



ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΣΤΗ ΔΗΜΟΣΙΑ ΔΙΟΙΚΗΣΗ

Διπλωματική Εργασία

**Η ΠΑΡΟΥΣΙΑΣΗ ΤΟΥ ΓΕΝΙΚΟΥ ΚΑΝΟΝΙΣΜΟΥ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ
ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ (ΕΕ) 2016/679 ΚΑΙ Η
ΕΦΑΡΜΟΓΗ ΤΟΥ ΣΤΗ ΔΗΜΟΣΙΑ ΔΙΟΙΚΗΣΗ**

της

ΕΛΙΣΑΒΕΤ ΧΡΙΣΤΟΔΟΥΛΙΔΟΥ

Υποβλήθηκε ως απαιτούμενο για την απόκτηση του μεταπτυχιακού διπλώματος
ειδίκευσης στη Δημόσια Διοίκηση

Ιανουάριος 2019

ΕΥΧΑΡΙΣΤΙΕΣ

Η παρούσα διπλωματική εργασία εκπονήθηκε στα πλαίσια του μεταπτυχιακού προγράμματος Δημόσιας Διοίκησης του τμήματος Οργάνωσης και Διοίκησης Επιχειρήσεων του Πανεπιστημίου Μακεδονίας. Ευχαριστώ θερμά όλους όσους συνέβαλαν στην εκπόνησή της και ιδιαίτερα τον επιβλέποντα καθηγητή μου, κ. Ιωάννη Τζιώνα, για την πολύτιμη βοήθειά του.

Θεσσαλονίκη, Ιανουάριος 2019

Χριστοδουλίδου Ελισάβετ

ΠΕΡΙΛΗΨΗ

Αντικείμενο της παρούσας μελέτης αποτελεί η προστασία δεδομένων προσωπικού χαρακτήρα στην ελληνική Δημόσια Διοίκηση μετά την θέσπιση του Γενικού Κανονισμού Προστασίας Δεδομένων ΕΕ 2016/679, που τέθηκε σε ισχύ τον Μάιο του 2018. Η διαχείριση τεράστιου όγκου δεδομένων από τους δημόσιους φορείς, σε συνάρτηση με τις νέες τεχνολογικές δυνατότητες, αποτελούν εν δυνάμει σύγχρονη απειλή για την ιδιωτικότητα και την ασφάλεια των προσωπικών δεδομένων των πολιτών. Η εφαρμογή του νέου Κανονισμού αναμένεται να αντιμετωπίσει αυτό τον κίνδυνο και να συμβάλει στην αποτελεσματικότερη και νομιμότερη επεξεργασία των προσωπικών δεδομένων. Αρχικά παρουσιάζεται μια ιστορική αναδρομή του δικαίου προστασίας δεδομένων προσωπικού χαρακτήρα, με αναφορά του σημαντικότερου ελληνικού και ενωσιακού νομοθετικού πλαισίου. Στη συνέχεια ακολουθεί η παρουσίαση του Κανονισμού, οι καινοτομίες που αυτός εισάγει σε σύγκριση με το προγενέστερο δίκαιο, όπως επίσης και η εν δυνάμει εφαρμογή του από τη Δημόσια Διοίκηση. Προκειμένου να διαπιστωθεί ο βαθμός συμμόρφωσης του δημόσιου τομέα και ο βαθμός ενσωμάτωσης του Κανονισμού έως σήμερα, διενεργήθηκε έρευνα στα Υπουργεία της χώρας, η οποία κατέδειξε την περιορισμένη αντίδραση στο νέο νομοθέτημα. Τέλος, αναφέρονται τα συμπεράσματα και οι προτάσεις προκειμένου να επιτευχθεί ο στόχος της εναρμόνισης της ελεύθερης κυκλοφορίας προσωπικών δεδομένων εντός της Ένωσης, με το υψηλό επίπεδο προστασίας των δεδομένων αυτών.

(Λέξεις κλειδιά: δεδομένα προσωπικού χαρακτήρα, Γενικός Κανονισμός Προστασίας Δεδομένων Προσωπικού χαρακτήρα, Δημόσια Διοίκηση).

ABSTRACT

The subject of this study is the protection of personal data in the Greek Public Administration following the adoption of the General Data Protection Regulation EU 2016/679, which entered into force in May 2018. The management of a huge volume of data by public bodies, in relation to new technological possibilities, is a potential modern threat to the privacy and security of citizens' personal data. Implementation of the new Regulation is expected to address this risk and contribute to more effective and legitimate processing of personal data. Initially, a historical review of the personal data protection law is presented, with reference to the most important Greek and EU legal frameworks. Then follows the presentation of the Regulation, the innovations it introduces compared to the previous law, as well as its potential application by the Public Administration. In order to determine the degree of compliance of the public sector and the degree of incorporation of the Regulation to date, an investigation was carried out at the Ministries of the country, which demonstrated the limited response to the new legislation. Finally, the conclusions and proposals are set out in order to achieve the objective of harmonizing the free movement of personal data within the Union, with a high level of protection for such data.

(Key words: personal data, General Data Protection Regulation, Public Administration).

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

<i>ΕΥΧΑΡΙΣΤΙΕΣ</i>	<i>ii</i>
<i>ΠΕΡΙΛΗΨΗ</i>	<i>iii</i>
<i>ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ</i>	<i>v</i>
<i>ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ</i>	<i>vi</i>
<i>1. Εισαγωγή</i>	<i>1</i>
<i>2. Ιστορική αναδρομή δικαίου προστασίας δεδομένων προσωπικού χαρακτήρα</i>	<i>3</i>
2.1. Νομοθετήματα «πρώτης, δεύτερης και τρίτης γενιάς»	3
2.2. Οδηγία 95/46/ΕΚ	7
2.3.Ελληνικό Νομοθετικό πλαίσιο	9
2.4.Νόμος 2472/1997	13
2.5.Διάρθρωση του Ν.2472/97: Βασικές έννοιες	17
2.6. Σύγχρονο Ενωσιακό Νομοθετικό Πλαίσιο Προστασίας Προσωπικών Δεδομένων	25
<i>3. Παρουσίαση Γενικού Κανονισμού για την προστασία Προσωπικών Δεδομένων</i>	<i>28</i>
3.1. Πρόλογος	28
3.2. Δικαιολογητικός λόγος θέσπισης του Κανονισμού	29
3.3. Παρουσίαση ΓΚΠΔ: Βασικές Αρχές Προστασίας – Δικαιώματα των Υποκειμένων	32
<i>4. Καινοτομίες που εφαρμόζονται σε ιδιωτικό και δημόσιο τομέα</i>	<i>35</i>
4.1. Νέα εργαλεία συμμόρφωσης με τον ΓΚΠΔ	35
4.2. Νέες Αρχές που εισάγει ο ΓΚΠΔ	41
4.3. Νέο πλαίσιο δικαιωμάτων που εισάγει ο ΓΚΠΔ	41
<i>5. Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων και Δημόσια Διοίκηση</i>	<i>49</i>
5.1. Καινοτομίες που αφορούν τη Δημόσια Διοίκηση	49
5.2. Υπεύθυνος Προστασίας Δεδομένων (Data Protection Officer)	51
5.3. Εφαρμογή ΓΚΠΔ στη Δημόσια Διοίκηση	59
5.4. Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ)	65
5.5. Συμμόρφωση της Δημόσιας Διοίκησης με τον ΓΚΠΔ	68
5.6. Βήματα προετοιμασίας του Δημοσίου Τομέα για τον ΓΚΠΔ	70
5.7. Αποτελέσματα έρευνας για την συμμόρφωση του Δημοσίου Τομέα στον ΓΚΠΔ	75
<i>6. Νομολογία που αφορά τον ΓΚΠΔ</i>	<i>79</i>
<i>7. Ο υπό ψήφιση Νόμος για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα σε εφαρμογή του ΓΚΠΔ και την ενσωμάτωση της Οδηγίας 2016/680/ΕΕ (ΣχΝΠΔΠΧ)</i>	<i>82</i>
<i>8. Προτάσεις για την ορθή εφαρμογή του ΓΚΠΔ στη Δημόσια Διοίκηση</i>	<i>85</i>
<i>9. Συμπεράσματα - Προβληματισμοί</i>	<i>88</i>
<i>10. Επίλογος</i>	<i>93</i>
<i>ΒΙΒΛΙΟΓΡΑΦΙΑ – ΑΡΘΡΟΓΡΑΦΙΑ</i>	<i>96</i>
<i>ΗΛΕΚΤΡΟΝΙΚΕΣ ΠΗΓΕΣ</i>	<i>101</i>
<i>ΠΑΡΑΡΤΗΜΑ</i>	<i>102</i>

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

Α.Α.	Ανεξάρτητη Αρχή
Α.Κ.	Αστικός Κώδικας
ανωτ.	ανωτέρω
Α.Π.	Άρειος Πάγος
Α.Π.Δ.Π.Χ.	Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
αρ.	αριθμός
άρθ.	άρθρο
Αρχή	Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
βλ.	βλέπε
Γ.Κ.Π.Δ.	Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων
γνμ.	γνωμοδότηση
Δ.Ε.Ε.	Δικαστήριο της Ευρωπαϊκής Ένωσης
ΔΕφΑθ	Διοικητικό Εφετείο Αθηνών
Δ.Ε.Ν.	Δελτίο Εργατικής Νομοθεσίας
Ε.Α.Α.	Εθνική Αναλογιστική Αρχή
εδ.	εδάφιο
Ε.Δ.Δ.Α.	Ευρωπαϊκό Δικαστήριο Δικαιωμάτων του Ανθρώπου
Ε.Ε.	Ευρωπαϊκή Ένωση
Ε.Ε.Δ.Α.	Ευρωπαϊκή Επιτροπή Δικαιωμάτων του Ανθρώπου
Ε.Ε.Π.Δ.	Ευρωπαϊός Επόπτης Προστασίας Δεδομένων
εκδ.	έκδοση
Ε.Ο.Π.Υ.Υ.	Εθνικός Οργανισμός Παροχής Υπηρεσιών Υγείας
Ε.Ο.Χ.	Ευρωπαϊκός Οικονομικός Χώρος
επόμε.	επόμενα
επιμ.	επιμέλεια
Ε.Σ.Δ.Α.	Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου
Ε.Σ.Π.Δ.	Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων
Ε.ΣΥ.Δ.	Εθνικό Σύστημα Διαπίστευσης
ΕφΑθ	Εφετείο Αθηνών
Ε.Φ.Κ.Α.	Ενιαίος Φορέας Κοινωνικής Ασφάλισης
Η.ΔΙ.Κ.Α.	Ηλεκτρονική Διακυβέρνηση Κοινωνικής Ασφάλισης
κ.ά.	και άλλα

N./ν.	νόμος
N.Π.Δ.Δ.	Νομικό Πρόσωπο Δημοσίου Δικαίου
N.Π.Ι.Δ.	Νομικό Πρόσωπο Ιδιωτικού Δικαίου
N.Σ.Κ.	Νομικό Συμβούλιο του Κράτους
O.Η.Ε.	Οργανισμός Ηνωμένων Εθνών
O.O.Σ.Α.	Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης
παρ.	παράγραφος
Π.Δ.	Προεδρικό Διάταγμα
περ.	περίπτωση
π.χ.	παραδείγματος χάριν
σελ.	σελίδα
Σ.	Σύνταγμα
Σ.Δ.Ο.Ε.	Σώμα Δίωξης Οικονομικού Εγκλήματος
Σ.Ε.Ε.	Συνθήκη για την Ευρωπαϊκή Ένωση
Σ.Λ.Ε.Ε.	Συνθήκη για τη Λειτουργία της Ευρωπαϊκής Ένωσης
ΣτΕ	Συμβούλιο της Επικρατείας
ΣυνθΕΚ	Συνθήκη Ιδρύσεως της Ευρωπαϊκής Κοινότητας
ΣχΝΠΔΠΧ	Σχέδιο Νόμου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
Τ.Π.Δ.Υ.	Ταμείο Προνοίας Δημοσίων Υπαλλήλων
Τ.Π.Ε.	Τεχνολογίες Πληροφοριών και Επικοινωνιών
υπ' αρ.	υπ' αριθμόν
Υ.Π.Δ.	Υπεύθυνος Προστασίας Δεδομένων
Χ.Θ.Δ.Ε.Ε.	Χάρτης Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης

1. Εισαγωγή

Η ραγδαία ανάπτυξη του διαδικτύου και η ψηφιακή τεχνολογία οδήγησαν στη δημιουργία νέων δεδομένων επικοινωνίας, καθιστώντας την ανταλλαγή πληροφοριών ιδιαίτερα εύκολη και γρήγορη. Τα ηλεκτρονικά δίκτυα όμως δεν αποτελούν αποκλειστικά και μόνον μέσα επικοινωνίας, αλλά και μέσα επεξεργασίας των διακινούμενων πληροφοριών, καθιστώντας την χρήση τους επικίνδυνη για την ιδιωτικότητα των ατόμων¹.

Η δυνατότητα πρόσβασης σε κάθε είδους πληροφορία εξυπηρετεί τις ανάγκες του σύγχρονου ανθρώπου όσον αφορά τη γρήγορη και εύκολη ανεύρεση δεδομένων, ελλοχεύουν όμως πολλοί κίνδυνοι από τη συλλογή και επεξεργασία των προσωπικών δεδομένων των φυσικών προσώπων², όπως για παράδειγμα η χειραγώγηση και η ακούσια «εργαλειοποίηση», κυρίως του χρήστη κοινωνικής δικτύωσης, του οποίου τα δεδομένα πωλούνται ως συναλλακτικά αγαθά σε εταιρίες διαχείρισης δεδομένων, προς εξυπηρέτηση αλλότριων συμφερόντων³.

Στην Εισηγητική Έκθεση του Ν.2472/1997 (Βουλή των Ελλήνων, 1996) γίνεται αναφορά στο μέγεθος των αλλαγών που επέφερε η κοινωνία της πληροφορίας, στην ανατροπή των κλασικών μεθόδων επικοινωνίας, διαχείρισης και ελέγχου σε δημόσιο και ιδιωτικό τομέα, όπως επίσης στον εκσυγχρονισμό της Δημόσιας Διοίκησης μέσω των πληροφοριακών συστημάτων. Ειδικότερα, επισημαίνεται η αλλαγή των παραδοσιακών μεθόδων συλλογής και χρήσης της πληροφορίας, καθόσον η χρήση των νέων τεχνολογιών⁴ επιτρέπει τη δημιουργία μιας «εικόνας» της προσωπικότητας των ανθρώπων, η οποία τους καθιστά «ελέγξιμους» και «χειραγωγήσιμους».

Σύμφωνα μάλιστα με την Οδηγία (ΕΕ) 2016/680⁵ «Οι ταχείες τεχνολογικές εξελίξεις και η παγκοσμιοποίηση έχουν δημιουργήσει νέες προκλήσεις για την προστασία των

¹ Βλ. Κ. Αρκουλή, Προστασία προσωπικών δεδομένων στις ηλεκτρονικές επικοινωνίες (2010), πρόλογος.

² Βλ. Α. Ψαροπούλου, Προστασία δεδομένων προσωπικού χαρακτήρα (2018), εισαγωγή.

³ Βλ. εισήγηση Φ. Παναγοπούλου-Κουτνατζή, Το νέο πλαίσιο δικαιωμάτων, σε: Α. Κοτσαλή/Κ. Μενουδάκο (επιμ.), Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων GDPR (2018), σελ.17. Χαρακτηριστικό παράδειγμα συλλογής προσωπικών δεδομένων πολιτών αποτελεί η εταιρία Calino ΑΕ, που είχε καταχωρημένα στοιχεία από 5.500.000 κατοίκους και 900.000 επιχειρήσεις χωρίς να έχει ενημερώσει τα υποκείμενα για τη συλλογή και επεξεργασία των δεδομένων τους, Απόφαση 83/2009 ΑΠΔΠΧ.

⁴ Παραδείγματα νέων τεχνολογιών αποτελούν τα νέα ψηφιακά εργαλεία (όπως οι μηχανές αναζήτησης), η εξέλιξη των πληροφοριακών συστημάτων και των τεχνολογιών επικοινωνιών (όπως το υπολογιστικό σύννεφο) και οι υπηρεσίες κοινωνικής δικτύωσης (ενδεικτικό παράδειγμα το facebook).

⁵ Βλ. αιτιολογική σκέψη 3 της Οδηγίας (ΕΕ) 2016/680.

προσωπικών δεδομένων. Η κλίμακα συλλογής και ανταλλαγής δεδομένων προσωπικού χαρακτήρα έχει αυξηθεί σημαντικά».

Ο Δημόσιος τομέας αντίστοιχα αξιοποιεί τις νέες τεχνολογίες για την ανάπτυξη εφαρμογών ηλεκτρονικής διακυβέρνησης και την προώθηση της συμμετοχικής δημοκρατίας, προκειμένου να εξυπηρετήσει τις ανάγκες της Δημόσιας Διοίκησης και γενικότερα όλων των φορέων δημόσιας εξουσίας, μέσω του συστηματικού σχεδιασμού των υπηρεσιών του⁶.

Συνεπώς η προστασία της ιδιωτικότητας αδιαμφισβήτητα αποτελεί βασικό διακύβευμα του 21^{ου} αιώνα, που καλείται να εξασφαλίσει η σύγχρονη νομοθεσία.

⁶ Βλ. Χ. Γεραρή, *Τα προσωπικά δεδομένα και οι νέες προκλήσεις (2010)*, σελ. 42-43.

2. Ιστορική αναδρομή δικαίου προστασίας δεδομένων προσωπικού χαρακτήρα

Το δίκαιο της προστασίας προσωπικών δεδομένων έχει ως αντικείμενο την προστασία του ατόμου από τους κινδύνους που προκαλεί η επεξεργασία των δεδομένων που το αφορούν⁷. Η προστασία των προσωπικών δεδομένων ή άλλως, το δικαίωμα πληροφοριακού αυτοκαθορισμού, αποτελεί ένα σχετικά νέο δικαίωμα, που οι απαρχές του εντοπίζονται μεν στη δεκαετία του 1980, η κατοχύρωσή του όμως επήλθε με την Οδηγία 95/46/EK⁸.

Πρόδρομοι των πρώτων εθνικών νομοθετημάτων προστασίας των προσωπικών δεδομένων και πιο συγκεκριμένα του δικαιώματος στην ιδιωτική ζωή, υπήρξαν η Οικουμενική Διακήρυξη των Δικαιωμάτων του Ανθρώπου του Οργανισμού Ηνωμένων Εθνών (ΟΗΕ) της 10^{ης} Δεκεμβρίου 1948 και η Ευρωπαϊκή Σύμβαση για την Προάσπιση των Δικαιωμάτων του Ανθρώπου και των Θεμελιωδών Ελευθεριών (ΕΣΔΑ) της 4^{ης} Νοεμβρίου 1950, όπου κατοχυρώνεται ο σεβασμός της ιδιωτικής και οικογενειακής ζωής, της κατοικίας και της αλληλογραφίας. Σύμφωνα με την παράγραφο 1 του άρθρου 8 της ΕΣΔΑ «Παν πρόσωπον δικαιούται εις τον σεβασμόν της ιδιωτικής και οικογενειακής ζωής του, της κατοικίας του και της αλληλογραφίας του». Στο ίδιο άρθρο απαγορεύεται η επέμβαση δημόσιας αρχής στην άσκηση του δικαιώματος τούτου, εκτός αν προβλέπεται από το νόμο και αποτελεί μέτρο αναγκαίο, κυρίως για την εθνική ή δημόσια ασφάλεια.

Από τη δεκαετία του 1970 εμφανίστηκε για πρώτη φορά στη νομοθεσία των ευρωπαϊκών χωρών και των ΗΠΑ το δικαίωμα προστασίας των προσωπικών δεδομένων, ως εξειδίκευση του δικαιώματος στην ιδιωτική ζωή⁹.

2.1. Νομοθετήματα «πρώτης, δεύτερης και τρίτης γενιάς»

Τα νομοθετήματα που αφορούν τα προσωπικά δεδομένα και την προστασία τους, διαχωρίζονται σε «πρώτης», «δεύτερης» και «τρίτης» γενιάς¹⁰. Το πρώτο πρωτοποριακό νομοθέτημα παγκοσμίως προήλθε από το ομόσπονδο γερμανικό

⁷ Βλ. *Ι. Γγγλεζάκη, Ευαίσθητα Προσωπικά Δεδομένα (2004), σελ.47.*

⁸ Βλ. *εισήγηση Σ. Βλαχόπουλου, Πρόσβαση στα Δημόσια Έγγραφα, σε: Α.Κοτσαλή/Κ. Μενουδάκο (επιμ.), όπ.ανωτ. (2018), σελ.41-42.*

⁹ Βλ. *Α. Κοτσαλή/Κ. Μενουδάκο (2018), όπ.ανωτ., εισαγωγή.*

¹⁰ Βλ. *Ε. Αλεξανδροπούλου-Αιγυπτιάδου, Προσωπικά Δεδομένα (2016), σελ.197.*

κρατίδιο της Έσσης το 1970¹¹, ενώ ακολούθησαν και άλλα Ευρωπαϊκά κράτη όπως η Σουηδία, η Αυστρία, η Γαλλία κ.ά. και οι ΗΠΑ, με τον ομοσπονδιακό νόμο Privacy Act¹² περί ιδιωτικότητας το 1974. Την ίδια περίοδο δραστηριοποιήθηκε σε διεθνές επίπεδο και ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ) το 1980, που εξέδωσε κατευθυντήριες γραμμές¹³ για την προστασία των προσωπικών δεδομένων, με έμφαση τις διασυνοριακές ροές πληροφοριών. Αν και οι «γραμμές» του ΟΟΣΑ δεν συνιστούν νομικά δεσμευτικές αρχές, θεωρούνται ένα καλό παράδειγμα καθιέρωσης ενός είδους διεθνούς εθίμου αντιμετώπισης των προβλημάτων που ανέκυπταν κυρίως από τη διεθνή ανταλλαγή δεδομένων¹⁴. Αιτία της εμφάνισης αυτών των νομοθετημάτων ήταν η διαπίστωση του κινδύνου παραβίασης της ιδιωτικής ζωής λόγω της τεχνολογικής ανάπτυξης και η ανάγκη αντιμετώπισης του κινδύνου αυτού. Οι νόμοι της πρώτης γενιάς αντικατοπτρίζουν το φόβο του νομοθέτη προς κάθε μορφή επεξεργασίας προσωπικών στοιχείων, γεγονός που οδήγησε αφενός σε αυστηρό, προληπτικό και κατασταλτικό έλεγχο και αφετέρου σε πρόβλεψη εξοντωτικών κυρώσεων.

Τα νομοθετήματα δεύτερης γενιάς εμφανίστηκαν τη δεκαετία του 1980 και αντιμετώπισαν θετικά πλέον την επιστήμη της Πληροφορικής, η οποία θα μπορούσε να αποτελέσει σύμμαχο στην ανάπτυξη¹⁵. Ο προβληματισμός εκείνης της περιόδου αφορούσε τη σύγκρουση του δικαιώματος προστασίας της ιδιωτικής ζωής με το δικαίωμα ελευθερίας της έκφρασης, ο οποίος οδήγησε στη Σύμβαση 108 της 28^{ης} Ιανουαρίου 1981¹⁶ του Συμβουλίου της Ευρώπης «για την προστασία των ατόμων από την αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων» (Σύμβαση του Στρασβούργου). Η Σύμβαση αυτή αποτελεί κείμενο σταθμό, διότι αποτελεί την πρώτη νομικά δεσμευτική διεθνή συνθήκη στον τομέα της προστασίας των

¹¹ Το οποίο οδήγησε στην ψήφιση του ομοσπονδιακού νόμου BDSG (*Bundesdatenschutzgesetz*) το 1977, βλ. Β. Σωτηρόπουλο, *Η Συνταγματική Προστασία των Προσωπικών Δεδομένων* (2006), σελ. 12.

¹² Ο οποίος συμπλήρωσε τον *Freedom of Information Act* του 1967 και αναγνώρισε ρητά το δικαίωμα του ατόμου για προστασία από την ηλεκτρονική επεξεργασία των πληροφοριών, βλ. Α. Γέροντα, *Η προστασία του πολίτη από την ηλεκτρονική επεξεργασία προσωπικών δεδομένων* (2002), σελ. 149.

¹³ «Αρχές που διέπουν την προστασία της προσωπικής σφαίρας του ανθρώπου και τις διασυνοριακές ροές προσωπικών στοιχείων»: συνοπτικά είναι η αρχή της περιορισμένης συγκέντρωσης και συλλογής των δεδομένων, η αρχή της ποιότητας των στοιχείων, η αρχή του προσδιορισμένου σκοπού, η αρχή της περιορισμένης χρήσης των προσωπικών στοιχείων, η αρχή των μέτρων ασφαλείας των προσωπικών δεδομένων, η αρχή της διαφάνειας, η αρχή της συμμετοχής και η αρχή της υπευθυνότητας, βλ. Α. Γέροντα (2002), *όπ.ανωτ.*, σελ. 78-79.

¹⁴ Βλ. Α. Γέροντα (2002), *όπ.ανωτ.*, σελ. 103 επόμε.

¹⁵ Βλ. Α. Γέροντα (2002), *όπ.ανωτ.*, σελ. 69 επόμε.

¹⁶ Βλ. διαδικτυακό σύνδεσμο: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108>.

προσωπικών δεδομένων, καίτοι στερούνταν αμέσου εφαρμογής¹⁷. Η σημαντικότητά της επαληθεύεται από το γεγονός ότι η 28^η Ιανουαρίου έχει ανακηρυχθεί από το Συμβούλιο της Ευρώπης ως ημέρα προστασίας προσωπικών δεδομένων.

Στα νομοθετήματα δεύτερης γενιάς ανήκει τόσο η Συμφωνία Σένγκεν¹⁸, που υπεγράφη στις 14 Ιουνίου 1985¹⁹, η οποία δημιούργησε κοινή βάση εθνικών δεδομένων μεταξύ των κρατών-μελών και είχε ως στόχο την καθιέρωση της ελεύθερης κυκλοφορίας των υπηκόων των κρατών που την υπέγραψαν, καθώς και την αστυνομική και δικαστική συνεργασία, όσο και οι «Κατευθυντήριες Αρχές για την προστασία προσωπικών δεδομένων σε αυτοματοποιημένα αρχεία» του ΟΗΕ.

Η πρώτη χαρακτηριστική περίπτωση όπου ανέκυψαν προβληματισμοί για την προστασία του πολίτη από την απεριόριστη συλλογή, επεξεργασία και καταχώρηση σε αρχεία προσωπικών πληροφοριών, ήταν αυτή της απογραφής του πληθυσμού της Ομοσπονδιακής Δημοκρατίας της Γερμανίας, την οποία προέβλεπε ομοσπονδιακός νόμος, που δημοσιεύτηκε στις 25 Μαρτίου 1982. Το νομοθέτημα αυτό προκάλεσε θύελλα αντιδράσεων στη Γερμανία, καθόσον επισημάνθηκαν οι κίνδυνοι της κρατικής κατοχής προσωπικών πληροφοριών, όπως το ονοματεπώνυμο, η ακριβής διεύθυνση, ο αριθμός τηλεφώνου, η ημερομηνία γέννησης, η οικογενειακή κατάσταση, το θρησκευτικό δόγμα, το επάγγελμα, η μόρφωση κ.ά. Μάλιστα στο νομοθέτημα υπήρχε πρόβλεψη για δυνατότητα αξιοποίησης των πληροφοριών και ανταλλαγής τους μεταξύ των κρατικών αρχών, ρυθμίσεις που επέτειναν τη δυσπιστία των πολιτών απέναντι στον τρόπο που ο κρατικός μηχανισμός αξιοποιούσε τη νέα τεχνολογία. Εν τέλει, η απογραφή που είχε οριστεί για τις 27 Απριλίου 1983 ματαιώθηκε βάσει της από 15.12.1983 απόφασης του Ομοσπονδιακού Συνταγματικού Δικαστηρίου της Γερμανίας, η οποία έκρινε ως αντισυνταγματικές ορισμένες διατάξεις του νομοθετήματος, επικαλούμενη το δικαίωμα της πληροφοριακής αυτοδιάθεσης ή του πληροφοριακού αυτοκαθορισμού. Το δικαίωμα αυτό αποτελεί εξειδίκευση του δικαιώματος ανάπτυξης της προσωπικότητας και δίνει τη δυνατότητα στον πολίτη να αποφασίζει ο ίδιος σχετικά με την αποκάλυψη και τη χρήση των

¹⁷ Η Ελλάδα κύρωσε τη Σύμβαση με το Ν.2068/1992, ενώ αρκετές χώρες όπως η Μ.Βρετανία, η Ιρλανδία, το Βέλγιο, η Ισπανία και η Πορτογαλία προηγήθηκαν, ψηφίζοντας κατά τη δεκαετία του 1980 ειδικούς νόμους για την προστασία των προσωπικών δεδομένων.

¹⁸ Βλ. ηλεκτρονική πηγή: <https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=LEGISUM%3A133020>.

¹⁹ Η οποία κυρώθηκε στην Ελλάδα με το Ν.2514/1997.

προσωπικών του στοιχείων, όπως επίσης να συμπροσδιορίζει πότε και υπό ποιες προϋποθέσεις είναι δυνατή η επεξεργασία των πληροφοριών που τον αφορούν²⁰.

Τέλος, η τρίτη γενιά νομοθετημάτων που εμφανίστηκαν τη δεκαετία του 1990 και ισχύουν ως σήμερα, αντανakλά την ανάγκη αντιμετώπισης από την Ευρωπαϊκή Ένωση (ΕΕ) των ραγδαίων τεχνολογικών εξελίξεων. Τα νομοθετήματα τρίτης γενιάς περιλαμβάνουν ενδεικτικά:

1) το άρθρο 8 του Χάρτη Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (ΧΘΔΕΕ), όπου διακηρύσσονται οι βασικές αρχές προστασίας, κατοχυρώνεται η νομιμότητα της επεξεργασίας των δεδομένων και τα δικαιώματα πρόσβασης και διόρθωσης, ενώ ταυτόχρονα προβλέπεται και η δημιουργία της ανεξάρτητης αρχής²¹ (Ευρωπαϊκή Ένωση, 2010),

2) το άρθρο 8 παράγραφος 1 ΕΣΔΑ, πρώην άρθρο 286 της Συνθήκης Ιδρύσεως της Ευρωπαϊκής Κοινότητας (ΣυνθΕΚ) και μετέπειτα 16 παράγραφος 1 της Συνθήκης της Λισαβόνας²² που τέθηκε σε ισχύ την 1^η Δεκεμβρίου 2009,

3) τις Οδηγίες 95/46/ΕΚ «για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών», 2002/58/ΕΚ «σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών» και τις επόμενες τροποποιητικές 2006/24/ΕΚ²³, 2009/136/ΕΚ²⁴ και την 2016/680/ΕΕ «σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τις αρμόδιες αρχές για την πρόληψη, διερεύνηση, διαπίστωση ή δίωξη ποινικών αδικημάτων ή την εκτέλεση ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία

²⁰ Βλ. Ι. Γγλιεζάκη (2004), *όπ.ανωτ.*, σελ.51.

²¹ Άρθ. 8 ΧΘΔΕΕ: «1.Κάθε πρόσωπο έχει δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν. 2.Η επεξεργασία αυτών των δεδομένων πρέπει να γίνεται νομίμως, για καθορισμένους σκοπούς και με βάση τη συγκατάθεση του ενδιαφερομένου ή για άλλους θεμιτούς λόγους που προβλέπονται από το νόμο. Κάθε πρόσωπο έχει δικαίωμα να έχει πρόσβαση στα συλλεγμένα δεδομένα που το αφορούν και να επιτυγχάνει τη διόρθωσή τους. 3.Ο σεβασμός των κανόνων αυτών υπόκειται στον έλεγχο ανεξάρτητης αρχής...»).

²² Άρθ. 16 παρ.1 Συνθήκης Λισαβόνας: «Κάθε πρόσωπο έχει δικαίωμα προστασίας των δεδομένων προσωπικού χαρακτήρα που το αφορούν», διαθέσιμο στο: https://www.ecb.europa.eu/ecb/legal/pdf/c_32620121026el.pdf.

²³ «Για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών και για την τροποποίηση της Οδηγίας 2002/58/ΕΚ».

²⁴ «Για την τροποποίηση της Οδηγίας 2002/22/ΕΚ για την καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών, της Οδηγίας 2002/58/ΕΚ σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και του Κανονισμού 2006/2004...».

των δεδομένων αυτών και για την κατάργηση της απόφασης πλαισίου 2008/977/ΔΕΥ του Συμβουλίου»,

4) τους Κανονισμούς 45/2001/ΕΚ «σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα όργανα και τους οργανισμούς της Κοινότητας και σχετικά με την ελεύθερη κυκλοφορία των δεδομένων αυτών» και (ΕΕ) 2016/679 (Γενικός Κανονισμός για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα, εφεξής ΓΚΠΔ).

Στην τρίτη γενιά νομοθεσιών ανήκουν και οι εθνικές νομοθεσίες των κρατών-μελών της ΕΕ, που θεσπίζουν διαδικαστικές εγγυήσεις προστασίας των δεδομένων, οι οποίες, είτε αναθεωρήθηκαν, είτε θεσπίστηκαν για πρώτη φορά, προκειμένου να εναρμονιστούν με τις Οδηγίες 95/46/ΕΚ και 2002/58/ΕΚ²⁵. Άξια αναφοράς είναι η εξαίρεση που εισάγει η διάταξη της παραγράφου 1 του άρθρου 15 της Οδηγίας 2002/58/ΕΚ, με την οποία παρέχεται η δυνατότητα στα κράτη-μέλη της ΕΕ να λαμβάνουν νομοθετικά μέτρα, με τα οποία θα περιορίζεται το απόρρητο των επικοινωνιών και των προσωπικών δεδομένων των χρηστών των τηλεπικοινωνιακών υπηρεσιών, στις περιπτώσεις που ο περιορισμός αυτός συνιστά αναγκαίο μέτρο για τη διαφύλαξη, μεταξύ άλλων, της εθνικής ασφάλειας και της εθνικής άμυνας²⁶.

Παρατηρείται λοιπόν μία εξέλιξη στο θεσμικό πλαίσιο της προστασίας των προσωπικών δεδομένων, καθόσον αυτά δεν αντιμετωπίζονται πλέον υπό το πρίσμα της ιδιωτικότητας, αλλά ως αυτοτελές ατομικό δικαίωμα, που προστατεύεται με ισχυρές διατάξεις και με εγγυήσεις για αποτελεσματική αντιμετώπιση των παραβιάσεων²⁷.

2.2. Οδηγία 95/46/ΕΚ

Όπως είναι γνωστό, οι Οδηγίες αποτελούν νομικές πράξεις της ΕΕ οι οποίες απαιτούν από τα κράτη-μέλη να επιτύχουν ένα συγκεκριμένο αποτέλεσμα, αφήνοντάς τους τη διακριτική ευχέρεια να επιλέξουν τον τρόπο επίτευξης του αποτελέσματος αυτού. Συνεπώς τα κράτη-μέλη οφείλουν να λαμβάνουν μέτρα ώστε να ενσωματώνουν,

²⁵ Βλ. Β. Σωτηρόπουλο (2006), *όπ.ανωτ.*, σελ.33.

²⁶ Βλ. Θ. Σιδηρόπουλο, *Το δίκαιο του διαδικτύου* (2003), σελ.206-207.

²⁷ Βλ. Κ. Μενουδάκο εισαγωγή σε: Α. Κοτσαλή/Κ. Μενουδάκο (επιμ.), *όπ.ανωτ.* (2018).

εντός της προβλεπόμενης προθεσμίας, τις Οδηγίες στο εθνικό τους δίκαιο, προκειμένου να επιτύχουν τους στόχους που αυτές ορίζουν²⁸.

Η Οδηγία 95/46/ΕΚ²⁹ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24^{ης} Οκτωβρίου 1995, αποτελεί σημαντική νομοθεσία της ΕΕ για την προστασία του ατόμου από την επεξεργασία των προσωπικών του δεδομένων. Αναγκαία προϋπόθεση της επιδιωκόμενης ελεύθερης κυκλοφορίας αγαθών, κεφαλαίων, υπηρεσιών και προσώπων εντός της ΕΕ σε ένα περιβάλλον τεχνολογικής «έκρηξης», ήταν η εναρμόνιση των νομοθεσιών των κρατών-μελών. Αυτό θα ήταν το πρώτο βήμα, ώστε να εξασφαλιστεί η προστασία των ατόμων από την επεξεργασία των δεδομένων τους, αλλά ταυτόχρονα να επιτευχθεί και η ελεύθερη κυκλοφορία των δεδομένων με ασφάλεια εντός του εδάφους της Κοινότητας. Συνεπώς η Οδηγία αποσκοπούσε στην εναρμόνιση των εθνικών νομοθεσιών, ώστε να διασφαλιστεί υψηλό επίπεδο προστασίας των πολιτών, ελεύθερη κυκλοφορία των δεδομένων και αποτελεσματική λειτουργία της εσωτερικής αγοράς. Ταυτόχρονα, η Οδηγία παρείχε στον εθνικό νομοθέτη περιθώρια ανάπτυξης πρωτοβουλιών ενόψει των εθνικών ιδιομορφιών³⁰.

Μάλιστα, οι εθνικές ανεξάρτητες εποπτικές αρχές, όπως η ΑΠΔΠΧ για την Ελλάδα, είναι απόρροια της Οδηγίας 95/46/ΕΚ, που τις καθιέρωσε προκειμένου να διαπιστώνουν τη συμμόρφωση προς την εθνική νομοθεσία ενσωμάτωσης³¹.

Η εφαρμογή της Οδηγίας ήταν υποχρεωτική για όλα τα κράτη-μέλη της ΕΕ και του Ευρωπαϊκού Οικονομικού Χώρου (ΕΟΧ)³², αφορούσε όμως την προστασία των δεδομένων μόνο στον τομέα της εσωτερικής αγοράς. Τα θέματα αστυνομικής ή δικαστικής συνεργασίας σε ποινικές υποθέσεις, όπως τα εγκλήματα στον Κυβερνοχώρο ή η καταπολέμηση της τρομοκρατίας³³ και του διασυνοριακού εγκλήματος, καλύπτονται από άλλο νομικό πλαίσιο³⁴.

²⁸ Ηλεκτρονική πηγή: https://ec.europa.eu/info/law/law-making-process/types-eu-law_el.

²⁹ Αντικαταστάθηκε με τον ΓΚΠΔ από 25-5-2018.

³⁰ Βλ. Ε. Αλεξανδροπούλου-Αιγυπτιάδου, *Ζητήματα από το Δίκαιο Πληροφορικής*, 2002, σελ.52.

³¹ Βλ. Ε. Αλεξανδροπούλου-Αιγυπτιάδου (2016), *όπ.ανωτ.*, σελ.208.

³² Ο ΕΟΧ δημιουργήθηκε το 1994 για να επεκτείνει την ισχύ των διατάξεων της ΕΕ για την εσωτερική αγορά της στις χώρες της Ευρωπαϊκής Ζώνης Ελεύθερων Συναλλαγών (ΕΖΕΣ).

³³ Για το φαινόμενο της τρομοκρατίας και τους κινδύνους που ενέχει για τους δημοκρατικούς θεσμούς βλ. Ζ. Καρδασιάδου, *Δημόσια ασφάλεια και προστασία των προσωπικών δεδομένων (2010)*, περί προληπτικής δράσης του κράτους και χρήσης της ερμηνευτικής αρχής «εν αμφιβολία υπέρ της ασφάλειας».

³⁴ Βλ. Ε. Αλεξανδροπούλου-Αιγυπτιάδου (2016), *όπ.ανωτ.*, σελ.208. Ενδεικτικά η Σύμβαση 108/1981 και η Σύσταση του Συμβουλίου της Ευρώπης για τον αστυνομικό τομέα.

Η Ομάδα προστασίας των προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα του άρθρου 29 της Οδηγίας 95/46/ΕΚ³⁵ ασκεί συμβουλευτικό έργο, εκδίδοντας γνωμοδοτήσεις πάνω σε σημαντικά ζητήματα και κυρίως για την προστασία δεδομένων σε χώρες εκτός ΕΕ³⁶. Με τον ΓΚΠΔ³⁷ η Ομάδα του άρθρου 29 μετεξελίχθηκε στο Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων, όργανο της ΕΕ με νομική προσωπικότητα.

Τα κράτη-μέλη, σύμφωνα με την παράγραφο 1 του άρθρου 32 της Οδηγίας, είχαν τριετή προθεσμία να προσαρμόσουν τη νομοθεσία τους, ήτοι έως τον Οκτώβριο του 1998 και για το λόγο αυτό η Ελλάδα θέσπισε το Ν.2472/1997, που αναλύεται παρακάτω και με τις διατάξεις του οποίου ενσωματώθηκε η Οδηγία 95/46/ΕΚ στην ελληνική έννομη τάξη.

2.3.Ελληνικό Νομοθετικό πλαίσιο

Το συνταγματικό πλαίσιο προστασίας της ιδιωτικής ζωής και των προσωπικών δεδομένων στην ελληνική επικράτεια περιέχεται στις διατάξεις που αφορούν τα ατομικά δικαιώματα και, ειδικότερα, εντάσσεται στο κανονιστικό υποσύνολο του πληροφοριακού Συντάγματος³⁸.

Ειδικότερα, με την παράγραφο 1 του άρθρου 2 του Συντάγματος³⁹ κατοχυρώνεται η αρχή του σεβασμού και της προστασίας της ανθρώπινης αξίας, με την παράγραφο 1 του άρθρου 5⁴⁰ προβλέπεται το δικαίωμα της ελεύθερης ανάπτυξης της προσωπικότητας και της συμμετοχής στην κοινωνική-οικονομική-πολιτική ζωή της

³⁵ Βλ. ηλεκτρονική πηγή: <http://ec.europa.eu/newsroom/article29/news> «Η Ομάδα Εργασίας του άρθ.29 είναι μια συμβουλευτική ομάδα, η οποία συγκροτείται από εκπροσώπους των αρχών προστασίας των δεδομένων των κρατών-μελών, ενεργεί ανεξάρτητα και είναι επιφορτισμένη, μεταξύ άλλων, με την εξέταση κάθε ζητήματος το οποίο αφορά την εφαρμογή των εθνικών μέτρων που θεσπίστηκαν βάσει της Οδηγίας 95/46/ΕΚ, προκειμένου να συμβάλει στην ομοιόμορφη εφαρμογή των μέτρων αυτών», βλ. εισήγηση Δ. Ζωγραφόπουλου, Ο ΓΚΠΔ και οι εργασιακές σχέσεις, σε: Α. Κοτσαλή/Κ. Μενουδάκο (2018), όπ.ανωτ., σελ.145.

³⁶ Βλ. Π. Αρμαμέντο/Β. Σωτηρόπουλο, Προσωπικά Δεδομένα - Ερμηνεία Ν.2472/1997(2005), πρόλογος.

³⁷ Άρθρα 68 επόμε. ΓΚΠΔ.

³⁸ Βλ. Β. Σωτηρόπουλο (2006), όπ.ανωτ., σελ.1. Το ελληνικό συνταγματικό κείμενο, μετά την αναθεώρηση του 2001, επιτρέπει τη θεματική συστηματοποίηση επιμέρους διατάξεων που αναφέρονται στο αγαθό της πληροφορίας. Ο όρος «κοινωνία της πληροφορίας» που εμφανίστηκε για πρώτη φορά το 1993 στη Λευκή Βίβλο της Ευρωπαϊκής Επιτροπής για την ανάπτυξη, την ανταγωνιστικότητα και την απασχόληση, συναντάται ρητά στο ελληνικό Σύνταγμα.

³⁹ «Ο σεβασμός και η προστασία της αξίας του ανθρώπου αποτελούν την πρωταρχική υποχρέωση της Πολιτείας».

⁴⁰ «Καθένας έχει δικαίωμα να αναπτύσσει ελεύθερα την προσωπικότητά του και να συμμετέχει στην κοινωνική, οικονομική και πολιτική ζωή της Χώρας, εφόσον δεν προσβάλλει τα δικαιώματα των άλλων και δεν παραβιάζει το Σύνταγμα ή τα χρηστά ήθη».

χώρας, με την παράγραφο 1 του άρθρου 9 εδάφια α και β⁴¹ θεμελιώνεται το άσυλο της κατοικίας και το απαραβίαστο της οικογενειακής και ιδιωτικής ζωής, ενώ με το άρθρο 19⁴² κατοχυρώνεται το απόρρητο της επικοινωνίας.

Οι παραπάνω συνταγματικές διατάξεις, σύμφωνα με την Εισηγητική Έκθεση του Ν.2472/1997, «ανάγουν την προστασία της αξίας του ανθρώπου σε πρωταρχική υποχρέωση της πολιτείας, προστατεύουν την ελεύθερη ανάπτυξη της προσωπικότητάς του και διασφαλίζουν την ιδιωτική και οικογενειακή του ζωή, καθώς και το απόρρητο των επικοινωνιών του».

Με τη Συνταγματική αναθεώρηση του 2001 (Ψήφισμα της 6.4.2001) προστέθηκε το άρθρο 5Α⁴³ περί του δικαιώματος στην ελεύθερη πληροφόρηση και της συμμετοχής στην κοινωνία της πληροφορίας. Η ρητή διασφάλιση όμως της προστασίας των προσωπικών δεδομένων και μάλιστα από ανεξάρτητη αρχή (άρθρο 101Α⁴⁴), η οποία αποτελεί επιπλέον θεσμική εγγύηση που εξασφαλίζει την αποτελεσματικότερη προστασία, επήλθε με το άρθρο 9Α⁴⁵, το οποίο συνταγματοποίησε την προστασία των προσωπικών δεδομένων.

Με τη διάταξη αυτή καταδεικνύεται η πρόθεση του νομοθέτη να προσαρμοστεί στις εξελίξεις της σύγχρονης τεχνολογίας, ενώ ταυτόχρονα καθιερώνεται ένα αμυντικό

⁴¹ «Η κατοικία του καθενός είναι άσυλο. Η ιδιωτική και οικογενειακή ζωή του ατόμου είναι απαραβίαστη».

⁴² «1. Το απόρρητο των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο είναι απόλυτα απαραβίαστο. Νόμος ορίζει τις εγγυήσεις υπό τις οποίες η δικαστική αρχή δεν δεσμεύεται από το απόρρητο για λόγους εθνικής ασφάλειας ή για διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων. **2. Νόμος ορίζει τα σχετικά με τη συγκρότηση, τη λειτουργία και τις αρμοδιότητες ανεξάρτητης αρχής που διασφαλίζει το απόρρητο της παραγράφου 1. **3. Απαγορεύεται η χρήση αποδεικτικών μέσων που έχουν αποκτηθεί κατά παράβαση του άρθρου αυτού και των άρθρων 9 και 9Α».

⁴³ «1. Καθένας έχει δικαίωμα στην πληροφόρηση όπως νόμος ορίζει. Περιορισμοί στο δικαίωμα αυτό είναι δυνατόν να επιβληθούν με νόμο μόνο εφόσον είναι απολύτως αναγκαίοι και δικαιολογούνται για λόγους εθνικής ασφάλειας, καταπολέμησης του εγκλήματος ή προστασίας δικαιωμάτων και συμφερόντων τρίτων. 2. Καθένας έχει δικαίωμα συμμετοχής στην Κοινωνία της Πληροφορίας. Η διευκόλυνση της πρόσβασης στις πληροφορίες που διακινούνται ηλεκτρονικά, καθώς και της παραγωγής, ανταλλαγής και διάδοσής τους αποτελεί υποχρέωση του Κράτους, τηρουμένων πάντοτε των εγγυήσεων των άρθρων 9, 9Α και 19».

⁴⁴ «1. Όπου από το Σύνταγμα προβλέπεται η συγκρότηση και η λειτουργία ανεξάρτητης αρχής, τα μέλη της διορίζονται με ορισμένη θητεία και διέπονται από προσωπική και λειτουργική ανεξαρτησία, όπως νόμος ορίζει. 2. Νόμος ορίζει τα σχετικά με την επιλογή και την υπηρεσιακή κατάσταση του επιστημονικού και λοιπού προσωπικού της υπηρεσίας που οργανώνεται για την υποστήριξη της λειτουργίας κάθε ανεξάρτητης αρχής. Τα πρόσωπα που στελεχώνουν τις ανεξάρτητες αρχές πρέπει να έχουν τα ανάλογα προσόντα, όπως νόμος ορίζει. Η επιλογή τους γίνεται με απόφαση της Διάσκεψης των προέδρων της Βουλής και με επιδίωξη ομοφωνίας ή πάντως με την αυξημένη πλειοψηφία των τεσσάρων πέμπτων των μελών της. Τα σχετικά με τη διαδικασία επιλογής ορίζονται από τον Κανονισμό της Βουλής. 3. Με τον Κανονισμό της Βουλής ρυθμίζονται όλα αφορούν τη σχέση των ανεξάρτητων αρχών με τη Βουλή και ο τρόπος άσκησης του κοινοβουλευτικού ελέγχου».

⁴⁵ «Καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα των προσωπικών του δεδομένων, όπως νόμος ορίζει. Η προστασία των προσωπικών δεδομένων διασφαλίζεται από ανεξάρτητη αρχή, που συγκροτείται και λειτουργεί όπως νόμος ορίζει».

δικαίωμα κατά των επεμβάσεων στις θεμελιώδεις ελευθερίες και κυρίως στο δικαίωμα της ιδιωτικής ζωής. Δεν περιορίζεται στην προστασία του ιδιωτικού βίου, αλλά καλύπτει το φάσμα της αθέμιτης συλλογής, επεξεργασίας και χρήσης προσωπικών δεδομένων με συμβατικό ή ηλεκτρονικό τρόπο. Μάλιστα αναπτύσσει ισχύ και στις σχέσεις μεταξύ ιδιωτών⁴⁶.

Εκτός από τις συνταγματικές ρυθμίσεις, η προστασία της ανθρώπινης αξιοπρέπειας προβλέπεται και στο αστικό δίκαιο. Το άρθρο 57 του Αστικού Κώδικα (ΑΚ) αποτελεί εξαιρετικά ευρεία και πρωτοποριακή διάταξη που προστατεύει το δικαίωμα της προσωπικότητας, στο οποίο συμπεριλαμβάνονται, μεταξύ άλλων, η αξιοπρέπεια, τα προσωπικά δεδομένα και το απόρρητο⁴⁷.

Όσον αφορά τις υποχρεώσεις της χώρας έναντι της ΕΕ βάσει των Οδηγιών 95/46/ΕΚ και 2002/58/ΕΚ, ο κοινός νομοθέτης προέβη σε ρυθμίσεις προκειμένου να ενισχύσει το ελληνικό νομοθετικό πλαίσιο για την προστασία των προσωπικών δεδομένων. Η συνταγματική προστασία και οι γενικές διατάξεις του ιδιωτικού δικαίου, εντάσσονται σε ένα γενικό θεσμικό πλαίσιο και δεν παρέχουν τα εχέγγυα ενός εξειδικευμένου τομεακού νομοθετήματος, ικανού να παρακολουθήσει την αλματώδη εξέλιξη της τεχνολογίας. Οι επί μέρους νόμοι που αφορούν την προστασία των προσωπικών δεδομένων στην Ελληνική επικράτεια είναι κυρίως οι κάτωθι:

Ο **N.2068/1992** αφορά την «Κύρωση της Ευρωπαϊκής Σύμβασης για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία πληροφοριών προσωπικού χαρακτήρα».

