ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΓΕΝΙΚΟ ΤΜΗΜΑ, ΛΑΡΙΣΑ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

«ΔΗΜΟΣΙΑ ΔΙΟΙΚΗΣΗ ΚΑΙ ΤΟΠΙΚΗ ΑΥΤΟΔΙΟΙΚΗΣΗ»

"Η προστασία των προσωπικών δεδομένων σύμφωνα με τον Γενικό Κανονισμό Προστασίας Δεδομένων (ΕΕ) 2016/679 (General Data Protection Regulation-GDPR) και η εφαρμογή του Κανονισμού στα ελληνικά πανεπιστήμια"

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΤΣΑΛΜΑ ΒΑΣΙΛΙΚΗ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΔΡ. ΙΩΑΝΝΗΣ ΠΑΠΑΔΗΜΟΠΟΥΛΟΣ

ΛΑΡΙΣΑ, ΦΕΒΡΟΥΑΡΙΟΣ 2021

Υπεύθυνη Δήλωση

«*Δηλώνω υπεύθυνα ότι η συγκεκριμένη μεταπτυχιακή διπλωματική εργασία για τη λήψη του μεταπτυχιακού τίτλου σπουδών του ΠΜΣ Πλήρους Φοίτησης του Πανεπιστημίου Θεσσαλίας «Δημόσια Διοίκηση και τοπική Αυτοδιοίκηση» έχει συγγραφεί από εμένα προσωπικά και δεν έχει υποβληθεί ούτε έχει εγκριθεί στο πλαίσιο κάποιου άλλου μεταπτυχιακού ή προπτυχιακού τίτλου σπουδών, στην Ελλάδα ή στο εξωτερικό. Η εργασία αυτή έχοντας εκπονηθεί από εμένα, αντιπροσωπεύει τις προσωπικές μου απόψεις επί του θέματος και το κείμενο είναι γραμμένο με τα δικά μου λόγια και δεν αποτελεί προϊόν λογοκλοπής από τρίτες πηγές. Οι πηγές στις οποίες ανέτρεξα για την εκπόνηση της συγκεκριμένης διπλωματικής αναφέρονται στο σύνολό τους, δίνοντας πλήρεις αναφορές στους συγγραφείς, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο*».

Η Δηλούσα

Βασιλική Τσάλμα

Ευχαριστίες

Η παρούσα διπλωματική εργασία εκπονήθηκε στα πλαίσια του μεταπτυχιακού προγράμματος Δημόσιας Διοίκησης και Τοπικής Αυτοδιοίκησης του Γενικού Τμήματος του Πανεπιστημίου Θεσσαλίας. Ευχαριστώ θερμά όλους όσους συνέβαλαν στην εκπόνησή της και ιδιαίτερα τον επιβλέποντα καθηγητή μου κ. Ιωάννη Παπαδημόπουλο για την πολύτιμη βοήθεια και καθοδήγησή του καθώς και τα μέλη της επιτροπής κ. Ρωσσίδη και κ. Δημολιού. Τέλος ευχαριστώ τα παιδιά μου για την αμέριστη κατανόηση και συμπαράστασή τους και για την ιδιαίτερη υπομονή που επέδειξαν καθ' όλο το χρονικό διάστημα συγγραφής της παρούσας μελέτης.

ΠΕΡΙΛΗΨΗ

Αντικείμενο της παρούσας μελέτης αποτελεί η προστασία των προσωπικών δεδομένων στα ελληνικά πανεπιστήμια μετά τη θέσπιση του Γενικού Κανονισμού Προστασίας Δεδομένων (ΕΕ) 2016/679 που τέθηκε σε ισχύ στις 25 Μαϊου 2018. Ο ΓΚΠΔ συνιστά την αναγκαία μεταρρύθμιση του προϋφιστάμενου θεσμικού πλαισίου της προστασίας των δεδομένων ενόψει της τεχνολογικής έκρηξης σε συνδυασμό με τις κανονιστικές ανεπάρκειες της προγενέστερης Οδηγίας 95/46/ΕΕ και την έλλειψη ομοιόμορφης και συνεκτικής εφαρμογής της εντός της Ε.Ε..Το αυστηρό και γραφειοκρατικό θεσμικό πλαίσιο που εισάγει ο νέος κανονισμός και ο φορμαλιστικός τρόπος εφαρμογής του σε συνδυασμό με τις βαρύτατες κυρώσεις που προβλέπει, προβληματίζει τους δημόσιους και ιδιωτικούς φορείς των κρατών μελών χωρίς να αφήνει περιθώρια απόκλισης αναφορικά με τη συμμόρφωσή τους. Προσδίδοντας ρόλο πρωταγωνιστή στον Υπεύθυνο Επεξεργασίας και μετακυλύοντας την ευθύνη της επεξεργασίας των δεδομένων σ' αυτόν αντί της εποπτικής αρχής, το νέο αυτό «ατυπικό υβρίδιο», όπως είθισται να αποκαλείται ο ΓΚΠΔ, ενισχύει τα δικαιώματα των φυσικών προσώπων, στηριζόμενο στις βασικές αρχές προστασίας των δεδομένων, τις οποίες συμπληρώνει με την θεσμοθέτηση της αρχής της λογοδοσίας. Ο ελληνικός κυρωτικός Ν. 4624/2019 που ψηφίστηκε υπό την απειλή προστίμου ύψους 2,5 εκατομμυρίων ευρώ από το Δικαστήριο της Ε.Ε. ήρθε να επισφραγίσει την ενίσχυση της προστασίας των προσωπικών δεδομένων στην εσωτερική έννομη τάξη. Η εφαρμογή του ΓΚΠΔ σε συνδυασμό με τα συμπληρωματικά μέτρα που θέτει η εθνική νομοθεσία, επιδιώκει να εξασφαλίσει τη σύννομη επεξεργασία του τεράστιου όγκου προσωπικών δεδομένων που διακινούνται εντός των πανεπιστημίων και να αντιμετωπίσει τους κινδύνους που ελλοχεύουν από τις ραγδαίες τεχνολογικές εξελίξεις. Αρχικά γίνεται αναφορά στην έννοια της ιδιωτικότητας, ειδικότερη έκφανση της οποίας αποτελεί η προστασία των προσωπικών δεδομένων. Εν συνεχεία γίνεται μια ανασκόπηση στο διεθνές και ενωσιακό συμβατικό πλαίσιο προστασίας της ιδιωτικότητας και των προσωπικών δεδομένων, στο χρονικό θεσμοθέτησης του ΓΚΠΔ και της εθνικής μας νομοθεσίας καθώς και στην ΑΠΔΠΧ, δοθέντος του σπουδαίου ρόλου που διαδραματίζει ως εποπτική αρχή και λόγω της ιδιαίτερης συμβολής της εν γένει. Ακολουθεί η ανάλυση των βασικότερων διατάξεων του ΓΚΠΔ και η εν δυνάμει εφαρμογή του εντός των ελληνικών πανεπιστημίων. Προκειμένου να διαπιστωθεί ο βαθμός συμμόρφωσης των τελευταίων διενεργήθηκε έρευνα στα πανεπιστήμια της χώρας, η οποία κατέδειξε την

πρόθεση εκ μέρους των Διοικήσεων των περισσοτέρων Α.Ε.Ι. να προσεγγίσουν με ζέση το νέο κανονισμό. Τέλος, παρατίθενται συμπεράσματα και οι προτάσεις προκειμένου να εξασφαλιστεί η διατήρηση της συμμόρφωσης υπό το πρίσμα της ευαισθητοποίησης και της αλλαγής κουλτούρας, προς την ανάπτυξη μιας περισσότερο ανθρωποκεντρικής φιλοσοφίας για το δίκαιο των προσωπικών δεδομένων.

Λέξεις κλειδιά: προστασία προσωπικών δεδομένων, ο Γενικός Κανονισμός για την προστασία των δεδομένων προσωπικού χαρακτήρα, ΑΠΔΠΧ, προσωπικά δεδομένα στα πανεπιστήμια, συμμόρφωση ΑΕΙ με τον ΓΚΠΔ, πολιτική ιδιωτικότητας στα Πανεπιστήμια.

ABSTRACT

The object of this study is the protection of personal data in Greek universities after the adoption of the General Data Protection Regulation (EU) 2016/679 which entered into force on 25 May 2018. The GDPR recommends the necessary reform of the pre-existing institutional framework of data protection in view of the technological explosion in combination with the regulatory shortcomings of the previous Directive 95/46 / EU and the lack of uniform and coherent implementation within the EU. The strict and bureaucratic institutional framework introduced by the new regulation and the formalistic way of its implementation combined with the severe sanctions it provides for, raises concerns for the public and private bodies of the Member States without leaving any space for divergence in their compliance with its requirements. By giving the Processor a leading role and passing on the responsibility of processing the data to him instead of the supervisory authority, this new "informal hybrid", as it is commonly called the GDPR, strengthens the rights of individuals, based on the basic principles of protection, which are supplemented by the institutionalization of the accountability principle. The Greek implementation Law 4624/2019, passed under the threat of a fine of 2.5 million euros by the EU Court, came to seal the strengthening of personal data protection in the internal legal order. The implementation of the GDPR in conjunction with the complementary measures set by the national legislation, seeks to ensure the lawful processing of huge volume of personal data which are moved within Greek universities and to face the risks that may caused by rapid technological developments. Initially, reference is made to the concept of privacy, a more specific manifestation of which is the protection of personal data. Afterwards comes a review of both international and EU contractual framework for privacy and personal data protection as well, the timing of the institutionalization of the regulation and our national legislation and the Hellenic DPA, cause of the important role it plays under Law 4624/2019 as a supervisory authority and its particular contribution in general. Then follows the analysis of the main provisions of the GDPR and its potential application within Greek universities. In order to determine the degree of compliance of the latter and the degree of GDPR integration in them, an investigation was carried out at the greek universities, which demonstrated the intention and effort of the Administrations of most HEIs to warmly approach the new EU legislation. Finally, conclusions and proposals are

set out in order to ensure compliance in the light of awareness and culture change towards the development of a more human-centered philosophy of personal data law.

Keywords: personal data protection, the General Regulation for the protection of personal data, Hellenic DPA, personal data in universities, HEI's compliance with the GDPR, Privacy Policy in Universities.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΠΙΝΑΚΑΣ ΣΥΝΤΟΜΟΓΡΑΦΙΩΝ

ΑΠΔΠΧ	Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
BCR	Binding Contractual Rules
ΓΚΠΔ	Γενικός Κανονισμός Προστασίας Δεδομένων
CNIL	Commission Nationale de l'Informatique et des Libertés
COPA	Child Online Protection Act
CSV	Comma Separated Values
ΔΕΕ	Δικαστήριο Ευρωπαϊκής Ένωσης
DPIA	Data Protection Impact Assessment
ΕΑΠΔ	Εκτίμηση Αντικτύπου Προσωπικών Δεδομένων
Ε.Ε.	Ευρωπαϊκή Ένωση
ΕΕΟ	Εταιρείες Είσπραξης Οφειλών
ΕΕΠΔ	Ευρωπαίος Επόπτης Προστασίας Δεδομένων
ΕΚΑΝΑ	Εθνικός Κατάλογος Ανεπιθύμητων Αλλοδαπών
ΕΟΧ	Ευρωπαϊκός Οικονομικός Χώρος
ENISA	European Union Agency for Cyber Security
ERP	Enterprise Resource Planning
ΕΣΠΔ	Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων
ΕΣΔΑ	Ευρωπαϊκή Σύμβαση για τα Δικαιώματα του Ανθρώπου
ΕΣΥΔ	Εθνικό Σύστημα Διαπίστευσης
FAQ	Frequently Asked Questions
GDPR	General Data Protection Regulation
GPS	Global Positioning System
Η.Ε.	Ηνωμένα Έθνη
ΗΠΑ	Ηνωμένες Πολιτείες της Αμερικής
JSON	Java Script Object Notation File
IP	Internet Protocol
IT	Information Technology

ΚΕΔΕ	Κώδικας Είσπραξης Δημοσίων Εσόδων
ΜΚΔ	Μέσα Κοινωνικής Δικτύωσης
MOU	Memorandum of Understanding
NIS	Network and Information System
ΝΠΙΔ	Νομικό Πρόσωπο Ιδιωτικού Δικαίου
ΝΠΔΔ	Νομικό Πρόσωπο Δημοσίου Δικαίου
ΟΗΕ	Οργανισμός Ηνωμένων Εθνών
ΟΟΣΑ	Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης
ΟΤΑ	Οργανισμοί Τοπικής Αυτοδιοίκησης
ΠΝΠ	Πράξη Νομοθετικού Περιεχομένου
PNR	Passenger Name Record Data
RFID	Radio Frequency Identification
SCC	Standard Contractual Clauses
Σ.	Σύνταγμα
ΣΔΟΕ	Σώμα Δίωξης Οικονομικού Εγκλήματος
ΣΕΒ	Σύνδεσμος Ελλήνων Βιομηχάνων και Βιοτεχνών
ΣΛΕΕ	Συνθήκη για τη Λειτουργία της Ευρωπαϊκής Ένωσης
ΣΠΣ	Σύστημα Πληροφοριών Σένγκεν
ΥΠΔ	Υπεύθυνος Προστασίας Δεδομένων
ΧΕΑΔ	Χώρος Ελευθερίας, Ασφαλείας και Δικαιοσύνης
ΧΘΔΑ	Χάρτης Θεμελιωδών Δικαιωμάτων Ανθρώπου
UIS	University Information System
UNESCO	United Nations Educational Scientific and Cultural Organisation
WP 29	Work Party 29
XML	Extensible Markup Language

Εισαγωγή

Διανύοντας την 4η φάση της τεχνολογίας (4.0. Industry) και βιώνοντας την εποχή της διάχυτης πληροφορίας και της χρήσης των «έξυπνων» συσκευών (κινητά, gadgets, έξυπνα σπίτια, έξυπνα αυτοκίνητα, έξυπνες κάρτες), το άτομο καλείται να ελέγξει την τύχη των προσωπικών του πληροφοριών που «ταξιδεύουν» με απίστευτη ταχύτητα μέσα στον κυβερνοχώρο. Η κοινωνία της πληροφορίας επέφερε σημαντικές αλλαγές και ανέτρεψε τις κλασσικές μεθόδους επικοινωνίας, διαχείρισης και ελέγχου τόσο στον δημόσιο όσο και στον ιδιωτικό τομέα ενώ οδήγησε στην ανάγκη εκσυγχρονισμού των πληροφοριακών συστημάτων της Δημόσιας Διοίκησης. Η μεταβολή των παραδοσιακών μεθόδων συλλογής και χρήσης της πληροφορίας, κατέστησε τα άτομα -μέσω της χρήσης των νέων τεχνολογιών που προωθούν τη δημιουργία μιας ψηφιακής «εικόνας» γι' αυτά - υποκείμενα χειραγώγησης και εργαλειοποίησης, με αποτέλεσμα να αντιμετωπίζονται περισσότερο ως «αγαθά προς πώληση». Η ταχύτητα διακίνησης των προσωπικών πληροφοριών εγκυμονεί κινδύνους που συχνά οδηγούν σε παραβιάσεις σχετικές με την άσκηση των δικαιωμάτων των υποκειμένων τους και στη μη εφαρμογή του υφιστάμενου θεσμικού πλαισίου προστασίας (Αρκουλή, 2010). Οι ταχείες τεχνολογικές εξελίξεις και η παγκοσμιοποίηση, δημιούργησαν νέες προκλήσεις για την προστασία της ιδιωτικότητας και της προστασίας των προσωπικών δεδομένων -ως ιδιαίτερης έκφανσης της πρώτης- μετά την μετάβαση από την βιομηχανική επανάσταση στην τεχνολογία της πληροφορίας, που αναμφίβολα συνιστά βασικό διακύβευμα του 21ου αιώνα και ανάγεται σε υψίστης σημασίας ζήτημα, που χρήζει άμεσης νομοθετικής διευθέτησης[1].

Προκειμένου να χαλιναγωγηθεί η ραγδαία τεχνολογική έκρηξη και να καλυφθούν τα κενά που δεν μπόρεσε να καλύψει η προϊσχύουσα Οδηγία 95/46/ΕΚ, που συνιστούσε το βασικό νομικό πλαίσιο για την προστασία του θεμελιώδους δικαιώματος των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα, υπεγράφη στις 27 Απριλίου 2016 ένα νέο ευρωπαϊκό νομοθέτημα, ενδεδυμένο αυτή τη φορά με την μορφή ενός άμεσα εφαρμοστέου και νομικά δεσμευτικού κανονισμού, ήτοι ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων, γνωστός και ως GDPR, ο οποίος κατήργησε την παρωχημένη Οδηγία 95/46/ΕΚ, επιδιώκοντας να επιφέρει την ομοιόμορφη και συνεκτική εφαρμογή του σε όλα τα κράτη-μέλη ΕΕ καθιερώνοντας ένα αυστηρό θεσμικό πλαίσιο κανόνων, προκειμένου να θωρακιστεί η ιδιωτικότητα και να μετατεθεί η ευθύνη της

[1] Βλ. Αιτιολ. Σκέψη 3 Οδηγίας (ΕΕ) 2016/680.

επεξεργασίας των προσωπικών πληροφοριών από το υποκείμενο, στον υπεύθυνο επεξεργασίας. Απώτερος στόχος του ήταν η επίτευξη μιας σχέσης ισορροπίας μεταξύ του δικαιώματος της προστασίας των προσωπικών δεδομένων και του δικαιώματος στην πληροφόρηση κατά τρόπο που να εξασφαλίζει τον σεβασμό των δικαιωμάτων, προάγοντας κατ' επέκταση την ελεύθερη και ανεμπόδιστη οικονομική ανάπτυξη και επιχειρηματική δραστηριότητα εν γένει. Οι βασικές αρχές και οι καινοτομίες του κανονισμού, καλούνται να εφαρμοστούν εντός αλλά ως ένα βαθμό και εκτός της Ε.Ε., από υπεύθυνους και εκτελούντες την επεξεργασία, τόσο σε δημόσιους όσο και ιδιωτικούς φορείς που κατ' αρχήν μοιάζουν να αγνοούν την πολυπλοκότητα και τον μηχανισμό του. Η ευαισθητοποίηση και η ενημέρωση γύρω από τα ζητήματα που καλείται να διευθετήσει, συνιστούν άμεσο στόχο των φορέων και οργανισμών, προκειμένου να καταστούν ικανοί να συμμορφωθούν με το νέο κανονιστικό πλαίσιο προστασίας, το οποίο απειλεί με δυσθεώρητα διοικητικά πρόστιμα τις Διοικήσεις τους σε περίπτωση παραβίασης ή μη συμμόρφωσής τους προς τις διατάξεις του.

Δημόσιοι φορείς που καλούνται να υπηρετήσουν το πνεύμα και τις αρχές του ΓΚΠΔ, είναι μεταξύ άλλων και τα ελληνικά πανεπιστήμια, τα οποία καθημερινά διαχειρίζονται πλήθος πληροφοριών του διοικητικού και διδακτικού προσωπικού, των φοιτητών και προμηθευτών τους. Στόχος της παρούσας μελέτης είναι να διερευνήσει ποιες αλλαγές επιφέρει ο νέος κανονισμός στο δίκαιο προστασίας των προσωπικών δεδομένων, πως εφαρμόζεται στα ελληνικά πανεπιστήμια κι εάν αυτά προβαίνουν σε ορισμό Υπευθύνου προστασίας δεδομένων. Περαιτέρω διερευνάται πως προετοιμάζονται οι Διοικήσεις των πανεπιστημίων για τη συμμόρφωση, ποιες διαδικασίες ακολουθούν, ποια μέτρα λαμβάνουν για να αποδείξουν τη συμμόρφωσή τους με τον κανονισμό. Τέλος βασικό ερώτημα προς διερεύνηση είναι το πως αντιλαμβάνονται εν τέλει τα ακαδημαϊκά ιδρύματα την θεσμική μεταρρύθμιση που εισήχθη και αν μπορούν να αναγάγουν τη συμμόρφωση σε ανταγωνιστικό αποτέλεσμα. Η παρούσα μελέτη στηρίζεται κατά κύριο λόγο στη βιβλιογραφική επισκόπηση και στη διερεύνηση της τεκμηρίωσης που συλλέχθηκε από τους επίσημους ιστότοπους των ελληνικών πανεπιστημίων.

Στο πρώτο κεφάλαιο της παρούσας μελέτης αναλύεται κατ' αρχήν η ιδιωτικότητα ως ευρύτερη της προστασίας των προσωπικών δεδομένων έννοια, εν συνεχεία γίνεται αναφορά στο διεθνές και ενωσιακό συμβατικό πλαίσιο που διέπει την προστασία των προσωπικών δεδομένων και στην εξέλιξή τους μέχρι τη θεσμοθέτηση του Γενικού

Κανονισμού. Στο δεύτερο κεφάλαιο γίνεται αναφορά στο ισχύον θεσμικό πλαίσιο προστασίας δεδομένων στην Ελλάδα καθώς και στην ΑΠΔΠΧ. Στο τρίτο κεφάλαιο αναλύεται το πλέγμα των βασικότερων διατάξεων του ΓΚΠΔ. Τέλος στο τέταρτο και τελευταίο κεφάλαιο αναλύεται η εφαρμογή του ΓΚΠΔ στα ελληνικά πανεπιστήμια και η συμμόρφωσή τους με αυτόν.

ΚΕΦΑΛΑΙΟ 1ο: Η ΠΡΟΣΤΑΣΙΑ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΚΑΙ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΕ ΔΙΕΘΝΕΣ ΚΑΙ ΕΝΩΣΙΑΚΟ ΕΠΙΠΕΔΟ

1. Περί της ιδιωτικότητας

Το ζήτημα της ιδιωτικότητας είναι άμεσα συνυφασμένο με την προστασία των προσωπικών δεδομένων. Η αναφορά στην έννοια της ιδιωτικότητας κρίνεται σκόπιμη προκειμένου να γίνει κατανοητή η έννοια και η ανάγκη προστασίας των προσωπικών δεδομένων. Στα πλαίσια μιας καθημερινής ζωής ενός «οικουμενικού ψηφιακού κόσμου» που χαρακτηρίζεται από την κινητικότητα των ατόμων και την γρήγορη και διαρκή διάδοση των δεδομένων του, τίθενται δύσκολα φραγμοί και μηχανισμοί διαφύλαξης της ιδιωτικότητας και του θεμελιώδους δικαιώματος στην ιδιωτική ζωή (Vilela, 2019). Το ζήτημα της προστασίας της ιδιωτικότητας έφερε στο προσκήνιο την ανάγκη δημιουργίας μιας νέας εφαρμοσμένης ηθικής, της «ηθικής των υπολογιστών» (Computer ethics) που προέκυψε όταν οι υπολογιστές αντικατέστησαν τον αναλογικό τρόπο διάδοσης των πληροφοριών με τον ψηφιακό, με αποτέλεσμα την ταχύτατη επεξεργασία τους και την δυσκολία διαχείρισης τους (Maner 1996). Η εφαρμοσμένη «ηθική των υπολογιστών» συνδέθηκε άρρηκτα με την ασφάλεια και την ιδιωτικότητα και αποτέλεσε τον προάγγελο την θεωρίας για την «ηθική της πληροφορίας», όπως αυτή εν τέλει διατυπώθηκε από τον Floridi στα τέλη της δεκαετίας του 1990 (Tavani, 2007).

Στη βιβλιογραφία η ιδιωτικότητα προσεγγίζεται άλλοτε ως *έννοια,* άλλοτε ως *δικαίωμα.* Μια άλλη προσέγγιση (De Cew, 1997) την θεωρεί *όρο συνδεόμενο με πολλά συμφέροντα* αφού καλείται να εξισορροπήσει τα οφέλη της ιδιωτικής ζωής με κείνα της δημόσιας ασφάλειας. Υπό αυτή την έννοια θεωρείται εν γένει *κοινωνικό αγαθό* (Τσαγκανού, 2014) ενώ ορισμένοι την θεωρούν *ως συμφέρον* σχετιζόμενο με κάποιον φορέα ή οργανισμό, προς όφελος του οποίου μπορεί να καμφθεί. Τέλος, μια άλλη προσέγγιση θεωρεί την ιδιωτικότητα *ως ένα είδος περιουσίας* που κατέχει το άτομο και που μπορεί να την διαχειρίζεται εντός της οικονομικής και εμπορικής σφαίρας (Hunter, 1995).

Νομικά η προστασία της ιδιωτικότητας βρίσκει έρεισμα στις αρχές του Wiener που απαντώνται στα σύγχρονα νομοθετικά κείμενα. Ήδη από το 1890 οι Warren & Brandeis αναγνωρίζουν την ιδιωτικότητα ως *δικαίωμα του κοινού δικαίου* και *ως μέσο προστασίας των επιλογών του ατόμου εντός του κοινωνικού πλαισίου*, η δε καθ' οιονδήποτε τρόπο αποκάλυψη της ιδιωτικής ζωής, χωρίς τη συναίνεσή του ατόμου και οι συνέπειες σε

περίπτωση παραβίασής της, συνιστούν προσβολή της αξιοπρέπειας, της ελευθερίας και της ασφάλειας του ατόμου.

Η ιδιωτικότητα διακρίνεται σε *α) φυσική ή σωματική, β) σχετική με την επιλογή και λήψη αποφάσεων, γ) ψυχολογική ή πνευματική* (Regan, 1995) και δ) *πληροφοριακή* (Parent, 1983). Η τελευταία αφορά προσωπικές πληροφορίες του ατόμου σχετικά με την προσωπική, κοινωνική, οικονομική του ζωή, το ιατρικό ιστορικό, τις θρησκευτικές ή πολιτικές του πεποιθήσεις, τα ακαδημαϊκά του προσόντα, και όσες εν γένει πληροφορίες καθίστανται αντικείμενο επεξεργασίας μέσω της χρήσης του διαδικτύου (emails, social media κλπ). Η προστασία της αποτέλεσε αντικείμενο συζήτησης και ενδιαφέροντος ήδη από το 1995, όταν πρωτοεμφανίστηκε η ιδέα της δημιουργίας αρχών προστασίας του απορρήτου μέσω του περιορισμού της διάδοσης ή του χρόνου διατήρησης των προσωπικών δεδομένων καθώς και η περιφρούρηση της ταυτότητας του ατόμου μέσω της ψευδωνυμιοποίησης (ENISA, 2014)[2]. Η *πληροφοριακή ιδιωτικότητα* ανάλογα με το άτομο ή την ιδιότητα, διακρίνεται στις εξής κατηγορίες:

1) *ιδιωτικότητα του καταναλωτή*, η οποία αφορά στις μέσω διαδικτύου συναλλαγές του ατόμου διαμέσου εμπορικών πλατφορμών που με τη χρήση των cookies[3] συλλέγουν προσωπικά δεδομένα.
2) *ιδιωτικότητα στην υγεία* (άλλως ιατρική), η οποία αναφέρεται στην προστασία του ιατρικού ιστορικού και των δεδομένων του ατόμου, τα οποία αντλούνται μέσω επαναλαμβανόμενων μοτίβων (data mining), με αποτέλεσμα να γίνεται ταυτοποίηση του ασθενή μέσα από τον συνδυασμό των στοιχείων του και την μετέπειτα ομαδοποίησή του (Vedder, 2004).

[2] Κάθε αναφορά περί ιδιωτικότητας στην παρούσα μελέτη, αφορά στην πληροφοριακή ιδιωτικότητα.
[3] Τα cookies είναι μικρά αρχεία κειμένου που αποστέλλονται μέσω μιας ιστοσελίδας προκειμένου να ανακτήσουν πληροφορίες. Χρησιμοποιούνται συνήθως για την α) αποτελεσματικότερη λειτουργία των ιστοτόπων που επιτυγχάνεται με την αποθήκευση των προτιμήσεων του χρήστη, β) για να παρακολουθείται η περιήγηση του χρήστη στο διαδίκτυο, να δημιουργούν προφίλ και να παρέχουν στοχευμένη διαφήμιση βάσει των προτιμήσεων του χρήστη για προωθητικούς σκοπούς. Διακρίνονται σε *προσωρινά (session cookies)*, τα οποία διαγράφονται μετά το πέρας της περιήγησης ή μετά το κλείσιμο του browser και σε *μόνιμα (persistent cookies),* τα οποία παραμένουν στο σκληρό δίσκο του υπολογιστή ή στη συσκευή μέχρι να διαγραφούν από τον ίδιο το χρήστη ή μέχρι να παρέλθει το προκαθορισμένο βάσει του κώδικα cookie χρονικό διάστημα. Επίσης υπάρχουν και τα *απολύτως απαραίτητα cookies* τα οποία είναι ουσιαστικής σημασίας για την ορθή λειτουργία ενός ιστοτόπου και τεχνικά απαραίτητα για την πραγματοποίηση της σύνδεσης σε συγκεκριμένο ιστότοπο, για τη χρήση των οποίων δεν απαιτείται η προηγούμενη αίτηση και λήψη συγκατάθεσης. Βλ. σχετικά ΓΚΠΔ: Οι νέοι κανόνες για την προστασία των δεδομένων και της ιδιωτικής ζωής στο διαδίκτυο διαθέσιμο σε https://www.lawspot.gr/nomikes-plirofories/voithitika-kemena/gkpd-oi-neoi-kanones-gia-tin-prostasia-ton-dedomenon-kai-tis

3) *ιδιωτικότητα της τοποθεσίας*, η οποία σχετίζεται με τις σύγχρονες φορητές συσκευές (smart phones, tablets κ.α.) που λόγω του αναμεταδότη που φέρουν επάνω τους, εκπέμπουν τη θέση της συσκευής και κατ' επέκταση του ατόμου, παρέχοντας ουσιαστικά διαρκώς πληροφορίες, οδηγίες ή προτάσεις βάσει του εντοπισμού της θέσης του.
4) *ιδιωτικότητα του εργαζομένου,* η οποία έχει να κάνει με τα προσωπικά δεδομένα - απλά και ευαίσθητα – των υποψήφιων ή ήδη εργαζομένων σε μια επιχείρηση ή οργανισμό, τα οποία συλλέγονται είτε κατά τη διαδικασία της πρόσληψής τους για λόγους ασφαλείας είτε κατά τη διάρκεια της απασχόλησής τους προς εξακρίβωση των συμβατικών τους υποχρεώσεων. Η ψηφιακή ή ηλεκτρονική παρακολούθηση των εργαζομένων πραγματώνεται μέσω της καταγραφής των δεδομένων τους από το εταιρικό λογισμικό (κλήσεις, emails, τοποθεσία, πλοήγηση σε ιστότοπους). Θεωρείται *δεδομένη και εν μέρει νόμιμη* καθώς -υπό τον μανδύα της συγκατάθεσης των εργαζομένων- επιτρέπει πέρα από τη συλλογή και αποθήκευση και την επεξεργασία πολλών προσωπικών τους δεδομένων σε δεύτερο χρόνο[4], γεγονός που καταδεικνύει ότι στο όνομα την εξασφάλισης της βιωσιμότητας και ανταγωνιστικότητας μιας επιχείρησης, θίγεται καταφανώς η ιδιωτικότητα του ατόμου.
Ωστόσο, ο έλεγχος του ατόμου προσκρούσει σε πολλές θεμελιώδεις αξίες, όπως είναι η αυτονομία, η ιδιωτικότητα και η ανθρώπινη αξιοπρέπεια, οι οποίες είναι πρωταρχικές στην Ε.Ε.. Οι O' Hara *et al, (*2004) υποστήριξαν ότι απαραίτητη προϋπόθεση για να εξασφαλιστεί η κοινωνική συνοχή είναι η αποκατάσταση της σχέσης εμπιστοσύνης με τους θεσμούς και το μέσο επίτευξής αυτού είναι η διαμόρφωση μιας οικουμενικής ψηφιακής κουλτούρας που να βασίζεται σε καίριες νομοθετικές ρυθμίσεις για την ασφάλεια, εκπαίδευση και συνεργασία μεταξύ οργανισμών και ατόμων. Η σύγχρονη διαπολιτισμική κοινωνία που διαπνέεται από σεβασμό, αλληλεπίδραση και συνύπαρξη περισσοτέρων πολιτισμικών στοιχείων, υπαγορεύει τη δημιουργία ενός παγκόσμιου κώδικα ηθικής γύρω από το υπό κρίση ζήτημα (Gotterbarn & Miller, 2017).

Ως εκ τούτου η προστασία της πληροφοριακής ιδιωτικότητας του ατόμου κατά την προαναφερθείσα έννοια και η ύπαρξη ενός στιβαρού θεσμικού πλαισίου μέσα στη δίνη της ραγδαίας τεχνολογικής εξέλιξης συνιστούσε επιτακτική ανάγκη.

[4] Οι πιο προηγμένες τεχνολογικά και πιο εξοικειωμένες με την κοινωνία ελέγχου χώρες, όπως λ.χ. η Σουηδία, έχουν εισαγάγει την εποπτεία μέσω βιομετρικών δεδομένων (δακτυλικό αποτύπωμα, υποδόρια τοποθέτηση πομπού ανίχνευσης κ.λ.π.) ως μέσο ελέγχου της ώρας προσέλευσης στον εργασιακό χώρο ή έγκρισης πρόσβασης σε εργασιακούς τομείς. Για το τι συνιστά βιομετρικά δεδομένα βλ. μεταξύ άλλων Τσιπτσέ & Κωστούλας, 2020.

2. Το διεθνές συμβατικό πλαίσιο για την προστασία της ιδιωτικότητας και των προσωπικών δεδομένων

Η προστασία της ιδιωτικότητας απασχόλησε από νωρίς το διεθνή νομοθέτη. Το δικαίωμα στην ιδιωτική ζωή συνιστά ένα από τα πλέον πρωταρχικά και θεμελιώδη δικαιώματα του ανθρώπου, το οποίο κινδυνεύει διαρκώς λόγω της ραγδαίας τεχνολογικής ανάπτυξης. Ήδη από το 1948 η Οικουμενική Διακήρυξη των Ανθρωπίνων Δικαιωμάτων των ΗΕ[5] και λίγο αργότερα, το 1950, η ΕΣΔΑ[6] το συμπεριέλαβαν στη λίστα με τα διεθνώς κατοχυρωμένα ανθρώπινα δικαιώματα, τακτική που ακολούθησαν και τα περισσότερα φιλελεύθερα συνταγματικά κείμενα πολλών κρατών.

Το δίκαιο της προστασίας των προσωπικών δεδομένων έχει ως αντικείμενο την προστασία του ατόμου από τους κινδύνους που προκαλούνται από την επεξεργασία τους (Ιγλλεζάκης, 2004). Το δικαίωμα αυτό, άλλως *δικαίωμα πληροφοριακού αυτοκαθορισμού*, συνιστά σχετικά νέο δικαίωμα που εμφανίστηκε στη δεκαετία του 1980, αν και νομοθετικά κατοχυρώθηκε μόλις στα μέσα της δεκαετίας του 1990. Τα νομοθετήματα που αφορούν την προστασία των δεδομένων διακρίνονται σε πρώτης, δεύτερης και τρίτης γενιάς (Αλεξανδροπούλου- Αιγυπτιάδου, 2016) και αποδεικνύουν την ύπαρξη της ανάγκης δημιουργίας ενός προστατευτικού πλέγματος για την ιδιωτικότητα, με την υιοθέτηση εξειδικευμένων ρυθμίσεων. Παράλληλα, καταδεικνύουν την ανησυχία του νομοθέτη αναφορικά με την επεξεργασία των δεδομένων, γεγονός που τον ώθησε στη θεσμοθέτηση του αυστηρού ελέγχου και των σημαντικών κυρώσεων.

Τα *νομοθετήματα πρώτης γενιάς* ανατρέχουν χρονικά στις αρχές της δεκαετίας του 1970, οπότε σωρεία νομοθετικών κειμένων θεσπίστηκαν για πρώτη φορά στην εσωτερική έννομη τάξη τόσο των ευρωπαϊκών κρατών[7] όσο και των ΗΠΑ[8]. Το 1980 ο ΟΟΣΑ υπήρξε

[5] Άρθρο 12 Οικουμενικής Διακήρυξης: *«Κανείς δεν επιτρέπεται να υποστεί αυθαίρετες επεμβάσεις στην ιδιωτική του ζωή, την οικογένεια, την κατοικία ή την αλληλογραφία του, ούτε προσβολές της τιμής και της υπόληψής του. Καθένας έχει το δικαίωμα να τον προστατεύουν οι νόμοι από επεμβάσεις και προσβολές αυτού του είδους»*

[6] Άρθρο 8 ΕΣΔΑ θεσπίζει το δικαίωμα σεβασμού της ιδιωτικής και οικογενειακής ζωής προβλέποντας ότι: *«Παν πρόσωπο δικαιούται εις τον σεβασμό της ιδιωτικής και οικογενειακής ζωής του, της κατοικίας του και της αλληλογραφίας του».* Η νομολογία του Ευρωπαϊκού Δικαστηρίου των Δικαιωμάτων του Ανθρώπου έχει αποφανθεί ότι πληροφορίες που αποθηκεύονται σε clouds και αφορούν την υγεία, την εθνική ταυτότητα, τη φυλετική καταγωγή, το δικαίωμα του ατόμου στην εικόνα του, τα βιομετρικά δεδομένα του (π.χ. DNA, προφίλ ή δακτυλικά αποτυπώματα), εμπίπτουν στην έννοια του άρθρου αυτού και χαίρουν προστασίας κατ' αναλογική εφαρμογή της εν λόγω διάταξης.

[7] Ο πρώτος νόμος για την Προστασία των προσωπικών δεδομένων καταγράφεται στο γερμανικό ομοσπονδιακό κρατίδιο της Έσσης. Η γερμανική νομοθεσία διαπνέεται από την αρχή της διαφάνειας με

ο πρώτος οργανισμός σε διεθνές επίπεδο που ασχολήθηκε με το ζήτημα της προστασίας των δεδομένων, εκδίδοντας Κατευθυντήριες Γραμμές «για την προστασία της προσωπικής σφαίρας του ανθρώπου και τις διασυνοριακές ροές προσωπικών στοιχείων» (Γέροντας, 2002), το παράδειγμα του οποίου ακολούθησε μια δεκαετία αργότερα και ο ΟΗΕ.

Τα *νομοθετήματα δεύτερης γενιάς*, εμφανίστηκαν τη δεκαετία του 1980 με μια διαφορετική προσέγγιση που συνίσταται στο ότι η πληροφορία μπορεί να αποτελεί πλέον σύμμαχο στην ανάπτυξη (Γέροντα, 2002). Η εν λόγω προσέγγιση είχε ως κεντρικό προβληματισμό τη σύγκρουση του δικαιώματος προστασίας της ιδιωτικής ζωής έναντι εκείνου της πληροφορίας. Έτσι στις 28 Ιανουαρίου 1981 το Συμβούλιο της Ευρώπης υπέγραψε στο Στρασβούργο τη Διεθνή Σύμβαση 108 *«για την προστασία του ατόμου έναντι της αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα»*, που ουσιαστικά αποτελεί και την πρώτη νομικά δεσμευτική, σε ευρωπαϊκό επίπεδο, πράξη για την προστασία των δεδομένων. Η εν λόγω Σύμβαση τέθηκε σε ισχύ την 1^{η} Οκτωβρίου 1985, οπότε και υπεγράφη και κυρώθηκε από πέντε ευρωπαϊκά κράτη[9] και, αν και στερούταν άμεσης εφαρμογής, πέτυχε να επιδράσει θετικά στις εθνικές έννομες τάξεις. Η χώρα μας την υπέγραψε στις 17 Φεβρουαρίου 1983 και την κύρωσε με το Ν. 2068/1992 (ΦΕΚ Α' 118) ενώ τέθηκε σε ισχύ μόλις την 1-12-1995 δυνάμει της ανακοίνωσης Φ0546/4173/19-9-1995 (ΦΕΚ Α' 207). Στα πλαίσια της 128^{ης} Συνόδου (17-18 Μαϊου 2018) της Επιτροπής των Υπουργών στο Έλσινορ της Δανίας, η εν λόγω Σύμβαση επικαιροποιήθηκε και μετονομάστηκε σε *«Σύμβαση για την Προστασία των Ατόμων από την Επεξεργασία Προσωπικών Δεδομένων»*[10].

Στα νομοθετήματα δεύτερης γενιάς ανήκουν και οι Κατευθυντήριες Γραμμές του ΟΗΕ αλλά και η Συνθήκη Σένγκεν που υπεγράφη στις 14-06-1985[11]και δημιούργησε μια κοινή βάση εθνικών δεδομένων στα κράτη μέλη, αποσκοπώντας στην ελεύθερη κυκλοφορία των

την έννοια του ελέγχου εκ μέρους του πολίτη, την ενημέρωσή του για την τήρηση των δεδομένων του από τις δημόσιες υπηρεσίες ή αρχές και το δικαίωμα διαγραφής.

[8] Στις ΗΠΑ ο πρώτος νόμος για την προστασία της ιδιωτικότητας ήταν η Privacy Act 1974. Ακόμη και σήμερα δεν υφίσταται ενιαίο νομοθετικό πλαίσιο για την προστασία τους αλλά έχουν θεσπιστεί εκατοντάδες νόμοι σε πολιτειακό και ομοσπονδιακό επίπεδο καθώς και επιμέρους τομεακές νομοθεσίες προστασίας των δεδομένων.

[9] Βλ. Προστασία των δεδομένων προσωπικού χαρακτήρα, διαθέσιμο σε : https://www.europarl.europa.eu/ftu/pdf/el/FTU_4.2.8.pdf

[10] Διαθέσιμη σε: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf

[11] Η εν λόγω Συνθήκη κυρώθηκε στη χώρα μας με το Ν.2514/1997.

υπηκόων των κρατών μελών που την υπέγραψαν, και στην αστυνομική και δικαστική συνεργασία[12].

3. Το ενωσιακό δίκαιο για την προστασία των προσωπικών δεδομένων

Σε επίπεδο πρωτογενούς ενωσιακού δικαίου η υπογραφή της Συνθήκης της Λισαβόνας σηματοδοτεί την εποχή των *νομοθετημάτων τρίτης γενιάς* και κατοχυρώνει πλέον ρητά το δικαίωμα στα προσωπικά δεδομένα. Μέχρι να τεθεί αυτή σε ισχύ, η νομοθεσία για την προστασία των δεδομένων στον χώρο ελευθερίας, ασφάλειας και δικαιοσύνης (ΧΕΑΔ) διακρινόταν ανάμεσα στον πρώτο πυλώνα (προστασία δεδομένων για προσωπικούς και εμπορικούς σκοπούς με τη χρήση της κοινοτικής μεθόδου) και στον τρίτο (προστασία των δεδομένων για σκοπούς επιβολής του νόμου σε διακυβερνητικό επίπεδο), διάκριση που εγκαταλείφθηκε με τη Συνθήκη της Λισαβόνας, προς εξασφάλιση μιας πιο στέρεης βάσης κι ενός πιο αποδοτικού συστήματος προστασίας των δεδομένων. Έτσι η ΣΛΕΕ αναγορεύει στο άρθρο 16[13] την προστασία των προσωπικών δεδομένων σε προστατευόμενο δικαίωμα ενώ ο Χάρτης των Θεμελιωδών Δικαιωμάτων της Ε.Ε. στο άρθρο 7[14] αναγνωρίζει τον σεβασμό της ιδιωτικής και οικογενειακής ζωής, ειδικότερη έκφανση της οποίας συνιστά η προστασία των δεδομένων προσωπικού χαρακτήρα που κατοχυρώνεται στο άρθρο 8[15] και είναι άρρηκτα συνδεδεμένο με αυτήν δικαίωμα αλλά ταυτόχρονα θεμελιώδες και ξεχωριστό δικαίωμα (Αποστολόπουλος, 2020)[16]. Μάλιστα η παρ.2 της ίδιας διάταξης

---

[12] Βλ. σχετικά: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=LEGISSUM%3Al33020.

[13] Το Άρθρο 16 ΣΛΕΕ, το οποίο διαδέχθηκε το άρθρο 286 ΣΕΚ ,έχει ως εξής :
«1. Κάθε πρόσωπο έχει δικαίωμα προστασίας των δεδομένων προσωπικού χαρακτήρα που το αφορούν. 2. Το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο, αποφασίζοντας σύμφωνα με τη συνήθη νομοθετική διαδικασία, θεσπίζουν τους κανόνες σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης, καθώς και από τα κράτη μέλη κατά την άσκηση δραστηριοτήτων που εμπίπτουν στο πεδίο εφαρμογής του δικαίου της Ένωσης, και σχετικά με την ελεύθερη κυκλοφορία των δεδομένων αυτών…».

[14] Άρθρο 7 Χάρτη Θεμελιωδών Δικαιωμάτων - Σεβασμός της ιδιωτικής και οικογενειακής ζωής
«Κάθε πρόσωπο έχει δικαίωμα στο σεβασμό της ιδιωτικής και οικογενειακής ζωής του, της κατοικίας του και των επικοινωνιών του».
βλ. Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης 2012/C 326/02, διαθέσιμος σε https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:12012P/TXT&from=EN

[15] Άρθρο 8 Χάρτη Θεμελιωδών Δικαιωμάτων- Προστασία των δεδομένων προσωπικού χαρακτήρα «*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 δικαιούται να έχει πρόσβαση στα συλλεγέντα δεδομένα που το αφορούν και να επιτυγχάνει τη διόρθωσή τους.3. Ο σεβασμός των κανόνων αυτών υπόκειται στον έλεγχο ανεξάρτητης αρχής*.», ομοίως διαθέσιμο ως ανωτέρω.

[16] Η προστασία των δεδομένων προσωπικού χαρακτήρα ως ένα θεμελιώδες δικαίωμα των πολιτών της Ευρωπαϊκής Ένωσης, διαθέσιμο σε : https://www.ethemis.gr/2020/06/12/

κάνει μνεία για το σύννομο της επεξεργασίας των δεδομένων αναγνωρίζοντας για πρώτη φορά δικαιώματα για την προστασία τους (πρόσβασης και διόρθωσης).

Περαιτέρω ο ευρωπαίος νομοθέτης ήδη από τα μέσα της δεκαετίας του 1990, έστρεψε το ενδιαφέρον του στην έκδοση νομοθετικών πράξεων[17]. Έτσι σε επίπεδο παράγωγου ενωσιακού δικαίου εκδόθηκε *η Οδηγία 95/46/ΕΚ περί προστασίας των προσωπικών δεδομένων*[18] που συνιστά κατ' ουσία την πρώτη βασική νομική πράξη της ΕΕ, που είχε ως στόχο της να εισαγάγει ένα ολοκληρωμένο θεσμικό πλαίσιο για την προστασία των δεδομένων προσωπικού χαρακτήρα, θέτοντας για πρώτη φορά τις προϋποθέσεις της σύννομης επεξεργασίας των προσωπικών δεδομένων, καθορίζοντας δικαιώματα για τα υποκείμενα των δεδομένων και θεσμοθετώντας την σύσταση ανεξάρτητων αρχών ελέγχου στα κράτη μέλη. Η εφαρμογή της Οδηγίας κατέστη υποχρεωτική για τα κράτη-μέλη της Ε.Ε. και για τα κράτη του ΕΟΧ, αναφορικά με την προστασία των δεδομένων στον τομέα της εσωτερικής αγοράς αλλά όχι επί ζητημάτων αστυνομικής ή δικαστικής συνεργασίας σε ποινικές υποθέσεις (π.χ. εγκλήματα στον Κυβερνοχώρο, καταπολέμηση της τρομοκρατίας και του διασυνοριακού εγκλήματος).

Το άρθρο 32 παρ. 1 της Οδηγίας 95/46/ΕΚ έδινε στα κράτη-μέλη τρία χρόνια προθεσμία έτσι ώστε ουσιαστικά να προσαρμόσουν μέχρι τον Οκτώβριο του 1998 την εθνική τους νομοθεσία. Η χώρα μας την ενσωμάτωσε στην εσωτερική έννομη τάξη με το Ν. 2472/1997 (ΦΕΚ Α' 50), ο οποίος θεωρήθηκε ότι αντιμετώπισε το ζήτημα της προστασίας υπό μια μάλλον μαξιμαλιστική προσέγγιση σε σχέση με την ίδια την Οδηγία, υποδηλώνοντας την ακτιβιστική διάθεση και τον έκδηλο ενθουσιασμό της περιόδου θέσπισής της, έναντι της ελεύθερης πρόσβασης στην πληροφορία, παρά την σαφή πρόθεση των σύγχρονων ευρωπαϊκών νομοθεσιών να αντιμετωπίζουν ως ισοδύναμα[19] τα δύο θεμελιώδη δικαιώματα (προστασία προσωπικών δεδομένων και ελευθερία τύπου (Παναγοπούλου-Κουτνατζή, 2017)[20].

[17] https://www.lawspot.gr/nomika-nea/prosopika-dedomena-syllogi-nomologias-apo-dikastirio-tis-eyropaikis-enosis

[18] Διαθέσιμη σε https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A31995L0046

[19] Στην εσωτερική μας έννομη τάξη και σύμφωνα με τις συνταγματικές επιταγές, όλα τα συνταγματικά κατοχυρωμένα ατομικά δικαιώματα, είναι ισοδύναμα έχοντας την ίδια τυπική ισχύ και χωρίς κάποιο να υπερισχύει έναντι άλλου (Δαγτόγλου,2012).

[20] Αντίθετα η αμερικανική νομοθεσία προωθεί την υπεροχή της ελευθερίας του τύπου έναντι άλλων ζωτικής φύσεως δικαιωμάτων. Στις ΗΠΑ η ελευθερία του λόγου προστατεύεται συνταγματικά ως ύψιστο έννομο αγαθό επί τη βάσει της Πρώτης Τροποποίησης του Αμερικανικού Συντάγματος, η οποία κάμπτεται

4. Η εξέλιξη του παράγωγου ενωσιακού θεσμικού πλαισίου – Το χρονικό της θεσμοθέτησης των δύο νέων Κανονισμών

Παρά το γεγονός ότι πολλά κράτη της Ε.Ε. έσπευσαν να υιοθετήσουν την Οδηγία 95/46/ΕΚ, αυτή δεν κατάφερε να εφαρμοστεί πλήρως σε πρακτικό επίπεδο αφού, όπως προαναφέρθηκε, δεν μπόρεσε να τιθασεύσει τις ραγδαία εξελισσόμενες νέες τεχνολογίες. Περαιτέρω η ίδια η φύση της ως κείμενο στερούμενο νομικής δεσμευτικότητας[21] και κατ' επέκταση μη δυναμένο να εξασφαλίσει ομοιόμορφη και συνεκτική εφαρμογή σε ευρωπαϊκό επίπεδο, αφόπλισε την ενιαία εφαρμογή της. Αναμφίβολα το θεσμικό πλαίσιο είχε κενά που έπρεπε επειγόντως να καλυφθούν από νεότερα, εκσυγχρονισμένα ενωσιακού δικαίου κείμενα.

Έτσι στις 18-12-2000 το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο εξέδωσαν τον Κανονισμό (ΕΚ) 45/2001, με σκοπό να διασφαλιστεί η συνεκτική και ομοιόμορφη εφαρμογή των κανόνων προστασίας των δεδομένων στο σύνολο των Κοινότητας και η ελεύθερη κυκλοφορία των προσωπικών δεδομένων μεταξύ των κρατών μελών και οργάνων και οργανισμών της Κοινότητας (Ιγγλεζάκης, 2008).

Το 2002 εκδόθηκε η Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (Οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες), η οποία κατ' ουσία συμπλήρωνε την Οδηγία 95/46/ΕΚ, εναρμονίζοντας τις διατάξεις της νομοθεσίας των κρατών μελών για την προστασία της ιδιωτικής ζωής σε σχέση με την επεξεργασία των δεδομένων στον τομέα αυτό. Η εν λόγω οδηγία τροποποιήθηκε από την Οδηγία 2009/136/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Νοεμβρίου 2009, ενώ υπό εξέταση τελούσε κι η νέα πρόταση κανονισμού για τον σεβασμό της ιδιωτικής ζωής και την προστασία των προσωπικών δεδομένων στις ηλεκτρονικές επικοινωνίες και την κατάργηση της οδηγίας 2002/58/ΕΚ.

σε εξαιρετικές περιπτώσεις, όπως π.χ. όταν πρόκειται για την Διαδικτυακή Προστασία των Παιδιών, που προστατεύεται με το Νόμο του 1998 (Child Online Protection Act 1998 – COPA).

[21] Υπενθυμίζεται ότι βάσει του άρθρου 288 παρ.3 ΣΛΕΕ η Οδηγία δεν είναι δεσμευτική. Δεσμευτικό είναι το επιδιωκόμενο αποτέλεσμα, γεγονός που υποδεικνύει εν μέρει τη δεσμευτικότητά της ενώ σηματοδοτεί την μη δεσμευτική εφαρμογή για τους αποδέκτες της.

Περαιτέρω, και εντός του πλαισίου του χώρου ελευθερίας, ασφάλειας και δικαιοσύνης, εκδόθηκε η απόφαση-πλαίσιο 2008/977/ΔΕΥ, η οποία ρύθμιζε έως τον Μάιο του 2018, την προστασία των δεδομένων προσωπικού χαρακτήρα στους τομείς της αστυνομικής και δικαστικής συνεργασίας σε ποινικές υποθέσεις και η οποία αποτέλεσε και τον προάγγελο της πρόσφατης σχετικά Οδηγίας (ΕΕ) 2016/680 για την προστασία των εν λόγω δεδομένων επί ποινικών αποφάσεων[22].

Το Δεκέμβριο του 2009, μετά την ολοκλήρωση του προγράμματος του Τάμπερε (τον Οκτώβριο 1999) και της Χάγης (το Νοέμβριο 2004), το Ευρωπαϊκό Συμβούλιο ενέκρινε το πολυετές πρόγραμμα που αφορούσε τον χώρο της ελευθερίας, ασφάλειας και δικαιοσύνης για την περίοδο 2010-2014, γνωστό ως *Πρόγραμμα της Στοκχόλμης*, στα συμπεράσματα του οποίου τέθηκαν οι στρατηγικές κατευθυντήριες γραμμές του νομοθετικού και επιχειρησιακού του προγραμματισμού που μεταξύ άλλων αναφέρονταν στην ορθότερη αντιμετώπιση του ζητήματος προστασίας των δεδομένων προσωπικού χαρακτήρα[23]. Στα πλαίσια της προσπάθειας αυτής η Ε.Ε. εξέδωσε στις 27-4-2016 δύο σπουδαία νομοθετήματα, ήτοι: α) τον Ευρωπαϊκό Κανονισμό (ΕΕ) 2016/679 που αφορά στην *«Προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων»* (Γενικό Κανονισμό για την Προστασία Δεδομένων – General Data Protection Regulation), γνωστό και ως GDPR (ΓΚΠΔ) και β) την Οδηγία (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, *«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»* (άλλως Οδηγία για την προστασία των δεδομένων στον τομέα της επιβολής του νόμου ή Οδηγία LED), που τέθηκαν αμφότερα σε ισχύ τον Μάιο του 2018[24].

[22] https://www.lawspot.gr/nomika-nea/prosopika-dedomena-syllogi-nomologias-apo-dikastirio-tis-eyropaikis-enosis

[23] https://www.europarl.europa.eu/ftu/pdf/el/FTU_4.2.8.pdf

[24] Η Οδηγία αυτή εφαρμόζεται από τις εισαγγελικές, δικαστικές και εν γένει διωκτικές αρχές και διασφαλίζει το θεμελιώδες δικαίωμα των πολιτών για προστασία των δεδομένων προσωπικού χαρακτήρα που χρησιμοποιούνται από εθνικές αρχές επιβολής του νόμου (Ελληνική Αστυνομία, Λιμενικό Σώμα, Ελληνική Ακτοφυλακή, Ειδική Γραμματεία του ΣΔΟΕ) και εν μέρει στις δραστηριότητες των εθνικών δικαστικών αρχών. Στόχος της είναι να εξασφαλίσει ένα ελάχιστο επίπεδο προστασίας των προσωπικών δεδομένων των θυμάτων, μαρτύρων και υπόπτων εγκλήματος και να διευκολύνει τη διασυνοριακή

Περαιτέρω εκδόθηκε και η συμπληρωματική Οδηγία 2016/681/ΕΕ *«σχετικά με τη χρήση δεδομένων που περιέχονται στις καταστάσεις επιβατών (PNR) για την πρόληψη, ανίχνευση, διερεύνηση και δίωξη τρομοκρατικών και σοβαρών εγκλημάτων»* ενώ δύο χρόνια αργότερα καταργήθηκε ο προαναφερόμενος κανονισμός (ΕΚ) 45/2001 και αντικαταστάθηκε από τον κανονισμό (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 23ης Οκτωβρίου 2018 *«για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης και την ελεύθερη κυκλοφορία των δεδομένων αυτών και για την κατάργηση του κανονισμού (ΕΚ) αριθ. 45/2001 και της απόφασης αριθ. 1247/2002/ΕΚ*», ο οποίος τέθηκε σε ισχύ στις 11 Δεκεμβρίου του 2018 (γνωστός ως Κανονισμός για την επεξεργασία δεδομένων προσωπικού χαρακτήρα από θεσμικά όργανα και οργανισμούς της Ένωσης).

Επιπλέον, παράλληλα με τον Κανονισμό, ξεκίνησε το Μάιο του 2018 και η υποχρέωση συμμόρφωσης των κρατών-μελών με την Οδηγία 1148/2016 *«για τα μέτρα ασφαλείας συστημάτων δικτύου και πληροφοριών»* (Network and Information Systems - NIS), στο πλαίσιο μιας ολοκληρωμένης ευρωπαϊκής πολιτικής για την κυβερνοασφάλεια [25] ενώ μετά το σκάνδαλο Facebook-Cambridge Analytica[26], που αποτέλεσε το έναυσμα για τη θέσπιση και του ΓΚΠΔ, επίκειτο η έκδοση του Κανονισμού e-privacy, που αποτελεί βασικό κομμάτι της μεταρρύθμισης του πλαισίου προστασίας των προσωπικών δεδομένων[27] και καταδεικνύει την προσδοκία ο νέος κανονισμός να συν-διαμορφώσει με τον ΓΚΠΔ το νέο

συνεργασία μεταξύ κρατών στον αγώνα κατά του εγκλήματος και της τρομοκρατίας. Η οδηγία αυτή που κατά τον Χελιουδάκη (2018) αποκαλείται ως «η μικρή αδερφή του ΓΚΠΔ» αποτελεί σημαντικότατο νομοθέτημα και λειτουργεί συμπληρωματικά με τον ΓΚΠΔ, βλ. σχετικά σε : www.homodigitalis.gr/posts/2373. Από την θέση της σε ισχύ κατήργησε την Απόφαση Πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου της 27ης Νοεμβρίου 2008 καθώς η τελευταία θεωρήθηκε ότι έθετε ένα φτωχό νομοθετικό πλαίσιο, είχε ιδιαίτερα περιορισμένο πεδίο εφαρμογής και δεν κατάφερε να εξασφαλίσει την ισορροπία ανάμεσα στα δικαιώματα των προσώπων και τις ανάγκες των αρχών επιβολής του νόμου.

