Ασκούνης	Κωνσταντίνος Σιασιάκος
Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.	Επιστημονικός Συνεργάτης

.....

Αργυρώ Αλεξοπούλου
Πτυχιούχος Πληροφορικής Πανεπιστημίου Πειραιώς

ΕΥΧΑΡΙΣΤΙΕΣ

Ευχαριστώ τον καθηγητή μου, κ. Κωνσταντίνο Σιασιάκο, για την επίβλεψη αυτής της διπλωματικής, και όλους αυτούς που συνέβαλαν στην εκπόνησης της.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΣΧΗΜΑΤΩΝ

ΠΕΡΙΛΗΨΗ

Ο Γενικός Κανονισμός για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών GDPR (General Data Protection Regulation) με αριθμό 2016/679, ψηφίστηκε στις 27 Απριλίου 2016, και είναι σε ισχύ από τις 25 Μαΐου 2018. Ο κανονισμός αυτός έρχεται να αντικαταστήσει την προηγούμενη οδηγία 95/46 που ήταν σε ισχύ από τις 13 Δεκεμβρίου 1995.

Ο κανονισμός GDPR, ορίζει το τοπίο επεξεργασίας προσωπικών δεδομένων που λαμβάνει χώρα στην Ευρωπαϊκή Οικονομική Ζώνη αλλά και την επεξεργασία προσωπικών δεδομένων ατόμων που βρίσκονται στην Ευρωπαϊκή Οικονομική Ζώνη.

Μία από τις σημαντικότερες αλλαγές που εισάγει ο κανονισμός αυτός, είναι η έννοια των προσωπικών δεδομένων, καθώς πλέον προσωπικό δεδομένο θεωρείται οποιαδήποτε πληροφορία σχετίζεται με ένα πρόσωπο που μπορεί να ταυτοποιηθεί άμεσα ή έμμεσα με τα δεδομένα αυτά.

Φυσικά ή νομικά πρόσωπα, δημόσιες αρχές, υπηρεσίες κτλ, μπορούν να επεξεργάζονται προσωπικά δεδομένα αποκλειστικά και μόνο, εφόσον πληρούν συγκεκριμένες προϋποθέσεις που υπαγορεύει ο κανονισμός GDPR όπως:

- Έχουν επαρκείς, νόμιμους και θεμιτούς λόγους
- Το υποκείμενο των δεδομένων είναι ενήμερο για την επεξεργασία
- Λαμβάνουν επαρκή μέτρα για την προστασία των δεδομένων

Παράλληλα το Υποκείμενο των Δεδομένων έχει πλέον αυξημένα δικαιώματα και μπορεί ανά πάσα στιγμή:

- Να ενημερωθεί για τις διαδικασίες επεξεργασίας που χρησιμοποιούνται
- Να έχει πρόσβαση στα δεδομένα του
- Να ζητήσει διόρθωση/ διαγραφή/ περιορισμό της επεξεργασίας των δεδομένων του

Οι οργανισμοί του δημοσίου τομέα, λόγω της φύσης και του ευρέος φάσματος υπηρεσιών που παρέχουν, έχουν την ανάγκη να κατέχουν και να

επεξεργάζονται τεράστιο όγκο προσωπικών δεδομένων. Οπότε είναι ξεκάθαρο πως το καινούριο αυτό τοπίο όσον αφορά την επεξεργασία προσωπικών δεδομένων, έχει σημαντικές επιπτώσεις στον τρόπο που οι δημόσιοι οργανισμοί λειτουργούν και παρέχουν τις υπηρεσίες τους.

Συγκεκριμένα η εργασία αυτή επικεντρώνεται κυρίως στο κομμάτι των συστημάτων ηλεκτρονικής διακυβέρνησης που χρησιμοποιούνται από τους οργανισμούς του δημοσίου τομέα, και στο πως η μέχρι πρότινος λειτουργία αυτών των ηλεκτρονικών συστημάτων, αλλάζει στην εποχή του GDPR.

Οι αλλαγές αυτές αφορούν τρεις βασικούς τομείς:

- Αλλαγές στην λειτουργία των συστημάτων ηλεκτρονικής διακυβέρνησης, που στοχεύουν κατά κύριο λόγο στο να διασφαλιστεί πως τα συστήματα παρέχουν στους χρήστες όλες τις δυνατότητες που υπαγορεύει ο κανονισμός
- Αλλαγές στο καθεστώς hosting και ασφάλειας, τόσο σε φυσικό όσο και σε επίπεδο εφαρμογών και δεδομένων
- Αλλαγές και προκλήσεις στις συνεργασίες με αναδόχους, όπου τα συστήματα ηλεκτρονικής διακυβέρνησης δημιουργούνται και συντηρούνται από τρίτα μέρη, εκτός του οργανισμού, που αναλαμβάνουν τον ρόλο του «Εκτελών την Επεξεργασία» (Data Processor), όπως ορίζεται από τον κανονισμό GDPR

Είναι γεγονός πως ο κανονισμός GDPR είναι αυτή την στιγμή, το ισχυρότερο καθεστώς προστασίας προσωπικών δεδομένων σε παγκόσμιο επίπεδο. Αυτή η πραγματικότητα, σε συνδυασμό με το αυξανόμενο ενδιαφέρον των ανθρώπων ανά τον κόσμο για την προστασία των προσωπικών τους δεδομένων, έχει ήδη οδηγήσει σε ένα ντόμινο νομοθεσιών ανά τον κόσμο στα πρότυπα του GDPR, και αυτή η τάση αναμένεται να συνεχιστεί.

Λέξεις Κλειδιά:
GDPR, προσωπικά δεδομένα, δημόσιοι οργανισμοί, συστήματα ηλεκτρονικής διακυβέρνησης, ασφάλεια προσωπικών δεδομένων

ABSTRACT

The Regulation of the European Parliament on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, GDPR (General Data Protection Regulation), 2016/679, was adopted on 27 April 2016, and became enforceable beginning 25 May 2018. This regulation repeals the Directive 95/46/EC which was enforceable since 13 December 1995.

The GDPR regulation, defines the personal data processing landscape, which takes place within the European Economic Area, as well as the processing of personal data of persons who are in the European Economic Area.

One of the most important changes which is introduced by this regulation, is the concept of personal data, since according to the regulation, personal data is considered to be any information relating to a person who can be identified directly or indirectly using these data.

Individuals or legal persons, public authorities, services etc. may only process personal data if they meet certain conditions required by the GDPR regulation, such as:

- Have sufficient, legitimate and legal reasons
- The data subject is aware of the processing
- Take adequate measures to protect the data

At the same time, the Data Subject now has increased rights and can at any time:

- Ask to be informed about the processing procedures used
- Access their data
- Ask for correction / deletion / limitation of data processing

Public sector organizations, due to the nature and wide range of services they provide, need to process a huge amount of personal data. It is clear that this

new landscape with regard to the processing of personal data, has a significant impact on the way public agencies operate and provide their services.

This paper focuses mainly on the electronic eGovernment systems used by public sector organizations, and how the operation of these eGovernment systems is changing in the era of GDPR.

These changes concern three main areas:

- Functional changes in eGovernment systems, which are primarily aimed at ensuring that these systems provide to the users all the possibilities that are required by the regulation
- Changes for hosting and security services, applicable to both the physical layer as well as the application and data layer
- Changes and challenges to partnerships with contractors, where eGovernment systems are created and maintained by third parties outside the organization that assume the role of the “Data Processor” as defined by the GDPR regulation

Right now, the GDPR regulation is the most powerful regime regarding data protection, on a global scale. This fact, in combination with the data subject’s increased interest in protecting their data, has already started a legislation domino across the globe, with more countries drafting and adopting local laws and regulations similar to GDPR. This trend is expected to continue.

Key Words:
GDPR, personal data, public sector, eGovernment systems, personal data privacy

Κεφάλαιο 1 – Γνωρίζοντας τον GDPR

1.1 Εισαγωγή

Ο Γενικός Κανονισμός για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών GDPR (General Data Protection Regulation) με αριθμό 2016/679, ψηφίστηκε στις 27 Απριλίου 2016, και είναι σε ισχύ από τις 25 Μαΐου 2018. Ο κανονισμός αυτός έρχεται να αντικαταστήσει την προηγούμενη οδηγία 95/46 που ήταν σε ισχύ από τις 13 Δεκεμβρίου 1995.

Είναι σημαντικό να σημειωθεί πως ο καινούριος αυτός ευρωπαϊκός κανονισμός είναι κανονισμός και όχι οδηγία. Παρακάτω παρατίθενται οι ορισμοί όπως δίνονται στην επίσημη ιστοσελίδα της Ευρωπαϊκής Ένωσης:

> *“Κανονισμοί*
>
> *Οι κανονισμοί είναι δεσμευτικές νομοθετικές πράξεις. Η εφαρμογή τους σε όλες τις χώρες της ΕΕ είναι υποχρεωτική. Για παράδειγμα, όταν η ΕΕ θέλησε να εφαρμόσει κοινές διασφαλίσεις για τα προϊόντα που εισάγονται από χώρες εκτός ΕΕ, το Συμβούλιο εξέδωσε έναν κανονισμό.*
>
> *Οδηγίες*
>
> *Οι οδηγίες είναι νομοθετικές πράξεις που ορίζουν έναν στόχο τον οποίο πρέπει να επιτύχουν όλες οι χώρες της ΕΕ. Ωστόσο, εναπόκειται σε κάθε χώρα να θεσπίσει τους δικούς της νόμους για την επίτευξη των στόχων αυτών. Ένα παράδειγμα είναι η οδηγία της ΕΕ για τα δικαιώματα των καταναλωτών, η οποία ενδυναμώνει τα δικαιώματα των καταναλωτών σε όλη την ΕΕ, π.χ. εξαλείφοντας κρυφές χρεώσεις και έξοδα στο διαδίκτυο, και παρατείνοντας την περίοδο κατά την οποία οι καταναλωτές μπορούν να υπαναχωρήσουν από μια σύμβαση πώλησης.”*
>
> *Πηγή:* https://europa.eu/european-union/eu-law/legal-acts_el

Αυτό σημαίνει πως ο κανονισμός GDPR, με όλες τις διατάξεις του, είναι σε ισχύ ομοιόμορφα από τις 25 Μαΐου 2018 σε όλη την Ευρωπαϊκή Ένωση, αυτούσιος και χωρίς να περάσει πρώτα για επεξεργασία, σχηματισμό εθνικής νομοθεσίας και ψήφιση από το εθνικό κοινοβούλιο κάθε κράτους μέλους.

1.2 Τι αφορά

Ο κανονισμός GDPR, ορίζει το τοπίο επεξεργασίας προσωπικών δεδομένων. Και πιο συγκεκριμένα οριοθετεί:

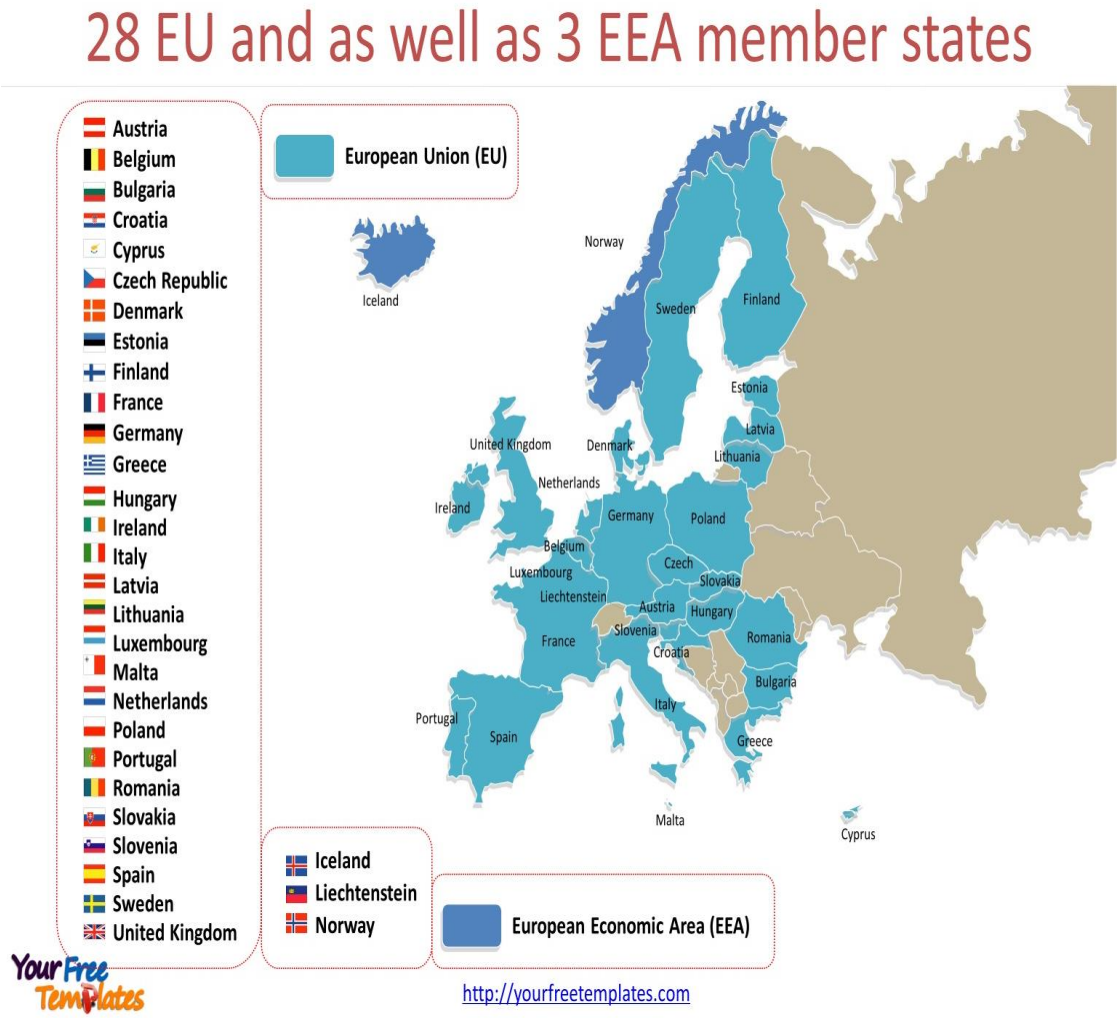
- Την επεξεργασία προσωπικών δεδομένων που λαμβάνει χώρα στην Ευρωπαϊκή Οικονομική Ζώνη (European Economic Area (EEA)).
- Την επεξεργασία προσωπικών δεδομένων ατόμων που βρίσκονται στην Ευρωπαϊκή Οικονομική Ζώνη (EEA) – ανεξάρτητα από την τοποθεσία στην οποία γίνεται η επεξεργασία αυτή.

1.3 Ποιόν αφορά

Σύμφωνα με τα παραπάνω, ο κανονισμός GDPR αφορά κάθε οργανισμό, οπουδήποτε στον κόσμο, που έχει στην κατοχή του προσωπικά δεδομένα Ευρωπαίων πολιτών, η ατόμων που βρίσκονται στην Ευρωπαϊκή Ένωση έστω και για περιορισμένο διάστημα (για παράδειγμα για διακοπές).

Οι χώρες που καλούνται άμεσα να συμμορφωθούν με τον κανονισμό είναι οι χώρες της Ευρωπαϊκής Οικονομικής Ζώνης (EEA) οι οποίες είναι οι παρακάτω:

- Κράτη μέλη της Ευρωπαϊκής Ένωσης: Αυστρία, Βέλγιο, Βουλγαρία, Κροατία, Κύπρος, Τσεχία, Δανία, Εσθονία, Φινλανδία, Γαλλία, Γερμανία, Ελλάδα, Ουγγαρία, Ιρλανδία, Ιταλία, Λετονία, Λιθουανία, Λουξεμβούργο, Μάλτα, Ολλανδία, Πολωνία, Πορτογαλία, Ρουμανία, Σλοβακία, Σλοβενία, Ισπανία, Σουηδία, Ηνωμένο Βασίλειο.
- Καθώς επίσης και οι: Ισλανδία, Λιχτενστάιν, Νορβηγία.



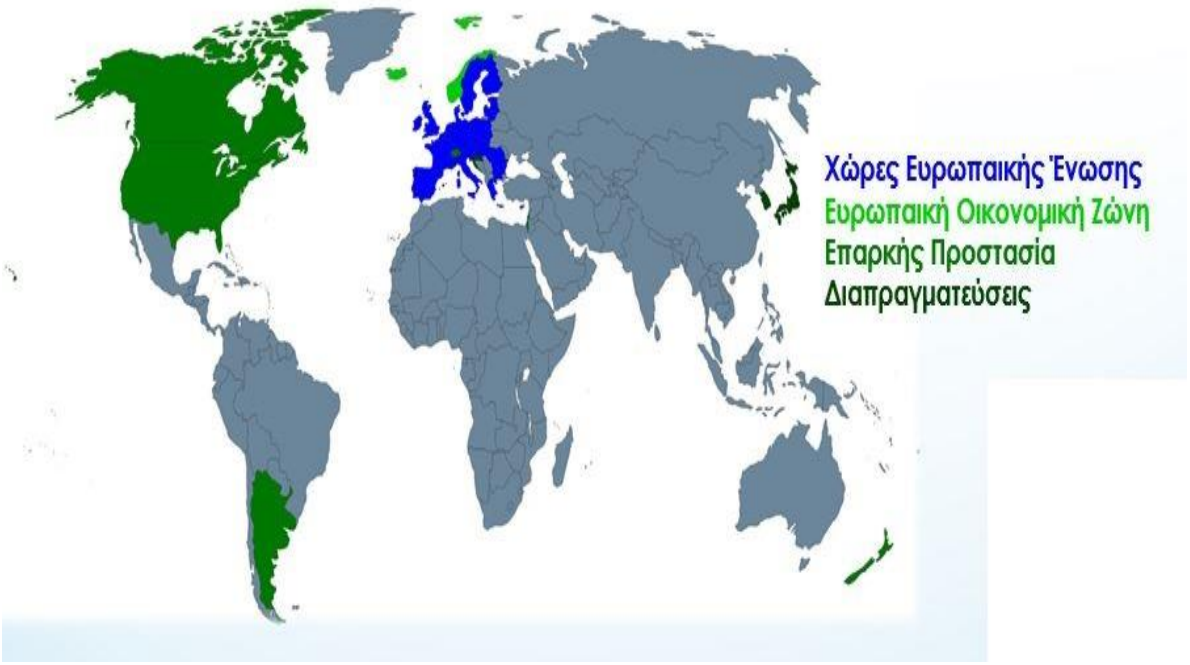
Εικόνα 1 *Ευρωπαϊκή Οικονομική Ζώνη*

Η Ευρωπαϊκή Επιτροπή έχει την εξουσία να καθορίσει (άρθρο 45 του κανονισμού GDPR 2016/679), αν κάποια χώρα πέρα από τις χώρες που ανήκουν στην Ευρωπαϊκή Οικονομική Ζώνη (ΕΕΑ), παρέχει επαρκές επίπεδο ασφάλειας των προσωπικών δεδομένων, είτε λόγω της εθνικής νομοθεσίας της, είτε λόγω διεθνών δεσμεύσεων που έχει πάρει. Μια τέτοια θετική απόφαση της Ευρωπαϊκής Επιτροπής σημαίνει πως τα δεδομένα μπορούν να αποστέλλονται από χώρες της Ευρωπαϊκής Οικονομικής Ζώνης (ΕΕΑ) σε αυτή την τρίτη χώρα, χωρίς να χρειαστεί να ληφθούν επιπλέον μέτρα προστασίας. Δηλαδή, η μεταβίβαση δεδομένων σε αυτές τις χώρες θα είναι σαν να ήταν εντός της ΕΕΑ.

Μέχρι στιγμής, η Ευρωπαϊκή Επιτροπή έχει αναγνωρίσει ότι οι παρακάτω χώρες παρέχουν επαρκή προστασία: Ανδόρα, Αργεντινή, Καναδάς (όσον

αφορά τους εμπορικούς οργανισμούς), Ισραήλ, Νήσος του Μαν, Νήσοι Φερόε, Γκέρνσεϋ, Τζέρσεϋ, Νέα Ζηλανδία, Ελβετία, Ουρουγουάη, Ηνωμένες Πολιτείες Αμερικής.

Επίσης υπάρχουν συζητήσεις με την Νότια Κορέα και την Ιαπωνία.



Εικόνα 2 *Παγκόσμιος Χάρτης GDPR*

1.4 Βασικές Αρχές και ορολογία

Οι βασικές αρχές και το πνεύμα του κανονισμού GDPR συνοψίζονται παρακάτω.

1. Νομιμότητα, δικαιοσύνη και διαφάνεια στην επεξεργασία προσωπικών δεδομένων
2. Περιορισμός του σκοπού επεξεργασίας
3. Ελαχιστοποίηση προσωπικών δεδομένων
4. Ακρίβεια προσωπικών δεδομένων
5. Περιορισμός μεθόδων επεξεργασίας
6. Ακεραιότητα και εμπιστευτικότητα των επεξεργασμένων δεδομένων
7. Υπευθυνότητα και λογοδοσία στην επεξεργασία προσωπικών δεδομένων

Αξίζει να αναφερθεί πως μία από τις σημαντικές αλλαγές που εισάγει ο κανονισμός αυτός, είναι η έννοια των προσωπικών δεδομένων. Για διευκόλυνση στην κατανόηση χρειάζεται να διευκρινιστούν οι κύριοι όροι του κανονισμού GDPR:

1. *Προσωπικά Δεδομένα (Personal Data)*: Οποιαδήποτε πληροφορία σχετίζεται με ένα ταυτοποιημένο ή ταυτοποιήσιμο πρόσωπο.
2. *Επεξεργασία Δεδομένων (Processing)*: Οποιαδήποτε δραστηριότητα αφορά τα δεδομένα.
3. *Υπεύθυνος Επεξεργασίας (Data Controller)*: Καθορίζει το σκοπό, την έκταση και τα μέσα επεξεργασίας.
4. *Εκτελών την επεξεργασία (Data Processor)*: Επεξεργάζεται τα προσωπικά δεδομένα σύμφωνα με τις οδηγίες του Υπεύθυνου Επεξεργασίας.
5. *Υποκείμενο δεδομένων (Data Subject)*: Το πρόσωπο του οποίου τα προσωπικά δεδομένα επεξεργάζονται.
6. *Αξιολόγηση των επιπτώσεων στην προστασία δεδομένων (Data Protection Impact Assessment)*: Αναγνώριση των κινδύνων.
7. *Δραστηριότητα επεξεργασίας δεδομένων (Data Processing Activity)*: Όλες οι διαδικασίες που περιλαμβάνουν επεξεργασία προσωπικών δεδομένων.

1.4.1 Προσωπικά Δεδομένα (Personal Data)

Όπως αναφέρθηκε και παραπάνω, μία από τις σημαντικότερες αλλαγές που εισάγει ο κανονισμός GDPR, είναι η έννοια των προσωπικών δεδομένων.

Προσωπικό δεδομένο για τον GDPR θεωρείται οποιαδήποτε πληροφορία σχετίζεται με ένα πρόσωπο που μπορεί να ταυτοποιηθεί άμεσα ή έμμεσα με τα δεδομένα αυτά. Για παράδειγμα:

- Όνομα, Επώνυμο, ψευδώνυμο
- Ταχυδρομική ή ηλεκτρονική διεύθυνση
- Προσωπικά αναγνωριστικά όπως ΑΦΜ, αριθμός ταυτότητας ή διαβατηρίου, άδεια οδήγησης, κτλ.
- Φύλο, ηλικία, ημερομηνία γέννησης

Όσον αφορά τις ειδικές κατηγορίες προσωπικών δεδομένων, σαν γενικός κανόνας δεν επιτρέπεται η κατοχή και επεξεργασία τους, εκτός συγκεκριμένων εξαιρέσεων που θα αναφερθούν παρακάτω. Για παράδειγμα:

- Φυλή ή εθνική ταυτότητα
- Πολιτικά πιστεύω
- Θρησκεία
- Συμμετοχή σε εργατικά σωματεία
- Γενετικά δεδομένα
- Βιομετρικά δεδομένα
- Υγεία
- Σεξουαλική ζωή ή προτιμήσεις

1.4.2 Επεξεργασία Δεδομένων (Processing)

Ως επεξεργασία των δεδομένων ορίζεται γενικά οποιαδήποτε δραστηριότητα αφορά τα δεδομένα. Όπως:

- Συλλογή, καταγραφή, οργάνωση, αλλαγή δομής, αποθήκευση
- Προσαρμογή, τροποποίηση, ανάκτηση
- Ανάγνωση, χρήση
- Αποστολή, διάδοση, διάθεση
- Συσχέτιση, συνδυασμός
- Περιορισμός, διαγραφή, καταστροφή

Για παράδειγμα, όλες οι υπογραμμισμένες λέξεις στην παρακάτω πρόταση, αποτελούν ενέργειες επεξεργασίας δεδομένων:

Λαμβάνουμε, και αποθηκεύουμε ένα αρχείο, το οποίο στη συνέχεια επεξεργαζόμαστε και αποστέλλουμε σε κάποιον τρίτο.