Ο **N.2251/1994** περί προστασίας των καταναλωτών και προάσπισης των δικαιωμάτων τους, ο οποίος αναφέρει στην παράγραφο 6 του άρθρου 4 ότι η χρησιμοποίηση των τεχνικών επικοινωνίας από τον προμηθευτή πρέπει να γίνεται κατά τέτοιο τρόπο, ώστε να μην προσβάλλεται η ιδιωτική ζωή του καταναλωτή.

Ο **N.2472/1997** «για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα» δημοσιεύτηκε στις 10-4-1997. Ενσωμάτωσε στην ελληνική έννομη τάξη την Οδηγία 95/46/ΕΚ και αποτελεί το βασικότερο νομοθέτημα στο πλαίσιο της προστασίας των προσωπικών δεδομένων. Αναφέρει στην Αιτιολογική του Έκθεση⁴⁸ ότι στις τεχνολογικά προηγμένες κοινωνίες θεωρείται αυτονόητο πως για να προστατευθεί το άτομο από την πληροφορική, δεν αρκούν οι γενικές διατάξεις

⁴⁶ Βλ. *I. Γγγλεζάκη (2004), όπ.ανωτ., σελ.57-58.*

⁴⁷ Βλ. *Κ. Αρκουλή (2010), όπ.ανωτ., σελ.23.*

⁴⁸ *ΚΝοΒ 1997 σελ 501.*

για την προστασία της προσωπικότητας, αλλά επιβάλλεται η ύπαρξη ειδικών ρυθμίσεων που να διασφαλίζουν τον φιλελεύθερο και δικαιοκρατικό χαρακτήρα της τεχνολογικής ανάπτυξης. Η θέσπιση ειδικών κανόνων για τη συλλογή και επεξεργασία των δεδομένων προσωπικού χαρακτήρα είναι υποχρεωτική για τον Έλληνα νομοθέτη, κατά τις συνταγματικές διατάξεις που προαναφέρθηκαν ανωτέρω. Ο Ν.2472/1997 καταργήθηκε με τον ΓΚΠΔ (ΕΕ) 2016/679.

Συμπληρωματικά, ο Ν.3471/2006⁴⁹ για «την προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του Ν.2472/1997», ρυθμίζει την προστασία χρηστών και συνδρομητών υπηρεσιών ηλεκτρονικών επικοινωνιών έναντι προσβολών των προσωπικών τους δεδομένων και ενσωματώνει στην ελληνική έννομη τάξη την ευρωπαϊκή Οδηγία 2002/58/ΕΚ⁵⁰. Σύμφωνα με την Αρκουλή (2010), ο νόμος αυτός ήρθε ως απόρροια της ανάγκης σαφούς οριοθέτησης της προστασίας της ιδιωτικής ζωής στο ψηφιακό περιβάλλον, η οποία, ως πρότινος, έβρισκε έρεισμα σε διάσπαρτες διατάξεις και στη γενική ρήτρα του άρθρου 57 ΑΚ, περί προστασίας της προσωπικότητας. Η προστασία του απορρήτου της ηλεκτρονικής επικοινωνίας, δηλαδή η απαγόρευση της ακρόασης, υποκλοπής, αποθήκευσης ή άλλου είδους παρακολούθησης ή επιτήρησης του περιεχομένου των ηλεκτρονικών επικοινωνιών και των εξωτερικών δεδομένων, αποτελεί μια σημαντική ρύθμιση του νόμου.

Με το άρθρο 12 του Ν.3783/2009 για την «Ταυτοποίηση των κατόχων και χρηστών εξοπλισμού και υπηρεσιών κινητής τεχνολογίας και άλλες διατάξεις», τροποποιήθηκε η παράγραφος 2 του άρθρου 3 του Ν.2472/1997.

Ο Ν.3917/2011 «για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις».

Ο Ν.4225/2014 που αφορά την «αναβάθμιση και βελτίωση των μηχανισμών είσπραξης των ασφαλιστικών φορέων, τα πρόστιμα για την ανασφάλιστη και αδήλωτη εργασία και λοιπές διατάξεις αρμοδιότητας Υπουργείου Εργασίας,

⁴⁹ Ο Ν.2774/1999 για την προστασία δεδομένων προσωπικού χαρακτήρα στις τηλεπικοινωνίες καταργήθηκε και αντικαταστάθηκε από το Ν.3471/2006.

⁵⁰ Η οποία τροποποιήθηκε με το Ν.4070/2012 «Ρυθμίσεις ηλεκτρονικών επικοινωνιών, μεταφορών, δημοσίων έργων και άλλες διατάξεις», άρθ.168 επόμε. σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών.

Κοινωνικής Ασφάλισης και Πρόνοιας», προβλέπει στις παραγράφους 1 και 2 του άρθρου 9, ειδικότερες ρυθμίσεις για την Εθνική Αναλογιστική Αρχή (ΕΑΑ) και την Ηλεκτρονική Διακυβέρνηση Κοινωνικής Ασφάλισης Α.Ε. (Η.ΔΙ.Κ.Α. Α.Ε.). Πιο συγκεκριμένα, η ΕΑΑ εξαιρείται από τις διατάξεις του Ν.2472/1997 αναφορικά με τα στοιχεία που συλλέγει και επεξεργάζεται κατά την άσκηση των αρμοδιοτήτων της, ενώ η Η.ΔΙ.Κ.Α. Α.Ε., κατόπιν έγγραφου ή ηλεκτρονικού αιτήματός της και χωρίς να απαιτείται προηγούμενη άδεια από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), υποχρεώνει το Ταμείο Πρόνοιας Δημοσίων Υπαλλήλων (ΤΠΔΥ) να της παρέχει κάθε διαθέσιμη πληροφορία σχετικά με τις καταβληθείσες μηνιαίες εισφορές εκάστου ασφαλισμένου, καθώς και τα μητρώα και στοιχεία ασφαλισμένων που έχει στην κατοχή του.

Ο Ν.4577/2018 δημοσιεύτηκε πρόσφατα και αφορά την ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας 2016/1148/ΕΕ σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφαλείας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση και άλλες διατάξεις. Επίσης νέο νομοθέτημα αποτελεί ο Ν.4579/2018⁵¹ για τα ονομαστικά αρχεία επιβατών στις πτήσεις αεροπλάνων εντός ή εκτός ΕΕ.

Αυτό που διαφαίνεται από τα παραπάνω είναι ότι το πρόβλημα που καλείται να αντιμετωπίσει ο νομοθέτης είναι διττό: αρχικά πρέπει να συνδυάσει την προστασία του ατόμου από την αθέμιτη επεξεργασία πληροφοριών που αφορούν την ιδιωτική του ζωή, με την αποτελεσματική χρήση της πληροφορικής, τόσο από το δημόσιο, όσο και από ιδιώτες, για την επιδίωξη σκοπών που η έννομη τάξη προστατεύει⁵². Ταυτόχρονα πρέπει να εξισορροπήσει τα συγκρουόμενα δικαιώματα αφενός του ατόμου στα προσωπικά του δεδομένα και αφετέρου του πολίτη στην ελεύθερη πληροφόρηση, στην επικοινωνία, στην επιστημονική έρευνα, στην ελευθερία της έκφρασης, του λόγου και του τύπου κ.ά.⁵³.

2.4.Νόμος 2472/1997

Προκειμένου να κατανοήσουμε τον ΓΚΠΔ, θα πρέπει προηγουμένως να αναλύσουμε το Ν.2472/1997, δεδομένου ότι ο Κανονισμός αποτελεί νομοθέτημα που προέκυψε

⁵¹ «Υποχρεώσεις αερομεταφορέων σχετικά με τα αρχεία επιβατών - προσαρμογή της νομοθεσίας στην Οδηγία (ΕΕ) 2016/681 και άλλες διατάξεις».

⁵² Βλ. Εισηγητική Έκθεση Ν.2472/1997 με ημερομηνία 17-6-1996.

⁵³ Βλ. Ε. Αλεξανδροπούλου-Αιγυπτιάδου (2016), *όπ.ανωτ.*, σελ.40.

εξελικτικά και που βασίζεται σε έννοιες και αρχές που περιγράφονται στον ελληνικό νόμο⁵⁴. Σύμφωνα με την εισηγητική έκθεση του νόμου, αυτός θεσπίστηκε αφενός για να ευθυγραμμιστεί με τις προαναφερόμενες συνταγματικές ρυθμίσεις προστασίας της ανθρώπινης αξίας, της ελεύθερης ανάπτυξης της προσωπικότητας και της διασφάλισης της ιδιωτικής και οικογενειακής ζωής και του απορρήτου των επικοινωνιών, και αφετέρου για να υιοθετήσει την Οδηγία 95/46/ΕΚ περί προστασίας των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ελεύθερης κυκλοφορίας των δεδομένων αυτών⁵⁵.

Στην Ελλάδα ο Ν.2472/1997 ρύθμιζε ad hoc την προστασία δεδομένων προσωπικού χαρακτήρα μέχρι την έναρξη ισχύος του ΓΚΠΔ. Έως την ψήφιση του νόμου, δεν υπήρχε νομοθέτημα που να ρυθμίζει επαρκώς και αποτελεσματικά την προστασία του ατόμου από την επεξεργασία των προσωπικών του δεδομένων⁵⁶. Σύμφωνα με το νομοσχέδιο, ο Ν.2472/1997 κλήθηκε να αντιμετωπίσει την ανάγκη συνδυασμού της προστασίας της ιδιωτικής ζωής, με την επεξεργασία προσωπικών δεδομένων για θεμιτούς δημόσιους και ιδιωτικούς σκοπούς. Για το λόγο αυτό διέλαβε ευρύ ορισμό των εννοιών «προσωπικά δεδομένα», «επεξεργασία» και «αρχείο», ώστε να καταλαμβάνεται από το ρυθμιστικό του πεδίο κάθε είδους επεξεργασία, αυτοματοποιημένη ή μη, δημόσια ή ιδιωτική. Επίσης, καθιέρωσε σύστημα γνωστοποίησης κάθε επεξεργασίας και άδειας για μια σειρά επεξεργασιών, καθιέρωσε εγγυήσεις, προέβλεψε αυστηρές κυρώσεις για την προστασία των υποκειμένων από παραβάσεις και ίδρυσε την ανεξάρτητη ΑΠΔΠΧ, προσδίδοντάς της αποφασιστικό ρόλο στο σύστημα προστασίας που ο ίδιος εισήγαγε. Μάλιστα, σύμφωνα με τα όσα αναφέρει ο Κων/νος Μενουδάκος, Πρόεδρος της ΑΠΔΠΧ, η Αρχή θα συνεχίσει να εφαρμόζει το Ν.2472/1997 και μετά τις 25 Μαΐου 2018, στο μέτρο που δεν έρχεται σε αντίθεση με τον ΓΚΠΔ⁵⁷.

Ο Ν.2472/97 αποτελεί συγκερασμό πολλών κλάδων του δικαίου, όπως συνταγματικού, ευρωπαϊκού, αστικού, ιδιωτικού διεθνούς, εμπορικού, εργατικού, διοικητικού, υπαλληλικού, πειθαρχικού και ποινικού⁵⁸. Η επιρροή του στην έννομη τάξη υπήρξε βαθιά και καταλυτική, καθόσον αποτελεί την πρώτη εξειδικευμένη

⁵⁴ Ο Ν.2472/1997 καταργήθηκε από τον ΓΚΠΔ ακολουθώντας την τύχη της Οδηγίας 95/46/ΕΚ.

⁵⁵ Βλ. Α. Γιαννακούλα – Μ. Μηλαπίδου, *Προσωπικά Δεδομένα* (2017), σελ. 4.

⁵⁶ Βλ. Μ. Μυλώση, *Η έννομη προστασία των δεδομένων οικονομικής συμπεριφοράς από την αθέμιτη ηλεκτρονική επεξεργασία τους: συγκριτική μελέτη της νομικής ρύθμισης σε Ελλάδα και Γαλλία* (2015), σελ.135.

⁵⁷ Βλ. *συνέντευξη σε Σ. Κετιτζιάν* (2018), διαθέσιμη στο: <http://www.epixeiro.gr/article/87275>.

⁵⁸ Βλ. Π. Αρμαμέντο – Β. Σωτηρόπουλο (2005), *όπ.ανωτ., πρόλογος*.

καταγραφή διατάξεων αναφορικά με τα προσωπικά δεδομένα και την προστασία τους, δεδομένου ότι η προγενέστερη του νόμου προστασία επιτυγχάνονταν μέσω «περιφερειακών» διατάξεων (είτε συνταγματικού, είτε αστικού δικαίου, είτε ειδικότερων νομοθετικών προβλέψεων περί απορρήτου)⁵⁹.

Βασική αρχή του νόμου⁶⁰, είναι ότι τα συστήματα επεξεργασίας δεδομένων, τα οποία αποτελούν εν δυνάμει απειλή, πρέπει να υπηρετούν τον άνθρωπο και να σέβονται τα δικαιώματά του και την ιδιωτική του ζωή.

Περιέχει κοινές ρυθμίσεις με την κοινοτική Οδηγία 95/46/EK όσον αφορά την επεξεργασία δεδομένων σε ιδιωτικό και δημόσιο τομέα, χωρίς να προβλέπει διαφοροποιημένους κανόνες για τους δύο αυτούς τομείς⁶¹.

Ο Ν.2472/1997 αποτελεί τον κορμό της προστασίας δεδομένων στη χώρα μας και περιέχει κανόνες ουσιαστικούς, οργανωτικούς, διαδικαστικούς και κυρωτικούς, οι οποίοι βοηθούν στην οριοθέτηση της συνταγματικά ανεκτής επεξεργασίας προσωπικών δεδομένων⁶². Σύμφωνα με τον Ιγγλεζάκη (2004), δεδομένης της διαρκώς εντεινόμενης ηλεκτρονικής επεξεργασίας και της ανάπτυξης της πληροφορικής τεχνολογίας στις σύγχρονες κοινωνίες, ο νομοθέτης επεδίωξε τη ρύθμιση της επεξεργασίας των δεδομένων, η οποία αποτελεί σοβαρή πηγή διακινδύνευσης.

Η εν δυνάμει διακινδύνευση οφείλεται στην αυθαίρετη επεξεργασία και αξιοποίηση των προσωπικών δεδομένων, κυρίως για εμπορικούς σκοπούς, εντός ή εκτός των ελληνικών συνόρων.

Αντικείμενο του νόμου αποτελεί η θέσπιση προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα για την προστασία των δικαιωμάτων και των θεμελιωδών ελευθεριών των φυσικών προσώπων και ιδίως της ιδιωτικής ζωής. Πεδίο εφαρμογής του είναι η επεξεργασία που τελείται από υπεύθυνο επεξεργασίας ή εκτελούνται την επεξεργασία που είναι εγκατεστημένος στην Ελλάδα ή σε τόπο όπου εφαρμόζεται το ελληνικό δίκαιο ή που χρησιμοποιεί μέσα επεξεργασίας που βρίσκονται στην Ελληνική Επικράτεια, καίτοι ο ίδιος είναι εγκατεστημένος σε Τρίτη Χώρα, σε προσωπικά δεδομένα που περιλαμβάνονται ή πρόκειται να περιληφθούν σε αρχεία. Ο νόμος δεν εφαρμόζεται⁶³ στις περιπτώσεις που η επεξεργασία εκτελείται

⁵⁹ Βλ. Μ. Μυλώση (2015), *όπ.ανωτ.*, σελ.131.

⁶⁰ Βλ. Α. Ψαροπούλου (2018), *όπ.ανωτ.*, εισαγωγή.

⁶¹ Βλ. Ι. Ιγγλεζάκη (2004), *όπ.ανωτ.*, σελ.64.

⁶² Βλ. Ι. Ιγγλεζάκη (2004), *όπ.ανωτ.*, σελ.48.

⁶³ Αρθ. 3 παρ. 2 Ν.2472/1997.

από φυσικό πρόσωπο για άσκηση προσωπικών ή οικιακών δραστηριοτήτων⁶⁴ αποκλειστικά, όπως για παράδειγμα η τήρηση προσωπικού αρχείου ηλεκτρονικών διευθύνσεων, ούτε σε περιπτώσεις επεξεργασίας, η οποία πραγματοποιείται από δημόσιες αρχές, όπου ορίζει ο νόμος ρητά. Συγκεκριμένα, στις περιπτώσεις που οι δικαστικές ή εισαγγελικές αρχές πραγματοποιούν επεξεργασία δεδομένων στα πλαίσια απονομής της δικαιοσύνης ή για την εξυπηρέτηση των αναγκών της λειτουργίας τους με σκοπό τη βεβαίωση ορισμένων εγκλημάτων⁶⁵, εφαρμόζονται οι ισχύουσες ουσιαστικές και δικονομικές ποινικές διατάξεις. Επίσης, οι διατάξεις του Ν.2472/1997 δεν εφαρμόζονται όταν η επεξεργασία τελείται από δημόσια αρχή με τη λειτουργία τεχνικών μέσων καταγραφής ήχου ή εικόνας με στόχο τη διαφύλαξη της ασφάλειας του κράτους, της άμυνας και της δημόσιας ασφάλειας. Κατά τον Πρόεδρο της ΑΠΔΠΧ Γεραρή (2010), η ανάγκη αντιμετώπισης σύγχρονων πολιτικών εξελίξεων, όπως η διεθνής τρομοκρατία και το διασυνοριακό έγκλημα, οδηγεί στην απαίτηση ενίσχυσης της δημόσιας ασφάλειας. Αυτός ο στόχος μπορεί να επιτευχθεί μέσω εντεινόμενων μέτρων παρακολούθησης των πολιτών, όπως επίσης μέσω προληπτικής συλλογής και επεξεργασίας όλο και περισσότερων προσωπικών δεδομένων. Στην ελληνική έννομη τάξη απαιτείται τυπικός νόμος ή προεδρικό διάταγμα ώστε να θεσπιστούν μέτρα που να περιορίζουν τα ατομικά δικαιώματα υπέρ της δημόσιας ασφάλειας και της εξιχνίασης αξιόποινων πράξεων, όπως για παράδειγμα η εγκατάσταση καμερών σε δημόσιους χώρους ή η δημιουργία εθνικής βάσης γενετικών αποτυπωμάτων (DNA)⁶⁶.

Ιδιαίτερο ενδιαφέρον παρουσιάζει η με αριθμό 2/2013 Γνωμοδότηση της ΑΠΔΠΧ που αφορά τον έλεγχο της νομιμότητας της σκοπούμενης δημοσιοποίησης από δημόσια αρχή, δεδομένων προσωπικού χαρακτήρα οφειλετών φορέων κοινωνικής ασφάλισης στο διαδίκτυο. Κατά την κρίση της Αρχής, η ανάρτηση στο διαδίκτυο προσωπικών δεδομένων φυσικών προσώπων από δημόσια αρχή, που λειτουργεί ως υπεύθυνος επεξεργασίας, πρέπει να προβλέπεται από νόμο που σέβεται τα προστατευόμενα δικαιώματα των άρθρων 7 και 8 της ΕΣΔΑ⁶⁷. Σύμφωνα μάλιστα με

⁶⁴ Βλ. εισήγηση Φ. Παναγοπούλου-Κουτνατζή, *Η προσωπική και οικιακή χρήση των προσωπικών δεδομένων*, σε: Α. Κοτσαλή (επιμ.), *Προσωπικά Δεδομένα* (2016), σελ.71 επόμ.

⁶⁵ Βλ. άρθρ. 3 παρ.2 εδάφ.β' Ν.2472/1997: «...εγκλημάτων που τιμωρούνται ως κακούργηματα ή πλημμελήματα με δόλο και ιδίως εγκλημάτων κατά της ζωής, κατά της γενετήσιας ελευθερίας, της οικονομικής εκμετάλλευσης της γενετήσιας ζωής, κατά της προσωπικής ελευθερίας, κατά της ιδιοκτησίας, κατά των περιουσιακών δικαιωμάτων, παραβάσεων της νομοθεσίας περί ναρκωτικών, επιβουλής της δημόσιας τάξης, ως και τελουμένων σε βάρος ανηλικών θυμάτων».

⁶⁶ Βλ. Γνωμοδοτήσεις ΑΠΔΠΧ με αρ. 1 και 2/2009, διαθέσιμες στον ιστότοπο της Αρχής.

⁶⁷ Μη επιβολή ποινής άνευ νόμου και δικαίωμα σεβασμού της ιδιωτικής και οικογενειακής ζωής.

τη νομολογία του Συμβουλίου της Επικρατείας (ΣτΕ), οι περιορισμοί των συνταγματικά κατοχυρωμένων ατομικών δικαιωμάτων πρέπει, μεταξύ άλλων, να ορίζονται, όπως προαναφέρθηκε ανωτέρω, με τυπικό νόμο ή με διάταγμα που εκδίδεται κατ' εξουσιοδότηση του τυπικού νόμου, να δικαιολογούνται από λόγους δημοσίου συμφέροντος και να περιορίζουν την ευρεία διακριτική ευχέρεια της Διοίκησης, τηρώντας την αρχή της αναλογικότητας, της προσφορότητας και της αναγκαιότητας των μέτρων⁶⁸. Οι κίνδυνοι που προκαλούν οι νέες τεχνολογίες, η παγκοσμιοποιημένη οικονομία και το γενικότερο καθήκον του κράτους να εγγυηθεί τη δημόσια ασφάλεια και τάξη, μπορούν να αντιμετωπιστούν με τις ενδεδειγμένες νομοθετικές πρωτοβουλίες και τις τεχνολογικές εφαρμογές, οι οποίες δε θα περιστέλλουν υπέρμετρα τις ατομικές ελευθερίες των πολιτών⁶⁹.

2.5.Διάρθρωση του Ν.2472/97: Βασικές έννοιες

Ο Ν.2472/1997 περιλαμβάνει 26 άρθρα κατανομημένα σε 6 κεφάλαια⁷⁰, ενώ έχει υποστεί πολλαπλές τροποποιήσεις έως σήμερα⁷¹. Σχετικές Οδηγίες της ΕΕ που μεσολάβησαν από τη δημοσίευση του νόμου, είναι ενδεικτικά η 1999/93/ΕΚ⁷² αναφορικά με το κοινοτικό πλαίσιο για τις ηλεκτρονικές υπογραφές, η 2000/31/ΕΚ⁷³ για το ηλεκτρονικό εμπόριο, η 2001/29/ΕΚ⁷⁴ για την εναρμόνιση του δικαιώματος του δημιουργού και συγγενικών δικαιωμάτων στην κοινωνία της πληροφορίας, η 2003/98/ΕΚ⁷⁵ για την περαιτέρω χρήση πληροφοριών του δημόσιου τομέα κ.ά. Ειδικά με την τελευταία Οδηγία θεσπίζονται κανόνες που διέπουν την χρήση και τις πρακτικές μεθόδους για τη διευκόλυνση της περαιτέρω χρήσης των υφιστάμενων εγγράφων, που βρίσκονται στην κατοχή φορέων του δημόσιου τομέα των κρατών μελών (πρόσβαση στα έγγραφα), ενώ ουδόλως θίγει την προστασία των φυσικών προσώπων έναντι της επεξεργασίας προσωπικών δεδομένων. Επίσης, το Νομικό

⁶⁸ Βλ. Ολομέλεια ΣτΕ 3665/2005, 3037/2008 και 2010/2010 στη ΝΟΜΟΣ.

⁶⁹ Βλ. Χ. Γεραρή (2010), *όπ. ανωτ.*, σελ.44.

⁷⁰ Κεφάλαιο Α' «Γενικές Διατάξεις», Κεφ.Β' «Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα», Κεφ.Γ' «Δικαιώματα του Υποκειμένου των Δεδομένων», Κεφ.Δ' «Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα», Κεφ.Ε' «Κυρώσεις» και Κεφ.ΣΤ' «Τελικές-Μεταβατικές Διατάξεις».

⁷¹ Βλ. Ν.2623/1998, 2703/1999, 2819/2000, 2915/2001, 3051/2002, 3090/2002, 3156/2003.

⁷² Βλ. άρθ. 8 «Προστασία Δεδομένων».

⁷³ Βλ. αιτιολογική σκέψη 14 περί αποκλειστικής εφαρμογής της Οδηγίας 95/46/ΕΚ για την προστασία προσώπων σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

⁷⁴ Βλ. άρθ. 9 περί εφαρμογής διατάξεων για την προστασία των δεδομένων προσωπικού χαρακτήρα και το σεβασμό της προσωπικής ζωής.

⁷⁵ Ηλεκτρονική πηγή: <https://eur-lex.europa.eu/legal-content/EL/ALL/?uri=CELEX%3A32003L0098>.

Συμβούλιο του Κράτους (ΝΣΚ) εξέδωσε Γνωμοδοτήσεις⁷⁶ για την εφαρμογή του Ν.2472/97 στον δημόσιο τομέα.

Ορισμοί⁷⁷

«**Δεδομένα προσωπικού χαρακτήρα ή προσωπικά δεδομένα**»: ο όρος «προσωπικά» (ή ατομικά) υιοθετήθηκε από το Σύνταγμα στο άρθρο 9Α, ενώ στην επιστήμη της πληροφορικής παρατηρείται ευρεία χρήση του όρου «data»⁷⁸, δηλαδή δεδομένα.

Σύμφωνα με την Οδηγία 95/46/EK και το Ν.2472/1997, προσωπικό δεδομένο αποτελεί κάθε πληροφορία που αναφέρεται σε συγκεκριμένο πρόσωπο, όπως το όνομα, η ηλικία του, το επάγγελμά του, η οικογενειακή του κατάσταση κ.ά. Κατά την Αλεξανδροπούλου (2016), «προσωπικό δεδομένο είναι κάθε πληροφορία που αναφέρεται σε συγκεκριμένο πρόσωπο (εν ζωή⁷⁹, φυσικό και όχι νομικό⁸⁰), ανεξαρτήτως πληροφοριακής αξίας και βαρύτητας». Υιοθετήθηκε λοιπόν ένας εξαιρετικά ευρύς ορισμός, καθόσον στην έννοια περιλαμβάνονται όλες οι πληροφορίες (σημαντικές και ασήμαντες) που μπορούν να συσχετιστούν με συγκεκριμένο πρόσωπο⁸¹. Ο ορισμός είναι εσκεμμένα ευρύς, ώστε να προσφέρει αντίστοιχα ευρεία προστασία στο υποκείμενο των δεδομένων, υπόκειται όμως σε περιορισμούς και δεν πρέπει να διευρύνεται υπερβολικά⁸². Συνεπώς, μια πληροφορία που δεν συνδέεται με συγκεκριμένο φυσικό πρόσωπο, ώστε να οδηγήσει στην άμεση⁸³ ή έμμεση⁸⁴ ταυτοποίηση αυτού, δεν αποτελεί προσωπικό δεδομένο⁸⁵. Στην έννοια αυτή δεν εμπίπτουν τα στατιστικής φύσεως συγκεντρωτικά στοιχεία, αφού δεν

⁷⁶ Βλ. ενδεικτικά: Γνωμοδοτήσεις με αρ. 13/2016 για χορήγηση ή μη αντιγράφων, αποσπασμάτων ή πιστοποιητικών από τα ληξιαρχικά βιβλία σε οποιονδήποτε αιτούντα και χωρίς τη δικαιολόγηση έννομου συμφέροντος, 193/2015 περί διόρθωσης στοιχείου στις εγγραφές των δημοτολογίων, 228/2010 για ανάρτηση πινάκων βαθμολογίας σε διαγωνισμό.

⁷⁷ Οι βασικές έννοιες περιλαμβάνονται στο άρθρ. 2 «Ορισμοί» του Ν.2472/1997.

⁷⁸ “Data are to this century what oil was to the last one: a driver of growth and change.[...]It changes the rules for markets and it demands new approaches from regulators”, (Anonymous, Economist 6-5-2017), βλ. Α. Λεμπέση, Γενικός Ευρωπαϊκός Κανονισμός για την προστασία προσωπικών δεδομένων (ΕΕ 2016/679) – Κατάργηση της Οδηγίας 95/46/EK – Συγκριτική μελέτη (2018α), σελ.499.

⁷⁹ Σύμφωνα με την Ομάδα Εργασίας του άρθρ.29, όπου στη Γνωμοδότησή της με αρ. 4/2007 ορίζει ρητά ότι τα δεδομένα αποβιωσάντων δεν αποτελούν προσωπικά δεδομένα.

⁸⁰ Όπως εταιρίες, οργανισμοί, δημόσιοι φορείς.

⁸¹ Βλ. Κ. Αρκουλή (2010), όπ.ανωτ., σελ.3.

⁸² Βλ. Γνωμοδότηση με αρ. 4/2007 της Ομάδας του άρθρ.29 και εισήγηση Φ. Μίτλεττον, Η έννοια των προσωπικών δεδομένων, σε: Α. Κοτσαλής (επιμ.), Προσωπικά Δεδομένα (2016), σελ.8.

⁸³ Όπως για παράδειγμα ο ΑΦΜ, ο ΑΜΚΑ κλπ.

⁸⁴ Όπως η φωτογραφία χωρίς ονοματεπώνυμο ή ακόμα και χωρίς να φαίνεται το πρόσωπο του υποκειμένου, σύμφωνα με την Απόφαση ΕφΑθ 3808/2014.

⁸⁵ Βλ ΑΠ 637/2013: «για να εμπίπτει η πληροφορία στην έννοια του προσωπικού δεδομένου, θα πρέπει να συνδέεται άμεσα με το υποκείμενο και τις προσωπικού χαρακτήρα ιδιότητες ή εκδηλώσεις αυτού».

μπορούν να προσδιορίσουν τα υποκείμενα των δεδομένων⁸⁶, όπως επίσης και τα ανώνυμα ή ανωνυμοποιημένα στοιχεία, ενώ οι αξιολογικές κρίσεις⁸⁷ δεν είναι σαφές εάν εμπίπτουν ή όχι στον ορισμό. Τα προσωπικά δεδομένα αποτελούν στοιχεία της προσωπικότητας του φυσικού προσώπου, το οποίο μπορεί να προσδιοριστεί ατομικά και συναντώνται συνήθως στον πληθυντικό αριθμό⁸⁸. Διαχωρίζονται σε «απλά» ή κοινά και «ευαίσθητα»⁸⁹, ανάλογα με την πληροφοριακή τους βαρύτητα όσον αφορά την ιδιωτικότητα⁹⁰ και με αυξημένη προστασία των δεδομένων που συγκροτούν τον «σκληρό πυρήνα» της ιδιωτικής ζωής και της προσωπικότητας, όπως αυτός γίνεται αντιληπτός στη χώρα μας⁹¹, προς αποφυγή διάκρισης, δυσμενούς μεταχείρισης, στιγματισμού ή ακόμα και κοινωνικού αποκλεισμού του υποκειμένου.

Σύμφωνα με το άρθρο 8 της Οδηγίας 95/46/ΕΚ, αρχικά απαγορεύεται η επεξεργασία ενός συνόλου προσωπικών δεδομένων που εμπεριέχουν ένα επιπρόσθετο πληροφοριακό φορτίο και αφορούν τη φυλετική ή εθνική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, τη συμμετοχή σε συνδικαλιστικές οργανώσεις, την υγεία και τη σεξουαλική ζωή. Με την παράγραφο β' του άρθρου 2 του Ν.2472/97, όπως τροποποιήθηκε με το άρθρο 18 του Ν.3471/2006, προστέθηκαν τα δεδομένα που αφορούν στην κοινωνική πρόνοια, στις ποινικές διώξεις ή καταδίκες και στη συμμετοχή σε συναφείς με τα ανωτέρω ενώσεις προσώπων. Καίτοι τα γενετικά δεδομένα⁹² δεν αναφέρονται ρητά στο νόμο, θεωρείται πως υπάγονται εξίσου στην ενισχυμένη νομική προστασία που απολαμβάνουν τα ευαίσθητα δεδομένα, σε αντίθεση με τα δεδομένα οικονομικής συμπεριφοράς, τα οποία εξαιρούνται από τον κατάλογο των ευαίσθητων δεδομένων⁹³. Με το νέο Κανονισμό, ο οποίος μετονόμασε τα ευαίσθητα δεδομένα σε «δεδομένα ειδικών κατηγοριών», προστίθενται, σε σχέση με την Οδηγία 95/46/ΕΚ, τα γενετικά δεδομένα⁹⁴, τα βιομετρικά δεδομένα⁹⁵, τα δεδομένα που αφορούν την

⁸⁶ Βλ. *Ι.Ιγγλεζάκη (2004), όπ.ανωτ., σελ.62 και Ε. Αλεξανδροπούλου-Αιγυπτιάδου (2016), όπ.ανωτ., σελ.44.*

⁸⁷ Βλ. *εισήγηση Φ. Μίτλεττον, Η έννοια των προσωπικών δεδομένων, σε: Α. Κοτσαλή (επιμ.), όπ.ανωτ., (2016), σελ.19 επόμε.*

⁸⁸ Βλ. *Π. Αρμαμέντο/Β. Σωτηρόπουλο (2005), όπ.ανωτ., σελ.19-21.*

⁸⁹ Βλ. *άρθρα 2β και 7 Ν.2472/1997, αιτιολογική σκέψη 10 Προοιμίου ΓΚΠΔ.*

⁹⁰ Βλ. *Ε. Αλεξανδροπούλου-Αιγυπτιάδου (2016), όπ.ανωτ., σελ.45.*

⁹¹ Βλ. *Εισηγητική Έκθεση Ν.2472/1997.*

⁹² Βλ. *υπ'αρ.15/2001 Γνωμοδότηση της ΑΠΔΠΧ. Επίσης αναφέρονται και στην αιτιολογική σκέψη 23 της Οδηγίας 2016/680/ΕΕ.*

⁹³ Βλ. *Μ. Μυλώση (2015), όπ.ανωτ., σελ.8.*

⁹⁴ Βλ. *άρθ. 4 περ.13, 9 παρ.1 ΓΚΠΔ.*

⁹⁵ Βλ. *άρθ. 4 περ.14, 9 παρ.1 ΓΚΠΔ.*

υγεία⁹⁶, οι διοικητικές κυρώσεις, οι δικαστικές αποφάσεις και τα ποινικά αδικήματα ή εικαζόμενα αδικήματα, οι ποινικές καταδίκες ή τα σχετικά μέτρα ασφαλείας⁹⁷. Εν κατακλείδι, ευαίσθητα είναι τα δεδομένα που αποκαλύπτουν πληροφορίες που αφορούν τις ανωτέρω κατηγορίες, ενώ απλά δεδομένα είναι όσα δεν είναι ευαίσθητα. Η σημασία της διάκρισης αφορά στη θέσπιση αυστηρότερων προϋποθέσεων, όσον αφορά την επεξεργασία των ευαίσθητων προσωπικών δεδομένων, καθόσον προαπαιτούμενη είναι η γραπτή συγκατάθεση του υποκειμένου τους, όπως επίσης και η λήψη άδειας από την ΑΠΔΠΧ, σε αντίθεση με τα απλά, όπου αρκεί η προφορική συγκατάθεση και η γνωστοποίηση στην Αρχή⁹⁸. Με άλλα λόγια, η διάκριση των προσωπικών δεδομένων επιφέρει συνέπειες στη νομική τους μεταχείριση και στον τρόπο επεξεργασίας τους⁹⁹. Κι ενώ ο Κανονισμός επίσης απαγορεύει την επεξεργασία των ευαίσθητων προσωπικών δεδομένων, εντούτοις, ορίζει ορισμένες εξαιρέσεις, στις οποίες, μεταξύ άλλων, ανήκει η προστασία του δημοσίου συμφέροντος και η άσκηση νομικών αξιώσεων. Στο άρθρο 4 του ΓΚΠΔ περιέχεται ο νέος ορισμός των δεδομένων προσωπικού χαρακτήρα, όπως επίσης και όλοι οι ορισμοί που θα απασχολήσουν το νέο νομοθέτημα.

«Υποκείμενο των προσωπικών δεδομένων»: το εν ζωή φυσικό πρόσωπο¹⁰⁰ στο οποίο αναφέρονται τα δεδομένα και του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί¹⁰¹.

«Επεξεργασία δεδομένων προσωπικού χαρακτήρα»¹⁰²: αποτελεί κάθε εργασία που εφαρμόζεται σε προσωπικά δεδομένα από το Δημόσιο, Νομικά Πρόσωπα Δημοσίου Δικαίου (ΝΠΔΔ), Νομικά Πρόσωπα Ιδιωτικού Δικαίου (ΝΠΙΔ), ενώσεις προσώπων ή φυσικό πρόσωπο, με τη χρήση ή χωρίς, αυτοματοποιημένων μεθόδων¹⁰³. Κρίνεται απολύτως αναγκαία για την παροχή δημόσιων υπηρεσιών, όπως σε νοσοκομεία, σχολεία, ασφαλιστικούς οργανισμούς κλπ. Ο νόμος απαριθμεί ενδεικτικά τις διάφορες μορφές επεξεργασίας, όπως η συλλογή, η καταχώρηση, η οργάνωση, η διατήρηση ή αποθήκευση, η τροποποίηση, η εξαγωγή, η χρήση, η διαβίβαση, η

⁹⁶ Βλ. άρθ. 4 περ.15, 9 παρ.1 ΓΚΠΔ.

⁹⁷ Βλ. Ι. Ιγγλεζάκη, *Το δικαίωμα στην ψηφιακή λήθη και οι περιορισμοί του* (2014), σελ.101.

⁹⁸ Βλ. Ε. Αλεξανδροπούλου-Αιγυπτιάδου (2016), *όπ.ανωτ.*, σελ.51-52.

⁹⁹ Βλ. Κ. Αρκουλή (2010), *όπ.ανωτ.*, σελ.4.

¹⁰⁰ Ο νόμος δεν εφαρμόζεται στα νομικά πρόσωπα, τα οποία προστατεύονται με γενικές διατάξεις για προστασία της προσωπικότητας, αθέμιτου ανταγωνισμού, Ν.3471/2006 κλπ, βλ. Ε. Αλεξανδροπούλου-Αιγυπτιάδου (2016), *όπ.ανωτ.*, σελ.60.

¹⁰¹ Βλ. άρθ. 2 εδ. γ Ν.2472/1997.

¹⁰² Βλ. άρθρα 2 εδ.δ Ν.2472/1997, 2 εδ.β Οδηγίας 95/46/ΕΚ και 4 παρ.2 ΓΚΠΔ.

¹⁰³ Βλ. Ι. Ιγγλεζάκη (2004), *όπ.ανωτ.*, σελ.62.

διάδοση ή κάθε άλλης μορφής διάθεση, η συσχέτιση ή ο συνδυασμός, η διασύνδεση, η δέσμευση (κλειδώμα), η διαγραφή και η καταστροφή.

Προκειμένου να κριθεί νόμιμη και συνταγματικά αποδεκτή η επεξεργασία των προσωπικών δεδομένων, πρέπει να εφαρμοστούν ορισμένες θεμελιώδεις **γενικές αρχές** που περιγράφονται στα άρθρα 4 και 10 του νόμου¹⁰⁴. Αυτές είναι περιληπτικά:

1) η αρχή της **νομιμότητας του σκοπού και του τρόπου επεξεργασίας**, σύμφωνα με την οποία η επεξεργασία πρέπει να πραγματοποιείται για νόμιμους, καθορισμένους και σαφείς σκοπούς και τα δεδομένα να συλλέγονται με θεμιτά και νόμιμα μέσα,

2) η αρχή της **αναλογικότητας ή της αναγκαιότητας της επεξεργασίας**, που επιτάσσει ότι, για να τύχουν νόμιμης επεξεργασίας τα δεδομένα, πρέπει να είναι πρόσφορα, δηλαδή κατάλληλα για την εξυπηρέτηση του σκοπού της επεξεργασίας, συναφή με αυτόν και όχι περισσότερα από όσα κάθε φορά απαιτούνται, εν όψει του σκοπού της επεξεργασίας¹⁰⁵. Για παράδειγμα, στην έκδοση Δελτίου Αστυνομικής Ταυτότητας είναι απαραίτητο το ονοματεπώνυμο και η ημερομηνία γέννησης του κατόχου και όχι το θρήσκευμα¹⁰⁶.

3) η αρχή της **ακρίβειας των δεδομένων**, κατά την οποία τα προσωπικά δεδομένα, για να τύχουν νόμιμης επεξεργασίας, πρέπει να είναι αληθή και να υποβάλλονται σε ενημέρωση, εάν μεταβάλλονται κατά την πάροδο του χρόνου,

4) η αρχή της **χρονικά πεπερασμένης διατήρησης**¹⁰⁷ των προσωπικών δεδομένων από τον υπεύθυνο επεξεργασίας, ο οποίος υποχρεούται να τα διατηρεί μόνο για συγκεκριμένη χρονική διάρκεια, ανάλογα με το χρόνο που απαιτεί η κάλυψη των σκοπών της επεξεργασίας κατά την κρίση της ΑΠΔΠΧ,

5) η αρχή της **μυστικότητας** που εγγυάται την τήρηση του απορρήτου κατά τη διεξαγωγή της επεξεργασίας και η αρχή της **ασφάλειας** των δεδομένων και της προστασίας τους από αθέμιτη επεξεργασία.

«**Αρχείο δεδομένων προσωπικού χαρακτήρα και διασύνδεση αρχείων**»: κάθε διαρθρωμένο σύνολο δεδομένων προσωπικού χαρακτήρα, τα οποία είναι προσιτά με γνώμονα συγκεκριμένα κριτήρια (φίλτρα)¹⁰⁸. Η έννοια του αρχείου είναι πολύ κρίσιμη, διότι οι διατάξεις του νόμου εφαρμόζονται μόνο στις περιπτώσεις που τα

¹⁰⁴ Βλ. επίσης και τον «Δεκάλογο του Υπευθύνου Επεξεργασίας», διαθέσιμος στο: http://www.dpa.gr/portal/page?_pageid=33,19278&_dad=portal&_schema=PORTAL.

¹⁰⁵ Βλ. Π. Αρμαμέντο/Β. Σωτηρόπουλο (2005), *όπ.ανωτ.*, σελ.123.

¹⁰⁶ Βλ. σύσταση ΑΠΔΠΧ προς Υπουργείο Δημόσιας Τάξης υπ'αρ. 510/17/15-5-2000.

¹⁰⁷ Βλ. Π. Αρμαμέντο/Β. Σωτηρόπουλο (2005), *όπ.ανωτ.*, σελ.135.

¹⁰⁸ Βλ. άρθ. 2 εδ. ε Ν.2472/1997 και άρθ. 2 εδ.γ Οδηγίας 95/46/ΕΚ: έννοια αρχείου «κάθε διαρθρωμένο σύνολο δεδομένων προσωπικού χαρακτήρα με γνώμονα συγκεκριμένα κριτήρια, είτε το σύνολο αυτό θα είναι συγκεντρωμένο, είτε αποκεντρωμένο, είτε καταναμημένο σε λειτουργική ή γεωγραφική βάση».

υπό επεξεργασία δεδομένα περιλαμβάνονται ή πρόκειται να περιληφθούν σε αρχείο¹⁰⁹. Μάλιστα, θεωρείται ο τρίτος ακρογωνιαίος λίθος στο σχήμα «προσωπικά δεδομένα-επεξεργασία-αρχείο»¹¹⁰, ενώ στον όρο συμπεριλαμβάνονται φυσικά και ηλεκτρονικά αρχεία. Άξιο αναφοράς είναι το γεγονός ότι στο νόμο δεν υπάρχει διάκριση μεταξύ δημόσιων και ιδιωτικών αρχείων, συνεπώς οι ίδιες ρυθμίσεις εφαρμόζονται και στις δύο περιπτώσεις, οποιοσδήποτε κι αν πραγματοποιεί την επεξεργασία. Διασύνδεση αρχείων είναι η συσχέτιση των δεδομένων ενός αρχείου με δεδομένα ενός άλλου που, είτε τηρείται από άλλον υπεύθυνο επεξεργασίας, είτε από τον ίδιο αλλά για διαφορετικό σκοπό. Στην περ.6 του άρθρου 4 του ΓΚΠΔ με τίτλο «σύστημα αρχειοθέτησης», επαναλαμβάνεται ο ορισμός της Οδηγίας 95/46/ΕΚ, στον οποίο προστίθεται κι ένα «χωροταξικό» κριτήριο στην έννοια του αρχείου¹¹¹. Χαρακτηριστικές περιπτώσεις αρχείων δεδομένων προσωπικού χαρακτήρα που απασχόλησαν κατά καιρούς τη δικαιοσύνη και την ΑΠΔΠΧ, υπήρξαν τα ιστορικά αρχεία και η πρόσβαση σε αυτά για ερευνητικούς σκοπούς, το ποινικό μητρώο και η δυνατότητα των εν δυνάμει εργοδοτών να ζητούν αντίγραφο αυτού από τους υποψήφιους, η τήρηση ιατρικού φακέλου και η πρόσβαση τρίτων σε αυτόν, η τήρηση και η πρόσβαση σε δημόσια βιβλία, η τήρηση υπηρεσιακών ή πειθαρχικών φακέλων κ.ά.¹¹²

«**Υπεύθυνος επεξεργασίας**»¹¹³: το πρόσωπο (φυσικό ή νομικό, ακόμα και δημόσιος οργανισμός) που καθορίζει το σκοπό και τον τρόπο επεξεργασίας δεδομένων προσωπικού χαρακτήρα, που εξουσιάζει το αρχείο και που φέρει την ευθύνη για την επεξεργασία που πραγματοποιείται. Ενδεικτικό παράδειγμα υπευθύνου επεξεργασίας στο ελληνικό δημόσιο είναι ο ΕΦΚΑ.

«**Εκτελών την επεξεργασία**»¹¹⁴: οποιοσδήποτε επεξεργάζεται προσωπικά δεδομένα για λογαριασμό του υπευθύνου επεξεργασίας.

«**Αποδέκτης της επεξεργασίας**»: το φυσικό ή νομικό πρόσωπο ή η δημόσια αρχή ή ο οργανισμός όπου απευθύνονται τα δεδομένα.

«**Συγκατάθεση του υποκειμένου των δεδομένων**»: η μονομερής δήλωση βούλησης του υποκειμένου, με την οποία αποδέχεται την επεξεργασία των δεδομένων του και η

¹⁰⁹ Βλ. άρθρ. 3 παρ. 1 Ν.2472/1997, ενδεικτικά Αποφάσεις ΑΠ 2515/2009 και ΑΠ 2079/2007.

¹¹⁰ Βλ. εισήγηση Φ. Μίτλεττον, *Αρχείο προσωπικών δεδομένων*, σε: Α. Κοτσαλή, *όπ.ανωτ.* (2016), σελ.60.

¹¹¹ Βλ. εισήγηση Φ. Μίτλεττον (2016), σε: Α. Κοτσαλή, *όπ.ανωτ.*, σελ.60.

¹¹² Βλ. εισήγηση Φ. Μίτλεττον (2016), σε: Α. Κοτσαλή, *όπ.ανωτ.*, σελ.67.

¹¹³ Βλ. και άρθρα 4 περ.7 και 24 επόμε. ΓΚΠΔ.

¹¹⁴ Βλ. και άρθρ. 28 ΓΚΠΔ.

οποία πρέπει να είναι ελεύθερη, ρητή, εξειδικευμένη και να ανακαλείται ελεύθερα. Αποτελεί αναγκαία προϋπόθεση νόμιμης επεξεργασίας, εκτός εάν συντρέχουν ορισμένες εξαιρέσεις που απαριθμούνται στο νόμο¹¹⁵.

Στα **δικαιώματα** των υποκειμένων των δεδομένων ανήκουν το δικαίωμα ενημέρωσης από τον υπεύθυνο επεξεργασίας, το δικαίωμα πρόσβασης, το δικαίωμα αντίρρησης και το δικαίωμα προσωρινής δικαστικής προστασίας, όπως αυτά αναλύονται στα άρθρα 11 έως 14 του νόμου. Τα δικαιώματα αυτά, τα οποία πηγάζουν από το άρθρο 9Α Σ¹¹⁶, μπορούν να περιοριστούν, αν η επεξεργασία γίνεται για λόγους εθνικής ασφάλειας ή με σκοπό τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων¹¹⁷.

«**Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ ή Αρχή)**»¹¹⁸: αποτελεί μία από τις πέντε Ανεξάρτητες Αρχές (ΑΑ)¹¹⁹ που προβλέπει το Σύνταγμα, οι οποίες αποτελούν μεν κρατικά όργανα, εκφεύγουν όμως του ιεραρχικού ελέγχου της κεντρικής κυβέρνησης και υπόκεινται μόνο σε δικαστικό έλεγχο νομιμότητας. Τα μέλη της απολαμβάνουν προσωπικής και λειτουργικής ανεξαρτησίας¹²⁰ όσον αφορά την υποχρέωση υπακοής στα εκτελεστικά όργανα, τα οποία δεν δύνανται να παρεμβαίνουν στον τρόπο με τον οποίο ασκούν τα καθήκοντά τους.

Η ΑΠΔΠΧ ιδρύθηκε στην ελληνική επικράτεια με το Ν.2472/1997, τέθηκε σε λειτουργία στις 10 Νοεμβρίου 1997 και κατοχυρώθηκε συνταγματικά με το άρθρο 9Α¹²¹ του αναθεωρημένου Συντάγματος 2001. Η συνταγματική κατοχύρωση της Αρχής καταδεικνύει τη σπουδαιότητα που αποδίδεται στην προστασία των προσωπικών δεδομένων, με μέριμνα και φροντίδα της Αρχής. Πιο συγκεκριμένα, με ευρείες αποφασιστικές αρμοδιότητες, εποπτεύει την εφαρμογή των νόμων και λοιπών ρυθμίσεων που αφορούν την προστασία του ατόμου από την επεξεργασία προσωπικών του δεδομένων, ενώ ταυτόχρονα οι αποφάσεις της είναι δεσμευτικές ως προς τα υπόλοιπα κρατικά όργανα.

¹¹⁵ Βλ. άρθ. 5 παρ.2 Ν.2472/1997 *εξαιρέσεις όπου επιτρέπεται η επεξεργασία και χωρίς τη συγκατάθεση του υποκειμένου.*

¹¹⁶ Βλ. Β. Σωτηρόπουλο, *Το άρθρο 9Α του Συντάγματος 1975/1986/2001 (χωρίς ημερομηνία)*, σελ.22: *το «δικαίωμα» του άρθρου 9Α είναι μια δέσμη δικαιωμάτων, η οποία εξειδικεύεται κατά την κοινή νομοθεσία και περιλαμβάνει τα αναφερόμενα ειδικότερα δικαιώματα..*

¹¹⁷ Βλ. Α. Ψαροπούλου (2018), *όπ.ανωτ.*, σελ.18.

