ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΛΟΠΟΝΝΗΣΟΥ
ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ
ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΘΕΜΑ: Μεθοδολογία, ανάλυση και εφαρμογή GDPR

ΣΠΟΥΔΑΣΤΡΙΑ: Αντωνοπούλου Αικατερίνη (3088)

ΕΠΟΠΤΕΥΩΝ ΚΑΘΗΓΗΤΗΣ: Τριανταφυλλου Βασίλειος

ΠΑΤΡΑ 2021

UNIVERSITY OF THE PELOPONNESE
SCHOOL OF ENGINEERING
DEPARTMENT OF ELECTRICAL
AND COMPUTER ENGINEERING

DIPLOMA THESIS

Tittle: Methodologies, analysis and application of GDPR

Student: Antwnopoulou Aikaterini (3088)

Supervisor: Triantafillou Vasileios

Patra, 2021

Ευχαριστίες

Αρχικά θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή τον κ. Τριανταφύλλου Βασίλη για την πολύτιμη βοήθεια που μου παρείχε κατά την διάρκεια της εκπόνησης της διπλωματικής μου εργασίας.
Επίσης θα ήθελα να ευχαριστήσω την οικογένεια μου για την στήριξη τα χρόνια των σπουδών μου.

Πίνακας περιεχομένων

ΠΕΡΙΛΗΨΗ

Εξαιτίας της διακρατικής μεταφοράς δεδομένων χρειάστηκε η Ευρωπαϊκή Ένωση να θεσπίσει την οδηγία 95/46/ΕΚ και στην συνέχεια ένα νόμο τον οποίο έπρεπε να τηρεί κάθε εταιρία η οποία επεξεργάζεται δεδομένα Ευρωπαίων πολιτών. Αυτός ο νόμος ονομάστηκε Γενικός Κανονισμός Προστασίας Δεδομένων GDPR ο οποίος τέθηκε σε εφαρμογή στις 25 Μαΐου 2018.

Σκοπός αυτής της διπλωματικής εργασίας είναι να αναλύσει τον ΓΚΠΔ περιγράφοντας το χρονικό ιστορικό καθώς και την αρχή καταχώρησης προσωπικών δεδομένων. Αναλύονται όροι όπως τι είναι προσωπικά δεδομένα, ποιος είναι ο υπεύθυνος επεξεργασίας προσωπικών δεδομένων, τι είναι εποπτική αρχή και τι είναι η αρχή προστασίας δεδομένων αλλά και ποιες είναι οι αρμοδιότητες τους.

Στην συνέχεια της εργασίας περιγράφονται οι Ευρωπαϊκές οδηγίες όπου θέσπισε η ΕΕ ,σε αρχικό στάδιο πριν προχωρήσει στον υποχρεωτικό νόμο, αναλύοντας τις διατάξεις και τα άρθρα που περιλαμβάνει καθώς και το νομοθετικό πλαίσιο και την ελληνική νομοθεσία .

Αναλύεται η δομή του Γενικού Κανονισμού για την προστασία των δεδομένων και τις βασικές αρχές που το διέπουν. Περιλαμβάνει τα δικαιώματα των υποκειμένων και τις υποχρεώσεις του Υπεύθυνου Επεξεργασίας Δεδομένων . Αναφέρει την έννοια του Risk Assesment, τις φάσεις της Εκτίμησης Αντίκτυπου στην Προστασία δεδομένων και την Συγκατάθεση του Υποκειμένου δεδομένων

Περιγράφει με αναλυτικό τρόπο ποια είναι τα τεχνικά και οργανωτικά μέτρα και τονίζει την σημαντικότητα τους. Στην συνέχεια ενημερώνει για την αρχή επιβολής κυρώσεων και πραγματοποίηση ελέγχων και τα πρόστιμα που ακολουθούν.

Έπειτα, δίνεται ιδιαίτερη έμφαση στις διαβιβάσεις δεδομένων σε χώρες που δεν ανήκουν στην ΕΕ στις λεγόμενες τρίτες χώρες

Εν κατακλείδι, περιγράφονται τα βήμα που πρέπει να ακολουθήσει η κάθε εταιρία για να αποκτήσει συμμόρφωση στον ΓΚΠΔ

ABSTRACT

Due to the transnational data transfer, it deemed necessary for the European Union to adopt Directive 95/46/EC and then a law that had to be adhered by every company that processes European citizens' data. This law was named the General Data Protection Regulation- GDPR which was implemented as the principle of registration of personal data.

The purpose of this diploma thesis is to analyze the GDPR by describing the history as well as the principle of registration of personal data. Terms such as personal data, who is responsible for

processing personal data, what is a supervisory authority and what is a data protection authority, but also what are their responsibilities are analyzed.

Additionally, the European directives adopted by the EU, at an early stage before proceeding to the mandatory law is described, analyzing the provisions and articles it contains as well as the legal framework and the Greek legislation.

The structure of the General Regulation for data protection and the basics principles that govern it are analyzed.

It concludes the rights of the subjects and the obligations of the Data Protection Officer.

Names the concept of Risk Assesment, the phases of Impact Assesment in Data Protection and the Consent of the Data Subject.

Describes in detail what the technical and organizational measures are and emphasizes their importance.

It then notifies the authorities to impose sanctions and carry out audits and the fines that follow.

Next, special emphasis is given on data transfers to non-EU countries in the so-called third countries.

In conclusion, the steps that each company must follow to achieve compliance with the GDPR are described.

Κεφάλαιο 1

1.1 Ιστορικό

Σύμφωνα με τον δικηγόρο Αποστολόπουλο (2020)[26] πολλές χώρες της Ευρώπης θέσπισαν την ιδιωτικότητα των δεδομένων και την αποδοχή του δικαιώματος του πολίτη να μπορεί να αποφασίζει αυτοδύναμα για τα στοιχεία με τα οποία σχετίζεται ο ίδιος . Η συνθήκη αυτή ώθησε πολλές επικράτειες στην ενστέρνιση νομοθεσιών που στοχεύουν στην υπεράσπιση των ατόμων στην μη πληρωδοτημένη είσοδο στα ιδιωτικά τους στοιχεία από τους διάφορους φορείς.

Η ιδέα της φύλαξης των προσωπικών στοιχείων στις Ευρωπαϊκές χώρες ξεκίνησε από την Γερμανία το 1970 η οποία συμβουλεύτηκε τους ήδη υπάρχον νόμους . Η χώρα αυτή παρουσίασε μια καινοτόμα νομοθεσία για την φύλαξη ιδιωτικότητας με την εγκόλπωση ενός διατάγματος με την ονομασία Κρατικός Νόμος Προστασίας Δεδομένων(State Data Protection Act) δίχως όμως την ύπαρξη πληροφοριών για τα προσωπικά δεδομένα παρόλα αυτά έδωσε το δικαίωμα για μερικά προνόμια σε άτομα καθώς και δέσμευσε όσους εργάζονται στην επεξεργασία δεδομένων.

1.2 Πως ξεκίνησε η ιστορία για την καταχώρηση προσωπικών δεδομένων

Στην μελέτη του ο Αποστολόπουλος συνεχίζει λέγοντας πως αυτή η καινοτομία υιοθετήθηκε και από άλλες χώρες της Ευρώπης ένα από αυτά είναι το Γερμανικό Ομοσπονδιακό Θέσπισμα Προστασίας Δεδομένων το 1977 (German Federal Data Protection Act of 1977).

Μολονότι αυτός ο νόμος θεσπίστηκε με σκοπό να προστατεύει την ιδιωτικότητα των πληροφοριών είχε ως αντίκτυπο στην εξελισσόμενη " οικονομία της πληροφορίας" . Καθώς υπήρχε η πρόκληση από κάποιους φορείς που είχαν την δυνατότητα να έχουν πρόσβαση σε εδάφη όπου επιθεωρούσαν την φύλαξη των πληροφοριών στην μετατροπή τους σε " παραδείσους δεδομένων" . Αυτή η διαδικασία έχει ως επακόλουθο την μη ορθή τήρηση του νόμου σε χώρες όπου είχαν πιο τελεσφόρα αποτελέσματα στον συγκεκριμένο νόμο.

Παράλληλα κατέβαλε ο πανικός πως οι χώρες με τους πιο απαιτητικούς και αυστηρούς ελέγχους θα φέρει ενδεχομένως νέα μέτρα με τα οποία θα μπορούν να αυξήσουν ακόμα περισσότερο την ανάσχεση των ελέγχων. Ως αποτέλεσμα θα είχε την μείωση στην μετακίνηση των πληροφοριών σε τρίτες χώρες εμποδίζοντας την άφθονη μετακίνηση των δεδομένων .

Όντως πολλά κράτη με την μη ακολουθία νόμου περί ασφάλειας των πληροφοριών ακόμα και τα κυβερνώντα κράτη στον χώρο της επιστήμης των δεδομένων , όπως η ΗΠΑ, έκριναν τα μέτρα για την μείωση της μετακίνησης της πληροφορίας από χώρα σε χώρα ακραία περιοριστικά και διασφαλιστικά . Αυτή η κατάσταση κατεύθυνε σε πολλά διακρατικά εγχειρήματα με την αποδοχή και εκούσιων αλλά και υποχρεωτικών λειτουργιών με στόχο να βοηθήσουν στο επίτευγμα ενός θεμελιώδες επιπέδου φύλαξης των προνομίων των ανθρώπων στα προσωπικά δεδομένα με τα οποία σχετίζονται όμως και για να συμβάλλουν στην αποφυγή θέσπισης των λεγόμενων "παραδείσων δεδομένων".

Συνεπώς, την δεκαετία του ‘80 διαμορφώθηκε ο Οργανισμός για την Οικονομική Συνεργασία και Ανάπτυξη (Organisation for Economic Co-operation and Development’s Recommendations of the Council- ‘OECD’) , έχοντας ως στόχο την στήριξη των κρατών της Ευρώπης στην οργάνωση της “οικονομικής και κοινωνικής” δραστηριοποίησης . Αρχικός σχετιζόταν με την επέκταση της ανάπτυξης της οικονομίας. Παράλληλα, ο συγκεκριμένος φορέας υπέδειξε και μια συλλογή από επτά κανονισμούς χωρίς όμως να υποχρεώνει τις “Κατευθυντήριες Γραμμές” για την φύλαξη των προσωπικών στοιχείων και την διακρατική μετακίνηση ιδιωτικών πληροφορίών (non-binding OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data).

Αυτοί οι κανονισμοί ανέφεραν μια ακολουθία από θεμελιώδης έννοιες που οι χώρες θα έπρεπε να αποδεχτούν ώστε να προφυλάξουν τους κατοίκους τους συγκριτικά με την εκμετάλλευση των δεδομένων τους. Σαν βασική ιδέα, προβάλλει , την αναγκαιότητα της εξασφάλισης των προσωπικών δεδομένων στην ελεύθερη μετακίνηση πληροφορίας αλλά και στην υιοθέτηση νόμων στις χώρες.

Εντούτοις, ήταν αναγκαία προϋπόθεση της ελάττωσης του στόχου που με αυτήν η χρησιμοποίηση των προσωπικών δεδομένων θα πρέπει να κινείται ανάμεσα στους “ ρητούς σκοπούς”(express purposes)

Αυτές οι “Κατευθυντήριες Γραμμές” τροποποιήθηκαν το 2013

Παράλληλα, το Ευρωπαϊκό συμβούλιο ενέκρινε την Σύμβαση No. 108 στις 28.01.1981 για την Προστασία των Φυσικών Προσώπων σχετικά με την Αυτόματη Επεξεργασία των Προσωπικών Δεδομένων (1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data).

Εντούτοις, η συγκεκριμένη Σύμβαση συντέλεσε μια “Διεθνή Σύμβαση” με σκοπό να θέσει τις βάσεις για μια υποχρεωτική νομοθεσία που θα προστάτευε τα προσωπικά δεδομένα.

Στο πέμπτο άρθρο της , περιγράφει ότι η επεξεργασία των πληροφοριών θα πρέπει να είναι νόμιμη. Ως διαμοιβή δεν θα επηρεάζεται η “ελεύθερη κυκλοφορία” στις χώρες.

Τέλος ο μελετητής αναφέρει πως η ενστέρνιση του Ενιαίου Ευρωπαϊκού θεσπίσματος το 1986 (Single European Act 1986) είχε ως σκοπό “ενιαία Ευρωπαϊκή αγορά” καταλήγοντας σε μια νομοθεσία Οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (Directive 95/46/EC). Αυτή η Οδηγία τοποθέτησε ένα δειξοδικό νομοσχέδιο για την φύλαξη ιδιωτικών πληροφοριών.

1.3 Ορισμοί

- **Προσωπικά δεδομένα [7] :**

Ο όρος προσωπικά δεδομένα είναι η αφετηρία του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR). Είναι οποιαδήποτε πληροφορία που σχετίζεται με φυσικό πρόσωπο που έχει ταυτοποιηθεί ή πρόκειται να ταυτοποιηθεί

Τα δεδομένα αυτά μπορεί να περιλαμβάνουν:

- όνομα
- στοιχεία κατοικίας
- στοιχεία ταυτότητας
- IP

- **Επεξεργασία [7]:**

Κάθε δραστηριότητα ή μια ομάδα δραστηριοτήτων που επιτελούνται σε προσωπικά δεδομένα είτε αυτόματα είτε όχι, όπως είναι η συλλογή, η καταγραφή, η οργάνωση, η δομή, η αποθήκευση, η προσαρμογή, η τροποποίηση, η διαγραφή και η καταστροφή.

- **Δεσμευτικοί εταιρικοί κανόνες**

Οι δεσμευτικοί εταιρικοί κανόνες (Binding Corporate Rules BCRs) αποτελεί το σύνολο των εσωτερικών κανόνων που εγκρίθηκε από πολυεθνικές επιχειρήσεις για να καθορίσουν τις παγκόσμιες πολιτικές τους για τις διεθνείς μεταφορές δεδομένων εντός του ίδιου εταιρικού ομίλου προς χώρες που δεν μοιράζονται το ίδιο επίπεδο προστασίας.

- **Περιορισμός επεξεργασίας [7] :**

Είναι η σήμανση των αποθηκευμένων προσωπικών στοιχείων με στόχο τον περιορισμό της επεξεργασίας τους στο μέλλον.

- **Εκτελών την επεξεργασίας[7]:**

Ο Ελεγκτής δεδομένων (Data Protection Act -DPA) καθορίζει τον λόγο και τον τρόπο με τον οποίο θα πραγματοποιηθεί η επεξεργασία δεδομένων . Αυτός που ορίζει έναν ελεγκτή μπορεί να είναι να είναι ένα άτομο ή η απόφαση να οριστεί από μια ομάδα ατόμων

- **Επεξεργαστής δεδομένων [7]:**

Ο επεξεργαστής δεδομένων επεξεργάζεται τα δεδομένα που παίρνει από τον ελεγκτή δεδομένων. Σε αντίθεση με τον DPA, το GDPR εισάγει συγκεκριμένες ευθύνες στον Επεξεργαστή. Αυτά είναι τα τρίτα μέρη που επεξεργάζονται δεδομένα για λογαριασμό του ελεγκτή δεδομένων και περιλαμβάνει παρόχους υπηρεσιών πληροφορικής.

- **Εποπτική Αρχή Προστασίας Δεδομένων:**

Η Εποπτική Αρχή Προστασίας Δεδομένων (ΕΑΠΔ ή Data Protection Impact Assessment (DPIA)) είναι απαραίτητη στον Κανονισμό επειδή υπάρχουν μεγάλες πιθανότητες υψηλού κινδύνου για τα προσωπικά δεδομένα των ατόμων

- **Υπεύθυνος Επεξεργασίας Δεδομένων:**

Σύμφωνα με τον Κανονισμό οι υπεύθυνοι επεξεργασίας δεδομένων και επεξεργαστές δεδομένων είναι απαραίτητο να θέσουν ένα στέλεχος ο οποίος επιβλέπει την προστασία δεδομένων. Αυτό το στέλεχος ονομάζεται Υπεύθυνος Επεξεργασίας Δεδομένων (Data Protection Officer -DPO)

Ο υπεύθυνος Προστασίας Δεδομένων είναι κάποιος που έχει επίσημα ευθύνη για τη συμμόρφωση με την προστασία δεδομένων εντός μιας επιχείρησης. Η επιχείρηση δεν είναι υποχρεωμένη να ορίσει έναν υπεύθυνο επεξεργασίας δεδομένων, έχει την υποχρέωση να το κάνει ότι ισχύουν τα παρακάτω:

- Ο οργανισμός να είναι δημόσια αρχή, ή
- Διενεργεί μεγάλης κλίμακας συστηματική παρακολούθηση ατόμων , ή
- Πραγματοποιείτε μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων ή δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα.

- **Αρχή Προστασίας Δεδομένων:**

Η αρχή Προστασίας δεδομένων (Data Protection Authority - DPA) είναι ο φορέας που προστατεύει το απόρρητο των δεδομένων των υποκειμένων και επιβάλλει τον Γενικό κανονισμό. Έχει δικαιοδοσία στις χώρες να επιβάλει τη συμμόρφωση με τον Κανονισμό και να επιβάλλει κυρώσεις σε οργανισμούς που αποτυγχάνουν να συμμορφωθούν. Είναι επίσης ο οργανισμός που εκπροσωπεί την εκάστοτε χώρα στο Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων.

- **Υποκείμενα Δεδομένων:**

Με τον όρο υποκείμενα δεδομένων στο Κανονισμό αναφέρεται στο άτομο στο οποίο τα δεδομένα συλλέγονται. Τα υποκείμενα δεδομένων μπορεί να είναι πελάτες μιας εταιρία, εργολάβοι, πωλητές και εργαζόμενοι.

- **Παραβίαση Προσωπικών Δεδομένων [7]:**

Ως παραβίαση προσωπικών δεδομένων νοείται η παραβίαση ασφάλειας που καταλήγει σε τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, μη επιτρεπτή αποκάλυψη ή πρόσβαση σε ιδιωτικά στοιχεία. Αυτό περιέχει παραβιάσεις που είναι επακόλουθα είτε τυχαίων αιτιών είτε εσκεμμένων. Όμως μια παραβίαση μπορεί να είναι κάτι πολύ παραπάνω από απώλεια δεδομένων.

- **Ψευδώνυμα δεδομένα [7]:**

Κάποιες ομάδες δεδομένων μπορούν να τροποποιηθούν με τέτοιο τρόπο ώστε να μην μπορούν τα άτομα να αναγνωριστούν από αυτά τα δεδομένα (είτε άμεσα είτε έμμεσα) χωρίς το κλειδί όπου μπορεί να αναγνωρίσει αυτά τα δεδομένα.

- **Διασυνοριακή επεξεργασία**

Αποτελεί την επεξεργασία των προσωπικών δεδομένων όταν ο υπεύθυνος επεξεργασίας είναι εγκατεστημένος σε παραπάνω από ένα κράτη ή η επεξεργασία δεδομένων πραγματοποιείται σε παραπάνω από ένα κράτη

- **Ευαίσθητα Προσωπικά Δεδομένα[18]**

Αποτελείται από μια ομάδα συγκεκριμένων κατηγοριών που πρέπει να αντιμετωπίζονται με επιπρόσθετη ασφάλεια. Περιέχουν στοιχεία σχετικά με:

  - Φυλετική ή εθνοτική καταγωγή
  - Πολιτικές απόψεις
  - Θρησκευτικές ή φιλοσοφικές πεποιθήσεις
  - Συνδικαλιστική ιδιότητα
  - Γενετικά δεδομένα
  - Βιομετρικά δεδομένα

- **Γενετικά Δεδομένα [7]:**

Τα δεδομένα αυτά θεωρούνται τα προσωπικά δεδομένα που σχετίζονται με τα κληρονομικά ή αποκτηθέντα γενετικά χαρακτηριστικά ενός ατόμου τα οποία περιλαμβάνουν πληροφορίες σχετικά με την φυσιολογία ή την υγεία αυτού του ατόμου και έχουν ανακληθεί από την ανάλυση ενός βιολογικού δείγματος του ατόμου.

- **Βιομετρικά Δεδομένα[7]:**

Τα δεδομένα αυτά έχουν ληφθεί χρησιμοποιώντας συγκεκριμένους τρόπους που αφορούν τα φυσικά, φυσιολογικά ή συμπεριφορικά χαρακτηριστικά του ατόμου. Αυτά τα δεδομένα επιτρέπουν ή επιβεβαιώνουν την μοναδική ταυτότητα του ατόμου.

- **Δεδομένα Υγείας [7]:**

Θεωρούμε τα δεδομένα μου ασχολούνται με την σωματική ή ψυχική υγεία ενός ατόμου. Περιέχει τις υπηρεσίες παροχής υγείας και μέσω αυτών μπορεί να παρθούν στοιχεία που αφορούν την υγεία του ατόμου.

Κεφάλαιο 2

2.1 Ευρωπαϊκές οδηγίες

Η Ευρωπαϊκή Ένωση αποδέχτηκε την φύλαξη των ιδιωτικών στοιχείων των φυσικών προσώπων τον 20ου αιώνα ως ένα αναγκαίο προνόμιο των πολιτών της. Όπως είδαμε και στην αρχή οι κανόνες που τέθηκαν αφορούσαν όλη την Ευρώπη και όχι τα κράτη μεμονωμένα καθώς η μετακίνηση των δεδομένων ήταν διακρατική.

Λόγω του ότι η Σύμβαση No. 108 επεξεργαζόταν μηχανικά τις πληροφορίες χωρίς όμως να εξασφαλίζει την απόλυτη προστασία των πολιτών με την έλλειψη πρωτοκόλλων ασφάλειας η Ευρωπαϊκή επιτροπή θέλοντας να διορθώσει τις ατέλειες της Σύμβασης No. 108 κατασκεύασε την Οδηγία 95/46/ΕΚ. Η συγκεκριμένη σύμβαση έχει παραπομπές και από τη "Σύμβαση του Συμβουλίου της Ευρώπης 1981" αλλά και από την "Ευρωπαϊκή Σύμβαση των Δικαιωμάτων του Ανθρώπου" σεβόμενο τα δικαιώματα και τις ελευθερίες των ανθρώπων, τονίζοντας το πόσο σημαντικό είναι το προνόμιο της μυστικότητας των στοιχείων των ατόμων.

Παρ' όλα αυτά όλα τα μέλη της Ευρώπης ακολούθησαν διαφορετικά μερικές περιπτώσεις, υποδεικνύοντας πως θα έπρεπε να γίνουν κάποιες διορθώσεις.