[25] https://www.sev.org.gr/Uploads/Documents/51628/meleti_sev_GDPR_final.pdf

[26] Αποτελεί μια από τις πιο γνωστές υποθέσεις που έλαβαν χώρα το 2018, όταν η βρετανική εταιρία ανάλυσης πολιτικών δεδομένων Cambridge Analytica ανακοίνωσε ότι απέκτησε κατά λάθος δεδομένα 10.000.000 χρηστών του Facebook, χωρίς τη συγκατάθεσή τους, τα οποία εν συνεχεία χρησιμοποίησε για να επηρεάσει την έκδοση πολιτικής απόφασης σχετικά με την προεδρική εκλογή του Ντόναλντ Τραμπ στις ΗΠΑ, βλ. σχετικά Wong, J.C. (22-03-2019), Facebook acknowledges concerns over Cambridge Analytica emerged earlier than reported, διαθέσιμο σε : https://www.theguardian.com/uk-news/2019/mar/21/facebook-knew-of-cambridge-analytica-data-misuse-earlier-than-reported-court-filing και Cambridge Analytica statement of the Article 29 Chair διαθέσιμο σε: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=617458

[27] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_20201119_eprivacy_regulation_el.pdf

ψηφιακό περιβάλλον, αποτελώντας lex specialis σε σχέση με αυτόν κι εξειδικεύοντας ορισμένα σημεία του, ως προς τα οποία θα υπερισχύουν έναντι του τελευταίου[28].

Εκτός από τους κανονισμούς και τις οδηγίες, το νομοθετικό οπλοστάσιο της Ε.Ε. συμπληρώθηκε και εξακολουθεί να συμπληρώνεται από αποφάσεις και κανονιστικές πράξεις του Ευρωπαίου Επόπτη Προστασίας Δεδομένων (ΕΕΠΔ)[29] αλλά και από αποφάσεις και οδηγίες των Εποπτικών Αρχών[30] (Τσιπτσέ & Κωστούλας, 2020) ενώ σε υψίστης σημασίας ερμηνευτικό εργαλείο αναδείχθηκαν και οι Οδηγίες της Ομάδας Εργασίας του άρθρου 29 (Work Party -WP 29)[31]. Η WP 29 υπήρξε η ανεξάρτητη ευρωπαϊκή ομάδα εργασίας που πρωτοασχολήθηκε με ζητήματα σχετικά με την προστασία της ιδιωτικής ζωής και των προσωπικών δεδομένων από το 1995 και μετά. Η δράση της που συνίστατο κυρίως στο να γνωμοδοτεί και δη επί σημαντικών ζητημάτων που αφορούν στην προστασία δεδομένων σε χώρες εκτός Ε.Ε. (Αρμαμέντο & Σωτηρόπουλος, 2005), να εκδίδει Κατευθυντήριες Γραμμές, γνωστές ως «Guidelines» εκτείνεται χρονικά έως τις 25 Μαΐου 2018[32], ημερομηνία κατά την οποία τέθηκε σε ισχύ ο ΓΚΠΔ, οπότε και έπαψε να ισχύει με αυτή τη μορφή και μετεξελίχθηκε στο σημερινό Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (ΕΣΠΔ) (European Data Protection Board-EBDP)[33] [34], το οποίο

[28] Για e-privacy βλ. σχετικά σε https://www.lawspot.gr/nomika-nea/eprivacy-ti-provlepei-neo-shedio-toy-kanonismoy-gia-tis-ilektronikes-epikoinonies. Περαιτέρω βλ. Δήλωση σχετικά με τον κανονισμό για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες και τον μελλοντικό ρόλο των εποπτικών αρχών και του ΕΣΠΔ (19-11-2020), διαθέσιμο σε: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_20201119_eprivacy_regulation_el.pdf

[29] Ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων (εφεξής ΕΕΠΔ) (European Data Protection Supervisor – EDPS) αποτελεί μια ανεξάρτητη εποπτική αρχή που επιτηρεί την τήρηση των υποχρεώσεων των οργάνων και οργανισμών της Ε.Ε. για την προστασία των προσωπικών δεδομένων και, πέραν της εποπτικής και γνωμοδοτικής του αρμοδιότητας, είναι επιφορτισμένος να εξασφαλίζει την συνεργασία. Δημιουργήθηκε το 2004 βάσει του κανονισμού (ΕΚ) 45/2001. Βλ. σχετικά σε: https://europa.eu/european-union/about-eu/institutions-bodies/european-data-protection-supervisor_en

[30] Αρμόδια εποπτική αρχή για την Ελλάδα είναι η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), που ανασυστήθηκε και ανακηρύχθηκε εποπτική αρχή με το Ν. 4624/2019 (ΦΕΚ 137 Α'/29-08-2019), βλ. σχετικά σε: www.dpa.gr.

[31] Εφεξής WP 29.

[32] Τα αρχεία της Ομάδας Εργασίας του άρθρου 29 (WP29) διατίθενται στον ιστότοπο: http://ec.europa.eu/justice/article-29/documentation/index_en.htm.

[33] Εφεξής χάριν συντομίας ΕΣΠΔ

[34] Το ΕΣΠΔ αποτελεί φορέα της Ε.Ε. με νομική προσωπικότητα, στα πλαίσια του οποίου συνεργάζονται οι εθνικές αρχές προστασίας δεδομένων, ο ΕΕΠΔ και η Επιτροπή. Απαρτίζεται από εκπροσώπους των 28 ανεξάρτητων εποπτικών αρχών όλων των κρατών μελών. Οι κύριες αρμοδιότητές του είναι να επιλύει τις μεταξύ των εθνικών εποπτικών αρχών διαφορές, να γνωμοδοτεί και να κατευθύνει σχετικά με τις βασικές έννοιες του Κανονισμού(ΕΕ) 2016/679 και της Οδηγίας (ΕΕ) 2016/680 , να διασφαλίσει τη συνεκτικότητα της εφαρμογής τους, να εκδίδει δεσμευτικές αποφάσεις έναντι των εθνικών εποπτικών αρχών, να γνωμοδοτεί στην Ευρωπαϊκή Επιτροπή και να εκδίδει συστάσεις με βέλτιστες πρακτικές. Οι αρμοδιότητές του ΕΣΠΔ είναι διευρυμένες σε σχέση με κείνες της WP29, κυρίως αναφορικά με την εξασφάλιση της συνεκτικότητας, προκειμένου ο ΓΚΠΔ να έχει καλύτερη τύχη σε σχέση με την προγενέστερη Οδηγία και να

διατηρεί τις αρχικές αρμοδιότητες και τον αποφασιστικό ρόλο που διέθετε η WP29 ενώ εκδίδει δεσμευτικές αποφάσεις σε περίπτωση διαφορών μεταξύ των εθνικών αρχών προστασίας δεδομένων, προωθώντας τη συνεπή εφαρμογή των κανόνων προστασίας σε όλη την Ε.Ε[35] (Τσιπτσέ & Κωστούλας, 2020).

Η θεσμική εξέλιξη στο δίκαιο της προστασίας των προσωπικών δεδομένων καταδεικνύει ότι πλέον υφίσταται αυτοτελής αντιμετώπισή τους που τα διαχωρίζει από την έννοια της ιδιωτικότητας καθώς πλέον συνιστούν αυτοτελές ατομικό δικαίωμα που προστατεύεται στους περισσότερους τομείς με νομοθετικά κείμενα ευρωπαϊκής και διεθνούς εμβέλειας, τα οποία δημιουργούν αυξημένα εχέγγυα για την προστασία των προσωπικών δεδομένων που τυγχάνουν επεξεργασίας (Μενουδάκος 2018, σε Κοτσαλή-Μενουδάκο).

εφαρμοστεί ομοιόμορφα στα κράτη μέλη. Μετά τον μετασχηματισμό του το ΕΣΠΔ, εκδίδει οδηγίες αλλά διατηρεί σε ισχύ, και δη επικαιροποιημένες, εκείνες της WP 29 (Τσιπτσέ & Κωστούλας, 2020). Βλ. επίσης European Union Agency for Fundamental Rights and Council of Europe, “Handbook on European data protection law”, 2018.

[35] Βλ. https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_387

ΚΕΦΑΛΑΙΟ 2ο: Η ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΗΝ ΕΛΛΑΔΑ

2. Το Ελληνικό Θεσμικό Πλαίσιο για την Προστασία των προσωπικών δεδομένων

2.1. Η συνταγματική κατοχύρωση του δικαιώματος προστασίας των προσωπικών δεδομένων

Η προστασία της ιδιωτικής ζωής από τα διεθνή νομοθετικά κείμενα που προαναφέρθηκαν και κυρίως από την Οικουμενική Διακήρυξη, την ΕΣΔΑ, την Ε.Σ. 108/1981, δεν άφησε ανεπηρέαστο τον έλληνα νομοθέτη κοινό και συνταγματικό. Η προστασία των προσωπικών δεδομένων κινούμενη εντός του ευρωπαϊκού πλαισίου, κατοχυρώθηκε συνταγματικά στην ελληνική έννομη τάξη μετά την ενσωμάτωση της ευρωπαϊκής οδηγίας στο εσωτερικό μας δίκαιο με το Ν. 2472/1997 (Βλαχόπουλος 2020)[36]. Όπως χαρακτηριστικά αναφέρει η Εισηγητική Έκθεση του Ν. 2472/1997 *«οι συνταγματικές διατάξεις 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»*.

Μετά τη συνταγματική αναθεώρηση του Συντάγματος με το ψήφισμα της 6ης Απριλίου 2001 προστέθηκε το άρθρο 5Α Σ. αναφορικά με το δικαίωμα στην ελεύθερη πληροφόρηση και τη συμμετοχή στην κοινωνία της πληροφορίας[37]. Η ρητή διασφάλιση της προστασίας των προσωπικών δεδομένων από μια συνταγματικά κατοχυρωμένη ανεξάρτητη αρχή

[36] Στο άρθρο 2 παρ.1 Σ. κατοχυρώνεται η αρχή του σεβασμού και της προστασίας της ανθρώπινης αξίας, στο άρθρο 5παρ. 1Σ το δικαίωμα της ελεύθερης ανάπτυξης της προσωπικότητας και της συμμετοχής στην κοινωνικο-οικονομική και πολιτική ζωή της χώρας, στην παρ. 1 εδ.α' και β' του άρθρου 9 Σ, το άσυλο της κατοικίας και το απαραβίαστο της οικογενειακής και ιδιωτικής ζωής, ενώ στο άρθρο 19 Σ το απόρρητο της επικοινωνίας.

[37] Άρθρο 5Α Σ. «*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»*

(άρθρο 101Α)[38] που να εξασφαλίζει τα εχέγγυα για την αποτελεσματικότερη προστασία τους[39], επήλθε εν τέλει με το άρθρο 9^{A} του Σ. [40]

Η ανάγκη δημιουργίας μιας ανεξάρτητης αρχής διαπιστώθηκε όταν εισήχθη η αυτοματοποίηση στην καθημερινότητα των δημόσιων και ιδιωτικών οργανισμών, προκειμένου να παταχθεί η γραφειοκρατία, να επιταχυνθεί η εξυπηρέτηση των πολιτών και πελατών και να εξασφαλιστεί η ευκολότερη πρόσβαση σε έγγραφα και υπηρεσίες. Οι νέες τεχνολογίες ανέδειξαν τη δύναμη της πληροφορίας που αποκτά άλλη υπόσταση εντός των πόρων ενός οργανισμού ενώ ταυτόχρονα σηματοδοτούν την έναρξη των παραβιάσεων της ιδιωτικότητας, της ελεύθερης επικοινωνίας και της ελευθερίας έκφρασης. Η διάταξη του άρθρου 9 Α Σ. καταδεικνύει την πρόθεση του νομοθέτη να προσαρμοστεί στις ραγδαίες εξελίξεις της τεχνολογίας δημιουργώντας ωστόσο ένα προπέτασμα στην αυθαίρετη παρέμβαση των θεμελιωδών δικαιωμάτων της ιδιωτικής ζωής από την αθέμιτη συλλογή, επεξεργασία και χρήση προσωπικών δεδομένων με συμβατικό ή ηλεκτρονικό τρόπο.

Η θεσμική εξέλιξη της προστασίας των προσωπικών δεδομένων κυρίως μετά την θεσμοθέτησή της από το παράγωγο ενωσιακό δίκαιο και τη θέσπιση ευρωπαϊκής νομοθεσίας, μετατοπίζει την αρχική κανονιστική προσέγγισή της προστασίας των προσωπικών δεδομένων ως έκφανση της ιδιωτικότητας, προς την κατεύθυνση μιας προσέγγισης που θεωρεί την προστασία των προσωπικών δεδομένων περισσότερο ως αυτοτελές ατομικό δικαίωμα που -σε περίπτωση παραβίασης- τελεί υπό αυξημένη κανονιστική προστασία συνδυασμένη με θεσμικές διαδικαστικές εγγυήσεις ελέγχου (Μενουδάκος, 2018).

[38] Άρθρο 5 παρ. *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».*

[39] Για να διασφαλιστούν και προστατευθούν τα παραπάνω δικαιώματα, η χώρα μας προέβη στη συνταγματική θεσμοθέτηση πέντε ανεξάρτητων αρχών, ήτοι της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), του Ανώτατου Συμβουλίου Επιλογής Προσωπικού (ΑΣΕΠ), του Εθνικού Συμβουλίου Ραδιοτηλεόρασης (ΕΣΡ) και του Συνηγόρου του Πολίτη, εκ των οποίων οι δύο πρώτες (η ΑΠΔΠΧ και η ΑΔΑΕ) ασκούν εποπτεία στην επεξεργασία προσωπικών δεδομένων.

[40]Άρθρο 9^{A} Σ *«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».*

Περαιτέρω, η προστασία της ανθρώπινης αξιοπρέπειας ρυθμίζεται και στη διάταξη άρθρου 57 ΑΚ που διαθέτει ευρεία διατύπωση, έτσι ώστε στα πλαίσια της προστασίας του δικαιώματος της προσωπικότητας, να εμπίπτουν μεταξύ άλλων η αξιοπρέπεια, τα προσωπικά δεδομένα και το απόρρητο.

Προς ενίσχυση του ελληνικού θεσμικού πλαισίου και αναφορικά με τις απορρέουσες από τις Οδηγίες 95/46/ΕΚ και 2002/58/ΕΚ υποχρεώσεις της χώρας μας έναντι της Ε.Ε., ο κοινός νομοθέτης προέβη σε περαιτέρω ρυθμίσεις, έτσι ώστε να θέσει τόσο τη συνταγματική προστασία όσο και τις γενικές διατάξεις του ιδιωτικού δικαίου, σε μια πιο στέρεη βάση για να μην συνιστούν απλώς και μόνον ένα *γενικό* θεσμικό πλαίσιο. Έτσι στις 10-4-1997 ψηφίστηκε ο Ν.2472/1997 που ενσωμάτωσε στην ελληνική έννομη τάξη την Οδηγία 95/46/ΕΚ, ο οποίος εν συνεχεία καταργήθηκε και αντικαταστάθηκε από τον κυρωτικό Ν. 4624/2019, καταργώντας την προϋφιστάμενη Οδηγία. Πριν γίνει αναφορά στο νέο νόμο παρατίθενται οι επί μέρους νόμοι που αφορούν την προστασία των προσωπικών δεδομένων στην εθνική μας έννομη τάξη.

2.2. Νομοθετικά κείμενα για την προστασία των προσωπικών δεδομένων

Ο έλληνας νομοθέτης επιδιώκοντας να προστατεύσει τα δεδομένα προσωπικού χαρακτήρα θέσπισε σωρεία νομοθετικών κειμένων, είτε συμμορφούμενος προς τις απαιτήσεις ή υποδείξεις του ενωσιακού νομοθέτη είτε κατόπιν δικής του πρωτοβουλίας. Τα σημαντικότερα είναι τα εξής:

Ο Ν.2068/1992 (ΦΕΚ Α΄ 118/9.7.1992) περί «Κύρωσης της Ευρωπαϊκής Σύμβασης για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία πληροφοριών προσωπικού χαρακτήρα».

Ο Ν.2251/1994 (ΦΕΚ Α΄ 191/16.11.1994) περί «Προστασίας των καταναλωτών και προάσπισης των δικαιωμάτων τους».

Ο Ν.3471/2006 (ΦΕΚ Α΄ 133/28.06.2006) 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.

Ο Ν.3783/2009 (ΦΕΚ Α΄ 136/7.8.2009) για την «Ταυτοποίηση των κατόχων και χρηστών εξοπλισμού και υπηρεσιών κινητής τεχνολογίας και άλλες διατάξεις».

Ο Ν.3917/2011 (ΦΕΚ Α΄ 22/21.2.2011) «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. 4070/2012 (ΦΕΚ Α΄82/10.4.2012) «για τις ρυθμίσεις Ηλεκτρονικών Επικοινωνιών, Μεταφορών, Δημοσίων Έργων και άλλες διατάξεις».

Ο Ν.4225/2014 (ΦΕΚ Α΄ 2/7.01.2014) για την «αναβάθμιση και βελτίωση των μηχανισμών είσπραξης των ασφαλιστικών φορέων, τα πρόστιμα για την ανασφάλιστη και αδήλωτη εργασία και λοιπές διατάξεις αρμοδιότητας Υπουργείου Εργασίας Κοινωνικής Ασφάλισης και Πρόνοιας»

Ο Ν.4579/2018 (ΦΕΚ Α΄ 201/3.12.2018) «για τα ονομαστικά αρχεία επιβατών στις πτήσεις αεροπλάνων εντός ή εκτός ΕΕ».

Ο Ν. 4624/2019 (ΦΕΚ Α΄ 137/2.8.2019) για την «Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις», ο οποίος αποτελεί και το ισχύον θεσμικό πλαίσιο προστασίας των προσωπικών δεδομένων στην χώρα μας.

2.3. Ο Νόμος 4624/2019

Στις 26 Αυγούστου 2019, ήτοι 15 μήνες μετά την θέση σε ισχύ του Γενικού Κανονισμού[41], ψηφίστηκε με τη διαδικασία του κατεπείγοντος, ύστερα από δημόσια διαβούλευση που διήρκεσε μόλις οχτώ ημέρες, ο πολυαναμενόμενος νόμος για την προστασία των προσωπικών δεδομένων, ο οποίος δημοσιεύθηκε στις 29 Αυγούστου 2019 στην Εφημερίδα της Κυβερνήσεως. Πρόκειται για το Ν. 4624/2019 που αφορά *«την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και*

[41] Σημειώνεται ότι η ψήφιση του Νόμου επισπεύσθηκε λόγω της παραπομπής της χώρας μας στο Δικαστήριο της Ευρωπαϊκής Ένωσης για την εκπρόθεσμη ενσωμάτωση της Οδηγίας LED.

ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις»[42].

Σκοπός του ήταν να αντικαταστήσει το νομοθετικό πλαίσιο που ρύθμιζε τη συγκρότηση και τη λειτουργία της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, να λάβει μέτρα εφαρμογής του Κανονισμού 2016/679 (ΓΚΠΔ/GDPR) και να ενσωματώσει στην εθνική νομοθεσία την Οδηγία (ΕΕ) 2016/680 (άλλως «Οδηγία LED») του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016. Με τα συμπληρωματικά μέτρα εφαρμογής του ΓΚΠΔ που θεσπίζει, αίρει τη νομική αβεβαιότητα που επικρατούσε λόγω της καθυστερημένης συμπλήρωσης του Κανονισμού και την μέχρι πρότινος παράλληλη ισχύ του Ν. 2472/1997, τον οποίο καταργεί διατηρώντας σε ισχύ μόνον τις διατάξεις του άρθρου 84 αυτού[43].

Από πλευράς διάρθρωσης ο Ν. 4624/2019 αποτελείται από τέσσερα κεφάλαια. Στο κεφάλαιο Α (άρθρα 1-8) προσδιορίζονται ο σκοπός και το πεδίο εφαρμογής του, ο ορισμός δημόσιου και ιδιωτικού φορέα και ο υποχρεωτικός διορισμός υπευθύνου προστασίας δεδομένων στους δημόσιους φορείς. Το κεφάλαιο Β (άρθρα 9-20) αποτελείται από διατάξεις για την οργάνωση και λειτουργία της ΑΠΔΠΧ, το κεφάλαιο Γ (άρθρα 21-42) θέτει συμπληρωματικά μέτρα εφαρμογής του ΓΚΠΔ για την επεξεργασία δεδομένων προσωπικού χαρακτήρα, ενώ στο κεφάλαιο Δ (άρθρα 43-87) ενσωματώνεται η Οδηγία (ΕΕ) 2016/680.

Ο σκοπός, όπως περιγράφεται ως άνω, και το ουσιαστικό πεδίο εφαρμογής του νόμου συμπίπτουν με εκείνο του ΓΚΠΔ. Όσον αφορά στο ουσιαστικό πεδίο εφαρμογής ο νόμος αναφέρεται σε επεξεργασία από δημόσιους ή ιδιωτικούς φορείς που διενεργείται εν όλω ή εν μέρει με αυτοματοποιημένα μέσα ή χειρόγραφα επί δεδομένων που περιλαμβάνονται σε σύστημα αρχειοθέτησης ενώ εξαιρείται του πεδίου εφαρμογής η επεξεργασία σε δεδομένα οικιακής χρήσης ή για εμπορική δραστηριότητα. Ως προς το εδαφικό πεδίο σημειώνεται ότι ο νόμος εφαρμόζεται στους δημόσιους φορείς ενώ στους ιδιωτικούς μόνο αν η επεξεργασία γίνεται εντός της ελληνικής επικράτειας ή αν η επεξεργασία γίνεται από

[42] ΦΕΚ 137/Α/29-08-2019

[43] Η διάταξη του άρθρου 84 Ν.2472/1997 αφορά την δημοσιοποίηση δεδομένων από τις εισαγγελικές αρχές στην περίπτωση συγκεκριμένων αδικημάτων, τη χρήση οπτικοακουστικού υλικού στις δημόσιες συναθροίσεις, τη διατήρηση του Μητρώου για την απαγόρευση αποστολής προωθητικών ενεργειών μέσω ταχυδρομείου, τη διάταξη περί σύστασης της Αρχής Προστασίας και τα πλαίσια επιβολής διοικητικών προστίμων στους ιδιωτικούς φορείς.

υπεύθυνο που έχει εγκατάσταση εντός των ορίων αυτής ή παρά το ότι αν δεν έχει την εγκατάσταση εντός αυτής, εμπίπτει ωστόσο στο πεδίο εφαρμογής του ΓΚΠΔ.

Ο νέος νόμος παραθέτει ορισμούς για τους δημόσιους και τους ιδιωτικούς φορείς και την εποπτική αρχή. Συγκεκριμένα το άρθρο 4 Ν. 4624/2019 ορίζει ότι:

«δημόσιος φορέας» είναι οι δημόσιες αρχές, οι ανεξάρτητες και οι διοικητικές, τα ΝΠΔΔ, οι ΟΤΑ α' και β' βαθμού, τα νομικά πρόσωπα και οι επιχειρήσεις αυτών, οι κρατικές ή δημόσιες επιχειρήσεις και οργανισμοί, τα ΝΠΙΔ που ανήκουν στο κράτος κατά 50% του ετήσιου προϋπολογισμού τους ή η διοίκησή τους ορίζεται από αυτό,

«ιδιωτικός φορέας» είναι το φυσικό ή νομικό πρόσωπο ή η ένωση προσώπων χωρίς νομική προσωπικότητα που δεν εμπίπτει στην έννοια του δημόσιου φορά

«αρμόδια εποπτική αρχή» είναι η Αρχή προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ).

Βέβαια ο Ν. 4624/2019 χαρακτηρίζεται από μια αρκετά μινιμαλιστική μορφή, γεγονός που συνεπάγεται την ασάφεια ορισμένων όρων[44] που νομολογιακά αμφισβητούνται και οι οποίοι δεν επεξηγούνται ούτε στην αιτιολογική αυτού έκθεση, από το κείμενο της οποίας απουσιάζουν κατευθυντήριες ερμηνευτικές γραμμές.

Ο νέος νόμος αφιερώνει ένα ολόκληρο κεφάλαιο στην ΑΠΔΠΧ καθώς προβλέπει την ανασύστασή της και την αναγόρευσή της, κατά τα οριζόμενα στον ΓΚΠΔ, σε εποπτική αρχή. Παρά την τάση των ευρωπαϊκών νομοθεσιών να θεσπίζουν μια ενιαία διοικητική αρχή τόσο για την προστασία των προσωπικών δεδομένων όσο και την ελευθερία της πληροφόρησης, ο έλληνας νομοθέτης δεν κατάφερε να μετεξελίξει την ΑΠΔΠΧ σε Αρχή Προστασίας Δεδομένων και Πρόσβασης στην Πληροφορία. Κι αυτό γιατί η πρόσβαση στην πληροφορία και η προστασία των προσωπικών δεδομένων είναι δικαιώματα που πρέπει να δρουν συμπληρωματικά και μόνον δευτερευόντως αντιθετικά. Η αδυναμία αυτή του έλληνα νομοθέτη αφήνει τρόπον τινά «έκθετη» την πρόσβαση στην πληροφορία έναντι της προστασίας των προσωπικών δεδομένων, τα οποία προστατεύονται από μια συνταγματικά κατοχυρωμένη ανεξάρτητη αρχή (Παναγοπούλου-Κουτνατζή, 2019).

Βασική είναι η διάταξη του άρθρου 5 Ν.4624/2019 για τη *νομική βάση επεξεργασίας*, κατά την οποία οι δημόσιοι φορείς δύνανται να επεξεργάζονται δεδομένα όταν αυτό κρίνεται

[44] Όπως για παράδειγμα ως προς το τι συνιστά σύστημα αρχειοθέτησης.

αναγκαίο για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας ενώ το άρθρο 6 αυτού προκρίνει τον *υποχρεωτικό ορισμό* του *υπευθύνου προστασίας δεδομένων* (ΥΠΔ) στους δημόσιους φορείς, θέτοντας ορισμένα κριτήρια ορισμού (εξειδικευμένες γνώσεις και ικανότητες) προς εκπλήρωση των καθηκόντων του, όπως αυτά ορίζονται στο άρθρο 8 του νόμου. Η εν λόγω διάταξη ενστερνίζεται τον γερμανικό νόμο που εφαρμόζεται εδώ και 30 και πλέον έτη, έλκοντας από αυτόν θετική επιρροή, στο μέτρο που μεταφέρεται η εμπειρία και η τεχνογνωσία μιας άλλης έννομης τάξης στο εσωτερικό μας δίκαιο (Παναγοπούλου-Κουτνατζή, 2019), πολλώ δε μάλλον όταν αυτή οδηγεί σε θετικά αποτελέσματα σχετικά με τη συμμόρφωση προς τον ΓΚΠΔ. Ο δημόσιος μάλιστα φορέας υποχρεούται σε κοινοποίηση των στοιχείων του ΥΠΔ στην Αρχή, εκτός αν κάτι τέτοιο δεν επιτρέπεται για λόγους εθνικής ασφάλειας.

Η *διάκριση* ωστόσο στην οποία προβαίνει ο νέος νόμος ανάλογα με το αν η επεξεργασία των προσωπικών δεδομένων διενεργείται από ιδιωτικούς ή από δημόσιους φορείς, προβληματίζει καθώς δημιουργεί ένα «καθεστώς δύο ταχυτήτων» με κίνδυνο το δημόσιο να δρα ελεύθερα και να επεξεργάζεται, τρόπον τινά, «ανεξέλεγκτα» τα προσωπικά δεδομένα των υποκειμένων που συναλλάσσονται με τις υπηρεσίες του (Παναγοπούλου-Κουτνατζή, 2019).

Ο Ν. 4624/2019 αποτυπώνει τη βούληση του Έλληνα νομοθέτη να προβεί σε εθνικές νομοθετικές επιλογές, στο μέτρο που του το επιτρέπει ο ΓΚΠΔ και στα πλαίσια της διακριτικής ευχέρειας που αναγνωρίζει στα κράτη μέλη υπό μορφή «ρητρών ανοίγματος» άλλως «ρητρών ευελιξίας» (Παναγοπούλου-Κουτνατζή, 2019)[45]. Έτσι περιέχει ρήτρες που αφορούν στην επεξεργασία δεδομένων ανηλίκων, στην επεξεργασία «ειδικών κατηγοριών δεδομένων» (ευαίσθητων), στον ακριβή καθορισμό των προϋποθέσεων υπό τις οποίες η επεξεργασία είναι σύννομη. Περαιτέρω αξιοποιεί την ευχέρεια που του δίνει ο ΓΚΠΔ ως προς την έκταση των εξαιρέσεων (άρθρο 23 παρ.1) και τη ρύθμιση ειδικών περιπτώσεων επεξεργασίας, όπως λ.χ. της επεξεργασίας που τυγχάνουν τα προσωπικά δεδομένα στο πλαίσιο της απασχόλησης ή για σκοπούς επιστημονικής έρευνας (Αιτιολ. Έκθεση ΣχΝ)[46].

Ως προς τη συγκατάθεση ανηλίκων η αυξημένη προστασία που θέτει γι' αυτούς ο ΓΚΠΔ, δεν απαγορεύει στον εθνικό νομοθέτη να προβεί κατά διακριτική ευχέρεια σε διαφορετική

[45] Βλ. σχετικά σε https://www.syntagmawatch.gr/trending-issues/nomos-4624-2019-kai-efarmogi-gdpr-polla-yposchomenos-alla-parallila-kathysterimenos/

[46] Ο ΓΚΠΔ εμπεριέχει πάνω από 70 ρήτρες ευελιξίας.

αντιμετώπιση της προστασίας αυτής. Σύμφωνα με τον ΓΚΠΔ τα προσωπικά δεδομένα των ανηλίκων κατά την προσφορά υπηρεσιών της κοινωνίας της πληροφορίας (π.χ. on-line βιντεοπαιχνίδια ή μέσα κοινωνικής δικτύωσης) τίθενται σε επεξεργασία μόνο εάν ο ανήλικος έχει συμπληρώσει το 16ο έτος της ηλικίας του και σε καμία περίπτωση δεν χωρεί επεξεργασία αν δεν έχει συμπληρώσει το 13ο έτος της ηλικίας του, ανεξάρτητα από το τι προβλέπει η εκάστοτε εθνική νομοθεσία. Το άρθρο 21 Ν. 4624/2019, δέχεται ως σύννομη την επεξεργασία που διενεργείται, όταν ο ανήλικος έχει συμπληρώσει το 15ο έτος της ηλικίας του και παρέχει τη συγκατάθεση του[47]. Διαφορετικά, απαιτείται η παροχή συγκατάθεσης του νόμιμου αντιπροσώπου του.

Ως προς την επεξεργασία «ειδικών κατηγοριών δεδομένων», πέρα από τις σχετικές διατάξεις του ΓΚΠΔ, ο Ν.4624/2019 προβλέπει ότι η επεξεργασία από δημόσιους και ιδιωτικούς φορείς επιτρέπεται ακόμη και χωρίς τη συγκατάθεση του υποκειμένου των δεδομένων, εάν είναι υποχρεωτική για λόγους παροχής υγείας και κοινωνικής περίθαλψης, κοινωνικής ασφάλισης και εκτίμησης της ικανότητας του ατόμου για εργασία, και υπό την προϋπόθεση να λαμβάνονται τα κατάλληλα μέτρα για την διαφύλαξη των συμφερόντων του υποκειμένου των δεδομένων, ενώ επιτρέπει την επεξεργασία ειδικών κατηγοριών δεδομένων μόνον από δημόσιους φορείς, όταν συντρέχουν λόγοι δημοσίου συμφέροντος, αποτροπή σημαντικής απειλής για την δημόσια ασφάλεια και λήψη ανθρωπιστικών μέτρων (άρθρο 22). Η προστιθέμενη ωστόσο αξία του νέου νόμου συνίσταται στο ότι απαγορεύει ρητά τη χρήση γενετικών δεδομένων για σκοπούς ασφάλισης υγείας και ζωής (άρθρο 23)[48].

Όσον αφορά στην επεξεργασία δεδομένων για άλλους σκοπούς το άρθρο 24 Ν. 4624/2019 προβλέπει ότι αυτή είναι δυνατή από δημόσιους φορείς για σκοπούς διαφορετικούς από αυτούς που είχαν συλλεχθεί, στις περιπτώσεις που είναι αναγκαία για τη δίωξη αδικημάτων, για λόγους δημόσιας ασφάλειας αλλά και προς αποτροπή βλάβης άλλου προσώπου. Ομοίως επιτρέπεται η επεξεργασία από ιδιωτικούς φορείς εάν τίθεται θέμα εθνικής ασφάλειας ή για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων τους (άρθρο 25). Τέτοια επεξεργασία από ιδιωτικούς φορείς επιτρέπεται για την αποτροπή

[47] Η νομοθετική αυτή επιλογή του 15ου έτους ηλικίας απηχεί και άλλες ρυθμίσεις του ελληνικού δικαίου (πχ. την ΑΚ 136 που αναγνωρίζει περιορισμένη δικαιοπρακτική ικανότητα σε άτομο ηλικίας 15 ετών).

[48] Η απαγόρευση αυτή είναι σύμφωνη με την αρχή που διακηρύσσεται στο άρθρο 12 παρ. 1 της Σύμβασης του Συμβουλίου της Ευρώπης για την προστασία των ανθρωπίνων δικαιωμάτων και της αξιοπρέπειας του ατόμου σε σχέση με τις εφαρμογές της βιολογίας και της ιατρικής (Σύμβαση για τα Ανθρώπινα Δικαιώματα και τη Βιοϊατρική) ενώ τελεί σε συμφωνία και με το πνεύμα του άρθρου 5 της Οικουμενικής Διακήρυξης για τα Γενετικά Δεδομένα του Ανθρώπου της UNESCO. Βλ. Αιτιολογική Έκθεση Σχ Ν., σελ. 14.

απειλών κατά της εθνικής ασφάλειας ή της δημόσιας ασφάλειας κατόπιν αιτήματος δημοσίου φορέα, για την δίωξη ποινικών αδικημάτων ή για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων, εκτός και εάν το συμφέρον του υποκειμένου των δεδομένων υπαγορεύει να μην τύχουν επεξεργασίας τα δεδομένα αυτά.

Ο νέος νόμος προβλέπει και άλλες περιπτώσεις επεξεργασίας προσωπικών δεδομένων, όπως αυτή που διενεργείται για δημοσιογραφικούς σκοπούς ή σκοπούς ακαδημαϊκής, καλλιτεχνικής ή λογοτεχνικής έκφρασης η οποία επιτρέπεται και χωρίς τη συγκατάθεση του υποκειμένου, εφόσον από τη στάθμιση του δικαιώματος στην ιδιωτική ζωή και του δικαιώματος στην πληροφόρηση υπερέχει το τελευταίο (άρθρο 28). Τάσσεται επομένως υπέρ της στάθμισης μεταξύ των εν λόγω δικαιωμάτων και της in concreto επιλογής ενός εκ των δύο.

Επίσης επιτρεπτή είναι και η επεξεργασία προσωπικών δεδομένων ακόμη και χωρίς τη συγκατάθεση του υποκειμένου εφόσον είναι αναγκαία για σκοπούς επιστημονικής ή ιστορικής έρευνας ή συλλογής ή τήρησης στατιστικών στοιχείων υπό την προϋπόθεση της τήρησης κατάλληλων μέτρων προστασίας, όπως η ψευδωνυμοποίηση και η κρυπτογράφηση, όποτε αυτό είναι εφικτό (άρθρο 30) .

Εξίσου ελεύθερη είναι και η κανονιστική επιλογή του έλληνα νομοθέτη αναφορικά με την ενσωμάτωση της Οδηγίας για την προστασία των δεδομένων που γίνονται αντικείμενο επεξεργασίας από τις αρμόδιες αρχές για τους σκοπούς επιβολής νόμου. Τα κράτη μέλη μπορούν να θεσπίζουν ισχυρότερες διασφαλίσεις από αυτές που προβλέπει η εν λόγω Οδηγία. Η ευελιξία αυτή του εθνικού νομοθέτη πρέπει να ερμηνεύεται υπό το πρίσμα της ενωσιακής νομοθεσίας, του ΧΘΔΑ, του άρθρου 16 ΣΛΕΕ αλλά και της νομολογίας του ΕΔΔΑ, του ΔΕΕ και των εθνικών δικαστηρίων.

Αντίστοιχος προβληματισμός δημιουργείται και από την έλλειψη επαρκών εγγυήσεων όσον αφορά στα δικαιώματα των υποκειμένων κατά την επεξεργασία των δεδομένων τους που αφορούν ποινικές καταδίκες καθώς και απ΄ την ανεξέλεγκτη δράση των δικαστικών και εισαγγελικών αρχών κατά την επεξεργασία δεδομένων, για τις οποίες (αρχές) δεν υφίσταται καν εποπτική αρχή ελέγχου αποτελούμενη από δικαστές, γεγονός που αντιβαίνει στη διάταξη του άρθρου 8 παρ. 3 του ΧΘΔΑ.

Παρά την έως πρότινος - βάσει του προγενέστερου Ν. 2472/1997 - τάση να επικρατεί η προστασία των προσωπικών δεδομένων έναντι της προστασίας της πληροφόρησης, ο νέος

νόμος παραχωρεί ένα μικρό προβάδισμα υπέρ της ελευθερίας του Τύπου, επεκφρασμένο ως περιορισμό του δικαιώματος των υποκειμένων όπως λ.χ. εκείνου της διαγραφής.

Επίσης, ο ελληνικός κυρωτικός νόμος δεν δίνει τη δυνατότητα σε μη κερδοσκοπικούς φορείς να εκπροσωπήσουν τους πολίτες ενώπιον των δικαστηρίων – διάταξη η οποία έρχεται σε σαφή αντίθεση με τον ευρωπαϊκό κανονισμό.

Εν κατακλείδι ο νέος νόμος, που προφανώς δεν στερείται ατελειών ή ανεπαρκειών και ο οποίος ψηφίστηκε σε χρόνο ρεκόρ υπό την απειλή ενός προστίμου 2,5 εκατομμυρίων ευρώ από το Δικαστήριο της Ε.Ε., κατάφερε ως ένα βαθμό να ρυθμίσει και αποσαφηνίσει αρκετά από τα ζητήματα για τα οποία είχε τη διακριτική ευχέρεια να το πράξει, επιδεικνύοντας ιδιαίτερη τόλμη και πυγμή στο να θέσει όρια στην επεξεργασία των προσωπικών δεδομένων. Ως προς τα ζητήματα που δεν κατάφερε να αποσαφηνίσει, καταλείπεται στην ΑΠΔΠΧ να θέσει κατευθυντήριες γραμμές μέσα από τις αποφάσεις και γνωμοδοτήσεις της καθώς και στα ελληνικά δικαστήρια (Παναγοπούλου-Κουτνατζή, 2019).

2.4. Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ)

Στα πλαίσια της προστασίας των προσωπικών δεδομένων στη χώρα μας σπουδαίο ρόλο διαδραματίζει η συνταγματικά κατοχυρωμένη Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ)[49]. Λόγω του ιδιαίτερα σημαντικού της ρόλου κρίνεται σκόπιμη η ιδιαίτερη αναφορά σ' αυτήν στο κείμενο της παρούσας μελέτης.

Η ΑΠΔΠΧ που ιδρύθηκε, όπως προαναφέρθηκε με τον Ν. 2472/1997, ανασυστήθηκε με τον Ν. 4624/2019 και ανακηρύχθηκε εποπτική αρχή[50] της Ελλάδας βάσει του ΓΚΠΔ. Όσον αφορά στην προστασία των προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών, η Αρχή εφαρμόζει αντίστοιχα τον Ν. 3471/2006[51] που, όπως προαναφέρθηκε, αντίστοιχα ενσωματώνει στο εθνικό δίκαιο την Ευρωπαϊκή Οδηγία 58/2002. Ήδη, υπό το προϊσχύον δίκαιο, η ΑΠΔΠΧ είχε μια σειρά αρμοδιοτήτων εν ευρεία έννοια ρυθμιστικών και ελεγκτικών. Μετά την εισαγωγή του ΓΚΠΔ και την αναγόρευσή της σε εποπτική αρχή, οι αρμοδιότητές της διευρύνθηκαν.

[49] Επίσημος ιστότοπος: https://www.dpa.gr/
[50] Σύμφωνα με τον ορισμό που δίνεται στο άρθρο 4 παρ. 21 εποπτική αρχή, είναι ανεξάρτητη δημόσια αρχή που συγκροτείται από κράτος μέλος σύμφωνα με το άρθρο 51, βλ. ΕΕ L 119/134, 4.05.2016.
[51] Βλ. ανωτέρω σελ. 30.

Βάσει των ρυθμιστικών της αρμοδιοτήτων η ΑΠΔΠΧ:

1.εκδίδει οδηγίες και κανονιστικές πράξεις για τη ρύθμιση τεχνικών θεμάτων

2.καλεί και επικουρεί επαγγελματικά σωματεία που τηρούν αρχεία δεδομένων, στην κατάρτιση κωδίκων δεοντολογίας

3.εξετάζει αιτήσεις του υπευθύνου επεξεργασίας, με τις οποίες ζητείται ο έλεγχος και η εξακρίβωση της νομιμότητας της επεξεργασίας

4.απευθύνει συστάσεις και υποδείξεις στους υπευθύνους επεξεργασία

5.συνεργάζεται με τις Αρχές άλλων κρατών μελών της Ε.Ε. και με το ΕΣΠΔ –

6.εκπροσωπεί τη χώρα μας στο ΕΣΠΔ

7.γνωμοδοτεί για νομοθετικές ή κανονιστικές ρυθμίσεις σχετικά με την επεξεργασία προσωπικών δεδομένων (ΑΠΔΠΧ, Ετήσια Έκθεση 2018).

Βάσει των ελεγκτικών της αρμοδιοτήτων η ΑΠΔΠΧ:

1.εξετάζει προσφυγές, καταγγελίες, αντιρρήσεις και παράπονα των υποκειμένων των δεδομένων για την εφαρμογή του νόμου και την προστασία των δικαιωμάτων τους.

2.διενεργεί διοικητικούς ελέγχους αυτεπαγγέλτως ή κατόπιν καταγγελίας, στο πλαίσιο των οποίων ελέγχονται η τεχνολογική υποδομή και τα μέσα επεξεργασίας των δεδομένων

3.εξετάζει τις γνωστοποιήσεις που υποβάλλονται

4.χορηγεί άδειες[52]

5.εξετάζει αιτήσεις για πρόσβαση σε δημόσια και ιδιωτικά έγγραφα που εμπεριέχουν δεδομένα τρίτων.

6.αποφαίνεται επί αιτήσεων διαγραφής από το Σύστημα Πληροφοριών Σένγκεν (ΣΠΣ-SIS) και τον Εθνικό Κατάλογο Ανεπιθύμητων Αλλοδαπών (ΕΚΑΝΑ) .

Οι βασικότερες διευρυμένες αρμοδιότητες της ΑΠΔΠΧ βάσει του ΓΚΠΔ

1.παρακολουθεί την εφαρμογή του ΓΚΠΔ

2.συμβάλλει στη συνεκτική εφαρμογή του σε όλη την Ε.Ε.

3.συνεργάζεται με τις εποπτικές αρχές των κρατών μελών της Ε.Ε. και με την Επιτροπή

4.εκτελεί τα καθήκοντα των άρθρων 57-58 ΓΚΠΔ ήτοι:

[52] Αυτές μπορεί να αφορούν την ίδρυση ή λειτουργία αρχείου ευαίσθητων δεδομένων, τη διαβίβαση δεδομένων σε χώρες εκτός Ε.Ε. τη διασύνδεση αρχείων στις περιπτώσεις ευαίσθητων δεδομένων ή χρήσης ενιαίου κωδικού.

4.1.προωθεί την ευαισθητοποίηση του κοινού και των υπευθύνων επεξεργασίας στα ζητήματα προστασίας προσωπικών δεδομένων δίνοντας ιδιαίτερη προσοχή όταν η επεξεργασία αφορά σε παιδιά.

4.2.συμβουλεύει το εθνικό κοινοβούλιο, την κυβέρνηση κ.α. όργανα για νομοθετικά και διοικητικά μέτρα σχετικά με την προστασία

4.3.παρέχει πληροφορίες στα υποκείμενα των δεδομένων (κατόπιν αιτήματός τους) για την άσκηση των δικαιωμάτων τους.

4.4.χειρίζεται καταγγελίες για παράβαση διατάξεων του ΓΚΠΔ[53]

4.5.διενεργεί έρευνες σχετικά με την εφαρμογή του ΓΚΠΔ.

4.6.καταρτίζει και διατηρεί κατάλογο απαιτήσεων για διενέργεια DPIA

4.7. παρέχει συμβουλές

4.8.εγκρίνει κώδικες δεοντολογίας και κριτήρια πιστοποίησης

4.9.συνεργάζεται με άλλες εποπτικές αρχές

4.10.συμβάλλει στις δραστηριότητες του ΕΣΠΔ

5.είναι αποκλειστικά αρμόδια σε επεξεργασία των προσωπικών δεδομένων από δημόσιους ή ιδιωτικούς φορείς όπου δεν εφαρμόζονται οι κανόνες συνεργασίας και συνεκτικότητας και ο «μηχανισμός μίας στάσης» [54]

6.καταρτίζει ετήσια έκθεση, την οποία υποβάλλει στη Βουλή και την κυβέρνηση και την δημοσιεύει στο κοινό, την Επιτροπή και το ΕΣΠΔ[55]

7.είναι αρμόδια ως Επικεφαλής ΕΑ για τη διασυνοριακή επεξεργασία[56]

8. συνεργάζεται με τις ΕΑ των κρατών μελών της ΕΕ παρέχοντας αμοιβαία συνδρομή και πραγματοποιώντας κοινές επιχειρήσεις, σε διμερές ή πολυμερές επίπεδο[57]

9.είναι αρμόδια για καταγγελία ή παραβίαση του ΓΚΠΔ σε διασυνοριακή επεξεργασία με τοπικές επιπτώσεις μόνο στο έδαφός της

10.εφαρμόζει τον μηχανισμό συνεκτικότητας (ΑΠΔΠΧ, Ετήσια Έκθεση 2018).

---

[53] Κυρίως ασχολείται με παραβιάσεις προσωπικών δεδομένων των εργαζομένων που συνίστανται στη χρήση παρεμβατικών μεθόδων (βιομετρικών, παρακολούθησης διαδικτυακής πλοήγησης ή ανταλλαγής ηλεκτρονικών μηνυμάτων, βιντεοσκόπησης κ.ο.κ.) που πραγματοποιούνται συλλήβδην στον εργασιακό χώρο στο όνομα της κερδοφορίας (Βασιλοπούλου σε Κοτσαλή & Μενουδάκο, 2020).

[54] Αιτιολογική σκέψη 128 ΓΚΠΔ, ΕΕ L 119/24, 4.05.2016.

[55] Άρθρο 59 ΓΚΠΔ ΕΕ L 119/71, 4.05.2016.

[56] Άρθρο 56 παρ. 1, αιτ. 124 του ΓΚΠΔ.Σ τις περιπτώσεις διασυνοριακής επεξεργασίας δεδομένων (άρθρο 4 παρ. 23 του ΓΚΠΔ) εφαρμόζεται, κατά κανόνα, ο μηχανισμός συνεργασίας μεταξύ της εθνικών εποπτικών αρχών (ΕΕΑ) και των ενδιαφερομένων εποπτικών αρχών, την πρωταρχική ευθύνη για την εποπτεία της οποίας έχει η ΕΕΑ (άρθρο 60, αιτ. 124-126 του ΓΚΠΔ; WP244rev.0113).

[57] Άρθρα 61-62, αιτ. σκ.133-134, 138 του ΓΚΠΔ σε συνδυασμό με άρθρο 10 παρ. 4 Ν. 4624/2019

ΚΕΦΑΛΑΙΟ 3ο: Ο ΓΕΝΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ (General Data Protection Regulation-GDPR)

3.1. Το χρονικό της έκδοσης του ΓΚΠΔ

Στις 27 Απριλίου 2016 υπεγράφη στις Βρυξέλλες από τον τότε Πρόεδρο του Ευρωπαϊκού Συμβουλίου Schulz ένας κανονισμός, του οποίου η επεξεργασία είχε ξεκινήσει, όπως προαναφέρθηκε, από το 2009 στο ξεκίνημα της παγκόσμιας οικονομικής κρίσης, όταν το δημόσιο χρέος είχε ανέλθει στα ύψη, ο φόβος της τρομοκρατίας ήταν διάχυτος στην Ευρώπη και το μεγάλο μεταναστατευτικό κύμα ήταν πλέον γεγονός. Τεράστιες μάζες ανθρώπων μετακινούνταν προς την Ευρώπη και μαζί με αυτούς και τα προσωπικά δεδομένα τους που κατά την είσοδό τους ή παραμονή τους συλλέγονται και τυγχάνουν επεξεργασίας είτε όταν στερούνται νομιμοποιητικών εγγράφων ή όταν εισέρχονταν ως θύματα πολέμου ή ως αιτούντες άσυλο σε μια προηγμένη επιχειρηματικά και πολιτισμικά Ευρώπη. Επιπλέον τα ανθρώπινα δικαιώματα κινδύνευαν την περίοδο εκείνη και από τις τρομοκρατικές επιθέσεις που λάμβαναν χώρα σε διάφορες ευρωπαϊκές πρωτεύουσες, σπέρνοντας το φόβο και προκαλώντας κοινωνικές ταραχές ενώ η ραγδαία τεχνολογική ανάπτυξη επέτεινε το γενικότερο κλίμα ανασφάλειας και αβεβαιότητας.

Το 2010, η Επιτροπή προέβη στη δημοσίευση μιας ανακοίνωσης για την ανασκόπηση του ζητήματος της προστασίας των προσωπικών δεδομένων και τον επαναπροσδιορισμό της σε νέα βάση. Στη διαδικασία που ξεκίνησε συμμετείχαν το Συμβούλιο, το Κοινοβούλιο, ο ΕΕΠΔ και η WP 29, δημοσιεύοντας τις απόψεις τους. Δύο χρόνια αργότερα η Επιτροπή δημοσίευσε σχέδιο Κανονισμού και Οδηγίας αντίστοιχα (De Hert, 2016) παραδίδοντας τη σκυτάλη για τη συνέχιση των εργασιών στο Συμβούλιο και το Ευρωπαϊκό Κοινοβούλιο, το οποίο με τη σειρά του ανέθεσε την υπόθεση στην Επιτροπή Πολιτικών Ελευθεριών, Δικαιοσύνης και Εσωτερικών Υποθέσεων (LIBE), ορίζοντας δύο εισηγητές, έναν για τον Κανονισμό κι έναν για την Οδηγία.

Στις αρχές του έτους 2013 το Κοινοβούλιο, προφανώς υπό την πίεση και των εκλογών, επίσπευσε την έκδοση των απόψεών του επί των κειμένων. Στη συνέχεια το Συμβούλιο και αφού παρήλθαν τρία σχεδόν χρόνια, έξι προεδρίες και σωρεία συναντήσεων, κατέληξε στη διατύπωση των τελικών προτάσεων τον Ιούνιο του 2015. Το τελικό κείμενο που αποτέλεσε αντικείμενο έντονων διαπραγματεύσεων και το οποίο υπέστη σημαντικές

αλλαγές για να καταλήξει εν τέλει να αποτελέσει «προϊόν» συμβιβασμού, ολοκληρώθηκε τον Δεκέμβριο του 2015, ενώ η όλη διαδικασία ολοκληρώθηκε σχετικά σύντομα λόγω των τρομοκρατικών επιθέσεων στο Παρίσι. Η τελική υπογραφή του Κανονισμού και της Οδηγίας έλαβαν χώρα στις 27 Απριλίου 2016αν και με μια καθυστέρηση καθώς έπρεπε να τύχουν της ανάλογης επεξεργασίας και μετάφρασης[58].

Κατά τον Albrecht (2016) ο νέος κανονισμός δεν θα άλλαζε μόνον την Ευρώπη αλλά και τον κόσμο όλο. Σκοπός του ήταν να οριοθετήσει σαφώς τις σε επίπεδο προσωπικών δεδομένων παραβιάσεις που προέκυπταν κατά την επεξεργασία ενώ έγινε εκτελεστός ώστε να προλάβει τις απειλές από την κυβερνο-επιθέσεις και να ανταποκριθεί σ' αυτές, διασφαλίζοντας μια μελλοντική ανθεκτικότητα σε σχέση με την προϋφιστάμενη οδηγία (Krystlik, 2017). Η επταετής και συγκρουσιακή πορεία έως την κατάρτιση του τελικού κειμένου του, καταδεικνύει την πολυπλοκότητα του συγκεκριμένου πεδίου πολιτικής, την υψηλή τεχνικότητα που το διέπει και την ταχύτητα με την οποία μεταβάλλονται κυρίως οι τεχνολογικοί όροι που το επηρεάζουν καθώς, πριν καλά καλά προλάβει να ρυθμίσει το εν λόγω πεδίο, η τεχνολογία το έχει ήδη ξεπεράσει.

Μέσα σ' αυτό το γενικό πλαίσιο ψηφίστηκαν τελικά ο Ευρωπαϊκός Κανονισμός (ΕΕ) 2016/679 και η Οδηγία 2016/680/ΕΕ τα οποία η χώρα μας ενσωμάτωσε στην εθνική νομοθεσία με τον προαναφερόμενο κυρωτικό Ν. 4624/2019[59].

3.2. Οι λόγοι θεσμοθέτησης του νέου Κανονισμού

Με δεδομένες τις πολιτικές και οικονομικές συνθήκες που σκιαγραφήθηκαν ανωτέρω, η θεσμοθέτηση ενός πλέγματος προστασίας των προσωπικών δεδομένων ήταν αναμενόμενη αλλά κι επιβεβλημένη. Η υπογραφή του ΓΚΠΔ επισφράγισε την αδήριτη ανάγκη πρόληψης από την τεχνολογική απειλή. Η αλματώδης τεχνολογική εξέλιξη που δημιούργησε νέες δυνατότητες και ευκαιρίες, εγκυμονούσε σωρεία κινδύνων αναφορικά με την προστασία των προσωπικών δεδομένων. Αυτό είχε ως αποτέλεσμα την ανάγκη να ανακαθοριστούν οι νομικές έννοιες και να θεσπιστούν νέες ρυθμίσεις, προκειμένου να

[58]Στις 4 Μαΐου 2016 ο Κανονισμός (ΕΚ) 2016/679 και η Οδηγία (ΕΕ) 2016/680 δημοσιεύθηκαν στην Επίσημη Εφημερίδα της ΕΕ, στις 5 Μαΐου 2016 τέθηκε σε ισχύ η Οδηγία και στις 24 Μαΐου 2016 και ο Κανονισμός. Στις 6 Μαΐου 2018 τα Κράτη Μέλη ανέλαβαν την υποχρέωση να ενσωματώσουν την Οδηγία στο εθνικό τους δίκαιο και στις 25 Μαΐου 2018 τον Κανονισμό, αντίστοιχα.

[59] Για Ν. 4624/2019 βλ. σχετικά όπ.α. σελ. 31 επ.

διασφαλιστεί η προστασία του υποκειμένου των δεδομένων και κατ' επέκταση του δημοκρατικού πολιτεύματος (Γέροντας, 2002).

Ως εκ τούτου ο βασικότερος ίσως λόγος της θεσμοθέτησης του ΓΚΠΔ ήταν η ανάγκη, που δημιουργήθηκε λόγω των τεχνολογικών αυτών εξελίξεων αλλά και της τεράστιας αξίας που απέκτησαν τα δεδομένα στη σύγχρονη εποχή, για επικαιροποίηση του δικαίου ώστε να παρακολουθήσει την τεχνολογία, να προσαρμοστεί στη σύγχρονη ψηφιακή πραγματικότητα για να θεμελιωθεί ένα κλίμα εμπιστοσύνης αναφορικά με την ασφάλεια των συναλλαγών και να επιτευχθεί μια ενιαία αντιμετώπιση στο εσωτερικό της 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 δεδομένων (Λεμπέση, 2018).

Επιπλέον οι αιτιολογικές σκέψεις 6 και 7 του Προοιμίου του ΓΚΠΔ αποτυπώνουν ως λόγους ανάγκης της θεσμοθέτησης ενός νέου κανονισμού εκτός από τις ραγδαίες τεχνολογικές εξελίξεις και την παγκοσμιοποίηση, την αύξηση της κλίμακας συλλογής και ανταλλαγής προσωπικών δεδομένων, την εντεινόμενη χρήση των δεδομένων από ιδιωτικές επιχειρήσεις και δημόσιες αρχές, κατά την επιδίωξη των δραστηριοτήτων τους και την αυξανόμενη οικειοθελή δημοσιοποίηση προσωπικών πληροφοριών από τα φυσικά πρόσωπα.

Πολύ σύντομα αποδείχθηκε και η αδυναμία της Οδηγίας 95/46/ΕΚ, που συνιστούσε το τότε ισχύον ενωσιακό δίκαιο, να παρακολουθήσει τη ραγδαία τεχνολογική εξέλιξη[60], την παγκοσμιοποίηση, την ελεύθερη και απρόσκοπτη πρόσβαση στο διαδίκτυο με την χρήση κινητών τερματικών συσκευών, τα μέσα κοινωνικής δικτύωσης και τις υπηρεσίες clouds (ΣΕΒ, 2018). Ένα από τα μειονεκτήματά της συνίστατο στο ότι δεν εστίαζε απευθείας στην προστασία των προσωπικών δεδομένων και δεν αντιμετώπισε την προστασία της ιδιωτικής ζωής ως απόλυτο δικαίωμα. Κι αυτό γιατί επεδίωκε την απελευθέρωση της κυκλοφορίας των δεδομένων στο εσωτερικό της Κοινότητας προς διευκόλυνση των

[60] Όταν εκδόθηκε η εν λόγω Οδηγία λίγοι γνώριζαν το διαδίκτυο και ελάχιστοι μπορούσαν να προβλέψουν την εξέλιξή του και το βαθμό διάδοσης, μέσω αυτού, προσωπικών πληροφοριών τόσο από τις ιδιωτικές επιχειρήσεις όσο και τις δημόσιες πλέον αρχές, ούτε φυσικά την διάθεση των ατόμων να επιτρέπουν την κυκλοφορία των δεδομένων τους μέσω των Μέσων Κοινωνικής Δικτύωσης ή την αύξηση της εμπορευματοποίησής τους. Σύμφωνα δε με μελέτη της International Data Corporation (IDC) εκτιμάται ότι το 2025 ο όγκος δεδομένων θα αυξηθεί από 16,1 ZB σε 163 ZB (1ZB=10 bytes), ο μέσος άνθρωπος θα αλληλεπιδρά σε μια συνδεδεμένη συσκευή 4.800 φορές ημερησίως ενώ η αξία της αγοράς των προσωπικών δεδομένων θα έχει ανέλθει το 2020 σε σχεδόν 1 τρις, βλ. σχετικά https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_387.

τεσσάρων κοινοτικών ελευθεριών με άκρο όριο το θεμελιώδες δικαίωμα της ιδιωτικότητας (Παναγοπούλου-Κουτνατζή, 2017). Εν μέσω περιβάλλοντος τεχνολογικής «έκρηξης», έπρεπε να εξασφαλίσει την εναρμόνιση των νομοθεσιών των κρατών-μελών για να διασφαλιστεί το υψηλό επίπεδο προστασίας των πολιτών, η ελεύθερη κυκλοφορία των δεδομένων και η αποτελεσματική λειτουργία της εσωτερικής αγοράς, στόχος δύσκολα πραγματοποιήσιμος αφού έδινε στον εθνικό νομοθέτη την ευχέρεια ανάπτυξης πρωτοβουλιών ανάλογα με τις ιδιαιτερότητες του δικαίου του .