¹¹⁸ Βλ. άρθ. 15 επόμε. Ν.2472/1997, 51 επόμε. ΓΚΠΔ και ιστότοπο Αρχής: www.dpa.gr.

¹¹⁹ Οι υπόλοιπες τέσσερις είναι: η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ- άρθ.19 παρ.2 Σ), το Ανώτατο Συμβούλιο Επιλογής Προσωπικού (ΑΣΕΠ- άρθ.103 παρ.7 Σ), το Εθνικό Συμβούλιο Ραδιοτηλεόρασης (ΕΣΡ- άρθ.15 παρ.2 Σ) και ο Συνήγορος του Πολίτη (ΣτΠ- άρθ.103 παρ.9 Σ).

¹²⁰ Με το άρθρο 101Α Συντάγματος κατοχυρώθηκε η προσωπική και λειτουργική ανεξαρτησία των μελών των ανεξάρτητων αρχών και η διαδικασία εκλογής των μελών τους.

¹²¹ «*Η προστασία των προσωπικών δεδομένων διασφαλίζεται από ανεξάρτητη αρχή, που συγκροτείται και λειτουργεί, όπως νόμος ορίζει*».

Στην ΑΠΔΠΧ¹²² καταφεύγουν με καταγγελίες ή προσφυγές τα φυσικά πρόσωπα όταν έχουν παράπονα σχετικά με την εφαρμογή του νόμου και την προστασία των δικαιωμάτων τους. Καταγγελίες ενώπιον της Αρχής της χώρας κατοικίας ή του υπευθύνου επεξεργασίας, μπορούν επίσης να υποβάλλουν και φορείς, οργανώσεις ή ενώσεις φυσικών προσώπων. Στον ενημερωτικό ρόλο της Αρχής εμπίπτει η εντός τριμήνου ενημέρωση του ενδιαφερόμενου για τα αποτελέσματα επί της καταγγελίας του, η ετήσια Έκθεση προς τη Βουλή, όπως επίσης και η παροχή πληροφοριών, για την άσκηση δικαιωμάτων, κατόπιν ατομικού αιτήματος. Η Αρχή εκδίδει οδηγίες, απευθύνει συστάσεις, γνωμοδοτεί, εκδίδει κανονιστικές πράξεις, χορηγεί άδειες, καταγγέλλει παραβάσεις, επιβάλλει κυρώσεις, διενεργεί διοικητικές εξετάσεις. Επίσης, εξετάζει αιτήσεις του υπευθύνου επεξεργασίας για έλεγχο της νομιμότητας της επεξεργασίας, συνεργάζεται με τις Αρχές των υπολοίπων κρατών-μελών και του Συμβουλίου της Ευρώπης, τηρεί Μητρώα Αρχείων & Επεξεργασιών, Αδειών και Αδειών Διαβίβασης, Διασυνδέσεων, Απορρήτων Αρχείων και Προσώπων που δεν επιθυμούν να περιλαμβάνονται σε αρχεία¹²³. Τέλος, στις αρμοδιότητες της Αρχής εμπίπτει και η ευαισθητοποίηση των ενδιαφερομένων μερών για τους επαπειλούμενους κινδύνους, τους υφιστάμενους κανόνες επεξεργασίας, την άσκηση δικαιωμάτων και τις εν γένει θεσμικές εγγυήσεις με ειδική αναφορά στην προστασία των παιδιών.

Σύμφωνα με το Ν.2472/1997, ο υπεύθυνος επεξεργασίας οφείλει να γνωστοποιήσει εγγράφως στην Αρχή τη σύσταση και λειτουργία αρχείου, όπως επίσης την έναρξη επεξεργασίας απλών προσωπικών δεδομένων. Κατ' εξαίρεση, μπορεί να επιτραπεί η δημιουργία αρχείου ευαίσθητων προσωπικών δεδομένων και η επεξεργασία τους, κατόπιν άδειας της Αρχής και συγκατάθεσης του υποκειμένου. Ως εξαίρεση της εξαίρεσης υπάρχουν περιπτώσεις απαλλαγής του υπευθύνου επεξεργασίας από την υποχρέωση γνωστοποίησης και λήψης άδειας (άρθρο 7Α), όπως για παράδειγμα όταν η επεξεργασία πραγματοποιείται αποκλειστικά για σκοπούς που συνδέονται άμεσα με παροχή υπηρεσιών στο δημόσιο τομέα, είναι αναγκαία για την εκπλήρωση νόμιμης υποχρέωσης και το υποκείμενο έχει προηγουμένως ενημερωθεί. Πάντως, με τον ΓΚΠΔ, η υποχρέωση γνωστοποίησης ή λήψης άδειας από την Αρχή, αντικαθίσταται από άλλες υποχρεώσεις (όπως η υποχρέωση διενέργειας εκτίμησης αντικτύπου που

¹²² Βλ. Γ. Ρουσόπουλο – Κ. Λιμνιώτη, *Προετοιμασία των Δημόσιων Οργανισμών για την εφαρμογή του νέου Κανονισμού* (2018), σελ.4.

¹²³ Βλ. Δ. Λεμπέση, (2018α), *όπ.ανωτ.*, σελ.510-511 και *άρθ.19 παρ.4 Ν.2472/1997*.

αναλύεται παρακάτω), που δίνουν έμφαση κυρίως στην πρόληψη. Άξιο αναφοράς, τέλος, αποτελεί το γεγονός ότι ο Ν.2472/1997 δεν ρυθμίζει την αστική ευθύνη¹²⁴ του Δημοσίου, των ΝΠΔΔ και των οργάνων τους¹²⁵, συνεπώς διέπεται από τις διατάξεις του ΕισΝΑΚ άρθρα 105 επόμε., σύμφωνα με τις οποίες, προϋποθέσεις της ευθύνης για παράνομη πράξη διοικητικού οργάνου είναι οι εξής: η πράξη ή παράλειψη α) να προήλθε από κρατικό όργανο, β) να ανήκει στην κυριαρχική διοίκηση, γ) να πραγματοποιήθηκε κατά την ενάσκηση δημόσιας εξουσίας, δ) να είναι παράνομη, να αντιβαίνει δηλαδή σε διάταξη του Ν.2472/1997 η οποία όμως δεν έχει τεθεί χάριν του γενικού συμφέροντος και ε) να έχει προκαλέσει ζημία, ενώ η υπαιτιότητα του οργάνου δεν εξετάζεται¹²⁶.

2.6. Σύγχρονο Ενωσιακό Νομοθετικό Πλαίσιο Προστασίας Προσωπικών Δεδομένων

Στον πρόλογο του Εγχειριδίου της **Σύμβασης 108** του Συμβουλίου της Ευρώπης αναφέρεται ότι «με την έναρξη ισχύος της Συνθήκης της Λισαβόνας τον Δεκέμβριο 2009, ο ΧΘΔΕΕ κατέστη νομικά δεσμευτικός, εξ' ου και το δικαίωμα προστασίας των προσωπικών δεδομένων προήχθη στο επίπεδο αυτοτελούς θεμελιώδους δικαιώματος».

Η Οδηγία **97/66/ΕΚ** του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 15ης Δεκεμβρίου 1997, περί επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και προστασίας της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα, διευκρινίζει και συμπληρώνει την Οδηγία 95/46/ΕΚ σε ό,τι αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα στον τομέα των τηλεπικοινωνιών.

Ο Κανονισμός **45/2001/ΕΚ** του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 18ης Δεκεμβρίου 2000, σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα όργανα και τους οργανισμούς της Κοινότητας και σχετικά με την ελεύθερη κυκλοφορία των δεδομένων αυτών. Ο εν λόγω προγενέστερος Κανονισμός συνεχίζει να εφαρμόζεται ταυτόχρονα με τον ΓΚΠΔ, ενώ, σύμφωνα με την αιτιολογική σκέψη 17 του

¹²⁴ Την υποχρέωση δηλαδή του Κράτους να αποκαταστήσει τη ζημία που προξένησαν παράνομα τα όργανά του σε ιδιώτη.

¹²⁵ Βλ. άρθ. 23 Ν.2472/1997.

¹²⁶ Βλ. I. Ιγγλεζάκη (2004), *όπ.ανωτ.*, σελ.288.

Προοιμίου του ΓΚΠΔ, θα πρέπει να υποστεί τις αναγκαίες προσαρμογές, προκειμένου να εξασφαλιστεί ένα συνεκτικό πλαίσιο προστασίας των δεδομένων στην Ένωση.

Η Οδηγία **2016/680/ΕΕ**¹²⁷ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27^{ης} Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές¹²⁸ για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών. Στόχος της είναι η εξασφάλιση αποτελεσματικής δικαστικής και αστυνομικής συνεργασίας σε ποινικές υποθέσεις. Για παράδειγμα, σύμφωνα με την αιτιολογική σκέψη 11, για τους σκοπούς της διερεύνησης ή της δίωξης αξιόποινης πράξης, σε συγκεκριμένες περιπτώσεις τα χρηματοπιστωτικά ιδρύματα παρέχουν τα προσωπικά δεδομένα στις αρμόδιες εθνικές αρχές σύμφωνα με το δίκαιο των κρατών μελών. Η Οδηγία, που αποκαλείται και η μικρή αδερφή του ΓΚΠΔ, δημοσιεύτηκε παράλληλα με αυτόν, ισχύει από τις 6-5-2018 και λειτουργεί συμπληρωματικά με τον Κανονισμό που θεσπίζει τους γενικούς κανόνες προστασίας των φυσικών προσώπων.

Πιο συγκεκριμένα¹²⁹, η Οδηγία αφορά στην επεξεργασία δεδομένων από τις εθνικές αρχές επιβολής του νόμου, όπως επί παραδείγματι από την Ελληνική Αστυνομία, το Λιμενικό Σώμα-την Ελληνική Ακτοφυλακή, καθώς και την Ειδική Γραμματεία του Σώματος Δίωξης Οικονομικού Εγκλήματος (ΣΔΟΕ). Επίσης, εφαρμόζεται και στις δραστηριότητες των εθνικών δικαστικών αρχών, ωστόσο ειδικά για τις διαδικασίες επεξεργασίας που αφορούν προσωπικά δεδομένα που σχετίζονται με ποινικές διαδικασίες, μπορούν να εφαρμόζονται σε κάθε κράτος-μέλος οι εθνικοί κανόνες ποινικών διαδικασιών, όπως ο Κώδικας Ποινικής Δικονομίας στην Ελληνική επικράτεια. Μάλιστα, στις περιπτώσεις της δικαστικής δικαιοδοσίας, αίρεται η δικαιοδοσία της ΑΠΔΠΧ επί της επεξεργασίας των προσωπικών δεδομένων, προκειμένου να διασφαλιστεί η δικαστική ανεξαρτησία. Επιπλέον, έγκειται στη δικαιοδοσία του κράτους-μέλους να προβλέψει την άρση της δικαιοδοσίας των

¹²⁷ Κατήργησε από τις 6-5-2018 την Απόφαση Πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου της 27ης Νοεμβρίου 2008 για την προστασία των δεδομένων προσωπικού χαρακτήρα που τυγχάνουν επεξεργασίας στο πλαίσιο της αστυνομικής και δικαστικής συνεργασίας σε ποινικές υποθέσεις.

¹²⁸ Στις αρμόδιες αρχές, σύμφωνα με την Οδηγία (αιτιολογική σκέψη 11 Προοιμίου ΓΚΠΔ), δεν περιλαμβάνονται μόνο δημόσιες αρχές, όπως δικαστικές αρχές, αστυνομικές αρχές ή άλλες αρχές επιβολής του νόμου, αλλά και κάθε άλλος φορέας που έχει ανατεθεί από το κράτος μέλος να ασκεί δημόσια εξουσία για τους σκοπούς της Οδηγίας.

¹²⁹ Βλ. Α. Χελιουδάκη (2018) 'Γιατί η μικρή αδερφή του GDPR πρέπει να σε απασχολεί ως πολίτη;' Διαθέσιμο στο: www.homodigitalis.gr/posts/2373.

εθνικών εποπτικών αρχών (δηλαδή της ΑΠΔΠΧ) στις περιπτώσεις της επεξεργασίας από τις εισαγγελικές αρχές, όταν αυτές ενεργούν στο πλαίσιο της δικαιοδοτικής τους αρμοδιότητας. Ωστόσο, η τήρηση της Οδηγίας από τις δικαστικές αρχές υπόκειται στον έλεγχο ανεξάρτητης αρχής, σύμφωνα με την παράγραφο 3 του άρθρου 8 του ΧΘΔΕΕ.

Στην αιτιολογική σκέψη 19 του ΓΚΠΔ αναφέρεται ότι η προστασία των φυσικών προσώπων έναντι της επεξεργασίας των προσωπικών τους δεδομένων από αρμόδιες αρχές για σκοπούς πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων, συμπεριλαμβανομένης της διασφάλισης έναντι των απειλών κατά της δημόσιας ασφάλειας και της πρόληψής τους, όπως και της ελεύθερης κυκλοφορίας των δεδομένων αυτών, αποτελεί αντικείμενο ειδικής ενωσιακής νομικής πράξης και, συνεπώς, ο Κανονισμός δεν εφαρμόζεται. Ωστόσο, τα δεδομένα που υφίστανται επεξεργασία από δημόσιες αρχές βάσει του ΓΚΠΔ, θα πρέπει, όταν χρησιμοποιούνται για αυτούς τους σκοπούς, να ρυθμίζονται από την Οδηγία 2016/680/ΕΕ.

Η Οδηγία 2016/680/ΕΕ αποτελεί σημαντικό νομοθέτημα, διότι αντικαθιστά το φτωχό νομοθετικό πλαίσιο της Απόφασης Πλαίσιο 2008/977/ΔΕΥ, η οποία είχε πολύ περιορισμένο πεδίο εφαρμογής και δεν πέτυχε να κρατήσει ισορροπία ανάμεσα στα δικαιώματα των προσώπων και τις ανάγκες των αρχών επιβολής του νόμου. Επιπροσθέτως, η Οδηγία αποτελεί το πρώτο νομοθέτημα που αποπειράθηκε να ρυθμίσει ενιαία στην ΕΕ την επεξεργασία των προσωπικών δεδομένων των κατοίκων κρατών-μελών από τις εθνικές αρχές επιβολής του νόμου.

3. Παρουσίαση Γενικού Κανονισμού για την προστασία Προσωπικών Δεδομένων

3.1. Πρόλογος

Ο νέος Γενικός Κανονισμός για τα Προσωπικά Δεδομένα (Κανονισμός ΕΕ 2016/679¹³⁰) τέθηκε σε ισχύ το Μάιο του 2018 και αφορά όλες τις επιχειρήσεις και τους φορείς (δημόσιους και ιδιωτικούς) που επεξεργάζονται προσωπικά δεδομένα Ευρωπαίων πολιτών, δηλαδή διατηρούν στοιχεία πελατών και χρηστών διαδικτύου¹³¹. Ο Κανονισμός έχει εφαρμογή ακόμα και εάν οι φορείς που εκτελούν την επεξεργασία έχουν έδρα και δραστηριότητα εκτός ΕΕ και ανεξαρτήτως του τόπου όπου πραγματοποιείται η επεξεργασία.

Ρυθμίζει ζητήματα επεξεργασίας, διαχείρισης και προστασίας των προσωπικών δεδομένων αλλά και ελεύθερης κυκλοφορίας των δεδομένων στην κοινοτική επικράτεια στα πλαίσια της ανάπτυξης της εσωτερικής της αγοράς¹³².

Αποτελεί την πιο πρόσφατη νομοθετική εξέλιξη της ΕΕ και είναι ένα ιδιαίτερα φιλόδοξο κείμενο, που έχει συγκεντρώσει τα επιστημονικά και επιχειρηματικά βλέμματα και που στοχεύει στη διαφύλαξη της ασφάλειας και της προστασίας των προσωπικών δεδομένων των φυσικών προσώπων¹³³. Πρόκειται για έναν «έξυπνο» Κανονισμό, δεδομένου ότι προϋποθέτει «έξυπνη» ερμηνεία και η εφαρμογή του προϋποθέτει την κατανόηση της ουσίας του¹³⁴, εγχείρημα διόλου ευκατόρθωτο. Στην αβεβαιότητα του σύγχρονου κόσμου και στις αλλεπάλληλες παραβιάσεις των προσωπικών δεδομένων, ο ΓΚΠΔ αποπειράται να διασφαλίσει ένα υψηλό επίπεδο προστασίας των δεδομένων και να αποτελέσει παγκόσμιο πρότυπο αντιμετώπισης των μελλοντικών κινδύνων κατά της ελευθερίας¹³⁵.

¹³⁰ «Κανονισμός 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27^{ης} Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της Οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων)».

¹³¹ Βλ. ηλεκτρονική πηγή: <http://mindigital.gr>.

¹³² Βλ. Δ. Λεμπέση (2018α), *όπ.ανωτ.*, σελ.499.

¹³³ Φυσικό πρόσωπο: αυτό του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί.

¹³⁴ Βλ. εισήγηση Φ. Μίτλεττον, *Ο μηχανισμός συνεργασίας και συνεκτικότητας (One Stop Shop)*, σε: Δ. Κοτσαλή/Κ. Μενουδάκο (επιμ.), *όπ.ανωτ.* (2018), σελ.284.

¹³⁵ Βλ. Ε. Πλατή, *Προσωπικά Δεδομένα GDPR (2018)*, σελ.105.

3.2. Δικαιολογητικός λόγος θέσπισης του Κανονισμού

Η αλματώδης τεχνολογική εξέλιξη δημιούργησε νέες δυνατότητες αλλά και κινδύνους όσον αφορά την προστασία των προσωπικών δεδομένων, επιβάλλοντας τον ανακαθορισμό των νομικών εννοιών και τη θέσπιση ειδικών ρυθμίσεων, ώστε να διασφαλιστεί η προστασία του υποκειμένου των δεδομένων και κατ' επέκταση η αποτελεσματική εφαρμογή του δημοκρατικού πολιτεύματος¹³⁶.

Προκειμένου να γίνει αντιληπτή η ουσία των διατάξεων του Κανονισμού, θεωρείται απαραίτητη η διευκρίνιση των πολιτικοοικονομικών συνθηκών που οδήγησαν στην υιοθέτησή του.

Ένας σημαντικός λόγος θέσπισης του Κανονισμού ήταν η ανάγκη που δημιουργήθηκε, λόγω των τεχνολογικών εξελίξεων και της τεράστιας αξίας των δεδομένων στη σύγχρονη εποχή, να επικαιροποιηθεί το δίκαιο και να συμβαδίσει με την τεχνολογία. Με άλλα λόγια, η νομοθετική αλλαγή ήταν επιβεβλημένη, ώστε να προσαρμοστεί στη σύγχρονη ψηφιακή τεχνολογία, να εδραιωθεί κλίμα εμπιστοσύνης ως προς την ασφάλεια των συναλλαγών και να υπάρξει ενιαία αντιμετώπιση σε όλη την ΕΕ. Ο ανταγωνισμός με την Αμερική και τις υπόλοιπες αναδυόμενες αγορές επέβαλε την ενίσχυση και τη σύγκλιση των ψηφιακών οικονομιών εντός της εσωτερικής αγοράς, μέσω της αύξησης των διασυνοριακών ροών προσωπικών δεδομένων¹³⁷. Με τον Κανονισμό, η ΕΕ εισήλθε σε μια νέα εποχή όσον αφορά το δίκαιο προστασίας των προσωπικών δεδομένων, καθόσον μετά από μία εικοσαετή εφαρμογή της Οδηγίας 95/46/ΕΚ, τέθηκαν οι βάσεις για τη δημιουργία ενός ενιαίου δικαίου προστασίας σε όλη την επικράτεια της ΕΕ¹³⁸. Η προϋπάρχουσα Οδηγία 95/46/ΕΚ περιλάμβανε μόλις 34 άρθρα, παρείχε κατευθυντήριες γραμμές, έθετε το πλαίσιο και τα όρια στα οποία θα έπρεπε να κινηθούν οι εθνικοί νομοθέτες ενσωματώνοντάς την στην εσωτερική έννομη τάξη, δεν είχε όμως την ισχύ και τη δεσμευτικότητα ενός Κανονισμού. Δεδομένου λοιπόν ότι είχαν ήδη παρέλθει αρκετά χρόνια από την έκδοση της Οδηγίας, μέσα στα οποία οι τεχνολογικές εξελίξεις που μεσολάβησαν ήταν ραγδαίες και τα υφιστάμενα εργαλεία προστασίας ανεπαρκή, θα έπρεπε και η νομοθεσία να προσαρμοστεί στη νέα ψηφιακή πραγματικότητα. Για το

¹³⁶ Βλ. Α. Γέροντα (2002), *όπ.ανωτ.*, σελ.259.

¹³⁷ Βλ. Δ. Λεμπέση (2018β) *όπ.ανωτ.*, σελ.595-596.

¹³⁸ Βλ. εισήγηση Σ. Βλαχόπουλου, *Πρόσβαση στα Δημόσια Έγγραφα*, σε: Α. Κοτσαλή/Κ. Μενουδάκο (επιμ.), *όπ.ανωτ* (2018), σελ.42.

λόγο τούτο, τον Ιανουάριο του 2012 δημοσιεύτηκε η Πρόταση Κανονισμού¹³⁹ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, που κατατέθηκε στις 25-1-2012 από την Ευρωπαϊκή Επιτροπή, για την αναθεώρηση της Οδηγίας 95/46/ΕΚ, την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών. Στόχος της επιλογής της νομικής μορφής του Κανονισμού, ο οποίος δεσμεύει υπεράνω συνόρων, είναι να εξομαλυνθούν τα ζητήματα που ανέκυψαν λόγω της απόκλισης της νομοθεσίας των κρατών-μελών, τα οποία κατέστησαν προβληματική τη λειτουργία της εσωτερικής αγοράς και τη συνεργασία των εθνικών αρχών, ενώ ταυτόχρονα δημιούργησαν σύγχυση στους υπευθύνους επεξεργασίας δεδομένων και ανασφάλεια στους πολίτες της ΕΕ.¹⁴⁰ Τέσσερα χρόνια μετά και κατόπιν επώδυνων διαπραγματεύσεων¹⁴¹, εκατοντάδων τροπολογιών, πολλών αποφάσεων του ΔΕΕ, γνωμοδοτήσεων της Επιτροπής και κατευθυντήριων οδηγιών της Ομάδας του άρθρου 29, αυτή η Πρόταση οδήγησε τελικά στην ψήφιση του ΓΚΠΔ στις 25-5-2016 και στην από 25-5-2018¹⁴² θέση του σε ισχύ. Το εγχείρημα της υιοθέτησής του ήταν εξαιρετικά απαιτητικό, διότι σε κάθε κράτος-μέλος διαφοροποιείται το ιστορικό και πολιτικό υπόβαθρο, η συνταγματική κατοχύρωση, τα έθιμα και συνεπώς η ομοιόμορφη αντιμετώπιση των περιπτώσεων επεξεργασίας προσωπικών δεδομένων εντός ΕΕ έμοιαζε με σενάριο επιστημονικής φαντασίας. Η εφαρμογή του είναι υποχρεωτική από όλα τα κράτη-μέλη, τα οποία οφείλουν να διασφαλίσουν ομοιόμορφη και συνεκτική εφαρμογή του σε ολόκληρη την Ένωση. Από τους βασικότερους στόχους του ΓΚΠΔ είναι η ενίσχυση των δικαιωμάτων των πολιτών, που επιτυγχάνεται με τη δημιουργία νέων δικαιωμάτων, την αναθεώρηση ήδη υπαρχόντων, τη δημιουργία νέων μηχανισμών για την προστασία τους, τη διεύρυνση των υποχρεώσεων των υπευθύνων επεξεργασίας, τη θεσμοθέτηση του υπευθύνου προστασίας δεδομένων και την πρόβλεψη αυστηρών διοικητικών προστίμων που φθάνουν έως και τα 20.000.000 ευρώ¹⁴³.

¹³⁹ Η Πρόταση στηρίζεται στα άρθρ. 8 του ΧΘΔΕΕ και 16, 114 παρ.1 της ΣΛΕΕ σύμφωνα με την αιτιολογική σκέψη 1 του ΓΚΠΔ, όπως αναλύονται παρακάτω.

¹⁴⁰ Βλ. Ι. Ιγγλεζάκη (2014), *όπ.ανωτ.*, σελ.100.

¹⁴¹ Βλ. ενδεικτικά συνεδρίαση Συμβουλίου της ΕΕ στις 25-10-2012, συζήτηση στο Συμβούλιο στις 6-6-2013 και 7-10-2013, πρώτη ανάγνωση πρότασης ενώπιον Ευρωπαϊκού Κοινοβουλίου στις 21-10-2013, από 21-11-2013 έκθεση με προτάσεις για αλλαγές από την Επιτροπή Πολιτικών Ελευθεριών Δικαιοσύνης και Εσωτερικών Υποθέσεων (σχέδιο ψηφίσματος του Ευρωπαϊκού Κοινοβουλίου), βλ. Ι. Ιγγλεζάκη (2014), *όπ.ανωτ.*, σελ.98.

¹⁴² Βλ. Ε. Αλεξανδροπούλου-Αιγυπτιάδου (2016), *όπ.ανωτ.*, σελ.216.

¹⁴³ Βλ. άρθρο 83 παράγραφος 5 ΓΚΠΔ και εισήγηση Φ. Παναγοπούλου-Κουντατζή, *Το νέο πλαίσιο δικαιωμάτων*, σε: Α. Κοτσαλή/Κ. Μενουδάκο (επιμ.), *όπ.ανωτ.* (2018), σελ 5-6.

Στο σημείο όμως αυτό δεν πρέπει να παραλείψουμε να αναφέρουμε και τις επιφυλάξεις που εκφράστηκαν όσον αφορά την τροποποίηση του κανονιστικού πλαισίου και την ανάγκη αναθεώρησης της Οδηγίας 95/46/ΕΚ¹⁴⁴. Η επιλογή της υιοθέτησης ενός Κανονισμού στη θέση της μεθόδου προσαρμογής δια των Οδηγιών, συνάντησε αντιδράσεις λόγω της μετάβασης από εθνικές σε ενωσιακές ρυθμίσεις, αφού η δεσμευτική ισχύς του Κανονισμού θα άφηνε στενά περιθώρια στον εθνικό νομοθέτη και στις ανεξάρτητες αρχές για δημιουργία εναλλακτικών πολιτικών προστασίας βάσει των εθνικών αντιλήψεων και συμφερόντων. Μάλιστα στη Γερμανία το Ομοσπονδιακό Συμβούλιο (Bundesrat) έκανε αναφορά για κίνδυνο πλήρους αποκλεισμού των εθνικών ρυθμίσεων, ενώ στη Γαλλία η Αρχή για την Πληροφορική και τις Ελευθερίες (CNIL) επίσης αντιτάχθηκε στη ρύθμιση μέσω Κανονισμού. Ειδικότερα, ο παραγκωνισμός της εθνικής νομοθεσίας χαρακτηρίστηκε από τον Δικαστή του Γερμανικού Ομοσπονδιακού Συνταγματικού Δικαστηρίου ως «ο αποχαιρετισμός των ατομικών δικαιωμάτων», αφού δε θα μπορεί πλέον να γίνεται, κατ' αρχήν, παραπομπή στις εθνικές διατάξεις και ο Κανονισμός θα κατισχύει έναντι κάθε εθνικής εξαίρεσης και δικαιοκίνησης που άπτεται των προσωπικών δεδομένων. Ωστόσο, ο ΓΚΠΔ έχει αρκετά χαρακτηριστικά Οδηγίας, διότι παρέχει στον εθνικό νομοθέτη τη διακριτική ευχέρεια να υιοθετήσει συγκεκριμένες επιλογές¹⁴⁵, όπως θα αναλυθεί παρακάτω.

Οι λόγοι που επέβαλαν την αναθεώρηση του νομικού πλαισίου και την αναμόρφωση του δικαίου για την προστασία των προσωπικών δεδομένων στην Ένωση, περιγράφονται αναλυτικά στις αιτιολογικές σκέψεις 6 και 7 του Προοιμίου του ΓΚΠΔ. Σε αυτές περιγράφονται ως λόγοι οι ραγδαίες τεχνολογικές εξελίξεις, η παγκοσμιοποίηση, η αύξηση της κλίμακας συλλογής και ανταλλαγής προσωπικών δεδομένων, η εντεινόμενη χρήση των δεδομένων από ιδιωτικές επιχειρήσεις και δημόσιες αρχές, κατά την επιδίωξη των δραστηριοτήτων τους και η αυξανόμενη δημοσιοποίηση προσωπικών πληροφοριών από τα φυσικά πρόσωπα. Η αναμόρφωση αυτή χαρακτηρίζεται από κανόνες συνεκτικότητας, που διασφαλίζονται από το νέο Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (ΕΣΠΔ) και τον Ευρωπαϊό Επόπτη, απλές διαδικασίες, συντονισμένες δράσεις, μεγαλύτερη εμπλοκή των χρηστών

¹⁴⁴ Για την έκφραση επικρίσεων όσον αφορά την επιλογή του Κανονισμού ως ρυθμιστικού εργαλείου βλ. Α. Μήτρον, ΓΚΠΔ (2017), σελ. 31 επόμενα.

¹⁴⁵ Βλ. Φ. Παναγοπούλου-Κουτνατζή, Ο Γενικός Κανονισμός για την Προστασία Δεδομένων 679/2016/ΕΕ (2017α), σελ.18-19.

δεδομένων, αποτελεσματική πληροφόρηση και ενίσχυση των εξουσιών επιβολής¹⁴⁶. Με αυτές τις πρακτικές και μέσω της αυστηρής εφαρμογής της νομοθεσίας, θα επιτευχθεί η ασφάλεια δικαίου και κατ' επέκταση η ασφάλεια των φυσικών προσώπων, των οικονομικών παραγόντων και των δημοσίων αρχών.

3.3. Παρουσίαση ΓΚΠΔ: Βασικές Αρχές Προστασίας – Δικαιώματα των Υποκειμένων

Ο νέος Κανονισμός έχει καθολική δεσμευτικότητα, άμεσο αποτέλεσμα και άμεση ισχύ σε όλη την Επικράτεια της ΕΕ και πλέον εφαρμόζονται οι ίδιες διατάξεις σε όλα τα κράτη-μέλη, σε αντίθεση με το παρελθόν, όπου κάθε κράτος ενσωμάτωσε στο εσωτερικό του δίκαιο την Οδηγία 95/46/ΕΚ με νομοθετικές παρεμβάσεις διαφορετικού περιεχομένου.

Νομοθετική βάση του Κανονισμού αποτελεί αρχικά το άρθρο 8 του ΧΘΔΕΕ καθώς επίσης και το άρθρο 16 της ΣΛΕΕ¹⁴⁷ (Ευρωπαϊκή Ένωση, 2012), το οποίο στην παράγραφο 1 ορίζει ότι «κάθε πρόσωπο έχει δικαίωμα προστασίας των δεδομένων προσωπικού χαρακτήρα που το αφορούν». Ο Κανονισμός αποτελείται από 99 άρθρα, συγκεντρωμένα σε 11 κεφάλαια, και 173 αιτιολογικές σκέψεις που αποτελούν πηγές ερμηνείας σε πολλούς προβληματισμούς που ανακύπτουν όσον αφορά την κατανόηση του κυρίως κειμένου. Καταλαμβάνει 88 σελίδες στην Επίσημη Εφημερίδα και πρόκειται συνεπώς για ένα εκτενές, πολύπλοκο νομοθέτημα, το οποίο εισάγει νέες αρχές επεξεργασίας και ενίσχυση των υποχρεώσεων του υπεύθυνου επεξεργασίας. Επίσης περιέχει ειδικές ρυθμίσεις για την προστασία των παιδιών¹⁴⁸, προβλέπει τη δυνατότητα ανάκλησης της συγκατάθεσης του υποκειμένου και γενικότερα αυστηρότερες κυρώσεις, ενώ θεσπίζει το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων, ενθαρρύνει τη θέσπιση μηχανισμών πιστοποίησης κ.α.¹⁴⁹.

Μία πρώτη προσέγγιση στα γενικά χαρακτηριστικά του νέου νομοθετήματος θα υποστήριζε ότι ενισχύεται η προστασία των υποκειμένων, δεδομένου ότι παρέχονται

¹⁴⁶ Βλ. Δ. Λεμπέση (2018α), *όπ.ανωτ.*, σελ.526.

¹⁴⁷ *Ενοποιημένη απόδοση της Συνθήκης για την Ευρωπαϊκή Ένωση και της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης (2012/C 326/01)*.

¹⁴⁸ Βλ. *αιτιολογική σκέψη 38 του Προοιμίου ΓΚΠΔ, όπου καθορίζεται η ανάγκη για ειδική προστασία των παιδιών και άρθρο 8 ΓΚΠΔ, όπου για σύννομη επεξεργασία απαιτείται η συγκατάθεση των ασκούντων τη γονική μέριμνα του ανήλικου, αιτιολογική σκέψη 58 και άρθρο 12 ΓΚΠΔ για υποχρέωση σαφήνειας κ.ά.*

¹⁴⁹ Βλ. Ε. Αλεξανδροπούλου-Αιγυπτιάδου (2016), *όπ.ανωτ.*, σελ.217.

νέα δικαιώματα στα φυσικά πρόσωπα, αυστηροποιούνται οι προϋποθέσεις συγκατάθεσης, ενώ ταυτόχρονα εισάγονται οι αρχές της υπευθυνότητας και της λογοδοσίας του υπευθύνου της επεξεργασίας. Ο ορισμός των προσωπικών δεδομένων διευρύνεται, περιλαμβάνοντας πλέον τα δεδομένα θέσης, τα βιομετρικά και τα γενετικά δεδομένα. Παράλληλα, ευνοεί την ασφαλή και ελεύθερη ροή των προσωπικών δεδομένων εντός του κοινοτικού χωρικού πλαισίου, με αποτέλεσμα να ενισχύεται η εμπιστοσύνη των πολιτών και η επιχειρηματικότητα¹⁵⁰. Πλην όμως, σύμφωνα με την αιτιολογική σκέψη 4 του Προοιμίου του ΓΚΠΔ, το δικαίωμα στην προστασία των προσωπικών δεδομένων δεν είναι απόλυτο, καθόσον συνεκτιμώνται και άλλοι παράγοντες¹⁵¹ υπό το πρίσμα της αρχής της αναλογικότητας. Συνεπώς, τουλάχιστον σε θεωρητικό επίπεδο, στο κείμενο του Κανονισμού δεν υφίσταται ιεραρχία στα ατομικά δικαιώματα. Προβληματισμοί προκύπτουν για την ύπαρξη «ηθικών φραγμών στη γνώση», για την αναγνώριση «νομικού μονοπωλίου του ατόμου πάνω στις πληροφορίες που το αφορούν», ή για τον περιορισμό της πληροφόρησης δυνάμει του ατομικού δικαιώματος στη σφαίρα του απορρήτου, το οποίο θέτει φραγμούς στην ελεύθερη κυκλοφορία των πληροφοριών προς διασφάλιση της ιδιωτικής αυτονομίας¹⁵².

Επιγραμματικά, ορισμένες από τις καινοτομίες που εισάγει ο ΓΚΠΔ είναι ο θεσμός του υπευθύνου προστασίας δεδομένων, το δικαίωμα στη λήθη και τη φορητότητα, οι αρχές της διαφάνειας και της λογοδοσίας και η υποχρέωση γνωστοποίησης παραβιάσεων προσωπικών δεδομένων στην Αρχή και στο υποκείμενο. Επίσης, υιοθετήθηκαν σύγχρονες έννοιες της επιστήμης της πληροφορικής, όπως για παράδειγμα η εκτίμηση επιπτώσεων (αντικτύπου) στις περιπτώσεις που η επεξεργασία κρίνεται επικίνδυνη για την ασφάλεια των προσωπικών δεδομένων (data protection impact assessment), η προσέγγιση με βάση τον κίνδυνο (risk-based approach)¹⁵³, η προστασία εκ σχεδιασμού και εξ ορισμού (privacy by design, privacy by default), η ασφάλεια δεδομένων ως οργανωτική αρχή κ.α.¹⁵⁴, κάποιες από τις οποίες αναλύονται κατωτέρω.

¹⁵⁰ Βλ. *Ε. Πλατή (2018), όπ.ανωτ., εισαγωγή.*

¹⁵¹ Βλ. *άρθρο 85 παράγραφος 1 ΓΚΠΔ: ελευθερία έκφρασης και πληροφόρησης.*

¹⁵² Βλ. *Κ. Χριστοδούλου, Δίκαιο Προσωπικών Δεδομένων (2013), σελ.12.*

¹⁵³ *Η διαπίστωση του βαθμού διακινδύνευσης των δικαιωμάτων των υποκειμένων γίνεται από τον υπεύθυνο επεξεργασίας, ο οποίος λαμβάνει ειδικά μέτρα, βλ. Ι. Ιγγλεζάκη (2018β), σελ. 77.*

¹⁵⁴ Βλ. *Ε. Πλατή (2018), όπ.ανωτ., σελ.6.*

Προστασία δεδομένων εργαζομένων

Έχει κριθεί από το ΕΔΔΑ ότι η επαγγελματική ζωή των εργαζομένων προστατεύεται όπως και η ιδιωτική ζωή βάσει του άρθρου 8 ΕΣΔΑ. Με αυτή την παραδοχή συμβαδίζει η νομολογία της ΑΠΔΠΧ και η Οδηγία 2001/115/ΕΚ¹⁵⁵, η οποία αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα των εργαζομένων¹⁵⁶, όπως επίσης και η Γνώμη 2/2017¹⁵⁷ της Ομάδας Εργασίας του άρθρου 29, σχετικά με τη χρήση νέων τεχνολογιών για την επεξεργασία των δεδομένων των εργαζομένων. Στην ίδια γραμμή κινήθηκε και ο ΓΚΠΔ, ορίζοντας πως τα κράτη-μέλη δύνανται να θεσπίζουν ειδικούς κανόνες για την αποτελεσματικότερη διαφύλαξη της αξιοπρέπειας, των εννόμων συμφερόντων και των θεμελιωδών δικαιωμάτων των εργαζομένων έναντι της επεξεργασίας των δεδομένων τους από τον εργοδότη. Επεξεργασία προσωπικών δεδομένων στις εργασιακές σχέσεις τελείται και στα πλαίσια της δημοσιοϋπαλληλικής σχέσης: το Δημόσιο επεξεργάζεται τα δεδομένα του υπαλλήλου από το στάδιο διαδικασίας επιλογής και διορισμού του, ως την οριστική λύση της σχέσης. Η δημοσιοϋπαλληλική σχέση αποτελεί μια ειδική κυριαρχική σχέση και ο δημόσιος υπάλληλος παρέχει την εργασία του υπό το καθεστώς μιας ιδιότυπης εξάρτησης από το Δημόσιο¹⁵⁸.

Αντίστοιχη ρύθμιση υπάρχει στο ελληνικό σχέδιο νόμου¹⁵⁹, όπου αναφέρεται, μεταξύ άλλων, η συλλογή δεδομένων με τη χρήση μεθόδων ελέγχου και παρακολούθησης και η υποχρέωση ενημέρωσης των εργαζομένων για την επεξεργασία των δεδομένων τους¹⁶⁰.

¹⁵⁵ Βλ. ηλεκτρονική πηγή:

http://www.dpa.gr/portal/page?_pageid=33,120908&_dad=portal&_schema=PORTAL

¹⁵⁶ Βλ. άρθρ. 88 ΓΚΠΔ.

¹⁵⁷ Βλ. ηλεκτρονική πηγή: <https://www.lawspot.gr/nomikes-plirofories/loipa-nomika/gnomi/gnomi-2-2017-omadas-ergasias-arthroy-29-shetika-me-tin>

¹⁵⁸ Βλ. Β. Δούκα, Προσωπικά δεδομένα και εργασιακές σχέσεις: Προστασία σύμφωνα με τον ΓΚΠΔ (2018), σελ. 641, 644.

¹⁵⁹ Βλ. άρθρ. 17 ΣχΝΠΔΠΧ.

¹⁶⁰ Βλ. Γ. Παναγοπούλου, Εποπτεία και επιβολή της τήρησης του ΓΚΠΔ (2018).

4. Καινοτομίες που εφαρμόζονται σε ιδιωτικό και δημόσιο τομέα

Στο κείμενο του ΓΚΠΔ εμφανίζονται όροι όπως λογοδοσία, διαφάνεια, αντικειμενικότητα, ακρίβεια, νομιμότητα, εμπιστευτικότητα, ακεραιότητα, οι οποίοι καταδεικνύουν εμφανώς το πνεύμα του νέου νομοθετήματος. Στα πλαίσια λοιπόν των νέων ρυθμίσεων, κάθε οντότητα και οργανισμός οφείλουν να ακολουθήσουν μια ολοκληρωμένη διαδικασία εσωτερικής προετοιμασίας που θα οδηγήσει στην εσωτερική συμμόρφωση με τον Κανονισμό.

4.1. Νέα εργαλεία συμμόρφωσης με τον ΓΚΠΔ

Με τον Κανονισμό εισάγονται νέα Εργαλεία συμμόρφωσης¹⁶¹, τα οποία είναι τα εξής:

1) Η προστασία των δεδομένων ήδη από τον σχεδιασμό (**Privacy by design**) και εξ ορισμού (**Privacy by default**)¹⁶²: στα πλαίσια των υποχρεώσεων του υπευθύνου επεξεργασίας εντάσσεται και η έννοια της προστασίας της ιδιωτικότητας κατά τον σχεδιασμό, η οποία προέρχεται αμιγώς από το χώρο της πληροφορικής και αφορά την ευθύνη του για προληπτική και όχι κατασταλτική αντιμετώπιση των προσβολών της ιδιωτικής σφαίρας. Ειδικότερα, ο υπεύθυνος επεξεργασίας εφαρμόζει τεχνικά και οργανωτικά μέτρα, όπως η ψευδωνυμοποίηση και η ελαχιστοποίηση των δεδομένων, κατά το σχεδιασμό του συστήματος επεξεργασίας και όχι εκ των υστέρων, προκειμένου να ενσωματωθούν οι απαραίτητες εγγυήσεις εφαρμογής των αρχών προστασίας δεδομένων. Έτσι θα διασφαλιστεί το πλαίσιο εντός του οποίου πρέπει αυτός να κινείται. Για να πετύχει τους στόχους του, λαμβάνει υπόψη του τις πρόσφατες τεχνολογικές εξελίξεις, το κόστος, τη φύση και το πεδίο εφαρμογής των μέτρων, το πλαίσιο και τους σκοπούς επεξεργασίας, όπως επίσης τους πιθανούς κινδύνους που μπορεί να επιφέρει η επεξεργασία στα δικαιώματα και τις ελευθερίες των φυσικών προσώπων (risk assessment). Σύμφωνα με την εξ ορισμού προστασία, υφίστανται προεπιλεγμένες ρυθμίσεις στο σύστημα, που διασφαλίζουν ότι θα τύχουν επεξεργασίας μόνο τα απαραίτητα για τον εκάστοτε σκοπό δεδομένα, κατά την αρχή της αναλογικότητας και της διαφάνειας. Με αυτό τον τρόπο περιορίζεται το εύρος

¹⁶¹ Βλ. Ρουσόπουλο – Λιμνιώτη (2018), *όπ.ανωτ.*, σελ. 12 επόμε.

¹⁶² Βλ. άρθ. 25 ΓΚΠΔ.

των δεδομένων προς επεξεργασία, ο βαθμός της επεξεργασίας και ο χρόνος αποθήκευσης των δεδομένων¹⁶³.

2) Τα **Αρχεία Δραστηριοτήτων Επεξεργασίας**¹⁶⁴: η τήρησή τους από τον υπεύθυνο επεξεργασίας είναι υποχρεωτική για τις επιχειρήσεις ή τους οργανισμούς που έχουν πάνω από 250 άτομα προσωπικό¹⁶⁵ και περιλαμβάνουν α)την ταυτότητα του υπευθύνου επεξεργασίας, του εκπροσώπου, του υπευθύνου προστασίας δεδομένων και τον τρόπο επικοινωνίας μαζί τους, β)τους σκοπούς της επεξεργασίας, γ)τις κατηγορίες των δεδομένων και των υποκειμένων των δεδομένων, δ)τις κατηγορίες των αποδεκτών, ε)τις διαβιβάσεις σε χώρες εκτός ΕΕ, στ)τις προθεσμίες διαγραφής των δεδομένων, ζ)τα μέτρα ασφαλείας.

3) Εξειδικευμένα **μέτρα ασφάλειας της επεξεργασίας**¹⁶⁶: ο ΓΚΠΔ επιδιώκει την ασφαλή επεξεργασία των δεδομένων έναντι των κινδύνων και για το λόγο αυτό εισάγει νέες ρυθμίσεις που αφορούν προτεινόμενα ενδεδειγμένα τεχνικά και οργανωτικά μέτρα. Τα μέτρα αυτά είναι η ψευδωνυμοποίηση¹⁶⁷ και η κρυπτογράφηση των δεδομένων, η διαρκής διασφάλιση του απορρήτου, της ακεραιότητας, της διαθεσιμότητας και της αξιοπιστίας των συστημάτων επεξεργασίας, η αποκατάσταση της διαθεσιμότητας και της πρόσβασης σε δεδομένα σε περίπτωση συμβάντος και η δοκιμή, η εκτίμηση και διαρκής αξιολόγηση της αποτελεσματικότητας των μέτρων διασφάλισης της ασφαλούς επεξεργασίας. Ο ΓΚΠΔ επίσης ενθαρρύνει την εκπόνηση και χρήση εγκεκριμένου κώδικα δεοντολογίας (ο οποίος περιγράφεται στο άρθρο 40 ΓΚΠΔ) ή τη θέσπιση μηχανισμού πιστοποίησης προστασίας δεδομένων (άρθρο 42 ΓΚΠΔ), που θα αποδεικνύει τη συμμόρφωση με τις απαιτήσεις ασφάλειας που ο ίδιος επιτάσσει. Πρακτικά, μία οντότητα μπορεί να περιορίσει τη μη εξουσιοδοτημένη πρόσβαση στα δεδομένα που τηρεί, λαμβάνοντας μέτρα, όπως ενδεικτικά την υιοθέτηση εσωτερικού κανονισμού ασφαλείας, την εγκατάσταση κατάλληλου λογισμικού προστασίας από ιούς, την ενεργοποίηση «τείχους προστασίας» (firewall), την φύλαξη αντιγράφων ασφαλείας

¹⁶³ Βλ. Γ. Γιαννόπουλο, ΓΚΠΔ: οι νέες υποχρεώσεις και η ευθύνη του Υπευθύνου Επεξεργασίας (2017), σελ.202.

¹⁶⁴ Βλ. άρθ. 30 ΓΚΠΔ.

¹⁶⁵ Κατ' εξαίρεση και οι επιχειρήσεις που έχουν λιγότερους από 250 εργαζομένους, εάν η επεξεργασία ενδέχεται να προκαλέσει κίνδυνο.

¹⁶⁶ Βλ. άρθρο 32 ΓΚΠΔ.

¹⁶⁷ Βλ. αιτιολογικές σκέψεις 28-29 Προοιμίου ΓΚΠΔ.

(backups), την πρόσβαση στα ευαίσθητα προσωπικά δεδομένα μόνο από εξουσιοδοτημένα άτομα και την προστασία δικτύου wi-fi με κωδικούς πρόσβασης¹⁶⁸.

4) Αντιμετώπιση **περιστατικών παραβίασης** μέσω κοινοποιήσεων-ανακοινώσεων¹⁶⁹: ως περιστατικά παραβίασης δεδομένων προσωπικού χαρακτήρα λογίζονται όσα οδηγούν σε τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, άνευ αδείας κοινολόγηση ή προσπέλαση των δεδομένων. Στην περίπτωση αυτή ακολουθείται από τον υπεύθυνο επεξεργασίας ένα πρωτόκολλο: μόλις ανιχνεύσει το περιστατικό παραβίασης, διερευνά την περίπτωση και αποκτά γνώση του περιστατικού. Εάν διαπιστωθεί ότι η παραβίαση δύναται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, γνωστοποιεί εντός 72 ωρών την παραβίαση στην εποπτική αρχή. Εάν δεν προκύψει κίνδυνος, δεν κοινοποιεί το περιστατικό στην Αρχή, σε κάθε όμως περίπτωση προβαίνει στην καταγραφή όλων των περιστατικών. Όταν μάλιστα η παραβίαση ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος ανακοινώνει άμεσα το περιστατικό στα επηρεαζόμενα φυσικά πρόσωπα και τα ενημερώνει για λήψη μέτρων αυτοπροστασίας (το δικαίωμα ενημέρωσης του υποκειμένου σε περίπτωση παραβίασης, αναλύεται παρακάτω).

5) **Εκτίμηση αντικτύπου** σχετικά με την προστασία δεδομένων (Data Protection Impact Assessment - DPIA)¹⁷⁰: αποτελεί ένα εργαλείο ελέγχου και απόδειξης συμμόρφωσης με τον Κανονισμό. Όταν ένα είδος επεξεργασίας ενέχει συγκεκριμένους κινδύνους για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας διενεργεί υποχρεωτικά, πριν την επεξεργασία, εκτίμηση των επιπτώσεων που θα έχει η σχεδιαζόμενη επεξεργασία στην προστασία των δεδομένων. Η DPIA μπορεί να εξασφαλίσει την τήρηση της θεμελιώδους αρχής προστασίας δεδομένων από τον σχεδιασμό (data protection by design), να καταδείξει τις απαιτούμενες τεχνολογικές λύσεις για τη διασφάλιση της ασφάλειας της επεξεργασίας, όπως επίσης να διευκολύνει την ορθή αξιολόγηση των περιστατικών παραβίασης των δεδομένων, εφόσον προβαίνει σε αποτίμηση κινδύνων, και να προτείνει τρόπους αντιμετώπισής τους. Περιλαμβάνει τουλάχιστον τη συστηματική περιγραφή των προβλεπόμενων πράξεων και σκοπών επεξεργασίας, το έννομο συμφέρον που επιδιώκει ο υπεύθυνος επεξεργασίας, εκτίμηση της αναγκαιότητας και

¹⁶⁸ Βλ. Κ. Κοντοπούλου, *Νέος Κανονισμός για την Προστασία Δεδομένων (GDPR)*, (2018), σελ. 526.

¹⁶⁹ Βλ. άρθρα 33-34 και αιτιολογική σκέψη 85 Προοιμίου ΓΚΠΔ.

¹⁷⁰ Βλ. άρθρα 35-36 και αιτιολογικές σκέψεις 84,90-95 Προοιμίου ΓΚΠΔ.