Αυτές οι οδηγίες σύμφωνα με Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 αναφέρονται παρακάτω σε κεφάλαια (lawspot.gr)[21]:

Κεφάλαιο 1: Γενικές διατάξεις

Άρθρο 1 – Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 – Στόχος της οδηγίας

Άρθρο 2 – Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 – Ορισμοί

Άρθρο 3 – Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 – Πεδίο Εφαρμογής

Άρθρο 4 – Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 – Εφαρμοστέο εθνικό δίκαιο

Κεφάλαιο 2: Γενικές προϋποθέσεις σχετικά με την θεμιτή επεξεργασία δεδομένων προσωπικού χαρακτήρα

Άρθρο 5 – Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995

ΤΜΗΜΑ 1: Αρχές που πρέπει να τηρούνται ως προς την ποιότητα των δεδομένων

Άρθρο 6 – Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995

ΤΜΗΜΑ 2: Βασικές αρχές την νομικής επεξεργασίας δεδομένων

Άρθρο 7 – Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995

ΤΜΗΜΑ 3: Ειδικές κατηγορίες επεξεργασίας

Άρθρο 8 – Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 – Επεξεργασία Ειδικών Κατηγοριών

Άρθρο 9 – Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 – Επεξεργασία δεδομένων προσωπικού Χαρακτήρα και ελευθερία έκφρασης

ΤΜΗΜΑ 4: Ενημέρωση του ενδιαφερόμενου προσώπου

Άρθρο 10 – Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 – Ενημέρωση σε περίπτωση συλλογής δεδομένων από το πρόσωπο στο οποίο ενδιαφέρονται

Άρθρο 11 – Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 – Ενημέρωση σε περίπτωση συλλογής δεδομένων όχι από το πρόσωπο στο οποίο ενδιαφέρονται

ΤΜΗΜΑ 5: Δικαίωμα πρόσβασης του προσώπου στο οποίο αναφέρονται τα δεδομένα

Άρθρο 12 – Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 – Δικαίωμα πρόσβασης

ΤΜΗΜΑ 6: Εξαιρέσεις και περιορισμοί

Άρθρο 13 – Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 – Εξαιρέσεις και περιορισμοί

ΤΜΗΜΑ 7: Δικαίωμα αντίταξης του προσώπου στο οποίο αναφέρονται τα δεδομένα

Άρθρο 14 – Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 – Δικαίωμα αντίταξης του προσώπου στο οποίο αναφέρονται τα δεδομένα

Άρθρο 15 – Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 – Αυτοματοποιημένες ατομικές αποφάσεις

Άρθρο 16 – Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 – Απόρρητο της επεξεργασίας

Άρθρο 17 – Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 – Ασφάλεια της επεξεργασίας

ΤΜΗΜΑ 9: Κοινοποίηση

Άρθρο 18 – Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 – Η υποχρέωση κοινοποίησης προς την αρχή ελέγχου

Άρθρο 19 – Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 – Περιεχόμενο της κοινοποίησης

Άρθρο 20 – Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 – Προηγούμενοι έλεγχοι

Άρθρο 21 – Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 – Δημοσιότητα των επεξεργασιών

- **Κεφάλαιο 3: Ένδικα μέσα, Ευθύνη και Κυρώσεις**

  Άρθρο 22 – Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 – Προσφυγή

  Άρθρο 23 – Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 – Ευθύνη

  Άρθρο 24 – Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 – Κυρώσεις

- **Κεφάλαιο 4: Διαβίβαση δεδομένων προσωπικού χαρακτήρα προς τρίτες χώρες**

Άρθρο 25 – Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 - Βασικές αρχές

Άρθρο 26 – Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 – Παρεκκλίσεις

- **Κεφάλαιο 5:Κώδικες δεοντολογίας**

  Άρθρο 27 – Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 –
- **Κεφάλαιο 5:Αρχή ελέγχου και ομάδα για την προστασία των προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα**

  Άρθρο 28 – Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 – Αρχή ελέγχου

  Άρθρο 29 – Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 – Ομάδα προστασίας των προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα

  Άρθρο 30 – Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995
- **Κεφάλαιο 6: Κοινοτικά μέτρα εκτέλεσης**

  Άρθρο 31 – Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 – Η επιτροπή

ΤΕΛΙΚΕΣ ΔΙΑΤΑΞΕΙΣ:

Άρθρο 32 – Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995

Άρθρο 33 – Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995

Άρθρο 34 – Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995

2.3 Νομοθετικό πλαίσιο

Η νομοθετική εξασφάλιση της διαφύλαξης των προσωπικών δεδομένων καθώς και η διαβεβαίωση της θεμιτής επεξεργασίας από τις κυβερνήσεις αλλά και από τους οργανισμούς έφερε σαν αποτέλεσμα την έναρξη μία νέας εποχής, της πληροφορίας και ψηφιακής πραγματικότητας.

Ως νομοθετικό πλαίσιο επικράτησε η σύμβαση No. 108 όμως μετά την σύσταση της Ευρωπαϊκής ένωσης, δημιουργήθηκε η ανάγκη για αρμονία στους νόμους καθώς πλέον οι διακρατικές σχέσεις αυξήθηκαν. Γι' αυτό τον λόγο ήταν αναγκαίο να βρεθεί μια προσέγγιση που θα έφερνε ομόνοια στους νόμους περί φύλαξης προσωπικών δεδομένων στα κράτη μέλη.

Η οδηγία 95/46/ΕΚ έδωσε λύση στο πρόβλημα αυτό θεσπίζοντας ουσιώδες αρχές που αφορούσαν την επεξεργασία των πληροφοριών, τα δικαιώματα των φυσικών προσώπων. Συνοπτικά τόνισε την αναγκαιότητα της σύστασης ομάδων με σκοπό την επίβλεψη της υπεράσπισης των ανθρώπων.

2.4 Ελληνική νομοθεσία

Η επίκουρος καθηγήτρια του Πανεπιστημίου Αιγαίου Λίλιαν Μήτρου περιγράφει την ελληνική νομοθεσία και υποστηρίζει πως η ελληνική νομοθεσία συμβαδίζει με την Ευρωπαϊκή νομοθεσία[17] .

Η αρχική προσπάθεια για την φύλαξη των ιδιωτικών στοιχείων των φυσικών προσώπων έγινε από την επιτροπή Χαλαζωνίτη το 1985. Η συγκεκριμένη επιτροπή επισήμανε τα "υπερευαίσθητα δεδομένα"

Έπειτα, από το 1989 έως το 1992, το Υπουργείο Δικαιοσύνης εισηγήθηκε νέες προτάσεις όμως όλες απορρίφθηκαν.

Το 1992 υλοποιείται η Κύρωση της Ευρωπαϊκής Σύμβασης No. 108 παραλείποντας ωστόσο τα νομοθετικά μέτρα.

Το 1994 ένα νομοσχέδιο θέσπισε Επιτροπή υπό τον Μιχάλη Δεκλερή. Το συγκεκριμένο νομοσχέδιο διαμόρφωσε , λαμβάνοντας υπόψιν της Οδηγία του 1995, Επιτροπή με πρόεδρο το καθηγητή Ν. Αλιβιζάτου και μέλη τους Δρόσος, Μήτρου, Φαρμάκης, Μυλωνόπουλος και Μποτόπουλος.

Στο πλαίσιο της Ελλάδας θεμελιώδης κανονισμοί αναφέρονται οι παρακάτω:

- Αναγνώριση του νόμου 2472/97 που περιλαμβάνει την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα

- Αναβάθμιση του νόμου 2774/99 και 3471/06 που σχετίζεται με τις ηλεκτρονικές επικοινωνίες
- Αλλαγές στον νόμο 2472/97
- Διάδοση του κανονισμού περί προστασίας δεδομένων

Βασικά χαρακτηριστικά της νομοθεσίας:

- οι κανόνες είχαν κοινό χαρακτήρα
- Αύξηση στους μηχανισμούς ελέγχου
- Μέση λύση στη σχέση διακαιώματα και συμφέροντα

Ο Στέφανος Μήτσιος στον άρθρο του με τίτλο "Law 4624/2019: Protection of Personal Data and Measures for the Implementation of the GDPR" [1] αναλύει τον νόμο 4624/2019 ο οποίος τέθηκε σε εφαρμογή στις 29/9/2019 τέθηκε με βάση τον οποίο θεσπίζει συμπληρωματικά μέτρα για την εφαρμογή του Γενικού Κανονισμού Προστασίας δεδομένων (GDPR) και προσθέτει την οδηγία 2016/680 ο οποίο δημοσιεύτηκε στην Εφημερίδα της Κυβέρνησης Ο νόμος αυτών συμπληρώνει τις διατάξεις του GDPR και προσθέτει και προσθέτει την οδηγία 2016/680 του Ευρωπαϊκού Κοινοβουλίου (Οδηγία LED). Ο καινούργιος νόμος περιέχει διατάξεις σε συγκεκριμένους τομείς που επιτρέπει ο κανονισμός οι χώρες της Ευρώπης να έχουν δική τους κρίση και καταστρέφει την νομική αβεβαιότητα που δημιουργείται από την καθυστερημένη συμπλήρωση του νόμου. Ο νόμος ακυρώνει τον προηγούμενο νόμο 2472/1997

Δομή:

Ο καινούργιος νόμος ολοκληρώνει τον Γενικό Κανονισμό σε μια σειρά τομέων Ο Α τομέας του νόμου ορίζει τον στόχο και το πεδίο εφαρμογής του, τους ορισμούς των δημόσιων και ιδιωτικών οντοτήτων και τον υποχρεωτικό ορισμό του υπευθύνου προστασίας δεδομένων σε δημόσιους φορείς. Το τμήμα Β περιλαμβάνει διατάξεις σχετικά με την οργάνωση και τη λειτουργία της Ελληνικής Αρχής Προστασίας Δεδομένων. Στον Γ τομέα εφαρμόζονται επιπρόσθετα μέτρα για την εφαρμογή του GDPR, ενώ το τμήμα Δ μεταφέρει την οδηγία LED στην ελληνική νομοθεσία.

Κύριες διατάξεις:

- Δημιουργία και λειτουργία της ΑΠΔΠΧ:

Η Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα(ΑΠΔΠΧ - Hellenic Data Protection Authority HDPA) επανέρχεται και δηλώνεται ως εποπτική αρχή στο Γενικό Κανονισμό.

- Συγκατάθεση ανηλίκων:

  Ο Γενικός Κανονισμός παρέχει αυξημένη προστασία στους ανήλικους όμως επιτρέπει στα κράτη να επιλέξουν τα ίδια την αύξηση της προστασίας. Τα δεδομένα ενός ανήλικου υποκείμενου θα επεξεργαστούν μόνο σε περίπτωση που είναι άνω των 15 ετών και έχει συναινέσει. Διαφορετικά θα κληθεί ο γονέας να δώσει συναίνεση.

- Επεξεργασία ειδικών κατηγοριών δεδομένων:

  Ο καινούργιος νόμος θεσπίζει ότι η επεξεργασία ειδικών κατηγοριών είτε από ιδιωτικούς είτε από δημόσιους οργανισμούς παρέχεται χωρίς την συναίνεση του ατόμου σε περιπτώσεις που αφορούν ιατρική και κοινωνική βοήθεια, Όμως η επεξεργασία γενετικών πληροφοριών είναι αυστηρά απαγορευμένη.

- Επεξεργασία για περαιτέρω σκοπούς:

  Η επεξεργασία προσωπικών πληροφοριών από δημόσιους οργανισμούς για λόγους διαφορετικούς από αυτούς που έχουν συλλεχθεί είναι αποδεκτό μόνο σε περιπτώσεις όπως η δίωξη εγκλημάτων ή για λόγους δημόσιας ασφάλειας. Επίσης η επεξεργασία από ιδιωτικούς οργανισμούς είναι αποδεκτό μόνο σε περιπτώσεις που θίγονται ζητήματα εθνικής άμυνας.

- Ειδικές καταστάσεις επεξεργασίας:

  Η επεξεργασία για λόγους δημοσιογραφίας, καλλιτεχνικούς, λογοτεχνικούς ή ακαδημαϊκούς παραχωρείται χωρίς συναίνεση του ατόμου όμως με την απαίτηση ότι το "δικαίωμα στην ιδιωτική ζωή" εξισώνεται από το " δικαίωμα στην ενημέρωση" .

- Εξαίρεση από την υποχρέωση ενημέρωσης:

  Ο υπεύθυνος επεξεργασίας απαλλάσσεται από το καθήκον της ενημέρωσης του υποκειμένου των δεδομένων όπως αναφέρει και ο ΓΚΠΔ στα άρθρα 13 και 14 σε συγκεκριμένες περιστάσεις για παράδειγμα αυτές που έβαζαν σε κίνδυνο την σωστή λειτουργία του Υπεύθυνου ή την δημόσια ασφάλεια.

- Επεξεργασία προσωπικών δεδομένων στο πλαίσιο απασχόλησης :

  Ο νέος νόμος έχει προσφέρει καινοτομίες έναντι του Γενικού Κανονισμού στο πλαίσιο της εργασίας. Ο εργοδότης έχει την δυνατότητα να επεξεργάζεται τα δεδομένα των υπαλλήλων του που σχετίζονται με την σύμβαση εργασίας τους. Όταν η επεξεργασία είναι εντός των

νομικών πλαισίων της συναίνεσης του εργαζόμενου τότε η ορθότητα της συναίνεσης κρίνεται ανάλογα με την σύμβαση εργασίας και τους όρους συγκατάθεσης. Οι κάμερες παρακολούθησης σε έναν επαγγελματικό χώρο είναι αναγκαίες μόνο για την προστασία προσώπων και αγαθών.

Κεφάλαιο 3

3.1 GDPR

Ο κανονισμός 2016/679 της Ευρωπαϊκής Ένωσης και του Συμβουλίου της 27ης Απριλίου σχετίζεται με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των προσωπικών δεδομένων με τα οποία σχετίζονται αλλά και την ελεύθερη μετακίνηση των πληροφοριών καθώς και την εξάλειψη της Οδηγίας 95/46/ΕΚ.

Κάθε επιχείρηση που βρίσκετε εντός των ορίων της Ευρωπαϊκής Ένωσης αλλά και στην περίπτωση που δεν βρίσκεται εντός ορίων αλλά ασχολείται με ιδιωτικά στοιχεία Ευρωπαίων πολιτών έχει νομικό καθήκον να ακολουθεί τον κανόνα του Γενικού Κανονισμού για την Προστασία Δεδομένων (GDPR) .

Το GDPR πρόκειται για ένα καινοτόμο νομοσχέδιο το οποίο διευθετεί την επεξεργασία ιδιωτικών στοιχείων που ανήκουν σε πολίτες της Ευρώπης από φορείς. Όμως δεν περιλαμβάνει επιχειρήσεις ή άλλα "νομικά πρόσωπα" καθώς και δεν συνδέεται με επαγγελματική ή οικιακή χρήση.

Θεωρείται ως μια απαραίτητη αναδιαμόρφωση του νομικού πλαισίου που σχετίζεται με την προφύλαξη των ατομικών στοιχείων αφού η προηγούμενη νομοθεσία είχε την αστοχία ως προς την ομοιοτυπία εφαρμογής του νόμου στις διάφορες χώρες της Ευρώπης έχοντας επιπτώσεις στις οικονομικές συναλλαγές.

Περιλαμβάνει δύο νομοθετικές πράξεις[25] :

- τον Γενικό κανονισμό προστασίας προσωπικών δεδομένων
- την Οδηγία προστασίας των δεδομένων στον τομέα επιβολής του νόμου 2016/680 η οποία αντικαθιστά την απόφαση πλαίσιο του 2008 για την προστασία των δεδομένων.

3.2 Γιατί χρειάζεται ένας κανονισμός;

Το GDPR παρουσίασε μια πολύ σημαντική διαφορά σε σχέση με την Οδηγία 95/46/ΕΚ που επικρατούσε μέχρι τότε , η διαφορά αυτή είναι πως η Ευρωπαϊκή Ένωση αποφάσισε να προβεί σε έναν κανονισμό και όχι σε μια Οδηγία[19].

Σύμφωνα με την Ευρωπαϊκή Ένωση "οι κανονισμοί είναι δεσμευτικές νομοθετικές πράξεις" καθώς και η υλοποίησή της στα κράτη μέλη είναι απαραίτητη.

Σε αντίθεση με τις Οδηγίες που αναφέρονται ως νομοθετικές πράξεις που καθιστούν έναν σκοπό που θέλουν να εκπληρώσουν.

3.4 Περιεχόμενα Κανονισμού

Οι δύο τομείς που ασκούν την μεγαλύτερη επιρροή στον Γενικό κανονισμό είναι η λογοδοσία και η επιβολή [28].

1. Λογοδοσία: Οι Οι οργανισμοί πρέπει να υιοθετήσουν τη νέα αρχή της λογοδοσίας που εισήχθη από τον GDPR και να περάσουν από τη «θεωρία στην πράξη» όσον αφορά τις προσπάθειές τους για την Προστασία Δεδομένων.
2. Επιβολή: Οι Αρχές Προστασίας Δεδομένων των κρατών μελών (DPA) πρέπει να επιβάλλουν αυστηρά τον Κανονισμό επιβάλλοντας ουσιαστικές κυρώσεις όταν οι οργανισμοί δεν μπορούν να αποδείξουν επαρκώς τη συμμόρφωση με την αρχή λογοδοσίας του GDPR.

Η αρχή της λογοδοσίας του ΓΚΠΔ

Η αναγνώριση ανάγκης της λογοδοσίας όσον αφορά το απόρρητο των δεδομένων δεν είναι νέα και μπορεί να φανεί στις κατευθυντήριες γραμμές για την προστασία της ιδιωτικής ζωής που εκδόθηκαν από τον Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ) το 1980. Η πρόθεση της νέας Αρχής λογοδοσίας GDPR είναι παρόμοια με αυτή των κατευθυντήριων γραμμών του ΟΟΣΑ για την προστασία της ιδιωτικής ζωής. Επιδιώκει να επιβεβαιώσει και να ενισχύσει την ευθύνη των Υπεύθυνων Επεξεργασίας και Επεξεργασίας Δεδομένων, σε σχέση με την Επεξεργασία των Προσωπικών Δεδομένων Ο Κανονισμός διέπετε από αρχές προστασίας δεδομένων που καταλήγουν στην συμμόρφωση. Αυτές οι αρχές αναλύουν τις υποχρεώσεις τις οποίες οι

επιχειρήσεις πρέπει να τηρούν όταν σχετίζονται με προσωπικά δεδομένα ατόμων. Ο κανονισμός ορίζει επτά βασικές αρχές οι οποίες ορίζονται στην αρχή της νομοθεσίας . Αυτές τις αρχές περιέγραψε ο Αραμπατζής Αναστάσιος στο άρθρο του "What are the 7 principles of GDPR" που δημοσιεύτηκε στις 27 Μαρτίου 2020 [5] και αναφέρεται στις εξής:

3.4.1 Νομιμότητα, δικαιοσύνη και διαφάνεια

Τα προσωπικά δεδομένα υποβάλλονται σε επεξεργασία η οποία είναι νόμιμη, δίκαιη και με διαφανή τρόπο σε σχέση με τα δεδομένα των ατόμων. Έτσι η επεξεργασία πραγματοποιείται μόνο όταν καλύπτεται από νομική άδεια ή από συναίνεση του ατόμου στο οποίο ανήκουν τα δεδομένα. Τα υποκείμενα θα πρέπει να μπορούν να καταλάβουν τι συμβαίνει στα προσωπικά τους δεδομένα. Για τον λόγο αυτό είναι αναγκαία η διαφάνεια η οποία απαιτεί:

- στοιχεία για τα υποκείμενα σχετικά με την ταυτότητα του υπεύθυνου επεξεργασίας
- στοιχεία για τα υποκείμενα σχετικά με τους σκοπούς επεξεργασίας
- επιπλέον στοιχεία σχετικά με τα υποκείμενα των δεδομένων και τα δικαιώματα τους να γνωρίζουν τις δραστηριότητες επεξεργασίας που έχουν υποστεί τα δεδομένα τους
- γνωστοποίηση των ατόμων σχετικά με τους κινδύνους, τους κανόνες, τις διασφαλίσεις και τα δικαιώματα τους σχετικά με την επεξεργασία.

Επιπροσθέτως οι σκοποί επεξεργασίας θα πρέπει να είναι σαφή, νόμιμοι και καθορισμένοι κατά την διάρκεια συλλογής από τα υποκείμενα δεδομένων.

3.4.2 Περιορισμός του σκοπού

Συλλέγονται για συγκεκριμένους νόμιμους σκοπούς και δεν υποβάλλονται σε επεξεργασία με τρόπους μη συμβατούς. Ο σκοπός επεξεργασίας δεδομένων συμβάλλει σημαντικά στις λειτουργίες του υπεύθυνου των δεδομένων

3.4.3 Ελαχιστοποίηση των δεδομένων

Τα δεδομένα είναι επαρκή, σχετικά και περιορίζονται στο αναγκαίο σε σχέση με τους σκοπούς επεξεργασίας. Δεν είναι απαραίτητη η ελαχιστοποίηση των δεδομένων στο ελάχιστο όμως είναι αναγκαία η ελαχιστοποίηση συλλογής δεδομένων σε ικανοποιητικό επίπεδο σχετικά με τους

σκοπούς επεξεργασίας. Με αποτέλεσμα να είναι απαραίτητη η εκτίμηση της αναλογικότητας των αναμενόμενων λειτουργιών επεξεργασίας. Οι φορείς θα πρέπει να προβληματιστούν αν τα στοιχεία που έχουν συσσωρευτεί είναι αναγκαία για την επίτευξη της επεξεργασίας.. Ανακεφαλαιώνοντας η ελαχιστοποίηση δεδομένων έχει ως σκοπό στην ελάττωση της συλλογής των δεδομένων όσο το δυνατόν για την ορθή επεξεργασία. Τα τεχνικά και οργανωτικά μέτρα πρέπει να εξασφαλίζουν την επίτευξη αυτής της αρχής.

3.4.4 Ακρίβεια

Τα δεδομένα πρέπει να είναι ακριβή και όταν είναι αναγκαίο ενημερωμένα, πρέπει να λαμβάνονται όλα τα νόμιμα μέτρα για να διασφαλιστεί ότι όλα τα ανακριβή δεδομένα διαγράφονται ή διορθώνονται χωρίς να υπάρξει καθυστέρηση. Καθώς τα προσωπικά δεδομένα αποδέχονται την ανοικοδόμηση στοιχείων ενός ατόμου θα πρέπει να είναι ακριβή για να επιτρέψουν αυτή την ανακατασκευή.