Οι διαφορές μεταξύ των κρατών μελών αναφορικά με την επεξεργασία και το επίπεδο της προστασίας των προσωπικών τους δεδομένων, ήταν πολλές με αποτέλεσμα η Οδηγία να μην μπορεί να υλοποιήσει τους στόχους της, να παρεμποδίζεται η ελεύθερη κυκλοφορία των δεδομένων στην Ε.Ε. και κατ' επέκταση η άσκηση των οικονομικών δραστηριοτήτων σε επίπεδο Ένωσης καθώς και να σημειώνεται στρέβλωση του ανταγωνισμού και παρακώλυση των αρχών στην εκτέλεση των υποχρεώσεών τους επί τη βάσει του ευρωπαϊκού δικαίου[61]. Αν και οι περισσότερες αρχές προστασίας των προσωπικών δεδομένων που υφίστανται στον ΓΚΠΔ, προϋπήρχαν και στο κείμενο της Οδηγίας, η τελευταία δεν κατάφερε να αποτρέψει τον κατακερματισμό της εφαρμογής της προστασίας τους σε όλη τη Ε.Ε., την ανασφάλεια δικαίου αλλά ούτε και να αντιμετωπίσει την ύπαρξη σοβαρών κινδύνων ως προς τα δεδομένα που προέκυπταν κυρίως σε επίπεδο επιγραμμικής δραστηριότητας (Παναγοπούλου-Κουτνατζή, 2017). Η προσπάθεια της οδηγίας να εναρμονίσει τις εθνικές νομοθεσίες στην προστασία των προσωπικών δεδομένων απέβη άκαρπη, καθώς τα κράτη μέλη εκμεταλλευόμενα την νομική της μορφή προς όφελός τους, δεν συμμορφώνονταν πλήρως με τις επιταγές της, με αποτέλεσμα να μην εξασφαλίζεται ενιαία και συνεκτική της εφαρμογή (ΣΕΒ 2018) [62].

Όλοι αυτοί οι λόγοι αυτοί που περιγράφουν το μετέωρο καθεστώς στο οποίο τελούσε η προστασία των προσωπικών δεδομένων αποκαλύπτουν τις ρυθμιστικές ελλείψεις της Οδηγίας και τα ασυμβίβαστα, με τη σύγχρονη τεχνολογική εξέλιξη, στοιχεία της και αποδεικνύουν ότι συνετέλεσαν στην δημιουργία ενός νέου ευρωπαϊκού νομοθετήματος, «ενδεδυμένου» αυτή τη φορά με τη μορφή ενός κανονισμού. Εύλογα μπορεί κανείς να πει

[61] Βλ. σχετικά ΣΕΒ 2018, διαθέσιμο σε: https://www.sev.org.gr/Uploads/Documents/51628/meleti_sev_GDPR_final.pdf

[62] Με δεδομένη την ύπαρξη 28 διαφορετικών εθνικών νομοθεσιών για την προστασία των προσωπικών δεδομένων, το αποτέλεσμα ήταν πολλές επιχειρήσεις να αντιμετωπίζουν περιορισμούς εισόδου σε νέες αγορές και να υφίστανται περιττά κόστη και διοικητικά βάρη συμμόρφωσης.

ότι ο νέος Κανονισμός αποτελεί μια χαρακτηριστική περίπτωση εκ των υστέρων ρύθμισης, όπου ο νομοθέτης έρχεται να «θεραπεύσει» δρώντας μάλλον κατασταλτικά παρά προληπτικά, δοθέντος ότι η τεχνολογία προπορεύεται του δικαίου και ίσως ακόμη και της ηθικής.

3.3. Τα βασικά χαρακτηριστικά του Κανονισμού και οι καινοτομίες που εισάγει

Ο νέος Κανονισμός, που αποτελεί και την πιο πρόσφατη νομοθετική εξέλιξη της Ε.Ε. αποτελεί ένα ιδιαίτερα φιλόδοξο κείμενο, που έχει συγκεντρώσει τα επιστημονικά και επιχειρηματικά βλέμματα που επιδιώκει να διαφυλάξει την ασφάλεια και την προστασία των προσωπικών δεδομένων των φυσικών προσώπων. Συνιστά έναν «έξυπνο» Κανονισμό, που χρήζει «έξυπνης» ερμηνείας και του οποίου η εφαρμογή προϋποθέτει την κατανόηση της ουσίας του (Μίττλετον 2018). Ο ΓΚΠΔ φιλοδοξεί μέσα σε καθεστώς αβεβαιότητας του σύγχρονου κόσμου και των αλλεπάλληλων παραβιάσεων των προσωπικών δεδομένων, να διασφαλίσει ένα υψηλό επίπεδο προστασίας των δεδομένων και να αποτελέσει παγκόσμιο πρότυπο αντιμετώπισης των μελλοντικών κινδύνων κατά της ελευθερίας.

Αντίθετα με την Οδηγία, ο ΓΚΠΔ -που από τη φύση του του διαθέτει γενική, καθολική και άμεση ισχύ, χωρίς περαιτέρω διαδικασία έκδοσης εθνικού νομοθετήματος για να ισχύσει ταυτόχρονα στο εσωτερικό των κρατών μελών-, εξασφάλισε ήδη από την υπογραφή του, το έως τότε ανύπαρκτο, ομοιόμορφο και συνεκτικό νομικό πλαίσιο προστασίας των προσωπικών δεδομένων εντός της Ε.Ε. (Μενουδάκος, 2018).

Ο Κανονισμός περιέχει, όπως προαναφέρθηκε, αρκετές *«ρήτρες ανοίγματος» ή «ρήτρες ευελιξίας»* με τις οποίες επιτρέπει στον εθνικό νομοθέτη κάθε κράτους μέλους, να προβαίνει σε «εσωτερικές επιλογές», να αποφαίνεται κατά το δικό του δίκαιο και να εξειδικεύει τους κανόνες του, αποδεικνύοντας πως πρόκειται για ένα ευέλικτο και δυναμικό ευρωπαϊκό συμβατικό κείμενο, προσαρμοσμένο στις σύγχρονες ανάγκες της οικονομικής, κοινωνικής και ιδιωτικής δράσης που τελεί σε άμεση σχέση με τα δεδομένα και την εξέλιξη της τεχνολογίας. Δικαίως χαρακτηρίζεται ως «κανονοδηγία» ή «ατυπικό υβρίδιο»[63], αν και αρκετοί θεωρούν ότι αυτή η ευελιξία θίγει την ιδιότητα του Κανονισμού ως ενωσιακό νομοθετικό κείμενο καθολικής και ομοιόμορφης εφαρμογής (Παναγοπούλου-Κουτνατζή, 2017 και αιτ. σκ. 10 ΓΚΠΔ).

[63] Βλ. σχετικά Αιτιολογική Έκθεση Ν. 4624/2019.

Παρά το γεγονός ότι δεν επεδίωξε τη ριζική αναμόρφωση του πλαισίου προστασίας των δεδομένων προσωπικού χαρακτήρα, ο ΓΚΠΔ την επαναπροσδιόρισε ως αυτοτελές θεμελιώδες δικαίωμα. Η ενσωμάτωση των κανόνων δικαίου που εισήγαγε στο εσωτερικό των κρατών μελών, επιδιώκει την ενίσχυση της προστασίας των προσωπικών δεδομένων και την θέσπιση ενός αυστηρού καθεστώτος, διατηρώντας τις βασικές αρχές του προϊσχύοντος θεσμικού πλαισίου αλλά προσθέτοντας σ' αυτές τη βασική αρχή της λογοδοσίας και την ασφάλεια, εμπλουτίζοντάς τες, κυρίως μέσω της νομολογίας του ΔΕΕ, υπό το πρίσμα μάλιστα ενός αποτελεσματικότερου ελέγχου του σεβασμού των κανονιστικού πλαισίου του ΓΚΠΔ, κι αποτελώντας έτσι το σκαλοπάτι για την μετάβαση στην τέταρτη γενιά κανόνων δικαίου αναφορικά με την προστασία των δεδομένων και της ιδιωτικότητας εν γένει (Μενουδάκος, 2018).

Βασικός στόχος του είναι να *διευρύνει* τα δικαιώματα των υποκειμένων των δεδομένων, προσθέτοντας το δικαίωμα στη λήθη και στη φορητότητα,[64] ενισχύοντας τη δικονομική θέση των υποκειμένων των προσωπικών δεδομένων. Παραταύτα, εξακολουθεί να μην ανάγει την προστασία των προσωπικών δεδομένων σε *απόλυτο δικαίωμα* που υπερισχύει έναντι της ελευθερίας του τύπου ή της πληροφόρησης, ασπαζόμενος κι αυτός την έλλειψη ιεραρχίας μεταξύ των ατομικών δικαιωμάτων και υιοθετώντας εν αμφιβολία τη στάθμιση εννόμων αγαθών και την πρόκριση ενός εκ των δύο συγκρουομένων δικαιωμάτων, επί τη βάσει της αρχής της αναλογικότητας, ως μια μορφή διανεμητικής δικαιοσύνης (Παναγοπούλου-Κουτνατζή, 2016).

Σε κάθε περίπτωση αντικατοπτρίζει τη βούληση του ευρωπαίου νομοθέτη αφενός μεν να διασφαλίσει ένα θεμελιώδες δικαίωμα που τελεί στο επίκεντρο του κώδικα αξιών της ευρωπαϊκής έννομης τάξης, ενόψει της ταχύτατης ψηφιακής εποχής και της παγκοσμιοποιημένης ψηφιακής οικονομίας[65] (Rodriguez Teresa des las Heras Ballell) αφετέρου δε, να εξασφαλίσει την *ορθή και απρόσκοπτη λειτουργία των επιχειρήσεων* και την *ενίσχυση της ενιαίας αγοράς*, που κι αυτή συνιστά θεμελιώδη βάση του ευρωπαϊκού οικοδομήματος[66]. Μάλιστα ο ΓΚΠΔ εν πρώτοις φαίνεται να δημιουργεί τα εχέγγυα ανάπτυξης των κατάλληλων συνθηκών για την προώθηση της άσκησης των οικονομικών

[64] https://ec.europa.eu/commission/presscorner/detail/en/MEMO_17_1441
[65] Άλλως «οικονομία ψηφιακής πλατφόρμας».
[66] Ερωτήσεις και απαντήσεις - Γενικός κανονισμός για την προστασία δεδομένων, διαθέσιμο σε https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_387

δραστηριοτήτων και του ανταγωνισμού, σεβόμενος την ιδιωτικότητα και τα προσωπικά δεδομένα (Μενουδάκος, 2018)[67].

Το πλέγμα προστασίας των δεδομένων εκτείνεται και στη συγκατάθεση των υποκειμένων για επεξεργασία και ιδιαιτέρως όταν πρόκειται για επεξεργασία δεδομένων ανηλίκων αποδεικνύοντας την αυξημένη έγνοια του νομοθέτη στην ευάλωτη αυτή κατηγορία υποκειμένων ενώ η εφαρμογή των διατάξεών του καταλαμβάνει τους δημόσιους και ιδιωτικούς φορείς εντός της Ε.Ε. αλλά και όσων διαχειρίζονται δεδομένα υποκειμένων με φυσική παρουσία στην Ε.Ε. που η έδρα τους βρίσκεται εκτός αυτής[68].

Περαιτέρω ο ΓΚΠΔ *ενισχύει το ρόλο και τις υποχρεώσεις των υπευθύνων επεξεργασίας* που διορίζονται πλέον υποχρεωτικά και καθορίζει τις απαιτούμενες ενέργειες αντιμετώπισης των περιστατικών παραβίασης, με πρώτη και *βασική υποχρέωσή του την γνωστοποίηση* της *παραβίασης προσωπικών δεδομένων στην εποπτική αρχή* αλλά *και στο ίδιο το υποκείμενο*, εάν η παραβίαση των δεδομένων ενδέχεται να θέσει *σε υψηλό κίνδυνο τα δικαιώματά του*[69]. Έτσι ο ΓΚΠΔ καταργεί τον προληπτικό έλεγχο που διενεργούταν από τις εποπτικές αρχές μέσω των γνωστοποιήσεων και της χορήγησης αδειών κι επιφέρει αλλαγές στις αρμοδιότητες τους, μεταθέτοντάς αρκετές απ' αυτές στο πρόσωπο που έχει τον πρωταγωνιστικό ρόλο στο νέο Κανονισμό, ήτοι τον υπεύθυνο επεξεργασίας.

Ο κανονισμός θέτει επίσης στον υπεύθυνο επεξεργασίας την υποχρέωση *εκπόνησης μελέτης επιπτώσεων/αντικτύπου πριν τη διενέργεια κάποιας επικίνδυνης επεξεργασίας* προσωπικών δεδομένων (Κανελλάκη, 2016), συγκεκριμενοποιεί τα *τεχνικά μέτρα* κάνοντας ρητή αναφορά στην τεχνική της *κρυπτογράφησης* (encryption) και της *ψευδωνυμοποίησης* (pseudonymisation)[70] και θεσμοθετεί ένα νέο όργανο, τον Υπεύθυνο Προστασίας Δεδομένων[71] (Παναγοπούλου-Κουτνατζή, 2017). Προβλέπει *βαρύτατες*

[67] Για τα οφέλη που θα έχουν οι επιχειρήσεις από την εφαρμογή του ΓΚΠΔ βλ. όπ.α. σε https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_387

[68] Βλ. Ομάδα Εργασίας άρθρου 29, Κατευθυντήριες Γραμμές για τη Συγκατάθεση σύμφωνα με το Κανονισμό 2016/679, 17/EN, WP 259.

[69] Για να γνωστοποιήσει ο υπεύθυνος επεξεργασίας την τυχόν διαρροή πρέπει να γνωρίζει σε τι ακριβώς συνίσταται αυτή, και για να είναι σε θέση να το γνωρίζει πρέπει να παρακολουθεί διαρκώς τις διαδικασίες, τα πρωτόκολλα και τις ροές δεδομένων, βλ. σχετικά https://www.sev.org.gr/Uploads/Documents/51628/meleti_sev_GDPR_final.pdf

[70] Βλ. σχετικά Λουκά Ν., Τεχνικά μέτρα του Γενικού Κανονισμού για την Προστασία Δεδομένων (GDPR), διαθέσιμο σε https:// www.dpoacademy.gr/el/arthra2/.

[71] Εφεξής ΥΠΔ.

διοικητικές κυρώσεις για τους παραβάτες, και αναγνωρίζει *αστική ευθύνη* προς αποζημίωση στον *υπεύθυνο επεξεργασίας όσο και τον εκτελούντα την επεξεργασία*.

Ο Κανονισμός διαπνέεται από την ιδέα της *καλής συνεργασίας* μεταξύ υπευθύνου επεξεργασίας και εποπτικών αρχών και *ενισχύει της διακρατική συνεργασία* μεταξύ των εθνικών Αρχών Προστασίας Δεδομένων θεσπίζοντας διαδικασίες, μηχανισμούς συνεργασίας και συνοχής, με τους οποίους διαφοροποιείται η δράση των εποπτικών αρχών και προωθείται η αμοιβαία συνδρομή και οι κοινοί έλεγχοι. Ο *μηχανισμός «one stop shop»*[72] που εισάγει, επιδιώκει μέσω της συνεργασίας μεταξύ εποπτικής αρχής του κράτους κύριας εγκατάστασης και των εθνικών αρχών, να πετύχει την ομοιόμορφη εφαρμογή του ΓΚΠΔ (Παναγοπούλου-Κουτνατζή, 2017).

Τέλος, ο κανονισμός εστιάζει στην *ανεξαρτησία των εποπτικών αρχών* οι οποίες διατηρούν την τριπλή λειτουργία, ενημερωτική, ρυθμιστική και ελεγκτική που διέθεταν και υπό το καθεστώς της προγενέστερης Οδηγίας.

Η πρόνοια της διετούς μεταβατικής περιόδου μέχρι να τεθεί σ' εφαρμογή ο ως άνω Κανονισμός, κρίθηκε απαραίτητη για να εξασφαλιστεί η πληρέστερη ενημέρωση και προετοιμασία των υπεύθυνων επεξεργασίας, εκτελούντων επεξεργασία, αρμόδιων εποπτικών αρχών, εθνικών νομοθεσιών και δικαστηρίων. Δοθέντος ότι η Ε.Ε. συνιστά σύνολο κρατών με διαφορετικά ήθη, ιστορία και κουλτούρες, θα έπρεπε αυτά να συγχρονιστούν σ' ενωσιακό επίπεδο στα πλαίσια του νέου Κανονισμού, προκειμένου να καλυφθούν οι σύγχρονες ψηφιακές ανάγκες (Μενουδάκος, 2018).

[72] Ο μηχανισμός συνεργασίας και συνεκτικότητας, γνωστός ως One Stop Shop (υπηρεσία μιας στάσης) συνιστά μια σημαντική καινοτομία του ΓΚΠΔ καθώς ισοδυναμεί με έναν αποτελεσματικό μηχανισμό εποπτείας και επιβολής, με αποφασιστικές αρμοδιότητες. Πρόκειται για ένα μονοαπευθυντικό σύστημα κατά το οποίο δίνεται η δυνατότητα να εξετάζονται ζητήματα προστασίας προσωπικών δεδομένων σε ένα κράτος μέλος στο οποίο αφορά η επεξεργασία, και του οποίου η εποπτική αρχή θεωρείται Επικεφαλής Εποπτική Αρχή (ΕΕΑ), όταν ένας υπεύθυνος επεξεργασίας ή εκτελών επεξεργασία είναι εγκατεστημένος σε περισσότερα από ένα κράτη μέλη.
Μέσω του μηχανισμού αυτού επιβεβαιώνεται η ευρωπαϊκή διάσταση του ΓΚΠΔ καθώς η επικεφαλής εποπτική αρχή συνεργάζεται με τις ενδιαφερόμενες εθνικές αρχές στην αρμοδιότητα των οποίων μπορεί να εμπίπτει μια υπόθεση και καθιερώνεται η διακρατική ισχύ των διοικητικών πράξεων στην ΕΕ. Αυτό πρακτικά σημαίνει ότι δια του μηχανισμού One Stop Shop μία διοικητική απόφαση που έχει ληφθεί σε ένα κράτος-μέλος είναι δεσμευτική και παράγει έννομα αποτελέσματα σε ολόκληρο το έδαφος της Ε.Ε. Ο μηχανισμός συνεργασίας αφορά κυρίως τη συνεργασία της επικεφαλής αρχής με τις ενδιαφερόμενες εποπτικές αρχές στα πλαίσια της διερεύνησης καταγγελίας που εμπλέκει περισσότερα από ένα κράτη-μέλη καθώς και οποιαδήποτε αρμοδιότητα των εποπτικών αρχών που αφορά σε διασυνοριακές πράξεις επεξεργασίας. Ο μηχανισμός συνεκτικότητας αφορά στις διασυνοριακές ροές δεδομένων και επιδιώκει να επιτύχει την επίλυση των διαφορών κατά τρόπο συνεκτικό. Αναφέρεται στη διαδικασία λήψης αποφάσεων από το ΕΣΠΔ.

3.4. Δομή και Διάρθρωση του Κανονισμού

Ο ΓΚΠΔ είναι ένα εκτενές νομικό κείμενο που αποτελείται από 11 κεφάλαια και 99 άρθρα[73], ξεκινώντας μάλιστα με ένα εξίσου μακροσκελές προοίμιο που εμπεριέχει 173 αιτιολογικές σκέψεις που οδήγησαν στην έκδοσή του.

Στο Κεφάλαιο Ι αναφέρονται οι *Γενικές διατάξεις* σχετικά με το αντικείμενο και τους στόχους του Κανονισμού, το ουσιαστικό και εδαφικό πεδίο εφαρμογής και τους βασικότερους ορισμούς (άρθρα 1-4).

Στο Κεφάλαιο ΙΙ αποτυπώνονται οι *Αρχές* επεξεργασίας των δεδομένων προσωπικού χαρακτήρα (άρθρο 5), οι προϋποθέσεις νομιμότητας της επεξεργασίας (άρθρο 6), οι προϋποθέσεις συγκατάθεσης (άρθρα 7,8) και άλλες σχετικές διατάξεις (άρθρα 9-11).

Το Κεφάλαιο ΙΙΙ αναφέρεται στα *Δικαιώματα του υποκειμένου* των δεδομένων και χωρίζεται σε 5 τμήματα. Το Τμήμα 1 (άρθρα 12-23) προβλέπει τα σχετικά με τη διαφάνεια και τις σχετικές ρυθμίσεις, το Τμήμα 2 (άρθρα 13-15) την ενημέρωση και πρόσβαση σε δεδομένα προσωπικού χαρακτήρα, το Τμήμα 3 (άρθρα 16-20) τη διόρθωση και διαγραφή, το Τμήμα 4 (άρθρο 21 & 22) το δικαίωμα εναντίωσης και την αυτοματοποιημένη ατομική λήψη αποφάσεων, το Τμήμα 5 (άρθρο 23) τους περιορισμούς των δικαιωμάτων.

Το Κεφάλαιο ΙV αναφέρεται στον υπεύθυνο επεξεργασίας και τον εκτελούντα την επεξεργασία, αποτελείται από πέντε Τμήματα (άρθρα 24 έως 43). Το Τμήμα 1 (άρθρα 24-31) αναφέρεται στις *Γενικές Υποχρεώσεις* του Υπεύθυνου επεξεργασίας, το Τμήμα 2 (άρθρα 32-34) στην *Ασφάλεια των Δεδομένων προσωπικού χαρακτήρα,* το Τμήμα 3 (άρθρα 35-36) στην *Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων και προηγούμενη διαβούλευση,* το Τμήμα 4 (άρθρα 37-39) στον *Υπεύθυνο προστασίας δεδομένων*.

Το Κεφάλαιο V αναφέρεται στις *Διαβιβάσεις δεδομένων Προσωπικού Χαρακτήρα προς τρίτες χώρες ή διεθνείς οργανισμούς* (άρθρα 44-50)[74].

Το Κεφάλαιο VI αναφέρεται στις *Ανεξάρτητες εποπτικές αρχές* και αποτελείται από 2 τμήματα (άρθρα 51-59) εκ των οποίων το Τμήμα 1 ασχολείται με το ανεξάρτητο καθεστώς που τις διέπει ενώ το Τμήμα 2 με την αρμοδιότητα, τα καθήκοντα και τις εξουσίες τους.

[73] Βλ. σχετικά Επίσημη Εφημερίδα Ευρωπαϊκής Ένωσης ΕΕ L 119/1, 4.5.2016

[74] Η ύπαρξη του κεφαλαίου αυτού οφείλεται στις πρόσφατες εξελίξεις στο μεταναστευτικό τομέα.

Το Κεφάλαιο VII (άρθρα 60-76) αναφέρεται στη *Συνεργασία και συνεκτικότητα* (άρθρα 60-76) και αποτελείται από 3 τμήματα. Το Τμήμα 1 αναφέρεται στη συνεργασία μεταξύ των εποπτικών αρχών των κρατών μελών, το Τμήμα 2 στον μηχανισμό συνεκτικότητας, τον τρόπο συνεργασίας μεταξύ των αρχών αλλά και την εμπλοκή του Συμβουλίου Προστασίας Δεδομένων, το Τμήμα 3 στο Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων.

Το Κεφάλαιο VIII (άρθρα 77-84) αναφέρεται στις *Προσφυγές, την Ευθύνη και τις Κυρώσεις* που επέρχονται επί παραβίασης προσωπικών δεδομένων.

Το Κεφάλαιο IX (άρθρα 85-93) εμπεριέχει *Διατάξεις που αφορούν ειδικές περιπτώσεις επεξεργασίας προσωπικών δεδομένων*, όπως εκείνη της επεξεργασίας και ελευθερίας έκφρασης και πληροφόρησης, επεξεργασίας και πρόσβασης του κοινού σε επίσημα έγγραφα, επεξεργασία του εθνικού αριθμού ταυτότητας, επεξεργασίας στο πλαίσιο της απασχόλησης, επεξεργασίας για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή για σκοπούς στατιστικούς.

Στο Κεφάλαιο X γίνεται ρητή αναφορά στις *Κατ' εξουσιοδότηση πράξεις και εκτελεστικές πράξεις* (άρθρα 92 και 93).

Το Κεφάλαιο XI που είναι και το τελευταίο, εμπεριέχει τις *Τελικές διατάξεις* (άρθρα 92 και 93) μεταξύ των οποίων είναι κι η διάταξη που καταργεί την οδηγία 95/46/ΕΚ.

3.5. Ανάλυση των βασικότερων διατάξεων του ΓΚΠΔ

3.5.1. Αντικείμενο και Στόχοι του Κανονισμού

Ο νέος κανονισμός εισάγει ένα σύνθετο θεσμικό πλαίσιο καθώς θεσπίζει *δύο ειδών* κανόνες, ήτοι *αυτούς που λειτουργούν προστατευτικά* για τα φυσικά πρόσωπα απέναντι στην επεξεργασία των προσωπικών τους δεδομένων *και αυτούς που αφορούν στην ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα* (άρθρο 1 παρ.1). Επιδιώκει αφενός να προστατεύσει θεμελιώδη δικαιώματα και ελευθερίες των ατόμων και δη το δικαίωμα στην προστασία των προσωπικών δεδομένων ως ειδικότερη έκφανση της ιδιωτικότητας του ατόμου (άρθρο παρ.2) κι αφετέρου να μην περιορίσει την ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα εντός της Ε.Ε. (άρθρο 1 παρ.3). Έτσι ο Κανονισμός καλείται να συγκεράσει δύο κατ' αρχήν αντιφατικά θεμελιώδη δικαιώματα, τα οποία εν πρώτοις λογίζονται ως ισότιμα και κανένα επικρατέστερο έναντι του άλλου, ειμή μόνον σε περίπτωση που αυτό κριθεί αναγκαίο και στο αντίστοιχο μέτρο.

3.5.2 Πεδίο Εφαρμογής Κανονισμού

Το πεδίο εφαρμογής του νέου Κανονισμού διακρίνεται σε ουσιαστικό και εδαφικό.

α. Ουσιαστικό πεδίο εφαρμογής

Ο ΓΚΠΔ εφαρμόζεται εν όλω ή εν μέρει και προστατεύει τα δεδομένα προσωπικού χαρακτήρα ανεξάρτητα από την τεχνολογία που χρησιμοποιείται για την επεξεργασία τους, ήτοι τόσο στην *αυτοματοποιημένη όσο και στη μη αυτοματοποιημένη*, άλλως χειροκίνητη επεξεργασία, αρκεί τα δεδομένα να είναι αρχειοθετημένα, δηλαδή οργανωμένα επί τη βάση προκαθορισμένων κριτηρίων (π.χ. αλφαβητική σειρά). Μ' αυτήν την έννοια υποστηρίζεται ότι είναι *τεχνολογικά ουδέτερος* (ΣΕΒ, 2018). Εξίσου αδιάφορος για τον ΓΚΠΔ, είναι κι *ο τρόπος αποθήκευσης των δεδομένων*. Έτσι είτε η αποθήκευσή τους γίνεται σε σύστημα τεχνολογίας πληροφοριών είτε μέσω βιντεοεπιτήρησης είτε σε έντυπη μορφή, η προστασία των δεδομένων, εμπίπτει στο πεδίο εφαρμογής του Κανονισμού (άρθρο 2 παρ.1)[75].

Ο ΓΚΠΔ εφαρμόζεται στα δεδομένα των *φυσικών μόνο προσώπων* και όχι των νομικών προσώπων, εκτός κι εάν πρόκειται να προστατέψει δεδομένα μιας μονοπρόσωπης εταιρίας ή ατομικής επιχείρησης που νομικά αντιμετωπίζεται ως φυσικό πρόσωπο.

Στο πεδίο εφαρμογής του εμπίπτουν προσωπικά δεδομένα που είτε *έχουν καταστεί ανώνυμα*, είτε έχουν *κρυπτογραφηθεί* είτε έχουν *χρησιμοποιηθεί γι' αυτά ψευδώνυμα* αλλά που *μπορούν να επαναταυτοποιήσουν ένα φυσικό πρόσωπο* καθώς εξακολουθούν να είναι δεδομένα προσωπικού χαρακτήρα. Αντίθετα, όσα έχουν καταστεί ανώνυμα αλλά το άτομο δεν μπορεί να ταυτοποιηθεί εκ νέου, δεν θεωρούνται προσωπικά δεδομένα και δεν εμπίπτουν στο πεδίο εφαρμογής του[76]. Δεν θεωρούνται προσωπικά δεδομένα ο ΑΦΜ εταιρίας, η ηλεκτρονική διεύθυνση μια εταιρίας (με την μορφή …..@όνομα εταιρία.com) ή ανώνυμα δεδομένα.

Ο ΓΚΠΔ *εξαιρεί* του πεδίου εφαρμογής του, τις δραστηριότητες *εκτός του πλαισίου της Ε.Ε.*, τις σχετικές με το κεφάλαιο 2 του τίτλου V ΣΕΕ, τις αποκλειστικά *οικογενειακές ή οικιακές* δραστηριότητες φυσικών προσώπων, *τις ποινικού χαρακτήρα* που εντάσσονται στην Οδηγία 2016/680/ΕΕ και *εκείνες που γίνονται για σκοπούς πρόληψης, διερεύνησης,*

[75] https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_el
[76] Βλ. σχετικά σε https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_el.

ανίχνευσης ή δίωξης ποινικών αδικημάτων ή εκτέλεσης ποινικών κυρώσεων συμπεριλαμβανομένης και της προστασίας και πρόληψης έναντι κινδύνων που απειλούν τη δημόσια ασφάλεια.

β. Εδαφικό πεδίο εφαρμογής

Οι διατάξεις του ΓΚΠΔ εφαρμόζονται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα *στο πλαίσιο των δραστηριοτήτων μιας εγκατάστασης ενός υπευθύνου επεξεργασίας* ή εκτελούντος την επεξεργασία στην Ένωση, *άσχετα με το αν η επεξεργασία πραγματοποιείται εντός ή εκτός της Ένωσης* (άρθρο 3 παρ. 1) (Tikkinen-Piri, Rohunen & Markkyka, 2018), υπενθυμίζοντας την πρόδηλη προσπάθεια παγκοσμιοποίησης του κανονισμού (Ιγγλεζάκης, 2004).

Επίσης εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα *υποκειμένων των δεδομένων που βρίσκονται στην Ε.Ε*. από υπεύθυνο ή εκτελούντα την επεξεργασία που *δεν είναι εγκατεστημένος στην Ε.Ε.*, εάν οι δραστηριότητες επεξεργασίας σχετίζονται είτε με την προσφορά αγαθών ή υπηρεσιών στα υποκείμενα δεδομένων είτε με την παρακολούθηση της συμπεριφοράς τους εντός της Ε.Ε. (άρθρο 3 παρ.2)[77].

Έτσι ο ΓΚΠΔ εφαρμόζεται σε όλους τους οργανισμούς (ιδιωτικού ή δημοσίου τομέα) εντός ή και εκτός Ε.Ε., οι οποίοι προσφέρουν αγαθά και υπηρεσίες σε άτομα που ζουν στο εσωτερικό της Ε.Ε., και συλλέγουν, αποθηκεύουν ή με οποιοδήποτε τρόπο επεξεργάζονται δεδομένα προσωπικού χαρακτήρα πελατών, προμηθευτών, συνεργατών και εργαζόμενων, προωθώντας την ομοιομορφία στο δίκαιο της προστασίας των δεδομένων κι εφαρμόζοντας την αρχή του τόπου της επιχείρησης και του υποκειμένου των δεδομένων (Παναγοπούλου-Κουτνατζή, 2017). Από τις διατάξεις διαφαίνεται η τάση του ευρωπαίου νομοθέτη να τον καταστήσει παγκόσμιο πρότυπο για την προστασία των προσωπικών δεδομένων στο σύνολο σχεδόν των επιχειρήσεων.

3.6. Ορισμός προσωπικών δεδομένων κατά τον ΓΚΠΔ

Σύμφωνα με τη διάταξη του άρθρου 4 παρ.1 «δεδομένα προσωπικού χαρακτήρα» είναι κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο

[77] Βλ. σχετικά https://ec.europa.eu/commission/presscorner/detail/en/MEMO_17_1441

(υποκείμενο των δεδομένων), ήτοι πληροφορίες βάσει των οποίων ταυτοποιείται ή αναγνωρίζεται ένα άτομο. Ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί άμεσα ή έμμεσα μέσω αναφοράς σε κάποιο αναγνωριστικό στοιχείο ταυτότητας (π.χ. όνομα, επώνυμο, ΑΦΜ, ΑΜΚΑ, αναγνωριστικός αριθμός κάρτας, δεδομένα θέσης) καθώς και οποιαδήποτε άλλη πληροφορία που προσιδιάζει στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητά του, μέσα από την οποία μπορεί να γίνει η εξακρίβωση της ταυτότητάς του (π.χ. δεδομένα που φυλάσσονται σε ιατρείο, διαγνωστικό κέντρο ή νοσοκομείο κ.λ.π.) (άρθρο 4 παρ.1). Διακρίνονται σε «απλά προσωπικά δεδομένα» και «ειδικών κατηγοριών» προσωπικά δεδομένα :

«Απλά προσωπικά δεδομένα» είναι τα δεδομένα της θέσης ενός φυσικού προσώπου καθώς και τα επιγραμμικά (on line) αναγνωριστικά στοιχεία ταυτότητας, τα οποία παρέχει συνήθως το υποκείμενο μέσα από συσκευές, εφαρμογές, εργαλεία και πρωτόκολλα και τα οποία διευκολύνουν τον εντοπισμό του υποκειμένου (π.χ. IP address, εντοπισμός θέσης μέσω GPS, cookies, RFID[78]).

«Ειδικών κατηγοριών προσωπικά δεδομένα» βάσει της διάταξης του άρθρου 9 παρ.1 είναι τα γενετικά[79], τα βιομετρικά[80] και τα προσωπικά δεδομένα που αφορούν την υγεία[81]

[78] Radio Frequency Identification, ήτοι ταυτοποίηση μέσω ραδιοσυχνοτήτων.

[79] Σύμφωνα με το ορισμό που δίνεται στο άρθρο 4 παρ. 13 ΓΚΠΔ : *«γενετικά δεδομένα»* είναι *τα δεδομένα προσωπικού χαρακτήρα που αφορούν γενετικά χαρακτηριστικά φυσικού προσώπου που κληρονομήθηκαν ή αποκτήθηκαν όπως προκύπτουν ιδίως από ανάλυση βιολογικού δείγματος του εν λόγω φυσικού προσώπου και τα οποία παρέχουν μοναδικές πληροφορίες σχετικά με τη φυσιολογία ή την υγεία του εν λόγω φυσικού προσώπου*.

[80] Σύμφωνα με τον ορισμό που δίνεται στο άρθρο 1 παρ. 14 ΓΚΠΔ: *«βιομετρικά δεδομένα»* είναι *δεδομένα προσωπικού χαρακτήρα τα οποία προκύπτουν από ειδική τεχνική επεξεργασία συνδεόμενη με φυσικά, βιολογικά ή συμπεριφορικά χαρακτηριστικά φυσικού προσώπου και τα οποία επιτρέπουν ή επιβεβαιώνουν την αδιαμφισβήτητη ταυτοποίηση του εν λόγω φυσικού προσώπου, όπως εικόνες προσώπου ή δακτυλοσκοπικά δεδομένα*.
Συνήθως αυτά χρησιμοποιούνται για την εκτέλεση εργασιών σε διαφορετικούς τομείς και υπό την ευθύνη κάποιων φορέων όπως λ.χ. για την είσοδο, έξοδο, πρόσβαση σε εργασιακό χώρο ή χώρο υψίστης ασφαλείας, για την ασφάλεια χρήσης λογισμικού, για τον συνοριακό έλεγχο, για την επαλήθευση γνησιότητας ταξιδιωτικών εγγράφων, στην ηλεκτρονική τραπεζική πρακτική, στην ηλεκτρονική υγεία, στην επιστημονική έρευνα αλλά και στην διενέργεια εγκληματολογικών ερευνών. Στην καθημερινότητα βιομετρικά δεδομένα αποθηκεύονται στις έξυπνες φορητές συσκευές , όπως π.χ. κινητά τηλέφωνα τα οποία προκειμένου να ξεκλειδώσουν το μενού τους, αναγνωρίζουν το χρήστη τους μέσω του δακτυλικού του αποτυπώματος ή της δομής του προσώπου του κ.λ.π.. Βλ. Ε. Βασιλόπουλο, σε Κοτσαλή & Μενουδάκο, 2020.

[81] Σύμφωνα με το ορισμό που δίνεται στο άρθρο 4 παρ. 15 ΓΚΠΔ: *«δεδομένα που αφορούν την υγεία»* είναι *τα δεδομένα προσωπικού χαρακτήρα τα οποία σχετίζονται με την σωματική ή ψυχική υγεία ενός φυσικού προσώπου ,περιλαμβανομένης της παροχής υπηρεσιών υγειονομικής φροντίδας και τα οποία αποκαλύπτουν πληροφορίες σχετικά με την κατάσταση της υγείας του*.

(ιατρικές διαγνώσεις, γνωματεύσεις, φαρμακευτικές συνταγές, συνταγές για κλινικές εξετάσεις, παραπεμπτικά, αποτελέσματα εργαστηριακών και απεικονιστικών εξετάσεων) ή εκείνα που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές πεποιθήσεις, τη συμμετοχή σε συνδικαλιστική οργάνωση, τις σεξουαλικές προτιμήσεις και το γενετήσιο προσανατολισμό, τις ποινικές διώξεις ή καταδίκες. Ο ΓΚΠΔ τα μετονόμασε από ευαίσθητα δεδομένα[82] σε «δεδομένα ειδικών κατηγοριών» και προσέθεσε (σε σχέση με την προγενέστερη Οδηγία 95/46/ΕΚ) σ' αυτά τα γενετικά δεδομένα, τα βιομετρικά δεδομένα, τα δεδομένα που αφορούν την υγεία, τις διοικητικές κυρώσεις, τις δικαστικές αποφάσεις και τα ποινικά αδικήματα ή εικαζόμενα αδικήματα, τις ποινικές καταδίκες ή τα σχετικά μέτρα ασφαλείας.

3.7. Οι αρχές που διαπνέουν το Γενικό Κανονισμό

Σύμφωνα με το άρθρο 5 ΓΚΠΔ ο Υπεύθυνος Επεξεργασίας και ο Εκτελών αυτήν πρέπει να εφαρμόζουν τις εξής βασικές αρχές κατά την επεξεργασία των προσωπικών δεδομένων:

α. αρχή νομιμότητας, αντικειμενικότητας και διαφάνειας

Η νομιμότητα της επεξεργασίας διασφαλίζεται όταν η επεξεργασία γίνεται σύμφωνα με κάποια από τις νομιμοποιητικές βάσεις του άρθρου 6 ΓΚΠΔ[83]. Η διαφάνεια[84] εξασφαλίζεται μέσω της παροχής κάθε πληροφορίας και ανακοίνωσης σχετικά με την επεξεργασία κατά τρόπο συνοπτικό, διαφανή και κατανοητό, σε εύκολα προσβάσιμη μορφή. Η πληροφόρηση ή ανακοίνωση πρέπει να είναι σαφής, διατυπωμένη σε απλή γλώσσα, να δίνεται στο υποκείμενο των δικαιωμάτων όταν ζητείται και εντός προθεσμίας ενός μήνα από την στιγμή που ζητείται. Όταν δεν είναι εφικτό, ο υπεύθυνος επεξεργασίας

[82] Βλ. σχετικά αναφορά στην Γνωμοδότηση υπ' αρ. 2/2018 της ΑΠΔΠΧ σε Ετήσια Έκθεση 2018, κατά την οποία η ΑΠΔΠΧ γνωμοδότησε κατόπιν αίτησης της Υπουργού Εργασίας, Κοινωνικής Ασφάλισης και Κοινωνικής Αλληλεγγύης επί του Νομοσχεδίου *«Μέτρα για την Προώθηση των Θεσμών της Αναδοχής και Υιοθεσίας,* διαθέσιμη σε https://www.dpa.gr/sites/default/files/2020-02/ANNUAL2018V30WEBPAGE_01.PDF

[83] Ήτοι : συναίνεση, υποχρέωση εκτέλεσης σύμβασης, επεξεργασία σε συμμόρφωση με έννομη υποχρέωση του υπεύθυνου επεξεργασίας ή προς διαφύλαξη ζωτικού συμφέροντος ή προς εκπλήρωση καθήκοντος δημοσίου συμφέροντος ή για άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας ή εξυπηρετεί το έννομο συμφέρον του χωρίς όμως να θίγει το συμφέρον του υποκειμένου, ειδικά αν αυτό είναι παιδί. Βλ. κατωτέρω σελ. 56-59.

[84] Η διαφάνεια αποτελείται από την ex ante και την ex post διαφάνεια, βλ. σχετικά Hildebrandt, Behavioural Biometric Profiling and Transparency Enhancing Tools., WP 7 Deliverable, Nov. 2009, διαθέσιμο σε http://www.fidis.net/. Βλ. επίσης και Ομάδα εργασίας του άρθρου 29 ,Κατευθυντήριες Γραμμές σχετικά με τη διαφάνεια βάσει του κανονισμού 2016/679, 17/EL, WP260 rev.01.

οφείλει να ενημερώσει το υποκείμενο για την αδυναμία αυτή καθώς και για τη δυνατότητα υποβολής καταγγελίας στην αρμόδια εποπτική αρχή (άρθρο 5 παρ.1α).

β. αρχή του περιορισμού του σκοπού

Σύμφωνα με το άρθρο 5 παρ. 1β, η συλλογή και επεξεργασία των *δεδομένων πρέπει να είναι περιορισμένη* και να γίνεται για συγκεκριμένους σκοπούς που δεν επιτρέπουν την υποβολή των δεδομένων σε περαιτέρω επεξεργασία, εκτός εάν πρόκειται για σκοπούς αρχειοθέτησης που εξυπηρετούν το δημόσιο συμφέρον ή για σκοπούς επιστημονικής ή ιστορικής έρευνας, ή στατιστικούς σκοπούς, και υπό τον όρο ότι οι χρησιμοποιούμενες μέθοδοι αποκλείουν την ταυτοποίηση των υποκειμένων των δεδομένων και παρέχουν τις κατάλληλες εγγυήσεις για την προστασία των δεδομένων τους[85].

γ. αρχή ελαχιστοποίησης των προσωπικών δεδομένων

Σύμφωνα με το άρθρο 5 παρ.1γ, η επεξεργασία των προσωπικών δεδομένων πρέπει να περιορίζεται στο αναγκαίο μέτρο τόσο όσον αφορά στον όγκο των δεδομένων όσο και όσον αφορά στο χρόνο διατήρησης αυτών. Βάσει της αρχής αυτής τα δεδομένα που τηρούνται πρέπει να είναι κατάλληλα, συναφή και περιορισμένα στα απολύτως αναγκαία για τους σκοπούς για τους οποίους εκτελείται η επεξεργασία. Όπως παρατηρείται ο κανονισμός αναφέρει ότι τα δεδομένα που θα τυγχάνουν επεξεργασίας πρέπει να είναι τα *πρόσφορα και αναγκαία* για την εκπλήρωση του σκοπού, παραπέμποντας έτσι στην ελαχιστοποίησή τους και κατ' ουσία στην αρχή της αναλογικότητας που επιβάλλει την ύπαρξη *συνάφειας* ανάμεσα στα δεδομένα που τηρούνται και στο σκοπό για τον οποίο συλλέγονται.

[85] Αντίστοιχα ο εθνικός νομοθέτης, στηριζόμενος στο άρθρο 6 παρ. 3ΓΚΠΔ εισάγει στο άρθρο 24 Ν. 4624/2019 μια εθνική νομική βάση επεξεργασίας, κάνοντας χρήση της «ρήτρας ανοίγματος» που επιτρέπει στους δημόσιους φορείς την επεξεργασία για διαφορετικό σκοπό, υπό την προϋπόθεση ότι ο υπεύθυνος επεξεργασίας δρα στα πλαίσια νομικής υποχρέωσης ή προς εκπλήρωση καθήκοντος προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας ή προς αποτροπή κινδύνου εθνικής ασφάλειας, εθνικής άμυνας ή δημόσιας ασφάλειας, για τη δίωξη ποινικών αδικημάτων και προς αποτροπή βλάβης των δικαιωμάτων άλλου προσώπου. Με τη διάταξη αυτή καλύπτονται όλες οι νομικές υποχρεώσεις του φάσματος των σχέσεων πολίτη -κράτους, καθιερώνεται το επιτρεπτό της επεξεργασίας δεδομένων από την κρατική αρχειοθέτηση έως τις τελωνειακές υπηρεσίες, *υπό την προϋπόθεση ότι αυτή η «για άλλο σκοπό» επεξεργασία δεν είναι αυθαίρετη αλλά στο αναγκαίο και αναλογικό μέτρο που αρμόζει σε μια δημοκρατική κοινωνία* (Αιτιολογική Έκθεση, σελ. 15). Η ίδια ευχέρεια δίνεται και στους ιδιωτικούς φορείς (άρθρο 25) όταν η επεξεργασία που γίνεται για διαφορετικό σκοπό αφορά εθνική ή δημόσια ασφάλεια, δίωξη ποινικών αδικημάτων ή για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων τους κατόπιν υποβολής αιτήματος δημοσίου φορέα, εκτός εάν υπερτερεί το συμφέρον του υποκειμένου των δεδομένων να μην τύχουν επεξεργασίας τα δεδομένα αυτά.

δ. αρχή της ακρίβειας

Στο άρθρο 5 παρ.1δ ο ΓΚΠΔ προβλέπει ότι τα προσωπικά δεδομένα πρέπει να είναι ακριβή και επικαιροποιημένα επισημαίνοντας ότι, στο όνομα της διασφάλισης *της ακρίβειας*, τυχόν ανακριβή σε σχέση με τους σκοπούς επεξεργασίας προσωπικά δεδομένα πρέπει, κατόπιν λήψης εύλογων μέτρων, να διαγράφονται άμεσα ή να διορθώνονται[86], το δε υποκείμενο θα πρέπει να έχει επαρκή ενημέρωση ως προς τα προσωπικά δεδομένα του που υφίστανται επεξεργασία.

ε. αρχή του περιορισμού της περιόδου διατήρησης και αποθήκευσης των προσωπικών δεδομένων

Μια ακόμη βασική αρχή που θέτει ο Κανονισμός είναι εκείνη που αφορά *στον περιορισμό της περιόδου διατήρησης και αποθήκευσης των προσωπικών δεδομένων*[87]. Αναφέρεται στην τήρηση των αρχείων των προσωπικών δεδομένων για τόσο χρονικό διάστημα όσο είναι απαραίτητο μέχρι να επιτευχθεί ο σκοπός επεξεργασίας. Εξαίρεση προβλέπεται στην περίπτωση κατά την οποία η επεξεργασία γίνεται για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς, οπότε η αποθήκευση των δεδομένων μπορεί να παραταθεί υπό την προϋπόθεση λήψης των κατάλληλων οργανωτικών μέτρων για τη διασφάλιση των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων (άρθρο 5 ε').

[86] Η ΑΠΔΠΧ έχει δεχτεί σωρεία καταγγελιών κατά τραπεζών για παραβίαση της εν λόγω αρχής, και δη για τηλεφωνικές οχλήσεις που πραγματοποιούνται στο πλαίσιο ενημέρωσης οφειλετών για ληξιπρόθεσμες απαιτήσεις είτε από τις τράπεζες είτε από Εταιρίες Ενημέρωσης Οφειλετών (ΕΕΟ) που ενεργούσαν για λογαριασμό των Τραπεζών. Χαρακτηριστικό είναι τα παραδείγματα καταγγελιών εντός του χρονικού διαστήματος 2015-2017 που στρέφονταν κατά της Alpha Bank , της Εθνικής Τράπεζας και της Τράπεζας Eurobank λόγω όχλησης σε λάθος πρόσωπο, μη επικαιροποίησης των στοιχείων των πελατών τους και παράλειψη διόρθωσης στοιχείων με σήμανση των τηλεφωνικών αριθμών, ως μη αντιστοιχούντων σε οφειλέτη-πελάτη των εν λόγω Τραπεζών. Στις αποφάσεις που εξέδωσε η αρχή επέβαλε πρόστιμο στις Τράπεζες ύψους 5.000 – 10.000 ευρώ για τις εν λόγω παραβιάσεις, βλ. σχετικά ΑΠΔΠΧ Ετήσια Έκθεση 2018, σελ. 56-57.

[87] Βλ. σχετικά αναφορά ΑΠΔΠΧ στη με αρ. 1/2018 Γνωμοδότησή της αναφορικά με ανάρτηση στοιχείων χρηματοδοτών πολιτικών κομμάτων στην ιστοσελίδα της Επιτροπής Ελέγχου της Βουλής για χρονικό διάστημα δέκα (10) ετών, η οποία κρίθηκε ότι όχι μόνον παραβιάζει την αρχή της αναλογικότητας αλλά και την αρχή της χρονικά πεπερασμένης διατήρησης των δεδομένων κατ' εφαρμογή του προϊσχύοντος άρθρου 4 παρ. 1 δ του Ν. 2472/1997, που ίσχυε κυρίως επί δημοσιοποίησης ευαίσθητων προσωπικών δεδομένων στο διαδίκτυο. Η σύσταση της Αρχής ήταν η μη διατήρησή τους πέραν της διετίας από την ανάρτησή τους.

στ. αρχή της ακεραιότητας και εμπιστευτικότητας

Ο ΓΚΠΔ στο άρθρο 5 παρ. 1στ' καθιερώνει την επεξεργασία που εγγυάται την ασφάλεια των προσωπικών δεδομένων κι η οποία επιτυγχάνεται με την χρησιμοποίηση κατάλληλων τεχνικών ή οργανωτικών μέτρων προκειμένου να αποτραπεί η μη εξουσιοδοτημένη ή παράνομη επεξεργασία, η τυχαία απώλεια, καταστροφή ή φθορά.

ζ. αρχή της λογοδοσίας

Το άρθρο 5 παρ. 2 εισάγει μια *νέα αρχή* που συνιστά καινοτομία σε σχέση με το προϊσχύον δίκαιο. Έτσι για πρώτη φορά, καθιερώνεται η υποχρέωση του υπεύθυνου επεξεργασίας να αποδεικνύει διαρκώς τη συμμόρφωση με τις προαναφερόμενες αρχές της παρ. 1 του ιδίου άρθρου. Σύμφωνα με τον ΓΚΠΔ κάθε δημόσιος ή ιδιωτικός φορέας πρέπει να ορίζει υπεύθυνο επεξεργασίας, επιφορτισμένο να διαμορφώνει τις διαδικασίες και τα τεχνικά και οργανωτικά συστήματα, κατά τέτοιο τρόπο, ώστε να τηρεί την εν λόγω αρχή και τις ιδιαίτερες εκφάνσεις της. Ο δε υποχρεωτικός ορισμός του υπευθύνου επεξεργασίας δημιουργεί τα εχέγγυα διασφάλισης των εν λόγω αρχών, καθώς δεν καθίσταται απλά αρμόδιος για τη διενέργεια της επεξεργασίας αλλά και υπεύθυνος (υπόλογος) για τη συμμόρφωσή του προς τον ΓΚΠΔ. Με αυτόν τον τρόπο μετακυλύεται το βάρος απόδειξης από τις αρχές προστασίας προσωπικών δεδομένων, σε όσους διαχειρίζονται τα προσωπικά δεδομένα, οι οποίοι υποχρεούνται σε περίπτωση ελέγχου να αποδείξουν ότι τελούν σε πλήρη εναρμόνιση με τις διατάξεις του ΓΚΠΔ. Οι υποχρεώσεις του υπευθύνου επεξεργασίας δεν είναι προκαθορισμένες και σταθερές πάντα αλλά διαμορφώνονται ανάλογα με τον κίνδυνο που ενδέχεται να προκύψει από την επεξεργασία, όπως αυτός εκτιμάται ήδη πριν την έναρξη της επεξεργασίας βάσει της προστασίας των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού (Protection by design and by default) και της Εκτίμησης Αντικτύπου (Data Protection Impact Assessment).

3.8. Η επεξεργασία των προσωπικών δεδομένων βάσει του ΓΚΠΔ – Διατυπώσεις νομιμότητας

Το άρθρο 4 παρ. 2 ΓΚΠΔ ορίζει ως «επεξεργασία» *κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή*

κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή». Η εν λόγω απαρίθμηση είναι ενδεικτική και αναφέρεται σε κάθε πράξη επεξεργασίας που πραγματοποιείται από φορείς ή οργανισμούς του Δημοσίου, ΝΠΔΔ, ΝΠΙΔ, ενώσεις προσώπων ή φυσικό πρόσωπο, όταν είναι απαραίτητη για την παροχή των αντίστοιχων υπηρεσιών, οπότε ο αρμόδιος φορέας αναλαμβάνει την υποχρέωση να διασφαλίσει την τήρηση των προϋποθέσεων νομιμότητας αυτής, δρώντας υπό το πρίσμα των προαναφερομένων αρχών[88].

Επιπλέον σύμφωνα με τη διάταξη του άρθρου 6 ΓΚΠΔ για να είναι σύννομη η επεξεργασία «απλών» προσωπικών δεδομένων πρέπει *διαζευκτικά* να συντρέχει μια από τις εξής έξι (6) νομιμοποιητικές βάσεις:

α*) το υποκείμενο των δεδομένων να έχει συναινέσει*[89] *στην επεξεργασία για έναν ή περισσότερους συγκεκριμένους σκοπούς,*
β) η επεξεργασία να είναι απαραίτητη για την εκτέλεση σύμβασης ή για να ληφθούν μέτρα πριν τη σύναψη σύμβασης,
γ) η επεξεργασία να είναι απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση του υπευθύνου επεξεργασίας,
δ) η επεξεργασία να είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου,
ε) η επεξεργασία να είναι απαραίτητη για την εκπλήρωση καθήκοντος προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας,
στ) η επεξεργασία να είναι απαραίτητη για τους σκοπούς που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, εκτός εάν έναντι των συμφερόντων αυτών υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου και ιδίως εάν το υποκείμενο των δεδομένων είναι παιδί.

Όταν χρησιμοποιείται ως νομιμοποιητική βάση η συγκατάθεση του υποκειμένου αυτή πρέπει να είναι σαφής και ξεκάθαρη για το σκοπό επεξεργασίας, ενώ μπορεί να δοθεί υπό μορφή γραπτής δήλωσης και να ανακληθεί ελεύθερα από το υποκείμενο ανά πάσα στιγμή,

[88] https://legal.heal-link.gr/index.php/personal-data-processing
[89] Συγκατάθεση του υποκειμένου των δεδομένων είναι κάθε ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν το αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν, βλ. άρθρο 4 παρ. 11 ΓΚΠΔ, ΕΕ L 119/34, 4.05.2016.

χωρίς να επιδρά στο κύρος της διαδικασίας που έλαβε χώρα πριν την ανάκλησή της. Προκειμένου δε να τηρούνται οι αυστηρές προϋποθέσεις συγκατάθεσης[90] κρίνεται σκόπιμο όλοι οι δημόσιοι και ιδιωτικοί φορείς να προβούν σε άμεσο εκσυγχρονισμό των μεθόδων και συστημάτων τους.

Όσον αφορά στην επεξεργασία των «ειδικής κατηγορίας» προσωπικών δεδομένων, η διάταξη του άρθρου 9 ΓΚΠΔ θέτει ως γενικό κανόνα την απαγόρευση επεξεργασίας τους. Ωστόσο η παρ. 2 του ιδίου άρθρου εισάγει εξαιρέσεις και ως εκ τούτου χωρεί επεξεργασία και επί αυτών των δεδομένων όλως εξαιρετικώς εάν:

α) το υποκείμενο έχει ρητά συναινέσει στην επεξεργασία τους για έναν ή περισσότερους σκοπούς, εκτός αν το δίκαιο του κράτους μέλους ή της Ένωσης προβλέπει ότι η απαγόρευση δεν μπορεί να αρθεί με μόνη τη λήψη της συγκατάθεσης αυτής,
β) η επεξεργασία είναι απαραίτητη για την εκτέλεση των υποχρεώσεων και την άσκηση των δικαιωμάτων του υπεύθυνου επεξεργασίας ή του υποκειμένου των δεδομένων στον τομέα του εργατικού δικαίου και δικαίου κοινωνικής ασφάλισης και κοινωνικής προστασίας, εφόσον επιτρέπεται από το δίκαιο της Ένωσης ή κράτους μέλους ή από συλλογική συμφωνία βάσει του εθνικού δικαίου και με τις κατάλληλες εγγυήσεις για τα δικαιώματα και τα συμφέροντα του υποκειμένου των δεδομένων,
γ) η επεξεργασία είναι αναγκαία για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου ή τρίτου εάν το υποκείμενο τελεί σε φυσική ή νομική αδυναμία να συγκατατεθεί,
δ) η επεξεργασία διενεργείται στο πλαίσιο δραστηριοτήτων ιδρύματος, οργάνωσης ή άλλου μη κερδοσκοπικού φορέα, αφορά αποκλειστικά τα δεδομένα των μελών και τα δεδομένα δεν διαβιβάζονται σε τρίτους,
ε) η επεξεργασία αφορά σε δεδομένα που προδήλως δημοσιοποιεί το ίδιο το υποκείμενο των δεδομένων,
στ) η επεξεργασία είναι απαραίτητη για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων ή όταν τα δικαστήρια ενεργούν υπό τη δικαιοδοτική τους ιδιότητα,
ζ) η επεξεργασία είναι απαραίτητη για λόγους ουσιαστικού δημοσίου συμφέροντος βάσει του δικαίου της Ένωσης ή κράτους μέλους,

[90] Οι αυστηρές προϋποθέσεις του ΓΚΠΔ ως προς τη συγκατάθεση, αποδεικνύουν την πρόθεσή του να την αναγορεύσει σε υψίστης σημασίας παράγοντα στο νέο καθεστώς προστασίας των δεδομένων.

η) η επεξεργασία είναι απαραίτητη για σκοπούς προληπτικής ιατρικής, ιατρικής διάγνωσης, παροχής υγειονομικής ή κοινωνικής περίθαλψης βάσει του δικαίου της Ένωσης ή κράτους μέλους,

θ) η επεξεργασία είναι απαραίτητη για λόγους δημοσίου συμφέροντος στον τομέα της δημόσιας υγείας βάσει του δικαίου της Ένωσης ή κράτους μέλους και

ι) η επεξεργασία είναι απαραίτητη για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον για σκοπούς επιστημονικής, ιατρικής έρευνας ή στατιστικούς σκοπούς βάσει του δικαίου της Ένωσης ή κράτους μέλους.

Όπως προκύπτει από την εν λόγω διάταξη ο ευρωπαίος νομοθέτης αναγνωρίζει για την επεξεργασία των ευαίσθητων προσωπικών δεδομένων, διευρυμένη προστασία θέτοντας αυστηρότερες προϋποθέσεις ενώ προβλέπει ως δικλείδες ασφαλείας, τη ρητή συγκατάθεση του υποκειμένου, τη συνδρομή λόγου δημοσίου συμφέροντος, χωρίς την προγενέστερη άδεια της ΑΠΔΠΧ και προκρίνει το δικαίωμα διαγραφής, την σε κάθε περίπτωση ανακοίνωση της παραβίασης των δεδομένων του, τη χρησιμοποίηση σαφούς και κατανοητής γλώσσας στις πολιτικές απορρήτου και την αυστηρή εφαρμογή του κανονισμού/εθνικού νόμου με την ταυτόχρονη επιβολή υψηλών προστίμων στις επιχειρήσεις ή οργανισμούς που τον παραβιάζουν[91]. Η παρ. 3 του άρθρου 9 ΓΚΠΔ θέτει «ρήτρα ανοίγματος» ή «ευελιξίας» υπέρ της εκάστοτε εθνικής νομοθεσίας[92].