της αναλογικότητας των πράξεων επεξεργασίας, εκτίμηση των κινδύνων ως προς τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων¹⁷¹, όπως επίσης και τα προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων. Η εποπτική αρχή, τη γνώμη της οποίας έχει ζητήσει ο υπεύθυνος πριν την επεξεργασία, οφείλει να καταρτίσει κατάλογο με τα είδη επεξεργασιών που απαιτούν διενέργεια εκτίμησης αντικτύπου, ενώ τα κράτη-μέλη δύνανται να κρίνουν αναγκαία την προγενέστερη εκπόνηση DPIA, όταν δημόσια αρχή ή φορέας σκοπεύει να εγκαθιδρύσει μια κοινή εφαρμογή ή πλατφόρμα επεξεργασίας¹⁷², όπως επίσης και στην περίπτωση που πρόκειται να εκδοθεί νομοθέτημα στο οποίο βασίζεται η άσκηση καθηκόντων δημόσιας αρχής ή φορέα και η οποία ρυθμίζει τη συγκεκριμένη πράξη ή σειρά πράξεων επεξεργασίας¹⁷³. Παρέχεται επίσης η διακριτική ευχέρεια στον εθνικό νομοθέτη να απαιτήσει από τον υπεύθυνο επεξεργασίας να λάβει προηγούμενη άδεια από την εποπτική αρχή, στην περίπτωση που η επεξεργασία αφορά εκτέλεση καθήκοντος του υπευθύνου προς το δημόσιο συμφέρον, περιλαμβανομένης της επεξεργασίας σε σχέση με την κοινωνική προστασία και τη δημόσια υγεία. Εάν, παρά τη διενέργεια εκτίμησης αντικτύπου, συνεχίζει να προκύπτει υψηλός κίνδυνος για τα δεδομένα, ακολουθεί εκ νέου διαβούλευση με την Αρχή.

6) Ο **Υπεύθυνος Προστασίας Δεδομένων** (εφεξής ΥΠΔ, ο θεσμός περιγράφεται κατωτέρω αναλυτικά)¹⁷⁴: ο εθελοντικός διορισμός του προσδίδει ανταγωνιστικό πλεονέκτημα στις επιχειρήσεις, διότι αποτελεί δείγμα λήψης μέτρων συμμόρφωσης. Υποχρεωτικός καθίσταται ο ορισμός του, όταν η επεξεργασία διενεργείται από δημόσια αρχή ή φορέα, όταν απαιτείται τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε μεγάλη κλίμακα¹⁷⁵ και όταν υπάρχει μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα¹⁷⁶ (άρθρο 9 ΓΚΠΔ) και δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα (άρθρο 10 ΓΚΠΔ). Η επεξεργασία δεδομένων ασθενών από ιδιώτη ιατρό ή η

¹⁷¹ Μεταξύ άλλων, όταν πρόκειται για μέτρα που βασίζονται σε κατάρτιση προφίλ, σε ζητήματα υγείας, στην αυτοματοποιημένη επιτήρηση δημόσιων χώρων κ.α., βλ. I. Ιγγλεζάκη (2014), *όπ.ανωτ.*, σελ.106.

¹⁷² Βλ. αιτιολογική σκέψη 92 Προοιμίου ΓΚΠΔ.

¹⁷³ Βλ. αιτιολογική σκέψη 93 Προοιμίου ΓΚΠΔ.

¹⁷⁴ Βλ. άρθρο 37 ΓΚΠΔ.

¹⁷⁵ Παραδείγματα επεξεργασιών μεγάλης κλίμακας: επεξεργασία δεδομένων πελατών σε τακτική βάση από τράπεζες, ασφαλιστικές εταιρίες ή εταιρίες παροχής υπηρεσιών διαδικτύου.

¹⁷⁶ Για παράδειγμα η επεξεργασία δεδομένων υγείας από ιατρικό κέντρο.

επεξεργασία δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα από ιδιώτη δικηγόρο, δεν συνιστούν επεξεργασία μεγάλης κλίμακας¹⁷⁷.

7) **Κώδικες Δεοντολογίας**¹⁷⁸: ο ΓΚΠΔ παροτρύνει την εκπόνηση κωδίκων δεοντολογίας, η τήρηση των οποίων θα αποτελεί ισχυρό μεν αλλά όχι αδιαμφισβήτητο αποδεικτικό μέσο ορθής εφαρμογής του. Μέσω των προτεινόμενων κωδίκων, επιχειρείται η διαπίστωση εφαρμογής του ΓΚΠΔ σε διάφορους τομείς, όπως η θεμιτή και με διαφάνεια επεξεργασία, η συλλογή δεδομένων προσωπικού χαρακτήρα, η ενημέρωση των υποκειμένων των δεδομένων και η άσκηση των δικαιωμάτων τους, η προστασία των παιδιών κ.ά., όπως περιγράφονται αναλυτικά στο άρθρο 40 του ΓΚΠΔ. Τους κώδικες εκπονούν ενώσεις που εκπροσωπούν τους υπευθύνους ή εκτελούντες την επεξεργασία και εγκρίνονται μόνο από την εποπτική αρχή, όταν ο κώδικας δεν έχει σχέση με δραστηριότητες επεξεργασίας σε περισσότερα του ενός κράτη-μέλη, ενώ, αν τα σχέδια κωδίκων αναφέρονται σε δραστηριότητες επεξεργασίας σε διάφορα κράτη-μέλη, εγκρίνονται και από το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (ΕΣΠΔ¹⁷⁹ ή European Data Protection Board –EDPB). Πάντως, για τη γενική ισχύ των κωδίκων δεοντολογίας αποφασίζει η Ευρωπαϊκή Επιτροπή.

8) **Πιστοποιήσεις**¹⁸⁰: όπως και με τους κώδικες δεοντολογίας, η θέσπιση μηχανισμού πιστοποίησης προστασίας δεδομένων, σφραγίδων και σημάτων προστασίας δεδομένων είναι προαιρετική, ενθαρρύνεται από τον ΓΚΠΔ, αφορά τις πράξεις επεξεργασίας και αποδεικνύει τη συμμόρφωση του υπευθύνου ή του εκτελούντα την επεξεργασία με τις διατάξεις του Κανονισμού. Άξια αναφοράς είναι η πρόβλεψη κοινής Πιστοποίησης, ήτοι της Ευρωπαϊκής Σφραγίδας Προστασίας Προσωπικών Δεδομένων, την οποία θα εκδίδουν οι αρμόδιες αρχές ελέγχου αφού επιβεβαιώσουν τη συμμόρφωση με τις διατάξεις του ΓΚΠΔ¹⁸¹. Οι πιστοποιήσεις διαρκούν το μέγιστο για τρία χρόνια και χορηγούνται από τους αναφερόμενους στο άρθρο 43 ΓΚΠΔ φορείς πιστοποίησης, οι οποίοι διαπιστεύονται είτε από την εποπτική αρχή, είτε από τον εθνικό οργανισμό διαπίστευσης¹⁸². Προκειμένου να εκδοθεί μια πιστοποίηση, θα

¹⁷⁷ Πηγή: <https://www.lawspot.gr/nomika-nea/gdpr-kai-ypeythynoi-prostasias-dedomenon-dpo-ti-prepei-na-gnorizete>

¹⁷⁸ Βλ. άρθρα 40-41 ΓΚΠΔ.

¹⁷⁹ Βλ. άρθρα 68 επ. ΓΚΠΔ και ηλεκτρονική πηγή: <https://edpb.europa.eu>.

¹⁸⁰ Βλ. άρθρα 42-43 ΓΚΠΔ.

¹⁸¹ Βλ. I. Ιγγλεζάκη (2014), *όπ.ανωτ.*, σελ.106.

¹⁸² Στην Ελλάδα υπάρχει το Εθνικό Σύστημα Διαπίστευσης (Ε.ΣΥ.Δ.), ιστότοπος: www.esyd.gr.

πρέπει να πληρούνται ορισμένα κριτήρια εγκεκριμένα από την εποπτική αρχή ή από το ΕΣΠΑ.

Δεδομένου ότι η γενική πρόβλεψη γνωστοποίησης της επεξεργασίας στην εποπτική αρχή και η δυνατότητα γνωμοδότησης από αυτήν, όπως προβλέπονταν από την Οδηγία 95/45/ΕΚ, έχουν καταργηθεί, οι Κώδικες Δεοντολογίας και οι Πιστοποιήσεις παρέχουν μία επιπρόσθετη εξασφάλιση τήρησης των προβλεπόμενων κανόνων. Στο ελληνικό ΣχΝΠΔΠΧ (άρθρο 15), προβλέπεται ότι η διαπίστευση των φορέων που χορηγούν πιστοποιήσεις θα πραγματοποιείται από το ΕΣΥΔ, σύμφωνα με το πρότυπο EN-ISO/IEC17065/2012.

9) Μία επίσης σημαντική καινοτομία του ΓΚΠΔ είναι ο **μηχανισμός συνεργασίας και συνεκτικότητας**, που είναι γνωστός ως One Stop Shop (υπηρεσία μιας στάσης)¹⁸³. Με τον μηχανισμό αυτό επιβεβαιώνεται η ευρωπαϊκή διάσταση του Κανονισμού, διότι καθιερώνει τη διακρατική ισχύ των διοικητικών πράξεων στην ΕΕ. Πιο συγκεκριμένα, ο θεσμός One Stop Shop σημαίνει ότι μία διοικητική απόφαση που έχει ληφθεί σε ένα κράτος-μέλος είναι δεσμευτική και παράγει έννομες συνέπειες σε ολόκληρο το έδαφος της Ένωσης. Πρόκειται για έναν αποτελεσματικό μηχανισμό εποπτείας και επιβολής, με αποφασιστικές αρμοδιότητες. Ο μηχανισμός συνεργασίας αφορά κυρίως τη συνεργασία της επικεφαλής αρχής με τις ενδιαφερόμενες εποπτικές αρχές σε περίπτωση διερεύνησης καταγγελίας που εμπλέκει περισσότερα του ενός κράτη-μέλη¹⁸⁴, αλλά και οποιαδήποτε αρμοδιότητα των εποπτικών αρχών (άρθρα 51 επόμεν. ΓΚΠΔ) που σχετίζεται με διασυνοριακές πράξεις επεξεργασίας. Ο μηχανισμός συνεκτικότητας αφορά στις διασυνοριακές ροές δεδομένων και αποπειράται να επιτύχει τον συνεκτικό τρόπο επίλυσης των διαφορών. Αναφέρεται στη διαδικασία λήψης αποφάσεων από το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (ΕΣΠΑ), το οποίο απαρτίζεται από τους επικεφαλής των εποπτικών αρχών των κρατών-μελών και τον Ευρωπαίο Επόπτη Προστασίας Δεδομένων (ΕΕΠΑ)¹⁸⁵. Οι επεξεργασίες δεδομένων από δημόσιους Οργανισμούς εμπίπτουν στην αρμοδιότητα της εποπτικής αρχής του κράτους-μέλους, διότι λαμβάνουν χώρα σε τοπικό επίπεδο και συνεπώς δεν εφαρμόζεται στις περιπτώσεις αυτές ο μηχανισμός συνεργασίας και συνεκτικότητας.

¹⁸³ Βλ. αιτιολογική σκέψη 10 Προομιόν ΓΚΠΔ, άρθρα 60 επόμεν. ΓΚΠΔ και εισήγηση Φ. Μίλεττον, *Ο μηχανισμός συνεργασίας και συνεκτικότητας (One Stop Shop)*, σε: Α. Κοτσαλή/Κ. Μενουδάκο (επιμ.), *όπ.ανωτ.* (2018), σελ. 284 επόμεν.

¹⁸⁴ Βλ. και άρθ. 57 παρ.1 εδ.στ' ΓΚΠΔ.

¹⁸⁵ Βλ. άρθ. 68 επόμεν. ΓΚΠΔ.

4.2. Νέες Αρχές που εισάγει ο ΓΚΠΔ

Όσον αφορά τις αρχές που διέπουν την επεξεργασία¹⁸⁶, στις γενικές αρχές που ήδη εφαρμόζονταν στην επεξεργασία των προσωπικών δεδομένων, όπως αναλύθηκαν παραπάνω (και απαριθμούνται στο άρθρο 6 της Οδηγίας 95/46/ΕΚ), προστέθηκαν και δύο νέες¹⁸⁷, ήτοι:

Η **Αρχή της Διαφάνειας**, σύμφωνα με την οποία τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε νόμιμη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο.

Η **Αρχή της Λογοδοσίας** (accountability), που θεσπίζει εκ νέου τη συνολική ευθύνη και υποχρέωση αποζημίωσης για τον υπεύθυνο επεξεργασίας. Συγκεκριμένα, επιβάλλει στον υπεύθυνο να είναι σε θέση να αποδείξει τη συμμόρφωση με τις αρχές που διέπουν την επεξεργασία, ήτοι της νομιμότητας, της αντικειμενικότητας, της διαφάνειας, του περιορισμού του σκοπού, της ελαχιστοποίησης των δεδομένων, της ακρίβειας, του περιορισμού της περιόδου αποθήκευσης, της ακεραιότητας και της εμπιστευτικότητας, όπως αυτές απαριθμούνται και αναλύονται στο άρθρο.

4.3. Νέο πλαίσιο δικαιωμάτων που εισάγει ο ΓΚΠΔ

Δικαίωμα διαγραφής («δικαίωμα στη λήθη»^{188, 189}): το δικαίωμα αυτό διαμορφώθηκε κυρίως μέσα από θεμελιώδεις αποφάσεις ανώτατων εθνικών δικαστηρίων, του ΕΔΔΑ¹⁹⁰ και του ΔΕΕ. Βασίζεται στη γενικότερη ελευθερία ανάπτυξης της προσωπικότητας του ατόμου της παραγράφου 1 του άρθρου 5 Σ, στην κατοχύρωση της ανθρώπινης αξίας της παραγράφου 1 του άρθρου 2 Σ, στο δικαίωμα προστασίας της ιδιωτικής ζωής του άρθρου 9 Σ και στην προστασία των προσωπικών δεδομένων και του πληροφοριακού αυτοκαθορισμού του ατόμου του άρθρου 9Α Σ.

¹⁸⁶ Συνοπτικά, κατά τον Ι. Ιγγλεζάκη (ηλεκτρονική πηγή: <https://www.slideshare.net/iglezakis/ss-83511848>), αναφέρονται οι αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τον ΓΚΠΔ.

¹⁸⁷ Βλ. άρθ. 5 ΓΚΠΔ.

¹⁸⁸ *Right to be forgotten*, βλ. άρθ. 17 ΓΚΠΔ και αιτιολογικές σκέψεις 65-66 του Προοιμίου ΓΚΠΔ.

¹⁸⁹ Βλ. εισήγηση Φ. Παναγοπούλου – Κουντατζή, *Το νέο πλαίσιο δικαιωμάτων*, σε: Α. Κοτσαλή-Κ. Μενουδάκο, *όπ.ανωτ* (2018), σελ 15 επόμ.

¹⁹⁰ Βλ. Φ. Παναγοπούλου-Κουντατζή, *Η εξέλιξη του δικαιώματος στη λήθη (2017)* και ενδεικτικά απόφαση *Segerstedt-Wiberg et al v. Sweden* του ΕΔΔΑ, υπέρ του δικαιώματος επανένταξης του ατόμου στην κοινωνία, περί διατήρησης ή μη αρχείων πολιτικά αντιφρονούντων από την εποχή του Ψυχρού Πολέμου.

Αποτελεί ένδειξη της μεταρρυθμιστικής πρόθεσης του νομοθέτη του ΓΚΠΔ για ενίσχυση της ικανότητας των φυσικών προσώπων να ελέγχουν τα δεδομένα τους¹⁹¹ και αφορά το δικαίωμα του ατόμου στην προσωπικότητά του και στο πώς θα την παρουσιάσει στους τρίτους. Διασφαλίζεται με τον τρόπο αυτό η ατομική αυτονομία και η προστασία από την ακούσια έκθεση, κυρίως στο διαδίκτυο (ψηφιακή λήθη), που πολλάκις μετατρέπει το υποκείμενο των δεδομένων σε εργαλείο εξυπηρέτησης εμπορικών και άλλων σκοπών. Ο διαδικτυακός «στιγματισμός» ενός χρήστη, λόγω της δημοσιότητας που έλαβε κάποια αρνητική πληροφορία γι' αυτόν, τον μετατρέπει σε «θύμα» του παρελθόντος του, αφού τα ψηφιακά δεδομένα που τον εκθέτουν, μένουν ανεξίτηλα και διαθέσιμα σε επικρίσεις των υπόλοιπων μελών της διαδικτυακής κοινότητας¹⁹². Βάσει λοιπόν του δικαιώματος αυτού, το υποκείμενο μπορεί να ζητήσει από τον υπεύθυνο της επεξεργασίας τη διαγραφή ή τη διόρθωση δεδομένων προσωπικού χαρακτήρα που το αφορούν, χωρίς αδικαιολόγητη καθυστέρηση και χωρίς την επίκληση ζημίας, εάν άρει τη συγκατάθεσή του ή εάν η διατήρηση των δεδομένων δεν είναι σύμφωνη με τον Κανονισμό και εφόσον δεν υφίστανται άλλοι νόμιμοι λόγοι διατήρησής τους¹⁹³. Ειδικότερα, το δικαίωμα «να λησμονηθεί» δίνει στο υποκείμενο τη δυνατότητα να σβήσει από το διαδίκτυο πληροφορίες που δεν επιθυμεί, αρκεί να μην είναι πλέον απαραίτητες σε σχέση με τους σκοπούς για τους οποίους συλλέχθηκαν, ή να μην υφίσταται νομική βάση ή νόμιμοι λόγοι για την επεξεργασία τους, ή να υποβλήθηκαν παράνομα σε επεξεργασία, ή να υφίσταται νομική υποχρέωση του υπευθύνου επεξεργασίας ή να αφορά παιδιά και να πρέπει να γίνει στάθμιση συμφερόντων κατά τα οριζόμενα στην αιτιολογική σκέψη 38 του ΓΚΠΔ. Σύμφωνα με τον Ευρωπαϊό Επόπτη Προστασίας Προσωπικών Δεδομένων, το δικαίωμα διαγραφής του ψηφιακού παρελθόντος συνδέεται με το δικαίωμα στη φορητότητα (όπως θα αναλυθεί παρακάτω), καθώς αμφότερα ενισχύουν τη θέση του υποκειμένου των δεδομένων¹⁹⁴. Το πρόβλημα ανακύπτει από τη μεγάλη συσσώρευση δεδομένων στο διαδίκτυο και τη δυνατότητα ανίχνευσής τους μέσω μηχανών αναζήτησης. Το δικαίωμα διαγραφής αφορά κατά κύριο λόγο, σύμφωνα με τη νομολογία¹⁹⁵ και τη διοικητική πρακτική των

¹⁹¹ Βλ. ανακοίνωση Επιτροπής που κατατέθηκε μαζί με τον ΓΚΠΔ.

¹⁹² Βλ. I. Γγλεζάκη (2014), *όπ.ανωτ.*, σελ.13-14.

¹⁹³ Βλ. I. Γγλεζάκη (2014), *όπ.ανωτ.*, σελ.108.

¹⁹⁴ Βλ. I. Γγλεζάκη (2014), *όπ.ανωτ.*, σελ.114.

¹⁹⁵ Βλ. ενδεικτικά προδικαστική παραπομπή ενώπιον του ΔΕΕ για το δικαίωμα της λήθης, υπόθεση C-131/12: προσφυγή πολίτη κατά της μηχανής αναζήτησης Google στην Ισπανία προκειμένου να μην

ανεξάρτητων αρχών, την απαλοιφή αποτελεσμάτων από τις μηχανές αναζήτησης στο διαδίκτυο. Ο χρήστης του διαδικτύου δικαιούται να αιτηθεί την αφαίρεση συνδέσμου, που με τη χρήση μιας λέξης - κλειδιού εμφανίζει πληροφορίες που το αφορούν και αποτελούν προσωπικά του δεδομένα, τα οποία δεν επιθυμεί να δημοσιοποιεί, ώστε να μη γίνεται εκ νέου αντικείμενο δημοσιογραφικού ή άλλου ενδιαφέροντος ένα δυσάρεστο κομμάτι του πρότερου βίου του¹⁹⁶. Ταυτόχρονα όμως ανακύπτει ζήτημα σύγκρουσης των ατομικών δικαιωμάτων - ελευθεριών, με την ελευθερία της έκφρασης, της πληροφόρησης, την ελευθερία του Τύπου¹⁹⁷ και τη δυνατότητα ανεμπόδιστης πρόσβασης στην πληροφορία¹⁹⁸. Εύλογη ανησυχία προκαλεί το γεγονός ότι η δυνατότητα ελέγχου του περιεχομένου του διαδικτύου, το οποίο μέχρι πρότινος αποτελούσε χώρο ελευθερίας, δύναται να αποτελέσει ένα είδος «λογοκρισίας», η οποία μπορεί να αποφευχθεί, εάν επιλέγεται η διαγραφή των πληροφοριών που δεν είναι χρήσιμες για την ενημέρωση του κοινού. Το δικαίωμα διαγραφής δεν είναι απόλυτο, αλλά υπόκειται σε στάθμιση συμφερόντων κατ' εφαρμογή της αρχής της αναλογικότητας και επιτρέπεται όταν δεν υπάρχει ηπιότερο μέσο για την επίτευξη του ίδιου σκοπού¹⁹⁹. Συνεπώς δεν μπορεί να ασκηθεί²⁰⁰ στις περιπτώσεις της τήρησης νομικής υποχρέωσης που επιβάλλει τη διατήρηση δεδομένων²⁰¹, για λόγους δημοσίου συμφέροντος στον τομέα της δημόσιας υγείας²⁰², για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς ιστορικούς,

εμφανίζεται η πληροφορία έκδοσης προγράμματος πλειστηριασμού σε βάρος της περιουσίας του λόγω ασφαλιστικών οφειλών, βλ. *I. Ιγγλεζάκη (2014), όπ.ανωτ., σελ.86 επόμε.*

¹⁹⁶ Βλ. *Φ. Παναγοπούλου-Κουτνατζή (2017γ), όπ.ανωτ.*

¹⁹⁷ Βλ. ενδεικτική νομολογία ΕΔΔΑ: υπόθεση *Mosley* κατά Ηνωμένου Βασιλείου περί χάραξης ορίων μεταξύ ιδιωτικότητας και ελευθερίας του Τύπου, αριθ.48009/08, 10.5.2011, Εφαρμογές ΔΔ 2011, σελ.287 επόμε.

¹⁹⁸ Βλ. άρθρο 17 παρ. 3 περ. α' ΓΚΠΔ, όπου ορίζεται ότι οι παράγραφοι 1 και 2 δεν εφαρμόζονται στο βαθμό που η επεξεργασία είναι απαραίτητη για την άσκηση του δικαιώματος ελευθερίας της έκφρασης και του δικαιώματος στην ενημέρωση. Για τη σύγκρουση ανάμεσα στην ελευθερία της έκφρασης και του τύπου, όπως κατοχυρώνεται στο άρθ. 10 ΕΣΔΑ και του δικαιώματος στην προστασία της ιδιωτικότητας (άρθ. 8 ΕΣΔΑ) υπάρχει πλούσια νομολογία του ΕΔΔΑ, όπως επί παραδείγματι η υπόθεση *Delfi* κατά Εσθονίας αριθ.64569/09/10-10-2013, η υπόθεση *Van Hannover* αριθ.2/7-2-2012 κ.ά., βλ. *I. Ιγγλεζάκη (2014), όπ.ανωτ., σελ.180 επόμε.*

¹⁹⁹ Βλ. *I. Ιγγλεζάκη (2014), όπ.ανωτ., σελ.189 επόμε.*

²⁰⁰ Στους λόγους εξαίρεσης από την υποχρέωση διαγραφής πρότεινε η Επιτροπή Βιομηχανίας, Έρευνας και Ενέργειας να προστεθεί και η πρόληψη ή ο εντοπισμός απάτης, η επιβεβαίωση στοιχείων ταυτότητας ή/και ο προσδιορισμός της φερεγγυότητας ή της ικανότητας πληρωμής, ενώ η Επιτροπή Εσωτερικής Αγοράς και Προστασίας των Καταναλωτών πρότεινε την αποθήκευση στοιχείων σχετικά με το ιστορικό της υπόθεσης, όταν ο υπεύθυνος επεξεργασίας είναι δημόσια αρχή, βλ. *I. Ιγγλεζάκη (2014), όπ.ανωτ., σελ.190.*

²⁰¹ Βλ. Οδηγία 2006/24/ΕΚ για την υποχρεωτική διατήρηση και μη διαγραφή δεδομένων στις περιπτώσεις που αναφέρει και Ν.3917/2011 που μετέφερε την Οδηγία στο ελληνικό δίκαιο.

²⁰² Σύμφωνα με το άρθ. 81 της πρότασης Κανονισμού, ως λόγοι δημοσίου συμφέροντος στον τομέα της δημόσιας υγείας αναφέρονται ενδεικτικά η προστασία κατά σοβαρών διασυννοριακών απειλών της υγείας ή η διασφάλιση ποιότητας και ασφάλειας για φαρμακευτικά προϊόντα ή ιατρικές συσκευές. «Δημόσια υγεία»: ερμηνεία όρου βάσει Κανονισμού αριθ.1338/2008 Ευρωπαϊκού Κοινοβουλίου.

στατιστικούς ή επιστημονικής έρευνας²⁰³, για την άσκηση του δικαιώματος ελευθερίας της έκφρασης, όταν υφίσταται λόγος περιορισμού της επεξεργασίας και όχι διαγραφής των δεδομένων και στις περιπτώσεις νομικής αξίωσης. Το όριο του δικαιώματος αυτού αναζητείται στην ελευθερία του πληροφορείν και του πληροφορείσθαι και δεν πρέπει να λαμβάνει χώρα διαγραφή γεγονότων που προκαλούν το εύλογο ενδιαφέρον ενημέρωσης του κοινού ή που συμβάλλουν στη διατήρηση της ιστορικής αλήθειας²⁰⁴. Το κράτος μάλιστα, προβαίνει στη δημοσιοποίηση μεγάλου αριθμού δεδομένων προσωπικού χαρακτήρα, στα πλαίσια της επικαλούμενης απαίτησης προστασίας του κοινωνικού συνόλου, της πρόληψης εγκλημάτων και της υπεράσπισης της διαφάνειας της κρατικής δράσης. Για το λόγο αυτό, για παράδειγμα, η διάταξη της περ.β' του άρθρου 2 Ν.2472/1997 επιτρέπει στην εισαγγελική αρχή και υπό ορισμένες προϋποθέσεις, να δημοσιοποιεί πληροφορίες αναφορικά με ποινικές διώξεις ή καταδίκες. Επίσης, μεγάλος αριθμός προσωπικών δεδομένων αναρτώνται υποχρεωτικά στο διαδίκτυο από δημόσιους φορείς, βάσει του Ν.3861/2010²⁰⁵ που αφορά το πρόγραμμα «Διαύγεια»²⁰⁶. Επιπροσθέτως, στο άρθρο 85 του Κώδικα Φορολογίας Εισοδήματος, προβλέπεται δυνατότητα δημοσιοποίησης από το Υπουργείο Οικονομικών, καταλόγου φορολογουμένων. Όλα τα παραπάνω συμβάλλουν στη δημιουργία τεράστιου αριθμού πληροφοριών, διαθέσιμων σε όλους ανεξαιρέτως, χωρίς χρονικούς ή άλλους περιορισμούς, δημιουργώντας ένα «Πανοπτικό» της Δημόσιας Διοίκησης, με τις αντίστοιχες αναμενόμενες παρενέργειες²⁰⁷. Οι κυρώσεις που επιβάλλονται για την παράβαση των δικαιωμάτων των υποκειμένων σύμφωνα με τα άρθρα 12 έως 22 του ΓΚΠΔ, επισύρουν κατά την παράγραφο 5 του άρθρου 83 του ΓΚΠΔ διοικητικά πρόστιμα έως 20.000.000 ευρώ για τον δημόσιο τομέα ή έως 4% του ετήσιου κύκλου εργασιών, σε περίπτωση που ο παραβάτης είναι επιχείρηση.

²⁰³ Βλ. και άρθ. 7 παρ.2 εδαφ.στ' Ν.2472/1997.

²⁰⁴ Βλ. απόφαση Ανωτάτου Ιαπωνικού Δικαστηρίου που τάχθηκε κατά του δικαιώματος στη λήθη για την περίπτωση παιδόφιλου, ηλεκτρονική πηγή: <https://www.theguardian.com/world/2017/feb/02/right-to-be-forgotten-online-suffers-setback-after-japan-court-ruling> και Φ. Παναγοπούλου-Κουτνατζή, Τα νέα δικαιώματα για τους πολίτες βάσει του ΓΚΠΔ: μια πρώτη αποτίμηση και συνταγματική αξιολόγηση (2017), σελ.88.

²⁰⁵ Ν.3861/2010 περί «Ενίσχυσης της διαφάνειας με την υποχρεωτική ανάρτηση νόμων και πράξεων των κυβερνητικών διοικητικών και αυτοδιοικητικών οργάνων στο διαδίκτυο "Πρόγραμμα Διαύγεια" και άλλες διατάξεις».

²⁰⁶ Βλ. ιστότοπο: <http://diavgeia.gov.gr/>.

²⁰⁷ Βλ. Ι. Ιγγλεζάκη (2014), όπ.ανωτ., σελ.10 επόμ.

Δικαίωμα στη φορητότητα²⁰⁸ των δεδομένων από έναν πάροχο υπηρεσίας σε έναν άλλο: πρόκειται για μία ακόμα νέα ρύθμιση του ΓΚΠΔ, σύμφωνα με την οποία το υποκείμενο μπορεί να ζητήσει από τον υπεύθυνο επεξεργασίας στον οποίο έχει παράσχει τα προσωπικά του δεδομένα, να τα λάβει δωρεάν²⁰⁹, ανεμπόδιστα, σε ηλεκτρονικό και δομημένο μορφότυπο συνήθους χρήσης²¹⁰ ή να τα διαβιβάσει αυτός απευθείας σε άλλο υπεύθυνο επεξεργασίας. Παρέχει δηλαδή, με άλλα λόγια, τη δυνατότητα στα υποκείμενα των προσωπικών δεδομένων, να παραλάβουν και να χρησιμοποιήσουν τα ψηφιοποιημένα δεδομένα που τους αφορούν, για άλλους σκοπούς, σε άλλες υπηρεσίες της επιλογής τους και μάλιστα η ενημέρωση εκ μέρους του υπευθύνου επεξεργασίας για την ύπαρξη αυτού του δικαιώματος, είναι υποχρεωτική. Το εν λόγω δικαίωμα παρέχεται όταν η επεξεργασία των δεδομένων βασίζεται σε συγκατάθεση του υποκειμένου (δηλαδή να έχουν χορηγηθεί από το ίδιο το υποκείμενο, του οποίου η ταυτότητα εξακριβώνεται για λόγους ασφαλείας) ή σε σύμβαση²¹¹ και όταν αυτή διενεργείται με αυτοματοποιημένα μέσα, συνεπώς δεν καλύπτει την περίπτωση των έγγραφων αρχείων, εκτός εάν αυτά ψηφιοποιηθούν. Ευνόητο είναι πως το δικαίωμα λήψης των δεδομένων δεν μπορεί να ασκηθεί κατά υπευθύνου που επεξεργάζεται προσωπικά δεδομένα κατά την εκπλήρωση καθήκοντος που του έχει νομίμως ανατεθεί και που εκτελείται χάριν του δημοσίου συμφέροντος ή κατά την ανατεθείσα άσκηση δημόσιας εξουσίας. Άλλη μία εξαίρεση άσκησης του εν λόγω δικαιώματος, είναι η περίπτωση όπου θίγονται δικαιώματα και ελευθερίες τρίτων προσώπων, δεδομένα των οποίων συνυπάρχουν με αυτά του υποκειμένου, όπως για παράδειγμα τα δεδομένα του τραπεζικού λογαριασμού. Η προθεσμία ικανοποίησης του αιτήματος φορητότητας είναι ένας μήνας²¹² από την παραλαβή του, με δικαίωμα παράτασης κατά δύο ακόμη μήνες, εάν κριθεί απαραίτητο.

Ο βαθύτερος στόχος του νομοθέτη στη δημιουργία του δικαιώματος στη φορητότητα, ήταν η ελεύθερη διασυνοριακή ροή των δεδομένων. Η μεταφορά δεδομένων μέσω μηχανικά αναγνώσιμων τύπων κοινώς χρησιμοποιούμενων, ευνοεί άλλωστε τη συνεργασία επιχειρήσεων, τον ανταγωνισμό μεταξύ των παρόχων υπηρεσιών και τη διαλειτουργικότητα. Στον αντίποδα των θετικών χαρακτηριστικών της εφαρμογής του

²⁰⁸ *The right to data portability*, βλ. άρθ. 20 ΓΚΠΔ.

²⁰⁹ Βλ. άρθ. 12 παρ. 5 ΓΚΠΔ με τους περιορισμούς που τίθενται σε αυτό.

²¹⁰ Στην αιτιολογική σκέψη 21 του Προοιμίου της Οδηγίας 2013/37/ΕΕ που αφορά την τροποποίηση της Οδηγίας 2003/98/ΕΚ σχετικά με την περαιτέρω χρήση πληροφοριών του δημόσιου τομέα, περιγράφεται η έννοια του εγγράφου σε μηχαναγνώσιμο μορφότυπο.

²¹¹ Χαρακτηριστικό παράδειγμα η δυνατότητα που παρέχει η διοίκηση να λαμβάνουν οι φορολογούμενοι με ηλεκτρονικά μέσα παλιότερα φορολογικά τους δεδομένα.

²¹² Βλ. άρθ. 12 παρ. 3 ΓΚΠΔ.

δικαιώματος, βρίσκεται η ανησυχία περί της ασφαλούς μεταφοράς των δεδομένων. Η διαβίβαση μπορεί να ελλοχεύει κινδύνους κλοπής, ή μεταφοράς σε λανθασμένο πρόσωπο, να είναι αθέμιτη, να ευνοήσει την παρακολούθηση των δεδομένων, κίνδυνοι που θα πρέπει να ληφθούν σοβαρά υπόψη και να ενισχυθούν τα μέτρα ασφαλείας με την ορθή εκμετάλλευση της τεχνολογίας²¹³.

Σκόπιμο κρίνεται στο σημείο αυτό να διασαφηνιστεί η ευρύτατα χρησιμοποιούμενη στον Κανονισμό νομική έννοια «**δημόσιο συμφέρον**», η οποία ταυτίζεται με το γενικό συμφέρον των πολιτών ενός κράτους. Συγκεκριμένα, ο όρος αφορά την ικανοποίηση βασικών αναγκών των πολιτών ενός κράτους, όπως επί παραδείγματι η εθνική άμυνα, η τάξη, η ασφάλεια, η υγεία, η παιδεία, η συγκοινωνία, η οικονομική ανάπτυξη κ.ά. Το δημόσιο συμφέρον μπορεί κάποιες φορές να αντιτίθεται προς τα συμφέροντα ορισμένων μελών της κοινωνίας, για το λόγο αυτό αποτελεί προϋπόθεση και όριο του συνταγματικά επιτρεπτού περιορισμού των ατομικών δικαιωμάτων²¹⁴.

Δικαίωμα ενημέρωσης σε περιπτώσεις παραβίασεως²¹⁵ (Data breach notification): όπως προαναφέρθηκε και σύμφωνα με την εκτίμηση 85 του Προοιμίου του ΓΚΠΔ, κρίνεται αναγκαία η έγκαιρη αντιμετώπιση παραβίασης προσωπικών δεδομένων προς αποφυγή των αναφερόμενων πιθανών βλαβών²¹⁶. Για το λόγο αυτό, ο ΓΚΠΔ διευρύνει το ήδη υφιστάμενο δικαίωμα ενημέρωσης του υποκειμένου και συγκεκριμένα θεσπίζει την υποχρέωση του υπευθύνου επεξεργασίας να γνωστοποιήσει το περιστατικό της παραβίασης τόσο στην εποπτική αρχή, όσο και στο υποκείμενο, εάν ενδέχεται να προκληθεί κίνδυνος στα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, προκειμένου να ληφθούν τα απαραίτητα μέτρα περιορισμού των δυσμενών συνεπειών. Στην ενημέρωση της Αρχής περιλαμβάνονται αρκετές λεπτομέρειες, όπως ο αριθμός των επηρεαζόμενων υποκειμένων, το είδος της παραβίασης, οι ενδεχόμενες συνέπειες, τα μέτρα που έχουν ληφθεί ή που πρέπει να ληφθούν κ.ά. Η παρούσα πρόβλεψη εξυπηρετεί το δικαίωμα του ατόμου για πληροφοριακό αυτοκαθορισμό και γνώση του αποδέκτη των δεδομένων του. Επίσης, βαρύτητα δίδεται στους χειρισμούς του υπευθύνου επεξεργασίας και στη συνεργασία του με την αρμόδια Αρχή²¹⁷.

²¹³ Βλ. εισήγηση Φ. Παναγοπούλου Κουτνατζή, *Το νέο πλαίσιο δικαιωμάτων*, σε: Α. Κοτσαλή/Κ. Μενουδάκο (επιμ.), *όπ.ανωτ.* (2018), σελ.23 επόμε.

²¹⁴ Βλ. Ε. Σπηλιωτόπουλο, *Εγχειρίδιο Διοικητικού Δικαίου*, τόμος I (2017), σελ.79 επόμε.

²¹⁵ Βλ. άρθρα 33 και 34 ΓΚΠΔ.

²¹⁶ Ενδεικτικά: απώλεια ελέγχου των δεδομένων, υποκλοπή ταυτότητας, βλάβη της φήμης κ.ά.

²¹⁷ Βλ. εισήγηση Φ. Παναγοπούλου-Κουτνατζή, *Το νέο πλαίσιο δικαιωμάτων*, σε: Α. Κοτσαλή/Κ. Μενουδάκο (επιμ.), *όπ.ανωτ.* (2018), σελ.32.

Δικαίωμα εξασφάλισης ανθρώπινης παρέμβασης ή αντίταξης στη δημιουργία προφίλ²¹⁸: πρόκειται για ένα ιδιότυπο δικαίωμα εναντίωσης, σύμφωνα με το οποίο το υποκείμενο των δεδομένων δικαιούται να μην υπόκειται σε απόφαση που παράγει έννομα αποτελέσματα που το αφορούν ή που το επηρεάζει σημαντικά, αν αυτή λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας, συμπεριλαμβανομένης της κατάρτισης «προφίλ»²¹⁹. Ωστόσο, κατ' εξαίρεση η επεξεργασία επιτρέπεται, όταν υφίσταται ρητή πρόβλεψη από το δίκαιο στο οποίο υπόκειται ο υπεύθυνος επεξεργασίας, κυρίως για σκοπούς παρακολούθησης και πρόληψης απάτης και φοροδιαφυγής, όταν η επεξεργασία είναι αναγκαία για σύναψη ή εκτέλεση σύμβασης μεταξύ υποκειμένου και υπευθύνου ή, τέλος, όταν υφίσταται ρητή συγκατάθεση του υποκειμένου. Σε κάθε περίπτωση όμως η επεξεργασία πρέπει να περιβάλλεται εγγυήσεων περί δικαιωμάτων εξασφάλισης ανθρώπινης παρέμβασης, περί ειδικής ενημέρωσης του υποκειμένου, διατυπώσεως της άποψής του, λήψης αιτιολογημένης απόφασης και αμφισβήτησης της απόφασης. Σύμφωνα με την Παναγοπούλου-Κουτνατζή (2018)²²⁰, το δικαίωμα στην ανθρώπινη παρέμβαση επιχειρεί να αντιμετωπίσει το φόβο εργαλειοποίησης του ατόμου και βασίζεται στα δικαιώματα της ελεύθερης ανάπτυξης της προσωπικότητας και της παρουσίας του εαυτού μας, δεδομένου ότι δεν είμαστε απλές πληροφορίες για να αξιολογούμαστε αποκλειστικά από μηχανές. Ο άνθρωπος είναι κάτι πιο προσωπικό από απλά δεδομένα και πρέπει να αντιμετωπίζεται ως προσωπικότητα βάσει της γνώμης που σχηματίζει ο τρίτος γι' αυτόν. Βέβαια θα πρέπει να συνεκτιμηθεί ο κίνδυνος της υποκειμενικής αξιολόγησης και των διακρίσεων, φόβος που δεν υφίσταται αν η απόφαση λαμβάνεται αποκλειστικά με τεχνικά μέσα.

Δικαίωμα περιορισμού της επεξεργασίας: ο ΓΚΠΔ κατοχυρώνει το δικαίωμα αυτό στο άρθρο 18, όπου απαριθμούνται οι περιπτώσεις που το υποκείμενο των δεδομένων δικαιούται να ζητήσει από τον υπεύθυνο επεξεργασίας τον περιορισμό της επεξεργασίας, προκειμένου να προστατευθεί προσωρινά εν όψει διαλεύκανσης της νομικής κατάστασης. Το δικαίωμα περιορισμού δεν αποτελεί νέο εξ ολοκλήρου

²¹⁸ Βλ. άρθ. 22 ΓΚΠΔ.

²¹⁹ *Profiling χρηστών σε τραπεζικό - χρηματοοικονομικό τομέα, υγειονομική περίθαλψη, φορολογία, ασφάλιση, μάρκετινγκ, διαφήμιση κ.ά. «Κατάρτιση προφίλ»:* οποιαδήποτε μορφή αυτοματοποιημένης επεξεργασίας προσωπικών δεδομένων που συνίσταται στη χρήση των δεδομένων για την αξιολόγηση πτυχών του φυσικού προσώπου, ιδίως στην ανάλυση ή πρόβλεψη στοιχείων που αφορούν την απόδοση στην εργασία, την οικονομική κατάσταση, την υγεία, τις προσωπικές προτιμήσεις, τα ενδιαφέροντα, την αξιοπιστία, τη συμπεριφορά, τη θέση ή τις μετακινήσεις του φυσικού προσώπου (Αιτιολογική σκέψη 71 Προοιμίου ΓΚΠΔ).

²²⁰ Σε Α. Κοτσαλή/Κ. Μενουδάκο (επιμ.), *όπ.ανωτ.*, σελ 34.

δημιούργημα του Κανονισμού, αλλά απόρροια του ήδη προϋπάρχοντος δικαιώματος αντιτάξεως και αυτό αποτελεί ένδειξη ότι σε γενικές γραμμές ο ΓΚΠΔ δεν δημιούργησε νέα δικαιώματα αλλά επικαιροποίησε ήδη υφιστάμενα και συνταγματικά κατοχυρωμένα. Χρήζει διερεύνησης εάν οι προεκτάσεις που δόθηκαν στα δικαιώματα από τον Κανονισμό αποδειχθούν αποτελεσματικές κατά την εφαρμογή τους.

Λοιπά δικαιώματα Υποκειμένων

Ένα από τα βασικά δικαιώματα που παρέχει ο Κανονισμός στα υποκείμενα των δεδομένων είναι το **δικαίωμα ενημέρωσης**²²¹: ο υπεύθυνος επεξεργασίας μεριμνά ώστε να παρέχονται στο υποκείμενο όλες οι πληροφορίες που αφορούν την επεξεργασία των δεδομένων του, με σαφή και κατανοητό τρόπο. Οφείλει να προβλέπει διαδικασίες και μηχανισμούς που αφορούν την άσκηση των δικαιωμάτων των υποκειμένων των δεδομένων, όπως επίσης τρόπους υποβολής ηλεκτρονικών αιτημάτων, ενώ υποχρεούται σε απάντηση εντός ορισμένων προθεσμιών και σε αιτιολόγηση επί απορρίψεως αιτήματος²²².

Το δικαίωμα **πρόσβασης στα δεδομένα** παρέχει στο υποκείμενο τη δυνατότητα να λαμβάνει από τον υπεύθυνο επεξεργασίας επιβεβαίωση για το κατά πόσο υφίστανται επεξεργασία τα προσωπικά δεδομένα του και να έχει πρόσβαση στις πληροφορίες που αναφέρει το άρθρο 15 ΓΚΠΔ²²³.

Άλλο ένα δικαίωμα του υποκειμένου αφορά τη **διόρθωση** των ανακριβών δεδομένων που το αφορούν και τη συμπλήρωση ελλιπών στοιχείων κατά το άρθρο 16 ΓΚΠΔ. Σύμφωνα τέλος με το δικαίωμα **εναντίωσης (αντίρρησης / αντίταξης)**, το υποκείμενο μπορεί ανά πάσα στιγμή να αντιτάσσεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που το αφορούν.

²²¹ Βλ. άρθ. 12 ΓΚΠΔ.

²²² Βλ. Δ. Ζωγραφόπουλο, *Οδηγός προετοιμασίας για τη συμμόρφωση προς τον ΓΚΠΔ/GDPR-Βασικές κατευθύνσεις (2018)*, σελ. 9.

²²³ *Επί παραδείγματι τους σκοπούς της επεξεργασίας, το δικαίωμα υποβολής καταγγελίας στην Αρχή κ.ά.*

5. Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων και Δημόσια Διοίκηση

5.1. Καινοτομίες που αφορούν τη Δημόσια Διοίκηση

Οι επιχειρησιακοί τομείς που ανήκουν στο Δημόσιο και παρουσιάζουν ενδιαφέρον όσον αφορά τα προσωπικά δεδομένα, είναι κυρίως η υγεία, η εκπαίδευση, η κοινωνική ασφάλιση, η φορολογία, η δικαιοσύνη και οι μεταφορές. Η έκρηξη της τεχνολογίας οδήγησε στην αύξηση του αριθμού των δεδομένων και στη δημιουργία τεχνολογικών όρων όπως «Cloud Computing²²⁴», «Big Data²²⁵» ή «Internet of Things²²⁶», οι οποίοι αναμένεται να τύχουν εφαρμογής ακόμα και από το Δημόσιο.

Η άποψη ότι τεχνολογία και δίκαιο βρίσκονται σε σχέση αντίθεσης και ανταγωνισμού πρέπει να αλλάξει και να αντικατασταθεί από την πεποίθηση ότι οι δύο αυτές έννοιες είναι αλληλοσυμπληρούμενες και αλληλοεξαρτώμενες.

Ειδικότερα²²⁷, στα πλαίσια του εκσυγχρονισμού της Δημόσιας Διοίκησης (στο εξής ΔΔ), εισήλθαν οι τεχνολογίες της πληροφορικής και των υπολογιστών, όπως επίσης και νέες διοικητικές πρακτικές, δημιουργώντας την Ηλεκτρονική Διακυβέρνηση (e-government), βάσει της οποίας παράγονται και διανέμονται ηλεκτρονικά οι υπηρεσίες. Η ΔΔ βρίσκεται σε ένα κομβικό σημείο όπου οφείλει να πετύχει τον ψηφιακό της μετασχηματισμό, αρχικά μέσω της διαλειτουργικότητας των πληροφοριακών της συστημάτων και της ανάπτυξης υπηρεσιών διαδικτύου. Η διαλειτουργικότητα αναφέρεται στη χρήση κοινών προτύπων επικοινωνίας μεταξύ των πληροφοριακών συστημάτων και μέσω αυτής, οι διοικητικοί φορείς είναι σε θέση να ανταλλάσσουν δεδομένα και οι πολίτες να εξυπηρετούνται από την παροχή ψηφιακών δημόσιων υπηρεσιών²²⁸. Μάλιστα, στο πλαίσιο της ανάπτυξης της πληροφοριακής υποδομής του δημόσιου τομέα, δημιουργήθηκε το Κυβερνητικό Υπολογιστικό Νέφος (Government Cloud ή G-Cloud), το οποίο αποτελεί ένα

²²⁴ Υπολογιστικό νέφος: όταν η επεξεργασία, η χρήση και η αποθήκευση των δεδομένων γίνεται διαδικτυακά και προσφέρει στο χρήστη ευελιξία και υψηλή αυτοματοποίηση.

²²⁵ Μεγάλα Δεδομένα: τεράστιος όγκος δεδομένων που είναι σχεδόν αδύνατον να επεξεργαστεί με τις παραδοσιακές μεθόδους.

²²⁶ Διαδίκτυο των πραγμάτων: η «έξυπνη» σύνδεση ηλεκτρονικών συσκευών μεταξύ τους, ώστε να επιτρέπεται στο χρήστη να τις ελέγχει από υπολογιστή ή κινητό.

²²⁷ Βλ. Μ. Μυλώση, *Ο Ευρωπαϊκός Κανονισμός Προστασίας Δεδομένων (ΕΕ) 2016/679 και οι αλλαγές που επιφέρει στην οργάνωση και τη λειτουργία της Δημόσιας Διοίκησης (2018)*, αδημοσίευτο.

²²⁸ Παραδείγματα διαλειτουργικότητας: η αυτεπάγγελτη αναζήτηση Πιστοποιητικού από μία Υπηρεσία σε μία άλλη, η αλληλεπίδραση μεταξύ ΕΦΚΑ & ΗΔΙΚΑ κ.ά.

πρωτοποριακό εγχείρημα της ελληνικής ΔΔ όσον αφορά την κοινή χρήση υπολογιστικών υποδομών από τους δημόσιους φορείς²²⁹.

Οι δημόσιοι φορείς οφείλουν, κατά την παροχή των υπηρεσιών, να μεριμνούν για την ασφάλεια των εφαρμοζόμενων πληροφοριακών συστημάτων και να τηρούν τις αρχές της νομιμότητας, της διαφάνειας και της χρηστής διοίκησης. Πληροφοριακή υποχρέωση της ΔΔ αποτελεί επίσης ο σεβασμός του δικαιώματος προστασίας των προσωπικών δεδομένων των φυσικών προσώπων και της ιδιωτικότητας αυτών. Για τους λόγους αυτούς θα πρέπει προληπτικά η Διοίκηση να διερευνά τις επιπτώσεις που θα έχει η επεξεργασία των δεδομένων των πολιτών, διασφαλίζοντας ότι η επεξεργασία θα πραγματοποιηθεί σε όσο το δυνατόν λιγότερα προσωπικά δεδομένα. Η συνεργασία με την εποπτική αρχή υπό τη μορφή γνωμοδοτήσεων, η αναζήτηση της συγκατάθεσης του ατόμου για την επεξεργασία των δεδομένων του και η εξασφάλιση του δικαιώματος ανάκλησης αυτής, αποτελούν βήματα προς τη θετική κατεύθυνση της συμμόρφωσης της ΔΔ με τον Κανονισμό.

Οι σύγχρονες επιταγές επιβάλλουν τον συγκερασμό των νέων αναγκών υπηρεσιών στην ελληνική επικράτεια, με την εξέλιξη των νέων τεχνολογιών και εφαρμογών. Η πλειοψηφία των δημοσίων φορέων²³⁰ διαχειρίζεται μεγάλο όγκο προσωπικών δεδομένων των πολιτών: ασφαλιστικοί φορείς, φορολογικές αρχές²³¹, φορείς που υπάγονται στο υπουργείο υγείας ή προστασίας του πολίτη κλπ.