3.4.5 Περιορισμός αποθήκευσης

Τα δεδομένα πρέπει να τηρούνται σε μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων για όσο χρόνο χρειάζεται για την επεξεργασία των δεδομένων. Ακόμα κι αν συλλέγετε και χρησιμοποιείτε προσωπικά δεδομένα δίκαια και νόμιμα, δεν μπορείτε να τα διατηρήσετε για μεγαλύτερο χρονικό διάστημα από ότι απαιτείται. Για την διασφάλιση του περιορισμού θα πρέπει ορίζονται χρονικά περιθώρια από τον υπεύθυνο. Ο υπεύθυνος έχει την υποχρέωση να διαγράφει τα προσωπικά δεδομένα.

3.4.6 Ακεραιότητα και εμπιστευτικότητα

Τα προσωπικά δεδομένα υποβάλλονται σε επεξεργασία με τρόπο που εξασφαλίζει την ασφάλεια των δεδομένων. Συμπεριλαμβάνει και την μη εξουσιοδοτημένη ή παράνομη επεξεργασία και σε περίπτωση απώλειας ή καταστροφής χρησιμοποιούνται κατάλληλα μέσα και εργαλεία.

3.4.7 Ευθύνη

Ο υπεύθυνος έχει την ευθύνη να αποδείξει την συμμόρφωση με την παράγραφο 1

3.5 Δικαιώματα υποκειμένων

Το GDPR προσφέρει 8 δικαιώματα στους πολίτες της Ευρωπαϊκής Ένωσης τα οποία αναφέρονται στην σελίδα **Target Integration [33]** και είναι τα εξής:

3.5.1 Δικαίωμα ενημέρωσης

Το δικαίωμα ενημέρωσης επιτρέπει στα άτομα να ενημερώνονται για τη συλλογή και τη χρήση των προσωπικών τους δεδομένων. Σε περίπτωση που μια επιχείρηση έχει συλλέξει δεδομένα από κάποιους πολίτες θα πρέπει να τους ενημερώσει σχετικά με τον σκοπό επεξεργασίας προσωπικών δεδομένων τους.
Ο κανονισμός παρουσιάζει μια περιγραφή των επικοινωνιών με υποκείμενα δεδομένων σε διάφορους τομείς, όπως τα συμφέροντα τρίτων και τα δικαιώματα των υποκειμένων δεδομένων. Τα άτομα πρέπει να είναι σε θέση να επικοινωνήσουν με τον υπεύθυνο επεξεργασίας δεδομένων για τυχόν απορίες που μπορεί να έχουν.

3.5.2 Δικαίωμα πρόσβασης

Το GDPR αποσαφηνίζει ότι παρέχει σε ανθρώπους να έχουν πρόσβαση στα προσωπικά τους στοιχεία επειδή μπορούν να επιβεβαιώσουν την γνησιότητα της επεξεργασίας. Αυτό το προνόμιο το παρέχει η Ευρωπαϊκή Ένωση στους κατοίκους της με το δικαίωμα πρόσβασης στα προσωπικά τους στοιχεία που επεξεργάζονται.

3.5.3 Δικαίωμα διόρθωσης

Επιτρέπει στα άτομα να διορθώσουν τις ανακρίβειες πληροφορίες ή να συμπληρώνουν σε περίπτωση που κάτι είναι ελλιπείς. Ένα άτομο μπορεί να καταθέσει αίτημα διόρθωσης χωρίς καμία καθυστέρηση. Το προνόμιο αυτό συσχετίζεται με τις υποχρεώσεις του υπεύθυνου επεξεργασίας. Ένα αίτημα όμως μπορεί να μην το δεχτούν.

3.5.4 Δικαίωμα διαγραφής

Γνωστό και ως "δικαίωμα στο να ξεχαστεί". Η γενική αρχή εδώ είναι ότι ένα άτομο έχει το δικαίωμα να ζητήσει τη διαγραφή ή την αφαίρεση των προσωπικών του δεδομένων. Παρ' όλα αυτά υπάρχουν περιπτώσεις που τα δεδομένα δεν μπορούν να διαγραφούν μετά την κατάθεση αιτήματος. Για να επιτρέψουν την διαγραφή των προσωπικών στοιχείων τα άτομα που κάνουν αίτηση θα πρέπει να πληρούν κάποιες προϋποθέσεις.

3.5.5 Δικαίωμα περιορισμού και επεξεργασίας

Αυτό το δικαίωμα σχετίζεται με το δικαίωμα διόρθωσης και με το δικαίωμα διαγραφής. Τα άτομα έχουν το δικαίωμα να περιορίζουν την επεξεργασία των προσωπικών τους στοιχείων.

3.5.6 Δικαίωμα στη φορητότητα δεδομένων

Επιτρέπει στα άτομα να ζητούν την μεταφορά των δεδομένων τους ή να λαμβάνουν και να επαναχρησιμοποιούν προσωπικά τους δεδομένα για δικούς τους σκοπούς σε διαφορετικές επιχειρήσεις. Αυτό είναι ιδιαίτερα σημαντικό για τις επιχειρήσεις που εξετάζουν και συλλέγουν δεδομένα.

3.5.7 Δικαίωμα αντίρρησης

Το υποκείμενο έχει το δικαίωμα να μπορεί να αντισταθεί, πληρώντας κάποιες προϋποθέσεις, που σχετίζονται με την επεξεργασία των δεδομένων τους .

3.5.8 Δικαιώματα που σχετίζονται με την αυτοματοποιημένη λήψη αποφάσεων συμπεριλαμβανομένου του προφίλ

Αυτό το δικαίωμα είναι μια προστασία έναντι μιας ενδεχομένως καταστροφικής απόφασης που μπορεί να ληφθεί χωρίς ανθρώπινη παρέμβαση. Εάν η αυτοματοποιημένη απόφαση βασίζεται σε ρητή συγκατάθεση ή έχει εγκριθεί από το νόμο, τότε αυτό το δικαίωμα δεν ισχύει πλέον.

3.6Υποχρεώσεις Υπεύθυνου Επεξεργασίας Δεδομένων

Ο Γενικός κανονισμός ορίζει συγκεκριμένες υποχρεώσεις για τον Υπεύθυνο επεξεργασίας όπου με βάση με τον Δημήτρη Αναστασόπουλο όπως ανέλυσε στο άρθρο του "Οδηγός GDPR για δικηγόρους" [4] ο Υπεύθυνος επεξεργασίας :

- έχει καθήκον να χρησιμοποιεί κατάλληλα τεχνικά και οργανωτικά μέτρα με σκοπό να εξασφαλίσει την προστασία των δεδομένων που επεξεργάζεται και να φροντίζει ώστε τα μέτρα αυτά να επικαιροποιούνται,
- έχει καθήκον να τηρεί αρχείο δραστηριοτήτων για την επεξεργασία δεδομένων που γίνεται υπ' ευθύνη του, στο οποίο θα αναφέρονται όλες οι κατάλληλες πληροφορίες για την ταυτοποίηση του υπευθύνου επεξεργασίας και για τον τρόπο επεξεργασίας,
- έχει καθήκον να εκτελεί πριν από την επεξεργασία εκτίμηση αντικτύπου των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα, όταν ένα είδος επεξεργασίας, υπάρχει περίπτωση να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των ατόμων,
- από την στιγμή που τα αποτελέσματα της εκτίμησης αντικτύπου επισημάνουν ότι η επεξεργασία δεδομένων ενέχει υψηλό κίνδυνο παραβίασης, ο υπεύθυνος επεξεργασίας πρέπει να προχωρήσει σε προηγούμενη διαβούλευση με την εποπτική αρχή
- έχει καθήκον υπό συνθήκες να γνωστοποιεί κάθε παραβίαση δεδομένων προσωπικού χαρακτήρα στην κατάλληλη εποπτική αρχή και να την ανακοινώνει στο υποκείμενο των δεδομένων,
- έχει καθήκον να διορίζει Υπεύθυνο Προστασίας Δεδομένων (DPO) με την προϋπόθεση ότι η επεξεργασία πραγματοποιείται από δημόσια αρχή ή φορέα, προτείνεται σε συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε μεγάλη κλίμακα

3.7 Υποχρεώσεις οργανισμών και τρίτων

Ο Δεληγιάννης Θοδωρής στο άρθρο "Τι είναι ο «GDPR» και ποιες οι υποχρεώσεις των επιχειρήσεων" που δημοσιεύθηκε στις 6/12/2017 [34] υποστηρίζει πως οι επιχειρήσεις που συσχετίζονται με προσωπικά δεδομένα Ευρωπαίων πολιτών ή έχουν έδρα τους την Ευρώπη είναι υποχρεωμένοι να ακολουθούν τον Γενικό Κανονισμό για την Προστασία των Δεδομένων αλλά και να πράττουν διαρκείς ελέγχους αξιοπιστίας του δικτύου.

Ο κανονισμός αυτός ορίζει μια ακολουθία από καθήκοντα στους αρμόδιους φορείς. Στις επιχειρήσεις ορίζεται ένας Υπεύθυνος που αναλαμβάνει αυτά τα δεδομένα και ακολουθεί ένα αρχείο δραστηριοτήτων που αφορά την επεξεργασία τους. Τα αρχεία περιλαμβάνουν τα εξής:

- Επωνυμία και στοιχεία επικοινωνίας της επιχείρησης
- Τους λόγους για την επεξεργασία των δεδομένων
- Περιγραφή των κατηγοριών των υποκειμένων των δεδομένων και των προσωπικών δεδομένων
- Κατηγορίες των οργανισμών που λαμβάνουν τα δεδομένα
- Διαβίβαση δεδομένων σε άλλη χώρα ή οργανισμό
- Προθεσμία για αφαίρεση δεδομένων, εάν είναι δυνατό
- Περιγραφή των μέτρων ασφαλείας που χρησιμοποιούνται κατά την επεξεργασία, εάν είναι εφικτό

Παρόλο που η διαδικασία συμμόρφωσης φαίνεται αρκετά περίπλοκη στην πραγματικότητα μπορεί να προσφέρει προνόμια στις επιχειρήσεις και παρέχει κάποια θετικά αντίκτυπα
καθώς ο κανονισμός μπορεί να τις διευκολύνει σε μεγάλο βαθμό . Αυτά τα τα βασικά οφέλη ανέλυσε ο John Edwards στο TechTargrt.com (14 Ιανουαρίου 2012) [29] σε έξι κατηγορίες οι οποίες είναι οι εξής:

1. Ευκολότερη επιχειρηματική διαδικασία αυτοματοποίησης
2. Αυξημένη εμπιστοσύνη και αξιοπιστία
3. Καλύτερη κατανόηση των δεδομένων που συλλέγονται
4. Βελτιωμένη διαχείριση δεδομένων
5. Προστατευμένη και ενισχυμένη φήμη επιχείρησης και επωνυμίας
6. Ένας ισότιμος χώρος ανταγωνισμού

3.8 Συγκατάθεση Υποκειμένου

Ο Γενικός Κανονισμός επιβάλει μερικούς όρους με σκοπό η επεξεργασία των προσωπικών δεδομένων να διατηρούνται στα νόμιμα πλαίσια. Σύμφωνα με τις δικηγόρους Ζωή Βαλαέτη και Πολυτίμη Ξηνταράκου στο άρθρο τους που δημοσίευσαν στην ιστοσελίδα lawspot.gr [22] που

αναλύουν το άρθρο 6 του Κανονισμού αναφέρεται και η "συγκατάθεση του υποκειμένου στην επεξεργασία". Με τον όρο συγκατάθεση θεωρούμε πως το άτομο στο οποίο ανήκουν τα δεδομένα έχει συμφωνήσει πλήρως με την διαδικασία επεξεργασίας των δεδομένων του. Ο Κανονισμός παρέχει μια ακολουθία από όρους:

- Η συναίνεση θα προσφέρεται ελεύθερα, αυτό όμως σημαίνει πως το πρόσωπο που ανήκουν τα δεδομένα θα πρέπει να μπορεί σε περίπτωση που το επιθυμεί να απορρίψει την επεξεργασία. Για αυτό τον λόγο το υποκείμενο θα πρέπει να μπορεί να επιλέξει μόνο του χωρίς καμία παραπλάνηση ή προτροπή με αθέμιτους τρόπους από τρίτους.
- Το άτομο θα πρέπει να συναινέσει στην επεξεργασία των δεδομένων του με απόλυτη σαφήνεια ως προς τον τρόπο επεξεργασίας τους και όχι με έναν γενικό τρόπο. Με αποτέλεσμα η συναίνεση να δημιουργεί μια ομάδα από λειτουργίες επεξεργασίας . Το άτομο θα πρέπει να συναινέσει σε όλα τα μέρη της επεξεργασίας καθώς στην περίπτωση μίας "γενικής" συναίνεσης το άτομο να πιθανόν να μην γνωρίζει όλα τα μέρη της με αποτέλεσμα την μη συναίνεση του.
- Ο υπεύθυνος επεξεργασίας δεδομένων θα πρέπει να γνωστοποιήσει όλα τα αναγκαία στοιχεία για την επεξεργασία με απόλυτα ευανάγνωστο τρόπο. Επίσης το άτομο θα πρέπει να γνωρίζει την "ταυτότητα του υπεύθυνου επεξεργασίας" , το είδος της επεξεργασίας των δεδομένων αλλά και το προνόμιο αναθεώρησης της συγκατάθεσης.
- Το άτομο στο οποίο ανήκουν τα δεδομένα θα πρέπει να έχει δηλώσει με απόλυτα ευδιάκριτο και αντιληπτό την συναίνεση του, σε κάθε άλλη περίπτωση η συναίνεση δεν είναι έγκυρη.
- Η δήλωση συναίνεσης είναι υποχρεωτικό να προηγείται σε χρόνο από την επεξεργασία. Οπότε ο Υπεύθυνος θα πρέπει να έχει ετοιμάσει την δήλωση πριν την διαδικασία της επεξεργασίας.

3.9 Risk Assessment

Οι υπεύθυνοι επεξεργασίας έχουν την υποχρέωση να αξιολογούν τους κινδύνους που αφορούν την επεξεργασία προσωπικών δεδομένων κάθε φορά πριν πραγματοποιηθεί η επεξεργασία. Η εκτίμηση επικινδυνότητας (risk assessment) παρέχει την δυνατότητα στους υπεύθυνους επεξεργασίας να προγραμματίσουν τα μέτρα που πρέπει να έχουν πάρει για να ελέγχουν τους κινδύνους και να εξασφαλίζουν την κατάλληλη επεξεργασία των προσωπικών δεδομένων εκ των προτέρων. Οι υπεύθυνοι επεξεργασίας πρέπει επίσης να εξασφαλίζουν ότι οι αρχές προστασίας δεδομένων

αντιμετωπίζουν με αποτελεσματικό τρόπο τους κινδύνους που συνδέονται με την επεξεργασία δεδομένων.

3.10 Εκτίμηση Αντίκτυπου στην Προστασία Δεδομένων

Ο DPO Pierre Faller αναφέρθηκε στο άρθρο του "The obligations of controllers towards Data Protection Authorities according to GDPR" [13] ότι ο κανονισμός παρέχει ένα εργαλείο το οποίο το οποίο ονομάζεται Εκτίμηση Αντίκτυπου Προστασίας Δεδομένων ΕΑΠΔ (Data Protection Impact Assesment - DPIA) το οποίο αναφέρεται στο Άρθρο 35 του Κανονισμού. Το ΕΑΠΔ αποτελείται από μερικές φάσεις που η κάθε μια μελετάει μια συγκεκριμένη ιδιότητα της επεξεργασίας των δεδομένων. Εάν η ομάδα αξιολόγησης θεωρήσει πως χρειάζεται να δοθεί περισσότερος χρόνος στην επεξεργασία ελέγχων ή για να αναζητήσει και να μελετήσει απειλές κατά την επεξεργασία, τότε θα πρέπει να τους δοθεί καθώς τα διορθωτικά μέτρα θα είναι η έκβαση αυτών των ελέγχων. Ο κανονισμός ορίζει τα ελάχιστα στοιχεία που μπαίνουν στην διαδικασία της αξιολόγησης τα οποία ορίζονται σε 5 φάσεις τις οποίες ανέλυσε ο αρθρογράφος :

- **Φάση 1**: Είναι μια αναλυτική λίστα της επεξεργασίας των δεδομένων που περιέχει στοιχεία όπως τα δεδομένα που χρησιμοποιεί, τις πληροφορίες των ελεγκτών και των επεξεργαστών καθώς και την νομική βάση που χρησιμοποιείται στα δεδομένα.
- **Φάση 2**: Καθορίζει τους νομικούς ελέγχους και τους ελέγχους αντιμετώπισης κινδύνων που εφαρμόζονται μέχρι εκείνη την στιγμή. Αυτή η φάση περιέχει το τρέχον και το υπάρχον σύνολο μέτρων από νομική, τεχνική, φυσική και οργανωτική άποψη. Ο σκοπός είναι ο έλεγχος τυχόν κινδύνων που ενδέχεται να εντοπιστούν πριν από την εφαρμογή της επεξεργασίας δεδομένων.
- **Φάση 3**: Εκθέτει τις πηγές κινδύνου για την επεξεργασία δεδομένων. Θέτει το εξής ερώτημα: «Θα υποφέρει η επιχείρησή μου από αυτήν τη νέα επεξεργασία δεδομένων και αν ναι πού και πότε θα υποφέρει;» Η συγκεκριμένη φάση εστιάζει σε πιθανές παρεμβολές απορρήτου.
- **Φάση 4**: Σχετίζεται με την ανάλυση και καταγραφή πιθανών αρνητικών γεγονότων και απειλών κατά την επεξεργασία δεδομένων. Η διάκρισή του από τη Φάση 3 είναι ότι θα

επικεντρωθεί στα προσωπικά δεδομένα των υποκειμένων των δεδομένων και τις πιθανές επιπτώσεις της νέας επεξεργασίας σε αυτά τα δεδομένα.

- **Φάση 5**: Έχει την μορφή αναφοράς και συνοψίζει την ανάλυση, τους τρέχοντες ελέγχους, τους κινδύνους για την επιχείρησή σας και τις απειλές για τα προσωπικά δεδομένα. Η έκθεση καθορίζει τις επιλογές του οργανισμού για την αντιμετώπιση κάθε εντοπισμένου κινδύνου, απειλής και ελαττώματος. Αναφέρει εάν κάθε επιλογή θα είχε ως αποτέλεσμα την εξάλειψη, τη μείωση ή την αποδοχή του κινδύνου. Η αναφορά θα καταγραφεί, θα διατηρηθεί και θα παρουσιαστεί στους κύριους διαχειριστές του οργανισμού σας. Αυτοί οι διαχειριστές μπορούν επομένως να αποφασίσουν εάν έχουν ληφθεί ενέργειες ή πρέπει να ληφθούν και να παρακολουθήσουν αυτές τις ενέργειες. Τέτοιες αναφορές συμβάλλουν στη συμμόρφωσή σας με την αρχή λογοδοσίας του GDPR.

Κεφάλαιο 4

4.1Τεχνικά και οργανωτικά μέτρα

Σύμφωνα με το άρθρο του KNOW YOUR COMPLIANCE (Ιούνιος 2020) [20] αναλύει πως ο Γενικός Κανονισμός Προστασίας Δεδομένων τονίζει ιδιαίτερα τον σημαντικό ρόλο που κατέχουν τα Τεχνικά και Οργανωτικά μέτρα. Τα μέτρα αυτά αποτελούν αναγκαιότητα για την εξασφάλιση της επεξεργασίας,της αποφυγή παραβιάσεων,της διασφάλισης των απαραίτητων ελεγκτών της επεξεργασίας, τα αρχεία των δραστηριοτήτων της επεξεργασίας, το απόρρητο από τον σχεδιασμό, τα ισχυρά θεμέλια για την εξασφάλιση των δικαιωμάτων των δεδομένων καθώς και τους άλλους τρόπους. Συνεχίζοντας, τα Τεχνικά και οργανωτικά μέτρα στον Γενικό Κανονισμό είναι " οι λειτουργίες, τα βήματα, οι έλεγχοι, τα συστήματα, οι διαδικασίες και τα μέτρα " τα οποία λαμβάνονται για την εξασφάλιση και φύλαξη των "προσωπικών δεδομένων" που επεξεργάζονται οι φορείς.

Επιπροσθέτως, το άρθρο αναλύει πια είναι αυτά τα μέτρα τα οποία εξαρτώνται με το μέγεθος της εταιρείας αλλά και τις δραστηριότητες της επεξεργασίας καθώς υπάρχει ένα μεγάλο εύρος τεχνικών και οργανωτικών μέτρων που είναι ικανά να προσφέρουν προστασία και ασφάλεια των προσωπικών δεδομένων.

Στην συνέχεια ο αρθρογράφος παραθέτει αρχικά τα **Οργανωτικά μέτρα** τα οποία είναι τα μέτρα που μπορούν να ερμηνευτούν "ως η προσέγγιση που ακολουθεί ένας οργανισμός για την

αξιολόγηση, την ανάπτυξη και την εφαρμογή ελέγχων που προστατεύουν τις πληροφορίες και προστατεύουν τα προσωπικά δεδομένα". Είναι πιθανό να περιέχουν τα παρακάτω:

- Πολιτικές Ασφάλειας Πληροφοριών: Ως προϋπόθεση για το αντικείμενο και το περιεχόμενο είναι το μέγεθος του φορέα καθώς και το είδος των απασχολήσεων της επεξεργασίας.
- Επιχειρησιακή συνέχεια: Σε αντίθεση με πριν εδώ δεν έχει σημασία το μέγεθος του φορέα . Κάθε φορέας υποχρεούται να περιέχει πρωτόκολλα και μέτρα τα οποία θέτουν αντίγραφα ασφαλείας των προσωπικών δεδομένων και την εξασφάλιση ότι είναι εφικτό να συντηρηθούν και σε περίπτωση που κριθεί απαραίτητο να τα επαναφέρουν.
- Εκτίμηση κινδύνου: Αυτό το μέτρο δεν είναι υποχρεωτικό παρόλα αυτά μπορεί να αποτελέσει ένα τρομερά τελεσφόρο μέτρο στην μείωση δεδομένων υψηλού κινδύνου όμως σε κάποιους τομείς κρίνεται νομικά απαραίτητο.
- Πολιτικές και Διαδικασίες: Με την χρήση αυτού του μέτρου μπορούν οι φορείς να κατανοήσουν τις υποχρεώσεις τους καθώς και τα βήματα που πρέπει να ακολουθήσουν σε ορισμένες περιπτώσεις.
- Πληροφορίες διαχείρισης και Αναφοράς: Η ανώτατη διοίκηση με την αναγκαία χρήση συχνών αναφορών και των πληροφοριών που μεταδίδονται σε αυτή είναι σε θέση να γνωρίζει αν είναι αρκετοί οι πόροι και οι χρηματοδοτήσεις αλλά και για την λογοδοσία σε όλα τα επίπεδα.
- Ευαισθητοποίηση και Εκπαίδευση: Τη νοοτροπία για την ασφάλεια και προστασία των δεδομένων επιτυγχάνουν οι υπάλληλοι, οι εργολάβοι αλλά και το κάθε τρίτο μέρος που βρίσκεται σε θέση να γνωρίζει τι αναμένεται καθώς και πως να διατηρηθεί η συμμόρφωση.
- Αξιολογήσεις και έλεγχοι: Ακόμα και αν έχει γίνει σωστή εφαρμογή όλων των πολιτικών, των ελέγχων και των μέτρων θα χρειαστούν συνεχής έλεγχοι και επανεξετάσεις όλων των λειτουργιών και των δραστηριοτήτων για να εξασφαλίσουμε ότι όλα λειτουργούν καταλλήλως.
- Δέουσα επιμέλεια: Οι συνεργασίες ενός φορέα είναι εξίσου σημαντικές με τις ευθύνες του ίδιου του φορέα. Όταν αποφασίζεις να διαβιβάσεις δεδομένα σε τρίτα μέρη τα οποία δεν μπορούν να εγγυηθούν ασφάλεια τότε ο ίδιος ο φορέας παύει να είναι αξιόπιστος. Γι' αυτό τον λόγο θα πρέπει να εκτελούνται συνεχής έλεγχοι δέουσας επιμέλειας σε προμηθευτές και παρόχους υπηρεσιών.

