ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ
ΤΜΗΜΑ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ
ΠΜΣ ΔΗΜΟΣΙΑ ΔΙΟΙΚΗΣΗ - ΔΗΜΟΣΙΟ ΜΑΝΑΤΖΜΕΝΤ

Διπλωματική εργασία που εκπονήθηκε στο Π.Μ.Σ. «Δημόσια Διοίκηση – Δημόσιο Μάνατζμεντ»

Η προστασία των Προσωπικών Δεδομένων των εργαζομένων στον Δημόσιο και Ιδιωτικό Τομέα υπό το πρίσμα των πρόσφατων νομοθετικών εξελίξεων (σύγκριση - αντιπαραβολή και προοπτικές εξέλιξης)

The protection of the employee's personal data in the Public and Private sector under the prism of recent legislative developments (comparison-comparisons and prospects of development)

ΜΑΡΙΑ ΛΟΥΝΤΟΥ
ΑΜ :1842

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΑΠΟΣΤΟΛΟΣ ΜΑΝΘΟΣ

ΑΙΓΑΛΕΩ ΙΟΥΝΙΟΣ 2021

Τα μέλη της Τριμελούς Επιτροπής

κ. Α.Μάνθος	κ. Σ.Ντάνος	κ. Σ.Μακρίδης
APOSTOLOS MANTHOS Digitally signed by APOSTOLOS MANTHOS Date: 2021.06.29 19:58:14 +03'00'	Stamatios Ntanos Digitally signed by Stamatios Ntanos Date: 2021.06.29 22:24:47 +03'00'	SAVVAS MAKRIDIS Digitally signed by SAVVAS MAKRIDIS Date: 2021.07.01 00:59:29 +03'00'

ΥΠΕΥΘΥΝΗ ΔΗΛΩΣΗ

Αυτή η διπλωματική εργασία υποβάλλεται από τον/την συγγραφέα της ως μερική εκπλήρωση των απαιτήσεων του Προγράμματος Μεταπτυχιακών Σπουδών «Δημόσια Διοίκηση – Δημόσιο Μάνατζμεντ» του Τμήματος Διοίκησης Επιχειρήσεων του Πανεπιστημίου Δυτικής Αττικής.

Υπεύθυνα δηλώνεται ότι, η συγκεκριμένη διπλωματική εργασία είναι πρωτότυπη και ότι εκπονήθηκε αποκλειστικά και μόνο από την Υπογράφουσα και μόνο για την απόκτηση του συγκεκριμένου μεταπτυχιακού τίτλου. Δεν έχει υποβληθεί ούτε έχει αξιολογηθεί στο πλαίσιο άλλου μεταπτυχιακού τίτλου σπουδών, στην Ελλάδα ή στο εξωτερικό.

Σε περίπτωση που διαπιστωθεί ότι μέρος της διπλωματικής εργασίας δεν αποτελεί πρωτότυπη δουλειά, αλλά αντιγραφή ήδη δημοσιευμένης εργασίας, ο/η φοιτητής/τρια θα απορρίπτεται οριστικά από το συγκεκριμένο πρόγραμμα σπουδών.

Ονοματεπώνυμο / Υπογραφή

Μαρία Λούντου

Στην οικογένεια μου

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

ΑΠΔΠΧ	Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
ΓΚΠΔ	Γενικός Κανονισμός Προστασίας Δεδομένων
ΕΣΔΑ	Ευρωπαϊκή Σύμβαση των Δικαιωμάτων του Ανθρώπου
Σ	Σύνταγμα

ΕΥΧΑΡΙΣΤΙΕΣ

Η παρούσα διπλωματική εργασία εκπονήθηκε στα πλαίσια του ΠΜΣ «*Δημόσια Διοίκηση – Δημόσιο Μάνατζμεντ*» του Τμήματος Διοίκησης Επιχειρήσεων του Πανεπιστημίου Δυτικής Αττικής.

Αισθάνομαι υποχρέωση να ευχαριστήσω όλους όσους συνέβαλαν με οποιοδήποτε τρόπο στην ολοκλήρωση των σπουδών μου και στην πραγματοποίησή της διπλωματικής μου εργασίας και ιδιαίτερα την οικογένεια μου που με ανέχτηκε όλη αυτή τη κοπιαστική περίοδο.

Τέλος, θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή κ. Μάνθο Απόστολο για την ευκαιρία που μου έδωσε να ασχοληθώ με ένα τόσο ενδιαφέρον θέμα, όπως επίσης και για την καθοδήγηση, τις σημαντικές υποδείξεις και τις διορθώσεις, που ήταν απαραίτητες για την επιτυχή ολοκλήρωσή της, καθώς και το σύνολο των καθηγητών μου στο μεταπτυχιακό πρόγραμμα για τις γνώσεις που μου μετέφεραν.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΔΙΑΓΡΑΜΜΑΤΩΝ

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

ΠΕΡΙΛΗΨΗ

Οι εξελίξεις στον τομέα της τεχνολογίας διευκολύνουν την αθέμιτη και ανεξέλεγκτη επεξεργασία των προσωπικών δεδομένων των εργαζομένων. Το ζήτημα που ανακύπτει είναι κρίσιμο γιατί παρέχονται πλέον οι τεχνικές δυνατότητες για πρόσβαση σε προσωπικά δεδομένα που δεν σχετίζονται με την εργασία και μπορεί να αποτελέσουν ζήτημα εκβιασμού ή απόλυσης στην εργασία. Συγκεκριμένα, στην παρούσα εργασία σκοπός της είναι εκτός της παρουσίασης του ΓΚΠΔ, η επικέντρωση σε μία προβληματική της προστασίας των προσωπικών δεδομένων, ήτοι στην προστασία των προσωπικών δεδομένων των εργαζομένων στον ιδιωτικό και δημόσιο τομέα με τη μορφή της σύγκρισης και αντιπαραβολής και υπό το πρίσμα των πρόσφατων νομοθετικών εξελίξεων. Τα δικαιώματα του υποκειμένου των δεδομένων είναι κατ' επέκταση και δικαιώματα των εργαζομένων. Στο ελληνικό Σύνταγμα σύμφωνα με το άρθρο 9Α για το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα, δεν προσδιορίζονται επακριβώς τα δικαιώματα αυτά. Στον ΓΚΠΔ τα δικαιώματα προσδιορίζονται επακριβώς και αποτελούν ένα από τα ουσιώδη στοιχεία του, ενώ εισάγονται και νέα δικαιώματα (φορητότητα, δικαίωμα στη λήθη κ.α.). Συνολικά, ανεξάρτητα αν είναι ή όχι εργαζόμενος στο δημόσιο τομέα, στον ΓΚΠΔ ο εργαζόμενος ως υποκείμενο προσωπικών δεδομένων δεν περιορίζεται στον πάροχο της εργασίας, αλλά περιλαμβάνει και τον υποψήφιο παροχής εργασίας και τον τερματίσαντα την παροχή εργασίας. Οι εργαζόμενοι στο δημόσιο τομέα υπερτερούν σε ωφελήματα από πλευράς ΓΚΠΔ σε σχέση με τους εργαζόμενους στο ιδιωτικό τομέα. Αυτό οφείλεται στη φύση του δημόσιου τομέα. Ωστόσο, η νέα νομοθεσία για την προστασία προσωπικών δεδομένων προσωπικού παρέχει ένα ασφαλές νομικό πλαίσιο για την αντιμετώπιση δύσκολων καταστάσεων. Η στήριξη σε βασικές αρχές επεξεργασίας δεδομένων και ο σεβασμός της αρχής της αναλογικότητας, ωθεί την προστασία των προσωπικών δεδομένων στην αρμονική συνύπαρξη με άλλα συγκρουόμενα αγαθά, ακόμα και σε περιόδους κρίσεως όπως η σημερινή.

Λέξεις Κλειδιά - Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, ΓΚΠΔ, Εργασιακές Σχέσεις, Σύνταγμα, Ιδιωτικότητα, προστασία προσωπικών δεδομένων, Δημόσια Διοίκηση

ABSTRACT

Developments in technology facilitate the unfair and uncontrolled processing of employees' personal data. The issue that arises is crucial because the technical possibilities for access to personal data that are not related to work are now provided and can be a matter of blackmail or dismissal at work. In particular, in the present work, its purpose is, apart from the presentation of the GDPR, to focus on a problem of the protection of personal data, that is, in the protection of personal data of employees in the private and public sector in the form of comparison and comparison and in the light of recent legislative developments. The rights of the data subject are therefore also the rights of the employees. The Greek Constitution, in accordance with Article 9A on the right to the protection of personal data, does not specify these rights. In the GDPR, the rights are precisely defined and constitute one of its essential elements, while new rights are introduced (portability, right to be forgotten, etc.). Overall, regardless of whether or not he is a public sector employee, in the GDPR the employee as a personal data subject is not limited to the job provider, but also includes the job applicant and the person terminating the job. Public sector employees outweigh the benefits in terms of GDPR over private sector employees. This is due to the nature of the public sector. However, the new legislation on the protection of personal data provides a secure legal framework for dealing with difficult situations. Relying on basic data processing principles and respecting the principle of proportionality, pushes the protection of personal data in the harmonious coexistence with other conflicting goods, even in times of crisis such as today.

Key words - Personal Data Protection Authority, GCC, Labor Relations, Constitution, Privacy, personal data protection, Public Administration

ΕΙΣΑΓΩΓΗ

Οι τεχνολογικές εξελίξεις στην Πληροφορική και Επικοινωνίες σε συνδυασμό με την επερχόμενη 4η Βιομηχανική Επανάσταση, οδηγούν σε νέες μορφές εργασίας, προκαλώντας ένα νέο περιβάλλον εργασιακών σχέσεων και αλλάζουν την ισορροπία μεταξύ εργασιακού και ιδιωτικού βίου. Η νέα τεχνολογία παρέχει στους εργοδότες τα εργαλεία να έχουν άνετη και εύκολη "χρήση" των προσωπικών δεδομένων του ανθρώπινου δυναμικού τους (διαδίκτυο, κινητά τηλέφωνα, μέσα κοινωνικής δικτύωσης κ.α.), μέχρι και την παρακολούθηση τους στο εργασιακό περιβάλλον. Επιπλέον, οι εργασιακές σχέσεις έχουν αλλάξει, με αποτέλεσμα ο εργαζόμενος να αλλάζει εργοδότη πιο συχνά, προσφέροντας έτσι δυνατότητες πρόσβασης χωρίς περιορισμούς από την πλειοψηφία των εργοδοτών.

Το ζήτημα της ασφάλειας των ατομικών δεδομένων αποτελεί αντικείμενο δημόσιας συζήτησης, το οποίο η τεχνολογική εξέλιξηέχει τρφοδοτήσει περαιτέρω λόγω των νέων κινδύνων που προκύπτουν για την προσωπικότητα και το ιδιωτικό βίο των εργαζομένων. Υπάρχει πλέον μια σύγκρουση συμφερόντων μεταξύ εργοδότη - εργαζόμενου στο χώρο των προσωπικών δεδομένων.

Από τη μια πλευρά η όποια εργοδοσία στα πλαίσια άσκησης του διευθυντικού της δικαιώματος, επιθυμεί να ελέγξει τη συμμόρφωση του εργαζομένου σχετικά με το πλαίσιο εργασίας που έχει συμφωνηθεί (τόπος, χρόνος, απόδοση κ.α.). Από την άλλη πλευρά, είναι κρίσιμη η ανάγκη προστασίας του εργαζομένου από μια χωρίς έλεγχο επεξεργασία των προσωπικών του δεδομένων για μη νόμιμους σκοπούς και άσχετους με τη σχέση εργασίας. Η χωρίς εμπόδια και περιορισμούς επεξεργασία προσωπικών δεδομένων από πλευράς εργοδοσίας θα καταστρατηγούσε ουσιώδη δικαιώματα του εργαζομένου. Ειδικότερα, η αποτελεσματική προστασία του ανθρώπινου δυναμικού έναντι της εκμετάλλευσης των ατομικών στοιχείων τους, στον εργασιακό περιβάλλον τους, απαιτεί την κατοχύρωση μέσων ελέγχου του σύννομου χαρακτήρα της πραγματοποιούμενης επεξεργασίας και άμυνας έναντι πιθανόν παραβιάσεων. Επιπλέον, οι διεθνείς τάσεις οδηγούν στην κατοχύρωση κάποιων συλλογικών δικαιωμάτων με βασική μέριμνα την ελάττωση της εξάρτησης του εργαζομένου από τον εργοδότη και εφαρμογή εργασιακής ειρήνης. Τα δικαιώματα αυτά θα πρέπει να κατοχυρώνονται εξίσου σε ιδιωτικό και δημόσιο τομέα, αφού ο κίνδυνος για τα προσωπικά δεδομένα των εργαζομένων είναι ίδιος. Επίσης, οι νέες τεχνολογίες δημιουργούν νέες δυνατότητες για "*ψηφιακή επιτήρηση*" του εργαζόμενου, όπου εμπεριέχει κρίσιμες απειλές για την ιδιωτικότητα και το ηθικό του εργαζόμενου. Για αυτό σε διάφορες χώρες

διαπιστώνεται ότι υπάρχει μικρό περιθώριο άμυνας του κάθε εργαζόμενου έναντι στην διαρκή παρακολούθηση με χρήση νέας τεχνολογίας, και έτσι, αναγνωρίζεται η αξία της συνδικαλιστικής υποστήριξης και προστασίας.

Μέσα σε αυτό το περιβάλλον, έρχεται ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ) της Ευρωπαϊκής Ένωσης, που ισχύει και στην Ελλάδα από τον Μάιο του 2018 και διαμορφώνει ένα σύστημα παράλληλης προστασίας τόσο του δικαιώματος πληροφόρησης του εργοδότη, όσο και του δικαιώματος πληροφοριακής αυτοδιάθεσης του εργαζομένου, όπως επίσης και ο νεότερος σχετικός νόμος 4624/2019 (ιδίως το άρθρο 27), που αφορά την δομή και λειτουργία της Αρχής και Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, την υιοθέτηση μέτρων για την εφαρμογή του Κανονισμού 2016/679 και την ενσωμάτωση στην εθνική νομοθεσία της σχετικής Οδηγίας της Ευρωπαϊκής Ένωσης (ΕΕ) 2016/80. Σύμφωνα με την αιτιολογική σκέψη 4 του ΓΚΠΔ το δικαίωμα της προστασίας των προσωπικών δεδομένων περιγράφεται ως εξής: "*πρέπει να εκτιμάται σε σχέση με τη λειτουργία του στην κοινωνία και να σταθμίζεται με άλλα θεμελιώδη δικαιώματα, σύμφωνα με την αρχή της αναλογικότητας*".

Σκοπός της παρούσας εργασίας είναι εκτός της παρουσίασης του ΓΚΠΔ, η επικέντρωση σε μία προβληματική της προστασίας των προσωπικών δεδομένων, ήτοι στην προστασία των προσωπικών δεδομένων των εργαζομένων στον ιδιωτικό και δημόσιο τομέα με τη μορφή της σύγκρισης και αντιπαραβολής και υπό το πρίσμα των πρόσφατων νομοθετικών εξελίξεων.

Τέλος, η διάρθρωση της εργασίας περιλαμβάνει τα εξής μέρη:

- προσωπικά δεδομένα και εργασιακός χώρος,
- προσωπικά δεδομένα και η προστασία τους στον δημόσιο τομέα,
- Συμπεράσματα.

ΜΕΡΟΣ ΠΡΩΤΟ:

ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ ΚΑΙ ΕΡΓΑΣΙΑΚΟΣ ΧΩΡΟΣ

Κεφάλαιο Πρώτο

Ιδιωτικότητα, Προσωπικά Δεδομένα και Προστασία

Στο κεφάλαιο αυτό γίνεται μια εισαγωγή στην έννοια της ιδιωτικότητας, παρουσιάζεται η διαχρονική εξέλιξη των ατομικών δεδομένων και της επεξεργασίας τους και τέλος, αναλύεται το σχετικό ελληνικό δίκαιο.

1.1 Η Ιδιωτικότητα του Ατόμου

Η διασφάλιση των προσωπικών δικαιωμάτων ήταν εξέλιξη των μεγάλων επαναστάσεων του 18ου και 19ου αιώνα, καθώς δημιουργήθηκε μια νέα κοινωνικό-πολιτική δομή, που οδήγησε στην έκφραση της ανάγκης για δικαίωμα στην ιδιωτικότητα. Ήδη στην Αρχαία Ελλάδα όπου παρουσιάστηκε για πρώτη φορά το πολίτευμα της δημοκρατίας, αναπτύχθηκε για πρώτη φορά το αγαθό των ατομικών δικαιωμάτων και της ιδιωτικότητας υπό το πρίσμα της ελευθερίας και της ισότητας. Επίσης, στη "*Γένεση*" παρουσιάζονται τα πρώτα στοιχεία έκφρασης της ιδιωτικότητας, αφού ο *Θεός* αντιστάθηκε στη δύναμη να εστιάσει το βλέμμα του στους γυμνούς πρωτόπλαστους (*Αδάμ, Εύα*) (Μάνεσης, 1979, Μήτρου, 2001, 2017).

Ιστορικά η ιδιωτικότητα συνδέεται με την προστασία της *οικίας (οίκος*). Η αίσθηση της οικίας ως "*καταφυγίου (απόσυρση και ιδιώτευση*)", εκφράζεται καλύτερα στην αγγλική γλώσσα ως "*home sweet home*" και "*there is no place like home*". Όμως, στον μεσαίωνα η οικία δεν αποτελεί παράδειγμα ιδιωτικότητας αλλά έναν δημόσιο χώρο που μπορεί να υποδεχτεί πέραν της οικογένειας, τους υπηρέτες αλλά και τους φιλοξενούμενους (Ariès, (1973, σ.54). Στην επόμενη ιστορικά περίοδο, πριν την εμφάνιση της Βιομηχανικής επανάστασης, η οικία αποτελούσε συχνά και *εργασιακό περιβάλλον* (εγκατάσταση χειροτεχνίας), όπου πραγματοποιούνταν τα επαγγελματικά και δημόσια ζητήματα της κάθε οικογένειας, παρά χώρο ιδιωτικότητας του προσώπου (Hareven, 1991, σ. 256). Εξυπηρετούσε κυρίως θέματα εργασίας παρά την απόσυρση και ιδιώτευση των κατοίκων του (Rybczynski, 1987, σ.11).

Η αλλαγή της αρχιτεκτονικής στις κατοικίες και στις πόλεις, συνδυάστηκε με την ραγδαία αύξηση της ισχύος της μεσαίας αστικής τάξης και την πληθυσμιακή αύξηση στα αστικά κέντρα, δημιουργώντας για πρώτη φορά μια σχέση μεταξύ ιδιωτικότητας και κατοικίας (Habermas, 1991). Ο Stone (1991, σ. 237) αναφέρει ότι, στην Αγγλία του 17ου αιώνα, ο διαχωρισμός των χώρων στο εσωτερικό περιβάλλον της οικίας, σε δημόσιους και ιδιωτικούς, δημιουργεί σταδιακά μια αίσθηση ιδιωτικότητας για κάθε κατοικίας (Meyer-

Spacks 2003). Οι διαχωρισμοί αυτοί επέτρεψαν να καλλιεργηθεί ένα κλίμα ιδιωτικής ζωής στο πλαίσιο της οικίας (Zeldin, l996).

Η σύνδεση *οίκου* και *ιδιωτικότητας* περιλαμβάνεται σε πολλές εθνικές νομοθεσίες. Στο ελληνικό σύνταγμα, στο άρθρο 9 §1 υιοθετείται ο οίκος ως χώρος ασύλου. Συγκεκριμένα, ο οίκος ως άσυλο προστατεύει το κάθε άνθρωπο από κάθε κίνδυνο (Solove 2002). Για παράδειγμα, στην υπόθεση *Boyd (1882)* εναντίον του κράτους των ΗΠΑ, το Ανώτατο Δικαστήριο δηλώνει εμφατικά την φράση "*ιερότητα του σπιτιού*" (Ακριβοπούλου, 2011, σ.10). Αντίστοιχα. ο συνταγματολόγος *Ν. Ι. Σαρίπολος* (1874, σ.192), σημειώνει: "Η δ' *ασυλία του οίκου δεν σημαίνει απλώς το σωματικώς τρόπον τινά απαραβίασιον, αλλά και το σέβας και το ακαταζήτητον περί των όλων των κατά τον ιδιωτικόν βίον συμβαινόντων εντός του ιερού τούτου της οικογένειας ασύλου*".

Συχνά αντικαθίσταται ο όρος "ι*διωτικότητα*" από τον όρο "*ιδιωτική σφαίρα*" (Δαγτόγλου, 2005, Δημητρόπουλος, 2005). Ο δεύτερος όρος συνήθως χρησιμοποιείται σε κράτη όπως η Γαλλία και Γερμανία, όπου το δικαίωμα στην ιδιωτική ζωή αποτέλεσε σε πρώτη φάση δικαίωμα στην προσωπικότητα και σε δεύτερη φάση μετεξελίχθηκε σε μια πιο διευρυμένη έκδοση πέραν της προσωπικότητας, που ονομάζονταν ιδιωτική σφαίρα (Γκίλη, 2013). Ο άγγλος *R. Kerr* πριν από το άρθρο των *Warren* & *Brandeis,* προσδιόρισε τον όρο "ι*διωτικότητα*" ως τον "*αμοιβαίο σεβασμό και οικειότητα (right to be left alone*)" (Rodota, 2004). Αρκετά χρόνια αργότερα, ο Westin (1967) την όρισε ως "η αξίωση των ατόμων και των ιδρυμάτων, να αποφασίζουν από μόνοι τους για το πότε, πως και μέχρι ποιο σημείο οι πληροφορίες που αφορούν αυτούς, θα διαβιβάζονται σε άλλους" (Solove, 2006).

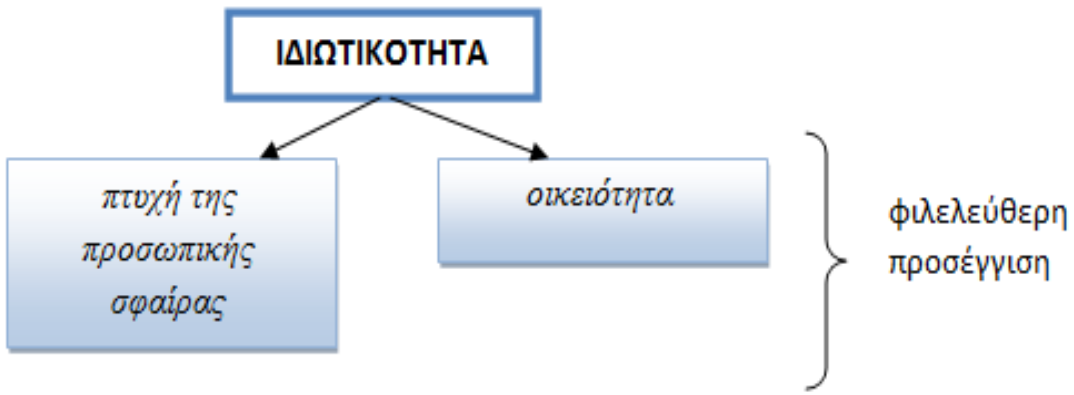
Στο δυτικό δίκαιο (κυρίως αγγλοσαξωνικό) εμπεριέχεται ο όρος "*privacy*" που προέρχεται από το λατινικό ρήμα "*privo (στα ελλην. στερώ*)". Έτσι, η έννοια "*privatus*" ανταποκρίνεται στην αρχαιοελληνική με την έννοια του "*ιδιώτη*", ενώ ο όρος "*privacy*" συνδέεται με τον όρο "α*πομόνωση*" και την "*αποχή*" από τη δημόσια ζωή, χωρίς παράλληλη ταύτιση με το περιεχόμενο του δικαιώματος στην ιδιωτική ζωή. Ωστόσο, δείχνει το υπόβαθρο πάνω στο οποίο τέθηκε ένα σύνολο δικαιωμάτων του ατόμου στην αυτονομία (Ακριβοπούλου, 2012).

Σύμφωνα με τον Καρακώστα (2012), η έννοια της ιδιωτικότητας αφορά "*το χώρο που αυτοπροσδιορίζει κάθε άτομο με στόχο να ασκεί μέσα σε αυτόν τις ατομικές και οικογενειακές δραστηριότητες χωρίς παρεμβάσεις και παρενοχλήσεις τρίτων. Ο χώρος αυτός εκτείνεται μεταξύ του ευρύτερου πλαισίου της κοινωνικής και επαγγελματικής ζωής ενός ατόμου και του απορρήτου του χώρου της αυστηρά προσωπικής ζωής του*". Στο ελληνικό δίκαιο η ιδιωτικότητα αφορά την δυναμική της συγκρότησης ενός ατόμου ελεύθερου, αυτόνομου

αυτεξούσιου, ανεξάρτητου και αυτοπροσδιοριζόμενου (Ακριβοπούλου, 2012, Μαυριά, 1982, Βουτσάκη, 2004).

Στην Επιστήμη και στην Φιλοσοφία του Δικαίου, ο όρος της ιδιωτικότητας ως δικαιώματος αποτελεί ένα σύνθετο ζήτημα, που ερμηνεύεται από τους μελετητές ανάλογα με την ιδεολογική θεώρησή τους. Στη σύγχρονη θεωρία της φιλοσοφίας του δικαίου αρχίζει να παρατηρείται μια τάση επανακατανόησης της ιδιωτικότητας, έναντι της φιλελεύθερης προσέγγιση της ιδιωτικότητας (απόλυτη διάκριση δημόσιου-ιδιωτικού). Το αποτέλεσμα ήταν να αναπτυχθούν δύο νέες, φιλελεύθερες προσεγγίσεις, που εστιάζουν στην αποσαφήνιση του περιεχομένου της, σχετικοποιώντας τον διαχωρισμό της από τον δημόσιο χώρο. Ειδικότερα (Διαγρ.1)(Ακριβοπούλου, 2011,σ.7-9, Cohen 2002):

- ως *οικειότητα,* η ιδιωτικότητα του ατόμου, επιτρέπει να επικοινωνεί με τους οικείους του, απολαμβάνοντας σχέσεις εμπιστοσύνης.
- ως *πτυχή της προσωπικής σφαίρας* του ατόμου, υπερβαίνει την τεχνητή διάκριση μεταξύ δημόσιου και ιδιωτικού ατόμου, προς την ενότητα του ατόμου, τόσο στην ιδιωτική όσο και στην κοινωνικο-πολιτική του ζωή.



Διάγραμμα 1. Οι δύο φιλελεύθερες προσεγγίσεις της ιδιωτικότητας

Το δικαίωμα στην ιδιωτικότητα εμφανίζει εξελικτικότητα κατά την πάροδο των χρόνων, ενώ αντίστοιχα, η προστασία που παρέχει στο πρόσωπο μεταβάλλεται δυναμικά στο πλαίσιο της κοινωνικής μεταβολής. Η αναγνώριση στην ιδιωτικότητα αποτελεί μια σύνθετη συνάντηση μεταξύ δικαίου και κοινωνικής εξέλιξης. Έτσι, η σύγχρονη προστασία του δεν είναι παρά η απόρροια της πληροφορικής έκρηξης και της τεχνολογικής προόδου, καθώς και των διακινδυνεύσεων που αυτή εγκυμονεί για την ιδιωτική σφαίρα του προσώπου. Στις μεταβολές αυτές, η ιδιωτικότητα δεν διαθέτει ως οδηγό μια απόλυτη, στατική διάκριση μεταξύ δημόσιου-ιδιωτικού αλλά μια διάκριση η οποία διαρκώς αναπροσδιορίζεται. Έτσι,

πρακτικές που θεωρούνταν δημόσιες σε ένα συγκεκριμένο ιστορικό και κοινωνικό πλαίσιο, σήμερα θεωρούνται ως ιδιωτικές (Solove 2002, σ. 1141). Για παράδειγμα, το γυμνό σώμα ενός ατόμου ήταν απόδειξη της ρώμης και της ανδρείας στον δημόσιο χώρο κατά την αρχαία εποχή, σήμερα αποκρύπτεται από τη δημοσιότητα, ως κατεξοχήν ιδιωτική του υπόθεση.

Επιπρόσθετα, στη θεωρία και στη φιλοσοφία, υπάρχει και η αρνητική προσέγγιση της ιδιωτικότητας. Η φιλόσοφος *Arend*t θέτει την ιδιωτικότητα του οίκου ως "*στέρηση του λόγου, της έκφρασης και των δικαιωμάτων της πόλεως*". Αντίστοιχα, ο *Posner* προσεγγίζει την ιδιωτικότητα ως "*καταφύγι*ο" για απόκρυψη μη νόμιμων αλλά και αρνητικών δράσεων. Και οι δύο προσεγγίσεις έχουν κοινό στοιχείο την ξεκάθαρη διάκριση δημόσιου - αρνητικού (Ακριβοπούλου, 2011, σ.1).

1.2 Προσωπικά Δεδομένα

Τα *δεδομένα (data*) είναι στοιχεία ή σύμβολα που περιέχουν κάποια πληροφορία. Στην σημερινή εποχή της *τεχνολογίας της πληροφορικής και των επικοινωνιών (ΤΠΕ*) ορίζεται κάθε πληροφορία που έχει διαμορφωθεί έτσι ώστε να είναι αποτελεσματική η μεταφορά και η επεξεργασία της. Η αξιοποίηση της τεχνολογίας των υπολογιστών και του διαδικτύου οδήγησε στην εποχή των ψηφιακών δεδομένων και στις νέες δυνατότητες επεξεργασίας και ανάλυση τους (π.χ. Big data analysis)(Πλατής, 2018, σ.14, Sivarajah et al., 2017, Lytras et al., 2012).

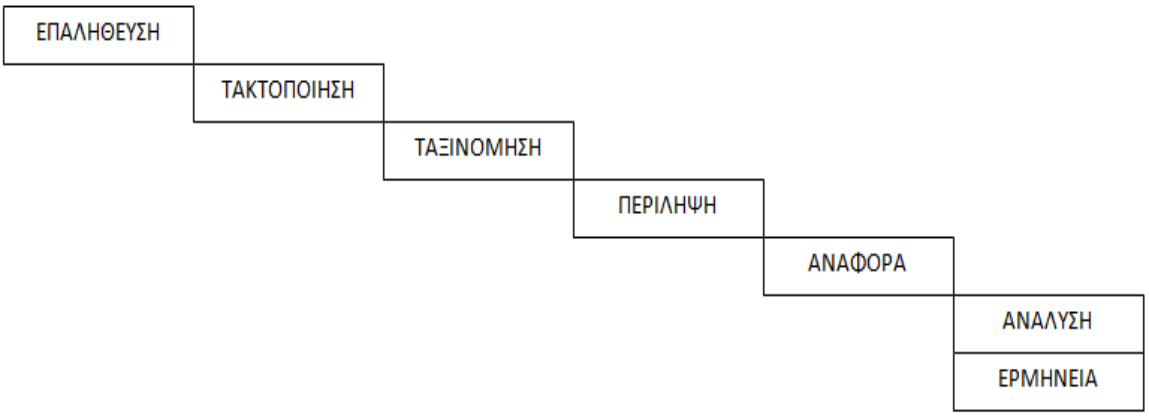
Ειδικότερα, τα *προσωπικά δεδομένα* αφορούν τα στοιχεία που συνδέονται με τα ίδια τα άτομα (φυσικά πρόσωπα) και είναι προσωπικού (ατομικού) χαρακτήρα. Προσωπικό μπορεί να είναι κάθε δεδομένο. Μια διευρυμένη ερμηνεία των προσωπικών δεδομένων τα ορίζει ως "*αν αφορούν την ταυτότητα, τα χαρακτηριστικά ή τη συμπεριφορά του ατόμου ή αν οι πληροφορίες αυτές χρησιμοποιούνται για να διαπιστωθεί ή επηρεαστεί ο τρόπος που το άτομο αντιμετωπίζεται ή χαρακτηρίζεται*"[1]. Όσον αφορά τη φύση του περιεχόμενου της πληροφορίας, αυτή μπορεί να συνδέεται με καθετί που διακρίνει ένα άτομο (φυσικά χαρακτηριστικά όπως ύψος, χρώμα ματιών, υποκειμενικά στοιχεία όπως απόψεις και δηλώσεις). Επίσης, ο φορέας και το μέσο που περιλαμβάνουν την πληροφορία, μπορεί να είναι αλφαριθμητικοί χαρακτήρες, γραφικά, ακουστικά δεδομένα, σε έντυπη ή ψηφιακή μορφή (Πλατής, 2018, σ.14, Κουκιάδης, 2019).

[1] Working Party on the Protection of Individuals with regard to the processing of their personal data, Opinion 4/2007 on the Concept of personal data, διαθέσιμο στο σύνδεσμο https://goo.gl/P1ESLX.

1.3 Επεξεργασία Προσωπικών Δεδομένων

Η επεξεργασία δεδομένων περιλαμβάνει τη *συλλογή* και *χειρισμό* των δεδομένων με σκοπό την εξαγωγή χρήσιμων πληροφοριών, χωρίς να είναι υποχρεωτικό να πραγματοποιηθούν και οι δύο. Μπορεί να υλοποιηθεί με παραδοσιακό (manual) τρόπο ή ψηφιακό τρόπο (υπολογιστής, διαδίκτυο). Είναι μια αξιολογικά *ουδέτερη διεργασία*, όπου χωρίς αυτή δεν μπορεί να υπάρξει οργανωμένη λειτουργία των επιχειρήσεων και του κράτους. Από την άλλη, αποτελεί τη βάση κρίσιμων λειτουργιών έρευνας και διαχείρισης επιχειρήσεων και οργανισμών προς όφελος της κοινωνίας. Η διαδικασία επεξεργασίας περιλαμβάνει τα εξής στάδια (Διαγρ.2)(Πλατής, 2018, σ.17):

- επαλήθευση
- τακτοποίηση με κάποια σειρά
- ταξινόμηση
- περίληψη
- αναφορά
- ανάλυση & ερμηνεία



Διάγραμμα 2. Διαδικασία Επεξεργασίας Προσωπικών Δεδομένων

Συνοψίζοντας, η προστασία δεδομένων πρέπει να προσφέρει στα άτομα ως καταναλωτές, πολίτες, πελάτες, εργαζόμενοι κ.α. τη δυνατότητα να διαθέτουν εκείνα τα μέσα για να ασκήσουν το δικαίωμα στην ιδιωτικότητα και στην προστασίας της. Επίσης, να προστατεύονται τα ατομικά στοιχεία τους (ευαίσθητα) από την κατάχρηση οποιουδήποτε είδους και έκτασης. Για να γίνουν όλα τα παραπάνω θα πρέπει να αναπτυχθεί ειδική νομοθεσία που να ρυθμίζει και να ελέγχει όλη την διαδικασία επεξεργασίας των προσωπικών δεδομένων από φυσικά ή τεχνολογικά μέσα διαχείρισης και ανάλυσης, που μπορεί να πραγματοποιούν κυβερνήσεις, επιχειρήσεις ή οργανισμών (Κυριαζόγλου, 2019, σ.17).