3.9. Τα δικαιώματα του υποκειμένου επεξεργασίας των προσωπικών δεδομένων

Ο ΓΚΠΔ διατήρησε τα προϋφιστάμενα δικαιώματα, ενίσχυσε ορισμένα από αυτά και εκσυγχρόνισε κάποια άλλα ενώ επιπροσθέτως εισήγαγε το δικαίωμα στη λήθη και το δικαίωμα στη φορητότητα. Το υποκείμενο έτσι «συμμετέχει» πλέον και αποκτά μεγαλύτερο έλεγχο στην επεξεργασία των δεδομένων του μέσω των ανανεωμένων δικαιωμάτων του κανονισμού, εκπληρώνοντας την πληροφοριακή αυτοδιάθεση και καλλιεργώντας την εμπιστοσύνη μεταξύ των πολιτών και όσων διαχειρίζονται τα προσωπικά τους δεδομένα[93]. Η άσκηση τους δεν είναι απεριόριστη καθώς εμπίπτει στους γενικούς περιορισμούς του άρθρου 23 ΓΚΠΔ, ενώ επί παραβίασης επισύρονται

[91] *Η χώρα μας -που έδειξε εξαρχής τη σαφή της πρόθεση να εφαρμόσει τον Κανονισμό – προστατεύει σε υψηλό βαθμό τα προσωπικά δεδομένα των πολιτών της, καταλαμβάνοντας μια από τις πρώτες θέσεις στη συμμόρφωση μ' αυτόν.»* (Ετήσια Έκθεση ΑΠΔΠΧ, 2018).

[92] Ο έλληνας νομοθέτης κάνοντας χρήση της ρήτρας εισήγαγε τη διάταξη του άρθρου 22 παρ. Ν. 4624/2019.

[93] Βλ. όπ.α. https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_387

διοικητικές κυρώσεις και αναγνωρίζεται αστική ευθύνη αποζημίωσης από τον υπεύθυνο επεξεργασίας ή τον εκτελούντα αυτήν και εις ολόκληρον όταν λειτουργούν από κοινού. Περαιτέρω το άρθρο 30 παρ. 2 του κυρωτικού νόμου Ν. 4624/2019 εισάγει, επί τη βάσει του άρθρου 89 παρ.2 «ρήτρα ανοίγματος» κατά την οποία συγκεκριμένα δικαιώματα, ήτοι τα δικαιώματα πρόσβασης, ενημέρωσης, περιορισμού, φορητότητας και εναντίωσης, μπορεί βάσει της εθνικής νομοθεσίας να τίθενται υπό περιορισμούς.

3.9.1 Η προστασία των δικαιωμάτων των παιδιών

Η προστασία των παιδιών στο νέο τεχνολογικό περιβάλλον έχει απασχολήσει ιδιαίτερα όχι μόνο τον ευρωπαίο αλλά και τον εθνικό νομοθέτη. Ο ΓΚΠΔ αποτυπώνει την ανησυχία του για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα ανήλικων τέκνων καθώς οι ανήλικοι ανήκουν σε μια ευάλωτη κοινωνική ομάδα, με μειωμένη επίγνωση των κινδύνων που διατρέχουν από την αθέμιτη επεξεργασία, ανησυχία που συνίσταται κυρίως στη χρήση δεδομένων των παιδιών με σκοπό την εμπορία ή την κατάρτιση προφίλ προσωπικότητας ή χρήστη και συλλογή δεδομένων παιδιών κατά τη χρήση απευθείας παρεχόμενων σ' αυτά διαδικτυακών υπηρεσιών[94].

Η προστιθέμενη αξία του ΓΚΠΔ στο ζήτημα αυτό συνίσταται στην χορήγηση της συναίνεσης πριν την επεξεργασία των δεδομένων, αποσαφηνίζοντας ότι αυτή είναι σύννομη όταν το παιδί έχει συμπληρώσει το 16^{ο} έτος της ηλικίας τους[95]. Σε αντίθετη περίπτωση για το σύννομο της επεξεργασίας απαιτείται η συναίνεση των γονέων (άρθρο 8 ΓΚΠΔ) [96]. Με τη διάταξη αυτή, ο ΓΚΠΔ δίνει στα κράτη μέλη τη διακριτική ευχέρεια να προβλέπουν στην εθνική τους νομοθεσία άλλο όριο ηλικίας, το οποίο ωστόσο σε καμία περίπτωση δεν μπορεί να επεκταθεί σε παιδί ηλικίας κάτω των 13 ετών. Έτσι ο κανονισμός προκειμένου να προστατέψει την ανηλικότητα στο διαδίκτυο, διευθετεί το ζήτημα της συγκατάθεσης θέτοντας ηλικιακά όρια, σεβόμενος ωστόσο τις ιδιαιτερότητες και τις νομοθετικές επιλογές των κρατών μελών[97].

[94] Βλ. σκέψη 38 του Προοιμίου ΓΚΠΔ.
[95] Βλ. Άρθρο 8 ΓΚΠΔ -Προϋποθέσεις που ισχύουν για τη συγκατάθεση παιδιού σε σχέση με τις υπηρεσίες της κοινωνίας των πληροφοριών, ΕΕ L 119/37, 4.5.2016
[96] Ο αντίλογος που διατυπώνεται απέναντι στη γονική συγκατάθεση σχετίζεται με την ελεύθερη ανάπτυξη της προσωπικότητας του παιδιού, την άσκηση του δικαιώματος επικοινωνίας του με φίλους, τη συμμετοχή τους σε εκπαιδευτικές ή κοινωνικές δράσεις άσχετα από τη βούληση των γονέων του, βλ. σχετικά με το ζήτημα αυτό σε Παναγοπούλου-Κουτνατζή, ΕφημΔΔ-1/2017.
[97] Όπως προαναφέρθηκε η Ελλάδα κάνοντας χρήση της ρήτρας ανοίγματος καθιέρωσε ως όριο ηλικίας το 15^{ο} (άρθρο 21 Ν. 4624/2019).

Έτσι το βάρος της ευθύνης αναφορικά με την επεξεργασία των προσωπικών δεδομένων, ανατίθεται στους ασκούντες τη γονική μέριμνα, οι οποίοι, αφού λάβουν υπόψη τη διαθέσιμη τεχνολογία, θα πρέπει να μεριμνήσουν για την επιλογή κατάλληλων μηχανισμών ελέγχου (πχ. εγκατάσταση προγράμματος γονικού ελέγχου, καταχώριση email ή τηλεφωνικού αριθμού τους ή και τραπεζικού λογαριασμού τους). Στην αιτιολογική σκέψη 38 του Προοιμίου ΓΚΠΔ, ορίζεται ότι η γονική συγκατάθεση δεν απαιτείται για υπηρεσίες πρόληψης ή παροχής συμβουλών στον ανήλικο, υπονοώντας τις γραμμές επικοινωνίας ψυχολογικής στήριξης ανηλίκων ή τις γραμμές για καταγγελίες τους αναφορικά με τυχόν κακοποίησή τους.

Η προστασία των ανηλίκων ενισχύεται και με τη διάταξη του άρθρου 12 ΓΚΠΔ όπου τονίζεται ότι αν η επεξεργασία απευθύνεται σε παιδί, πρέπει να διατυπώνεται κατά τρόπο σαφή σε απλή γλώσσα, ώστε να γίνεται εύκολα αντιληπτή.

3.9.2. Τα ήδη αναγνωρισμένα και επικαιροποιημένα από τον ΓΚΠΔ δικαιώματα

3.9.2.1. Το δικαίωμα ενημέρωσης - διαφάνεια

Πρόκειται για το δικαίωμα του φυσικού προσώπου να γνωρίζει ποιος επεξεργάζεται τα προσωπικά δεδομένα που έχει παραχωρήσει, ποια ακριβώς είναι αυτά και για ποιόν λόγο τα διαθέτει προς επεξεργασία (άρθρο 12Κ)[98]. Βάσει του ΓΚΠΔ τα φυσικά πρόσωπα (υποκείμενα των δεδομένων) έχουν δικαίωμα να ενημερώνονται με ακρίβεια και σαφήνεια για τη συλλογή και επεξεργασία των προσωπικών τους δεδομένων, δικαίωμα που διέπεται από την αρχή της διαφάνειας, σύμφωνα με την οποία η ενημέρωση πρέπει να είναι συνοπτική, διαφανής, κατανοητή, εύκολα προσβάσιμη και διατυπωμένη σε απλή και σαφή γλώσσα, ενώ κρίνεται σκόπιμο να αποφεύγονται αόριστοι όροι (λ.χ. «θα μπορούσε», «ενδέχεται», «πιθανόν να…» κ.λπ.).

Σε περίπτωση παραβίασης προσωπικών του δεδομένων το δικαίωμα αυτό επεκτείνεται υποχρεωτικά από τον υπεύθυνο επεξεργασίας εν πρώτοις στην εποπτική αρχή (άρθρο 33Κ)[99] και εν συνεχεία και στα ίδια τα υποκείμενα (άρθρο 34Κ)[100], εάν αυτό υπαγορεύει η

[98] Βλ. Άρθρο 12 ΓΚΠΔ - Διαφανής ενημέρωση, ανακοίνωση και ρυθμίσεις για την άσκηση των δικαιωμάτων του υποκειμένου των δεδομένων, ΕΕ L 119/39, 4.5.2016

[99] Βλ. άρθρο 33 ΓΚΠΔ -Γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα στην εποπτική αρχή ΕΕ L 119/52, 4.5.2016

[100] Βλ. άρθρο 34 ΓΚΠΔ -Ανακοίνωση παραβίασης δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων, ΕΕ L 119/52, 4.5.2016

φύση των δεδομένων που παραβιάστηκαν και ενδέχεται να επέλθει σοβαρός κίνδυνος για τα δικαιώματα και τις ελευθερίες αυτών[101]. Η ενημέρωση πρέπει να είναι λεπτομερής και να εκθέτει το είδος των δεδομένων, τον αριθμό των ατόμων που θίγονται, τα άτομα που έλαβαν γνώση των προσωπικών δεδομένων, τον τρόπο αναγνώρισης της παραβίασης κ.λ.π. Επιπλέον η ενημέρωση πρέπει να εκτείνεται και στον τρόπο με τον οποίο θα γίνει η διαχείριση του περιστατικού, ήτοι τις υφιστάμενες διαδικασίες αντιμετώπισης, τα υπό λήψη μέτρα, τα υφιστάμενα μέτρα ασφαλείας καθώς και τα διορθωτικά, τα στοιχεία επικοινωνίας του υπευθύνου επεξεργασίας κ.ο.κ.

Το εν λόγω δικαίωμα συνιστά ιδιαίτερη έκφανση του δικαιώματος πληροφοριακού αυτοκαθορισμού του ατόμου, στηριζόμενο στο δικαίωμά του να γνωρίζει τον αποδέκτη των δεδομένων του ακόμη και επί παραβίασης, ενώ ταυτόχρονα υποδηλώνει μια στοιχειώδη εντιμότητα στο χειρισμό εκ μέρους του υπεύθυνου επεξεργασίας, μέσα από τη συνεργασία του τελευταίου με την αρμόδια εποπτική αρχή και την ενημέρωση του υποκειμένου, ώστε να λάβει τυχόν μέτρα σχετικά με την παραβίαση (ΣΕΒ, 2018).

Περαιτέρω βάσει του ΓΚΠΔ ο υπεύθυνος επεξεργασίας δημόσιου ή ιδιωτικού φορέα, έχει υποχρέωση ενημέρωσης των υποκειμένων των προσωπικών δεδομένων που έχουν συλλεγεί είτε από το ίδιο (άρθρο 13) είτε από άλλες πηγές (άρθρο 14). Ωστόσο ο εθνικός νομοθέτης στα άρθρα 31 και 32 του Ν. 4624/2019 κάνοντας χρήση της «ρήτρας ανοίγματος» προβλέπει την *απαλλαγή του υπεύθυνου επεξεργασίας δημόσιου ή ιδιωτικού φορέα* από την αντίστοιχη υποχρέωση σε κάποιες περιπτώσεις συλλογής πληροφοριών είτε από το ίδιο το υποκείμενο (άρθρο 31) είτε από τρίτους (άρθρο 32)[102]. Σε αντιστάθμισμα ο υπεύθυνος επεξεργασίας πρέπει να λαμβάνει τα *κατάλληλα μέτρα προστασίας* (π.χ. παροχή πληροφοριών στο κοινό μέσω δημοσίευσης σε προσιτή μορφή σε δημόσιο ιστότοπο του υπευθύνου επεξεργασίας) και να αιτιολογεί εγγράφως τους λόγους για τους οποίους δεν

[101] Αν η γνωστοποίηση δε γίνει στο ως άνω χρονικό όριο των 72 ωρών, τότε χρήζει αιτιολογίας με αναφορά στους λόγους της καθυστέρησης.

[102] Αυτό συμβαίνει όταν : τα προσωπικά δεδομένα δόθηκαν για άλλο σκοπό και πλέον η επεξεργασία τους γίνεται για σκοπό διαφορετικό, η ενημέρωση θέτει σε κίνδυνο την ορθή εκτέλεση των καθηκόντων του υπευθύνου επεξεργασίας ή τη δημόσια ασφάλεια ή την θεμελίωση ή άσκηση νομικών αξιώσεων. Ειδικότερα στην περίπτωση κατά την οποία η επεξεργασία γίνεται από δημόσιους φορείς και τα δεδομένα έχουν συλλεγεί από τρίτες πηγές, το δικαίωμα ενημέρωσης μπορεί να καμφθεί, εάν η άσκησή του θέτει σε κίνδυνο την ορθή εκτέλεση των καθηκόντων του υπευθύνου ή την εθνική ή δημόσια ασφάλεια, ενώ στην περίπτωση που η επεξεργασία γίνεται από ιδιωτικούς φορείς, το δικαίωμα ενημέρωσης του υποκειμένου ενδέχεται να περιοριστεί αν η ενημέρωση μπορεί να βλάψει την θεμελίωση ή άσκηση νομικών αξιώσεων ή όταν πρόκειται για δεδομένα συμβάσεων που αποσκοπούν στην πρόληψη ζημιών από την τέλεση ποινικών αδικημάτων ή αν ο υπεύθυνος επεξεργασίας έχει ενημερωθεί από δημόσιο φορέα ότι η τυχόν δημοσιοποίησή τους θα θέσει σε κίνδυνο την εθνική ή δημόσια ασφάλεια (άρθρο 32 Ν. 4624/2019).

προέβη σε ενημέρωση. Η αιτιολόγηση μάλιστα της άρνησης παροχής πληροφοριών, εμπίπτει στο έλεγχο της ΑΠΔΠΧ (Αιτιολογική Έκθεση, σελ. 24-25).

3.9.2.2. Το δικαίωμα πρόσβασης

Είναι το δικαίωμα του ατόμου να ζητά την ελεύθερη πρόσβαση στα προσωπικά του δεδομένα που τηρεί κάποιος φορέας, οργανισμός ή επιχείρηση (άρθρο 15 ΓΚΠΔ)[103]. Θεωρείται βασικό υποκειμενικό δικαίωμα προστασίας των δεδομένων και δικαίως χαρακτηρίζεται ως η Magna Charta της προστασίας των δεδομένων προσωπικού χαρακτήρα. Βάσει αυτού τα υποκείμενα των δεδομένων δικαιούνται να λαμβάνουν επιβεβαίωση για την επεξεργασία των δεδομένων τους (ήτοι τους σκοπούς επεξεργασίας, τις κατηγορίες δεδομένων, τους αποδέκτες των δεδομένων, το χρονικό διάστημα διατήρησής τους, την υποβολή αιτήματος διόρθωσης, διαγραφής, περιορισμού επεξεργασίας ή καταγγελίας κλπ (άρθρο 15 παρ.1), ακόμη και σε περίπτωση διαβίβασής τους (άρθρο 15 παρ. 2) και να λαμβάνουν αντίγραφο των δεδομένων τους που τυγχάνουν επεξεργασίας (άρθρο 15 παρ. 3). Ο υπεύθυνος επεξεργασίας οφείλει να ανταποκριθεί στην αίτηση του υποκειμένου χωρίς υπαίτια καθυστέρηση εντός ενός (1) μήνα από την υποβολή του αιτήματος ενώ η προθεσμία αυτή μπορεί να παραταθεί για χρονικό διάστημα δύο (2) μηνών, σε περίπτωση που το υποβληθέν αίτημα είναι περίπλοκο ή ο όγκος των αντιγράφων που πρέπει να χορηγήσει ο υπεύθυνος επεξεργασίας είναι ιδιαιτέρως μεγάλος. Ο τελευταίος μάλιστα οφείλει να ενημερώσει σχετικά με την παράταση μέσα σε ένα μήνα από την υποβολή του αιτήματος.

Το άρθρο 33 Ν. 4624/2019 ωστόσο περιορίζει την άσκηση του δικαιώματος πρόσβασης του άρθρου 15 ΓΚΠΔ, όταν : α) δεν υφίσταται υποχρέωση ενημέρωσης του υποκειμένου εκ μέρους του φορέα, γιατί αυτή θα έθετε σε κίνδυνο την εθνική ή τη δημόσια ασφάλεια ή η τυχόν δημοσιοποίηση θα έβλαπτε την εθνική άμυνα ή ασφάλεια και τη δημόσια ασφάλεια σε περίπτωση επεξεργασίας για σκοπό επιβολής του νόμου ή β) όταν τα δεδομένα του καταγράφηκαν και δεν μπορούν να διαγραφούν επειδή υπάρχουν νομικές ή κανονιστικές διατάξεις που καθιστούν υποχρεωτική τη διατήρηση ή τον έλεγχό τους, όπως λ.χ. συμβαίνει στις περιπτώσεις αποθήκευσής τους σε φορολογικές βάσεις δεδομένων ή

[103] Βλ. σχετικά άρθρο 13-Πληροφορίες που παρέχονται εάν τα δεδομένα προσωπικού χαρακτήρα συλλέγονται από το υποκείμενο των δεδομένων
άρθρο 14 - Πληροφορίες που παρέχονται εάν τα δεδομένα προσωπικού χαρακτήρα δεν έχουν συλλεγεί από το υποκείμενο των δεδομένων και
άρθρο 15- Δικαίωμα πρόσβασης του υποκειμένου των δεδομένων, ΕΕ L 119/40-43, 4.5.2016

λήψης δαχτυλικών αποτυπωμάτων για έκδοση ταυτοτήτων ή άλλων νομιμοποιητικών εγγράφων κ.λ.π.

Επιπροσθέτως πρέπει να συντρέχουν δυο ακόμη προϋποθέσεις για να περιοριστεί η πρόσβαση, ήτοι να καθίσταται δύσκολη για τον υπεύθυνο επεξεργασίας η παροχή πληροφοριών και τα κατάλληλα τεχνικά και οργανωτικά μέτρα να καθιστούν αδύνατη την επεξεργασία για άλλους σκοπούς.

3.9.2.3. Το δικαίωμα διόρθωσης

Το δικαίωμα του υποκειμένου να αιτείται τη διόρθωση ανακριβών δεδομένων[104] του ή τη συμπλήρωση ελλιπών στοιχείων προβλέπεται στο άρθρο 16 ΓΚΠΔ[105], το οποίο ορίζει ότι μπορεί να ασκηθεί γραπτώς ή προφορικώς ενώ ο υπεύθυνος επεξεργασίας οφείλει να συμμορφωθεί εντός προθεσμίας ενός μηνός, με ενδεχόμενη δίμηνη παράταση από την υποβολή του αιτήματος, όπως εκτέθηκε ανωτέρω[106].

3.9.2.4. Το δικαίωμα περιορισμού της επεξεργασίας

Αυτό σύμφωνα με το άρθρο 18 ΓΚΠΔ συνίσταται στο δικαίωμα του φυσικού προσώπου να αιτείται τον περιορισμό της επεξεργασίας των δεδομένων του όταν: α) η ακρίβειά τους αμφισβητείται και για όσο διάστημα απαιτείται μέχρι να εξακριβώσει ο υπεύθυνος επεξεργασίας την αλήθεια, β) η επεξεργασία είναι παράνομη και το υποκείμενο δεν επιθυμεί την πλήρη διαγραφή των δεδομένων του γ) τα δεδομένα είναι πλέον περιττά για τον υπεύθυνο επεξεργασίας γιατί έπαψε να ισχύει ο σκοπός επεξεργασίας και το υποκείμενο τα χρειάζεται για την άσκηση νομικής αξίωσης ή δ) το υποκείμενο εναντιώνεται στην αυτοματοποιημένη επεξεργασία και εκκρεμεί η επαλήθευση αναφορικά με το εάν και κατά πόσο οι νόμιμοι λόγοι του υπευθύνου επεξεργασίας υπερισχύουν έναντι των δικών του.[107]

Το άρθρο 18 παρ.2 ΓΚΠΔ προβλέπει ότι σε περίπτωση περιορισμού της επεξεργασίας, τα δεδομένα ενός φυσικού προσώπου είναι δεκτικά μόνον αποθήκευσης και όχι άλλης πράξης

[104] Σύμφωνα με τις Κατευθυντήριες Γραμμές της Ομάδας 29 τα προσωπικά δεδομένα θεωρούνται:
-ανακριβή όταν είναι εσφαλμένα, όπως λ.χ. όταν στην προσωπική κατάσταση κάποιου αναγράφεται έγγαμος ενώ είναι άγαμος ή διαζευγμένος
-ελλιπή όταν η έλλειψη είναι τέτοια, ώστε να μπορεί να οδηγήσει σε παραπλάνηση ή παρερμηνεία .
[105] Βλ. άρθρο 16 ΓΚΠΔ- Δικαίωμα διόρθωσης, ΕΕ L 119/43, 4.5.2016.
[106] https://www.dpa.gr/el/polites/gkpd/dikaiwma_diorthwsis
[107] Βλ. άρθρο 18 ΓΚΠΔ - Δικαίωμα περιορισμού της επεξεργασίας, ΕΕ L 119/44, 4.5.2016
ΕΕ L 119/44 4.5.2016

επεξεργασίας, εκτός εάν το υποκείμενό τους συμφωνεί. Στα πλαίσια της άσκησης του δικαιώματος αυτού ο ΓΚΠΔ προβλέπει ότι τα δεδομένα μπορούν α) να μεταφερθούν προσωρινά σε άλλο σύστημα, β) οι χρήστες να μην έχουν πρόσβαση σ' αυτά, γ) τα δεδομένα να μην είναι προσωρινά διαθέσιμα στην ιστοσελίδα. Ειδικότερα στην περίπτωση των ανακριβών στοιχείων ισοδυναμεί με μια τρόπον τινά προσωρινή προστασία που δίνεται μέχρι να διαλευκανθεί μια νομική κατάσταση.

Το δικαίωμα αυτό είναι εναλλακτικό του δικαιώματος διαγραφής (άρθρο 16ΓΚΠΔ) και εναντίωσης (άρθρο 21ΓΚΠΔ) -το οποίο αναφύεται από την προστασία προσωπικών δεδομένων κατ' άρθρο 9^{A} Σ- και του οποίου συνιστά προέκταση, αλλά *μπορεί να ασκηθεί συνδυαστικά* με τα ως άνω δικαιώματα, δεν είναι απόλυτο αφού κάμπτεται όταν συντρέχουν ορισμένες προϋποθέσεις και ασκείται είτε εγγράφως είτε προφορικά.

3.9.2.5. Το δικαίωμα εναντίωσης

Το δικαίωμα εναντίωσης συνίσταται στη δυνατότητα του υποκειμένου να εναντιώνεται, άλλως να αντιτάσσεται, ανά πάσα στιγμή και για λόγους σχετικά με την ιδιαίτερη κατάστασή του, στην επεξεργασία των προσωπικών του δεδομένων από συγκεκριμένο φορέα ή οργανισμό αρκεί να μη θίγεται το δημόσιο συμφέρον (άρθρο 21 ΓΚΠΔ).[108] Στην περίπτωση αυτή ο υπεύθυνος επεξεργασίας οφείλει να διακόψει την επεξεργασία, εκτός κι αν συντρέχουν λόγοι επιτακτικοί που υπερισχύουν των συμφερόντων, δικαιωμάτων και ελευθεριών του υποκειμένου. Το εν λόγω δικαίωμα μπορεί να ασκηθεί ανά πάσα στιγμή και επί επεξεργασίας που γίνεται για σκοπούς εμπορικής προώθησης (παρ.2-5). Ο υπεύθυνος επεξεργασίας οφείλει να ενημερώσει το υποκείμενο το αργότερο στην πρώτη επικοινωνία σχετικά με την ύπαρξη του εν λόγω δικαιώματος.

Σε περίπτωση επεξεργασίας για σκοπούς επιστημονικούς, στατιστικούς ή ιστορικής έρευνας, το υποκείμενο δικαιούται να εναντιωθεί ως περιγράφεται ανωτέρω, εκτός κι αν η επεξεργασία κρίνεται αναγκαία για την εκτέλεση καθήκοντος που ασκείται για λόγους δημοσίου συμφέροντος και πάντα βέβαια υπό τις προϋποθέσεις λήψης τεχνικών και οργανωτικών μέτρων που διασφαλίζουν την αρχή ελαχιστοποίησης.

Το δικαίωμα αυτό υπόκειται σε νόμιμους περιορισμούς στο μέτρο και βαθμό που δεν θίγουν τον πυρήνα του και αφορούν αναγκαία και αναλογικά μέτρα που οφείλει να

[108] Βλ. Άρθρο 21 - Δικαίωμα εναντίωσης, ΕΕ L 119/45, 4.5.2016

λαμβάνει κάθε δημοκρατική κοινωνία, προκειμένου να εξυπηρετηθούν οι αναφερόμενοι στη διάταξη του άρθρου 23 παρ.1^{α}' και υπό τους όρους της παρ. 2 αυτού αναφορικά με το ελάχιστο περιεχόμενό τους. Έτσι σύμφωνα με το άρθρο 35 του κυρωτικού Ν. 4624/2019 το δικαίωμα εναντίωσης του υποκειμένου στην ελληνική έννομη τάξη περιορίζεται όταν πρόκειται για επεξεργασία που γίνεται από δημόσιο φορέα, όταν αυτή επιβάλλεται από υπέρτερο δημόσιο συμφέρον που υπερισχύει έναντι των συμφερόντων του υποκειμένου ή όταν προβλέπεται από διάταξη νόμου[109].

3.9.2.6. Το δικαίωμα στην ανθρώπινη παρέμβαση

Πρόκειται για το δικαίωμα του υποκειμένου να προβάλει αντιρρήσεις όταν μια απόφαση που το αφορά βασίζεται αποκλειστικά σε αυτοματοποιημένη επεξεργασία, όπως είναι η αυτόματη άρνηση επιγραμμικής (on line) αίτησης πίστωσης ή η πρακτική ηλεκτρονικής πρόσληψης χωρίς της ανθρώπινη παρέμβαση, συμπεριλαμβανομένης και της κατάρτισης προφίλ για την αξιολόγηση προσωπικών πτυχών ενός ατόμου (π.χ. ανάλυση πτυχών που αφορούν επιδόσεις του σε εργασία, οικονομική κατάσταση, υγεία, σεξουαλικές προτιμήσεις κ.λ.π.) και η απόφαση αυτή παράγει έννομα αποτελέσματα ή έχει σημαντικές γι' αυτόν επιπτώσεις (άρθρο 22 ΓΚΠΔ). Ως εκ τούτου η διάταξη του άρθρου 22 σε συνδυασμό με την αιτιολογική σκέψη 71 του Προοιμίου επιδιώκει να αντιμετωπίσει τον κίνδυνο της εργαλειοποίησης του ατόμου.

Η παρ. 2 του ιδίου άρθρου προβλέπει ότι επιτρέπεται η λήψη απόφασης που βασίζεται στην αυτοματοποιημένη επεξεργασία όταν α) είναι αναγκαία για τη σύναψη ή την εκτέλεση σύμβασης μεταξύ του υποκειμένου και του υπευθύνου επεξεργασίας των δεδομένων, β) επιτρέπεται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους στο οποίο υπόκειται ο υπεύθυνος επεξεργασίας και το οποίο προβλέπει επίσης κατάλληλα μέτρα για την προστασία των δικαιωμάτων, των ελευθεριών και των έννομων συμφερόντων του υποκειμένου των δεδομένων ή γ) βασίζεται στη ρητή συγκατάθεση του υποκειμένου των δεδομένων.

Ο λόγος θεσμοθέτησής του συνίσταται στο να διασφαλιστεί ο σεβασμός της ανθρώπινης ουσίας και υπόστασης με την έννοια της πιο σύνθετης υπόστασης του ανθρώπου και όχι μόνο με την μορφή της ύπαρξής του ως απλή πληροφορία. Συνιστά ειδικότερη έκφανση του δικαιώματος ελεύθερης ανάπτυξης της προσωπικότητας και όχι απλή αλγοριθμική

[109] Βλ. σχετικά Αιτιολογική Έκθεση ΣχΝόμου, σελ. 27.

αξιολόγησή του από μηχανές που σταδιακά μπορεί να οδηγήσει στην εξ ολοκλήρου παρακολούθηση του ατόμου στην πλήρη στέρηση της αυτενέργειας και στην απώλεια των αντιδράσεων του ατόμου (Παναγοπούλου-Κουτνατζή, 2017).

3.10. Δύο νέα δικαιώματα

Πέρα από τα προαναφερόμενα δικαιώματα που ο επικαιροποίησε ο Κανονισμός, εισήγαγε δύο νέα πολύ ουσιαστικά δικαιώματα, αυτά της λήθης και της φορητότητας.

3.10.1. Το δικαίωμα διαγραφής (δικαίωμα στη λήθη)

Το δικαίωμα διαγραφής, άλλως «δικαίωμα στη λήθη»[110] είναι το δικαίωμα του υποκειμένου να αιτείται τη διαγραφή ορισμένων προσωπικών του δεδομένων όταν συντρέχουν ορισμένες προϋποθέσεις, όπως λ.χ. όταν εκλείπει ο λόγος διατήρησης ή αποθήκευσης κάποιων προσωπικών δεδομένων ή όταν ανακαλείται η συγκατάθεση του προς επεξεργασία καθώς δεν υπάρχει άλλη νομική βάση, οπότε τα δεδομένα του πρέπει να διαγραφούν ή ακόμη και όταν τα δεδομένα του έχουν υποστεί παράνομη επεξεργασία ή όταν το υποκείμενο αντιτάσσεται στην επεξεργασία των δεδομένων του. Τα περισσότερα από τα αιτήματα αυτά απευθύνονται κυρίως σε φορείς που διαχειρίζονται μηχανές αναζήτησης σε ρόλο υπεύθυνου επεξεργασίας (Tankard, 2016).

Το δικαίωμα στη λήθη διαμορφώθηκε κυρίως μέσα από θεμελιώδεις αποφάσεις ανώτατων εθνικών δικαστηρίων, του ΕΔΔΑ και του ΔΕΕ και ουσιαστικά συνιστά το δικαίωμα διαμόρφωσης της ψηφιακής παρουσίασης του ατόμου. Τα περισσότερα αιτήματα διαγραφής απευθύνονται σε διάφορες ψηφιακές μηχανές αναζήτησης[111]. Το υποκείμενο μπορεί να αιτηθεί τη διαγραφή συνδέσμου από τα αποτελέσματα αναζήτησης, όπου με τη χρήση μιας λέξης κλειδιού, εμφανίζονται τα προσωπικά του στοιχεία, τα οποία δεν επιθυμεί να δημοσιοποιεί λ.χ. το ονοματεπώνυμο τινός σε άρθρο εφημερίδας αναφορικά

---

[110] Βλ. Άρθρο 17: Δικαίωμα διαγραφής (δικαίωμα στη λήθη) , ΕΕ L 119/43, 4.5.2016, και αιτιολογική σκέψη 65-66.

[111] Έναυσμα για την θεσμοθέτηση του εν λόγω δικαιώματος υπήρξε ήδη από το 2014 η υπόθεση Google Spain SL and Google Inc v. Agencia Espanola de Proteccion de Datos and Mario Costeja Gonzales, στα πλαίσια της οποίας τέθηκε η νομολογιακή αρχή που αναγνώρισε στην Ε.Ε. το δικαίωμα να μπορεί να διαγράφει προσωπικά δεδομένα από τις μηχανές αναζήτησης της Google κατόπιν αιτήματος του υποκειμένου. Απόφαση του Δικαστηρίου της 13ης Μαΐου 2014 (τμήμα μείζονος συνθέσεως), διαθέσιμη σε http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130dedba4c61f58b547f28acdf409a72ebee7.e34KaxiLc3eQc40LaxqMbN4Pb3aOe0?text=&docid=152065&pageIndex=0&doclang=EL&mode=lst&dir=&occ=first&part=1&cid=762827
Βλ. σχετικά Απόφαση ΔΕΕ 13-05-2014 (c-131/2-12), Γνώμη WP 225. 26-11-2014.

με τη χορήγηση δανείου εξοφληθέντος από αυτόν σε παρελθόντα χρόνο ή η προηγούμενη ποινική καταδίκη που έχει ήδη εκτίσει (Ετήσια Έκθεση ΑΠΔΠΧ, 2018) το υποκείμενο των δεδομένων. Η μηχανή οφείλει άμεσα να προβεί στην εν λόγω διαγραφή εάν το υποκείμενο των δεδομένων δεν είναι δημόσιο πρόσωπο ή αν υπερισχύει το συμφέρον του έναντι του γενικότερου δημόσιου συμφέροντος περί πρόσβασης στις πληροφορίες.

Το εν λόγω δικαίωμα συνιστά απόρροια της γενικότερης ελευθερίας ανάπτυξης της προσωπικότητας του ατόμου (άρθρο 5 παρ.1 Σ), τελεί σε συνάρτηση τόσο με την κατοχύρωση της αξίας του ανθρώπου (άρθρο 2 παρ.1Σ) όσο και με το δικαίωμα προστασίας της ιδιωτικής ζωής (άρθρο 9 Σ) και της προστασίας των προσωπικών δεδομένων και του πληροφοριακού αυτοκαθορισμού του ατόμου (άρθρο 9^{A} Σ), με την έννοια να μην καθίσταται το άτομο αντικείμενο δημοσιογραφικού ενδιαφέροντος για αρνητικές πτυχές του πρότερου βίου του (Παναγοπούλου-Κουτνατζή, 2017). Με αυτή την έννοια συνιστά έκφανση του δικαιώματος του ατόμου στην παρουσίαση της δημόσιας εικόνας του εαυτού του και έγκειται στη λελογισμένη προστασία του από την ακούσια και χωρίς όρια δημόσια έκθεσή του, ώστε το άτομο να μην μετατρέπεται από υποκείμενο σε εργαλείο μέσα από την απεριόριστη υποβολή πληροφοριών του στα πλαίσια έρευνας από δημόσιους ή ιδιωτικούς φορείς προς εξυπηρέτηση άλλων σκοπών (π.χ. εμπορικών) (Ιγγλεζάκης, 2014). Γι' αυτό κι η συγκατάθεση και μόνον του ατόμου δεν επαρκεί να το προστατέψει από τυχόν κινδύνους διάδοσης των προσωπικών του πληροφοριών.

Αν και αρχικά εισήχθη ως δικαίωμα στη λήθη, πρακτικά κατέληξε να αναγράφεται και να χρησιμοποιείται ως δικαίωμα διαγραφής, δοθέντος ότι η ψηφιακή λήθη αποδεικνύεται μη ρεαλιστική και τεχνικά ανέφικτη. Νομολογιακά και σε επίπεδο διοικητικής πρακτικής γίνεται αντιληπτό μάλλον περισσότερο ως δικαίωμα αφαίρεσης από τη λίστα αναζήτησης (de-listing) ή αφαίρεσης από τηρούμενα αρχεία (de-indexing), παρά ως ένα απόλυτο δικαίωμα, κατά το οποίο θα ήταν εφικτό το ίδιο το υποκείμενο να αφαιρεί προσωπικά δεδομένα του που έχουν δημοσιευθεί ακόμη και από μέσα κοινωνικής δικτύωσης, αναγνωρίζοντας έτσι ως μοναδική εξαίρεση, την διατήρησή τους για λόγους επιτακτικούς (Παναγοπούλου-Κουτνατζή, 2017).

Περαιτέρω δεν συνιστά απόλυτο δικαίωμα καθώς υπάρχει ένα άκρο όριο στην εφαρμογή του. Σημειώνεται ότι η άσκηση του δικαιώματος στη λήθη αποκλείεται όταν η επεξεργασία είναι αναγκαία: α) για λόγους που ανάγονται στην ελευθερία της έκφρασης και στο δικαίωμα στην ενημέρωση, β) εφόσον η επεξεργασία επιβάλλεται βάσει του

ενωσιακού ή του εθνικού δικαίου του κράτους μέλους στο οποίο υπάγεται ο υπεύθυνος επεξεργασίας ή για λόγους εκπλήρωσης καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο της επεξεργασίας, γ) για λόγους δημόσιου συμφέροντος στον τομέα της δημόσιας υγείας, δ) για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς, εφόσον το δικαίωμα είναι πιθανόν να καταστήσει αδύνατη ή να εμποδίσει σε μεγάλο βαθμό την επίτευξη σκοπών της επεξεργασίας, ή ε) για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων (άρθρο 17 παρ. 3ΓΚΠΔ).

Ο πιο βασικός περιορισμός που γνωρίζει είναι αυτός που σχετίζεται με την άσκηση του δικαιώματος στην ελευθερία έκφρασης του άρθρου 14 Σ. όσον αφορά σε γεγονότα εύλογου ενδιαφέροντος ενημέρωσης του κοινού. Σκοπός του άρθρου 17 ΓΚΠΔ είναι η προστασία της *προσωπικότητας έναντι της ελευθερίας της πληροφορίας* θέτοντας, στον υπεύθυνο επεξεργασίας που δημοσιοποίησε προσωπικά δεδομένα, την υποχρέωση να τα διαγράψει πάραυτα, εάν δεν συντρέχει νόμιμος λόγος διατήρησής τους και επιπλέον να ενημερώσει κάθε τρίτο που έχει προβεί σε αναπαραγωγή τους σχετικά με το αίτημα διαγραφής (Tassis & Peristeraki, 2014). Βέβαια οι πολέμιοι του δικαιώματος στη λήθη κάνουν λόγο για επέμβαση στην ελεύθερη διάδοση της πληροφορίας και για δημιουργία καθεστώτος ανελευθερίας στο διαδίκτυο[112], επιχείρημα που ωστόσο δεν ευσταθεί αφού δεν γίνεται λόγος για διαγραφή του περιεχομένου ενός ιστότοπου αλλά για διαγραφή των στοιχείων ενός ατόμου από έναν ιστότοπο (Παναγοπούλου-Κουτνατζή, 2017).

Η προστιθέμενη αξία του δικαιώματος στη λήθη αναδεικνύεται κυρίως στις περιπτώσεις επεξεργασίας δεδομένων ανηλίκων, στις οποίες οι γονείς μπορούν να αιτηθούν την άμεση διαγραφή από τον υπεύθυνο επεξεργασίας όλων των προσωπικών δεδομένων των ανηλίκων τέκνων τους που έχουν δημοσιευθεί ή συλλεχθεί σε κοινωνικό δίκτυο, σε εφαρμογή ή πλατφόρμα για το χρονικό διάστημα μέχρι την ενηλικίωσή του ακόμη και για όσα δόθηκαν στο παρελθόν.

Τέλος, σύμφωνα με το άρθρο 34 του Ν. 4624/2019 περιορίζεται το κατ' άρθρο 17 παρ. 1 ΓΚΠΔ, προστατευόμενο δικαίωμα διαγραφής δεδομένων σε περιπτώσεις μη

[112] Βλ. σχετικά Powels (2015) Right to be forgotten: Swiss cheese internet or database of ruin?, διαθέσιμο σε https://www.theguardian.com/technology/2015/aug/01/right-to-be-forgotten-google-swiss-cheese-internet-database-of-ruin

αυτοματοποιημένης επεξεργασίας (ήτοι όσων τηρούνται σε φυσικά αρχεία) από δημόσιο ή ιδιωτικό φορέα, όταν λόγω της ιδιαίτερης φύσης της αποθήκευσής τους, είναι αδύνατη η διαγραφή ή απαιτείται προς τούτο δυσανάλογα μεγάλη προσπάθεια, καθώς και όταν τούτο αντίκειται στις συμβατικές ή νόμιμες περιόδους διατήρησης. Επιπλέον, σε ορισμένες περιπτώσεις αυτοματοποιημένης επεξεργασίας αντί της διαγραφής δύναται να εφαρμόζεται περιορισμός στην επεξεργασία (Αιτιολογική Έκθεση ΣχΝ, σελ.27).

3.10.2. Το δικαίωμα στη φορητότητα των δεδομένων

Όπως προκύπτει συνδυαστικά από την αιτιολογική σκέψη 68 του Προοιμίου και το άρθρο 20 ΓΚΠΔ, πρόκειται για το δικαίωμα του ατόμου να λαμβάνει τα προσωπικά δεδομένα που έχει παράσχει σε κάποιον υπεύθυνο επεξεργασίας, σε δομημένο και κοινά χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα διαλειτουργικό μορφότυπο και να τα διαβιβάζει σε άλλον υπεύθυνο επεξεργασίας, όταν η επεξεργασία γίνεται με αυτοματοποιημένο τρόπο. Παρέχει δηλαδή στα υποκείμενα έναν ευέλικτο τρόπο διαχείρισης εκ μέρους τους, των προσωπικών τους δεδομένων έτσι ώστε να διακινούν, αντιγράφουν ή μεταφέρουν εύκολα τα δεδομένα τους από ένα περιβάλλον τεχνολογίας σε ένα άλλο.

Οι σωρρευτικά συντρέχουσες προϋποθέσεις για την εφαρμογή του δικαιώματος αυτού είναι να υπάρχει *επεξεργασία,* -επί τη βάσει *συγκατάθεσης ή σύμβασης –, και αυτή να είναι αυτοματοποιημένη*. Άρα η διάταξη δεν εφαρμόζεται στα έγγραφα αρχεία που έχουν παρασχεθεί, ειμή μόνον εάν ο υπεύθυνος τα έχει ψηφιοποιήσει και το υποκείμενο τα ζητήσει. Περαιτέρω τα *δεδομένα πρέπει να αφορούν το υποκείμενο και να έχουν δοθεί από αυτό* (συνειδητά και ενεργητικά, όπως π.χ. τα στοιχεία σε λογαριασμό που καταχωρούνται με ηλεκτρονικά μέσα) ή *να έχουν συλλεχθεί από τη δράση ενός χρήστη κατά τη χρήση κάποιας υπηρεσίας ή συσκευής* και να είναι αυτά ακριβώς που έχουν παρασχεθεί από αυτό ή συλλεχθεί, και όχι συναγόμενα από τον υπεύθυνο επεξεργασίας ενώ η *άσκηση του* ίδιου του δικαιώματος *δεν πρέπει να επιδρά στα δικαιώματα και τις ελευθερίες τρίτων*. Επίσης τα δεδομένα του να έχουν παρασχεθεί σε *δομημένο, κοινά χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα, διαλειτουργικό μορφότυπο*[113], ήτοι όχι με κρυπτογραφημένους

[113] Ένα έγγραφο θεωρείται έγγραφο σε μηχαναγνώσιμο μορφότυπο όταν είναι σε μορφή αρχείου διαρθρωμένου, έτσι ώστε οι εφαρμογές λογισμικού να μπορούν να εντοπίσουν, αναγνωρίσουν και εξαγάγουν από αυτό συγκεκριμένα δεδομένα. Μηχαναγνώσιμα δεδομένα είναι εκείνα που έχουν κωδικοποιηθεί σε αρχεία διαρθρωμένα σε μηχαναγνώσιμο μορφότυπο βλ. σχετικά Κατευθυντήρια γραμμή

χαρακτήρες καθώς κάτι τέτοιο θα παρεμπόδιζε την ελεύθερη παροχή τους από τον έναν υπεύθυνο επεξεργασίας στον άλλο. Αν τα δεδομένα δεν μπορούν να εξαχθούν από τα έγγραφα, τότε αυτά δεν είναι έγγραφα σε μηχανανγώσιμο μορφότυπο και δεν εφαρμόζεται η διάταξη. Τα κράτη μέλη πρέπει να προωθούν τη χρήση μηχαναγνώσιμων μορφοτύπων (π.χ. XML, JSON, CSV), έτσι ώστε να δημιουργηθούν διαλειτουργικά και συμβατά συστήματα που θα επιτρέπουν τους καταναλωτές να μεταφέρονται σε διαφορετικά υπολογιστικά νέφη (clouds).

Κατ' ουσία το δικαίωμα στη φορητότητα απορρέει από το δικαίωμα της ελεύθερης ανάπτυξης προσωπικότητας. Συνιστά ιδιαίτερη έκφανση του δικαιώματος πρόσβασης στα προσωπικά δεδομένα - κυρίως όσον αφορά στο αντίστοιχο δικαίωμα που προβλέπεται στις τομεακές νομοθεσίες (π.χ. ηλεκτρονικές επικοινωνίες) - με βασικό του γνώρισμα το στοιχείο την ανεμπόδιστης παροχής των προσωπικών δεδομένων από πάροχο σε πάροχο, μέσω της ως άνω δομημένης και κοινά χρησιμοποιούμενης και μηχανικά αναγνώσιμης μορφής.

Το δικαίωμα στη φορητότητα[114] ενισχύει την προστασία των δεδομένων, βελτιώνει τον ανταγωνισμό μεταξύ των παρόχων υπηρεσιών και εξαλείφει τα αδικαιολόγητα εμπόδια που περιορίζουν τη διασυνοριακή ροή δεδομένων. Έτσι τα υποκείμενα των προσωπικών δεδομένων μπορούν να αποκτήσουν και επαναχρησιμοποιήσουν τα δεδομένα τους για δικούς τους σκοπούς σε διαφορετικές υπηρεσίες[115]. Ο κίνδυνος που ελλοχεύει είναι ορισμένες εταιρίες που συλλέγουν και αποθηκεύουν δεδομένα (απλά και ευαίσθητα) να τα διαβιβάσουν για το δικό τους συμφέρον, αθέμιτα και χωρίς να ζητήσουν την απαραίτητη συγκατάθεση του υποκειμένου τους ενώ έχει διατυπωθεί και η άποψη ότι μέσω της διαβίβασής τους διευκολύνεται η παρακολούθηση του υποκειμένου τους.

Εν κατακλείδι τα περισσότερα από τα ως άνω αναλυθέντα δικαιώματα συνιστούν μια περισσότερο επικαιροποιημένη εκδοχή τους, που αποσκοπεί στο να εξασφαλίσει τη μεγαλύτερη δυνατή και ομοιόμορφη προστασία του υποκειμένου τους υπό το πρίσμα του

που δίνεται στη σκέψη 21 του Προοιμίου της Οδηγίας 2013/37/ΕΕ (για την τροποποίηση της Οδηγίας 2003/98/ΕΚ σχετικά με την περαιτέρω χρήση πληροφοριών του δημόσιου τομέα).

[114] Βλ. Ομάδα Εργασίας άρθρου 29, Κατευθυντήριες γραμμές σχετικά με το δικαίωμα στη φορητότητα των δεδομένων, 16/EL, WP 242 rev.01

[115] Π.χ. για να μεταφέρουν δεδομένα προσωπικού χαρακτήρα από το Facebook σε άλλη πλατφόρμα δικτύωσης.

νέου κανονισμού ενώ η εισαγωγή του δικαιώματος στη λήθη και τη φορητότητα συμπληρώνει το εν λόγω θεσμικό πλαίσιο προστασίας των προσωπικών δεδομένων.

3.11. Τα εμπλεκόμενα πρόσωπα στην επεξεργασία προσωπικών δεδομένων

Ο ΓΚΔΠ αναγνωρίζει τα εξής πρόσωπα ως άμεσα εμπλεκόμενα στη διαδικασία επεξεργασίας των προσωπικών δεδομένων:

Ο «Υπεύθυνος επεξεργασίας» είναι το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα. Όταν οι σκοποί και ο τρόπος της επεξεργασίας αυτής καθορίζονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια για τον διορισμό του, μπορούν να προβλέπονται από το δίκαιο της Ένωσης ή από το δίκαιο του κράτους μέλους (άρθρο 4 παρ.7 ΓΚΠΔ). Ο υπεύθυνος επεξεργασίας βάσει του ΓΚΠΔ δεν υποχρεούται να γνωστοποιήσει την επεξεργασία στην Αρχή, ωστόσο οφείλει, όπως προαναφέρθηκε, να μεριμνά για την ικανοποίηση των δικαιωμάτων του υποκειμένου και να σταθμίζει το υπέρτερο συμφέρον σε σχέση με τα δικαιώματα αυτά[116].

Ο «Εκτελών την επεξεργασία» είναι το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας (άρθρο 4 παρ.8 ΓΚΠΔ).

Όταν η επεξεργασία γίνεται από τον εκτελούντα αυτήν, πρέπει να διέπεται είτε από σύμβαση είτε από το νόμο και να ορίζει το αντικείμενο της επεξεργασίας, τη διάρκεια της επεξεργασίας, τη φύση και το σκοπό της, το είδος των δεδομένων και τις κατηγορίες υποκειμένων των δεδομένων καθώς και τις υποχρεώσεις και τα δικαιώματα του υπεύθυνου επεξεργασίας (άρθρο 28 παρ. 3). Τόσο ο υπεύθυνος επεξεργασίας όσο και ο εκτελών την επεξεργασία ευθύνονται για τη διασφάλιση και απόδειξη της τήρησης των διατυπώσεων νομιμότητας της επεξεργασίας σύμφωνα με τα οριζόμενα στον ΓΚΠΔ (άρθρα 32 και 24 ΓΚΠΔ) εξού και σε περίπτωση παραβίασης ευθύνονται από κοινού και εις ολόκληρον.

Ο «Αποδέκτης» είναι το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας, στα οποία κοινοποιούνται τα δεδομένα προσωπικού χαρακτήρα, είτε πρόκειται για τρίτον είτε όχι (άρθρο 4 παρ. 9ΓΚΠΔ). Δεν θεωρούνται αποδέκτες οι δημόσιες αρχές που

[116] Βλ. σχετικά Ετήσια Έκθεση ΑΠΔΠΧ, 2018 σελ. 65

ενδέχεται να λάβουν δεδομένα προσωπικού χαρακτήρα στο πλαίσιο συγκεκριμένης έρευνας σύμφωνα με το δίκαιο της Ένωσης ή κράτους μέλους.

«Τρίτος» είναι οποιοδήποτε φυσικό ή νομικό πρόσωπο, δημόσια αρχή, υπηρεσία ή φορέας, με εξαίρεση το υποκείμενο των δεδομένων, τον υπεύθυνο επεξεργασίας, τον εκτελούντα την επεξεργασία και τα πρόσωπα τα οποία, υπό την άμεση εποπτεία του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα.

3.12. Οι υποχρεώσεις του υπεύθυνου επεξεργασίας και η χρήση των εργαλείων του ΓΚΠΔ

Ο νέος κανονισμός εισάγει ορισμένα νέα εργαλεία συμμόρφωσης, των οποίων η χρήση ανατίθεται κυρίως στο υπεύθυνο επεξεργασίας υπό μορφή τήρησης ορισμένων εκ μέρους του υποχρεώσεων, απορρεουσών από τις *βασικές αρχές και κυρίως την ενισχυμένη αρχή της διαφάνειας*, τον *τρόπο συλλογής, επεξεργασίας* και *τήρησης δεδομένων* και τη *νέα αρχή της λογοδοσίας*, κατά την οποία ο υπεύθυνος αυτής φέρει την ευθύνη και πρέπει να αποδείξει τη συμμόρφωσή του με όλες τις αρχές που διέπουν την επεξεργασία.

Ο υπεύθυνος επεξεργασίας πρέπει να εφαρμόσει όλα τα απαραίτητα και κατάλληλα τεχνικά και οργανωτικά μέτρα όχι μόνον για να διασφαλίσει αλλά και για να αποδείξει το σύννομο της επεξεργασίας, αφού λάβει υπόψη του ένα ευρύ φάσμα παραγόντων, όπως τη φύση, το πεδίο εφαρμογής του ΓΚΠΔ, το πλαίσιο και τους σκοπούς επεξεργασίας αλλά και τους κίνδυνους που μπορούν να επέλθουν για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων (άρθρο 24 ΓΚΠΔ). Τα ως άνω μέτρα μπορεί να εμπεριέχουν *πολιτικές προστασίας δεδομένων* (άρθρο 24 παρ.2) ή να συνίστανται στην *εκπόνηση εγκεκριμένων κωδίκων δεοντολογίας ή μηχανισμού πιστοποίησης*. Μέσω αυτών ο υπεύθυνος επεξεργασίας αποδεικνύει τη συμμόρφωσή του με τις υποχρεώσεις του (άρθρου 24 παρ. 3).

α. Η προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού (Data Protection by design and by default)

Η έννοια της *προστασίας των δεδομένων κατά τον σχεδιασμό*, που εμπεριέχεται στη διάταξη του άρθρου 25 ΓΚΠΔ, προέρχεται από το χώρο της πληροφορικής και συνίσταται στην διασφάλιση της ιδιωτικότητας ως βασική και κατά κανόνα ενσωματωμένη επιλογή

ενός συστήματος, μιας εφαρμογής ή μιας επεξεργασίας, που αποσκοπεί στην προστασία του, μέχρι τώρα αποδεδειγμένα ελάχιστα έως καθόλου ενημερωμένου χρήστη, σχετικά με τους επερχόμενους κινδύνους από την κοινοποίηση των δεδομένων του. Ουσιαστικά συνίσταται στην ευθύνη του υπεύθυνου επεξεργασίας να δράσει κατά τρόπο *προληπτικό* και όχι να αντιμετωπίσει κατασταλτικά την παραβίαση της ιδιωτικής ζωής και την προσβολή της ιδιωτικής σφαίρας.

Η προστασία της ιδιωτικότητας διά του σχεδιασμού (protection by design) προηγείται του σταδίου της εξ ορισμού προστασίας (privacy by default) καθώς απαιτεί τη λήψη συγκεκριμένων μέτρων κατά το σχεδιασμό ενός συστήματος που αφορούν: α) τον *όγκο και την ποιότητα* των δεδομένων των οποίων η επεξεργασία είναι αναγκαία *(μέσω της ψευδωνυμοποίησης και ελαχιστοποίησης),* β) την *αξιολόγηση των κινδύνων (Risk Assessment)* που μπορεί να επέλθουν από την επεξεργασία και *των επιπτώσεών* τους στην ιδιωτικότητα (τέτοιο μέτρο μεταξύ άλλων είναι και η εκπόνηση μελέτης εκτίμησης αντικτύπου) και γ) την *υιοθέτηση της αρχής της εξ ορισμού προστασίας (Protection by default).*

Δρώντας προληπτικά και δη στη *φάση του σχεδιασμού (protection by design)* κι όχι εκ των υστέρων, και λαμβάνοντας τα ως άνω μέτρα, ο υπεύθυνος επεξεργασίας δημιουργεί αυξημένα εχέγγυα εφαρμογής των αρχών της προστασίας δεδομένων, αφού προηγουμένως έχει συνεκτιμήσει ορισμένους παράγοντες, όπως τις πρόσφατες τεχνολογικές εξελίξεις, το κόστος, τη φύση και το πεδίο εφαρμογής των μέτρων, το πλαίσιο και τους σκοπούς επεξεργασίας, τους ενδεχόμενους κινδύνους που μπορεί να υποστούν τα δικαιώματα και οι ελευθερίες των φυσικών προσώπων, προβαίνοντας σε εκτίμηση κινδύνου.

Αφετέρου σύμφωνα με την *εξ ορισμού προστασία*, ο υπεύθυνος επεξεργασίας πρέπει να μεριμνήσει, ώστε κάθε σύστημα να διαθέτει ορισμένες *προεπιλεγμένες ρυθμίσεις*, που θα διασφαλίζουν ότι επεξεργασίας τυγχάνουν *μόνο* τα απαραίτητα για το σκοπό επεξεργασίας δεδομένα, σύμφωνα με την αρχή της αναλογικότητας και της διαφάνειας. Πρόκειται κατ' ουσία για την εφαρμογή προϊόντων και υπηρεσιών (ηλεκτρονικών και μη) που δημιουργούν φιλικές συνθήκες για την προστασία από τον αρχικό σχεδιασμό τους. Κλασσικό παράδειγμα συνιστούν οι υπηρεσίες ηλεκτρονικής κοινωνικής δικτύωσης, όπου εξαρχής πρέπει να δίνεται η δυνατότητα στο χρήστη να επιλέγει τις ρυθμίσεις που θα προστατεύουν περισσότερο τα προσωπικά του δεδομένα.

Βάσει της *προστασίας από το σχεδιασμό και εξ ορισμού* ο υπεύθυνος επεξεργασίας πρέπει πρωτίστως να προβαίνει σε χαρτογράφηση της ροής των δεδομένων (data flow mapping) στην οποία θα συμμετέχει *το σύνολο* του οργανισμού ή της επιχείρησης αφού η προστασία της ιδιωτικότητας ήδη από τη φάση του σχεδιασμού, προϋποθέτει ότι όλες οι υπηρεσίες και τα επιμέρους τμήματα, εξετάζουν τα δεδομένα τους και τον τρόπο με τον οποίο θα τα χειρίζονται. Η θεώρηση των προσωπικών δεδομένων από τη σκοπιά της ιδιωτικότητάς τους ήδη από την έναρξη της ανάπτυξης του προϊόντος και καθ' όλη την αλυσίδα του εφοδιασμού έως τον τελικό πελάτη, συνιστά και τον πυρήνα του Κανονισμού, που οδηγεί στον περιορισμό του εύρους και του βαθμού επεξεργασίας, αλλά και του χρόνου αποθήκευσης των δεδομένων, εφαρμόζοντας τις αρχές που διαπνέουν τον ίδιο ΓΚΠΔ και υλοποιώντας τις επιταγές του[117].

β. Η υποχρέωση τήρησης αρχείου δραστηριοτήτων επεξεργασίας

Ο υπεύθυνος επεξεργασίας ή ο εκτελών αυτήν, υποχρεούται περαιτέρω σύμφωνα με το άρθρο 30 ΓΚΠΔ να τηρεί αρχείο (φυσικό ή ηλεκτρονικό) δραστηριοτήτων επεξεργασίας: α) για επιχειρήσεις ή οργανισμούς που απασχολούν περισσότερα από 250 άτομα προσωπικό, β) όταν η επεξεργασία είναι συστηματική και εγκυμονεί κινδύνους για τα δεδομένα ή γ) όταν περιλαμβάνει ειδικές κατηγορίες δεδομένων των άρθρων 9 και 10 ΓΚΠΔ (βιομετρικά, γενετικά, σχετικά με ποινικές καταδίκες κ.α.). Τα αρχεία αυτά τίθενται στην διάθεση της εκάστοτε εποπτικής Αρχής αν το ζητήσει για να ασκήσει τις αρμοδιότητές της και εμπεριέχουν: 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 τυχόν διαβιβάσεις σε χώρες εκτός ΕΕ, στ) τις προθεσμίες διαγραφής των δεδομένων, ζ) τα μέτρα ασφαλείας.