Οι νομικές αλλαγές όμως που επέφερε ο ΓΚΠΔ στον δημόσιο τομέα είναι λιγότερο έντονες²³², καθόσον: α) η συγκατάθεση του υποκειμένου δεν κρίνεται εξίσου σημαντική όπως στον ιδιωτικό τομέα, β) βάσει του εδαφίου ε' της παραγράφου 1 του άρθρου 6, το Δημόσιο χρησιμοποιεί ως νομική βάση και δικαιολογία της επεξεργασίας των δεδομένων που εκτελεί και που την καθιστά νόμιμη, την επιδίωξη του δημοσίου συμφέροντος και την άσκηση δημόσιας εξουσίας και γ) τα δικαιώματα του υποκειμένου στη λήθη και στη φορητότητα των δεδομένων του θεωρούνται περιορισμένης ή και απίθανης εφαρμογής.

²²⁹ Βλ. ιστότοπο: <https://www.gcloud.ktpae.gr>.

²³⁰ Βλ. Εγκύκλιο ΔΙΔΔΑ /Φ.10/οικ.22518/22-6-2018 του Υπουργείου Διοικητικής Ανασυγκρότησης περί δημοσίευσης του επικαιροποιημένου «Μητρώου Υπηρεσιών και Φορέων της Ελληνικής Διοίκησης» έτους 2018, ηλεκτρονική πηγή: http://www.minadmin.gov.gr/wp-content/uploads/20180626_mitrowo_yphr_for.pdf.

²³¹ Στο άρθρ. 7 παρ.2 περ.ε' Ν.2472/1997 αίρεται η απαγόρευση επεξεργασίας ευαίσθητων δεδομένων όταν αυτή εκτελείται από Δημόσια Αρχή και είναι αναγκαία, μεταξύ άλλων, για την άσκηση δημοσίου φορολογικού ελέγχου ή δημόσιου ελέγχου κοινωνικών παροχών.

²³² Βλ. Ε. Σιουγλέ, ΓΚΠΔ και δικαιώματα των υποκειμένων των δεδομένων (2018), σελ.95.

5.2. Υπεύθυνος Προστασίας Δεδομένων (Data Protection Officer)

Μια από τις σημαντικές καινοτομίες που εισήγαγε ο ΓΚΠΔ, είναι η πρόβλεψη περί υποχρεωτικού ορισμού Υπευθύνου Προστασίας Δεδομένων (ΥΠΔ) για ορισμένες κατηγορίες υπευθύνων επεξεργασίας.

«Ο ΥΠΔ διευκολύνει τη συμμόρφωση του υπευθύνου επεξεργασίας και του εκτελούντος την επεξεργασία με τις διατάξεις του ΓΚΠΔ και μεσολαβεί μεταξύ των διαφόρων ενδιαφερομένων (όπως για παράδειγμα οι εποπτικές αρχές ή τα υποκείμενα των δεδομένων). Ο ρόλος του είναι συμβουλευτικός, όχι αποφασιστικός, και δεν φέρει προσωπική ευθύνη για τη μη συμμόρφωση με τον Κανονισμό²³³», καθώς οι αποφάσεις λαμβάνονται πάντα από τη Διοίκηση, στην οποία ο ίδιος λογοδοτεί απευθείας.

Ο θεσμός του ΥΠΔ στην ΕΕ προβλεπόταν στην Οδηγία 95/46/ΕΚ ως προαιρετικό μέτρο: στην παράγραφο 2 του άρθρου 18 προβλέπεται η δυνατότητα των κρατών-μελών να θεσπίσουν στο εσωτερικό τους δίκαιο το θεσμό του ΥΠΔ. Υποχρεωτικό ορισμό ΥΠΔ βάσει της Οδηγίας 95/46/ΕΚ συναντάμε στις νομοθεσίες ευρωπαϊκών κρατών όπως η Γερμανία, η Ισπανία, η Σλοβακία. Ειδικά στον γερμανικό νόμο του 2003 προβλέπεται γενική υποχρέωση διορισμού ΥΠΔ στο δημόσιο τομέα, ενώ στον ιδιωτικό γίνεται ο εξής διαχωρισμός: αν στην επιχείρηση διενεργείται αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων, διορίζεται ΥΠΔ αν απασχολείται προσωπικό άνω των εννέα ατόμων, ενώ αν η επεξεργασία δεν είναι αυτοματοποιημένη, το όριο ανέρχεται στα είκοσι άτομα²³⁴. Δεδομένου ότι στην Ελλάδα ο Ν.2472/1997 δεν είχε αντίστοιχη πρόβλεψη, ο θεσμός είναι πρωτόγνωρος για το ελληνικό δημόσιο και γι' αυτό αναμένεται να προκαλέσει μεγάλες αλλαγές²³⁵.

Βασικές ρυθμίσεις για τον ΥΠΔ περιλαμβάνονται στα άρθρα 37 έως 39 του ΓΚΠΔ, 32 έως 34 της Οδηγίας 2016/680/ΕΕ²³⁶ και στην αιτιολογική σκέψη 97 του Προοιμίου του ΓΚΠΔ.

²³³ Βλ. ηλεκτρονική πηγή: www.dpa.gr.

²³⁴ Βλ. Ι. Γγγλεζάκη, *Ο ΓΚΠΔ (2018β)*, σελ. 96.

²³⁵ Βλ. Ι. Γγγλεζάκη, *Ο Υπεύθυνος Προστασίας Δεδομένων κατά τον Κανονισμό 2016/679 και την Οδηγία 2016/680 (2018α)*, σελ.66.

²³⁶ Αφορά την επεξεργασία προσωπικών δεδομένων για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων κλπ., όπως αναλύεται ανωτέρω.

Ορισμός Υπευθύνου Προσωπικών Δεδομένων

Τη θέση του ΥΠΔ μπορεί να λάβει είτε υπάλληλος του φορέα (full time), ο οποίος δηλαδή τελεί σε σχέση εξαρτημένης εργασίας με τον υπεύθυνο ή τον εκτελούντα την επεξεργασία, είτε τρίτος με εξωτερική ανάθεση (part time), να παρέχει δηλαδή τις υπηρεσίες του με σύμβαση παροχής υπηρεσιών (εξωτερικός συνεργάτης). Τα κριτήρια με τα οποία θα κριθεί το είδος της συνεργασίας, είναι κυρίως το μέγεθος του Οργανισμού, ο όγκος των δεδομένων που επεξεργάζεται και ο χρόνος που απαιτείται για την εκπλήρωση των αρμοδιοτήτων του ΥΠΔ. Στην πράξη πάντως θα πρέπει να αποφεύγεται η ανάθεση του ρόλου ως «συμπληρωματικό καθήκον» σε κάποιο παραδοσιακό όργανο του φορέα, όπως επί παραδείγματι στο Νομικό Σύμβουλο ή στον Υπεύθυνο Τεχνικής Επεξεργασίας²³⁷.

Στο άρθρο 14 του ΣχΝΠΔΠΧ που αφορά τον ορισμό ΥΠΔ, εξαιρούνται από την υποχρέωση ορισμού ΥΠΔ μαζί με τα δικαστήρια και οι εισαγγελικές αρχές, ενώ στην παράγραφο 3 προβλέπεται ότι ο ορισμός του γίνεται εγγράφως, απαιτείται δηλαδή σύναψη σύμβασης ανάθεσης μεταξύ του υπευθύνου επεξεργασίας ή του εκτελούντα την επεξεργασία και του προσώπου που αναλαμβάνει, η οποία θα είναι ορισμένου χρόνου. Το διάστημα όμως δε θα πρέπει να είναι σύντομο, προκειμένου να διασφαλιστεί η ανεξαρτησία του ΥΠΔ, δεδομένου ότι στην ίδια διάταξη προβλέπεται και η δυνατότητα καταγγελίας της σύμβασης για σπουδαίο λόγο²³⁸ (κατά τα άρθρα 672-674 ΑΚ). Όσον αφορά το περιεχόμενο της σύμβασης, κατά το ίδιο άρθρο, αυτή περιλαμβάνει τη θέση, τα καθήκοντα του ΥΠΔ σύμφωνα με τα άρθρα 28 και 39 του ΓΚΠΔ και τον τρόπο με τον οποίο θα τα ασκεί.

Διχογνωμία επικρατεί περί του εάν επιτρέπεται να οριστεί και νομικό πρόσωπο²³⁹ ως ΥΠΔ πέραν του φυσικού, διότι σε Γνώμη της Ομάδας Εργασίας του άρθρου 29, αναφέρεται ότι τα καθήκοντα του ΥΠΔ μπορούν να ασκούνται βάσει σύμβασης παροχής υπηρεσιών, η οποία συνάπτεται με φυσικό πρόσωπο ή Οργανισμό εκτός του υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία. Αντίθετη άποψη²⁴⁰ υποστηρίζει ότι ο ΥΠΔ πρέπει να είναι φυσικό πρόσωπο, αφού στο άρθρο 37 παρ.6 του ΓΚΠΔ αναφέρεται ότι μπορεί να είναι μέλος του προσωπικού του υπευθύνου

²³⁷ Βλ. Α. Βαρβέρη, *Τεχνικά και οργανωτικά θέματα – η «υποχρεωτική» τοποθέτηση ΥΠΔ (2017)*, σελ.212.

²³⁸ Α.χ. ανάρμοστη συμπεριφορά, παράβαση συμβατικής υποχρέωσης, εξαπάτηση, πρόκληση σωματικών βλαβών κ.ά.

²³⁹ Όπως για παράδειγμα δικηγορική εταιρία ή εταιρία συμβούλων επιχειρήσεων.

²⁴⁰ Βλ. Ι. Ιγγλεζάκη, *Ο Υπεύθυνος Προστασίας Δεδομένων κατά τον Κανονισμό 2016/679 και την Οδηγία 2016/680 (2018α)*, όπ.ανωτ., σελ.67.

επεξεργασίας ή του εκτελούντος την επεξεργασία, ενώ η υποχρέωση εχεμύθειας που τον βαρύνει²⁴¹ επιφέρει ποινική ευθύνη, την οποία δε μπορεί να αναλάβει ένα νομικό πρόσωπο.

Ο ΥΠΔ εκφεύγει της δημοσιοϋπαλληλικής ιεραρχίας και λογοδοτεί απευθείας στο υψηλότερο διοικητικό επίπεδο, συνεπώς, ακόμα και εάν τη θέση του ΥΠΔ έχει λάβει υπάλληλος του φορέα, αυτός απολαμβάνει ανεξαρτησίας, όπως ορίζει η παράγραφος 3 του άρθρου 38 ΓΚΠΔ και η αιτιολογική σκέψη 97 του Προοιμίου, δηλαδή δε λαμβάνει εντολές για την άσκηση των καθηκόντων του, δεν απολύεται και δεν υφίσταται κυρώσεις επειδή επιτέλεσε τα καθήκοντά του. Όλα αυτά όμως δε συνεπάγονται και εξουσία λήψης αποφάσεων εκ μέρους του. Σκόπιμο μάλιστα κρίνεται να ανακοινώνεται ο ορισμός του με επίσημο τρόπο σε όλο το προσωπικό, ώστε να καθίσταται σε όλους γνωστή η ύπαρξη και οι αρμοδιότητές του, διαδικασία που δεν έχει ακόμα τύχει ευρείας εφαρμογής στην ελληνική ΔΔ.

Αρμοδιότητες και καθήκοντα του Υπευθύνου Προσωπικών Δεδομένων

Ο ΥΠΔ, μαζί με τον υπεύθυνο επεξεργασίας (άλλως data «controller», δηλαδή το φυσικό ή νομικό πρόσωπο που ελέγχει / εξουσιάζει το αρχείο), ο οποίος καθορίζει τον σκοπό και τους τρόπους επεξεργασίας, αποτελούν τους διαχειριστές των προσωπικών δεδομένων. Ο ΥΠΔ δεν είναι υπεύθυνος να τηρεί τη νομοθεσία των προσωπικών δεδομένων, αλλά να παρακολουθεί τη συμμόρφωση του Οργανισμού με τις διατάξεις του ΓΚΠΔ²⁴². Συγκεκριμένα, ο ΥΠΔ είναι το πρόσωπο που με τις ειδικές γνώσεις δικαίου και πρακτικών προστασίας δεδομένων που διαθέτει, βοηθά τον υπεύθυνο ή τον εκτελούντα την επεξεργασία στην παρακολούθηση της εσωτερικής συμμόρφωσης με τον ΓΚΠΔ²⁴³. Ευθύνεται έναντι του υπευθύνου επεξεργασίας για δόλο ή βαριά αμέλεια λόγω παράλειψης τέλεσης καθήκοντος, ενώ υπεύθυνος να διασφαλίζει και να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τον ΓΚΠΔ, είναι ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία (άλλως data processor). Κατά βάση αυτοί οι δύο οφείλουν να διασφαλίζουν τη συμμετοχή του ΥΠΔ σε όλα τα ζητήματα που αφορούν την προστασία των προσωπικών δεδομένων. Πρακτικά αυτό σημαίνει ότι ο ΥΠΔ θα πρέπει να συμμετέχει στις συσκέψεις των στελεχών της διοίκησης του Οργανισμού και στη λήψη αποφάσεων που σχετίζονται με την προστασία των δεδομένων.

²⁴¹ Βλ. άρθρ. 14 παρ. 5 ΣχΝΠΔΠΧ.

²⁴² Βλ. Δ. Λεμπέση (2018β), *όπ.ανωτ.*, σελ.608.

²⁴³ Βλ. Ι. Ιγγλεζάκη (2018β), *όπ.ανωτ.*, σελ.97.

Καθόσον ο ρόλος του είναι συμβουλευτικός, θα πρέπει να ζητείται η γνώμη του σε όλα τα σχετικά με τις αρμοδιότητές του ζητήματα και έτσι, με τις προτάσεις του, να συνεισφέρει στην ταχύτερη συμμόρφωση. Στις περιπτώσεις που η γνώμη του, η οποία έχει βαρύνουσα σημασία, δεν γίνει αποδεκτή, πρέπει να καταγράφονται οι λόγοι απόκλισης από τις τεκμηριωμένες συμβουλές και υποδείξεις του²⁴⁴.

Ο θεσμός του ΥΠΔ παρέχει εγγυήσεις ανεξαρτησίας και συμμόρφωσης με τα κατά νόμο οριζόμενα και η συνεισφορά του, όπως προελέχθη, έγκειται στο γεγονός ότι οι προτάσεις του μπορούν να οδηγήσουν στην ταχύτερη συμμόρφωση του φορέα. Υποχρεώσεις του υπευθύνου επεξεργασίας και του εκτελούντα την επεξεργασία σύμφωνα με την παράγραφο 2 του άρθρου 38 ΓΚΠΔ, αποτελούν η στήριξη του ΥΠΔ στην άσκηση των καθηκόντων του, η παροχή ελεύθερης πρόσβασης στα δεδομένα προσωπικού χαρακτήρα, σε όλα τα τμήματα του Οργανισμού και στις πράξεις επεξεργασίας και η παροχή των απαραίτητων πόρων, προκειμένου αυτός να ασκεί αβίαστα τα καθήκοντά του και να διατηρεί την εμπειρογνώσια του. Στις αρμοδιότητες του ΥΠΔ κατά το άρθρο 39 του ΓΚΠΔ εντάσσεται η παρακολούθηση της «εσωτερικής» συμμόρφωσης του Οργανισμού με την εν γένει νομοθεσία προστασίας προσωπικών δεδομένων και η παρέμβασή του σε περίπτωση διαπίστωσης σφάλματος, η ενημέρωση του υπευθύνου επεξεργασίας, του εκτελούντα την επεξεργασία και του προσωπικού του Οργανισμού για τις υποχρεώσεις τους σχετικά με την προστασία προσωπικών δεδομένων, η κατάρτιση και εκπαίδευση του προσωπικού, η διενέργεια ελέγχων. Επικεντρώνεται πρωτίστως στις περιπτώσεις υψηλού κινδύνου, ενώ, επιπλέον, καθήκον του αποτελεί η παροχή συμβουλών σχετικά με την εκτίμηση αντικτύπου και η παρακολούθηση της υλοποίησής της σύμφωνα με το άρθρο 35 του ΓΚΠΔ. Αν και υπεύθυνοι για την τήρηση αρχείων δραστηριοτήτων είναι ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία, ωστόσο στην πράξη ο ΥΠΔ δημιουργεί αρχεία και τηρεί μητρώο των πράξεων επεξεργασίας, προκειμένου να παρακολουθεί τη συμμόρφωση του Οργανισμού²⁴⁵. Όσον αφορά τη σχέση του με την εποπτική αρχή, ο ΥΠΔ συνεργάζεται μαζί της και ενεργεί ως σημείο επικοινωνίας μεταξύ Αρχής και υποκειμένων των δεδομένων για θέματα επεξεργασίας. Το «καθηκοντολόγιο» του ΥΠΔ που αναφέρει το άρθρο 39 του

²⁴⁴ Βλ. Ομάδα Εργασίας άρθ. 29, κατευθυντήριες γραμμές σχετικά με τους ΥΠΔ, 13-12-2016, WP 243, rev.01, σελ.18.

²⁴⁵ Βλ. I. Ιγγλεζάκη (2018β), *όπ.ανωτ.*, σελ.110.

ΓΚΠΔ είναι ενδεικτικό, αφού τα κράτη-μέλη μπορούν να προβλέψουν στη νομοθεσία τους επιπλέον αρμοδιότητες.

Ειδικότερα, η παράγραφος 5 του άρθρου 38 ΓΚΠΔ επιβάλλει τη δέσμευση του ΥΠΔ από την τήρηση του απορρήτου ή της εμπιστευτικότητας, ενώ το ΣχΝΠΔΠΧ εξειδικεύει την υποχρέωση εχεμύθειας και προβλέπει ότι ο ΥΠΔ οφείλει να μην ανακοινώνει ή αποκαλύπτει σε τρίτο γεγονότα ή πληροφορίες που περιήλθαν σε γνώση του λόγω της θέσης του, κατά την εκτέλεση των καθηκόντων του ή επ' ευκαιρία αυτών. Σε περίπτωση παραβίασης της υποχρέωσης αυτής, το ΣχΝΠΔΠΧ προβλέπει σε βάρος του ΥΠΔ ποινικές κυρώσεις, ήτοι ποινή φυλάκισης τουλάχιστον ενός έτους και χρηματική ποινή από 10.000 έως 100.000 ευρώ²⁴⁶. Η υποχρέωση του εθνικού νομοθέτη για τη θέσπιση ποινικών κυρώσεων ή διοικητικών μέτρων, ιδίως για τις πράξεις για τις οποίες δεν επιβάλλονται διοικητικά πρόστιμα και αφορούν βαρύτερες προσβολές της ιδιωτικότητας εκ της επεξεργασίας προσωπικών δεδομένων, πηγάζει από το άρθρο 84 ΓΚΠΔ²⁴⁷.

Υπεύθυνος Προστασίας Δεδομένων και Δημόσια Διοίκηση

Με τον ΓΚΠΔ, ο θεσμός του ΥΠΔ έγινε υποχρεωτικός για ορισμένες κατηγορίες υπευθύνων επεξεργασίας και εκτελούντων την επεξεργασία και ειδικότερα, μεταξύ άλλων, στις περιπτώσεις που η επεξεργασία διενεργείται από δημόσια αρχή ή φορέα²⁴⁸ που εκπληρώνει δημόσιο καθήκον ή ασκεί δημόσια εξουσία. Ο δημόσιος τομέας έχει ευρεία έννοια στον ΓΚΠΔ, καθόσον στο κείμενό του δεν περιλαμβάνεται ορισμός για τη Δημόσια Αρχή ή Οργανισμό: σύμφωνα με την Ομάδα Εργασίας του άρθρου 29²⁴⁹, μείζονος σημασίας κρίνεται η αποστολή ενός Οργανισμού και κατά πόσο αυτή εξυπηρετεί το δημόσιο συμφέρον με την παροχή υπηρεσιών δημοσίου σκοπού (λ.χ. δημόσιες μεταφορές, ενέργεια, ύδρευση, δημόσιες υποδομές, υπηρεσίες πρόνοιας)²⁵⁰, ασχέτως εάν ο Οργανισμός ανήκει στο δημόσιο ή όχι. Στις δημόσιες αρχές περιλαμβάνονται όλες οι εθνικής εμβέλειας, περιφερειακές ή τοπικές αρχές,

²⁴⁶ Άρθ. 70 παρ. 5 ΣχΝΠΔΠΧ: «Υπεύθυνος Προστασίας Δεδομένων που παραβιάζει την υποχρέωση εχεμύθειας που τον βαραίνει στο πλαίσιο του επαγγελματικού απορρήτου ανακοινώνοντας ή αποκαλύπτοντας σε άλλον γεγονότα ή πληροφορίες που περιήλθαν σε γνώση του από τη θέση του κατά την εκτέλεση των καθηκόντων του ή επ' ευκαιρία αυτών, με σκοπό να ωφεληθεί ο ίδιος ή τρίτος, ή για να βλάψει τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία ή το υποκείμενο των δεδομένων ή οποιονδήποτε τρίτο, τιμωρείται με ποινή φυλάκισης τουλάχιστον ενός (1) έτους και χρηματική ποινή από 10.000 έως 100.000 ευρώ, εάν η πράξη δεν τιμωρείται βαρύτερα από άλλες διατάξεις».

²⁴⁷ Βλ. Γ. Νούσκαλη, *Η ποινική προστασία προσωπικών δεδομένων μετά τον Κανονισμό 679/2016 και το σχετικό ελληνικό νομοσχέδιο (2018)*, σελ. 271 και άρθ. 70 ΣχΝΠΔΠΧ.

²⁴⁸ Με εξαίρεση τα δικαστήρια που ενεργούν στα πλαίσια της δικαιοδοτικής τους αρμοδιότητας.

²⁴⁹ “Guidelines on Data Protection Officers (DPO’s)”.

²⁵⁰ Βλ. Γ. Λαζαράκο, *Ο θεσμός του ΥΠΔ (Data Protection Officer) στο νέο νομοθετικό πλαίσιο των προσωπικών δεδομένων μετά την υιοθέτηση του Κανονισμού (ΕΕ) 679/2016 (2016)*, σελ.245.

όπως επίσης και τα νομικά πρόσωπα που διέπονται από το δημόσιο δίκαιο. Ιδιαίτερο ενδιαφέρον παρουσιάζουν τα Νομικά Πρόσωπα Ιδιωτικού Δικαίου (ΝΠΙΔ) ή τα νομικά πρόσωπα που τους έχει ανατεθεί κοινωφελής υπηρεσία, όπως επί παραδείγματι οι εταιρίες που διαχειρίζονται τις δημόσιες συγκοινωνίες, οι τηλεοπτικοί σταθμοί, οι σύλλογοι και τα πειθαρχικά όργανα σε περιπτώσεις νομοθετικώς κατοχυρωμένων επαγγελμάτων (δικηγόροι, φαρμακοποιοί κλπ): στις περιπτώσεις αυτές ο ορισμός ΥΠΔ κρίνεται προαιρετικός, εν αμφιβολία όμως, συνιστάται ως καλή πρακτική, δεδομένου ότι τα υποκείμενα των δεδομένων δεν έχουν επιλογή ως προς τη διαχείριση των δεδομένων τους²⁵¹.

Στις δημόσιες υπηρεσίες τα βήματα που πρέπει να ακολουθηθούν για την έναρξη λειτουργίας ΥΠΔ είναι τα εξής²⁵²: αρχικά γίνεται πρόσκληση εκδήλωσης ενδιαφέροντος, αξιολόγηση υποψηφιοτήτων και επιλογή του καταλληλότερου ΥΠΔ. Ταυτόχρονα με τον ορισμό του ΥΠΔ και του αναπληρωτή του, θα πρέπει να ιδρυθεί αυτοτελές γραφείο ή τμήμα προστασίας δεδομένων προσωπικού χαρακτήρα, το οποίο θα στελεχώνεται από το αντίστοιχο προσωπικό ανάλογα με τη δυναμικότητα του φορέα, την φύση και το είδος των δεδομένων που επεξεργάζεται. Κι ενώ ήδη πριν από τη στελέχωση του γραφείου θα πρέπει να έχει προηγηθεί ενημέρωση των ανώτερων στελεχών του Οργανισμού για το περιεχόμενο του Κανονισμού, σε δεύτερο χρόνο θα πρέπει να πραγματοποιηθεί ενημέρωση και του λοιπού ανθρώπινου δυναμικού. Στη συνέχεια συντάσσεται Κανονισμός λειτουργίας και γίνεται καταγραφή των επεξεργασιών δεδομένων που πραγματοποιούνται. Εάν ο Οργανισμός φτάσει στο επίπεδο αυτό, ακολουθεί η συμμετοχή του ΥΠΔ στις συσκέψεις των στελεχών και η αναβάθμιση της διαδικτυακής υποδομής. Στο τέλος συντάσσεται η ετήσια έκθεση με τα πεπραγμένα που θα οδηγήσει στη βελτίωση της λειτουργίας του ΥΠΔ .

Οι υποψήφιοι πρέπει να διαθέτουν τα περιγραφόμενα στην παράγραφο 5 του άρθρου 37 ΓΚΠΔ προσόντα, να διακρίνονται για το ήθος και την ακεραιότητά τους, ενώ δεν τίθεται περιορισμός στο επαγγελματικό αντικείμενο που μπορεί να έχουν²⁵³, αφού αρκεί να διαθέτουν επαρκείς νομικές γνώσεις στα προσωπικά δεδομένα, σε συνδυασμό με ουσιαστικές γνώσεις πληροφορικής. Τούτο σημαίνει ότι δεν απαιτείται να ανήκει σε νομοθετικά κατοχυρωμένο, βάσει της παραγράφου 3 του άρθρου 2 Π.Δ.

²⁵¹ Βλ. Δ. Λεμπέση (2018β), *όπ.ανωτ.*, σελ. 611.

²⁵² Βλ. Β. Σωτηρόπουλο (2017), *Υπεύθυνος Προστασίας Δεδομένων*.

²⁵³ Σε αντίθεση με αυτό που ίσχυε στη Γερμανία, όπου διορίζονταν αποκλειστικά δικηγόροι ή νομικοί που πέτυχαν στις εξετάσεις άσκησης επαγγέλματος.

165/2000, επάγγελμα. Σε κάθε δε περίπτωση, θα πρέπει να γνωρίζει τη δομή, τα πληροφοριακά συστήματα και τα συστήματα ασφαλείας του δημόσιου φορέα που υπηρετεί, να έχει πρόσβαση σε άλλα τμήματα όπως το νομικό, το τμήμα πληροφορικής ή ανθρωπίνου δυναμικού, καθώς επίσης και να ενημερώνεται διαρκώς επί των θεμάτων που τον αφορούν²⁵⁴. Βέβαιο είναι πως πρέπει να διασφαλίζεται η τήρηση της εμπιστευτικότητας και η ανυπαρξία σύγκρουσης συμφερόντων²⁵⁵ στην περίπτωση που ο ΥΠΔ επιτελεί και άλλα καθήκοντα ή υποχρεώσεις, στα πλαίσια της πολυσχιδούς δραστηριότητάς του. Σύμφωνα με την ΑΠΔΠΧ²⁵⁶, για να διοριστεί κάποιος στη θέση του ΥΠΔ, δεν είναι απαραίτητη η πιστοποίηση επαγγελματικών προσόντων από φορέα πιστοποίησης. Με αφορμή τον ΓΚΠΔ υπήρξε έντονη δραστηριότητα από φορείς, κατά κύριο λόγο κερδοσκοπικούς, για παροχή συμβουλευτικών υπηρεσιών σχετικά με τη συμμόρφωση με το νέο Κανονισμό, για προσφορά εκπαιδευτικών προγραμμάτων επαγγελματικής κατάρτισης και για παροχή υπηρεσιών πιστοποίησης ΥΠΔ. Η προσφερόμενη εκπαίδευση μέσω προγραμμάτων αντιμετωπίζεται μεν θετικά, η δε ύλη μπορεί να χαρακτηριστεί συναφής με τον ΓΚΠΔ και τη θέση του ΥΠΔ, η επιλογή της όμως αποτελεί αποκλειστική ευθύνη των φορέων που τα παρέχουν κι όχι προαπαιτούμενο από τον ΓΚΠΔ. Η δε πιστοποίηση προστασίας δεδομένων από φορείς πιστοποίησης του άρθρου 15 του ΣχΝΠΔΠΧ, αφορά τους υπευθύνους επεξεργασίας και τους εκτελούντες την επεξεργασία που επιθυμούν να πιστοποιηθούν εθελοντικά και όχι τους ΥΠΔ. Επίσης, ο ίδιος ΥΠΔ μπορεί να αναλάβει δύο ή και περισσότερους δημόσιους φορείς ή να ασκεί καθήκοντα με παράλληλη ανάθεση, αρκεί να παραμένει εύκολα προσβάσιμος σε επικοινωνία και να μην υπάρχει ασυμβίβαστο. Για να επιτευχθεί η προσβασιμότητά του, ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία οφείλει να δημοσιεύσει τα στοιχεία επικοινωνίας του ΥΠΔ, όπως τη διεύθυνση ηλεκτρονικής αλληλογραφίας ή τον τηλεφωνικό του αριθμό και να τα ανακοινώσει στην εποπτική αρχή²⁵⁷, ενώ στην παράγραφο 4 του άρθρου 14 του ΣχΝΠΔΠΧ προβλέπεται ότι ο υπεύθυνος και ο εκτελών κοινοποιούν στην Αρχή το όνομα και την ιδιότητα του ΥΠΔ. Η δε Αρχή ακόμα δεν έχει αποφανθεί εάν μπορεί η ίδια να δημοσιοποιεί τα στοιχεία των ΥΠΔ, καθόσον ο ΓΚΠΔ δεν είναι σαφής στο σημείο αυτό, σε αντίθεση με το

²⁵⁴ Βλ. Γ. Λαζαράκο, *Ο θεσμός του ΥΠΔ (Data Protection Officer) στο νέο νομοθετικό πλαίσιο των προσωπικών δεδομένων μετά την υιοθέτηση του Κανονισμού (ΕΕ) 679/2016 (2016)*, όπ.ανωτ., σελ.249.

²⁵⁵ Προτείνεται η κατάρτιση Πολιτικών Σύγκρουσης Συμφερόντων.

²⁵⁶ Βλ. ανακοίνωση με αρ.Γ/ΕΞ/6007/9-8-2017 και Ι. Ιγγλεζάκη, *Ο ΥΠΔ κατά τον Κανονισμό 2016/679 και την Οδηγία 2016/680 (2018α)*, όπ.ανωτ., σελ.67.

²⁵⁷ Βλ. άρθ. 37 παρ.7 ΓΚΠΔ.

N.2472/1997²⁵⁸. Η σημασία της τήρησης δημοσιότητας στο θεσμό του ΥΠΔ είναι μεγάλη, διότι εξασφαλίζεται αφενός η εύκολη και άμεση επικοινωνία των υποκειμένων και της Αρχής με τον ΥΠΔ χωρίς τη μεσολάβηση τρίτων και αφετέρου η τήρηση της εμπιστευτικότητας. Καλή πρακτική μπορεί να θεωρηθεί η ύπαρξη γραμμής άμεσης επικοινωνίας με τον ΥΠΔ στον δικτυακό τόπο του Οργανισμού²⁵⁹.

Σύμφωνα με την με αρ. 7/2017 Γνωμοδότηση της ΑΠΔΠΧ, η συμμετοχή μέλους ή υπαλλήλου της Αρχής, με ή χωρίς αμοιβή, σε ενέργειες παροχής συμβουλευτικών υπηρεσιών, πιστοποίησης ή εκπαίδευσης σε θέματα που αφορούν τον ΓΚΠΔ, συνιστά ασυμβίβαστο με την ιδιότητά του. Εξαιρέση αποτελεί η αμισθί παροχή συμβουλευτικών υπηρεσιών αποκλειστικά σε φορείς του δημοσίου τομέα και εφόσον ο στόχος των προσφερόμενων υπηρεσιών είναι η απλή καθοδήγηση και ενημέρωση των φορέων σε θέματα που αφορούν τις υποχρεώσεις που προκύπτουν από τον ΓΚΠΔ.

Συναφείς έννοιες με τον ΥΠΔ είναι ο θεσμός του Υπευθύνου Διασφάλισης Απορρήτου, ο οποίος, σύμφωνα με την παράγραφο 2 του άρθρου 3 Ν.3674/2008²⁶⁰, είναι αρμόδιος να εφαρμόσει ειδικό σχέδιο πολιτικής ασφάλειας για τη διασφάλιση του απορρήτου των ηλεκτρονικών επικοινωνιών και ο θεσμός του Υπευθύνου Ασφάλειας Δεδομένων, κατά την παράγραφο 2 του άρθρου 7 Ν.3917/2011²⁶¹, στον οποίο επίσης ανατίθεται η εφαρμογή ειδικού σχεδίου πολιτικής ασφάλειας.

Τέλος, κατά την παράγραφο 4 περίπτωση α' του άρθρου 83 ΓΚΠΔ, η παραβίαση της υποχρέωσης του υπευθύνου επεξεργασίας και του εκτελούντα την επεξεργασία να διορίσουν ΥΠΔ, επισύρει κατά του δημοσίου διοικητικά πρόστιμα ύψους έως και 10.000.000 ευρώ, ανεξαρτήτως μάλιστα της επιβολής άλλων προστίμων λόγω παραβίασης έτερης διάταξης του ΓΚΠΔ. Εάν όμως ο υπεύθυνος επεξεργασίας αποδείξει ότι είναι συνεπής στις υποχρεώσεις του, όσον αφορά τον ΥΠΔ, αυτό θα συνεκτιμηθεί, προκειμένου να μειωθεί το πρόστιμο που θα του επιβληθεί λόγω παραβίασης άλλης διάταξης. Πότε όμως ο δημόσιος φορέας καθίσταται υπερήμερος ως προς την υποχρέωσή του να ορίσει ΥΠΔ και συνεπώς δυνητικά υπόχρεος προστίμου; Η απάντηση στο ερώτημα θα δοθεί στο μέλλον, μιας και ακόμα δεν

²⁵⁸ Κατά την Αρχή, ο ΓΚΠΔ δεν προβλέπει δημοσιοποίηση του καταλόγου (ως τηρηθέν αρχείο από την Αρχή), όπως προέβλεπε ο Ν.2472/1997. Κατά τον Ι. Ιγγλεζάκη, Ο Υπεύθυνος Προστασίας Δεδομένων κατά τον Κανονισμό 2016/679 και την Οδηγία 2016/680 (2018), όπ.ανωτ, σελ.68, η δημοσιοποίηση του καταλόγου ΥΠΔ από την Αρχή αποτελεί βέλτιστη πρακτική που υπηρετεί την αρχή της διαφάνειας.

²⁵⁹ Βλ. Ι. Ιγγλεζάκη (2018β), όπ.ανωτ., σελ.105.

²⁶⁰ Ν.3674/2008 περί «Ενίσχυσης του θεσμικού πλαισίου διασφάλισης του απορρήτου της τηλεφωνικής επικοινωνίας και άλλες διατάξεις», βλ. σχετ. Ι. Ιγγλεζάκη (2018β), όπ.ανωτ., σελ. 97.

²⁶¹ Όπως αναφέρθηκε ανωτέρω.

υπήρξε έλεγχος για την έγκαιρη ή μη συμμόρφωση της ΔΔ στις επιταγές του Κανονισμού.

5.3. Εφαρμογή ΓΚΠΔ στη Δημόσια Διοίκηση

Όπως είναι γνωστό, στις βασικές δραστηριότητες των δημοσίων αρχών ανήκει η επεξεργασία ευαίσθητων δεδομένων και η επεξεργασία δεδομένων μεγάλης κλίμακας (όπως η επεξεργασία δεδομένων ασθενών ενός νοσοκομείου) και συνεπώς η ΔΔ οφείλει να προσαρμοστεί στα νέα δεδομένα του Κανονισμού. Το νέο νομοθέτημα δεν τροποποιεί απλά ορισμένα σημεία του προϋφιστάμενου καθεστώτος, αλλά φαίνεται να αντιμετωπίζει με διαφορετικό τρόπο το ζήτημα των προσωπικών δεδομένων, σε συνάρτηση με την κρατική παρέμβαση λόγω δημοσίου συμφέροντος. Εισάγει μάλιστα ένα νέο είδος δημόσιας ρύθμισης, με στόχο την αποτελεσματικότητα της προστασίας των προσωπικών δεδομένων και τον εκσυγχρονισμό του δημόσιου τομέα μέσω της ψηφιοποίησης των υπηρεσιών του. Προκειμένου να ενισχυθεί η ασφάλεια δικαίου και η εμπιστοσύνη του πολίτη έναντι του υπέρμετρου κρατικού παρεμβατισμού, των δυσλειτουργιών της δημόσιας εποπτείας και της έλλειψης τεχνογνωσίας στη ΔΔ, επελέγη να δοθεί έμφαση στην πρόληψη αντί στην καταστολή, μέσω των μέτρων, των εργαλείων και των καινοτομιών που εισήγαγε²⁶².

Το ελληνικό δημόσιο, μέσω του υπευθύνου επεξεργασίας, υποχρεούται να λαμβάνει αποτελεσματικά μέτρα²⁶³ που να διασφαλίζουν την τήρηση των απαιτήσεων του Κανονισμού, όπως επίσης να είναι σε θέση να αποδεικνύει τη συμμόρφωση των δραστηριοτήτων επεξεργασίας με τον ΓΚΠΔ²⁶⁴.

Στις υποχρεώσεις των φορέων του δημόσιου τομέα²⁶⁵ εντάσσεται η δημιουργία και τήρηση ηλεκτρονικών αρχείων για τα ηλεκτρονικά έγγραφα που εκδίδουν, κατέχουν ή διακινούν. Μάλιστα, οι διαδικασίες επεξεργασίας των ηλεκτρονικών εγγράφων πρέπει να τηρούν τους όρους ασφάλειας, όπως επίσης να εγγυώνται την ακεραιότητα, την αυθεντικότητα και την εμπιστευτικότητα των εγγράφων και των δεδομένων που αυτά περιέχουν. Τα ηλεκτρονικά αρχεία του δημόσιου τομέα πρέπει να τηρούνται με

²⁶² Βλ. Γ. Δελλή, *Για μια αποτελεσματική δημόσια προστασία των προσωπικών δεδομένων: ο «θανμαστός καινούριος κόσμος» του Κανονισμού (ΕΕ) 679/2016, (2017).*

²⁶³ *Τα οποία θα πρέπει να συνεκτιμούν, μεταξύ άλλων, τους σκοπούς της επεξεργασίας και τον κίνδυνο για τα προσωπικά δικαιώματα-προσωπικές ελευθερίες.*

²⁶⁴ Βλ. αιτιολογικές σκέψεις 74 και 78 Προοιμίου του ΓΚΠΔ.

²⁶⁵ Βλ. Μ. Μυλώση, *Ηλεκτρονική Διακυβέρνηση στη ΔΔ – Πληροφοριακές υποχρεώσεις των φορέων του δημοσίου τομέα, (2018).*

τέτοιο τρόπο, ώστε να εξασφαλίζεται η διατηρησιμότητα, η προσβασιμότητα και η αναγνωσιμότητα των εγγράφων που περιέχουν. Ειδικότερα, κάθε δημόσιος φορέας τηρεί σύστημα ηλεκτρονικού πρωτοκόλλου, βάσει του οποίου εκδίδεται μοναδικός αριθμός αποδεικτικού καταχώρησης.

Τα υποκείμενα των δεδομένων απολαμβάνουν το δικαίωμα πρόσβασης στα ηλεκτρονικά έγγραφα που τηρεί η ΔΔ, μελέτης και χορήγησης αντιγράφου. Το δικαίωμα πρόσβασης και επικοινωνίας με τους φορείς του δημοσίου, μπορεί να πραγματοποιηθεί με τη χρήση Τεχνολογιών Πληροφορικής και Επικοινωνιών (ΤΠΕ)²⁶⁶. Τα φυσικά πρόσωπα δικαιούνται να συναλλάσσονται με τη ΔΔ μέσω ΤΠΕ, κάνοντας χρήση πληροφοριακών συστημάτων.

Δικαίωμα πρόσβασης στα διοικητικά έγγραφα

Αφορά την πρόσβαση σε έγγραφα που εκδίδουν ή κατέχουν οι διοικητικές αρχές του κράτους και εμφανίστηκε για πρώτη φορά στην παράγραφο 3 του άρθρου 10 του Συντάγματος 1975, ως υποχρέωση των διοικητικών αρχών να παρέχουν πληροφορίες επί αιτήσεως, υπό τον όρο ύπαρξης νομοθετικής πρόβλεψης. Ακολούθησε το άρθρο 16 του Ν.1599/1986 περί δικαιώματος γνώσης διοικητικών εγγράφων²⁶⁷ και το άρθρο 5 του Ν.2690/1999²⁶⁸ περί δικαιώματος πρόσβασης στα διοικητικά έγγραφα, με βασική προϋπόθεση τη συνδρομή εύλογου ενδιαφέροντος στο πρόσωπο του αιτούντος πρόσβαση σε δημόσια έγγραφα²⁶⁹. Ακολούθως, το Προεδρικό Διάταγμα 28/2015 αφορά στην Κωδικοποίηση διατάξεων για την πρόσβαση σε δημόσια έγγραφα και στοιχεία. Τέλος, στο αναθεωρημένο Σύνταγμα του 2001, τροποποιήθηκε η παράγραφος 3 του άρθρου 10 και πλέον ορίζεται ότι η αρμόδια αρχή είναι υποχρεωμένη να απαντά σε αιτήματα για παροχή πληροφοριών και χορήγηση εγγράφων, εντός ορισμένης προθεσμίας²⁷⁰. Άλλωστε η τήρηση της διαφάνειας αποτελεί βασική υποχρέωση της πολιτείας και κατ' επέκταση της σύγχρονης δημόσιας διοίκησης. Η διοίκηση οφείλει να θέσει στη διάθεση του διοικουμένου

²⁶⁶ Ορισμός ΤΠΕ (αγγλικά IT: Information Technology): «το σύνολο των επαγγελματικών χώρων οι οποίοι σχετίζονται με τη μελέτη, σχεδίαση, ανάπτυξη, υλοποίηση, συντήρηση και διαχείριση υπολογιστικών πληροφοριακών συστημάτων, κυρίως όσον αφορά εφαρμογές λογισμικού και υλικού υπολογιστών. Τα επαγγέλματα ΤΠΕ βασίζονται στην ανάπτυξη, εγκατάσταση και συντήρηση προϊόντων πληροφορικής και τηλεπικοινωνιών, με στόχο την παραγωγή, αποθήκευση, διαχείριση και μετάδοση πληροφοριών κάθε τύπου (Wikipedia)».

²⁶⁷ Ως διοικητικά έγγραφα ορίζονται «όλα τα έγγραφα που συντάσσονται από όργανα του δημοσίου τομέα, ιδίως εκθέσεις, μελέτες, πρακτικά, στατιστικά στοιχεία, εγκύκλιοι οδηγίες, απαντήσεις της διοίκησης, γνωμοδοτήσεις και αποφάσεις».

²⁶⁸ Κώδικας Διοικητικής Διαδικασίας, άρθ. 5.

²⁶⁹ Βλ. ενδεικτικά ΣτΕ 1397/199, 1214/2000, ΔΕφΑθ 368/2011, Γνμ. ΝΣΚ 92/2005.

²⁷⁰ Σχετικός είναι και ο Ν.3448/2006 για την περαιτέρω χρήση πληροφοριών του δημοσίου τομέα.

οποιοδήποτε στοιχείο είναι πρόσφορο για την προάσπιση των συμφερόντων του, παρέχοντας ορθή, πλήρη και ειλικρινή ενημέρωση βάσει των αρχών του κράτους δικαίου²⁷¹. Το δικαίωμα προστασίας των προσωπικών δεδομένων και το δικαίωμα πρόσβασης σε διοικητικά έγγραφα κατοχυρώθηκαν μεν θεσμικά, αμφοτέρωθεν σε συνταγματικό επίπεδο, δημιουργήθηκαν όμως νομικοί προβληματισμοί που αφορούν τα όρια εφαρμογής των δικαιωμάτων σε περίπτωση σύγκρουσης²⁷². Το πλέον προφανές ερώτημα που τίθεται είναι ποιο δικαίωμα θα προκριθεί στην περίπτωση που υποβληθεί αίτημα για χορήγηση διοικητικού εγγράφου που περιέχει προσωπικά δεδομένα τρίτου προσώπου. Πότε η ΔΔ υποχρεούται να χορηγήσει το έγγραφο, πότε δικαιούται να αρνηθεί με επίκληση της προστασίας των δεδομένων προσωπικού χαρακτήρα και ποια κριτήρια πρέπει να λάβει υπόψη κατά τη λήψη της απόφασής της; Σύμφωνα με τη διάταξη του άρθρου 86 του ΓΚΠΔ που αφορά την επεξεργασία και πρόσβαση του κοινού σε επίσημα έγγραφα, η δημόσια αρχή που κατέχει δημόσια έγγραφα τα οποία περιλαμβάνουν δεδομένα προσωπικού χαρακτήρα για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον, μπορεί να τα κοινοποιεί σύμφωνα με το δίκαιο της Ένωσης, ή του κράτους-μέλους, συμβιβάζοντας την πρόσβαση του κοινού σε επίσημα έγγραφα με το δικαίωμα στην προστασία των δεδομένων. Συμπερασματικά λοιπόν ο ΓΚΠΔ δεν προκρίνει ένα από τα δύο προστατευόμενα δικαιώματα, αλλά παραπέμπει στην εθνική έννομη τάξη, όπου όμως δεν εφαρμόζεται η ιεράρχηση μεταξύ των συνταγματικών διατάξεων και συνεπώς πρόκειται για ισοδύναμα δικαιώματα. Τη λύση για τη σχέση μεταξύ του συνταγματικά κατοχυρωμένου στο άρθρο 9Α Σ δικαιώματος της πληροφοριακής αυτοδιάθεσης του ατόμου και της επίσης συνταγματικά κατοχυρωμένης στα άρθρα 5Α και 10 παρ.3 Σ αρχής της διαφάνειας της κρατικής δράσης, ήρθε να δώσει η Αρχή με τη υπ' αριθμ. 6/2013 Γνωμοδότησή της. Στο σημείο αυτό θα πρέπει να επισημανθεί το εξειδικευμένο δικαίωμα πρόσβασης του υποκειμένου στα δεδομένα του, το οποίο αποτελεί θεμελιώδη αρχή του δικαίου προστασίας προσωπικών δεδομένων και προβλέπεται στα άρθρα 12 Ν.2472/1997 και 15 ΓΚΠΔ²⁷³. Με άλλα λόγια, οι διατάξεις αυτές παρέχουν στον διοικούμενο πρόσθετη ενίσχυση για

²⁷¹ Βλ. Κ. Σπανού (επιμ.), *Πρόσβαση στα έγγραφα και διαφάνεια της διοικητικής δράσης (2010)*, εισήγηση Κ. Ανδρικήκη, σελ.19.

²⁷² Βλ. εισήγηση Σ. Βλαχόπουλου, *Πρόσβαση στα δημόσια έγγραφα*, σε: Α. Κοτσαλής/Κ. Μενουδάκος (επιμ.), *όπ.ανωτ.* (2018), σελ.43.

²⁷³ Βλ. Α. Γέροντα (2002), *όπ.ανωτ.*, σελ. 229 επόμεν., όπου αναφέρει, σχετικά με το δικαίωμα πρόσβασης στα αρχεία, και το άρθρ. 2 παρ. 3 Ν.2716/1999 περί «Ανάπτυξης και εκσυγχρονισμού των υπηρεσιών ψυχικής υγείας και άλλες διατάξεις», στο οποίο συμπεριλαμβάνεται ρητά το δικαίωμα των ατόμων με ψυχικές διαταραχές για πρόσβαση στα δεδομένα των αρχείων που τα αφορούν.

ικανοποίηση του αιτήματός του, όταν η πρόσβαση αφορά δικά του προσωπικά δεδομένα. Η υπ' αριθμ. 6/2013 Γνωμοδότηση της Αρχής, διέκρινε τα απλά από τα ευαίσθητα δεδομένα, επεσήμανε την αναγκαιότητα της συγκατάθεσης του υποκειμένου για την επεξεργασία των απλών δεδομένων και τις περιπτώσεις που κατ' εξαίρεση επιτρέπεται η επεξεργασία και χωρίς τη συγκατάθεση, έδωσε βαρύτητα στη νομολογία του ΣτΕ και τις γνωμοδοτήσεις του Νομικού Συμβουλίου του Κράτους (ΝΣΚ), υπογράμμισε την αναγκαιότητα συνδρομής εύλογου ενδιαφέροντος στο πρόσωπο του αιτούντος πρόσβαση σε δημόσιο έγγραφο και υπέδειξε την αναγκαιότητα προηγούμενης άδειας από την Αρχή, στις περιπτώσεις αιτήματος επεξεργασίας ευαίσθητων προσωπικών δεδομένων από τρίτο ενδιαφερόμενο. Η ανωνυμοποίηση και η απάλειψη των προσωπικών δεδομένων τρίτων από το χορηγούμενο δημόσιο έγγραφο, αποτελούν μια αποτελεσματική λύση στον προβληματισμό της σύγκρουσης των δικαιωμάτων πρόσβασης στα διοικητικά έγγραφα και προστασίας των προσωπικών δεδομένων. Το ΣχΝΠΔΠΧ προβλέπει στην παράγραφο 4 του άρθρου 18 τις περιπτώσεις που επιτρέπεται η πρόσβαση σε δεδομένα προσωπικού χαρακτήρα που τηρούνται για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον.

Στη συνέχεια, όσον αφορά τα δικαιώματα των πολιτών, σύμφωνα με την επίσημη ιστοσελίδα της Ευρωπαϊκής Επιτροπής της ΕΕ²⁷⁴, τα φυσικά πρόσωπα μπορούν να επικοινωνήσουν με έναν δημόσιο Οργανισμό και να ασκήσουν τα δικαιώματά τους βάσει ΓΚΠΔ, ήτοι τα δικαιώματα πρόσβασης, διόρθωσης, διαγραφής, περιορισμού, φορητότητας, εναντίωσης, το δικαίωμα να μην υπόκεινται σε αυτοματοποιημένη λήψη αποφάσεων, όπως αυτά αναπτύχθηκαν ανωτέρω. Άξιο αναφοράς αποτελεί το δικαίωμα των πολιτών να αντιταχθούν στην επεξεργασία προσωπικών δεδομένων από τη ΔΔ για λόγους δημοσίου συμφέροντος. Η ΔΔ από την πλευρά της δύναται να απορρίψει το αίτημα και να συνεχίσει την επεξεργασία, εφόσον αποδείξει ότι υφίστανται επιτακτικοί και νόμιμοι λόγοι επεξεργασίας, οι οποίοι υπερισχύουν των ατομικών συμφερόντων και δικαιωμάτων, ή ότι τα δεδομένα είναι αναγκαία για τη σύσταση, άσκηση ή υπεράσπιση νομικών απαιτήσεων. Ειδικότερα, όσον αφορά το δικαίωμα διαβίβασης (φορητότητας) δεδομένων, τα άτομα δεν μπορούν να το ασκήσουν όταν τα δεδομένα κρίνονται απαραίτητα για την εκπλήρωση καθήκοντος

²⁷⁴ Βλ. ηλεκτρονική πηγή: <https://ec.europa.eu>.