1.4 Ιστορική και Νομοθετική Εξέλιξη

Το δίκαιο περί προστασίας των προσωπικών δεδομένων έχει μια ιστορία τουλάχιστον ενός αιώνα. Το 1890 δύο διακεκριμένοι αμερικανοί νομικοί (*Warren, Brandeis*) δημοσίευσαν ένα άρθρο με τίτλο "*The Right to Privacy*", που θεωρήθηκε επιτομή στην ιστορία της Αμερικανικής νομικής επιστήμης, αφού τίθεται για πρώτη φορά η ανάγκη προστασίας της *ιδιωτικότητας* του ατόμου, ως ένα νέο ατομικό δικαίωμα (Warren and Brandeis, 1890). Πιο συγκεκριμένα, η αξία του άρθρου αφορά τη πρώτη οριοθέτηση της "*ιδιωτικής σφαίρας*" ως βασικό στοιχείο της ατομικής ελευθερίας στην σύγχρονη εποχή, σύμφωνα με τις τεχνολογικές εξελίξεις εκείνης της εποχής (κορύφωση της 2ης Βιομηχανικής Επανάστασης) και την συνεχώς αυξανόμενη επιρροή του κράτους, των μέσων μαζικής ενημέρωσης, των επιχειρήσεων κ.α. Η άποψη που καταθέτουν είναι η ανάγκη για δημιουργία ενός νέου δικαίου που να ανταποκρίνεται στις τεχνολογικές εξελίξεις, Αυτή προέκυψε από την έλλειψη της υπάρχουσας νομοθεσίας να προστατεύσει επαρκώς τον πολίτη από "*...τη διαρκώς αναπτυσσόμενη διείσδυση του Τύπου, των φωτογράφων, της επιχείρησης ή του οποιαδήποτε μορφής ιδιοκτήτη κάθε είδους σύγχρονης συσκευής που δύναται να καταγράφει και να αναπαραγάγει περιεχόμενο εικόνας και ήχου...*". Δηλαδή εστιάζει στις νέες τεχνολογικές εφευρέσεις και διοικητικές πρακτικές και στην υποχρέωση να τεθούν σαφή όρια μεταξύ δημόσιου και ιδιωτικού βίου (Κουκιάδης, 2019, σ.21-2).

Μετά το Β΄ Παγκόσμιο πόλεμο τα περισσότερα κράτη, κυρίως ευρωπαϊκά, θέλησαν να προστατεύσουν τα προσωπικά δεδομένα των πολιτών τους. Έτσι, στον ΟΗΕ το 1948 μέσω ψηφοφορίας, ενεργοποιήθηκε η *Οικουμενική Διακήρυξη για τα Ανθρώπινα Δικαιώματα*, που στο άρθρο 12 περιγράφεται "*κανείς δεν επιτρέπεται να υποστεί αυθαίρετες επεμβάσεις στην ιδιωτική ζωή το, την οικογένεια, την κατοικία ή την αλληλογραφία του, ούτε προσβολές της τιμής και της υπόληψης του. Καθένας έχει το δικαίωμα να τον προστατεύουν οι νόμοι από επεμβάσεις και προσβολές, αυτού του είδους*."[2]. Ακολούθησαν και άλλες σχετικές πρωτοβουλίες από τον ΟΗΕ για αναβαθμισμένη φύλαξη της ιδιωτικότητας, και ειδικότερα, στην προστασία των ατομικών δεδομένων, όπως οι "*Guidelines for the Regulation of Computerized Personal Data File*s" το 1990 (Κουκιάδης, 2019, σ.23).

Διαχρονικά το κρίσιμο πρόβλημα στην επεξεργασία των προσωπικών δεδομένων είναι η προστασία των προσωπικών δεδομένων ως προστασία της ιδιωτικότητας. Η σύνδεση τους έγινε κατά τον 20ο αιώνα όταν τα δύο βασικά προβλήματα της μεταπολεμικής κοινωνίας έθεσαν επιτακτικά το ζήτημα της επάρκειας στην προστασία των προσωπικών

[2] Οικουμενική Διακήρυξη για τα Δικαιώματα του Ανθρώπου, διαθέσιμη σε https://www.ohchr.org.

δεδομένων κυρίως κατά την επεξεργασίας τους: η γραφειοκρατία και οι τεχνολογικές εξελίξεις. Η κρατική παρέμβαση μέσα από τις σύνθετες δομές της (ληξιαρχείο, εφορία κ.α.) σε συνδυασμό με το εκάστοτε κανονιστικό πλαίσιο επέτρεψαν την "*παρακολούθηση*" της καθημερινότητας του πολίτη, προβλημάτισαν την κοινή γνώμη και προκάλεσαν με τη σειρά τους αντιδράσεις στο πως το κράτος μπορεί να δικαιολογεί την επεξεργασία δεδομένων για σκοπούς που δεν αποκαλύπτονται πάντα. Αντίστοιχα η τεχνολογική εξέλιξη με την είσοδο των υπολογιστών, των βάσεων δεδομένων, της τεχνητής νοημοσύνης και του διαδικτύου, βελτίωσαν την διαδικασία επεξεργασίας, αλλά από την άλλη καλλιέργησαν το έδαφος για ασύλληπτες δυνατότητες επεξεργασίας, που εύκολα μπορούσαν να παραβούν το όποιο νομοθετικό πλαίσιο ελέγχου (Evans and Martin, 2018).

Έτσι, οι κοινωνικές πιέσεις και ο κίνδυνος για υποκλοπή ευαίσθητών προσωπικών στοιχείων από αθέμιτη ή μη νόμιμη επεξεργασία προσωπικών δεδομένων, οδήγησε σε μια έντονη διεργασία πολλά κράτη στην μεταπολεμική εποχή. Κατά συνέπεια η όποια αντιμετώπιση και επίλυση προσαρμόστηκε σε κάθε χώρα σύμφωνα με την νομοθετική κουλτούρα της αλλά και σε υπερεθνικό επίπεδο (π.χ. ΕΟΚ-ΕΕ), ανάλογα με τους εκάστοτε συσχετισμούς. Ειδικότερα, το 1950 το Συμβούλιο της Ευρώπης υπέγραψε την *Ευρωπαϊκή Σύμβαση των Δικαιωμάτων του Ανθρώπου (ΕΣΔΑ*), με ισχύ από το 1953. Είναι ένα νομικά δεσμευτικό κείμενο για το Ευρωπαϊκό Δικαστήριο των Δικαιωμάτων του Ανθρώπου, όπου τιμωρεί παραβάσεις κρατών (Κουκιάδης, 2019, Πλατής, 2018).

Η δεκαετία του '70 αποτέλεσε το ορόσημο για τη δημιουργία ενός θεσμικού πλαισίου προστασίας των πολιτών από την αθέμιτη επεξεργασία δεδομένων του κράτους ή των επιχειρήσεων. Το *Συμβούλιο της Ευρώπης* εκτίμησε ότι οι τεχνολογικές εξελίξεις δεν λαμβάνονταν υπόψη από τις εθνικές νομοθεσίες. Έτσι, το 1968 δημοσίευσε τη *Σύσταση 509* σχετικά με τα προσωπικά δεδομένα και τις επιστημονικές τεχνολογικές εξελίξεις, εστιάζοντας στην προστασία δεδομένων στις τράπεζες δεδομένων στο δημόσιο και ιδιωτικό τομέα. Στην Γερμανία σε επίπεδο ομόσπονδου κρατιδίου, η Έσση το 1970 θέσπισε για πρώτη σε διεθνή κλίμακα, νομοθεσία για την προστασία των Δεδομένων. Αυτό οφείλονταν στην ευαισθησία που είχε δημιουργηθεί στην Γερμανική έννομη τάξη σχετικά με το Ναζιστικό καθεστώς (1933-45) που παραβίασε με τον πιο ωμό τρόπο τα προσωπικά δεδομένων των πολιτών (Εβραίοι, ομοφυλόφιλοι κ.α.). Ακολούθησε το 1973 η Σουηδία, το 1977 η Γερμανία και η Γαλλία το 1978, ενώ αρκετά κράτη της Ευρώπης προέβλεψαν σε συνταγματικό επίπεδο τη προστασία δεδομένων (Πορτογαλία, Ισπανία, Αυστρία)(Κουκιάδης, 2019, Πλατής, 2018).

Το 1980, ο *ΟΟΣΑ (Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης*) εξέδωσε τις κατευθυντήριες αρχές για την "*προστασία της ιδιωτικότητας και τη διασυνοριακή αποστολή*

προσωπικών δικαιωμάτων", θέτοντας ένα μη δεσμευτικό κείμενο αρχών που πρέπει να διέπουν την επεξεργασία δεδομένων. Στα τέλη της δεκαετίας του '70, το *Συμβούλιο της Ευρώπης* τροποποίησε το προηγούμενο κείμενο του σχετικά με την προστασία των δεδομένων των πολιτών, προτείνοντας τη *Σύμβαση 108* που λάμβανε υπόψη τις τεχνολογικές εξελίξεις της εποχής (πληροφοριακά συστήματα, τράπεζες πληροφοριών κ.α.) και ειδικότερα την *αυτοματοποιημένη διαδικασία επεξεργασίας δεδομένων*. Η σύμβαση αυτή για πολλά χρόνια αποτέλεσε το βασικό κείμενο για την προστασία των δεδομένων στην Ευρώπη. Η Συνθήκη του Μάαστριχτ το 1992 με τη δημιουργία της Ευρωπαϊκής Ένωσης προέκτεινε την ευρωπαϊκή κανονιστική θεώρηση και σε θέματα πολιτικά και κοινωνικά. Η Συνθήκη της Λισσαβόνας σε επίπεδο πρωτογενούς Ευρωπαϊκού δικαίου, στο άρθρο 16 παρ.1 γίνεται για πρώτη αναφορά στην "*προστασία προσωπικών δεδομένων*" ως εξής[3]:

Άρθρο 16
παράγραφος 1
Κάθε πρόσωπο έχει δικαίωμα προστασίας των δεδομένων προσωπικού χαρακτήρα που το αφορούν.

Σε επίπεδο δευτερογενούς Ευρωπαϊκού δικαίου, η *Οδηγία 95/46/ΕΚ* θέτει ένα διττό στόχο (Κουκιάδης, 2019):

- προστασία των δεδομένων,
- διευκόλυνση της ελεύθερης και νόμιμης κυκλοφορίας των πληροφοριών και των προσωπικών δεδομένων.

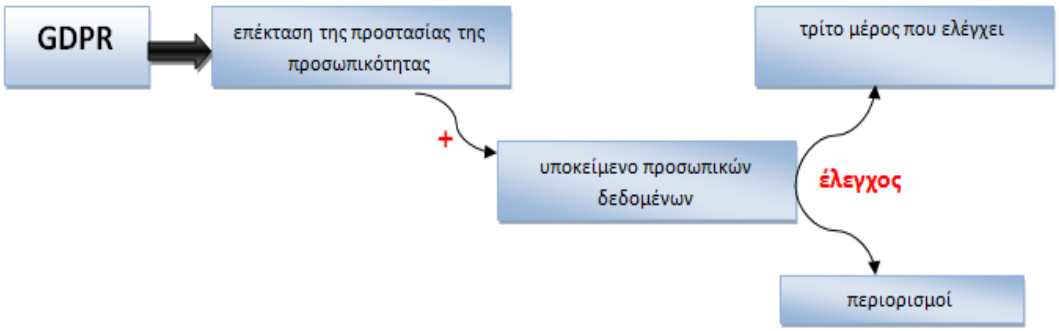
Το νομικό πλαίσιο που τέθηκε με την Οδηγία αυτή τροποποιήθηκε με *τον Γενικό Κανονισμό για την Προστασία Δεδομένων 2016/679/ΕΕ (ΓΚΠΔ, GDPR*), που τέθηκε σε εφαρμογή στις 25-5-2018, χωρίς την ανάγκη ύπαρξης ειδικού νόμου από τα κράτη της ΕΕ για την έναρξη της ισχύος του γενικού κανονισμού. Ωστόσο, για κάποια εξειδικευμένα θέματα προβλέπεται η δημιουργία ρυθμίσεων από τις εθνικές νομοθεσίες. Για τις εργασιακές σχέσεις προβλέπεται οι ρυθμίσεις να μπορούν να πραγματοποιηθούν και με τις συλλογικές συμβάσεις εργασίας και αντίστοιχους κανονισμούς. Παράλληλα εκδόθηκε η *Οδηγία 2016/680/27-4-2016* για την προστασία των ατόμων έναντι επεξεργασίας ατομικών δεδομένων στους λεγόμενους τομείς του ποινικού δικαίου, όπου τέθηκε σε ισχύ με το νόμο 4624/2019, που αποτελεί την τελευταία νομοθετική εξέλιξη στο εγχώριο δίκαιο (Κουκιάδης, 2019).

Το 1997, η ΕΕ προχώρησε στην πρόβλεψη ειδικότερων διατάξεων (Οδηγίες 97/66/ΕΚ, 2002/58/ΕΚ) για την προσαρμογή στις τεχνολογικές εξελίξεις (τηλεπικοινωνίες,

[3] Συνθήκη Λισσαβόνας για την ΕΕ 2012/c 326/01, διαθέσιμο στο https://eur-lex.europa.eu.

διαδίκτυο, κ.α.) και στις αντίστοιχες αλλαγές στην αγορά (π.χ. ηλεκτρονικό εμπόριο), έτσι ώστε να παρέχεται ανάλογο επίπεδο προστασίας των δεδομένων και του ιδιωτικού βίου σε όλους τους πολίτες-χρήστες, ανεξάρτητα των διαθέσιμων υπηρεσιών επικοινωνιών και χρησιμοποιούμενων τεχνολογιών. Γενικά, η οδηγία είναι εργαλείο δευτερογενούς δικαίου στην ΕΕ και δεν παράγει αυτόματα έννομα αποτελέσματα για τους πολίτες, αλλά πρέπει να ενταχθεί στο εθνικό δίκαιο μέσω εθνικών νόμων (Πλατής, 2018, σ.28).

Σε επίπεδο ΕΕ, βασικό κείμενο αναφοράς είναι και ο *Χάρτης Θεμελιωδών Δικαιωμάτων (ΧΘΔ*), που αποτελεί Πρωτογενές δίκαιο της ΕΕ (*άρθρο 8.1.2* & *11*). Ο νέος κανονισμός συμπληρώνει τις παραδοσιακές αρχές προστασίας της προσωπικότητας (ο άνθρωπος είναι αυτοτελές αντικείμενο προστασίας με καθορισμό όρων προσβολής και παροχής αυτοτελούς προστασίας), προσθέτοντας νέα στοιχεία που υποβοηθούν στην εξειδίκευση των παραδοσιακών αρχών και στη διεύρυνση της προστασίας της προσωπικότητας, οδηγώντας σε ένα νέο σύστημα δικαίου που διατηρεί την αυτοτέλεια της προστασίας των προσωπικών δεδομένων. Πρόκειται για επέκταση της προστασίας της ανθρώπινης προσωπικότητας σε όλες τις εκφάνσεις και ως υποκείμενου προσωπικών δεδομένων, με περιορισμούς και έλεγχο από τρίτο (π.χ. από μια ανεξάρτητη αρχή)(Διαγρ.3)(Κουκιάδης, 2019, σ.36).



Διάγραμμα 3. Θεωρητικό πλαίσιο του νέου κανονισμού GDPR

Τέλος, η προστασία προσωπικών δεδομένων στο νέο κανονιστικό πλαίσιο (GDPR) δεν απαγορεύει σε κάθε περίπτωση την επεξεργασία, αλλά οι ρυθμίσεις για την επεξεργασία δεδομένων στοχεύουν σε συμβιβασμό δύο αντίπαλων δικαιωμάτων, το δικαίωμα της πληροφόρησης ή *πληροφοριακής ελευθερίας* και το δικαίωμα του *πληροφοριακού αυτοπροσδιορισμού ή πληροφορικής αυτοδιάθεσης*, που προσφέρει μια νέα κατεύθυνση στον όρο της προσωπικότητας και στην προστασία του ιδιωτικού βίου, περιλαμβανόμενου και του οικογενειακού. Πλέον το άτομο προσδιορίζεται και ως υποκείμενο προσωπικών δεδομένων και γίνεται υποκείμενο αντίστοιχων δικαιωμάτων. Σύμφωνα με τον Κουκιάδη (2019, σ. 40) προκύπτει ο συγκρουσιακός χαρακτήρας των δύο επιδιωκόμενων δικαιωμάτων του νέου

κανονισμού και παράλληλα, ο συμπληρωματικός χαρακτήρας τους, αφού το ένα αποτελεί φραγμό στο άλλο. Για αυτό το κεντρικό πρόβλημα του είναι ο συμβιβασμός που πρέπει να επέλθει ανάμεσα σε αυτά τα δύο δικαιώματα, ώστε να υπάρξει ισορροπία.

1.5 Η Συνταγματική Προστασία της Ιδιωτικότητας και των Προσωπικών Δεδομένων

Η ιδιωτική ζωή (ιδιωτικότητα) κατοχυρώνεται συνταγματικά μέσω του άρθρου 9 παρ. 1, (Δαγτόγλου, 2005, σ.397). Επιπλέον, το απαραβίαστο της ιδιωτικότητας αφορά την απαγόρευση δημοσιοποιήσεως της ζωής του κάθε ατόμου (Μαλαγαρδή, 2010, Κουκιάδης, 2008). Παράλληλα, στο Ελληνικό Σύνταγμα στο άρθρο 9Α, κάθε άτομο μπορεί να έχει το δικαίωμα της προστασίας από την εκμετάλλευση των ατομικών του δεδομένων. Επίσης, το δικαίωμα προστασίας έχει διαφορετικό χαρακτήρα από την κρατική υποχρέωση προστασίας για άλλα δικαιώματα (άρθρο 25)(Τσεβά, 2010, σ.82). Γενικά, η συνταγματική κατοχύρωση προέκυψε λόγω των τεχνολογικών εξελίξεων που παρέχει η νέα τεχνολογία (Χρυσόγονος, 2017, Ηλιάδου, 2016). Η ψηφιακή επεξεργασία πληροφοριών δημιουργεί περιορισμούς στην δυνατότητα πληροφοριακού αυτοκαθορισμού (Δόνο, 2004, Παναγοπούλου-Κουτνατζή, 2017, Χρυσόγονος, 2017).

1.6 Η Προστασία Προσωπικών Δεδομένων κατά το Ελληνικό Δίκαιο

Μετά την κύρωση της Σύμβασης 108 στην Ελλάδα, ακολούθησε νομοθετική πρωτοβουλία εναρμόνισης με το κοινοτικό κεκτημένο. Αυτή ήταν ο *Ν.2472/1997*, που αποτελεί τον πρώτο ελληνικό νόμο, που προέκυψε από την Οδηγία 95/26/ΕΚ. Ο νόμος προκάλεσε πλήθος αλλαγών ενσωματώνοντας τις βασικές αρχές της Οδηγίας και των διεθνών συμβάσεων σχετικά με τη σύννομη και θεμιτή επεξεργασία προσωπικών δεδομένων, ενώ για πρώτη φορά στο ελληνικό δίκαιο τίθενται ειδικές δικλείδες ασφαλείας για την προστασία από την επεξεργασία ευαίσθητων δεδομένων. Επίσης, ορίζεται για πρώτη φορά και η ίδρυση της *Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα* ως αρμόδιας ανεξάρτητης εποπτικής αρχής, στα πρότυπα της γαλλικής *Commission Nationale de l' informatique et des liberteses (CNIL*). Περιλάμβανε 26 άρθρα σε έξι κεφάλαια. Στο άρθρο 1 του νόμου διαφαίνεται ξεκάθαρα ο προστατευτικός σκοπός του νόμου, μέσω της οριοθέτησης προϋποθέσεων για την επεξεργασία δεδομένων ατομικού χαρακτήρα. Οι προϋποθέσεις αυτές αφορούν την προστασία των δικαιωμάτων και των θεμελιωδών ελευθεριών των φυσικών προσώπων και της ιδιωτικής ζωής. Ακολούθησε η *Οδηγία 115/2001* της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα που ρύθμιζε το πρόβλημα επεξεργασίας προσωπικών δεδομένων

στον εργασιακό χώρο. Δεν περιέχονταν κανονιστικές ρυθμίσεις αλλά ερμηνευτικές διατάξεις των νομοθετικών ρυθμίσεων που αφορούν αντικειμενικό πεδίο εφαρμογής του Ν. 2472/1997. Ειδικότερα, ερμηνεύονται οι κανόνες των Ν.2472/97 και 2774/99 (προστασία προσωπικών δεδομένων και ιδιωτικής ζωής στο πεδίο των ηλεκτρονικών επικοινωνιών και του απόρρητου των επικοινωνιών), ώστε να είναι ευκολότερη και σαφέστερη η εφαρμογή των αρχών των νόμων, με στόχο την αποτελεσματικότερη προστασία των προσωπικών δεδομένων των εργαζομένων λόγω αρκετών σχετικών καταγγελιών. Ακολούθησε ο Ν.3471/2006 που κατάργησε στο σύνολο του τον 2774/99. Δηλώνει ότι απαγορεύεται η ακρόαση, υποκλοπή, αποθήκευση ή άλλο είδος παρακολούθησης ή επιτήρησης των ηλεκτρονικών επικοινωνιών και των συναφών δεδομένων κίνησης και θέσης και παράλληλα τιμωρεί με φυλάκιση & πρόστιμο όποιον κάνει τέτοιες παραβάσεις. Το απόρρητο των επικοινωνιών εκτείνεται και στα δεδομένα κίνησης και θέσης, ενώ ταυτόχρονα εκτός από τους χρήστες ή άνευ της συγκατάθεσης αυτών δεν επιτρέπεται η πρόσβαση σε διαφορετικά πρόσωπα, εκτός αν προβλέπεται από κάποια ειδική ρύθμιση. Ο νόμος αυτός υπερισχύει του νόμου 3471/2006 σε θέματα σχετικά με τις διαδικτυακές υπηρεσίες επικοινωνίας και την εκμετάλλευση δεδομένων ατομικού χαρακτήρα στις ηλεκτρονικές επικοινωνίες. Στη συνέχεια, ψηφίστηκε ο Ν.3917/2011 που ενσωματώνει τις απαιτήσεις που έθετε η Οδηγία 2006/24/ΕΚ, όπου γίνεται τροποποίηση των Ν. 2472/97 & Ν. 3471/2006 και της Οδηγίας 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12-7-2002. Τέλος, με τον νόμο 4624/2019, υιοθετήθηκε ένα νέο πλαίσιο λειτουργίας της ΑΠΔΠΧ, η εφαρμογή του ΓΚΠΔ και η ενσωμάτωση της Οδηγίας ΕΕ 2016/680 (Αλεξανδροπούλου-Αιγυπτιάδου, 2007, Αυγουστιανάκη, 2001, Πλατής, 2018, Κουκιάδης, 2019).

Τέλος, το ελληνικό δίκαιο είχε ήδη σε πρωτόλεια μορφή στοιχεία της προστασίας της ιδιωτικότητας. Από το 1945 ο Αστικός κώδικας (άρθρο 57) είχε διατάξεις περί προστασίας της ιδιωτικότητας, ενώ ο Ποινικός κώδικας εξειδικεύεται στην προστασία προσωπικών δεδομένων ενισχύοντας την αυξημένη προστασία του απορρήτου των επικοινωνιών και της ιδιωτικής συνομιλίας (άρθρο 370Α, απόρροια του άρθρου 33 παρ.7 του Ν.2172/1973, του άρθρου 1 του Ν.1291/82 & άρθρο 6 παρ. 8 Ν.3090/2002 και ο Ν.4624/2019)(Δημητρόπουλος, 2005, Ζερμιώτη, 2012, Κουκιάδης, 2019).

Κεφάλαιο Δεύτερο

Η Έννοια των Προσωπικών Δεδομένων κατά τον Κανονισμό ΓΚΠΔ (GDPR)

Στο κεφάλαιο αυτό γίνεται παρουσίαση του κανονισμού ΓΚΠΔ (GDPR) όπως αυτός εντάχθηκε στην ελληνική νομοθεσία σε σχέση με τον κανονισμό 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων ατομικού χαρακτήρα και για την ελεύθερη διακίνηση των δεδομένων.

2.1 Το Πλαίσιο του Κανονισμού

Η Ευρωπαϊκή νομοθεσία οριοθετεί την προστασία των προσωπικών δεδομένων σε σχέση με την επεξεργασία τους ως ένα βασικό ατομικό δικαίωμα, που βασίζεται στο Χάρτη *Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (ΕΕ)* και στην Συνθήκη λειτουργίας της. Επιπλέον, η αυτονομία των πολιτών στις σύγχρονες κοινωνίες θεωρείται ότι απειλείται λόγω των νέων τεχνολογιών και της παγκοσμιοποίησης. Έτσι, οι νέες αυτές συνθήκες που δημιουργούν ένα νέο κλίμα διαμόρφωσης ιδεών και αντιλήψεων, σε συνδυασμό με τις νέες τεχνολογικές δυνατότητες στο πεδίο της ανταλλαγής, επεξεργασίας και διακίνησης προσωπικών δεδομένων, οδηγεί στην ανάγκη για ένα ισχυρό πλαίσιο νομικής προστασίας των προσωπικών δεδομένων στην Ευρώπη (Πλατής, 2018, Κυριαζόγλου, 2019, Κουκιάδης, 2019).

Η *ασφάλεια δικαίου* θα πρέπει να αντιμετωπίζεται με απώτερο σκοπό την αμοιβαία εμπιστοσύνη και αλληλεπίδραση μεταξύ των κρατών της ΕΕ. Ο *Γενικός Κανονισμός Προστασίας των Δεδομένων (ΓΚΠΔ, GDPR)* στοχεύει στην προστασία των ατομικών δεδομένων εντός της Ευρωπαϊκής Ένωσης. Ειδικότερα, ο *Κανονισμός 2016/679* της ΕΕ (ΓΚΠΔ), ψηφίστηκε στις 27-4-2016 αντικαθιστώντας την ισχύουσα Οδηγία περί Προστασίας Δεδομένων του 1995 (*95/46/ΕΚ*), που ενσωματώθηκε στα κράτη μέλη της ΕΕ, και στην Ελλάδα με τον *Νόμο 2472/1999*. Ο ΓΚΠΔ αποτελεί τη μεγαλύτερη νομοθετική αλλαγή στην προστασία προσωπικών δεδομένων την τελευταία εικοσαετία. Εφαρμόστηκε υποχρεωτικά στα κράτη μέλη της ΕΕ στις 25-5-2018. Πρόκειται για ένα νέο, ενιαίο και άμεσα εφαρμόσιμο κανονιστικό πλαίσιο, που ρυθμίζει την επεξεργασία δεδομένων προσωπικού χαρακτήρα ατόμων που βρίσκονται στην ΕΕ, από άλλα άτομα, επιχειρήσεις, οργανισμούς ή φορείς. Δεσμεύει όλα τα κράτη - μέλη για την υιοθέτηση και εφαρμογή του, ενώ τους δίνει δυνατότητα να εξειδικεύσουν τις επιμέρους διατάξεις του έτσι ώστε, να προσαρμοσθεί στην

εκάστοτε εθνική νομοθεσία. Πιο συγκεκριμένα, ο νέος κανονισμός μέσω των *Αιτιολογικών Σκέψεων* του *Προοιμίου 10* & *19*, παρέχει προτεραιότητα στα κράτη μέλη μέσα από ρήτρες ευελιξίας να εξειδικεύσουν τους κανόνες του ΓΚΠΔ (Μήτρου, 2017, Borchardt, 2011).

Η σημασία του ΓΚΠΔ είναι μεγάλη, λόγω της εκρηκτικής αύξησης της παραγωγής δεδομένων (Fawcett and Provost, 2019). Ο νέος κανονισμός εστιάζει στην αντιμετώπιση αυτής της νέας κατάστασης, ενώ στο επόμενο διάγραμμα φαίνονται συνοπτικά οι ανάγκες που οδήγησαν στην δημιουργία του νέου κανονισμού (ΣΕΒ, 2018).

Ραγδαίες τεχνολογικές εξελίξεις	– Αύξηση της έκτασης και έντασης της συλλογής, ανταλλαγής και επεξεργασίας δεδομένων προσωπικού χαρακτήρα – Αύξηση περιπτώσεων παραβίασης της ασφάλειας δεδομένων προσωπικού χαρακτήρα
Ασυμμετρία εφαρμογής της Οδηγίας 95/46/ΕΚ από τα κράτη-μέλη	– Ανασφάλεια δικαίου - Αποκλίσεις κατά την εκτέλεση και εφαρμογή – Στρέβλωση του ανταγωνισμού μεταξύ κρατών-μελών

Διάγραμμα 4. Ανάγκες για την δημιουργία του ΓΚΠΔ

Ο βασικός σκοπός του ΓΚΠΔ είναι η προστασία των ατόμων από τις δυνατότητες που προφέρει η ψηφιακή τεχνολογία στην εκμετάλλευση των ατομικών δεδομένων που ωθείται και από την παγκοσμιοποίησης στην οικονομία (Νίκας και Χριστοδούλου, 2012, Κυριαζόγλου, 2019, Πλατής, 2018). Συνολικά, ο ΓΚΠΔ έχει πέντε (5) βασικά χαρακτηριστικά (ΣΕΒ, 2018):

- έχει γενική εφαρμογή, στην δημόσια και ιδιωτική σφαίρα της οικονομίας και διοίκησης.
- έχει άμεση εφαρμογή, με αμετάκλητη ημερομηνία έναρξης υιοθέτησης σε διακοινοτικό επίπεδο (25/05/2018).
- διαθέτει χαρακτηριστικά Οδηγίας, αφού επιτρέπει την εξειδίκευση από τα κράτη μέλη.
- προβλέπει σημαντικά διοικητικά πρόστιμα (έως €20 εκ. ή έως το 4% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών, ανάλογα με το ποιο είναι υψηλότερο), σύμφωνα με το είδος της παραβίασης των διατάξεων του ΓΚΠΔ.
- είναι αντικείμενο πολυετών διαπραγματεύσεων που διενεργήθηκαν από διαφορετικά γκρουπ συμφερόντων που οδήγησαν σε ένα συμβιβασμό, όπου δείχνει τη σημαντικότητα και τις επιδράσεις του στην αγορά.

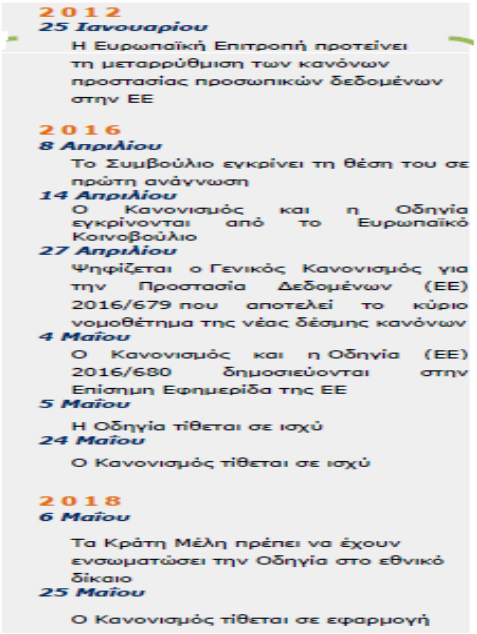
Επιπρόσθετα, ο ΓΚΠΔ ταυτίζεται με πολιτικές και διαδικασίες των φορέων που εφαρμόζεται (εταιρείες, οργανισμοί), με υποδομές, με πράξεις αυτοδέσμευσης του

μάνατζμεντ, με το ανθρώπινο δυναμικό και με την οργανωσιακή κουλτούρα. Αυτό σημαίνει ότι αποτελεί έναν εναλλακτικό τρόπο οργάνωσης και λειτουργίας ενός φορέα που εστιάζει στη διαφύλαξη των ατομικών δεδομένων. Δηλαδή, λαμβάνει όλα τα αναγκαία μέτρα για να διαφυλάξει τα ατομικά δεδομένα. Επίσης, εισάγει κάποιες καινοτομίες στο πλαίσιο προστασίας των προσωπικών δεδομένων, όπως φαίνεται στο επόμενο διάγραμμα (ΣΕΒ, 2018).

✓ Ενίσχυση δικαιωμάτων υποκειμένων	✓ Αυστηριοποίηση κυρώσεων
✓ Ενίσχυση δικαιώματος στη λήθη	✓ Σύσταση Ευρωπαϊκού Συμβούλιου Προστασίας Δεδομένων
✓ Θέσπιση δικαιώματος στη φορητότητα	✓ Θέσπιση μηχανισμού συνεκτικότητας
✓ Μεταφορά βάρους απόδειξης στους Υπευθύνους Επεξεργασίας (Λογοδοσία)	✓ Θεσμοθέτηση της Αρχής της Διαφάνειας

Διάγραμμα 5. Καινοτομίες του ΓΚΠΔ

Τέλος, στο επόμενο διάγραμμα φαίνεται αναλυτικά το χρονοδιάγραμμα για την σχεδίαση και τελική εφαρμογή στην ΕΕ του ΓΚΠΔ.



Διάγραμμα 6. Χρονοδιάγραμμα σχεδίασης και εφαρμογής του ΓΚΠΔ

2.2 Διάρθρωση ΓΚΠΔ

Η δομή του ΓΚΠΔ περιλαμβάνει ένα προοίμιο, 11 κεφάλαια, 99 άρθρα και 17 επιμέρους τμήματα. Συγκεκριμένα, τα δύο πρώτα κεφάλαια αφορούν τις γενικές αρχές του Κανονισμού, το τρίτο κεφάλαιο αφορά τα ατομικά δικαιώματα σχετικά με τα δεδομένα του. Το επόμενο κεφάλαιο αναφέρεται στον υπεύθυνο επεξεργασίας και στον εκτελών την επεξεργασία. Στα

υπόλοιπα κεφάλαια αναφέρεται σε ειδικά θέματα της προστασίας δεδομένων, όπως διαβιβάσεις δεδομένων προς τρίτες χώρες ή οργανισμούς (κεφ. 5), εποπτικές αρχές (κεφ. 6), συνεργασία και συνεκτικότητα (κεφ. 7), προσφυγές, ευθύνες και κυρώσεις (κεφ. 8), διατάξεις για ειδικές περιπτώσεις (κεφ. 9), εξουσιοδότηση πράξεων και εκτελεστικές πράξεις (κεφ. 10) και τελικές διατάξεις (κεφ. 11) (Διαγρ.7)(Πλατής, 2018, Κυριαζόγλου, 2019, Κουκιάδης, 2019).