Τα **Τεχνικά μέτρα** αναφέρει το άρθρο πως θεωρούνται "ως τα μέτρα και οι έλεγχοι που παρέχονται σε συστήματα και τεχνολογικές πτυχές ενός οργανισμού, όπως συσκευές, δίκτυα και υλικό." Η προφύλαξη αυτών τον πτυχών έχει εξαιρετικά μεγάλη σημασία στην ασφάλεια των δεδομένων. Μερικά από τα μέρη που μπορούν να θεωρηθούν ως τεχνικά μέτρα αναφέρονται παρακάτω:

- Ασφάλεια κτιρίου: Η χρήση σφοδρών μέτρων και πρωτοκόλλων για την εξασφάλιση της πρόσβασης για τα γραφεία και τα κτήρια καθώς και την επιμόρφωση των υπαλλήλων για αυτούς του ελέγχους. Τα κτήρια θα πρέπει να περιλαμβάνουν κλειστό κύκλωμα παρακολούθησης και συναγερμούς αλλά και το προσωπικό θα πρέπει να φοράει κατάλληλο εξοπλισμό έτσι ώστε να αποφευχθεί η είσοδος σε άτομα που δεν ανήκουν σε δυναμικό του κτηρίου.
- Απόρριψη: Η ορθή απόρριψη των εγγράφων και των συσκευών μαζί με την προστασία για αυτά που χάθηκαν είναι και αυτά μέρος των τεχνικών μέτρων που επιβάλλει το GDPR. Ο τεμαχισμός και η πιστοποιημένη απόρριψη αρχείων σε έντυπη μορφή είναι υποχρεωτική όταν τα προσωπικά δεδομένα υπάρχουν σε έντυπη μορφή.
- Ασφάλεια στον κυβερνοχώρο: Το συγκριμένο τεχνικό μέτρο έχει τόσο μεγάλο εύρος το οποίο είναι δύσκολο να αναλυθεί. Στο πιο σημαντικό επίπεδο, τα τείχη προστασίας, οι σαρώσεις κακόβουλου λογισμικού, η προστασία από ιούς και οι ενημερώσεις κώδικα και αναβαθμίσεις είναι αναγκαίες σε όλες τις συσκευές και τα δίκτυα που επιτρέπουν την πρόσβαση σε εμπιστευτικά και προσωπικά δεδομένα.
- Κωδικοί πρόσβασης: Ο Γενικός κανονισμός επιβάλλει την χρήση ισχυρών κωδικών οι οποία θα πρέπει να αλλάζουν ανά τακτά χρονικά διαστήματα. Επίσης, οι εργαζόμενοι θα πρέπει να είναι σωστά ενημερωμένοι για την τήρηση των κανόνων ασφαλείας που σχετίζονται με τους κωδικούς όσο αφορά την μυστικότητα τους.
- BYOD και απομακρυσμένη πρόσβαση: Με τον όρο BYOD (Bring Your One Device) εννοούμε πως ο εργαζόμενος θα πρέπει να παρέχει ο ίδιος την δική του συσκευή στην δουλεία ή να χρησιμοποιήσουν μια φορητή συσκευή όταν βρίσκονται εκτός γραφείου. Αυτές οι συσκευές επειδή έχουν στοιχεία της εταιρίας θα πρέπει να προστατεύονται και να ελέγχονται ανά τακτικά χρονικά διαστήματα.

Μελετώντας ένα επιπλέον άρθρο των Dominik Huth και Florian Matthes με τίτλο "Appropriate Technical and Organizational Measures": Identifying Privacy Engineering Approaches to Meet GDPR Requirements (2021)" [37] όπου πραγματοποίησαν μια έρευνα αναλύοντας το νομικό

κείμενο που αναφέρεται στα " Τεχνικά και Οργανωτικά μέτρα" και εξηγούν τις ιδιότητες απορρήτου. Για τον προσδιορισμό των ιδιοτήτων απορρήτου όρισαν τρεις κατηγορίες

- Κατηγορία 1: ιδιότητες που εξυπηρετούν ως όροι-ομπρέλα και θα έπρεπε να οριστούν λεπτομερέστερα («IOI»),
- Κατηγορία 2: όροι που ονομάζουν συγκεκριμένα, ορθά καθιερωμένες ιδιότητες απορρήτου ("PP"),
- Κατηγορία 3: ιδιότητες που αναφέρονται ειδικά για την εκπλήρωση αιτημάτων υποκειμένων δεδομένων («DSR»)

Στην συνέχεια οι αρθρογράφοι παραθέτουν μια λίστα με κάποιες Προσεγγίσεις της Μηχανικής Προστασίας Προσωπικών Δεδομένων και εξηγούν 12 ιδιότητες απορρήτου που αναφέρθηκαν στην λίστα.

- Ψευδώνυμο/Μη αναγνωρισιμότητα: «Επεξεργασία προσωπικών δεδομένων με τέτοιο τρόπο ώστε τα προσωπικά δεδομένα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο δεδομένων χωρίς τη χρήση επιπλέον πληροφοριών» (GDPR).
- Αποσύνδεση: " Αδυναμία ενός επιδρομέα να καθορίσει δύο αντικείμενα ενδιαφέροντος (IOI) εάν σχετίζονται ή όχι."
- Έλεγχος πρόσβασης/Εξουσιοδότηση: εννοούμε πως η πρόσβαση στα περιουσιακά στοιχεία είναι εξουσιοδοτημένη και περιορισμένη βάσει επιχειρηματικών απαιτήσεων και απαιτήσεων ασφάλειας" (ISO)
- Ακεραιότητα: Διαφύλαξη από τυχαία απώλεια, καταστροφή ή ζημιά» (GDPR)
- Εμπιστευτικότητα: "Προστασία από μη εξουσιοδοτημένη ή παράνομη επεξεργασία" (GDPR)
- Διαθεσιμότητα/Πρόσβαση: «ιδιότητα πρόσβασης και χρήσης κατόπιν αιτήματος από εξουσιοδοτημένη οντότητα" (ISO)
- Ελαχιστοποίηση δεδομένων: "επαρκής, σχετική και περιορισμένη σε ό,τι είναι απαραίτητο" (GDPR)
- Πληροφορίες/διαφάνεια: "επεξεργασία με διαφανή τρόπο" (GDPR)
- Περιορισμός αποθήκευσης: αποθήκευση δεδομένων «όχι περισσότερο από όσο είναι απαραίτητο για τους σκοπούς για τους οποίους τα προσωπικά δεδομένα υποβάλλονται σε επεξεργασία» (GDPR)

- Περιορισμός σκοπού: "συλλέγεται για καθορισμένους, σαφείς και νόμιμους σκοπούς" (GDPR)
- Υπευθυνότητα: "απόδειξη ότι η επεξεργασία πραγματοποιείται σύμφωνα με τον κανονισμό" (GDPR)
- Κρυπτογράφηση: "μέτρα προστασίας που καθιστούν τα δεδομένα ακατανόητα σε οποιοδήποτε άτομο που δεν είναι εξουσιοδοτημένος να έχει πρόσβαση σε αυτό» (GDPR)

4.2 Αρχή επιβολής κυρώσεων και πραγματοποίηση ελέγχων

Ο Δημήτρης Αναστασόπουλος στο άρθρο του με τίτλο “Οδηγός GDPR για δικηγόρους” [4] δήλωσε πως “Ο υπεύθυνος επεξεργασίας και ο ελεγκτής επεξεργασίας επιδέχεται κυρώσεις σε καταστάσεις μη τήρησης των διατάξεων του Γενικού Κανονισμού. Η ελληνική εποπτική αρχή που ονομάζεται Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) παρέχεται προς το υπεύθυνο επεξεργασίας ή τον ελεγκτή της επεξεργασίας” :

- να κατευθύνει υποδείξεις “σκοπούμενες πράξεις επεξεργασίας” να παραβιάζουν τον Γενικό κανονισμό,
- να κατευθύνει καταγγελία όταν πράξεις επεξεργασίας έχουν παραβιάσει τους κανονισμούς του Γενικού κανονισμού,
- διατάζει την συμμόρφωση προς τις απαιτήσεις του ατόμου για τα δικαιώματα επεξεργασίας των δεδομένων του,
- θεσπίζει προσωρινά ή μόνιμα ανάσχεση ή καταστολή της επεξεργασίας,
- επιβάλλει περιορισμό στην επεξεργασία των δεδομένων σε τρίτες χώρες οι οποίες αποδεκτές ή σε κρατικούς φορείς,
- υπαναχωρεί την πιστοποίηση ή απαιτεί από τον φορέα της πιστοποίησης να υπαναχωρήσει στην έκδοση ενός πιστοποιητικού ή απαιτεί από τον φορέα της πιστοποίησης να μην εκδώσει το εν λόγω πιστοποιητικό σε περίπτωση που τα αιτήματα δεν καλύπτονται ή δεν καλύπτονται πλέον,
- θεσπίζει διοικητικό πρόστιμο. Το διοικητικό πρόστιμο που επιβάλλεται εξαρτάται από την κατηγορία της παράβασης

4.3 Διαδικασία παραβίασης ασφάλειας δεδομένων

Η καταπάτηση δεδομένων προσωπικού χαρακτήρα σύμφωνα με την απόφαση 14/2019 [10] στο άρθρο 4 του Γενικού Κανονισμού αναφέρει ρητά "η παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία".

Συνεχίζοντας με την παράγραφο 3 του άρθρου 33 θεσπίζει ότι " σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα, ο υπεύθυνος επεξεργασίας γνωστοποιεί αμελλητί και, αν είναι δυνατό, εντός 72 ωρών από τη στιγμή που αποκτά γνώση του γεγονότος την παραβίαση των δεδομένων προσωπικού χαρακτήρα στην αρμόδια εποπτική αρχή, εκτός εάν η παραβίαση δεδομένων προσωπικού χαρακτήρα δεν ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Όταν η γνωστοποίηση στην εποπτική αρχή δεν πραγματοποιείται εντός 72 ωρών, συνοδεύεται από αιτιολόγηση για την καθυστέρηση".

Η παράγραφος συνεχίζει με τα περιεχόμενα της γνωστοποίησης:

- τη φύση της παραβίασης,
- το όνομα και τα στοιχεία επικοινωνίας του υπευθύνου επεξεργασίας ή άλλου σημείου επαφής από το οποίο μπορούν να ληφθούν πρόσθετες πληροφορίες,
- τις πιθανές συνέπειες της παραβίασης,
- τα μέτρα που πάρθηκαν ή πρέπει να παρθούν για την αντιμετώπιση της παραβίασης,
- καθώς και όπου ενδείκνυται μέτρα για την άμβλυνση ενδεχόμενων δυσμενών συνέπειών της.

4.4 Πρόστιμα

Σύμφωνα με τον Γενικό Κανονισμό Προστασίας Δεδομένων οι εποπτικές αρχές έχουν την δυνατότητα να επιβάλλουν πρόστιμα σε όποιους δεν συμμορφώνονται με τον Κανονισμό ή να ακολουθήσουν άλλες ποινές. Τα αδικήματα αυτά μπορεί να περιέχουν:

- εκδίδοντας προειδοποιήσεις και επιπλήξεις
- επιβολή μόνιμων ή προσωρινών απαγορεύσεων στην επεξεργασία δεδομένων
- εντολή διόρθωσης, περιορισμού ή διαγραφής δεδομένων

- αναστολή διαβίβασης δεδομένων σε τρίτες χώρες

Η μεγαλύτερη ανησυχία των επιχειρήσεων είναι η επιβολή πρόστιμου καθώς τα όρια είναι πολύ υψηλά

Η ιστοσελίδα sixfifty ανήρτησε ένα άρθρο με τίτλο "GDPR Penalties and Type of Violations " ανέλυσε τα επίπεδα των ποινών και τις κατηγορίες της παραβίασης [32].

Επίπεδα ποινών:

Για να μπορέσουν οι εποπτικές αρχές να ορίσουν την ποινή των οργανισμών πρέπει να εξετάσουν τις παρεμβάσεις αυτές πολύ σχολαστικά Το μέγιστο πρόστιμο για παραβίαση του GDPR είναι 2% του ετήσιου παγκόσμιου κύκλου εργασιών ή 10 εκατομμύρια ευρώ (όποιο είναι μεγαλύτερο) για παράβαση κατηγορίας 1. Και το 4% του ετήσιου παγκόσμιου τζίρου μιας εταιρείας ή 20 εκατομμύρια ευρώ (όποιο είναι μεγαλύτερο) για παράβαση της κατηγορίας 2.

Παραβιάσεις Κατηγορίας 1:

Οι παραβιάσεις σε αυτή την κατηγορία του Κανονισμού βασίζονται στις παρακάτω παραβιάσεις:

- Άρθρο 8 : προϋποθέσεις για την συγκατάθεση των παιδιών
- Άρθρο 11 : επεξεργασία που δεν απαιτεί ταυτοποίηση
- Άρθρα 25-39: γενικές υποχρεώσεις των υπεύθυνων επεξεργασίας και των επεξεργαστών
- Άρθρο 42 : πιστοποίηση
- Άρθρο 43 : οργανισμοί πιστοποίησης

Παραβιάσεις Κατηγορίας 2:

Οι παραβιάσεις σε αυτή την κατηγορία του Κανονισμού βασίζονται στις παρακάτω παραβιάσεις:

- Άρθρο 5 : Αρχές επεξεργασίας δεδομένων
- Άρθρο 6 : προϋποθέσεις συναίνεσης
- Άρθρο 9 : επεξεργασία ειδικών κατηγοριών δεδομένων
- Άρθρα 12-22 : δικαιώματα υποκειμένων δεδομένων
- Τα άρθρα 44-49 : μεταφέρουν δεδομένα σε τρίτες χώρες ή/και διεθνείς οργανισμούς

Ευθύνη Υπεύθυνου Επεξεργασίας Δεδομένων -DPO :

Πολλές εταιρείες χρησιμοποιούν τρίτα μέρη, όπως υπηρεσίες αποθήκευσης ηλεκτρονικού ταχυδρομείου ή cloud, για τον χειρισμό των δεδομένων τους. Αυτό μπορεί να είναι χρήσιμο για την τήρηση του GDPR εάν το τρίτο μέρος έχει υψηλότερη τεχνολογική ικανότητα όμως δεν απαλλάσσει τον οργανισμό πρόσληψης (δηλαδή τον υπεύθυνο επεξεργασίας-DPO) από τη διασφάλιση ότι τα προσωπικά δεδομένα υποβάλλονται σε επεξεργασία σύμφωνα με τον GDPR. Σε περίπτωση όμως που ο υπεύθυνος επεξεργασίας μπορεί να αποδείξει με σαφήνεια ότι "δεν ήταν σε καμία περίπτωση υπεύθυνος για το γεγονός που προκάλεσε τη ζημία", θα είναι πλήρως υπεύθυνος για οποιαδήποτε παράβαση προκλήθηκε από μη συμμορφούμενο τρίτο μέρος.
Για το λόγο αυτό, είναι σημαντικό να ελέγχονται προσεκτικά όλες οι υπηρεσίες τρίτων που χρησιμοποιούνται για την βεβαίωση ότι έχουν καλή ιστορία για την ασφάλεια.

Ο Γενικός Κανονισμός στο άρθρο 39 περιγράφει μερικές από τις ευθύνες του DPO [35] :

- Ενημερώνει και συμβουλεύει τον υπεύθυνο επεξεργασίας ή τον ελεγκτή,
- παρακολουθεί τη συμμόρφωση με τον Γενικό Κανονισμό και το εθνικό δίκαιο σχετικά με την προστασία των δεδομένων,
- παρακινεί τον φορέα, όταν απαιτείται, επιτελεί μελέτες επιπτώσεων σχετικά με την ασφάλεια δεδομένων και παρακολουθεί την πραγματοποίησή τους,
- συνεργάζεται και αποτελεί το μέσω επικοινωνίας με την εποπτική αρχή

Κεφάλαιο 5

5.1 Διαβιβάσεις δεδομένων σε τρίτες χώρες

Στην σημερινή εποχή, υπάρχουν τεράστιες διακρατικές μεταφορές προσωπικών δεδομένων τα οποία μερικές φορές αποθηκεύονται σε διακομιστές σε διαφορετικά κράτη. Η προστασία που προσφέρει ο Γενικός Κανονισμός για την Προστασία Δεδομένων (ΓΚΠΔ) συνοδεύεται από τα δεδομένα, πράγμα που σημαίνει ότι οι κανόνες που προστατεύουν τα προσωπικά δεδομένα και

εξακολουθούν να ισχύουν ανεξάρτητα από το πού προσφέρονται τα δεδομένα. Αυτό ισχύει επίσης όταν τα δεδομένα μεταφέρονται σε χώρα που δεν είναι μέλος της ΕΕ.

Ο Γενικός Κανονισμός προσφέρει ποικίλα εργαλεία για την διαμόρφωση μεταφορών δεδομένων από την ΕΕ σε τρίτες χώρες.

Σύμφωνα με την Ευρωπαϊκή Επιτροπή ο ΓΚΠΔ προσφέρει εργαλεία τα οποία περιβάλλουν τις διαβιβάσεις δεδομένων από την ΕΕ προς μια τρίτη χώρα:

- Υπάρχουν περιπτώσεις όπου μια τρίτη χώρα μπορεί να ανακοινωθεί από την Ευρωπαϊκή Επιτροπή ως "προσφέρουσα επαρκές επίπεδο προστασίας" αυτό υποδηλώνει ότι έχει δοθεί η άδεια να μεταφερθούν τα δεδομένα σε ένα άλλον φορέα στην συγκεκριμένη τρίτη χώρα χωρίς να χρειάζεται από τον αποστολέα των δεδομένων να προσφέρει επιπλέον εγγυήσεις ή όρους με αποτέλεσμα όταν μεταφέρεις δεδομένα σε μία "επαρκή" τρίτη χώρα" να ταυτίζεται με την μεταφορά δεδομένων σε χώρες εντός Ευρωπαϊκής Ένωσης.
- Όμως σε περιπτώσεις που δεν υπάρχει επαρκής προστασία είναι εφικτό να γίνει η διαβίβαση των δεδομένων με την χρήση των απαραίτητων εγγυήσεων και με τον όρο ότι τα προσωπικά δεδομένα των ατόμων έχουν στην κατοχή τους "εκτελεστά δικαιώματα και πραγματικά ένδικα" μέσα. Αυτές οι εγγυήσεις περιέχουν τα παρακάτω:
  - Σε περίπτωση ομίλου επιχειρήσεων που εκτελούν "κοινή οικονομική δραστηριότητα" οι επιχειρήσεις έχουν την δυνατότητα να διαβιβάσουν προσωπικά δεδομένα με βάση "τους αποκαλούμενους δεσμευτικούς εταιρικούς κανόνες"
  - Συμβατικές ρυθμίσεις με τον δέκτη των προσωπικών δεδομένων
  - Συμμόρφωση με τον κώδικα δεοντολογίας ή μηχανισμού πιστοποίησης ταυτόχρονα με την χρήση "δεσμευτικών και εκτελών δεσμεύσεων από τον αποδέκτη" που αφορούν την τήρηση των απαραίτητων εγγυήσεων για την ασφάλεια των προσωπικών δεδομένων κατά την διαβίβαση.
- Σε περιπτώσεις όπου προβλέπεται η μεταφορά προσωπικών δεδομένων χωρίς να επιδέχεται σε απόφαση επάρκειας αλλά και χωρίς τις απαραίτητες εγγυήσεις είναι εφικτό να πραγματοποιηθεί η διαβίβαση με βάση συγκεκριμένες εξαιρέσεις.

Σύμφωνα με το άρθρο της ιστοσελίδας Robin Data το οποίο δημοσίευσε ο Prof. Döring [9] και αναφέρει τις χώρες που δεν ανήκουν εντός Ευρωπαϊκής Ένωσης και προσφέρουν επαρκές επίπεδο προστασίας δεδομένων. Ο επίσημη λίστα της ΕΕ περιγράφεται παρακάτω:

- Ανδόρα
- Αργεντινή
- Καναδάς

- Νησιά Φερόε
- Γκέρνσεϊ
- Ισραήλ
- Νήσος Μαν
- Ιαπωνία
- Τζέρσεϊ
- Νέα Ζηλανδία
- Ελβετία
- Ουρουγουάη

5.2 Διαβίβαση Δεδομένων Ηνωμένες Πολιτείες Αμερικής (ΗΠΑ)

Ο Prof. Tobias Döring στο άρθρο ξεκαθαρίζει πως οι ΗΠΑ δεν θεωρούνται ως χώρα με επαρκές επίπεδο προστασίας δεδομένων. Αυτό ευθύνεται στην λεγόμενη USA PATRIOT ACT [14] των ΗΠΑ ή αλλιώς ο Νόμος των Πατριωτών ο οποίος έχει ως στόχο να αποφύγει και να τιμωρήσει τρομοκρατικές επιθέσεις στις Ηνωμένες Πολιτείες και να ενισχύσει τα ερευνητικά εργαλεία επιβολής του νόμου. Αυτός ο νόμος παρέχει στην κυβέρνηση περισσότερα δικαιώματα στα δεδομένα μια εταιρίας. Στο παρελθόν η διαβίβαση δεδομένων μεταξύ της Ευρωπαϊκής Ένωσης και των ΗΠΑ γινόταν με την Συμφωνία Ασφαλούς Λιμένα όμως αυτή η συμφωνία ανακοινώθηκε άκυρη από το Ευρωπαϊκό Δικαστήριο το 2015. Αυτή η ακύρωση είχε ως αποτέλεσμα την υιοθέτηση μιας νέας συμφωνίας η οποία ονομάζεται "η Ασπίδα Απορρήτου ΕΕ-ΗΠΑ" . Η Ασπίδα Απορρήτου εγκρίθηκε από την Ευρωπαϊκή Επιτροπή τον Ιούλιο του 2016 και κηρύχθηκε άκυρη από το Ευρωπαϊκό Δικαστήριο στις 16.07.2020. Ως επακόλουθο δεν είναι πλέον εφικτό να επεξεργάζονται προσωπικά στοιχεία τα οποία προέρχονται από πολίτες της Ευρωπαϊκής Ένωσης. Από τις 4 Ιουνίου 2021, η Ευρωπαϊκή Επιτροπή έχει δεχτεί νέες τυποποιημένες συμβατικές ρήτρες της Ευρωπαϊκής Ένωσης.