γ. Η υποχρέωση τήρησης εξειδικευμένων μέτρων ασφαλείας

Ο ΓΚΠΔ προκειμένου να εξασφαλίσει την ασφαλή επεξεργασία των προσωπικών δεδομένων έναντι των κινδύνων, καθιερώνει την αντίστοιχη υποχρέωση ασφαλείας στον υπεύθυνο επεξεργασίας. Με τον όρο ασφάλεια πληροφορίας/δεδομένων (information/data security) εννοούμε την μεθοδολογία, τις μεθόδους και τεχνικές που καλείται να αναπτύξει και εφαρμόσει ο υπεύθυνος προστασίας για να εξασφαλιστούν η α) εμπιστευτικότητα

[117] https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_387

(confidentiality), β) η ακεραιότητα (integrity) και γ) η διαθεσιμότητα (availability). Γι' αυτό στη διάταξη του άρθρου 32 ο ΓΚΠΔ προβλέπει τα ενδεδειγμένα και εξειδικευμένα τεχνικά και οργανωτικά μέτρα ασφαλούς επεξεργασίας, ήτοι:

α) ψευδωνυμοποίηση και κρυπτογράφηση
β) διασφάλιση απορρήτου, ακεραιότητας, διαθεσιμότητας και αξιοπιστίας,
γ) αποκατάσταση διαθεσιμότητας και πρόσβασης σε περίπτωση συμβάντος,
δ) δοκιμή, εκτίμηση και διαρκής αξιολόγηση της αποτελεσματικότητας των μέτρων,
ε) χρήση εγκεκριμένου κώδικα δεοντολογίας ή μηχανισμού πιστοποίησης για την απόδειξη της συμμόρφωσης
στ) διαδικασίες χειρισμού περιστατικών παραβίασης (Strecht, 2019).

δ. Η υποχρέωση γνωστοποίησης

Σύμφωνα με τα άρθρα 33 και 34ΓΚΠΔ ο υπεύθυνος επεξεργασίας οφείλει να ακολουθήσει μια συγκεκριμένη διαδικασία, σε περίπτωση που επέλθει κάποιο περιστατικό παραβίασης δεδομένων. Περιστατικά παραβίασης δεδομένων προσωπικού χαρακτήρα κατά το άρθρο 4 παρ. 12, είναι εκείνα που οδηγούν σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ αδείας κοινολόγηση ή πρόσβαση δεδομένων που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατά άλλο τρόπο σε επεξεργασία[118]. Η παραβίαση είναι μια μορφή περιστατικού ασφαλείας σύμφωνα με τις Κατευθυντήριες Γραμμές του WP 29 (Strecht, 2019)[119]. Έτσι σε περίπτωση παραβίασης ο υπεύθυνος επεξεργασίας πρέπει να ακολουθήσει το εξής πρωτόκολλο: μόλις ανιχνεύσει το περιστατικό παραβίασης, πρέπει να διερευνήσει την περίπτωση και να λάβει ακριβή γνώση του περιστατικού. Εάν διαπιστώσει ότι η παραβίαση δύναται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, υποχρεούται αμελλητί και σε κάθε περίπτωση εντός 72 ωρών να γνωστοποιήσει την παραβίαση στην εποπτική αρχή. Εάν δεν προκύψει κίνδυνος, δεν είναι υπόχρεος σε κοινοποίηση του περιστατικού στην Αρχή, ωστόσο σε κάθε περίπτωση προβαίνει σε καταγραφή όλων των περιστατικών. Αν όμως η παραβίαση ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος υποχρεούται να ανακοινώσει αμελλητί το περιστατικό στα επηρεαζόμενα

[118] Βλ. άρθρα 33 και 34 ΓΚΠΔ, ΕΕ L 119/52, 4.5.2016. Βλ. επίσης και Ομάδα εργασίας άρθρο 29, Guidelines on Personal data breach notification under Regulation 2016/679, 18/EN, WP 250rev.01.,
[119] Βλ. σχετικά Article 29 Data Protection Working Party. Guidelines on Personal data breach notification under regulation 2016/679, Technical Report October, 2017, καθώς και Article 29 Data Protection Working Party. Opinion 03/2014 on Personal Data Breach Notification, Technical Report March, 2014.

φυσικά πρόσωπα και να τα ενημερώσει για λήψη μέτρων αυτοπροστασίας (Grey & Brown, 2020).

ε. Η Υποχρέωση διενέργειας Εκτίμησης Αντικτύπου Προσωπικών Δεδομένων

Ο υπεύθυνος επεξεργασίας οφείλει, κατά το άρθρο 35 ΓΚΠΔ[120], να διενεργεί εκτίμηση επιπτώσεων/αντικτύπου (Data protection impact assessment -DPIA)[121] όταν η επεξεργασία ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των ατόμων, πριν προβεί στην επεξεργασία, ώστε να διαγνώσει τις τυχόν επιπτώσεις που θα έχει η εν λόγω επεξεργασία στην προστασία των δεδομένων. Πρόκειται ουσιαστικά για ένα εργαλείο ελέγχου και απόδειξης συμμόρφωσης με τον ΓΚΠΔ που χρησιμοποιείται όταν η επεξεργασία είναι: συστηματική, μεγάλης κλίμακας, αφορά ειδικές κατηγορίες δεδομένων και βασίζεται στη χρήση νέων τεχνολογιών[122] (άρθρο 35 παρ. 3 ΓΚΠΔ). Η διάταξη αυτή αναγνωρίζει ενδεικτικά τις πράξεις επεξεργασίας που ενέχουν υψηλό κίνδυνο αλλά η παρ. 4 του άρθρου 35 λειτουργώντας συμπληρωματικά, προβλέπει ότι η εποπτική αρχή καταρτίζει και δημοσιοποιεί κατάλογο με τις πράξεις επεξεργασίας για τις οποίες θεωρεί απαραίτητη τη διενέργεια μελέτης αντικτύπου, τον οποίο ανακοινώνει στο ΕΣΠΔ[123].

Η DPIA επιδιώκει να εξασφαλίσει την τήρηση της θεμελιώδους αρχής προστασίας δεδομένων από τον σχεδιασμό (protection by design), να καταδείξει τις απαιτούμενες τεχνολογικές λύσεις για τη διασφάλιση της ασφαλούς επεξεργασίας, όπως επίσης να διευκολύνει την ορθή αξιολόγηση των περιστατικών παραβίασης των δεδομένων. Σύμφωνα με τις Κατευθυντήριες Γραμμές της WP 29, συνιστά *«μια διαδικασία που έχει σχεδιαστεί για να περιγράψει την επεξεργασία, να αξιολογήσει την αναγκαιότητα και την αναλογικότητά της και να συνδράμει στη διαχείριση των κινδύνων για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων που συνεπάγεται η επεξεργασία των δεδομένων*

[120] Βλ. άρθρο 35 ΓΚΠΔ, ΕΕ L 119/53, 4.5.2016.
[121] Εφεξής DPIA.
[122] https://www.dpa.gr/el/foreis/ektimisi_adiktipou_kai_diavouleush/ektimisi_adiktipou
[123] Η ΑΠΔΠΧ κατάρτισε, βάσει της διάταξης αυτής σχέδιο καταλόγου με τα είδη των πράξεων επεξεργασίας που υπόκεινται στην υποχρέωση για διενέργεια DPIA. Πριν την έκδοση του εν λόγω καταλόγου εφάρμοσε, το μηχανισμό συνεκτικότητας, ανακοινώνοντας το σχέδιο καταλόγου στο ΕΣΠΔ, το οποίο στη συνεδρίαση της ολομέλειας της 25ης Σεπτεμβρίου 2018, εξέδωσε τη Γνώμη 7/2018 σχετικά με το σχέδιο ΑΠΔΠΧ. Η Αρχή, με την με αριθμό 65/2018 Απόφασή της, αποφάσισε, (κατ' άρθρο 64 παρ. 7 του ΓΚΠΔ), την τροποποίηση του καταλόγου ΕΑΠΔ βάσει των συστάσεων της γνώμης 7/2018 του ΕΣΠΔ και την ανακοίνωσή του στο ΕΣΠΔ, που δημοσιεύθηκε στο ΦΕΚ Β' 1622/10-5-2019.

προσωπικού χαρακτήρα, με την αξιολόγησή τους και τον καθορισμό μέτρων για την αντιμετώπισή τους.» [124]

Έτσι η DPIA περιλαμβάνει τη συστηματική περιγραφή των προβλεπόμενων πράξεων και σκοπών επεξεργασίας, το έννομο συμφέρον που επιδιώκει ο υπεύθυνος επεξεργασίας, εκτίμηση αναγκαιότητας και αναλογικότητας των πράξεων επεξεργασίας, εκτίμηση κινδύνων ως προς τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, καθώς επίσης και τα προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων. Εάν μάλιστα, σύμφωνα με τη διενεργηθείσα εκτίμηση επιπτώσεων και παρά την πρόβλεψη μέτρων προστασίας, ο βαθμός επικινδυνότητας της επεξεργασίας παραμένει υψηλός, ο υπεύθυνος επεξεργασίας υποχρεούται να προβεί σε προηγούμενη διαβούλευση με την αρμόδια εποπτική Αρχή και να ζητήσει την γνώμη της και δη όταν η επεξεργασία αφορά εκτέλεση καθήκοντος του υπευθύνου προς το δημόσιο συμφέρον, περιλαμβανομένης της επεξεργασίας σε σχέση με την κοινωνική προστασία και τη δημόσια υγεία. Και εάν ο κίνδυνος συνεχίζει να είναι υψηλός για τα δεδομένα, ακολουθεί εκ νέου διαβούλευση με την Αρχή. Στην περίπτωση αυτή η εποπτική αρχή, οφείλει να συντάξει κατάλογο με τα είδη επεξεργασιών που χρήζουν διενέργειας εκτίμησης αντικτύπου. Περαιτέρω τα κράτη-μέλη δύνανται να κρίνουν αναγκαία την προγενέστερη εκπόνηση DPIA, όταν κάποιος οργανισμός ή επιχείρηση σκοπεύει να εφαρμόσει μια κοινή πλατφόρμα επεξεργασίας ή αν πρόκειται να εκδοθεί κάποιο νομοθέτημα που προβλέπει την άσκηση καθηκόντων ενός οργανισμού ή επιχείρησης και ρυθμίζει τη συγκεκριμένη πράξη επεξεργασίας.

στ. Η εκπόνηση και τήρηση Κώδικα Δεοντολογίας

Ο Κώδικας Δεοντολογίας (άρθρο 40 ΓΚΠΔ), συνιστά ένα ακόμη ισχυρό μέσο απόδειξης ορθής εφαρμογής του ΓΚΠΔ. Γι' αυτό τα κράτη μέλη, οι εποπτικές αρχές και το ΕΣΠΔ ενθαρρύνουν την εκπόνησή του καθώς μέσω αυτού επιχειρείται ο έλεγχος εφαρμογής σε διάφορους τομείς, η θεμιτή και διαφανής επεξεργασία ή συλλογή δεδομένων προσωπικού χαρακτήρα, η ορθή ενημέρωση των υποκειμένων των δεδομένων και η άσκηση των δικαιωμάτων τους, η προστασία των παιδιών κ.ά..

Η εκπόνησή τους ανατίθεται συνήθως σε ενώσεις που εκπροσωπούν τους υπευθύνους ή τους εκτελούντες την επεξεργασία και η έγκρισή τους διενεργείται από την αρμόδια

[124] Βλ. Ομάδα Εργασίας άρθρου 29, Κατευθυντήριες Γραμμές για την εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) και καθορισμός του κατά πόσον η επεξεργασία «ενδέχεται να επιφέρει υψηλό κίνδυνο» για τους σκοπούς του κανονισμού 2016/679, 17/EN, WP 248 rev.01, p.4.

εποπτική αρχή, όταν ο κώδικας σχετίζεται με επεξεργασία εντός των ορίων του κράτους μέλους, ενώ, αν το σχέδιο κώδικα αναφέρεται σε επεξεργασία όπου εμπλέκονται περισσότερα κράτη-μέλη, τότε χρήζει έγκρισης και από το ΕΣΠΔ. Αρμόδια για την γενική ισχύ των κωδίκων δεοντολογίας είναι η Ευρωπαϊκή Επιτροπή.

Σε πρακτικό επίπεδο ένας οργανισμός ή μια επιχείρηση μπορεί μέσω των προβλέψεών του στον Κώδικα Δεοντολογίας, να αποτρέψει ή περιορίσει την μη εξουσιοδοτημένη πρόσβαση με τη λήψη κατάλληλων μέτρων, όπως π.χ. μέσω εσωτερικού κανονισμού ασφαλείας, εγκατάστασης κατάλληλου λογισμικού προστασίας από ιούς, ενεργοποίησης «τείχους προστασίας» (firewall), φύλαξης αντιγράφων ασφαλείας (backups), προστασίας δικτύου wi-fi με κωδικούς πρόσβασης κ.α..

ζ. Η Πιστοποίηση

Ο ΓΚΠΔ προβλέπει περαιτέρω ως μέθοδο ελέγχου εφαρμογής και συμμόρφωσης την Πιστοποίηση του άρθρου 42, θεσπίζοντας εθελοντικά και με διαφανείς διαδικασίες έναν μηχανισμό πιστοποίησης προστασίας δεδομένων, σφραγίδων και σημάτων προστασίας δεδομένων αναφορικά με τις πράξεις επεξεργασίας του υπευθύνου ή του εκτελούντα την επεξεργασία με τις διατάξεις του ΓΚΠΔ.

Το άρθρο 42 παρ. 5 προβλέπει την περίπτωση της κοινής Πιστοποίησης, ήτοι της Ευρωπαϊκής Σφραγίδας Προστασίας Προσωπικών Δεδομένων, η οποία χορηγείται όταν πληρούνται τα κριτήρια του άρθρου 58 παρ.3 και εν συνεχεία εγκριθούν από την εποπτική αρχή ή το ΕΣΠΔ. Στην παρ. 3 του άρθρου 42 γίνεται μνεία για τη μέγιστη διάρκεια της πιστοποίησης που είναι 3τής και η οποία μπορεί να ανανεωθεί από τους αρμόδιους φορείς πιστοποίησης του άρθρο 43 του ΓΚ που είναι διαπιστευμένοι είτε από την εποπτική αρχή, είτε από τον εθνικό οργανισμό διαπίστευσης. Κατ' εφαρμογή του άρθρου 43 ΓΚΠΔ, ο κυρωτικός Ν. 4624/2019 στη διάταξη του άρθρου 37 παρ.1 ορίζει αρμόδιο για τη διαπίστευση των φορέων πιστοποίησης στην Ελλάδα, το Εθνικό Σύστημα Διαπίστευσης (Ε.ΣΥ.Δ.)[125] το οποίο λειτουργεί με βάση το πρότυπο EN-ISO/IEC17065:2012[126].

η. Οι διαβιβάσεις

Ο ΓΚΠΔ προβαίνει στον εξορθολογισμό των διεθνών διαβιβάσεων. Σύμφωνα με τη διάταξη του άρθρου 44 του ΓΚΠΔ, κάθε διαβίβαση δεδομένων προς τρίτη χώρα ή διεθνή

[125] Βλ. σχετικά www.esyd.gr
[126] Άρθρο 37-Διαπίστευση φορέων πιστοποίησης και πιστοποίηση, Αιτιολογική Έκθεση ΣχΝ, σελ. 27

οργανισμό πρέπει να είναι νόμιμη σύμφωνα με τις γενικές διατάξεις των άρθρων 5, 6, 9 και τους όρους του Κεφαλαίου V. Κατά την πάγια ερμηνεία των διατάξεων της WP29, *οι διεθνείς διαβιβάσεις πρέπει να προσεγγίζονται «ολιστικά και πολυεπίπεδα» («holistic and layered approach»)*, ήτοι ως βάση νομιμότητας της διεθνούς διαβίβασης να προτιμώνται οι αποφάσεις επάρκειας (άρθρο 45 ΓΚΠΔ)[127]. Ελλείψει τέτοιας απόφασης, ο υπεύθυνος επεξεργασίας ή εκτελών, που επιθυμεί να διαβιβάσει προσωπικά δεδομένα εκτός Ε.Ε., πρέπει να παρέχει τις κατάλληλες εγγυήσεις χρησιμοποιώντας κάποιο από τα εργαλεία διαβίβασης του άρθρου 46 ΓΚΠΔ, δηλαδή τους Δεσμευτικούς Εταιρικούς Κανόνες (BCR)[128] ή τις τυποποιημένες συμβατικές ρήτρες ή τον εγκεκριμένο κώδικα δεοντολογίας κ.λπ.. Στην περίπτωση που δεν μπορεί να εφαρμοστεί κανείς από τους ως άνω μηχανισμούς των άρθρων 45-46, ύστατη λύση συνιστά η υπό προϋποθέσεις εφαρμογή, των παρεκκλίσεων του άρθρου 49 του ΓΚΠΔ (ΑΠΔΠΧ)[129].

Εν κατακλείδι σημειώνεται ότι τα ανωτέρω εργαλεία αναδεικνύονται σε υψίστης σημασίας μέσα επίτευξης των στόχων του νέου Κανονισμού καθώς η κατά μεγάλο ποσοστό σωρρευτική χρησιμοποίησή τους από τον υπεύθυνο επεξεργασίας, μπορεί να δημιουργήσει αυξημένα εχέγγυα για την προστασία των προσωπικών δεδομένων στα πλαίσια της επεξεργασίας τους τόσο από ιδιωτικούς όσο και από δημόσιους φορείς.

---

[127] Οι διαβιβάσεις βάσει απόφασης επάρκειας της Επιτροπής δεν απαιτούν έκδοση άδειας απ΄ την εποπτική αρχή και μπορεί να αφορούν είτε τρίτη χώρα στο σύνολό της είτε έδαφος ή συγκεκριμένο τομέα ή τομείς της τρίτης χώρας ή του διεθνούς οργανισμού. Μέχρι σήμερα, η Επιτροπή έχει εκδώσει 12 αποφάσεις επάρκειας για τις εξής χώρες: Ανδόρα, Αργεντινή, Καναδά, νήσους Φερόες, Γκέρνσεϊ, Ισραήλ, νήσο του Μαν, Τζέρσεϊ, Νέα Ζηλανδία, Ελβετία, Ουρουγουάη και ΗΠΑ (μόνο στο πλαίσιο του Privacy Shield). Μετά την απόφαση Schrems, οι υπάρχουσες αποφάσεις επάρκειας τροποποιήθηκαν με την εκτελεστική απόφαση (ΕΕ) 2016/2295. Ιδιαίτερη βαρύτητα έχει η 2016/1250 απόφαση επάρκειας της Επιτροπής που αφορά την επάρκεια προστασίας του μηχανισμού της Ασπίδας Προστασίας (Privacy Shield), την οποία ωστόσο το ΔΕΕ έκρινε ανίσχυρη δυνάμει της C‑311/18 απόφασης που εξέδωσε στις 16-07-2020, παραπέμποντας ουσιαστικά στις τυποποιημένες συμβατικές ρήτρες 2010/87 (SCC) για τη διαβίβαση προσωπικών δεδομένων στις ΗΠΑ, αρκεί επί τη βάσει αυτών ο εξαγωγέας και ο εισαγωγέας των δεδομένων να εξασφαλίζουν το επίπεδο προστασίας που κατοχυρώνει ο ΓΚΠΔ, βλ. απόφαση C‑311/18 - 16-07-2020, διαθέσιμη σε : http://curia.europa.eu/juris/document/document.jsf;jsessionid=699F5010F9ED77A76EF28523A1A60EE9?text=&docid=228677&pageIndex=0&doclang=EL&mode=req&dir=&occ=first&part=1&cid=10320201 . Βλ. και https://www.dpa.gr/el/enimerwtiko/thematikes_enotites/diavivaseis_ee/schrems_II

[128] Δεσμευτικοί Εταιρικοί Κανόνες (BCR) είναι οι πολιτικές προστασίας δεδομένων προσωπικού χαρακτήρα τις οποίες ακολουθεί ένας υπεύθυνος επεξεργασίας ή εκτελών την επεξεργασία εγκατεστημένος στο έδαφος κράτους μέλους για διαβιβάσεις ή δέσμη διαβιβάσεων δεδομένων προσωπικού χαρακτήρα σε υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία σε μια ή περισσότερες τρίτες χώρες εντός ομίλου επιχειρήσεων ή ομίλου εταιριών που ασκεί κοινή οικονομική δραστηριότητα, βλ. άρθρο 4 παρ. 20 ΕΕ L 119/34, 4.05.2016.

[129] Βλ. επίσημη ιστοσελίδα ΑΠΔΠΧ https://www.dpa.gr/el/enimerwtiko/thematikes_enotites/diavivaseis_ee

3.13. Ο Υπεύθυνος Προστασίας Δεδομένων

Σύμφωνα με τον ΓΚΠΔ «Υπεύθυνος Προστασίας Δεδομένων» (ΥΠΔ) (Data Protection Officer-DPO) είναι το άτομο που διευκολύνει τη συμμόρφωση του υπεύθυνου επεξεργασίας και του εκτελούντος την επεξεργασία και το οποίο μεσολαβεί μεταξύ των ενδιαφερομένων μερών (π.χ. εποπτικές αρχές, υποκείμενα δεδομένων) ενώ κατά το Βαρβέρη (2018) *«είναι η φωνή της συνείδησης της επιχείρησης»*. Ο ΥΠΔ διορίζεται βάσει των επαγγελματικών του προσόντων και κυρίως της εμπειρογνωσίας του στον τομέα του δικαίου και των πρακτικών περί προστασίας δεδομένων[130], καθώς και βάσει της ικανότητας εκπλήρωσης των καθηκόντων που αναφέρονται στο άρθρο 39 ΓΚΠΔ (Sousa & Bessa Vilela, 2019). Ο ρόλος του είναι κυρίως *συμβουλευτικός*, καθώς αναφέρεται απευθείας στη διοίκηση ενός φορέα και στο προσωπικό του σχετικά με τις υποχρεώσεις τους για την προστασία των δεδομένων και όχι αποφασιστικός αφού δεν υπέχει προσωπική ευθύνη στην περίπτωση μη συμμόρφωσης προς τις διατάξεις του ΓΚΠΔ. Σύμφωνα με τη διάταξη του άρθρου 37 ΓΚΠΔ, ο ΥΠΔ ορίζεται από τον υπεύθυνο επεξεργασίας και τον εκτελούντα την επεξεργασία υποχρεωτικά όταν α) η επεξεργασία διενεργείται από δημόσια αρχή ή φορέα πλην των δικαστηρίων, β) οι βασικές δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν πράξεις επεξεργασίας που λόγω της φύσης και/ή των σκοπών τους, απαιτούν τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων[131] ή γ) οι βασικές δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, συνιστούν μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα και δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα[132].

Οι αρμοδιότητές του ΥΠΔ προβλέπονται στο άρθρο 39 ΓΚΠΔ και συνίστανται στα εξής:

[130] Βλ. άρθρο 37 παρ. 5 ΕΕ L 119/55 4.5.2016

[131] Χαρακτηριστικό παράδειγμα είναι τα νοσοκομεία, οι εταιρίες παρακολούθησης και συστημάτων ασφαλείας κ.α. Ως «τακτική και συστηματική παρακολούθηση» ορίζεται εκείνη που περιλαμβάνει όλες τις μορφές ανίχνευσης και κατάρτισης προφίλ στο διαδίκτυο, συμπεριλαμβανομένων των σκοπών της συμπεριφορικής διαφήμισης, η στοχευμένη επικοινωνία με email, ο γεωεντοπισμός, η χρήση κλειστών κυκλωμάτων παρακολούθησης. Βλ. σχετικά σε https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations_el

[132] Ενδεικτικά αναφέρουμε ως χαρακτηριστικά παραδείγματα επεξεργασίας δεδομένων μεγάλης κλίμακας, αυτήν που γίνεται σε τράπεζες, νοσοκομεία, ασφαλιστικές εταιρίες, εταιρίες μηχανοργάνωσης, εταιρίες επεξεργασίας δεδομένων καταναλωτών. Αντίθετα η επεξεργασία δεδομένων ασθενών από ιδιώτη ιατρό ή η επεξεργασία δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα από ιδιώτη δικηγόρο, δεν συνιστούν επεξεργασία μεγάλης κλίμακας.

α) ενημερώνει και συμβουλεύει τον υπεύθυνο επεξεργασίας ή τον εκτελούντα επεξεργασία και τους υπαλλήλους του σχετικά με τις απορρέουσες από τον ΓΚΠΔ υποχρεώσεις,
β) παρακολουθεί τη συμμόρφωση με τον ΓΚΠΔ, με διατάξεις της Ένωσης ή του κράτους μέλους σχετικά με την προστασία δεδομένων και τις πολιτικές τους συμπεριλαμβανομένων της ανάθεσης αρμοδιοτήτων, της ευαισθητοποίησης και της κατάρτισης των υπαλλήλων που μετέχουν στις πράξεις επεξεργασίας και των ελέγχων
γ) παρέχει συμβουλές, όταν ζητείται, όσον αφορά την εκτίμηση αντικτύπου και παρακολουθεί την υλοποίησή της,
δ) συνεργάζεται με την εποπτική αρχή και
ε) ενεργεί ως σημείο επικοινωνίας για την εποπτική αρχή και τα φυσικά πρόσωπα για ζητήματα που σχετίζονται με την επεξεργασία, συμπεριλαμβανομένης και της προηγούμενης διαβούλευσης του άρθρου 36.

Ο ΥΠΔ, σε περίπτωση πλημμελούς εκτέλεσης των υποχρεώσεών, ευθύνεται έναντι του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία, αλλά όχι έναντι του υποκειμένου των δεδομένων ή της αρμόδιας αρχής. Αν και εν πρώτοις θεωρείται ότι έχει έναν μάλλον επιφανειακό ρόλο λόγω των αρμοδιοτήτων του αλλά και του μη υποχρεωτικού ορισμού του στους ιδιωτικούς φορείς, στην πραγματικότητα είναι πολύ σημαντικός. Μάλιστα στις περιπτώσεις που κάποιος ιδιωτικός φορέας ορίζει ΥΠΔ αν και δεν υποχρεούται προς τούτο, αποκτά ένα ανταγωνιστικό πλεονέκτημα έναντι των υπολοίπων, καθώς ο οικειοθελής (και όχι αναγκαστικός) διορισμός του συνιστά συνετή κι υπεύθυνη τακτική αλλά και ένδειξη λήψης μέτρων συμμόρφωσης.

3.14. Διοικητικά Πρόστιμα

Τα διοικητικά πρόστιμα αποτελούν κεντρικό στοιχείο του νέου καθεστώτος επιβολής που έχει θεσπιστεί με τον ΓΚΠΔ, και ένα ισχυρό εργαλείο στα χέρια των εποπτικών αρχών, μαζί με τα υπόλοιπα μέτρα του άρθρου 58, για την εφαρμογή των διατάξεών του. Ο κανονισμός θέτει δύο ανώτατα όρια προστίμων σε περίπτωση που δεν τηρούνται οι κανόνες του. Τα διοικητικά πρόστιμα που προβλέπει είναι :

Α) έως 10.000.000 ευρώ ή σε περίπτωση επιχειρήσεων έως το 2% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους ανάλογα με το ποιο από τα δύο κριτήρια οδηγεί σε υψηλότερο πρόστιμο η παραβίαση των υποχρεώσεων:

α) του υπευθύνου επεξεργασίας και του εκτελούντος την επεξεργασία [133]

β) του φορέα πιστοποίησης των επιχειρήσεων

γ) του φορέα παρακολούθησης

Β. έως 20.000.000 ή σε περίπτωση επιχειρήσεων έως το 4% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους ανάλογα με το ποιο από τα δύο κριτήρια οδηγεί σε υψηλότερο πρόστιμο η παραβίαση

α) των βασικών αρχών για την επεξεργασία

β) των δικαιωμάτων των υποκειμένων των δεδομένων[134]

γ) διατάξεων για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε αποδέκτη σε τρίτη χώρα ή σε διεθνή οργανισμό

δ) οποιωνδήποτε άλλων υποχρεώσεων προκύπτουν από δίκαιο του κράτους μέλους

ε) η μη συμμόρφωση προς εντολή ή προς προσωρινό ή οριστικό περιορισμό της επεξεργασίας ή προς αναστολή της κυκλοφορίας δεδομένων που επιβάλλει η εποπτική αρχή κατ' άρθρο 58 παρ.2 ή μη παροχή πρόσβασης κατά παράβαση του άρθρου 58 παρ. 1 του ΓΚΠΔ.

Εντός του ως άνω πλαισίου η WP 29 δημοσίευσε, στις κατευθυντήριες γραμμές για τις εποπτικές αρχές όσον αφορά την εφαρμογή των μέτρων που αναφέρονται στο άρθρο 58 παράγραφοι 1, 2 και 3 και τον καθορισμό διοικητικών προστίμων δυνάμει του άρθρου 83, οι οποίες μάλιστα είναι ενδεικτικές[135]. Σκοπός τους είναι η δημιουργία ενός κοινού πλαισίου κατανόησης και ερμηνείας των διατάξεων του άρθρου 83 ΓΚΠΔ από τις εποπτικές αρχές, καθώς και η αλληλεπίδρασή του με τα άρθρα 58 και 70. Έτσι το ΕΣΠΔ και οι εθνικές εποπτικές αρχές συμφωνούν να χρησιμοποιήσουν τις κατευθυντήριες γραμμές ως κοινό έδαφος για μία ενιαία προσέγγιση.

[133] Για π.χ. όταν δεν προβαίνουν σε διενέργεια DPIA.

[134] Η CNIL (Commission Nationale de l'Informatique et des Libertés) επέβαλε στην Google LLC 60.000.000 ευρώ και στη θυγατρική της Google Ireland Limited 40.000.000 ευρώ για τρεις παραβιάσεις του άρθρου 82 ΓΚΠΔ ήτοι για α) εγκατάσταση cookies χωρίς προηγούμενη συγκατάθεση χρηστών, β) πλημμελή ενημέρωση των χρηστών, γ) πλημμελή ικανοποίηση του δικαιώματος των χρηστών. Για τον υπολογισμό του διοικητικού προστίμου που επέβαλε η CNIL στη Google και τη θυγατρική της έλαβε υπόψη της το μεγάλο αριθμό χρηστών που επισκεπτόταν την ιστοσελίδα τους και τα τεράστια οικονομικά οφέλη που έχουν προσκομίσει από τις πρακτικές αυτές

[135] Βλ. σχετικά Ομάδα εργασίας του άρθρου 29 για την προστασία των Δεδομένων, 17 EL, WP 253, Κατευθυντήριες γραμμές για την εφαρμογή και τον καθορισμό διοικητικών προστίμων για τους σκοπούς του κανονισμού 2016/679 που εκδόθηκαν στις 3 Οκτωβρίου 2017.

Η χώρα μας με τη διάταξη του άρθρου 39 Ν. 4624/2019 προβλέπει ότι σε περίπτωση παραβίασης του ΓΚΠΔ εκ μέρους φορέων του δημοσίου τομέα μπορεί να επιβληθεί από την ΑΠΔΠΧ διοικητικό πρόστιμο έως 10.000.000 ευρώ, κατόπιν διοικητικής πράξης επιβολής προστίμου της ΑΠΔΠΧ, ανάλογα με τη βαρύτητα και τη διάρκεια της παραβίασης της προκαλούμενης ζημιάς (άρθρο 39 παρ.1), το οποίο θα εισπραχθεί από αυτήν κατά τις διατάξεις του ΚΕΔΕ. Η παρ. 2 αναφέρεται στα κριτήρια (φύση, βαρύτητα, διάρκεια παράβασης, επαναληπτικότητά της, κατηγορίες προσωπικών δεδομένων κ.λ.π.) που λαμβάνονται υπόψη για την επιβολή των ως άνω κυρώσεων.

Αντίθετα η διάταξη του άρθρου 39 εξαιρεί σιωπηρά τους ιδιωτικούς φορείς από το πεδίο εφαρμογής του, για τους οποίους όπως συνάγεται εξ αντιδιαστολής, διατηρείται άθικτο το πλαίσιο των προαναφερόμενων προστίμων του ΓΚΠΔ εις βάρος τους, τα οποία δύνανται να ανέλθουν μέχρι και σε ποσοστό 2% ή 4% επί του ετησίου τζίρου μιας επιχείρησης (Αιτιολογική Έκθεση ΣχΝ., σελ. 30).

3.15. Ποινικές Κυρώσεις

Το άρθρο 84 παρ. 1 ΓΚΠΔ[136] αναθέτει στα κράτη μέλη να θεσπίζουν κανόνες που εμπεριέχουν κυρώσεις σε περίπτωση παραβίασης των διατάξεών του, πλην των διοικητικών που θεσμοθετεί στο άρθρο 83 καθώς και να λαμβάνουν τα κατάλληλα μέτρα για να διασφαλίσουν την εφαρμογή τους, συστήνοντας μάλιστα στα κράτη μέλη οι προβλεπόμενες κυρώσεις να είναι ανάλογες, αποτελεσματικές και αποτρεπτικές, αρκεί η επιβολή τους να μην προσκρούει στην αρχή ne bis in idem, βάσει της ερμηνείας του ΔΕΕ. Σε συμμόρφωση προς τη διάταξη αυτή ο Ν. 4624/2019 θεσπίζει στο άρθρο 38 παρ. 1 τις αντίστοιχες ποινικές κυρώσεις[137].

Στην παρ. 2 θέτει την υποχρέωση στα κράτη μέλη να κοινοποιούν τις εθνικές διατάξεις τους που εμπεριέχουν τους ως άνω κανόνες, στην Επιτροπή έως τις 25.05.2018 και αμελλητί σε περίπτωση τυχόν τροποποίησής τους.

[136] Βλ. άρθρο 84 ΓΚΠΔ ΕΕ L 119/834.5.2019.

[137] Αυτές είναι: α)ποινή φυλάκισης έως ένα έτους σε περίπτωση που οποιοσδήποτε επεμβαίνει με οποιονδήποτε τρόπο σε σύστημα αρχειοθέτησης προσωπικών δεδομένων, το διαγράφει, αντιγράφει και εν γένει χρησιμοποιεί παράνομα, β) ποινή φυλάκισης τουλάχιστον ενός έτους και χρηματικής ποινής 100.000 ευρώ αν πρόκειται για ειδικές κατηγορίες δεδομένων, γ) κάθειρξη έως 10 χρόνια, εάν με τις ως άνω περιγραφόμενες αξιόποινες πράξεις ο υπαίτιος σκοπεύει να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος ή να προκαλέσει περιουσιακή ζημία και το συνολικό όφελος ή η ζημία υπερβαίνει τις 120.000 ευρώ, δ) με κάθειρξη και χρηματική ποινή έως 300.000 ευρώ αν από τις αξιόποινες πράξεις συντρέχει κίνδυνος για την ελεύθερη λειτουργία του δημοκρατικού πολιτεύματος ή την εθνική ασφάλεια. Τα ως άνω αδικήματα διώκονται αυτεπαγγέλτως.

Εν κατακλείδι, ο ΓΚΠΔ αποδεικνύεται ότι εξασφαλίζει ένα αυξημένο πλαίσιο προστασίας για τα υποκείμενα των προσωπικών δεδομένων. Εκτός από τις αρχές επεξεργασίας, καθιερώνει τα βασικά δικαιώματα που μπορούν να απολαμβάνουν υπό το νέο καθεστώς τα υποκείμενα των δεδομένων, ενώ αναγνωρίζει τον υπεύθυνο επεξεργασίας ως αρμόδιο όργανο εξασφάλισης του σύννομου αυτής, καθιστώντας τον ταυτόχρονα υπόλογο να αποδεικνύει την ορθή εφαρμογή και συμμόρφωση του προς τις επιταγές του κανονισμού. Για να τον διευκολύνει μάλιστα ο ΓΚΠΔ του παραχωρεί απλόχερα άφθονα μέσα και εργαλεία, όπως την εκτίμηση αντικτύπου, την τήρηση αρχείου δραστηριοτήτων αλλά και την ευχέρεια λήψης τεχνικών και οργανωτικών μέσων όπως είναι η ψευδωνυμοποίηση, κρυπτογράφηση κ.λ.π. σε συμμόρφωση με την τήρηση της αρχής της ασφάλειας, ενώ προκρίνει την «προστασία από τον σχεδιασμό και εξ ορισμού» ως την κατάλληλη προληπτική εκείνη διαδικασία που πρέπει να ακολουθεί κάθε φορέας ή επιχείρηση πριν καν επεξεργαστεί προσωπικά δεδομένα. Περαιτέρω η υποχρεωτική γνωστοποίηση σε περίπτωση παραβίασης προς την αρμόδια αρχή και προς το ίδιο το υποκείμενο, όταν απειλείται σοβαρός κίνδυνος γι’ αυτό, σε συνδυασμό με τα ιδιαίτερα υψηλά πρόστιμα που προβλέπει ο ΓΚΠΔ, κατατείνει στο συμπέρασμα ότι πρόκειται για ένα αυστηρό νομοθέτημα, το οποίο ωστόσο διακατέχεται από μια ευελιξία στο μέτρο που επιτρέπει στις εθνικές νομοθεσίες να αποφαίνονται για επιμέρους ζητήματα -είτε χρησιμοποιώντας «ρήτρες ανοίγματος» είτε επιτρέποντας ευθέως στον εθνικό νομοθέτη να δρα αυτοβούλως όπως για τις ποινικές κυρώσεις επί παραβίασης.

ΚΕΦΑΛΑΙΟ 4ο: Η ΕΦΑΡΜΟΓΗ ΤΟΥ ΓΚΠΔ ΣΤΑ ΕΛΛΗΝΙΚΑ ΠΑΝΕΠΙΣΤΗΜΙΑ

4.1.Η Διάρθρωση της Ανώτατης Εκπαίδευσης στην Ελλάδα– Νομική Μορφή ΑΕΙ

Τα εκπαιδευτικά, άλλως ακαδημαϊκά, ιδρύματα συνιστούν το χώρο όπου κατεξοχήν κατοχυρώνεται η ακαδημαϊκή ελευθερία στη μάθηση, την έρευνα και τη διδασκαλία, η ελευθερία έκφρασης, η ανάπτυξη κριτικής ικανότητας, η διακίνηση ιδεών, η διάχυση της γνώσης με την έρευνα και τη διδασκαλία και της ανάπτυξης των τεχνών, η αξιοποίηση των ερευνητικών αποτελεσμάτων και η προώθηση της καινοτομίας και η εν γένει διαμόρφωση ελεύθερων και υπεύθυνων πολιτών.

Στην Ελλάδα υπάρχουν δυο κατηγορίες εκπαίδευσης, η δημόσια και η ιδιωτική, ενώ ανάλογα με τη βαθμίδα διακρίνεται σε πρωτοβάθμια, δευτεροβάθμια και τριτοβάθμια. Η τριτοβάθμια εκπαίδευση αποτελείται από δύο παράλληλους τομείς:

Α) τον πανεπιστημιακό τομέα που περιλαμβάνει τα Πανεπιστήμια, τα Πολυτεχνεία, και την Ανώτατη Σχολή Καλών Τεχνών, τα οποία αποκαλούνται Πανεπιστήμια και

Β) τον τεχνολογικό τομέα που περιλαμβάνει τα Τεχνολογικά Εκπαιδευτικά Ιδρύματα (Τ.Ε.Ι.) και την Ανώτατη Σχολή Παιδαγωγικής και Τεχνολογικής Εκπαίδευσης (Α.Σ.ΠΑΙ.ΤΕ.), τα οποία αποκαλούνται ΤΕΙ.

Όλα τα ανώτατα εκπαιδευτικά ιδρύματα τριτοβάθμιας εκπαίδευσης στην Ελλάδα είναι δημόσια. Τα πανεπιστήμια της χώρας μας είναι τα εξής:

1. Ανωτάτη Σχολή Καλών Τεχνών (Α.Σ.Κ.Τ.)
2. Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης (Α.Π.Θ.)
3. Διεθνές Πανεπιστήμιο Ελλάδος (International Hellenic University, IHU)
4. Εθνικό Μετσόβιο Πολυτεχνείο (Ε.Μ.Π.)
5. Ελληνικό Μεσογειακό Πανεπιστήμιο (ΕΛ.ΜΕ.ΠΑ.) (πρώην Τ.Ε.Ι. Κρήτης)
6. Γεωπονικό Πανεπιστήμιο Αθηνών (Γ.Π.Α.)
7. Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών (Ε.Κ.Π.Α.)
8. Πανεπιστήμιο Δυτικής Αττικής (ΠΑ.Δ.Α.) (συνένωση του Α.Τ.Ε.Ι. Αθήνας και του Α.Ε.Ι. Πειραιά Τ.Τ.)
9. Πανεπιστήμιο Πατρών
10. Πανεπιστήμιο Κρήτης
11. Πολυτεχνείο Κρήτης

12. Πανεπιστήμιο Ιωαννίνων
13. Δημοκρίτειο Πανεπιστήμιο Θράκης (Δ.Π.Θ.)
14. Πανεπιστήμιο Θεσσαλίας
15. Οικονομικό Πανεπιστήμιο Αθηνών (Ο.Π.Α.)
16. Πάντειο Πανεπιστήμιο Κοινωνικών και Πολιτικών Επιστημών
17. Πανεπιστήμιο Πειραιώς (ΠΑ.ΠΕΙ.)
18. Πανεπιστήμιο Μακεδονίας (ΠΑ.ΜΑΚ.)
19. Πανεπιστήμιο Δυτικής Μακεδονίας
20. Πανεπιστήμιο Πελοποννήσου (ΠΑ.ΠΕΛ.)
21. Πανεπιστήμιο Αιγαίου
22. Ιόνιο Πανεπιστήμιο
23. Χαροκόπειο Πανεπιστήμιο
24. Ελληνικό Ανοικτό Πανεπιστήμιο (Ε.Α.Π.)
25. Ανώτατες Σχολές Τουριστικής Εκπαίδευσης Ρόδου και Κρήτης (ΑΣΤΕ)
26. Ανώτατη Σχολή Παιδαγωγικής και Τεχνολογικής Εκπαίδευσης (Α.Σ.ΠΑΙ.Τ.Ε.) [138].
27. Στρατιωτική Σχολή Αξιωματικών Σωμάτων (ΣΣΑΣ)
28. Στρατιωτική Σχολή Ευελπίδων (ΣΣΕ)

Το ισχύον θεσμικό πλαίσιο για την οργάνωση, λειτουργία και διοίκηση των Α.Ε.Ι. ρυθμίζεται σήμερα από δύο νομοθετικά κείμενα, το Ν. 4009/2011 (ΦΕΚ Α 195/06-09-2011) και το Ν. 4485/2017 (ΦΕΚ 114/04-08-2017). Τα ιδρύματα των δύο αυτών τομέων ανώτατης εκπαίδευσης λειτουργούν παράλληλα με διακριτή φυσιογνωμία, σκοπό και αποστολή που διαφοροποιούνται κατά τις ισχύουσες για το καθένα από αυτά διατάξεις (Κωτσίκης, 2007). Κατά το άρθρο 1 του Ν. 4485/2017, τα Α.Ε.Ι. είναι νομικά πρόσωπα δημοσίου δικαίου πλήρως αυτοδιοικούμενα. Η εποπτεία του κράτους ασκείται από τον Υπουργό Παιδείας, Έρευνας και Θρησκευμάτων, σύμφωνα με τα οριζόμενα στο άρθρο 16 του Συντάγματος και τον οικείο νόμο.

Κατά το άρθρο 7 παρ. 1 του Ν.4485/2017 *«Με προεδρικό διάταγμα, που εκδίδεται με πρόταση των Υπουργών Παιδείας, Έρευνας και Θρησκευμάτων, Οικονομικής και Διοικητικής Ανασυγκρότησης, εγκρίνεται ο Οργανισμός κάθε ΑΕΙ, ύστερα από πρόταση της*

[138] https://el.wikipedia.org/wiki/%CE%91%CE%BD%CF%8E%CF%84%CE%B1%CF%84%CE%B1_%CE%B5%CE%BA%CF%80%CE%B1%CE%B9%CE%B4%CE%B5%CF%85%CF%84%CE%B9%CE%BA%CE%AC_%CE%B9%CE%B4%CF%81%CF%8D%CE%BC%CE%B1%CF%84%CE%B1_%CF%83%CF%84%CE%B7%CE%BD_%CE%95%CE%BB%CE%BB%CE%AC%CE%B4%CE%B1

Συγκλήτου» ενώ η παρ. 2 προβλέπει ότι με τον Οργανισμό καθορίζονται τα θέματα της οργανωτικής δομής και λειτουργίας του ιδρύματος.

4.1.1. Το προσωπικό των ΑΕΙ

Το προσωπικό των ΑΕΙ, διακρίνεται βάσει του αντικειμένου ενασχόλησής τους διακρίνεται σε: α) καθηγητές που ασκούν το διδακτικό[139] και ερευνητικό έργο στα Α.Ε.Ι. και σε β) λοιπό προσωπικό.

α. Διδακτικό και εργαστηριακό προσωπικό

Εδώ εμπίπτουν τα μέλη της κατηγορίας του: i. Ειδικού Εκπαιδευτικού Προσωπικού (Ε.Ε.Π.) που επιτελούν ειδικό εκπαιδευτικό -διδακτικό έργο στα Α.Ε.Ι. (άρθρο 29 παρ.1^{α}), ii. Εργαστηριακού Διδακτικού Προσωπικού (Ε.ΔΙ.Π.) επιτελούν εργαστηριακό – εφαρμοσμένο διδακτικό έργο στα Α.Ε.Ι. (άρθρο 29 παρ.2^{α}), iii. Τα μέλη της κατηγορίας του Ειδικού Τεχνικού Εργαστηριακού Προσωπικού (Ε.Τ.Ε.Π.) παρέχουν έργο υποδομής στην εν γένει λειτουργία των Α.Ε.Ι., προσφέροντας εξειδικευμένες τεχνικές εργαστηριακές υπηρεσίες (άρθρο 29 παρ.3^{α})

β. Η Γραμματεία και το Διοικητικό Προσωπικό

Ο Προϊστάμενος του διοικητικού προσωπικού είναι ο γραμματέας του ιδρύματος, ο οποίος είναι πρόσωπο εγνωσμένου κύρους, πτυχιούχος Α.Ε.Ι., με πολύ καλή γνώση τουλάχιστον μίας ξένης γλώσσας και αυξημένη διοικητική εμπειρία (άρθρο 28 παρ.1) Τα μέλη του διοικητικού προσωπικού ασκούν τη διοικητική και γραμματειακή υποστήριξη όλων των υπηρεσιών του ιδρύματος, όπως αυτές καθορίζονται στον Οργανισμό του ιδρύματος (άρθρο 28 παρ.5).

4.1.2. Οι Φοιτητές

Είναι τα φυσικά πρόσωπα που κατά το άρθρο 49 αποκτούν την ιδιότητα του φοιτητή με την εγγραφή του σε Α.Ε.Ι. η οποία διατηρείται μέχρι την απονομή του τίτλου του αντίστοιχου κύκλου σπουδών. Διακρίνονται σε προπτυχιακούς, μεταπτυχιακούς, διδακτορικούς και μεταδιδακτορικούς (άρθρο 2 Ν. 4485/2017).

[139] Ως διδακτικό έργο νοείται αυτό που ορίζεται στο άρθρο 31, ενώ το ερευνητικό έργο περιλαμβάνει ιδίως τη βασική ή εφαρμοσμένη έρευνα, την καθοδήγηση διπλωματικών εργασιών, μεταπτυχιακών διπλωμάτων και διδακτορικών διατριβών και συμμετοχή σε συνέδρια και ερευνητικά σεμινάρια.

Η επιλογή στελέχωσης του ακαδημαϊκού και διοικητικού προσωπικού, γίνεται από το εκάστοτε Α.Ε.Ι. ενώ η επιλογή των φοιτητών γίνεται σύμφωνα με τις διατυπώσεις του νόμου περί εισαγωγής τους κατόπιν διενέργειας εξετάσεων (πανελληνίων) επί τη βάσει βαθμολογίας που αποτελεί και το αξιολογικό κριτήριο για την εισαγωγή τους.

4.1.3. Χρηματοδότηση Α.Ε.Ι.

Η χρηματοδότηση για τη λειτουργία των Α.Ε.Ι. γίνεται από το κράτος για την εκπλήρωση της αποστολής τους στο πλαίσιο των συμφωνιών προγραμματικού σχεδιασμού και των κανόνων κατανομής της δημόσιας χρηματοδότησης. Η διαχείριση των οικονομικών πόρων γίνεται με ευθύνη των Α.Ε.Ι.[140] ενώ δεν αποκλείεται η σύσταση σε κάθε Α.Ε.Ι. ειδικού Ν.Π.Ι.Δ. με τη μορφή ανώνυμης εταιρείας, για την αξιοποίηση και διαχείριση των πόρων του (άρθρο 58ν.4009/2011).

4.2. Τα Προσωπικά Δεδομένα στα Πανεπιστήμια

Η έκρηξη της τεχνολογίας οδήγησε στην αύξηση του αριθμού των δεδομένων και στη δημιουργία τεχνολογικών όρων όπως «Cloud Computing»[141], «Big Data»[142] ή «Internet of Things»[143], που τυγχάνουν εφαρμογής τόσο σε επιχειρήσεις όσο και σε δημόσιους φορείς, όπως είναι τα Πανεπιστήμια. Σ' αυτά καθημερινά διακινείται τεράστιος όγκος προσωπικών δεδομένων όλων των μελών της ακαδημαϊκής κοινότητας όπως μελών ΔΕΠ, διοικητικού προσωπικού μόνιμου και αορίστου χρόνου, επιστημονικών συνεργατών, διδασκόντων, αποφοίτων, μετεχόντων σε εκπαιδευτικά προγράμματα πρακτικής άσκησης φοιτητών, αλλοδαπών φοιτητών, υπότροφων, υποψήφιων διδακτόρων, προμηθευτών, επιχειρήσεων, ιδιωτών ως λήπτες υπηρεσιών που παρέχουν τα πανεπιστήμια, εξωτερικών συνεργατών/συμβαλλομένων μέρων (π.χ. εκμισθωτές ακινήτων, δωρητές κ.α.), μετεχόντων σε εκδηλώσεις υπό την αιγίδα των πανεπιστημίων, εργολάβων και προστηθέντων τους, τρίτων που έχουν πρόσβαση στα ηλεκτρονικά συστήματα των πανεπιστήμιων.

[140] Άρθρο 57 Ν.4009/2011.

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

[142] Μεγάλα Δεδομένα: τεράστιος όγκος δεδομένων που είναι σχεδόν αδύνατον να επεξεργαστεί με τις παραδοσιακές μεθόδους

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

4.2.1. Τα προσωπικά δεδομένα των εργαζομένων στα Πανεπιστήμια

Το ζήτημα της προστασίας των προσωπικών δεδομένων σχετίζεται με το σύνολο του προσωπικού που απασχολείται σε ένα Α.Ε.Ι. Το διοικητικό προσωπικό των πανεπιστημίων, εφαρμόζει καθημερινά περίπλοκες και χρονοβόρες διαδικασίες που σχετίζονται με τη διακίνηση, επεξεργασία, διαχείριση και αποθήκευση τεράστιου όγκου εγγράφων/εντύπων/αρχείων που εμπεριέχουν προσωπικά δεδομένα φυσικών προσώπων που τηρούνται είτε σε ηλεκτρονικές βάσεις δεδομένων είτε σε φυσικά αρχεία, προς εξυπηρέτηση των συναλλαγών με εργαζόμενους, φοιτητές και προμηθευτές. Περαιτέρω το προσωπικό του Πανεπιστημίου επεξεργάζεται καθημερινά προσωπικά δεδομένα που αντλεί από την ηλεκτρονική της ιστοσελίδα, όπου παρατίθενται πληροφορίες για το εν λόγω ίδρυμα, την Διοίκηση, την Έρευνα, μέσω της οποίας οι ενδιαφερόμενοι μπορεί να υποβάλουν αίτημα ή να εκδηλώσουν ενδιαφέρον. Τα δεδομένα αυτά μπορεί να αφορούν: α) διαδικασίες εκλογής ή μονιμοποίησης μελών ΔΕΠ, αξιολόγησης, συγγραφής δημοσιεύσεων, έργου, μονογραφιών κλπ.[144] β) διαδικασίες σχετικά με προκηρύξεις για πλήρωση θέσης διοικητικού προσωπικού, που απασχολείται σε διάφορες υπηρεσίες του πανεπιστημίου (διοικητικές, οικονομικές, τεχνικές) και είναι επιφορτισμένα με την οικονομική διαχείριση (κατάρτιση προϋπολογισμού, μισθοδοσίες, διαγωνισμούς κ.λ.π.), την διοίκηση προσωπικού (διακίνηση εγγράφων, υπηρεσιακή κατάσταση εργαζομένων κ.λ.π.), τις τεχνικές υπηρεσίες (εκπόνηση, επίβλεψη, συντήρηση μελετών και έργων) και με τη μηχανοργάνωση (συντήρηση υλικού και λογισμικού εξοπλισμού του ιδρύματος), τη διαχείριση ακαδημαϊκών ζητημάτων που αφορούν τους φοιτητές (εγγραφή, σίτιση, στέγαση, υποτροφίες, ιατροφαρμακευτική και νοσοκομειακή περίθαλψη)[145].

Μετά την πρόσληψή τους τα μέλη του προσωπικού των πανεπιστημίων αποκτούν έναν αριθμό μητρώου-κλειδί, ο οποίος δεν μεταβάλλεται ούτε παραποιείται. Τα δεδομένα του προσωπικού των πανεπιστημίων και τα στοιχεία ταυτοποίησής τους (ΔΑΤ, ΑΦΜ, ΑΜΚΑ, οικογενειακή κατάσταση, ονοματεπώνυμο, διεύθυνση μόνιμης κατοικίας, ηλεκτρονική διεύθυνση, ημερομηνίες γέννησης, πρόσληψης, αδειών, δεδομένα οικονομικά ή και περιουσιακής κατάστασης, όπως τραπεζικοί λογαριασμοί, IBAN, δάνεια, κατασχέσεις εις

[144] Το πληροφοριακό σύστημα που υποστηρίζει τις διαδικασίες εκλογής ονομάζεται ΑΠΕΛΛΑ https://apella.minedu.gov.gr/.

[145] Βλ. σχετικά όπως ανωτέρω σε: https://pulse.microsoft.com/uploads/prod/2018/03/WorkProductivity_GDPRforEducation_KickStartGuide.pdf

χείρας του πανεπιστημίου ως τρίτου κ.λ.π.), δεδομένα σχετικά με το προσοντολόγιο του διοικητικού, ακαδημαϊκού, ερευνητικού προσωπικού, καταχωρούνται στο σύστημα του ιδρύματος. Όταν παύσει η εργασιακή σχέση μεταξύ του ατόμου και του οργανισμού ο φάκελός του απενεργοποιείται, οι χρήστες δεν έχουν πλέον εικόνα αυτού, ειμή μόνο με τη χρήση ειδικού κωδικού, ωστόσο τα δεδομένα του παραμένουν αποθηκευμένα στο σύστημα και συνήθως δεν διαγράφονται ποτέ.

Τόσο ο προϊσχύον Ν. 2472/1997[146] όσο και ο πρόσφατος Ν. 4624/2019[147] εμπεριέχουν διατάξεις προστατευτικές για τα προσωπικά δεδομένα των εργαζομένων, τονίζοντας ότι και αυτοί απολαμβάνουν της προστασίας των αναγνωρισμένων δικαιωμάτων βάσει ΓΚΠΔ. Η σύγχρονη «ψηφιακή επιτήρηση» δεν θεωρείται σύννομη κατά τον ΓΚΠΔ όταν είναι διαρκής και δεν εμπεριέχει τη συγκατάθεση του εργαζομένου-υποκειμένου των δεδομένων. Αντίθετα το άρθρο 27 παρ.1 Ν. 4624/2019 θέτει μια κανονιστική ρύθμιση, προβλέποντας ότι ο εργοδότης μπορεί να επεξεργάζεται προσωπικά δεδομένα των εργαζομένων *χωρίς τη συγκατάθεση τους* μόνο εφόσον είναι αναγκαίο για την σύναψη, την κατάρτιση και την εκτέλεση της σύμβασης εργασίας, έτσι ώστε να εξασφαλίζεται μια στάθμιση των συμφερόντων του εργοδότη και του δικαιώματος προσωπικότητας του εργαζομένου και αυτά τα δύο να τελούν σε μια «ήπια ισορροπία» (Αιτιολογική Έκθεση ΣχΝ, σελ. 17)[148].

Η παρ. 2 του άρθρου 27 Ν. 4624/2019 καθιερώνει ως κατ' εξαίρεση νομική βάση την συγκατάθεση του εργαζομένου, η οποία θα πρέπει να *κριθεί εάν είναι προϊόν ελεύθερης επιλογής συνεκτιμώντας το βαθμό εξάρτησης του εργαζομένου από την υφιστάμενη σύμβαση εργασίας καθώς και τις περιστάσεις κάτω από τις οποίες δόθηκε η συγκατάθεσή του*[149].

[146] άρθρα 11-14 Ν. 2472/1997

[147] Άρθρα 33-35 Ν. 4624/2019

[148] Η λάθρα παρακολούθηση εκ μέρους του εργοδότη της χρήσης ή των περιηγήσεων που κάνει ο εργαζόμενος στο διαδίκτυο εν ώρα εργασίας, τελεί εκτός του άρθρου 27 παρ.1. Γι αυτήν υπάρχει μηχανισμός ελέγχου του εργοδότη επί τη βάσει του άρθρου 8 ΕΣΔΑ. Αντίθετα στο πεδίο εφαρμογής της εν λόγω διάταξης εμπίπτουν τα συστήματα whistleblowing.

[149] Βλ. σχετικά και Απόφαση 77/2016 ΑΠΔΠΧ η οποία, παραπέμπει για τη συγκατάθεση ως ισχυρή νομιμοποιητική βάση, στην Οδηγία της με αριθμό 115/2001, που αναφέρει μεταξύ άλλων, ότι «*στην περίπτωση των σχέσεων απασχόλησης, η εγγενής ανισότητα των μερών και η κατά κανόνα σχέση εξάρτησης των εργαζομένων θέτει εν αμφιβόλω την ελευθερία της συγκατάθεσης των εργαζομένων, στοιχείο απαραίτητο για την εγκυρότητα της επεξεργασίας, όπως προκύπτει από τους γενικούς κανόνες του δικαίου αλλά και συγκεκριμένα από το συνδυασμό των άρθρων 2 ια, 5 παρ. 1 και 7 παρ. 2α του Νόμου για την προστασία προσωπικών δεδομένων».* Κατά συνέπεια το στοιχείο της εξάρτησης, που διέπει συνήθως τις σχέσεις εργοδότη-εργαζόμενου αποδυναμώνει τη βαρύτητα της ελεύθερης συγκατάθεσης και ως εκ τούτου η συγκατάθεση αυτή δεν θα μπορούσε να αποτελέσει νομιμοποιητική βάση επεξεργασίας

Στην παρ. 3 το άρθρο 27 Ν. 4624/2019 προβλέπει τη δυνατότητα επεξεργασίας «ευαίσθητων» ή «ειδικών κατηγοριών» προσωπικών δεδομένων των εργαζομένων, εκ μέρους του Πανεπιστημίου, εάν η επεξεργασία αυτή υπαγορεύεται για λόγους άσκησης των δικαιωμάτων ή των νομίμων υποχρεώσεων που προέρχονται από το εργατικό δίκαιο, το δίκαιο της κοινωνικής ασφάλισης και της κοινωνικής προστασίας και αν κρίνεται αναμφίβολα ότι το έννομο συμφέρον των εργαζομένων, δεν υπερτερεί έναντι της επεξεργασίας αυτής. Η εν λόγω διάταξη εισάγει παρέκκλιση από τον γενικό κανόνα του άρθρου 9 παρ.1 ΓΚΠΔ και τελεί υπό τον όρο λήψης των κατάλληλων μέτρων προστασίας των εργαζομένων.