Διάγραμμα 7. Δομή ΓΚΠΔ

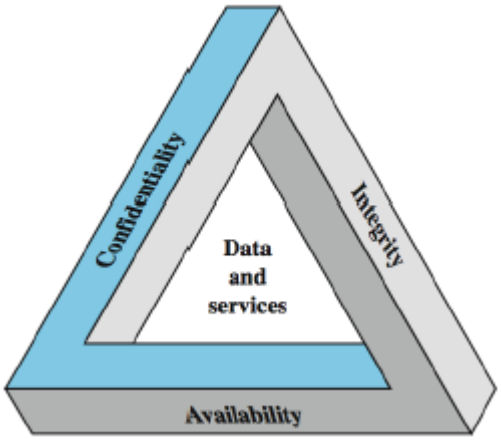
2.3 Εμπιστευτικότητα και Απόρρητο Δεδομένων

Ο ΓΚΠΔ διέπεται από τις ακόλουθες ιδιότητες, όσο αφορά τα προσωπικά δεδομένα και τη διαχείριση τους, για να επιτευχθεί ασφάλεια (Κυριαζόγλου, 2019, Κουκιάδης, 2019):

- *εμπιστευτικότητα*. Αφορά την προσωπική πληροφορία, επειδή είναι ευαίσθητη.
- *απόρρητο*. Αντίστοιχα μια προσωπική πληροφορία θα πρέπει να είναι απόρρητη, είτε αφορά εργασιακή διαδικασία, είτε διαγωνιστική διαδικασία.

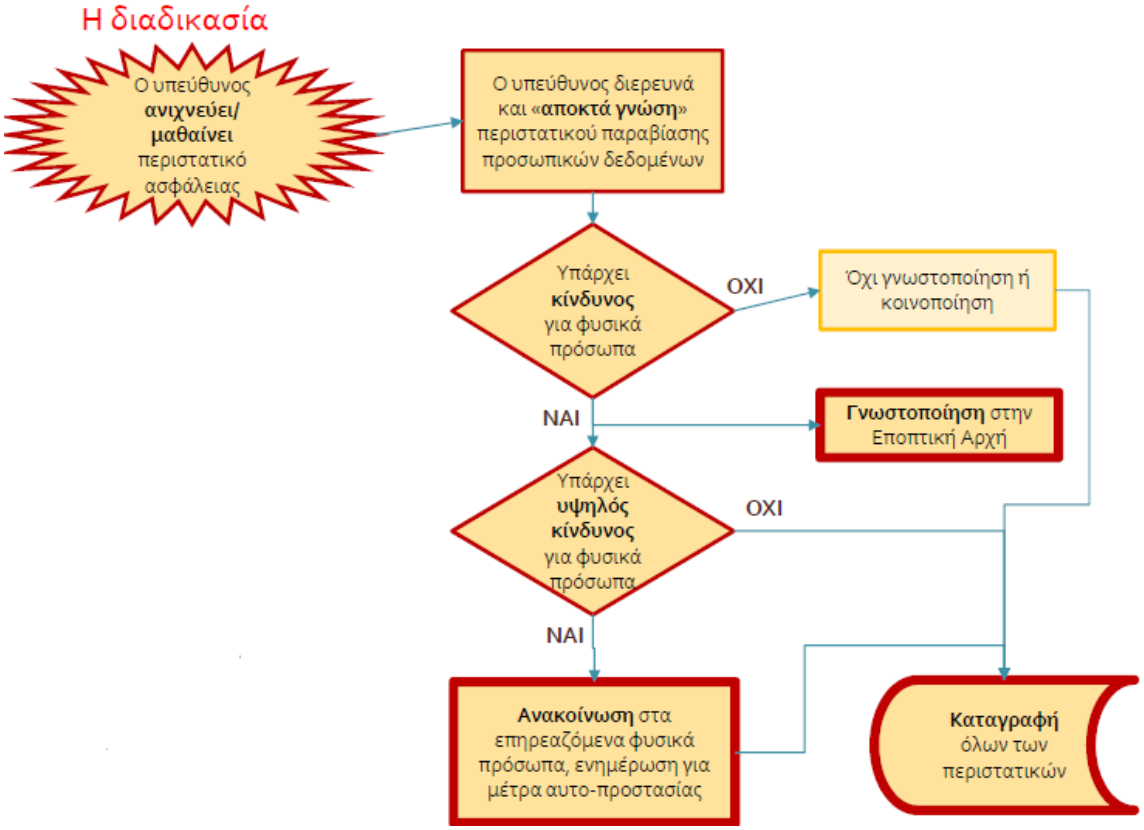
Συνοψίζοντας, οι στόχοι ασφάλειας σύμφωνα με το πνεύμα του ΓΚΠΔ, είναι οι εξής (Διαγρ.8) (Πλατής, 2018):

- *Εμπιστευτικότητα (confidentiality)*.
- *Ακεραιότητα (integrity)*.
- Διαθεσιμότητα (availability).



Διάγραμμα 8. Τρίπτυχο CIA

Επίσης, στο επόμενο διάγραμμα φαίνεται η διαδικασία αντιμετώπισης μιας παραβίασης δεδομένων προσωπικού χαρακτήρα[4]:



Διάγραμμα 9. Παράδειγμα Παραβίασης Ατομικών Δεδομένων

2.4 Βασικές Αρχές

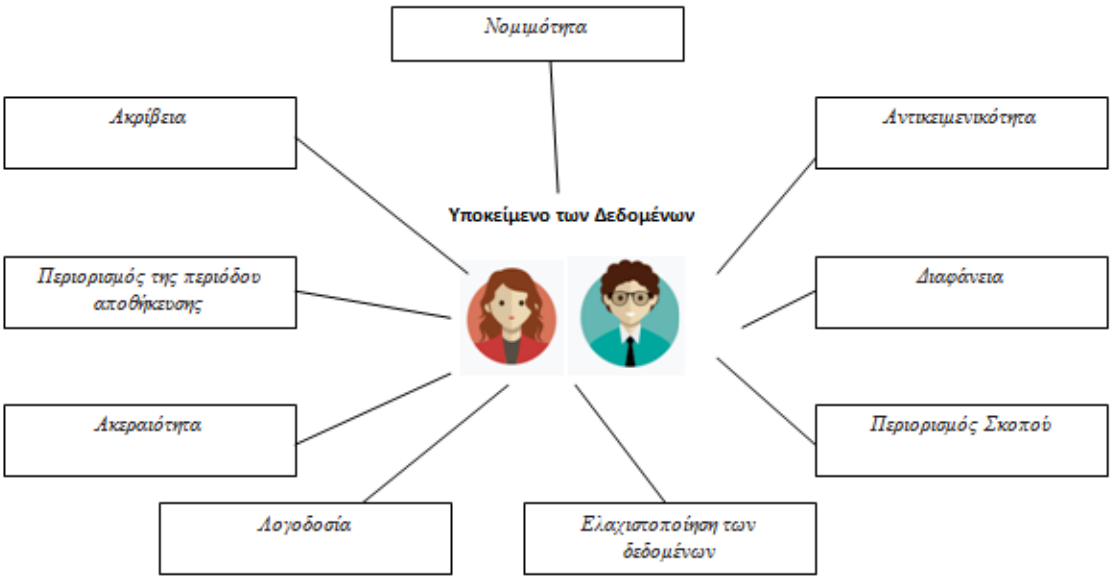
Ο ΓΚΠΔ επαναπροσδιορίζει τις προϋπάρχουσες θεμελιώδεις αρχές, ενισχύοντας τες με τη σύνδεση με την αρχή της λογοδοσίας. Ο ΥπΕ καλείται όχι μόνο να συμμορφώνεται, αλλά να

[4] Guidelines on Personal data breach notification under Regulation 2016/679 (wp250rev.01), www.dpa.gr.

αποδεικνύει τη συμμόρφωσή του με αυτές. Σύμφωνα με τον ΓΚΠΔ, οι αρχές που διέπουν την επεξεργασία δεδομένων ατομικού χαρακτήρα, είναι οι εξής (Διαγρ.10) (Πλατής, 2018, Κυριαζόγλου, 2019, Κουκιάδης, 2019):

- *Νομιμότητα*, τα δεδομένα πρέπει να υποβάλλονται σε σύννομη και θεμιτή επεξεργασία. Για παράδειγμα, συχνά η νομιμότητα χάνεται όταν τα δεδομένα στο αρχείο καταγραφής έχουν δηλωθεί για σκοπό Α και νόμιμη βάση Α και ο ΥπΕ ή ο ΕκΕπ την επεξεργασία τα αξιοποιεί για άλλο σκοπό (π.χ. Β).
- *Αντικειμενικότητα.*
- *Διαφάνεια,* η επεξεργασία πρέπει να γίνεται με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων. Στο πλαίσιο της διαφάνειας, οι επιχειρήσεις ή οργανισμοί πρέπει να προσφέρουν στα υποκείμενα πληροφορίες, σχετικά με το ποιος επεξεργάζεται τι και γιατί (αιτιολόγηση).
- *Περιορισμός Σκοπού*, όπου αφορά την αρχή ότι τα δεδομένα προσωπικού χαρακτήρα που συλλέγονται σύμφωνα με ρητούς και νόμιμους σκοπούς, δεν υποβάλλονται σε επεξεργασία κατά τρόπο ασύμβατο προς αυτούς. Υπάρχει η εξαίρεση για αρχειοθέτηση για δημόσιο συμφέρον, ή επιστημονικούς ή ιστορικούς σκοπούς (άρθρο 89, παρ.1).
- *Ελαχιστοποίηση των δεδομένων.* Χρησιμοποιούνται μόνο όσα δεδομένα είναι κατάλληλα και συναφή με τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία.
- *Ακρίβεια.* Τα δεδομένα πρέπει να διακρίνονται από ακρίβεια και, να επικαιροποιούνται, όταν είναι απαραίτητο. Επίσης, πρέπει να λαμβάνονται όλα τα απαραίτητα μέτρα για την άμεση διαγραφή ή διόρθωση δεδομένων προσωπικού χαρακτήρα, που έχουν ανακρίβεια, σε σχέση με τους σκοπούς της επεξεργασίας.
- *Περιορισμός της περιόδου αποθήκευσης.* Η διατήρηση των δεδομένων υπό μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων, αφορά τη περίοδο που χρειάζεται για τους σκοπούς της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα. Η αποθήκευση τέτοιων δεδομένων μπορεί να διαρκεί μεγάλα χρονικά διαστήματα, εφόσον θα υποβάλλονται σε επεξεργασία αποκλειστικά για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς λόγους (άρθρο 89, παρ.1). Απαραίτητη προϋπόθεση, η ύπαρξη κατάλληλων οργανωτικών και τεχνικών μέτρων για τη διασφάλιση των δικαιωμάτων και ελευθεριών του υποκείμενου των δεδομένων.

- *Ακεραιότητα.* Τα δεδομένα επεξεργάζονται με τέτοιο τρόπο έτσι ώστε να διασφαλίζεται η ασφάλεια των δεδομένων προσωπικού χαρακτήρα (π.χ. από μη εξουσιοδοτημένη ή μη νόμιμη επεξεργασία, τυχαία απώλεια, καταστροφή ή φθορά) (άρθρο 89, παρ.1).
- *Λογοδοσία.* Ο ΥπΕ έχει την ευθύνη για την απόδειξη της συμμόρφωσης με το άρθρο 5, παράγραφο 1.

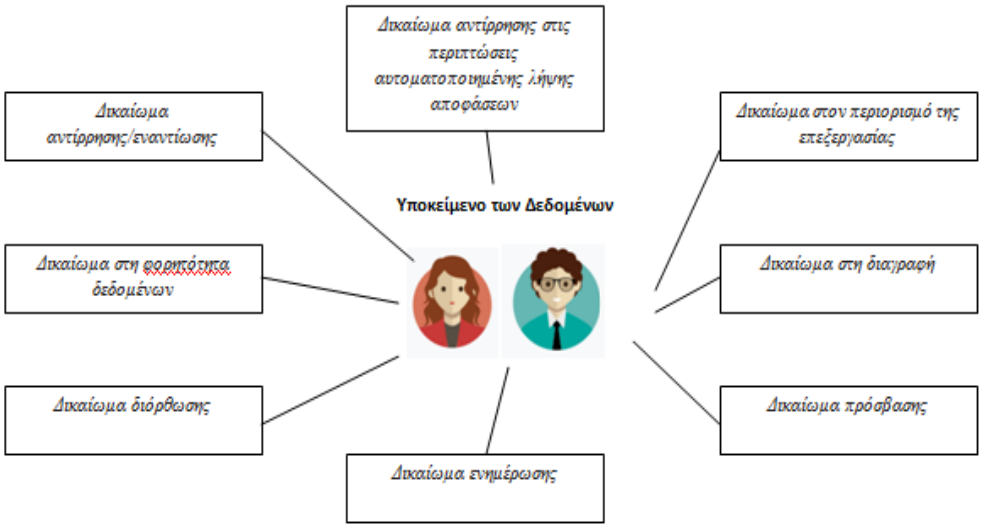


Διάγραμμα 10. Βασικές Αρχές ΓΚΠΔ

2.5 Δικαιώματα του Υποκείμενου των Δεδομένων

Τα δικαιώματα του υποκείμενου των δεδομένων στον ΓΚΠΔ είναι τα ακόλουθα (Διαγρ.11) (Πλατής, 2018, Κυριαζόγλου, 2019, Κουκιάδης, 2019):

- *Δικαίωμα ενημέρωσης.*
- *Δικαίωμα πρόσβασης.*
- *Δικαίωμα διόρθωσης.*
- *Δικαίωμα στη διαγραφή («δικαίωμα στη λήθη»).*
- *Δικαίωμα στη φορητότητα δεδομένων.*
- *Δικαίωμα στον περιορισμό της επεξεργασίας.*
- *Δικαίωμα αντίρρησης/εναντίωσης.*
- *Δικαίωμα αντίρρησης στις περιπτώσεις αυτοματοποιημένης λήψης αποφάσεων.*



Διάγραμμα 11. Δικαιώματα του Υποκείμενου των Δεδομένων, σύμφωνα με το ΓΚΠΔ

2.6 Βασικές Κατηγορίες Νόμιμων Βάσεων

Οι βασικές κατηγορίες Νόμιμων Βάσεων που αφορά την επεξεργασία και διαχείριση δεδομένων, σύμφωνα με τον ΓΚΠΔ και είναι οι ακόλουθες (Διαγρ.12) (Πλατής, 2018, Κουκιάδης, 2019):

- *Ζωτικό Συμφέρον (όχι Διακριτική Ευχέρεια).*
- *Δημόσια Αρχή - Νόμιμη Υποχρέωση (όχι Διακριτική Ευχέρεια).*
- *Σύμβαση - Συγκατάθεση (Διακριτική Ευχέρεια).*
- *Έννομο Συμφέρον του Υπεύθυνου Επεξεργασίας (διακριτική ευχέρεια).*

Διάγραμμα 12. Το πλαίσιο των βασικών κατηγοριών των Νόμιμων Βάσεων, σύμφωνα με το ΓΚΠΔ

Κεφάλαιο Τρίτο

Εργασιακές Σχέσεις και ο Κανονισμός GDPR

Στο κεφάλαιο αυτό γίνεται παρουσίαση της σχέσης μεταξύ Εργασιακών Σχέσεων και του κανονισμού ΓΚΠΔ (GDPR), όσον αφορά το δικαίωμα της επεξεργασίας δεδομένων των εργαζομένων, τη σημασία της για τις εργασιακές σχέσεις και την έννομη προστασία του εργαζόμενου ως υποκειμένου προσωπικών δεδομένων.

3.1 Επεξεργασία Δεδομένων Εργαζομένων και Συγκατάθεση

Σε κάθε επιχείρηση ή οργανισμό του δημόσιου ή ιδιωτικού τομέα, η διαχείριση των προσωπικών δεδομένων του προσωπικού τους, αποτελεί νομική υποχρέωση κάθε εργοδότη. Για παράδειγμα, στο Δημόσιο τομέα, η επεξεργασία των δεδομένων των δημοσίων υπαλλήλων, εντοπίζεται κυρίως στην τήρηση του προσωπικού μητρώου τους, καθώς και στις πειθαρχικές διαδικασίες (βάση του υπαλληλικού κώδικα, που κατοχυρώνει αντίστοιχα εργασιακά δικαιώματα για το προσωπικό της δημόσιας διοίκησης). Έτσι, τα ατομικά δεδομένα (π.χ. ονοματεπώνυμο, εργασιακή εμπειρία, εκπαιδευτικό υπόβαθρο), όσο και πιο ευαίσθητα δεδομένα (π.χ. ιατρικό ιστορικό) βρίσκονται στη διάθεση των εργοδοτών (Πλατής, 2018, Κουκιάδης, 2019).

Ο ΓΚΠΔ δέχεται την επεξεργασία σε δύο περιπτώσεις: με *συγκατάθεση* του εργαζόμενου ή με το *απαραίτητο* της επεξεργασίας. Αυτό ισχύει για όλα τα δεδομένα. Υπάρχουν διαφοροποιήσεις ανάλογα με τον αν πρόκειται για απλά δεδομένα ή δεδομένα ειδικών κατηγοριών (ευαίσθητα δεδομένα). Από την άλλη, οι εργαζόμενοι συνήθως σπάνια μπορούν να αρνηθούν ή να ανακαλέσουν τη συγκατάθεσή τους, λόγω της εργασιακής εξάρτησης που έχουν με τον εργοδότη. Εκτός από σπάνιες περιπτώσεις, οι εργοδότες βασίζονται σε ένα άλλο νομικό πλαίσιο παρά στη συγκατάθεση, όπως η ανάγκη επεξεργασίας για το νόμιμο συμφέρον τους. Ωστόσο, αυτό από μόνο του δεν επαρκεί για να διαγράψει τα δικαιώματα και τις ελευθερίες των εργαζομένων (Κουκιάδης, 2019).

Ειδικότερα, η συγκατάθεση του υποκείμενου προσωπικών δεδομένων αποτελεί ένα από τα στοιχεία που αρκεί για την δυνατότητα να επιτραπεί η επεξεργασία τους, στο πλαίσιο του δικαιώματος της αυτοδιάθεσης. Ο πιθανός αποκλεισμός της συγκατάθεσης θα θεωρούνταν αντισυνταγματικός. Ωστόσο, η συγκατάθεση πρέπει να ακολουθεί το δικαίωμα σεβασμού της αξιοπρέπειας του ατόμου. Έτσι, σε όλες τις περιπτώσεις παροχής της συγκατάθεσης, αυτή πρέπει να είναι δήλωση βουλήσεως ελεύθερα ανακλητή ανά πάσα στιγμή με ισχύ για το μέλλον (άρθρο 7, παρ.3). Αυτή πρέπει να είναι ρητή και διακριτή ως

προς το συγκεκριμένο σκοπό για τον οποίο γίνεται και ταυτόχρονα, σαφής. Η συγκατάθεση συνιστά παραίτηση από την άρνηση επεξεργασίας προσωπικών δεδομένων, αλλά δεν ισχύει και για τις βασικές αρχές επεξεργασίας, για τις οποίες δεν υπάρχει παραίτηση, πέραν αντίθετης διάταξης. Επομένως, η συγκατάθεση δεν μπορεί να ταυτισθεί με την παραίτηση. Βέβαια, η συγκατάθεση ξεπερνιέται, αν υπάρχουν οι σχετικές πληροφορίες, ήδη στο διαδίκτυο (Κουκιάδης, 2019).

Η συγκατάθεση πρέπει να είναι ελεύθερη και για αυτό ο ΓΚΠΔ στο άρθρο 4.11 προσδιορίζει ευθέως την έννοια της συγκατάθεσης. Συγκεκριμένα αναφέρει "*κάθε ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει, με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, αν αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν*". Δηλαδή δεν απαιτείται να είναι έγγραφη, αλλά να είναι βέβαιη από κάθε πλευρά. Ωστόσο, η προφορική συγκατάθεση είναι παρακινδυνευμένη ενέργεια. Ο ΓΚΠΔ με την φράση "*...ή με σαφή θετική ενέργεια....*" φαίνεται να μην αποκλείει και την έμμεση συγκατάθεση του υποκείμενου (Αλεξανδροπούλου-Αιγυπτιάδου, 2007).

Η νομιμοποίηση της συγκατάθεσης για επεξεργασία προσωπικών δεδομένων, μπορεί να επιφέρει κινδύνους για τον εργαζόμενο. Για τις εργασιακές σχέσεις, το σημαντικότερο είναι η "*ελευθερία βούλησης*" του υποκείμενου των δεδομένων, που δύσκολα επαληθεύεται λόγω της εξάρτησης του εργαζόμενου, όπως έχει ήδη σημειωθεί. Όμως, στις εργασιακές σχέσεις υπάρχει μεγάλο ρίσκο η επεξεργασία να βασίζεται μόνο στη συγκατάθεση, αφού στις περισσότερες περιπτώσεις δεν είναι εφικτή η ελεύθερη επιλογή από τον εργαζόμενο, ανεξάρτητα από το εάν αφορά το στάδιο της πρόσληψης ή σε μεταγενέστερο στάδιο. Στις περιπτώσεις που γίνεται δεκτή η συγκατάθεση στις εργασιακές σχέσεις, ειδικά στις επιχειρήσεις με πολλούς εργαζόμενους, το γεγονός ότι η συγκατάθεση δόθηκε από την πλειοψηφία του προσωπικού δεν δίνει την νομιμότητα για επεξεργασία δεδομένων και αυτών που δεν έδωσαν την συγκατάθεση τους, αφού προϋποθέτει ατομική βούληση. Πάντως, εκτιμάται ότι πρακτικά δεν μπορεί να αποτελέσει νόμιμη βάση η συγκατάθεση για επεξεργασία προσωπικών δεδομένων στις εργασιακές σχέσεις. Θα πρέπει να σημειωθεί ότι αυτή η θέση δεν πρέπει να θεωρείται απόλυτη, ιδιαίτερα για τα ανώτερα στελέχη που έχουν μεγάλη δυνατότητα διαπραγμάτευσης στην δυνατότητα διαμόρφωσης των εργασιακών όρων. Επίσης, για να αποφευχθεί η όποια αμφισβήτηση για το αν υπάρχει ελεύθερη ή μη βούληση του εργαζόμενου, θα πρέπει να αποφεύγεται η συγκατάθεση ως νόμιμη βάση για την επεξεργασία δεδομένων, και ο εργοδότης θα πρέπει να στραφεί σε μια από τις υπόλοιπες αναφερόμενες προϋποθέσεις του άρθρου 6, παρ.1 (Κοτσαλής, 2016, Κουκιάδης, 2019).

Η συγκατάθεση δεν απαιτείται όταν η επεξεργασία είναι απαραίτητη. Το απαραίτητο δεν σημαίνει και αναγκαίο. Το απαραίτητο προσδιορίζει την ύπαρξη του δικαιώματος της επεξεργασίας, που συνεπάγεται ότι η σχετική πληροφορία πρέπει να συνδέεται με τον επιδιωκόμενο σκοπό. Προηγείται η εκτίμηση του απαραίτητου και ακολουθεί κατά την επεξεργασία, η εφαρμογή του αναγκαίου ως προσδιοριστικού στοιχείου της έκτασης της επιτρεπόμενης επεξεργασίας, με τη λήψη των κατάλληλων μέτρων. Η κρίση αυτή για το αναγκαίο, υπόκειται σε δικαστικό έλεγχο[5]. Γενικά ο ΓΚΠΔ αναφέρει ρητώς τις περιπτώσεις εκείνες που η επεξεργασία κρίνεται απαραίτητη. αυτές ορίζονται ξεχωριστά για τα απλά δεδομένα (άρθρο 6) και ξεχωριστά για τις ειδικές κατηγορίες (άρθρο 9).

Επίσης, η επεξεργασία των δεδομένων έχει διαφοροποιήσεις σε σχέση με απλά δεδομένα και ειδικές κατηγορίες δεδομένων. Συγκεκριμένα, για την πρώτη κατηγορία δεδομένων, η συγκατάθεση μπορεί να είναι γενική, ενώ αν είναι ειδική, δεν μπορεί να χρησιμοποιηθεί για άλλο σκοπό. Όσο αφορά το στοιχείο του απαραίτητου, όταν αυτό υπάρχει, δεν καθιστά και πάλι αναγκαία τη συγκατάθεση. Ειδικά για την περίπτωση επεξεργασίας με την βοήθεια τεχνολογικών μέσων (υπολογιστής), ο ΓΚΠΔ τονίζει ότι πρέπει να διασφαλιστεί η αξιοποίηση κατάλληλων μέτρων προστασίας. Στο πλαίσιο αυτό, κατ' ελάχιστο, πρέπει να είναι δυνατή η παρέμβαση του εργαζόμενου (Δούκα, 2011, Κουκιάδης, 2019).

Από την άλλη, για τη δεύτερη κατηγορία δεδομένων, που αφορά ειδικές κατηγορίες και συνδέονται με την ταυτοποίηση ενός ατόμου (π.χ. εργαζόμενου), τίθενται ιδιαίτερα προβλήματα για την νόμιμη επεξεργασία τους. Έτσι, σε αυτά υπάρχει ο ρητός κανόνας, της απαγόρευσης επεξεργασίας. Υπάρχει η υποχρέωση του απόρρητου και η δυνατότητα θέσπισης επιπλέον περιορισμών από τα κράτη μέλη της ΕΕ, για την δυνατότητα επιβολής ειδικών πρόσθετων όρων για τη συγκατάθεση (άρθρο 9.2, α). Αυτή πρέπει να είναι ρητή και να δίνεται για συγκεκριμένο σκοπό, όπως ρυθμίζεται στο άρθρο 9. Επίσης, για τις εργασιακές σχέσεις, αυτή καθορίζεται με ένα περιορισμό, που αφορά την άρση της απαγόρευσης της επεξεργασίας, όταν είναι απαραίτητη για ειδικούς λόγους. Όμως σε κάθε περίπτωση για να είναι θεμιτή η επεξεργασία, υπάρχει ο περιορισμός να τηρείται υποχρεωτικά το απόρρητο υπό την ευθύνη του επαγγελματία. Οι όποιες εξαιρέσεις για την επεξεργασία τέτοιων ατομικών δεδομένων περιγράφονται στο άρθρο 9, παρ.2, περ.β του ΓΚΠΔ για τις εργασιακές σχέσεις. Σύμφωνα με τον ΓΚΠΔ, οι εθνικές ρυθμίσεις για να είναι συμβατές με τον κανονισμό για τις εξαιρέσεις, θα πρέπει να προβλέπουν εγγυήσεις για τα θεμελιώδη

[5] ΣτΕ 1108/2017, ΝΟΜΟΣ

δικαιώματα και συμφέροντα του εργαζόμενου για την επεξεργασία ευαίσθητων ατομικών δικαιωμάτων (Ιγγλεζάκη, 2014, Αρμαμέντο και Σωτηρόπουλο, 2005).

3.2 Σχέση Εργαζόμενου - Εργοδότη

Ένα σημαντικό θέμα για τις εργασιακές σχέσεις, αφορά την *εξάρτηση του εργαζόμενου από τον εργοδότη* και τα *όρια διαφύλαξης της ιδιωτικής ζωής* του. Συγκεκριμένα (Αλεξανδροπούλου-Αιγυπτιάδου, 2007, Δούκα, 2011, Κουκιάδης, 2019, Σπυρόπουλος κ.α., 2017, Χρυσόγονος, 2017):

- *η κάλυψη της ιδιωτικής ζωής από το δικαίωμα του πληροφοριακού αυτοπροσδιορισμού.* Αυτό περιλαμβάνει και το δικαίωμα προστασίας και του ιδιωτικού βίου, χωρίς διάκριση σε απόρρητα και μη στοιχεία και ούτε από πιθανή δημοσίευση στη δημόσια σφαίρα (π.χ. διαδίκτυο). Η άποψη ότι η εθελοντική παροχή στοιχείων από τον εργαζόμενο μπορεί να επιτρέψει την επεξεργασία δεδομένων, με επιφύλαξη μπορεί να γίνει δεκτή. Άλλο γνώση ή μη μιας πληροφορίας που αφορά το πεδίο άγνοιας, που επιβάλλεται για τον εργοδότη, άλλο ο τρόπος απόκτησης της γνώσης και άλλο η αξιοποίηση μιας πληροφορίας. Το κρίσιμο ζήτημα δεν είναι η συλλογή της πληροφορίας αλλά η δυνατότητα επεξεργασία τους. Επιπλέον, σε αυτό το ζήτημα προστίθεται και η προστασία της ελεύθερης ανταλλαγής πληροφοριών και της ελευθερίας δραστηριότητας και επικοινωνίας, που συνθέτουν την προσωπική σφαίρα κάθε εργαζόμενου με την ευρεία έννοια. Αυτό που είναι σημαντικό, αφορά τη διασφάλιση της προσωπικής ζωής, που είναι έννοια ευρύτερη της ιδιωτικής ζωής. Θα πρέπει να σημειωθεί σε ότι αφορά ζητήματα ιδιωτικότητας, αυτά αποτελούν σύνηθες αντικείμενο κανονισμών ή συμβάσεων εργασίας.
- *τα δεδομένα του ιδιωτικού βίου*. Υπάρχει ιδιαίτερη αναφορά στα δεδομένα ιδιωτικού βίου λόγω διαφόρων διακρίσεων σχετικών με την ιδιωτικότητα, όπου συνύπαρξη επαγγελματικής και ιδιωτικής ζωής, καθιστά κάποιες φορές δυσδιάκριτα τα όρια μεταξύ τους. Επίσης, κρίσιμο ζήτημα είναι και το θέμα της προστασίας του ιδιωτικού βίου ενός εργαζόμενου, όταν δέχεται έντονη πίεση από την άσκηση του διευθυντικού δικαιώματος του εργοδότη, πέραν κάποιων ορίων (π.χ. απαίτηση για πρόσβαση σε ευαίσθητα δεδομένα). Το σημαντικό δεν είναι η ίδια η επεξεργασία των δεδομένων, αλλά ο καθορισμός των ορίων της διατηρούμενης αυτονομίας του εργαζόμενου από τους περιορισμούς που θέτει η μισθωτή σχέση του με την εντονότερη μορφή δέσμευσης, που επιβάλλει την εξάρτηση του. Άρα πρέπει να τεθούν όρια νόμιμης

επεξεργασίας, σε συνδυασμό με την αξιολόγηση του απαραίτητου και του αναγκαίου της επεξεργασίας. Παράλληλα, θα πρέπει να γίνεται εξέταση του βαθμού σύνδεσης επαγγελματικής και ιδιωτικής ζωής. Κατά συνέπεια, ο εργοδότης πρέπει να αποδεικνύει το νόμιμο της επεξεργασίας και θα πρέπει να ενημερώνει τον εργαζόμενο για την επικείμενη επεξεργασία, η οποία θα πρέπει να γίνεται παρουσία του και να μη θίγονται βασικά δικαιώματα του. Για παράδειγμα, στην σημερινή εποχή της πληροφορικής, ο εργοδότης θα πρέπει να καταστήσει γνωστό στον εργαζόμενου ότι απαγορεύεται ρητά η χρήση υπολογιστή της επιχείρησης για προσωπικά δεδομένα του. Όσο αφορά τα ψηφιακά κοινωνικά δίκτυα (social media), δε επιτρέπεται ο εργοδότης να αξιοποιεί δημοσιεύσιμες πληροφορίες από κοινωνικά δίκτυα, αφού συνιστά "*παράνομη υποκλοπή ταυτότητας*".

- *παρακολούθηση επικοινωνιών και προστασία απορρήτου*. Υπάρχει νομική κατοχύρωση με τη ρητή φράση ότι είναι απόλυτα απαραβίαστο. Όμως υπάρχει εξουσιοδότηση στο νόμο να καθορίσει την άρση, αλλά μόνο για λόγους εθνικής ασφάλειας ή για την εξακρίβωση ιδιαίτερα σοβαρών εγκληματικών πράξεων.

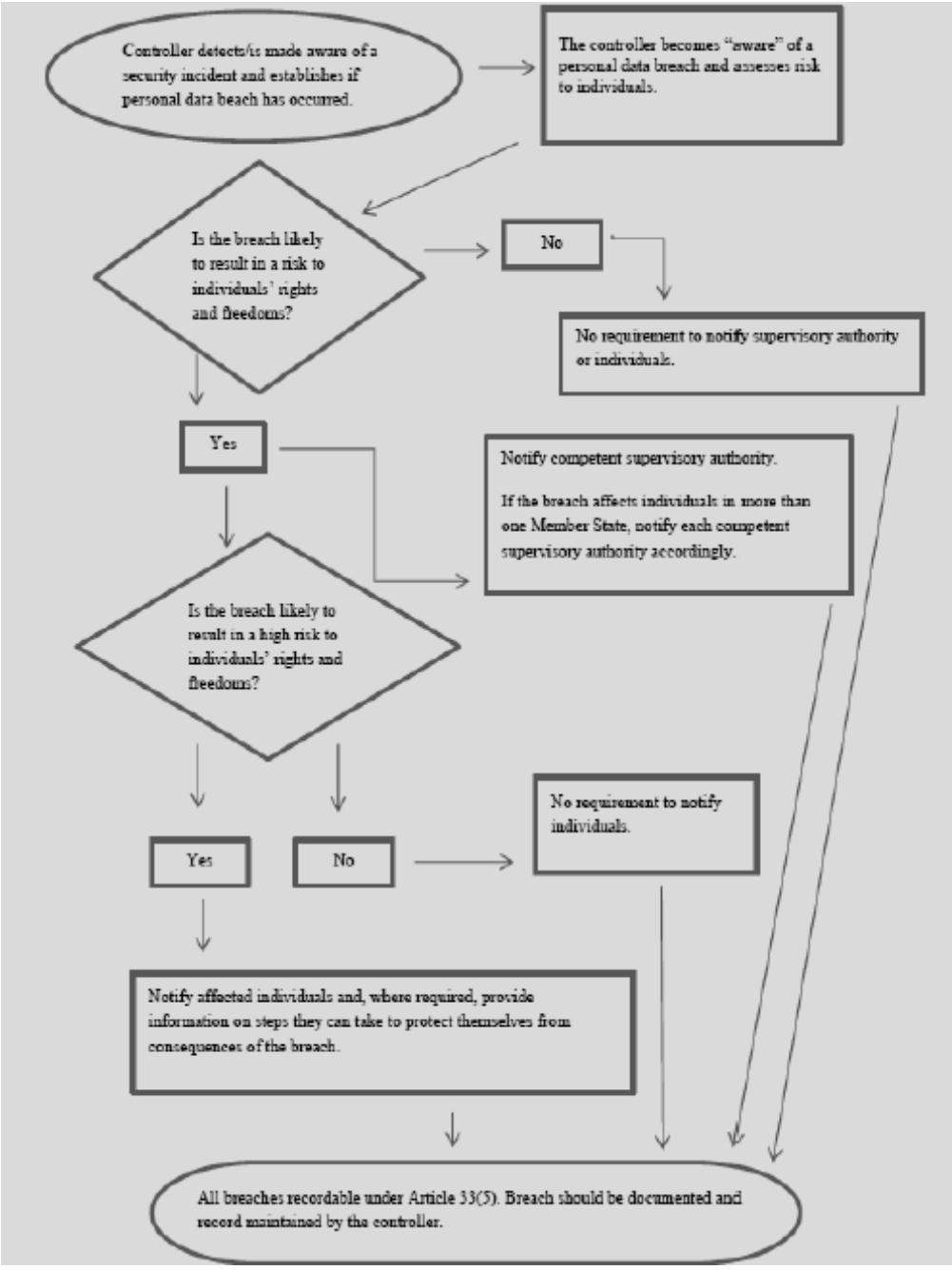
Επιπρόσθετα, η τήρηση ενός *αρχείου επεξεργασίας δεδομένων* στις εργασιακές σχέσεις έχει μεγάλη σημασία. Καθορίζεται στο άρθρο 30 του ΓΚΠΔ, αφού αποτελεί ένα εργαλείο υποβοήθησης της νόμιμης επεξεργασίας και αξιολόγησης της. Είναι υποχρεωτικό για επιχειρήσεις με περισσότερους από 250 εργαζόμενους, αλλά και σε μικρότερο αριθμό εργαζόμενων, με τη προϋπόθεση να υπάρχει δυνητικά κίνδυνος από την εκμετάλλευση των ατομικών δεδομένων για τα εργασιακά δικαιώματα.