5.3 Διαβίβαση δεδομένων σε μη ασφαλείς τρίτες χώρες

Μελετώντας την έρευνα της δικηγόρου Nina Diercks και του Υπεύθυνου Προστασίας Εσωτερικών Δεδομένων Heiko Markus Roth (30 Αυγούστου 2021) [9] οι οποίοι αναλύουν την προσέγγιση βάση- κινδύνου στην Εκτίμηση Επιπτώσεων Μεταφοράς (Transfer Impact Assesment - TIA) σύμφωνα με τις νέες τυποποιημένες ρήτρες (SCC) της Ευρωπαϊκής Επιτροπής .

Υποστηρίζουν πως οι επιχειρήσεις διατρέχουν υψηλό κίνδυνο με την διαβίβαση δεδομένων σε τρίτες χώρες μετά την απόφαση Schrems II [6]. Σύμφωνα με αυτή την απόφαση που δημοσιεύθηκε τον Ιούλιο του 2020 το Δικαστήριο της Ευρωπαϊκής Ένωσης (ΕΕ) εξέδωσε ετυμηγορία που έκρινε ότι η ασπίδα προστασίας δεδομένων ΕΕ-ΗΠΑ, στην οποία βασίστηκαν πολλές εταιρείες για τη μεταφορά των δεδομένων τους μεταξύ των ΗΠΑ και της ΕΕ, ακυρώθηκε λόγω για τις ανησυχίες σχετικά με την παρακολούθηση από τις αμερικανικές πολιτείες και τις υπηρεσίες επιβολής του νόμου. Αυτή η ετυμηγορία έγινε αργότερα γνωστή ως Schrems II (από τον Max Schrems, έναν ακτιβιστή και δικηγόρο που ξεκίνησε αυτό το νομικό έπος μετά τις καταγγελίες του κατά του Facebook το 2013).

Παρόλο που η Επιτροπή της ΕΕ έχει θεσπίσει ρήτρες και έχει υιοθετήσει την " Αξιολόγηση Επιπτώσεων Μεταφοράς " που αναφέρεται στο άρθρο 14 εξακολουθεί να υπάρχει μια ανασφάλεια γύρω από το πεδίο εφαρμογής.

Αρχές προσέγγισης βάσεις- κινδύνου: Αναφέρεται ως μια " κανονιστική θεωρία " κατά την οποία οι υποχρεώσεις προστασίας δεδομένων εγκλιματίζονται στην κατάσταση κινδύνου για τα δικαιώματα και τις ελευθερίες των ατόμων στα οποία ανήκουν τα δικαιώματα. Στα όρια αυτά απειλή σημαίνει " ένα σενάριο με συμβάν και τις συνέπειές της που αξιολογούνται ως προς τη σοβαρότητά της απειλής και την πιθανότητα εμφάνισής της ". Η συγκεκριμένη προσέγγιση δεν έχει ως σκοπό την " μόχλευση" των υποχρεώσεων των προσωπικών δεδομένων αλλά έχει ως σκοπό την όξυνση και την βαθμονόμηση των κατάλληλων τεχνικών και οργανωτικών μέτρων σύμφωνα με τους ρεαλιστικούς κινδύνους επεξεργασίας. Η προσέγγιση λαμβάνει υπόψη το γεγονός ότι, ενώ καμία επεξεργασία δεν είναι ακίνδυνη, δεν οδηγεί κάθε κίνδυνος σε αδικαιολόγητη παραβίαση των δικαιωμάτων των υποκειμένων των δεδομένων. Η Ευρωπαϊκή Επιτροπή Προστασίας Δεδομένων έχει αρνηθεί ότι αυτή η προσέγγιση του Γενικού Κανονισμού μπορεί να λαμβάνεται υπόψη στα όρια της μεταφοράς από τρίτες χώρες σύμφωνα με το άρθρο 46 του Κανονισμού. Συνεπώς, εντελώς ανεξάρτητα από τον τύπο των δεδομένων που μεταφέρονται ο μόνος αποφασιστικός παράγοντας θα ήταν εάν η νομική κατάσταση της αποδέκτριας χώρας είχε επαρκές επίπεδο προστασίας ή/και εάν η επεξεργασία δεδομένων θα μπορούσε να προστατευθεί με άλλο τρόπο με πρόσθετα μέτρα.

1.Η εκτίμηση κινδύνου στην ρήτρα 14 του SCC: η Εκτίμηση Επιπτώσεων Μεταφοράς (ΕΕΜ - TIA)

Σύμφωνα με την συγκεκριμένη ρήτρα α) Τα SCC μέρη πρέπει να εγγυηθούν πως δεν έχουν κανέναν λόγο να θεωρούν ότι οι "νομικές διατάξεις και πρακτικές" στη χώρα του αποδέκτη δεδομένων εμποδίζουν τον αποδέκτη δεδομένων να πραγματοποιήσει τις υποχρεώσεις του βάσει

της σύμβασης, προκειμένου να εξασφαλιστεί το απαραίτητο επίπεδο προστασίας για τα διαβιβαζόμενα δεδομένα. β) η ρήτρα 14 παραθέτει ποικίλες πτυχές σε τρεις ομάδες υποθέσεων οι οποίες πρέπει να λαμβάνονται υπόψη στο πλαίσιο της εξασφάλισης:

- **i.** οι ειδικές συνθήκες της μεταφοράς που περιέχουν το μήκος της αλυσίδας επεξεργασίας, τον αριθμό των παραγόντων που έχουν εμπλακεί και των διαύλων μετάδοσης που έχουν χρησιμοποιηθεί, τις επερχόμενες μεταφορές, τον τύπο του αποδέκτη, τον σκοπό της επεξεργασίας, τις κατηγορίες και την μορφή που διαβιβάζονται τα δεδομένα, τον κλάδο στον οποίο ολοκληρώνεται η διαβίβαση και την αποθήκευση των δεδομένων που διαβιβάζονται.
- **ii.** Τους " νόμους και τις πρακτικές " της τρίτης χώρας προορισμού συμπεριλαμβανομένων εκείνων που απαιτούν την αποκάλυψη δεδομένων σε δημόσιες αρχές ή που επιτρέπουν την πρόσβαση σε αυτές τις αρχές και σχετίζονται με τις ειδικές συνθήκες της διαβίβασης των δεδομένων αλλά και τους ισχύοντες περιορισμούς και διασφαλίσεις. Όλες τις σχετικές συνθήκες, τεχνικές ή οργανωτικές εξασφαλίσεις που έχουν υποβληθεί σε εφαρμογή για την ολοκλήρωση των διασφαλίσεων βάσει αυτών των ρητρών,

2. Άρνηση της αρχής της προσέγγισης βάσει κινδύνου στο πλαίσιο του άρθρου 46

γ) από το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων(ΕΣΠΔ). Τον Νοέμβριο του 2020 το ΕΣΠΔ παρουσίασε ένα σχέδιο νόμου με μέτρα που ολοκληρώνουν τα εργαλεία διαβίβασης για την εξασφάλιση της συμμόρφωσης με το επίπεδο προστασίας των προσωπικών δεδομένων της ΕΕ και υποβλήθηκε σε δημόσια διαβούλευση. Στις 18.06.2021 δημοσιεύθηκε μια δεύτερη έκδοση επιπλέον τον Μάιο του 2021 δημοσιεύτηκε μια κοινή γνωμοδότηση σχετικά με την εκτελεστική απόφαση "Η Ευρωπαϊκή Διοίκηση των Ηνωμένων Πολιτειών (ΕΔΗΠ) " για τις τυποποιημένες συμβατικές ρήτρες για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα προς τρίτες χώρες.

Αυτά τα έγγραφα είναι μια μόνιμη διαβίβαση δεδομένων σε μη ασφαλές τρίτες χώρες είναι σχεδόν αποκλειστικά σημαντικό η εκάστοτε τρίτη χώρα να έχει επαρκές επίπεδο προστασίας με βάσει την νομοθεσία 28 στην οποία αναφέρεται αυτολεξεί "Η εκτίμησή σας θα πρέπει να επικεντρωθεί πρώτα και κύρια στη νομοθεσία τρίτων χωρών που σχετίζεται με τη μεταφορά σας και τη μεταφορά του άρθρου 46 GDPR εργαλείο στο οποίο βασίζεστε "

Το ΕΣΠΔ επιβάλλει υποχρεώσεις επαλήθευσης στον υπεύθυνο εξαγωγέα δεδομένων σχετικά με τις διαβιβάσεις σε τρίτες χώρες. Όμως αυτές οι υποχρεώσεις υπερβαίνουν τις απαιτήσεις του Γενικού Κανονισμού και αγνοούν την προσέγγιση βάσει κινδύνου .

α) Αξιολόγηση του επαρκούς επιπέδου προστασίας σύμφωνα με το ΕΣΠΔ

Για την αξιολόγηση του επαρκούς επιπέδου προστασίας, το ΕΣΠΔ αναφέρεται στη Σύστασή του 2/2020 για τα θεμελιώδη μέτρα επιτήρησης. Κατά συνέπεια το ΕΣΠΔ απαιτεί από τον εξαγωγέα δεδομένων να ελέγξει εάν και ποια ένδικα μέσα υπάρχουν κατά την επίσημη δίωξη και των δικαιωμάτων πρόσβασης και εάν αυτά συμμορφώνονται με το άρθρο 47 του " Χάρτη των θεμελιωδών δικαιωμάτων της ΕΕ(ΧΘΔ)".

Για να μπορέσει να πραγματοποιηθεί η διαβίβαση δεδομένων σε τρίτες χώρες ο υπεύθυνος δεδομένων θα πρέπει να αξιολογήσει την "νομική πρακτική" της χώρας αυτής. Σε περίπτωση που η νομική κατάσταση δεν σέβεται τον πυρήνα των θεμελιωδών δικαιωμάτων και ελευθεριών του ΧΘΔ τότε η διαβίβαση δεδομένων δεν μπορεί να πραγματοποιηθεί. Ο υπεύθυνος επεξεργασίας εξετάζει και την νομοθεσία αλλά και την τρέχουσα νομική κατάσταση και είναι καθήκον του να αξιολογήσει μια ξένη νομική κατάσταση. Αυτό σημαίνει ότι η συμβατική διασφάλιση μέσω των τυπικών συμβατικών ρητρών κατά την έννοια του άρθρου 46 παράγραφος 2 γ) του GDPR δεν θα είχε στην πραγματικότητα καμία αξία, καθώς ο υπεύθυνος επεξεργασίας πρέπει ωστόσο να πραγματοποιήσει πλήρη συνολική αξιολόγηση.

Επομένως, όπως αναφερθήκαμε και πριν η εξέταση της νομικής κατάστασης και πρακτικής μπορεί επομένως να οδηγήσει μόνο σε δύο αποτελέσματα:

- **i.** είτε υπάρχει επαρκές επίπεδο προστασίας και είναι δυνατή η μεταφορά δεδομένων
- **ii.** ή δεν υπάρχει επαρκές επίπεδο προστασίας.

β) Άρνηση της αρχής της προσέγγισης βάσει κινδύνου από το ΕΣΠΔ

Επομένως, δεν υπάρχει περιθώριο για το ΕΣΠΔ να υιοθετήσει μια προσέγγιση βάσει κινδύνου για την αξιολόγηση του παραδεκτού των μεταφορών από τρίτες χώρες μέσω του TIA σύμφωνα με τη ρήτρα 14 του SCC.

Ενώ το ΕΣΠΔ αναφέρει ότι " αντικειμενικοί παράγοντες " μπορούν να ληφθούν υπόψη στο πλαίσιο του TIA και αναλυτικά:

- **i.** τους σκοπούς για τους οποίους μεταφέρονται και υποβάλλονται σε επεξεργασία τα δεδομένα
- **ii.** το είδος των οντοτήτων που εμπλέκονται στην επεξεργασία
- **iii.** τον τομέα στον οποίο πραγματοποιείται η μετάδοση
- **iv.** τις κατηγορίες προσωπικών δεδομένων που διαβιβάζονται

v. πιθανή αποθήκευση δεδομένων σε τρίτη χώρα ή απλή απομακρυσμένη πρόσβαση σε δεδομένα που είναι αποθηκευμένα στην ΕΕ ή στον ΕΟΧ, τη μορφή των δεδομένων που θα διαβιβαστούν

vi. την πιθανή περαιτέρω μεταφορά δεδομένων από την πρώτη τρίτη χώρα σε άλλη τρίτη χώρα

Σύμφωνα με το ΕΣΠΔ αυτοί οι " αντικειμενικοί παράγοντες" πρέπει να χρησιμοποιούνται αποκλειστικά για την αξιολόγηση "αν υπάρχει κάτι στη νομοθεσία ή την πρακτική της τρίτης χώρας προορισμού που εμποδίζει τον εισαγωγέα δεδομένων να εκπληρώσει τις υποχρεώσεις του βάσει των σχεδίων SCC στο το πλαίσιο της συγκεκριμένης μεταφοράς, θα πρέπει να βασίζεται σε αντικειμενικούς παράγοντες, ανεξάρτητα από την πιθανότητα πρόσβασης στα προσωπικά δεδομένα".

Οι αρθρογράφοι καταλήγουν στο συμπέρασμα πως το ΕΣΠΔ επιβάλλει στον υπεύθυνο εξαγωγέα δεδομένων στο πλαίσιο του ΤΙΑ, αφενός, μια συνολική εξέταση της νομικής κατάστασης και της νομικής πρακτικής της τρίτης χώρας, την οποία οι ίδιες οι εποπτικές αρχές δεν είναι σε θέση να πραγματοποιήσουν και η οποία υπερβαίνει τα απαιτούμενα από το άρθρο 46 GDPR.

3.Παραδεκτό μιας πιο προσανατολισμένης στον κίνδυνο ερμηνείας του άρθρου 46

Η δημιουργία του ΕΣΠΔ οδηγεί σε μια ερμηνεία μηδενικής ανοχής του άρθρου 46 του Γενικού Κανονισμού. Δεν αφήνει περιθώρια για αξιολόγηση προσανατολισμένη στον κίνδυνο στη συγκεκριμένη περίπτωση και αντισταθμίζει την υποχρέωση για ΤΙΑ που ορίζεται στο άρθρο 14 . Αυτό δεν είναι πειστικό. Υπάρχουν καλύτερα επιχειρήματα για μια πιο προσανατολισμένη στον κίνδυνο ερμηνεία. Η αποφασιστική αρχή για το ΤΙΑ είναι: Εάν τα δεδομένα διαβιβάζονται σε τρίτη χώρα και ο εξαγωγέας δεν μπορεί να γνωρίζει με απόλυτη βεβαιότητα εάν η επεξεργασία κατά παράβαση του ευρωπαϊκού δικαίου θα συμβεί στη συγκεκριμένη περίπτωση κατά τη διάρκεια και μετά τη διαβίβαση, τότε ο εξαγωγέας δεδομένων μπορεί να προβεί σε αξιολόγηση αναλογικότητας που περιλαμβάνει επίσης τους συγκεκριμένους κινδύνους. Στη μοντελοποίηση κινδύνου, η πιθανότητα να συμβεί παραβίαση του ευρωπαϊκού δικαίου στην τρίτη χώρα στη συγκεκριμένη περίπτωση πρέπει επίσης να υπερβαίνει ένα ορισμένο όριο σημαντικότητας. Εάν ο εξαγωγέας δεδομένων καταλήξει στο συμπέρασμα στο πλαίσιο του ΤΙΑ ότι αυτό το όριο σημαντικότητας δεν θα ξεπεραστεί στη συγκεκριμένη μεταφορά δεδομένων, πληρεί την απαίτηση του άρθρου. 46. Αυτό οδηγεί στο αποτέλεσμα πως οι υποθετικοί κίνδυνοι χωρίς καμία αναφορά στην συγκεκριμένη διαβίβαση σε τρίτη χώρα δεν επαρκούν για να επιβεβαιώσουν την παρανομία.

1. **“Ότι σπείρεις θα θερίσεις ”Schrems II εξίσωση των οργάνων του κεφαλαίου 5 του ΓΚΠΔ**

   Το Ευρωπαϊκό Δικαστήριο δήλωσε στο άρθρο 44 του ΓΚΠΔ ότι το ίδιο πρότυπο για το επίπεδο προστασίας θα πρέπει να ισχύει για όλους τους τύπους διαβιβάσεων δεδομένων στο Κεφάλαιο 5, ανεξάρτητα από το μέσο ασφαλείας και ειδικότερα εξασφαλίζοντας ένα επίπεδο προστασίας ουσιαστικά ισοδύναμο με αυτό που εγγυάται η Ευρωπαϊκή Ένωση. Σε αυτό το σημείο παρατήρησαν οι μελετητές πως το ΕΣΠΔ φάνηκε να υιοθετεί ότι εάν η απόφαση επάρκειας για μια τρίτη χώρα δεν είναι “ουσιαστικά ισοδύναμη” με το ευρωπαϊκό δίκαιο, άλλα μέσα από το Κεφάλαιο 5 μπορούν να χρησιμοποιηθούν μόνο για μεταφορά στην ίδια τρίτη χώρα και συνεχίζουν υποστηρίζοντας πως τόσο αυτή η εξίσωση των θεμελιωδώς διαφορετικών μέσων ασφαλείας όσο και η δογματικά αμφίβολη εξαγωγή του ενιαίου προτύπου που δημιουργήθηκε για το “ουσιαστικά ισοδύναμο” από τον Schrems II δεν είναι μόνο προβληματικά, αλλά πρέπει να απορριφθούν.

2. **Το άρθρο 46 έχει διαφορετική εντολή προστασίας και πεδίο εφαρμογής από το άρθρο 45**

   Συγκρίνοντας τα επιμέρους μέσα διασφάλισης του Κεφαλαίου 5 του GDPR μεταξύ τους, γίνονται εμφανείς διαρθρωτικές διαφορές στο πεδίο και την εστίαση της παρεχόμενης προστασίας, οι οποίες ήδη μιλούν ενάντια σε μια «εξίσωση» του άρθρου. 45 και 46. Ενώ η Ευρωπαϊκή Επιτροπή αξιολογεί το επίπεδο προστασίας μιας αποδέκτριας χώρας μέσω μιας απόφασης επάρκειας σε μια χρονοβόρα και τυπική διαδικασία στο πρώτο στάδιο γενικά, δηλαδή ανεξάρτητα από τον κλάδο, την επιχειρηματική διαδικασία και την εταιρεία, βάσει της νομοθεσίας για τον εξαγωγέα (άρθρο 45 GDPR) το SCC αφορά ακριβώς μια διοργανωτική και σχετική με τη μεταφορά αξιολόγηση βάσει TIA που θα τεκμηριωθεί για τη συγκεκριμένη περίπτωση από τα ίδια τα μέρη (άρθρο 46 GDPR). Σε περιπτώσεις που ούτε το άρθρο 45 αλλά ούτε και το άρθρο 46 του ΓΚΠΔ επιτρέπει την διαβίβαση για συγκεκριμένες καταστάσεις χωρίς να χρειάζεται να διενεργηθεί τόσο αναλυτικό TIA όπως συμβαίνει στην περίπτωση του SCC. Το SCC βρίσκεται την μέση των δύο οργάνων και σε αντίθεση με την απόφαση επάρκειας, έχουν θερμορρυθμιστικό χαρακτήρα όσον αφορά τον εξαγωγέα.

3. **Η αυτορρύθμιση και η αντιμετώπιση των κινδύνων είναι εγγενείς των τυπικών συμβατικών ρητρών(SCC)**

   Υπάρχουν πολλά μέσα στον GDPR για την αυτορρύθμιση, π.χ. η προδιαγραφή τεχνικών και οργανωτικών μέτρων σύμφωνα με το άρθρο. 32 ή η εξέταση και ο χειρισμός δυνητικής επεξεργασίας υψηλού κινδύνου και η υποχρέωση διενέργειας εκτίμησης επιπτώσεων στην προστασία δεδομένων σύμφωνα με το άρθρο. 35 GDPR. Το κοινό χαρακτηριστικό αυτών των μέσων είναι ότι παρέχουν στον υπεύθυνο επεξεργασίας ένα περιθώριο πρόβλεψης στη λήψη αποφάσεων για να κλιμακώσει τα προστατευτικά μέτρα κατά την αντιμετώπιση των σχετικών αβεβαιοτήτων. Τίποτα άλλο δεν ισχύει για το καθήκον της TIA σύμφωνα με τα SCC: Η TIA είναι σύμφωνα με τον στόχο της, άρρηκτα συνδεδεμένη με αβεβαιότητες που απαιτούν προϋποθέσεις. η οποία σε ορισμένα σημεία θα είναι πέρα από τις δυνατότητες του εξαγωγέα δεδομένων για διορατικότητα, αξιολόγηση και επιρροή. Το ΕΣΠΔ φαίνεται να αναγνωρίζει αυτό το πρόβλημα. Το τι είναι "κατάλληλο" μπορεί να προσδιοριστεί μόνο μετά από αξιολόγηση βάση- προσανατολισμένη στον κίνδυνο. Το "κατάλληλο" πρέπει να προσδιορίζεται εκεί λαμβάνοντας υπόψη, μεταξύ άλλων, "τη φύση, το εύρος, το πλαίσιο και τους σκοπούς της επεξεργασίας καθώς και τον κίνδυνο διαφορετικής πιθανότητας και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων". Δεν μπορεί δηλαδή να υπάρξει απόλυτη προστασία του απορρήτου, άρα υπάρχει και εξέταση αναλογικότητας. Αυτό είναι στη φύση των πραγμάτων: καμία επεξεργασία δεδομένων δεν είναι ακίνδυνη - αυτό ισχύει για εγχώριες και ενδοευρωπαϊκές, αλλά και διεθνείς διαβιβάσεις δεδομένων. Ως εκ τούτου, μια απόφαση επιλογής που λαμβάνει υπόψη τους πραγματικούς κινδύνους της επεξεργασίας χρησιμεύει επίσης ως διορθωτική για τη φαινομενικά απόλυτη προστασία των προσωπικών δεδομένων και ως εκ τούτου για τη διατήρηση της αναλογικότητας.