Επίσης η διάταξη του άρθρου 27 παρ. 7 Ν. 4624/2019 αναφέρεται στην επεξεργασία των δεδομένων των εργαζομένων που συλλέγονται μέσω κλειστού κυκλώματος οπτικής καταγραφής εντός του εργασιακού χώρου, είτε είναι δημοσίως προσβάσιμος είτε όχι, επιτρέποντάς την όταν κρίνεται αναγκαία για την προστασία προσώπων και αγαθών και υπό την προϋπόθεση ότι δεν θα χρησιμοποιούνται ως κριτήριο αξιολόγησης της εργασιακής αποδοτικότητας και ότι οι εργαζόμενοι θα ενημερώνονται εγγράφως ή με ηλεκτρονικά μέσα για την εγκατάσταση και λειτουργία του κυκλώματος καταγραφής.

4.2.2. Τα προσωπικά δεδομένα των φοιτητών

Η άλλη ομάδα εμπλεκομένων εντός της ακαδημαϊκής κοινότητας που παρέχει προσωπικά δεδομένα στα Πανεπιστήμια είναι οι φοιτητές. Η συλλογή των δεδομένων τους γίνεται κατά την διαδικασία υποβολής αιτήσεων ή δήλωσης εγγραφής τους, κατά την υπογραφή σύμβασης ή κατά τη σύναψη άλλης έννομης σχέσης. Επίσης συλλογή δεδομένων μπορεί να προκύψει από τη χρήση του ιστοτόπου, των ηλεκτρονικών πλατφορμών ή άλλων ηλεκτρονικών προγραμμάτων και μέσω επικοινωνίας, μέσω αλληλογραφίας, συμπλήρωσης ερευνών προς βελτίωση υπηρεσιών, συμμετοχής σε ερευνητικό πρόγραμμα ή σε εκδηλώσεις υπό την αιγίδα ενός πανεπιστημίου.

Ο συνηθέστερος τρόπος συλλογής δεδομένων είναι η ηλεκτρονική υποβολή αίτησης εγγραφής στα ΑΕΙ, κατά την οποία επισυνάπτονται τα απαραίτητα δικαιολογητικά του φοιτητή μέσω της ηλεκτρονικής εφαρμογής του Υπουργείου (https://eregister.it.minedu.gov.gr), με τη χρήση ενός κωδικού υποψηφίου που του

προσωπικών του δεδομένων *(βλ. σχετικά και Γνωμοδότηση 8/2001 της Ομάδας Εργασίας του άρθρου 29 για την επεξεργασία προσωπικών δεδομένων στο εργασιακό πλαίσιο).*

χορηγείται για τη συμμετοχή του στις εξετάσεις. Η μεταφορά των προσωπικών τους δεδομένων, όπως αποτυπώνονται στο μηχανογραφικό, γίνεται ηλεκτρονικά από το Υπουργείο προς το πανεπιστήμιο εγγραφής του επιτυχόντος και καταχωρούνται αυτομάτως στο σύστημα. Τέτοια δεδομένα είναι τα στοιχεία ταυτότητας, τα δημογραφικά στοιχεία, τα στοιχεία επικοινωνίας, ο βαθμός αποφοίτησής του, η βαθμολογική επίδοση φοιτητή [150], τα πτυχία, ο αριθμός δημοτολογίου, η διεύθυνση μόνιμης κατοικίας του, η ηλεκτρονική του διεύθυνση, οι παρουσίες του στα μαθήματα, τα έργα πνευματικής ιδιοκτησίας, τυχόν φωτογραφικό υλικό ή οπτικοακουστικό υλικό. Πολλές φορές μάλιστα τα Πανεπιστήμια ζητούν από τους φοιτητές την επικαιροποίηση των προσωπικών τους δεδομένων ή ακόμη και την αποκάλυψη «ευαίσθητων» προσωπικών δεδομένων που αφορούν και άλλα μέλη της οικογενείας τους, όπως π.χ. δεδομένα που αφορούν το οικογενειακό εισόδημα, την ανεργία, την οικογενειακή ή ακόμη και ιατρική κατάσταση τους ή των μελών της οικογενείας τους όπως π.χ. συμβαίνει επί αιτήσεως μετεγγραφής φοιτητή, προκειμένου να μεταβεί σε αντίστοιχη σχολή άλλου ιδρύματος για να διευκολύνει οικονομικά την οικογένειά του[151].

Μετά την εγγραφή ενός φοιτητή, του χορηγείται από τη γραμματεία του πανεπιστημίου ειδικός μοναδικός αριθμός και κωδικός–κλειδί για να αποκτά πρόσβαση στις ηλεκτρονικές υπηρεσίες του ιδρύματος, στη βιβλιοθήκη, στις παροχές σίτισης, στη (δωρεάν) χορήγηση συγγραμμάτων, στην υγειονομική περίθαλψη και στη μετακίνηση με πάσο-κάρτα στα μέσα μαζικής μεταφοράς. Ο κωδικός-κλειδί παραμένει ενεργός μέχρι την αποφοίτησή του από το Πανεπιστήμιο, οπότε και καταργείται αλλά τα στοιχεία του φοιτητή συνήθως παραμένουν καταχωρημένα στη βάση δεδομένων του ιδρύματος και δεν διαγράφονται ποτέ.

4.2.3. Τα προσωπικά δεδομένα των προμηθευτών

Πολλές φορές τα Πανεπιστήμια συνάπτουν συμβάσεις με εξωτερικούς συνεργάτες ή προμηθευτές στους οποίους ανατίθεται η διεκπεραίωση εργασιών ή η εκτέλεση έργων για

[150] Προσωπικά δεδομένα συνιστά και η βαθμολογία των μαθημάτων εξαμήνου, η οποία απαγορεύεται να αναρτηθεί δημοσίως στον ιστότοπο του πανεπιστημίου ή σε πίνακες ανακοινώσεων με το ονοματεπώνυμο του φοιτητή, ενώ αντίθετα προκρίνεται η λύση της ανάρτησης βάσει αριθμού μητρώου φοιτητή, βλ. σχετικά Vilela (2019), Challenges for the Implementation of the GDPR in Higher Education Institutions in Portugal, Proceedings of EDULEARN 19 Conference 1st-3rd July 2019, Palma, Mallorca, Spain, P. 1232

[151] Τα Πανεπιστήμια προβλέπουν το χρόνο τήρησης ευαίσθητων προσωπικών δεδομένων σύμφωνα με την εθνική νομοθεσία και τους σκοπούς επεξεργασίας και μεριμνούν για την ασφαλή καταστροφή τους όταν παρέλθει ο χρόνος τήρησης.

λογαριασμό τους. Κλασικό παράδειγμα είναι η σύναψη σύμβασης με εταιρίες ανάπτυξης και υποστήριξης λογισμικού κ.α. Στην περίπτωση αυτή οι συνεργάτες ή προμηθευτές έχουν την ιδιότητα του «Αποδέκτη» προσωπικών δεδομένων και ενίοτε του «υποκειμένου» δεδομένων, όταν τα προσωπικά τους δεδομένα συλλέγονται από την οικονομική υπηρεσία του πανεπιστημίου για φορολογικούς λόγους.

4.3. Η εφαρμογή του ΓΚΠΔ στα ελληνικά πανεπιστήμια

Από τη θέση του ΓΚΠΔ σε ισχύ, έγινε σαφές ότι κατέστη αναγκαία η γενικότερη αναβάθμιση των λειτουργικών δομών των επιχειρήσεων και των οργανισμών και τον εκσυγχρονισμό των πολιτικών τήρησης και διαχείρισης των δεδομένων προκειμένου να ενισχυθούν οι δεσμοί εμπιστοσύνης στις συναλλαγές με τους ιδιωτικούς και δημόσιους φορείς που ήδη από τις 25 Μαΐου 2018 θα έπρεπε θεωρητικά να είναι σε θέση να επιδείξουν τη δέουσα επιμέλεια, και υπευθυνότητα αποδεικνύοντας την ετοιμότητά τους για άμεση ανταπόκριση στις απαιτήσεις του νέου πλαισίου[152].Σύμφωνα με τον ΓΚΠΔ αυτό το βάρος ευθύνης και απόδειξης συμμόρφωσης μετακυλύεται πλέον στον Υπεύθυνο επεξεργασίας του εκάστοτε φορέα.

Στα πλαίσια του ως άνω εκσυγχρονισμού εισήλθαν και στα πανεπιστήμια οι τεχνολογίες της πληροφορικής και των υπολογιστών, όπως επίσης και νέες διοικητικές πρακτικές, δημιουργώντας την Ηλεκτρονική Διακυβέρνηση (e-government), βάσει της οποίας παρέχονται πλέον ηλεκτρονικά οι περισσότερες υπηρεσίες (Μυλώση, 2018). Ο ψηφιακός μετασχηματισμός επιτυγχάνεται μέσω της διαλειτουργικότητας των πληροφοριακών 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 υπηρεσιών.

Οι δημόσιοι φορείς στους οποίους εμπίπτουν και τα πανεπιστήμια 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 και στα πλαίσια της πληροφοριακής τους υποχρέωσης να σέβονται το δικαίωμα προστασίας των προσωπικών δεδομένων και της ιδιωτικότητας.

[152] Βλ. σχετικά ΣΕΒ 2018, διαθέσιμο σε :
https://www.sev.org.gr/Uploads/Documents/51628/meleti_sev_GDPR_final.pdf

Η Διοίκηση των πανεπιστημίων οφείλει να διερευνά τις επιπτώσεις που θα έχει η επεξεργασία των δεδομένων των εργαζομένων και φοιτητών, διασφαλίζοντας μάλιστα ότι αυτή θα πραγματοποιηθεί σε όσο το δυνατόν λιγότερα προσωπικά δεδομένα. Περαιτέρω καλείται να συνεργάζεται με την αρμόδια εποπτική αρχή. Μάλιστα στα πλαίσια της συνεργασίας αυτής το άρθρο 17 παρ. 4 ν. 4624/2019 προβλέπει ότι η ΑΠΔΠΧ μπορεί να συνάπτει μνημόνια συνεργασίας με ανώτατα εκπαιδευτικά ιδρύματα, με σκοπό την αμοιβαία ανταλλαγή πληροφοριών και την αμοιβαία συνδρομή για θέματα που εμπίπτουν στην αρμοδιότητά της, που περιλαμβάνει κυρίως την ενημέρωση και πραγματοποίηση ερευνών και μελετών, τη συνδρομή σε έρευνες και ελέγχους και τη διενέργεια αυτοψιών με βάση ερωτήματα που καταρτίζει η Αρχή.

Η αναζήτηση της συγκατάθεσης του ατόμου για την επεξεργασία των δεδομένων του και η εξασφάλιση του δικαιώματος ανάκλησης αυτής, αποτελούν επίσης σημαντικά βήματα προς τη θετική κατεύθυνση της συμμόρφωσης των πανεπιστημίων με τον Κανονισμό. Οι σύγχρονες απαιτήσεις υποδεικνύουν ότι πρέπει να επέλθει ένας συγκερασμός ανάμεσα στις νέες ανάγκες για παροχή υπηρεσιών και στην εξέλιξη των νέων τεχνολογιών και εφαρμογών.

Βέβαια οι μεταβολές που επέφερε ο ΓΚΠΔ σε νομικό επίπεδο στους δημόσιους φορείς, συμπεριλαμβανομένων και των πανεπιστημίων, δεν είναι τόσο έντονες καθόσον: α) η συγκατάθεση του υποκειμένου δεν καθίσταται τόσο σημαντική όσο στον ιδιωτικό τομέα και χρησιμοποιείται μόνον δευτερευόντως, β) το Δημόσιο επικαλείται και χρησιμοποιεί ως νομική και δικαιολογητική βάση επεξεργασίας την επιδίωξη του δημοσίου συμφέροντος και την άσκηση δημόσιας εξουσίας (άρθρο 6 παρ.1 ε') και γ) τα δικαιώματα του υποκειμένου στη λήθη και στη φορητότητα των δεδομένων τις περισσότερες φορές περιορίζονται ή σπανίως εφαρμόζονται.

Ο αντίκτυπος του ΓΚΠΔ στα πανεπιστήμια είναι ιδιαίτερα μεγάλος. Μέσω της εφαρμογής του τα ακαδημαϊκά ιδρύματα καθίστανται περισσότερο υπεύθυνα για τα δεδομένα που τηρούν. Ως εκ τούτου είναι σημαντικό να διαθέτουν οργανωμένα αρχεία (Μυλώση, 2018) και τεκμηρίωση που να εξηγεί για ποιο λόγο και με ποιόν τρόπο συλλέχθηκαν τα

δεδομένα, ποιος έχει πρόσβαση σ' αυτά, για πόσο χρονικό διάστημα θα διατηρηθούν ή εάν θα καταστούν ανώνυμα[153].

Στα πλαίσια της εφαρμογής του ΓΚΠΔ στα ελληνικά πανεπιστήμια σημειώνεται ότι:

Το Πανεπιστήμιο λειτουργεί ως Υπεύθυνος Επεξεργασίας ή εκτελών Επεξεργασία.

Το προσωπικό, οι φοιτητές και ενίοτε οι προμηθευτές συνιστούν υποκείμενα προσωπικών δεδομένων, ενώ συνήθως οι προμηθευτές ή το δημόσιο αποτελούν τους αποδέκτες

Οι πληροφορίες που παρέχονται συνιστούν δεδομένα προσωπικού χαρακτήρα απλά ή ευαίσθητα (όταν εμπεριέχουν πληροφορίες υγείας ή γενετικά, βιομετρικά κ.α. δεδομένα) και συνήθως συνιστούν δεδομένα μεγάλης κλίμακας.

Η επεξεργασία συνίσταται στη συλλογή και αποθήκευση κ.λ.π. των δεδομένων σε αρχεία

Η νομιμοποιητική βάση συνήθως είναι η ανάγκη συμμόρφωσης με νομική υποχρέωση ή η εκτέλεση καθήκοντος υπέρ του δημοσίου συμφέροντος ή κατά την άσκηση δημόσιας εξουσίας του Πανεπιστημίου και σπανιότερα, όπως προαναφέρθηκε, η συναίνεση του υποκειμένου**,** με το σκεπτικό ότι πολλές ταυτόχρονα νομικές βάσεις επεξεργασίας δε συνάδουν με τη φύση και την αποστολή τους, ενώ η απόκτηση και η διατήρηση της συγκατάθεσης επάγεται αλλαγές στις διαδικασίες, τα έγγραφα και τα συστήματα του ιδρύματος (Strecht, 2019).

Όταν νομιμοποιητική βάση επεξεργασίας είναι η συγκατάθεση[154], αυτή πρέπει να παρέχεται ελεύθερα, με σαφή, θετική ενέργεια, για κάθε σκοπό επεξεργασίας χωριστά και να είναι συγκεκριμένη, ρητή με πλήρη επίγνωση του υποκειμένου της (Sidlauskas & Limba, 2019), να παρέχεται με οποιοδήποτε πρόσφορο τρόπο, που να επιτρέπει την απόδειξη της εκδήλωσης της βούλησής του λαμβάνοντας υπόψιν την αρχή της αναλογικότητας, να μην τελεί υπό αιρέσεις ή περιορισμούς και να συνοδεύεται από κατάλληλη ενημέρωση για την επεξεργασία των προσωπικών δεδομένων του φυσικού προσώπου[155], να εφαρμόζεται στα αρχεία που εμπεριέχουν cookies, για τα οποία συνήθως οι περισσότεροι φορείς υιοθετούν ξεχωριστές πολιτικές. Οι εν λόγω συγκαταθέσεις των

[153] Βλ. σχετικά: How universities have to adapt under the new EU General Data Protection Regulation (GDPR) διαθέσιμο σε https://blog.fullfabric.com/how-universities-have-to-adapt-under-the-new-eu-general-data-protection-regulation-gdpr

[154] Βλ. σχετικά υποσημ. 63 σελ. 36 παρούσας μελέτης.

[155] Η σιωπή, τα προσυμπληρωμένα τετραγωνίδια ή η αδράνεια του φυσικού προσώπου δεν συνιστούν σύννομη συγκατάθεση.

υποκειμένων τηρούνται σε αρχεία των οποίων η ισχύς ή η ανάκλησή τους παρακολουθείται

Αρχείο είναι κάθε διαρθρωμένο σύνολο προσωπικών δεδομένων (συγκεντρωμένο ή αποκεντρωμένο ή κατανεμημένο σε λειτουργική ή γεωγραφική βάση, ηλεκτρονικό ή έντυπο) που είναι προσβάσιμα με γνώμονα συγκεκριμένα κριτήρια. Αρχεία είναι και τα *cookies* και τα *αρχεία καταγραφής διακομιστών*, στα οποία τα Πανεπιστήμια καταγράφουν αυτόματα τις πληροφορίες που συλλέγουν μέσω των ιστοτόπων τους, δίνοντας πληροφορίες για τον τύπο ή την έκδοση του προγράμματος το λειτουργικό σύστημα, την διεύθυνση URL, το όνομα του κεντρικού υπολογιστή, την διεύθυνση IP του χρήστη.

Η διαδικασία επεξεργασίας των ηλεκτρονικών εγγράφων πρέπει να γίνεται κατά τρόπο που να τηρεί και τους ανάλογους όρους ασφάλειας και να εγγυάται την ακεραιότητα, αυθεντικότητα και εμπιστευτικότητα των εγγράφων και των δεδομένων που εμπεριέχουν. Τα ηλεκτρονικά αρχεία των πανεπιστημίων πρέπει να τηρούνται κατά τέτοιο τρόπο, ώστε να εξασφαλίζεται η διατηρησιμότητα, η προσβασιμότητα και η αναγνωσιμότητα των εγγράφων που περιέχουν. Κάθε δημόσιος φορέας τηρεί σύστημα ηλεκτρονικού πρωτοκόλλου, βάσει του οποίου εκδίδεται μοναδικός αριθμός αποδεικτικού καταχώρησης. Κάθε υποκείμενο έχει το δικαίωμα πρόσβασης στα ηλεκτρονικά έγγραφα που τηρεί το πανεπιστήμιο και αίτησης χορήγησης αντιγράφου αυτών.

Στην πράξη τα πανεπιστήμια συνήθως τηρούν αρχεία υπό μορφή φυσικών εγγράφων ή σε λειτουργικά συστήματα. Τέτοια είναι τα συστήματα ενδοεπιχειρησιακού σχεδιασμού ERP (Enterprise Resource Planning,) που παρέχουν ενσωματωμένη διαχείριση των βασικών διαδικασιών[156] ή τα Πληροφοριακά συστήματα των Πανεπιστημίων UIS (University Information Systems). Και τα δύο αυτά συστήματα εμπεριέχουν βάσεις δεδομένων που διαθέτουν χρήσιμες πηγές προσωπικών δεδομένων, έτσι ώστε να δημιουργούνται μοντέλα πρόβλεψης, ήτοι μια εφαρμογή που λέγεται data mining ή εξόρυξη δεδομένων (Tavani,

[156] Ήτοι ενσωματώνουν εσωτερικές και εξωτερικές πληροφορίες διαχείρισης σε έναν ολόκληρο οργανισμό συνδυάζοντας χρηματοδότηση/λογιστική, κατασκευή, πωλήσεις και υπηρεσίες, διαχείριση πελατειακών σχέσεων κτλ. Τα συστήματα ERP αυτοματοποιούν αυτές τις δραστηριότητες με μια ολοκληρωμένη εφαρμογή λογισμικού, με σκοπό να διευκολύνουν τη ροή των πληροφοριών μεταξύ όλων των επιχειρησιακών λειτουργιών μέσα στα όρια της οργάνωσης και να επιτύχουν τις συνδέσεις προς τα έξω με τα ενδιαφερόμενα μέρη, βλ. σχετικά https://el.wikipedia.org/wiki/%CE%A3%CF%8D%CF%83%CF%84%CE%B7%CE%BC%CE%B1_%CE%B5%CE%BD%CE%B4%CE%BF%CE%B5%CF%80%CE%B9%CF%87%CE%B5%CE%B9%CF%81%CE%B7%CF%83%CE%B9%CE%B1%CE%BA%CE%BF%CF%8D_%CF%83%CF%87%CE%B5%CE%B4%CE%B9%CE%B1%CF%83%CE%BC%CE%BF%CF%8D

1999), η οποία συνεπάγεται την ανάκτηση της αυτόματης γνώσης από τις βάσεις δεδομένων (Strecht, 2019).

Τα πανεπιστήμια ως Ν.Π.Δ.Δ. συνιστούν οντότητες που εμπίπτουν στο πεδίο εφαρμογής του ΓΚΠΔ, ευρισκόμενα εντός Ε.Ε. και προσφέροντας αγαθά ή υπηρεσίες συμπεριλαμβανομένων και των εκπαιδευτικών, που μπορεί να είναι:

1) ανταλλαγή επικοινωνίας με πρώην φοιτητές που βρίσκονται στην Ε.Ε.

2) άμεσο μάρκετινγκ προγραμμάτων εξ αποστάσεως εκπαίδευσης (e-learning) σε φοιτητές που βρίσκονται στην Ε.Ε.

3) αποδοχή αιτήσεων από φοιτητές που βρίσκονται στην Ε.Ε.

4) παροχή εξ αποστάσεως εκπαίδευσης σε φοιτητές που βρίσκονται στην Ε.Ε.

5) συνεργασία με ιδρύματα τριτοβάθμιας εκπαίδευσης που είναι εγκατεστημένα στην Ε.Ε. για παροχή υπηρεσιών σε άτομα που βρίσκονται στην Ε.Ε. (Dunn, 2018)(Johnson, 2018).

Το Πανεπιστήμιο προσφέρει τις ως άνω υπηρεσίες/ αγαθά σε άτομα που βρίσκονται με φυσική παρουσία (έστω και προσωρινά) εντός της Ε.Ε. και μπορεί να είναι :

-πολίτες ή κάτοικοι της Ε.Ε.

-υποψήφιοι φοιτητές/ υπάλληλοι πανεπιστημίου κράτους μη μέλους της Ε.Ε.[157],

- φοιτητές που δεν έχουν την ιθαγένεια κράτους μέλους Ε.Ε. αλλά σπουδάζουν σε κράτος μέλος της Ε.Ε.

-φοιτητές που βρίσκονται σε κράτος μέλος της Ε.Ε. και φοιτούν διαδικτυακά σε πανεπιστήμιο κράτους μη μέλους της Ε.Ε.

-απόφοιτοι πανεπιστημίου κράτους μη μέλους της Ε.Ε. που βρίσκονται στην Ε.Ε.

-φοιτητές που έχουν ιθαγένεια/διαμονή σε κράτος μέλος Ε.Ε. αλλά παρακολουθούν on line εκπαίδευση λ.χ. στις ΗΠΑ[158]

Στις ως άνω περιπτώσεις επεξεργασίας τα δεδομένα φοιτητών προστατεύονται από τον ΓΚΠΔ, για όσο χρονικό διάστημα τα υποκείμενά τους έχουν φυσική παρουσία σε κάποιο κράτος μέλος Ε.Ε.[159]

[157] Όπως αλλοδαποί φοιτητές ή μέλη ΔΕΠ σε κινητικότητα μέσω προγραμμάτων ανταλλαγής, πρόσφυγες ή μετανάστες που ενδεχομένως παρακολουθούν προγράμματα διά βίου μάθησης, βλ. σχετικά μεταξύ άλλων Πολιτική Προστασίας Προσωπικών Δεδομένων – Πανεπιστήμιο Δυτικής Μακεδονίας, διαθέσιμη σε: https://www.uom.gr/downloads/terms/Politiki-Prostasias-UOM.pdf

[158] Στις ΗΠΑ ισχύει ο ομοσπονδιακός νόμος περί οικογενειακών εκπαιδευτικών δικαιωμάτων και απορρήτου (FERPA) (20 USC § 1232g; 34 CFR Part 99) που προστατεύει το απόρρητο των αρχείων εκπαίδευσης των σπουδαστών, βλ. σχετικά https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

Ως εκ τούτου τα πανεπιστήμια καλούνται να προβαίνουν σε σύννομη επεξεργασία και να συμμορφώνονται με τις διατάξεις του ΓΚΠΔ, να εφαρμόζουν τις αρχές που τον διαπνέουν και να σέβονται τα δικαιώματά τους[160], ενσωματώνοντας τις υποχρεώσεις του Κανονισμού στην κουλτούρα και στη λειτουργία τους. Κατά την επεξεργασία το Πανεπιστήμιο ως υπεύθυνος επεξεργασίας των προσωπικών δεδομένων των εργαζομένων, των φοιτητών και προμηθευτών πρέπει να δρα κατά τρόπο διαφανή, όταν ζητά πληροφορίες να χρησιμοποιούνται μόνο για τους αιτηθέντες σκοπούς, να περιορίζονται στο αναγκαίο μέτρο και να επικαιροποιούνται, να αποθηκεύονται κατά τον ελάχιστο αναγκαίο χρόνο.

Για να επιτευχθεί αυτό πρέπει να λάβει καταρχήν μια σαφή και οριοθετημένη πολιτική που να προσδιορίζει α) τους ρόλους και τις ευθύνες του προσωπικού β) να απαντά στα βασικά ερωτήματα ποιος ξεκινάει τις εργασίες για τα προσωπικά δεδομένα, ποιος τις διεκπεραιώνει και ποιος τις εγκρίνει γ) να προσδιορίζει τα προσωπικά δεδομένα που συλλέγει δ) να επανεξετάζει όλες τις διαδικασίες, ώστε να αναγνωρίζονται οι τυχόν παραβιάσεις και οι σχετικοί κίνδυνοι, και εν συνεχεία τα κατάλληλα τεχνικά και οργανωτικά μέτρα (π.χ. ψευδωνυμοποίηση, κρυπτογράφηση, ανωνυμοποίηση) και να επιλέξει την προληπτική προστασία των δεδομένων μέσω της εφαρμογής της προστασίας «από τον σχεδιασμό και εξ ορισμού». Απαραίτητη προϋπόθεση συνιστά ο υπεύθυνος επεξεργασίας να εξετάσει ποιο είναι το τρέχον επίπεδο συμμόρφωσης μέσω της διενέργειας μιας gap analysis σε συνδυασμό με σωστό σχεδιασμό (Mekovec & Peras, 2020). Αν κριθεί ότι η επεξεργασία είναι επικίνδυνη για τα υποκείμενα, τότε οφείλει να προβεί και σε εκπόνηση μελέτης DPIA.

Η εφαρμογή του ΓΚΠΔ στο μέτρο της επιβολής προστίμων αναφέρεται κυρίως σε κερδοσκοπικούς οργανισμούς (Spicer 2018). Αυτό βέβαια δε σημαίνει ότι δεν είναι πιθανή η επιβολή διοικητικών κυρώσεων και στα ακαδημαϊκά ιδρύματα, η οποία μπορεί να μην αγγίζει τα δυσθεώρητα πρόστιμα που επιβάλλονται σε επιχειρήσεις, ωστόσο θα έχει τεράστιες οικονομικές επιπτώσεις για τη Διοίκησή τους και σημαντική προσβολή του

[159] Όπως χαρακτηριστικά αναφέρει ο Cormack (2017), ο κανόνας είναι ότι *«Για όσο τα πόδια τους βρίσκονται στο έδαφος της Ε.Ε., ο GDPR ισχύει για αυτούς. Μόλις επιβιβαστούν σε αεροπλάνο και αυτό βγει εκτός Ε.Ε., το GDPR δεν ισχύει πλέον για αυτούς»*, βλ. https://www.jisc.ac.uk/blog/a-year-to-get-your-act-together-how-universities-and-colleges-should-be-preparing-for-new-data-regulations?lang=en

[160] Ειδικά όσον αφορά στο δικαίωμα στη λήθη διατυπώνονται αμφιβολίες σχετικά με το αν μπορεί να προστατευθεί κατά τις διατάξεις του ΓΚΠΔ δοθέντος ότι οι περισσότεροι εσωτερικοί κανονισμοί πανεπιστημίων εισάγουν την υποχρέωση να τηρούνται εσαεί τα αρχεία φοιτητών και αποφοίτων. Το ίδιο ισχύει και για τις διπλωματικές που πρόκειται να δημοσιοποιηθούν καθώς θεωρούνται συνεισφορά στη γνώση και πρέπει να είναι προσβάσιμες σε όλους όσους επιθυμούν να εμβαθύνουν σε συγκεκριμένο αντικείμενο (Vilela, 2019).

κύρους και της φήμης τους, σε περίπτωση διαπίστωσης έλλειψης ισχυρών ελέγχων ασφαλείας δεδομένων.

Σε κάθε περίπτωση τα πανεπιστήμια πρέπει κατά την εφαρμογή του ΓΚΠΔ και συμμόρφωσή τους να αντιληφθούν και τα πιθανά οφέλη. Αυτά συνίστανται κυρίως στο ότι θα αυξηθεί η ευαισθητοποίηση για την προστασία των προσωπικών δεδομένων, θα αναδιοργανωθεί η δομή και η λειτουργία τους και θα υιοθετηθούν καλές πρακτικές (Garber, 2018). Η υιοθέτησή τους ακούγεται ιδανική αλλά συνιστά σαφώς ένα δύσκολο εγχείρημα που απαιτεί εντατική προσπάθεια, ενημέρωση, εκπαίδευση και συνδυαστική χρήση των κατευθυντήριων γραμμών του ΕΣΠΔ και της νομολογίας των δικαστηρίων.

Κάθε πανεπιστήμιο οφείλει να μεταβάλει τον τρόπο διαχείρισης των υπό επεξεργασία δεδομένων. Αυτό πρακτικά σημαίνει ότι ο υπεύθυνος επεξεργασίας τεκμηριώνει τους λόγους για τους οποίους διατηρεί τα αρχεία που εμπεριέχουν δεδομένα, τον τρόπο συλλογής των δεδομένων, το χρόνο διατήρησής τους και το χρόνο διαγραφής αυτών, το χρόνο ανωνυμοποίησής τους και την εξουσιοδοτημένη πρόσβαση σ’ αυτά. Μ’ αυτόν τον τρόπο θα αναπτύξει βαθμιαία μια διαφορετική κουλτούρα που θα χαρακτηρίζεται για την υπεύθυνη και ηθική διαχείριση των πληροφοριών που δέχεται, ενισχύοντας το κλίμα εμπιστοσύνης μεταξύ αυτού και των ατόμων που παραχωρούν τα προσωπικά τους δεδομένα, σε όποια νομιμοποιητική βάση κι αν στηρίζεται η χορήγησή τους και με όποια σχέση κι αν τα συνδέει με το εν λόγω ίδρυμα (σύμβαση, νομική υποχρέωση κλπ.), υπηρετώντας επάξια το ρόλο και την ιδιότητά τους ως χώρων ανάπτυξης και καλλιέργειας πνεύματος.

Η εν λόγω προσέγγιση σχετίζεται άμεσα με τον κύκλο ζωής της πληροφορίας που συλλέγεται και είναι θεμελιώδης για την ανάπτυξη διεθνών προτύπων αναφορικά με την ποιότητα και την ασφάλεια των πληροφοριών, προκειμένου να συμβάλει στους στόχους των θεσμικών οργάνων αναφορικά με την προστασία της ιδιωτικότητας. Αν και προωθείται η ιδέα της κατάρτισης κωδίκων δεοντολογίας και ενθαρρύνεται η υιοθέτηση μηχανισμών πιστοποίησης προστασίας δεδομένων, δεν επιβάλλεται από τον εσωτερικό κανονισμό των Πανεπιστημίων ένα συγκεκριμένο σύνολο τεχνικών προτύπων (Dunn, 2018).

Η αποτελεσματικότητα του ΓΚΠΔ θα αναφανεί όταν το σύνολο των οντοτήτων, προβεί σε ορθή εφαρμογή του και οι υπεύθυνοι και εκτελούντες την επεξεργασία δεδομένων,

προσεγγίσουν τις επιταγές του όχι υπό το πρίσμα του υποχρεωτικού βάρους ή του φόβου της επιβολής κύρωσης αλλά ως ευκαιρία αναδιοργάνωσης, αλλαγής κουλτούρας και εν γένει πολιτικής, με σημείο εκκίνησης τηη κρισιμότητα του απορρήτου των προσωπικών δεδομένων, την οργάνωσή του και την ασφάλεια αυτών. Το δικαίωμα στη λήθη ή στη φορητότητα, η υποχρέωση γνωστοποίησης της παραβίασης στην ΑΠΔΠΧ, η λογοδοσία του υπευθύνου ή του εκτελούντα την επεξεργασία, η μεταφορά του κέντρου βάρους από τις κατασταλτικές δυνατότητες των αρχών στις προληπτικές ενέργειες των εμπλεκομένων και άλλες αλλαγές, αποτελούν παράγοντες που οδηγούν στην ανάγκη για αλλαγή κουλτούρας (Γιαννόπουλο, 2017).

Στις 25-5-2018 τα πανεπιστήμια της χώρας μας κλήθηκαν να αναγνωρίσουν την ανάγκη εφαρμογής των διατάξεων του ΓΚΠΔ στο εσωτερικό τους. Αφού ενημερώθηκαν, όφειλαν να συμμορφωθούν με τις αρχές και το πνεύμα της νέας εποχής της τεχνολογικής εξέλιξης λειτουργώντας σε πλήρη εναρμόνιση με τον ΓΚΠΔ. Για να το πετύχουν αυτό έπρεπε να προβούν σε σωστό και άμεσο προγραμματισμό που συνίσταται στην ενημέρωση της Διοίκησης για το νέο θεσμικό-κανονιστικό πλαίσιο και του προσωπικού, σε ορισμό Υπευθύνου Προστασίας, σε έλεγχο των ειδοποιήσεων απορρήτου, σε έλεγχο σεβασμού των δικαιωμάτων του υποκειμένου, σε έλεγχο του τρόπου χορήγησης της συγκατάθεσης, ό,που αυτή ζητείται και σε ανάπτυξη νέων διαδικασιών για τη λήψη της συγκατάθεσης αυτής, καθώς και σε προετοιμασία και ασκήσεις για το ενδεχόμενο παραβίασης προσωπικών δεδομένων (Sidlauskas & Limba, 2019).

Για να αποδείξει ένα πανεπιστήμιο την συμμόρφωσή του προς τις επιταγές του ΓΚΠΔ οφείλει να προβεί σε σειρά ενεργειών που διασφαλίζουν τις πρακτικές ασφαλείας δεδομένων, να εφαρμόσει περιορισμούς απορρήτου και πολιτικών χρήσης των προσωπικών δεδομένων, να αναπτύξει κατάλληλη διαδικασία συλλογής προσωπικών δεδομένων, να εφαρμόσει κατάλληλα μέτρα προστασίας προσωπικών δεδομένων και να συμμορφωθεί πλήρως με τη διαδικασία γνωστοποίησης σε περίπτωση παραβίασης των δεδομένων. Η συμμόρφωση πρέπει να θεαθεί όχι ως μια πρωτοβουλία στον τομέα της πληροφορικής και τεχνολογίας αλλά ως μια οργανωτική προσπάθεια που απαιτεί τη δέσμευση της θεσμικής ηγεσίας να δώσει προτεραιότητα στους πόρους, τις πολιτικές και τις διαδικασίες (Dunn, 2018). Επομένως απαραίτητες προϋποθέσεις με οριζόντια ισχύ ήταν πρωτίστως να ευαισθητοποιηθεί η Διοίκηση των πανεπιστημίων για τη συμμόρφωση, να διατεθούν οι ανάλογοι πόροι (οικονομικοί και ανθρώπινοι) και η τεχνογνωσία, ώστε τα

ακαδημαϊκά ιδρύματα να καταστούν περισσότερο υπεύθυνα για τα δεδομένα που διατηρούν (Sidlauskas & Limba, 2019).

4.4. Βήματα προετοιμασίας των πανεπιστημίων για τον ΓΚΠΔ

Σύμφωνα με τις αρχές που έχει εκδώσει η ΑΠΔΠΧ για να επιτευχθεί η συμμόρφωση ενός φορέα με τις επιταγές του ΓΚΔΠ, πρέπει να ακολουθηθούν ορισμένα βήματα προετοιμασίας ώστε να είναι σε θέση να ανταπεξέλθουν στις νέες τους υποχρεώσεις. Έτσι και τα πανεπιστήμια[161] καλούνται πριν εφαρμόσουν τον ΓΚΠΔ να ακολουθήσουν τα εξής βήματα :

1. Ενημέρωση. Να ενημερώσουν το προσωπικό τους για τις μεταβολές που επέρχονται από το νέο κανονιστικό πλαίσιο προστασίας δεδομένων. Να το εκπαιδεύσουν και ευαισθητοποιήσουν δίνοντας έμφαση στις επιπτώσεις σε περίπτωση παραβίασης. Να αξιολογήσουν τους πιθανούς κινδύνους για τα δεδομένα που συλλέγονται και διαμορφώσουν τη στρατηγική αντιμετώπισής τους.

2.Καταγραφή. Να τηρούν ειδικά αρχεία επεξεργασίας δεδομένων, στα οποία πρέπει να καταγράφονται λεπτομερώς ποια δεδομένα τηρούνται και ποια μεταβιβάζονται, τι είδους επεξεργασία γίνεται, ποιος είναι ο σκοπός επεξεργασίας και ποια η νομιμοποιητική της βάση. Η τήρηση αρχείων ισοδυναμεί με καταγραφή, ανάλυση και εκτίμηση της υφιστάμενης κατάστασης και των διαδικασιών που εφαρμόζει το πανεπιστήμιο καθώς και των ελλείψεών του (data mapping[162], gap analysis[163]).

[161] Οι υφιστάμενες εναλλακτικές προσεγγίσεις συμμόρφωσης των εκπαιδευτικών ιδρυμάτων προς τον ΓΚΠΔ είναι α) της Microsoft (2018), β) της Podnar (2017) και γ) του Cormack (2017), βλ. Habbabeh, *et al.* (2019), pp.226-228.

[162]Η «χαρτογράφηση» (data mapping) είναι μια εξαιρετικά σημαντική διαδικασία που επιτρέπει να διερευνηθεί ποια είναι τα προσωπικά δεδομένα που επεξεργάζεται το πανεπιστήμιο (είδος δεδομένων, τρόπος κτήσης, σκοπός και κατηγορία στην οποία ανήκουν τα δεδομένα), πού φυλάσσονται, για πόσο χρονικό διάστημα, ποιός έχει πρόσβαση, εάν υπάρχει συγκατάθεση υποκειμένου, εάν υπάρχει διαδικασία καταστροφής, ποιά μέτρα έχουν ληφθεί για την προστασία τους, βλ. σχετικά και P. Mouncey, Planning for the GDPR: evolution rather than revolution, SRA Research Matters: March 2018:1

[163] Η Gap Analysis διενεργείται για να προσδιορίσει ποιά στοιχεία του ΓΚΠΔ ισχύουν και ποιά πρέπει να προστεθούν ή μεταβληθούν για να επιτευχθεί το επιθυμητό επίπεδο συμμόρφωσης. Συνίσταται στην σύγκριση των προϋποθέσεων του κανονισμού με τις διαδικασίες του οργανισμού και δείχνει τους ανθρώπινους πόρους που είναι αναγκαίοι για τη μείωση των κινδύνων. Αποτελεί ένα χρήσιμο εργαλείο κατανόησης του πώς ο ΓΚΠΔ επιδρά σε έναν οργανισμό και πως ο οργανισμός πρέπει να αναθεωρήσει τις αδυναμίες του. Βοηθάει τους ελεγκτές/υπεύθυνους επεξεργασίας να αναγνωρίσουν τους κινδύνους εντός των προβλεπομένων από τον ΓΚΠΔ διαδικασιών συμμόρφωσης και να προσδιορίσουν τους αναγκαίους πόρους για την εφαρμογή βελτιώσεων (Mekovec & Peras, 2020)

3.Έλεγχος τήρησης συμμόρφωσης. Να εξετάζουν διαρκώς εάν κατά την επεξεργασία τηρούνται οι αρχές της σύννομης επεξεργασίας και αν γίνονται σεβαστά τα δικαιώματα των υποκειμένων (ειδικές ρήτρες στις συμβάσεις με προσωπικό, πελάτες και προμηθευτές)

4.Έλεγχος συγκατάθεσης. Να εξετάζουν τις μεθόδους που εφαρμόζουν για την εξασφάλιση συγκατάθεσης για κάθε επιδιωκόμενο σκοπό επεξεργασίας.

5.Αναθεώρηση πολιτικών προστασίας δεδομένων και διαδικασιών. Να βελτιώνουν και επικαιροποιούν τις υφιστάμενες διαδικασίες και πολιτικές για τον χειρισμό των αιτημάτων και την ικανοποίηση των δικαιωμάτων των υποκειμένων, κυρίως όσον αφορά στην διαγραφή δεδομένων (δικαίωμα στη λήθη) ή την παροχή τους σε αναγνώσιμο ηλεκτρονικό μορφότυπο (φορητότητα). Να υποδείξουν οργανωτικά και τεχνικά μέτρα συμμόρφωσης προς το ΓΚΠΔ. Να δημιουργήσουν πρότυπα έντυπα (λήψη συγκατάθεσης, emails, όρους χρήσης ιστοτόπου, πολιτική cookies κ.α.)

6. Εκτίμηση επιπτώσεων/αντικτύπου. Να φροντίσουν να είναι σε θέση να εκτιμούν τις πιθανότητες επέλευσης κινδύνων και τις συνέπειες στα προσωπικά δεδομένα.

7. Ορισμός Υπεύθυνου Προστασίας Δεδομένων. Να ορίσουν υποχρεωτικά ΥΠΔ σύμφωνα με τα προβλεπόμενα στον ΓΚΠΔ[164]. Ο ΥΠΔ έχοντας σαφή γνώση του ΓΚΠΔ και της τεχνολογίας συνιστά ένα από τα πλέον ανεκτίμητα περιουσιακά στοιχεία ενός πανεπιστημίου γιατί όχι μόνον εξασφαλίζει τη συμμόρφωση αλλά λειτουργεί και ως εκπαιδευτής εξηγώντας στο προσωπικό τις επερχόμενες μεταβολές, κατά τρόπο ευθύ και σχετικό με τις ιδιαιτερότητες του ιδρύματος.

8. Παραβιάσεις δεδομένων. Να υιοθετήσουν μεθόδους για την ανίχνευση, καταγραφή και διερεύνηση περιστατικών παραβιάσεων. Να μεριμνήσουν για την απόκτηση ανάλογης διαδικασίας σχετικά με τις γνωστοποιήσεις στην ΑΠΔΠΧ και τα υποκείμενα των δεδομένων που επεξεργάζονται. Ένας καλός τρόπος είναι η ανάπτυξη σχεδίου αντιμετώπισης περιστατικών παραβίασης συστημάτων και απώλειας δεδομένων (Incident Response Plan).

9. Δραστηριότητα σε περισσότερα κράτη μέλη. Σε τέτοιου είδους περιπτώσεις να φροντίζουν να προτείνουν το κράτος της κύριας εγκατάστασής τους.

[164] Η υποχρέωση των διοικήσεων των πανεπιστήμιων να προβούν υποχρεωτικά σε ορισμό ΥΠΔ προκύπτει ευθέως από τη διάταξη του άρθρου 6 του Ν.4624/2019 για τους δημόσιους φορείς.

10. Διαβιβάσεις δεδομένων εκτός Ε.Ε. Σε περίπτωση διαβίβασης δεδομένων σε τρίτες χώρες, να επιλέγουν βάσει ποιού μηχανισμού διαβίβασης πρόκειται να κινηθούν (δεσμευτικοί εταιρικοί κανόνες (BCRs), τυποποιημένες συμβατικές ρήτρες (SCCs), πιστοποιήσεις στο Privacy Shield (για τις ΗΠΑ)).

4. 5. Η Συμμόρφωση των Πανεπιστημίων με τον ΓΚΠΔ

4. 5.1. Γενικά

Υπό το πρίσμα των διατάξεων του ΓΚΠΔ κρίνεται σκόπιμο οι φορείς και οι οργανισμοί να μην αντιμετωπίζουν την εφαρμογή του ως μια υποχρέωση στατική και σημειακή που εξαντλείται στην ανάθεση της σύνταξης μιας έκθεσης σε κάποιο εξωτερικό σύμβουλο, στην αγορά πρόσθετων πληροφοριακών συστημάτων ή στον απλό ορισμό κάποιου στελέχους ως ΥΠΔ και στη γνωστοποίηση των στοιχείων του στην ΑΠΔΠΧ. Οι περισσότεροι δημόσιοι οργανισμοί λόγω της φύσης τους προβαίνουν σε περιορισμένες ενέργειες προετοιμασίας και απέχουν από την πλήρη συμμόρφωσή τους. Οι λόγοι που κατατείνουν σ' αυτό είναι η αύξηση του φόρτου εργασίας που θα επέλθει στον φορέα με την ενασχόλησή του με ένα ζήτημα με το οποίο δεν είναι εξοικειωμένος καθώς επίσης κι η έλλειψη οικονομικών πόρων. Είναι βέβαια αναγκαίο να κατανοήσουν όλοι οι οργανισμοί ότι η πρόληψη είναι καλύτερη από την καταστολή και να αναθέσουν αρμοδιότητες σε κάποιον εσωτερικό ή εξωτερικό σύμβουλο που θα αναλάβει ενεργά το ρόλο του ΥΠΔ, ο ορισμός του οποίου όπως προαναφέρθηκε, είναι υποχρεωτικός στην περίπτωση των δημόσιων φορέων, ανεξάρτητα από το μέγεθός τους.

Είναι μείζονος σημασίας ο ΓΚΠΔ να γίνει αντιληπτός ως αναπόσπαστο οργανικό κομμάτι της λειτουργίας και της κουλτούρας των πανεπιστημίων. Εάν κάθε πανεπιστήμιο εφαρμόσει ένα Πρόγραμμα και υιοθετήσει έναν Οδηγό, θα ωθήσει στον εκσυγχρονισμό και την αναδιάρθρωσή του και αναμφίβολα θα αναδείξει τη συμβολή του κανονισμού (ΣΕΒ, 2018). Κατ' επέκταση, η συμμόρφωση συνιστά ευκαιρία που θα προσδώσει ανταγωνιστικό πλεονέκτημα και θα ενισχύσει την αξία των πανεπιστημίων, επενδύοντας στην ασφάλεια των δεδομένων του προσωπικού, των φοιτητών και των προμηθευτών μέσα από μια ουσιαστική και «έξυπνη συμμόρφωση» που μακροπρόθεσμα θα αναφανεί ότι το χρηματικό και διοικητικό κόστος της καθημερινής λειτουργία τους, δεν είναι εν τέλει και όπως αποδεικνύεται εκ του αποτελέσματος, τόσο υψηλό. Κατόπιν έρευνας που

διενεργήθηκε διαπιστώθηκε ότι τα περισσότερα πανεπιστήμια υποδέχθηκαν με ζέση τον ΓΚΠΔ, γεγονός που συνιστά θετικό βήμα για την προστασία των δεδομένων.

Οι δημόσιοι φορείς μεταξύ των οποίων και τα περισσότερα ακαδημαϊκά ιδρύματα της χώρας καλούνται να υιοθετήσουν ένα πρόγραμμα για την Προστασία των Δεδομένων των υποκειμένων τους. Η Διοίκηση πρέπει να επιλέξει σε ποιόν θα αναθέσει το έργο της συμμόρφωσης (Τσιπτσέ & Κωστούλας 2020), ήτοι σε εργαζόμενο ή σε σύμβουλο συμμόρφωσης. Πρωτίστως διεξάγεται μια εκτίμηση με το υφιστάμενο επίπεδο συμμόρφωσης για την επεξεργασία των δεδομένων και εν συνεχεία καταρτίζεται σχέδιο δράσης με τα προτεινόμενα μέτρα συμμόρφωσης (Habbabeh, Schneider & Asprion, 2019). Το επόμενο βήμα είναι ο ορισμός ομάδας εργασίας εντός του οργανισμού, αρμόδιας να επικοινωνεί με τον υπεύθυνο συμμόρφωσης. Οι εργασίες ξεκινούν με την συμπλήρωση ενός ερωτηματολογίου αυτοαξιολόγησης αποτελούμενο από ερωτήματα κανονιστικής, οργανωτικής αλλά και τεχνικής φύσης αναφορικά με το επίπεδο προστασίας που υφίσταται στον εκάστοτε οργανισμό (Habbabeh, Schneider & Asprion, 2019).

Στη φάση αυτή κρίνεται απαραίτητη η ενημέρωση του προσωπικού αναφορικά με το επικείμενο πρόγραμμα συμμόρφωσης κατά το πρότυπο του κύκλου του Deming (Check, Plan, Do, Act) το οποίο διακρίνεται σε επιμέρους στάδια και απαρτίζεται από τις εξής διαδικασίες :

1. την *αξιολόγηση*, κατά την οποία γίνεται η χαρτογράφηση δεδομένων και ροών δεδομένων, διενεργείται έλεγχος κι επιθεώρηση των πληροφοριακών και των νομικών συστημάτων
2. τον *σχεδιασμό*, στα πλαίσια του οποίου εκπονείται η εκτίμηση αντικτύπου προστασίας δεδομένων
3.την *υλοποίηση*, η οποία περιλαμβάνει το σχεδιασμό, την υλοποίηση τεχνικών και οργανωτικών μέτρων συμμόρφωσης, την εκπαίδευση και την επιθεώρηση προγράμματος συμμόρφωσης
4. και τη *λειτουργία* του συστήματος, η οποία σχετίζεται με τον ορισμό του υπευθύνου επεξεργασίας με τα ανάλογα καθήκοντα, προσόντα και προδιαγραφές

Η λήψη των τεχνικών και οργανωτικών μέτρων στο στάδιο της υλοποίησης εμπεριέχει την καθιέρωση πολιτικών προστασίας των δεδομένων και διαδικασιών ενώ η καθιέρωση κώδικα δεοντολογίας και μηχανισμών πιστοποίησης αποδεικνύει τη συμμόρφωσή με τον

ΓΚΠΔ (άρθρο 24 παρ.3 ΓΚΠΔ). Ο ορισμός του ΥΠΔ γίνεται συνήθως με επίσημη δημοσιοποίηση των στοιχείων επικοινωνίας του στον οικείο ιστότοπο του εκάστοτε οργανισμού. Προτεραιότητα δίνεται επίσης στο απόρρητο των δεδομένων και τη ασφάλεια[165], ενώ ο έλεγχος των δεδομένων προωθείται με ενημερωμένες πολιτικές απορρήτου, υγιή συστήματα ασφαλείας και ελαχιστοποίηση των δεδομένων.

Κάθε στάδιο συνοδεύεται από χρονοδιάγραμμα υλοποίησης, η χρονική διάρκεια του οποίου ποικίλλει. Η υλοποίηση του έργου συμμόρφωσης τεκμηριώνεται με τις εκθέσεις και μελέτες σε μορφή αρχείων που παραδίδει ο υπεύθυνος συμμόρφωσης (Τσιπτσέ & Κωστούλας, 2020).

4.5.2. Οι φάσεις συμμόρφωσης με τον ΓΚΠΔ

Όπως κάθε φορέας έτσι και τα πανεπιστήμια στα πλαίσια της συμμόρφωσής τους προς το ΓΚΠΔ οφείλουν να ακολουθήσουν τις εξής φάσεις συμμόρφωσης:

Α' φάση συμμόρφωσης

Στη φάση αυτή αρχικά γίνεται η πρώτη ενημέρωση του οργανισμού αναφορικά με το κανονιστικό πλαίσιο του ΓΚΠΔ και τους σκοπούς του, ακολουθούν οι συναντήσεις με τη διοίκηση, το προσωπικό καθώς και με όλα τα τμήματα του πανεπιστημίου και με τους εξωτερικούς συνεργάτες και δη τη νομική υπηρεσία και την υπηρεσία μηχανογραφικής υποστήριξης. Εν συνεχεία διενεργείται η επιτόπια επιθεώρηση των υποδομών όπου τηρούνται ευαίσθητα δεδομένα (είτε σε φυσικά αρχεία είτε σε ηλεκτρονικά). Το αμέσως επόμενο βήμα που ακολουθείται είναι εκείνο της εκπαίδευσης του προσωπικού και της Διοίκησης σχετικά με τις βασικές έννοιες του ΓΚΠΔ, τις απαραίτητες ενέργειες υλοποίησης και το γενικό πλάνο δράσης που αποσκοπεί στην σταδιακή δημιουργία μιας κουλτούρας σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα στην καθημερινότητα. Κατά τη διάρκειά της ο υπεύθυνος επεξεργασίας πρέπει να μεριμνά για την τήρηση ορισμένων αρχείων όπως το Ευρετήριο Προσωπικών Δεδομένων[166], το Αρχείο

[165] Βλ. σχετικά μεταξύ άλλων και GDPR Part One: The Basics for Universities (May 18, 2018) διαθέσιμο σε: https://degreeanalytics.com/gdpr-partone/

[166] Το Ευρετήριο Προσωπικών Δεδομένων (Data Inventory) είναι ένα πίνακας όπου αναγράφεται το είδος των προσωπικών δεδομένων που διαχειρίζεται ένας δημόσιος φορέας, ο τρόπος αποθήκευσης και επεξεργασίας τους, ο επιτρεπόμενος χρόνος αποθήκευσης, η μεθοδολογία διαγραφής ή καταστροφής κλπ.

Ροών Δεδομένων[167], το Αρχείο Χαρτογράφησης[168] και το Αρχείο Δραστηριοτήτων Επεξεργασίας[169].

Πριν ολοκληρωθεί η πρώτη φάση κρίνεται σκόπιμο να ξεκινήσει η υλοποίηση κρίσιμων διορθωτικών οργανωτικών και τεχνικών μέτρων αφού προηγουμένως συνταχθεί μια ανεπίσημη έκθεση πρώτων κρίσιμων ευρημάτων σχετικά με το ποιος έχει πρόσβαση στα δεδομένα, με το αν υπάρχει επαρκής ή ελλιπής φυσική ασφάλεια (π.χ. είναι εκτεθειμένα και χωρίς ασφάλεια αρχεία ή όχι) ή τεχνική ασφάλεια (π.χ. υπάρχει ή όχι firewall, antivirus κλπ) ή νομική ή κανονιστική συμμόρφωση (πχ. υπάρχουν ή όχι έντυπα συγκατάθεσης ή πολιτική προστασίας δεδομένων) (Τσιπτσέ & Κωστούλας, 2020). Προς τούτο είναι αναγκαίο τη δεδομένη χρονική στιγμή να υλοποιούνται και οι αντίστοιχες διορθωτικές ενέργειες που αφορούν τη φυσική ασφάλεια, τη σύνταξη και παράδοση των αναγκαίων κανονιστικών και νομικών κειμένων (πχ. έντυπα ενημέρωσης, συγκατάθεσης υποκειμένων), τη διευθέτηση ζητημάτων σχετικών με την ασφάλεια της ηλεκτρονικής πληροφορίας (IT-Security), τη σύνταξη ειδικής ενότητας στην ιστοσελίδα του κάθε πανεπιστημίου σχετικά με τη συμμόρφωσή του κατά τον ΓΚΠΔ, την ανάρτηση Πολιτικής Προστασίας Προσωπικών Δεδομένων, χρήσης και διαχείρισης cookies με δυνατότητα αποδοχής ή άρνησης κ.α.

Β' φάση συμμόρφωσης

Το πρώτο βήμα της φάσης αυτής συνίσταται στην πραγματοποίηση νέων συναντήσεων, συζητήσεων για τα παραδοτέα αρχεία της πρώτης φάσης και στην ανάλυση των ερωτημάτων ενώ παράλληλα διεξάγονται νέες εκπαιδεύσεις. Η επόμενη κίνηση είναι να προβεί ο υπεύθυνος στην Ανάλυση Αποκλίσεων (Gap Analysis) ώστε να διαπιστωθούν οι νομικές/κανονιστικές, οργανωτικές και τεχνικές αποκλίσεις από τις απαιτήσεις του ΓΚΠΔ και να μπορεί να ανιχνεύσει τα προβληματικά πεδία της αρχικής χαρτογράφησης και να τα συσχετίσει με τις απαιτήσεις του ΓΚΠΔ. Η εν λόγω ανάλυση επιτρέπει τη σύγκριση της δεδομένης κατάστασης με την επιθυμητή (Τσιπτσέ & Κωστούλας, 2020) και λαμβάνει

[167] Αρχείο Ροών Δεδομένων (Data Flow Mapping) σ' αυτό παρατίθενται ανά φάση οι προαναφερόμενες πληροφορίες, αποτυπωμένες σε πίνακες ροής εργασιών (flow charts) που απεικονίζουν τον τρόπο ροής των προσωπικών δεδομένων εντός και εκτός του φορέα.

[168] Το Αρχείο Χαρτογράφησης (Data Mapping) συνιστά ανάλυση της υφιστάμενης κατάστασης αναφορικά με την προστασία των προσωπικών δεδομένων εντός του πανεπιστημίου και τους κινδύνους που ελλοχεύουν ανά δράση ή τμήμα.

[169] Το Αρχείο Δραστηριοτήτων Επεξεργασίας (Processing Activities) το οποίο προετοιμάζεται μαζί με το αρχείο χαρτογράφησης, κυρίως όταν ένας φορέας απασχολεί περισσότερα από 250 εργαζόμενους

χώρα για κάθε δράση του Πανεπιστημίου και ως προς όλα τα ζητήματα (διαχείρισης προσωπικού, μηχανογραφικά ή ασφαλείας της πληροφορίας, φυσικής ή οργανωτικής ασφάλειας, σε έντυπα και αρχεία κ.λ.π). Η πλέον βασική ωστόσο ενέργεια στην παρούσα φάση είναι η υλοποίηση μιας συνολικής ανάλυσης κινδύνων (Risk Assessment)[170] σχετικά με τα ευρήματα που εντοπίστηκαν στη φάση της χαρτογράφησης, η οποία μάλιστα θα πρέπει να υλοποιείται τόσο πριν όσο και μετά την εφαρμογή των προτεινόμενων μέτρων προστασίας δεδομένων (Τσιπτσέ & Κωστούλας, 2020).

Γ΄ φάση συμμόρφωσης

Η τρίτη φάση συμμόρφωσης εκκινεί και αυτή με τις συναντήσεις, στις οποίες συζητούνται τα παραδοτέα αρχεία, γίνεται αναφορά στους κινδύνους και στα κατάλληλα τεχνικά και οργανωτικά μέτρα που πρέπει να ληφθούν. Εν συνεχεία πραγματοποιούνται οι τελικές εκπαιδεύσεις. Όπως παρατηρείται η εκπαίδευση είναι μια διαδικασία διαρκής που ενυπάρχει σε κάθε φάση συμμόρφωσης, γεγονός που αποδεικνύει τη σπουδαιότητά της αλλά και τη βαρύτητα που της αποδίδεται προκειμένου να εξασφαλιστεί η ευαισθητοποίηση και η αλλαγή κουλτούρας. Εν συνεχεία ακολουθεί η παράδοση του Προγράμματος Υλοποίησης Προτεινόμενων Μέτρων για την Προστασία των Δεδομένων (Data Protection Measures), η οποία είναι ουσιαστικά μια λίστα που απαριθμεί ορισμένα μέτρα με ρητή αναφορά στο ποιος θα τα υλοποιήσει, στο status της υλοποίησης και στο χρονοδιάγραμμα υλοποίησης το οποίο τηρεί και ενημερώνει ο ΥΠΔ (Τσιπτσέ & Κωστούλας, 2020). Γνωρίζοντας πλέον τις αποκλίσεις και του κινδύνους που διαπιστώθηκαν στην προηγούμενη φάση, ο υπεύθυνος καλείται να καλύψει κενά και να εξαλείψει κινδύνους. Γι' αυτό σχεδιάζονται και διανέμονται οι επίσημα καταγεγραμμένες πολιτικές, διαδικασίες και οδηγίες εργασίας που αφορούν στην ασφάλεια των δεδομένων.