Η εργοδοσία θα πρέπει να λάβει υπόψη για την επεξεργασία των δεδομένων των εργαζομένων, τη *συγκατάθεση* του εργαζόμενου. Ο όρος *συγκατάθεση* που χρησιμοποιείται από τον ΓΚΠΔ, δηλώνει στην ουσία την συναίνεση του υποκείμενου, την εκ των προτέρων συγκατάθεση του, η οποία παρέχεται πριν την έναρξη της επεξεργασίας. Δηλαδή, διαφέρει από την *έγκριση*, που αφορά την εκ των υστέρων συγκατάθεση. Ωστόσο, πρέπει να σημειωθεί ότι, η συγκατάθεση δεν συνεπάγεται σε καμία περίπτωση την παραίτηση του υποκείμενου από το δικαίωμα προστασίας των προσωπικών του δεδομένων. Αντίθετα, η συγκατάθεση ως πηγή νομιμοποίηση της επεξεργασίας, εγγυάται την διαφύλαξη των δικαιωμάτων του (Αλεξανδροπούλου-Αιγυπτιάδου, 2007).

Η συναίνεση θα πρέπει να συγκεντρώνει συγκεκριμένα χαρακτηριστικά: να είναι *ελεύθερη* (να μην αποτελεί προϊόν πίεσης αλλά πραγματικής βούλησης), *ρητή* (να φανερώνει ξεκάθαρα την βούληση του εργαζόμενου για άδεια στην επεξεργασία των ατομικών δεδομένων του), *ανακλητή* (να υπάρχει η δυνατότητα ανάκλησης, όποτε επιθυμεί, χωρίς να

θίγεται η νομιμότητα της επεξεργασίας των δεδομένων μέχρι εκείνη τη στιγμή), *συγκεκριμένη* (να είναι σαφές και εύκολα κατανοητό στο υποκείμενο των δεδομένων, ότι συναινεί για συγκεκριμένο σκοπό), και *εν πλήρη επιγνώσει* (πλήρη πληροφόρηση για ατομικά δεδομένα θα χρησιμοποιηθούν για το συγκεκριμένο σκοπό επεξεργασίας) (Πλατής, 2018, Κυριαζόγλου, 2019, Κουκιάδης, 2019).

Η παραβίαση μπορεί να έχει πολλά και σημαντικά αρνητικά αποτελέσματα για τα άτομα. Στο επόμενο διάγραμμα, φαίνεται η Διαδικασίας Αναγγελίας Παραβίασης Δεδομένων (WP250, 2017).



Διάγραμμα 13. Διάγραμμα Ροής Διαδικασίας Αναγγελίας Παραβίασης Δεδομένων

3.3 Προστασία Δεδομένων και Τεχνολογία Επεξεργασίας

Οι κανόνες για την προστασία των προσωπικών δεδομένων ισχύουν ανεξάρτητα από την χρήση ή μη, τεχνολογίας. Ο ΓΚΠΔ κάνει αναφορά για λήψη αποφάσεων με τη χρήση αυτοματοποιημένης επεξεργασίας, που προβλεπόταν ήδη στην Οδηγία 95/46 και στο σχετικό νόμο 2472/1997, με την επιφύλαξη ότι αυτή δεν ξεχώριζε αποκλειστική και μη αποκλειστική αυτοματοποιημένη επεξεργασία δεδομένων (Αρμαμέντο, και Σωτηρόπουλο, 2005).

Στην επεξεργασία με υπολογιστή συμπεριλαμβάνεται και η κατάρτιση προφίλ, με την προϋπόθεση η επεξεργασία να παράγει οποιοδήποτε έννομο αποτέλεσμα ή έστω να επηρεάζει σημαντικά τον εργαζόμενο (άρθρο 22). Ο χαρακτηρισμός της επεξεργασίας ως αυτοματοποιημένης ανήκει στη δικαστική κρίση με βάση την εκάστοτε τεχνολογική εξέλιξη. Επίσης, η προβλεπόμενη ρύθμιση από τον ΓΚΠΔ για την αυτοματοποιημένη ατομική λήψη αποφάσεων αφορά κάθε εργαζόμενο και ευρύτερα κάθε επεξεργασία από δημόσια ή ιδιωτική εξουσία. Έχει διαπιστωθεί ότι οι νέες τεχνολογίες παρέχουν δυνατότητες για εισβολή στον ιδιωτικό βίο του κάθε ατόμου, με πιθανές δυσάρεστες επιπτώσεις. Στο εργασιακό περιβάλλον, όταν ο εργοδότης διαθέτει αυξημένη ιδιωτική εξουσία επί του εργαζόμενου, τότε εμφανίζονται διάφοροι κίνδυνοι σχετικά με τα δικαιώματα και το απόρρητο των δεδομένων του. Οι νέες τεχνολογίες της Πληροφορικής και των Επικοινωνιών έχουν καταστεί αναπόσπαστο μέρος στη σύγχρονη διαχείριση μιας επιχείρησης ή οργανισμού (Κοτσαλή, 2016). Έτσι, οι όποιοι κίνδυνοι στην επεξεργασία των προσωπικών δεδομένων από την χρήση τεχνολογίας, μπορεί να εμφανισθούν στα εξής πεδία (Κουκιάδης, 2019):

- *στην κατάρτιση προφίλ με αυτοματοποιημένη επεξεργασία*. Η επεξεργασία αυτή στο εργασιακό περιβάλλον υποτίθεται ότι αντικειμενοποιεί την εργοδοτική κρίση, ωστόσο υποκρύπτει αυθαίρετους κινδύνους αξιολογήσεων του εργαζομένου. Αυτό είναι ένα καθοριστικό στοιχείο για τη συνολική συμπεριφορά απέναντι στον εργαζόμενο. Επιπλέον, ο ΓΚΠΔ εστιάζει στο προσδιορισμό της έννοιας του προφίλ και της σημασίας που έχει για την εργασιακή απόδοση. Έχει παρατηρηθεί στο μοντέρνο μάνατζμεντ ότι, κατά τις προσλήψεις προσωπικού όλη η έμφαση δίνεται στη λεπτομερή κατάταξη των υποψηφίων σε κατηγορίες ανάλογα με τα ψυχικά και φυσικά δεδομένα. Γενικά, ο κανονισμός συνδέει την κατάρτιση του προφίλ με την αυτοματοποιημένη επεξεργασία, που αποτελεί μια προχωρημένη μορφή σχηματισμού προφίλ, ιδιαίτερα αξιοποιήσιμη από την διαχείριση ανθρώπινου δυναμικού (HRM).
- *στα στοιχεία του συστήματος αυτοματοποιημένης επεξεργασίας στις σχέσεις εργασίας*. Σύμφωνα με το άρθρο 22 του ΓΚΠΔ, η αυτοματοποιημένη επεξεργασία προβλέπει

ένα υποσύστημα με τρεις πυλώνες: ο πρώτος αφορά το δικαίωμα της μη συναίνεσης, ο δεύτερος τη δυνατότητα επεξεργασίας με μονομερή απόφαση του ΥπΕ και ο τρίτος αφορά την επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων. Το επιτρεπτό της επεξεργασίας στις εργασιακές σχέσεις αφορά (άρθρο 22, παρ.2): (α) το αναγκαίο της επεξεργασίας για τη σύναψη και εκτέλεση σύμβασης σύμφωνα με τον ΓΚΠΔ, και (β) τη ρητή πρόβλεψη από το δίκαιο της ΕΕ ή το εθνικό, για το επιτρεπτό της επεξεργασίας δεδομένων, εφόσον αυτή συνοδεύεται με μέτρα κατάλληλα προστασίας. Επίσης, στις δύο περιπτώσεις επεξεργασίας χωρίς συγκατάθεση, για την νομιμότητα της αυτοματοποιημένης επεξεργασίας, γίνεται ειδική αναφορά σε κατάλληλα μέτρα προστασίας, που πρέπει να λαμβάνονται από τον ΓΚΠΔ όπως: τη πρόβλεψη δυνατότητας παρέμβασης του υπεύθυνου στα πορίσματα της αυτοματοποιημένης επεξεργασίας και τη διασφάλιση του δικαιώματος του εργαζόμενου να εκφράσει την άποψη του για τη χρήση ενός συγκεκριμένου ατομικού δεδομένου. Επιπλέον, μετά την ολοκλήρωση της επεξεργασίας, υπάρχει το δικαίωμα του εργαζόμενου για αμφισβήτηση των πορισμάτων της αυτοματοποιημένης επεξεργασίας. Για την επεξεργασία ειδικών κατηγοριών δεν υπάρχουν οι εξαιρέσεις των γενικών προσωπικών δεδομένων, αλλά προβλέπονται εξαιρέσεις για λόγους δημόσιου συμφέροντος. Όλα αυτά δημιουργούν αξιώσεις για κάθε εργαζόμενο με δυνατότητα προσφυγής στα δικαστήρια και λήψης ακόμη και ασφαλιστικών μέτρων, που προβλέπεται από το Ν.2472/1992 (άρθρο 14, παρ.1). Η μη σύννομη επεξεργασία συνιστά παραβίαση νόμιμων ενοχικών υποχρεώσεων από τη σχέση εργασίας και αντίστοιχος είναι ο δικαστικός έλεγχος.

Τέλος, υπάρχει ειδική πρόβλεψη για την προσωρινή δικαστική προστασία, αφού η αυτοματοποιημένη επεξεργασία στις εργασιακές σχέσεις, που οδηγεί πάλι σε εργοδοτική απόφαση, υπόκειται σε δικαστικό έλεγχο. Ειδική πρόβλεψη υπάρχει για προσωρινή δικαστική προστασία του εργαζόμενου για αποφάσεις που λαμβάνονται αποκλειστικά με αυτοματοποιημένη επεξεργασία από τον νόμο 2472.97 (άρθρο 14 παρ.1). Ο εργαζόμενος μπορεί να επιδιώκει αναστολή εκτέλεσης αποφάσεων της εργοδοσίας που θίγουν τα δικαιώματα του (μετάθεση, απόλυση κ.α.), χωρίς την συνδρομή άλλων ουσιαστικών προϋποθέσεων.

3.4 Νέες Τεχνολογίες Επιτήρησης στον Εργασιακό Χώρο

Σήμερα, με την εκρηκτική ανάπτυξη των νέων τεχνολογιών και του διαδικτύου, η επιτήρηση των εργαζομένων από τον εργοδότη, δεν πραγματοποιείται πλέον με τη φυσική του

παρουσία, αλλά με την χρήση εξελιγμένων τεχνολογικά μέσων (π.χ. διαδίκτυο, κάμερες, αισθητήρες κίνησης κ.α.)(Jenero and Mapes-Riordan, 1992, Kidder and Bloom, 2001, Lane, 2003, Winstanley at al., 1996, Winstanley and Woodall, 2000).

Η ελληνική εποπτική αρχή (ΑΠΔΠΧ) με την *115/2001 Οδηγία*, επιχείρησε να προσαρμόσει την νομοθεσία για τα προσωπικά δεδομένα στο πνεύμα των διατάξεων του εργατικού δικαίου (Mitrou and Karyda, 2006, Μήτρου, 2017). Η συλλογή των δεδομένων ατομικού χαρακτήρα πρέπει να συνδέεται άμεσα με την απασχόληση και την οργάνωση της εργασίας και να μην διεισδύει στην "*προσωπική σφαίρα*" των εργαζομένων. Πρέπει ακόμα να υπάρχουν χώροι που δεν παρακολουθούνται αλλά και να εξασφαλίζεται η ύπαρξη τηλεπικοινωνιακών μέσων για να αναπτύσσουν και προσωπική επικοινωνία. Ηπιότερα μέτρα που μπορεί να ληφθούν, είναι για παράδειγμα, η τοποθέτηση συναγερμού ή η πραγματοποίηση του ελέγχου από προσωπικό ασφαλείας (Δούκα, 2011).

Όσον αφορά την χρήση βίντεο, επεσήμανε η οδηγία την υποχρέωση το υπεύθυνου επεξεργασίας να τοποθετεί τις κάμερες με τέτοιο τρόπο, έτσι ώστε να μην συλλέγονται περισσότερα δεδομένα από όσα είναι απολύτως αναγκαία. Για παράδειγμα, δεν επιτρέπεται στους εξωτερικούς χώρους της επιχείρησης, διότι υπάρχει κίνδυνος παρακολούθησης των περαστικών. Μόνο σε εξαιρετικές περιπτώσεις, όπως στα ΑΤΜ των τραπεζών, μπορεί να γίνει δεκτή μια τέτοια λήψη. Επιπλέον, απαγορεύεται να χρησιμοποιηθεί ως μέσο αξιολόγησης της παραγωγικότητας των εργαζομένων. Αυτή η απαγόρευση μπορεί να καμφθεί μόνο όταν συντρέχουν εξαιρετικοί λόγοι προστασίας της ασφάλειας και της υγείας των εργαζομένων ή προστασίας κρίσιμων υποδομών (π.χ. στρατιωτικά εργοστάσια, εργοστάσια ηλεκτροδότησης). Αυτό συνεπάγεται ότι σε εργασιακούς χώρους όπως είναι τα γραφεία μιας επιχείρησης ή οργανισμού, δεν επιτρέπεται η επιτήρηση των εργαζομένων με αυτοματοποιημένα μέσα (Δούκα, 2011, Μήτρου, 2017).

Η 1/2011 Οδηγία αποτέλεσε την βάση για την έκδοση μεταγενέστερων Αποφάσεων της ΑΠΔΠΧ, ακολουθώντας το πνεύμα της και όπου έκριναν σε πολλές περιπτώσεις ότι απαγορεύεται η επιτήρηση με χρήση βίντεο των εργαζομένων, εντός των εργασιακών χώρων, εκτός από εξαιρετικές περιπτώσεις όπου αυτό δικαιολογείται από την φύση και τις συνθήκες της εργασίας και για λόγους προστασίας της υγείας και της ασφάλειας των εργαζομένων ή προστασίας κρίσιμων υποδομών[6]. Για παράδειγμα, κρίθηκε ότι πρέπει να αφαιρεθεί κάμερα που τοποθετήθηκε σε κουζίνα αλλά και στο εσωτερικό του καταστήματος, στους χώρους των γραφείων και στις θέσεις εργασίας των εργαζομένων σε δικηγορική εταιρία και σε τεχνική

[6] Αποφάσεις ΑΠΔΠΧ, 4/2009, 12/2014, 20/2017, 1/2018, 40/2018, 41/2018.

εταιρία μελετών. Ειδικότερα, στην τεχνική εταιρία που ήταν ανάδοχος της μελέτης του Εθνικού Κτηματολογίου, είχε τοποθετήσει 30 κάμερες στον εργασιακό χώρο χωρίς καμία σχετική προειδοποίηση προς τους εργαζόμενους. Μια εργαζόμενη προσέφυγε στην ΑΠΔΠΧ, καταγγέλλοντας ότι έλαβε υποχρεωτικά άδεια άνευ αποδοχών ως ποινή επειδή έκανε διάλειμμα κατά την διάρκεια της εργασίας απαντώντας σε μηνύματα στο κινητό της τηλέφωνο. Από την πλευρά της, η τεχνική εταιρεία, δικαιολογήθηκε ότι οι κάμερες χρησιμοποιούνται για φύλαξη εξοπλισμού, επειδή υπήρχαν περιστατικά κλοπής, ενώ είχαν τοποθετηθεί ενημερωτικές πινακίδες σε όλους τους ορόφους. Όσον αφορά την καταγγελία της εργαζομένου, η εταιρεία απάντησε ότι η κατά την κρίση της εταιρίας χαμηλή παραγωγικότητα της, προέκυψε από δειγματοληπτικούς ελέγχους και όχι από την παρακολούθηση μέσω κάμερας. Η Εποπτική Αρχή αποφάνθηκε ότι δεν υπήρχε ικανοποιητική ενημέρωση των εργαζομένων και ότι το ενδεχόμενο κλοπών μπορούσε να αποτραπεί με χρήση ηπιότερων μέτρων, όπως με την τοποθέτηση καμερών στον εξωτερικό χώρο του κτιρίου, ενώ κατέληξε στην διαπίστωση ότι "*η επιτήρηση με βίντεο των γραφείων και των θέσεων εργασίας των εργαζομένων συνιστά υπέρμετρη προσβολή των προσωπικών τους δεδομένων ενώ αποτελεί απρόσφορο και αναποτελεσματικό μέτρο για την προστασία του εξοπλισμού από κλοπή ή την ασφαλή επεξεργασία των τηρούμενων προσωπικών δεδομένων*"[7].

Το Ευρωπαϊκο Δικαστήριο Δικαιωμάτων του Ανθρώπου (ΕΔΔΑ) το 2019 έκανε μια στροφή στη νομολογία του. Ειδικότερα, στην υπόθεση *Lopez Ribalda and Others v. Spain*, η Ολομέλεια του δικαστηρίου δέχτηκε ότι ήταν νόμιμη η παρακολούθηση με κρυφές κάμερες υπαλλήλων γνωστής αλυσίδας σουπερμάρκετ, που ήταν ύποπτοι για κλοπές. Στάθμισε το δικαίωμα των εργαζομένων στην ιδιωτικότητα και το δικαίωμα του εργοδότη στην προστασία της ιδιοκτησίας του. Τελικά έκρινε ότι η ύπαρξη εύλογης υποψίας για διάπραξη σοβαρού παραπτώματος και η έκταση των ζημιών που εντοπίστηκαν στην παρούσα υπόθεση, συνιστούν σοβαρή δικαιολογία για την παρακολούθηση των εργαζομένων ακόμα και χωρίς προηγούμενη ενημέρωσή τους για την εγκατάσταση κλειστού κυκλώματος τηλεόρασης (CCTV). Με βάση το σκεπτικό αυτό, η ΕΔΔΑ απέρριψε την προσφυγή των εργαζομένων, καθώς δέχτηκε ότι δεν υπήρξε παραβίαση[8]. Ωστόσο είχε προηγηθεί απόφαση του 3ου Τμήματος του δικαστηρίου που δικαίωνε τους προσφεύγοντες, καθώς έκρινε ότι η κρυφή παρακολούθηση/εποπτεία δεν είναι νόμιμη, αφού υπάρχει η υποχρέωση προηγούμενης και ρητής ενημέρωσης που υπέχει ο εργοδότης[9].

[7] ΑΠΔΠΧ, Απόφαση 20/2017.
[8] ΕΔΔΑ, Lopez Ribalda and Others v. Spain, 17.10.2019, No 1874/13, 8567/2013.
[9] ΕΔΔΑ, Lopez Ribalda and Others v. Spain, 9.01.2018, No 1874/13, 8567/2013.

3.5 Η έννομη προστασία του εργαζόμενου ως υποκειμένου προσωπικών δεδομένων

Η πρόβλεψη κυρώσεων και η παροχή ένδικων βοηθημάτων αποτελούν το πυρήνα της προσφερόμενης προστασίας και οι κυρώσεις αποτελούν κατά τον ΓΚΠΔ, βασικό μέρος του συστήματος αποτελεσματικής εφαρμογής της προστασίας προσωπικών δεδομένων. Άλλες προβλέπονται από τον ΓΚΠΔ και άλλες από τις Εθνικές νομοθεσίες.

Ο εργαζόμενος όπως κάθε υποκείμενο προσωπικών δεδομένων, διαθέτει ένα οπλοστάσιο από ένδικα βοηθήματα. Ωστόσο, οι κυρώσεις που προβλέπονται λειτουργούν ανεξάρτητα από τις κυρώσεις παραβίασης της εργατικής νομοθεσίας. Όμως, υπάρχει μια αλληλεπίδραση μεταξύ ΓΚΠΔ και εργατικής νομοθεσίας, όπου θέτει διάφορα νομικά προβλήματα ως αποτέλεσμα της διπλής ιδιότητας του εργαζόμενου ως παρόχου εργασίας και ως υποκείμενου δεδομένων και της ιδιότητας του εργοδότη ως αποδέκτη της εργασίας και ως υπεύθυνου της επεξεργασίας (Κουκιάδης, 2019).

Η αποτελεσματικότερη προστασία είναι η προληπτική, αφού έτσι αποφεύγονται τετελεσμένα γεγονότα. Ο ΓΚΠΔ δίνει βάρος στην προληπτική διάσταση, αλλά σε κάθε περίπτωση, η αποτελεσματική προστασία πρέπει να περιλαμβάνει κυρώσεις. Ο ΓΚΠΔ έχει διάφορες κυρώσεις που συμπορεύονται με την εθνική νομοθεσία και τις αντίστοιχες κυρώσεις. Για παράδειγμα, στην Ελλάδα ισχύει ο Ν. 2472/97, που προβλέπει ένα σύνολο κυρώσεων: διοικητικές, αστικές και ποινικές (άρθρα 21, 22, 23, 24). Αυτές οι κυρώσεις θα πρέπει να εναρμονιστούν με τις κυρώσεις του ΓΚΠΔ, για αποφυγή διπλών κυρώσεων (Κοτσαλή, 2016).

Πιο συγκεκριμένα, από τον ΓΚΠΔ προβλέπονται οι εξής κυρώσεις (Διάγρ. 14) ((Πλατής, 2018, Κουκιάδης, 2019):

- *διοικητικές κυρώσεις*. η αρχική διοικητική κύρωση ανήκει στην Ανεξάρτητη Αρχή Προσωπικών Δεδομένων (ΑΠΔΠΧ), που ως δέκτης καταγγελίας σύμφωνα με το άρθρο 77 του ΓΚΠΔ και με τις εκτεταμένες εξουσίες ελέγχου και παρακολούθησης (άρθρο 57, 58), αποκτά άμεση γνώση των παραβάσεων. Επίσης, διαθέτει με διάφορες εξουσίες, όπως προειδοποίηση του ΥπΕ, εντολή συμπλήρωσης, ανάκληση τυχόν άδειας επεξεργασίας, καταστροφή αρχείου[10]. Όμως η βασική αρμοδιότητα είναι η επιβολή προστίμων κλιμακωτά, έτσι ώστε να συνδέονται με διάφορα στοιχεία. Η ΑΠΔΠΧ εξετάζει την νομιμότητα της εκμετάλλευσης των ατομικών δεδομένων, ενώ τη νομιμότητα της απόφασης της εργοδοσίας (π.χ. απόλυση) την ελέγχουν τα δικαστήρια. Οι κυρώσεις βαραίνουν τον ΥπΕ χωρίς να απαιτείται πταίσμα (άρθρο

[10] ΣτΕ 1851/2016.

83). Επιπλέον, η καθιέρωση αντικειμενικής ευθύνης αποτελεί βασική επιλογή και ισχύει εν μέρει και για την αστική ευθύνη, που γίνεται δεκτή ως νόθος αντικειμενική ευθύνη. Επιχειρείται μια μετεξέλιξη της ευθύνης διακινδύνευσης που βασίζεται στην αντίληψη ότι εκείνος που προσφεύγει ή αξιοποιεί πηγές κινδύνων και απολαμβάνει σχετικών ωφελημάτων, πρέπει να φέρει το βάρος του σχετικού κινδύνου (Κοτσαλής, 2016). Ο ΓΚΠΔ επιβάλλει επιμέρους κριτήρια διοικητικών κυρώσεων από την αρμόδια εποπτική Αρχή (βαθμός πταίσματος, φύση παράβασης, διάρκεια, υποτροπή κ.α.). Διαφοροποιεί το ύψος του προστίμου για την περίπτωση επιχειρήσεων για τις οποίες λαμβάνονται υπόψη ο συνολικός, παγκόσμιος κύκλος εργασιών του προηγούμενου οικονομικού έτους, με ανώτατο όριο το 2% ή 4%, ανάλογα με την παράβαση (άρθρο 83, παρ.3,4). Τα πρόστιμα στο εργασιακό περιβάλλον βαρύνουν τον εργοδότη ως υπεύθυνου επεξεργασίας, που σε επιχειρήσεις είναι το νομικό πρόσωπο, και τον ΕΚΕπ (άρθρο 83, παρ.3,4α). Ειδικότερα, για τις εργασιακές σχέσεις ισχύει η δυνατότητα εκπροσώπησης του εργαζόμενου από φορείς γενικού συμφέροντος, που πρέπει να ενταχθούν σε αυτούς και οι συνδικαλιστικές οργανώσεις (άρθρο 80).

- *αστικές κυρώσεις*. Η παράνομη επεξεργασία δεδομένων δημιουργεί και αστική ευθύνη, που είναι αποκαταστατική και αποζημιωτική (αδικοπραξία). Επιπλέον, για τον εργαζόμενο ισχύει ενδοσυμβατική ευθύνη, αφού συνδέεται με τον εργοδότη με ενοχική σχέση. Η αστική αποζημιωτική ευθύνη προβλέπεται ρητά από τον ΓΚΠΔ: "*...Κάθε πρόσωπο το οποίο υπέστη υλική ή μη υλική ζημιά ως αποτέλεσμα παραβίασης του παρόντος κανονισμού δικαιούται αποζημίωση από τον ΥπΕ ή τον ΕκΕπ για τη ζημία που υπέστη...*" (άρθρο 82, παρ.1). Ωστόσο, για το ζήτημα της αστικής ευθύνης για αποζημίωση, ο ΓΚΠΔ επέφερε μια διαφοροποίηση. Θεωρήθηκε ότι ο ΓΚΠΔ και ο Ν.2472/97 δημιουργούν μια νέα μορφή αστικού αδικήματος. Αυτή η εξέλιξη θεωρήθηκε σημαντική, γιατί θεσπίζονται όροι που συμβάλλουν στην επιπλέον ενίσχυση της προστασίας του εργαζόμενου (ή όποιου υποκείμενου δεδομένων), ενώ επανακαθορίστηκε η ευθύνη του υποκείμενου των προσωπικών δεδομένων (Λαδάς, 2018, Κοτσαλής, 2016). Η ευθύνη σύμφωνα με τον ΓΚΠΔ βαρύνει εξίσου τον ΥπΕ και τον ΕκΕπ, χωρίς να ενδιαφέρει η ανάθεση ή μη της επεξεργασίας σε τρίτα πρόσωπα. Το ζήτημα για το αν συντρέχει ευθύνη εις ολοκληρίαν, λόγω της πολυμορφίας των περιπτώσεων πρέπει να αντιμετωπισθεί κατά περίπτωση με αναφορά στον εθνικό δίκαιο (Παναγοπούλου-Κουτνατζή, 2017). Προϋπόθεση για την καταβολή αποζημίωσης ή χρηματικής ικανοποίησης, είναι η απόδειξη υλικής ή

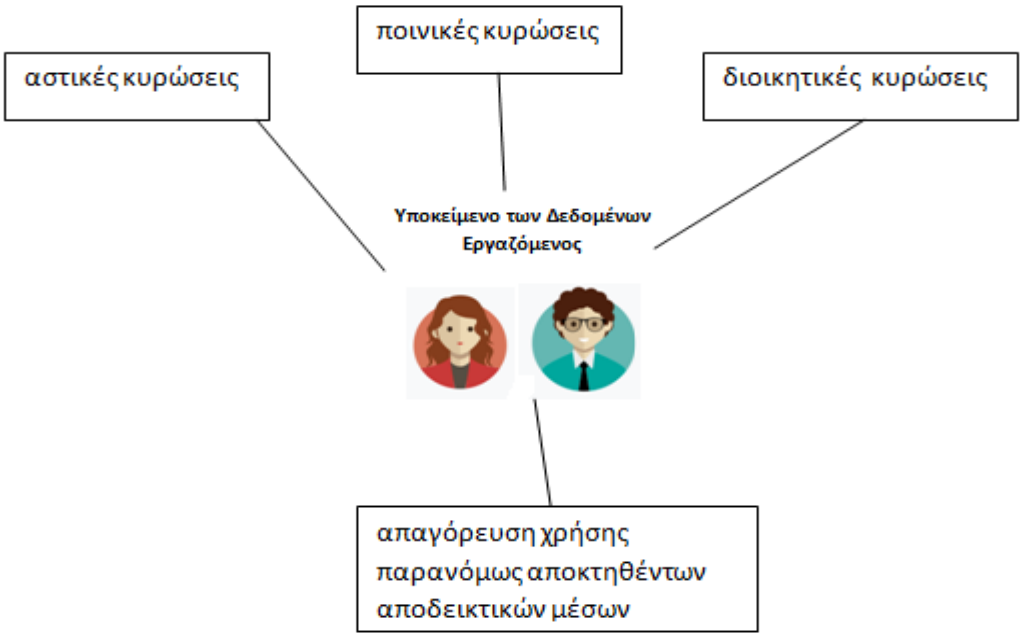
ηθικής βλάβης. Η ηθική βλάβη συνίσταται στη ψυχική διαταραχή που αισθάνεται το άτομο, όπως και στην προσβολή της προσωπικότητας (Σταθόπουλος, 2000). Επιπρόσθετα, υπάρχει και η ενδοσυμβατική ευθύνη για τις εργασιακές σχέσεις, κατά την οποία η παράνομη επεξεργασία συνιστά παραβίαση ενοχικών υποχρεώσεων του εργοδότη, όπως η παραβίαση της υποχρέωσης πρόνοιας, της υποχρέωσης ίσης μεταχείρισης, η κατάχρηση άσκησης δικαιωμάτων κ.α. Πιο συγκεκριμένα, αν η παράνομη επεξεργασία δεδομένων οδηγεί σε εργοδοτικές αποφάσεις που θίγουν εργασιακά δικαιώματα (παράλειψη προαγωγής, πειθαρχική ποινή κ.α.), η σχετική αγωγή μπορεί να περιλαμβάνει πέρα από το αίτημα για αποζημίωση και ικανοποίηση σχετικού δικαιώματος με ακυρότητα της συγκεκριμένης απόφασης. Αυτή η δυνατότητα ανοίγει νέους τρόπους ελέγχου και νέες δυσχέρειες καταχρηστικής άσκησης του διευθυντικού δικαιώματος από την εργοδοσία (σοβαρός λόγος καταγγελίας της σύμβασης).

- *ποινικές κυρώσεις*. Η ποινική προστασία είναι θέμα εθνικής νομοθεσίας. Στην Ελληνική νομοθεσία έχουν προβλεφθεί σχετικές ποινικές κυρώσεις ιδιαίτερα αυστηρές (Ν.2472/97, άρθρο 22). Η νομοθεσία αναφέρεται σε επιμέρους αδικήματα με πρόβλεψη χρηματικών ποινών και φυλάκιση, που σε ορισμένες περιπτώσεις επισείει μέχρι και ποινές κάθειρξης. Επίσης, στις περιπτώσεις συλλογική σύμβασης εργασίας, η μη συμμόρφωση προς τον κανονισμό, αποτελεί και παραβίαση εργατικής νομοθεσίας, με τις προβλεπόμενες αντίστοιχες ποινικές κυρώσεις.

Τέλος, από δικονομική άποψη, γεννιούνται νέα ζητήματα από τον ΓΚΠΔ, όπως το θέμα της απόδειξης. Για την παροχή νομικής προστασίας εμπλέκεται αναγκαστικά και το θέμα της απόδειξης. Η εργοδοσία για να θεμελιώσει τους ισχυρισμούς της για την νομιμότητα της απόφασής της που θίγει συμφέροντα εργαζόμενου, προσφεύγει σε διάφορα δεδομένα για να αποδείξει τη βασιμότητα των ισχυρισμών της. Η αξιοποίηση αποδεικτικών μέσων, παρανόμως αποκτηθέντων, δεν μπορεί να αποτελέσουν νόμιμο αποδεικτικό μέσο. Δηλαδή απαγορεύεται ρητά η χρήση αποδεικτικών μέσων που έχουν αποκτηθεί κατά παράβαση του απορρήτου (άρθρο 19, παρ.3Σ). Η απαγόρευση διατυπώνεται κατά τρόπο απόλυτο, με συγκεκριμένη ειδική εξαίρεση, με στόχο να περιοριστεί η τάση της νομολογίας για περιορισμό των περιπτώσεων απαγόρευσης.

Ένα άλλο ζήτημα αφορά τη δικαστική εκπροσώπηση από τη συνδικαλιστική οργάνωση. Αυτή δεν προβλέπεται από τον ΓΚΠΔ, ενώ από το εθνικό δίκαιο, η νομιμοποίηση της συνδικαλιστικής οργάνωσης για άσκηση αγωγής υπέρ των μελών επιτρέπεται μόνο για τα εργασιακά δικαιώματα που απορρέουν από τις συλλογικές συμβάσεις και άλλες διατάξεις

που εξομοιώνονται με αυτές, εκτός εάν υπάρχει ρητή αντίθετη δήλωση του εργαζόμενου. Επίσης, η έγερση των σχετικών αγωγών από τον εργαζόμενο μπορεί να έχει διάφορα αιτήματα. Για να μην αόριστες, θα πρέπει να αναφέρονται σε συγκεκριμένη παράβαση του ΓΚΠΔ και ότι αυτή έχει επίπτωση στην παραβίαση κάποιου δικαιώματος που αναγνωρίζεται στο υποκείμενο προσωπικών δεδομένων.