που εκτελείται προς το δημόσιο συμφέρον ή για την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας. Πάντως η ΔΔ υποχρεούται να απαντά στις αιτήσεις των πολιτών χωρίς αδικαιολόγητη καθυστέρηση και μάλιστα εντός μηνός από την παραλαβή της αίτησης, με δικαίωμα παράτασης δύο μηνών, εάν το αίτημα είναι πολύπλοκο ή εάν ο αριθμός των αιτημάτων είναι μεγάλος. Η ΔΔ μπορεί να ζητήσει πρόσθετες πληροφορίες για να επιβεβαιώσει την ταυτότητα του αιτούντα και, βεβαίως, να απορρίψει το αίτημα, εκθέτοντας τους λόγους απόρριψης, οι οποίοι κατά κύριο λόγο αφορούν την επίκληση της ασφάλειας του Κράτους και του δημοσίου συμφέροντος, ενημερώνοντας τον αιτούντα για το δικαίωμά του να υποβάλλει καταγγελία στην Αρχή²⁷⁵.

Σύμφωνα με τις οδηγίες του Υπουργείου Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης²⁷⁶ για την προετοιμασία του δημόσιου φορέα να εφαρμόσει τον ΓΚΠΔ, απαιτείται αρχικά καταγραφή των κατηγοριών των προσωπικών δεδομένων φυσικών προσώπων που τυγχάνουν «επεξεργασίας» (όπως αναλύεται ο όρος ανωτέρω) από το φορέα. Ο φορέας μπορεί να λειτουργεί είτε ως υπεύθυνος επεξεργασίας, είτε ως εκτελών την επεξεργασία. Επίσης, πρέπει να καταγραφούν τα «αρχεία» που ο φορέας τηρεί, όπως αυτά ορίζονται κυρίως στο άρθρο 30²⁷⁷ ΓΚΠΔ, σύμφωνα με το οποίο κάθε υπεύθυνος επεξεργασίας ή εκτελών την επεξεργασία (και κατά περίπτωση οι εκπρόσωποί τους), τηρούν αρχείο δραστηριοτήτων επεξεργασίας, το οποίο περιλαμβάνει τα οριζόμενα στο άρθρο αυτό²⁷⁸.

Στη συνέχεια απαιτείται η καταγραφή των απαιτούμενων ενεργειών, προκειμένου ο φορέας να συμμορφωθεί με τις υποχρεώσεις που επιβάλλουν οι διατάξεις του Κανονισμού και να διασφαλιστεί ο σεβασμός των υποκειμένων των προσωπικών δεδομένων, που μπορεί να είναι είτε εργαζόμενοι του φορέα είτε διοικούμενοι. Κατόπιν πραγματοποιείται έλεγχος από τον υπεύθυνο επεξεργασίας για το ενδεχόμενο να προκύψει υψηλός κίνδυνος για τα δικαιώματα και τις ελευθερίες των υποκειμένων από τη σχεδιαζόμενη επεξεργασία. Βάσει του άρθρου 35 του ΓΚΠΔ περί «εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων», εάν διαπιστωθεί υψηλός κίνδυνος, ο υπεύθυνος επεξεργασίας διενεργεί, πριν από την επεξεργασία,

²⁷⁵ Κεφάλαιο III ΓΚΠΔ για τα δικαιώματα του υποκειμένου των δεδομένων.

²⁷⁶ Βλ. ηλεκτρονική πηγή: <http://mindigital.gr>.

²⁷⁷ Άρθρο 30 ΓΚΠΔ: «Αρχεία των δραστηριοτήτων επεξεργασίας».

²⁷⁸ Ενδεικτικά περιλαμβάνει: τα στοιχεία του υπεύθυνου επεξεργασίας, τους σκοπούς της επεξεργασίας, τους αποδέκτες στους οποίους θα γνωστοποιηθούν τα δεδομένα κ.ά.

εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα.

Επίσης, πριν από την επεξεργασία των δεδομένων προσωπικού χαρακτήρα, η ΔΔ πρέπει να ενημερώνει τα υποκείμενα για την επεξεργασία των δεδομένων τους, για τα δικαιώματά τους, για τους σκοπούς που επιδιώκονται με την επεξεργασία, για τους τύπους των δεδομένων που συλλέχθηκαν και για τους παραλήπτες των δεδομένων²⁷⁹.

Ο σημαντικότερος στόχος είναι η διασφάλιση υψηλού επιπέδου προστασίας δεδομένων από τη ΔΔ και για να επιτευχθεί θα πρέπει να σχεδιασθούν και να τεθούν σε λειτουργία αντίστοιχες διαδικασίες. Στο άρθρο 25 ΓΚΠΔ περιγράφεται η προστασία δεδομένων ήδη από το σχεδιασμό και εξ ορισμού, όπως επίσης και οι αντίστοιχες υποχρεώσεις, προκειμένου να παρέχονται οι απαραίτητες εγγυήσεις συμμόρφωσης με τον Κανονισμό. Στην περίπτωση τυχαίας ή παράνομης αποκάλυψης προσωπικών δεδομένων σε μη εξουσιοδοτημένους παραλήπτες, ή στην περίπτωση που τα δεδομένα είναι προσωρινά μη διαθέσιμα ή τροποποιημένα, η ΔΔ πρέπει να κοινοποιήσει την παραβίαση στην Αρχή και πιθανώς να ενημερώσει τα υποκείμενα, όπως αναλύθηκε και παραπάνω.

Τέλος, σύμφωνα με τα άρθρα 37 και 38 ΓΚΠΔ, υποχρεωτικός καθίσταται ο διορισμός σε κάθε δημόσιο φορέα, **Υπευθύνου Προστασίας Δεδομένων**, του οποίου τα καθήκοντα περιγράφονται στο άρθρο 39 ΓΚΠΔ. Ο ρόλος του ΥΠΔ είναι, όπως προειπώθηκε, αρχικά συμβουλευτικός, καθόσον οφείλει να ενημερώνει και να συμβουλεύει τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία και τους εργαζόμενους που διενεργούν επεξεργασίες, για τις υποχρεώσεις τους που απορρέουν από τον Κανονισμό ή από άλλες ευρωπαϊκές ή εθνικές διατάξεις, όσον αφορά την προστασία των προσωπικών δεδομένων. Πρέπει επίσης να διασφαλίζει την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων για την εξασφάλιση της προστασίας των προσωπικών δεδομένων. Η βασική ευθύνη για τη νομιμότητα της επεξεργασίας εξακολουθεί να βαρύνει τον υπεύθυνο επεξεργασίας, στον οποίο απευθύνονται οι επιταγές του ΓΚΠΔ, ενώ οι υποχρεώσεις του εκτελούντος την επεξεργασία προκύπτουν από τη μεταξύ τους συναφθείσα σύμβαση²⁸⁰. Δυνάμει μάλιστα της σύμβασης αυτής, ο εκτελών την επεξεργασία καθίσταται αλληλεγγύως και εις ολόκληρον συνυπεύθυνος με τον υπεύθυνο επεξεργασίας, εάν καθορίσει τους σκοπούς και τα μέσα της επεξεργασίας κατά παράβαση του Κανονισμού. Ο

²⁷⁹ Ηλεκτρονική πηγή: <https://ec.europa.eu>.

²⁸⁰ Βλ. άρθρο 28 παρ. 3 ΓΚΠΔ.

εκτελών²⁸¹ που ενεργεί κατ'εντολή του υπευθύνου²⁸², οφείλει να συνδράμει τον υπεύθυνο κατά την εκτέλεση των υποχρεώσεων που απορρέουν από τον ΓΚΠΔ, να τον ενημερώνει όταν υποπέσει στην αντίληψή του παράνομη εντολή²⁸³ ή παραβίαση δεδομένων²⁸⁴, να τηρεί αρχείο των δραστηριοτήτων επεξεργασίας που διεξάγονται εκ μέρους του υπευθύνου²⁸⁵, να συνεργάζεται με την εποπτική αρχή²⁸⁶ και να ορίζει ΥΠΔ μαζί με τον υπεύθυνο. Εάν οριστεί, με σύμβαση ή με άλλη νομική πράξη, εξωτερικός συνεργάτης που θα αναλάβει ορισμένα τμήματα επεξεργασίας, θα πρέπει να παρέχονται επαρκείς εγγυήσεις ότι θα ληφθούν τα κατάλληλα μέτρα για να πληρούνται τα πρότυπα του Κανονισμού.

5.4. Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ)

Ο ΓΚΠΔ δίνει έμφαση στη λειτουργία των εποπτικών αρχών και στην κατοχύρωση της ανεξαρτησίας τους²⁸⁷. Σκοπός τους παραμένει η παρακολούθηση της εφαρμογής του ΓΚΠΔ, η προστασία των θεμελιωδών δικαιωμάτων και ελευθεριών των φυσικών προσώπων και η διευκόλυνση της ελεύθερης κυκλοφορίας των προσωπικών δεδομένων στην ευρωπαϊκή κοινότητα. Οι Αρχές διατηρούν τον τριπλό τους ρόλο, ήτοι ενημερωτικό, ρυθμιστικό και ελεγκτικό. Οι εποπτικές αρχές συμβάλλουν στη συνεκτική εφαρμογή του ΓΚΠΔ σε ολόκληρη την ΕΕ και για το λόγο αυτό συνεργάζονται μεταξύ τους αλλά και με την Επιτροπή²⁸⁸.

Κομβικός ο ρόλος της Αρχής στη ΔΔ, πρωτίστως εποπτικός, καθόσον εποπτεύει την εύρυθμη διαλειτουργικότητα των πληροφοριακών συστημάτων, την ανταλλαγή δεδομένων με τρίτους φορείς και την τήρηση αρχείων. Υποστηρίζει, καθοδηγεί αλλά και προειδοποιεί τους υπεύθυνους επεξεργασίας στην εκπλήρωση των νέων υποχρεώσεών τους, καθώς προκύπτουν νέα ζητήματα και ανάγκες που πρέπει να αντιμετωπιστούν από τις Δημόσιες Υπηρεσίες²⁸⁹. Η τεχνολογική εξέλιξη επιβάλλει τον εκσυγχρονισμό της ΔΔ, με αρωγό την ΑΠΔΠΧ στον τομέα της προστασίας των

²⁸¹ Αρμοδιότητες του Εκτελούντος την Επεξεργασία ορίζονται στο άρθρο 28 ΓΚΠΔ.

²⁸² Σύμφωνα με τα οριζόμενα στα άρθρα 28 παρ.3^α και 29 ΓΚΠΔ.

²⁸³ Βλ. άρθρο 28 παρ. 3 ΓΚΠΔ.

²⁸⁴ Βλ. άρθρο 33 παρ. 2 ΓΚΠΔ.

²⁸⁵ Βλ. άρθρο 30 παρ. 2 ΓΚΠΔ.

²⁸⁶ Βλ. άρθρο 31 ΓΚΠΔ.

²⁸⁷ Βλ. από 22-5-2018 συνέντευξη του Κ.Μενουδάκου στο ηλεκτρονικό περιοδικό *epixeiro.gr*, ηλεκτρονική πηγή: <http://www.epixeiro.gr/article/87275>.

²⁸⁸ Βλ. Γ. Παπαγοπούλου, *Εποπτεία και επιβολή της τήρησης του ΓΚΠΔ (2018)*, όπ.ανωτ.

²⁸⁹ Βλ. Μ. Μυλώση (2018), όπ.ανωτ.

δεδομένων. Με τον ΓΚΠΔ ενισχύθηκε η συνεργασία μεταξύ των εθνικών αρχών προστασίας προσωπικών δεδομένων, προκειμένου να διασφαλίζεται η συνεκτική εφαρμογή και επιβολή του Κανονισμού στην εσωτερική αγορά, όπως ορίζει η αιτιολογική σκέψη 133 του Προοιμίου ΓΚΠΔ και ταυτόχρονα δόθηκε έμφαση στην κατοχύρωση της ανεξαρτησίας των εποπτικών αρχών.

Επιπλέον, κατά την αιτιολογική σκέψη 136, με τον ΓΚΠΔ συστάθηκε Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (ΕΣΠΔ)²⁹⁰ που εδρεύει στις Βρυξέλλες και αποτελεί έναν ανεξάρτητο ευρωπαϊκό οργανισμό με νομική προσωπικότητα, ο οποίος συμβάλλει στην εξασφάλιση μηχανισμού συνεκτικότητας μεταξύ των εποπτικών αρχών στην Ένωση και προάγει τη συνεργασία μεταξύ τους²⁹¹. Πρόκειται για όργανο ανάλογο της Ομάδας Εργασίας του άρθρου 29, αλλά διαθέτει πιο ουσιαστικές αρμοδιότητες. Όπως προαναφέρθηκε, το ΕΣΠΔ απαρτίζεται²⁹² από εκπροσώπους των εθνικών αρχών προστασίας δεδομένων και από τον ΕΕΠΔ²⁹³. Ο ρόλος του ΕΕΠΔ είναι να διασφαλίζει ότι, κατά την επεξεργασία προσωπικών δεδομένων, τα όργανα και οι οργανισμοί της ΕΕ σέβονται το δικαίωμα των πολιτών για προστασία της ιδιωτικής τους ζωής και συμμορφώνονται με τους κανόνες. Επιπρόσθετα, ο ΕΕΠΔ έχει συμβουλευτικό ρόλο επί των θεμάτων επεξεργασίας, διενεργεί έρευνες, διεκπεραιώνει καταγγελίες, παρακολουθεί νέες τεχνολογίες που θα μπορούσαν να έχουν επιπτώσεις στην προστασία των δεδομένων και συνεργάζεται με τις εθνικές αρχές προστασίας των κρατών-μελών.

Σύμφωνα με τον ΓΚΠΔ, οι εποπτικές αρχές συνεχίζουν να διατηρούν την ενημερωτική, ρυθμιστική και ελεγκτική λειτουργία που προέβλεπε η Οδηγία. Ειδικότερα, οι εποπτικές αρχές έχουν εξουσίες²⁹⁴ διερεύνησης, επίπληξης, διόρθωσης ή διαγραφής προσωπικών δεδομένων, κυρωτικές, αδειοδοτικές και συμβουλευτικές εξουσίες (ιδίως στις περιπτώσεις καταγγελιών φυσικών προσώπων²⁹⁵), όπως επίσης και την εξουσία να παραπέμπουν παραβάσεις των διατάξεων του Κανονισμού στις δικαστικές αρχές και να συμμετέχουν σε νομικές διαδικασίες. Επιπροσθέτως, στις ανωτέρω εξουσίες θα πρέπει να περιλαμβάνεται και η εξουσία περιορισμού ή απαγόρευσης της επεξεργασίας, η επιβολή διοικητικού προστίμου, όπως επίσης και η

²⁹⁰ Σύμφωνα με την εκτίμηση 139 του Προοιμίου ΓΚΠΔ, το Συμβούλιο Προστασίας Δεδομένων θα πρέπει να συσταθεί ως ανεξάρτητος φορέας της Ένωσης, ο οποίος θα προάγει τη συνεκτική εφαρμογή του Κανονισμού.

²⁹¹ *European Data Protection Board*, ιστότοπος: <https://edpb.europa.eu>.

²⁹² Οι εποπτικές αρχές των κρατών της ΕΖΕΣ και του ΕΟΧ είναι μέλη χωρίς δικαίωμα ψήφου.

²⁹³ Ιστότοπος: <https://edps.europa.eu>

²⁹⁴ Βλ. και αιτιολογική σκέψη 129 του Προοιμίου ΓΚΠΔ.

²⁹⁵ Βλ. αιτιολογική σκέψη 141 του Προοιμίου ΓΚΠΔ.

δυνατότητα θέσπισης προσωρινών μέτρων σε επείγουσα ανάγκη, ιδίως όταν υπάρχει κίνδυνος να παρεμποδισθεί σημαντικά η άσκηση δικαιώματος ενός υποκειμένου²⁹⁶.

Αν συγκρίνουμε τις αρμοδιότητες της Αρχής κατά το Ν.2472/97 και κατά τον ΓΚΠΔ²⁹⁷, θα μπορούσαμε να πούμε ότι κατά το προγενέστερο νομοθέτημα οι ρυθμιστικές της αρμοδιότητες περιελάμβαναν την καθοδήγηση μέσω οδηγιών και γνωμοδοτήσεων όσον αφορά την ενιαία εφαρμογή των ρυθμίσεων σε εθνικό και ευρωπαϊκό επίπεδο, την έκδοση κανονιστικών πράξεων, τη συνδρομή στην κατάρτιση κωδίκων δεοντολογίας, όπως επίσης την απάντηση σε αιτήσεις και ερωτήματα του υπευθύνου επεξεργασίας, προκειμένου να ελεγχθεί η νομιμότητα της επεξεργασίας. Στις ελεγκτικές αρμοδιότητες της Αρχής περιλαμβάνονταν ενδεικτικά οι διοικητικοί έλεγχοι, η επιβολή συστάσεων-υποδείξεων-κυρώσεων, η χορήγηση αδειών και διαβιβάσεων (για παράδειγμα αρχείου ευαίσθητων δεδομένων, διαβίβασης δεδομένων εκτός ΕΕ, διασύνδεσης αρχείων) κ.ά. Η ουσιαστική διαφορά σε σχέση με το Ν.2472/1997 είναι ότι πλέον οι προειδοποιήσεις, οι εντολές, τα πρόστιμα κλπ. μπορούν να απευθύνονται και στους εκτελούντες την επεξεργασία²⁹⁸.

Το ενδιαφέρον όμως επικεντρώνεται στις αρμοδιότητες που επιφυλάσσει στην ΑΠΔΠΧ ο ΓΚΠΔ και κατά πόσο με το νέο νομοθετικό πλαίσιο που αναλύεται στο Κεφάλαιο VI άρθρα 51 επόμενα, αυτές διαφοροποιήθηκαν ή όχι. Στο άρθρο 31 προβλέπεται η συνεργασία του υπευθύνου επεξεργασίας (ή του εκτελούντα την επεξεργασία) με την Αρχή, κατόπιν αιτήματος. Στις ελεγκτικές αρμοδιότητες περιλαμβάνεται ενδεικτικά η υποχρέωση γνωστοποίησης στην Αρχή περιστατικών παραβίασης δεδομένων προσωπικού χαρακτήρα²⁹⁹, η κατάρτιση καταλόγων δραστηριοτήτων υψηλού κινδύνου που υπόκεινται στην απαίτηση για διενέργεια εκτίμησης αντικτύπου και η προηγούμενη διαβούλευση με την παροχή γραπτών συμβουλών στον υπεύθυνο επεξεργασίας³⁰⁰, ενεργός ρόλος στις διαβιβάσεις δεδομένων προς τρίτες χώρες ή διεθνείς οργανισμούς κατά τα άρθρα 44 επόμενα ΓΚΠΔ και εξουσίες έρευνας, διορθωτικές, αδειοδοτικές και συμβουλευτικές³⁰¹. Στις ρυθμιστικές αρμοδιότητες της ΑΠΔΠΧ³⁰² εμπίπτει η συνεργασία με τους ΥΠΔ, η ενθάρρυνση των φορέων για εκπόνηση Κωδίκων Δεοντολογίας και θέσπιση

²⁹⁶ Βλ. αιτιολογική σκέψη 137 Προομίου ΓΚΠΔ.

²⁹⁷ Βλ. Γ. Ρουσόπουλο – Κ. Λιμνιώτη (2018), *όπ. ανωτ.*, σελ. 5.

²⁹⁸ Βλ. Γ. Παναγοπούλου (2018), *Εποπτεία και επιβολή της τήρησης του ΓΚΠΔ, όπ. ανωτ.*

²⁹⁹ Βλ. άρθρο 33 ΓΚΠΔ.

³⁰⁰ Βλ. άρθρα 35-36 ΓΚΠΔ.

³⁰¹ Βλ. άρθρο 58 ΓΚΠΔ.

³⁰² Βλ. άρθρα 39 επόμεν. ΓΚΠΔ.

μηχανισμών Πιστοποίησης προστασίας δεδομένων, η αρμοδιότητα στο ΕΣΠΑ ³⁰³ προκειμένου να συμβάλλει στη συνεκτική εφαρμογή του Κανονισμού κ.ά.

Συμπερασματικά λοιπόν, στα κύρια καθήκοντα της εποπτικής αρχής εμπίπτει η παρακολούθηση και επιβολή της εφαρμογής του ΓΚΠΔ, η ευαισθητοποίηση των ενδιαφερόμενων μερών σε ζητήματα όπως οι δραστηριότητες που απευθύνονται σε παιδιά, η παροχή συμβουλών προς την Κυβέρνηση και άλλους φορείς, η παροχή πληροφοριών στα υποκείμενα των δεδομένων, ο χειρισμός των καταγγελιών και η διενέργεια ερευνών μέσω της απαραίτητης πρόσβασης σε όλα τα απαιτούμενα δεδομένα³⁰⁴.

Όσον αφορά τη σχέση της ΑΠΔΠΧ με τον δημόσιο τομέα, όταν αυτός λειτουργεί ως υπεύθυνος επεξεργασίας, η Αρχή γνωμοδοτεί σε κάθε ρύθμιση που αφορά την επεξεργασία και την προστασία των προσωπικών δεδομένων. Όταν η ρύθμιση αφορά νομοθετικό ή διοικητικό μέτρο, η αρμοδιότητα της Αρχής είναι συμβουλευτική. Επίσης, σύμφωνα με τα άρθρα 35-36 ΓΚΠΔ, πριν εφαρμοστεί οποιοδήποτε νέο μέτρο ή διάταξη, πρέπει να προηγηθεί η Εκτίμηση Αντικτύπου και διαβούλευση με την εποπτική αρχή, την οποία ο νέος Κανονισμός επιβάλλει, όταν πρόκειται να εκδοθεί ένα νομοθετικό ή κανονιστικό μέτρο³⁰⁵.

5.5. Συμμόρφωση της Δημόσιας Διοίκησης με τον ΓΚΠΔ

Η ΔΔ υπόκειται στους κανόνες του ΓΚΠΔ όταν επεξεργάζεται προσωπικά δεδομένα που αφορούν ένα φυσικό πρόσωπο. Μάλιστα, ευθύνη των εθνικών διοικήσεων αποτελεί η στήριξη της περιφερειακής και της τοπικής διοίκησης, προκειμένου να προετοιμαστούν για την εφαρμογή του Κανονισμού, ο οποίος θα συντελέσει στην ενίσχυση της διαφάνειας της ΔΔ και της αύξησης της εμπιστοσύνης των πολιτών προς αυτήν. Η πλειοψηφία των δεδομένων προσωπικού χαρακτήρα που τηρούν οι Δημόσιες Διοικήσεις, συνήθως υποβάλλεται σε επεξεργασία λόγω νομικής υποχρέωσης ή λόγω εκτέλεσης καθήκοντος προς το δημόσιο συμφέρον, κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας. Σύμφωνα με την Ευρωπαϊκή Επιτροπή, κατά την επεξεργασία η ΔΔ οφείλει να σέβεται ορισμένες βασικές αρχές, όπως η δίκαιη και νόμιμη επεξεργασία σύμφωνα με τους

³⁰³ Βλ. άρθρα 68 επόμε. ΓΚΠΔ.

³⁰⁴ Βλ. Γ. Παναγοπούλου (2018), *όπ.ανωτ.*

³⁰⁵ Βλ. και άρθ. 13 ΣχΝΠΔΠΧ.

καθορισμένους σκοπούς και η ελαχιστοποίηση των δεδομένων. Εάν η επεξεργασία εκτελείται βάσει νόμου, ο νόμος αυτός θα πρέπει να διασφαλίζει την τήρηση των αρχών που επιβάλλει ο ΓΚΠΔ.

Λόγω όμως της κοινά αποδεκτής «ιδιαιτερότητας» του δημόσιου τομέα³⁰⁶, στον ΓΚΠΔ υπάρχουν ορισμένες εξαιρέσεις και αυτός δεν εφαρμόζεται όταν η επεξεργασία δεδομένων προσωπικού χαρακτήρα αφορά την κοινή πολιτική ασφάλειας και άμυνας της χώρας³⁰⁷, όπως επίσης όταν η επεξεργασία πραγματοποιείται από αρμόδιες αρχές για σκοπούς πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή εκτέλεσης ποινικών κυρώσεων, συμπεριλαμβανομένης της προστασίας και πρόληψης έναντι κινδύνων που απειλούν τη δημόσια ασφάλεια³⁰⁸. Επίσης, προς διευκόλυνση των ελέγχων που διενεργούν οι δημόσιες αρχές (όπως φορολογικές και τελωνειακές, μονάδες οικονομικής έρευνας, ανεξάρτητες διοικητικές αρχές ή αρχές χρηματοπιστωτικών αγορών), αυτές δεν θεωρούνται αποδέκτες, αν λάβουν προσωπικά δεδομένα που τους είναι απαραίτητα για τη διενέργεια συγκεκριμένης έρευνας για το γενικό συμφέρον, σύμφωνα με το δίκαιο της Ένωσης ή κράτους-μέλους³⁰⁹. Στην περίπτωση αυτή, η επεξεργασία θα πρέπει να συμβαδίζει με τους ισχύοντες κανόνες προστασίας των δεδομένων, ανάλογα με τους σκοπούς της επεξεργασίας.

Κατά τη μεταβατική περίοδο λοιπόν που μεσολάβησε μεταξύ της ψήφισης του ΓΚΠΔ και της τελικής εφαρμογής του, θα έπρεπε οι δημόσιες αρχές που επεξεργάζονται προσωπικά δεδομένα, να αξιολογήσουν τις αλλαγές που επήλθαν, κυρίως αναφορικά με τις υποχρεώσεις τους ως υπεύθυνοι ή εκτελούντες την επεξεργασία και να σχεδιάσουν στρατηγική προσαρμογής τους στις νέες απαιτήσεις³¹⁰.

Ερωτήματα προς απάντηση αποτελούν το κατά πόσο έχει ξεκινήσει η υλοποίηση του ΓΚΠΔ και η συμμόρφωση του ελληνικού δημόσιου τομέα, το εάν έχουν ληφθεί τα απαραίτητα μέτρα και το εάν έχει διατεθεί χρόνος και χρήμα για την επίτευξη των επιταγών του νέου νομοθετήματος.

³⁰⁶ Βλ. *Ε. Σιουγλέ (2018), όπ.ανωτ., σελ. 94 επόμε.*

³⁰⁷ Βλ. *άρθ. 2 παρ.2 εδ.β ΓΚΠΔ και 42 επόμε. ΣΕΕ.*

³⁰⁸ Βλ. *άρθ. 2 παρ.2 εδ.δ ΓΚΠΔ και Οδηγία 680/2016/ΕΕ όπως αναλύθηκε ανωτέρω.*

³⁰⁹ Βλ. *άρθ. 4 παρ. 9 και αιτιολογική σκέψη 31 ΓΚΠΔ.*

³¹⁰ Βλ. *Γ. Λαζαράκο, Ο θεσμός του ΥΠΔ (Data Protection Officer) στο νέο νομοθετικό πλαίσιο των προσωπικών δεδομένων μετά την υιοθέτηση του Κανονισμού (ΕΕ) 679/2016 (2016), όπ.ανωτ., σελ.243.*

5.6. Βήματα προετοιμασίας του Δημόσιου Τομέα για τον ΓΚΠΔ

Προκειμένου να επιτευχθεί η συμμόρφωση της ΔΔ στις επιταγές του Κανονισμού, θα έπρεπε να ακολουθηθούν ορισμένα βήματα³¹¹ που θα προετοίμαζαν τους δημόσιους φορείς ώστε να ανταπεξέλθουν στις νέες τους υποχρεώσεις. Οι νέες έννοιες που εισήχθησαν με τον ΓΚΠΔ, όπως το δικαίωμα στη λήθη ή στη φορητότητα, η υποχρέωση γνωστοποίησης της παραβίασης στην ΑΠΔΠΧ και η λογοδοσία του υπευθύνου ή του εκτελούντα την επεξεργασία, η μεταφορά του κέντρου βάρους από τις κατασταλτικές δυνατότητες των αρχών στις προληπτικές ενέργειες των εμπλεκόμενων και άλλες αλλαγές, οδήγησαν στην ανάγκη καλλιέργειας «κουλτούρας προστασίας δεδομένων»³¹². Η αναζήτηση της ενημέρωσης, η διαρκής επαγρύπνηση, η αναλυτική πληροφόρηση, η κατανόηση και ερμηνεία των διατάξεων, η μελέτη των εσωτερικών Κανονισμών κάθε Οργανισμού, η χαρτογράφηση όλων των δεδομένων κ.ά., αποτελούν κάποια βασικά βήματα.

Ειδικότερα, σύμφωνα με τις οδηγίες της Αρχής³¹³, πρωτεύει η ενημέρωση του ανθρώπινου δυναμικού για τις επερχόμενες αλλαγές. Είναι πολύ σημαντικό να γνωρίζει το προσωπικό τις επιπτώσεις των παραβιάσεων, τους κινδύνους που ελλοχεύουν και τους τρόπους αντιμετώπισης αυτών. Κάθε Οργανισμός που διαθέτει ειδικό αρχείο επεξεργασιών, θα πρέπει να καταγράψει με λεπτομέρεια τα δεδομένα που διατηρεί και τις επεξεργασίες στις οποίες προβαίνει. Απαραίτητη ενέργεια αποτελεί ο διαρκής έλεγχος τήρησης των αρχών επεξεργασίας και σεβασμού των δικαιωμάτων των υποκειμένων. Ο δημόσιος φορέας οφείλει να είναι σε θέση να ανταποκριθεί σε ένα νόμιμο αίτημα διαγραφής και να μην επαναπαύεται στην άγνοια των πολιτών. Κατόπιν, θα πρέπει να εξασφαλιστεί η συγκατάθεση για κάθε σκοπό της επεξεργασίας, να επικαιροποιηθούν οι πολιτικές προστασίας των δεδομένων και να πραγματοποιηθεί εκτίμηση αντικτύπου. Φυσικά, μεταξύ άλλων, ο δημόσιος Οργανισμός οφείλει να ορίσει ΥΠΔ και να ανακαλύψει μεθόδους που να ανιχνεύουν πιθανές παραβιάσεις, τις οποίες οφείλει να αποτρέπει δια της ασφαλούς επεξεργασίας των προσωπικών δεδομένων μέσω των κατάλληλων μέτρων.

³¹¹ Η ΑΠΔΠΧ έχει εκδώσει οδηγίες για την προετοιμασία των φορέων σε 10 βήματα, ηλεκτρονική πηγή: http://www.dpa.gr/portal/page?_pageid=33,209418&_dad=portal&_schema=PORTAL.

³¹² Βλ. Γ. Γιαννόπουλο, ΓΚΠΔ: οι νέες υποχρεώσεις και η ευθύνη του Υπευθύνου Επεξεργασίας (2017), όπ.ανωτ., σελ.206.

³¹³ Βλ. και Ι. Ιγγλεζάκη «Κανονισμός Προστασίας Δεδομένων» στο διαδίκτυο, ηλεκτρονική πηγή: <http://iglezakis.gr/>

Η φύση των υποχρεώσεων κάθε φορέα εξαρτάται από διάφορους παράγοντες³¹⁴, όπως το είδος της επεξεργασίας δεδομένων που πραγματοποιείται και οι εκτιμώμενοι κίνδυνοι. Η ευθύνη της συμμόρφωσης αφορά τον υπεύθυνο επεξεργασίας και τον εκτελούντα την επεξεργασία, όμως κατά τη διάρκεια προετοιμασίας εμπλέκονται πολλοί ενδιαφερόμενοι από τους οποίους εξαρτάται το τελικό αποτέλεσμα, όπως για παράδειγμα το νομικό τμήμα ή το τμήμα πληροφορικής του φορέα.

Αρχικά πρέπει να τονιστεί ότι οι δημόσιοι φορείς που δεν έχουν ακόμα ανταποκριθεί στην υιοθέτηση του νέου νομοθετήματος, οφείλουν να δράσουν άμεσα, συστηματικά και βάσει σχεδίου. Δυστυχώς στην πλειοψηφία τους τα υπουργεία έχουν προβεί σε πολύ περιορισμένες ενέργειες «ουσιαστικής» συμμόρφωσης, οι οποίες κατά κύριο λόγο εξαντλούνται στον ορισμό ΥΠΔ και την κοινοποίηση των στοιχείων του στην ΑΠΔΠΧ. Διαπιστώθηκε λοιπόν, κατόπιν έρευνας, ότι το πρώτο βήμα, το οποίο είναι η ετοιμασία ενός πλάνου που περιλαμβάνει την συνοπτική καταγραφή των αναγκαίων βημάτων συμμόρφωσης, τον ορισμό χρονοδιαγράμματος, την προετοιμασία για αντιμετώπιση των ελλείψεων, την ενημέρωση του ανθρώπινου δυναμικού όσον αφορά την αλλαγή του νομικού πλαισίου, τα δικαιώματα των φυσικών προσώπων και τις υποχρεώσεις των υπηρεσιών, στην πλειοψηφία των Οργανισμών δεν έχει πραγματοποιηθεί. Ένας από τους πιθανούς λόγους είναι η αύξηση του φόρτου εργασίας που θα επέλθει στον φορέα, όμως αυτό που πρέπει να συνειδητοποιήσουν οι δημόσιοι φορείς είναι ότι η πρόληψη αποτελεί τον καλύτερο σύμμαχο στην αντιμετώπιση των μελλοντικών προβλημάτων³¹⁵. Για το λόγο αυτό θα πρέπει να ανατεθούν άμεσα αρμοδιότητες και ρόλοι, όπως ο ορισμός ΥΠΔ, που αποτελεί βασική υποχρέωση κάθε δημόσιας αρχής ή φορέα, ανεξαρτήτως μεγέθους του και που θα βοηθήσει αποτελεσματικά στην υλοποίηση του ΓΚΠΔ.

Επόμενο βήμα αποτελεί η αναγνώριση των δραστηριοτήτων επεξεργασίας προσωπικών δεδομένων και η καταγραφή τους από τον υπεύθυνο επεξεργασίας ή τον εκπρόσωπο αυτού. Αναφέρθηκε ανωτέρω τι περιλαμβάνει ο όρος «επεξεργασία» και συνακόλουθα καθίσταται σαφές ότι υπάρχει ενδεχόμενο να διαφύγει της προσοχής κάποια δραστηριότητα, που δεν θα χαρακτηρίζεται ευθέως ως επεξεργασία. Η αποθήκευση προσωπικών δεδομένων είναι η συνηθέστερη μορφή επεξεργασίας στο Δημόσιο, δεδομένης της ύπαρξης πολλών αρχείων, από το απλό αρχείο τήρησης εγγράφων, το αρχείο προσωπικού και το αρχείο πρωτοκόλλου, μέχρι τα αρχεία σε

³¹⁴ Βλ. Γ. Ρουσόπουλο – Κ. Λιμνιώτη (2018), *όπ. ανωτ.*, σελ. 23 επόμε.

³¹⁵ Βλ. Ε. Σιουγλέ (2018), *όπ. ανωτ.*, σελ. 97-98.

ηλεκτρονικές εφαρμογές, τα ειδικά μητρώα³¹⁶, το αρχείο καταγραφής οπτικού υλικού για λόγους ασφαλείας κ.ά. Για την προσφορότερη καταγραφή, καλό θα ήταν να προηγηθεί κατηγοριοποίηση των δραστηριοτήτων βάσει κριτηρίων, όπως για παράδειγμα ανάλογα με τον σκοπό που κάθε επεξεργασία εξυπηρετεί. Όπως προαναφέρθηκε, όποιος φορέας απασχολεί πάνω από 250 εργαζομένους, οφείλει ανεξαιρέτως να τηρεί αρχείο δραστηριοτήτων επεξεργασίας. Υπάρχουν όμως ορισμένες εξαιρέσεις, που εάν συντρέχουν, επιβάλλουν την τήρηση αρχείου και σε μικρότερους δημόσιους Οργανισμούς. Αυτές είναι η δυνατότητα να προκαλέσει η επεξεργασία κίνδυνο για τα δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων, η μη περιστασιακή επεξεργασία και η επεξεργασία ευαίσθητων δεδομένων ή δεδομένων που αφορούν ποινικές καταδίκες.

Ακολούθως, ο δημόσιος Οργανισμός θα πρέπει να εξετάσει εάν πετυχαίνει τη συμμόρφωση με τον Κανονισμό, ήτοι εάν εφαρμόζει τις αρχές νόμιμης επεξεργασίας των δεδομένων και εάν γίνονται σεβαστά τα δικαιώματα των υποκειμένων. Για να απαντηθεί το ερώτημα τούτο, ελέγχονται ορισμένες παράμετροι, όπως η νομοθετική στοιχειοθέτηση της επεξεργασίας που διενεργείται, η πραγματοποίηση της επεξεργασίας εντός των πλαισίων του ορισθέντος σκοπού και βάσει των εντολών του υπευθύνου επεξεργασίας, η τήρηση της αρχής της αναγκαιότητας προκειμένου να τυγχάνουν επεξεργασίας μόνο τα απαραίτητα για την επίτευξη του σκοπού δεδομένα κ.ά. Ταυτόχρονα, ελέγχεται η ασφάλεια της τήρησης και επεξεργασίας των δεδομένων: ερωτήσεις όπως ποιοι υπάλληλοι έχουν και ποιοι θα έπρεπε να έχουν πρόσβαση στα δεδομένα, αν λαμβάνονται επαρκή μέτρα για περιορισμό των επαπειλούμενων κινδύνων, αν εφαρμόζονται οι πρακτικές της κρυπτογράφησης, της ψευδωνυμοποίησης, της ανωνυμοποίησης και της εμπιστευτικότητας όπου είναι απαραίτητο, αν υπάρχει άδεια του υπευθύνου επεξεργασίας για την εκτελούμενη επεξεργασία, θα πρέπει να λάβουν απαντήσεις σε εύλογο χρονικό διάστημα. Επιπλέον, προσοχή απαιτείται στις περιπτώσεις διαβίβασης δεδομένων σε τρίτους (δημόσιους οργανισμούς, εταιρίες, πολίτες) ή και εκτός ΕΕ. Ο ΓΚΠΔ προβλέπει στο εδάφιο δ' της παραγράφου 1 του άρθρου 49 αποκλίσεις από τις γενικές αρχές διαβίβασης προσωπικών δεδομένων προς τρίτες χώρες ή διεθνείς οργανισμούς, όταν η διαβίβαση είναι απαραίτητη για σημαντικούς λόγους δημοσίου συμφέροντος. Επίσης θα πρέπει να πραγματοποιηθεί έλεγχος αν η συλλογή των δεδομένων γίνεται

³¹⁶ Για παράδειγμα: μητρώο ΥΠΔ που τηρεί η ΑΠΔΠΧ.

με συγκατάθεση σύμφωνα με τον ΓΚΠΔ και εάν οι συνεργαζόμενες εταιρίες συμμορφώνονται με τις επιταγές του. Ο ΓΚΠΔ προβλέπει νέα και επαυξημένα δικαιώματα για τους πολίτες και την ικανοποίησή τους σε στενά χρονικά πλαίσια, άρα το Δημόσιο οφείλει να διαθέτει τις κατάλληλες διαδικασίες και το προσωπικό, ώστε να ανταπεξέλθει στα αιτήματά τους³¹⁷.

Η ασφάλεια της επεξεργασίας των προσωπικών δεδομένων πρέπει να αποτελεί τη βασική μέριμνα της ΔΔ, δεδομένου του τεράστιου όγκου αρχείων που διαθέτει και διαχειρίζεται. Προκειμένου να αποφευχθούν περιστατικά θεμιτής ή αθέμιτης παραβίασης, θα πρέπει να ληφθούν τα κατάλληλα τεχνικά και οργανωτικά μέτρα και δεν επαρκεί ένα απλό κείμενο Πολιτικής Προστασίας Προσωπικών Δεδομένων ή Απορρήτου. Είναι πολύ κρίσιμο να αποτρέπονται παρόμοια περιστατικά, αλλά και να ανιχνεύεται εγκαίρως ένα περιστατικό παραβίασης, ώστε να περιοριστούν οι επαπειλούμενοι κίνδυνοι. Οι δημόσιοι φορείς θα πρέπει να είναι σε θέση να γνωρίζουν τι ακριβώς συνιστά περιστατικό παραβίασης δεδομένων και να το αξιολογούν, ώστε να ενημερώνεται άμεσα ο υπεύθυνος επεξεργασίας, κατόπιν το ενδιαφερόμενο πρόσωπο, όπως περιγράφεται ανωτέρω, και ακολούθως η ΑΠΔΠΧ.

Αν τηρηθούν αυτές οι τακτικές πρόληψης, θα περιοριστούν και οι επαπειλούμενες κυρώσεις κατά του Δημοσίου, όπως αυτές προβλέπονται από τον Κανονισμό στα άρθρα 77 επόμενα, τα οποία αφορούν το καθεστώς προσφυγών, ευθύνης και κυρώσεων. Κατά το άρθρο 77 ΓΚΠΔ, κάθε υποκείμενο που θεωρεί ότι η επεξεργασία των προσωπικών του δεδομένων του είναι παράνομη, δικαιούται να υποβάλλει καταγγελία (διοικητική προσφυγή) σε εποπτική αρχή. Το άρθρο 78 ΓΚΠΔ παρέχει στα φυσικά ή νομικά πρόσωπα το δικαίωμα της πραγματικής δικαστικής προσφυγής κατά νομικά δεσμευτικής απόφασης εποπτικής αρχής που τα αφορά, ενώ το άρθρο 79 ΓΚΠΔ ρυθμίζει το δικαίωμα δικαστικής προσφυγής κατά υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία.

Ειδικότερα, αν η ΔΔ δε συμμορφώνεται με τους κανόνες προστασίας δεδομένων, η Αρχή έχει στη διάθεσή της διάφορα εργαλεία και εξουσίες που μπορεί να χρησιμοποιήσει, όπως αυτά προβλέπονται στο άρθρο 58 ΓΚΠΔ³¹⁸ αλλά και όπως θεσπίζουν εθνικοί νόμοι, οι οποίοι μπορούν να προσδώσουν στην Αρχή πρόσθετες εξουσίες. Αρχικά, στην περίπτωση που η Διοίκηση έχει προβεί σε πιθανή

³¹⁷ Βλ. Γ. Παναγοπούλου (2018), *Εποπτεία και επιβολή της τήρησης του ΓΚΠΔ*, ό.π.ανωτ.

³¹⁸ Βλ. ηλεκτρονική πηγή: <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/public-administrations-and-data-protection>, άρθρα 82-84 ΓΚΠΔ, αιτιολογικές σκέψεις 129, 146-148, 150, 151 Προοιμίου ΓΚΠΔ.

(«εικαζόμενη») παράβαση του Κανονισμού, η Αρχή μπορεί να εκδώσει προειδοποίηση, την οποία θα απευθύνει προς τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία. Εάν υπάρξει διαπιστωμένη παράβαση διατάξεων του ΓΚΠΔ, οι δυνατότητες της Αρχής περιλαμβάνουν, μεταξύ άλλων, την επίπληξη και την προσωρινή ή οριστική απαγόρευση της επεξεργασίας. Επίσης, οι δημόσιες αρχές και φορείς ενδέχεται να υπόκεινται σε διοικητικά πρόστιμα, αν αυτό επιβάλλεται από τον εθνικό νόμο του κράτους-μέλους περί προστασίας των προσωπικών δεδομένων. Στην Ελλάδα δεν έχει ακόμα εκδοθεί ο αντίστοιχος νόμος, σύμφωνα όμως με το σχέδιο αυτού και το άρθρο 69, είναι δυνατή η επιβολή προστίμων και σε δημόσιες αρχές και φορείς του δημόσιου τομέα. Για τη λήψη της απόφασης και τον καθορισμό του ύψους των προστίμων, λαμβάνονται υπόψη ορισμένα κριτήρια και παράγοντες, όπως η φύση, η σοβαρότητα και η διάρκεια της παράβασης, ο αριθμός των θιγόμενων υποκειμένων και ο βαθμός ζημίας που υπέστησαν, ο δόλος ή η αμέλεια που προκάλεσε την παράβαση, οι ενέργειες στις οποίες προέβη ο υπεύθυνος ή ο εκτελών την επεξεργασία προκειμένου να επανορθώσει τη βλάβη που επήλθε, τυχόν σχετικές προηγούμενες παραβάσεις, η συμμόρφωση προς εντολή της Αρχής κ.ά. Άξιο αναφοράς αποτελεί το ύψος των διοικητικών προστίμων, το οποίο μπορεί να φτάσει στο ποσό των 20.000.000 ευρώ. Τα διοικητικά πρόστιμα πάντως θα πρέπει να είναι αποτελεσματικά, αναλογικά και αποτρεπτικά, διότι, όταν αυτά είναι υψηλά, συμβάλλουν στη διασφάλιση της επιβολής και της συμμόρφωσης μέσω της πρόληψης.

Επιπλέον, τα πρόσωπα που υπέστησαν ζημία λόγω παραβίασης του Κανονισμού από έναν δημόσιο Οργανισμό, μπορούν να διεκδικήσουν αποζημίωση από τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία (αστική ευθύνη). Η έννοια της «ζημίας» πρέπει να ερμηνεύεται διασταλτικά και περιλαμβάνει τις υλικές και μη ζημίες, όπως για παράδειγμα οικονομικές απώλειες και ηθικές βλάβες. Τα υποκείμενα των δεδομένων πρέπει να λαμβάνουν πλήρη και ουσιαστική αποζημίωση για τη ζημία που υπέστησαν ανεξαρτήτως αριθμού των Οργανισμών που εμπλέκονται στην επεξεργασία των δεδομένων τους. Τέλος, η αποζημίωση μπορεί να αναζητηθεί είτε απευθείας από τον δημόσιο φορέα, είτε ενώπιον των αρμόδιων εθνικών δικαστηρίων του κράτους-μέλους.

5.7. Αποτελέσματα έρευνας για την συμμόρφωση του Δημοσίου Τομέα στον ΓΚΠΔ

Διεξήχθη έρευνα με αντικείμενο τη συμμόρφωση των διαφόρων Υπουργείων με τον ΓΚΠΔ και τον υποχρεωτικό ορισμό ΥΠΔ, κατά την οποία υπεβλήθη γραπτό ερώτημα προς όλα τα Υπουργεία, περί του εάν έχει οριστεί ΥΠΔ και σε ποιες ενέργειες έχει προβεί το κάθε Υπουργείο προκειμένου να εφαρμόσει τον Κανονισμό.

Το Υπουργείο Υγείας υπήρξε πρωτοπόρο στην έγκαιρη οργάνωση και προετοιμασία των εποπτευόμενων φορέων παροχής υπηρεσιών υγείας για συμμόρφωση με τα οριζόμενα στον ΓΚΠΔ³¹⁹. Προς επίρρωση αυτού του ισχυρισμού αναφέρεται ενδεικτικά η από 12-3-2018 προκήρυξη ηλεκτρονικού δημόσιου ανοιχτού διεθνούς διαγωνισμού για την επιλογή αναδόχου, με σκοπό την υλοποίηση του έργου «Λογισμικό αρχειοθέτησης και διακίνησης εγγράφων και Παροχή υπηρεσιών προσδιορισμού επιπέδου συμμόρφωσης με τον Εθνικό Οργανισμό Παροχής Υπηρεσιών Υγείας (ΕΟΠΥΥ) σχετικά με τον GDPR»³²⁰. Το Υπουργείο προέβη εγκαίρως στον ορισμό ΥΠΔ σύμφωνα με τις διατάξεις των άρθρων 37-39 του ΓΚΠΔ, σε αντίθεση με τους περισσότερους δημόσιους φορείς, οι οποίοι φάνηκαν απροετοίμαστοι. Μάλιστα, έχει δημιουργήσει δύο διευθύνσεις ηλεκτρονικού ταχυδρομείου για επικοινωνία με τον ΥΠΔ του Υπουργείου³²¹, ο οποίος είναι νομικός, ειδικός επιστήμονας της ΑΠΔΠΧ αποσπασμένος στο Υπουργείο. Σαν δεύτερο βήμα, τον Ιούλιο του 2018 ο ΥΠΔ προέβη στη σύνταξη εγκυκλίου οδηγού προετοιμασίας, με βασικό γνώμονα την προστασία των ατόμων έναντι της επεξεργασίας των προσωπικών τους ευαίσθητων ή μη δεδομένων³²². Η σχετική εγκύκλιος συντάχθηκε προκειμένου να ενισχυθούν οι δράσεις συμμόρφωσης ως προς τον ΓΚΠΔ και περιέχει συνοπτική παρουσίαση του Κανονισμού, τα βασικά βήματα προετοιμασίας και εφαρμογής από τους φορείς υπηρεσιών υγείας, ρυθμίσεις που αφορούν τους ΥΠΔ, ερωτήματα και προβληματισμούς του προσωπικού του Υπουργείου σχετικά με τις υποχρεώσεις των φορέων και τα δικαιώματα των ασθενών και, τέλος, τη διαδικασία εκτέλεσης μελέτης αντικτύπου. Επόμενο βήμα του

³¹⁹ Βλ. ιστότοπο: <http://www.moh.gov.gr/articles/gdpr>.

³²⁰ Βλ. Δ. Λεμπέση (2018β), *όπ.ανωτ.*, σελ. 605.

³²¹ Ηλεκτρονικές διευθύνσεις: dpo@moh.gov.gr και gdpr@moh.gov.gr

³²² Οδηγός Προετοιμασίας-Βασικές Κατευθύνσεις του Υπουργείου Υγείας για τη συμμόρφωση προς τον ΓΚΠΔ: «Σε ένα ασθενοκεντρικό σύστημα παροχής υπηρεσιών υγείας, η προστασία του ατόμου έναντι της επεξεργασίας δεδομένων του προσωπικού χαρακτήρα δεν συνιστά απλή επιλογή, αλλά πρωταρχικό σκοπό του συστήματος».

Υπουργείου αποτελεί η δημιουργία ενότητας ενημερωτικού χαρακτήρα σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα στον τομέα της υγείας.

Η ΑΠΔΠΧ απάντησε στις 14-11-2018 ότι έχει στη διάθεσή της κατάλογο των ΥΠΔ που έχουν ορίσει κάποια Υπουργεία (όχι όλα), τα στοιχεία τους όμως δεν είναι κοινοποιήσιμα από την Αρχή αλλά απευθείας από το κάθε Υπουργείο, στο οποίο θα πρέπει να απευθυνθεί κάποιος προσωπικά κι ότι κατά τα λοιπά δεν έχει άλλα στοιχεία για την περαιτέρω συμμόρφωση του δημοσίου τομέα.