1.4.3 Υπεύθυνος Επεξεργασίας (Data Controller)

Ο Υπεύθυνος Επεξεργασίας, είναι ένα φυσικό ή νομικό πρόσωπο, μια δημόσια αρχή, μια υπηρεσία κτλ, και είναι ο κατεξοχήν ενδιαφερόμενος για τη χρήση των δεδομένων. Πιο συγκεκριμένα:

- Καθορίζει τον σκοπό, την έκταση και τα μέσα επεξεργασίας
- Μπορεί να ενεργεί μόνος ή από κοινού με άλλους φορείς / Υπεύθυνους Επεξεργασίας

Για παράδειγμα:

- Το τμήμα ανθρώπινου δυναμικού μιας επιχείρησης είναι Υπεύθυνος Επεξεργασίας όσον αφορά τα προσωπικά δεδομένα των υπαλλήλων της επιχείρησης.
- Η Αστυνομία είναι Υπεύθυνος Επεξεργασίας όσον αφορά τα δεδομένα των πολιτών.

1.4.4 Εκτελών την επεξεργασία (Data Processor)

Ο Εκτελών την επεξεργασία, είναι ένα φυσικό ή νομικό πρόσωπο, μια δημόσια αρχή, μια υπηρεσία κτλ, και επεξεργάζεται τα προσωπικά δεδομένα σύμφωνα με τις οδηγίες του Υπεύθυνου Επεξεργασίας.

Για παράδειγμα:

- Το τμήμα μηχανογράφησης μιας επιχείρησης είναι ο Εκτελών την επεξεργασία, σύμφωνα με τις οδηγίες του τμήματος ανθρώπινου δυναμικού της επιχείρησης.
- Ένα τυπογραφείο που έχει αναλάβει την εκτύπωση των διαβατηρίων, είναι ο Εκτελών την επεξεργασία, σύμφωνα με τις οδηγίες της Αστυνομίας.

1.4.5 Υποκείμενο Δεδομένων (Data Subject)

Υποκείμενο Δεδομένων είναι το πρόσωπο του οποίου τα προσωπικά δεδομένα επεξεργάζονται. Πιο συγκεκριμένα:

- Πρέπει να είναι φυσικό πρόσωπο (όχι νομικό)
- Πρέπει να είναι εν ζωή
- Πρέπει να είναι ταυτοποιημένο ή ταυτοποιήσιμο

1.5 Προβλεπόμενες Κυρώσεις

Σε περίπτωση παραβίασης των διατάξεων του κανονισμού GDPR, ο κανονισμός προβλέπει σημαντικές κυρώσεις:

- Για μη συμμόρφωση με τις προβλεπόμενες διαδικασίες, ασφάλεια δεδομένων κτλ, προβλέπεται πρόστιμο έως και 10 εκατομμύρια ευρώ ή, σε περίπτωση επιχειρήσεων, έως το 2% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους, ανάλογα με το ποιο ποσό είναι υψηλότερο
- Για μη συμμόρφωση με τις βασικές αρχές του κανονισμού, παραβίαση των δικαιωμάτων των υποκειμένων των δεδομένων κτλ, προβλέπεται πρόστιμο έως και 20 εκατομμύρια ευρώ ή, σε περίπτωση επιχειρήσεων, έως το 4% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους, ανάλογα με το ποιο ποσό είναι υψηλότερο

Εικόνα 3 *Ποινές για μη-συμμόρφωση με τον κανονισμό GDPR*

Ωστόσο είναι σημαντικό να αναφερθεί πως οι νομοθέτες φυσικά γνωρίζουν πως κανένα πρωτόκολλο ασφαλείας δεν είναι τέλειο και παραβιάσεις δεδομένων

συμβαίνουν στο σύγχρονο επιχειρηματικό περιβάλλον. Οι επιχειρήσεις/ φορείς/ υπηρεσίες που μπορούν να αποδείξουν ότι έχει γίνει σημαντική προσπάθεια συμμόρφωσης με τις διατάξεις του κανονισμού GDPR και ότι εφαρμόζονται συγκεκριμένες πολιτικές, πρωτόκολλα και διαδικασίες προστασίας δεδομένων, θα έχουν πολύ καλύτερες πιθανότητες να αποφύγουν πρόστιμα και κυρώσεις σε περίπτωση παραβίασης της ασφάλειας των δεδομένων.

1.6 Σε περίπτωση παραβίασης της ασφάλειας των δεδομένων

Σε περίπτωση παραβίασης της ασφάλειας των προσωπικών δεδομένων, πρέπει να ειδοποιηθεί αμέσως ο Υπεύθυνος Προστασίας Δεδομένων, καθώς και η διοίκηση του οργανισμού/ επιχείρησης/ φορέα/ αρχής/ υπηρεσίας κτλ.

Μέσα σε 72 ώρες πρέπει να γίνει η απαραίτητη έρευνα και να ληφθεί μια απόφαση για την σωστή διαχείριση της κατάστασης σύμφωνα με τις διατάξεις του κανονισμού GDPR. Όλες οι απαραίτητες διαδικασίες που περιλαμβάνουν επικοινωνία με τις αρμόδιες αρχές αλλά και με τα υποκείμενα των δεδομένων γίνονται από τον Υπεύθυνο Προστασίας Δεδομένων.

1.7 Σύνοψη

Συνοψίζοντας τα βασικά σημεία του κανονισμού GDPR, οι οργανισμοί μπορούν να επεξεργάζονται προσωπικά δεδομένα εφόσον πληρούν συγκεκριμένες προϋποθέσεις, όπως για παράδειγμα:

- Έχουν επαρκείς, νόμιμους και θεμιτούς λόγους
- Το υποκείμενο των δεδομένων είναι ενήμερο για την επεξεργασία
- Λαμβάνουν επαρκή μέτρα για την προστασία των δεδομένων
- Σε περίπτωση που τα προσωπικά δεδομένα αφορούν παιδιά ή ευαίσθητα δεδομένα, λαμβάνονται ειδικά μέτρα προστασίας
- Έχουν ορίσει έναν Υπεύθυνο Προστασίας Δεδομένων (Data Protection Officer) ο οποίος:
    - Κατέχει συμβουλευτικό ρόλο
    - Ελέγχει το κατά πόσο οι χρησιμοποιούμενες πρακτικές συμμορφώνονται με τον κανονισμό GDPR

- Είναι υπεύθυνος για την επικοινωνία με τις αρχές αλλά και με τα υποκείμενα των δεδομένων

Το Υποκείμενο των Δεδομένων έχει συγκεκριμένα δικαιώματα και μπορεί ανά πάσα στιγμή:

- Να ενημερωθεί για τις διαδικασίες επεξεργασίας που χρησιμοποιούνται
- Να έχει πρόσβαση στα δεδομένα του – το αίτημα αυτό πρέπει να ικανοποιηθεί μέσα σε 30 ημέρες από τον Υπεύθυνο για την επεξεργασία/ Εκτελών την επεξεργασία
- Να ζητήσει διόρθωση των δεδομένων του, σε περίπτωση που υπάρχουν λάθη
- Να ζητήσει την διαγραφή των δεδομένων του
- Να ζητήσει τον περιορισμό της επεξεργασίας των δεδομένων του

Κεφάλαιο 2 – GDPR και Δημόσιος Τομέας

2.1 Εισαγωγή

Στο προηγούμενο κεφάλαιο έγινε μια εισαγωγή σχετικά με τον κανονισμό GDPR, τι αφορά, ποιόν αφορά, τι αλλαγές φέρνει και τι κυρώσεις προβλέπει.

Σε αυτό το κεφάλαιο επικεντρωνόμαστε περισσότερο στο πως ο κανονισμός αυτός επηρεάζει συγκεκριμένα τους οργανισμούς του δημοσίου τομέα, εάν εφαρμόζεται σε αυτούς, και με τι ιδιαιτερότητες καθώς και τι ιδιαίτερες ανάγκες και προκλήσεις προκύπτουν για τους δημόσιους οργανισμούς.

2.2 Εφαρμόζεται ο κανονισμός στον Δημόσιο τομέα;

Μία από τις μεγαλύτερες παρεξηγήσεις σχετικά με τον κανονισμό GDPR, είναι ότι δεν ισχύει για οργανισμούς του δημόσιου τομέα. Στην πραγματικότητα, πολλοί οργανισμοί του δημόσιου τομέα πρέπει να συμμορφωθούν με τον κανονισμό GDPR.

Για παράδειγμα στο παρακάτω απόσπασμα από τον κανονισμό γίνεται ξεκάθαρη αναφορά στον δημόσιο τομέα:

> *“(6) Οι ραγδαίες τεχνολογικές εξελίξεις και η παγκοσμιοποίηση δημιούργησαν νέες προκλήσεις για την προστασία των δεδομένων προσωπικού χαρακτήρα. Η κλίμακα της συλλογής και της ανταλλαγής δεδομένων προσωπικού χαρακτήρα αυξήθηκε σημαντικά. Η τεχνολογία επιτρέπει τόσο σε ιδιωτικές επιχειρήσεις όσο και σε δημόσιες αρχές να κάνουν χρήση δεδομένων προσωπικού χαρακτήρα σε πρωτοφανή κλίμακα για την επιδίωξη των δραστηριοτήτων τους.”*
>
> *Πηγή: https://publications.europa.eu/el/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1*

Διαβάζοντας τον κανονισμό γίνεται επίσης ξεκάθαρο πως δημόσιοι οργανισμοί μπορούν να έχουν τους ρόλους του Υπεύθυνου Επεξεργασίας (Data Controller) αλλά και του Εκτελών την επεξεργασία (Data Processor):

"Άρθρο 4

7) «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,

8) «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,"

Πηγή: https://publications.europa.eu/el/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1

Επίσης γίνεται λόγος ακόμα και για πρόστιμα σε δημόσιους οργανισμούς σε περίπτωση μη συμμόρφωσης με τον κανονισμό:

"(150)…. Θα πρέπει να εναπόκειται στα κράτη μέλη να αποφασίζουν εάν και σε ποιο βαθμό μπορούν να επιβάλλονται διοικητικά πρόστιμα σε δημόσιες αρχές. Η επιβολή διοικητικού προστίμου ή η προειδοποίηση δεν θίγει την εφαρμογή των λοιπών εξουσιών των εποπτικών αρχών ή άλλων κυρώσεων δυνάμει του παρόντος κανονισμού."

Πηγή: https://publications.europa.eu/el/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1

2.3 Ανάγκη συλλογής και επεξεργασίας Προσωπικών Δεδομένων

Οι οργανισμοί του δημοσίου τομέα, λόγω της φύσης και του ευρέος φάσματος υπηρεσιών που παρέχουν, έχουν την ανάγκη να κατέχουν και να επεξεργάζονται τεράστιο όγκο προσωπικών δεδομένων. Όπως αναφέρθηκε και παραπάνω προσωπικό δεδομένο θεωρείται οτιδήποτε προσδιορίζει ένα άτομο (φωτογραφίες, όνομα, επώνυμο, ημερομηνία γέννησης, διεύθυνση κατοικίας, εξαρτώμενα πρόσωπα, φυλετική ή εθνική καταγωγή, θρησκευτικές/ πολιτικές/ κοινωνικές πεποιθήσεις, υγεία, φύλο, σεξουαλικές προτιμήσεις κλπ). Επιπρόσθετα, εφόσον οι οργανισμοί του δημοσίου τομέα συναλλάσσονται συχνά με πολίτες από ευάλωτες κοινωνικές ομάδες, είναι ακόμα πιο κρίσιμο να δοθεί έμφαση στην ασφάλεια των δεδομένων.

Στα πλαίσια της καθημερινής λειτουργίας τους, επεξεργάζονται τακτικά προσωπικά δεδομένα, οπότε οι ίδιοι οι οργανισμοί είναι υπεύθυνοι για την προστασία των δεδομένων των πολιτών. Για αυτούς τους λόγους είναι επιτακτική η ανάγκη για υιοθέτηση πολιτικών και διαδικασιών για την αποθήκευση και την προσπέλαση των δεδομένων, αλλά δυστυχώς, οι δημόσιοι οργανισμοί είναι συχνά σε έλλειψη πόρων και προσωπικού, γεγονός που δυσκολεύει τον σχεδιασμό αλλά και την υλοποίηση τέτοιων πολιτικών και διαδικασιών.

2.4 Παρωχημένα και ανακριβή δεδομένα

Πέρα από τον όγκο των προσωπικών δεδομένων που συλλέγουν και διατηρούν, ένας ακόμη παράγοντας που πρέπει να ληφθεί υπόψιν είναι το κατά πόσο τα δεδομένα αυτά είναι σχετικά ή απαραίτητα για την διεκπεραίωση των εργασιών του οργανισμού καθώς και το κατά πόσο είναι ακριβή. Συχνά οι βάσεις δεδομένων και τα συστήματα αρχειοθέτησης είναι υπερφορτωμένα με μαζικές ποσότητες παρωχημένων και περιττών πληροφοριών. Οι οργανισμοί πρέπει να εξετάσουν και να προσδιορίσουν ποια είναι τα δεδομένα που κατέχουν, και αν αυτά είναι χρήσιμα και ακριβή.

Ως εκ τούτου, εμφανίζεται η ανάγκη για πιο ισχυρά πληροφοριακά συστήματα, ικανά να διαχειριστούν τον όγκο των δεδομένων και να εξασφαλίσουν επαρκή

προστασία. Για πολλούς οργανισμούς αυτό είναι αρκετά δύσκολο, καθώς συχνά χρησιμοποιούν παλαιά τεχνολογία η οποία συνήθως είναι ξεπερασμένη και δεν μπορεί να καλύψει τις νέες απαιτήσεις.

2.5 Ιδιαιτερότητες του κανονισμού GDPR για τον δημόσιο τομέα

Εδώ πρέπει να αναφέρουμε πως ο δημόσιος τομέας υπόκειται σε ορισμένες εξαιρέσεις από τον κανονισμό GDPR, σε αντίθεση με τον ιδιωτικό τομέα.

Για παράδειγμα, το δικαίωμα του υποκειμένου των δεδομένων να ζητήσει διαγραφή των δεδομένων του (δικαίωμα στη λήθη) δεν ισχύει για τον δημόσιο τομέα, εάν η διαγραφή αυτή εμποδίζει την εκπλήρωση ενός έργου που εκτελείται για το δημόσιο συμφέρον όσον αφορά την υγεία, την ανάγκη αρχειοθέτησης, ή υπηρετεί επιστημονικούς, ιστορικούς ή στατιστικούς σκοπούς:

> *“Άρθρο 17*
>
> *3.Οι παράγραφοι 1 και 2 (δικαίωμα στη λήθη – διαγραφή δεδομένων) δεν εφαρμόζονται στον βαθμό που η επεξεργασία είναι απαραίτητη:*
>
> *γ) για λόγους δημόσιου συμφέροντος στον τομέα της δημόσιας υγείας σύμφωνα με το άρθρο 9 παράγραφος 2 στοιχεία η) και θ), καθώς και το άρθρο 9 παράγραφος 3,*
>
> *δ) για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς σύμφωνα με το άρθρο 89 παράγραφος 1, εφόσον το δικαίωμα που αναφέρεται στην παράγραφο 1 είναι πιθανόν να καταστήσει αδύνατη ή να εμποδίσει σε μεγάλο βαθμό την επίτευξη σκοπών της εν λόγω επεξεργασίας…”*
>
> *Πηγή: https://publications.europa.eu/el/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1*

Επίσης ο κανονισμός GDPR δεν εφαρμόζεται όσον αφορά συλλογή και επεξεργασία δεδομένων από δημόσιους οργανισμούς όταν ο σκοπός είναι η δημόσια ασφάλεια, η πρόληψη και η καταπολέμηση εγκληματικών ενεργειών, κτλ:

> *"(19) Η προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, της διερεύνησης, της ανίχνευσης ή της δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων, συμπεριλαμβανομένης της διασφάλισης έναντι των απειλών κατά της δημόσιας ασφάλειας και της πρόληψής τους και της ελεύθερης κυκλοφορίας των δεδομένων αυτών, αποτελεί το αντικείμενο ειδικής ενωσιακής νομικής πράξης. Ο παρών κανονισμός δεν θα πρέπει συνεπώς να εφαρμόζεται σε δραστηριότητες επεξεργασίας για τους σκοπούς αυτούς. Ωστόσο, τα δεδομένα προσωπικού χαρακτήρα που υφίστανται επεξεργασία από δημόσιες αρχές βάσει του παρόντος κανονισμού θα πρέπει, όταν χρησιμοποιούνται για αυτούς τους σκοπούς, να ρυθμίζονται από ειδικότερη ενωσιακή νομική πράξη, δηλαδή την οδηγία (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (1). Τα κράτη μέλη μπορούν να αναθέτουν στις αρμόδιες αρχές κατά την έννοια της οδηγίας (ΕΕ) 2016/680 καθήκοντα που δεν ασκούνται απαραιτήτως για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων, συμπεριλαμβανομένης της διασφάλισης έναντι των απειλών κατά της δημόσιας ασφάλειας και της πρόληψής τους, ούτως ώστε η επεξεργασία δεδομένων προσωπικού χαρακτήρα για αυτούς τους άλλους σκοπούς, εφόσον εμπίπτει στο πεδίο εφαρμογής του ενωσιακού δικαίου, να υπάγεται στο πεδίο εφαρμογής του παρόντος κανονισμού."*
>
> *Πηγή:* https://publications.europa.eu/el/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1

Ο κανονισμός δεν εφαρμόζεται επίσης για δεδομένα που αφορούν εγκλήματα πολέμου κτλ:

> *"(158) … Στα κράτη μέλη θα πρέπει επίσης να δοθεί το δικαίωμα να προβλέπουν περαιτέρω επεξεργασία δεδομένων προσωπικού χαρακτήρα για σκοπούς αρχειοθέτησης, λόγου χάρη με στόχο την παροχή συγκεκριμένων πληροφοριών σχετικών με πολιτική συμπεριφορά σε πρώην απολυταρχικά καθεστώτα, γενοκτονία, εγκλήματα κατά της ανθρωπότητας, ιδίως το Ολοκαύτωμα, ή εγκλήματα πολέμου."*
>
> *Πηγή: https://publications.europa.eu/el/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1*

Ρητή αναφορά γίνεται και στην δυνατότητα των δημόσιων οργανισμών να παρέχουν πρόσβαση στο κοινό σε προσωπικά δεδομένα, όταν αυτό γίνεται για το δημόσιο συμφέρον:

> *"(154) Ο παρών κανονισμός επιτρέπει να λαμβάνεται υπόψη η αρχή της πρόσβασης του κοινού στα επίσημα έγγραφα κατά την εφαρμογή του παρόντος κανονισμού. Η πρόσβαση του κοινού σε επίσημα έγγραφα μπορεί να θεωρηθεί ως δημόσιο συμφέρον. Τα δεδομένα προσωπικού χαρακτήρα σε έγγραφα που τηρούνται από δημόσια αρχή ή δημόσιο φορέα θα πρέπει να μπορούν να κοινολογούνται δημοσίως από την εν λόγω αρχή ή τον φορέα εάν η κοινολόγηση προβλέπεται από το δίκαιο της Ένωσης ή το δίκαιο του κράτους μέλους στο οποίο υπάγεται η δημόσια αρχή ή ο δημόσιος φορέας. Τα δίκαια αυτά θα πρέπει να συμφιλιώνουν την πρόσβαση του κοινού σε επίσημα έγγραφα και την περαιτέρω χρήση πληροφοριών του δημόσιου τομέα με το δικαίωμα προστασίας δεδομένων προσωπικού χαρακτήρα και μπορούν, συνεπώς, να προβλέπουν την αναγκαία συμφιλίωση με το δικαίωμα προστασίας δεδομένων προσωπικού χαρακτήρα δυνάμει του παρόντος κανονισμού…"*

Πηγή: https://publications.europa.eu/el/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1

Όσον αφορά τα διοικητικά πρόστιμα που προβλέπονται από τις διατάξεις του κανονισμού GDPR, σε αντίθεση με τον ιδιωτικό τομέα, το κάθε κράτος μέλος θα μπορεί να αποφασίσει αν τα πρόστιμα αυτά θα αφορούν δημόσιους οργανισμούς η όχι.

(150) … Θα πρέπει να εναπόκειται στα κράτη μέλη να αποφασίζουν εάν και σε ποιο βαθμό μπορούν να επιβάλλονται διοικητικά πρόστιμα σε δημόσιες αρχές. Η επιβολή διοικητικού προστίμου ή η προειδοποίηση δεν θίγει την εφαρμογή των λοιπών εξουσιών των εποπτικών αρχών ή άλλων κυρώσεων δυνάμει του παρόντος κανονισμού.

Πηγή: https://publications.europa.eu/el/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1

2.6 Ανάγκες του δημόσιου τομέα για συμμόρφωση με τον κανονισμό GDPR

Καθώς ο κανονισμός GDPR παρέχει πολύ μεγαλύτερο έλεγχο στα υποκείμενα των δεδομένων, δίνοντάς τους το δικαίωμα πρόσβασης στις προσωπικές τους πληροφορίες κατόπιν αιτήματος, οι οργανισμοί πρέπει να είναι σε θέση να ανταποκρίνονται εγκαίρως σε αυτά τα αιτήματα. Όλα τα υποκείμενα των δεδομένων έχουν το δικαίωμα να υποβάλλουν αίτηση αιτήματος πρόσβασης (SAR). Με απλά λόγια, όλοι έχουν δικαίωμα πρόσβασης στα προσωπικά τους δεδομένα κατόπιν αιτήματος και οι οργανισμοί υποχρεούνται να απαντούν σε αυτά τα αιτήματα εντός 30 ημερών σύμφωνα με τις διατάξεις του κανονισμού GDPR. Οι δημόσιοι οργανισμοί θα πρέπει να διασφαλίσουν ότι υπάρχουν ισχυρά συστήματα επεξεργασίας δεδομένων για την αντιμετώπιση των νέων δικαιωμάτων που αποκτούν τα υποκείμενα των δεδομένων, καθώς υπάρχει κίνδυνος σημαντικών προστίμων σε περίπτωση παραβίασης του κανονισμού. Αυτό αναμφίβολα θα δημιουργήσει πρόσθετη διοικητική εργασία για όλους τους οργανισμούς του δημόσιου τομέα.

Μόλις εξασφαλιστεί ότι ένας δημόσιος οργανισμός ικανοποιεί τον κανονισμό GDPR, και ότι οι απαραίτητες πολιτικές και διαδικασίες έχουν μελετηθεί και εφαρμοστεί, υπάρχει ακόμα ένα σημείο που θα πρέπει να προσεχθεί και αυτό είναι η συνεχής διαχείριση των διαδικασιών. Σύμφωνα με τον κανονισμό GDPR, οι δημόσιοι οργανισμοί θα πρέπει να σχεδιάζουν και να προγραμματίζουν τακτικές αξιολογήσεις κινδύνου για τον εντοπισμό οποιωνδήποτε αδυναμιών στα συστήματα επεξεργασίας δεδομένων ώστε να διασφαλίζεται η συνεχής ασφάλεια των δεδομένων. Είναι επιτακτική ανάγκη οι δημόσιοι οργανισμοί να φροντίσουν ότι όλοι οι εργαζόμενοι που «αγγίζουν» τα δεδομένα, είναι άρτια εκπαιδευμένοι και ενημερωμένοι για τις αλλαγές, ικανοί να αναγνωρίσουν και να αναφέρουν οποιοδήποτε θέμα προκύψει που είναι πιθανό να παραβιάζει τον κανονισμό GDPR.

Σαν μέρος των αυστηρότερων απαιτήσεων του κανονισμού GDPR, η συγκατάθεση του υποκειμένου των δεδομένων πρέπει να είναι ρητή και οι αντίστοιχες φόρμες πρέπει να είναι εύκολα κατανοητές χωρίς χρήση πολύπλοκης νομικής ορολογίας. Ο κανονισμός δίνει τη δυνατότητα στα άτομα να ελέγχουν τα προσωπικά τους δεδομένα, ενώ ταυτόχρονα καθιστά τους οργανισμούς που επεξεργάζονται τα δεδομένα αυτά υπεύθυνους για την ασφάλειά τους. Ένα κοινό πρόβλημα στο δημόσιο τομέα είναι ότι πολλά άτομα δεν κατέχουν ένα ψηφιακό αποτύπωμα, οπότε οι οργανισμοί πρέπει να είναι σε θέση να παρέχουν τη συγκατάθεσή τους τόσο σε έντυπη όσο και σε ηλεκτρονική μορφή. Η διαδικασία πρέπει να είναι εύκολα κατανοητή, απαλλαγμένη από ορολογία και χωρίς να απαιτεί γνώσεις υπολογιστή.