Διάγραμμα 14. Νομική προστασία του εργαζόμενου ως υποκείμενου Προσωπικών Δεδομένων

3.6 Προστασία Δεδομένων Υγείας Εργαζομένων και Δημόσια Υγεία (Covid-19)

Η προστασία των δεδομένων υγείας των εργαζομένων, εφαρμόζεται από πολύ αυστηρούς κανόνες (Πλατής, 2018, Κουκιάδης, 2019, Κυριαζόγλου, 2019). Από την άλλη, η προφύλαξη της δημόσιας υγείας ανήκει στο πλαίσιο του δημοσίου συμφέροντος. Εάν νοσήσει ένα σημαντικό ποσοστό του πληθυσμού και αυξηθεί η θνητότητα, αυτό θα επιβαρύνει το δημόσιο συμφέρον σε διάφορα πεδία: πληθυσμιακά, οικονομικά, κοινωνικά (Σπηλιωτόπουλο, 2011, σ.92, Βενιζέλος, 1990, σ.45, Ηλιάδου, 2016, σ.83, Μανιτάκη, 1994, Τάχο, 2008). Επιπλέον, το δικαίωμα στην υγεία στο Ελληνικό Σύνταγμα έχει δύο πλευρές: ατομικό και κοινωνικό δικαίωμα (Δαγτόγλου, 2005, σ.253, Χρυσόγονο και Βλαχόπουλο, 2017, σ.575, Κριάρη-Κατράνη, 1999, σ.47).

Η εμφάνιση της πανδημίας (Covid-19) ανάγκασε τις επιχειρήσεις και οργανισμούς να προβούν σε ευρεία συλλογή προσωπικών δεδομένων με στόχο την πρόληψη ή/και τον περιορισμό της. Τα μέτρα αυτά μπορούν να περιλαμβάνουν επεξεργασία τόσο προσωπικών δεδομένων όσο και ειδικών κατηγοριών δεδομένων. Τα πρώτα αφορούν καταγραφή

πληροφοριών σχετικών με ταξίδια, πληροφορίες σχετικά με συμβάντα που σχετίζονται με τη μόλυνση καθώς και την ιχνηλάτηση επαφών. Τα ειδικών κατηγοριών, αφορούν δεδομένα σχετικά με την υγεία (π.χ. εξετάσεις υγείας, καταγραφή συμπτωμάτων). Αυτά μπορούν να συλλέγονται μέσω ερωτηματολογίων, ιατρικών ελέγχων και θερμικών καμερών, ενώ μπορεί να αφορούν εργαζόμενους, συνεργάτες, πολίτες καθώς και επισκέπτες, προμηθευτές ή / και εκπροσώπους πελατών. Η συμμόρφωση στη Δημόσια Διοίκηση με την νομοθεσία προστασίας προσωπικών δεδομένων κατά τη λήψη μέτρων είναι υποχρεωτική (άρθρο 1 παρ. 3 της ΠΝΠ της 25/02/2020). Αντίστοιχα, τα μέτρα που λαμβάνονται στον Ιδιωτικό τομέα, απαιτείται να εναρμονίζονται πλήρως με τον ΓΚΠΔ και τον Ν. 4624/2019.

Πιο συγκεκριμένα, για λόγους δημοσίου συμφέροντος και της έννομης υποχρεώσεως για μεταβίβαση ατομικών δεδομένων στο πλαίσιο της προσπάθειας καταπολέμησης του Covid-19, εκδόθηκε η *Πράξη Νομοθετικού Περιεχομένου (ΠΝΠ)* με τίτλο "*Κατεπείγοντα μέτρα αντιμετώπισης της ανάγκης περιορισμού της διασποράς του κορωνοϊού COVID-19*"[11]. Η ΠΝΠ εκδόθηκε σύμφωνα με το Ελληνικό Σύνταγμα και το άρθρο 44 παρ. 1 (έκτακτες & επείγουσες περιστάσεις). Επιπρόσθετα, στο άρθρο 5 παρ. 1 της ΠΝΠ αναφέρεται ρητά ότι ο *Εθνικός Οργανισμός Δημόσιας Υγείας (ΕΟΔΥ*), παρέχει προς τη *Γενική Γραμματεία Πολιτικής Προστασίας (ΓΓΠΠ*), δεδομένα ατομικού χαρακτήρα επιδημιολογικού συσχετισμού.

Υπό το πρίσμα του ΓΚΠΔ, της ΑΠΔΠΧ, των μέτρων που λαμβάνουν έναντι της πανδημίας και της αρχής της λογοδοσίας και της υποχρέωσης "*Προστασίας Δεδομένων από τον Σχεδιασμό και εξ Ορισμού"*, οι εργοδότες πρέπει να [12]:

- να ζητείται γνώμη του Υπευθύνου Προστασίας Δεδομένων (DPO) ήδη από τον σχεδιασμό των μέτρων, εφόσον υπάρχει κάτι τέτοιος,
- να σχεδιάζονται τα απαραίτητα μέτρα σύμφωνα με την Προστασία των Δεδομένων ήδη από τον "*Σχεδιασμό και εξ Ορισμού*",
- να προσφέρεται η απαιτούμενη ενημέρωση στα υποκείμενα των δεδομένων (εργαζόμενους) σχετικά με κάθε επιδιωκόμενη επεξεργασία,
- να υπάρχει σεβασμός των δικαιωμάτων των εργαζομένων καθ' όλη την διάρκεια των πράξεων επεξεργασίας,
- να εφαρμόζονται σχετικές Εταιρικές Πολιτικές και Διαδικασίες (π.χ. Πολιτική για την υγεία στο χώρο εργασίας κατά την διάρκεια της πανδημίας κ.α.),

[11] ΦΕΚ Α 64/14.3.2019.

[12] https://www.ey.com/el_gr/tax/tax-alerts/greece-covid-19-how-should-greek-companies-respond-in-compliance-with-the-gdpr [πρόσβαση 12/11/2020].

- να διατηρείται τεκμηρίωση σχετικά με τις νομικές βάσεις των σχεδιαζόμενων μέτρων προστασίας, συμπεριλαμβανομένων των σχετικών ασκήσεων στάθμισης,
- να εκπονείται *Εκτίμηση Αντικτύπου για την Προστασία Δεδομένων*, και
- να διατηρούνται κατάλληλα μέτρα για την ασφάλεια και την εμπιστευτικότητα των ατομικών δεδομένων.

ΜΕΡΟΣ ΔΕΥΤΕΡΟ:

ΤΑ ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ ΚΑΙ Η ΠΡΟΣΤΑΣΙΑ ΤΟΥΣ ΣΤΟΝ ΔΗΜΟΣΙΟ ΤΟΜΕΑ

Κεφάλαιο Τέταρτο

Προστασία και Επεξεργασία Προσωπικών Δεδομένων στο Δημόσιο Τομέα

Στο κεφάλαιο αυτό γίνεται παρουσίαση του πλαισίου προστασίας και αξιοποίησης των προσωπικών δεδομένων στην Δημόσια Διοίκηση (ΔΔ) σε σχέση με τον ΓΚΠΔ, οι καινοτομίες που εισάγονται αλλά και ο ρόλος του υπεύθυνου επεξεργασίας δεδομένων στο δημόσιο τομέα.

4.1 Καινοτομίες στη Δημόσια Διοίκηση και ΓΚΠΔ

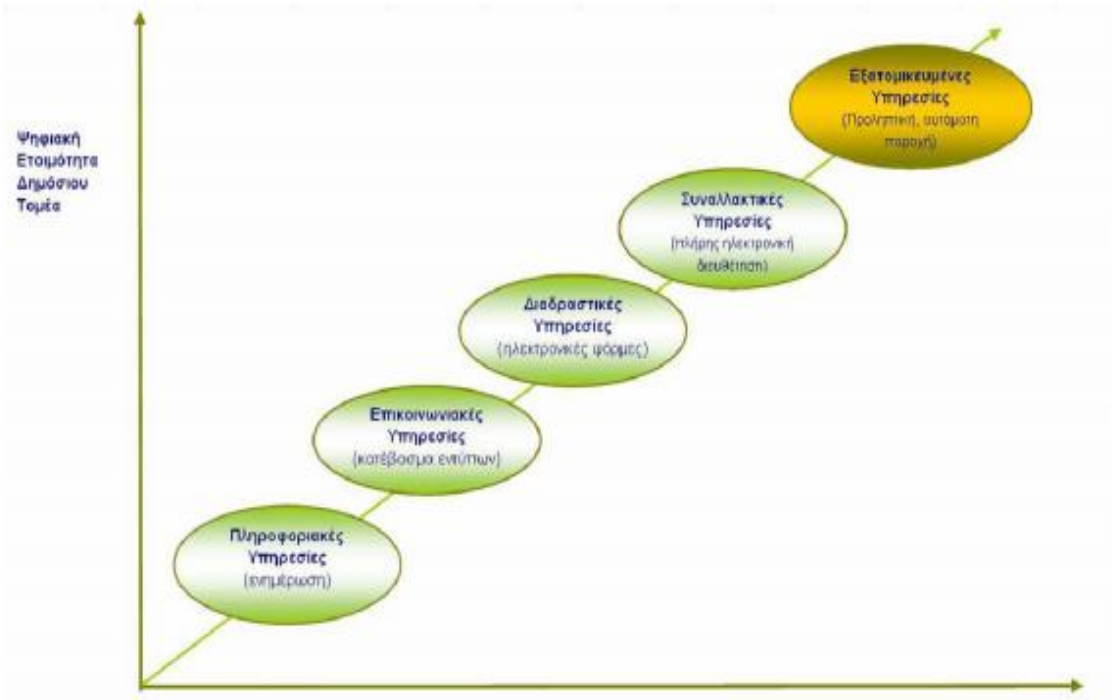
Ο ΓΚΠΔ στοχεύει στην προστασία των ατόμων και ειδικότερα των θεμελιωδών δικαιωμάτων και ελευθεριών τους, έναντι της επεξεργασίας δεδομένων ατομικού χαρακτήρα και της ελεύθερης κυκλοφορίας αυτών (Κουκιάδης, 2019, Κυριαζόγλου, 2019).

Η Δημόσια Διοίκηση και οι τομείς της έχουν ιδιαίτερο ενδιαφέρον σχετικά με τον ΓΚΠΔ, όσον αφορά τα ατομικά δεδομένα. Οι νέες τεχνολογίες οδήγησαν στην έκρηξη των δεδομένων και στην εμφάνιση νέων γνωστικών αντικειμένων όπως "*υπολογιστικό νέφος (clouding*)", "*μεγάλος όγκος δεδομένων (big data*) ή "*διαδίκτυο των πραγμάτων (Internet of Things, IoT*)", τα οποία αναμένεται να έχουν ευρεία εφαρμογή στο Δημόσιο τομέα και ιδιαίτερα στο χώρο της παροχή υπηρεσιών ηλεκτρονικής διακυβέρνησης (Δουκίδης, 2019).

Ο όρος "*ηλεκτρονική διακυβέρνηση (e-governance)*" δεν είναι μια απλή εφαρμογή της πληροφορικής και των επικοινωνιών (ΤΠΕ) στη δημόσια διοίκηση. Είναι ένας διακλαδικός τομέας που διαπλέκονται αρκετοί διαφορετικοί κλάδοι. Επίσης συνυπάρχουν πολλαπλά πεδία πολιτικών, τα οποία πρέπει να αντιμετωπιστούν όπως η προστασία προσωπικών δεδομένων (Διαγρ.15)(Seifert and Petersen, 2002, Pardo, 2000, Garson, 2004).

Διάγραμμα 15. Το πλαίσιο της ηλεκτρονικής διακυβέρνησης

Ο όγκος των πληροφοριών που οι φορείς της Δημόσιας Διοίκησης δημιουργούν, ενημερώνουν και διαχειρίζονται καθημερινά, είναι πλέον τεράστιος. Τα πελατο-κεντρικά προγράμματα ηλεκτρονικής διακυβέρνησης εστιάζουν στην ουσιώδη φύση της πληροφορίας και στην ευκολία ανταλλαγής της, ενώ ταυτόχρονα προσπαθούν να ισορροπήσουν τη συχνά σύντομη ζωή της πληροφορίας (Διαγρ.16)(Δουκίδης, 2019).



Διάγραμμα 16. Επίπεδα υπηρεσιών της ηλεκτρονικής διακυβέρνησης

Ο βασικός σκοπός όλων των προγραμμάτων υιοθέτησης της ηλεκτρονικής διακυβέρνησης είναι η παροχή στους πολίτες ενός αποτελεσματικού εργαλείου, με το οποίο να "*επικοινωνούν* / αλληλεπιδρούν" με τη δημόσια διοίκηση. Αυτό οφείλεται στη βελτιστοποίηση της ροής των πληροφοριών, και με την παροχή ασφάλειας στην συναλλαγή (Δουκίδης, 2019, Σιουγλέ, 2018).

Τέλος, οι πληροφορίες αποτελούν το μεγαλύτερο περιουσιακό στοιχείο για το Κράτος, και αυτό για το οποίο πάντα τίθενται τα μεγαλύτερα ζητήματα σχετικά με την ελευθερία πρόσβασης σε αυτές. Παρόλα αυτά, η απρόσκοπτη αναζήτηση και πρόσβαση κυβερνητικών πληροφοριών είναι ο βασικός πυρήνας της ηλεκτρονικής δημοκρατίας και διακυβέρνησης (Διαγρ.17). Στην Ελλάδα το θεσμικό πλαίσιο πριν τον ΓΚΠΔ, έχει προνοήσει για αυτά τα θέματα με το Ν. 3448/2006, το Ν. 3861/2010 και τον Κανονισμό Επικοινωνίας Δημοσίων Υπηρεσιών (ΚΕΔΥ) του 2003 (Λαζακίδου, 2019).

Διάγραμμα 17. Συνιστώσες ηλεκτρονικής διακυβέρνησης

4.2 Προσωπικά Δεδομένα και Δημόσια Διοίκηση

Η Δημόσια Διοίκηση υπόκειται στους κανόνες του νέου κανονισμού όταν επεξεργάζεται δεδομένα προσωπικού χαρακτήρα που συνδέονται με φυσικά πρόσωπα (πολίτες ή εργαζόμενοι). Οι εθνικές αρχές είναι υπεύθυνες για την υποστήριξη των περιφερειακών και τοπικών αρχών κατά την προετοιμασία τους για την εφαρμογή του ΓΚΠΔ. Η πλειοψηφία των δεδομένων προσωπικού χαρακτήρα που τηρούνται στης δημόσιες υπηρεσίες, τίθενται σε επεξεργασία με συνήθως μια νομική υποχρέωση ως βάση, εφόσον εξυπηρετείται το δημόσιο συμφέρον ή άσκηση δημόσιας εξουσίας. Κατά την επεξεργασία κάθε δημόσια υπηρεσία οφείλει να τηρεί ορισμένες βασικές αρχές για τα προσωπικά δεδομένα (άρθρο 5, ΓΚΠΔ) , όπως (Κυριαζόγλου, 2019):

- να υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων.
- συλλογή για καθορισμένους, ρητούς και νόμιμους σκοπούς (ακολουθώντας τον εκάστοτε υπαλληλικό κώδικα όσο αφορά το προσωπικό μητρώο του υπαλλήλου) και δεν υποβάλλονται σε επιπλέον επεξεργασία κατά τρόπο ασύμβατο προς αυτούς. Ειδικότερα, το ατομικό μητρώο του δημοσίου υπαλλήλου είναι ο υπηρεσιακός φάκελος με όλα εκείνα τα στοιχεία που προσδιορίζουν την ατομική, οικογενειακή, περιουσιακή και υπηρεσιακή κατάσταση του, και τηρείται από την υπηρεσία στην

οποία υπηρετεί. Το ατομικό μητρώο έχει ιδιαίτερη σημασία για κάθε δημόσιο υπάλληλο, αφού τον συνοδεύει σε όλη τη εργασιακή ζωή του και μετά τη λήξη της για αρκετό χρονικό διάστημα, καθώς τηρείται μέχρι το τέλος της ζωής του, ή μέχρι 10 έτη από την καθ΄ οιονδήποτε τρόπο απομάκρυνση του από την υπηρεσία[13]. Ωστόσο, αν αφορά αρχειοθέτηση ή επιστημονική έρευνα, δεν θεωρείται στο Δημόσιο ασύμβατο.

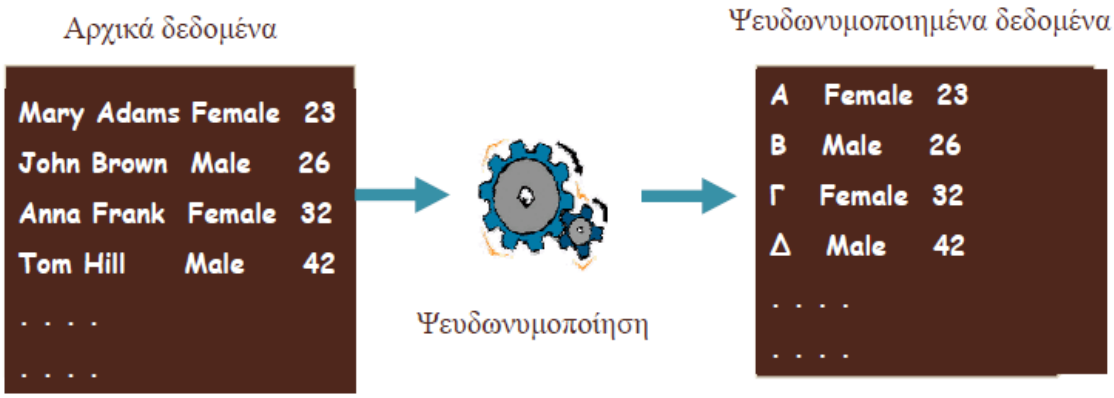
- είναι κατάλληλα, συναφή και περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία.
- είναι ακριβή και όταν κρίνεται αναγκαίο, επικαιροποιούνται, ενώ θα πρέπει να λαμβάνονται όλα εκείνα τα μέτρα για την άμεση διαγραφή ή διόρθωση τους αν είναι ανακριβή.
- να διατηρούνται σε μορφή που παρέχει την δυνατότητα ταυτοποίησης των υποκείμενων των δεδομένων μόνο για το χρονικό διάστημα που απαιτείται από τους σκοπούς της επεξεργασίας των δεδομένων. Τα προσωπικά δεδομένα μπορούν να αποθηκεύονται για μεγάλα διαστήματα για λόγους αρχειοθέτησης, δημόσιου συμφέροντος ή στατιστικούς λόγους (άρθρο 89, παρ.1). Πρέπει όμως να λαμβάνονται όλα εκείνα τα τεχνικά και οργανωτικά μέτρα για την προάσπιση των δικαιωμάτων και ελευθεριών του υποκείμενου των δεδομένων (περιορισμός της περιόδου αποθήκευσης).
- να υποβάλλονται σε επεξεργασία έτσι ώστε να υπάρχει εγγύηση για την ασφάλεια τους από παράνομη χρήση ή μη εξουσιοδοτημένη πρόσβαση (ακεραιότητα, εμπιστευτικότητα).

Για παράδειγμα, στην χρήση πληροφοριακών συστημάτων στο δημόσιο τομέα (π.χ. www.data.gov.gr) θα πρέπει (Κουκιάδης, 2019, Κυριαζόγλου, 2019, Δουκίδης, 2019):

- Αρχικά πρέπει να γίνεται προσπάθεια για *ψευδωνυμοποίηση (*δεν αποτελεί ανωνυμοποίηση)(Διαγρ.18). Στον ΓΚΠΔ η *ψευδωνυμοποίηση* ορίζεται ρητά ως: "*η επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο ώστε τα δεδομένα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρωματικές πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα*

[13] Η ΑΠΔΠΧ στην Οδηγία 115/2001 περιγράφει ότι η λύση της εργασιακής σχέση δεν συνεπάγεται και αποδέσμευση από τους κανόνες και θεμιτής επεξεργασίας των προσωπικών δεδομένων (Οδηγία 115/2011, Β' Αντικείμενο - πεδίο εφαρμογής, σ.6).

προκειμένου να διασφαλιστεί ότι δεν μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο.



Διάγραμμα 18. Διαδικασία ψευδωνυμοποίησης

- Εάν δεν έχει γίνει ή δεν ενδείκνυται, θα πρέπει να αναζητείται *συγκατάθεση* για τη συγκεκριμένη χρήση. Ο υπαλληλικός κώδικας δίνει τη δυνατότητα στον υπάλληλο να εκφράζει τη διαφωνία του για δεδομένα που αναφέρονται αποκλειστικά για την ιδιωτική ζωή του και δεν σχετίζονται με την υπηρεσιακή του κατάσταση ή για περιεχόμενο των καταχωρημένων δεδομένων, όταν είναι ανακριβή[14].
- Εάν δεν υπάρχει συγκατάθεση, τότε πρέπει να εξετάζεται η περίπτωση του *εννόμου συμφέροντος (το έννομο συμφέρον δεν εφαρμόζεται στην επεξεργασία που διενεργείται από δημόσιες αρχές κατά την άσκηση των καθηκόντων τους*).
- Θα πρέπει να απαντηθεί τότε το ερώτημα: *Η διάθεση για περαιτέρω χρήση είναι άσκηση καθήκοντος;*
- Ενημέρωση του υποκειμένου, δικαιώματα και πρόβλεψη διεπαφών (interface) για την άσκησή τους (οι ιστοσελίδες της ηλεκτρονικής διακυβέρνησης θα πρέπει να παρέχουν ακριβή και αξιόπιστη σχετική πληροφόρηση).

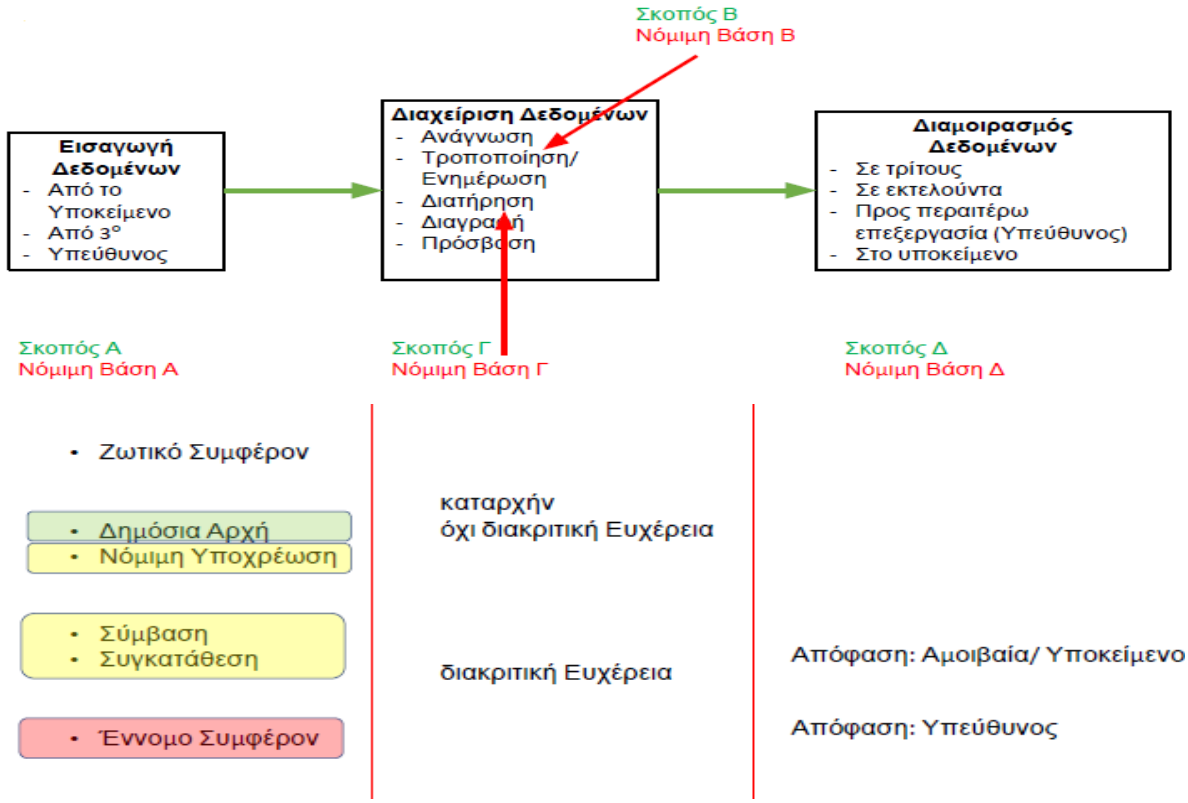
Άλλο ένα παράδειγμα, αφορά τον *σκοπό και τη νόμιμη βάση* για την επεξεργασία δεδομένων προσωπικού χαρακτήρα (Σπηλιοπούλου, 2019). Ειδικότερα, θα πρέπει (Διαγρ.19):

- να προσδιορίζεται η χρήση στον κύκλο ζωής των δεδομένων.
- να εξετάζεται εάν καλύπτει η νόμιμη βάση σε κάθε στάδιο αυτών:
    - εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον;
    - συγκατάθεση;

[14] Ν. 2683/99 (ΥΚ), άρθρο 23, παρ.2, Γνωμοδότηση υπ' αριθμ. 326/2005 του ΝΣΚ , όπου ο υπάλληλος αποκλειστικά έχει το δικαίωμα να λάβει γνώση των στοιχείων του προσωπικού του μητρώου, ενώ αποκλείεται η γνώση και πρόσβαση οποιουδήποτε τρίτου στο περιεχόμενο των στοιχείων αυτών.

- έννομο συμφέρον;
- σκοποί αρχειοθέτησης, επιστημονικής ή ιστορικής έρευνας ή στατιστικοί σκοποί;

- να καταγράφεται ο σκοπός και η νόμιμη βάση.



Διάγραμμα 19. Παράδειγμα Σκοπού και Νόμιμης Βάσης

Όσον αφορά τα μέτρα για την προστασία και ασφάλεια των ατομικών δεδομένων, θα πρέπει να ισχύουν τα εξής (Σπηλιοπούλου, 2019):

- "*ακεραιότητα*" & "*εμπιστευτικότητα*": υποβάλλονται σε επεξεργασία κατά́ τρόπο που εγγυάται την απόλυτη ασφάλεια των δεδομένων, μεταξύ́ άλλων την προστασία τους από́ μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή́ ή φθορά́. Μια τέτοια επεξεργασία ασφάλειας είναι η κρυπτογράφηση. Πιο συγκεκριμένα, τα δεδομένα μετασχηματίζονται σε ακατάληπτη μορφή με βάση κάποιον εξειδικευμένο (κρυπτογραφικό) αλγόριθμο αλλά και με τη χρήση ενός μυστικού κλειδιού (key/cipher). Μόνο αν κάποιο άτομο γνωρίζει το μυστικό κλειδί μπορεί να ανακτήσει τα αρχικά δεδομένα από τα κρυπτογραφημένα. Επομένως, είναι αντιστρεπτή η διαδικασία (αποκρυπτογράφηση), αλλά μόνο από εξουσιοδοτημένους χρήστες, που είναι γνώστες του κλειδιού αποκρυπτογράφησης. Οι αλγόριθμοι κρυπτογράφησης θεωρούνται ασφαλείς, ως πρότυπα κρυπτογράφησης, αλλά πάντα υπάρχει ο κίνδυνος διάρρηξης τους (Διαγρ.20). Ο αντικειμενικός στόχος της

κρυπτογραφίας είναι η ασφαλής παροχή επικοινωνίας και ανταλλαγής μηνυμάτων σε δύο άτομα. Αυτή η ικανότητα της κρυπτογραφίας είναι σύμφωνη με το πνεύμα του ΓΚΠΔ, αλλά και χρήσιμη στα συστήματα ηλεκτρονικής διακυβέρνησης. Ένα τυπικό κρυπτογραφικό σύστημα (διαδικασίες κρυπτογράφησης - αποκρυπτογράφησης) αποτελείται από μία πεντάδα απαραίτητων για την ασφαλή επικοινωνία ή μετατροπή των δεδομένων, παραμέτρων/χαρακτηριστικών (P,C,k,E,D)(Διαγρ.21) (Kahn, 1996, Κάτος και Στεφανίδης, 2003):

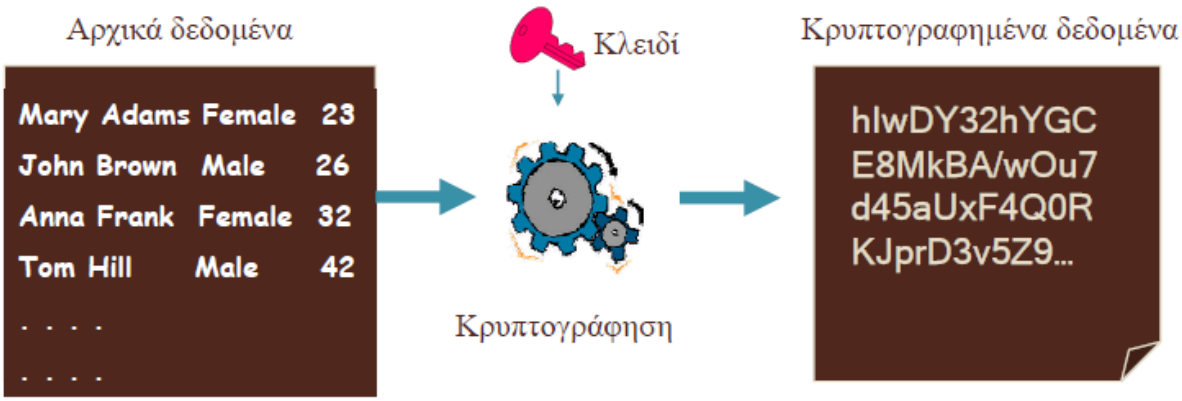
I. Το P είναι ο χώρος όλων των δυνατών μηνυμάτων ή ανοικτών κειμένων.

II. Το C είναι ο χώρος όλων των δυνατών κρυπτογραφημένων μηνυμάτων ή δεδομένων προς κρυπτογράφηση.

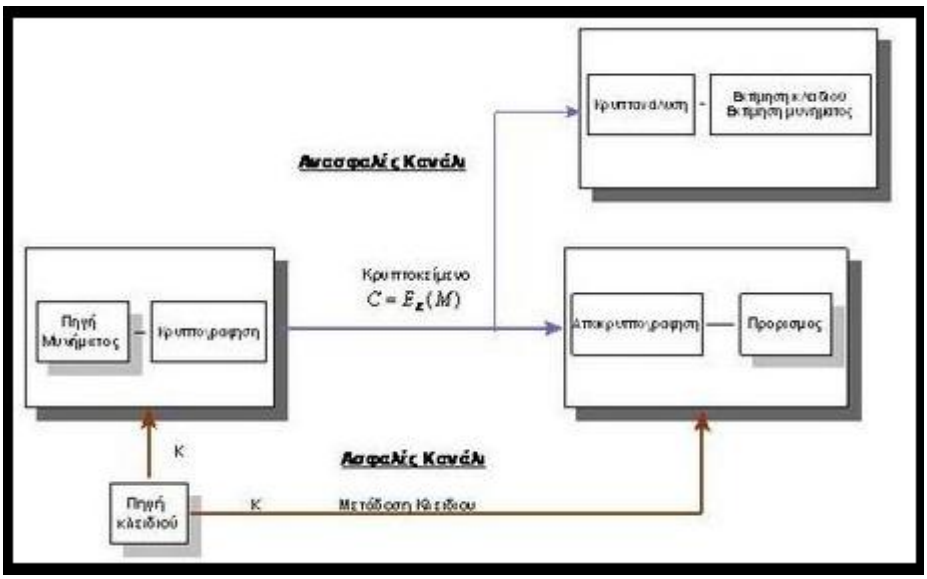
III. Το k είναι ο χώρος όλων των δυνατών κλειδιών (κλειδοχώρος)

IV. Η E είναι ο κρυπτογραφικός μετασχηματισμός (κρυπτογραφική συνάρτηση).

V. Η D είναι η αντίστροφη συνάρτηση (μετασχηματισμός αποκρυπτογράφησης).



Διάγραμμα 20. Διαδικασία ψευδωνυμοποίησης



Διάγραμμα 21. Τυπικό Κρυπτογραφικό Σύστημα

- να καταγράφονται οι Πολιτικές Ασφάλειας.
- υα υπάρχει Data Management Plan, όπου απαιτείται.
- αξιοποίηση Μηχανισμών Παρακολούθησης (DPO/ Επιτροπή Ηθικής και Δεοντολογίας).
- χρήση Συστημάτων ενημέρωσης υποκειμένου.
- εύχρηστοι τρόποι για την άσκηση των δικαιωμάτων εκ μέρους του υποκειμένου.

Επιπλέον, προτείνεται η χρήση ανοικτών τεχνολογιών για την προστασία ατομικών δεδομένων στο δημόσιο τομέα (Σπηλιοπούλου, 2019):

- Λογισμικά Προστασίας Διαρροής Δεδομένων (π.χ. Open DLP).
- Κρυπτογράφησης Δεδομένων για να είναι προσβάσιμα μόνο από εξουσιοδοτημένα άτομα που διαθέτουν ένα κωδικό πρόσβασης (πχ.. TrueCrypt).
- Κρυπτογράφηση των μηνυμάτων email για προστασία από μη εξουσιοδοτημένη χρήση (π.χ. GnuPG).
- Λογισμικό που χρησιμοποιούνται για την πρόληψη, ανίχνευση και κατάργηση κακόβουλου λογισμικού (π.χ. ClamAV).
- Αναγνώριση περιστατικών παραβίασης ευαίσθητων και εμπιστευτικών δεδομένων (π.χ. Snort).
- Ασφαλείς Επικοινωνίες μέσω Δικτύων (π.χ. OpenSSH).

Τέλος, όσο αφορά την δυνατότητα τα προσωπικά δεδομένα να είναι ανοικτά στη Δημόσια Διοίκηση, σύμφωνα με τον ΓΚΠΔ και την σχετική τεχνολογία, μπορεί υπό τα εξής κριτήρια (Σπηλιοπούλου, 2019, Κυριαζόγλου, 2019):

- ακολουθώντας το ΓΚΠΔ (GDPR): "*Αναζητούμε τρόπους που επιτρέπουν την ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα διασφαλίζοντας παράλληλα υψηλό επίπεδο προστασίας των δεδομένων προσωπικού χαρακτήρα*".
- *Στη Δημόσια Διοίκηση,* προτεραιότητα το κανονιστικό πλαίσιο (νόμοι, προεδρικά διατάγματα, ΥΑ, ΠΥΣ. κοκ.).
- Ερμηνευτικοί εγκύκλιοι είναι απαραίτητοι.
- Πρωτοβουλίες της ίδιας της Διοίκησης για πραγματική προστασία και αξιοποίηση των προσωπικών δεδομένων με τη βοήθεια του DPO (δημιουργία βέλτιστων πρακτικών, forum DPO δημόσιας διοίκησης).