Το Υπουργείο **Παιδείας, Έρευνας και Θρησκευμάτων** απάντησε στις 15-11-2018 ότι έχει εκδοθεί η υπ' αρ. 123622/Γ1/20-7-2018 (ΑΔΑ: ΩΣΙΒ4653ΠΣ-Υ7Μ) Απόφαση με θέμα: «Ορισμός Υπευθύνου Προστασίας Δεδομένων (Data protection Officer-DPO) του Υπουργείου Παιδείας, Έρευνας και Θρησκευμάτων».

Το Υπουργείο **Διοικητικής Ανασυγκρότησης** απάντησε στις 20-11-2018 δια της ΥΠΔ του³²³, ότι μέσω διαγωνισμού θα γίνει η επιλογή αναδόχου για να λάβει ως υπηρεσία τη χαρτογράφηση των διαδικασιών, την εκπόνηση των απαραίτητων μελετών, την προετοιμασία εκπαιδευτικού υλικού, την προετοιμασία σημειωμάτων και άλλων απαραίτητων για τη συμμόρφωση με τον ΓΚΠΔ.

Το Υπουργείο **Εργασίας, Κοινωνικής Ασφάλισης και Αλληλεγγύης** απάντησε ότι, δυνάμει της υπ' αρ. 31935/Δ1.11180/08-06-2018 Υπουργικής Απόφασης, έχει οριστεί ΥΠΔ υπάλληλος του Υπουργείου.

Στις 27-11-2018, το Υπουργείο **Εξωτερικών** δια του ΥΠΔ του³²⁴ απάντησε ότι με την υπ' αρ. Π37Α-39039/05.07.2018 απόφαση του Υπουργού Εξωτερικών, έχει ορισθεί ΥΠΔ για το Υπουργείο και με την υπ' αρ. Π37Α-42781/23.07.2018 απόφαση, έχει συγκροτηθεί ομάδα Εργασίας για την υποστήριξη του ΥΠΔ του Υπουργείου (Ομάδα Προστασίας Προσωπικών Δεδομένων). Επίσης, η ανωτέρω ομάδα βρίσκεται στη διαδικασία καταγραφής δραστηριοτήτων του Υπουργείου που ενσωματώνουν επεξεργασία προσωπικών δεδομένων.

Το Υπουργείο **Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων** έχει ορίσει ΥΠΔ³²⁵ με την υπ' αρ. 52740/10-7-2018 Υπουργική απόφαση, ενώ ως προς το θέμα της ενσωμάτωσης της σχετικής οδηγίας για την προστασία των προσωπικών δεδομένων, αυτή δεν έχει ενσωματωθεί έως σήμερα.

³²³ Ηλεκτρονική διεύθυνση: dpo@ydmed.gov.gr.

³²⁴ Ηλεκτρονική διεύθυνση: dpo@mfa.gr.

³²⁵ Ηλεκτρονική διεύθυνση: dpo@justice.gov.gr.

Το Υπουργείο **Οικονομικών**, ως επεξεργαζόμενο πλήθος φορολογικών δεδομένων προσωπικού χαρακτήρα³²⁶, απάντησε στις 12-12-2018 ότι όλες οι Γενικές Διευθύνσεις του Υπουργείου ενημερώθηκαν πλήρως για τον ΓΚΠΔ. Ειδικά η Γενική Γραμματεία Πληροφοριακών Συστημάτων³²⁷ προχώρησε στην καταγραφή των συστημάτων και των ενεργειών κάθε διεύθυνσης και κάθε τμήματος, ενώ η μελέτη και καταγραφή των διαδικασιών των εκάστοτε συστημάτων ανατέθηκε σε ειδικό εξωτερικό σύμβουλο. Το πιο σημαντικό όμως είναι ότι δημιουργήθηκε με τον Οργανισμό του Υπουργείου, αυτοτελές γραφείο ΥΠΔ, με πενταμελή σύνθεση, σε συμμόρφωση με τον ΓΚΠΔ και προκειμένου να προαχθεί η κουλτούρα της προστασίας προσωπικών δεδομένων εντός του φορέα.

Το Υπουργείο **Εσωτερικών** έχει επίσης ορίσει ΥΠΔ βάσει της υπ' αρ. ΑΠ 23837/29-5-2018 Απόφασης του Υπουργού, ο οποίος είναι υπάλληλος της μονάδας εσωτερικού ελέγχου του Υπουργείου³²⁸.

Το Υπουργείο **Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης** έχει ορίσει ΥΠΔ³²⁹ και αναπληρωτή, αλλά δεν απάντησε εγγράφως.

Ο τομέας **Μακεδονίας-Θράκης** του Υπουργείου Εσωτερικών απάντησε στις 12-12-2018 δια αρμοδίου υπαλλήλου του, ότι λόγω φόρτου εργασίας δεν είναι σε θέση να απαντήσει στο υποβληθέν έγγραφο αίτημα χορήγησης πληροφοριών.

Στο **Υπουργείο Αγροτικής Ανάπτυξης και Τροφίμων** έχει προκηρυχθεί συνοπτικός διαγωνισμός για την εξεύρεση αναδόχου για την παροχή υπηρεσιών συμμόρφωσης του Υπουργείου και των εποπτευόμενων φορέων Ε.Φ.Ε.Τ. και ΕΛΓΟ-ΔΗΜΗΤΡΑ προς τις απαιτήσεις του ΓΚΠΔ και λήψης απαραίτητων διορθωτικών μέτρων [Διακήρυξη αριθ. 3507/Χ.Δ/2018 Συνοπτικού (Πρόχειρου) Διαγωνισμού], ενώ οι διαδικασίες ορισμού του/της ΥΠΔ δεν έχουν ολοκληρωθεί ακόμα.

Στις 28-12-2018 απάντησε το **Υπουργείο Εθνικής Άμυνας** ότι κατ' εφαρμογή του άρθρου 37 του ΓΚΠΔ για τον ορισμό ΥΠΔ στο Υπουργείο και στις δομές του,

³²⁶ Το Υπουργείο Οικονομικών έχει πολλές φορές απασχολήσει την ΑΠΔΠΧ για τη νομιμότητα του μέτρου της δημοσιοποίησης στο διαδίκτυο, φορολογικών προσωπικών δεδομένων. Ενδεικτικά: Απόφαση με αρ. 54/2011, Γνωμοδοτήσεις με αρ. 1/2011 και 4/2011 ΑΠΔΠΧ δημοσιευμένες στον διαδικτυακό τόπο της Αρχής www.dpa.gr.

³²⁷ Σύμφωνα με την υπ'αρ. 98/2013 Απόφαση της ΑΠΔΠΧ, υπεύθυνο επεξεργασίας του Υπουργείου Οικονομικών αποτελεί η Γενική Γραμματεία Πληροφοριακών Συστημάτων, βλ. και εισήγηση Δ. Ζωγραφόπουλου, Ο έλεγχος της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα στις επεξεργασίες φορολογικών δεδομένων προσωπικού χαρακτήρα, σε: Α. Κοτσαλή (επιμ.), *όπ.ανωτ.* (2016), σελ.273.

³²⁸ Ηλεκτρονική διεύθυνση: s.theoxaris@ypes.gr

³²⁹ Ηλεκτρονική διεύθυνση: dpo@mindigital.gr

λαμβανομένων υπόψη των παραμέτρων του οργανωτικού μεγέθους και της πολυεπίπεδης οργανωτικής δομής των Ενόπλων Δυνάμεων, έχουν αναληφθεί ενέργειες και η διαδικασία βρίσκεται σε εξέλιξη.

Τα υπόλοιπα Υπουργεία, ήτοι: Πολιτισμού και Αθλητισμού, Περιβάλλοντος και Ενέργειας, Προστασίας του Πολίτη, Ναυτιλίας και Νησιώτικης Πολιτικής, Υποδομών και Μεταφορών, Ψηφιακής Πολιτικής-Τηλεπικοινωνιών και Ενημέρωσης, Αιγαίου, Τουρισμού και Μεταναστευτικής Πολιτικής δεν παρείχαν πληροφορίες, ενώ εύλογη απορία δημιουργεί η διαφορετική αντιμετώπιση των φορέων της Κυβέρνησης επί του αυτού θέματος, όπως επίσης και η έλλειψη ενημέρωσης των υπαλλήλων εκάστου Υπουργείου για τις μεταρρυθμίσεις που έλαβαν χώρα και για το νέο νομοθετικό πλαίσιο.

Ενδιαφέρον θα παρουσίαζε **μελλοντική έρευνα** στον δημόσιο τομέα, μετά την πάροδο ορισμένου χρονικού διαστήματος, σχετικά με την ενημέρωση των ενδιαφερόμενων μερών και την υλοποίηση στην πράξη του νέου θεσμού.

6. Νομολογία που αφορά τον ΓΚΠΔ

Δεδομένης της πολύ πρόσφατης εφαρμογής του ΓΚΠΔ, δεν υφίσταται ακόμα νομολογία από τα εθνικά ή κοινοτικά Δικαστήρια και για το λόγο αυτό η έκδοση συστάσεων και γνωμοδοτήσεων από τις Αρχές θα δημιουργήσει νομολογιακές αναφορές που θα βοηθήσουν στην επίλυση ερωτημάτων³³⁰.

Στις 29-6-2018 το ΔΕΕ εξέδωσε το υπ' αριθμ. 96/18 ανακοινωθέν τύπου, σύμφωνα με το οποίο και στα πλαίσια της έναρξης ισχύος του ΓΚΠΔ, από την 1η Ιουλίου 2018 θα τηρείται ανωνυμία στις προδικαστικές υποθέσεις όσον αφορά τα φυσικά πρόσωπα. Η πρώτη χώρα της ΕΕ που επέβαλε πρόστιμο για παραβίαση του ΓΚΠΔ ήταν η Αυστρία. Συγκεκριμένα, η ΑΠΔΠΧ της εν λόγω χώρας, επέβαλε σε εταιρία λιανικής πώλησης πρόστιμο 4.800 ευρώ για παράνομο σύστημα βιντεοεπιτήρησης³³¹. Ακολούθως, η πορτογαλική εποπτική αρχή επέβαλε στις 17-7-2018 πρόστιμο 400.000 ευρώ σε νοσοκομείο για παραβίαση του ΓΚΠΔ και συγκεκριμένα επειδή δεν έλαβε τα κατάλληλα μέτρα υπέρ της προστασίας των προσωπικών δεδομένων των ασθενών.

Η Αρχή για την Προστασία των Δεδομένων και την Ελευθερία της Πληροφόρησης του Baden-Wuerttemberg (LfDI) υπήρξε η πρώτη γερμανική αρχή προστασίας δεδομένων που επέβαλε πρόστιμο στο πλαίσιο του Γενικού Κανονισμού για την Προστασία Δεδομένων. Συγκεκριμένα, επιβλήθηκε πρόστιμο 20.000 ευρώ σε εταιρία για παραβίαση της υποχρέωσής της να διασφαλίζει την ασφάλεια της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα, σύμφωνα με το εδ.α' της παρ.1 του άρθρου 32 του ΓΚΠΔ (ψευδωνυμοποίηση και κρυπτογράφηση δεδομένων προσωπικού χαρακτήρα)³³².

Στην Ελλάδα, με την υπ' αρ. 46/2018 Απόφαση³³³ και την ενημέρωση³³⁴ της ΑΠΔΠΧ επισημαίνεται ότι μετά τη θέση σε ισχύ του ΓΚΠΔ (25 Μαΐου 2018), δεν υφίσταται πλέον υποχρέωση γνωστοποίησης τήρησης αρχείου ή επεξεργασίας ή βιντεοεπιτήρησης στην Αρχή. Το αρχείο δραστηριοτήτων τηρείται πλέον εσωτερικά στην επιχείρηση ή στον φορέα και διατίθεται στην Αρχή σε περίπτωση που ζητηθεί.

³³⁰ Βλ. Γ. Γιαννόπουλο (2017), *όπ.ανωτ.*, σελ.206.

³³¹ Βλ. ηλεκτρονική πηγή: <https://iapp.org/news/a/austria-announces-first-gdpr-fine/>

³³² Βλ. ηλεκτρονική πηγή:

<https://www.lawspot.gr/nomika-nea/epivlithike-proti-prostimo-gia-paraviasii-toy-gdpr-sti-germania>

³³³ Βλ. ηλεκτρονική πηγή:

<http://www.dpa.gr/APDPXPortlets/htdocs/documentDisplay.jsp?docid=190,91,28,53,5,70,162,36>.

³³⁴ Βλ. ηλεκτρονική πηγή:

<http://www.dpa.gr/APDPXPortlets/htdocs/documentSDisplay.jsp?docid=28,12,241,205,38,93,67,87>.

Επίσης, παύει η χορήγηση αδειών από την Αρχή για την επεξεργασία ευαίσθητων δεδομένων και συνεπώς συνάγεται το συμπέρασμα ότι το βάρος του προληπτικού ελέγχου της λήψης μέτρων συμμόρφωσης μετατοπίζεται πλέον από τις εποπτικές αρχές στον υπεύθυνο ή στον εκτελούντα την επεξεργασία³³⁵.

Με την υπ' αρ. 66/2018 Απόφασή της η Αρχή απηύθυνε επίπληξη σε υπεύθυνο επεξεργασίας για μη νόμιμη επεξεργασία δεδομένων με σκοπό την αποστολή μηνυμάτων διαφημιστικού χαρακτήρα μέσω της εφαρμογής Viber³³⁶. Με τις υπ' αρ. 67, 68 και 69/2018 Αποφάσεις³³⁷, αντίστοιχα απηύθυνε επίπληξη σε υπεύθυνο επεξεργασίας για παραβίαση των άρθρων 32 και 5 παρ.1 εδ.στ' του ΓΚΠΔ αναφορικά με την ασφάλεια της επεξεργασίας³³⁸ και σε τράπεζες, για μη έγκαιρη γνωστοποίηση περιστατικού παραβίασης προσωπικών δεδομένων.

Η τελευταία ανακοίνωση της Αρχής στις 20-12-2018 είναι η Γ/ΕΞ/10281 που αφορά συγκεντρωτικά στοιχεία γνωστοποιήσεων περιστατικών παραβίασης δεδομένων προσωπικού χαρακτήρα κατά τους πρώτους έξι μήνες εφαρμογής του ΓΚΠΔ. Σύμφωνα με αυτήν, υποβλήθηκαν στην ΑΠΔΠΧ 66 γνωστοποιήσεις περιστατικών παραβίασης δεδομένων προσωπικού χαρακτήρα, από τις οποίες στις 36 οι υπεύθυνοι επεξεργασίας δεδομένων προχώρησαν σε ανακοίνωση του περιστατικού στα επηρεαζόμενα φυσικά πρόσωπα. Έως σήμερα, η Αρχή έχει εκδώσει τρεις αποφάσεις (τις 67, 68 και 69/2018) που σχετίζονται με τα ανωτέρω περιστατικά, ενώ τουλάχιστον άλλα 9 περιστατικά είναι υπό εξέταση και, παράλληλα, για 6 από αυτά συνεργάζεται με συναρμόδιες αρχές της ΕΕ.

Στην ανακοίνωσή της η Αρχή περιλαμβάνει συμβουλές προς υπευθύνους και εκτελούντες την επεξεργασία δεδομένων, επιστώντας τους την προσοχή στα εξής σημεία: 1) στην αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου που περιέχουν δεδομένα προσωπικού χαρακτήρα, σε λανθασμένους αποδέκτες και 2) στην εξαπάτηση χειριστών ηλεκτρονικών υπολογιστών από κακόβουλα μηνύματα που

³³⁵ Βλ. Γ. Λαζαράκο (2016), *όπ.ανωτ.*, σελ.243.

³³⁶ Η Απόφαση με αρ. 46/24-5-2018 που αναλύθηκε ανωτέρω, εξέτασε ανακύπτοντα ζητήματα εφαρμοστέου δικαίου κατά την μεταβατική περίοδο μέχρι τη δημοσίευση του εθνικού νόμου (αρμοδιότητα της Αρχής για χορήγηση αδειών σε περιπτώσεις μη επιβαλλόμενες από τον ΓΚΠΔ) και η υπ' αρ. 52/28-6-2018 αφορά ανακύπτοντα ζητήματα εφαρμοστέου δικαίου μετά την έναρξη ισχύος του ΓΚΠΔ (αρμοδιότητα της Αρχής σύμφωνα με τον ΓΚΠΔ, να επιλαμβάνεται επί ερωτημάτων και αιτήσεων υπευθύνων επεξεργασίας, των υποκειμένων των δεδομένων ή / και τρίτων σχετικά με ζητήματα επεξεργασίας προσωπικών δεδομένων).

³³⁷ Όλες οι αποφάσεις είναι διαθέσιμες στον ιστότοπο της ΑΠΔΠΧ: www.dpa.gr.

³³⁸ Η εταιρεία δεν είχε μεριμνήσει για ενημέρωση του χρησιμοποιούμενου λογισμικού και δεν διέθετε επαρκείς μηχανισμούς για την ανίχνευση επιθέσεων ασφαλείας, ούτε διαδικασίες για την τακτική αξιολόγηση των μέτρων ασφαλείας.

μπορεί να οδηγήσει σε εγκατάσταση κακόβουλου λογισμικού. Προς αντιμετώπιση των κινδύνων αυτών, η Αρχή συστήνει την υλοποίηση δράσεων ευαισθητοποίησης των χρηστών. Επίσης, σημαντικός αριθμός περιστατικών παραβίασης οφείλεται στο χρησιμοποιούμενο λογισμικό και για το λόγο αυτό οι υπεύθυνοι και οι εκτελούντες την επεξεργασία προσωπικών δεδομένων οφείλουν να καταβάλλουν κάθε δυνατό έλεγχο πριν τη χρήση του, να διαθέτουν διαδικασία αντιμετώπισης προβλημάτων, να ελέγχουν τις ρυθμίσεις των διακομιστών διαδικτύου, ώστε να μην καθίστανται προσβάσιμες μη δημόσιες πληροφορίες και να επικαιροποιούν άμεσα το λογισμικό τους με κάθε νέα έκδοση ασφάλειας. Τέλος, η ανακοίνωση αναφέρει ότι εμφανίστηκαν περιστατικά κλοπής ή απώλειας ηλεκτρονικών υπολογιστών και αποθηκευτικών μέσων και συστήνει τη χρήση λογισμικού κρυπτογράφησης.

Βάσιμα πιθανολογείται ότι η ερμηνεία που θα δώσει εν καιρώ το Ευρωπαϊκό Δικαστήριο κατά την εξέταση των νομικών ζητημάτων που θα ανακύψουν, θα συμβάλλει στην ορθή εφαρμογή του Κανονισμού.

7. Ο υπό ψήφιση Νόμος για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα σε εφαρμογή του ΓΚΠΔ και την ενσωμάτωση της Οδηγίας 2016/680/ΕΕ (ΣχΝΠΔΠΧ)

Παρά τη φύση του Κανονισμού, ο οποίος ισχύει πλήρως και ενιαία σε όλα τα κράτη-μέλη χωρίς να απαιτείται έκδοση ειδικής πράξης εφαρμογής, ο ΓΚΠΔ παρέχει στα κράτη-μέλη ευελιξία να ψηφίσουν διατάξεις για τις περιπτώσεις που προβλέπονται παρεκκλίσεις και ανάγκη εξειδίκευσης των κανόνων του³³⁹.

Ενώ λοιπόν οι διαβουλεύσεις³⁴⁰ για το νέο εθνικό νόμο³⁴¹, που θα έχει εφαρμογή στην ελληνική επικράτεια, ξεκίνησαν στις 20-2-2018, ολοκληρώθηκαν στις 5-3-2018 και η ψήφισή του αναμενόταν πριν την έναρξη ισχύος του Κανονισμού, ακόμα αναμένεται η κατάθεσή του ενώπιον της Βουλής. Ο εφαρμοστικός αυτός νόμος θεσπίζει νομοθετικά μέτρα για την εφαρμογή του ΓΚΠΔ, ενσωματώνει στην ελληνική έννομη τάξη τις διατάξεις της Οδηγίας 2016/680/ΕΕ³⁴² (όπως αναλύθηκε ανωτέρω) και αντικαθιστά πλήρως το Ν.2472/1997. Αντικείμενό του αποτελεί η θέσπιση των προϋποθέσεων για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία των δικαιωμάτων και των ελευθεριών των φυσικών προσώπων και ιδίως του δικαιώματος προστασίας προσωπικών δεδομένων. Σκοπός του είναι να συμπληρώσει τυχόν κενά του Κανονισμού, ώστε αυτός να εφαρμοστεί αποτελεσματικά στην Ελλάδα. Στο δημοσιευμένο νομοσχέδιο³⁴³ έχουν αποτυπωθεί ορισμένα άρθρα του ΓΚΠΔ και το σύνολο της Οδηγίας 2016/680/ΕΕ, ενώ οι υπόλοιπες διατάξεις έχουν ούτως ή άλλως άμεση ισχύ στην ελληνική επικράτεια. Πάντως, με μια πρώτη ματιά διακρίνεται πως δεν ακολουθεί την ίδια διάταξη και

³³⁹ Βλ. Α. Μήτρον (2017), *όπ.ανωτ.*, σελ.36.

³⁴⁰ Βλ. στατιστικά στοιχεία: 127 σχόλια επί της διαβούλευσης, 11448 ο συνολικός αριθμός των σχολίων.

³⁴¹ Ηλεκτρονική πηγή: <http://www.opengov.gr/ministryofjustice/?p=9331>, τίτλος νόμου: «Θέσπιση νομοθετικών μέτρων για την εφαρμογή του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της Οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) και ενσωμάτωση στην εθνική έννομη τάξη της Οδηγίας 2016/680/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της απόφασης-πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου και συμπληρωματικές διατάξεις».

³⁴² Η οποία έπρεπε να έχει ενσωματωθεί στην ελληνική έννομη τάξη έως τις 6-5-2018.

³⁴³ Υπουργείο Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων (2018).

δομή με τον ΓΚΠΔ, με αποτέλεσμα να παρουσιάζει προβλήματα στην κατανόηση του περιεχομένου του³⁴⁴.

Ο ΓΚΠΔ παρουσιάζει χαρακτηριστικά Οδηγίας, όπως προαναφέρθηκε, διότι παρέχει στους εθνικούς νομοθέτες τη διακριτική ευχέρεια να θεσπίσουν διατάξεις και να υιοθετήσουν κάποια από τις προτεινόμενες επιλογές³⁴⁵, προκειμένου να προσαρμόσουν τις ρυθμίσεις του στα δεδομένα της χώρας τους. Με την παροχή όμως ευρείας διακριτικής ευχέρειας στα κράτη - μέλη, ελλοχεύει ο κίνδυνος της ανομοιομορφης εφαρμογής του Κανονισμού, γι' αυτό οι εθνικοί νομοθέτες πρέπει να επιδείξουν σύνεση στις επιλογές τους³⁴⁶.

Εν προκειμένω, στα άρθρα 85 έως 91 ΓΚΠΔ προβλέπονται εξαιρέσεις, που παρέχουν στον εθνικό νομοθέτη τη δυνατότητα να ρυθμίσει δια νόμου κάποιες συγκεκριμένες περιπτώσεις και να μη δεσμεύεται απόλυτα από τον Κανονισμό, παρά μόνο από τις γενικές αρχές που τον διέπουν. Αυτές οι περιπτώσεις αφορούν την επεξεργασία σε σχέση με: α) την ελευθερία έκφρασης και πληροφόρησης, β) την πρόσβαση του κοινού στα επίσημα έγγραφα, γ) τον εθνικό αριθμό ταυτότητας, δ) την εργασιακή απασχόληση, ε) τους σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής-ιστορικής έρευνας ή στατιστικούς σκοπούς³⁴⁷, στ) την υποχρέωση τήρησης απορρήτου, και ζ) τους υφιστάμενους κανόνες προστασίας των δεδομένων εκκλησιών και θρησκευτικών ενώσεων.

Ως ευρωπαϊκός Κανονισμός, αποτελεί δεσμευτική νομοθετική πράξη και εργαλείο εναρμόνισης, αφού έχει αυτόματη και ομοιόμορφη ισχύ σε όλα τα κράτη-μέλη της ΕΕ, χωρίς να απαιτείται ενσωμάτωσή του στο εθνικό δίκαιο. Όλοι όσοι εμπίπτουν στο πεδίο εφαρμογής του, ήτοι τα κράτη-μέλη, τα όργανα αυτών, τα δικαστήρια, οι αρχές και οι πολίτες, δεσμεύονται άμεσα από το ενωσιακό δίκαιο, χωρίς να δικαιούνται να καταφεύγουν σε εθνικές ρυθμίσεις που αποκλίνουν των διατάξεων ενός Κανονισμού³⁴⁸. Ωστόσο, σύμφωνα με το ελληνικό νομοσχέδιο που κρίθηκε σκόπιμο από τον Έλληνα νομοθέτη να εκπονηθεί, είναι βέβαιο πως θα υπάρξουν εθνικές αποκλίσεις. Για παράδειγμα, ο Έλληνας νομοθέτης προβλέπει στα άρθρα 31 έως 34 μόνο τα δικαιώματα ενημέρωσης, πρόσβασης, διόρθωσης ή διαγραφής και

³⁴⁴ Βλ. Α. Λεμπέση (2018α), *όπ.ανωτ.*, σελ.525-526.

³⁴⁵ Ενδεικτικά: αιτιολογικές σκέψεις 129, 142, 150, 152, 155 Προοιμίου ΓΚΠΔ.

³⁴⁶ Βλ. Φ. Παναγοπούλου-Κουτνατζή (2017α), *όπ.ανωτ.*, σελ.19.

³⁴⁷ Βλ. Ι. Ιγγλεζάκη, Ο ΓΚΠΔ (Κανονισμός 2016/679), (2018β), *όπ.ανωτ.*, σελ. 142 επόμε.

³⁴⁸ Βλ. Α. Μήτρου (2017), *όπ.ανωτ.*, σελ.36.

περιορισμού της επεξεργασίας και όχι τα δικαιώματα της εναντίωσης και της φορητότητας.

Η σχετική νομοθεσία διαρκώς εξελίσσεται παράλληλα με τις οικονομικές, κοινωνικές και τεχνολογικές εξελίξεις και η επιτυχία της θα κριθεί εκ του αποτελέσματος.

Ο Έλληνας νομοθέτης θα πρέπει να σταθμίσει προσεκτικά την προστασία της προσωπικής ζωής σε συνάρτηση με την απελευθέρωση της κυκλοφορίας των δεδομένων εντός της Κοινότητας, χωρίς να δίνει προβάδισμα μόνο στην προστασία (όπως συνέβαινε στο Ν.2472/97), αλλά να συνυπολογίζει και τα άλλα συνταγματικώς προστατευόμενα έννομα αγαθά, όπως την ελευθερία του Τύπου³⁴⁹. Συγκεκριμένα, σύμφωνα με την αιτιολογική σκέψη 153 του Προοιμίου ΓΚΠΔ και την παράγραφο 1 του άρθρου 85, το δίκαιο των κρατών - μελών θα πρέπει να συμφιλώνει τα δικαιώματα της ελευθερίας της έκφρασης και της πληροφόρησης³⁵⁰, με το δικαίωμα προστασίας των δεδομένων προσωπικού χαρακτήρα και για το λόγο αυτό, τα κράτη - μέλη οφείλουν να θεσπίσουν νομοθετικά μέτρα που να προβλέπουν τις αναγκαίες εξαιρέσεις, ώστε να εξισορροπούν τα εν λόγω δικαιώματα.

Ένα ακόμα χαρακτηριστικό παράδειγμα όπου παρέχεται στον εθνικό νομοθέτη η δυνατότητα απόκλισης, αποτελεί η ρύθμιση που αφορά τα ευαίσθητα προσωπικά δεδομένα: τα κράτη - μέλη μπορούν να θεσπίσουν αυστηρότερες διατάξεις για την προστασία τους. Στην παράγραφο 5 του άρθρου 36 ΓΚΠΔ, δίνεται διακριτική ευχέρεια στο κράτος - μέλος να απαιτήσει διαβούλευση και προηγούμενη άδεια από την εποπτική αρχή, σε σχέση με την επεξεργασία που αφορά την εκτέλεση καθήκοντος προς το δημόσιο συμφέρον. Εθνικές αποκλίσεις επίσης επιτρέπονται στις διατάξεις για την επεξεργασία δεδομένων στις εργασιακές σχέσεις, στον καθορισμό της ηλικίας ανηλικού ως προς τη συγκατάθεσή του σχετικά με την προσφορά υπηρεσιών της κοινωνίας των πληροφοριών (άρθρο 8 ΓΚΠΔ), στη δυνατότητα περιορισμού δικαιωμάτων για την κατοχύρωση της δημόσιας ασφάλειας και τη διασφάλιση δημοσίου συμφέροντος (αιτιολογική σκέψη 73 Προοιμίου ΓΚΠΔ) κ.ά.³⁵¹. Ενόψει της ψήφισης του νόμου, παρουσιάζει μεγάλο ενδιαφέρον το περιεχόμενο του τελικού κειμένου, ώστε να αξιολογηθεί στην οριστική του μορφή.

³⁴⁹ Περίπτωση λίστας Λαγκάρντ που θέτει ερωτηματικά για το τι υπερισχύει μεταξύ της προστασίας των προσωπικών δεδομένων και της ελευθερίας της πληροφόρησης (βλ. Φ. Παναγοπούλου-Κουτνατζή «Η λίστα Λαγκάρντ και τα όρια της ελευθερίας του τύπου», *ΕφημΔΔ* 2012, σ.744 επ.)

³⁵⁰ Στην πληροφόρηση περιλαμβάνονται η δημοσιογραφική, η πανεπιστημιακή, η καλλιτεχνική και η λογοτεχνική.

³⁵¹ Βλ. Δ. Λεμπέση (2018α), *όπ.ανωτ.*, σελ.501.

8. Προτάσεις για την ορθή εφαρμογή του ΓΚΠΔ στη Δημόσια Διοίκηση

Μία πολύ σημαντική ενέργεια που πρέπει να λαμβάνει χώρα, είναι ο έλεγχος τήρησης των αρχών νόμιμης επεξεργασίας, ο οποίος πρέπει να είναι διαρκής (εφαρμογή της θεωρίας του κύκλου του Deming). Επίσης, κρίνεται αναγκαία η ουσιαστική ενημέρωση των πολιτών για τα νέα και επαυξημένα δικαιώματά τους ως προς την προστασία των προσωπικών τους δεδομένων και η τήρηση των νόμιμων προθεσμιών ικανοποίησης των δικαιωμάτων, επεξεργασίας και αποθήκευσης. Η τήρηση σαφών προθεσμιών απάντησης επί των αιτημάτων, τα οποία θα μπορούν να υποβάλλονται και ηλεκτρονικά προς διευκόλυνση του κοινού, είναι επίσης πολύ σημαντική. Πρόσφορο είναι να αναθεωρηθούν, ως προς το περιεχόμενό τους, τα έντυπα συλλογής δεδομένων των πολιτών και να δημιουργηθούν πρότυπα έγγραφα είτε ικανοποίησης των αιτημάτων τους, είτε απόρριψης με ειδική αιτιολόγηση. Υπό το φως αυτών των σκέψεων λοιπόν, οδηγούμαστε στο συμπέρασμα ότι η καταγραφή, η συμμόρφωση και η ενημέρωση των πολιτών πρέπει να αντιμετωπιστούν ενιαία από τον φορέα.

Ταυτόχρονα, θεωρείται επιβεβλημένη η εκπαίδευση των υπαλλήλων των δημόσιων φορέων, ώστε να είναι σε θέση να κατανοήσουν τις αλλαγές, να ανταπεξέρχονται στα αιτήματα των πολιτών και να μπορούν να χειριστούν δύσκολες περιπτώσεις, αν παραστεί ανάγκη. Δεν αρκεί η απλή κοινοποίηση του κειμένου του ΓΚΠΔ στο προσωπικό του φορέα και ο ορισμός ΥΠΑ προκειμένου να είναι «σύννομες» οι υπηρεσίες με τις επιταγές του Κανονισμού. Θα πρέπει να δημοσιοποιούνται τα στοιχεία του ΥΠΑ και να διευκολύνεται η επικοινωνία μαζί του. Επίσης το Δημόσιο οφείλει να ερευνήσει τα κενά που τυχόν υπάρχουν όσον αφορά π.χ. τον εξοπλισμό, την κατάρτιση, την επικοινωνία των ενδιαφερόμενων μερών και να εγκαταστήσει τις κατάλληλες υποδομές ανάλογα με το είδος παρεχόμενης υπηρεσίας (εξειδικευμένες ρυθμίσεις για τομείς που αφορούν τη δημόσια υγεία, τις ποινικές καταδίκες ή την επεξεργασία ευαίσθητων δεδομένων³⁵²).

Μία ορθή κίνηση στην οποία μπορεί να προβεί η ΔΔ είναι η εκτίμηση αντικτύπου (DPIA), η οποία παρουσιάστηκε παραπάνω και αποτελεί πρακτική που δύναται να αποκαλύψει προβληματικά σημεία του φορέα ως προς την τήρηση της νομοθεσίας. Όπως λοιπόν προαναφέρθηκε, οι περιπτώσεις όπου ο δημόσιος φορέας υποχρεούται

³⁵² Η ανάγκη προσαρμογής στον ΓΚΠΔ είναι μεγαλύτερη για τις δημόσιες αρχές που επεξεργάζονται ευαίσθητα προσωπικά δεδομένα σε μεγάλη κλίμακα, όπως για παράδειγμα τα δημόσια νοσοκομεία.

να προβεί σε DPIA³⁵³, είναι οι πράξεις επεξεργασίας μεγάλης κλίμακας και σημαντικής ποσότητας δεδομένων, σε περιφερειακό, εθνικό ή υπερεθνικό επίπεδο, οι οποίες ενδέχεται να επιφέρουν υψηλό κίνδυνο σε μεγάλο αριθμό υποκειμένων. Η DPIA αποτελεί μια αποτελεσματική πρακτική που μπορεί να ακολουθήσει ο δημόσιος τομέας, ανεξαρτήτου υποχρεωτικότητας, προκειμένου να εξασφαλιστεί η σύννομη επεξεργασία και να αποκαλυφθούν τυχόν κενά στις τηρούμενες διαδικασίες επεξεργασίας. Πρέπει να εφαρμόζεται προγενέστερη εκτίμηση αντικτύπου, όταν μια δημόσια αρχή σκοπεύει να εγκαθιδρύσει μια κοινή εφαρμογή ή πλατφόρμα επεξεργασίας, ή όταν πρόκειται να ψηφιστεί νέα διάταξη που αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα (προτείνεται να συμπεριλαμβάνεται στην αιτιολογική έκθεση του νομοθετήματος ξεχωριστή έκθεση επιπτώσεων της συγκεκριμένης διάταξης). Με άλλα λόγια, κρίνεται σκόπιμη η διενέργεια DPIA σε κάθε δημόσιο έργο και σε κάθε νέα επεξεργασία και μάλιστα η εκτίμηση πρέπει να αποτελεί μέρος της αρχικής μελέτης. Χρήσιμη και αναγκαία για τον μετριασμό των κινδύνων είναι η διαβούλευση με την εποπτική αρχή, όταν υπάρχει αμφιβολία και προκύπτει υψηλός κίνδυνος για τα δικαιώματα, ή πριν την έκδοση νομοθετικών ή κανονιστικών μέτρων επεξεργασίας. Καθόσον λοιπόν η διενέργεια εκτίμησης αντικτύπου στο δημόσιο κρίνεται μεγάλης σημασίας, θα πρέπει οι Οργανισμοί να ενεργοποιηθούν και να ορίσουν τους εμπλεκόμενους στη διαδικασία εφαρμογής και αξιολόγησης των αποτελεσμάτων της εκτίμησης, ώστε να αποκομίσουν και τα αντίστοιχα οφέλη.

Ως εναλλακτικές λύσεις υπέρ του περιορισμού περαιτέρω επεξεργασίας και διάδοσης των προσωπικών δεδομένων, προτείνονται η ενημέρωση των προσώπων για την επεξεργασία των δεδομένων τους από τους υπευθύνους επεξεργασίας με σαφήνεια και διαφάνεια, η ευαισθητοποίηση των πολιτών σχετικά με τους κινδύνους της επεξεργασίας, η ελαχιστοποίηση των δεδομένων, η άσκηση των παρεχόμενων από τον Κανονισμό δικαιωμάτων της πρόσβασης και της διόρθωσης, η ανωνυμοποίηση ή η κρυπτογράφηση των δεδομένων και η τήρηση αποτελεσματικών κυρώσεων σε περιπτώσεις παραβίασης της προστασίας των δεδομένων. Οι λύσεις αυτές προφανώς θα βελτιώσουν την επιδιωκόμενη προστασία των προσωπικών δεδομένων έναντι του κανόνα της δημοσιοποίησης και αναδημοσίευσης πλήθους προσωπικών δεδομένων στο διαδίκτυο και της αλόγιστης επεξεργασίας τους από δημόσιους φορείς. Βαρύτητα

³⁵³ Βλ. άρθ. 35 ΓΚΠΔ.

επίσης πρέπει να δοθεί στην ενίσχυση της αποτελεσματικότητας του δικαιώματος διαγραφής των δημοσιοποιημένων δεδομένων, όταν το άτομο αντιτάσσεται στην επεξεργασία, προκειμένου να μην έρχεται αντιμέτωπο με το παρελθόν του³⁵⁴.

Μια ορθή βάση για την αποτελεσματική λειτουργία του νέου θεσμού είναι η εξειδίκευση και ερμηνεία ορισμένων διατάξεων που παρουσιάζουν αμφιβολία ή αοριστία, ώστε να εξασφαλιστεί η ορθή εφαρμογή τους σύμφωνα με το πνεύμα του νόμου. Οι κατευθυντήριες γραμμές της Ομάδας Εργασίας του άρθρου 29 μπορούν να φανούν ιδιαίτερα χρήσιμες προς αυτό τον σκοπό.

Έργο των νομικών και των οικονομολόγων σε βάθος χρόνου, αποτελεί η διαπίστωση εάν ο Κανονισμός προστάτευσε αποτελεσματικά τα δεδομένα προσωπικού χαρακτήρα των φυσικών προσώπων και εάν όντως εξυπηρέτησε τη λειτουργία της κοινής εσωτερικής αγοράς, καθώς αμφότερα αποτελούν πρωταρχικούς στόχους του νομοθετήματος. Κατά δε το άρθρο 97 ΓΚΠΔ, έως τις 25-5-2020 και στη συνέχεια ανά τέσσερα έτη, η Επιτροπή θα υποβάλλει Εκθέσεις αξιολόγησης και αναθεώρησης του Κανονισμού στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο.

³⁵⁴ Βλ. *I. Γγγλεζάκη (2014), όπ.ανωτ., σελ.211 επόμ.*

9. Συμπεράσματα - Προβληματισμοί

Η εξέλιξη του εθνικού θεσμικού πλαισίου αλλά κυρίως του ενωσιακού με την πάροδο των ετών, καταδεικνύει την τάση για ενίσχυση της προστασίας των προσωπικών δεδομένων μέσω της αυστηροποίησης των κυρώσεων και της διεύρυνσης των δικαιωμάτων των υποκειμένων³⁵⁵.

Είναι σαφές πως η δημιουργία του νέου ενωσιακού νομοθετήματος που ψηφίστηκε στις 27/4/2016 και τέθηκε σε εφαρμογή στις 25/5/2018, αποτελεί ένα σημαντικό βήμα προς την διασφάλιση των θεμελιωδών δικαιωμάτων των ατόμων. Η διετής μεταβατική περίοδος που μεσολάβησε μεταξύ της ψήφισης και της εφαρμογής του Κανονισμού, ήταν επαρκής ώστε να προετοιμαστούν όλοι οι ενδιαφερόμενοι για την εφαρμογή των νέων ρυθμίσεων. Η τεχνολογία αποτελεί την κυριότερη πηγή του προβλήματος που καλείται να αντιμετωπίσει ο ΓΚΠΔ, αλλά ταυτόχρονα αποτελεί και το κύριο μέσον επίλυσής του. Η σωστή αξιοποίηση της σύγχρονης τεχνολογίας θα συμβάλλει σε μεγάλο βαθμό κατά της παγκόσμιας απειλής ενάντια στην ιδιωτικότητα του ατόμου και την εμπορευματοποίηση των προσωπικών του δεδομένων (κοινωνικά δίκτυα κλπ). Ο νέος Κανονισμός που αντικατέστησε την Οδηγία 95/46/EK, δείχνει αγαθές προθέσεις ως προς τη διασφάλιση της δημοκρατίας, δεν αποτελεί όμως πανάκεια από μόνος του, ούτε επιφέρει ριζικές αλλαγές στην προστασία των προσωπικών δεδομένων. Δεν προτείνει επαναστατικές μεθόδους αντιμετώπισης των κινδύνων, αντίθετα ασπάζεται τις βασικές αρχές προστασίας, οι οποίες μάλιστα ενισχύθηκαν από τη νομολογία και παράλληλα εισάγει τους προαναφερόμενους νεωτερισμούς, προς ενίσχυση του ελέγχου του σεβασμού των κανόνων προστασίας³⁵⁶. Σε ορισμένες περιπτώσεις προβλέπει μεν αρκετά αυστηρές κυρώσεις, η απειλή όμως μιας ποινής δεν αποτελεί λόγο επιτυχίας και εφαρμογής ενός νομοθετήματος. Η επιτυχία του θα κριθεί σε βάθος χρόνου και θα εξαρτηθεί, μεταξύ άλλων, από το βαθμό που ο καθένας μας συνειδητοποιήσει το μέγεθος της απειλής και συμβαδίσει με το σκεπτικό του νέου νομοθετήματος, ώστε αυτό να μην καταστεί άλλη μια γραφειοκρατική αγκύλωση³⁵⁷. Το νέο νομοθετικό πλαίσιο απαιτεί προσαρμογές από όλους τους εμπλεκόμενους φορείς, είτε πρόκειται για εθνικές διοικήσεις ή αρχές προστασίας δεδομένων, είτε για τους υπευθύνους επεξεργασίας,

³⁵⁵ Βλ. Α. Κοτσαλή/Κ. Μενουδάκο (2018), *όπ.ανωτ.*

³⁵⁶ Βλ. Α. Κοτσαλή/Κ. Μενουδάκο (2018), *όπ.ανωτ.*

³⁵⁷ Βλ. Ε. Πλατή (2018), *όπ.ανωτ.*, σελ.4.

είτε, τέλος, για τα ίδια τα υποκείμενα των υπό επεξεργασία δεδομένων. Τις προσεχείς δεκαετίες θα κριθεί εάν ο ΓΚΠΔ εισήγαγε την τέταρτη γενιά νομοθετημάτων για την προστασία των προσωπικών δεδομένων και εάν αντιμετώπισε με επιτυχία τις προκλήσεις της σύγχρονης εποχής, διασφαλίζοντας επιτυχώς το δικαίωμα της ιδιωτικότητας, το οποίο αποτελεί και το βασικότερο ζητούμενο³⁵⁸.

Επιφυλάξεις επίσης δημιουργεί η επιθυμία για ενιαία και εναρμονισμένη ρύθμιση στην ΕΕ, δεδομένων των υφιστάμενων εθνικών αποκλίσεων και της ήδη αποτυχημένης απόπειρας δημιουργίας ευρωπαϊκού αστικού κώδικα³⁵⁹.

Στις αρνητικές κριτικές του ΓΚΠΔ ανήκει η διαπίστωση ότι αυτός δεν κατάφερε να λύσει το πρόβλημα της σύγκρουσης των διατάξεων που προστατεύουν την ιδιωτικότητα, με αυτές που επιτρέπουν επεμβάσεις σε αυτήν. Δεδομένου ότι δεν ιεραρχούνται μεταξύ τους τα προστατευόμενα δικαιώματα, θα συνεχίσει να υφίσταται το πρόβλημα πρόκρισης, ή μη, της προστασίας των προσωπικών δεδομένων έναντι άλλων συνταγματικά κατοχυρωμένων δικαιωμάτων. Σημαντικό είναι να τονιστεί ότι το δικαίωμα στην προστασία των προσωπικών δεδομένων δεν αποτελεί ένα απόλυτο – «τυραννικό» δικαίωμα και γι' αυτό θα πρέπει ο Έλληνας νομοθέτης του υπό διαμόρφωση νόμου περί προστασίας προσωπικών δεδομένων, να εξισορροπήσει τα συγκρουόμενα συνταγματικά αγαθά επί τη βάση της αρχής της αναλογικότητας³⁶⁰.

Στα αρνητικά επίσης χαρακτηριστικά του ΓΚΠΔ, σύμφωνα με την Αλεξανδροπούλου (2016), ανήκει η μεγάλη του έκταση και ο μεγάλος αριθμός εξουσιοδοτήσεων προς την Επιτροπή ή τα κράτη-μέλη για λεπτομερέστερη ρύθμιση ποικίλων θεμάτων. Αρκετές επιφυλάξεις εκφράστηκαν για την ενίσχυση της κανονιστικής εξουσίας της Επιτροπής, καθόσον αυτή δύναται να επεμβαίνει ακόμη και σε μεμονωμένα περιστατικά, με αποτέλεσμα να καταστρατηγείται ο ρόλος των εθνικών ανεξάρτητων αρχών³⁶¹.

Ο δημόσιος τομέας όφειλε να δράσει προληπτικά, ώστε κατά την ημερομηνία που τέθηκε σε ισχύ ο ΓΚΠΔ, ήτοι την 25/5/2018 και μετά δύο χρόνια από την ψήφισή του, να έχει συμμορφωθεί με τις απαιτήσεις που ο νέος Κανονισμός επιβάλλει. Το πρώτο βήμα στο οποίο θα έπρεπε να έχει προβεί, είναι η προετοιμασία που θα περιλάμβανε χρονοδιαγράμματα και οργανογράμματα, προκειμένου να

³⁵⁸ Βλ. Ε. Πλατή (2018), *όπ.ανωτ.*, εισαγωγή.

³⁵⁹ Βλ. Δ. Λεμπέση (2018β), *όπ. ανωτ.*, σελ.604.

³⁶⁰ Βλ. Φ. Παναγοπούλου – Κουτνατζή, *Τα νέα δικαιώματα για τους πολίτες βάσει του ΓΚΠΔ: μια πρώτη αποτίμηση και συνταγματική αξιολόγηση* (2017β), σελ.82-83.

³⁶¹ Βλ. Α. Μήτρου (2017), *όπ.ανωτ.*, σελ.35.

αναθεωρηθούν οι υφιστάμενες πολιτικές προστασίας προσωπικών δεδομένων. Η τήρηση των υποχρεώσεων της Διοίκησης όπως αναλύθηκαν παραπάνω και ο ανασχεδιασμός των εσωτερικών διαδικασιών της (reengineering) αποτελούν σκόπιμη και απολύτως αναγκαία αυτοδέσμευση, σε συνδυασμό με την εξασφάλιση ετοιμότητας άμεσης αντίδρασης, κατά τα νόμιμα, στις περιπτώσεις παραβιάσεων³⁶². Η ασφαλής επεξεργασία των προσωπικών δεδομένων με τα κατάλληλα τεχνικά και οργανωτικά μέτρα παραμένει ζητούμενο στη ΔΔ. Πέραν λοιπόν των καθιερωμένων μέτρων ασφαλείας, η ΔΔ οφείλει να είναι σε θέση να ανιχνεύσει και να αξιολογήσει ένα περιστατικό, αναπτύσσοντας ειδική πολιτική χειρισμού περιστατικών παραβίασης.

Από την ανάλυση που προηγήθηκε, καταδείχθηκε ότι τα απαιτούμενα από τον Κανονισμό μέτρα αποτελούν μια απαιτητική εργασία εκ μέρους των στελεχών που θα ευθύνονται για τη σύννομη λειτουργία του Οργανισμού. Προς την κατεύθυνση αυτή, σημαντική βοήθεια προσφέρουν τα πρότυπα πιστοποίησης και τυποποίησης διαδικασιών, όπως το ISO 27001 (διεθνές πρότυπο για την ασφάλεια των πληροφοριών) ή το ISO 27018 (πρότυπο για την προστασία προσωπικών δεδομένων στο υπολογιστικό νέφος)³⁶³.

Αναγκαίο επίσης βήμα για τη ΔΔ αποτελεί η διαβάθμιση της πρόσβασης στα δεδομένα από τις διάφορες βαθμίδες στελεχών και υπαλλήλων δημοσίων υπηρεσιών. Έτσι θα περιοριστεί η «εσωτερική απειλή»³⁶⁴ από τους εργαζομένους, οι οποίοι έχουν πρόσβαση σε όλα τα δεδομένα ανεξαιρέτως, γεγονός που μπορεί να οδηγήσει σε κακή χρήση των προνομίων και σε πράξη παραβίασης.

Ένα από τα προβλήματα που δε φαίνεται να έχει βρει λύση με τον Κανονισμό, είναι η σύγκρουση μεταξύ της προστασίας των προσωπικών δεδομένων και της πρόσβασης στα δημόσια έγγραφα³⁶⁵. Κατά την Οδηγία 2016/680/ΕΕ «Σύμφωνα με τον Κανονισμό (ΕΕ) αριθ. 2016/679, τα δεδομένα προσωπικού χαρακτήρα που περιέχονται σε επίσημα έγγραφα που τηρούνται από δημόσια αρχή ή από δημόσιο ή ιδιωτικό φορέα για την εκτέλεση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον, μπορούν να γνωστοποιούνται από την εν λόγω αρχή ή φορέα σύμφωνα με το κρατικό δίκαιο στο οποίο υπάγεται η δημόσια αρχή ή ο οργανισμός, προκειμένου

³⁶² Βλ. *Ε. Σιουγλέ (2018), όπ.ανωτ., σελ.105.*

³⁶³ Βλ. *Α. Βαρβέρη (2017), όπ. ανωτ., σελ. 214.*

³⁶⁴ Βλ. *εισήγηση Α. Μήτρου, Η προστασία δεδομένων των εργαζομένων σε: Α.Κοτσαλή (επιμ.), όπ. ανωτ. (2016), σελ.197.*

³⁶⁵ Βλ. *αιτιολογική σκέψη 154 Προοιμίου ΓΚΠΔ και εισήγηση Σ. Βλαχόπουλου, Πρόσβαση στα δημόσια έγγραφα σε: Α. Κοτσαλή/Κ. Μενουδάκο (επιμ.), όπ.ανωτ. (2018), σελ.39 επόμε.*

να συμβιβάσει την πρόσβαση του κοινού στα επίσημα έγγραφα με το δικαίωμα προστασίας των δεδομένων προσωπικού χαρακτήρα».