Ο κανονισμός GDPR μπορεί να θεωρηθεί ως μια ευκαιρία για να διαχωριστούν τα πολύτιμα δεδομένα από τις παρωχημένες ή λανθασμένες πληροφορίες, καθιστώντας ευκολότερη τη διατήρηση της ποιότητας των δεδομένων. Ο νέος κανονισμός εξουσιοδοτεί το υποκείμενο των δεδομένων και του δίνει τον έλεγχο των προσωπικών του δεδομένων. Δίνει έτσι την ευκαιρία στους ιδιώτες να διαχειρίζονται ποιες δικές τους πληροφορίες μοιράζονται, που και για ποιους σκοπούς.

Οι οργανισμοί του δημόσιου τομέα θα πρέπει να επικεντρωθούν στον σημαντικότερο παράγοντα, το υποκείμενο των δεδομένων, ενώ παράλληλα θα

πρέπει να χρησιμοποιήσουν την ευκαιρία αυτή για να «καθαρίσουν» τα δεδομένα τους, και να απαλλαγούν από τις περιττές πληροφορίες. Δεν υπάρχει αμφιβολία ότι αυτό είναι μια πρόκληση και οι δημόσιοι οργανισμοί θα πρέπει να εξετάσουν το ενδεχόμενο συνεργασίας με εξωτερικούς συνεργάτες, σε όποιο επίπεδο δεν μπορούν να ανταπεξέλθουν λόγω παρωχημένης τεχνολογίας, έλλειψη τεχνογνωσίας, ανεπαρκές προσωπικού, κτλ.

2.7 Εκπαίδευση του προσωπικού για τον κανονισμό GDPR

Μια πολύ σημαντική παράμετρος που δεν πρέπει να παραβλεφθεί, είναι η εκπαίδευση των υπαλλήλων ενός οργανισμού. Ακόμα και αν ένας οργανισμός διασφαλίσει τη συμμόρφωση των πολιτικών και των διαδικασιών του με τις διατάξεις του κανονισμού GDPR, ένα απλό λάθος από έναν υπάλληλο μπορεί να οδηγήσει σε παραβίαση της ασφάλειας των δεδομένων που επεξεργάζεται ο οργανισμός. Για αυτόν τον λόγο, είναι σημαντικό το προσωπικό του οργανισμού να κατανοεί τις απαιτήσεις και τις αλλαγές που εισάγει ο κανονισμός GDPR, καθώς οι αλλαγές αυτές ασφαλώς θα επηρεάσουν τον τρόπο που εκπληρώνουν τα καθημερινά τους καθήκοντα.

Υπάρχει ανάγκη για αλλαγή της κουλτούρας στους οργανισμούς όσον αφορά την ιδιωτικότητα των δεδομένων, όπου η ασφάλεια θα είναι η βασική προτεραιότητα.

Ο κανονισμός GDPR δεν διευκρινίζει τι οφείλει να περιλαμβάνει μια ολοκληρωμένη και επαρκής εκπαίδευση. Κατ’ αυτόν τον τρόπο, ο Υπεύθυνος Προστασίας Δεδομένων (DPO) του οργανισμού, επιφορτίζεται με την ευθύνη να ενημερώσει και να εκπαιδεύσει το προσωπικό που εμπλέκεται στις διαδικασίες επεξεργασίας δεδομένων, και να επιλέξει τις κατάλληλες μεθόδους και το κατάλληλο περιεχόμενο, με βάση τις ιδιαιτερότητες του κάθε οργανισμού.

Για τον σχεδιασμό και την επιτυχή διεξαγωγή αυτής της εκπαίδευσης, πρέπει να ληφθούν υπόψιν οι παρακάτω παράγοντες:

1. Προδιαγραφές, απαιτήσεις και ανάγκες του οργανισμού

Όπως είπαμε και λίγο παραπάνω, ο κανονισμός GDPR δεν ορίζει κάποιο συγκεκριμένο πλάνο για την εκπαίδευση των υπαλλήλων. Δεν υπάρχει μια ενιαία προσέγγιση για την κατάρτιση του προσωπικού. Κάθε οργανισμός πρέπει να διαμορφώσει το πρόγραμμά του σύμφωνα με διάφορους παράγοντες, από τους οποίους ο πρώτος που πρέπει να ληφθεί υπόψιν, είναι το μέγεθος του ίδιου του οργανισμού.

Μικρός αριθμός εργαζομένων, σημαίνει πως η εκπαίδευση μπορεί να γίνει με πολύ πρακτικούς όρους, και ο εκπαιδευτής μπορεί να παράσχει εξειδικευμένη βοήθεια σε μικρές ομάδες εργαζομένων, η ακόμα και σε κάθε εργαζόμενο ξεχωριστά. Παράλληλα όμως, μικρός αριθμός εργαζομένων μεταφράζεται συνήθως και σε λιγότερους διαθέσιμους πόρους. Οι μικροί οργανισμοί δεν μπορούν να στείλουν πολλά άτομα ταυτόχρονα για εκπαίδευση, καθώς αυτό πολύ πιθανό να μεταφράζεται σε παύση τουλάχιστον κάποιων εκ των δραστηριοτήτων του οργανισμού.

Για όλους αυτούς τους λόγους, η συνολική εκπαίδευση θα είναι επίσης ακριβότερη κατ’ άτομο σε μικρούς οργανισμούς απ’ ότι σε οργανισμούς που έχουν περισσότερο προσωπικό, γεγονός που τους δίνει την ευχέρεια να οργανώσουν μεγαλύτερες ομάδες εκπαίδευσης.

2. Παράγοντες που θα κρίνουν ένα επιτυχημένο πρόγραμμα εκπαίδευσης

Είναι σημαντικό να μπορεί ο οργανισμός να «μετρήσει» την επιτυχία του προγράμματος εκπαίδευσης που θέτει σε εφαρμογή. Με αυτόν τον τρόπο μπορεί να φανεί η ανάγκη για αλλαγές στο πρόγραμμα αυτό, με σκοπό την βελτίωση της αποτελεσματικότητάς του.

Για αυτόν τον λόγο είναι χρήσιμο να τεθούν μετρήσιμοι στόχοι, όπου αυτό είναι δυνατόν. Οι στόχοι αυτοί εξαρτώνται σε μεγάλο βαθμό από το είδος του οργανισμού, το μέγεθός του, τις δραστηριότητες του, τις υπηρεσίες που παρέχει, το επίπεδο των υπαλλήλων, κτλ. Κάποια παραδείγματα τέτοιων μετρήσιμων στόχων μπορεί να είναι η πτώση των συμβάντων ασφαλείας που

προκύπτουν από ανθρώπινο σφάλμα κατά τη διάρκεια ενός έτους, ή μηδενικές επιτυχημένες απάτες «ψαρέματος» δεδομένων.

Ιδανικά, για πιο αποτελεσματική μέτρηση της επιτυχίας του προγράμματος εκπαίδευσης, θα έπρεπε να υπάρχουν στοιχεία για τα επίπεδα των μεταβλητών αυτών από το διάστημα πριν από την εκπαίδευση, αλλά αυτό σημαίνει πως ο οργανισμός θα έπρεπε να παρακολουθεί αυτά τα στοιχεία από πριν. Οι περισσότεροι οργανισμοί δεν το κάνουν αυτό. Παρόλα αυτά, το πρόβλημα αυτό μπορεί να ξεπεραστεί αν οι στόχοι τεθούν αρχικά σε πιο βραχυπρόθεσμο επίπεδο, ώστε να μπορεί να εκτιμηθεί η βελτίωση που σημειώνεται μετά από ένα μήνα, μετά από δύο, ή τρεις μήνες, και στη συνέχεια να οριστούν μακροπρόθεσμοι στόχοι, με βάση τα δεδομένα αυτά.

3. Ενεργή συμμετοχή του προσωπικού

Μια συνήθης παγίδα στην οποία πέφτουν πολλοί οργανισμοί όταν σχεδιάζουν και υλοποιούν διάφορα προγράμματα εκπαίδευσης για το προσωπικό τους, είναι πως η εκπαίδευση καταλήγει απλά σε μια «παθητική ενημέρωση», όπου οι εργαζόμενοι συγκεντρώνονται σε μια αίθουσα και απλά ακούνε μια πολύωρη παρουσίαση. Η μέθοδος αυτή έχει αποδειχθεί πολλές φορές ως η πλέον αναποτελεσματική.

Αντί για αυτό, ο οργανισμός θα πρέπει να φροντίσει ώστε η εκπαίδευση να είναι μια συνεχής διαδικασία που αποτελεί μέρος της κουλτούρας του οργανισμού.

Η συμμετοχή του προσωπικού, με διάφορους τρόπους, είναι απαραίτητη για τη διαδικασία αυτή. Διαφορετικοί άνθρωποι μαθαίνουν με διαφορετικούς τρόπους. Για παράδειγμα, κάποιοι βοηθιούνται περισσότερο ακούγοντας μια διάλεξη, η διαβάζοντας μια μελέτη, ενώ άλλοι προτιμούν πιο διαδραστικές μεθόδους.

Για διασφάλιση μεγαλύτερων ποσοστών επιτυχίας, οι οργανισμοί πρέπει να χρησιμοποιούν όσο το δυνατόν περισσότερες από τις διαφορετικές αυτές προσεγγίσεις:

- σεμινάρια,
- διαλέξεις και παρουσιάσεις,

- μαθήματα ηλεκτρονικής μάθησης,
- ηλεκτρονικά τεστ «γνώσεων»,
- ενημερωτικά μηνύματα ηλεκτρονικού ταχυδρομείου,
- αφίσες με βασικές πληροφορίες στον εργασιακό χώρο, κτλ.

4. Εστίαση στη πράξη και όχι στην θεωρητική γνώση

Ακόμα και αν οι εργαζόμενοι καταφέρουν να εξεταστούν με επιτυχία σε μια θεωρητική εξέταση, αυτό δεν εξασφαλίζει απαραίτητα ότι θα μπορέσουν να ενεργήσουν σωστά και στην πράξη. Ένα ενδεικτικό παράδειγμα είναι το ηλεκτρονικό ψάρεμα. Οι περισσότεροι άνθρωποι κατά τη διάρκεια μιας θεωρητικής εξέτασης, μπορούν να αναγνωρίσουν «ύποπτα» μηνύματα ηλεκτρονικού ταχυδρομείου, αλλά στην καθημερινότητά τους, όταν βρίσκονται στο γραφείο τους, ενδέχεται να κάνουν κλικ σε κάποιον κακόβουλο σύνδεσμο, είτε από κεκτημένη ταχύτητα, είτε από αμέλεια.

Για να γεφυρωθεί το χάσμα ανάμεσα στη θεωρητική γνώση και στην πράξη, τα σενάρια που χρησιμοποιούνται κατά την εκπαίδευση θα πρέπει να είναι όσο το δυνατόν πιο αληθοφανή και ρεαλιστικά.

Για παράδειγμα, ένας καλός τρόπος για να εκτιμηθεί η ετοιμότητα του προσωπικού να εντοπίζει ηλεκτρονικά μηνύματα ηλεκτρονικού ψαρέματος, είναι η διεξαγωγή μιας προσομοίωσης «επίθεσης», σε ανύποπτο χρόνο.

5. Επιλογή της κατάλληλης χρονικής στιγμής για την έναρξη της εκπαίδευσης

Η εκπαίδευση του προσωπικού απαιτεί χρόνο, αν ο στόχος είναι η μέγιστη αποτελεσματικότητα. Είναι σημαντικό να δοθεί προτεραιότητα στον προσεκτικό σχεδιασμό του προγράμματος εκπαίδευσης και του εκπαιδευτικού υλικού, με βάση τις ιδιαίτερες ανάγκες και απαιτήσεις του οργανισμού, ακόμα και αν αυτό σημαίνει πως η έναρξη του προγράμματος θα καθυστερήσει.

Ή διεξαγωγή ενός «έτοιμου» προγράμματος βιαστικά, χωρίς να ληφθούν υπόψιν οι ιδιαιτερότητες του οργανισμού, δεν θα ωφελήσει τον οργανισμό μακροπρόθεσμα.

6. Ερμηνεία των αποτελεσμάτων

Όσον αφορά στην ερμηνεία των αποτελεσμάτων ενός εκπαιδευτικού κύκλου, χρειάζεται υπομονή, καθώς κανένα πρόγραμμα εκπαίδευσης δεν θα επιφέρει δραστικές αλλαγές εν μία νυκτί. Ειδικά όσον αφορά υπαλλήλους μεγαλύτερης ηλικίας που κάνουν παρόμοια δουλειά για αρκετά χρόνια, οι συνήθειες χρόνων δεν θα διορθωθούν αμέσως μετά από ένα σεμινάριο.

Είναι σημαντικό ο οργανισμός και οι εργαζόμενοι να δείξουν εμπιστοσύνη στη διαδικασία, και να συνεχιστούν οι προσπάθειες βελτίωσης μέσω συνεχούς εκπαίδευσης ακόμη και αν τα άμεσα αποτελέσματα είναι αμελητέα. Το προσωπικό σταδιακά θα αρχίσει να εξοικειώνεται με τον νέο τρόπο σκέψης και αντιμετώπισης των καθημερινών του καθηκόντων, και με την πάροδο του χρόνου θα αποκτάει όλο και περισσότερη εμπειρία.

2.8 Σύνοψη

Συνοψίζοντας, οι οργανισμοί του δημοσίου τομέα οφείλουν και αυτοί να συμμορφωθούν με τον κανονισμό GDPR, κάτι το οποίο αναφέρεται ρητά στο κείμενο του κανονισμού. Παρόλα αυτά ο κανονισμός αναγνωρίζει τις ιδιαιτερότητες των δημόσιων οργανισμών, και σε αυτήν την κατεύθυνση επιτρέπει την απόκλιση από κάποιες βασικές αρχές του κανονισμού, υπό συγκεκριμένες προϋποθέσεις. Για παράδειγμα, το δικαίωμα του Υποκειμένου των Δεδομένων στη Λήθη, δεν ισχύει στην περίπτωση που μια τέτοια διαγραφή δεδομένων εμποδίζει την εκπλήρωση ενός έργου που εκτελείται για το δημόσιο συμφέρον.

Οι οργανισμοί του δημοσίου τομέα έρχονται επίσης αντιμέτωποι με ιδιαίτερες προκλήσεις, στην προσπάθεια για συμμόρφωση με τον κανονισμό GDPR. Τέτοιες προκλήσεις προκύπτουν κυρίως από τον όγκο των δεδομένων που αναγκάζονται να διατηρούν, την γραφειοκρατία που πολλές φορές οδηγεί σε παρωχημένα και ανακριβή δεδομένα, την έλλειψη προσωπικού σε αρκετές περιπτώσεις, αλλά και το γεγονός ότι πολλοί οργανισμοί λόγω της φύσης τους, αναγκάζονται να διαχειρίζονται ευαίσθητα προσωπικά δεδομένα, δεδομένα ευπαθών ομάδων, κτλ.

Κεφάλαιο 3 – Το GDPR οδηγεί σε αλλαγές στα συστήματα ηλεκτρονικής διακυβέρνησης του δημοσίου τομέα

3.1 Εισαγωγή

Στο προηγούμενο κεφάλαιο αναλύθηκε το πως ο κανονισμός GDPR επηρεάζει τους δημόσιους οργανισμούς. Στη συνέχεια η ανάλυση αυτή γίνεται πιο συγκεκριμένη και επικεντρώνεται στα συστήματα ηλεκτρονικής διακυβέρνησης που χρησιμοποιούνται από τους δημόσιους οργανισμούς στα πλαίσια των δραστηριοτήτων τους και στις αλλαγές που οφείλουν να υλοποιηθούν κατά την προσπάθεια συμμόρφωσης με τον κανονισμό.

3.2 Αλλαγές στις λειτουργίες των online eGoverment συστημάτων

Σε αυτό το κεφάλαιο θα αναλύσουμε κάποιες από τις πιο κοινές λειτουργίες που οφείλει να αναλύσει και κατ’ επέκταση να τροποποιήσει, κάθε δημόσιος οργανισμός που κάνει χρήση συστημάτων ηλεκτρονικής διακυβέρνησης.

3.2.1 Λειτουργίες ηλεκτρονικής εγγραφής

Όπως υποδηλώνει το όνομα, η διαδικασία εγγραφής είναι μια διαδικασία που κάθε χρήστης οφείλει να ολοκληρώσει προκειμένου να κάνει χρήση οποιουδήποτε ηλεκτρονικού συστήματος, πόσο μάλλον συστήματος ηλεκτρονικής διακυβέρνησης.

Τα προσωπικά δεδομένα που ζητούνται από τον χρήστη κατά τη διαδικασία εγγραφής, μπορούν να διαφέρουν ανάλογα με τον σκοπό του εκάστοτε συστήματος ηλεκτρονικής διακυβέρνησης. Ωστόσο, πάντα είναι απαραίτητη μια διεύθυνση ηλεκτρονικού ταχυδρομείου, κατ’ ελάχιστο. Για την πλειοψηφία των συστημάτων ηλεκτρονικής διακυβέρνησης όμως, είναι απαραίτητα αρκετά περισσότερα στοιχεία, όπως το νόμιμο όνομα και επώνυμο, το φύλο, φορολογικά στοιχεία όπως το ΑΦΜ, αριθμός ταυτότητας ΄η/και διαβατηρίου, κτλ. Σε κάποιες ακραίες περιπτώσεις μπορεί να είναι απαραίτητα ακόμα και ευαίσθητα προσωπικά δεδομένα όπως για παράδειγμα ιατρικά δεδομένα κτλ.

Με βάση τα όσα αναλύθηκαν στα προηγούμενα κεφάλαια, προσωπικά δεδομένα είναι όλες οι πληροφορίες σχετικά με ένα προσδιορισμένο ή αναγνωρίσιμο φυσικό πρόσωπο. Όπως το όνομα, αλλά και διεύθυνση ηλεκτρονικού ταχυδρομείου, διεύθυνση IP ή αναγνωριστικό cookie. Αξίζει να σημειωθεί επίσης, πως ακόμα και οι ψευδοποιημένες πληροφορίες, θεωρούνται επίσης προσωπικά δεδομένα, διότι εξακολουθεί να είναι δυνατή η αναγνώριση ενός συγκεκριμένου προσώπου (ακόμη και αν χρειάζεται να συνδυαστούν πολλαπλές βάσεις δεδομένων από διάφορα μέρη για να αναγνωριστεί).

Ο κανονισμός GDPR καθιστά σαφές, πως για οποιαδήποτε επεξεργασία προσωπικών δεδομένων, είναι απαραίτητο το υποκείμενο των δεδομένων να έχει δώσει την ρητή συγκατάθεσή του, καθώς επίσης και να έχει τη δυνατότητα ανά πάσα στιγμή να αποσύρει αυτήν του την συγκατάθεση.

Η έγκυρη συγκατάθεση βάσει του κανονισμού GDPR πρέπει να είναι μια "ελεύθερη, συγκεκριμένη, ενημερωμένη και αδιαμφισβήτητη έκφραση θέλησης". Αυτό σημαίνει ότι:

1. η χορήγηση της συγκατάθεσης πρέπει να είναι μια σαφής ενεργή ενέργεια (για παράδειγμα η επιλογή συγκεκριμένης επιλογής σε ηλεκτρονικό πεδίο),
2. το υποκείμενο των δεδομένων δεν μπορεί να εξαναγκαστεί στην επιλογή αυτή (για παράδειγμα μέσω προεπιλογής),
3. η επιλογή που παρέχεται στο υποκείμενο των δεδομένων πρέπει να είναι σαφώς ορισμένη, ώστε οι χρήστες να γνωρίζουν ακριβώς σε τι δίνουν την συγκατάθεση τους,
4. το υποκείμενο των δεδομένων πρέπει να έχει επαρκείς πληροφορίες σχετικά με το πως θα χρησιμοποιηθούν τα προσωπικά του δεδομένα.

Για να ικανοποιούνται όλες οι παραπάνω οδηγίες που υπαγορεύει ο κανονισμός GDPR, οι δημόσιοι οργανισμοί οφείλουν να αναλύσουν την διεργασία της ηλεκτρονικής εγγραφής στα ηλεκτρονικά συστήματα ηλεκτρονικής διακυβέρνησης, και να υλοποιήσουν στοχευμένες αλλαγές. Τα βασικά στοιχεία αυτών των αλλαγών αναλύονται παρακάτω:

1. Όταν ένας μη-εγγεγραμμένος χρήστης της εφαρμογής, επιλέξει να ξεκινήσει τη διαδικασία ηλεκτρονικής εγγραφής, τότε πριν καν το σύστημα παρουσιάσει την φόρμα εγγραφής, θα πρέπει να ανακατευθύνει τον χρήστη σε μία καινούρια σελίδα «Πολιτική Δεδομένων». Η σελίδα αυτή θα πρέπει να περιγράφει με σαφήνεια την πολιτική που ακολουθείται ως προς τα προσωπικά δεδομένα και τη χρήση τους, και όλες τις απαραίτητες πληροφορίες που πρέπει να γνωρίζει ο χρήστης προκειμένου να μπορεί να αποφασίσει αν επιθυμεί να δώσει την συγκατάθεση του για την χρήση των προσωπικών δεδομένων του, από τη συγκεκριμένη υπηρεσία. Στο τέλος της σελίδας αυτής πρέπει να είναι διαθέσιμες δυο σαφείς επιλογές, «Αποδέχομαι» και «Δεν αποδέχομαι». Σε περίπτωση που τα δεδομένα πρόκειται να χρησιμοποιηθούν με περισσότερους από έναν τρόπους, η για περισσότερους από έναν σκοπούς, τότε οι επιλογές «Αποδέχομαι» και «Δεν αποδέχομαι» πρέπει να υπάρχουν ξεχωριστά για κάθε διαφορετική περίπτωση, επιτρέποντας στον χρήστη να επιλέξει κατά περίπτωση.
2. Όταν ο χρήστης πατήσει την επιλογή «Αποδέχομαι» για κάθε διαφορετικό σκοπό που αναφέρεται στη σελίδα, τότε το σύστημα απλά θα τον ανακατευθύνει στην σελίδα εγγραφής, όπου και θα μπορέσει να συνεχίσει κανονικά με την ηλεκτρονική του εγγραφή. Με την ολοκλήρωση της διαδικασίας ηλεκτρονικής εγγραφής, το σύστημα θα πρέπει να καταχωρεί την ημερομηνία και ώρα όπου ο χρήστης έδωσε τη συγκατάθεσή του.
3. Όταν ο χρήστης πατήσει την επιλογή «Δεν αποδέχομαι» για κάποιον από τους σκοπούς που περιγράφονται, σε περίπτωση που είναι δυνατή η λειτουργία του ηλεκτρονικού συστήματος χωρίς την χρήση των δεδομένων με αυτό τον τρόπο, τότε η επιλογή του χρήστη θα γίνει σεβαστή και θα του επιτραπεί η εγγραφή στο σύστημα. Θα πρέπει να εμφανίζεται ένα μήνυμα που θα καθιστά σαφές στον χρήστη ακριβώς ποιες λειτουργίες δε θα είναι διαθέσιμες, σε περίπτωση που δεν δώσει την συγκατάθεση του για αυτόν το σκοπό. Με την αποδοχή του χρήστη στον περιορισμό αυτό, το σύστημα θα ανακατευθύνει τον χρήστη στην σελίδα εγγραφής, όπου και θα μπορέσει να συνεχίσει κανονικά με την ηλεκτρονική του εγγραφή. Με την ολοκλήρωση της διαδικασίας

ηλεκτρονικής εγγραφής, το σύστημα θα πρέπει να καταχωρεί ακριβώς για ποιους σκοπούς ο χρήστης έδωσε τη συγκατάθεσή του και για ποιους δεν την έδωσε, καθώς και θα καταγράφει την ημερομηνία και ώρα.

4. Όταν ο χρήστης πατήσει την επιλογή «Δεν αποδέχομαι» για κάποιον από τους σκοπούς που περιγράφονται, αλλά δεν είναι δυνατή η λειτουργία του ηλεκτρονικού συστήματος χωρίς την χρήση των δεδομένων με αυτό τον τρόπο, τότε ο χρήστης δεν ανακατευθύνεται στην σελίδα εγγραφής. Θα πρέπει να εμφανίζεται ένα μήνυμα που θα καθιστά σαφές στον χρήστη ότι το σύστημα δεν μπορεί να λειτουργήσει χωρίς τη συγκατάθεσή του στην συγκεκριμένη χρήση των δεδομένων του, και δεν θα του επιτρέπεται να συνεχίσει με την διαδικασία της εγγραφής.

3.2.2 Διαγραφή/ ανωνυμοποίηση λογαριασμού χρήστη

Μια εξίσου πολύ σημαντική πτυχή της συγκατάθεσης σύμφωνα με τον κανονισμό GDPR, είναι ότι το υποκείμενο των δεδομένων θα πρέπει να έχει τη δυνατότητα να ανακαλέσει την συγκατάθεση που έχει δώσει για την χρήση των δεδομένων του, ανά πάσα στιγμή. Η διαδικασία ανάκλησης της συγκατάθεσης πρέπει να είναι εξίσου εύκολη με την παροχή της.