4. **Η αναλογικότητα προστατεύει από μη αποδεκτή τοπική προσαρμογή δεδομένων**

   Το Ευρωπαϊκό Δικαστήριο αναφέρει πως στο Schrems II η προστασία των προσωπικών δεδομένων δεν είναι απόλυτη. Ωστόσο, τα δικαιώματα που κατοχυρώνονται στα άρθρα 7 και 8 του Χάρτη δεν είναι απόλυτα δικαιώματα, αλλά πρέπει να λαμβάνονται υπόψη σε σχέση με τη λειτουργία τους στην κοινωνία. Η επιβολή της ερμηνείας "0-ανοχής" από τις αρχές αναπόφευκτα παρεμβαίνει στα δικαιώματα και τις ελευθερίες τρίτων που παραχωρούνται από το CFR. Μόνο μια ερμηνεία προσανατολισμένη στον κίνδυνο

διατηρεί αυτήν την αναλογικότητα. Ως εκ τούτου, είναι επίσης συνεπές ότι η προσέγγιση βάσει κινδύνου αναφέρεται σε όλες τις εργασίες επεξεργασίας, συμπεριλαμβανομένων των μεταφορών σύμφωνα με το άρθρο. 44 του GDPR. Ο Γενικός Κανονισμός δεν προσφέρει κανένα υποκατάστατο για το SCC που να είναι σχετικό στην επιχειρηματική πρακτική. Όλο αυτό το αποτέλεσμα θα ήταν αντίθετο με την αναλογικότητα. Αυτό ισχύει επίσης για την κατανόηση που έχει ο GDPR για τη σημασία των διεθνών διαβιβάσεων δεδομένων για το διεθνές εμπόριο και θα εξουδετερώσει τις προσπάθειες της ΕΕ να αποφύγει τους φραγμούς του διεθνούς εμπορίου. Επομένως, οι απαιτήσεις συμμόρφωσης του ΓΚΠΔ έχουν δημιουργήσει μια "de facto" απαίτηση για τους εκτελούντες της επεξεργασίας δεδομένων εκτός ΕΕ να εντοπίζουν δεδομένα, κάτι που σύμφωνα με τους αρθρογράφους θα το καθιστά αδύνατο.

5. Συμπέρασμα

Δεν προκύπτουν «υποκειμενικά» ή ακόμη και αυθαίρετα αποτελέσματα από μια ερμηνεία προσανατολισμένη στον κίνδυνο, η οποία θα έπρεπε να αγνοηθεί στη χρηστικότητα του SCC σύμφωνα με το άρθρο 46. Ο υπολογισμός της πιθανότητας μπορεί να πραγματοποιηθεί με κανονικό, αντικειμενικά κατανοητό τρόπο και με επαναφορά σε όργανα που έχουν αποδειχθεί σε άλλους κλάδους. Ένα πολύ καλό παράδειγμα είναι το εργαλείο που αναπτύχθηκε από τον Rosenthal για το «Cloud Computing: Risk Assessment of Lawly Access By Foreign

Τέλος, οι αρθρογράφοι καταλήγουν σε κάποια συμπεράσματα και σε κάποιες συστάσεις. Αρχικά, σύμφωνα με την τρέχουσα νομική γνώμη του EDPB καθώς και των εθνικών εποπτικών αρχών, μόνο η νομοθεσία και η πρακτική της αποδέκτριας χώρας πρέπει να αξιολογούνται στο πλαίσιο των μεταφορών από τρίτη χώρα σύμφωνα με το άρθρο 46 γ)GDPR ως μέρος αξιολόγησης επιπτώσεων στη μεταφορά. Όπως φαίνεται, η αρχή της προσέγγισης βάσει κινδύνου του GDPR πρέπει επίσης να λαμβάνεται υπόψη σε μια εκτίμηση επιπτώσεων στη μεταφορά κατά την έννοια του άρθρου. 46 γ) GDPR και ρήτρα 14 β) του SCC και περιλαμβάνονται μέσω αξιολόγησης αναλογικότητας. Οι αποφάσεις της Επιτροπής της ΕΕ, όπως η εκτελεστική απόφαση για το SCC, αποτελούν παράγωγο δίκαιο της ΕΕ.

Για τα τμήματα του ανθρώπινου δυναμικού, αυτό σημαίνει τα εξής:

Οι διαβιβάσεις δεδομένων σε μη ασφαλείς τρίτες χώρες πρέπει να υποβάλλονται σε εκτίμηση επιπτώσεων στη μεταφορά, ανεξάρτητα από το εάν είναι εσωτερικές ή εξωτερικές του ομίλου. Διαφορετικά, οι απαιτήσεις σύμφωνα με το άρθρο. 46 γ) Ο GDPR και η ρήτρα 14 του SCC δεν

πληρούνται, και επομένως η μεταφορά δεδομένων είναι παράνομη. Αυτό αρχικά φαίνεται να σημαίνει τεράστιο πρόσθετο φόρτο εργασίας για τα τμήματα του ανθρώπινου δυναμικού. Ωστόσο, εάν αυτά έχουν ήδη τεκμηριωθεί κατάλληλα στο αρχείο των δραστηριοτήτων επεξεργασίας σύμφωνα με το άρθρο. 30 GDPR και αναλύεται στο πλαίσιο μιας ανάλυσης κατωφλίου κατά την έννοια του άρθρου. 35 GDPR, το βήμα προς μια ΤΙΑ δεν είναι πλέον μεγάλο. Αυτό ισχύει ιδιαίτερα όταν αναλογιστεί κανείς την προσπάθεια που απαιτείται τακτικά για να αλλάξει ένα τέτοιο σύστημα. Σε αντίθεση με τη μάλλον ανέφικτη υπόθεση των εκπροσώπων των αρχών ότι ένα σύστημα διαχείρισης που υποβάλλει αίτηση μπορεί να αλλάξει χωρίς προβλήματα, η πραγματικότητα δείχνει ότι σε περισσότερο από το 50% των εταιρειών πρέπει να προγραμματιστούν τουλάχιστον δώδεκα μήνες και επομένως σημαντικοί οικονομικοί πόροι και πόροι προσωπικού. Σε αυτό το πλαίσιο, μια ΤΙΑ βασισμένη στον κίνδυνο είναι το προφανές και τακτικά επίσης πιο οικονομικά αποδοτικό βήμα για να επαληθευτεί εάν οι υπάρχουσες μεταφορές δεδομένων μπορούν να συνεχιστούν σύμφωνα με τη νομοθεσία.

Κεφάλαιο 6

6.1 Μεθοδολογία συμμόρφωσης GDPR

Ο Axel Freiherr von dem Bussche και ο Paul Voigt [24] μελέτησαν και ανέλυσαν τα βήματα συμμόρφωσης του ΓΚΠΔ τα οποία είναι τα εξής:

- **Βήμα 1: Ανάλυση κενών**

  Προκειμένου να αξιολογηθεί η προστασία δεδομένων μιας εταιρείας To Do's, θα πρέπει να πραγματοποιηθεί μια «ανάλυση χάσματος» μεταξύ της τρέχουσας κατάστασης συμμόρφωσης με την προστασία δεδομένων και των υποχρεώσεων που απορρέουν από τον GDPR.

  Έτσι, σε ένα πρώτο βήμα, η εταιρεία θα πρέπει να συλλέγει πληροφορίες σχετικά με τις τρέχουσες δραστηριότητές της για την προστασία δεδομένων (π.χ. (i) ποιες οντότητες/τμήματα επεξεργάζονται τι είδους δεδομένα για ποιους σκοπούς, (ii) εσωτερικές

ευθύνες, (iii) π πως προστατεύονται τα δεδομένα των υποκειμένων (iv) έχουν διοριστεί υπεύθυνοι προστασίας δεδομένων, (v) ποια μέτρα ασφαλείας ισχύουν

Σε ένα δεύτερο βήμα, η εταιρεία πρέπει να αξιολογήσει ποιες απαιτήσεις που απορρέουν από τον GDPR ισχύουν ειδικά.

- **Βήμα 2: Ανάλυση κινδύνου**

  Οι προσπάθειες για την εφαρμογή των απαιτήσεων GDPR είναι γενικά υψηλές δεν μπορούν εύλογα να εκπληρωθούν όλες οι απαιτήσεις ταυτόχρονα. Η εταιρεία θα πρέπει να αξιολογήσει τι είδους δραστηριότητες επεξεργασίας δεδομένων αποτελούν τον μεγαλύτερο κίνδυνο για (i) τις δραστηριότητές της και/ή (ii) τα δικαιώματα των υποκειμένων των δεδομένων καθώς και (iii) ποιοι κίνδυνοι οδηγούν πιθανότατα σε υψηλά πρόστιμα και τακτοποιεί τους πόρους της αντίστοιχα. Οι προσπάθειες για συμμόρφωση με την προστασία δεδομένων θα πρέπει να είναι υψηλότερες για επικίνδυνες δραστηριότητες επεξεργασίας και χαμηλότερες για λιγότερο επικίνδυνες δραστηριότητες επεξεργασίας.

- **Βήμα 3: Καθοδήγηση έργου και προγραμματισμός πόρων/προϋπολογισμού**

  Η διαδικασία εφαρμογής του GDPR απαιτεί συνεργασία μεταξύ των ευρωπαϊκών οντοτήτων της εταιρείας, καθώς και επίγνωση των To Do's σε επίπεδο διαχείρισης της εταιρείας. Η εταιρεία θα πρέπει να αναθέσει τις ευθύνες του έργου στο βασικό προσωπικό στα εμπλεκόμενα γραφεία της ΕΕ και να ορίσει έναν «επικεφαλής» διευθυντή έργου. Αυτός θα μπορούσε επίσης να είναι εξωτερικός σύμβουλος.
  Η εταιρεία πρέπει να διαθέσει τους απαιτούμενους πόρους. Ο σχεδιασμός θα πρέπει ειδικότερα να καλύπτει (i) εσωτερικούς πόρους, όπως το προσωπικό που απαιτείται για την υλοποίηση, (ii) τα νομικά έξοδα καθώς και (iii) τα έξοδα πληροφορικής

- **Βήμα 4: Εφαρμογή μιας συμβατής δομής προστασίας δεδομένων**

  Ο GDPR περιλαμβάνει μια σειρά από αυστηρές απαιτήσεις προστασίας δεδομένων, όπως:

  - Ολοκληρωμένα δικαιώματα των υποκειμένων των δεδομένων
  - Οργανωτικές απαιτήσεις
  - Υποχρεώσεις ειδοποίησης
  - Συμβατικές απαιτήσεις

  Προκειμένου να ανταπεξέλθει σε αυτές τις υποχρεώσεις, η εταιρεία πρέπει να εφαρμόσει έναν αποτελεσματικό οργανισμό προστασίας δεδομένων:

<u>Σύστημα Διαχείρισης Προστασίας Δεδομένων</u>

Ο ΓΚΠΔ ορίζει μια σειρά από απαιτήσεις που είναι δύσκολο να αντιμετωπιστούν εάν δεν εφαρμοστεί ένα ενδελεχές σύστημα διαχείρισης προστασίας δεδομένων. Ένα τέτοιο σύστημα θα πρέπει να λειτουργεί σε ολόκληρη την ομάδα, καθώς ακόμη και ζητήματα προστασίας δεδομένων σε μικρότερα γραφεία εταιρειών μπορεί να οδηγήσουν σε υψηλά πρόστιμα για τον εταιρικό όμιλο στο σύνολό του.

a) Καθορισμένοι ρόλοι και αρμοδιότητες στις εμπλεκόμενες οντότητες της Εταιρείας

Η εταιρεία θα πρέπει να δημιουργήσει μια δομή προσώπων που είναι υπεύθυνα για την προστασία δεδομένων σε όλα τα γραφεία της ΕΕ, καθώς και έναν υπεύθυνο επικεφαλής στα κεντρικά γραφεία. Η αντίστοιχη δομή θα πρέπει να επιτρέπει (i) την εύκολη παροχή εντολών ή/και συμβουλών σχετικά με την προστασία δεδομένων στα εμπλεκόμενα γραφεία καθώς και (ii) την επικοινωνία των θεμάτων που σχετίζονται με την προστασία δεδομένων στον επικεφαλής

b) Διαδικασίες και έννοιες

Πολλές από τις υποχρεώσεις του GDPR μπορούν να εφαρμοστούν αποτελεσματικά μόνο εάν υπάρχουν αντίστοιχες έννοιες, πολιτικές και τυπικές διαδικασίες λειτουργίας.

c) Εκπαίδευση

Οι εργαζόμενοι θα πρέπει να εκπαιδεύονται στις υποχρεώσεις και τις ευθύνες τους που απορρέουν από τον GDPR. Η εταιρεία θα πρέπει να προσαρμόσει την εκπαίδευση στα καθήκοντα του εργαζομένου. Από αυτή την άποψη, είναι λογικό να χαρτογραφηθούν οι απαιτήσεις εκπαίδευσης σε μια έννοια εκπαίδευσης. Αυτή η έννοια θα πρέπει επίσης να αντικατοπτρίζει τον κύκλο της εκπαίδευσης.

d) Τεκμηρίωση Συμμόρφωσης

Η εταιρεία πρέπει να εφαρμόσει τα κατάλληλα μέτρα για να αποδείξει τη συμμόρφωση με τις απαιτήσεις του GDPR. Εάν δεν αποδειχθεί η συνεχής συμμόρφωση κατόπιν αιτήματος των εποπτικών αρχών, ενδέχεται να επιβληθούν πρόστιμα. Οι εσωτερικές διαδικασίες προστασίας δεδομένων θα πρέπει να επανεξετάζονται και να ενημερώνονται συχνά. Για το σκοπό αυτό, η εταιρεία θα πρέπει να διενεργεί τακτικούς εσωτερικούς ελέγχους GDPR.

<u>Συμφωνίες επεξεργασίας δεδομένων</u>

Λόγω του μεγάλου αριθμού συμφωνιών που πρέπει να συνάψει η εταιρεία με εσωτερικά και εξωτερικά μέρη, οι εταιρείες θα πρέπει να εφαρμόζουν μια λογική στρατηγική διαχείρισης συμβάσεων επεξεργασίας δεδομένων:

- Η χρήση υπευθύνων επεξεργασίας δεδομένων θα επιτρέπεται μόνο εάν συναφθούν ολοκληρωμένες συμφωνίες επεξεργασίας δεδομένων. Εάν υπάρχουν συμφωνίες πριν από τον GDPR, αυτές θα πρέπει να ελεγχθούν για να διαπιστωθεί εάν συμμορφώνονται με τις απαιτήσεις του GDPR ή πρέπει να ενημερωθούν. Αυτό μπορεί επίσης να ισχύει για ενδοεταιρική κοινή χρήση δεδομένων.
- Σε ορισμένες περιπτώσεις, διάφορες εταιρικές οντότητες μπορεί να θεωρηθούν ως από κοινού υπεύθυνοι επεξεργασίας δεδομένων εάν καθορίζουν από κοινού τους σκοπούς και τα μέσα επεξεργασίας δεδομένων. Σε τέτοιες περιπτώσεις, πρέπει γενικά να συνάπτονται συμφωνίες επεξεργασίας δεδομένων μεταξύ των εμπλεκόμενων φορέων.
- Εάν τα προσωπικά δεδομένα μεταφέρονται από τον ΕΟΧ σε χώρα εκτός του ΕΟΧ, ενδέχεται να απαιτηθούν πρόσθετες συμφωνίες μεταφοράς δεδομένων

- **Βήμα 5: Απαιτήσεις τοπικών πρόσθετων**

  Εκτός από τις απαιτήσεις GDPR σε επίπεδο ΕΕ, πρέπει να αξιολογηθεί εάν ισχύουν πρόσθετες εθνικές απαιτήσεις.

  Τα κράτη μέλη της ΕΕ έχουν ευρεία διακριτική ευχέρεια να θεσπίσουν πρόσθετους εθνικούς κανονισμούς που τροποποιούν ή/και βελτιώνουν τον GDPR.
  Στις περισσότερες χώρες του ΕΟΧ, υπάρχουν πρόσθετες απαιτήσεις σχετικά με την απασχόληση και με την επεξεργασία δεδομένων ανθρώπινου δυναμικού

- **Βήμα 6: Αντιμετώπιση του Brexit**

  Πολλοί διεθνείς όμιλοι εταιρειών έχουν την ευρωπαϊκή έδρα τους στο Ηνωμένο Βασίλειο, το οποίο δεν αποτελεί πλέον μέρος της Ευρωπαϊκής Ένωσης. Μέσω της νομοθεσίας του Ηνωμένου Βασιλείου, οι απαιτήσεις GDPR ενδέχεται να συνεχίσουν να ισχύουν για τα γραφεία της εταιρείας στο Ηνωμένο Βασίλειο. Ωστόσο, η μεταφορά δεδομένων από άλλα γραφεία της εταιρείας στον ΕΟΧ σε οποιοδήποτε γραφείο του Ηνωμένου Βασιλείου θα απαιτήσει πρόσθετες διασφαλίσεις που μπορεί να οδηγήσει σε νομικά ζητήματα. Οι επηρεαζόμενες εταιρείες θα πρέπει να λάβουν προφυλάξεις προστασίας δεδομένων για το Brexit.

6.2 Data mapping- Χαρτογράφηση δεδομένων

Σύμφωνα με το άρθρο που δημοσίευσε η ιστοσελίδα securitii.ai με τίτλο 'GDPR Data Mapping: What it is and How to Comply?" (26/5/2021) [30] αναφέρουν πως η χαρτογράφηση δεδομένων αποτελεί ένα ουσιαστικό στοιχείο του Γενικού Κανονισμού. Θεωρείται ότι είναι το θεμελιώδες βήμα για την εκπλήρωση όλων των άλλων νομικών απαιτήσεων βάσει του GDPR μερικά παραδείγματα είναι η ανταπόκριση σε αιτήματα των υποκειμένων των δεδομένων, η διεξαγωγή αξιολογήσεων επιπτώσεων στην προστασία δεδομένων ή η τήρηση αρχείων δραστηριοτήτων επεξεργασίας δεδομένων. Στην συνέχεια αναφέρουν κάποια παραδείγματα σχετικά με την συμμόρφωση απορρήτου βάσει χαρτογράφησης δεδομένων είναι τα εξής:

- Αρχεία Δραστηριοτήτων Επεξεργασίας:

  Το άρθρο 30 του Γενικού Κανονισμού απαιτεί από τους υπεύθυνους επεξεργασίας και τους εκτελούντες την επεξεργασία να τηρούν Αρχείο των Δραστηριοτήτων Επεξεργασίας Δεδομένων(ΑΔΕΔ) Οι ΑΔΕΔ περιλαμβάνουν πληροφορίες σχετικά με τη δραστηριότητα της διαδικασίας, όπως ο σκοπός της επεξεργασίας, η νομική βάση, η κατάσταση συναίνεσης, οι διασυνοριακές μεταφορές, η κατάσταση DPIA και άλλα. Η χαρτογράφηση δεδομένων βοηθά τους οργανισμούς να συμμορφώνονται με τον GDPR συλλέγοντας και διατηρώντας μια λίστα δραστηριοτήτων επεξεργασίας δεδομένων σε όλη την επιχείρηση.
- Εκτιμήσεις Επιπτώσεων Προστασίας Δεδομένων:

  Το άρθρο 35 του ΓΚΠΔ απαιτεί από τους οργανισμούς να διενεργούν αξιολογήσεις επιπτώσεων στην προστασία δεδομένων (ΕΑΠΔ) όπου η επεξεργασία είναι πιθανό να οδηγήσει σε υψηλό κίνδυνο για τα άτομα. Μια τέτοια DPIA πρέπει να λαμβάνει υπόψη τη φύση, το εύρος, το πλαίσιο και τους σκοπούς της επεξεργασίας. Για τη διεξαγωγή αποτελεσματικών DPIA, οι οργανισμοί πρέπει να είναι σε θέση να τεκμηριώνουν τους τύπους δεδομένων που συλλέγουν, πότε και πώς συλλέγονται και χρησιμοποιούνται αυτά τα δεδομένα, πού αποθηκεύονται τα δεδομένα, πώς ρέουν δεδομένα μέσω διαφόρων συστημάτων και προμηθευτών, όλα αυτά είναι επιτυγχάνεται μέσω της χαρτογράφησης δεδομένων.
- Διαχείριση παραβίασης

  Το άρθρο 33 του ΓΚΠΔ απαιτεί από τους οργανισμούς να κοινοποιούν στην εποπτική αρχή τις παραβιάσεις προσωπικών δεδομένων που είναι πιθανό να θέτουν σε κίνδυνο τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων το αργότερο 72 ώρες αφότου λάβουν γνώση της παραβίασης. Όταν ο κίνδυνος για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων είναι υψηλός, οι οργανισμοί πρέπει να

κοινοποιούν τις παραβιάσεις προσωπικών δεδομένων στα επηρεαζόμενα υποκείμενα των δεδομένων χωρίς αδικαιολόγητη καθυστέρηση. Η αντιστοίχιση δεδομένων βοηθά τους οργανισμούς να εντοπίζουν γρήγορα τα επηρεαζόμενα υποκείμενα δεδομένων και τα διακυβευμένα δεδομένα σε οποιοδήποτε περιστατικό ασφαλείας. Επιτρέπει επίσης στους οργανισμούς να αξιολογούν τους κινδύνους για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων που προκύπτουν από παραβίαση ασφάλειας, βοηθώντας έτσι τους οργανισμούς να αναφέρουν μόνο τις παραβιάσεις προσωπικών δεδομένων που πληρούν ένα απαιτούμενο όριο κινδύνου στους κατάλληλους ενδιαφερόμενους. Ως αποτέλεσμα, είναι σε θέση να τηρούν τα χρονοδιαγράμματα ειδοποιήσεων βάσει του GDPR.