4.3 Ο Υπεύθυνος Επεξεργασίας Προσωπικών Δεδομένων

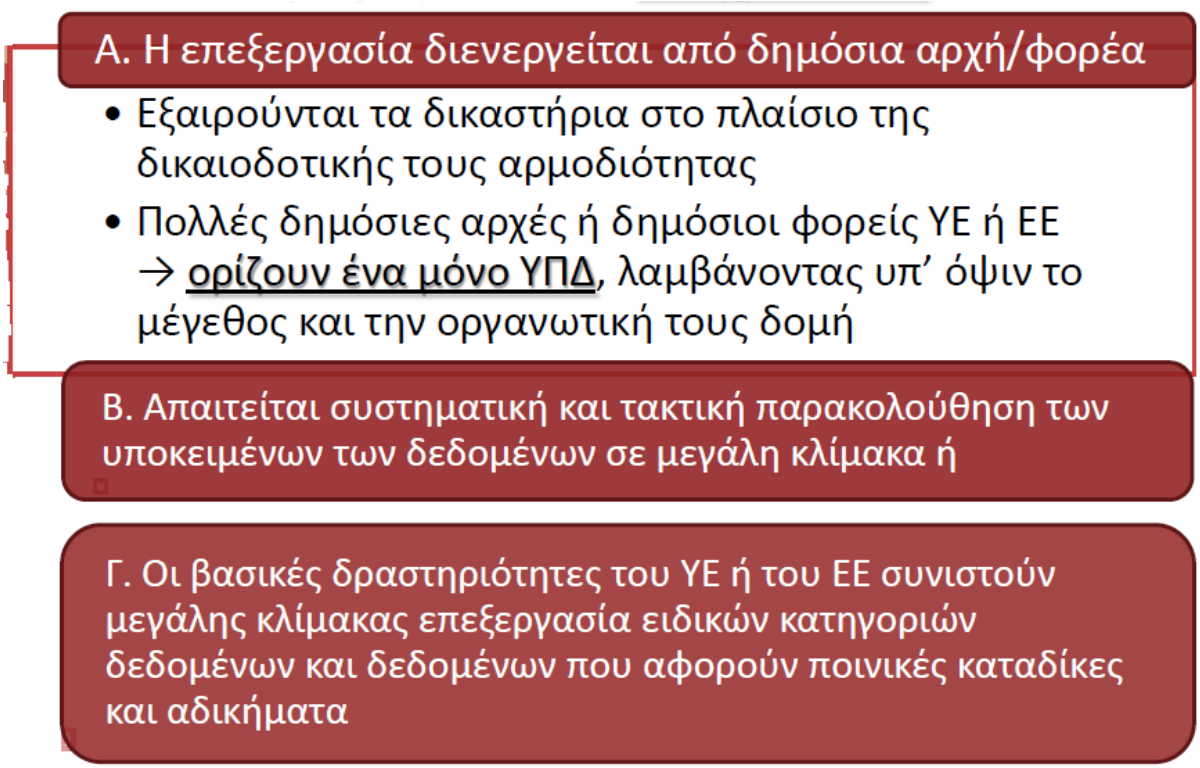
Ο ΓΚΠΔ και ο νόμος 4624/2019, θέτει μια σημαντική καινοτομία με την υποχρεωτικότητα του Υπευθύνου Προστασίας Δεδομένων (ΥΠΔ)(άρθρα 37-39). Συγκεκριμένα: "*Ο ΥΠΔ διευκολύνει τη συμμόρφωση του υπευθύνου επεξεργασίας και του εκτελούντος την επεξεργασία με τις διατάξεις του ΓΚΠΔ και μεσολαβεί μεταξύ των διαφόρων ενδιαφερομένων (π.χ. εποπτικές αρχές, υποκείμενα των δεδομένων)*"[15]. Ο ρόλος του είναι συμβουλευτικός, ενώ δεν φέρει ευθύνη για τη μη συμμόρφωση με τον Κανονισμό, αφού οι αποφάσεις λαμβάνονται πάντα από τη Διοίκηση, στην οποία λογοδοτεί απευθείας (Κουκιάδης, 2019, Κυριαζόγλου, 2019, Ιγγλεζάκη, 2018α).

Ο θεσμός αυτός είχε υιοθετηθεί στην πράξη και πριν τον ΓΚΠΔ, αλλά με αυτό τον κανονισμό έγινε υποχρεωτικός. Ειδικότερα, προβλεπόταν στην Οδηγία 95/46/ΕΚ ως προαιρετικό μέτρο (παρ. 2 του άρθρου 18), για να θεσπιστεί στο εσωτερικό δίκαιο των κρατών-μελών. Όμως υπάρχει υποχρεωτικός ορισμός ΥΠΔ βάση της προηγούμενης οδηγίας σε κράτη της ΕΕ όπως η Γερμανία, η Ισπανία, η Σλοβακία. Συγκεκριμένα, στη Γερμανία το 2003 με νομοθετική παρέμβαση, προβλέπεται γενική υποχρέωση διορισμού ΥΠΔ στη Δημόσια Διοίκηση, ενώ στον ιδιωτικό τομέα γίνεται ο διαχωρισμός με βάση κάποια κριτήρια (Ιγγλεζάκη, 2018α, 2018β, Βαρβέρης, 2017, Λεμπέση, 2018α, Λεμπέση, 2018β):

- δυνατότητα αυτοματοποιημένης επεξεργασίας προσωπικών δεδομένων & προσωπικό άνω των εννέα ατόμων.
- μη αυτοματοποιημένη επεξεργασία δεδομένων, & προσωπικό άνω των εννέα ατόμων.

Στην Ελλάδα ο σχετικός νόμος (Ν.2472/1997) δεν προέβλεπε το θεσμό, και για αυτό είναι πρωτόγνωρος για την ελληνική δημόσια διοίκηση και προβλέπεται ότι θα προκαλέσει σημαντικές αλλαγές. Ο θεσμός του είναι ανεξάρτητος, ενώ συνεργάζεται με την εποπτική αρχή και αποτελεί κόμβο επικοινωνίας της με τα υποκείμενα των δεδομένων για θέματα επεξεργασίας ατομικών δεδομένων (άρθρο 39)(Διαγρ.22)(Βαρβέρης, 2017, Ιγγλεζάκη, 2018α, Κυριαζόγλου, 2019, Μυλώση, 2018, Λεμπέση, 2018β, Σωτηρόπουλος, 2017).

[15] www.dpa.gr.



Διάγραμμα 22. Ορισμός ΥΠΔ

Κεφάλαιο Πέμπτο

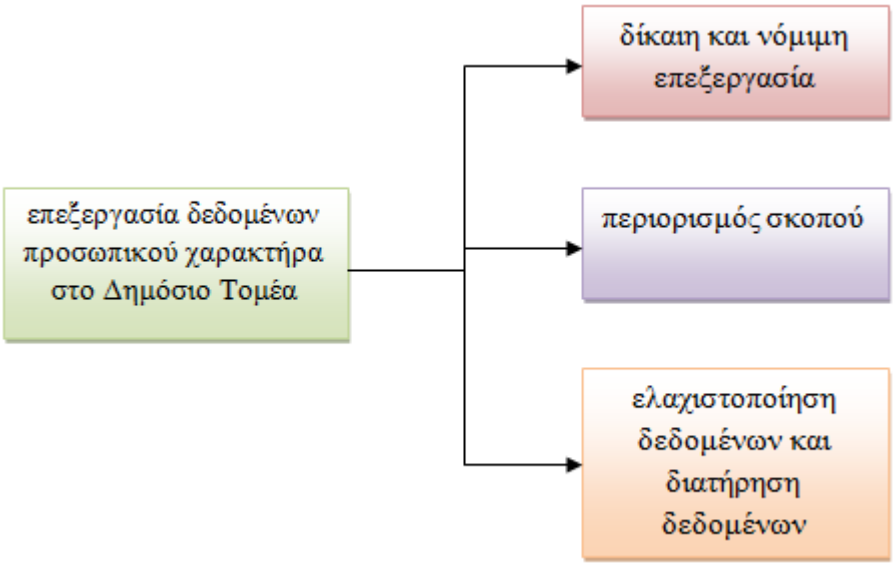
Εφαρμογή του ΓΚΠΔ στο Δημόσιο Τομέα και στο Προσωπικό του

Στο κεφάλαιο αυτό παρουσιάζεται η διαδικασία υιοθέτησης του ΓΚΠΔ το δημόσιο τομέα και στο προσωπικό του, με εστίαση στην Ελληνική Δημόσια Διοίκηση και η Αρχή Προστασίας Προσωπικών Δεδομένων.

5.1 Υιοθέτηση του ΓΚΠΔ στη Δημόσια Διοίκηση

Ο δημόσιος τομέας αποτελεί ένα από τα δύο πεδία εφαρμογής του ΓΚΠΔ. Ως "*δημόσιος φορέας*" ορίζεται ως εξής (Ν. 4624, άρθρο 4 - ορισμοί): "*οι δημόσιες αρχές, οι ανεξάρτητες και ρυθμιστικές διοικητικές αρχές, τα νομικά πρόσωπα δημοσίου δικαίου, οι οργανισμοί τοπικής αυτοδιοίκησης πρώτου και δεύτερου βαθμού και τα νομικά πρόσωπα και οι επιχειρήσεις αυτών, οι κρατικές ή δημόσιες επιχειρήσεις και οργανισμοί, τα νομικά πρόσωπα ιδιωτικού δικαίου που ανήκουν στο κράτος ή επιχορηγούνται κατά 50% τουλάχιστον του ετήσιου προϋπολογισμού τους ή η διοίκησή τους ορίζεται από αυτό*".

Η κάθε Δημόσια Διοίκηση οφείλει να προσαρμοστεί στα νέα δεδομένα του ΓΚΠΔ. Ο νέος κανονισμός δεν αλλάζει κάποια σημεία της προηγούμενης νομοθεσίας, αλλά αντιμετωπίζει με διαφορετική φιλοσοφία το αντικείμενο των προσωπικών δεδομένων, σε σχέση με την κρατική παρέμβαση λόγω δημοσίου συμφέροντος. Κάθε δημόσια διοίκηση πρέπει να ακολουθεί τους κανόνες του ΓΚΠΔ όταν επεξεργάζεται δεδομένα προσωπικού χαρακτήρα που αφορούν ένα φυσικό πρόσωπο (Διαγρ.23) [16] (Δελλής, 2017, Μυλώση, 2018, Δουκίδης, 2019).



Διάγραμμα 23. Βασικές Αρχές που διέπουν την Δημόσια Διοίκηση

[16] https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations_el

5.2 ΓΚΠΔ και Αιτήματα των Πολιτών προς τη Δημόσια Διοίκηση

Τα φυσικά πρόσωπα μπορούν να επικοινωνήσουν με κάθε δημόσια αρχή για να ασκήσουν τα δικαιώματά τους βάσει του ΓΚΠΔ, ήτοι (Κουκιάδης, 2019, Κυριαζόγλου, 2019, Ιγγλεζάκη, 2018α):

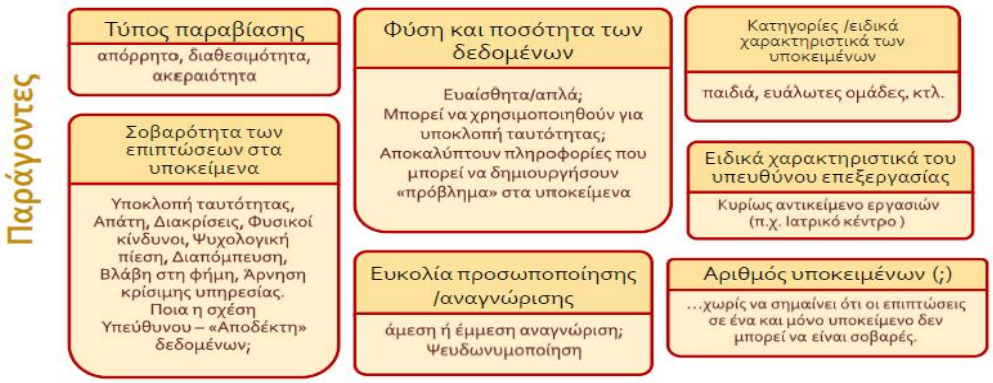
- δικαιώματα πρόσβασης
- διόρθωση
- διαγραφή (δικαίωμα στη λήθη)
- περιορισμό
- αντίταξης
- μη υπαγωγής σε αυτοματοποιημένη λήψη αποφάσεων

Επίσης, υπάρχει το δικαίωμα εναντίωσης από πλευράς των φυσικών προσώπων στην επεξεργασία προσωπικών δεδομένων από την δημόσια διοίκηση για λόγους δημόσιου συμφέροντος. Επιπλέον, οι πολίτες έχουν την δυνατότητα διεκδίκησης αποζημίωσης εφόσον υπάρχει δημόσιος φορέας που έχει παραβιάσει τον ΓΚΠΔ, με συνέπεια να υποστούν υλική ζημία, ενώ η αξίωση αποζημίωσης γεννιέται άμεσα σε βάρος του άμεσα στον υπαίτιο δημόσιο φορέα ή με δικαστική προσφυγή στα αρμόδια εθνικά δικαστήρια του κράτους μέλους της ΕΕ (Κυριαζόγλου, 2019).

5.3 Βήματα Προετοιμασίας Εφαρμογής του ΓΚΠΔ στο Δημόσιο

Οι μεθοδολογίες προετοιμασίας για την υιοθέτηση του ΓΚΠΔ μπορούν να συνοψιστούν στα εξής βήματα (Κυριαζόγλου, 2019, Ιγγλεζάκη, 2018α):

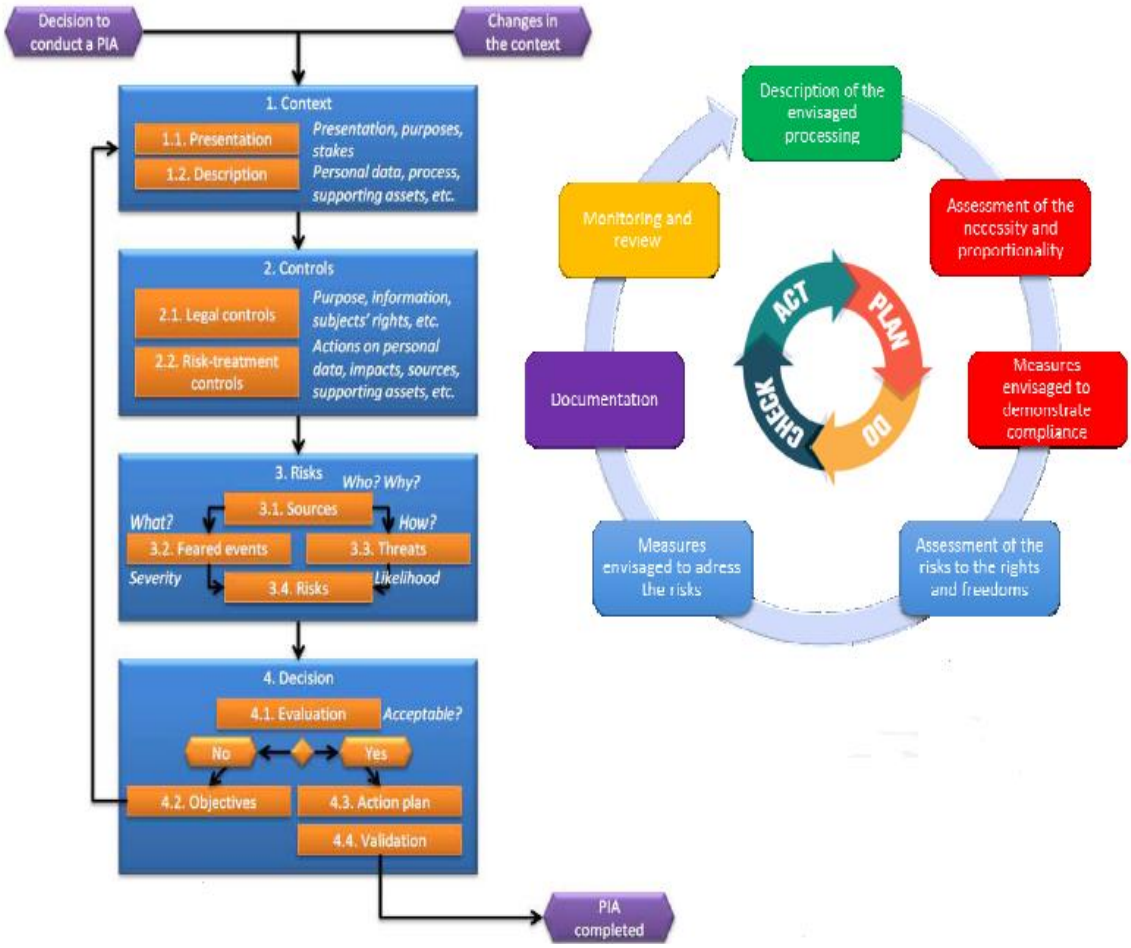
- *Διορισμός ενός Υπευθύνου Προστασίας Δεδομένων ("DPO")*.
- *Αναγνώριση, κατάταξη και χαρτογράφηση δεδομένων*.
- *Κατάταξη και προτεραιότητα στις ενέργειες συμμόρφωσης*.
- *Διαχείριση κινδύνων* (Διαγρ.24).



Διάγραμμα 24. Αξιολόγηση Κινδύνου - Παράγοντες

Η Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων (Έκθεση DPIA) (Διαγρ.25) αφορά:

- συστηματική περιγραφή των προβλεπόμενων πράξεων επεξεργασίας, των σκοπών της επεξεργασίας και της νομικής βάσης.
- εκτίμηση αναγκαιότητας και αναλογικότητας των πράξεων επεξεργασίας.
- εκτίμηση κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων (πολιτών ή εργαζόμενων).
- προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων.



Διάγραμμα 25. Διαδικασία DPIA

Μία έκθεση DPIA ουσιαστικά μπορεί να διασφαλίσει την αρχή "*data protection by design*" (Διαγρ.26). Επίσης, αναμένεται να καταδείξει τις τεχνολογικές λύσεις που απαιτούνται για την ασφάλεια της επεξεργασίας. Η αποτίμηση κινδύνων και οι τρόποι αντιμετώπισής τους, που πραγματοποιούνται στο πλαίσιο της έκθεσης, διευκολύνουν την αξιολόγηση των περιστατικών παραβίασης δεδομένων.

Διάγραμμα 26. Διασφάλιση της έκθεσης DPIA της αρχής " *data protection by design*"

Επιπρόσθετα, για λόγους ασφάλειας, η τήρηση και περαιτέρω επεξεργασία των δεδομένων, θα πρέπει να επιλεχθεί η διαδικασία της κρυπτογράφησης ή / και ψευδωνυμοποίηση. Επίσης, να καταγραφούν τα πρόσωπα που πρέπει να έχουν πρόσβαση. Επιπλέον, οι συνεργαζόμενες εταιρείες πρέπει να παρέχουν εγγυήσεις για τη συμμόρφωση με το ΓΚΠΔ. Ο έλεγχος ως προς το αν τηρούνται οι αρχές που διέπουν τη νόμιμη επεξεργασία των δεδομένων και αν γίνονται σεβαστά τα δικαιώματα των προσώπων (ΓΚΠΔ) πρέπει να είναι διαρκής.

Στο πλαίσιο του συντονισμού της ασφάλειας των δεδομένων στον τομέα του Δημοσίου τομέα στην Ελλάδα, όλοι οι δημόσιοι φορείς ορίζουν *Υπεύθυνο Ασφάλειας Πληροφοριών και Δικτύων,* που θα λειτουργεί ως σύνδεσμος με την αρμόδια Γενική Γραμματεία και θα είναι εκπρόσωπος του φορέα του. Επιπλέον, η Γενική Γραμματεία συμμετέχει στην ομάδα συμμόρφωσης του Εθνικού δικαίου με την οδηγία NIS (Network and Information Security), αλλά και στο cooperation group, όπου γίνεται ανταλλαγή βέλτιστων πρακτικών (best practices) μεταξύ των κρατών μελών της ΕΕ (Κουκιάδης, 2019, Κυριαζόγλου, 2019).

5.4 Ο Νόμος 4624/2019

Ο νόμος αυτός περιλαμβάνει αριθμό επιπλέον σημαντικών μέτρων που στοχεύουν στα εξής[17]:

- αντικατάσταση του υπάρχοντος κανονιστικού πλαισίου που αφορά την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.
- λήψη μέτρων εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου & Συμβουλίου της 27-4-2016.
- ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016.

Ειδικότερα, η νέα αυτή νομοθετική πρωτοβουλία περιλαμβάνει τα εξής:

- Οι δημόσιοι φορείς/οργανισμοί έχουν την δυνατότητα να προβούν σε επεξεργασία δεδομένων ατομικού χαρακτήρα, εφόσον η επεξεργασία κρίνεται απαραίτητη για το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας (άρθρο 5). Ο υπεύθυνος επεξεργασίας είναι υποχρεωμένος από την νομοθεσία να λαμβάνει τα μέτρα εκείνα που διασφαλίζουν τις αρχές που διέπουν την επεξεργασία των δεδομένων, σύμφωνα με το άρθρο 6 του ΓΚΠΔ.
- Το άρθρο 6, αφορά την περιγραφή του ορισμού του υπεύθυνου προστασίας δεδομένων σε δημόσιους φορείς. Πιο συγκεκριμένα[18]:
    - Υπεύθυνο Προστασίας Δεδομένων (ΥΠΔ) διαθέτει και ο δημόσιος τομέας, όπου μπορεί να είναι δημόσιος υπάλληλος, ή κάποιο άτομο με σύμβαση παροχής υπηρεσιών.
    - Η επιλογή του ΥΠΔ βασίζεται στα επαγγελματικά προσόντα του, με έμφαση στην εξειδίκευση σε θέματα δικαίου προστασίας των ατομικών δεδομένων.
    - Ο κάθε δημόσιος φορέας/οργανισμός είναι υποχρεωμένος να υποβάλει σε δημοσίευση, τα στοιχεία επικοινωνίας του ΥΠΔ και τα ανακοινώνει στην εποπτική Αρχή, εκτός και αν δεν επιτρέπεται για ειδικούς λόγους (π.χ. εθνικής ασφάλειας).
- Το άρθρο 7, αφορά τα εξής:

[17] ΑΑΔΕ, https://www.aade.gr/sites/default/files/2020-06/%CE%BD.%204624%202019%20%CE%95%CF%86%CE%B1%CF%81%CE%BC%CE%BF%CF%83%CF%84%CE%B9%CE%BA%CF%8C%CF%82%20%CE%93%CE%9A%CE%A0%CE%94%20%26%20%CE%B5%CE%BD%CF%83%CF%89%CE%BC%CE%AC%CF%84%CF%89%CF%83%CE%B7%20%CE%BF%CE%B4%CE%B7%CE%B3%CE%AF%CE%B1%CF%82%202016%20680.pdf.

[18] https://www.e-nomothesia.gr/kat-dedomena-prosopikou-kharaktera/nomos-4624-2019-phek-137a-29-8-2019.html [Πρόσβαση 2/11/2020].

- ο δημόσιος φορές/οργανισμός εξασφαλίζει ότι ο ΥΠΔ συμμετέχει σε όλα τα σχετικά ζητήματα που αφορούν την προστασία των ατομικών δεδομένων.
- ο δημόσιος φορές/οργανισμός υποστηρίζει το έργο του ΥΠΔ.
- ο δημόσιος φορές/οργανισμός εξασφαλίζει ότι ο ΥΠΔ δεν λαμβάνει εντολές κατά την εκτέλεση των καθηκόντων του αλλά αναφέρεται απευθείας στο ανώτατο ιεραρχικά προϊστάμενο όργανο του φορέα/οργανισμού και δεν θα υποστεί κυρώσεις ή απόλυση επειδή εκτέλεσε τα καθήκοντα του.
- Η καταγγελία της σύμβασης εργασίας ή η ανάκληση ανάθεσης καθηκόντων του ΥΠΔ, στην περίπτωση που είναι υπάλληλος του δημόσιου φορέα, επιτρέπεται αποκλειστικά σε σπουδαίες περιπτώσεις.
- Τα υποκείμενα των δεδομένων μπορούν να συμβουλεύονται τον ΥΠΔ για κάθε θέμα που αφορά την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την άσκηση των δικαιωμάτων τους βάσει του ΓΚΠΔ ή άλλης σχετικής νομοθεσίας.
- Εάν ο ΥΠΔ λάβει γνώση δεδομένων Προσωπικού Χαρακτήρα κατά την άσκηση του έργου του, για τα οποία ο επικεφαλής του δημόσιου φορέα/οργανισμού αρνηθεί να καταθέσει ως μάρτυρας για επαγγελματικούς λόγους (ατομικό του δικαίωμα), το δικαίωμα αυτό έχει ισχύ και για τον ΥΠΔ και τους βοηθούς του.

- Το άρθρο 8, αφορά τα καθήκοντα του ΥΠΔ σύμφωνα με τον ΓΚΠΔ και επίσης:
  - ενημερώνει και συμβουλεύει τον δημόσιο φορέα/οργανισμό και τους εργαζόμενους του που διενεργούν την επεξεργασία σχετικά με τις υποχρεώσεις τους.
  - παρακολουθεί την τήρηση των διατάξεων του ΓΚΠΔ και κάθε σχετικής νομοθεσίας για την προστασία δεδομένων προσωπικού χαρακτήρα, και των πολιτικών του δημόσιου φορέα/οργανισμού.
  - συμβουλεύει για την εκτίμηση αντικτύπου.
  - συνεργάζεται με την Εποπτική Αρχή.
  - ενεργεί και ως σημείο επαφής με την Εποπτική Αρχή σε θέματα που αφορούν την επεξεργασία, συμπεριλαμβανομένης της διαβούλευσης (άρθρο 67).
  - Τα καθήκοντα του ΥΠΔ όταν ορίζεται από δικαστικές και εισαγγελικές αρχές δεν μπορούν να αφορούν τις πράξεις επεξεργασίας που διενεργούνται από τις δικαστικές και εισαγγελικές αρχές στο πλαίσιο της δικαστικής λειτουργίας και των δικαστικών τους καθηκόντων.

- Ο ΥΠΔ έχει τη δυνατότητα να έχει και άλλα καθήκοντα.

- Το άρθρο 24, αφορά την επεξεργασία ατομικών δεδομένων για άλλους σκοπούς από δημόσιους φορείς/οργανισμούς. Αυτή επιτρέπεται εφόσον η επεξεργασία κρίνεται αναγκαία για την ολοκλήρωση των καθηκόντων τους, υπό τις προϋποθέσεις:
  - να είναι απαραίτητο να υποστούν έλεγχο πληροφορίες που παρέχονται από το υποκείμενο των δεδομένων, επειδή υπάρχουν βάσιμες ενδείξειςότι είναι λανθασμένες.
  - για λόγους εθνικής ασφαλείας ή τη διασφάλιση φορολογικών/τελωνειακών εσόδων.
  - για διώξεις ποινικών αδικημάτων.
  - για επεξεργασία ειδικών κατηγοριών δεδομένων ατομικού χαρακτήρα (άρθρο 9, παρ. 1, παρ.2, άρθρο 22 ΓΚΠΔ).
- Το άρθρο 26, αφορά τη διαβίβαση δεδομένων ατομικού χαρακτήρα από δημόσιους φορείς/οργανισμούς. Αυτή επιτρέπεται εφόσον κρίνεται απαραίτητο για την εκτέλεση των καθηκόντων του φορέα/οργανισμού που διαβιβάζει ή του τρίτου στον οποίο διαβιβάζονται τα δεδομένα και με την προϋπόθεση να πληρούνται επακριβώς οι αιτιάσεις για επεξεργασία σύμφωνα με το άρθρο 24. Ο τρίτος που λαμβάνει τα δεδομένω, τα επεξεργάζεται εφόσον ικανοποιούν τον σκοπό για τον οποίο διαβιβάσθηκαν. Η επεξεργασία για άλλους σκοπούς μπορεί να γίνουν σύμφωνα με τις προϋποθέσεις του άρθρου 24. Τέλος, μπορούν να δαιβιβασθούν σε ιδιωτικούς φορείς/οργανισμούς σύμφωνα με κάποιες προϋποθέσεις: πληρούνται οι προϋποθέσεις του άρθρου 24, ο τρίτος που λαμβάνει τα δεδομένα έχει έχει έννομο συμφέρον να είναι σε γνώση της διαβίβασης και το υποκείμενο των δεδομένων δεν έχει έννομο συμφέρον να μην διαβιβασθούν τα δεδομένα του και η επεξεργασία κρίνεται απαραίτητη για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων.
- Το άρθρο 27 αφορά την επεξεργασία δεδομένων ατομικού χαρακτήρα στο πλαίσιο των σχέσεων απασχόλησης. Οι προϋποθέσεις είναι:
  - αφορούν σύναψης σύμβασης εργασίας ή μετά τη σύναψη της σύμβασης εργασίας για την εκτέλεσή της.
  - όταν η επεξεργασία δεδομένων ατομικού χαρακτήρα του εργαζομένου έχει κατ’ εξαίρεση ως νομική βάση τη συγκατάθεσή του, εφόσον ήταν αποτέλεσμα ελεύθερης επιλογής.

- κατά παρέκκλιση από το άρθρο 9 παρ. 1 του ΓΚΠΔ, για τους σκοπούς της σύμβασης εργασίας επιτρέπεται, όταν είναι απαραίτητη από το εργατικό δίκαιο, το δίκαιο της κοινωνικής ασφάλισης και της κοινωνικής προστασίας.
- για σκοπούς σύμβασης εργασίας Τα διαπραγματευόμενα μέρη συμμορφώνονται με το άρθρο 88 παράγραφος 2 του ΓΚΠΔ.
- ο υπεύθυνοσ επεξεργασίας παίρνει μέτρα ώστε να ακολουθούνται οι αρχές προστασίας ατομικών δεδομένων που ορίζονται στο άρθρο 5 του ΓΚΠΔ.
- Η επεξεργασία δεδομένων προσωπικού χαρακτήρα μέσω κλειστού κυκλώματος οπτικής καταγραφής εντός των χώρων εργασίας, είτε είναι δημοσίως προσβάσιμοι είτε μη, επιτρέπεται μόνο εάν είναι απαραίτητη για την προστασία προσώπων και αγαθών.

- Τα άρθρα 53-59, αφορούν το ορισμό των δικαιωμάτων του υποκειμένου, όπως: το δικαίωμα ενημέρωσης, πρόσβασης, διόρθωσης ή διαγραφής δεδομένων, το δικαίωμα υποβολής καταγγελίας στην εποπτική Αρχή και δικαίωμα σε ποινικές έρευνες και διαδικασίες.
- Τα άρθρα 80 και 82, αφορούν το ορισμό των ευθυνών και των κυρώσεων του εκτελούντος την επεξεργασία.

Η νέα νομοθεσία αποτελεί μια πολύ σημαντική παρέμβαση που προϋποθέτει να προσαρμοστούν οι δράσεις συμμόρφωσης ΓΚΠΔ, στις επιπλέον υποχρεώσεις της νέας νομοθεσίας. Στην επεξεργασία ειδικών κατηγοριών (ευαίσθητων) δεδομένων, εισάγονται οι προϋποθέσεις χρήσης για κάποιες από τις νομικές βάσεις επεξεργασίας του ΓΚΠΔ, ενώ τέθηκε η υποχρέωση των υπεύθυνων επεξεργασίας, η παροχή περαιτέρω μέτρων προστασίας των συμφερόντων του υποκειμένου των δεδομένων. Βασικό σημείο της νέας νομοθεσίας αποτελούν οι διατάξεις για την επεξεργασία δεδομένων στο πεδίο των εργασιακών σχέσεων. Ορίζονται συγκεκριμένες νομικές βάσεις επεξεργασίας δεδομένων, ενώ προβλέπεται με ρητό τρόπο, η διαδικασία χρήσης της συγκατάθεσης ως νομική βάση στην εργασία μόνο καθ' εξαίρεση, και παρέχονται τα κριτήρια που θα πρέπει να χρησιμοποιούν οι εργοδότες για να βεβαιωθούν πως η συγκατάθεση χαρακτηρίζεται από ελευθερίας και νομιμότητα. Επιπλέον, εισάγεται πρόβλεψη για επεξεργασία προσωπικών δεδομένων στη βάση συλλογικών συμβάσεων εργασίας (Ιγγλεζάκης, 2018β, Παναγοπούλου-Κουτνατζή, 2017).

5.5 Προστασία Προσωπικών Δεδομένων Εργαζομένων Δημόσιου Τομέα

Ο ΓΚΠΔ σε συνδυασμό με τον Ν. 4624/19 παρέχει σημαντική προστασία των εργαζομένων τόσο στο Δημόσιο όσο και στο ιδιωτικό τομέα. Στην νέα νομοθεσία όσο αφορά το Δημόσιο τίθενται οι εξής ορισμοί[19,20]:

- *"Εργαζόμενοι":* Εργαζόμενοι Ιδιωτικού ή Δημοσίου Τομέα, οι υποψήφιοι προς εργασία, και οι πρώην εργαζόμενοι.
- *"Εργοδότης"***:** Φυσικό ή νομικό πρόσωπο που προσδιορίζει δεσμευτικά την οργάνωση, το περιεχόμενο και γενικά τους όρους της εργασίας, περιλαμβάνοντας το σύνολο των μορφών απασχόλησης (τακτικός, έκτακτος, ωρομίσθιος κοκ.).
- *"Σχέση εξάρτησης":* Είναι η εργασία υπό τον έλεγχο και την εποπτεία του εργοδότη, ανεξαρτήτως κύρους της σχέσης απασχόλησης.