Οι βασικές πολιτικές είναι οι Πολιτικές Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και άλλες Τυποποιημένες Διαδικασίες Λειτουργίας (Standard Operating Procedures – SOPs) που άλλοτε είναι νέες άλλοτε πάλι προσαρμόζονται στις υφιστάμενες διαδικασίες που έχει ήδη αναπτύξει ένας οργανισμός (Τσιπτσέ & Κωστούλας, 2020).

[170] Η risk assessment είναι γενικότερη της Μελέτης Αντικτύπου (dpia) η οποία αποτελεί υποκατηγορία της πρώτης με κοινούς στόχους και κοινές αρχές.

Οι κυριότερες διαδικασίες είναι η πολιτική προστασίας προσωπικών δεδομένων, ο ορισμός και οι αρμοδιότητες DPO[171], τα θεμελιώδη δικαιώματα υποκειμένων, το σχέδιο αντιμετώπισης παραβιάσεων προσωπικών δεδομένων, η μελέτη εκτίμησης αντικτύπου, η διαχείριση/ικανοποίηση αιτημάτων υποκειμένων-διαχείριση καταγγελιών, οι διαβιβάσεις δεδομένων προς τρίτες χώρες κλπ

Οι συνηθέστερες οδηγίες εργασίας είναι οδηγίες που αφορούν στην τήρηση και προστασία ηλεκτρονικών αρχείων, έλεγχο ηλεκτρονικής πρόσβασης, διαχείριση email, απαγόρευση αποστολής ή ανάρτησης δεδομένων μέσω διαδικτυακών εφαρμογών, τήρηση αρχείων καταγραφής, ασφάλεια συνδέσεων-επικοινωνιών-λογισμικού, έλεγχος φυσικής πρόσβασης σε συγκεκριμένους χώρους, προστασία εντύπων και φυσικών αρχείων που εμπεριέχουν δεδομένα, καταστροφή δεδομένων, διαχείριση περιστατικών παραβίασης δεδομένων, εκπαίδευση προσωπικού για την προστασία δεδομένων, προφορική ή τηλεφωνική κοινοποίηση δεδομένων κ.α.

Μετά την παράδοση των Πολιτικών, Διαδικασιών, Οδηγιών Εργασίας, Εντύπων και λοιπών μέτρων, το Πρόγραμμα Συμμόρφωσης ολοκληρώνεται (Τσιπτσέ & Κωστούλας, 2020). Εάν κάθε πανεπιστήμιο τηρήσει την ως άνω τακτική πρόληψης θα περιοριστούν οι παραβιάσεις των προσωπικών δεδομένων των εργαζομένων και φοιτητών και οι εις βάρος των Διοικήσεών τους απειλές που αφορούν τα πρόστιμα, τις προσφυγές και την ευθύνη. Υπενθυμίζεται ότι βάσει του ΓΚΠΔ κάθε υποκείμενο του οποίου τα προσωπικά δεδομένα έχουν παραβιαστεί ή έχει στερηθεί την άσκηση τυχόν απορρέοντος από τον κανονισμό δικαιώματός του, έχει δικαίωμα να προβεί σε καταγγελία στην ΑΠΔΠΧ[172] ή να προσφύγει δικαστικά κατά απόφασης αυτής που το αφορά (άρθρο 78 σε συνδυασμό με άρθρο 40 Ν. 4624/2019) ή κατά υπευθύνου επεξεργασίας ή εκτελούντος επεξεργασία (άρθρο 79), οι οποίοι ενέχονται εις ολόκληρον (αστική ευθύνη) για υλικές και μη ζημίες.

[171] Ο ρόλος αυτός προσδίδει έναν υψηλό βαθμό ανεξαρτησίας που επιβεβαιώνει ότι το πανεπιστήμιο δρα αντικειμενικά ως προς την επιβεβαίωση ότι τα προσωπικά δεδομένα τυγχάνουν υπεύθυνης επεξεργασίας, P. Mouncey, 2018, pp. 1-2.

[172] Αν ένα πανεπιστήμιο προβεί σε παράνομη επεξεργασία ή παραβιάσει καθ' οιονδήποτε τρόπο τον ΓΚΠΔ, η ΑΠΔΠΧ μπορεί να εκδώσει προειδοποίηση προς τον υπεύθυνο επεξεργασίας/εκτελούντα αυτή, αν διαπιστώσει παραβίαση μπορεί να προβεί σε σύσταση ή ακόμη και να διατάξει την προσωρινή ή οριστική επεξεργασία των συγκεκριμένων προσωπικών δεδομένων, να επιβάλει πρόστιμο βάσει του ΓΚΠΔ και της εθνικής νομοθεσίας (στην περίπτωση της Ελλάδας βάσει του άρθρου 39 ν. 4624/2019). Σε κάθε περίπτωση τα επιβαλλόμενα πρόστιμα πρέπει να είναι αποτελεσματικά, αναλογικά και αποτρεπτικά.

4.5.3. Αποτελέσματα έρευνας αναφορικά με τη συμμόρφωση των Πανεπιστημίων με τον ΓΚΠΔ

Διεξήχθη έρευνα με αντικείμενο διερεύνησης τη συμμόρφωση των ελληνικών πανεπιστημίων προς τις επιταγές του ΓΚΠΔ, σύμφωνα με τα προβλεπόμενα στη διεθνή βιβλιογραφία σε συνδυασμό με αναλυτική ανασκόπηση των ιστότοπων των Α.Ε.Ι.. Ειδικότερα αντικείμενο διερεύνησης αποτέλεσε το αν οι διοικήσεις των πανεπιστημίων έχουν προβεί σε διορισμό ΥΠΔ καθώς και στις απαιτούμενες ενέργειες συμμόρφωσης προς τον ΓΚΠΔ, αν έχουν υιοθετήσει πολιτικές προστασίας προσωπικών δεδομένων, αν έχουν διαμορφώσει ή επικαιροποιήσει τις διαδικασίες που εφαρμόζουν και τα αναρτημένα στους επίσημους ιστοτόπους τους έντυπα.

Όπως διαπιστώθηκε τα περισσότερα πανεπιστήμια έχουν καταρτίσει σχέδιο δράσης και έχουν προβεί στη λήψη μέτρων συμμόρφωσης. Συγκεκριμένα ορισμένα πανεπιστήμια υιοθετούν εκτενείς και πολυσέλιδους Οδηγούς συμμόρφωσης που εμπεριέχουν Κώδικα Δεοντολογίας, Πολιτικές προστασίας, διαδικασίες, οδηγίες ενημέρωσης, πρότυπα έντυπα αιτήσεων και ενδεικτικά κείμενα πληροφόρησης[173]. Τα περισσότερα βέβαια υιοθετούν μεμονωμένες Πολιτικές προστασίας και διαδικασίες ιδιωτικότητας και προστασίας δεδομένων προσωπικού χαρακτήρα, οι οποίες συνοδεύονται ενίοτε από έγγραφη δήλωση του Πανεπιστημίου περί συμμόρφωσης, έντυπο υποβολής αιτήματος του υποκειμένου των δεδομένων ενώ κάποια άλλα περιορίζονται στην ανάρτηση Δήλωσης απορρήτου.[174] Επίσης τα περισσότερα από τα ελληνικά πανεπιστήμια υιοθετούν ξεχωριστή Πολιτική για τα Cookies.

Οι Κώδικες Δεοντολογίας[175] αποσκοπούν στην ενίσχυση της τήρησης του σεβασμού των διατάξεων για την προστασία των προσωπικών δεδομένων εντός της ακαδημαϊκής κοινότητας. Επιδιώκουν να οριοθετήσουν τις γενικές κατευθύνσεις για την τήρηση των απορρεουσών από τον ΓΚΠΔ και από την εκάστοτε νομοθεσία, υποχρεώσεων. Συνιστούν δεσμευτικά κείμενα για το εκάστοτε ακαδημαϊκό ίδρυμα και συμβάλλουν στην ορθή εφαρμογή λαμβάνοντας υπόψη τα ιδιαίτερα χαρακτηριστικά του ΓΚΠΔ, την εθνική νομοθεσία, τις γενικές κατευθυντήριες γραμμές, γνωμοδοτήσεις της ΑΠΔΠΧ και του ΕΣΠΔ. Ισοδυναμούν με έμπρακτη ένδειξη συμμόρφωσης προς το ΓΚΔΠ ενώ συνήθως

[173] Το παράδειγμα αυτό ακολουθούν το Πανεπιστήμιο Πατρών καθώς και το Πανεπιστήμιο Κρήτης.
[174] Όπως το Διεθνές Πανεπιστήμιο της Ελλάδας και η Βιβλιοθήκη - Κέντρο Πληροφόρησης του Παντείου Πανεπιστημίου.
[175] Κώδικα Δεοντολογίας υιοθετεί το Πανεπιστήμιο Πατρών, βλ. σχετικά κατωτέρω σελ. 114-115.

αποτυπώνουν και ενισχύουν τις θεμελιώδεις αρχές επεξεργασίας δημιουργώντας ένα διαφανές πλαίσιο που τυγχάνει σεβασμού από το σύνολο της ακαδημαϊκής κοινότητας και συνδράμουν τους εργαζόμενους, τους συνεργάτες και φοιτητές να αντιλαμβάνονται το περιβάλλον εντός του οποίου ενσωματώνεται καθώς και τη γενικότερη κουλτούρα συνεργασίας που αποπνέει ο ΓΚΠΔ.

Οι πολιτικές προστασίας[176] επιδιώκουν να διευκολύνουν τη διαχείριση των προσωπικών δεδομένων από όλες τις διοικητικές μονάδες τους. Υιοθετούνται είτε μεμονωμένα είτε εμπεριέχονται σε Οδηγούς συμμόρφωσης. Συνιστούν ιδιαίτερες δράσεις των Πανεπιστημίων ανά τομέα με εξειδικευμένο αντικείμενο και επιδιώκουν να διασφαλίσουν πλήρως της προστασία όλων των μελών της ακαδημαϊκής κοινότητας, των συνεργατών και λοιπών ενδιαφερομένων μερών[177]. Συνοδεύονται από διαδικασίες και έγγραφα που ετοιμάζονται από τη νομική υπηρεσία του κάθε ιδρύματος ή από εξωτερικό νομικό σύμβουλο. Πολιτικές προστασίας ιδιωτικότητας και προστασίας προσωπικών δεδομένων έχουν υιοθετήσει τα περισσότερα πανεπιστήμια της χώρας. Συγκεκριμένα:

Η Ανωτάτη Σχολή Καλών Τεχνών (Α.Σ.Κ.Τ.) ορίζει ΥΠΔ[178], καθορίζει τα καθήκοντα του, γνωστοποιεί τα στοιχεία επικοινωνίας του και υιοθετεί πολιτική προστασίας προσωπικών δεδομένων, και παραπέμπει σε μια πολιτική προστασίας προσωπικών δεδομένων[179].

Το Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης (Α.Π.Θ.) ενημερώνει στον οικείο ιστότοπο ότι έχει προβεί στον ορισμό ΥΠΔ δυνάμει της ΑΔΑ: 6ΘΡ346Ψ8ΧΒ-0ΕΩ κατ' εφαρμογή των διατάξεων των άρθρων 37 έως και 39 ΓΚΠΔ[180]. Περαιτέρω υιοθέτησε Πολιτική Προστασίας προσωπικών δεδομένων βάσει του ΓΚΠΔ της ΕΕ (ΕΕ) 2016/679 και του Ν. 4624/2019[181], την οποία επιφυλάσσεται να επικαιροποιεί ή συμπληρώνει σύμφωνα με το εκάστοτε νομοθετικό και κανονιστικό πλαίσιο και εν συνεχεία να την αναρτά ώστε να είναι διαθέσιμη στο διαδικτυακό τόπο του ΑΠΘ. Επίσης, σε συμμόρφωση με το άρθρο 12 της από 11.3.2020 ΠΝΠ (Α'55), όπως αυτή κυρώθηκε με το Ν. 4682/2020 (ΦΕΚ 46/Α/3-4-2020), κατά την οποία η εκπαιδευτική διαδικασία των προπτυχιακών και μεταπτυχιακών

[176] Υποδειγματική πολιτική εύκολα προσαρμόσιμη στα δεδομένα ενός οργανισμού βρίσκεται δημοσιευμένη στην ιστοσελίδα της ENISA, διαθέσιμη στο https://www.enisa.europa.eu/about-enisa/privacy-policy
[177] Βλ. σχετικά μεταξύ άλλων και σε https://www.sans.org/security-resources/policies
[178] http://www.asfa.gr/dioikisi/upeuthhnos-gdpr-gr
[179] http://www.asfa.gr/images/prosopika-dedomena.pdf
[180] https://www.auth.gr/gdpr
[181] https://www.auth.gr/sites/default/files/politiki_prostasias_apth.pdf

προγραμμάτων σπουδών στα Α.Ε.Ι. δύναται να γίνεται με μέσα εξ αποστάσεως εκπαίδευσης για όσο διάστημα διαρκεί η προσωρινή απαγόρευση της εκπαιδευτικής λειτουργίας με φυσική παρουσία, το ΑΠΘ υιοθέτησε ξεχωριστή Πολιτική για την προστασία προσωπικών δεδομένων και τηλεκπαίδευση λόγω εκτάκτων μέτρων περιορισμού της διασποράς του κορονοϊού[182]. Βάσει αυτής το ΑΠΘ πραγματοποιεί εξ αποστάσεως διδασκαλία/τηλεκπαίδευση κατά την οποία λαμβάνει όλα τα απαραίτητα τεχνικά και οργανωτικά μέτρα για τη διασφάλιση της προστασίας των προσωπικών δεδομένων των φοιτητών. Κατά τη διεξαγωγή τηλεκπαίδευσης καταγράφονται η φωνή και η εικόνα, που συνιστούν προσωπικά δεδομένα του φοιτητή εν τη εννοία του ΓΚΠΔ και του Ν. 4624/2019. Ως εκ τούτου δίνεται η δυνατότητα στο φοιτητή να επιλέξει τις κατάλληλες ρυθμίσεις μη καταγραφής μέσω των πλατφορμών τηλεκπαίδευσης (π.χ. αποκλεισμός κάμερας, μικροφώνου κλπ). Εν προκειμένω η καταγραφή που συνιστά επεξεργασία, έχει ως νομιμοποιητική βάση τη συμμόρφωση του ΑΠΘ προς έννομη υποχρέωση που θέτει η ως άνω Π.Ν.Π. με τη λήψη κάθε πρόσφορου μέσου διαφύλαξης της ασφάλειας, ακρίβειας και εμπιστευτικότητας των δεδομένων, στα πλαίσια της οποίας απαγορεύεται η βιντεοσκόπηση, ηχογράφηση ή η με οποιονδήποτε τρόπο ανάρτηση σε ΜΚΔ. Επίσης το ΑΠΘ σε συμμόρφωση με ίδια ως άνω ΠΝΠ με την από 9-5-2020 Απόφαση της Συγκλήτου του ΑΠΘ για τη διενέργεια εξετάσεων του εαρινού εξαμήνου 2020 και τη με αριθμό 59181/Ζ1 απόφαση του Υφυπουργού Παιδείας και Θρησκευμάτων (ΦΕΚ 1935/20-5-2020, τ. Β), πραγματοποιεί εξ αποστάσεως εξετάσεις για το εαρινό εξάμηνο του ακαδημαϊκού έτους 2019-2020 με σκοπό την εκπλήρωση του καθήκοντός του προς το δημόσιο συμφέρον, όπως αυτό διατυπώνεται στο άρθρο 16 παρ. 5 Σ. και μπορεί να εκπληρωθεί κάτω από τις εξαιρετικές περιστάσεις της πανδημίας του κορωνοϊού. Για την εφαρμογή του ως άνω σκοπού υιοθέτησε Πολιτική για την τήρηση, συλλογή και επεξεργασία των προσωπικών δεδομένων κατά τη διενέργεια των εξετάσεων με τη χρήση εξ αποστάσεως μεθόδων αξιολόγησης[183]. Τέλος, το ΑΠΘ υιοθέτησε και ξεχωριστή Πολιτική για τα Cookies[184]. Από τα ως άνω αναφερόμενα αποδεικνύεται η πρόθεση της Διοίκησης του εν λόγω πανεπιστημίου να συμμορφωθεί πλήρως με τον ΓΚΠΔ. Οι δύο τελευταίες μάλιστα πολιτικές που υιοθετεί αποδεικνύουν ότι ακόμη και στην περίπτωση της πανδημίας, η προστασία των προσωπικών δεδομένων των φοιτητών δεν εκφεύγει της

[182] https://www.auth.gr/sites/default/files/dilosi_apth_gia_tilekpaideysi-1.pdf
[183] https://www.auth.gr/sites/default/files/politiki_exetaseon_.pdf
[184] https://www.auth.gr/cookie-policy

προσοχής της Διοίκησης του Πανεπιστημίου και παραμένει στα ζητήματα που επιδιώκει να διασφαλίσει.

Το Διεθνές Πανεπιστήμιο Ελλάδος (ΔΙ.ΠΑ.Ε) υιοθετεί Δήλωση Απορρήτου σύμφωνα με την οποία αναλαμβάνει τη δέσμευση τήρησης της πολιτικής προστασίας των δικαιωμάτων και ελευθεριών των ατόμων ως προς την επεξεργασία των προσωπικών δεδομένων τους σύμφωνα με το ΓΚΠΔ[185]. Περαιτέρω ορίζει ελεγκτή δεδομένων το ίδιο το πανεπιστήμιο. Προβλέπει τα σχετικά με τη διάρκεια επεξεργασίας, τα δικαιώματα των υποκειμένων, τη χρήση του ιστοτόπου σε παιδιά άνω των 16 ετών, την ανωνυμοποίηση, την καταγραφή κλήσεων για σκοπούς βελτίωσης ποιότητας, τη συγκατάθεση του υποκειμένου και την ανάκλησή της, τη δημιουργία προφίλ χρήστη, την κατάρτιση προφίλ εκδήλωσης και στις ειδικές κατηγορίες δεδομένων. Επίσης υιοθετεί ξεχωριστή πολιτική για τα cookies[186].

Το Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών (Ε.Κ.Π.Α.) συμμορφώνεται με τον ΓΚΠΔ μέσω Πολιτικής Ιδιωτικότητας και Προστασίας Δεδομένων Προσωπικού Χαρακτήρα την οποία υιοθέτησε το 2018 και στην οποία αναφέρει ρητά ότι η στάση της Διοίκησης του Πανεπιστημίου είναι να συμμορφωθεί προς το ΓΚΠΔ και μέσω της εν λόγω πολιτικής να είναι σε θέση να αποδεικνύει τη συμμόρφωσή της με το ΓΚΠΔ και άλλες σχετικές νομοθεσίες[187]. Περαιτέρω ορίζει ΥΠΔ και τεκμηριώνει την επιλογή του αυτή αναφέροντας τρεις σχετικούς δικαιολογητικούς λόγους στο κείμενο της Πολιτικής του ήτοι 1) ότι το πανεπιστήμιο είναι δημόσια αρχή, 2) εκτελεί επεξεργασίες μεγάλης κλίμακας και 3) επεξεργάζεται ιδιαίτερα ευαίσθητες κατηγορίες δεδομένων σε μεγάλη κλίμακα. Στο τελευταίο μάλιστα κεφάλαιο της Πολιτικής αναγράφεται και ο τρόπος με τον οποίο η Διοίκηση του ΕΚΠ εφαρμόζει τη Συμμόρφωση προς το ΓΚΠΔ. Τέλος υιοθετεί και πολιτική για τα Cookies[188].

Το Πανεπιστήμιο Δυτικής Αττικής (ΠΑ.Δ.Α.) υιοθετεί Πολιτική για τα Προσωπικά Δεδομένα στις εξ αποστάσεως εξετάσεις[189] για τα προσωπικά δεδομένα που συλλέγονται αναφορικά με την εν λόγω διαδικασία, στην οποία ρητά ορίζεται ότι *απαγορεύεται η με*

[185] https://www.ihu.gr/privacy-notice-el
[186] https://www.ihu.gr/cookies-el
[187] https://www.uoa.gr/fileadmin/user_upload/main_uoa_images/to_panepisthmio/PolitikiIdiwtikotitas_ProstasiasDedomenwn.pdf
[188] https://www.uoa.gr/fileadmin/user_upload/main_uoa_images/to_panepisthmio/Cookies_Policy_EKPA.pdf
[189] https://www.uniwa.gr/to-panepistimio/politikes-kanonismoi-diadikasies/politiki-gia-ta-prosopika-dedomena-stis-ex-apostaseos-exetaseis/

οποιονδήποτε τρόπο καταγραφή, βιντεοσκόπηση, ηχογράφηση, όπως επίσης η αναπαραγωγή, αναδημοσίευση της διαδικασίας αξιολόγησης και εξέτασης που διενεργείται μέσω σύγχρονης τηλεδιάσκεψης από οποιονδήποτε συμμετέχοντα. Σε περίπτωση παράβασης της άνω απαγόρευσης, προβλέπεται η άμεση κίνηση της διαδικασίας επιβολής όλων των νόμιμων κυρώσεων και ιδίως η άσκηση ποινικής δίωξης κατά του υπαιτίου. Περαιτέρω το ΠΑ.ΔΑ. υιοθετεί Δήλωση απορρήτου.

Το Πανεπιστήμιο Πατρών αναφέρεται στα προσωπικά δεδομένα με ένα εισαγωγικό έγγραφο πληροφόρησης για την προστασία των δεδομένων σύμφωνα με τον ΓΚΠΔ (ΕΕ) 2016/679 και τον Ν. 4624/2019[190]. Διαθέτει έναν εκτενέστατο Οδηγό συμμόρφωσης στο ΓΚΠΔ[191] που αποτυπώνει όλο το Πρόγραμμα Προστασίας Δεδομένων και το οποίο εμπεριέχει Κώδικα δεοντολογίας, Πολιτική προστασίας προσωπικών δεδομένων, Πολιτική προστασίας των εργαζομένων, Πολιτική για τη συλλογή και χρήση ευαίσθητων προσωπικών δεδομένων, Πολιτική συνεργατών πανεπιστημίου, αρμοδιότητες και καθήκοντα του ΥΠΔ, Διαδικασία διαχείρισης αιτημάτων φυσικών προσώπων, Διαδικασία για την διαχείριση συγκατάθεσης, Οδηγίες για τη διαχείριση ιστοτόπων και ενσωματωμένη Πολιτική cookies, ενδεικτικά κείμενα συγκατάθεσης κλπ. Περαιτέρω διαθέτει έναν εκτενή Οδηγό για την Ασφάλεια των Πληροφοριών[192], ο οποίος εμπεριέχει Security Plan, Οργανωτικά και Τεχνικά Μέτρα ασφαλείας καθώς και μέτρα φυσικής ασφαλείας. Το πλαίσιο συμμόρφωσης συμπληρώνεται από έντυπη-φόρμα υποβολής αιτήματος από το υποκείμενο των δεδομένων[193] καθώς και την με αριθμό πρωτ. 620/28181 και ΑΔΑ: Ψ5ΕΚ469Β7Θ-ΞΦΑ πράξη ορισμού ΥΠΔ[194]. Πρόκειται για ένα πρότυπο πλαίσιο συμμόρφωσης, το οποίο αποτελεί παράδειγμα προς μίμηση και για τα υπόλοιπα πανεπιστήμια.

Το Πανεπιστήμιο Κρήτης δηλώνει τη συμμόρφωση του στον ΓΚΠΔ με ένα αρχικό έγγραφο δυνάμει του οποίου ορίζει ΥΠΔ[195] γνωστοποιώντας το ονοματεπώνυμο και email επικοινωνίας μαζί της και παραπέμπει στον Οδηγό Συμμόρφωσης[196] που έχει υιοθετήσει

[190] http://www.upatras.gr/el/node/8947
[191] https://www.upatras.gr/sites/www.upatras.gr/files/odigos_symmorfosis_ston_gkpd.pdf
[192] https://www.upatras.gr/sites/www.upatras.gr/files/shedio_asfaleias_pliroforion.pdf
[193] https://www.upatras.gr/sites/www.upatras.gr/files/forma_ypovolis_aitimatos.pdf
[194] https://www.upatras.gr/sites/www.upatras.gr/files/orismos_ypeythynoy_prostasias_dedomenon_ypd_sto_panepistimio_patron_0.pdf
[195] https://www.uoc.gr/university/gdpr.html
[196] https://www.uoc.gr/files/items/7/7133/guidance_for_compliance_with_gdpr.pdf

και στο Έντυπο άσκησης δικαιώματος υποκειμένου δεδομένων. Ο οδηγός συμμόρφωσης είναι σαφής και κατατοπιστικός, αν και ίσως όχι τόσο εκτενής όσο του Πανεπιστημίου Πατρών, χωρίς ωστόσο να αφήνει αρρύθμιστα ζητήματα καθώς παραθέτει τις βασικές διατάξεις του ΓΚΠΔ και κάνει ρητή αναφορά στα δικαιώματα των υποκειμένων, τη συναίνεσή τους, την ενημέρωσή τους κατ' αρθ. 13 και 14 ΓΚΠΔ, τα μέτρα ασφαλείας και προστασίας των δεδομένων, το αρχείο δραστηριοτήτων επεξεργασίας, καθώς και την επεξεργασία για σκοπούς επιστημονικής έρευνας. Ιδιαιτέρως χρήσιμη κρίνεται η αναφορά στο τέλος του οδηγού σε FAQ επί των οποίων δίνονται και οι αντίστοιχες απαντήσεις. Ο οδηγός κλείνει με υποδείγματα εντύπων (έντυπο ενημέρωσης για συλλογή, για φωτογράφηση/βιντεοσκόπηση σε εξέλιξη ή για φωτογράφιση ή βιντεοσκόπηση πριν τη φωτογράφηση)[197]. Έντυπο υποβολής αίτησης άσκησης δικαιώματος από το υποκείμενο των δεδομένων (άρθρα 15-22 ΓΚΠΔ) παρατίθεται ξεχωριστά στον επίσημο ιστότοπο του πανεπιστημίου.

Το Πολυτεχνείο Κρήτης προβαίνει σε συνοπτική Ενημέρωση για την Προστασία των Προσωπικών Δεδομένων, αναφέροντας ότι το ίδιο λειτουργεί ως Υπεύθυνος Επεξεργασίας. Υιοθετεί Πολιτική Προστασίας Ιδιωτικότητας-Δεδομένα προσωπικού Χαρακτήρα[198], στην οποία ουσιαστικά αναπαράγει τις βασικότερες διατάξεις του ΓΚΠΔ. Στο τέλος της Πολιτικής αναφέρεται ως χρόνος διατήρησης των δεδομένων εκείνος που απαιτείται είτε βάσει της συναλλακτικής σχέσης που συνδέει το Υποκείμενο με το Πολυτεχνείο είτε βάσει της εθνικής νομοθεσίας. Περαιτέρω παραπέμπει σε έντυπο-φόρμα

[197] Ειδικότερα ως προς την βιντεοσκόπηση είχε υποβληθεί στο παρελθόν στην ΑΠΔΠΧ η υπ' αριθμ. πρωτ. Γ/ΕΙΣ/3190/22-05-2014 καταγγελία φοιτητή κατά την οποία σε αμφιθέατρα του Πανεπιστημίου Κρήτης είχαν τοποθετηθεί κάμερες για τα «Ανοικτά Ακαδημαϊκά Μαθήματα του Πανεπιστημίου Κρήτης», χωρίς προηγούμενη ενημέρωση της ακαδημαϊκής κοινότητας και χωρίς την αίτηση και λήψη της προγενέστερης συγκατάθεσης φοιτητών και καθηγητών. Επί της εν λόγω καταγγελίας η ΑΠΔΠΧ εξέδωσε την με αριθμό 77/2016 απόφασή της κατά την οποία απεύθυνε βάσει του άρθρου 19 παρ. 1 στ΄ και 21 παρ. 1 α΄ ν. 2472/1997, αυστηρή προειδοποίηση στο Πανεπιστήμιο Κρήτης για την παραβίαση του άρθρου 6 ν. 2472/1997, καθώς και αυστηρή προειδοποίηση να προβεί εντός ευλόγου χρονικού διαστήματος στις απαραίτητες ενέργειες για σύννομη λειτουργία των εν λόγω καμερών σύμφωνα με τις προϋποθέσεις νόμιμης λειτουργίας που παρέθετε στο σημείο 9 του σκεπτικού της, ενημερώνοντας σχετικά την Αρχή. Βλ. σχετικά υπ' αρ. 77/2016 απόφαση ΑΠΔΠΧ διαθέσιμη σε: https://www.dpa.gr/sites/default/files/2019-10/77_2016anonym_0.pdf

[198] https://www.tuc.gr/fileadmin/various/privacy/%CE%A0%CE%BF%CE%BB%CE%B9%CF%84%CE%B9%CE%BA%CE%AE_%CE%A0%CF%81%CE%BF%CF%83%CF%84%CE%B1%CF%83%CE%AF%CE%B1%CF%82_%CF%84%CE%B7%CF%82_%CE%99%CE%B4%CE%B9%CF%89%CF%84%CE%B9%CE%BA%CF%8C%CF%84%CE%B7%CF%84%CE%B1%CF%82_%CE%BA%CE%B1%CE%B9_%CF%84%CF%89%CE%BD_%CE%A0%CF%81%CE%BF%CF%83%CF%89%CF%80%CE%B9%CE%BA%CF%8E%CE%BD_%CE%94%CE%B5%CE%B4%CE%BF%CE%BC%CE%AD%CE%BD%CF%89%CE%BD.pdf

υποβολής αιτήματος από το υποκείμενο των δεδομένων. Επίσης εμπεριέχει ξεχωριστή Πολιτική cookies[199].

Το Πανεπιστήμιο Ιωαννίνων περιορίζεται στον ορισμό ΥΠΔ γνωστοποιώντας τα στοιχεία της και τα στοιχεία επικοινωνίας μαζί του και σε μια σύντομη αναφορά στα προσωπικά δεδομένα, την διάκρισή τους σε απλά και ειδικών κατηγοριών, βάσει του ΓΚΠΔ, την παράθεση των ορισμών του ΓΚΠΔ, παραπέμποντας ευθέως τα υποκείμενα στο κείμενο του κανονισμού και στον εθνικό κυρωτικό Ν. 4624/2019, τον οποίο αναρτά στα αρχεία-συνδέσμους[200].

Το Δημοκρίτειο Πανεπιστήμιο Θράκης (Δ.Π.Θ.) διαθέτει ένα πλήρες πλαίσιο συμμόρφωσης προς τον ΓΚΠΔ. Στην εισαγωγική της αναφορά για την προστασία των δεδομένων κάνει λόγο για την υπ' αριθ. 33/16/4-07-2019 απόφαση της Συγκλήτου του Δ.Π.Θ. βάσει της οποίας εγκρίθηκαν τα κείμενα και οι ενέργειες δημοσιοποίησης στην ιστοσελίδα του ΔΠΘ που αφορούν στον ΓΚΠΔ. Κατά συνέπεια αποδεικνύει ότι διαθέτει ένα ολοκληρωμένο Πρόγραμμα για την Προστασία των Δεδομένων Προσωπικού Χαρακτήρα για να εξασφαλιστεί πλήρως η προστασία των φοιτητών, εργαζομένων, συνεργατών και όλων των ενδιαφερομένων μερών. Ορίζει ΥΠΔ παραθέτοντας τα στοιχεία της και τα στοιχεία επικοινωνίας μαζί της, και προβλέποντας ότι είναι υπεύθυνη για τον έλεγχο και τη βελτίωση των απαραίτητων πολιτικών και διαδικασιών για την προστασία των προσωπικών δεδομένων, και ότι στόχος της είναι η διαρκής βελτίωση της συμμόρφωσης του Πανεπιστημίου με το ΓΚΠΔ. Εν συνεχεία παραθέτει τα σχετικά με την προστασία των δεδομένων κείμενα, ήτοι τη Δέσμευση του πανεπιστημίου για τον ΓΚΠΔ[201], Ενημέρωση για τον ΓΚΠΔ[202], Πολιτική Προστασίας της Ιδιωτικότητας και των Προσωπικών Δεδομένων[203] η οποία έχει κοινοποιηθεί στο σύνολο της ακαδημαϊκής κοινότητας και σε όλα τα εμπλεκόμενα τρίτα ή ενδιαφερόμενα μέρη και συνιστά κατά κύριο λόγο αναπαραγωγή των βασικότερων διατάξεων του ΓΚΠΔ, του Νόμου 4624/2019

[199] https://www.tuc.gr/index.php?id=10652
[200] Βλ. επίσημο ιστότοπο: https://www.uoi.gr/dioikisi/gdpr/
[201] Η δέσμευση του ΔΠΘ στην Προστασία των Προσωπικών Δεδομένων αποδεικνύεται με την υλοποίηση Προγράμματος Προστασίας Προσωπικών Δεδομένων και την παροχή των απαραίτητων πόρων για την εφαρμογή και την ανάπτυξη αποτελεσματικών τεχνικών και οργανωτικών μέτρων. Το ΔΠΘ φροντίζει για τη διεξαγωγή, σε τακτική βάση, επιθεώρησης της απόδοσης του προγράμματος προστασίας και κατάλληλης αναθεώρησης όλων των σχετικών πολιτικών και διαδικασιών, βλ. σχετικά σε https://duth.gr/Portals/0/%20%20%20%20%20%20%281%29.pdf
[202] https://duth.gr/Portals/0/Enhmerosi%20kanonismos.pdf
[203] https://duth.gr/Portals/0/Privacy_Policy.pdf

για τα προσωπικά δεδομένα, Συστάσεις αναφορικά με την τηλεκπαίδευση[204], Εισήγηση αναφορικά με την εξ αποστάσεως εξέταση[205] και Πολιτική προστασίας τους κατά τη χρήση εξ αποστάσεως μεθόδων αξιολόγησης, στην οποία αναφέρεται μεταξύ άλλων ότι το ΔΠΘ ως υπεύθυνος επεξεργασίας προέβη βάσει του άρθρου 35 και σε εκπόνηση DPIA για την προστασία των προσωπικών δεδομένων που θα τύχουν επεξεργασίας στα πλαίσια των εξ αποστάσεως μεθόδων αξιολόγησης των φοιτητών.

Το Πάντειο Πανεπιστήμιο Κοινωνικών και Πολιτικών Επιστημών υιοθετεί Πολιτική Απορρήτου[206] δίνοντας οδηγίες και συστάσεις σχετικά με τη χρήση των πολυμέσων, των cookies, το ενσωματωμένο περιεχόμενο από άλλους ιστότοπους, τον διαδραστικό χάρτη, τα βίντεο, παραπέμποντας στις επιμέρους πολιτικές ιδιωτικότητας, ενώ ρητή αναφορά γίνεται και στα αρχεία καταγραφής, για τα οποία διευκρινίζεται ότι, παρότι συλλέγονται δεδομένα όπως η IP address και ο user agent, αυτά διαβιβάζονται σε εξουσιοδοτημένο και ρητά ονομαζόμενο στην Δήλωση Απορρήτου, εξωτερικό συνεργάτη της Διεύθυνσης Μηχανοργάνωσης και αποσαφηνίζεται ότι σε καμία περίπτωση τα εν λόγω δεδομένα δεν συνδέονται με προσωποποιημένες (ταυτοποιημένες) πληροφορίες.

Η Βιβλιοθήκη και το Κέντρο Πληροφόρησης (Βι.ΚεΠ.) του Παντείου Πανεπιστημίου υιοθετούν επίσης Πολιτική Απορρήτου[207] με Δήλωση Προστασίας για τα προσωπικά δεδομένα, βάσει της οποίας η ΒιΚεΠ αναγνωρίζει τη σημασία των προσωπικών δεδομένων των μελών, επισκεπτών,-τριων και δεσμεύεται για την προστασία τους, σε συμμόρφωση με το ισχύον κανονιστικό πλαίσιο για την προστασία δεδομένων προσωπικού χαρακτήρα.

---

[204] Αυτές αφορούν κυρίως στην επεξεργασία που γίνεται μέσω καταγραφής (φωνής, εικόνας ή ανάρτησης προσωπικών δεδομένων. Πριν την επεξεργασία πρέπει να ενημερώνονται οι φοιτητές για τους σκοπούς, τη νόμιμη βάση, το χρόνο διατήρησης του αρχείο καταγραφής και του χρόνου ανάρτησης, τα δικαιώματά τους κλπ και φοιτητές και διδάσκοντες να χορηγούν τη συγκατάθεσή τους, βλ. σχετικά σε https://duth.gr/Portals/0/%20%20%20%20%20%20%20%20%20%20.pdf

[205] Σ' αυτήν αναφέρονται ποια δεδομένα συλλέγονται και πότε καθώς και για πόσο χρονικό διάστημα διατηρούνται κατά περίπτωση, βλ. σχετικά σε https://duth.gr/Portals/0/GDPRex20_1.pdf

[206] https://www.panteion.gr/politiki-aporritou/

[207] https://library.panteion.gr/%CF%80%CE%BB%CE%B7%CF%81%CE%BF%CF%86%CE%BF%CF%81%CE%AF%CE%B5%CF%82/%CE%B4%CE%AE%CE%BB%CF%89%CF%83%CE%B7-%CF%80%CF%81%CE%BF%CF%83%CF%84%CE%B1%CF%83%CE%AF%CE%B1%CF%82-%CF%80%CF%81%CE%BF%CF%83%CF%89%CF%80%CE%B9%CE%BA%CF%8E%CE%BD-%CE%B4%CE%B5%CE%B4%CE%BF%CE%BC%CE%AD/

Το Πανεπιστήμιο Πειραιώς (ΠΑ.ΠΕΙ.)[208] στην δήλωσή της για την προστασία Δεδομένων Προσωπικού Χαρακτήρα εμπεριέχει όλα τα έγγραφα που αφορούν στο πλαίσιο της συμμόρφωσης που διαθέτει και συγκεκριμένα Ενημέρωση των υποκειμένων των προσωπικών δεδομένων, Δελτίο Τύπου για την επεξεργασία δεδομένων προσωπικού χαρακτήρα στο πλαίσιο της διαχείρισης του COVID-19, Κατευθυντήριες Γραμμές για την Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα στο πλαίσιο της Διαχείρισης του COVID-19 ενώ υιοθετεί εκτενή Πολιτική Ιδιωτικότητας και Προστασίας Δεδομένων[209], έντυπο συγκατάθεσης για συμμετοχή σε επιστημονική έρευνα[210], έντυπο άσκησης δικαιωμάτων υποκειμένων των δεδομένων[211] και έντυπο αίτησης ανάκλησης συγκατάθεσης των υποκειμένων των δεδομένων[212].

Το Πανεπιστήμιο Μακεδονίας (ΠΑ.ΜΑΚ.) στην αρχική σελίδα του για τα προσωπικά δεδομένα, αναφέρει ότι υιοθετεί Πολιτική Προστασίας Δεδομένων Προσωπικού Χαρακτήρα[213], η οποία αφού εγκρίθηκε στα πλαίσια της υπ' αριθ. 8/3.12.2020 συνεδρίαση του Πρυτανικού Συμβουλίου, καθορίζει και διατυπώνει το κανονιστικό πλαίσιο και τις αρχές που εφαρμόζει το Πανεπιστήμιο, αναφορικά με την επεξεργασία των προσωπικών δεδομένων και την προστασία της ασφάλειας, της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητάς τους, και, ενημερώνει, τους χρήστες/επισκέπτες σχετικά με τον τρόπο συλλογής, χρήσης και κοινοποίησης των προσωπικών τους δεδομένων[214]. Επιπλέον υιοθετεί ξεχωριστή Πολιτική για τα cookies[215].

Το Πανεπιστήμιο Δυτικής Μακεδονίας υιοθετεί Πολιτική Προστασίας Προσωπικών Δεδομένων[216] με εισαγωγική Δήλωση Εφαρμογής του ΓΚΠΔ χωρίς να προβαίνει σε περαιτέρω ιδιαίτερες διατυπώσεις σχετικά με την προστασία των δεδομένων πλην των αναφερομένων στον κανονισμό.

---

[208] https://www.unipi.gr/unipi/el/gdpr.html
[209] https://www.unipi.gr/unipi/images/various/GDPR/UNIPI_GDPR_privacy_policy_short.pdf
[210] https://www.unipi.gr/unipi/images/various/GDPR/Entupo_dilwsis_sugkatathesis_gia_epistimoniki_ereuna.pdf
[211] https://www.unipi.gr/unipi/images/various/GDPR/Entupo_askisis_twn_dikaiomatwn_twn_upokeimenwn_twn_dedomenwn.pdf
[212] https://www.unipi.gr/unipi/images/various/GDPR/Entupo_aitisis_anaklisis_sugkatathesis_twn_upokeimenwn_twn_dedomenwn.pdf
[213] https://www.uom.gr/downloads/terms/Politiki-Prostasias-UOM.pdf
[214] https://www.uom.gr/terms
[215] https://www.uom.gr/downloads/terms/Potlitiki-Cookies-UOM.pdf
[216] https://www.uowm.gr/to-panepistimio/politiki-poiotitas/politiki-prostasias-prosopikon-dedomenon/

Το Πανεπιστήμιο Πελοποννήσου (ΠΑ.ΠΕΛ.)[217] στην αρχική σελίδα περιορίζεται στο να αναρτήσει Πολιτική Προσωπικών Δεδομένων η οποία συνοψίζεται σε μια δήλωση ότι *το Πανεπιστήμιο δεσμεύεται να προστατεύει και να σέβεται την ιδιωτικότητα των χρηστών των ηλεκτρονικών υπηρεσιών του, και συμμορφώνεται με το Γενικό Κανονισμό για την Προστασία Δεδομένων (Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016), ότι δεν προτίθεται να αποκαλύπτει προσωπικά δεδομένα σε τρίτους και ότι εφαρμόζει εύλογες πολιτικές και τεχνικά και οργανωτικά μέτρα, προκειμένου να προστατεύει τα προσωπικά δεδομένα των χρηστών*, χωρίς ωστόσο να τις εξειδικεύει ή να τις παραθέτει.

Το Πανεπιστήμιο Αιγαίου [218] στην αρχική του σελίδα ορίζει ότι η Πολιτική Προστασίας Δεδομένων αποτυπώνει την πρόθεση του Πανεπιστημίου να προστατέψει τα προσωπικά δεδομένα που τελούν υπό επεξεργασία, έτσι ώστε να επιτυγχάνεται η συμμόρφωση με τις απαιτήσεις του ΓΚΠΔ 2016/679 και περιλαμβάνει τον σκοπό και τους επιμέρους στόχους που θέτει η Διοίκηση αναφορικά με την προστασία δεδομένων προσωπικού χαρακτήρα, καθώς και τις οδηγίες, διαδικασίες, κανόνες, ρόλους και υπευθυνότητες που αφορούν τόσο στην προστασία των δεδομένων αυτών όσο και στην ιδιωτικότητα των υποκειμένων των δεδομένων. Η εφαρμογή της Πολιτικής αυτής έχει δεσμευτικό χαρακτήρα για όλα τα μέλη του Ιδρύματος που μετέχουν (άμεσα ή έμμεσα) στην επεξεργασία δεδομένων προσωπικού χαρακτήρα και αφορά στο σύνολο των συγκεκριμένων δεδομένων, τα οποία επεξεργάζεται το Πανεπιστήμιο Αιγαίου, με αυτοματοποιημένα ή μη αυτοματοποιημένα μέσα. Στα πλαίσια της υπ' αριθ. 11/12.06.2020 συνεδρίασης της Συγκλήτου το Πανεπιστήμιο Αιγαίου υιοθέτησε ένα μακροσκελέστατο και αναλυτικότατο κείμενο 127 σελίδων, το οποίο αποτυπώνει τις «Πολιτικές και Διαδικασίες Προστασίας Δεδομένων Προσωπικού Χαρακτήρα»[219] το οποίο διαρθρώνεται σε 3 Μέρη. Στο Α΄ Μέρος περιγράφεται η Πολιτική Προστασίας Δεδομένων, στο Β' Μέρος αναλύονται οι διαδικασίες που ακολουθεί το Πανεπιστήμιο στα Πλαίσια της Εφαρμογής της Πολιτικής προστασίας Δεδομένων ενώ το Γ' Μέρος εμπεριέχονται τα Παραρτήματα, ήτοι τα Έντυπα που χρησιμοποιεί το Πανεπιστήμιο για τη δήλωση συγκατάθεσης, την ανάκληση αυτής, την

[217] https://www.uop.gr/arxiki/prosopika-dedomena
[218] https://www.aegean.gr/%CF%80%CE%BF%CE%BB%CE%B9%CF%84%CE%B9%CE%BA%CE%AE-%CF%80%CF%81%CE%BF%CF%83%CF%84%CE%B1%CF%83%CE%AF%CE%B1%CF%82-%CE%B4%CE%B5%CE%B4%CE%BF%CE%BC%CE%AD%CE%BD%CF%89%CE%BD-%CF%84%CE%BF%CF%85-%CE%B9%CE%B4%CF%81%CF%8D%CE%BC%CE%B1%CF%84%CE%BF%CF%82-gdpr
[219] https://www.aegean.gr/sites/default/files/static/20/09/uaegean_gdpr.pdf

αναφορά περιστατικού παραβίασης των δεδομένων, την άσκηση των δικαιωμάτων και ειδικό έντυπο για την άσκηση του δικαιώματος ενημέρωσης, πρόσβασης, διαχείρισης αιτήματος, Στο Γ' Μέρος παρατίθενται επίσης μέχρι και υποδείγματα αρχείων για τις δραστηριότητες επεξεργασίας, φόρμα ανάλυσης και αξιολόγησης περιστατικού παραβίασης δεδομένων, και έντυπο συγκατάθεσης για επιστημονική έρευνα.

Αποτελεί ουσιαστικά την πληρέστερη προσέγγιση στο ζήτημα της συμμόρφωσης με το ΓΚΠΔ, ένα κείμενο υποδειγματικό, συγκεντρωτικό που δεν αφήνει περιθώρια αμφιβολίας ως προς το περιεχόμενό του ενώ διευθετεί κάθε ζήτημα που ήθελε προκύψει σε περίπτωση επέλευσης περιστατικού παραβίασης. Περιέχει ακόμη ενσωματωμένη και την Πολιτική για τα cookies με αποτέλεσμα, αν και δεν έχει την τυπική και εξωτερική μορφή Οδηγού, να λειτουργεί ως οδηγός συμμόρφωσης, παρέχοντας ένα ενιαίο πλαίσιο για την προστασία των δεδομένων και συνδράμωντας το υποκείμενο να κατανοήσει εις βάθος όχι μόνον τον κανονισμό αλλά και τις πτυχές της συμμόρφωσης στις επιταγές του.

Το Ιόνιο Πανεπιστήμιο υιοθέτησε με την από 20-01-2021 εγκριτική απόφαση της Συγκλήτου μια Ιδρυματική Πολιτική Προστασίας Δεδομένων και Ιδιωτικότητας[220], η οποία ουσιαστικά αναπαράγει τις βασικές διατάξεις του ΓΚΠΔ, στην οποία επισυνάπτεται στο τέλος και μια Φόρμα Υποβολής Αιτήματος από το Υποκείμενο των δεδομένων[221]. Η πολιτική για την προστασία των δεδομένων που ακολουθεί το συγκεκριμένο πανεπιστήμιο αντικατοπτρίζει τη συνήθη τακτική που ακολουθούν τα περισσότερα ακαδημαϊκά ιδρύματα στα πλαίσια της συμμόρφωσης με τον ΓΚΠΔ χωρίς ιδιαίτερες διατυπώσεις. Περαιτέρω το Ιόνιο πανεπιστήμιο υιοθετεί ξεχωριστή Πολιτική για τα Cookies[222].

Το Ελληνικό Ανοικτό Πανεπιστήμιο (Ε.Α.Π.) στη σελίδα για την Ομάδα Προστασίας των Δεδομένων [223] αναφέρει ότι όρισε από το Μάιο 2018 Ομάδα Προστασίας Δεδομένων, με σκοπό την λήψη κατάλληλων μέτρων και αποφάσεων, ώστε να προστατεύεται η εμπιστευτικότητα, η ακεραιότητα, η διαθεσιμότητα και η σύννομη επεξεργασία των δεδομένων προσωπικού χαρακτήρα, όπως προβλέπει ο ΓΚΠΔ και η εθνική νομοθεσία και ορίζει υπεύθυνο επεξεργασίας και ΥΠΔ γνωστοποιώντας τα στοιχεία επικοινωνίας. Υιοθετεί μια σύντομη Πολιτική Προστασίας Προσωπικών Δεδομένων με ένα ακόμη κείμενο το οποίο αποτυπώνει τις βασικές έννοιες και διατάξεις του ΓΚΠΔ.

[220] https://gdpr.ionio.gr/gr/policy/privacy-policy/
[221] file:///C:/Users/user/Downloads/IU-pf-01589-13001-gr%20(1).pdf
[222] https://gdpr.ionio.gr/gr/policy/cookies/
[223] https://www.eap.gr/data-protection-team/

Η Ανώτατη Σχολή Παιδαγωγικής και Τεχνολογικής Εκπαίδευσης (Α.Σ.ΠΑΙ.Τ.Ε.) [224] προβαίνει σε Ενημέρωση[225] της Α.Σ.ΠΑΙ.Τ.Ε. για την Προστασία των Προσωπικών Δεδομένων σύμφωνα με τον Κανονισμό (ΕΕ) 2016/679 και τη σχετική ελληνική νομοθεσία και υιοθετεί μια Πολιτική για την Ιδιωτικότητα και την Προστασία των Προσωπικών Δεδομένων[226], πανομοιότυπη με κείνη του ΕΚΠΑ. Συνοδεύεται από φόρμα υποβολής αιτήματος[227] από το υποκείμενο των δεδομένων ακολουθώντας το μοντέλο των περισσοτέρων πανεπιστημίων ως προς το συγκεκριμένο έντυπο, και τέλος υιοθετεί ξεχωριστή πολιτική cookies[228].

Το Ελληνικό Μεσογειακό Πανεπιστήμιο (ΕΛ.ΜΕ.ΠΑ.) (πρώην Τ.Ε.Ι. Κρήτης)[229] υιοθετεί Πολιτική προστασίας δεδομένων προσωπικού χαρακτήρα για να κοινοποιούνται προς κάθε ενδιαφερόμενο ή εμπλεκόμενο στις διαδικασίες διαχείρισης δεδομένων οι βασικές αρχές του Πανεπιστημίου, αναφέρεται στον ευρύτερο στρατηγικό σχεδιασμό για την προστασία τους και παραθέτει τους μηχανισμούς, τις διαδικασίες και τα ληφθέντα μέτρα. Στο τέλος αυτής αναγράφει τα στοιχεία της ΕΠΕ στην οποία έχει αναθέσει χρέη ΥΠΔ.

Το Πανεπιστήμιο Θεσσαλίας υιοθετεί Πολιτική Απορρήτου[230] για την προστασία προσωπικών δεδομένων στην οποία δηλώνει ότι το ίδιο το Πανεπιστήμιο είναι Υπεύθυνος Επεξεργασίας των προσωπικών δεδομένων που αντλούνται κατά την πλοήγηση στον διαδικτυακό ιστότοπο της Διεύθυνσης Μηχανοργάνωσης του ΠΘ (https://it.uth.gr) ενώ Υπεύθυνος Προστασίας Δεδομένων είναι η εταιρεία Priority Quality Consultants S.A. στην ηλεκτρονική διεύθυνση dpo@uth.gr. Επιπλέον το Πανεπιστήμιο Θεσσαλίας προβαίνει σε Ενημέρωση για την επεξεργασία των προσωπικών δεδομένων μέσω του συστήματος βιντεοεπιτήρησης[231] και Ενημέρωση φυσικών προσώπων σχετικά με την

[224] https://www.aspete.gr/index.php/el/29-2014-02-01-22-33-17/2014-02-01-22-38-47/2014-02-15-19-04-22/1262-gdpr.html
[225] http://files.aspete.gr/aspete/noc/GDPR/Kanonismos_privacy%20notice.pdf
[226] http://files.aspete.gr/aspete/noc/GDPR/Idiotikotika-Kai_Prostasia_Dedomenon.pdf
[227] https://www.aspete.gr/index.php/el/29-2014-02-01-22-33-17/2014-02-01-22-38-47/2014-02-15-19-04-22/1262-gdpr.html
[228] http://files.aspete.gr/aspete/noc/GDPR/Cookies_ASPETE.pdf
[229] https://www.hmu.gr/el/hmu/16346
[230] https://www.uth.gr/privacypolicy.
[231] https://www.uth.gr/videoepitirisi_uth. Στην εν λόγω ενημέρωση γνωστοποιείται ότι Υπεύθυνος Επεξεργασίας των δεδομένων προσωπικού χαρακτήρα που υπόκεινται σε επεξεργασία στα πλαίσια της λειτουργίας του συστήματος βιντεοεπιτήρησης είναι το ίδιο το Πανεπιστήμιο, η διεύθυνση είναι Αργοναυτών & Φιλελλήνων Τ.Κ. 38221 Βόλος, το τηλ. επικοινωνίας είναι +30 2421074000 ενώ Υπεύθυνος Προστασίας Προσωπικών Δεδομένων είναι και πάλι η εταιρεία Priority Quality Consultants S.A. στην ηλεκτρονική διεύθυνση-email: dpo@uth.gr .Τα προσωπικά δεδομένα που συλλέγονται είναι δεδομένα εικόνας (βίντεο), τα οποία διατηρούνται για χρονικό διάστημα 72 ωρών και η νομική βάση είναι η

επεξεργασία των δεδομένων κατά τη διενέργεια εξ αποστάσεως εξετάσεων[232]. Περαιτέρω έχει αναρτήσει στον επίσημο διαδικτυακό ιστότοπό του τεσσάρων περίπου λεπτών βίντεο ευαισθητοποίησης[233] για το ΓΚΠΔ ενώ διοργανώνει Ημερίδες GDPR για την ακαδημαϊκή κοινότητα[234]. Τέλος διαθέτει και ξεχωριστά αναρτημένη Πολιτική για τα Cookies, στην οποία παρατίθεται πίνακας με το είδος των cookies που χρησιμοποιούνται, το χρόνο τήρησής τους και τον αποδέκτη ή την κατηγορία αποδεκτών των δεδομένων αυτών.[235]

Το Χαροκόπειο Πανεπιστήμιο γνωστοποιεί δια του ιστοτόπου του ότι ΥΠΔ είναι το ίδιο το Πανεπιστήμιο, ήτοι παραθέτοντας στα στοιχεία ΥΠΔ το email dpo@hua.gr χωρίς να φαίνεται να υιοθετεί κάποια ιδιαίτερη Πολιτική προστασίας για γα προσωπικά δεδομένα[236].

Η Ανώτατη Σχολή Τουριστικής Εκπαίδευσης Ρόδου υιοθετεί Πολιτική για τα cookies[237] ενώ η Ανώτατη Σχολή Τουριστικής Εκπαίδευσης Κρήτης[238] δεν αναρτά στον επίσημο ιστότοπό της καμία πολιτική προστασίας για τα προσωπικά δεδομένα ούτε γνωστοποιεί στοιχεία υπευθύνου προστασίας δεδομένων.

επεξεργασία προς εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στο Πανεπιστήμιο.

[232] Η από 26-01-2021 υπ' αριθ. πρωτ. 1106/21/ΓΠ απόφαση του Πανεπιστημίου απευθυνόμενη στην ακαδημαϊκή κοινότητα, ορίζει τους ίδιους ως άνω, ως Υπεύθυνους Επεξεργασίας και Προστασίας Δεδομένων αντίστοιχα, απαριθμεί επακριβώς ποια δεδομένα επεξεργάζεται το Πανεπιστήμιο στα πλαίσια της εν λόγω δράσης και σε ποια νομιμοποιητική βάση επεξεργασίας στηρίζεται, δηλώνει ότι έχει λάβει τα κατάλληλα τεχνικά και οργανωτικά μέτρα και έχει προβεί σε Μελέτη Εκτίμησης Αντικτύπου, καθώς και ότι τηρεί αρχεία καταγραφής συμβάντων των υποδομών για επαρκές χρονικό διάστημα. Τέλος διασφαλίζει ότι έχει αποκλειστεί η λειτουργικότητά τους για καταγραφή εικόνας και ήχου προς διασφάλιση της προστασίας των δεδομένων των μετεχόντων στην εν λόγω διαδικασία και απαγορεύει ρητά την βιντεοσκόπηση, την ηχογράφηση, την με οποιονδήποτε τρόπο δημοσίευση, κοινοποίηση, ανάρτηση ή διανομή εν μέρει ή εν όλω της εν λόγω εξεταστικής διαδικασίας εκ μέρους των μετεχόντων.

[233] Διαθέσιμο σε: https://www.uth.gr/news/gkppd-gdpr-binteo-eyaisthitopoiisis

[234] Με πιο πρόσφατη αυτή που έλαβε χώρα στις 18 και 20 Ιανουαρίου 2021 με σκοπό τη διενέργεια δράσεων ευαισθητοποίησης και ενημέρωσης του συνόλου των μελών της ακαδημαϊκής κοινότητας σε θέματα προσωπικών δεδομένων, η οποία ολοκληρώθηκε σε πέντε παρουσιάσεις σε ευρύ κοινό με τη χρήση της πλατφόρμας MS-teams λόγω των ιδιαίτερων συνθηκών της περιόδου. Στις παρουσιάσεις αναλύθηκαν τα εξής ζητήματα : Ορισμοί και Βασικές αρχές του ΓΚΠΔ, ασφάλεια δεδομένων και παραβιάσεις, Πολιτικές και Διαδικασίες- Οδηγίες GDPR στο Πανεπιστήμιο Θεσσαλίας ενώ παρουσιάστηκε κι ένα ενημερωτικό video. Η τελευταία παρουσίαση αναφερόταν στις Καλές πρακτικές και τη χρήση των social media. Βλ. σχετικά σε: https://www.uth.gr/academicnews/imerides-gdpr-gia-tin-akadimaiki-koinotita-pth

[235] https://www.uth.gr/cookiespolicy

[236] https://www.hua.gr/index.php/el/

[237] https://asterodos.edu.gr/cookie-policy/

[238] http://astecrete.edu.gr/

Το Οικονομικό Πανεπιστήμιο Αθηνών (Ο.Π.Α.) με το από 3-12-2019 δελτίο τύπου[239] του αναφέρεται σε ένα νέο καινοτόμο λογισμικό που δημιουργήθηκε κατόπιν πανεπιστημιακής έρευνας διεξαχθείσας στο ΟΠΑ για την προστασία των προσωπικών δεδομένων. Δοθέντος ότι τα δεδομένα προσωπικού χαρακτήρα που επεξεργάζονται οι διάφορες ηλεκτρονικές εφαρμογές δεν μπορούν να ελεγχθούν αποτελεσματικά από τα υποκείμενά τους με αποτέλεσμα να δημιουργούνται τακτικά φαινόμενα διαρροών τους, το ΟΠΑ ακολουθώντας τη προστασία από το σχεδιασμό αναπτύσσει την αρχιτεκτονική ενός λογισμικού που λέγεται PDGuard και η οποία χρησιμοποιεί στοιχεία της τεχνολογίας λογισμικού σε συνδυασμό με την εφαρμοσμένη κρυπτογραφία. Ως εκ τούτου τα προσωπικά δεδομένα αποθηκεύονται πάντα κρυπτογραφημένα ενώ η επεξεργασία γίνεται μέσω ειδικής προγραμματιστικής διεπαφής που λαμβάνει εξουσιοδότηση μέσω μιας έμπιστης τρίτης οντότητας, η οποία εξασφαλίζει στο χρήστη τον αξιόπιστο έλεγχο του τρόπου διαχείρισης των δεδομένων τους βάσει του ΓΚΔΠ.