Η ανάκληση της συγκατάθεσης του χρήστη στην χρήση των δεδομένων του σύμφωνα με την πολιτική δεδομένων του συστήματος, θα πρέπει να μπορεί να γίνει ανά πάσα στιγμή. Η επιλογή αυτή πρέπει να είναι εύκολα προσβάσιμη στο ηλεκτρονικό προφίλ του κάθε χρήστη, και θα πρέπει η διαδικασία να είναι σαφής και κατανοητή.

Όταν ο χρήστης επιλέξει να ανακαλέσει την συγκατάθεσή του για κάποιον από τους σκοπούς του συστήματος, σε περίπτωση που είναι δυνατή η λειτουργία του ηλεκτρονικού συστήματος χωρίς την χρήση των δεδομένων με αυτό τον τρόπο, τότε η επιλογή του χρήστη θα γίνει σεβαστή. Θα πρέπει να παρουσιάζεται ένα μήνυμα που θα καθιστά σαφές στον χρήστη ακριβώς ποιες λειτουργίες δε θα είναι διαθέσιμες, σε περίπτωση που ανακαλέσει την συγκατάθεση του για αυτόν το σκοπό. Με την αποδοχή του χρήστη στον περιορισμό αυτό, το σύστημα θα αποθηκεύει τις καινούριες προτιμήσεις του

χρήστη, και ο χρήστης θα μπορεί να συνεχίσει την χρήση του συστήματος, με τις καινούριες συνθήκες που προκύπτουν από την ανάκληση αυτής της συγκατάθεσης.

Στην περίπτωση όμως που ο χρήστης επιλέξει να ανακαλέσει την συγκατάθεσή του για κάποιον από τους σκοπούς του συστήματος, αλλά δεν είναι δυνατή η λειτουργία του ηλεκτρονικού συστήματος χωρίς την χρήση των δεδομένων με αυτό τον τρόπο, θα πρέπει το σύστημα να παρουσιάζει ένα μήνυμα που θα καθιστά σαφές στον χρήστη ότι το σύστημα δεν μπορεί να λειτουργήσει χωρίς τη συγκατάθεσή του, και θα του δίνει την επιλογή να ζητήσει τη διαγραφή του λογαριασμού του.

3.2.2.1 Παράγοντες που εμποδίζουν/ απαγορεύουν την πλήρη διαγραφή

Σε αυτό το σημείο πρέπει να σημειωθεί πως στα ηλεκτρονικά συστήματα, δεν είναι πάντα εφικτή η πλήρης διαγραφή ενός λογαριασμού χρήστη σε φυσικό επίπεδο, καθώς μπορεί να μην επιτρέπεται σε επίπεδο βάσης δεδομένων, προκειμένου να διατηρηθεί η ακεραιότητα της βάσης δεδομένων αλλά και των δεδομένων αυτών καθ’ εαυτών. Ιδιαίτερα αν ο χρήστης έχει ήδη προβεί σε διάφορες ενέργειες στο σύστημα, η φυσική διαγραφή του πιθανό να μην είναι δυνατή. Αντίθετα, στην περίπτωση που ο χρήστης δεν έχει συμμετάσχει ενεργά, τότε κατά πάσα πιθανότητα η φυσική διαγραφή του λογαριασμού είναι εφικτή.

Παράλληλα, και ιδιαιτέρως για τα συστήματα ηλεκτρονικής διακυβέρνησης, πιθανώς να υπάρχει νομική υποχρέωση για την διατήρηση της συνέχειας των δεδομένων. Σύμφωνα με τον κανονισμό GDPR, οι οργανισμοί δεν έχουν την υποχρέωση να το διαγράψουν προσωπικά δεδομένα μετά από αίτημα του υποκειμένου των δεδομένων, στις ακόλουθες περιπτώσεις:

1. τα προσωπικά δεδομένα που κατέχει ο οργανισμός, είναι απαραίτητα για την άσκηση του δικαιώματος της ελευθερίας έκφρασης.
2. υπάρχει νομική υποχρέωση να διατηρούνται αυτά τα δεδομένα.
3. για λόγους δημόσιου συμφέροντος (για παράδειγμα σκοπούς δημόσιας υγείας, επιστημονικής, στατιστικής ή ιστορικής έρευνας).

Ανάλογα με τον σκοπό και τη φύση του ηλεκτρονικού συστήματος, ένα η παραπάνω από τα κριτήρια αυτά μπορεί να δίνουν την ευχέρεια στον οργανισμό να αρνηθεί την διαγραφή του λογαριασμού, εξ ολοκλήρου, ή εν μέρει. Σε αυτή την περίπτωση, το σύστημα θα πρέπει να ενημερώνει τον χρήστη που αιτείται την διαγραφή των δεδομένων του, για τους λόγους που αυτό το αίτημα δεν μπορεί να ικανοποιηθεί. Η εξήγηση αυτή θα πρέπει να είναι άμεση, σαφής και κατανοητή.

3.2.2.2 Ανωνυμοποίηση

Σε κάποιες περιπτώσεις, ενώ η φυσική διαγραφή των δεδομένων δεν είναι δυνατή, παρόλα αυτά δεν είναι απαραίτητη η διατήρηση της ταυτότητας του χρήστη. Σε αυτές τις περιπτώσεις, θα πρέπει να υποστηρίζεται η ανωνυμοποίηση του λογαριασμού.

Η ανωνυμοποίηση είναι ένα πολύτιμο εργαλείο που επιτρέπει την κοινή χρήση των δεδομένων, διατηρώντας παράλληλα την ιδιωτικότητα. Η διαδικασία ανωνυμοποίησης δεδομένων απαιτεί την αλλαγή των αναγνωριστικών με κάποιο τρόπο, όπως η αφαίρεση, υποκατάσταση, παραμόρφωση, γενίκευση ή συσσωμάτωση.

Ο κανονισμός GDPR αναφέρεται συγκεκριμένα στις ανώνυμες πληροφορίες και τις διαχωρίζει από τις ψευδωνυμοποιημένες:

> *“(26) Οι αρχές της προστασίας δεδομένων θα πρέπει να εφαρμόζονται σε κάθε πληροφορία η οποία αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο. Τα δεδομένα προσωπικού χαρακτήρα που έχουν υποστεί ψευδωνυμοποίηση, η οποία θα μπορούσε να αποδοθεί σε φυσικό πρόσωπο με τη χρήση συμπληρωματικών πληροφοριών, θα πρέπει να θεωρούνται πληροφορίες σχετικά με ταυτοποιήσιμο φυσικό πρόσωπο. Για να κριθεί κατά πόσον ένα φυσικό πρόσωπο είναι ταυτοποιήσιμο, θα πρέπει να λαμβάνονται υπόψη όλα τα μέσα τα οποία είναι ευλόγως πιθανό ότι θα χρησιμοποιηθούν, όπως για παράδειγμα ο διαχωρισμός του, είτε από τον υπεύθυνο επεξεργασίας είτε από τρίτο για την άμεση ή έμμεση εξακρίβωση*

της ταυτότητας του φυσικού προσώπου. Για να διαπιστωθεί κατά πόσον κάποια μέσα είναι ευλόγως πιθανό ότι θα χρησιμοποιηθούν για την εξακρίβωση της ταυτότητας του φυσικού προσώπου, θα πρέπει να λαμβάνονται υπόψη όλοι οι αντικειμενικοί παράγοντες, όπως τα έξοδα και ο χρόνος που απαιτούνται για την ταυτοποίηση, λαμβανομένων υπόψη της τεχνολογίας που είναι διαθέσιμη κατά τον χρόνο της επεξεργασίας και των εξελίξεων της τεχνολογίας. Οι αρχές της προστασίας δεδομένων δεν θα πρέπει συνεπώς να εφαρμόζονται σε ανώνυμες πληροφορίες, δηλαδή πληροφορίες που δεν σχετίζονται προς ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο ή σε δεδομένα προσωπικού χαρακτήρα που έχουν καταστεί ανώνυμα κατά τρόπο ώστε η ταυτότητα του υποκειμένου των δεδομένων να μην μπορεί ή να μην μπορεί πλέον να εξακριβωθεί. Ο παρών κανονισμός δεν αφορά συνεπώς την επεξεργασία τέτοιων ανώνυμων πληροφοριών, ούτε μεταξύ άλλων για στατιστικούς ή ερευνητικούς σκοπούς. "

Πηγή: https://publications.europa.eu/el/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1

Η ανωνυμοποίηση λοιπόν είναι η διαδικασία της κατάργησης των προσωπικών αναγνωριστικών, τόσο των άμεσων όσο και των έμμεσων, που είναι ικανά να οδηγήσουν στην αναγνώριση ενός ατόμου. Ένα άτομο μπορεί να αναγνωριστεί άμεσα από προσωπικά δεδομένα όπως το όνομα, η διεύθυνση, το ΑΦΜ, ο αριθμός ταυτότητας, ο ταχυδρομικός κώδικας, ο αριθμός τηλεφώνου, η φωτογραφία ή κάποιο άλλο μοναδικό προσωπικό χαρακτηριστικό.

Επίσης, ένα άτομο μπορεί να είναι έμμεσα αναγνωρίσιμο όταν ορισμένες πληροφορίες συνδέονται μαζί με άλλες πηγές πληροφοριών, συμπεριλαμβανομένου του τόπου εργασίας, του τίτλου εργασίας, του μισθού, του ταχυδρομικού κώδικα ή ακόμη και του γεγονότος ότι έχουν συγκεκριμένη διάγνωση ή κατάσταση.

Μόλις τα δεδομένα είναι πραγματικά ανώνυμα και τα άτομα δεν είναι πλέον αναγνωρίσιμα, τα δεδομένα δεν εμπίπτουν πλέον στο πεδίο εφαρμογής του GDPR, καθώς οι διατάξεις του κανονισμού GDPR δεν ισχύουν για τις ανωνυμοποιημένες πληροφορίες. Οπότε μπορεί να συνεχιστεί απρόσκοπτα η επεξεργασία των ανωνυμοποιημένων αυτών δεδομένων.

Ο οργανισμός οφείλει να αναλύσει τις απαιτήσεις του ηλεκτρονικού συστήματος, αλλά και τις λειτουργικές και νομικές απαιτήσεις της παρεχόμενης υπηρεσίας, και να αποφασίσει ποιες πληροφορίες πρέπει να διατηρηθούν για να είναι χρήσιμα τα δεδομένα και ποιες μπορούν να αλλάξουν κατά τη διαδικασία της ανωνυμοποίησης. Η αφαίρεση βασικών μεταβλητών, η εφαρμογή ψευδωνύμων, η γενίκευση και η αφαίρεση των πληροφοριών πλαισίου από τα αρχεία κειμένου και η σύγχυση των δεδομένων εικόνας ή βίντεο θα μπορούσαν να οδηγήσουν σε απώλεια σημαντικών λεπτομερειών ή σε εσφαλμένα συμπεράσματα.

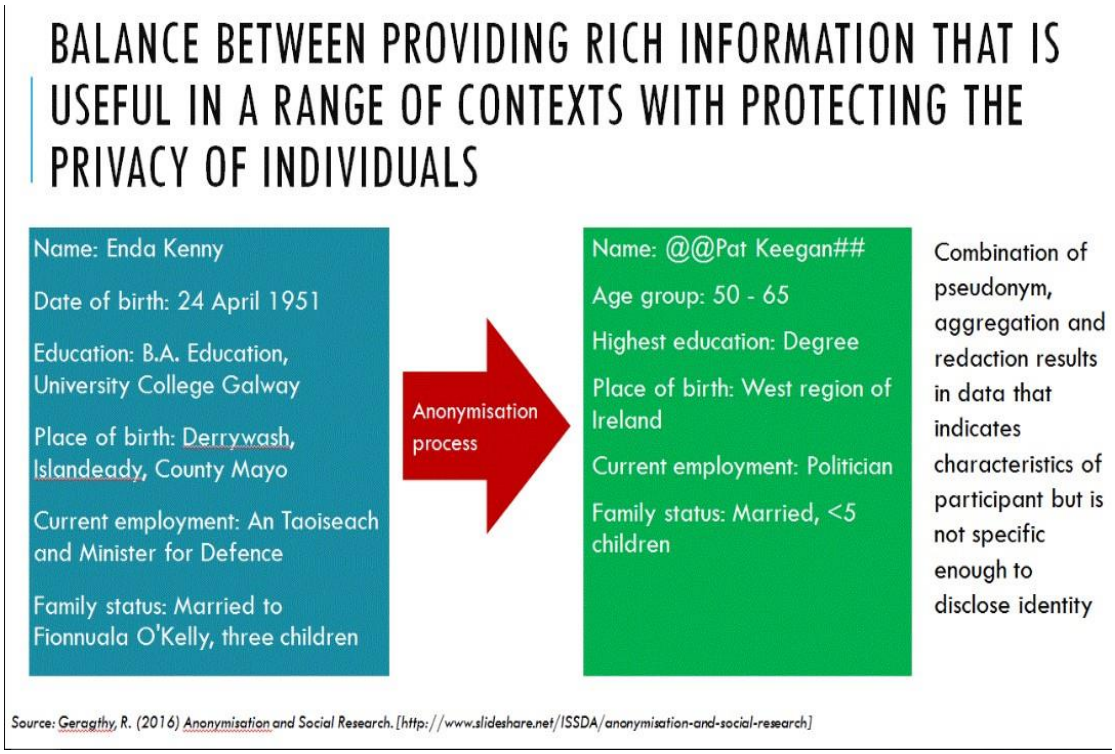
Η διαδικασία ανωνυμοποίησης συνήθως περιλαμβάνει την αφαίρεση ή τη συσσωμάτωση των μεταβλητών ή τη μείωση της ακρίβειάς τους.

Οι συνηθέστερες τεχνικές ανωνυμοποίησης είναι οι παρακάτω:

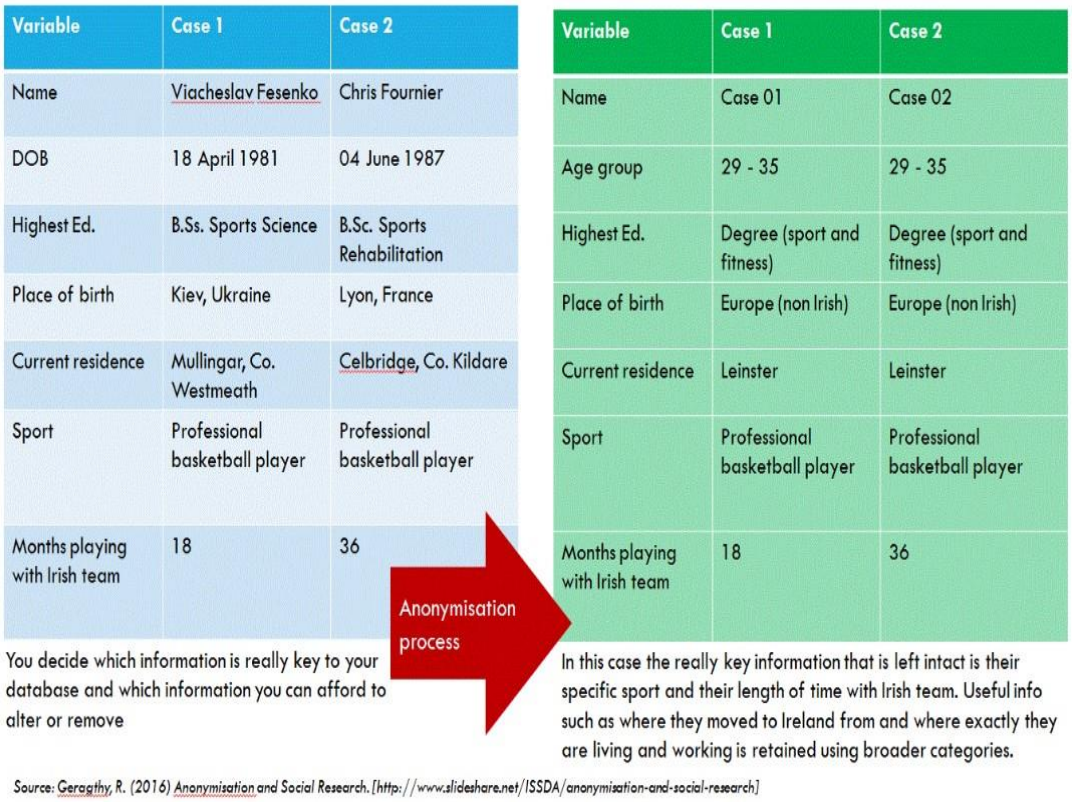
1. Αφαίρεση των άμεσων αναγνωριστικών από το σύνολο δεδομένων. Για παράδειγμα, κατάργηση εντελώς του ονόματος, η αντικατάσταση του από έναν τυχαία δημιουργημένο κωδικό.
2. Μείωση της ακρίβειας μιας μεταβλητής όπως η ηλικία ή ο τόπος διαμονής. Κατά γενικό κανόνα, συνηθίζεται να κρατείται το χαμηλότερο δυνατό επίπεδο γεωαναφοράς το οποίο δεν προδίδει την ταυτότητα του υποκειμένου των δεδομένων. Η ακριβής κλίμακα εξαρτάται από τον τύπο των δεδομένων που συλλέγονται, αλλά πολύ λεπτομερείς γεωαναφορές, όπως πλήρεις ταχυδρομικοί κώδικες, ονόματα μικρών πόλεων ή χωριών είναι πιθανόν να είναι προβληματικές. Οι κωδικοποιημένες ή κατηγορικές μεταβλητές μπορούν να συγκεντρωθούν σε ευρύτερους κώδικες. Εάν η συσσωμάτωση μίας μεταβλητής δεν είναι δυνατή, αξίζει να εξεταστεί το ενδεχόμενο να πρέπει να αφαιρεθεί εντελώς από το σύνολο των δεδομένων. Για

παράδειγμα: αντί για την πλήρη ημερομηνία γέννησης μπορεί να διατηρηθεί μόνο το έτος γέννησης, η ακόμα και ένα εύρος ετών, αντί για τον πλήρη ταχυδρομικό κωδικό, μπορεί να διατηρηθεί ο ευρύτερος τομέας (όπως τα 3 πρώτα ψηφία), κτλ.

Παρακάτω παρατίθενται δύο παραδείγματα ανωνυμοποιημένων δεδομένων, που όμως διατηρούν την αξία χρήσης τους:



Εικόνα 4 *Ανωνυμοποίηση Δεδομένων - Παράδειγμα 1*



Εικόνα 5 *Ανωνυμοποίηση Δεδομένων - Παράδειγμα 2*

3.2.2.3 Αλλαγή πολιτικής δεδομένων

Εκτός από την αυθόρμητη ενέργεια του χρήστη να ανακαλέσει την συγκατάθεση του ή/και να αιτηθεί την πλήρη διαγραφή του λογαριασμού του, η επιλογή αυτή πρέπει να παρέχεται και από το σύστημα στην περίπτωση που υπάρξουν αλλαγές στην υπάρχουσα πολιτική δεδομένων, όπως περιγράφεται παρακάτω.

1. Σε περίπτωση που ο τρόπος χρήσης των δεδομένων των χρηστών του συστήματος αλλάξει, τότε θα πρέπει να γίνει ενημέρωση της σελίδας «Πολιτική Δεδομένων». Αυτό συνεπάγεται πως όλοι οι ήδη εγγεγραμμένοι χρήστες του συστήματος θα πρέπει να δώσουν ξανά την συγκατάθεσή τους στην νέα αυτή πολιτική δεδομένων. Οι διαχειριστές του συστήματος θα πρέπει να μπορούν να ξεκινήσουν την διαδικασία αυτή.
2. Σε περίπτωση αλλαγής της πολιτικής δεδομένων, το σύστημα θα παρουσιάζει την ενημερωμένη αυτή σελίδα σε κάθε χρήστη, την επόμενη

φορά που αυτός θα συνδεθεί στο σύστημα. Η σελίδα αυτή θα λειτουργεί με τον τρόπο που περιεγράφηκε παραπάνω.

3. Σε περίπτωση που ο χρήστης αποδεχθεί την καινούρια πολιτική δεδομένων, η συγκατάθεση του θα καταγράφεται, και το σύστημα θα τον ανακατευθύνει στην κεντρική σελίδα του συστήματος.
4. Σε περίπτωση που ο χρήστης δεν αποδεχθεί την καινούρια πολιτική δεδομένων, θα πρέπει να ανακατευθύνεται σε μια σελίδα που να εξηγεί πως το σύστημα δεν μπορεί να λειτουργήσει χωρίς τη συγκατάθεσή του και κατ' επέκταση δεν μπορεί να του επιτραπεί να παραμείνει συνδεδεμένος. Παράλληλα θα πρέπει το σύστημα να δίνει την επιλογή στον χρήστη να διαγράψει τον λογαριασμό του.
5. Αν ο χρήστης δεν επιλέξει τη διαγραφή του λογαριασμού του, τότε το σύστημα θα τον αποσυνδέει και θα τον ανακατευθύνει στην κεντρική δημόσια σελίδα του συστήματος. Η σελίδα με την ανανεωμένη πολιτική δεδομένων, θα παρουσιαστεί ξανά την επόμενη φορά που ο χρήστης θα συνδεθεί στο σύστημα.
6. Όταν ο χρήστης επιλέξει να διαγράψει τον λογαριασμό του, το σύστημα θα πρέπει να παρουσιάζει ένα μήνυμα που θα περιγράφει με σαφήνεια τις συνέπειες της επιλογής αυτής, και να ζητάει από τον χρήστη να επιβεβαιώσει την επιλογή του αυτή. Με την επιβεβαίωση αυτή του χρήστη, το σύστημα θα τον αποσυνδέει, και αν είναι τεχνικά δυνατόν θα διαγράφει εντελώς τον λογαριασμό του, αλλιώς θα τον ανωνυμοποιεί. Αν ο χρήστης δεν επιβεβαιώσει την διαγραφή του λογαριασμού, τότε το σύστημα θα τον αποσυνδέει και θα τον ανακατευθύνει στην κεντρική δημόσια σελίδα του συστήματος. Ο λογαριασμός του χρήστη δε θα διαγράφεται και η σελίδα με την ανανεωμένη πολιτική δεδομένων, θα παρουσιαστεί ξανά την επόμενη φορά που ο χρήστης θα συνδεθεί στο σύστημα.

3.2.3 Μηχανές αναζήτησης

Μία ακόμα αρκετά κοινή λειτουργία των περισσότερων συστημάτων ηλεκτρονικής διακυβέρνησης, που επηρεάζεται από τον κανονισμό GDPR,

είναι οι μηχανές αναζήτησης εντός του συστήματος, οι οποίες επιτρέπουν την αναζήτηση χρηστών.

Για την καλύτερη προστασία της ιδιωτικότητας των χρηστών, οι εντός συστήματος μηχανές αναζήτησης θα πρέπει να μην επιστρέφουν ποτέ σαν αποτέλεσμα όλους τους χρήστες του συστήματος. Επίσης, δεν θα πρέπει να επιτρέπουν την αναζήτηση χρηστών χωρίς συγκεκριμένα κριτήρια αναζήτησης. Αυτό κρίνεται απαραίτητο ώστε να διασφαλίσει πως η αναζήτηση μπορεί να γίνει μόνο αν ο χρήστης που την εκτελεί γνωρίζει ήδη κάποιο κριτήριο με το οποίο ψάχνει, και δεν μπορεί να εκμεταλλευτεί την λειτουργία αναζήτησης που παρέχεται από το σύστημα με σκοπό να «ψαρέψει» πληροφορίες για άλλους χρήστες του συστήματος.

Παράλληλα, ο οργανισμός θα πρέπει να εξετάσει τη σχετικότητα των πληροφοριών που δίνονται για κάθε χρήστη, στα αποτελέσματα της αναζήτησης. Είναι απαραίτητο, οι πληροφορίες που δίνονται να είναι οι ελάχιστες δυνατές ώστε να ικανοποιούνται οι λειτουργικές και οργανικές απαιτήσεις της λειτουργίας αυτής. Για παράδειγμα, μια λειτουργία αναζήτησης που έχει ως σκοπό την αναζήτηση χρηστών που έχουν δηλώσει συμμετοχή σε έναν ηλεκτρονικό διαγωνισμό, ώστε να τους αποσταλούν κάποιες διευκρινήσεις, δεν χρειάζεται να περιλαμβάνει την φυσική διεύθυνση του χρήστη, ή την ηλικία και το φύλο του.

3.2.4 Διαχείριση αρχείου καταγραφής δραστηριότητας

Όπως αναφέρθηκε και παραπάνω, ο κανονισμός GDPR ορίζει πως το υποκείμενο των δεδομένων έχει το δικαίωμα να έχει πρόσβαση στα δεδομένα του. Μπορεί οπότε ανά πάσα στιγμή, να αιτηθεί για να λάβει μια λίστα με όλα τα προσωπικά του δεδομένα που έχει στην κατοχή του και επεξεργάζεται οποιοσδήποτε οργανισμός. Οι οργανισμοί έχουν την υποχρέωση να ικανοποιήσουν αυτό το αίτημα μέσα σε 30 ημέρες.