- Διαχείριση συναίνεσης:

  Ενώ βασίζεται στη συναίνεση του χρήστη ως νόμιμη βάση επεξεργασίας δεδομένων, το άρθρο 4 του GDPR απαιτεί τη εν λόγω συγκατάθεση να παρέχεται ελεύθερα, συγκεκριμένη, ενημερωμένη και σαφής ένδειξη των επιθυμιών του υποκειμένου των δεδομένων. Επιπλέον, τα υποκείμενα των δεδομένων πρέπει επίσης να μπορούν να αποσύρουν τη συγκατάθεσή τους ανά πάσα στιγμή και χωρίς καμία βλάβη. Η αντιστοίχιση δεδομένων βοηθά τους οργανισμούς να προσδιορίσουν ποιες δραστηριότητες επεξεργασίας βασίζονται στη συναίνεση ως νομική βάση, να επισημάνουν πού μπορεί να χρειαστούν μηχανισμοί σύλληψης συναίνεσης και να διευκολύνουν την ανάκληση της συναίνεσης.

- Εκπλήρωση Δικαιωμάτων υποκειμένων δεδομένων:

  Ο Γενικός Κανονισμός εκχωρεί πολλά δικαιώματα στα υποκείμενα των δεδομένων σε σχέση με τα προσωπικά τους δεδομένα, συμπεριλαμβανομένων των δικαιωμάτων πρόσβαση σε αντίγραφο προσωπικών δεδομένων, διόρθωση ή διαγραφή προσωπικών δεδομένων, περιορισμός της επεξεργασίας προσωπικών δεδομένων και θύρα προσωπικών δεδομένων. Μόλις ασκηθούν αυτά τα δικαιώματα από το υποκείμενο των δεδομένων, ο εκτελών επεξεργασίας και ο υπεύθυνος επεξεργασίας δεδομένων πρέπει να ανταποκριθούν σε τέτοια αιτήματα εντός καθορισμένων χρονικών πλαισίων. Η χαρτογράφηση δεδομένων βοηθά τους οργανισμούς να προσδιορίσουν πού βρίσκονται τα δεδομένα του υποκειμένου των δεδομένων και να διευκολύνει το αίτημα του υποκειμένου των δεδομένων. Επιτρέπει στους οργανισμούς να ανταποκριθούν στο αίτημα ενός υποκειμένου των δεδομένων εντός της προβλεπόμενης προθεσμίας βάσει του GDPR.

- Βασικά Στοιχεία Χαρτογράφησης Δεδομένων

Τα 5 βασικά στοιχεία της Χαρτογράφησης Δεδομένων είναι τα εξής:

1.Επιτρέπει στις επιχειρήσεις να οργανώνουν, να καταλογοποιούν, να διαχειρίζονται και να δομούν δεδομένα για λειτουργικές ανάγκες

2. Επιτρέπει στους οργανισμούς να έχουν εύκολη πρόσβαση και να βρίσκουν σχετικά δεδομένα όποτε απαιτείται

3.Κάνει τη διαχείριση και την προστασία των δεδομένων πιο αποτελεσματική, δηλαδή τα πιο επικίνδυνα δεδομένα έχουν πιο ισχυρή ασφάλεια

4. Ενεργοποιεί την παρακολούθηση ροής δεδομένων

5. Βοηθά στη διατήρηση επαρκών αρχείων των δραστηριοτήτων επεξεργασίας δεδομένων

- Βασικές προκλήσεις της χαρτογράφησης δεδομένων:

  Υπάρχουν πολλαπλά στοιχεία συλλογής και επεξεργασίας δεδομένων σε συνδυασμό με εσωτερική και με υποδομή αποθήκευσης εφαρμογών και αποθήκευσης που βασίζεται σε cloud, με εξαιρετικά ρευστές συμφωνίες κοινής χρήσης και επεξεργασίας δεδομένων. Καθώς περισσότερο από το 80% του φόρτου εργασίας των επιχειρήσεων μεταφέρεται πλέον στο cloud, οι οργανισμοί δυσκολεύονται να τεκμηριώσουν και να παρακολουθήσουν τη ροή πληροφοριών εντός της υποδομής cloud του προμηθευτή τους. Επίσης, χωρίς μια συλλογική τεκμηρίωση και περιβάλλον ανταλλαγής γνώσεων, είναι χαρακτηριστικό για τέτοιες γνώσεις επιχειρηματικής διαδικασίας να εγκλωβίζονται στο μυαλό των ειδικών του θέματος, καθιστώντας σχεδόν αδύνατη τη δημιουργία και τη διατήρηση ακριβούς αρχείου δεδομένων. Η αντιστοίχιση δεδομένων που ενεργοποιείται από τη μεθοδολογία PrivacyOps βοηθά στην επίλυση όλων αυτών των προκλήσεων. Παρέχει μια πλήρως αυτοματοποιημένη, ενιαία και ασφαλή πλατφόρμα σε οργανισμούς που τους βοηθά να διεξάγουν αποτελεσματική και ολιστική χαρτογράφηση δεδομένων.

- Χαρτογράφηση δεδομένων και το πλαίσιο PrivacyOps

  Είναι μια καλή λύση χαρτογράφησης δεδομένων που βοηθά τις εταιρείες να αποκτήσουν πλήρη προβολή και έλεγχο των προσωπικών δεδομένων και διευκολύνει τη συνεργασία όχι μόνο εντός του οργανισμού αλλά και εξωτερικά. Το πλαίσιο PrivacyOps απαιτεί ένα σύστημα καταγραφής, ένα σύστημα γνώσης, ένα σύστημα αφοσίωσης και ένα σύστημα αυτοματισμού για να φέρει όλες τις μικρές και μεσαίες επιχειρήσεις (ΜΜΕ) σε ένα μέρος για την τεκμηρίωση και παρακολούθηση της ροής των πληροφοριών σε μία πλατφόρμα. Οποιαδήποτε λύση χαρτογράφησης δεδομένων σύμφωνα με τη μεθοδολογία PrivacyOps παρέχει τις ακόλουθες δυνατότητες:

- Ένα σύστημα Καταγραφής

  Ένα σύστημα καταγραφής διατηρεί

  - Ροές πληροφοριών εντός του οργανισμού, μεταξύ οργανισμών αλλά και εκτός του οργανισμού καθώς και ροή δεδομένων μεταξύ των χωρών.
  - Εκτεταμένα μεταδεδομένα για κάθε στοιχείο σε έναν χάρτη δεδομένων, συμπεριλαμβανομένων τον τύπο των δεδομένων, την μορφή των δεδομένων, Τοποθεσία, Υπευθυνότητα, Λίστα πρόσβασης.
  - Ένας ορισμός όλων των τύπων χαρακτηριστικών των προσωπικών δεδομένων που χειρίζεται το στοιχείο χάρτη δεδομένων
  - Ένα αρχείο του σκοπού της συλλογής, επεξεργασίας ή αποθήκευσης δεδομένων μαζί με νομική αιτιολόγηση για αυτές τις δραστηριότητες
  - Εύκολες στην δημιουργία αναφορών του Άρθρου 30 που μπορούν να κοινοποιηθούν εσωτερικά και να διατεθούν άμεσα στις εποπτικές αρχές και τους ελεγκτές

- <u>Ένα σύστημα Γνώσης:</u>
  - Παρέχει μια επεκτάσιμη, οργανωτική βιβλιοθήκη εικονιδίων
  - Επιτρέπει στους χρήστες να ορίσουν στοιχεία μία φορά και να τα χρησιμοποιήσουν σε πολλούς χάρτες δεδομένων ή διαγράμματα ροής επιχειρηματικών διαδικασιών
  - Επιτρέπει στους χρήστες να κλωνοποιούν και να βελτιώνουν υπάρχοντες χάρτες δεδομένων, καθιστώντας τη διαδικασία αποτελεσματική και επεκτάσιμη
  - Επιτρέπει στους χρήστες να περιγράψουν τη ροή πληροφοριών σε ένα οπτικό, εύκολα κατανοητό artboard
  - Διασφαλίζει ότι οι σωστοί χρήστες και οι ΜΜΕ δημιουργούν, συνεργάζονται και παρέχουν ανατροφοδότηση σχετικά με τις ροές πληροφοριών
  - Παρέχει έξυπνες επιλογές σύνδεσης που παρακολουθούν τα χαρακτηριστικά προσωπικών δεδομένων μαζί με τη ροή πληροφοριών
  - Λειτουργεί ως το απόθεμα όλων των περιουσιακών στοιχείων της επιχειρηματικής ροής.

- Επιτρέπει στους χρήστες να περιγράψουν τη ροή πληροφοριών σε ένα οπτικό, εύκολα κατανοητό artboard.
- Λειτουργεί ως διεπαφή με το σύστημα εγγραφής για τη συλλογή πληροφοριών σχετικά με τις ροές δεδομένων καταγράφοντας όλα τα χαρακτηριστικά αυτής της ροής, συμπεριλαμβανομένων της κατεύθυνσης, των ιδιοτήτων, των περιορισμών και της ιδιοκτησίας
- Μειώνει τις αβεβαιότητες στις επιχειρηματικές ροές όπου κανονικά θα πρέπει να ζητηθεί η γνώμη ενός ή περισσότερων ειδικών σε θέματα.
- Υποστηρίζει επιχειρηματικές και οργανωτικές δυνατότητες λήψης αποφάσεων μέσω ενός συνδυασμού εγγραφών επιχειρηματικής ροής, μεταδεδομένων στοιχείων, ιδιοκτησίας συστήματος και πληροφοριών που δημιουργούνται από το σύστημα, συμπεριλαμβανομένων ταξινόμησης δεδομένων και ειδοποιήσεων απορρήτου.

- <u>Ένα Σύστημα Δέσμευσης και Συνεργασίας</u>

  Ένα τέτοια σύστημα επιτρέπει:
  - Αντιστοίχιση σύνθετων ροών δεδομένων και διαγραμμάτων επιχειρηματικών διαδικασιών σε ένα ευέλικτο και συνεργατικό artboard
  - Συνεργασία με πολλούς ειδικούς σε θέματα και ιδιοκτήτες διεργασιών/λύσεων απρόσκοπτα σε έναν ενιαίο, συλλογικό χάρτη δεδομένων
  - Δυνατότητες ανταλλαγής μηνυμάτων για επικοινωνία και πρόσκληση συνεργατών
  - Συνεργασία με ομάδες σε οποιαδήποτε συσκευή σε πολλές πλατφόρμες και γεωγραφικές περιοχές
  - Ένα συνεργατικό, εύκολο στη χρήση περιβάλλον που διασφαλίζει ότι ο χάρτης δεδομένων είναι πάντα ενημερωμένος μέσω αυτοματισμού, ειδοποιήσεων και ειδοποιήσεων πολιτικής
- <u>Ένα σύστημα αυτοματισμού και διορατικότητας</u>

  Ένα σύστημα αυτοματισμού επιτρέπει:
  - Αυτοματοποιημένη δημιουργία χάρτη δεδομένων μέσω απορρόφησης μεταδεδομένων
  - Αυτόματη σάρωση και ταξινόμηση δεδομένων σε εκατοντάδες τοποθεσίες για συμπλήρωση ιδιοτήτων για στοιχεία χάρτη.

- Η χρήση των χαρακτηριστικών προσωπικών δεδομένων που ανακαλύφθηκαν κατά τη διάρκεια των ζωντανών σαρώσεων δεδομένων ως μεταδεδομένων στοιχείων στους χάρτες δεδομένων
- Περιοδικές εκ νέου σαρώσεις για να διασφαλιστεί ότι τα δεδομένα είναι πάντα ενημερωμένα
- Αυτόματη παρακολούθηση στοιχείων χαρτών και ροών διεργασιών για παραβιάσεις συμμόρφωσης, όπως συλλογή δεδομένων χωρίς συναίνεση, ακατάλληλα δικαιώματα πρόσβασης κ.λπ.
- Ανάλυση επιπτώσεων παραβίασης, όπως ισχύει για τις ροές δεδομένων και τις επιχειρηματικές διαδικασίες
  Ειδοποιήσεις βάσει πολιτικής για τον εντοπισμό αδύναμων διαδικασιών ασφάλειας ή/και μη συμμόρφωσης με νομικές ή κανονιστικές απαιτήσεις
- Παρακολούθηση συναίνεσης σε κάθε στάδιο της ροής δεδομένων και επισήμανση δεδομένων που ενδέχεται να συλλεχθούν, να αποθηκευτούν ή να υποβληθούν σε επεξεργασία χωρίς συγκατάθεση

Τέλος αναφέρουν πως η χαρτογράφηση δεδομένων με μη αυτόματες μεθόδους απλώς δεν πρόκειται να περιορισ**τ**εί δεδομένου του πρόσθετου χρόνου, του κόστους και των πόρων - για να μην αναφέρουμε τον κίνδυνο εξάπλωσης δεδομένων και ανθρώπινου λάθους. Για να επωφεληθεί από μια πραγματικά ισχυρή δομή χαρτογράφησης δεδομένων, κάθε επιχείρηση πρέπει να υιοθετήσει το πλαίσιο PrivacyOps. Η επένδυση σε ένα τέτοιο πλαίσιο θα είναι εξαιρετικά επωφελής για οποιονδήποτε οργανισμό, καθώς θα είναι έτοιμος να συμμορφωθεί με όλους τους κανονισμούς περί απορρήτου δεδομένων - όχι μόνο τους τρέχοντες αλλά και αυτούς που πρόκειται να ακολουθήσουν.

6.3 Πως το Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών υπολογιστών του Πανεπιστημίου Πελοποννήσου να προετοιμαστεί για τον Γενικό Κανονισμό Προστασίας Δεδομένων.

Εκτός από τις επιχειρήσεις θα πρέπει να συμμορφωθούν και τα πανεπιστήμια στον Γενικό Κανονισμό Προστασίας Δεδομένων. Αυτό βέβαια μπορεί να είναι μεγάλη ανατροπή για να

πανεπιστήμια αλλά και να στοιχίσει σε πόρους. Μελετώντας το άρθρο της Kate Tattersfield με τίτλο How universities have to adapt under the new EU General Data Protection Regulation (GDPR) [15].

Το άρθρο αναφέρει κάποια βήματα τα όποια θα πρέπει να ακολουθήσουν τα πανεπιστήμια για την ομαλή ένταξη τους στον ΓΚΠΔ.

- **Βήμα 1: Γνωρίστε τα δεδομένα από μέσα προς τα έξω**

  Αυτά το βήμα σχετίζεται αποκλειστικά με την αναθεώρηση. Τα πανεπιστήμια θα πρέπει να κατανοήσουν ποια δεδομένα κατέχουν επί του παρόντος, εισέρχονται και ποίες είναι οι πηγές μαζί με το ποιος έχει πρόσβαση σε αυτά. Γνωρίζοντας αυτό θα διασφαλιστεί ότι το ίδρυμα είναι σε συγχρονισμό με την προαναφερθείσα πτυχή λογοδοσίας του κανονισμού.

  Είναι επίσης χρήσιμο να αναθεωρήσετε τον νέο Κώδικα Πρακτικής της Δήλωσης Απορρήτου του ICO και να αξιολογήσετε τον τρόπο με τον οποίο λαμβάνεται αυτή τη στιγμή η συγκατάθεση από το πανεπιστήμιο. επίσης, τη βάση στην οποία μοιράζεται με τρίτες εταιρείες. Τα ιδρύματα θα πρέπει να στοχεύουν στην ανάπτυξη μιας στρατηγικής «απόρρητο βάσει σχεδιασμού» εφαρμόζοντας αξιολογήσεις επιπτώσεων στο απόρρητο για νέα επεξεργασία δεδομένων.

- **Βήμα 2: Ορίστε έναν υπεύθυνο προστασίας δεδομένων (DPO)**

  Οι υπεύθυνοι προστασίας δεδομένων με ορθή κατανόηση του Γενικού Κανονισμού αποτελούν το σημαντικότερο “ περιουσιακό στοιχείο ” ενός ιδρύματος όσο αφορά το Κανονισμό. Διαχειρίζονται την διαδικασία της μεταβίβασης καθώς είναι υπεύθυνοι για την διατήρηση της συμμόρφωσης της σχολής με του κανόνες. Παράλληλα έχει και τον ρόλο του εκπαιδευτικού εξηγώντας τις αλλαγές με τρόπο που είναι τόσο απλός όσο και σχετικός με το ίδρυμα στο οποίο εργάζονται. Σύμφωνα με το Άρθρο 29 του Κανονισμού η ομάδα

- **Βήμα 3: Τα ιδρύματα θα πρέπει να βεβαιωθούν ότι τα δικαιώματα ενός ατόμου μπορούν να επικυρωθούν**

  Το σημαντικότερο σημείο του ΓΚΠΔ είναι ότι προσφέρει στα άτομα περισσότερα δικαιώματα και ελέγχους στα προσωπικά τους δεδομένα. Αρχικά τα πανεπιστημιακά ιδρύματα θα πρέπει να έχουν διασφαλίσει ότι τα νέα δικαιώματα προστατεύονται στο έπακρο.

Λειτουργίες Γραμματείας τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Πληροφορικής

βήμα1: Συλλογή δεδομένων για τις τρέχουσες δραστηριότητες της για την προστασία δεδομένων (π.χ. (i) ποιες οντότητες/τμήματα επεξεργάζονται τι είδους δεδομένα για ποιους σκοπούς, (ii) εσωτερικές ευθύνες, (iii) πως προστατεύονται τα δεδομένα των υποκειμένων (iv) έχουν οριστεί υπεύθυνοι προστασίας δεδομένων, (v) ποια μέτρα ασφαλείας ισχύουν Σε ένα δεύτερο βήμα, η εταιρεία πρέπει να αξιολογήσει ποιες απαιτήσεις που απορρέουν από τον GDPR ισχύουν ειδικά.

i. ποιες οντότητες/τμήματα επεξεργάζονται τι είδους δεδομένα για ποιους σκοπού

- Οντότητες/τμήματα:
  - καθηγητές
  - Φοιτητές
  - Διοικητικά μέλη
  - Ερευνητικά μέλη
- τι είδους δεδομένα:
  - Φυλετική ή εθνοτική καταγωγή που ανήκουν στα ευαίσθητα δεδομένα
  - Δεδομένα Υγείας : σχετικά με την νόσο Covid-19
  - Βιομετρικά δεδομένα: δεδομένα επιτρέπουν ή επιβεβαιώνουν την μοναδική ταυτότητα του ατόμου
  - Προσωπικά δεδομένα
    - όνομα
    - Στοιχεία κατοικίας
    - Στοιχεία σχολικής ταυτότητας
    - IP
- Σκοποί επεξεργασίας

ii. Εσωτερικές Ευθύνες

- Email
- Estudents
- Eclass

ΦΟΙΤΗΤΕΣ

ΜΗΤΡΩΟ	Τηρείται σε φυσική ή ηλεκτρονική μορφή	Στο φυσικό μητρώο έχουν πρόσβαση μόνο τα μέλη της γραμματείας και χωρίζεται σε 3 μέρη : 1) Ενεργοί φοιτητές 2) Πτυχιούχοι 3) Διαγραμμένοι	Ο Αριθμός Μητρώου μπορεί να δημοσιευθεί ελεύθερα καθώς είναι ατομικός και μόνο η γραμματεία και ο φοιτητής γνωρίζει ότι του ανήκει. Άρα το ονοματεπώνυμο στο οποίο αντιστοιχεί ο Α.Μ. υπόκειται στον νόμο περί προστασίας δεδομένων.

ΕΓΓΡΑΦΕΣ	Γίνονται αρχικά με την αποστολή ονομάτων από το Υπ. Παιδείας με την εξής σειρά : Υπ. Παιδείας → Τμήμα σπουδών Π. Πελοποννήσου (Κόρινθος) → Γραμματεία → Τμήμα ηλεκτρονικής διακυβέρνησης → καταχώριση σε ηλεκτρονικό αρχείο	Κατόπιν καλούνται οι επιτυχόντες (με ανακοίνωση στο site) να στείλουν στοιχεία αυτοπροσωπείας (αντίγραφο ΑΔΤ, ηλεκτρονική προεγγραφή από ΥΠ. Παιδείας) και με τα στοιχεία αυτά δημιουργείται και το φυσικό αρχείο	Οι πρωτοετείς φοιτητές ενημερώνονται αρχικά μέσω των προσωπικών τους email με την επιλογή BCC και κατόπιν στις λίστες φοιτητών που έχουν αποδέκτες τα ακαδημαϊκά τους email όπου ο κάθε φοιτητής έχει πρόσβαση μέσω κωδικών που εκδίδει μόνος του μέσω του site studentaccount.uop.gr	Η γραμματεία οφείλει να ενημερώνει ατομικά τον ενδιαφερόμενο φοιτητή και να έχει ως αποδέκτη αποκλειστικά τον ίδιον καθώς η κοινοποίηση των στοιχείων του έρχεται ενάντια στον νόμο GDPR.

ΜΕΤΑΓΡΑΦΕΣ	Οι αιτήσεις γίνονται σε πλατφόρμα του Υπ. Παιδείας και στη γραμματεία ανακοινώνονται τα τελικά αποτελέσματα. Κατόπιν ελέγχου μέρους των δικαιολογητικών μοριοδότησης (όλα εκτός των οικονομικών που ελέγχονται από την ΑΑΔΕ) καλούνται οι επιτυχόντες να ολοκληρώσουν τη μεταγραφή τους προσκομίζοντας διαγραφή από το τμήμα προέλευσης	Για τις ΜΕΤΑΓΑΦΕΣ ισχύει ακριβώς το ίδιο με τις ΕΓΓΡΑΦΕΣ.

ΚΑΤΑΤΑΚΤΗΡΙΕΣ ΕΞΕΤΑΣΕΙΣ	Τα ονόματα των επιτυχόντων των κατατακτήριων εξετάσεων ανακοινώνονται με αριθμό Δελτίου Ταυτότητας ή Μισά Ονόματα	Σύμφωνα με τον νόμο GDPR απαγορεύεται η δημοσιοποίηση των ονομάτων των φοιτητών γι΄αυτό τον λόγο εμφανίζονται μόνο τα αρχικά του ονοματεπωνύμου ή ο αριθμός ταυτότητας

ΔΙΑΓΡΑΦΗ ΦΟΙΤΗΤΩΝ	Για την διαγραφή φοιτητών πρέπει οι ενδιαφερόμενοι να προσκομίσουν Υπεύθυνη Δήλωση που να ζητούν τη διαγραφή τους.	Η υπεύθυνη δήλωση πρέπει να έχει εκδοθεί από το gov.gr ή με γνήσιο υπογραφής από ΚΕΠ	Τα στοιχεία των φοιτητών που διαγράφονται από ένα τμήμα υπόκεινται στον νόμο περί προστασίας δεδομένων. Έτσι η γραμματεία ενημερώνει ατομικά τους φοιτητές.