Το Γεωπονικό Πανεπιστήμιο Αθηνών (Γ.Π.Α.) στα πλαίσια της υπ' αριθ. 570/21.05.2020 Συνεδρίασης της Συγκλήτου του[240], αποφάσισε την κατά κανόνα εξ αποστάσεως διεξαγωγή των εξετάσεων της εαρινής εξεταστικής περιόδου του Ακαδημαϊκού Έτους 2019-2020, όλων των Ακαδημαϊκών Τμημάτων των Σχολών του, και μόνο κατ' εξαίρεση την με φυσική παρουσία εξέταση, τονίζοντας ότι η εν λόγω απόφαση της τελεί σε πλήρη εναρμόνιση με το ισχύον θεσμικό πλαίσιο και την πολιτική προστασίας των προσωπικών δεδομένων. Οι φοιτητές που επέλεξαν να εξεταστούν ηλεκτρονικά συναινούν στην αμφίδρομη οπτικοακουστική αλληλεπίδραση κατά τη διεξαγωγή της εξέτασης ενώ ρητά απαγορεύεται η από οποιονδήποτε εγγραφή/βιντεοσκόπηση των εξετάσεων.

Το Εθνικό Μετσόβιο Πολυτεχνείο (Ε.Μ.Π.)[241] από τη διενεργηθείσα έρευνα δεν προκύπτει ότι υιοθετεί κάποια ιδιαίτερη πολιτική προστασίας για τα προσωπικά δεδομένα.

Οι Στρατιωτικές Σχολές (Αξιωματικών Σωμάτων[242] και Ευελπίδων[243]) υιοθετούν Πολιτική Απορρήτου ενώ υποστηρίζονται από το ΚΕ.Π.Υ.Ε.Σ[244], το οποίο έχει αναπτύξει Σύστημα

[239] https://www.aueb.gr/el/content/pdguard-neo-kainotomo-logismiko-apo-panepistimiaki-ereyna-sto-oikonomiko-panepistimio
[240] https://www2.aua.gr/el/news-events/nea/odigies-gia-ti-diexagogi-ton-ex-apostaseos-exetaseon
[241] https://www.ntua.gr/el/
[242] https://ssas.army.gr/
[243] https://sse.army.gr/

Διαχείρισης Ασφάλειας Πληροφοριών και Πιστοποίηση, σύμφωνα με το διεθνές πρότυπο EN ISO 27001:2013, μετά από επιθεώρηση του Οργανισμού Πιστοποίησης TÜV Austria Hellas. Το ISO 27001 είναι το πιο γνωστό Διεθνές Πρότυπο Συστημάτων Διαχείρισης Ασφάλειας Πληροφοριών που καθορίζει τις απαιτήσεις για την εφαρμογή, τη διατήρηση και τη συνεχή βελτίωση ενός συστήματος διαχείρισης της ασφάλειας των πληροφοριών στο πλαίσιο της οργάνωσης[245]. Περιλαμβάνει τις απαιτήσεις για την εκτίμηση και αντιμετώπιση των κινδύνων ασφάλειας των πληροφοριών, προσαρμοσμένων στις ανάγκες του οργανισμού. Το πρότυπο EN ISO 27001:2013 εξασφαλίζει την επάρκεια στις διαδικασίες και στα μέτρα ελέγχου σε θέματα εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των πληροφοριών για την προστασία των δεδομένων και των εμπλεκόμενων πόρων, σε κάθε δραστηριότητα της Μονάδας. Οι περιοχές ελέγχου αναλύονται σε 114 σημεία και καλύπτουν θέματα φυσικής ασφάλειας, λογικής ασφάλειας, δικτυακής ασφάλειας, διαβάθμισης πληροφοριών, ανάπτυξης και συντήρησης Πληροφοριακών Συστημάτων καθώς και διαχείρισης περιστατικών ασφαλείας. Επιπρόσθετα το πρότυπο προστατεύει τις πληροφορίες από οποιοδήποτε αναγνωρισμένο κίνδυνο μέσω της εφαρμογής διαδικασιών εντοπισμού, διαβάθμισης και ανάλυσης επικινδυνότητας και τη θέσπιση σημείων ελέγχου των πληροφοριών είτε αφορούν σε ηλεκτρονικά είτε σε έντυπα δεδομένα. Τέλος το πρότυπο προβλέπει την κατάρτιση σχεδίων Επιχειρησιακής Συνέχειας (Business Continuity Plan) και Ανάκαμψης από Καταστροφή (Disaster Recovery Plan). Η πιστοποίηση EN ISO 27001:2013 τεκμηριώνει την υποδομή που διαθέτει η Μονάδα για την προστασία και ασφάλεια των δεδομένων που διαχειρίζεται καθώς και την αποδεδειγμένη δέσμευση του Γενικού Επιτελείου Στρατού και των Ενόπλων Δυνάμεων συνολικά στη ανάπτυξη και διαχείριση ασφαλών Πληροφοριακών Συστημάτων, υψηλής επιχειρησιακής ετοιμότητας και διαθεσιμότητας.

Εν κατακλείδι, από τη διενεργηθείσα έρευνα και τα παραπάνω εκτιθέμενα προκύπτει, η τάση των περισσοτέρων πανεπιστημίων να συμμορφωθούν με τους κανόνες που θέτει ο ΓΚΠΔ και να κινητοποιηθούν προς την κατεύθυνση την προστασίας των δεδομένων από επεξεργασίες που πλήττουν την πληροφοριακή αυτοδιάθεση του ατόμου. Λίγο έως πολύ φαίνεται πως τα ελληνικά Πανεπιστήμια έχουν αντιληφθεί την ανάγκη ύπαρξης ενός κλίματος ασφάλειας από την τεχνολογική εξέλιξη εντός της ακαδημαϊκής κοινότητας,

[244] http://army.gr/el/organosi/monades-ypiresies/kentro-pliroforikis-ypostirixis-ellinikoy-stratoy-kepyes/pistopoiiseis

[245] https://bqc.gr/iso-27001?gclid=Cj0KCQjwutaCBhDfARIsAJHWnHugAQ_hlDfbK1SXixLO8MXvETtcTkstd-FC4qE0U2gG_XWsV7FKpNQaAvG2EALw_wcB

προσπαθώντας να δημιουργήσουν ένα προστατευτικό πλέγμα με την υιοθέτηση Οδηγών συμμόρφωσης, κωδίκων δεοντολογίας αλλά και με την καθιέρωση νέων ή με την επικαιροποίηση ήδη υφισταμένων Πολιτικών προστασίας ιδιωτικότητας ή προσωπικών δεδομένων και με την ανανέωση των εντύπων και τη δημιουργία πρότυπων εντύπων που χρησιμοποιούν τα υποκείμενα όταν επιθυμούν να υποβάλλουν αίτημα προστασίας για κάποιο από τα δικαιώματα που τους παραχωρεί ο ΓΚΠΔ. Ιδιαίτερη εντύπωση προκαλεί η ετοιμότητα μάλιστα πολλών εξ αυτών να προετοιμαστούν κατάλληλα όσον αφορά στην προστασία των προσωπικών δεδομένων στα πλαίσια της εξ αποστάσεως on line διδασκαλίας και διενέργειας εξ αποστάσεως εξέτασης, ως μέτρο περιορισμού της διασποράς της πανδημίας. Η υιοθέτηση ξεχωριστών πολιτικών προστασίας για τις εν λόγω δράσεις προς αντιμετώπιση τυχόν ζητημάτων παραβίασης δεδομένων, καταδεικνύει το αυξημένο ενδιαφέρον της ακαδημαϊκής κοινότητας να λειτουργήσει προληπτικά, λαμβάνοντας μέτρα προστασίας και διευκρινίζοντας τις νομικές συνέπειες σε περίπτωση αθέτησης των οριζομένων στο ΓΚΠΔ, με κυριότερο ζήτημα εκείνο της βιντεοσκόπησης ή καταγραφής οπτικού ή ακουστικού υλικού.

Ενδιαφέρον θα παρουσίαζε μια μελλοντική διερεύνηση στο χώρο της ακαδημαϊκής κοινότητας εν γένει μετά την παρέλευση ικανοποιητικού χρονικού διαστήματος από την έναρξη ισχύος του ελληνικού κυρωτικού νόμου, και δη αναφορικά με την διατήρηση της συμμόρφωσης, την ανανέωση και επικαιροποίηση των πολιτικών, διαδικασιών και οδηγιών των πανεπιστημίων σε σχέση με τον ΓΚΠΔ αλλά και την διαρκή συνέπεια στη λήψη των κατάλληλων μέτρων προστασίας έναντι των εξελισσομένων τεχνολογιών και προς αποτροπή σύγχρονων τεχνολογικών απειλών καθώς και την ανεπάρκεια των διατάξεων του ισχύοντος θεσμικού πλαισίου.

4.5.4. Προτάσεις για την ορθή εφαρμογή και διατήρηση της συμμόρφωσης με τον ΓΚΠΔ

Η υλοποίηση του Προγράμματος συμμόρφωσης εκ μέρους των πανεπιστημίων συνιστά την έμπρακτη απόδειξη της συμμόρφωσής τους προς το ΓΚΠΔ, η οποία ωστόσο μόνη της δεν είναι αρκετή. Το στάδιο μετά την ολοκλήρωση του εν λόγω Προγράμματος κρίνεται ιδιαίτερα σημαντικό και είναι ζωτικής σημασίας καθώς σχετίζεται με τις προσπάθειες του εκάστοτε Πανεπιστημίου να διατηρήσει όλα τα επίπεδα ασφαλείας. Αυτό είναι και το χρονικό σημείο κατά το οποίο η Διοίκηση εκάστου Πανεπιστημίου πρέπει να αποδείξει τη δέσμευσή της αναπτύξει την «κουλτούρα» για την προστασία των προσωπικών

δεδομένων, η οποία θα πρέπει να έχει διάρκεια και συνοχή, προκειμένου να εξασφαλίσει την αναδιοργάνωση, την ομαλή και απρόσκοπτη λειτουργία, τη διατήρηση του κύρους και της φήμης του και εν τέλει το ανταγωνιστικό αποτέλεσμα που επιθυμεί.

Για να επιτευχθούν τα ανωτέρω απαιτείται διαρκής συνέπεια και έλεγχος τήρησης των αρχών σύννομης επεξεργασίας κατά το πρότυπο της θεωρίας του κύκλου του Deming, ενημέρωση των υποκειμένων για τα νέα επικαιροποιημένα βάσει του ΓΚΠΔ δικαιώματά τους, τήρηση των προθεσμιών ικανοποίησης των δικαιωμάτων, σεβασμός των χρονικών ορίων επεξεργασίας και αποθήκευσης, τήρηση προθεσμιών ανταπόκρισης στα αιτήματα των υποκειμένων, διαρκής επικαιροποίηση των εντύπων (φορμών) και κειμένων που απευθύνονται στους επισκέπτες-χρήστες, φοιτητές και λοιπούς ενδιαφερόμενους που παρέχουν τα δεδομένα τους στο εκάστοτε πανεπιστήμιο.

Έτσι κάθε πανεπιστήμιο πρέπει να προσεγγίζει κατά τρόπο ενιαίο την καταγραφή των δεδομένων, τη συμμόρφωση προς το ΓΚΠΔ και την ενημέρωση των υποκειμένων τους, ενώ δεν πρέπει να απαξιώνει τη σημασία που πρέπει να αποδίδεται στο ζήτημα της εκπαίδευσης του προσωπικού του, το οποίο πρέπει να μπορεί να αντιληφθεί τις επελθούσες νομοθετικές μεταβολές, να ανταπεξέρχεται στις νέες απαιτήσεις και κυρίως σ΄αυτές που αναφέρονται στα αιτήματα των υποκειμένων των δεδομένων και να αναδεικνύει το ρόλο του ΥΠΔ μέσα από τη γνωστοποίηση των στοιχείων του καθώς και των στοιχείων επικοινωνίας μαζί του, έτσι ώστε να διασφαλίζεται η άμεση επικοινωνία και η πληρέστερη ικανοποίηση των αιτημάτων των υποκειμένων. Περαιτέρω τα πανεπιστήμια πρέπει να προβαίνουν σε έναν διαρκή έλεγχο αναφορικά με τον εξοπλισμό, τις τεχνολογικές υποδομές, τα κατάλληλα λογισμικά, τα οποία πρέπει να ελέγχονται πριν τη χρήση τους ή να επικαιροποιούνται άμεσα σε περίπτωση κάθε νέας έκδοσης ασφαλείας, να διαθέτουν διαδικασία αντιμετώπισης προβλημάτων, να προβαίνουν σε έλεγχο των ρυθμίσεων των διακομιστών διαδικτύου, ώστε να μην καθίστανται προσβάσιμες οι μη δημόσιες πληροφορίες. Αναγκαία επίσης κρίνεται και η διενέργεια προγραμματισμένων επιθεωρήσεων και η λήψη μέτρων, όπως είναι η υιοθέτηση κώδικα δεοντολογίας, πολιτικών προστασίας και πιστοποιήσεων.

Οι αλλαγές που έφερε ο ΓΚΠΔ είχαν ως επακόλουθο το αυξημένο κόστος για τις διοικήσεις των Πανεπιστημίων, για το οποίο απαιτείται η εξεύρεση αναγκαίων οικονομικών πόρων, ώστε να προσαρμοστούν τα μηχανογραφικά συστήματα στις προδιαγραφές που θέτει ο κανονισμός. Προκειμένου να επέλθει η αποτελεσματική

διαχείριση της αλλαγής, να δημιουργηθεί ένα νέο όραμα, να αναπτυχθεί μια υποστηρικτική πολιτική αλλά και να διατηρηθεί αυτή η αλλαγή, τα Πανεπιστήμια πρέπει να συνειδητοποιήσουν τους λόγους για τους οποίους υιοθετήθηκε ο ΓΚΠΔ και να αναγνωρίσουν σε ποια κατάσταση βρίσκονται και που θέλουν να φτάσουν, υιοθετώντας την πρακτική Plan-Do-Check-Act για την προστασία των προσωπικών δεδομένων.

Στα πλαίσια της συνολικής αυτής κινητοποίησης, οι διοικήσεις των πανεπιστημίων που ενεργούν ως υπεύθυνοι επεξεργασίας, πρέπει να υιοθετούν την προστασία από το σχεδιασμό και την στα πλαίσια αυτής διενέργεια DPIA. Η επέλευση ενός συμβάντος παραβίασης π.χ. διαρροής προσωπικών δεδομένων φοιτητών ή εργαζομένων, συνιστά λόγο εγρήγορσης και κινητήρια δύναμη για τη Διοίκηση κάθε πανεπιστημίου, η οποία δεν θα πρέπει σε καμία περίπτωση να εφησυχάζει. Η εκπόνηση DPIA μπορεί να λειτουργήσει αποτρεπτικά για σωρεία κινδύνων και κατ' επέκταση προστατευτικά για τα προσωπικά δεδομένα, ειδικά όταν επίκειται κοινή εφαρμογή ή πλατφόρμα επεξεργασίας ή όταν πρόκειται να θεσπιστεί νέα διάταξη αναφορικά με την επεξεργασία των προσωπικών δεδομένων. Στις περιπτώσεις αυτές η εκτίμηση πρέπει να αποτελεί μέρος της αρχικής μελέτης. Περαιτέρω ιδιαιτέρως χρήσιμη αποδεικνύεται κι η διαβούλευση με την εποπτική αρχή αν ο κίνδυνος είναι υψηλός για τα δικαιώματα πριν την έκδοση νομοθετικών ή κανονιστικών μέτρων επεξεργασίας.

Επιπλέον η ενημέρωση των υποκειμένων από τους υπεύθυνους επεξεργασίας για την άσκηση των δικαιωμάτων πρόσβασης και διαγραφής, για την ελαχιστοποίηση των δεδομένων τους, η χρήση τεχνικών και οργανωτικών μέτρων όπως η ανωνυμοποίηση κι η κρυπτογράφηση είναι παράγοντες που θα συντελέσουν σε μια βελτιωμένη εκδοχή της προστασίας των δεδομένων εντός της ακαδημαϊκής κοινότητας και της απεριόριστης επεξεργασίας αυτών και θα αποτρέψουν τη δημιουργία του λεγόμενου ψηφιακού μωσαϊκού του ανθρώπινου προσώπου, απόρροια του οποίου είναι ο έλεγχος και η εμπορευματοποίηση της ιδιωτικότητας και του απορρήτου και του ιδίου του ατόμου εν γένει.

Εξίσου ζωτικής σημασίας είναι και η διαρκής επιμόρφωση του προσωπικού των Πανεπιστημίων και των εμπλεκομένων στην επεξεργασία μερών, η οποία επιτυγχάνεται με συνεχείς δράσεις, επιμορφωτικά σεμινάρια, ημερίδες για την προστασία των δεδομένων και την εξέλιξη του θεσμικού πλαισίου που διαμορφώνεται σε σχέση με τον ΓΚΠΔ.

Εν κατακλείδι οι Διοικήσεις όλων των Πανεπιστημίων της χώρας θα πρέπει να αντιμετωπίζουν την συμμόρφωση με το ΓΚΠΔ με μια ολιστική προσέγγιση που θα έχει ως κύριο χαρακτηριστικό της την διαμόρφωση συνείδησης αναφορικά με την προστασία των δεδομένων και θα βασίζεται στη διαρκή υποχρέωση συμμόρφωσης, ενημέρωσης, επιμόρφωσης κι ενασχόλησης με την προστασία, από την οποία επιδιώκεται να δημιουργηθεί και να καλλιεργηθεί μια νέα νοοτροπία που θα εισαγάγει ένα νέο μοντέλο βασισμένο στη δημιουργία κι ενδυνάμωση των δεσμών εμπιστοσύνης στις συμβατικές σχέσεις (Chmielarz, 2019). Προς αυτή την κατεύθυνση θα βοηθήσουν και οι ερμηνευτικές οδηγίες και οι κατευθυντήριες γραμμές του ΕΣΠΔ ενώ μια αποτίμηση για το πλαίσιο που θεσπίζει ο ΓΚΠΔ θα παρέχουν και οι Εκθέσεις αξιολόγησης και αναθεώρησης του Κανονισμού που συντάσσει η Επιτροπή και υποβάλει στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο, δυνάμει του άρθρου 97 ΓΚΠΔ.

4.5.5. Συμπεράσματα

Ο νέος κανονισμός για την προστασία των προσωπικών δεδομένων είναι πλέον γεγονός και ήρθε για να μείνει για όσο θα είναι σε θέση να παρακολουθεί τις τεχνολογικές εξελίξεις. Κύρια επιδίωξη του είναι η προληπτική δράση γύρω από το ζήτημα της προστασίας των προσωπικών δεδομένων μέσα από τη θέσπιση υποχρεώσεων για τον υπεύθυνο επεξεργασίας αυτών. Το αυστηρό θεσμικό και γραφειοκρατικό πλαίσιο που θέτει, προϋποθέτει το σεβασμό των αρχών που το διέπουν και την διασφάλιση της άσκησης των δικαιωμάτων των υποκειμένων τους ενώ επιδιώκει να εξασφαλίσει την ομοιόμορφη και συνεκτική εφαρμογή του εντός της Ε.Ε. επισύροντας, επί παραβίασης, βαρύτατες διοικητικές κυρώσεις που λειτουργούν ενισχυτικά προς την κατεύθυνση της συμμόρφωσης με το πνεύμα του και τις επιταγές του κανονισμού.

Στα δύο χρόνια εφαρμογής του Γενικού Κανονισμού στην Ελλάδα, τα πρώτα δείγματα είναι αρκετά ενθαρρυντικά, κυρίως όσον αφορά στα δικαιώματα των υποκειμένων, στον ορισμό ΥΠΔ και δη στον Ιδιωτικό τομέα, και στην εξασφάλιση ενός βασικού επιπέδου ασφαλείας των προσωπικών δεδομένων. Αυτό βέβαια δεν σημαίνει ότι δεν διαπιστώνονται προβλήματα στην εφαρμογή του, με χαρακτηριστικότερα ίσως την ανεπαρκή συμμόρφωση των φορέων με τη νομοθεσία αναφορικά με τα cookies, την ελλιπή ενημέρωση των υποκειμένων σχετικά με τις πράξεις επεξεργασίας των δεδομένων τους και την καθυστέρηση του δημόσιου κυρίως τομέα να αναλάβει τις υποχρεώσεις που έχει βάσει του ΓΚΠΔ ειδικά ως προς τη διαφάνεια.

Ο ελληνικός κυρωτικός νόμος 4624/2019 που αντικατέστησε το νομοθετικό πλαίσιο αναφορικά με τη συγκρότηση και τη λειτουργία της ΑΠΔΠΧ, επεδίωξε να λάβει μέτρα εφαρμογής του Κανονισμού 2016/679 και να ενσωματώσει στην εθνική νομοθεσία την Οδηγία (ΕΕ) 2016/680 («Οδηγία LED»), καταφέρνοντας ως ένα τουλάχιστον βαθμό να άρει την έως πρότινος υφιστάμενη νομική αβεβαιότητα. Έκανε ωστόσο και ευρεία χρήση της διακριτικής ευχέρειας που του έδωσε ο ΓΚΠΔ, υιοθετώντας αρκετές «ρήτρες ανοίγματος» με αποτέλεσμα να παρεκκλίνει σε ορισμένα ζητήματα από όσα προβλέπει ο κανονισμός, κυρίως όσον αφορά στην επεξεργασία των δεδομένων ανηλίκων, στην επεξεργασία «ειδικών κατηγοριών δεδομένων» (ευαίσθητων) και στον ακριβή καθορισμό των προϋποθέσεων υπό τις οποίες η επεξεργασία είναι σύννομη.

Ιδιαίτερα σημαντικός αποδεικνύεται ο ρόλος της ΑΠΔΠΧ. Η ελληνική αρχή, αν και στερούμενη πόρων και δη ανθρώπινων, κατέβαλε τεράστιες προσπάθειες για να προετοιμαστεί αλλά και να προετοιμάσει αναφορικά με την εφαρμογή του ΓΚΠΔ, αναπροσαρμόζοντας τον τρόπο λειτουργίας της και εμπλουτίζοντας την ιστοσελίδα της με οδηγίες και υποδείγματα προς ενημέρωση όσων ασχολούνται με την επεξεργασία. Διατηρώντας τον τριπλό της ρόλο εκτελεί πλέον και καθήκοντα εποπτικής αρχής, επιφορτισμένη με τη διενέργεια κοινών δράσεων και ελέγχων με άλλα κράτη μέλη στα πλαίσια των διαδικασιών συνεργασίας και συνεκτικότητας, αναλαμβάνοντας έναντι των ομολόγων της υποχρεώσεις που καλείται να φέρει εις πέρας εντός αυστηρών προθεσμιών ενώ μέσω της πρακτικής που εφαρμόζει υπό την ιδιότητά της αυτή και σε συνδυασμό με τις κατευθυντήριες γραμμές του ΕΣΠΔ και τη νομολογία των δικαστηρίων, αποσαφηνίζει και προσδιορίζει νέες έννοιες και πτυχές γύρω από το ζήτημα της προστασίας των προσωπικών δεδομένων.

Τα περισσότερα ακαδημαϊκά ιδρύματα της χώρας μας δεν υπήρξαν αδιάφορα απέναντι στον ΓΚΠΔ και κατέβαλαν ικανοποιητικές προσπάθειες συμμόρφωσης . Πρωτίστως ενημερώθηκαν για το νέο θεσμικό πλαίσιο προβαίνοντας αρχικά στην ευαισθητοποίηση του προσωπικού τους κι εν συνεχεία προχωρώντας στη λήψη των κατάλληλων μέτρων για τη διασφάλιση της προστασίας. Στα πλαίσια της προσπάθειάς τους αυτής εκσυγχρόνισαν τις τεχνολογικές τους υποδομές και τα συστήματα ασφαλείας, υιοθέτησαν οδηγούς που εμπεριέχουν κώδικες δεοντολογίας και πολιτικές προστασίας, επικαιροποίησαν τις διαδικασίες και τα έντυπά τους. Η αποφυγή επιβολής διοικητικών κυρώσεων σαφώς συνιστά παράγοντα συνετής συμπεριφοράς εκ μέρους των Διοικήσεών τους αλλά όχι τον

μοναδικό. Τα Πανεπιστήμια αποδεικνύουν ότι αντιμετωπίζουν τη συμμόρφωσή τους υπό ένα διαφορετικό πρίσμα, ήτοι ως έναυσμα, πρόκληση και ευκαιρία εκσυγχρονισμού των υφιστάμενων πολιτικών και διαδικασιών και αναπροσαρμογής της οργανωτικής τους δομής βάσει προτύπων ασφαλείας στην επεξεργασία των δεδομένων αλλά και ως προοπτική που θα τους προσφέρει ανταγωνιστικό πλεονέκτημα για αναβάθμιση της ποιότητας των παρεχόμενων υπηρεσιών και ενίσχυση της καινοτομίας εντός της ακαδημαϊκής κοινότητας, που αποτελεί κατεξοχήν χώρο καλλιέργειας πνεύματος, διάδοσης ιδεών και γνώσεων και προώθησης της έρευνας, εξασφαλίζοντας όχι μόνον την προστασία των υποκειμένων -που σε μεγάλο ποσοστό είναι το ίδιο το προσωπικό τους – αλλά και τη διατήρηση του κύρους και της φήμης τους.

Είναι γεγονός ότι η συμμόρφωσή προς το προστατευτικό πλέγμα διατάξεων που θέτει ο ΓΚΠΔ συνεπάγεται υψηλά κόστη, εκπαίδευση, διαρκή ενημέρωση, τεχνογνωσία και πολύπλοκες διαδικασίες, με τις οποίες δεν είναι ακόμη πλήρως εξοικειωμένες οι διοικήσεις τους. Ωστόσο αναπτύσσοντας την κατάλληλη υποδομή και δημιουργώντας την ανάλογη παιδεία και κουλτούρα σεβασμού αναφορικά με την προστασία των προσωπικών δεδομένων και την ανάδειξή της σε πυρήνα της καθημερινής τους λειτουργίας, θα αποδείξουν περίτρανα στο άτομο που μετέχει στην κοινωνία της πληροφορίας, ότι είναι διαρκώς σε θέση να το προστατεύουν, μετατρέποντας την περί συμμόρφωσης υποχρέωση σε ευαισθητοποίηση και προώθηση μιας νέας κουλτούρας. Μιας κουλτούρας που είναι άμεσα συνυφασμένη με την «έξυπνη συμμόρφωση» και η οποία εκφεύγει των ορίων της επιβολής διοικητικών προστίμων. Μ’ αυτόν τον τρόπο θα ενισχυθεί η εμπιστοσύνη μεταξύ των εμπλεκομένων στην επεξεργασία μερών και θα αναδειχθεί ο ανθρωποκεντρικός ρόλος του κανονισμού. Η συμμόρφωση με το πνεύμα, τις αρχές και τις επιταγές του ΓΚΠΔ είναι μια διαρκής υπόθεση που πρέπει να διατηρείται και να αναβαθμίζεται, που απαιτεί εντατική προσπάθεια τόσο σε επίπεδο ενημέρωσης και εκπαίδευσης όσο και σε επίπεδο ανάπτυξης βέλτιστων πρακτικών. Μένει να δούμε σε ποιο βαθμό μπορεί να αξιοποιηθεί, ώστε να αναδείξει όλα τα οφέλη του κανονισμού, προασπιζόμενη πάντα τα θεμελιώδη δικαιώματα των ευρωπαίων πολιτών.

ΒΙΒΛΙΟΓΡΑΦΙΚΕΣ ΑΝΑΦΟΡΕΣ

ΕΛΛΗΝΟΓΛΩΣΣΕΣ

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

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

Αποστολόπουλος, Β., (2020). Μια ιστορική αναδρομή στην προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα στην Ευρώπη, διαθέσιμο σε https://www.dikastiko.gr/articles/vasilis-apostolopoylos-mia-istoriki-anadromi-stin-prostasia-ton-fysikon-prosopon-enanti-tis-epexergasias-dedomenon-prosopikoy-charaktira-stin-eyropi/ [πρόσβαση 15.12.2020]

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.

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

Βαρβέρης, 11-12 Μαΐου 2018, 2ο ετήσιο συνέδριο E-themis «Προσωπικά δεδομένα και δικηγορία-Μια νέα πραγματικότητα, ένα νέο κεφάλαιο στο νομικό κόσμο», διαθέσιμο σε: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations_el [πρόσβαση 12.11.20]

Βλαχόπουλος, Σ., (2018). *Πρόσβαση στα δημόσια έγγραφα*, σε Κοτσαλή, Λ. & Μενουδάκο, Κ. (2018), Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων (GDPR), Νομική Διάσταση και πρακτική εφαρμογή, Αθήνα, Νομική Βιβλιοθήκη.

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

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

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

Γιαννόπουλος, Γ., Μήτρου, Λ., Τσόλιας, Γρ. (2018). *Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων (GDPR), Νομική Διάσταση και πρακτική εφαρμογή*, Αθήνα, Νομική Βιβλιοθήκη.

Δαγτόγλου, Π. (2012)., *Συνταγματικό Δίκαιο - Ατομικά Δικαιώματα, 4η έκδοση*, Αθήνα-Θεσσαλονίκη, Εκδόσεις Σάκκουλα.

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*.

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

Κανελλάκη, Μ., (2016), Ο νέος Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων, Τα πλαίσια ασάφειας και οι προβληματισμοί πάνω στις νέες διατάξεις, *Ένθα, Μάιος 2016.*

Καρκατζούνης, Β. Προστασία δεδομένων ήδη από το σχεδιασμό (by design) και εξ ορισμού (by default). Μία πρώτη προσέγγιση του άρθρου 25 ΓΚΠΔ, διαθέσιμο σε: https://www.crimetimes.gr/%CF%80%CF%81%CE%BF%CF%83%CF%84%CE%B1%CF%83%CE%AF%CE%B1-%CE%B4%CE%B5%CE%B4%CE%BF%CE%BC%CE%AD%CE%BD%CF%89%CE%BD-%CE%AE%CE%B4%CE%B7-%CE%B1%CF%80%CF%8C-%CF%84%CE%BF-%CF%83%CF%87%CE%B5%CE%B4%CE%B9%CE%B1/ [πρόσβαση: 19-01-2021]

Κόνδη Κ. (2019), Προστασία Δεδομένων by Design & by Default: Ένα Αληθινό Στοίχημα, διαθέσιμο σε: https://www.capital.gr/arthra/3387975/prostasia-dedomenon-by-design-by-default-ena-alithino-stoixima [πρόσβαση23.01.2021]

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.

Κωτσίκης, Ε. (2007). *Εκπαιδευτική Διοίκηση και Πολιτική*. Αθήνα: Εκδόσεις Έλλην.

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.

Λουκά Ν., Τεχνικά μέτρα του Γενικού Κανονισμού για την Προστασία Δεδομένων (GDPR), διαθέσιμο σε https:// www.dpoacademy.gr/el/arthra2/, [πρόσβαση 15.01.2021]

Μήτρου, Λ. (2002). *Η προστασία των προσωπικών δεδομένων στο πεδίο των εργασιακών σχέσεων – Η συμβολή της Αρχής. Σε Π. Δόνος κ.ά. (2002), Η Αρχή Προστασίας Προσωπικών Δεδομένων και η επαύξηση της προστασίας των δικαιωμάτων*, Αθήνα-Θεσσαλονίκη.

Μίττλετον, Φ. (2018), *Ο μηχανισμός συνεργασίας και συνεκτικότητας (one stop shop), σε Κοτσαλή, Λ., Μενουδάκο, Κ. (Επιμ.). (2018), Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων (GDPR).* Αθήνα: Νομική Βιβλιοθήκη, σσ. 283-297.

Μπούρκα, Α. (2015) Privacy on Data Protection by Design, ENISA (Ιανουάριος, 2015). Διαθέσιμο σε: https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design [πρόσβαση 22.01.2021]

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 σε: https://www.didaktorika.gr/eadd/handle/10442/42327. [πρόσβαση 20.01.2021]

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

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 σε:https://www.ethemis.gr/epistimoniki-arthrografia-fereniki-panagopoulou-koutnatzi.htm, [πρόσβαση 29.11.2020].

ΣΕΒ, Οδηγός Συμμόρφωσης, *Ο νέος Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR) Εφαρμογή και προκλήσεις για τις επιχειρήσεις στην εποχή της ψηφιοποίησης Μια πρωτοβουλία της Ομάδας Εργασίας του ΣΕΒ για τα Προσωπικά Δεδομένα*, Αθήνα, Οκτώβριος 2018

Τσαγκανού, Π. (2014). *Η κοινωνική παράμετρος στην προστασία της ιδιωτικότητας του ατόμου – χρήστη νέων τεχνολογιών*. Διπλωματική εργασία. Πανεπιστήμιο Πατρών.

Τσιπτσέ, Ο. & Κωστούλας Δ. (2020) *Η συμμόρφωση με τον Γενικό Κανονισμό Προστασίας Δεδομένων, GDPR EU 2016/679, Πρακτικά ζητήματα – Υποδείγματα* , Ιανουάριος 2020, Θεσ/νίκη, Εκδόσεις Νομόραμα.

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 16.11.2020].

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

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 05.11.2020]

ΞΕΝΟΓΛΩΣΣΕΣ

Albrecht, J. P. (2016). How the GDPR Will Change the World. *Eur. Data Prot. L. Rev., 2, 287.*

Chmielarz, G. (2019). Role of data security policy at higher education institutions in the light of legislative changes introduced by the GDPR, *Proceedings Of The 9TH International Conference On Management, "People, Planet and Profit: Sustainable business and society", Volume II, ICoM 2019*, pp.258-247, Retrieved from Proceedings-icom-2019jun13-volume_ii-doi-ed_da.pdf [access 23.01.2021]

Cormack, A. (2017, 24 May). A year to get your act together: How universities and colleges should be preparing for new data regulations. Retrieved from www.jisc.ac.uk/blog/a-year-to-get-your-act-together-how-universities-and-colleges-should-be-preparing-for-new-data-regulations [access 20.01.2021]

Dunn B. (2018). A personal data primer: How higher education institutions can prepare for the GDPR. Habbabeh, Schneider & Asprion (2019), Data Privacy Assessment: An Exemplary Case for Higher Education Institutions, *International Journal of Management, Knowledge and Learning*, 8(2), p.226-228

De Cew, J.W. (1997). *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*. Cornell University Press, Ithaca, NY.

De Hert, P. (2016). The new GDPR: Still a sound system for the protection of individuals? *Computer Law & Security Review*, 32(2016), pp.179-194.

European Union Agency for Fundamental Rights and Council of Europe, *"Handbook on European data protection law", 2018*.

ENISA (2014). Privacy and data protection by design-from policy to engineering. Retrieved from www.enisa.europa.eu [πρόσβαση 30.01.2021]

Floridi, L. (1999). Information ethics: on the philosophical foundations of computer ethics. *Ethics and Information Technology*, 1(1), pp.37–56.

Garber, J. (2018). GDPR-compliance nightmare or business opportunity? *Computer Fraud & Security, No. 6*, pp.14–15.

Gotterbarn, D. and Miller, K.W. (2017). Yes, but… our response to: " professional ethics in the information age". *Journal of Information, Communication and Ethics in Society, 15(4)*, pp. 357-361.

Grey R. Orret & Brown Raymond (2020), *Cyber Security Practitioner's Guide, Chapter 8: GDPR Compliance: Incident Response and Breach Notification Challenges, March, 2020*, Retrieved from https://doi.org/10.1142/11390. [access 18.01.2021]

Habbabeh, A., Schneider, B., & Asprion, P. M., (2019) Data Privacy Assessment: An Exemplary Case for Higher Education Institutions, International Journal of Management, Knowledge and Learning, 8(2), pp.221–241

Hildebrandt M. (2009), *Behavioural Biometric Profiling and Transparency Enhancing Tools.*WP7 Deliverable, Nov. 2009, Retrieved from http:fidis.net/ [access 15.01.2021]

Hunter, L. (1995). Public image. Σε K.E. Himma & H.T. Tavani (Eds..), *The handbook of information and computer ethics*. New Jersey, Wiley.

Johnson, J., Your Higher Education Institution's Compliance With The GDPR, July 23, 2018, retrieved from: https://www.powerslaw.com/higher-education-institutions-gdpr/ [πρόσβαση 21.02.2021]

ICO. (n.d.) Guide to the General Data Protection Regulation (GDPR). Retrieved from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr [πρόσβαση 17.01.2021]

Iglezakis, I. (2014). The Right to be forgotten in the Google Spain Case (case C131/12): a clear victory for data protection or an obstacle for the internet? *4th International Conference on Information Law*.

Krystlik, J., (2017). With GDPR, preparation is everything, *Computer Fraud & Security, Volume 2017, Issue 6, June 2017,* pp.5-8

Maner, W. (1996). Unique ethical problems in information technology. *Science and engineering ethics*, 2(2), pp.137-154.

Mekovec, R. & Peras, D., (2020). Implementation of the General Data Protection Regulation: Case of Higher Education Institution, *International Journal of e-Education, e-Business, e-Management and e-Learning, Volume 10, Number 1, March 2020,* pp.104-112

Microsoft. (2018). *GDPR for Education*. Retrieved from https://pulse.microsoft.com/uploads/prod/2018/03/WorkProductivity_GDPRforEducation_KickStartGuide.pdf. [access 20.01.2021]

Mouncey P., Planning for the GDPR: evolution rather than revolution, *SRA Research Matters, March 2018.*

O'Hara, K., Alani, H., Kalfoglou, Y. and Shadbolt, N. (2004). Trust strategies for the semantic web. Σε Π. Τσαγκανού (2014). Η κοινωνική παράμετρος στην προστασία της ιδιωτικότητας του ατόμου – χρήστη Νέων Τεχνολογιών. Πανεπιστήμιο Πατρών.

Parent, W.A. (1983a). Privacy, morality and the law. *Philosophy and Public Affairs,* 12(4), 269–288.

Parent,W. A. (1983b). A new definition of privacy for the law. *Law and Philosophy*, 2, 305–338.

Podnar, K. (2017, 21 September). Is your university ready to pass the GDPR exam? Retrieved from https://medium.com/kpodnar/is-your-universityready-to-pass-the-gdpr-exam-eac6641cebbc [access 18.12.2020]

Powels, (2015). Right to be forgotten: Swiss cheese internet or database of ruin?, Retrieved from https://www.theguardian.com/technology/2015/aug/01/right-to-be-forgotten-google-swiss-cheese-internet-database-of-ruin [access 15.1.2020]

Regan, 1995 Regan, P.M. (1995). Legislating Privacy: Technology, Social Values, and Public Policy. University of North Carolina Press, Chapel Hill, NC.

Rodriguez de las Heras Ballell, T. , (2017). The Legal Anatomy of Electronic Platforms: A Prior Study to Assess the Need of a Law of Platforms in the EU, The Italian Law Journal, Vol. 03, No. 01, pp.151-176

Šidlauskas, A., & Limba T. General Data Protection Regulation Implementation In Higher Education Institutions, *Proceedings of EDULEARN19 Conference 1st-3rd July 2019, Palma, Mallorca, Spain*, pp.2040-2047

Spicer Z. D. (2018), What is GDPR and why should you care? *International Journal on Innovations in Online Education* 2 (1), 2018.

Tankard, C. (2016). What the GDPR means for businesses. *Network Security*, No. 6.pp.5-8

Tassis, S. & Peristeraki, M., (2014). The Extraterritorial Scope of the "Right to Be Forgotten" and the Rights and Obligations of Search Engine Operators Located Outside the EU, European Networks Law and Regulation 3/2014, *Lexxion Verlagsgesellschaft mbH*.

Tavani, H.T. (1999). Informational privacy, data mining, and the internet. *Ethics and Information Technology*, 1(2), 137–145.

Tavani, H.T. (2007c). Floridi's ontological theory of informational privacy: some implications and challenges, σε K.E. Himma et al. (Eds.). Proceedings of the Seventh International Conference on Computer Ethics: *Philosophical Enquiry (CEPE 2007)*. Centre for Telematics and Information Technology, Enschede, The Netherlands ,pp.385–396, σε Ethics and Information Technology, 10, in press.

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, 34(1), pp.134-153

Vedder, A. H. (2004). KDD, privacy, individuality, and fairness. Χτο E.K. Himma & H.T. Tavani. (Eds.).(2008). The handbook of information and computer ethics. New Jersey, Wiley.

Vilela, N. B., & M. Sousa, (2019). The Impact Of GDPR In The Higher Education – The Case Of The 1st Cycle Of Studies In Law, *Proceedings of EDULEARN19 Conference 1st-3rd July 2019, Palma, Mallorca, Spain*

Vilela, N.B., (2019). Challenges For The Implementation Of The GDPR In Higher Education Institutions In Portugal, *Proceedings of EDULEARN19 Conference 1st-3rd July 2019, Palma, Mallorca, Spain*

Wong, J.C. (22-03-2019), Facebook acknowledges concerns over Cambridge Analytica emerged earlier than reported, διαθέσιμο σε : https://www.theguardian.com/uk-news/2019/mar/21/facebook-knew-of-cambridge-analytica-data-misuse-earlier-than-reported-court-filing

ΝΟΜΟΘΕΤΙΚΑ ΚΕΙΜΕΝΑ

Διεθνή

Ευρωπαϊκή Σύμβαση των Δικαιωμάτων του Ανθρώπου 1950, διαθέσιμη σε https://www.echr.coe.int/Documents/Convention_ELL.pdf [πρόσβαση 16.11.2020]

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.

Κανονισμός (ΕΕ) 2016/679 του ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων), Επίσημη Εφημερίδα Ευρωπαϊκής Ένωσης ΕΕ L 119/1, 4.5.2016

Οδηγία (ΕΕ) 2016/680 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ 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, διαθέσιμη σε: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016L0680&from=EL [πρόσβαση 10.11.2020]

Οδηγία 95/46/ΕΚ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 24ης Οκτωβρίου 1995 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών. Διαθέσιμη σε: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:31995L0046&from=EL [πρόσβαση 16.01.2021]

Οικουμενική Διακήρυξη των Ανθρωπίνων Δικαιωμάτων 1948, διαθέσιμη σε https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/grk.pdf [πρόσβαση 20.11.2020]

Εθνικά

Ν.2068/1992 (ΦΕΚ Α΄118/09.07.1992)

Ν.2251/1994 (ΦΕΚ 191/16.11.1994)

Ν. 2472/1997 (ΦΕΚ Α΄ 50/10.04.1997)

Ν.3471/2006 (ΦΕΚ Α΄133/28.06.2006)

Ν.3783/2009 (ΦΕΚ Α΄136/07.08.2009)

Ο Ν.3917/2011 (ΦΕΚ Α΄ 22/21.02.2011)

Ο Ν. 4070/2012 (ΦΕΚ Α΄ 82/10.04.2012)

Ο Ν.4225/2014 (ΦΕΚ Α΄ 2/07.01.2014)

Ο Ν.4579/2018 (ΦΕΚ Α΄ 201/03.12.2018)

Ν. 4624/2019 (ΦΕΚ Α΄ 137/02.08.2019)

Ν. 4009/2011 (ΦΕΚ Α΄ 195/06.09.2011)

Ν. 4485/2017 (ΦΕΚ Α΄ 114/04.08.2017)

Σύνταγμα της Ελλάδας 27/5/2008 Θ' Αναθεωρητική Βουλή των Ελλήνων

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

Αιτιολογική Έκθεση στο σχέδιο νόμου «Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016, διαθέσιμη σε: https://www.hellenicparliament.gr/UserFiles/2f026f42-950c-4efc-b950-340c4fb76a24/ODHGIA.pdf [πρόσβαση 23.01.2020]

ΝΟΜΟΛΟΓΙΑ

- Απόφαση ΔΕΕ C-131/2-12, Google Spain SL and Google Inc v. Agencia Espanola de Proteccion de Datos and Mario Costeja Gonzales (13-05-2014) http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130dedba4c61f58b547f28acdf409a72ebee7.e34KaxiLc3eQc40LaxqMbN4Pb3aOe0?text=&docid=152065&pageIndex=0&doclang=EL&mode=lst&dir=&occ=first&part=1&cid=762827 [πρόσβαση 19.12.2020]

-Απόφαση ΔΕΕ C-311/18 (16-07-2020), διαθέσιμη σε : http://curia.europa.eu/juris/document/document.jsf;jsessionid=699F5010F9ED77A76EF28

523A1A60EE9?text=&docid=228677&pageIndex=0&doclang=EL&mode=req&dir=&occ=first&part=1&cid=10320201 [πρόσβαση 19.12.2020]

ΓΝΩΜΟΔΟΤΗΣΕΙΣ-ΑΠΟΦΑΣΕΙΣ-ΟΔΗΓΙΕΣ-ΚΑΤΕΥΘΥΝΤΗΡΙΕΣ ΓΡΑΜΜΕΣ

ΑΠΔΠΧ

Ετήσια Έκθεση 2018

Απόφαση υπ' αρ. 77/2016 Απόφασή της διαθέσιμη σε:

Γνωμοδότηση υπ' αρ. 1/2018

Γνωμοδότηση υπ' αρ. 2/2018

Απόφαση υπ' αριθ. 65/2018, Κατάλογος με τα είδη των πράξεων επεξεργασίας που υπόκεινται στην απαίτηση για διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων σύμφωνα με το άρθρο 35 παρ. 4 του ΓΚΠΔ (ΦΕΚ Β' 1622)

WP 29 - ΕΣΠΔ

Ομάδα Εργασίας άρθρου 29, Κατευθυντήριες γραμμές σχετικά με το δικαίωμα στη φορητότητα των δεδομένων, 16/EL, WP 242 rev.01

Ομάδα Εργασίας άρθρου 29, Κατευθυντήριες Γραμμές για την εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) και καθορισμός του κατά πόσον η επεξεργασία «ενδέχεται να επιφέρει υψηλό κίνδυνο» για τους σκοπούς του κανονισμού 2016/679, 17/EN, WP 248 rev.01, p.4.

Ομάδα εργασίας άρθρου 29, Guidelines on Personal data breach notification under Regulation 2016/679, 18/EN, WP 250rev.01.

Ομάδα εργασίας άρθρου 29 για την προστασία των Δεδομένων, 17 EL, WP 253, Κατευθυντήριες γραμμές για την εφαρμογή και τον καθορισμό διοικητικών προστίμων για τους σκοπούς του κανονισμού 2016/679 που εκδόθηκαν στις 3 Οκτωβρίου 2017.

Ομάδα εργασίας του άρθρου 29 για την προστασία των Δεδομένων, 17 EL, WP 253, Κατευθυντήριες γραμμές για την εφαρμογή και τον καθορισμό διοικητικών προστίμων για τους σκοπούς του κανονισμού 2016/679 που εκδόθηκαν στις 3 Οκτωβρίου 2017.

Ομάδα Εργασίας άρθρου 29, Κατευθυντήριες Γραμμές για τη Συγκατάθεση σύμφωνα με το Κανονισμό 2016/679, 17/EN, WP 259.

Ομάδα Εργασίας άρθρου 29 , Κατευθυντήριες Γραμμές σχετικά με τη Διαφάνεια βάσει του κανονισμού 2016/679, 17/EL, WP 260 rev.01

Article 29 Data Protection Working Party, Guidelines on the implementation of the court of Justice of the european union judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (aepd) and Mario Costeja González" C-131/12, WP 225, 14/EN, adopted on 26 November 2014

Article 29 Data Protection Working Party, Opinion 03/2014 on Personal Data Breach Notification, Technical Report March, 2014, 693/14/EN, WP 213, Adopted on 25 March 2014.

Article 29 Data Protection Working Party, Guidelines on Personal data breach notification under regulation 2016/679, Technical Report October, 2017

Article 29 Data Protection Working Party, Guidelines for identifying a controller or processor's lead supervisory authority, 16/EN, WP 244 rev.01, Adopted on 13 December 2016 As last Revised and Adopted on 5 April 2017

Δήλωση σχετικά με τον κανονισμό για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες και τον μελλοντικό ρόλο των εποπτικών αρχών και του ΕΣΠΔ (19-11-2020), διαθέσιμο σε https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_20201119_eprivacy_regulation_el.pdf [πρόσβαση 22.12.2020]

ΟΟΣΑ

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

ΗΛΕΚΤΡΟΝΙΚΕΣ ΠΗΓΕΣ – ΔΙΑΔΙΚΤΥΟ

https://www.aegean.gr/%CF%80%CE%BF%CE%BB%CE%B9%CF%84%CE%B9%CE%BA%CE%AE-%CF%80%CF%81%CE%BF%CF%83%CF%84%CE%B1%CF%83%CE%AF%CE%B1%CF%82-%CE%B4%CE%B5%CE%B4%CE%BF%CE%BC%CE%AD%CE%BD%CF%89%CE%BD-%CF%84%CE%BF%CF%85-%CE%B9%CE%B4%CF%81%CF%8D%CE%BC%CE%B1%CF%84%CE%BF%CF%82-gdpr

https://www.aegean.gr/sites/default/files/static/20/09/uaegean

https://apella.minedu.gov.gr/

http://army.gr/el/organosi/monades-ypiresies/kentro-pliroforikis-ypostirixis-ellinikoy-stratoy-kepyes/pistopoiiseis

https://bqc.gr/iso-27001?gclid=Cj0KCQjwutaCBhDfARIsAJHWnHugAQ_hlDfbK1SXixLO8MXvETtcTkstd-FC4qE0U2gG_XWsV7FKpNQaAvG2EALw_wcB

http://www.asfa.gr/dioikisi/upeuthhnos-gdpr-gr

http://www.asfa.gr/images/prosopika-dedomena.pdf

https://www.aspete.gr/index.php/el/29-2014-02-01-22-33-17/2014-02-01-22-38-47/2014-02-15-19-04-22/1262-gdpr.html

http://files.aspete.gr/aspete/noc/GDPR/Kanonismos_privacy%20notice.pdf

http://files.aspete.gr/aspete/noc/GDPR/Idiotikotika-Kai_Prostasia_Dedomenon.pdf

http://files.aspete.gr/aspete/noc/GDPR/Cookies_ASPETE.pdf
gdpr.pdf

https://www.aueb.gr/el/content/pdguard-neo-kainotomo-logismiko-apo-panepistimiaki-ereyna-sto-oikonomiko-panepistimio

https://www2.aua.gr/el/news-events/nea/odigies-gia-ti-diexagogi-ton-ex-apostaseos-exetaseon

https://asterodos.edu.gr/cookie-policy/

http://astecrete.edu.gr/

https://www.auth.gr/gdpr

https://www.auth.gr/sites/default/files/politiki_prostasias_apth.pdf

https://www.auth.gr/sites/default/files/dilosi_apth_gia_tilekpaideysi-1.pdf

https://www.auth.gr/sites/default/files/politiki_exetaseon_.pdf

https://www.auth.gr/cookie-policy

https://blog.fullfabric.com/how-universities-have-to-adapt-under-the-new-eu-general-data-protection-regulation-gdpr

https://www.dpa.gr/

https://www.dpa.gr/el/polites/gkpd/dikaiwma_diorthwsis

https://www.dpa.gr/el/foreis/ektimisi_adiktipou_kai_diavouleush/ektimisi_adiktipou

https://www.dpa.gr/el/enimerwtiko/thematikes_enotites/diavivaseis_ee

https://www.dpa.gr/el/foreis/ektimisi_adiktipou_kai_diavouleush/ektimisi_adiktipou

https://www.dpa.gr/el/enimerwtiko/thematikes_enotites/diavivaseis_ee/schrems_II

https://www.dpoacademy.gr/el/arthra2/

https://duth.gr/Portals/0/Enhmerosi%20kanonismos.pdf

https://duth.gr/Portals/0/Privacy_Policy.pdfhttps://duth.gr/Portals/0/%20%20%20%20%20%20%20%20%20%20%20.pdf

https://duth.gr/Portals/0/GDPRex20_1.pdf

https://eregister.it.minedu.gov.gr

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_20201119_eprivacy_regulation_el.pdf

https://www.enisa.europa.eu/about-enisa/privacy-policy

https://www.ethemis.gr/2020/06/12/

https://europa.eu/european-union/about-eu/institutions-bodies/european-data-protection-supervisor_en

http://ec.europa.eu/justice/article-29/documentation/index_en.htm

https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_387

https://ec.europa.eu/commission/presscorner/detail/en/MEMO_17_1441

https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=617458

https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=LEGISSUM%3Al33020

https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_el

https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_el

https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:12012P/TXT&from=EN

https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=LEGISSUM%3Al33020.

https://www.europarl.europa.eu/ftu/pdf/el/FTU_4.2.8.pdf

https://fpf.org/blog/gdprhighered/

https://gdpr.ionio.gr/gr/policy/privacy-policy/

https://gdpr.ionio.gr/gr/policy/cookies/

https://www.ihu.gr/privacy-notice-el

https://www.hmu.gr/el/hmu/16346

https://www.hua.gr/index.php/el/

https://www.ihu.gr/cookies-el

https://www.lawspot.gr/nomika-nea/prosopika-dedomena-syllogi-nomologias-apo-dikastirio-tis-eyropaikis-enosis

https://www.lawspot.gr/nomika-nea/eprivacy-ti-provlepei-neo-shedio-toy-kanonismoy-gia-tis-ilektronikes-epikoinonies

https://www.lawspot.gr/nomikes-plirofories/voithitika-kemena/gkpd-oi-neoi-kanones-gia-tin-prostasia-ton-dedomenon-kai-tis

https://legal.heal-link.gr/index.php/personal-data-processing

https://www.panteion.gr/politiki-aporritou/

https://library.panteion.gr/%CF%80%CE%BB%CE%B7%CF%81%CE%BF%CF%86%CE%BF%CF%81%CE%AF%CE%B5%CF%82/%CE%B4%CE%AE%CE%BB%CF%89%CF%83%CE%B7-%CF%80%CF%81%CE%BF%CF%83%CF%84%CE%B1%CF%83%CE%AF%CE%B1%CF%82-%CF%80%CF%81%CE%BF%CF%83%CF%89%CF%80%CE%B9%CE%BA%CF%8E%CE%BD-%CE%B4%CE%B5%CE%B4%CE%BF%CE%BC%CE%AD/

https://pulse.microsoft.com/uploads/prod/2018/03/WorkProductivity_GDPRforEducation_KickStartGuide.pdf

https://www.sans.org/security-resources/policies

https://ssas.army.gr/

https://sse.army.gr/

https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf

https://www.sev.org.gr/Uploads/Documents/51628/meleti_sev_GDPR_final.pdf

https://www.syntagmawatch.gr/trending-issues/nomos-4624-2019-kai-efarmogi-gdpr-polla-yposchomenos-alla-parallila-kathysterimenos/

https://www.theguardian.com/uk-news/2019/mar/21/facebook-knew-of-cambridge-analytica-data-misuse-earlier-than-reported-court-filing

https://www.tuc.gr/fileadmin/various/privacy/%CE%A0%CE%BF%CE%BB%CE%B9%CF%84%CE%B9%CE%BA%CE%AE_%CE%A0%CF%81%CE%BF%CF%83%CF%84%CE%B1%CF%83%CE%AF%CE%B1%CF%82_%CF%84%CE%B7%CF%82_%CE%99%CE%B4%CE%B9%CF%89%CF%84%CE%B9%CE%BA%CF%8C%CF%84%CE%B7%CF%84%CE%B1%CF%82_%CE%BA%CE%B1%CE%B9_%CF%84%CF%89%CE%BD_%CE%A0%CF%81%CE%BF%CF%83%CF%89%CF%80%CE%B9%CE%BA%CF

%8E%CE%BD_%CE%94%CE%B5%CE%B4%CE%BF%CE%BC%CE%AD%CE%BD%CF%89%CE%BD.pdfhttps://www.tuc.gr/index.php?id=10652

https://www.unipi.gr/unipi/el/gdpr.html

https://www.unipi.gr/unipi/images/various/GDPR/UNIPI_GDPR_privacy_policy_short.pdf

https://www.unipi.gr/unipi/images/various/GDPR/Entupo_dilwsis_sugkatathesis_gia_epistimoniki_ereuna.pdf

https://www.unipi.gr/unipi/images/various/GDPR/Entupo_askisis_twn_dikaiomatwn_twn_upokeimenwn_twn_dedomenwn.pdf

https://www.unipi.gr/unipi/images/various/GDPR/Entupo_aitisis_anaklisis_sugkatathesis_twn_upokeimenwn_twn_dedomenwn.pdf

https://www.uniwa.gr/to-panepistimio/politikes-kanonismoi-diadikasies/politiki-gia-ta-prosopika-dedomena-stis-ex-apostaseos-exetaseis/

https://www.uoa.gr/fileadmin/user_upload/main_uoa_images/to_panepisthmio/PolitikiIdiwtikotitas_ProstasiasDedomenwn.pdf

https://www.uoa.gr/fileadmin/user_upload/main_uoa_images/to_panepisthmio/Cookies_Policy_EKPA.pdf

https://www.uoc.gr/university/gdpr.html

https://www.uoc.gr/files/items/7/7133/guidance_for_compliance_with_gdpr.pdf

https://www.uoi.gr/dioikisi/gdpr/https://duth.gr/Portals/0/%20%20%20%20%20%20%281%29.pdf

https://www.uom.gr/downloads/terms/Politiki-Prostasias-UOM.pdf

https://www.uom.gr/terms

https://www.uom.gr/downloads/terms/Potlitiki-Cookies-UOM.pdf

https://www.uowm.gr/to-panepistimio/politiki-poiotitas/politiki-prostasias-prosopikon-dedomenon/https://www.uop.gr/arxiki/prosopika-dedomena

http://www.upatras.gr/el/node/8947

https://www.upatras.gr/sites/www.upatras.gr/files/odigos_symmorfosis_ston_gkpd.pdf

https://www.upatras.gr/sites/www.upatras.gr/files/shedio_asfaleias_pliroforion.pdf

https://www.upatras.gr/sites/www.upatras.gr/files/forma_ypovolis_aitimatos.pdf

https://www.upatras.gr/sites/www.upatras.gr/files/orismos_ypeythynoy_prostasias_dedomenon_ypd_sto_panepistimio_patron_0.pdf

https://www.uth.gr/privacypolicy

https://www.uth.gr/videoepitirisi_uth https://www.uth.gr/news/gkppd-gdpr-binteo-eyaisthitopoiisis

https://www.uth.gr/academicnews/imerides-gdpr-gia-tin-akadimaiki-koinotita-pth

https://www.uth.gr/cookiespolicy

https://el.wikipedia.org/wiki/%CE%91%CE%BD%CF%8E%CF%84%CE%B1%CF%84%CE%B1_%CE%B5%CE%BA%CF%80%CE%B1%CE%B9%CE%B4%CE%B5%CF%85%CF%84%CE%B9%CE%BA%CE%AC_%CE%B9%CE%B4%CF%81%CF%8D%CE%BC%CE%B1%CF%84%CE%B1_%CF%83%CF%84%CE%B7%CE%BD_%CE%95%CE%BB%CE%BB%CE%AC%CE%B4%CE%B1

file:///C:/Users/user/Downloads/IU-pf-01589-13001-gr%20(1).pdf