Η διαδικασία αυτή δεν είναι απαραίτητο να γίνεται με τρόπο αυτοματοποιημένο ηλεκτρονικά, και ισχύει τόσο για τα δεδομένα που υπάρχουν και υφίστανται επεξεργασία σε ηλεκτρονικά συστήματα, όσο και για δεδομένα που υπάρχουν και υφίστανται επεξεργασία εκτός ηλεκτρονικών συστημάτων.

Υπάρχουν αρκετοί διαφορετικοί τρόποι για να συμμορφωθούν οι δημόσιοι οργανισμοί με αυτή τη διάταξη του GDPR:

1. *Επεξεργασία των αιτημάτων εκτός συστήματος*: Ο χρήστης στέλνει το αίτημά του ηλεκτρονικά, είτε με ένα απλό μήνυμα ηλεκτρονικού ταχυδρομείου, είτε μέσω κάποιας καινούριας λειτουργίας του ηλεκτρονικού συστήματος, που θα επιτρέπει στον χρήστη να στείλει το αίτημά του στους υπευθύνους. Οι υπεύθυνοι επεξεργάζονται τα αιτήματα αυτά, δημιουργούν τα απαραίτητα αρχεία που περιλαμβάνουν όλα τα δεδομένα του χρήστη, και του τα στέλνουν σαν απάντηση στο ηλεκτρονικό του μήνυμα.
2. *Επεξεργασία των αιτημάτων εντός συστήματος*: Η επιλογή αυτή περιλαμβάνει την δημιουργία μιας καινούριας λειτουργίας στο ηλεκτρονικό σύστημα. Ο χρήστης θα πρέπει να έχει τη δυνατότητα να ζητήσει τη δημιουργία του αρχείου αυτού μέσω του λογαριασμού του στο σύστημα. Η διαδικασία θα πρέπει να είναι σαφής και απλή, και να είναι διαθέσιμη στη σελίδα του ηλεκτρονικού προφίλ του χρήστη. Ο χρήστης θα μπορεί να πατήσει ένα κουμπί, και αυτομάτως το σύστημα θα συγκεντρώνει μια λίστα η οποία θα περιλαμβάνει όλες τις ενέργειες κατά τις οποίες έγινε επεξεργασία των δεδομένων του χρήστη, είτε από τον ίδιο τον χρήστη, είτε από άλλους χρήστες του συστήματος, είτε από το ίδιο το σύστημα. Για κάθε ενέργεια που περιλαμβάνεται στη λίστα αυτή θα πρέπει να είναι σαφές, ποια προσωπικά δεδομένα υπέστησαν επεξεργασία, από ποιόν, πότε, και για ποιόν σκοπό. Η λίστα αυτή θα πρέπει να είναι σε μορφή που επιτρέπει την ανάγνωση και την επεξεργασία από όλα τα προγράμματα υπολογιστικών φύλλων, εμπορικά και ανοιχτού λογισμικού.

   Σε περίπτωση που η λειτουργία αυτή είναι απαιτητική για το σύστημα, και χρειάζεται αρκετό χρόνο για να εκτελεστεί, ή για συστήματα με μεγάλο όγκο δεδομένων και χρηστών, όπου μια τέτοια λειτουργία θα μπορούσε πιθανόν να υπερφορτώσει το σύστημα και να επιδεινώσει την απόδοσή του, η δημιουργία αυτή μπορεί να γίνει ετεροχρονισμένα. Ο χρήστης ζητάει την δημιουργία του αρχείου, με το πάτημα ενός κουμπιού που είναι διαθέσιμο στο προφίλ του, και το σύστημα καταγράφει το

αίτημα αυτό, και παρουσιάζει ένα μήνυμα στον χρήστη, ότι το αίτημά του έχει καταγραφεί, και βρίσκεται υπό επεξεργασία. Η δημιουργία του αρχείου θα μπαίνει σε σειρά προτεραιότητας, και θα εκτελείται εκτός ωρών αιχμής (για παράδειγμα τη νύχτα). Όταν το αρχείο του χρήστη είναι έτοιμο, τότε το σύστημα θα τον ενημερώνει μέσω ηλεκτρονικού ταχυδρομείου, και ο χρήστης θα μπορεί να συνδεθεί στο σύστημα και να κατεβάσει το αρχείο, μέσω ενός συνδέσμου στο προφίλ του. Για λόγους βέλτιστης χρήσης των πόρων του συστήματος, τα αρχεία αυτά δεν θα αποθηκεύονται επ' αόριστόν. Όταν ο χρήστης κατεβάσει το αρχείο, αυτό πλέον θα μπορεί να διαγραφεί από το σύστημα, και ο χρήστης θα μπορεί να αιτηθεί τη δημιουργία καινούριου αρχείου. Σε περίπτωση που ο χρήστης επιλέξει να μην κατεβάσει το αρχείο που είναι διαθέσιμο, αυτό θα διαγράφεται μετά από κάποιες ημέρες (όχι λιγότερες από επτά). Ο περιορισμός αυτός θα πρέπει να γίνει γνωστός στον χρήστη, και να αναφέρεται ρητά και στο μήνυμα επιβεβαίωσης που παρουσιάζεται με την καταχώρηση του αιτήματος, αλλά και στο μήνυμα ηλεκτρονικού ταχυδρομείου που ενημερώνει τον χρήστη ότι το αρχείο είναι διαθέσιμο.

3.2.5 Διαχείριση cookies

Τα cookies αναφέρονται μόνο μία φορά στο κείμενο του κανονισμού GDPR, αλλά αυτή η αναφορά έχει περιπλέκει αρκετά τον τρόπο που τα cookies χρησιμοποιούνταν στις προ GDPR μέρες:

> *"(30) Τα φυσικά πρόσωπα μπορεί να συνδέονται με επιγραμμικά αναγνωριστικά στοιχεία ταυτότητας, τα οποία παρέχονται από τις συσκευές, τις εφαρμογές, τα εργαλεία και τα πρωτόκολλά τους, όπως διευθύνσεις διαδικτυακού πρωτοκόλλου, αναγνωριστικά cookies ή άλλα αναγνωριστικά στοιχεία όπως ετικέτες αναγνώρισης μέσω ραδιοσυχνοτήτων. Αυτά μπορεί να αφήνουν ίχνη τα οποία, ιδίως όταν συνδυαστούν με μοναδικά αναγνωριστικά στοιχεία ταυτότητας και άλλες πληροφορίες που λαμβάνουν οι εξυπηρετητές, μπορούν να χρησιμοποιηθούν για να δημιουργηθεί το προφίλ των φυσικών προσώπων και να αναγνωριστεί η ταυτότητά τους."*

Πηγή: *https://publications.europa.eu/el/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1*

Αυτό σημαίνει πως, στις περιπτώσεις που τα cookies είναι ικανά για να κάνουν τον χρήστη αναγνωρίσιμο, τότε θεωρούνται προσωπικά δεδομένα.

Αρχικά να πούμε πως τα cookies είναι πλέον αναπόσπαστο κομμάτι της ηλεκτρονικής μας ζωής. Είναι ένα μικρό κομμάτι δεδομένων που αποστέλλεται από μία ιστοσελίδα και αποθηκεύεται στον υπολογιστή του χρήστη από το πρόγραμμα περιήγησης ενώ ο χρήστης περιηγείται. Τα cookies σχεδιάστηκαν ως ένας αξιόπιστος μηχανισμός που να μπορούν να αξιοποιήσουν οι ιστοσελίδες για να θυμούνται χρήσιμες πληροφορίες, ή για να καταγράφουν τις δραστηριότητες του χρήστη. Για παράδειγμα, προϊόντα που είναι στο καλάθι του χρήστη για εμπορικά ηλεκτρονικά καταστήματα ή στοιχεία που έχει εισάγει ο χρήστης σε φόρμες, όπως όνομα, διεύθυνση, κωδικοί πρόσβασης κτλ.

Γίνεται έτσι κατανοητό πως η μεγάλη πλειοψηφία των cookies εμπίπτει όντως στον κανονισμό GDPR, καθώς θεωρούνται προσωπικά δεδομένα.

Για πολλές από τις λειτουργίες των περισσότερων συστημάτων ηλεκτρονικής διακυβέρνησης, τα cookies είναι απαραίτητα, και χωρίς αυτά το σύστημα δεν μπορεί να λειτουργήσει.

Οπότε, κάθε δημόσιος οργανισμός που χρησιμοποιεί κάποιο ηλεκτρονικό σύστημα διακυβέρνησης, οφείλει να κάνει ειδική μνεία στα cookies, και να ζητήσει ρητή συγκατάθεση από τους χρήστες του, για την χρήση των cookies.

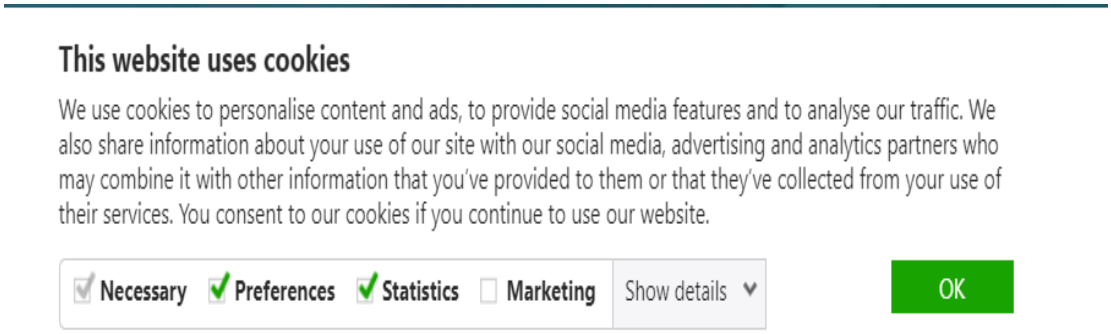
Σύμφωνα με τον κανονισμό GDPR, για να θεωρείται επαρκής η συγκατάθεση του χρήστη για την χρήση cookies:

1. Πρέπει να είναι σαφές για τον χρήστη, σε τι δίνει την συγκατάθεσή του και πρέπει να είναι δυνατή η αποδοχή και η απόρριψη των διαφόρων τύπων cookies.
2. Πρέπει η συγκατάθεση να δίνεται με μια καταφατική, θετική ενέργεια που δεν μπορεί να παρερμηνευθεί.

3. Πρέπει να έχει δοθεί προτού ξεκινήσει η όποια επεξεργασία των δεδομένων προσωπικού χαρακτήρα.
4. Πρέπει να μπορεί να ανακληθεί από τον χρήστη εύκολο και σαφή τρόπο.
5. Επίσης ο χρήστης ανά πάσα στιγμή μπορεί να ζητήσει τη διαγραφή όλων των προσωπικών δεδομένων του.
6. Κάθε συγκατάθεση που έχει δοθεί από τον χρήστη πρέπει να καταγράφεται στο σύστημα, και να τηρείται αρχείο.

Οι παραπάνω απαιτήσεις του κανονισμού GDPR καθιστούν τις περισσότερες ειδοποιήσεις για cookie που χρησιμοποιούνταν πριν από την εφαρμογή του GDPR ξεπερασμένες. Για παράδειγμα, η σιωπηρή συγκατάθεση και η συναίνεση που δίνεται απλώς με την επίσκεψη σε μία ιστοσελίδα δεν αρκεί. Το ίδιο ισχύει και για τα αναδυόμενα παράθυρα και τα banners που δηλώνουν ότι "Χρησιμοποιώντας αυτόν τον ιστότοπο, δίνετε τη συγκατάθεσή σας για την χρήση cookies". Ένα απλό κουμπί «OK» για την αποδοχή των cookies δεν επαρκεί επίσης.

Για παράδειγμα το παρακάτω μήνυμα ικανοποιεί τις απαιτήσεις του κανονισμού GDPR:



Εικόνα 6 *Παράδειγμα banner συγκατάθεσης για cookies που συμμορφώνεται με τον κανονισμό GDPR.*

Παρακάτω περιγράφονται οι λόγοι που το μήνυμα αυτό καλύπτει όλες τις απαιτήσεις του κανονισμού, και μπορεί να χρησιμοποιηθεί σαν παράδειγμα για τους οργανισμούς που αναλύουν τις αλλαγές που θα πρέπει να υλοποιήσουν ως προς την πολιτική των cookies που ακολουθούν.

1. Αρχικά, όλα τα είδη cookies (εκτός από τα απολύτως απαραίτητα για την λειτουργία της ιστοσελίδας) είναι ανενεργά, μέχρις ότου ο χρήστης να δώσει την συγκατάθεσή του.
2. Οι πληροφορίες που δίνονται στον χρήστη, είναι ακριβείς και σαφείς, και παρουσιάζονται σε απλή γλώσσα.
3. Ο χρήστης μπορεί να επιλέξει να δει ολόκληρη τη λίστα των cookies, με τις απαραίτητες περιγραφές όσον αφορά τα δεδομένα που χρησιμοποιεί κάθε cookie, αλλά και την χρησιμότητα και την λειτουργία του.
4. Τα cookies χωρίζονται σε σαφείς κατηγορίες, και ο χρήστης μπορεί να επιλέξει να αποδεχτεί οποιονδήποτε συνδυασμό από αυτές τις κατηγορίες, και να απορρίψει τις υπόλοιπες. Η μόνη κατηγορία cookies που δεν μπορεί να αποεπιλέξει ο χρήστης είναι τα cookies που είναι απολύτως απαραίτητα για την λειτουργία του συστήματος. Πρέπει να αναφερθεί επίσης, πως για όσες κατηγορίες δεν χρησιμοποιούν προσωπικά δεδομένα, η επιλογή μπορεί να είναι προ-επιλεγμένη, ενώ οι κατηγορίες που χρησιμοποιούν προσωπικά δεδομένα πρέπει να είναι απαραιτήτως μη-επιλεγμένη αρχικά, καθώς για να πληρούνται οι απαιτήσεις του κανονισμού GDPR, ο χρήστης πρέπει να κάνει την επιλογή αυτή με δική του σαφή ενέργεια.
5. Ο χρήστης μπορεί να δει ανά πάσα στιγμή τι επιλογές είναι ήδη σε ισχύ, και να αλλάξει την συγκατάθεση του άμεσα και εύκολα μέσα από το προφίλ του.
6. Κάθε επιλογή του χρήστη που αφορά την συγκατάθεση του, αποθηκεύεται στο σύστημα, με όλες τις απαραίτητες λεπτομέρειες (για παράδειγμα ημερομηνία και ώρα).
7. Κάθε δώδεκα μήνες, το σύστημα παρουσιάζει ξανά το banner αυτό στον χρήστη, ζητώντας την ανανέωση της συγκατάθεσης για την χρήστη των cookies.
8. Σε περίπτωση αλλαγής της πολιτικής του συστήματος περί cookies, το banner αυτό θα εμφανιστεί ξανά σε όλους τους χρήστες του συστήματος, ζητώντας ξανά την συγκατάθεση τους.

3.3 Hosting των ηλεκτρονικών συστημάτων και ασφάλεια

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα σχετίζεται σε κάθε περίπτωση φυσικά με έναν ορισμένο βαθμό κινδύνου. Ειδικά στις μέρες μας, όπου οι επιθέσεις στον κυβερνοχώρο είναι σχεδόν αναπόφευκτες. Αυτό είναι μια πραγματικότητα, που φυσικά αναγνωρίζει και ο κανονισμός GDPR. Για αυτόν τον λόγο άλλωστε οι οργανισμοί που μπορούν να αποδείξουν ότι έχει γίνει σημαντική προσπάθεια συμμόρφωσης με τις διατάξεις του κανονισμού GDPR και ότι εφαρμόζονται συγκεκριμένες πολιτικές, πρωτόκολλα και διαδικασίες προστασίας δεδομένων, θα έχουν πολύ καλύτερες πιθανότητες να αποφύγουν πρόστιμα και κυρώσεις σε περίπτωση παραβίασης της ασφάλειας των δεδομένων.

Για αυτόν τον λόγο πρέπει οι οργανισμοί να φροντίσουν έχουν σε εφαρμογή, και να μπορούν να επιδείξουν συγκεκριμένες μεθόδους και πρακτικές όσον αφορά την ασφάλεια των δεδομένων των χρηστών τους.

3.3.1 Ασφάλεια

Ο κανονισμός GDPR ορίζει ότι οι οργανισμοί οφείλουν να λαμβάνουν επαρκή μέτρα για την προστασία των προσωπικών δεδομένων των χρηστών των συστημάτων τους, από παραβιάσεις ασφαλείας. Σύμφωνα με το Άρθρο 4 του κανονισμού, η παραβίαση δεδομένων ορίζεται ως οποιοδήποτε περιστατικό που οδηγεί στην απώλεια, διαγραφή, τροποποίηση ή μη εξουσιοδοτημένη αποκάλυψη δεδομένων:

> *“12) «παραβίαση δεδομένων προσωπικού χαρακτήρα»: ή παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία,”*
>
> *Πηγή: https://publications.europa.eu/el/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1*

Αυτός ο ορισμός είναι αρκετά διαφορετικός από τις μέχρι τώρα ευρέως χρησιμοποιούμενες πρακτικές ως προς την ασφάλεια. Πλέον μια παραβίαση μπορεί να προκληθεί ακόμα και από εσωτερικά λάθη χειρισμού των δεδομένων και όχι μόνο από εξωτερικές επιθέσεις.

Σε κάθε περίπτωση παραβίασης της ασφάλειας των προσωπικών δεδομένων, είτε εξαιτίας εσωτερικού λάθος χειρισμού, είτε από εξωτερική επίθεση, πρέπει να ειδοποιηθεί αμέσως ο Υπεύθυνος Προστασίας Δεδομένων, καθώς και η διοίκηση του οργανισμού άμεσα. Μέσα σε 72 ώρες πρέπει να ολοκληρωθεί η απαραίτητη έρευνα και να ληφθεί μια απόφαση για την σωστή διαχείριση της κατάστασης σύμφωνα με τις διατάξεις του κανονισμού GDPR.

Ανεξάρτητα από το αν το hosting του συστήματος γίνεται εντός του ίδιου του οργανισμού, ή έχει ανατεθεί σε ανάδοχο, πρέπει ο οργανισμός να μπορεί να ελέγξει και να πιστοποιήσει ότι κάθε δυνατό μέτρο ασφαλείας είναι σε ισχύ, ιδιαιτέρως σε ότι αφορά προσωπικά δεδομένα, σύμφωνα με τις διατάξεις του κανονισμού GDPR.

Η ασφάλεια θα πρέπει να λαμβάνεται υπόψιν σε όλα τα επίπεδα από το φυσικό επίπεδο και το επίπεδο δικτύου μέχρι την ασφάλεια διακομιστή και την ασφάλεια εφαρμογών και δεδομένων.

Το σύστημα πρέπει να στεγάζεται σε ένα προστατευμένο και κλιματιζόμενο δωμάτιο. Επίσης, πρέπει να είναι σε ισχύ μέτρα για την επαρκή φυσική ασφάλεια του δωματίου, όπως για παράδειγμα προσωπικό ασφαλείας, συναγερμός κτλ.. Παράλληλα η πρόσβαση σε μη εξουσιοδοτημένο προσωπικό πρέπει να μην είναι δυνατή και να διασφαλίζεται με μηχανικά και ηλεκτρονικά μέσα. Η λίστα των προσώπων που έχουν εξουσιοδοτηθεί να έχουν πρόσβαση στο δωμάτιο όπου φιλοξενείται ο εξοπλισμός, θα πρέπει επίσης να είναι κοινοποιημένη σε όλα τα ενδιαφερόμενα μέρη, και κάθε αλλαγή σε αυτή τη λίστα θα πρέπει να αιτιολογείται και να κοινοποιείται άμεσα.

3.3.2 Disaster recovery site

Οι απαιτήσεις του κανονισμού GDPR ισχύουν εξίσου και για τα συστήματα disaster recovery, και όχι μόνο για συστήματα παραγωγής. Ανεξάρτητα από το

αν το hosting του συστήματος γίνεται εντός του ίδιου του οργανισμού, ή έχει ανατεθεί σε ανάδοχο, μετά την εφαρμογή του κανονισμού GDPR οι συνθήκες και οι απαιτήσεις αλλάζουν σημαντικά. Συγκεκριμένα το άρθρο 32 παράγραφος 1 του νέου κανονισμού GDPR ορίζει τα εξής:

> *"1.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, ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων, περιλαμβανομένων, μεταξύ άλλων, κατά περίπτωση: α) της ψευδωνυμοποίησης και της κρυπτογράφησης δεδομένων προσωπικού χαρακτήρα, 4.5.2016 L 119/51 Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης EL β) της δυνατότητας διασφάλισης του απορρήτου, της ακεραιότητας, της διαθεσιμότητας και της αξιοπιστίας των συστημάτων και των υπηρεσιών επεξεργασίας σε συνεχή βάση, γ) της δυνατότητας αποκατάστασης της διαθεσιμότητας και της πρόσβασης σε δεδομένα προσωπικού χαρακτήρα σε εύθετο χρόνο σε περίπτωση φυσικού ή τεχνικού συμβάντος, δ) διαδικασίας για την τακτική δοκιμή, εκτίμηση και αξιολόγηση της αποτελεσματικότητας των τεχνικών και των οργανωτικών μέτρων για τη διασφάλιση της ασφάλειας της επεξεργασίας."*
>
> *Πηγή: https://publications.europa.eu/el/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1*

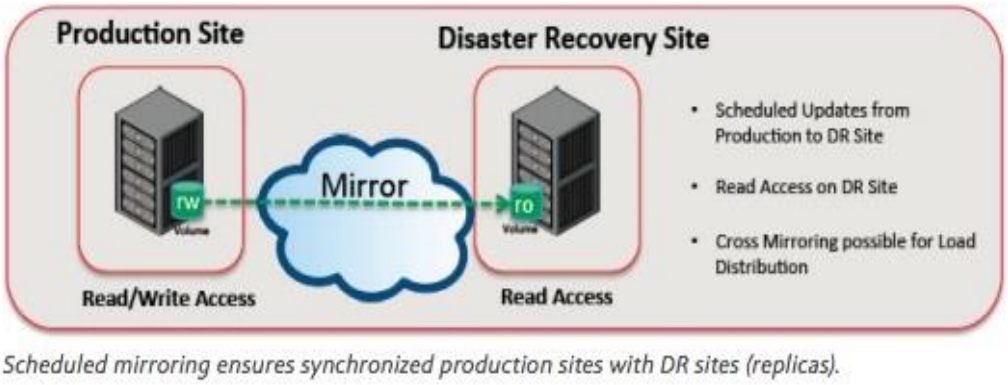
Στο παραπάνω άρθρο 32 του κανονισμού GDPR, τονίζονται ιδιαίτερα δύο σημαντικές απαιτήσεις:

1. Η δυνατότητα γρήγορης αποκατάστασης της διαθεσιμότητας των δεδομένων και της πρόσβασης σε αυτά
2. Η ικανότητα δοκιμής και αξιολόγησης της αποτελεσματικότητας των διαδικασιών προστασίας δεδομένων

Με βάση τα παραπάνω, η πραγματοποίηση εβδομαδιαίων backup των δεδομένων, δεν επαρκεί πλέον. Ο κανονισμός GDPR υπαγορεύει ότι οι οργανισμοί οφείλουν να διασφαλίσουν ότι τα δεδομένα μπορούν να ανακτηθούν εγκαίρως και να λάβουν τεκμηριωμένα βήματα για να εξασφαλιστεί η αποτελεσματικότητα των διαδικασιών που χρησιμοποιούν.

Παράλληλα, οι οργανισμοί θα πρέπει να είναι σε θέση να επιδείξουν τις διαδικασίες σχετικά με την ασφάλεια, τη διαθεσιμότητα, την αποκατάσταση και τη δοκιμή των συστημάτων ηλεκτρονικής διακυβέρνησης που χρησιμοποιούν, συμπεριλαμβανομένου και της πολιτικής περί disaster recovery. Επιπλέον, αυτές οι διαδικασίες πρέπει να είναι κατάλληλες για την εξασφάλιση της έγκαιρης και αποτελεσματικής ανάκτησης των δεδομένων, χωρίς κίνδυνο για την εμπιστευτικότητα και την ακεραιότητα των δεδομένων των χρηστών του συστήματος.

Για την διασφάλιση ότι μια φυσική απειλή δεν θα θέσει σε κίνδυνο τα δεδομένα των χρηστών, μία συνήθης τακτική είναι να διατηρούνται τα συστήματα παραγωγής σε διαφορετική τοποθεσία (με απόσταση μεγαλύτερη από 20 χιλιόμετρα) από τα συστήματα disaster recovery. Με αυτόν τον τρόπο, ελαχιστοποιούνται οι πιθανότητες ταυτόχρονης αποτυχίας και των δύο συστημάτων, και παράλληλα εξασφαλίζεται ένας πολύ μικρός χρόνος αποκατάστασης.