Φυσικά οι επερχόμενες αλλαγές θα επιφέρουν και σημαντικό κόστος στο δημόσιο, το οποίο θα πρέπει να υπολογιστεί και να βρεθούν οι αναγκαίοι πόροι: η προσαρμογή των μηχανογραφικών συστημάτων στο επίπεδο προδιαγραφών ασφαλείας του ΓΚΠΔ είναι ιδιαίτερα απαιτητική και απαιτεί μεγάλο χρονικό διάστημα, ενώ η δυστοκία προγραμματισμού στον δημόσιο τομέα αποτελεί κοινό τόπο. Για μια αποτελεσματική διαχείριση αλλαγής (Effective Change Management), θα πρέπει να εξασφαλιστεί η υποκίνηση αλλαγής, η δημιουργία οράματος, η ανάπτυξη πολιτικής υποστήριξης, η διαχείριση της μεταβατικής περιόδου και η διατήρηση της αλλαγής³⁶⁶. Οι επιχειρήσεις αποτυγχάνουν στην προσπάθειά τους να υλοποιήσουν έργα ανασχεδιασμού διαδικασιών, λόγω της κακής διαχείρισης της αλλαγής και της αντίστασης σε αυτήν. Οι Οργανισμοί πρέπει να συνειδητοποιήσουν τους λόγους που επιτάσσουν την ενσωμάτωση των αλλαγών που επιβάλλει ο ΓΚΠΔ, να προσδιορίσουν την παρούσα και την επιθυμητή μελλοντική κατάσταση και να πετύχουν την επιθυμητή μετάβαση. Η υιοθέτηση της πρακτικής Plan-Do-Check-Act στην προστασία των προσωπικών δεδομένων, σε συνδυασμό με την αναθεώρηση των διαδικασιών, θα εξασφαλίσει τη σταδιακή και ολοκληρωτική συμμόρφωση του φορέα³⁶⁷.

Ένας από τους πιο έντονους προβληματισμούς της σύγχρονης εποχής, αποτελεί το φαινόμενο του υποβιβασμού των χρηστών του διαδικτύου, εν αγνοία τους, από υποκείμενα των δεδομένων σε αντικείμενα επιτήρησης³⁶⁸. Αυτό συμβαίνει διότι συλλέγονται ή υποκλέπτονται προσωπικά στοιχεία των χρηστών, με τα οποία δημιουργούνται αρχεία από όπου μπορεί να αντληθούν πληροφορίες για τα ενδιαφέροντα και τις συνήθειες του ατόμου. Έτσι δημιουργείται ένα «ψηφιακό μωσαϊκό του ανθρώπινου προσώπου³⁶⁹», το οποίο καθίσταται ελέγξιμο και εμπορευματοποιήσιμο, καθώς θεμελιώδη δικαιώματα όπως η ιδιωτικότητα ή το απόρρητο των επικοινωνιών καταστρατηγούνται επανειλημμένως. Ένα στοίχημα που θα πρέπει να κερδίσει ο ΓΚΠΔ είναι η αντιμετώπιση του παραπάνω φαινομένου για

³⁶⁶ Βλ. εισήγηση Φ. Βούζα, *Εισαγωγή Καινοτομιών και Αλλαγών στη ΔΔ (2018)*, Παν/μιο Μακεδονίας, τμήμα ΟΔΕ, σελ.10.

³⁶⁷ Βλ. Ε. Σιουγλέ (2018), *όπ.ανωτ.*, σελ.106.

³⁶⁸ Βλ. Κ. Αρκουλή (2010), *όπ.ανωτ.*, σελ.15.

³⁶⁹ Βλ. Γ. Καμίνης, *Βήμα Ιδεών*, τεύχος 10, Φεβρουάριος 2008, διαθέσιμο στο: <http://www.dpa.gr/APDPXPortlets/htdocs/documentSDisplay.jsp?docid=17,165,243,28,112,14,12,168>.

την προστασία των χρηστών που δεν διαθέτουν τις απαιτούμενες τεχνικές γνώσεις για να αυτοπροστατευτούν.

Παρόλαυτά³⁷⁰, στον δημόσιο τομέα παρατηρούνται και αξιέπαινες προσπάθειες για εκσυγχρονισμό και δημιουργία υποδομών που διασφαλίζουν την εφαρμογή του ΓΚΠΔ. Η ΔΔ βρίσκεται σε κομβικό σημείο αλλαγής της κουλτούρας όσον αφορά την προστασία της ιδιωτικότητας, έχει όμως να διανύσει πολύ δρόμο ακόμα κι αυτό θα πρέπει να πραγματοποιηθεί μέσω της διαρκούς επιμόρφωσης των στελεχών της, δεδομένου ότι η ενημέρωση δεν μπορεί να περιληφθεί ουσιαστικά στο κείμενο μιας απλής Εγκυκλίου. Δυστυχώς δεν έχει ακόμα επιτευχθεί η επιθυμητή διαμόρφωση συνείδησης προστασίας προσωπικών δεδομένων (awareness) στο δημόσιο.

³⁷⁰ Βλ. *Μ. Μυλώση (2018), όπ.ανωτ.*

10. Επίλογος

Η συζήτηση για την προστασία των δεδομένων προσωπικού χαρακτήρα απασχολεί έντονα τον δυτικό κόσμο εδώ και δεκαετίες κι ένας νέος κλάδος δικαίου έχει γεννηθεί, με αποστολή του την προστασία των δεδομένων από επεξεργασίες που παραβιάζουν την πληροφοριακή αυτοδιάθεση του ατόμου.

Στις 25 Μαΐου 2018 τέθηκε σε εφαρμογή το νέο ενωσιακό νομοθέτημα που αντικατέστησε την Οδηγία 95/46/EK και συνέβαλε στην εξέλιξη της νομικής προστασίας των προσωπικών δεδομένων, χωρίς ωστόσο να εισάγει ιδιαίτερες καινοτομίες στον τομέα αυτό. Το νομοθέτημα βασίζεται σε αρχές γνωστές από την καταργούμενη Οδηγία, τις οποίες αναπτύσσει, λαμβάνοντας υπόψη του την πλούσια νομολογία που μεσολάβησε στο μεσοδιάστημα των είκοσι ετών. Ορισμένοι μάλιστα ορισμοί έχουν ληφθεί αυτούσιοι από την Οδηγία, ενώ άλλοι τροποποιούνται ή συμπληρώνονται με νέα στοιχεία. Μπορεί το έτος 2018 να ήταν η χρονιά που η πλειοψηφία των φυσικών και νομικών προσώπων ήρθε για πρώτη φορά σε επαφή με τον όρο GDPR, αδιαμφισβήτητα όμως το 2019 θα είναι ένα έτος ορόσημο στην ατζέντα των δημόσιων και ιδιωτικών επιχειρήσεων που θα κληθούν να εφαρμόσουν τις νέες διατάξεις και να επιβεβαιωθούν, ή όχι, οι προσδοκίες των συντακτών του Κανονισμού.

Το γενικό συμπέρασμα που εξάγεται είναι ότι ο Γενικός Κανονισμός διευρύνει τα δικαιώματα των υποκειμένων των προσωπικών δεδομένων και ταυτόχρονα αυξάνει τις υποχρεώσεις των υπευθύνων επεξεργασίας των δεδομένων, τις οποίες εν μέρει επεκτείνει και στους εκτελούντες την επεξεργασία. Επίσης, προβλέπει νέες διαδικασίες με σκοπό την αποτελεσματικότερη εφαρμογή των κανόνων προστασίας, ενώ ταυτόχρονα προωθεί την εγρήγορση των ενδιαφερομένων μερών, όσον αφορά τα δικαιώματα και τις υποχρεώσεις τους. Το παράδοξο που παρατηρείται είναι ότι στην πλειοψηφία τους οι πολίτες χρησιμοποιούν τα προσωπικά τους δεδομένα ως συναλλακτικά αγαθά και τα κοινοποιούν με προθυμία, προκειμένου να πετύχουν ως αντάλλαγμα ένα δώρο ή μία έκπτωση στο προϊόν που τους ενδιαφέρει, ενώ ταυτόχρονα οι ίδιοι επιθυμούν αυστηρή εφαρμογή συστημάτων προστασίας της

ιδιωτικότητάς τους³⁷¹. Απώτερος στόχος του ΓΚΠΔ είναι η διαμόρφωση ενός ισχυρότερου και συνεκτικότερου νομικού προστατευτικού πλαισίου, που θα έχει ομοιόμορφη εφαρμογή σε όλη την ΕΕ³⁷². Αρωγοί στην προσπάθεια ερμηνείας και επωφελούς χρήσης του ΓΚΠΔ, ο οποίος αποτελεί δύσκολο και απαιτητικό νομικό κείμενο, είναι τα εθνικά Δικαστήρια και το ΔΕΕ³⁷³.

Η προστασία της ιδιωτικότητας στον αιώνα της «αβάσταχτης μνήμης» αποτελεί αδιαμφισβήτητα ένα μεγάλο «στοίχημα», σύμφωνα όμως με τον καθηγητή Μιχάλη Σταθόπουλο δεν μπορούν να θυσιάζονται τα πάντα στο βωμό των προσωπικών δεδομένων. Ζητούμενο αποτελεί η ανεύρεση της χρυσής τομής μεταξύ της προστασίας της ιδιωτικότητας του πολίτη και της εξασφάλισης της αποτελεσματικής κρατικής δράσης, σε συνδυασμό με την ελευθερία δράσης των υπόλοιπων πολιτών³⁷⁴.

Με τη συνδρομή της σύγχρονης πληροφορικής τεχνολογίας, παρέχεται η δυνατότητα άντλησης και καταχώρησης στοιχείων που αφορούν την προσωπική κατάσταση ενός συγκεκριμένου, προσδιορίσιμου φυσικού προσώπου³⁷⁵. Επιπλέον, με τη χρήση των πληροφοριακών συστημάτων, αυτές οι προσωπικές πληροφορίες μπορούν να συσχετισθούν και να συμπληρωθούν, σχηματίζοντας ένα πλήρες πορτραίτο (προφίλ) της προσωπικότητας, βάσει του οποίου ελέγχεται η συμπεριφορά του προσώπου. Έτσι το άτομο δύναται να μετατραπεί σε «αντικαταστατό μέγεθος και σε πληροφοριακό αντικείμενο» και να συμμετάσχει ακούσια σε ένα παιχνίδι αλλότριων συμφερόντων, όπου η ζωή του θα αποτελεί αντικείμενο παρακολούθησης όπως ο Μεγάλος Αδερφός του Όργουελ³⁷⁶. Από την άλλη πλευρά όμως δεν έχει αποδειχθεί ότι όλες οι καινοτόμες τεχνολογικές υπηρεσίες συλλογής και επεξεργασίας πληροφοριών στοχεύουν στην καταστρατήγηση της ιδιωτικότητας. Υπό το φως αυτών των σκέψεων οδηγούμαστε στο συμπέρασμα ότι θα πρέπει να επικεντρωθούμε στις κακόβουλες τεχνολογικές καινοτομίες, που αποσκοπούν στην κατάχρηση των προσωπικών δεδομένων και να τις εξαλείψουμε, ενώ ταυτόχρονα να εκμεταλλευτούμε τις υπόλοιπες προς όφελός μας, προκειμένου να αναπτυχθούν νέοι

³⁷¹ Βλ. εισήγηση Σ. Τάσση, *Τεχνολογία και Ιδιωτικότητα*, σε: Α.Κοτσαλή (επιμ.), *όπ.ανωτ.* (2016), σελ.336 επόμενα.

³⁷² Βλ.συνέντευξη Κ. Μενουδάκου στις 22-5-2018, *όπ.ανωτ.*

³⁷³ Βλ. εισήγηση Φ. Μίτλεττον, *Ο μηχανισμός συνεργασίας και συνεκτικότητας (One Stop Shop)*, σε: Α. Κοτσαλή-Κ. Μενουδάκο (επιμ.), *όπ.ανωτ.* (2018), σελ.297.

³⁷⁴ Βλ. εισήγηση Δ. Λιάπη, *Το δίκαιο των προσωπικών δεδομένων - Κατακτήσεις, αμφισβητήσεις, προκλήσεις και προοπτικές*, σε: Α.Κοτσαλή (επιμ.), *όπ.ανωτ.* (2016), σελ.464-465.

³⁷⁵ Βλ. Α. Γέροντα (2002), *όπ.ανωτ.*, σελ 71.

³⁷⁶ Στο μυθιστόρημα του Τζ. Όργουελ «1984» χαρακτηριστική είναι η αναφορά στον Μεγάλο Αδερφό (τον ανύπαρκτο πολιτικό ηγέτη της χώρας) που υποδηλώνει καθεστώς παρακολούθησης (Βικιπαίδεια).

τρόποι προστασίας των δεδομένων³⁷⁷ και να ανακαλύψουμε τον «Θαυμαστό Καινούριο Κόσμο»³⁷⁸ του ΓΚΠΔ. Η αναγκαστική αλλαγή των συστημάτων προστασίας θα επιφέρει την αναπόφευκτη αλλαγή νοοτροπίας κατά τα οριζόμενα στον ΓΚΠΔ. Άλλωστε, σύμφωνα με τα λόγια που αποδίδονται στον διάσημο επιστήμονα Charles Darwin: «Δεν είναι το ισχυρότερο από τα είδη που επιβιώνει, ούτε το εξυπνότερο. Είναι αυτό προσαρμόζεται καλύτερα στην αλλαγή».

³⁷⁷ Βλ. εισήγηση Σ. Τάσση, *Τεχνολογία και ιδιωτικότητα*, σε: Α. Κοτσαλή (επιμ.), *όπ.ανωτ.* (2016), σελ.351.

³⁷⁸ Βιβλίο του Aldus Huxley, βλ. και Γ. Δελλή (2018), *όπ. ανωτ.*

ΒΙΒΛΙΟΓΡΑΦΙΑ – ΑΡΘΡΟΓΡΑΦΙΑ

Αιτιολογική Έκθεση στο σχέδιο νόμου «Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα». Αθήνα, 17 Ιουνίου 1996.

Αλεξανδροπούλου – Αιγυπτιάδου, Ε. (2016), *Προσωπικά Δεδομένα*. Αθήνα: Νομική Βιβλιοθήκη.

Αλεξανδροπούλου – Αιγυπτιάδου, Ε. (2002), *Ζητήματα από το Δίκαιο της Πληροφορικής*. Αθήνα - Θεσσαλονίκη: Α. Σάκκουλας.

Αρκουλή, Κ.Γ. (2010), *Προστασία προσωπικών δεδομένων στις ηλεκτρονικές επικοινωνίες*. Αθήνα: Νομική Βιβλιοθήκη.

Αρμαμέντος, Π., Σωτηρόπουλος, Β. (2005), *Προσωπικά Δεδομένα - Ερμηνεία Ν.2472/1997*. Αθήνα – Θεσσαλονίκη: Α. Σάκκουλας.

Anonymous (2017), «Data is giving rise to a new economy», *Economist*. Διαθέσιμο στο: <https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy> [πρόσβαση 02.12.2018].

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

Βικελίδου Κ. (2017), «Αρχές και καλές πρακτικές για την ποιοτική εξυπηρέτηση του πολίτη – ΑΠΔΠΧ», *Επιμορφωτικό πρόγραμμα του Περιφερειακού Ινστιτούτου Επιμόρφωσης Θεσσαλονίκης*. Θεσσαλονίκη, Ιούλιος 2017.

Βουλή των Ελλήνων (1996), Εισηγητική Έκθεση στο σχέδιο νόμου «Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα». Διαθέσιμο στο: https://webcache.googleusercontent.com/search?q=cache:NLD-0ZaudIEJ:https://www.hellenicparliament.gr/UserFiles/2f026f42-950c-4efc-b950-340c4fb76a24/NOM_NOM_EE_2472_UA23.DOC+&cd=3&hl=el&ct=clnk&gl=gr [πρόσβαση 13.12.2018].

Γεραρής, Χ. (2010), «Τα προσωπικά δεδομένα και οι νέες προκλήσεις», *Δίκαιο Μέσων Ενημέρωσης και Επικοινωνίας (ΔιΜΕΕ)*, 1/2010, σσ. 42-44.

Γέροντας, Α. (2002), *Η προστασία του πολίτη από την ηλεκτρονική επεξεργασία προσωπικών δεδομένων*. Αθήνα – Θεσσαλονίκη: Α. Σάκκουλας.

Γιαννακούλα, Α., Μηλαπίδου, Μ. (Επιμ.). (2017), *Προσωπικά Δεδομένα*. Αθήνα: Νομική Βιβλιοθήκη.

Γιαννόπουλος, Γ. (2017), «Γενικός Κανονισμός Προστασίας Δεδομένων: οι νέες υποχρεώσεις και η ευθύνη του Υπευθύνου Επεξεργασίας», *Εφημερίδα Διοικητικού Δικαίου*, 2/2017, σσ. 199-205.

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.

Δούκα, Β. (2018), «Προσωπικά Δεδομένα και εργασιακές σχέσεις: Προστασία σύμφωνα με τον Γενικό Κανονισμό Προστασίας Δεδομένων», *Επιθεώρηση Εργατικού Δικαίου*, 77(6), σσ. 641-664.

Ευρωπαϊκή Ένωση (2010), *Χάρτης των θεμελιωδών δικαιωμάτων της Ευρωπαϊκής Ένωσης*. Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης C83/391, 30.03.2010.

Ευρωπαϊκή Ένωση (2012), *Ενοποιημένη απόδοση της συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης*. Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης C326/47, 26.10.2012.

Ζωγραφόπουλος, Δ. (2018), «Οδηγός προετοιμασίας για τη συμμόρφωση προς τον ΓΚΠΔ/GDPR - Βασικές κατευθύνσεις». Υπουργείο Υγείας.

Ιγγλεζάκης, Ι. (2004), *Ευαίσθητα Προσωπικά Δεδομένα*. Αθήνα – Θεσσαλονίκη: Α. Σάκκουλας.

Ιγγλεζάκης, Ι. (2014), *Το δικαίωμα στην ψηφιακή λήθη και οι περιορισμοί του*. Αθήνα – Θεσσαλονίκη: Α. Σάκκουλας.

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.

Καμίνης, Γ. (2008), «Ο κίνδυνος μιας ‘πανοπτικής δημόσιας διοίκησης’», *Βήμα Ιδεών*, τ.10, Φεβρουάριος 2008. Διαθέσιμο στο: <http://www.dpa.gr/APDPXPortlets/htdocs/documentSDisplay.jsp?docid=17,165,243,28,112,14,12,168> [πρόσβαση 20.12.2018].

Καρδασιάδου, Ζ. (2010), «Δημόσια ασφάλεια και προστασία των προσωπικών δεδομένων», *Δίκαιο Μέσων Ενημέρωσης και Επικοινωνίας (ΔιΜΕΕ)*, 2/2010, σσ. 207-210.

Κετιτζιάν, Σ. (2018), «Κωνσταντίνος Μενουδάκος: η 25^η Μαΐου δεν αποτελεί την ημερομηνία ολοκλήρωσης αλλά έναρξης της εφαρμογής του Γενικού Κανονισμού», *Επιχειρώ*, 22 Μαΐου. Διαθέσιμο στο: <http://www.epixeiro.gr/article/87275> [πρόσβαση 10.11.2018].

Κοντοπούλου, Κ. (2018), «Νέος Κανονισμός για την Προστασία Δεδομένων (GDPR) - Προσωπικό απόρρητο, Έλεγχοι, Γνωστοποιήσεις, Διαφάνεια, Επιμόρφωση, Τεχνολογία πληροφοριών και Επικοινωνίας», *Επιχείρηση*, 6/2018, σσ. 523-530.

Κοτσαλής, Λ., Μενουδάκος, Κ. (Επιμ.). (2018), *Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων (GDPR)*. Αθήνα: Νομική Βιβλιοθήκη.

Κοτσαλής, Λ. (Επιμ.). (2016), *Προσωπικά Δεδομένα: ανάλυση-σχόλια-εφαρμογή*. Αθήνα: Νομική Βιβλιοθήκη.

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.

Μήτρου, Λ. (2017), *Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων*. Αθήνα – Θεσσαλονίκη: Α. Σάκκουλας.

Μυλώση, Μ. (2015), *Η έννομη προστασία των δεδομένων οικονομικής συμπεριφοράς από την αθέμιτη ηλεκτρονική επεξεργασία τους: συγκριτική μελέτη της νομικής ρύθμισης σε Ελλάδα και Γαλλία*. (Μη εκδοθείσα διδακτορική διατριβή). Πανεπιστήμιο Μακεδονίας, Τμήμα Εφαρμοσμένης Πληροφορικής. Διαθέσιμη στο: <https://www.didaktorika.gr/eadd/handle/10442/42327>.

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

Νούσκαλης, Γ. (2018), «Η ποινική προστασία προσωπικών δεδομένων μετά τον Κανονισμό 679/2016 και το σχετικό ελληνικό νομοσχέδιο. Ορισμένες πρώτες σκέψεις και επισημάνσεις», *Ποινική Δικαιοσύνη*, 3/2018, σσ. 270-275.

ΟΟΣΑ (1980), *Κατευθυντήριες γραμμές για την προστασία της ιδιωτικής ζωής και τις διασυννοριακές ροές δεδομένων προσωπικού χαρακτήρα*. Παρίσι: ΟΟΣΑ.

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.

Παναγοπούλου-Κουτνατζή, Φ. (2017α), *Ο Γενικός Κανονισμός για την Προστασία Δεδομένων 679/2016/ΕΕ*. Αθήνα – Θεσσαλονίκη: Α. Σάκκουλας.

Παναγοπούλου-Κουτνατζή, Φ. (2017β), «Τα νέα δικαιώματα για τους πολίτες βάσει του Γενικού Κανονισμού Προστασίας Δεδομένων: μια πρώτη αποτίμηση και συνταγματική αξιολόγηση», *Εφημερίδα Διοικητικού Δικαίου*, 1/2017, σσ. 81-98.

Παναγοπούλου-Κουτνατζή, Φ. (2017γ), *Η εξέλιξη του δικαιώματος στη λήθη*. Διαθέσιμο στο: <https://www.ethemis.gr/epistimoniki-arthrografia-fereniki-panagoroulou-koutnatzi.html> [πρόσβαση 02.12.2018].

Πλατής, Ε. (2018), *Προσωπικά Δεδομένα: Προστασία GDPR*. Αθήνα: Παπαδόπουλος.

Ρουσόπουλος, Γ., Λιμνιώτης, Κ. (2018), «Προετοιμασία των Δημόσιων Οργανισμών για την εφαρμογή του νέου Κανονισμού - Τα εργαλεία συμμόρφωσης για τη μετάβαση από το Ν.2472/1997 στον ΓΚΠΔ», *ΙΝΕΠ-ΕΚΔΔΑ, Προετοιμασία για τον ΓΚΠΔ*. Θεσσαλονίκη, 11 Μαΐου.

Σιδηρόπουλος, Θ. (2003), *Το δίκαιο του διαδικτύου*. Αθήνα – Θεσσαλονίκη: Α. Σάκκουλας.

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.

Σπανού, Κ. (Επιμ.). (2010), *Πρόσβαση στα έγγραφα και διαφάνεια της διοικητικής δράσης*. Αθήνα – Θεσσαλονίκη: Α. Σάκκουλας.

Σπηλιωτόπουλος, Ε. (2017), *Εγχειρίδιο Διοικητικού Δικαίου – Τόμος Ι*. Αθήνα: Νομική Βιβλιοθήκη.

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

Σωτηρόπουλος, Β. (χωρίς ημερομηνία), *Το άρθρο 9Α του Συντάγματος 1975/1986/2001*. Διαθέσιμο στο: <http://www.greeklaws.com/pubs/uploads/596.pdf> [πρόσβαση 16.11.2018].

Σωτηρόπουλος, Β. (2006), *Η Συνταγματική Προστασία των Προσωπικών Δεδομένων*. Αθήνα – Θεσσαλονίκη: Α. Σάκκουλας.

Υπουργείο Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων (2018), *Σχέδιο Νόμου για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα*. Διαθέσιμο στο: http://www.opengov.gr/ministryofjustice/wp-content/uploads/downloads/2018/02/sxedio_nomou_prostasia_pd.pdf [πρόσβαση 05.11.2018].

Χελιουδάκης, Λ. (2018), «Γιατί η μικρή αδερφή του GDPR πρέπει να σε απασχολεί ως πολίτη;», *Homo Digitalis*, 4 Σεπτεμβρίου. Διαθέσιμο στο: <https://www.homodigitalis.gr/posts/2373> [πρόσβαση 05.11.2018]

Χριστοδούλου, Κ. (2013), *Δίκαιο Προσωπικών Δεδομένων*. Αθήνα: Νομική Βιβλιοθήκη.

Ψαροπούλου, Α. (2018), *Προστασία Δεδομένων Προσωπικού Χαρακτήρα*. (Μη εκδοθείσα μεταπτυχιακή εργασία). Πανεπιστήμιο Μακεδονίας, ΠΜΣ Δημόσια Διοίκηση.

ΗΛΕΚΤΡΟΝΙΚΕΣ ΠΗΓΕΣ

<https://www.lawspot.gr/>

<http://iglezakis.gr/>

<https://ec.europa.eu>

<http://mindigital.gr>

www.dpa.gr

<http://diavgeia.gov.gr/>

www.esyd.gr

https://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358

ΠΑΡΑΡΤΗΜΑ

Επιχειρήθηκε ηλεκτρονική και τηλεφωνική επικοινωνία με 19 Υπουργεία και την ΑΠΔΠΧ προς αναζήτηση πληροφοριών σχετικά με τη συμμόρφωση του δημόσιου τομέα προς τον ΓΚΠΔ και τις ενέργειες στις οποίες η ΔΔ έχει προβεί ως τώρα γι' αυτό τον σκοπό. Οι έγγραφες απαντήσεις που συγκεντρώθηκαν παρατάσσονται αυτούσιες, ενώ τα στοιχεία των αποστολών αποκρύπτονται και είναι στη διάθεση της συγγραφέως:

1) ΑΠΑΝΤΗΣΗ ΥΠΟΥΡΓΕΙΟΥ ΔΙΟΙΚΗΤΙΚΗΣ ΑΝΑΣΥΓΚΡΟΤΗΣΗΣ

From: [dpo](#)

Sent: Tuesday, November 20, 2018 11:51 AM

To: '[elsaki](#)'

Subject: GDPR info

Καλημέρα σας.

Το Υπουργείο μας έχει ορίσει DPO και μέσω διαγωνισμού θα γίνει η επιλογή αναδόχου για να λάβει ως υπηρεσία τη χαρτογράφηση των διαδικασιών, την εκπόνηση των απαραίτητων μελετών, προετοιμασία εκπαιδευτικού υλικού, προετοιμασία σημειωμάτων, και άλλων απαραίτητων για τη συμμόρφωση με τον ΓΚΠΔ (GDPR).

[παραλείπεται όνομα αποστολέα]

Υπουργείο Διοικητικής Ανασυγκρότησης

DPO

Λεωφ. Βασ. Σοφίας 15, 10674 Αθήνα

FAX: +30 2109286020

e-mail: dpo@ydmed.gov.gr

2) ΑΠΑΝΤΗΣΗ ΥΠΟΥΡΓΕΙΟΥ ΕΞΩΤΕΡΙΚΩΝ

From: [Data Protection Office](#)

Sent: Tuesday, November 27, 2018 3:39 PM

To: [elsaki](#)

Subject: Re: GDPR INFO

Καλησπέρα σας,

θα θέλαμε να σας γνωστοποιήσουμε πως με την υπ'αριθμ. πρωτ. Π37Α-39039/05.07.2018 απόφαση του Υπουργού Εξωτερικών έχει ορισθεί Υπεύθυνος Προστασίας Δεδομένων για το Υπουργείο μας και με την υπ'αριθμ. πρωτ. Π37Α-42781/23.07.2018 απόφαση έχει συγκροτηθεί ομάδα Εργασίας για την υποστήριξη του Υπευθύνου Προστασίας Δεδομένων του Υπουργείου Εξωτερικών. Ανωτέρω ομάδα βρίσκεται στη διαδικασία εκπόνησης καταγραφής δραστηριοτήτων του Υπουργείου μας που ενσωματώνουν επεξεργασία προσωπικών δεδομένων.

Με εκτίμηση,

Ομάδα Προστασίας Προσωπικών Δεδομένων

3)ΑΠΑΝΤΗΣΕΙΣ ΥΠΟΥΡΓΕΙΟΥ ΕΡΓΑΣΙΑΣ

A)From: [Τμήμα Οργάνωσης, Εκπαίδευσης και Επιμόρφωσης](#)

Sent: Monday, November 26, 2018 12:06 PM

To: ['elsaki'](#)

Subject: RE: ΚΑΝΟΝΙΣΜΟΣ Ε.Ε. 2016/679

Σας ενημερώνουμε ότι το τμήμα μας δεν είναι αρμόδιο για τα προσωπικά δεδομένα και από αυτά που γνωρίζουμε δεν έχει ακόμη οριστεί υπεύθυνος για τα προσωπικά δεδομένα.

B)Από: [παραλείπεται όνομα και ηλεκτρονική διεύθυνση αποστολέα]

Συνημμένα

10:04 π.μ.

Προς: mpm18044@uom.edu.gr

Κα Χριστοδούλου,

Σας αποστέλλω συνημμένα την υπ' αριθ. 31935/Δ1.11180/08-06-2018 Υπουργική Απόφαση, δυνάμει της οποίας ορίστηκε υπεύθυνη προστασίας προσωπικών δεδομένων του Υπουργείου η υπάλληλος Γεωργία Ακούλογλου (τηλ επικοινωνίας: 213 1516244).

Στη διάθεσή σας για οποιαδήποτε διευκρίνιση,

Με εκτίμηση

[παραλείπεται όνομα αποστολέα]

Υπουργείο Εργασίας, Κοινωνικής Ασφάλισης και Κοινωνικής Αλληλεγγύης

Γενική Δ/ση Διοικητικής Υποστήριξης & Ηλεκτρονικής Διακυβέρνησης

Δ/ση Υποστήριξης Ανθρώπινου Δυναμικού & Υπηρεσιών

Τμήμα Διοίκησης Ανθρώπινου Δυναμικού ΥΠ.Ε.Κ.Α.Α. & ΣΕΠΕ

Στάδιου 29, Αθήνα 101 10

Τηλ; 213 1516131

Fax: 210 5240712

E-mail: [παραλείπεται]

4)ΑΠΑΝΤΗΣΗ ΥΠΟΥΡΓΕΙΟΥ ΠΑΙΔΕΙΑΣ

From: [παραλείπεται όνομα αποστολέα]

Sent: Thursday, November 15, 2018 11:23 AM

To: c-elisab@otenet.gr

Cc: [παραλείπεται όνομα]

Subject: Κανονισμός Προστασίας Προσωπικών Δεδομένων

Σε απάντηση του από 11-11-2018 ηλεκτρονικού μηνύματός σας, σας ενημερώνουμε ότι έχει εκδοθεί από την Υπηρεσία μας η αριθμ. 123622/Γ1/20-7-2018(ΑΔΑ: ΩΣΙΒ4653ΠΣ-Υ7Μ) Απόφαση με θέμα: «Ορισμός Υπευθύνου Προστασίας Δεδομένων (Data protection Officer-DPO) του Υπουργείου Παιδείας, Έρευνας και Θρησκευμάτων».

[παραλείπεται όνομα αποστολέα]

Υπουργείο Παιδείας, Έρευνας και Θρησκευμάτων

Δ/νση Ανθρώπινου Δυναμικού Γ.Γ. Υπουργείου

Τμήμα Α΄ Ανθρώπινου Δυναμικού της Γενικής Γραμματείας

του Υπουργείου και της Γενικής Γραμματείας Θρησκευμάτων

Τηλ. 210-3442345

Fax. 210-3442365

Email [παραλείπεται]

5)ΑΠΑΝΤΗΣΗ ΥΠΟΥΡΓΕΙΟΥ ΟΙΚΟΝΟΜΙΚΩΝ

----- Forwarded message -----

From: [παραλείπεται όνομα και ηλεκτρονική διεύθυνση αποστολέα]

Date: Τετ, 12 Δεκ 2018 στις 11:28 π.μ.

Subject: RE: GDPR info

To: ELISAVET CHRISTODOULIDOU <mpm18044@uom.edu.gr>

Καλημέρα σας και καλή επιτυχία στο μεταπτυχιακό σας

Στη Γενική Γραμματεία Πληροφοριακών Συστημάτων του Υπ. Οικονομικών υπάρχει πλήρης ενημέρωση για τον Κανονισμό της ΕΕ_679/2016 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27^{ης} Απριλίου του 2016. Βέβαια δεν μείναμε μόνο στην ενημέρωση αλλά και στις απαραίτητες ενέργειες για την καταγραφή των συστημάτων και των ενεργειών κάθε διεύθυνσης και κάθε τμήματος. Ταυτόχρονα ενεργήσαμε τα δέοντα προκειμένου να ανατεθεί σε ειδικό εξωτερικό σύμβουλο, η μελέτη και καταγραφή των διαδικασιών των εκάστοτε συστημάτων, καταγραφή

αντικτύπου κλπ. Επίσης, οι γενικές διευθύνσεις έχουν ενημερωθεί, έτσι ώστε όλα τα συστήματα που παραλαμβάνονται από δω και το εξής να έχουν την πρόβλεψη του Γενικού Κανονισμού Προσωπικών Δεδομένων (ΓΚΠΔ) της ΕΕ_679/2016.

Τέλος στον Οργανισμό του Υπουργείου υπάρχει η πρόβλεψη για συγκεκριμένη δομή, ως εξής:

.... «Δημιουργείται Αυτοτελές Γραφείο Υπεύθυνου Προστασίας Προσωπικών Δεδομένων (Data Protection Officer-DPO), υπαγόμενο στον Υπουργό Οικονομικών, σύμφωνα με τον Γενικό Κανονισμό Προσωπικών Δεδομένων (ΓΚΠΔ) της ΕΕ_679/2016 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27^{ης} Απριλίου του 2016, το οποίο είναι υποχρεωτικό σύμφωνα και με την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ). Ο Υπεύθυνος Προστασίας Προσωπικών Δεδομένων (DPO), προάγει την κουλτούρα της προστασίας προσωπικών δεδομένων εντός του Οργανισμού ή Φορέα και έχει τις κάτωθι αρμοδιότητες:

α) Να ενημερώνει και να συμβουλεύει τον Οργανισμό και τους υπαλλήλους του σχετικά με τις υποχρεώσεις τους που απορρέουν από τον Κανονισμό και τις άλλες διατάξεις περί προστασίας δεδομένων.

β) Να παρακολουθεί την εσωτερική συμμόρφωση με τον Κανονισμό και άλλες διατάξεις περί προστασίας δεδομένων (π.χ. προσδιορισμός και διαχείριση δραστηριοτήτων επεξεργασίας, εκπαίδευση προσωπικού, διενέργεια εσωτερικών ελέγχων).

γ) Να παρέχει συμβουλές για την εκτίμηση αντικτύπου και να παρακολουθεί την υλοποίησή της.

δ) Να είναι το πρώτο σημείο επαφής για τις εποπτικές αρχές και τα υποκείμενα των δεδομένων (εργαζόμενοι, πελάτες κ.λ.π.).

ε) Να συνεργάζεται με την εποπτική Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ).

Ο Υπεύθυνος Προστασίας Προσωπικών Δεδομένων (DPO), 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). Ο ρόλος του είναι συμβουλευτικός (όχι αποφασιστικός) και δεν φέρει προσωπική ευθύνη για τη μη συμμόρφωση με τον Κανονισμό. Υπεύθυνος να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τον ΓΚΠΔ είναι ο υπεύθυνος επεξεργασίας ή ο

εκτελών την επεξεργασία. Προβλέπονται συγκεκριμένα καθήκοντα του DPO και αντίστοιχες υποχρεώσεις. Παράβαση των σχετικών με τον DPO διατάξεων επιφέρει κυρώσεις (βλ. άρθρα 37-38 και 83 σε συνδυασμό με αιτιολογική σκέψη 97 του ΓΚΠΔ).

Το Γραφείο θα έχει πενταμελή (5) σύνθεση, αποτελούμενο από τον Επικεφαλής DPO, δύο (2) υπαλλήλους ΠΕ-Πληροφορικής, ένα (1) υπάλληλο Διοικητικού-Οικονομικού με πτυχίο Νομικής και ένα (1) υπάλληλο ΔΕ-Προσωπικού Η/Υ.»

Σας ευχαριστώ εκ των προτέρων



[παραλείπεται όνομα αποστολέα]

πρ. Γενικός Διευθυντής

Υποδομών και Υπηρεσιών

Πληροφορικής - Επικοινωνιών

ΥΠΟΥΡΓΕΙΟ ΟΙΚΟΝΟΜΙΚΩΝ

Γενική Γραμματεία Πληροφοριακών Συστημάτων

Τηλ: 210 4803243, 210 4803207,08

E-Mail: [παραλείπεται]

6)ΑΠΑΝΤΗΣΗ ΥΠΟΥΡΓΕΙΟΥ ΥΓΕΙΑΣ

----- Forwarded message -----

From: DATA PROTECTION OFFICER <dpo@moh.gov.gr>

Date: Τετ, 12 Δεκ 2018 στις 4:19 μ.μ.

Subject: RE: ΑΝΑΖΗΤΗΣΗ ΠΛΗΡΟΦΟΡΙΩΝ

To: ELISAVET CHRISTODOULIDOU <mpm18044@uom.edu.gr>

Κυρία Χριστοδουλίδου καλησπέρα σας.

Σε απάντηση του συνημμένου αιτήματός σας, σας αποστέλλουμε σύντομο βιογραφικό σημείωμα, σχετικά με τις ερωτήσεις σας. Για περισσότερες πληροφορίες μπορείτε να επιχειρήσετε τηλεφωνική επικοινωνία στον αναγραφόμενο αριθμό τηλεφώνου.

Σας ευχαριστούμε για την επικοινωνία,

Δημήτρης Ζωγραφόπουλος
Υπουργείο Υγείας
Δικηγόρος (ΔΝ) – Ειδικός επιστήμονας,
Υπεύθυνος Προστασίας Δεδομένων (DPO)
Τηλ.: 213 216 12 54
e-mail: dpo@moh.gv.gr / gdpr@moh.gov.gr

7)ΑΠΑΝΤΗΣΗ ΥΠΟΥΡΓΕΙΟΥ ΔΙΚΑΙΟΣΥΝΗΣ

From: [παραλείπεται όνομα αποστολέα]
Sent: Wednesday, December 12, 2018 9:54 AM
To: c-elisab@otenet.gr

Καλημέρα σας,

Στο site του Υπουργείου μας αναφέρεται ο υπεύθυνος επεξεργασίας καθώς και τα στοιχεία επικοινωνίας του.

Ως προς το θέμα της ενσωμάτωσης της σχετικής οδηγίας για την προστασία των προσωπικών δεδομένων αυτή δεν έχει ενσωματωθεί έως σήμερα.

Με εκτίμηση

[παραλείπεται όνομα αποστολέα]

Προισταμένη Δ/νσης

(Από το site του Υπουργείου Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων
Δικαιωμάτων: <http://www.ministryofjustice.gr/site/dpo.aspx>)

«Υπεύθυνος Προστασίας Δεδομένων

*Για οποιαδήποτε πληροφορία σχετικά με την επεξεργασία των προσωπικών δεδομένων της **Κεντρικής Υπηρεσίας του Υπουργείου Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων** μπορείτε να επικοινωνείτε με την Υπεύθυνη Προστασίας Δεδομένων, Νικολέτα Μολυμπάκη (αριθ. 52740/10.07.2018 υπουργική απόφαση), συμπληρώνοντας την παρακάτω φόρμα».*

8) ΑΠΑΝΤΗΣΗ ΤΟΜΕΑ ΜΑΚΕΔΟΝΙΑΣ – ΘΡΑΚΗΣ

From: [παραλείπεται όνομα αποστολέα]

Sent: Wednesday, December 12, 2018 2:03 PM

To: c-elisab@otenet.gr

Καλημέρα

Απαντώντας στο e-mail σας, αναφορικά με το αντικείμενο του θέματος, σας πληροφορούμε ότι λόγω μεγάλου φόρτου εργασίας στο συγκεκριμένο χρονικό διάστημα, δεν μπορούμε να ανταποκριθούμε στο αίτημά σας.

[παραλείπεται όνομα αποστολέα]

Προϊστάμενη Διεύθυνσης Διοικητικής Υποστήριξης & Η.Δ.

του Υπουργείου Εσωτερικών/Τομέας Μακεδονίας Θράκης

Τηλ.: 2310-379492

Fax: 2310-285250

Ηλ. Ταχ.: [παραλείπεται]

9) ΑΠΑΝΤΗΣΗ ΥΠΟΥΡΓΕΙΟΥ ΕΣΩΤΕΡΙΚΩΝ

From: [παραλείπεται όνομα και ηλεκτρονική διεύθυνση αποστολέα]

Date: Δευ, 24 Δεκ 2018 στις 9:52 π.μ.

Subject: RE: ΣΥΜΜΟΡΦΩΣΗ ΥΠ.ΕΣΩΤΕΡΙΚΩΝ ΜΕ GDPR

To: ELISAVET CHRISTODOULIDOU <mpm18044@uom.edu.gr>

Cc: [παραλείπεται όνομα και ηλεκτρονική διεύθυνση]

Καλημέρα κυρία Χριστοδουλίδου,

Ονομάζομαι [παραλείπεται όνομα] είμαι υπάλληλος του Τμήματος Προσωπικού της Διεύθυνσης Διοικητικής Υποστήριξης.

Εχθές μου χρεώθηκε το email που στείλατε στις 10/12.

Σας κοινοποιώ την απόφαση του Υπουργού Εσωτερικών περί ορισμού Υπευθύνου Προστασίας Δεδομένων. Υπεύθυνος ορίστηκε ο κύριος Σταμάτης Θεοχάρης (email: s.theoxaris@ypes.gr και τηλέφωνο επικοινωνίας: 2131522504).

Του προώθησα τα email σας, για να επικοινωνήσει μαζί σας.

Σας εύχομαι καλές γιορτές.

«Θέμα : Αναζήτηση πληροφοριών από πολίτη για τις ενέργειες του Υπουργείου Εσωτερικών αναφορικά με τη συμμόρφωσή του με τις διατάξεις του Γενικού Κανονισμού Προστασίας Δεδομένων

Σχετικό :

1. Το από 21.12.2018 ηλεκτρονικό μήνυμα της κας [παραλείπεται όνομα] αναφορικά με το θέμα
2. Το από 10.12.2018 ηλεκτρονικό μήνυμα της κας Ελισάβετ Χριστοδουλίδου προς τη Διεύθυνση Διοικητικής Υποστήριξης του Υπουργείου Εσωτερικών σχετικά με τη «ΣΥΜΜΟΡΦΩΣΗ ΥΠ.ΕΣΩΤΕΡΙΚΩΝ ΜΕ GDPR»

Σε απάντηση των ανωτέρω σχετικών σας γνωρίζω τα κάτωθι σχετικά με τις αρμοδιότητες του Υπευθύνου Προστασίας Δεδομένων – DPO.

Ο Υπεύθυνος Προστασίας Δεδομένων (DPO) διευκολύνει τη συμμόρφωση του υπευθύνου επεξεργασίας και του εκτελούντος την επεξεργασία με τις διατάξεις του Γενικού Κανονισμού Προστασίας (General Data Protection Regulation, GDPR) και μεσολαβεί μεταξύ των διαφόρων ενδιαφερομένων (π.χ. εποπτικές αρχές, υποκείμενα των δεδομένων). Ο ρόλος του είναι συμβουλευτικός και όχι αποφασιστικός και δε φέρει προσωπική ευθύνη για τη μη συμμόρφωση του υπευθύνου επεξεργασίας ή του εκτελούντα την επεξεργασία των δεδομένων με τον Κανονισμό. Υπεύθυνος να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τον ΓΚΠΔ είναι ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία. Προβλέπονται συγκεκριμένα καθήκοντα του DPO και αντίστοιχες υποχρεώσεις του εργοδότη του. Παράβαση των σχετικών με τον DPO διατάξεων επιφέρει κυρώσεις (βλ. άρθρα 37-38 και 83 σε συνδυασμό με αιτιολογική σκέψη 97 του ΓΚΠΔ).

Ειδικότερα, σύμφωνα με το άρθρο 39 του Γενικού Κανονισμού Προστασίας Δεδομένων – ΓΚΠΔ, στις αρμοδιότητες του DPO ανήκουν τουλάχιστον τα εξής :

«...α) ενημερώνει και συμβουλεύει τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία και τους υπαλλήλους που επεξεργάζονται τις υποχρεώσεις τους που απορρέουν από τον παρόντα κανονισμό και από άλλες διατάξεις της Ένωσης ή του κράτους μέλους σχετικά με την προστασία δεδομένων, β) παρακολουθεί τη συμμόρφωση με τον παρόντα κανονισμό, με άλλες διατάξεις της Ένωσης ή του κράτους μέλους σχετικά με την προστασία δεδομένων και με τις πολιτικές του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία σε σχέση με την προστασία των δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων της ανάθεσης αρμοδιοτήτων, της ευαισθητοποίησης και της κατάρτισης των υπαλλήλων που συμμετέχουν στις πράξεις επεξεργασίας, και των σχετικών ελέγχων, γ) παρέχει συμβουλές, όταν ζητείται, όσον αφορά την εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων και παρακολουθεί την υλοποίησή της σύμφωνα με το άρθρο 35, δ) συνεργάζεται με την εποπτική αρχή, ε) ενεργεί ως σημείο επικοινωνίας για την εποπτική αρχή για ζητήματα που σχετίζονται με την επεξεργασία, περιλαμβανομένης της προηγούμενης διαβούλευσης που αναφέρεται στο άρθρο 36, και πραγματοποιεί διαβουλεύσεις, ανάλογα με την περίπτωση, για οποιοδήποτε άλλο θέμα....»

Κατόπιν, των ανωτέρω και δεδομένου ότι με την υπ' αριθμ. ΑΠ 23837/29.5.2018 απόφαση του Υπουργού Εσωτερικών ορίστηκε ως DPO του Υπουργείου Εσωτερικών με την οποία δεν μου ανατίθενται πλέον των ανωτέρω άλλα καθήκοντα, σας γνωρίζω ότι ως DPO του Υπουργείου δεν έχω αρμοδιότητα να αποδεικνύω την συμμόρφωση του φορέα προς τα οριζόμενα των διατάξεων του ΓΚΠΔ. Αντίθετα η αρμοδιότητα απόδειξης της συμμόρφωσης με τις διατάξεις του ΓΚΠΔ ρητά ανήκει στις αρμοδιότητες του Υπεύθυνου Επεξεργασίας και συνεπώς θα πρέπει άμεσα η υπηρεσία να επιληφθεί του θέματος.

**Ο Υπεύθυνος Προστασίας
Προσωπικών Δεδομένων**

Σταμάτης Θεοχάρης

10) ΑΠΑΝΤΗΣΗ ΥΠΟΥΡΓΕΙΟΥ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ

Συμμορφωση Υπ. Εθνικής Αμυνας με GDPR

Gdosy Dadp gdosy_dadp@mod.mil.gr 11:30 π.μ. (Πριν από 5 ώρες)

Κυρία Χριστοδουλίδου,

Σε απάντηση του από 10 Δεκ 2018 ηλεκτρονικού σας μηνύματος, σας γνωρίζουμε ότι έχουν αναληφθεί ενέργειες, κατ' εφαρμογή του άρθρου 37 του Γενικού Κανονισμού για την Προστασία Δεδομένων [(Κανονισμός ΕΕ) 2016/679], για τον ορισμό Υπεύθυνου Προστασίας Δεδομένων στο Υπουργείο Εθνικής Άμυνας και στις δομές του, λαμβανομένων υπόψη των παραμέτρων του οργανωτικού μεγέθους και της πολυεπίπεδης οργανωτικής δομής των Ενόπλων Δυνάμεων, η δε διαδικασία βρίσκεται σε εξέλιξη. Με εκτίμηση,

Τχης (ΝΟΜ) [παραλείπεται όνομα]

Επιτελής Τμήματος Στρατολογικών Διοικητικών και Νομικών Θεμάτων

Δνσης Ανθρώπινου Δυναμικού & Περιβάλλοντος

Υπουργείου Εθνικής Άμυνας

11) ΑΠΑΝΤΗΣΗ ΥΠΟΥΡΓΕΙΟΥ ΑΓΡΟΤΙΚΗΣ ΑΝΑΠΤΥΞΗΣ ΚΑΙ ΤΡΟΦΙΜΩΝ

RE: ΥπΑΑΤ | Υπουργείο Αγροτικής Ανάπτυξης & Τροφίμων: ΠΛΗΡΟΦΟΡΙΕΣ ΓΙΑ ΚΑΝΟΝΙΣΜΟ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

info info@minagric.gr Παρ, 21 Δεκ 2018, 1:42 μ.μ.

Κα Χριστοδουλίδου,

σε απάντηση του ερωτήματός σας, θα θέλαμε να σας ενημερώσουμε ότι στο Υπουργείο Αγροτικής Ανάπτυξης και Τροφίμων έχει προκηρυχθεί συνοπτικός διαγωνισμός για την εξεύρεση αναδόχου για την παροχή υπηρεσιών συμμόρφωσης του Υπουργείου και των εποπτευόμενων φορέων Ε.Φ.Ε.Τ. και ΕΛΓΟ-ΔΗΜΗΤΡΑ προς τις απαιτήσεις του Γενικού Κανονισμού Προστασίας Δεδομένων (General Data Protection Regulation - GDPR) και λήψης απαραίτητων διορθωτικών μέτρων [Διακήρυξη αριθ. 3507/Χ.Δ/2018 Συνοπτικού (Πρόχειρου) Διαγωνισμού].

Η γνωστοποίηση των στοιχείων επικοινωνίας του/της Υπευθύνου Προστασίας Δεδομένων (DPO), δεν είναι στην παρούσα φάση εφικτή, δεδομένου ότι οι διαδικασίες ορισμού του/της Υπευθύνου δεν έχουν ολοκληρωθεί.

Με εκτίμηση

12) ΥΠΟΥΡΓΕΙΟ ΨΗΦΙΑΚΗΣ ΠΟΛΙΤΙΚΗΣ, ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ ΚΑΙ ΕΝΗΜΕΡΩΣΗΣ

(Από το site του Υπουργείου Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης: <http://www.mindigital.gr/index.php/8-static/2903-dpo>)

Σας ενημερώνουμε ότι έχει οριστεί Υπεύθυνος Προστασίας Δεδομένων (ΥΠΔ /DPO) για το ΥΨΗΠΤΕ ο κος Κοσμόπουλος Αθανάσιος με αναπληρωτή τον κο Κατέρη Ευάγγελο. Μπορείτε να επικοινωνείτε για κάθε θέμα που αφορά την προστασία προσωπικών δεδομένων και να στέλνετε τις παρατηρήσεις ή ερωτήματά σας για ζητήματα προσωπικών δεδομένων, τα οποία αφορούν τις αρμοδιότητες του ΥΨΗΠΤΕ. Σε κάθε άλλη περίπτωση αρμόδιος είναι ο ΥΠΔ του εκάστοτε, σχετικού με το ζήτημα, Υπουργείου ή φορέα.

Στοιχεία επικοινωνίας:

Email (κοινό): dpo@mindigital.gr

Κοσμόπουλος Αθανάσιος

Τηλ: 2131500571

Λέκκα 23-25, 105 52 Αθήνα

Κατέρης Ευάγγελος

2109098253

Αλ.Πάντου και Φραγκούδη 11 , 101 63 Αθήνα