Ο Ελληνικός υπαλληλικός κώδικας δεν ρυθμίζει τον ειδικότερο τρόπο άσκησης των δικαιωμάτων που κατοχυρώνονται υπέρ του εργαζόμενου στο δημόσιο, αλλά ορίζεται ότι ο τρόπος τήρησης και ενημέρωσης του προσωπικού μητρώου των εργαζομένων, ο χρόνος περιοδικής καταστροφής των εκθέσεων αξιολόγησης των ουσιαστικών προσόντων, η μετά από αίτηση αφαίρεση στοιχείων, καθώς και κάθε σχετική διαδικασία ή άλλη λεπτομέρεια θα καθορίζονται με προεδρικό διάταγμα. Ωστόσο, σε σχετικό προεδρικό διάταγμα που εκδόθηκε κατ΄ εξουσιοδότηση του Ν. 2683/99, απουσιάζουν διατάξεις με αντικείμενο τον τρόπο άσκησης των προβλεπόμενων δικαιωμάτων, ενώ ειδική μέριμνα λαμβάνεται μόνο για την καταστροφή των εκθέσεων αξιολόγησης. Συγκεκριμένα, για τις εκθέσεις αξιολόγησης οι ρυθμίσεις του υπαλληλικού κώδικα φαίνεται να συμβαδίζουν πλήρως με την αρχή της χρονικά περιορισμένης διάρκειας τήρησης των δεδομένων που εισάγει ο Ν.2472/97, που επιβάλλει την τήρηση των δεδομένων μόνο για το χρονικό διάστημα που είναι αναγκαίο για την εκπλήρωση των σκοπών της επεξεργασίας[21,22]. Όμως, σε όλες τις περιπτώσεις που τηρούνται προσωπικά δεδομένα τους, απολαμβάνουν τα δικαιώματα προστασία τους, σύμφωνα με την κείμενη νομοθεσία, με τις προβλεπόμενες εξαιρέσεις.

Ο ΓΚΠΔ για τους εργαζομένους στο δημόσιο τομέα[23] ως υποκείμενα δεδομένων περιλαμβάνει (Διάγρ.27)(Κουκιάδης, 2019, Πλατής, 2018):

Α. Δικαιώματα Εργαζομένων

[19] Οδηγία 115/2001 ΑΠΔΠΧ.
[20] https://www.lawspot.gr/gdpr/dedomena-ergazomenon.
[21] Ν.2683/99, άρθρο 23, παρ.6.
[22] ΠΔ 178/2004, άρθρο 3 - πρόβλεψη για το ατομικό μητρώο να περιλαμβάνονται μόνο οι ατομικές εκθέσεις αξιολόγησης της τελευταίας πενταετίας ή σχετίζονται με εκκρεμείς δίκες, ενώ οι υπόλοιπες αφαιρούνται και καταστρέφονται τον Ιανουάριο κάθε έτους με καθορισμένη διαδικασία.
[23] Σε πολλά σημεία ισχύουν τα ίδια και για τους εργαζόμενους στον ιδιωτικό τομέα.

- Το *δικαίωμα ενημέρωσης* (άρθρο 12), που περιλαμβάνει την υποχρέωση του εργοδότη (Δημόσιο) να παρέχει διαφάνεια ως προς τον τρόπο με τον οποίο θα χρησιμοποιούνται τα προσωπικά δεδομένα. Ειδικότερα:
    - Διαφανή πολιτική ενημέρωσης των υποκειμένων δεδομένων, έτσι ώστε κάθε υποκείμενο να μπορεί να ασκεί τα δικαιώματα του αποτελεσματικά.
    - Να αποφεύγεται η υπερπληροφόρηση, ενώ κάθε πληροφορία και ανακοίνωση σχετικά με την επεξεργασία προσωπικών δεδομένων πρέπει να είναι εύκολα προσβάσιμη, κατανοητή, με σαφή και απλή γλώσσα.
    - Να γίνεται χρήση γραπτή ή/και ηλεκτρονικής μορφής επικοινωνίας.
    - Η προθεσμία ενημέρωσης να είναι ένας (1) μήνας με δυνατότητα παράτασης (μέχρι 2 μήνες).
    - Κάθε αίτηση δεν αντιστοιχεί και σε υποχρέωση για ενέργεια, αλλά οπωσδήποτε θα πρέπει να υπάρξει σχετική ενημέρωση (προσοχή στα καταχρηστικά αιτήματα).
- Το *δικαίωμα πρόσβασης* (άρθρα 13-15), που αφορά το αίτημα για πρόσβαση στα προσωπικά δεδομένα του εργαζομένου. Ειδικότερα:
    - Δικαίωμα ελέγχου της επεξεργασίας των ατομικών δεδομένων, έχει το υποκείμενο δεδομένων (εργαζόμενος), για άσκηση των δικαιωμάτων που του παρέχει ο κανονισμός και η νομοθεσία.
    - Το δικαίωμα του δεν χρήζει αιτιολόγησης.
    - Έχει πρόσβαση σε πληροφορίες όπως: (i) σκοπό επεξεργασίας, (ii) κατηγορίες δεδομένων, (iii) αποδέκτες, (iiii) χρονικό διάστημα διατήρησης, (v) ύπαρξη δικαιώματος υποβολής αιτήματος για διόρθωση, διαγραφή κλπ, (vi) δικαίωμα υποβολής καταγγελίας στην εποπτική αρχή, και (vii) προέλευσή τους.
- Το *δικαίωμα της διόρθωσης* των δεδομένων που είναι ανακριβή ή ελλιπή (άρθρο 16). Πιο αναλυτικά:
    - Δικαίωμα απαίτησης από τον υπεύθυνο επεξεργασίας για διόρθωση ανακριβών δεδομένων του φακέλου του, ή επικαιροποίηση, ή συμπλήρωση ελλιπών δεδομένων.
    - Ελλιπή είναι δεδομένα που οδηγούν σε παραπλάνηση ή παρεξήγηση (π.χ. αναγνώριση ενός πενταετούς διπλώματος επιστήμης μηχανικού ότι έχει πιστοποιηθεί ως Integrated Master, σύμφωνα με την κείμενη νομοθεσία).
- *Δικαίωμα διαγραφής (λήθης*) (άρθρο 17). Ειδικότερα:

- Το υποκείμενο δεδομένων δικαιούται να ζητήσει από τον υπεύθυνο επεξεργασίας τη διαγραφή των δεδομένων του, όταν ισχύουν ένας ή περισσότεροι από τους ακόλουθους λόγους:
    1. Τα δεδομένα δεν είναι αναγκαία για τους σκοπούς της επεξεργασίας.
    2. Το υποκείμενο δεδομένων έχει ανακαλέσει τη συναίνεσή του ως νομική βάση επεξεργασίας και δεν υπάρχει άλλη.
    3. Το υποκείμενο δεδομένων αντιτίθεται στην επεξεργασία και δεν υπάρχουν πιεστικοί λόγοι για αυτή.
    4. Τα προσωπικά δεδομένα έτυχαν επεξεργασίας παράνομα.
    5. Τα προσωπικά δεδομένα πρέπει να διαγραφούν ώστε να τηρηθεί νομική υποχρέωση.
    6. Τα προσωπικά δεδομένα συλλέχθηκαν σε σχέση με την προσφορά υπηρεσιών της κοινωνίας της πληροφορίας (νέες τεχνολογίες και διαδίκτυο).
- Η διάταξη της παρ.3 του άρθρου 17, είναι πολύ σημαντική, επειδή δεν εφαρμόζονται όλοι οι προηγούμενοι λόγοι όταν η επεξεργασία είναι απαραίτητη (δημόσιο συμφέρον, αρχειοθέτηση, θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων).
- Δεν απαιτείται επίκληση ζημίας.

- *Δικαίωμα περιορισμού της επεξεργασίας* (άρθρο 18). Πιο αναλυτικά:
    - Το υποκείμενο δεδομένων (εργαζόμενος) έχει δικαίωμα να εξασφαλίζει από τον υπεύθυνο επεξεργασίας τον περιορισμό της επεξεργασίας των δεδομένων του σε συγκεκριμένες περιπτώσεις:
        1. Η ακρίβεια των προσωπικών δεδομένων αμφισβητείται από το υποκείμενο για χρονικό διάστημα που επιτρέπει στον υπεύθυνο επεξεργασίας να τα επαληθεύσει.
        2. Η επεξεργασία είναι παράνομη.
        3. Ο υπεύθυνος επεξεργασίας δεν χρειάζεται πια τα δεδομένα, τα χρειάζεται όμως ο εργαζόμενος για άσκηση νομικών αξιώσεων.
        4. Ο εργαζόμενος έχει αντιρρήσεις για την επεξεργασία και ζητά την προσωρινή αναστολή, μέχρις ότου να ολοκληρωθεί ο έλεγχος βασιμότητας των αντιρρήσεων του.
        5. ενημέρωση του εργαζόμενου για την άρση του περιορισμού.

- *Δικαίωμα στη φορητότητα* των δεδομένων (άρθρο 20). Αναλυτικά:
    - Ο εργαζόμενος έχει δικαίωμα να λάβει ή να ζητήσει τη μεταφορά των δεδομένων του, σε "*ψηφιακή*" μορφή, από έναν υπεύθυνο επεξεργασίας σε άλλον, εφόσον πληρούνται συγκεκριμένες προϋποθέσεις.
    - Αφορά σε δεδομένα που λήφθηκαν με βάση τη νομική βάση της συναίνεσης, ή όταν η επεξεργασία διενεργείται με αυτοματοποιημένα μέσα (υπολογιστή).
    - Δεν αφορά σε παραδοσιακά αρχεία δεδομένων (σε έντυπη μορφή).
    - Η μεταφορά γίνεται από υπεύθυνο επεξεργασίας προς υπεύθυνο επεξεργασίας.
    - Αφορά μόνο στα ατομικά δεδομένα και όχι σε εργασία (στοιχεία αξιολόγησης) του φορέα, που συνοδεύει ή αφορά στα δεδομένα.
- *Δικαίωμα εναντίωσης* στην επεξεργασία (άρθρο 21), που αφορά μια ιδιαίτερη κατάσταση, όπως είναι οι ειδικές περιστάσεις της ζωής του κάθε ανθρώπου, νομικές, κοινωνικές, οικογενειακές καταστάσεις ανάγκης.
- *Δικαίωμα στην ανθρώπινη παρέμβαση* (άρθρο 22), όταν υπόκειται σε απόφαση που λαμβάνεται αποκλειστικά με αυτοματοποιημένη επεξεργασία, χωρίς τα ατομικά χαρακτηριστικά του.

Β. Συναίνεση

Αφορά περιπτώσεις (συνήθως σπάνιες) που η επεξεργασία των προσωπικών δεδομένων θα γίνεται επί τη βάσει της συναίνεσης (εφόσον προηγείται αναλυτική ενημέρωση), ισχύουν τα ακόλουθα (άρθρα 4,7):

- Συναίνεση του υποκειμένου των δεδομένων (ελεύθερη, ρητή, σε πλήρη επίγνωση, με γραπτή δήλωση ή με σαφή θετική ενέργεια).
- Όταν η επεξεργασία βασίζεται σε συναίνεση, ο υπεύθυνος επεξεργασίας πρέπει να είναι σε θέση να αποδείξει ότι το υποκείμενο των δεδομένων (εργαζόμενος) συγκατατέθηκε στην επεξεργασία.
- Εάν η συναίνεση του υποκειμένου των δεδομένων παρέχεται στο πλαίσιο γραπτής δήλωσης, που αφορά και άλλα θέματα, το αίτημα για συναίνεση υποβάλλεται κατά τρόπο διακριτό και σαφή.
- Ο εργαζόμενος (υποκείμενο των δεδομένων) έχει δικαίωμα να ανακαλέσει τη συναίνεσή του ανά πάσα στιγμή.

Γ. Ενημέρωση Εργαζομένων

Σύμφωνα με τον κανονισμό (άρθρο 13), κάθε φορέας θα πρέπει κατά τη συλλογή και επεξεργασία δεδομένων προσωπικού χαρακτήρα στο έντυπο ενημέρωσης να περιλαμβάνει τα

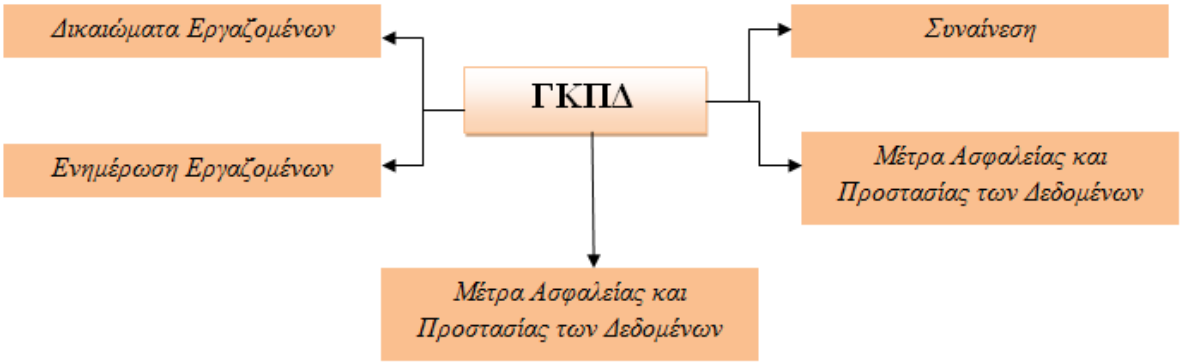
στοιχεία, όπως: ατομικά στοιχεία του υποκείμενου δεδομένων, τον σκοπό, τους αποδέκτες, το χρόνο διατήρησης των ατομικών δεομένων, τη δυνατότητα άσκησης δικαιωμάτων και τυχόν κινδύνους.

Δ. Μέτρα Ασφαλείας και Προστασίας των Δεδομένων

Το άρθρο 25 περιγράφει τις υποχρεώσεις του υπεύθυνου επεξεργασίας, ενώ το άρθρο 32 περιγράφει τα μέτρα ασφαλείας και προστασίας των ατομικών δεδομένων (π.χ. ψευδωνυμοποίηση).

Ε. Αρχείο Δραστηριοτήτων Επεξεργασίας

Το άρθρο 30 αναφέρεται σε αυτό, που αποτελεί το βασικό εργαλείο απόδειξης τήρησης της αρχής της λογοδοσίας.



Διάγραμμα 27. Πλαίσιο Προστασίας Εργαζομένων στο Δημόσιο Τομέα (ΓΚΠΔ)

Για παράδειγμα, το Πανεπιστήμιο Κρήτης (φορέας - ΝΠΔΔ) υιοθετώντας τον ΓΚΠΔ (υποχρεωτικότητα εφαρμογής του) για το προσωπικό του αλλά και τους άλλους εμπλεκόμενους (φοιτητές, επισκέπτες κλπ.) περιγράφει τα εξής, εξειδικεύοντας σύμφωνα με τη φύση και αποστολή του[24]:

- Για τις ανάγκες του, υποκείμενα δεδομένων δεν αποτελούν μόνο όσοι ωφελούνται από τις υπηρεσίες του Πανεπιστημίου, όπως οι φοιτητές, αλλά και οι εργαζόμενοι σε αυτό, για τους οποίους συλλέγονται και επεξεργάζονται δεδομένα προσωπικού χαρακτήρα (απλά και ειδικών κατηγοριών).
- Ο υπεύθυνος επεξεργασίας του Πανεπιστημίου Κρήτης και σε εφαρμογή της αρχής της λογοδοσίας, που θεσπίζει στο άρθρο 5 ο ΓΚΠΔ, οφείλει να αποδεικνύει εγγράφως ότι τηρεί τις εξής αρχές:
    - Της νομιμότητας, της αντικειμενικότητας και της διαφάνειας.
    - Του περιορισμού του σκοπού.

[24] Οδηγός Συμμόρφωσης στον ΓΚΠΔ, Πανεπιστήμιο Κρήτης, Μάρτιος 2019, (Συντ. Ε. Βενέδικτου, υπ. Προστασίας Δεδομένων), www.uoc.gr [πεόσβαση 2/11/20].

- Της ελαχιστοποίησης και ακρίβειας των δεδομένων, που συλλέγονται.
- Του περιορισμού (και εξ αρχής ορισμού) της περιόδου αποθήκευσης. Για μεγαλύτερη χρονική περίοδο και εφόσον προβλέπεται από τον ΓΚΠΔ ή το εθνικό δίκαιο, θα πρέπει να επιλέγεται η διαδικασία ψευδωνυμοποίησης και ανωνυμοποίησης.
- Της ακεραιότητας και της εμπιστευτικότητας. Δεν έχουν πρόσβαση όλοι οι εργαζόμενοι του Πανεπιστημίου σε όλα τα δεδομένα, αλλά μόνο σε αυτά που τους επιτρέπουν να ασκούν τα καθήκοντά τους. Όλο το προσωπικό του φορέα θα πρέπει να αυτοπεριορίζονται στον πεδίο αυτό. Δεδομένα ειδικών κατηγοριών αποστέλλονται με αυξημένα μέτρα προστασίας (χρήση κρυπτογράφησης, ειδικές ενδείξεις απορρήτου και εμπιστευτικότητας).

- Για το Πανεπιστήμιο Κρήτης, δύο είναι οι νομικές βάσεις (προϋποθέσεις) που είναι προσφορότερες, και καθιστούν την επεξεργασία απλών δεδομένων προσωπικού χαρακτήρα νόμιμη: οι (γ) και (ε) περιπτώσεις του άρθρου 6 του ΓΚΠΔ. Ειδικότερα:
  - Ανάγκη συμμόρφωσης σε έννομη υποχρέωση του Πανεπιστημίου.
  - Ανάγκη εκπλήρωσης καθήκοντος υπέρ του δημοσίου συμφέροντος ή κατά την άσκηση δημόσιας εξουσίας του Πανεπιστημίου.

  Επιπλέον, ισχύουν τα εξής:
  - Κατά βάση, δεν θα πρέπει να χρησιμοποιείται ως βάση η συναίνεση, διότι δεν συνάδει με τη φύση και την αποστολή του Φορέα.
  - Στα έντυπα ενημέρωσης δεν μπορούν να τεθούν πολλές ή εναλλακτικές νομικές βάσεις. Αντίθετα, επιλέγεται μόνο μία, αυτή που συμφωνεί με τη φύση των δεδομένων (ανεξάρτητα κατηγορίας τους) και με τον σκοπό της συλλογής και επεξεργασίας τους.
  - Στα έντυπα ενημέρωσης, ο εργαζόμενος θέτει την υπογραφή του υπό την ένδειξη "*ενημερώθηκα*" ή "έλαβα γνώση των ανωτέρω και όχι "*συναινώ*".
- Τα άρθρα 9 & 10 αναφέρονται στις 10 νομικές βάσεις (προϋποθέσεις) και στους όρους που καθιστούν νόμιμη την επεξεργασία ειδικών κατηγοριών προσωπικών κατηγοριών. Από αυτές τα (α), (β) (στ), (ζ) και (ι) είναι προσφορότερες (κατά περίπτωση) από τον φορέα:
  - (α) η συναίνεση,
  - (β) η ανάγκη εκτέλεσης υποχρεώσεων και άσκησης δικαιωμάτων του φορέα στους τομείς του εργατικού δικαίου, του δικαίου κοινωνικής ασφάλισης και του δικαίου κοινωνικής προστασίας,

- (στ) η άσκηση νομικών αξιώσεων,
- (ζ) λόγοι ουσιαστικού δημοσίου συμφέροντος ανάλογου προς τον επιδιωκόμενο σκοπό και
- (ι) σκοποί αρχειοθέτησης προς το δημόσιο συμφέρον, για επιστημονική και ιστορική έρευνα και για στατιστικούς λόγους.

- Για το φορέα ο ορισμός Υπευθύνου Προστασίας Δεδομένων είναι υποχρεωτικός. Η θέση του στο οργανόγραμμα και οι αρμοδιότητές του καθορίζονται ειδικώς στα άρθρα 38 και 39 του ΓΚΠΔ.
- Τα άρθρα 85 - 91 του ΓΚΠΔ αφορούν τις ειδικές περιπτώσεις επεξεργασίας. Σημαντικό άρθρο για την αποστολή του Φορέα είναι το άρθρο 89, που παρέχει τη δυνατότητα στα κράτη μέλη της ΕΕ να θεσπίζουν κατάλληλες εγγυήσεις και παρεκκλίσεις σχετικά με την επεξεργασία για σκοπούς αρχειοθέτησης για λόγους δημοσίου συμφέροντος ή για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς.
- *Δικαιώματα Προσωπικού ως υποκείμενα Δεδομένων*. Το αρμόδιο προσωπικό πρέπει πάντα να επαληθεύει την ταυτότητα του αιτούντος την άσκηση δικαιώματός του και να απαντά εγγράφως μέσα στις προθεσμίες, που ορίζει ο ΓΚΠΔ (άρθρο 12 παρ. 3 & 4: κατά περίπτωση), είτε άμεσα είτε μέσα σε ένα μήνα, είτε μέσα σε δύο μήνες είτε, στην περίπτωση που δεν έχουν προβεί σε κάποια ενέργεια οι αρμόδιοι υπάλληλοι, τότε μέσα σε ένα μήνα γίνεται ενημέρωση γιατί δεν έγινε κάποια ενέργεια και πότε προβλέπεται η απάντηση.
- Στο φορέα δεν γίνεται συλλογή και επεξεργασία δεδομένων προσωπικού χαρακτήρα χωρίς ενημέρωση του υποκειμένου τους και υπογραφή του εντύπου ενημέρωσης, που θα περιλαμβάνει τα στοιχεία, όπως:
  - την ταυτότητα και τα στοιχεία επικοινωνίας του υπευθύνου επεξεργασίας,
  - τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων,
  - τους σκοπούς της επεξεργασίας και τη νομική βάση για την επεξεργασία,
  - τα έννομα συμφέροντα εάν η επεξεργασία βασίζεται στο άρθρο 6 (παρ. 1 στοιχείο στ),
  - τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων προσωπικού χαρακτήρα, εφόσον υπάρχουν,
  - κατά περίπτωση, την πρόθεση του υπευθύνου επεξεργασίας να διαβιβάσει δεδομένα προσωπικού χαρακτήρα σε τρίτη χώρα ή διεθνή φορέα,

- το χρόνο αποθήκευσης των δεδομένων,
- τη τυχόν δυνατότητα άσκησης δικαιωμάτων,
- πιθανούς κινδύνους από την επεξεργασία των δεδομένων.

- *Ενημέρωση υποκείμενων δικαιωμάτων* (άρθρο 14). Ο φορέας παρέχει στο υποκείμενο τις εξής πληροφορίες:
  - την ταυτότητα και τα στοιχεία επικοινωνίας του υπευθύνου επεξεργασίας,
  - τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων,
  - τις σχετικές κατηγορίες προσωπικών δεδομένων,
  - τους αποδέκτες,
  - κατά περίπτωση, την πρόθεση του υπεύθυνου επεξεργασίας να διαβιβάσει δεδομένα προσωπικού χαρακτήρα,
  - κατά περίπτωση, την πρόθεση του υπεύθυνου επεξεργασίας να διαβιβάσει δεδομένα προσωπικού χαρακτήρα, σε τρίτη χώρα ή διεθνή φορέα,
  - το χρόνο αποθήκευσης των δεδομένων,
  - τη τυχόν δυνατότητα άσκησης δικαιωμάτων
  - την δυνατότητα ανάκλησης της συγκατάθεσης του,
  - το δικαίωμα υποβολής καταγγελίας στην ΑΠΔΠΧ,
  - την πηγή των δεδομένων,
  - την ύπαρξη αυτοματοποιημένης λήψης απόφασης,
  - πιθανούς κινδύνους από την επεξεργασία των δεδομένων.
- *Εξαιρέσεις και Περιορισμοί στην άσκηση των δικαιωμάτων*. Ο φορέας παρέχει τέτοιες πληροφορίες όταν:
  - εντός εύλογης προθεσμίας από την απόκτηση και το αργότερο εντός μήνα,
  - στην πρώτη επικοινωνία με το υποκείμενο δεδομένων, όταν τα δεδομένα πρόκειται να χρησιμοποιηθούν για επικοινωνία με το υποκείμενο,
  - στην γνωστοποίηση σε άλλο αποδέκτη (άλλο φορέα, τρίτο πρόσωπο), όταν τα δεδομένα γνωστοποιούνται πρώτη φορά.

  Δεν απαιτείται να τηρηθούν τα παραπάνω όταν:
  - όταν το υποκείμενο δεδομένων έχει όλες τις πληροφορίες,,
  - όταν η παροχή των πληροφοριών είναι αδύνατη ή δυσανάλογα δύσκολη (πρέπει να ληφθούν τα απαραίτητα μέτρα προστασίας και ασφάλειας),
  - όταν η απόκτηση ή κοινολόγηση προβλέπεται από νομοθεσία προστασίας των εννόμων συμφερόντων του υποκειμένου δεδομένων,
  - λόγοι εμπιστευτικότητας (υποχρέωση απορρήτου).

- *Μέτρα Ασφαλείας και Προστασίας των Δεδομένων* (άρθρα 25, 32). Πέρα από τις απαιτήσεις των άρθρων του Κανονισμού, ο φορέας θα πρέπει:
    - να εφαρμόζει την ανωνυμοποίηση, κυρίως για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς λόγους,
    - να προσδιορίζει εγγράφως, με βάση τα καθηκοντολόγιά και τις αρμοδιότητές τους, ποια πρόσωπα (ονομαστικά) είναι εξουσιοδοτημένα για συγκεκριμένες ενέργειες,
    - να τηρεί αντίγραφα ασφαλείας αρχείων με δεδομένα προσωπικού χαρακτήρα,
    - να αποφεύγει ρητώς χρήση εξωτερικών αποθηκευτικών μέσων και να μην εξάγονται αρχεία για εργασία στο σπίτι,
    - να έχει φύλαξη χώρων,
    - να ακολουθεί την αρχή του "*clean desk*" και να μην μπορούν να δουν τρίτοι έγγραφα και αρχεία με δεδομένα προσωπικού χαρακτήρα,
    - να επικαιροποιεί τα λογισμικά και τα λογισμικά προστασίας από ιούς (antivirus, firewall).
    - να καταστρέφει όλα τα αρχεία δεδομένων με την ολοκλήρωση του χρόνου τήρησής τους.
- *αρχείο Δραστηριοτήτων επεξεργασίας* (άρθρο 30). Χρησιμοποιείται για να ικανοποιείται η αρχή της λογοδοσίας. Ο φορέας το τηρεί σε γραπτή και σε ηλεκτρονική μορφή.
- *Ειδικά Θέματα*. Ειδικότερα το Πανεπιστήμιο Κρήτης:
    - Δεν απαιτεί να λαμβάνει συναίνεση του προσωπικού του για την αξιοποίηση των ατομικών δεδομένων. Η συναίνεση του υποκειμένου είναι απαραίτητη νομική βάση για να έχει νομιμότητα η επεξεργασία δεδομένων προσωπικού χαρακτήρα μόνο όταν δεν συντρέχει καμία από τις περιπτώσεις (β), (γ) & (ε) του άρθρου 6 (παρ.1) για τα απλά δεδομένα και του άρθρου 9 παρ.2 των περιπτώσεων (β), (ζ) & (ι) για τα δεδομένα ειδικών κατηγοριών. Επίσης, δεν είναι απαραίτητη όταν απαιτείται από διάταξη νόμου, όπως, για παράδειγμα, όταν διεξάγεται έρευνα από την *Ιατρική Σχολή* ή το *Βιολογικό τμήμα* στο πλαίσιο κλινικών δοκιμών μιας θεραπείας. Αν απαιτηθεί συναίνεση, τότε αυτή είναι έγγραφη μετά από πλήρη ενημέρωση.
    - Σε περίπτωση ένα τρίτο πρόσωπο (π.χ. δικηγόρος) ζητήσει δεδομένα προσωπικού χαρακτήρα εργαζομένων του Φορέα, δικαιούται εφόσον, καταθέσει έγγραφη αίτηση και αποδείξει ότι είναι εξουσιοδοτημένος προς

αυτό. Δεν επιτρέπεται να γνωστοποιείται ούτε το γεγονός ότι κάποιος είναι εργαζόμενος με οποιαδήποτε σχέση στο Πανεπιστήμιο.

- Σε περίπτωση εισαγγελικής παραγγελίας, το Πανεπιστήμιο συμμορφώνεται με αυτή. Έτσι αποφεύγεται η ύπαρξη ποινικών κυρώσεων, αλλά αν για οποιοδήποτε λόγο, κριθεί το αίτημα της παραγγελίας αβάσιμο, θα πρέπει να αποσταλεί στην Εισαγγελία έγγραφη αιτιολογημένη απάντηση.
- Δεν παρέχονται πληροφορίες για δεδομένα προσωπικού χαρακτήρα προφορικά (εφαρμογή της αρχής της λογοδοσίας).
- Μετά την εφαρμογή του ΓΚΠΔ, δεν είναι υποχρεωμένος ο φορέας να γνωστοποιεί στην ΑΠΔΠΧ την ύπαρξη και λειτουργία αρχείου λόγω εγκατάστασης και λειτουργίας κλειστού κυκλώματος τηλεόρασης. Ωστόσο, πρέπει να τηρεί όλα εκείνα τα μέτρα και διαδικασίες σύμφωνα με τον Κανονισμό. Η εγκατάσταση συστήματος βιντεοσκόπησης είναι νόμιμη για το σκοπό της ασφάλειας προσώπων και αγαθών για απαγορευμένους χώρους σε μη εξουσιοδοτημένα πρόσωπα.
- Επιτρέπεται η ανάρτηση δεδομένων προσωπικού χαρακτήρα στο "*Διαύγεια*", ακολουθώντας τις αρχές του άρθρου 5 του ΓΚΠΔ (ιδιαίτερα της ελαχιστοποίησης δεομένων).
- "*Αποδέκτης*" για την τήρηση της υποχρέωσης ενημέρωσης των εργαζομένων θεωρείται κάθε φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας. Ωστόσο, οι δημόσιες αρχές, που ζητούν να λάβουν δεδομένα, στο πλαίσιο συγκεκριμένης έρευνας, δεν θεωρούνται αποδέκτες. Ο μη χαρακτηρισμός μιας δημόσιας αρχής ως "αποδέκτη", σημαίνει τη μη υποχρέωση του φορέα να τη συμπεριλάβει στα έντυπα ενημέρωσης και να ενημερώσει το υποκείμενο δεδομένων (εργαζόμενο) για μία τέτοια μεταφορά.

Ακολουθεί ένα έντυπο (Υπόδειγμα) ως παράδειγμα, του Πανεπιστημίου της Κρήτης, που αφορά την ενημέρωση για φωτογράφιση / βιντεοσκόπηση σε εξέλιξη:

Σας ενημερώνουμε ότι πραγματοποιείται φωτογράφιση και βιντεοσκόπηση του χώρου του συνεδρίου, των συνέδρων και όλων των συμμετεχόντων σε αυτό για τους σκοπούς του συνεδρίου …… της Σχολής …… του Πανεπιστημίου Κρήτης. Η φωτογράφιση και η βιντεοσκόπηση γίνονται για σκοπούς εκπαιδευτικούς, ερευνητικούς και αρχειακούς. Οι φωτογραφίες και τα βίντεο θα αναρτηθούν στο διαδίκτυο, στην ιστοσελίδα του Πανεπιστημίου Κρήτης καθώς και …. Αν δεν

επιθυμείτε τη λήψη φωτογραφίας σας ή τη βιντεοσκόπησή σας, σας παρακαλούμε ενημερώστε την / τον ……., τηλ…… Για περισσότερες πληροφορίες σχετικά με τη διαδικασία φωτογράφισης και βιντεοσκόπησης και την χρήση αυτών, σας παρακαλούμε επικοινωνήστε με τον συντονιστή της συνεδρίας κ. ……., τηλ. …….. Για περισσότερες πληροφορίες σχετικά με την πολιτική του Πανεπιστημίου Κρήτης αναφορικά με την προστασία των προσωπικών σας δεδομένων, μπορείτε να επικοινωνήσετε με την Υπεύθυνη Προστασίας Δεδομένων dpo@uoc.gr».

Συνοψίζοντας, ο ΓΚΠΔ εστιάζει περισσότερο στις επιχειρήσεις για τους υπόλοιπους άξονες των εργασιακών σχέσεων, όπως για παράδειγμα, την αρχή της υποχρέωσης λογοδοσίας. Αντίστοιχα για τις κυρώσεις, τις αξιολογήσεις των επιπτώσεων στην προστασία των δεδομένων (*Data Protection Impact Assessments - DPIAs*). Για το Δημόσιο, ο ΓΚΠΔ προσπαθεί να επιβάλλει διαβούλευση με την ΑΠΔΠΧ κατά την εκπόνηση ενός νομοθετικού ή κανονιστικού μέτρου. Η ΑΠΔΠΧ γνωμοδοτεί για κάθε ρύθμιση που αφορά την επεξεργασία και προστασία δεδομένων προσωπικού χαρακτήρα, και σε σχέση με τον Δημόσιο τομέα (ως υπεύθυνο επεξεργασίας προσωπικών δεδομένων) (Διαγρ.28):

- συμβουλεύει (για νομοθετικά και διοικητικά μέτρα, σύμφωνα με το εθνικό δίκαιο).
- υλοποιεί εκτίμηση αντικτύπου (απαραίτητα προς την εφαρμογή κάθε νέου μέτρου), ως μέρος γενικής εκτίμησης αντικτύπου στο πλαίσιο έγκρισης της νομικής βάσης, ή πριν την εφαρμογή μιας διάταξης.
- υποχρέωση DPO για κάθε δημόσιο φορέα.

Ωστόσο, η συμμόρφωση με το ΓΚΠΔ στην Δημόσια Διοίκηση, θα πρέπει να αντιμετωπιστεί ως μία συστηματική δράση, με τον κατάλληλο σχεδιασμό, ιδιαίτερα για την προστασία των προσωπικών δεδομένων[25,26].

Συνολικά, ανεξάρτητα αν είναι ή όχι εργαζόμενος στο δημόσιο τομέα, στον ΓΚΠΔ, ο εργαζόμενος ως υποκείμενο προσωπικών δεδομένων δεν περιορίζεται στον πάροχο της εργασίας, αλλά περιλαμβάνει και τον υποψήφιο παροχής εργασίας και τον τερματίσαντα την παροχή εργασίας. Στο επόμενο πίνακα φαίνεται μια σύγκριση μεταξύ δημόσιου υπάλληλου

[25] Ευρωπαϊκή Επιτροπή – Κατευθυντήριες γραμμές Ο.Ε. άρθρου 29 Οδηγίας 95/46/ΕΚ http://ec.europa.eu/justice/data-protection/article-29/index_en.htm και http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/GDPR/FILES%20GDPR/WP243REV01_EL.PDF.

[26] Ευρωπαίος Επόπτης Προστασίας Δεδομένων – DPO Corner , https://edps.europa.eu/data-protection/eu-institutions-dpo_en.

(μόνιμου) και ιδιωτικού υπάλληλου (όλων των πιθανών εργασιακών σχέσεων)(Κουκιάδης, 2019, σ.71).