Εικόνα 7 *Disaster recovery map*

3.3.3 Κρυπτογράφηση δεδομένων

Η κρυπτογράφηση των δεδομένων είναι επίσης μια αποτελεσματική μέθοδος, με την οποία οι οργανισμοί μπορούν να μειώσουν την πιθανότητα παραβίασης των δεδομένων των χρηστών τους.

Η κρυπτογράφηση αναφέρεται στη διαδικασία που μετατρέπει την καθαρή πληροφορία σε κωδικοποιημένη. Η κωδικοποιημένη αυτή πληροφορία, έχει δημιουργηθεί χρησιμοποιώντας ένα κλειδί κρυπτογράφησης, και οι πληροφορίες αυτές μπορούν να επανέλθουν στην αρχική «καθαρή» μορφή τους μόνο με το σωστό κλειδί αποκωδικοποίησης. Η μέθοδος αυτή, ελαχιστοποιεί τον κίνδυνο παραβίασης της ασφάλειας κατά την επεξεργασία δεδομένων, καθώς τα κρυπτογραφημένα δεδομένα δεν μπορούν να αναγνωστούν από τρίτους που δεν έχουν το σωστό κλειδί.

3.4 Προκλήσεις στα συμβόλαια με αναδόχους/ παρόχους συστημάτων και υπηρεσιών

Ο κανονισμός GDPR φέρει ιδιαίτερες προκλήσεις στους οργανισμούς που έχουν αναθέσει την δημιουργία, την συντήρηση ή το hosting των ηλεκτρονικών συστημάτων τους σε αναδόχους / εξωτερικούς συνεργάτες / επιχειρήσεις εκτός από τα πλαίσια του ίδιου του οργανισμού.

Αρχικά, το σημαντικότερο βήμα που πρέπει να γίνει στις περιπτώσεις αυτές, είναι να γίνει σαφής διαχωρισμός των ρόλων και των ευθυνών των ενδιαφερόμενων μερών. Αυτό είναι κάτι που πρέπει να συμφωνηθεί από κοινού, και να επισφραγιστεί με κάποιο δεσμευτικό συμβόλαιο. Κατ' αυτόν τον τρόπο, διασφαλίζεται πως δεν θα υπάρχει κάποια παρανόηση ως προς τις ευθύνες του καθενός στην ικανοποίηση των απαιτήσεων του κανονισμού GDPR. Σε αντίθετη περίπτωση, υπάρχει ο κίνδυνος να μην καλύπτονται κάποιες από τις απαιτήσεις του κανονισμού, από τις διαδικασίες που θα είναι σε ισχύ είτε από την μεριά του οργανισμού είτε από την μεριά του αναδόχου. Επίσης, ένα τέτοιο συμβόλαιο διασφαλίζει παράλληλα, ότι ακόμα και στην περίπτωση που υπάρξει κάποια παραβίαση, θα είναι σαφές ποιο από τα ενδιαφερόμενα μέρη φέρει την ευθύνη, και οφείλει να επωμιστεί τις όποιες κυρώσεις.

3.4.1 Ανάγκη για σαφή ορισμό δραστηριοτήτων και ευθύνης κάθε ενδιαφερόμενου μέρους

Ο οργανισμός που έχει την «ιδιοκτησία» του ηλεκτρονικού συστήματος διακυβέρνησης έχει τον ρόλο του «Υπευθύνου της Επεξεργασίας» (Data controller).

Ο ανάδοχος / εξωτερικός συνεργάτης / επιχείρηση που έχει αναλάβει την δημιουργία, την συντήρηση ή το hosting των ηλεκτρονικών συστημάτων του οργανισμού - «Υπευθύνου της Επεξεργασίας», έχει τον ρόλο του «Εκτελών την Επεξεργασία» (Data Processor).

Με βάση τον παραπάνω αρχικό διαχωρισμό, γίνεται εύκολα κατανοητό, πως σύμφωνα με τον κανονισμό GDPR, ο οργανισμός - «Υπεύθυνος της Επεξεργασίας», έχει την ευθύνη για την ανάλυση των απαιτήσεων του κανονισμού GDPR. Σε περίπτωση που αυτή η ανάλυση επισημάνει κάποιες απαραίτητες αλλαγές προκειμένου να επιτευχθεί η συμμόρφωση με τον κανονισμό, η ευθύνη για την υλοποίηση τους και για την έναρξη της λειτουργίας τους στο παραγωγικό σύστημα, πέφτει επίσης στον οργανισμό «Υπεύθυνος της Επεξεργασίας».

Είναι ξεκάθαρο πως ο ανάδοχος - «Εκτελών την Επεξεργασία», δεν μπορεί να ορίσει τέτοιου είδους αλλαγές, παρά μόνο να υλοποιήσει τις αλλαγές που θα του υποδείξει ο οργανισμός - «Υπεύθυνος της Επεξεργασίας». Ως εκ τούτου, η ευθύνη του αναδόχου θα είναι να βοηθήσει τον οργανισμό - «Υπεύθυνος της Επεξεργασίας» στην εκπλήρωση των υποχρεώσεών του όσον αφορά τον κανονισμό GDPR, υλοποιώντας τα μέτρα που ο οργανισμός κρίνει αναγκαία.

Όπως αναφέρθηκε και παραπάνω, είναι απαραίτητο να γίνει σαφής διαχωρισμός των ρόλων και των ευθυνών των ενδιαφερόμενων μερών και η από κοινού αυτή συμφωνία πρέπει να και να επισφραγιστεί με κάποιο δεσμευτικό συμβόλαιο. Παρακάτω παρατίθενται τα βασικότερα σημεία που θα πρέπει να καλύπτει το συμβόλαιο αυτό:

1. Όλα τα ενδιαφερόμενα μέρη αναλαμβάνουν την υποχρέωση να τηρούν το νόμο, και τις διατάξεις του κανονισμού GDPR.
2. Ο οργανισμός - «Υπεύθυνος της Επεξεργασίας» θα παρέχει στον ανάδοχο - «Εκτελών την Επεξεργασία», όλα τα απαραίτητα δεδομένα που είναι απαραίτητα για την εκτέλεση των καθηκόντων που του αναθέτει η εν λόγω σύμβαση.
3. Ο ανάδοχος - «Εκτελών την Επεξεργασία», θα επεξεργαστεί τα Δεδομένα σύμφωνα με τις οδηγίες του οργανισμού - «Υπευθύνου της Επεξεργασίας», και σύμφωνα με τους κανόνες της συγκεκριμένης σύμβασης.
4. Εκτός από την περίπτωση που ο οργανισμός - «Υπεύθυνος της Επεξεργασίας» εξουσιοδοτεί ρητώς ή του δίνει οδηγίες, ο ανάδοχος - «Εκτελών την Επεξεργασία», δεν θα κοινοποιήσει δεδομένα σε τρίτους.
5. Ο ανάδοχος - «Εκτελών την Επεξεργασία» θα τηρεί αρχείο των δραστηριοτήτων επεξεργασίας που εκτελεί για τον οργανισμό - «Υπεύθυνο της Επεξεργασίας». Ο κανονισμός GDPR, και ειδικότερα το Άρθρο 30 - Μητρώο δραστηριοτήτων επεξεργασίας, απαριθμεί τα στοιχεία που πρέπει να περιλαμβάνονται στο μητρώο αυτό. Μετά από αίτημα του οργανισμού - «Υπεύθυνου της Επεξεργασίας», ο ανάδοχος - «Εκτελών την Επεξεργασία» υποχρεούται να υποβάλει αυτό το μητρώο. Ο ανάδοχος - «Εκτελών την Επεξεργασία» αναλαμβάνει επίσης να

εξασφαλίσει ότι το μητρώο θα είναι σε λειτουργία το αργότερο εντός 14 ημερολογιακών ημερών από την έναρξη του συμβολαίου.

6. Ο ανάδοχος - «Εκτελών την Επεξεργασία», αναλαμβάνει την υποχρέωση να ενημερώνει τα πρόσωπα που ενεργούν υπό την εποπτεία του για τις διατάξεις του κανονισμού GDPR και των εκτελεστικών διατάξεών του.
7. Ο οργανισμός - «Υπεύθυνος της Επεξεργασίας» μπορεί ανά πάσα στιγμή να ζητήσει από τον ανάδοχο - «Εκτελών την Επεξεργασία», αντίγραφο των δεδομένων που υποβάλλονται σε επεξεργασία.

   Επιπροσθέτως, ο ανάδοχος - «Εκτελών την Επεξεργασία», δεν μπορεί να αντιγράψει τα διαθέσιμα δεδομένα, εκτός εάν πρόκειται για σκοπούς δημιουργίας αντιγράφων ασφαλείας ή αν το αντίγραφο είναι απαραίτητο για την εκτέλεση των καθηκόντων που του έχουν ανατεθεί από τον οργανισμό - «Υπεύθυνο της Επεξεργασίας».

   Οι ίδιοι περιορισμοί και υποχρεώσεις που ισχύουν για τα αρχικά δεδομένα ισχύουν για όλα τα αντίγραφα των δεδομένων.

   Κατόπιν αιτήματος του οργανισμού - «Υπεύθυνου της Επεξεργασίας», ο ανάδοχος - «Εκτελών την Επεξεργασία», οφείλει, χωρίς αδικαιολόγητη καθυστέρηση, να θέσει στη διάθεση και / ή να καταστρέψει ανεπανόρθωτα όλα τα αντίγραφα των δεδομένων που έχουν υποστεί επεξεργασία από τον ανάδοχο - «Εκτελών την Επεξεργασία», ή για λογαριασμό του αναδόχου - «Εκτελών την Επεξεργασία».

   Ο ανάδοχος - «Εκτελών την Επεξεργασία» δεν θα καταχωρήσει ποτέ τα δεδομένα σε τόπο εκτός της Ευρωπαϊκής Οικονομική Ζώνης και ποτέ δεν θα τα μεταβιβάσει σε χώρες εκτός της Ευρωπαϊκής Οικονομική Ζώνης. Επιπρόσθετα, ο ανάδοχος - «Εκτελών την Επεξεργασία» δεν θα καταχωρήσει τα δεδομένα σε τόπο εκτός της ευρωπαϊκής επικράτειας, χωρίς την προηγούμενη έγγραφη εξουσιοδότηση του οργανισμού - «Υπευθύνου της Επεξεργασίας». Επίσης, ο οργανισμός - «Υπεύθυνος της Επεξεργασίας» μπορεί να επισυνάπτει όρους σε αυτήν του την εξουσιοδότηση, οι οποίοι θα πρέπει να γίνονται σεβαστοί και να εφαρμόζονται από τον ανάδοχος - «Εκτελών την Επεξεργασία».

8. Ο ανάδοχος - «Εκτελών την Επεξεργασία» οφείλει να τεκμηριώνει, όλα τα μέτρα που λαμβάνονται για την προστασία των δεδομένων και ο οργανισμός - «Υπεύθυνος της Επεξεργασίας» μπορεί ανά πάσα στιγμή να ζητήσει από τον ανάδοχο - «Εκτελών την Επεξεργασία», να αιτιολογήσει τα ληφθέντα προστατευτικά μέτρα και να παράσχει τις σχετικές πληροφορίες.
9. Ο ανάδοχος - «Εκτελών την Επεξεργασία» οφείλει να ορίσει, έναν Υπεύθυνο Προστασίας Δεδομένων (DPO) και να παρέχει, μια γενική περιγραφή των τεχνικών και οργανωτικών μέτρων ασφαλείας.
10. Ο ανάδοχος - «Εκτελών την Επεξεργασία» θα προβεί στις απαραίτητες ενέργειες για να διασφαλίσει ότι τα τεχνικά και οργανωτικά μέτρα είναι επαρκή για την προστασία των δεδομένων από τυχαία ή μη εξουσιοδοτημένη καταστροφή, από τυχαία απώλεια, καθώς και από τροποποίηση, πρόσβαση και οποιαδήποτε άλλη μη εξουσιοδοτημένη επεξεργασία δεδομένων.
11. Ο ανάδοχος - «Εκτελών την Επεξεργασία» εγγυάται - στο μέτρο του τεχνικού δυνατού - την ακεραιότητα, τη διαθεσιμότητα και την εμπιστευτικότητα των δεδομένων που επεξεργάζεται για λογαριασμό του οργανισμού - «Υπευθύνου της Επεξεργασίας».

    Για το σκοπό αυτό, πρέπει να εφαρμόζει και να χρησιμοποιεί τεχνολογίες και τεχνικές ασφαλείας σύμφωνα με τις βέλτιστες πρακτικές της βιομηχανίας, σύμφωνα με τις συστάσεις του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων.
12. Οι δραστηριότητες των χρηστών του συστήματος και τα αντίστοιχα δεδομένα καταγράφονται σε αρχεία καταγραφής.
13. Ο ανάδοχος - «Εκτελών την Επεξεργασία» χρησιμοποιεί συγκεκριμένες διαδικασίες για να εξασφαλίσει τη διαθεσιμότητα των πληροφοριών, του λογισμικού και άλλων πόρων, συμπεριλαμβανομένων των διαδικασιών για την εξασφάλιση διαθεσιμότητας κατά τις κρίσιμες στιγμές.
14. Ο οργανισμός - «Υπεύθυνος της Επεξεργασίας» δύναται ανά πάσα στιγμή να γνωστοποιήσει στον ανάδοχο - «Εκτελών την Επεξεργασία» πληροφορίες σχετικά με πιθανά νέα πρότυπα ασφαλείας, και να ζητήσει να συζητηθεί η προσαρμογή των μεθόδων εργασίας του αναδόχου -

«Εκτελών την Επεξεργασία» ώστε να ικανοποιούνται τυχόν νέες απαιτήσεις.

15. Ο ανάδοχος - «Εκτελών την Επεξεργασία» οφείλει να εξασφαλίζει ότι τα πρόσωπα που εργάζονται για λογαριασμό του, έχουν πρόσβαση αποκλειστικά και μόνο στα δεδομένα που είναι απαραίτητα για την εκπλήρωση των καθηκόντων τους για λογαριασμό του οργανισμού - «Υπευθύνου της Επεξεργασίας». Αυτό ισχύει για το μόνιμο ή έκτακτο προσωπικό και για κάθε τρίτο μέρος που εμπλέκεται άμεσα ή έμμεσα στις δραστηριότητες του αναδόχου - «Εκτελών την Επεξεργασία».
16. Ο ανάδοχος - «Εκτελών την Επεξεργασία» λαμβάνει μέτρα για την πρόληψη, ανίχνευση ή παρεμπόδιση με άλλο τρόπο της ακατάλληλης χρήσης ή / και της κατάχρησης συστημάτων και δικτύων.
17. Τα δίκτυα και τα συστήματα πληροφοριών παρακολουθούνται και διαχειρίζονται ενεργά από τον ανάδοχο - «Εκτελών την Επεξεργασία».
18. Ο ανάδοχος - «Εκτελών την Επεξεργασία» παρέχει φυσικούς και / ή ηλεκτρονικούς μηχανισμούς πρόσβασης στα συστήματα και τα δεδομένα του οργανισμού - «Υπευθύνου της Επεξεργασίας». Αυτοί οι μηχανισμοί πρέπει να περιλαμβάνουν μια μέθοδο που είναι σαφώς ασφαλής ώστε να επιτρέπει την πρόσβαση στα δεδομένα.
19. Ο ανάδοχος - «Εκτελών την Επεξεργασία» παρέχει ενημερωμένο κατάλογο μόνιμου ή έκτακτου προσωπικού και οποιωνδήποτε τρίτων εμπλέκονται άμεσα ή έμμεσα στην επεξεργασία των δεδομένων του οργανισμού - «Υπευθύνου της Επεξεργασίας», καθώς και τις άδειες που έχουν σχετικά με τα δεδομένα που υφίστανται επεξεργασία.
20. Ο ανάδοχος - «Εκτελών την Επεξεργασία» είναι υπεύθυνος για την ασφάλεια και την ορθή χρήση των ονομάτων χρηστών και των κωδικών πρόσβασης (συμπεριλαμβανομένης της τακτικής αλλαγής αυτών των κωδικών) για την πρόσβαση στα δεδομένα και την επεξεργασία τους. Ο ανάδοχος - «Εκτελών την Επεξεργασία» αναλαμβάνει επίσης να καταβάλει κάθε προσπάθεια για να διασφαλίσει ότι κάθε πρόσωπο που έχει πρόσβαση στα δεδομένα διατηρεί την εμπιστευτικότητα των κωδικών πρόσβασής του.
21. Ο ανάδοχος - «Εκτελών την Επεξεργασία» αναλαμβάνει την υποχρέωση να αναφέρει όλες τις (απόπειρες) επεξεργασίας δεδομένων ή την

πρόσβαση σε παράνομα ή μη εξουσιοδοτημένα δεδομένα. Ο ανάδοχος - «Εκτελών την Επεξεργασία» θα αναφέρει χωρίς αδικαιολόγητη καθυστέρηση οποιοδήποτε τέτοιο περιστατικό στον υπεύθυνο επεξεργασίας και το αργότερο 24 ώρες μετά το περιστατικό. Επιπλέον, ο ανάδοχος - «Εκτελών την Επεξεργασία» θα λάβει όλα τα μέτρα που είναι εύλογα αναγκαία για την πρόληψη ή τον περιορισμό της (μετέπειτα) παραβίασης των μέτρων ασφαλείας.

22. Κατά την αναφορά ενός περιστατικού, ο ανάδοχος - «Εκτελών την Επεξεργασία» θα επικοινωνήσει στον οργανισμό - «Υπεύθυνο της Επεξεργασίας» τουλάχιστον τις παρακάτω πληροφορίες:
    a. την φύση του συμβάντος
    b. την ημερομηνία και ώρα της διαπίστωσης
    c. τα δεδομένα που επηρεάστηκαν με οποιονδήποτε τρόπο
    d. τα μέτρα που λαμβάνονται άμεσα για τον περιορισμό των ζημιών
    e. την ημερομηνία και ώρα του κλεισίματος του συμβάντος
    f. καθώς επίσης και ποια διαρθρωτικά μέτρα ελήφθησαν για να αποφευχθεί αυτό το είδος συμβάντος στο μέλλον
23. Ο ανάδοχος - «Εκτελών την Επεξεργασία» και κάθε πρόσωπο που ενεργεί για λογαριασμό του πρέπει να σέβεται την αυστηρή εμπιστευτικότητα των δεδομένων που υποβάλλονται σε επεξεργασία για λογαριασμό του οργανισμού - «Υπευθύνου της Επεξεργασίας».

    Μια εξαίρεση από αυτόν τον κανόνα είναι δυνατή μόνο αν μια νομική απαίτηση ή μια δικαστική εντολή υποχρεώνει τον ανάδοχο - «Εκτελών την Επεξεργασία» να επικοινωνήσει συγκεκριμένα δεδομένα.
24. Κάθε πρόσωπο που έχει πρόσβαση στα δεδομένα πρέπει να δεσμεύεται από υποχρέωση εμπιστευτικότητας και πρέπει να υπογράψει έγγραφο για το σκοπό αυτό.

    Η υποχρέωση αυτή θα παραμείνει σε ισχύ ακόμα και μετά τη μεταφορά ή τη λύση της παρούσας σύμβασης.
25. Μετά τον τερματισμό της σύμβασης μεταξύ του οργανισμού - «Υπευθύνου της Επεξεργασίας» και του αναδόχου - «Εκτελών την Επεξεργασία» , ο ανάδοχος - «Εκτελών την Επεξεργασία» θα παρέχει στον οργανισμό - «Υπεύθυνο της Επεξεργασίας» ή σε οποιοδήποτε άλλο πρόσωπο που ορίζεται από τον οργανισμό - «Υπεύθυνο της

Επεξεργασίας» επικαιροποιημένο αντίγραφο των Δεδομένων που υποβάλλονται σε επεξεργασία με τη μορφή που συμφωνήθηκε μεταξύ των ενδιαφερομένων μερών. Θα παρέχει επίσης κάθε πληροφορία ή έγγραφο που είναι απαραίτητο για την περαιτέρω επεξεργασία των δεδομένων.

26. Ο ανάδοχος - «Εκτελών την Επεξεργασία» θα παρέχει εγκαίρως και με επιμέλεια όλα τα δεδομένα.
27. Μόλις ολοκληρωθεί η μεταφορά όλων των δεδομένων, ο ανάδοχος - «Εκτελών την Επεξεργασία» θα παύσει χωρίς αδικαιολόγητη καθυστέρηση οποιαδήποτε επεξεργασία των δεδομένων και θα καταστρέψει οποιοδήποτε αντίγραφο των δεδομένων και Βάσεων Δεδομένων που εξακολουθεί να κατέχει, εκτός εάν συμφωνηθεί διαφορετικά μεταξύ των ενδιαφερομένων μερών.
28. Επιπλέον, μόλις ολοκληρωθούν αυτές οι καταστροφές, θα στείλει πιστοποιητικό καταστροφής στον οργανισμό - «Υπεύθυνο της Επεξεργασίας».

3.4.2 Αύξηση κόστους για την συντήρηση και το hosting

Όπως αναφέρθηκε στο προηγούμενο κεφάλαιο, σύμφωνα με τον κανονισμό GDPR, ο οργανισμός - «Υπεύθυνος της Επεξεργασίας», έχει την ευθύνη για την ανάλυση των απαιτήσεων του κανονισμού GDPR, καθώς και για την υλοποίηση τους και για την έναρξη της λειτουργίας τους στο παραγωγικό σύστημα.

Συχνά, αυτό σημαίνει πως οι οργανισμοί θα επιβαρυνθούν με το επιπλέον κόστος για την πρόσληψη ειδικών συμβούλων που θα είναι σε θέση να διεξάγουν και να επικυρώσουν το αποτέλεσμα της ανάλυσης αυτής, καθώς μπορεί να μην διαθέτουν προσωπικό που να μπορεί να αναλάβει την διεξαγωγή αυτής της ανάλυσης, από την πλευρά την νομική ή/ και την τεχνική.

Επίσης, σε περίπτωση που η ανάλυση αυτή υποδείξει όντως συγκεκριμένες αλλαγές που πρέπει να υλοποιηθούν για να επιτευχθεί η συμμόρφωση με τον κανονισμό GDPR, η ευθύνη για την παραγγελία της υλοποίησης αυτών των

αλλαγών ή των νέων λειτουργιών, βαραίνει τον οργανισμό - «Υπεύθυνο της Επεξεργασίας».

Το γεγονός αυτό συνεπάγεται, σχεδόν σε όλες τις περιπτώσεις, επιπλέον κόστος, ανάλογα με το είδος του συμβολαίου για την συντήρηση ή/ και το hosting του ηλεκτρονικού συστήματος, που υπάρχει ανάμεσα στον οργανισμό - «Υπεύθυνο της Επεξεργασίας» και στον ο ανάδοχο - «Εκτελών την Επεξεργασία».

Η αποφυγή αυτού του αρχικού κόστους για την υλοποίηση καινούριων λειτουργιών του συστήματος, ή αλλαγών στις ήδη υπάρχουσες, δεν μπορεί να υποστηριχθεί με βάση τις διατάξεις του κανονισμού GDPR. Οι οργανισμοί θα πρέπει να φροντίσουν για την έγκαιρη εξασφάλιση επαρκούς χρηματοδότησης, και να διασφαλίσουν την έγκαιρη παραγγελία των αλλαγών αυτών.

Παράλληλα, δεδομένου ότι ο κανονισμός GDPR αλλάζει κατά πολύ τις μέχρι πρότινος συνήθεις πρακτικές όσον αφορά το hosting ηλεκτρονικών εφαρμογών, και την ασφάλεια των δεδομένων, είναι αναμενόμενο ότι θα αυξηθούν και οι τιμές για παροχή υπηρεσιών hosting.

3.5 Σύνοψη

Συνοψίζοντας, οι πιο σημαντικές αλλαγές που προκύπτουν για τους δημοσίους οργανισμούς, αφορούν τρεις βασικούς τομείς:

- Αλλαγές στην λειτουργία των συστημάτων ηλεκτρονικής διακυβέρνησης, που στοχεύουν κατά κύριο λόγο στο να διασφαλιστεί πως τα συστήματα παρέχουν στους χρήστες όλες τις δυνατότητες που υπαγορεύει ο κανονισμός
- Αλλαγές στο καθεστώς hosting και ασφάλειας, τόσο σε φυσικό όσο και σε επίπεδο εφαρμογών και δεδομένων
- Αλλαγές και προκλήσεις στις συνεργασίες με αναδόχους, όπου τα συστήματα ηλεκτρονικής διακυβέρνησης δημιουργούνται και συντηρούνται από τρίτα μέρη, εκτός του οργανισμού, που αναλαμβάνουν τον ρόλο του «Εκτελών την Επεξεργασία» (Data Processor), όπως ορίζεται από τον κανονισμό GDPR.