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ	Η πτυχιακή εργασία εκπονείται και	Μετά την εξέταση κατατίθεται στη	Η δημοσίευση των στοιχείων των

	παρουσιάζεται σύμφωνα με τον κανονισμό διπλωματικών.	βιβλιοθήκη και είναι διαθέσιμη διαδικτυακά	φοιτητών καθώς και το θέμα της πτυχιακής εργασίας που εκπονούν δεν υπόκειται στον νόμο GDPR οπότε τα στοιχεία είναι ελεύθερα στην δημοσίευση τους αλλά και η ίδια η εργασία μπορεί να δημοσιευθεί.

ΔΗΛΩΣΗ ΜΑΘΗΜΑΤΩΝ	Eclass, estudents, eudoxws, academic κλπ	Πραγματοποιούνται ηλεκτρονικά σε πλατφόρμες με χρήση προσωπικών κωδικών	Η δήλωση μαθημάτων γίνεται ατομικά από τους φοιτητές με τα προσωπικά τους στοιχεία.

ΒΑΘΜΟΛΟΓΙΑ	Οι βαθμολογίες κατατίθενται από τους διδάσκοντες και καταχωρούνται μαζικά.	Οι φοιτητές μπορούν να λάβουν γνώσει μόνο μέσω estudents με χρήση προσωπικών κωδικών.	Η δημοσίευση των βαθμολογιών μαζί με τα ονόματα των φοιτητών είναι παράνομη αφού είναι προσωπικά δεδομένα. Αυτός είναι ο λόγος που η γραμματεία καταθέτει την βαθμολογία ατομικά.

ΒΕΒΑΙΩΣΕΙΣ	Οι βεβαιώσεις και οι αναλυτικές	Οι βεβαιώσεις που

	εκδίδονται μετά από αίτηση μέσω estudents ή από το ακαδημαϊκό email και αποστέλλονται στα ακαδημαϊκά τους email.	ζητούν οι φοιτητές είναι προσωπικά στοιχεία και η γραμματεία τις εκδίδει ατομικά στον ενδιαφερόμενο φοιτητή στους προσωπικούς ακαδημαϊκούς λογαριασμούς.

Περιγραφή έργου γραμματείας Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

- Διοικητικά Θέματα
  1. Τήρηση ηλεκτρονικού πρωτοκόλλου εισερχομένων και εξερχομένων εγγράφων που αφορούν το τμήμα,
  2. τήρηση της σχετικής με το τμήμα νομοθεσίας,
  3. σύνταξη και τήρηση πρακτικών των συνεδριάσεων της Συνέλευσης του τμήματος, όπως και των συνεδριάσεων των εκλεκτορικών σωμάτων,
  4. διαδικασία εκλογής, μονιμοποίησης και εξέλιξης μελών Ε.Π.
  5. σύνταξη και διακίνηση διαβιβαστικών εγγράφων που αφορούν το τμήμα,
  6. θέματα που αφορούν έκτακτο προσωπικό του τμήματος,
  7. διακίνηση και εξαγωγή αλληλογραφίας που αφορά θέματα του τμήματος προς το ΥΠ. Π.Ε.Θ και προς άλλους φορείς,
  8. στατιστικά στοιχεία που ζητούνται από υπηρεσίες του ΥΠ. Π.Ε.Θ και αφορούν τα τακτικά μέλη Ε.Π., το εκπαιδευτικό προσωπικό με σύμβαση ορισμένου χρόνου, τους σπουδαστές και το διοικητικό προσωπικό του τμήματος,
  9. αρχειοθέτηση εισερχόμενων και εξερχομένων εγγράφων,
  10. συνεχής και αδιάλειπτη ενημέρωση σε εκπαιδευτικούς, σπουδαστές και πολίτες με καθοιονδήποτε τρόπο.

- Θέματα που αφορούν τους Φοιτητές του τμήματος

1. Τήρηση μητρώου σπουδαστών, εγγραφές και ενημέρωση πρωτοετών,
2. διαδικασίες σχετικά με τις μετεγγραφές σπουδαστών από και προς άλλα Τ.Ε.Ι.
3. διαδικασία σχετικά με κατατακτήριες εξετάσεις στο τμήμα μας πτυχιούχων άλλων τμημάτων της Τριτοβάθμιας εκπ/σης του εσωτερικού,
4. διαδικασία σχετικά με διαγραφές σπουδαστών
5. διαδικασίες σχετικά με την πτυχιακή εργασία και την πρακτική άσκηση των σπουδαστών, που είναι απαραίτητες προϋποθέσεις για την λήψη του πτυχίου τους,
6. καταχώρηση συγγραμμάτων στην πλατφόρμα <<ΕΥΔΟΞΟΣ>>, προκειμένου να χορηγηθούν στους σπουδαστές μετά την ηλεκτρονική τους δήλωση σε ορισμένες προθεσμίες,
7. προετοιμασία για την διεξαγωγή των εξετάσεων και ηλεκτρονική καταχώριση των βαθμολογιών μετά την διεξαγωγή τους,
8. εξαγωγή βεβαιώσεων και αναλυτικών βαθμολογιών μετά από αίτηση των σπουδαστών,
9. έλεγχο για την έκδοση δελτίων ταυτότητας και ειδικού εισιτηρίου, προκειμένου να χορηγηθούν στους σπουδαστές μετά από ηλεκτρονική τους δήλωση,
10. διαδικασία για την χορήγηση πτυχίων στους σπουδαστές και τήρηση μητρώου πτυχιούχων του τμήματος,
11. συνεχής και αδιάλειπτη ενημέρωση στους σπουδαστές μέσω θυρίδας, τηλεφώνου και ανακοινώσεων.

Μηχανογράφηση Τμήματος Ηλεκτρολόγων Μηχανικών Τ.Ε.

Το τμήμα Ηλεκτρολόγων Μηχανικών Τ.Ε. είναι μηχανογραφημένο ως προς τις παρεχόμενες υπηρεσίες αρμοδιότητάς του, τόσο προς τους φοιτητές τους ως προς τους εκπαιδευτικούς, ως προς της γενικότερης μηχανογράφησης του Ιδρύματος.

Α. Φοιτητές

Υπάρχει Φοιτητολόγιο, το οποίο καλύπτει όλες τις φάσεις των προπτυχιακών σπουδών των φοιτητών του Τμήματος: Ατομικά στοιχεία, στοιχεία εγγραφής, στοιχεία επικοινωνίας, πρόγραμμα σπουδών, δηλώσεις μαθημάτων, βαθμολογία, αναφορές, στατιστικά στοιχεία, στοιχεία ΑΜΚΑ κλπ.

Οι φοιτητές έχουν πρόσβαση σε ηλεκτρονικές υπηρεσίες μέσω διαδικτύου. Χρησιμοποιούν τις ηλεκτρονικές υπηρεσίες για πληροφόρηση, υποβολή δηλώσεων μαθημάτων, για χορήγηση βεβαιώσεων σπουδών, για αναλυτική βαθμολογία των μαθημάτων εξεταστικής κλπ.

Η Γραμματεία χρησιμοποιεί τις ηλεκτρονικές υπηρεσίες web για διεκπεραίωση των ζητούμενων αιτήσεων, πληροφόρηση δηλώσεων μαθημάτων, ανάρτηση ανακοινώσεων, αποστολή μαζικών email στους φοιτητές κλπ.,

Η καταχώρηση των συγγραμμάτων γίνεται μέσω της ηλεκτρονικής πλατφόρμας eudoxus.gr και ο έλεγχος των αιτήσεων των φοιτητών για ακαδημαϊκή ταυτότητα πραγματοποιείται μέσω της πλατφόρμας academicid.minedu.gov.gr

Β. Εκπαιδευτικό Προσωπικό

Οι εκπαιδευτικοί χρησιμοποιούν τις ηλεκτρονικές υπηρεσίες για καταχώρηση και κατάθεση της βαθμολογίας των μαθημάτων της εξεταστικής.

Οι Επιστημονικοί και Εργαστηριακοί Συνεργάτες υποβάλλουν μέσω διαδικτύου αίτηση προς το Τμήμα και η Γραμματεία μέσω του λογισμικού που χρησιμοποιεί, ενημερώνεται με τα στοιχεία των αιτούντων.

Το λογισμικό των Συνεργατών χρησιμοποιείται για καταχώρηση με συστημικό τρόπο των αναθέσεων των συνεργατών, την καταχώρηση των μηνιαίων πραγματοποιηθεισών ωρών διδασκαλίας, τη λήψη πληροφοριών για τη ΜΟ.ΔΙ.Π και τη λήψη στατιστικών στοιχείων.

Περιγραφή έργου που επιτελέστηκε

1. Τήρηση ηλεκτρονικού πρωτοκόλλου,
2. ενημέρωση νομοθεσίας,
3. σύνταξη διαβιβαστικών εγγράφων, σύνταξη των πρακτικών των συνεδριάσεων του Συμβουλίου και της Γενικής Συνέλευσης του τμήματος όπως και των εκλεκτορικών σωμάτων,
4. διαδικασίες εκλογής, μονιμοποίησης και εξέλιξης μελών Ε.Π.,
5. ενημέρωση εκπαιδευτικών,
6. διεκπεραίωση θεμάτων σχετικών με εγγραφές, κατατακτήριες εξετάσεις, ορκωμοσίες, και υποτροφίες σπουδαστών,
7. εξαγωγή βεβαιώσεων και αναλυτικών βαθμολογιών, έλεγχο βαθμολογιών και ηλεκτρονική καταχώρηση, έλεγχο πτυχίων, έλεγχο για πάσο,
8. ανάρτηση ανακοινώσεων για ενημέρωση σπουδαστών,
9. συμπλήρωση στατιστικών στοιχείων,
10. θέματα που αφορούν του επιστημονικούς – εργαστηριακούς συνεργάτες του τμήματος,

11. διεξαγωγή αλληλογραφίας και παραγωγή φωτοαντίγραφων,
12. καταχώρηση συγγραμμάτων στο ηλεκτρονικό σύστημα Εύδοξος,
13. τακτοποίηση φυσικού αρχείου,
14. έλεγχο και έκδοση πιστοποιητικού για στεγαστικό επίδομα,
15. έκδοση βιβλιάριου υγείας στους σπουδαστές,
16. διεκπεραίωση πτυχιακής και πρακτικής Άσκησης σπουδαστών,
17. FAX, τηλέφωνα, γρήγορη και σωστή εξυπηρέτηση των σπουδαστών, και των πολιτών μέσω τηλεφώνου ή αλληλογραφίας,
18. άψογη συνεργασία με τους εκπαιδευτικούς του Τμήματος, τους φοιτητές και τους συναδέλφους.

Πίνακας Ορολογίας

Ελληνική Ορολογία	Αγγλική Ορολογία
Γενικός Κανονισμός Προστασίας Δεδομένων	General Data Protection Regulation
Οδηγία 95/46/ΕΚ	Directive 95/46/EC
Κρατικός Νόμος Προστασίας Δεδομένων	State Data Protection Act
Γερμανικό Ομοσπονδιακό Θέσπισμα Προστασίας Δεδομένων το 1977	German Federal Data Protection Act of 1977
Οργανισμός για την Οικονομική Συνεργασία και Ανάπτυξη	Organisation for Economic Co-operation and Development's Recommendations of the Council
"Κατευθυντήριες Γραμμές" για την φύλαξη των προσωπικών στοιχείων και την διακρατική μετακίνηση ιδιωτικών πληροφοριών	non-binding OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
Προστασία των Φυσικών Προσώπων σχετικά με την Αυτόματη Επεξεργασία των Προσωπικών Δεδομένων	Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data
Δεσμευτικοί εταιρικοί κανόνες	Binding Corporate Rules BCRs
Ελεγκτής δεδομένων	Data Protection Act
Εποπτική Αρχή Προστασίας Δεδομένων	Data Protection Impact Assessment
Υπεύθυνος Επεξεργασίας Δεδομένων	Data Protection Officer
Αρχή Προστασίας δεδομένων	Data Protection Authority

Προστασία Προσωπικών Δεδομένων και μέτρα για την εφαρμογή του ΓΚΠΔ	Protection of Personal Data and Measures for the Implementation of the GDPR
Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα	Hellenic Data Protection Authority
Εκτίμηση Επικινδυνότητας	Risk Assessment
Εκτίμηση Αντίκτυπου Προστασίας Δεδομένων	Data Protection Impact Assesment
Τεχνικά και Οργανωτικά μέτρα	Technical and Organisation Measures
Εκτίμηση Επιπτώσεων Μεταφοράς	Transfer Impact Assesment
Η Ευρωπαϊκή Διοίκηση των Ηνωμένων Πολιτειών	The European Administration of the United States
Χάρτη των θεμελιωδών δικαιωμάτων της ΕΕ	Map of Fundamental Rights of EU

Βιβλιογραφικές Αναφορές

1. 2021. [online] Available at: <https://www.ey.com/en_gr/tax/tax-alerts/ey-law-alert-law-4624-2019-protection-of-personal-data-and-measures-for-the-implementation-of-the-gdpr> [Accessed 21 July 2021].
2. Ευρωπαϊκή Ένωση. 2021.*Κανονισμοί, οδηγίες και άλλες νομοθετικές πράξεις | Ευρωπαϊκή Ένωση*. [online] Available at: <https://europa.eu/european-union/law/legal-acts_el> [Accessed 6 June 2021].
3. Ευρωπαϊκή Επιτροπή - European Commission. 2021. *Τι κανόνες ισχύουν εάν ο οργανισμός μου διαβιβάζει δεδομένα εκτός της ΕΕ;*. [online] Available at: <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_el> [Accessed 2 December 2021].
4. ΜεΤοΔικηγόρο |. 2022.*Οδηγός GDPR για Δικηγόρους/e-HelpDesk/ΜεΤοΔικηγόρο | ΜεΤοΔικηγόρο*. [online] Available at: <https://www.metodikigoro.gr/odhgos-gdpr-gia-dikhgorous-ehelp-desk-metodikigoro/> [Accessed 21 January 2022].
5. Arampatzis, A., 2021.*What are the 7 Principles of the GDPR?*. [online] ITEGRITI. Available at: <https://itegriti.com/2020/compliance/what-are-seven-principles-gdpr/> [Accessed 11 June 2021].

6. Cano, S., 2021.*What is Schrems II and how does it affect your data protection in 2021? - Thales blog*. [online] Thales blog. Available at: <https://dis-blog.thalesgroup.com/security/2021/04/29/what-is-schrems-ii-and-how-does-it-affect-your-data-protection-in-2021/> [Accessed 5 December 2021].

7. Datenschutz-Grundverordnung (DSGVO). 2021. *Art. 4 DSGVO – Begriffsbestimmungen | Datenschutz-Grundverordnung (DSGVO)*. [online] Available at: <https://dsgvo-gesetz.de/art-4-dsgvo/> [Accessed 14 July 2021].

8. Dione.lib.unipi.gr. 2021. [online] Available at: <https://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/12210/%CE%92%CE%91%CE%9B%CE%91%CE%92%CE%91%CE%9D%CE%97%CE%A3%20%20GDPR.pdf?sequence=5&isAllowed=y> [Accessed 3 June 2021].

9. Döring, P., Schwabe, C., Schwabe, C., clauses, T., Schwabe, C., Schwabe, C., FIDO2, P., Döring, P., Döring, P. and Internet, D., 2021.*Data transmission to countries outside the European Union (third countries)*. [online] Robin Data GmbH. Available at: <https://www.robin-data.io/en/data-protection-academy/wiki/data-transmission-to-third-countries> [Accessed 4 December 2021].

10. Dpa.gr. 2022. [online] Available at: <https://www.dpa.gr/sites/default/files/2019-09/apofasi142019.pdf> [Accessed 21 February 2022].

11. Ec.europa.eu. 2021. [online] Available at: <https://ec.europa.eu/info/sites/default/files/data-protection-factsheet-sme-obligations_en.pdf> [Accessed 15 June 2021].

12. epixeiro.gr *Η επιχειρηματικότητα στο προσκήνιο. 2021.Μια ιστορική αναδρομή για το πως φτάσαμε στο GDPR.* [online] Available at: <https://www.epixeiro.gr/article/86602> [Accessed 5 June 2021].

13. EUGDPRAcademy. 2021.*GDPR Data Protection Impact Assessment: 5-step methodology*. [online] Available at: <https://advisera.com/eugdpracademy/knowledgebase/5-phases-of-the-eu-gdpr-data-protection-impact-assessment/> [Accessed 9 June 2021].

14. Fincen.gov. 2021.*USA PATRIOT Act | FinCEN.gov*. [online] Available at: <https://www.fincen.gov/resources/statutes-regulations/usa-patriot-act> [Accessed 4 December 2021].

15. Fullfabric.com. 2022. *How universities have to adapt under the new EU General Data Protection Regulation (GDPR) | Full Fabric*. [online] Available at:

<https://www.fullfabric.com/articles/how-universities-have-to-adapt-under-the-new-eu-general-data-protection-regulation-gdpr> [Accessed 15 January 2022].

16. Ico.org.uk. 2021. *Personal data breaches*. [online] Available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/> [Accessed 14 July 2021].

17. Icsd.aegean.gr. 2021. [online] Available at: <http://www.icsd.aegean.gr/website_files/proptyxiako/133077942.ppt> [Accessed 3 June 2021].

18. Irwin, L., 2021. *GDPR | Personal Data vs Sensitive Data: What's the Difference?*. [online] IT Governance UK Blog. Available at: <https://www.itgovernance.co.uk/blog/the-gdpr-do-you-know-the-difference-between-personal-data-and-sensitive-data#what-is-sensitive-personal-data> [Accessed 14 July 2021].

19. Karalivanos, P. and S.A., N., 2021.*GDPR: Τι είναι; Ορισμός, Πεδίο Εφαρμογής και Παραδείγματα - ΝΗΡΗΪΣ Α.Ε.*. [online] ΝΗΡΗΪΣ Α.Ε. Available at: <https://www.niriis.gr/gdpr/gdpr-ti-einai/> [Accessed 6 June 2021]

20. Knowyourcompliance.com. 2021. [online] Available at: <https://www.knowyourcompliance.com/gdpr-technical-organisational-measures/> [Accessed 22 November 2021].

21. Lawspot. 2021.*Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995*. [online] Available at: <https://www.lawspot.gr/nomikes-plirofories/nomothesia/odigia-95-46-ek-toy-eyropaikoy-koinovoylioy-kai-toy-symvoylioy-tis> [Accessed 3 June 2021].

22. Lawspot.gr. 2021. *Συγκατάθεση | Lawspot*. [online] Available at: <https://www.lawspot.gr/gdpr/consent> [Accessed 20 July 2021].

23. Lawspot.gr. 2021.*Συχνές Ερωτήσεις GDPR | Lawspot.* [online] Available at: <https://www.lawspot.gr/gdpr/faq> [Accessed 5 June 2021].

24. Lexology. 2021.*Step Plan GDPR Implementation.* [online] Available at: <https://www.lexology.com/library/detail.aspx?g=c6e07042-2af5-4214-9ac8-d1b510d62ce7> [Accessed 11 December 2021].

25. Mark Consulting. 2021.*Mark Consulting - GDPR DPO.* [online] Available at: <https://www.markconsulting.gr/services/gdrp-dpo/> [Accessed 5 June 2021]

26. Naftemporiki.gr. 2021.*Προστασία δεδομένων: Από τους πρώτους νόμους του '70 στον GDPR.* [online] Available at: <https://www.naftemporiki.gr/finance/story/1559429/gdpr> [Accessed 1 June 2021].

27. Privacy & Information Security Law Blog. 2021.*CNIL Publishes Six Step Methodology and Tools to Prepare for GDPR*. [online] Available at: <https://www.huntonprivacyblog.com/2017/03/17/cnil-publishes-six-step-methodology-tools-prepare-gdpr/> [Accessed 10 June 2021].

28. Scribd. 2022.*MetaCompliance Best Practices Implementation Guide | PDF | Personally Identifiable Information | Information Privacy.* [online] Available at: <https://www.scribd.com/document/377357428/MetaCompliance-Best-Practices-Implementation-Guide> [Accessed 19 January 2022].

29. SearchDataBackup. 2021*6 business benefits of data protection and GDPR compliance*. [online] Available at: <https://searchdatabackup.techtarget.com/tip/6-business-benefits-of-data-protection-and-GDPR-compliance> [Accessed 15 June 2021].

30. Securiti. 2021.*GDPR Data Mapping: How to conduct and comply? - Securiti*. [online] Available at: <https://securiti.ai/blog/gdpr-data-mapping/> [Accessed 11 December 2021].

31. Shanley, D., 2021.*6 Steps to Prepare for General Data Protection Regulation*. [online] Flowforma.com. Available at: <https://www.flowforma.com/blog/6-steps-to-prepare-for-general-data-protection-regulation> [Accessed 10 June 2021].

32. SixFifty. 2022.*GDPR Penalties and Type of Violations | GDPR Compliance | SixFifty*. [online] Available at: <https://www.sixfifty.com/gdpr-penalties-and-type-of-violations/> [Accessed 21 February 2022].

33. Target Integration. 2021.*8 Rights given to every EU citizen by GDPR - Target Integration*. [online] Available at: <https://www.targetintegration.com/8-rights-by-gdpr-to-eu-citizen/> [Accessed 8 June 2021].

34. Taxheaven.gr. 2021.*Άρθρα Τι είναι ο «GDPR» και ποιες οι υποχρεώσεις των επιχειρήσεων.* [online] Available at: <https://www.taxheaven.gr/circulars/27607/arora-ti-einai-o-gdpr-kai-poies-oi-ypoxrewseis-twn-epixeirhsewn> [Accessed 9 June 2021].

35. Vollmer, N., 2022.*Άρθρο 39 ΕΕ Γενικός Κανονισμός για την Προστασία Δεδομένων. Privacy/Privazy according to plan.*. [online] Privacy-regulation.eu. Available at: <https://www.privacy-regulation.eu/el/39.htm> [Accessed 21 February 2022].

36. Wolterskluwer.com. 2021.*Data Transfer to unsafe Third Countries*. [online] Available at: <https://www.wolterskluwer.com/en/expert-insights/data-transfer-to-unsafe-third-countries> [Accessed 10 December 2021].

37. Wwwmatthes.in.tum.de. 2021. [online] Available at: <https://wwwmatthes.in.tum.de/file/14qun4klf0r0d/Sebis-Public-Website/-/Appropriate-Technical-and-Organizational-Measures-Identifying-Privacy-Engineering-Approaches-to-Meet-GDPR-Requirements/Huth%20AMCIS2019.pdf> [Accessed 26 November 2021].