Διάγραμμα 28. ΑΠΔΠΧ και Δημόσια Διοίκηση

Πίνακας 1. Σύγκριση Δημόσιων - Ιδιωτικών Υπαλλήλων

Δημόσιοι υπάλληλοι	**Ιδιωτικοί υπάλληλοι**
Μονιμότητα (Ελληνικό Σύνταγμα)	Μη μονιμότητα (ευάλωτος)
Δικαίωμα ενημέρωσης (άρθρο 12, ΓΚΠΔ)	
Δικαίωμα διόρθωσης/διαγραφή (άρθρα 16 & 17, ΓΚΠΔ)	Δικαίωμα ενημέρωσης (άρθρο 12, ΓΚΠΔ)
Δικαίωμα πρόσβασης (άρθρο 13-15, ΓΚΠΔ)	Δικαίωμα διόρθωσης/διαγραφής **(**άρθρο 16 & 17 ΓΚΠΔ)
εργασιακό δικαίωμα "*εναντίωσης στην επεξεργασία*" (άρθρο 21, ΓΚΠΔ)	Δικαίωμα πρόσβασης (άρθρο 13-15, ΓΚΠΔ)
φορητότητα δεδομένων (άρθρο 20, ΓΚΠΔ)	εργασιακό δικαίωμα "*εναντίωσης στην επεξεργασία*" (άρθρο 21, ΓΚΠΔ)
επεξεργασία δεδομένων (περιορισμένες λόγω της συνταγματικής προστασίας της ιδιότητας του δημοσίου υπαλλήλου)(Υπαλληλικός κώδικας)	φορητότητα δεδομένων **(**άρθρο 20, ΓΚΠΔ)
ΥΠΔ με συγκεκριμένες αρμοδιότητες και ρόλους[27]	επεξεργασία δεδομένων (πρωτογενή & δευτερογενή)
	ΥΠΔ με συγκεκριμένες αρμοδιότητες και ρόλους
	Η συναίνεση ή συγκατάθεση (πιο δύσκολα

[27] Εξαιρούνται τα δικαστήρια στο πλαίσιο της δικαιοδοτικής τους αρμοδιότητας. Πολλές δημόσιες αρχές ή δημόσιοι φορείς ΥΕ ή ΕΕ ορίζουν ένα μόνο υπεύθυνο προστασίας δεδομένων, λαμβάνοντας υπ' όψιν το μέγεθος και την οργανωτική τους δομή.

Η συναίνεση ή συγκατάθεση του υποκειμένου είναι η ελεύθερη ένδειξη βουλήσεως	λόγω μη μονιμότητας) Ανισορροπία στον συσχετισμό δυνάμεων μεταξύ εργοδότη και εργαζόμενου
Τρόποι παρακολούθησης στο χώρο εργασίας με νέα τεχνικά μέσα (monitoring) και κανονισμοί ελέγχου (άρθρα 85-89, ΓΚΠΔ)	Τρόποι παρακολούθησης στο χώρο εργασίας με νέα τεχνικά μέσα (monitoring) και κανονισμοί ελέγχου (άρθρα 85-89, ΓΚΠΔ)
	Κυρώσεις για παραβάσεις στην επεξεργασία προσωπικών δεδομένων (άρθρο 83, ΓΚΠΔ)
Κυρώσεις για παραβάσεις στην επεξεργασία προσωπικών δεδομένων (άρθρο 83, ΓΚΠΔ)	

5.6 Αρχή Προστασίας Προσωπικών Δεδομένων και Προστασία Προσωπικών Δεδομένων Δημοσίων Υπαλλήλων

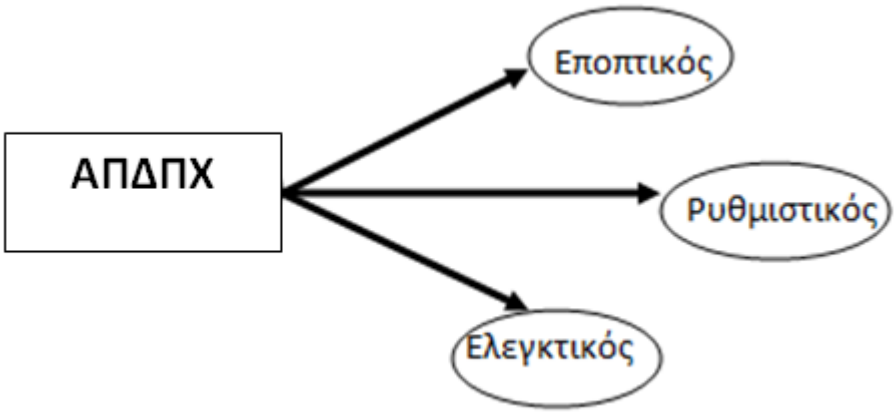
Στην Ελλάδα, η *Αρχή Προστασίας Προσωπικών Δεδομένων (ΑΠΠΔ*), αποτελεί κεντρικό όργανο εφαρμογής των ρυθμίσεων του Ν. 2472/97, που συνιστάται ως *Ανεξάρτητη Διοικητική Αρχή (ΑΔΑ*), με δικό της προϋπολογισμό. Δημιουργήθηκε στο πρότυπο της αντίστοιχης γαλλικής *Commission National de l' Informatique et de Libertés (CNIL),* ενώ τις παρέχονται βάση νομοθεσίας ευρύτατες προληπτικές και κατασταλτικές αρμοδιότητες. Για λόγους συνταγματικής τάξης, υπάγεται στον Υπουργό Δικαιοσύνης, για έλεγχο νομιμότητας. Ακόμα, υπόκειται σε κοινοβουλευτικό έλεγχο, μέσω της Επιτροπής Θεσμών και Διαφάνειας της Βουλής σύμφωνα με τον Κανονισμό της Βουλής. Οι Αποφάσεις της υπόκεινται στο νομικό έλεγχο των Ελληνικών Διοικητικών Δικαστηρίων. Τέλος, οι αρμοδιότητες της διακρίνονται σε (Διαγρ.29)(Κυριαζόγλου, 2019, Παναγοπούλου, 2018, Λαζαράκος, 2016):

- Εποπτικές και ελεγκτικές αρμοδιότητες.
- Αποφασιστικές και κυρωτικές αρμοδιότητες.
- Νομοθετικές και γνωμοδοτικές αρμοδιότητες.

Η ΑΠΔΠΧ γνωμοδοτεί για το προσωπικό των δημοσίων υπαλλήλων, με σημαντική αξία, ιδιαίτερα μετά την υιοθέτηση του ΓΚΠΔ αλλά και του νόμου 4624/2019. Για παράδειγμα, η γνωμοδότηση κατόπιν διαβούλευσης βάσει του άρθρου 36 ΓΚΠΔ σχετικά με υπολειπόμενο υψηλό κίνδυνο κατά την ανάρτηση δεδομένων ειδικών κατηγοριών στο διαδικτυακό τόπο

του ΑΣΕΠ[28]. Πιο συγκεκριμένα, η ΑΠΔΠΧ γνωμοδότησε τα εξής, σύμφωνα με τον ΓΚΠΔ και το Ν.4624/2019[29]:

- Οι συνυποψήφιοι που μετέχουν στους σχετικούς πίνακες, των διενεργηθέντων διαγωνισμών, έχουν πρόσβαση σε όλα τα στοιχεία (τόσο των ιδίων όσο και των λοιπών υποψηφίων), λόγω ότι πρέπει να ικανοποιείται το συνταγματικά κατοχυρωμένο δικαίωμα στη διαφάνεια.
- Το ευρύτερο κοινό θα μπορεί να ενημερώνεται για τα αποτελέσματα των διαγωνισμών μέσω της ανάρτησης των μικτών πινάκων κατάταξης (με γενικές και ειδικές θέσεις) και διοριστέων χωρίς να υπάρχει επεξηγηματική ένδειξη της συγκεκριμένης ειδικής κατηγορίας, που ανήκει ο κάθε υποψήφιος και χωρίς τα στοιχεία της ταυτότητας του (ονοματεπώνυμο, πατρώνυμο, μητρώνυμο, ΑΔΤ).
- Ο χρόνος διατήρησης των πινάκων προτείνεται να περιοριστεί στον απολύτως αναγκαίο και απαραίτητο και σύμφωνα με τον αρχικώς επιδιωκόμενο σκοπό της ανάρτησης.
- Τα μέτρα που προτείνονται θα πρέπει να εφαρμοστούν και από τον εκάστοτε δημόσιο φορέα πρόσληψης, είτε στο κατάστημα της υπηρεσίας του, είτε στο διαδικτυακό του τόπο.



Διάγραμμα 29. Οι ρόλοι της ΑΠΔΠΧ

[28] https://www.dpa.gr/portal/page?_pageid=33,120923&_dad=portal&_schema=PORTAL [πρόσβαση 2/11/2020].
[29] ΑΠΔΠΧ, Γνωμοδότηση 2/2020, (αρ. πρωτ. Γ/ΕΞ/2342/08-04-2020).

ΣΥΜΠΕΡΑΣΜΑΤΑ

Η προφύλαξη των ατομικών δεδομένων δεν είναι το απόλυτο δικαίωμα. Αυτό περιγράφεται επαρκώς στον *Γενικό Κανονισμό Προστασίας Δεδομένων-ΓΚΠΔ (679/2016/ΕΕ)*. Συνοψίζοντας ο ΓΚΠΔ προσφέρει τα εξής στην κοινωνία:

- ενισχύει το θεμελιώδες δικαίωμα της προστασίας προσωπικών δεδομένων.
- ενσωματώνει την προστασία δεδομένων στις επιχειρησιακές διαδικασίες. Ειδικότερα, "μ*εταφέρει*" το βάρος στους φορείς (δημόσιους ή ιδιωτικούς) στο να αυτο-συμμορφώνονται και να μπορούν να το αποδεικνύουν όποτε χρειαστεί (καταγραφή). Επίσης, εξαλείφεται η γραφειοκρατία που παρείχε κατάλληλο επίπεδο προστασίας.
- νέα δικαιώματα για τα φυσικά πρόσωπα, με νέες υποχρεώσεις για υπευθύνους και εκτελούντες.
- Νέος ρόλος της Αρχής Προστασίας Προσωπικών Δεδομένων
- Η προστασία προσωπικών δεδομένων δεν θα πρέπει να θεωρείται ως "*εμπόδ*ιο" στις λειτουργίες των φορέων. Ο ΓΚΠΔ θα πρέπει να εκληφθεί ως ένα πολύτιμο εργαλείο για εργοδότες, εργαζόμενους και πολίτες.

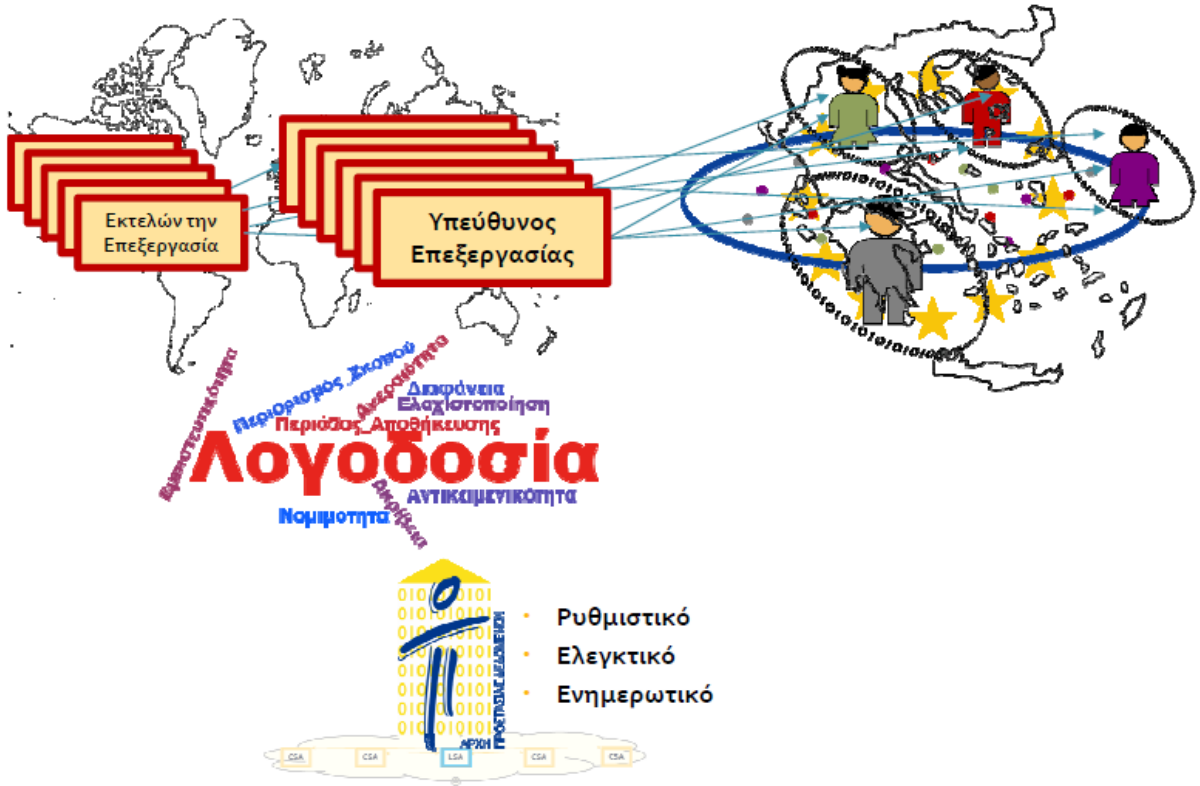
Η προστασία των ατομικών δεδομένων περιλαμβάνει και τα αντίστοιχα δικαιώματα των εργαζομένων. Στην Ελλάδα, συνταγματικά (άρθρο 9Α) το δικαίωμα στην προστασία των δεδομένων ατομικού χαρακτήρα, δεν προσδιορίζονται με σαφήνεια. Αντίθετα, στον νέο ΓΚΠΔ τα ατομικά δικαιώματα προσδιορίζονται επακριβώς, ενώ θεωρούνται ως ένα από τα πλέον ουσιώδη στοιχεία του, ενώ εισάγονται νέα δικαιώματα, όπως: φορητότητα, δικαίωμα στη λήθη κ.α. Στον ΓΚΠΔ τα δικαιώματα διακρίνονται σε πέντε (5) μέρη:

- Διαφάνεια και Ρυθμίσεις,
- Ενημέρωση και πρόσβαση σε Δεδομένα προσωπικού χαρακτήρα,
- Διόρθωση και διαγραφή,
- Δικαίωμα εναντίωσης και αυτοματοποιημένη ατομική λήψη αποφάσεων και
- Περιορισμοί.

Τέλος, οι ουσιαστικές αλλαγές για την προστασία των προσωπικών δεδομένων στο ΓΚΠΔ είναι οι εξής (Διαγρ.30):

- ο υπεύθυνος της επεξεργασίας,
- ο εκτελών την επεξεργασία,
- λογοδοσία,
- Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα ως Αρχή Εφαρμογής του ΓΚΠΔ,

- εισαγωγή νέων εργαλείων για τη συμμόρφωση με τη νομοθεσία,
- τεκμηρίωση κάθε πράξης επεξεργασίας (κατάργηση της υποχρέωσης γνωστοποίησης στις εποπτικές Αρχές),
- υποχρέωση ορισμού Υπεύθυνου Προστασίας Δεδομένων (DPO).
- οι "*προ-καθορισμένες*" ρυθμίσεις πρέπει να είναι οι πιο φιλικές προς την ιδιωτικότητα,
- απαιτήσεις για ασφαλή επεξεργασία, με εξειδίκευση, με πρόταση «ενδεδειγμένων» τεχνικών και οργανωτικών μέτρων και χρήση εγκεκριμένου κώδικα δεοντολογίας ή μηχανισμού πιστοποίησης (προαιρετικό αλλά με ενθάρρυνση από τον κανονισμό) και
- εκτίμηση αντικτύπου (επιπτώσεων) σχετικά μετ ην προστασία δεδομένων (DPIA).



Διάγραμμα 30. Οι αλλαγές του ΓΚΠΔ

Οι εργαζόμενοι στο δημόσιο τομέα υπερτερούν σε ωφελήματα από πλευράς ΓΚΠΔ σε σχέση με τους εργαζόμενους στο ιδιωτικό τομέα. Επίσης, ο νεώτερος νόμος 4624 παρέχει επιπλέον εχέγγυα για το δημόσιο τομέα από ότι τον ιδιωτικό. Ωστόσο, η νέα νομοθεσία για την προστασία προσωπικών δεδομένων προσωπικού παρέχει ένα ασφαλές νομοθετικό πλαίσιο αντιμετώπισης των δύσκολων καταστάσεων. Η στήριξη σε βασικές αρχές επεξεργασίας δεδομένων και ο σεβασμός της αρχής της αναλογικότητας, ωθεί την προστασία των προσωπικών δεδομένων στην αρμονική συνύπαρξη με άλλα συγκρουόμενα αγαθά, ακόμα και σε περιόδους κρίσεως όπως η σημερινή.

ΒΙΒΛΙΟΓΡΑΦΙΑ

ΕΛΛΗΝΙΚΗ

Ακριβοπούλου, Χ. (2011). Η ιδιωτικότητα του προσώπου μέσα από τη συνθετική αντίθεση δημόσιου-ιδιωτικού. *Επιστήμη και Κοινωνία*, τεύχος 26, σ.1-25.

Ακριβοπούλου, Χ. (2012). *Το δικαίωμα στην ιδιωτική ζωή από τη γένεση στη σύγχρονη διαμόρφωση και προστασία του*. Εκδ. Α. Σάκκουλα, Αθήνα.

Αλεξανδροπούλου-Αιγυπτιάδου, Ε. 2007. *Προσωπικά Δεδομένα*. Εκδ. Α. Σάκκουλα, Αθήνα-Κομοτηνή.

Αρμαμέντο, Π. και Β. Σωτηρόπουλο, 2005. Προσωπικά Δεδομένα, ερμηνεία νόμου 2472/1997. Εκδ. Α. Σάκκουλα, Αθήνα.

Αυγουστιανάκη, Μ. Προστασία του ατόμου από την επεξεργασία προσωπικών δεδομένων, ΔτΑ No11/2001.

Βαρβέρης, Α. (2017), «Τεχνικά και οργανωτικά θέματα – η 'υποχρεωτική' τοποθέτηση Υπευθύνου Προστασίας Δεδομένων», *Εφημερίδα Διοικητικού Δικαίου*, 2/2017, σσ. 207-214.

Βενιζέλο, Ε. (1990). *Γενικό συμφέρον και περιορισμοί των συνταγματικών δικαιωμάτων, Κριτική προσέγγιση των τάσεων της νομολογίας*. Εκδόσεις Παρατηρητής, Θεσσαλονίκη.

Βουτσάκη, Β. 2004. Το δικαίωμα στην ιδιωτική ζωή: υποκειμενικές και αντικειμενικές πτυχές, σε Γ. ΠΑπαδημητρίου (επιμ.), *Νέες Τεχνολογίες και συνταγματικά δικαιώματα,* Αθήνα.

Borchardt, K.-D. (2011). Το αλφάβητο του δικαίου της Ευρωπαϊκής Ένωσης. Ευρωπαϊκή Ένωση.

Γκίλη, Α. 2013. Το δικαίωμα στην ιδιωτική ζωή, για το μάθημα των Ατομικών και Κοινωνικών Δικαιωμάτων, Αθήνα. σελ. 8-10.

Δαγτόγλου, Π.Δ. 2005. *Συνταγματικό Δίκαιο, Ατομικά Δικαιώματα* Α', Εκδ. Α. Σάκκουλα, Αθήνα.

Δελλής, Γ. (2017), «Για μια αποτελεσματική δημόσια προστασία των προσωπικών δεδομένων: ο 'θαυμαστός καινούριος κόσμος' του Κανονισμού (ΕΕ) 679/2016», *Εφημερίδα Διοικητικού Δικαίου*, 1/2017, σσ. 2-8.

Δημητρόπουλος, Α. 2005. Συνταγματικό Δίκαιο, Ειδικό μέρος. Παραδόσεις συνταγματικού δικαίου, τόμος ΙΙΙ, τεύχη IV επ. ια' έκδοση, Αθήνα.

Δόνο, Π. (2004). Τεχνολογική διακινδύνευση και προστασία προσωπικών δεδομένων, σε: Νέες τεχνολογίες και συνταγματικά δικαιώματα, Αθήνα-Θεσσαλονίκη.

Δούκα, Β. (2011). Η προστασία των προσωπικών δεδομένων στη σχέση εργασίας. Εκδόσεις Σάκκουλα, Αθήνα.

Δουκίδης, Γ.Ι. (επιμ.)(2019). Το Ψηφιακό Μέλλον. Εκδόσεις Ι. Σιδέρη, Αθήνα.

Evans, A. and Martin, K. 2018. *Εισαγωγή στην Πληροφορική* (2η έκδοση). Εκδ. Κριτική, Αθήνα.

Fawcett, T. and Provost, F. (2019). *Η επιστήμη των δεδομένων για επιχειρήσεις*. Εκδόσεις Κλειδάριθμος, Αθήνα.

Ζερμιώτη, Κ. Δημόσια Πρόσωπα και προστασία της προσωπικότητας (δημόσια πρόσωπα). Διπλωματική Εργασία, ΕΚΠΑ, ΝΟΠΕ, τμήμα Νομικής, Αθήνα, 2012.

Ηλιάδου, Α.Ν. (2016*).* Η συνταγματική προστασία των δεδομένων προσωπικού χαρακτήρα, σε: Λεωνίδα Κοτσαλή (επιμ.), Προσωπικά Δεδομένα: Ανάλυση-Σχόλια-Εφαρμογή, Εκδόσεις Νομική Βιβλιοθήκη, Αθήνα.

Ιγγλεζάκη, Ι. 2014. Ευαίσθητα Προσωπικά Δεδομένα. Εκδ. Α. Σάκκουλα, Αθήνα.

Ιγγλεζάκης, Ι. (2018α), «Ο υπεύθυνος προστασίας δεδομένων κατά τον Κανονισμό 2016/679 και την Οδηγία 2016/680», *Συνήγορος*, 125/2018, σσ. 66-69.

Ιγγλεζάκης, Ι. (2018β), *Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (Κανονισμός 2016/679).* Αθήνα: Interactive Books.

Καρακώστα, Ι. (2012). Το δίκαιο της προσωπικότητας, *Νομική Βιβλιοθήκη*, Αθήνα, σελ. 35-55.

Κάτος, Β.Α. και Γ.Χ. Στεφανίδης, (2003). *Τεχνικές Κρυπτογραφίας & Κρυπτανάλυσης*, Εκδόσεις ΖΥΓΟΣ, Θεσ/νίκη.

Kidder R, Bloom S, (2001) «Ηθική υγεία» στο «Ηθική των Επιχειρήσεων - αντιμέτωποι με το ζήτημα» The Economist Books, Εκδόσεις Κέρκυρα.

Κοτσαλής, Λ. (Επιμ.) 2016. Προσωπικά Δεδομένα - Ανάλυση - Σχόλια - Εφαρμογή. Νομική Βιβλιοθήκη.

Κουκιάδης, Ι.Δ. (επιμ.), (2008). Η παραδοσιακή προστασία της προσωπικότητας του εργαζομένου, σε: Προστασία Προσωπικότητας, Αθήνα-Θεσσαλονίκη.

Κουκιάδης, Ι. Δ. (2019). *Ο εργαζόμενος ως υποκείμενο προσωπικών δεδομένων, κατά το Γενικό Κανονισμό Προστασίας Δεδομένων*. Εκδ. Σάκκουλα, Αθήνα.

Κριάρη-Κατράνη, Ι. (1999). *Γενετική Τεχνολογία και θεμελιώδη δικαιώματα*. Εκδόσεις Σάκκουλα, Αθήνα - Θεσσαλονίκη.

Κυριαζόγλου, Ι. 2019. *Προστασία Προσωπικών Δεδομένων*. Εκδόσεις FYLATOS-PUBLISHING.

Λαδάς, Δ.Ν. (2018). Το δικαίωμα της Προσωπικότητας του Εργαζόμενου: Συμβολή στο Δίκαιο της εκμετάλλευσης. Νομική Βιβλιοθήκη.

Λαζακίδου, Α. (2019). Ηλεκτρονική Διακυβέρνηση & Ηλεκτρονικές Υπηρεσίες προς πολίτες και επιχειρήσεις. Εκδόσεις Δίσιγμα, Αθήνα.

Λαζαράκος, Γ. (2016), «Ο θεσμός του υπεύθυνου προστασίας προσωπικών δεδομένων (Data Protection Officer) στο νέο νομοθετικό πλαίσιο των προσωπικών δεδομένων μετά την υιοθέτηση του Κανονισμού (ΕΕ) 679/2016», *Εφαρμογές Δημοσίου Δικαίου*, ΙΙΙ/2016, σσ. 243-252.

Λεμπέση, Δ. (2018α), «Γενικός Ευρωπαϊκός Κανονισμός για την προστασία προσωπικών δεδομένων (ΕΕ 2016/679) – Κατάργηση της Οδηγίας 95/46/ΕΚ – Συγκριτική μελέτη», *Δελτίο Εργατικής Νομοθεσίας*, 74(1732), σσ. 498-527.

Λεμπέση, Δ. (2018β), «Γενικός Ευρωπαϊκός Κανονισμός για την προστασία προσωπικών δεδομένων (ΕΕ 2016/679) – Κατάργηση της Οδηγίας 95/46/ΕΚ – Συγκριτική μελέτη», *Δελτίο Εργατικής Νομοθεσίας*, 74(1733), σσ. 595-626.

Μαλαγαρδή,Α.Κ. (2010). *Νέες τεχνολογίες-προσωπικά δεδομένα και εργατικό δίκαιο*. Εκδόσεις Αντ. Ν. Σάκκουλα, Αθήνα-Κομοτηνή.

Μάνεσης, Α. (1978). Συνταγματικά Δικαιώματα, Πανεπιστημιακές Παραδόσεις, Εκδ. Οίκος Α. Σάκκουλα, Θεσ/νίκη.

Μανιτάκη, Α. (1994). *Κράτος δικαίου και δικαστικός έλεγχος της συνταγματικότητας*. Εκδόσεις Σάκκουλα, Θεσσαλονίκη.

Μαυριά, Κ. 1982. *Το συνταγματικό δίκαιο του ιδιωτικού βίου*. Εκδ. Α. Σάκκουλα, Αθήνα.

Μήτρου, Λ. (2001). Προστασία Προσωπικών Δεδομένων: ένα νέο δικαίωμα; Στο έργο Δ. Τσάτσου - Εθ. Βενιζέλου - Ξ. Κοντιάδη (επιμ.), *Το νέο Σύνταγμα* - Πρακτικά συνεδρίου για το αναθεωρημένο Σύνταγμα του 1975/1986/2001, Αθήνα- Κομοτηνή.

Μήτρου, Λ. (2017). Ιδιωτικότητα, προσωπικά δεδομένα και εργασιακές σχέσεις. *Επιθεώρησις Εργατικού Δικαίου*, τόμος 76, τεύχος 2, σελ. 140-155.

Μυλώση, Μ. (2018), «Ο Ευρωπαϊκός Κανονισμός Προστασίας Δεδομένων (ΕΕ) 2016/679 και οι αλλαγές που επιφέρει στην οργάνωση και τη λειτουργία της Δημόσιας Διοίκησης», *9ο Πανελλήνιο Συνέδριο Ε.Ε.Ν.Ε.-ΘΕΜΙΣ: Προσωπικά δεδομένα & δικηγορία. Μια νέα πραγματικότητα-ένα νέο κεφάλαιο στο νομικό κόσμο*. Ιωάννινα, 11-12 Μαΐου.

Νίκας, Χ. και Χριστοδούλου, Δ. (2012). *Η Διεθνής Οικονομική στην Εποχή της Παγκοσμιοποίησης*. Εκδόσεις Επίκεντρο, Αθήνα.

Παναγοπούλου-Κουτνατζή, Φ. (2017). Ο Γενικός Κανονισμός για την προστασία των Δεδομένων 679/2016/ΕΕ. Εκδ. Οίκος Α. Σάκκουλα, Αθήνα-Θεσ/νίκη.

Παναγοπούλου, Γ. (2018), «Εποπτεία και επιβολή της τήρησης του ΓΚΠΔ», *Επιμορφωτικό πρόγραμμα του Περιφερειακού Ινστιτούτου Επιμόρφωσης Θεσσαλονίκης: Γενικός Κανονισμός*

Προστασίας Δεδομένων – Οι υποχρεώσεις της Δημόσιας Διοίκησης. Θεσσαλονίκη, Μάιος 2018.

Πλατής, Ε. (2018). *Προσωπικά Δεδομένα, προστασία GDPR*. Εκδ. Παπαδόπουλος, Αθήνα.

Σαρίπολος, ΝΤ. (1874). *Πραγματεία του Συνταγματικού Δικαίου.* Αθήνα: Τυπογραφείο Μιχαήλ Ν. Αγγελίδη.

ΣΕΒ (2018). *Ο νέος Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR*). Στέγη της Ελληνικής Βιομηχανίας, Αθήνα.

Σιουγλέ, Ε. (2018), «Δικαιώματα των υποκειμένων των δεδομένων», *Επιμορφωτικό πρόγραμμα του Περιφερειακού Ινστιτούτου Επιμόρφωσης Θεσσαλονίκης: Γενικός Κανονισμός Προστασίας Δεδομένων – Οι υποχρεώσεις της Δημόσιας Διοίκησης*. Θεσσαλονίκη, Μάιος 2018.

Σπυρόπουλος, Φ. Κοντιάδης, Ξ. Ανθόπουλος, Χ. Γεραπετρίτης, Γ. (2017). Σύνταγμα:Κατ' άρθρο ερμηνεία. Εκδ. Α. Σάκκουλας, Αθήνα.

Σπηλιοπούλου, Π. (2019). Προστασία και Αξιοποίηση Προσωπικών Δεδομένων από τον Δημόσιο τομέα. Παρουσίαση στο ΕΕΛΛΑΚ, Οργανισμός Ανοιχτών Τεχνολογιών, www.gfoss.eu.

Σπηλιωτόπουλο, Ε.Π. (2011). *Εγχειρίδιο Διοικητικού Δικαίου* – Τόμος 1. Εκδόσεις Νομική Βιβλιοθήκη, Αθήνα.

Σταθόπουλος, Μ. (2000). Η χρήση προσωπικών δεδομένων και η διαπάλη μεταξύ ελευθεριών των κατόχων τους και ελευθεριών των υποκείμενων. ΝοΒ, σ.1.

Σωτηρόπουλος, Β. (2017), *Υπεύθυνος Προστασίας Δεδομένων*. Αθήνα – Θεσσαλονίκη: Α. Σάκκουλας.

Τάχο, Α.Ι. (2008). Ελληνικό Διοικητικό Δίκαιο, 9η έκδοση, Εκδόσεις Σάκκουλα, Αθήνα-Θεσσαλονίκη.

Τσεβά, Α.Δ. (2010). Προσωπικά δεδομένα και μέσα ενημέρωσης, Εκδόσεις Αντ. Ν. Σάκκουλα, Αθήνα-Κομοτηνή.

Χρυσόγονος, Κ. (2017). Ατομικά και κοινωνικά δικαιώματα (4η έκδοση). Νομική Βιβλιοθήκη.

Χρυσόγονο, Κ.Χ. και Βλαχόπουλο Σ.Β. (2017). Ατομικά και Κοινωνικά Δικαιώματα, 4η αναθεωρημένη έκδοση, Εκδόσεις Νομική Βιβλιοθήκη, Αθήνα.

ΞΕΝΗ

Ariès, Ph. (1973). 'The Family and the City in the Old World and the New', στο V. Tutte & B. Meyerhoff,(επιμ.), *Changing Images of the Family*, Harmondsworth: Penguin.

Garson, DG 2004, 'The Promise of Digital Government, in A Pavlichev and GD Garson (eds.), Digital Government: Principles and Best Practises, Idea Group Publishing, Hershey, pp. 2-15.

Habermas, J. (1991). *The Structural Transformation of the Public Sphere: An Inquiry into the Category of Bourgeois Society.* Cambridge: MIT Press.

Hareven, T.K. (1991). 'The Home and the Family in Historical Perspective', *Social Research,* 58: 253-285.

Jenero K. A, Mapes-Riordan L. D. (1992) "Electronic Monitoring of Employees and the elusive right to privacy" Employee Relations L.J. Vol.18, No.1, Summer 1992, Aspen Publishers Inc, USA.

Kahn, D. (1996). *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*, Scribner.

Lane F. S. (2003) "The naked employee: How technology is compromising workplace privacy" – AMACOM books, NY, USA.

Lytras, M., Raghavan, V., & Damiani, E. (2017). Cognitive computing and big data analytics research: From metaphors to value space for collective wisdom in human decision making and smart machines. *International Journal on Semantic Web and Information Systems, 13*(1), 1–10.

Meyer-Spacks, P. (2003). *Privacy, Concealing the Eighteenth-Century Self.* Chicago & London: The University of Chicago Press.

Mitrou L. and Karyda M., (2006). Employees'privacy vs. employers' security: can they bebalanced?. *Telematics and Informatics*, Vol. 23 Issue 2006.

Pardo, TA 2000, 'Realizing the Promise of Digital Government: It's More Than Building A Website', Information Magazine Impacts, viewed 21 July 2009, from .

Rodota, S. 2004. Privacy, Freedom and Dignity - Closing Remarks at the 26th International Conference on Privacy and Personal Data Protection.

Rybczynski, W. (1987). *Home: A short history of an idea.* New York: Penguin.

Seifert, JW and Petersen, RE 2002, 'The Promise of All Thing E?: Expectations and Challenges of Emergent Electronic Government', Perspectives on Global Development and Technology, vol. 1, issue 2, pp. 193-212.

Sivarajah, U., Kamal, M. M., Irani, Z., & Weerakkody, V. (2017). Critical analysis of big data challenges and analytical methods. *Journal of Business Research, 70*, 263–286.

Solove, D. (2002). ‘Conceptualizing Privacy’, *California Law Review*. 90:1087-1155.

Solove, D. 2006. A Taxonomy of Privacy, University of Penn Law Review, Vol.154, No 3, pp. 479-564.

Stone, L. (1991). ‘The Public and Private Stately Homes of England, 1500-1990’, *Social Research,* 58:227-265.

Tynan D. (2005) “Computer Privacy Annoyances” - O’Reilly, USA.

Warren, S.D. and Brandeis, L.D. (1890). The Right to Privacy, 5 (4*) Harvard Law Review*, p. 193.

Westin, A. 1967. Privacy and Freedom, 1st edition, New York.

Winstanley D, Woodall J, Heery E, (1996) “Business ethics and human resource management” – Personnel Review Vol.25 No.6 MCB University Press, UK

Winstanley D, Woodall J, (2000) “The ethical dimension of human resource management” – Human Resource Management Journal Vol.10 No2, UK

WP250, W. (2017). Guidelines on Personal data breach notification under Regulation 2016/670.

Zeldin, Th. (1996). *An Intimate History of Humanity*. London: Minerva.