Κεφάλαιο 4 – Συμπεράσματα και lessons learned από τον πρώτο χρόνο εφαρμογής του κανονισμού GDPR

4.1 Εισαγωγή

Ένα χρόνο μετά την έναρξη της εφαρμογής του κανονισμού GDPR, είναι η ώρα για έναν πρώτο ολοκληρωμένο απολογισμό, με σκοπό την επισκόπηση του προηγούμενου έτους, την αξιολόγηση της τρέχουσας κατάστασης, και τον σχεδιασμό για το μέλλον.

Στο κεφάλαιο αυτό παρατίθενται και αναλύονται τα σημαντικότερα αποτελέσματα ερευνών που διεξήχθησαν μετά την εφαρμογή του κανονισμού, με θέμα τα ζητήματα που προέκυψαν κατά την προσπάθεια των οργανισμών για συμμόρφωση, τα κρούσματα παραβίασης της ασφάλειας που σημειώθηκαν, αλλά και την άποψη των ιδιωτών για τον κανονισμό.

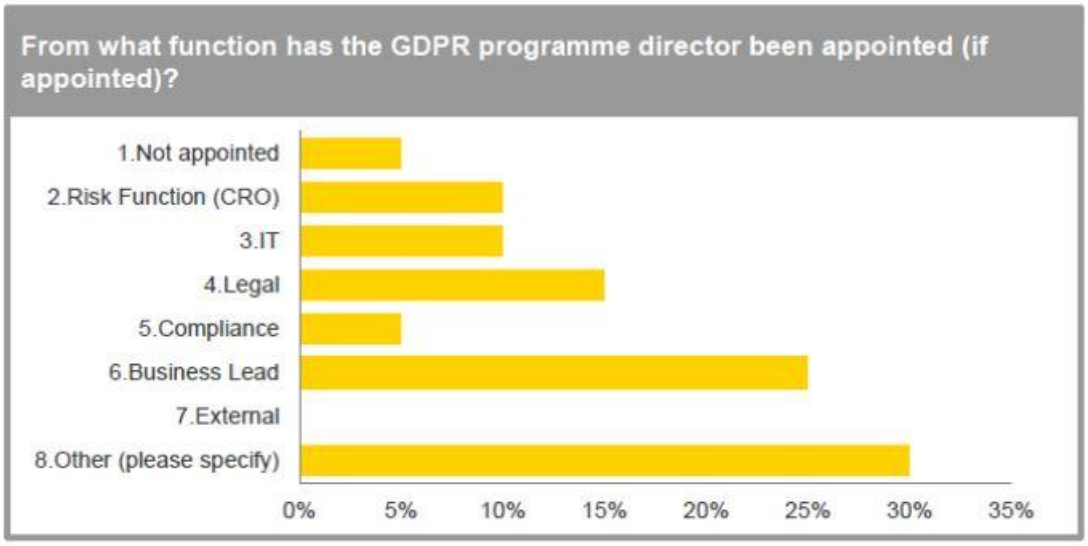
4.2 Lessons learned

Σε αυτήν την κατεύθυνση, η Διεθνής Ένωση Επαγγελματιών Προστασίας Προσωπικών Δεδομένων (IAPP - International Association of Privacy Professionals), διεξήγαγε μια έρευνα (Πηγή: https://iapp.org/media/pdf/resource_center/EY_Implementing_GDPR.pdf) και εξήγαγε κάποια πρώτα στατιστικά στοιχεία σχετικά με τα βήματα που έχουν ήδη κάνει οι οργανισμοί, τους τομείς που συνάντησαν τις περισσότερες δυσκολίες, τα κίνητρα που τους οδήγησαν στην εφαρμογή των διαφόρων μέτρων κτλ. Παρακάτω, παρατίθενται τα σημαντικότερα στοιχεία που προκύπτουν από αυτήν την έρευνα.

4.2.1 Επιλογή επικεφαλούς του προγράμματος συμμόρφωσης με τον κανονισμό GDPR

Στην ερώτηση «Από ποιον τομέα προέρχεται ο επιλεγμένος επικεφαλής του προγράμματος συμμόρφωσης με τον κανονισμό GDPR εντός της εταιρείας», οι απαντήσεις ήταν μοιρασμένες. Φαίνεται πως δεν υπάρχει μια συγκεκριμένη επιλογή που να θεωρείται γενικότερα ως προτιμώμενη από τους ερωτηθέντες οργανισμούς. Η πιο δημοφιλής επιλογή, ωστόσο ήταν ο « Επιχειρηματικός

τομέας» με 25%, ακολουθούμενη από τον «Νομικό τομέα» με 15%, και τον «τομέα Πληροφορικής» και «τομέα Διαχείρισης Ρίσκου» με 10%.



Εικόνα 8 *Επιλογή επικεφαλούς του προγράμματος GDPR εντός του οργανισμού*

4.2.2 Κορυφαίες προτεραιότητες, προβλήματα και προκλήσεις

Από την έρευνα προέκυψαν:

Ως κορυφαίες προτεραιότητες:

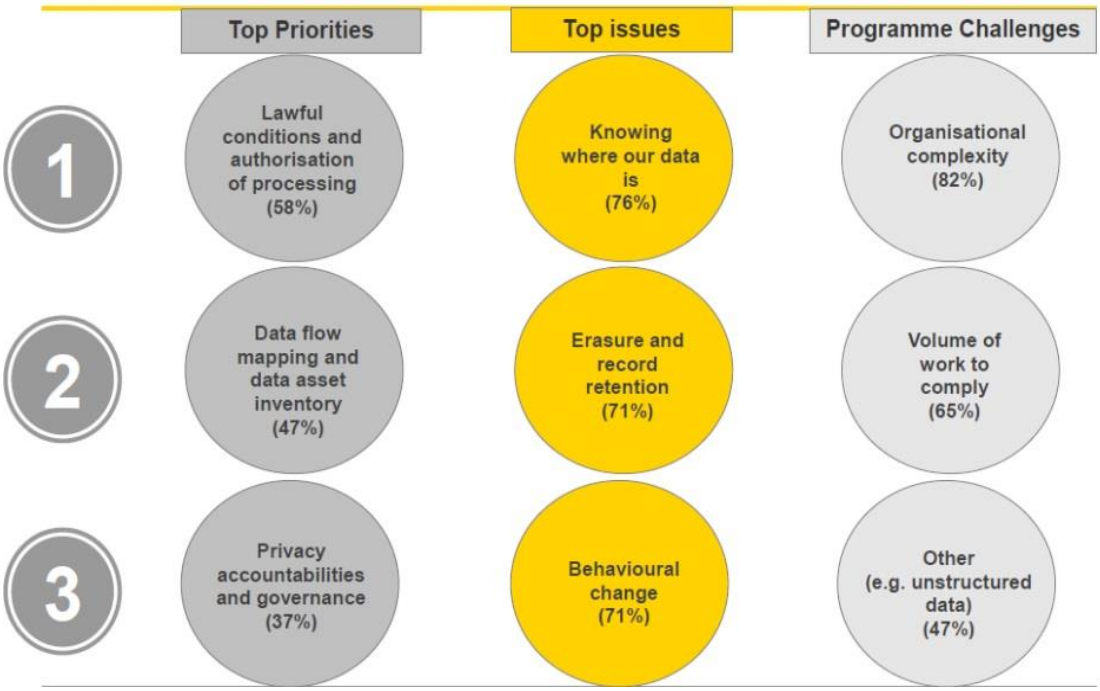
1. Οι νόμιμες συνθήκες και η έγκριση της επεξεργασίας, με 58%
2. Η χαρτογράφηση της ροής δεδομένων και απογραφή των δεδομένων που διαθέτει ο οργανισμός, με 47%
3. Η διαχείριση και η υπευθυνότητα ως προς την ιδιωτικότητα των δεδομένων, με 37%

Ως κορυφαία προβλήματα:

1. Η γνώση του που βρίσκονται τα δεδομένα, με 76%
2. Η διαγραφή και η διατήρηση αρχείου, με 71%
3. Η αλλαγή στην συμπεριφορά του προσωπικού, με 71%

Ως κορυφαίες προκλήσεις:

1. Η πολυπλοκότητα της δομής του οργανισμού, με 82%
2. Ο όγκος της εργασίας που απαιτεί η συμμόρφωση με τον κανονισμό, με 65%
3. Λοιπές προκλήσεις, όπως μη-δομημένα δεδομένα, με 47%

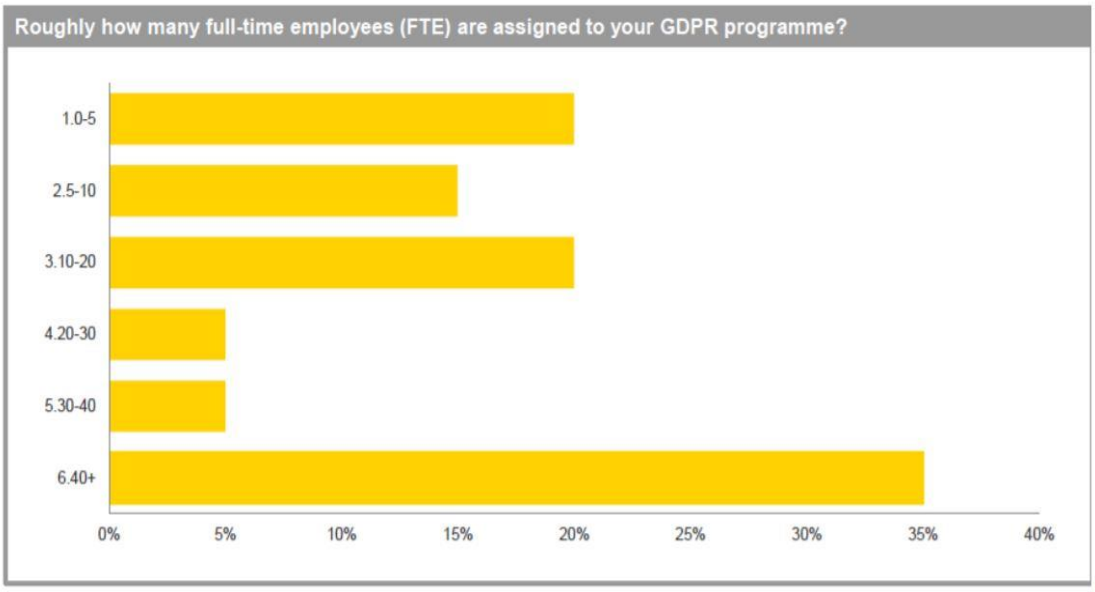


Εικόνα 9 *Κορυφαίες προτεραιότητες, προβλήματα και προκλήσεις*

4.2.3 Απαιτήσεις σε προσωπικό

Από τους ερωτηθέντες οργανισμούς,

- το 35% έχει αναθέσει στο πρόγραμμα συμμόρφωσης με τον κανονισμό GDPR, περισσότερους από έξι εργαζομένους πλήρους απασχόλησης,
- το 30% των οργανισμών έχει αναθέσει από τρεις έως έξι.
- και το υπόλοιπο 35%, από έναν μέχρι τρεις.



Εικόνα 10 *Αριθμός εργαζομένων στο πρόγραμμα GDPR*

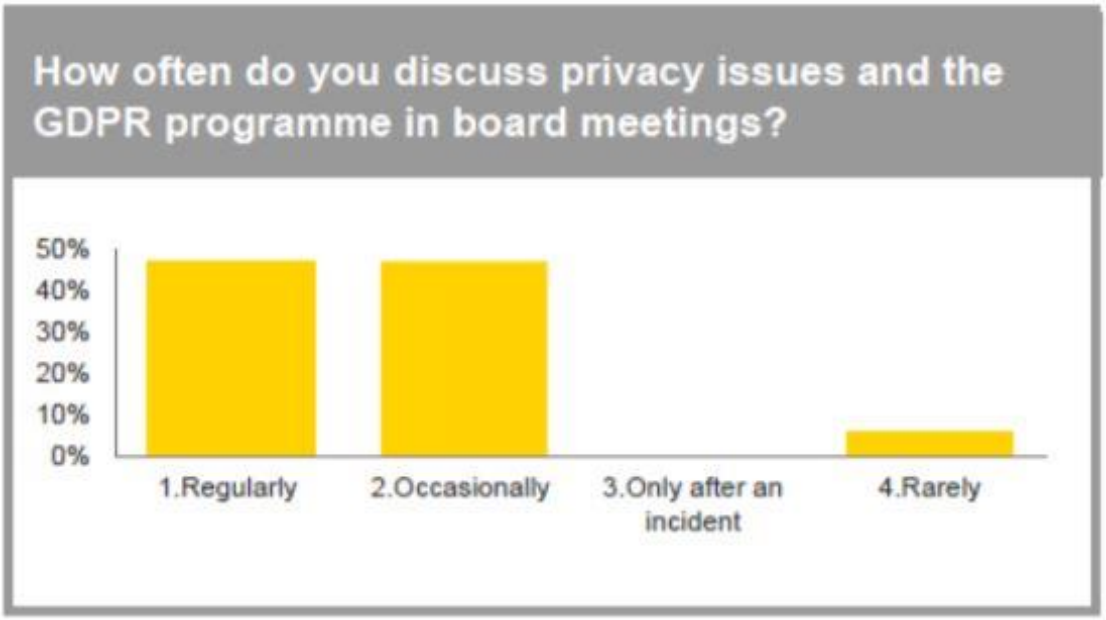
4.2.4 Reporting, και διοικητικά συμβούλια

Όσον αφορά τις αναφορές ως προς την πρόοδο του προγράμματος συμμόρφωσης με τον κανονισμό GDPR, που απευθύνονται στα ανώτερα στελέχη, το 20% των ερωτηθέντων οργανισμών δήλωσε πως είναι εβδομαδιαίες, ενώ το 30% των οργανισμών δήλωσε πως ετοιμάζει τέτοιες αναφορές δύο φορές τον μήνα, και το 35% μία φορά τον μήνα.

Εικόνα 11 *Συχνότητα εσωτερικών αναφορών σχετικά με τον κανονισμό GDPR*

Οι οργανισμοί κλήθηκαν να απαντήσουν επίσης πόσο συχνά συζητούνται οποιαδήποτε ζητήματα σχετικά με το πρόγραμμα συμμόρφωσης με τον

κανονισμό GDPR, στα διοικητικά συμβούλια των ανώτερων στελεχών. Μόνο οι μισοί οργανισμοί δήλωσαν πως συζητούν τέτοια ζητήματα τακτικά, ενώ οι άλλοι μισοί μόνο περιστασιακά η ακόμα και σπάνια.

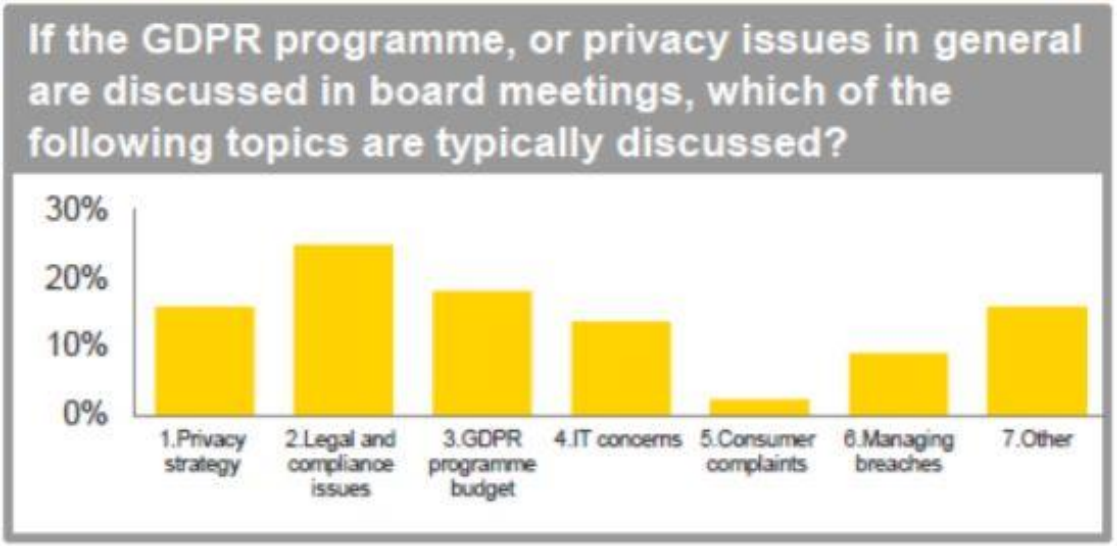


Εικόνα 12 *Συχνότητα συζητήσεων περί του κανονισμού GDPR στα διοικητικά συμβούλια*

Σε αυτήν την κατεύθυνση, ζητήθηκε από τους συμμετέχοντες οργανισμούς να αναφέρουν τι είδους ζητήματα συζητούν σχετικά με το πρόγραμμα συμμόρφωσης με τον κανονισμό GDPR.

Η πιο δημοφιλής απάντηση ήταν νομικά ζητήματα, και ζητήματα συμμόρφωσης, με 25%, ακολουθούμενη από τα ζητήματα προϋπολογισμού, και προβλημάτων πληροφορικής.

Αξίζει εδώ να τονίσουμε, πως τα παράπονα των τελικών χρηστών ήταν το τελευταίο θέμα συζήτησης, με λιγότερο από 5% των απαντήσεων.



Εικόνα 13 *Θέματα συζήτησης για τον κανονισμό GDPR στα διοικητικά συμβούλια*

4.2.5 Χρήση τεχνολογίας

Οι οργανισμοί ερωτήθηκαν επίσης για το εάν χρησιμοποιούν τεχνολογικές λύσεις στην προσπάθειά τους για συμμόρφωση με τον κανονισμό GDPR, και εάν αυτές οι τεχνολογικές λύσεις είναι καινούριες, η αν προϋπήρχαν στον οργανισμό ακόμα και πριν το GDPR.

Συγκεκριμένα δόθηκαν οι παρακάτω κατηγορίες τεχνολογικών λύσεων:

- Εφαρμογές τρίτων
- Ρομποτική
- Αυτοματοποίηση διαδικασιών
- Συστήματα διαχείρισης συναίνεσης
- Υπηρεσίες ασφαλούς μεταφοράς αρχείων

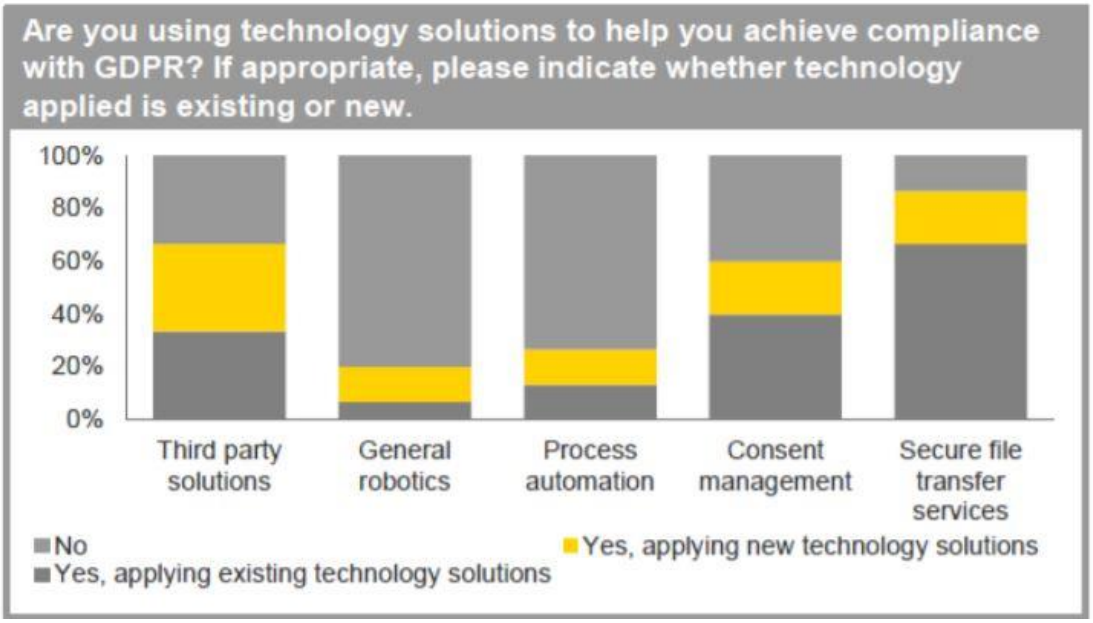
Η πιο συχνά χρησιμοποιούμενη κατηγορία τεχνολογικών λύσεων ήταν οι υπηρεσίες ασφαλούς μεταφοράς αρχείων, με περίπου το 90% των οργανισμών να δηλώνει ότι κάνει χρήση τέτοιων υπηρεσιών. Αξίζει επίσης να σημειωθεί πως το 70% δήλωσε πως οι υπηρεσίες αυτές προϋπήρχαν, ενώ μόνο το 20% δήλωσε πως οι υπηρεσίες αυτές μπήκαν σε χρήση με αφορμή το πρόγραμμα συμμόρφωσης του οργανισμού με τον κανονισμό GDPR.

Στην δεύτερη θέση έρχονται οι εφαρμογές τρίτων, με το 65% των οργανισμών να δηλώνει πως κάνει χρήση τέτοιων τεχνολογικών λύσεων. Αυτή ήταν και η

κατηγορία που σημειώθηκε το μεγαλύτερο ποσοστό καινούριων τεχνολογικών λύσεων, με ποσοστό 35%, έναντι του 30% που σημείωσαν οι προϋπάρχουσες τεχνολογικές λύσεις αυτής της κατηγορίας.

Στην τρίτη θέση ακολουθούν τα συστήματα διαχείρισης συναίνεσης, με 60%. Τα δύο τρίτα των οργανισμών που κάνουν χρήση τέτοιων συστημάτων, δήλωσαν πως χρησιμοποιούν προϋπάρχουσες τεχνολογικές λύσεις.

Οι κατηγορίες ρομποτική και αυτοματοποίηση διαδικασιών σημείωσαν πολύ χαμηλά ποσοστά, με περίπου το 20% των οργανισμών να δηλώνει πως χρησιμοποιεί τέτοιες λύσεις στο πρόγραμμα συμμόρφωσης με τον κανονισμό GDPR.



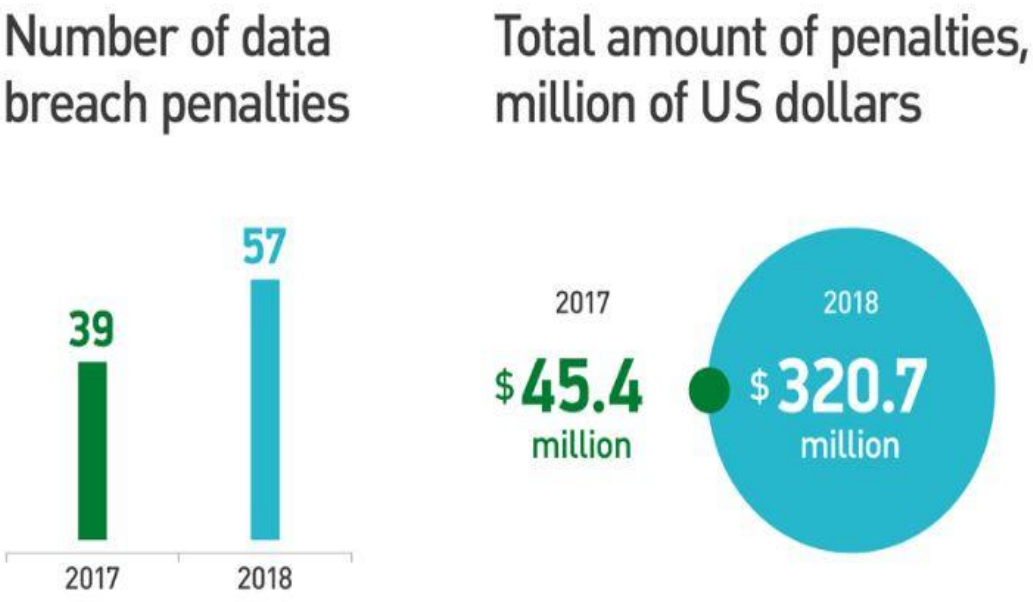
Εικόνα 14 *Χρήση τεχνολογίας*

4.3 Κρούσματα παραβίασης ασφάλειας και ποινές

Ο οργανισμός InfoWatch Analytics Center, διεξήγαγε μια παγκόσμια έρευνα (https://infowatch.com/news/101490) όπου συγκέντρωσε και σύγκρινε τα στοιχεία για τις παραβιάσεις ασφαλείας και τις ποινές που δόθηκαν το 2017 και το 2018, σε εμπορικές επιχειρήσεις αλλά και σε δημοσίους οργανισμούς.

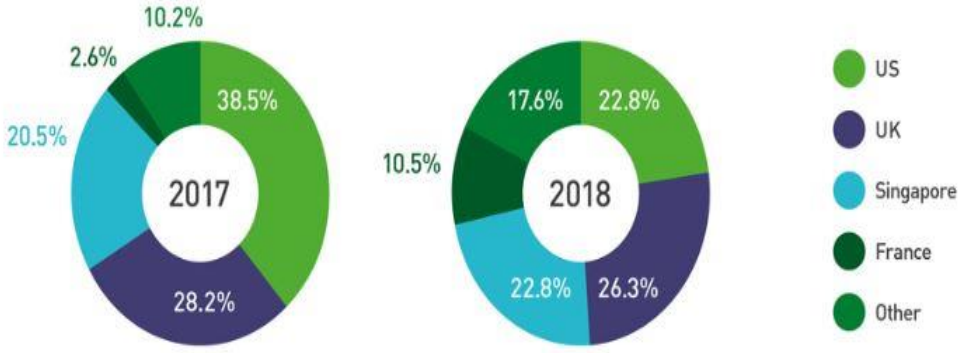
Σε παγκόσμιο επίπεδο, ο αριθμός των παραβιάσεων δεδομένων που σημειώθηκαν, αλλά και το μέγεθος των ποινών που δόθηκαν είναι σε αυξητική τροχιά. Το 2017 σημειώθηκαν 39 πρόστιμα, και το συνολικό ποσό ανήλθε στα

45 εκατομμύρια δολάρια, ενώ το 2018 ο αριθμός των προστίμων ανέβηκε στα 57 με το συνολικό ποσό να ξεπερνά τα 320 εκατομμύρια δολάρια.



Εικόνα 15 *Πρόστιμα για παραβιάσεις ασφαλείας δεδομένων 2017-1018*

Επίσης, το 2018 τέτοιες κυρώσεις για διαρροές προσωπικών δεδομένων εφαρμόστηκαν έναντι οργανισμών σε 11 χώρες (Αυστρία, Βραζιλία, Ηνωμένο Βασίλειο, Γερμανία, Ολλανδία, Ισπανία, Ιταλία, Πορτογαλία, Σιγκαπούρη, ΗΠΑ και Γαλλία), ενώ το 2017 οι ποινές αφορούσαν μόνο 8 χώρες. Οι αρχές στη Γαλλία έγιναν αρκετά αυστηρότερες, και έδωσαν έξι ποινές το 2018, ενώ το 2017 είχαν δώσει μόλις μία.



Εικόνα 16 *Πρόστιμα ανά χώρα*

Στις Ηνωμένες Πολιτείες Αμερικής, η μέση τιμή της οικονομικής ποινής ανά περιστατικό παραβίασης δεδομένων, οκταπλασιάστηκε το 2018, αγγίζοντας τα 23,3 εκατομμύρια δολάρια.

Στο Ηνωμένο Βασίλειο, η μέση τιμή της οικονομικής ποινής ανά περιστατικό παραβίασης δεδομένων, δεκατετραπλασιάστηκε το 2018, φτάνοντας τα 1,69 εκατομμύρια δολάρια.

Σε κάποιες άλλες χώρες, με αντίστοιχα περιστατικά, η μέση οικονομική ποινή το λιγότερο διπλασιάστηκε, ξεπερνώντας το 1 εκατομμύριο δολάρια.

Η Σιγκαπούρη, σημείωσε αύξηση της μέσης οικονομικής ποινής περίπου στα 10,000 δολάρια, και παραμένει η μοναδική Ασιατική χώρα που έχει καθιερωμένη πρακτική στην εφαρμογή προστίμων για περιστατικά παραβίασης δεδομένων.

Εικόνα 17 *Μέση οικονομική ποινή ανά χώρα 2017-2018*

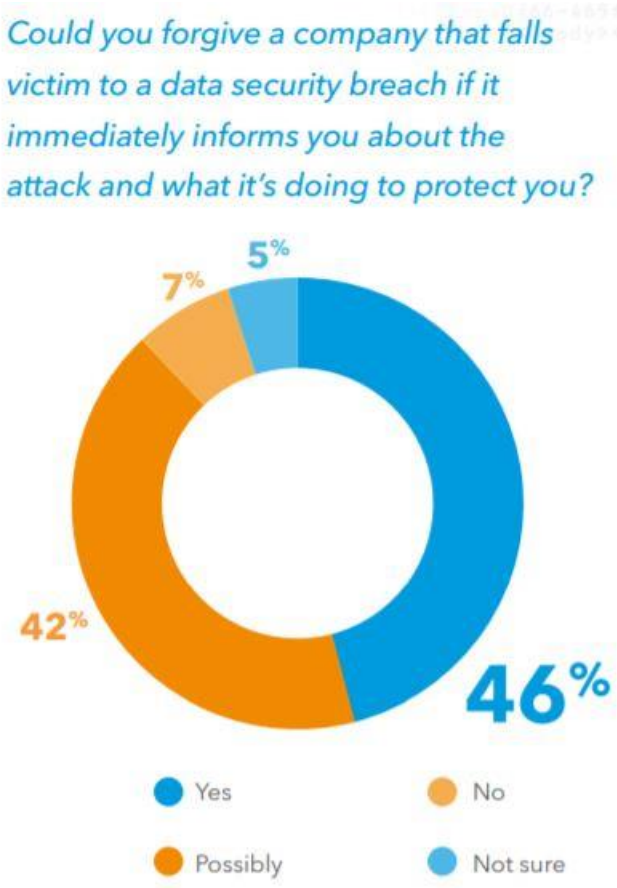
4.4 Η άποψη των ιδιωτών

Η Ackamai διεξήγαγε μια έρευνα (https://www.akamai.com/us/en/multimedia/documents/report/akamai-research-consumer-attitudes-toward-data-privacy.pdf) που απευθυνόταν

αποκλειστικά σε ιδιώτες, ή όπως τους ονομάζει ο κανονισμός GDPR, Υποκείμενα των Δεδομένων.

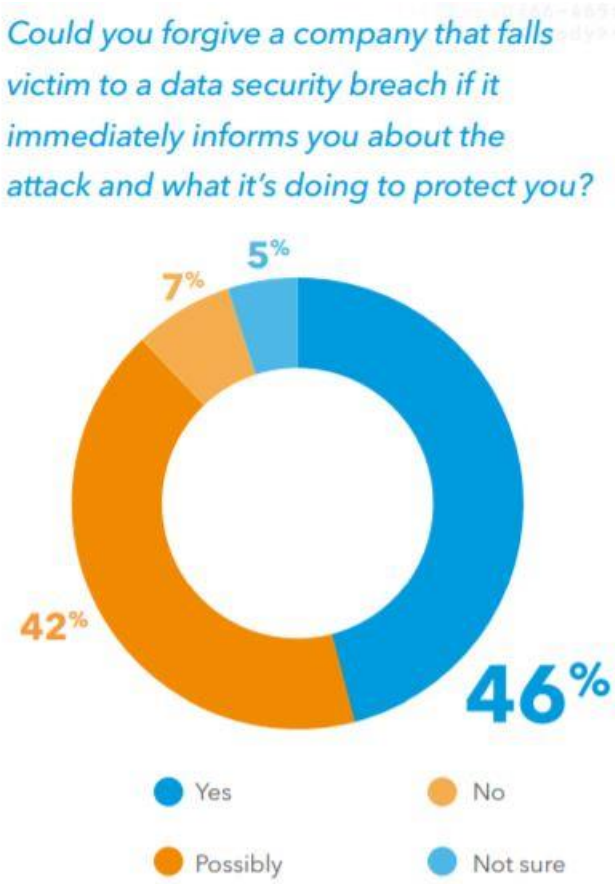
Η έρευνα αυτή υποδεικνύει πως οι ιδιώτες «συγχωρούν» πολύ εύκολα τους οργανισμούς, παρά τις πιθανές παραβιάσεις των δεδομένων τους, αρκεί οι οργανισμοί να δείξουν προσπάθεια.

Συγκεκριμένα, το 46% των ερωτηθέντων δήλωσε πως θα συγχωρούσε μια παραβίαση των δεδομένων του, αρκεί ο οργανισμός να τον ενημέρωνε άμεσα για το περιστατικό, καθώς και για το πως ανταποκρίνεται σε αυτήν την περίπτωση.



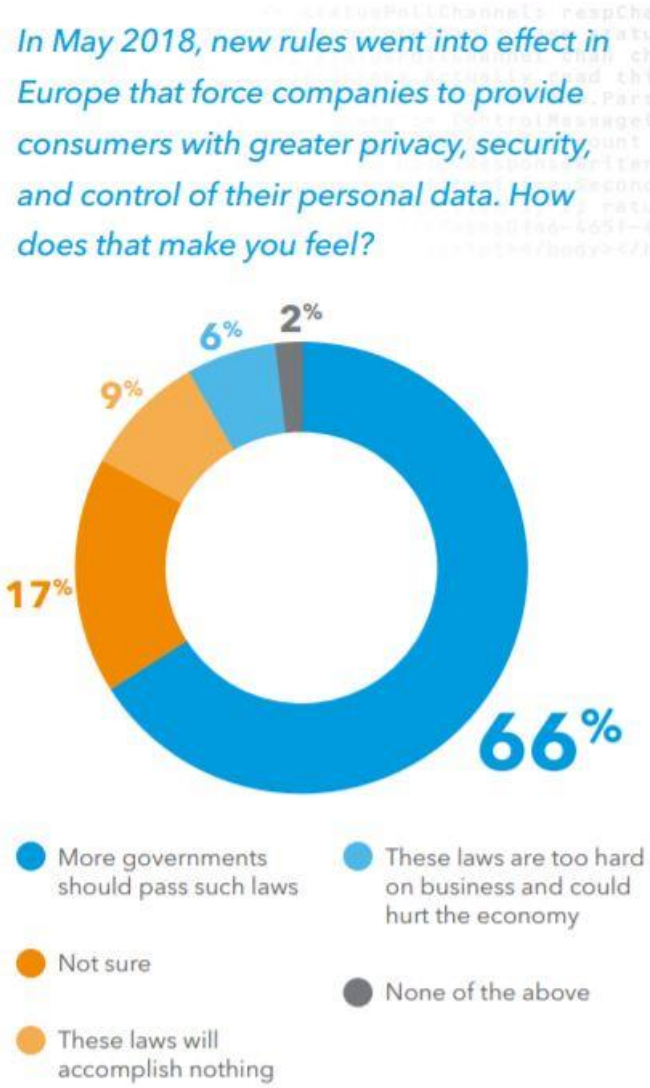
Εικόνα 18 *Αντιδράσεις ιδιωτών σε παραβίαση των δεδομένων τους*

Η έρευνα αυτή επίσης δείχνει πως ο αριθμός των ιδιωτών που προσπαθεί ενεργά να προστατέψει τα προσωπικά του δεδομένα, αυξάνεται. Το 71% των ερωτηθέντων δήλωσε πως χρησιμοποιεί λογισμικό για να προστατέψει τα δεδομένα του στο διαδίκτυο.



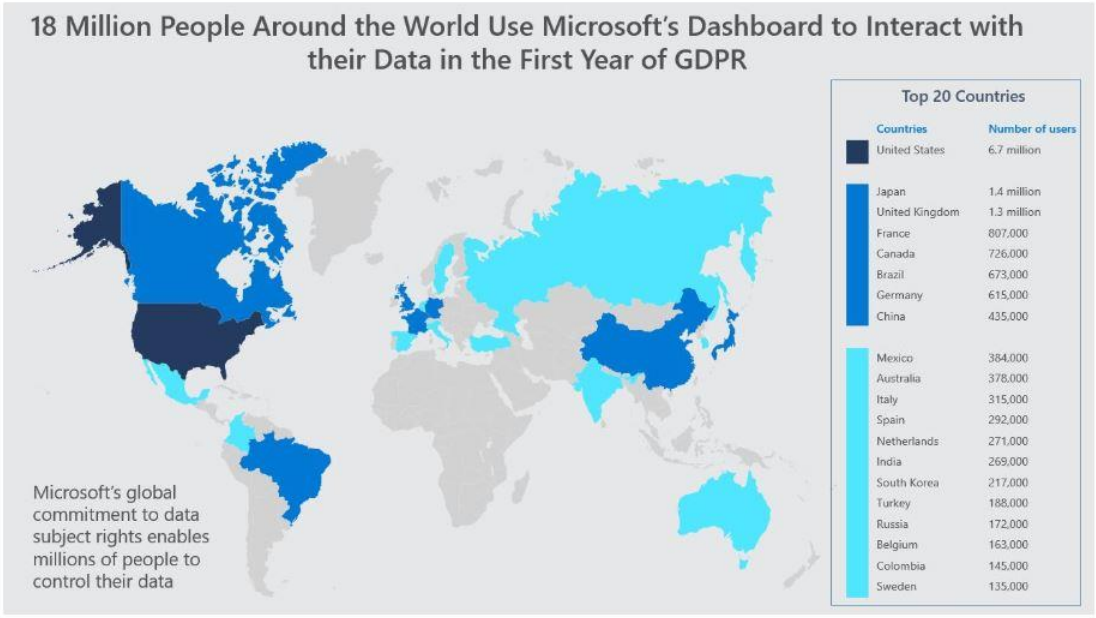
Εικόνα 19 *Χρήση λογισμικού προστασίας δεδομένων*

Το 66% των ερωτηθέντων, δήλωσε πως βλέπει θετικά τον ευρωπαϊκό κανονισμό GDPR και πως περισσότερες κυβερνήσεις ανά τον κόσμο θα έπρεπε να εφαρμόσουν αντίστοιχες νομοθεσίες. Ένα μικρό ποσοστό μόνο (9%) δήλωσε πως θεωρεί ότι τέτοιες νομοθεσίες είναι αναποτελεσματικές ή ότι θα ζημιώσει σημαντικά τις επιχειρήσεις και την οικονομία (6%).



Εικόνα 20 *Η άποψη των ιδιωτών για τον κανονισμό GDPR*

Η τάση αυτή των καταναλωτών ανά την υφήλιο, για καλύτερο έλεγχο των προσωπικών τους δεδομένων, φαίνεται να επιβεβαιώνεται και από τα στοιχεία που έδωσε στην δημοσιότητα η Microsoft, ως προς την χρήση της πλατφόρμας ελέγχου ιδιωτικότητας που παρέχει στους χρήστες της σε παγκόσμιο επίπεδο.



Εικόνα 21 *Δεδομένα χρήσης της πλατφόρμας MS Dashboard, σε παγκόσμιο επίπεδο*

Περισσότεροι από 18 εκατομμύρια άνθρωποι ανά την υφήλιο, χρησιμοποίησαν την πλατφόρμα της Microsoft, για να αλληλοεπιδράσουν με τα δεδομένα τους. Ο αυξανόμενος αριθμός αυτών των χρηστών, μας δείχνει ξεκάθαρα πως οι άνθρωποι θέλουν να έχουν την δύναμη να ελέγχουν τα δεδομένα τους.

Η πλειοψηφία αυτών των χρηστών προέρχεται από τις Ηνωμένες Πολιτείες Αμερικής (περίπου 6,7 εκατομμύρια). Επίσης ο αριθμός των χρηστών από την Ευρώπη είναι πολύ υψηλός, κάτι που δεν προκαλεί έκπληξη, αφού ο κανονισμός GDPR αφορά άμεσα τους πολίτες της Ευρωπαϊκής Ένωσης. Παρόλα αυτά όμως, η ζήτηση είναι παγκόσμια σύμφωνα με τα στοιχεία της Microsoft. Η δεύτερη χώρα μετά τις ΗΠΑ είναι η Ιαπωνία, και ο Καναδάς είναι στην πέμπτη θέση. Στην πρώτη δεκάδα των χωρών με την μεγαλύτερη χρήση της πλατφόρμας, βλέπουμε επίσης την Βραζιλία, την Κίνα, το Μεξικό και την Αυστραλία.

4.5 Παγκόσμια επιρροή

Όπως είναι ξεκάθαρο από τα στοιχεία που παρουσιάστηκαν στο προηγούμενο κεφάλαιο, η ανησυχία σε παγκόσμιο επίπεδο όσον αφορά το πόσα προσωπικά

δεδομένα συλλέγονται, και το ρίσκο που εμπεριέχεται στις χρησιμοποιούμενες μεθόδους, είναι σε αυξητική τροχιά.

Ο κανονισμός GDPR είναι αυτή την στιγμή, το ισχυρότερο καθεστώς προστασίας προσωπικών δεδομένων σε παγκόσμιο επίπεδο, και πολλοί πιστεύουν ότι θα λειτουργήσει ως το «χρυσό πρότυπο», και για άλλες χώρες.

Ο κανονισμός GDPR όπως έχει αναφερθεί ήδη, απαιτεί από όλους τους οργανισμούς που επεξεργάζονται προσωπικά δεδομένα προσώπων που είναι εντός της Ευρωπαϊκής Οικονομικής Ζώνης, να συμμορφωθούν με τις διατάξεις του, ακόμα και αν ο εν λόγω οργανισμός είναι εκτός Ευρωπαϊκής Οικονομικής Ζώνης και η επεξεργασία γίνεται επίσης εκτός Ευρωπαϊκής Οικονομικής Ζώνης. Αυτή η απαίτηση προσδίδει επιπλέον κύρος στον κανονισμό, και μπορεί εύκολα να χρησιμοποιηθεί από πολίτες τρίτων χωρών, για να απαιτήσουν αντίστοιχες νομοθεσίες.

Η εφαρμογή του κανονισμού GDPR, έχει βελτιώσει τον τρόπο με τον οποίο οι οργανισμοί χειρίζονται τα προσωπικά δεδομένα των χρηστών τους, και έχει εμπνεύσει ένα παγκόσμιο κίνημα που έχει οδηγήσει χώρες από όλο τον κόσμο να υιοθετήσουν νέους νόμους περί προστασίας προσωπικών δεδομένων, που έχουν διαμορφωθεί με βάσει τον κανονισμό GDPR σαν πρότυπο.

Η Βραζιλία, η Κίνα, η Ινδία, η Ιαπωνία, η Νότια Κορέα, η Σιγκαπούρη και η Ταϊλάνδη συγκαταλέγονται μεταξύ των κρατών που ψήφισαν νέους νόμους, πρότειναν νέα νομοθεσία ή σκέφτονται να αλλάξουν τους υπάρχοντες νόμους με τρόπο τέτοιο ώστε να τους φέρουν πιο κοντά στις απαιτήσεις του κανονισμού GDPR.

Ο Καναδάς έχει υιοθετήσει επίσης νομοθεσία αντίστοιχη με τον κανονισμό GDPR. Μέχρι στιγμής, οι Ηνωμένες Πολιτείες Αμερικής δεν διαθέτουν κάποια αντίστοιχη νομοθεσία, με μόνη εξαίρεση την πολιτεία της Καλιφόρνια στην οποία έχει ψηφιστεί ένας κανονισμός για την προστασία της ιδιωτικής ζωής του καταναλωτή, παρόμοιος με τον κανονισμό GDPR. Παρόλα αυτά, με βάση το παγκόσμιο τοπίο στον τομέα της προστασίας δεδομένων, αλλά και τις απαιτήσεις των καταναλωτών στην μετά – GDPR εποχή, είναι μόνο θέμα

χρόνου πριν η πίεση των καταναλωτών οδηγήσει σε παρόμοια νομοθεσία και στις ΗΠΑ.

4.6 Σύνοψη

Συνοψίζοντας, από την μελέτη των στοιχείων που παρουσιάστηκαν σε αυτό το κεφάλαιο, είναι ξεκάθαρο πως η ανησυχία περί προστασίας των προσωπικών δεδομένων και της ιδιωτικότητας, συνεχώς και αυξάνεται σε παγκόσμιο επίπεδο. Παρόλα αυτά οι ιδιώτες φαίνεται να «συγχωρούν» πολύ εύκολα τους οργανισμούς, παρά τις πιθανές παραβιάσεις των δεδομένων τους, αρκεί οι οργανισμοί να δείξουν προσπάθεια

Ο ευρωπαϊκός κανονισμός GDPR, είναι αυτή την στιγμή το ισχυρότερο καθεστώς προστασίας προσωπικών δεδομένων σε παγκόσμιο επίπεδο. Παράλληλα οι καταναλωτές ανά την υφήλιο, βλέπουν θετικά τον ευρωπαϊκό κανονισμό GDPR και θεωρούν πως περισσότερες κυβερνήσεις ανά τον κόσμο θα έπρεπε να εφαρμόσουν αντίστοιχες νομοθεσίες. Μάλιστα ήδη πολλές χώρες έχουν ήδη ξεκινήσει την προσπάθεια για δημιουργία αντίστοιχων νομοθεσιών σε τοπικό επίπεδο. Για αυτόν τον λόγο πολλοί ειδικοί πιστεύουν ότι η τάση αυτή θα συνεχιστεί και ο κανονισμός GDPR θα λειτουργήσει ως το «χρυσό πρότυπο» για την προστασία των προσωπικών δεδομένων σε παγκόσμιο επίπεδο.

ΒΙΒΛΙΟΓΡΑΦΙΑ – ΠΗΓΕΣ ΑΠΟ ΤΟ ΔΙΑΔΙΚΤΥΟ

Κανονισμός 2016/679/ΕΕ 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), Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης αριθ. L 119/1 της 4/5/2016. Διαθέσιμη στο Διαδίκτυο στη διεύθυνση: http://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32016R0679

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, Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης αριθ. L 281 της 23/11/1995. Διαθέσιμη στο Διαδίκτυο στη διεύθυνση: https://eur-lex.europa.eu/legal-content/el/TXT/?uri=CELEX%3A31995L0046

https://publications.europa.eu/el/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1

https://europa.eu/european-union/eu-law/legal-acts_el

https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

https://www.gdpreu.org/the-regulation/key-concepts/data-controllers-and-processors/

http://www.globallegalpost.com/blogs/blagging-the-blogs/the-global-impact-of-gdpr---what-companies-need-to-know-16947516/

https://www.techrepublic.com/article/gdpr-compliance-deadline-is-approaching-10-things-to-do-right-away/

https://www.cookiebot.com/en/gdpr-cookies/

https://en.wikipedia.org/wiki/Data_anonymization

https://gdpr.report/news/2017/11/07/data-masking-anonymisation-pseudonymisation/

https://www.ucl.ac.uk/legal-services/guidance/gdpr-anonymisation-pseudonymisation

https://iapp.org/news/a/does-anonymization-or-de-identification-require-consent-under-the-gdpr/

https://www.ionos.com/digitalguide/websites/digital-law/general-data-protection-regulation-new-rules-for-businesses/

https://digitalguardian.com/blog/what-data-encryption

https://en.wikipedia.org/wiki/Encryption

https://en.wikipedia.org/wiki/Disaster_recovery

https://searchdisasterrecovery.techtarget.com/definition/disaster-recovery

https://mapr.com/tech-briefs/disaster-recovery/

https://platform.sh/blog/data-protection-by-design-and-default/

https://www.hitachi-systems-security.com/blog/one-year-after-gdpr-lessons-learned/

https://www.akamai.com/us/en/multimedia/documents/report/akamai-research-consumer-attitudes-toward-data-privacy.pdf

https://www.paymentscardsandmobile.com/psd2-and-gdpr-one-year-on-time-to-act/

https://www.consumersinternational.org/media/155133/gdpr-briefing.pdf

https://www.ey.com/Publication/vwLUAssets/ey-gdpr-lessons-learned/$FILE/ey-gdpr-lessons-learned.pdf

https://www.cmo.com/features/articles/2018/9/11/experts-share-5-gdpr-lessons.html#gs.gxq6tf

https://diginomica.com/government-bodies-can-learn-gdpr-use-cases-private-sector

https://iapp.org/media/pdf/resource_center/EY_Implementing_GDPR.pdf

https://blogs.microsoft.com/on-the-issues/2019/05/20/gdprs-first-anniversary-a-year-of-progress-in-privacy-protection/

https://infowatch.com/news/101490

https://www.trendmicro.com/vinfo/ph/security/definition/data-breach

https://www.itgovernance.eu/blog/en/7-tips-to-help-you-implement-a-gdpr-staff-awareness-training-programme

https://platform.sh/blog/your-guide-to-gdpr-compliance-training-your-employees/

ΠΗΓΕΣ ΕΙΚΟΝΩΝ

Εικόνες 1-2: https://yourfreetemplates.com

Εικόνες 4-5: https://www.slideshare.net/ISSDA/anonymisation-and-social-research

Εικόνα 6: https://www.cookiebot.com/en/gdpr-cookies/

Εικόνα 7: https://mapr.com/tech-briefs/disaster-recovery/

Εικόνες 8-14: https://iapp.org/media/pdf/resource_center/EY_Implementing_GDPR.pdf

Εικόνες 15-17: https://infowatch.com/news/101490

Εικόνες 18-20: https://www.akamai.com/us/en/multimedia/documents/report/akamai-research-consumer-attitudes-toward-data-privacy.pdf

Εικόνα 21: https://blogs.microsoft.com/on-the-issues/2019/05/20/gdprs-first-anniversary-a-year-of-progress-in-privacy-protection/