



ΙΟΝΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

Τμήμα Αρχειονομίας, Βιβλιοθηκονομίας & Μουσειολογίας

Μ.Π.Σ.

**ΔΙΑΧΕΙΡΙΣΗ ΚΑΙ ΑΝΑΔΕΙΞΗ ΠΟΛΙΤΙΣΤΙΚΗΣ
ΠΛΗΡΟΦΟΡΙΑΣ**

*Αρχεία και Δίκτυα Προστασίας
Προσωπικών Δεδομένων*

Μεταπτυχιακή Φοιτήτρια: Ελένη Μπαλού

A.M: MABM201913

Τριμελής Επιτροπή: Μαριέττα Μινώτου, Μανόλης Δρακάκης

Επόπτρια - Διδάσκουσα: Μαρία Μπότη – Κανελλοπούλου

ΚΕΡΚΥΡΑ
Δεκέμβριος 2021

Περιεχόμενα

Περίληψη	3
Abstract	4
Ευχαριστίες	5
1. Εισαγωγή	6
2. Βιβλιογραφική Επισκόπηση	10
3. Αρχεία: Ορισμός και Δίκαιο	14
4. Βασικές Αρχές Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένων	23
5. Προσωπικά Δεδομένα και Ιδιωτικότητα	34
6. Αρχεία και Επεξεργασία Προσωπικών Δεδομένων	44
7. Αρχεία και Ασφάλεια Προσωπικών Δεδομένων	52
8. Δίκτυα Προστασίας Προσωπικών Δεδομένων	60
9. Συμπεράσματα	66
Βιβλιογραφία - Δικτυογραφία	68

Περίληψη

Η παρούσα διπλωματική εργασία έχει ως στόχο να εξετάσει το μείζον ζήτημα των προσωπικών δεδομένων, ως προς την επεξεργασία και διαχείριση τους όπως αυτά αντιμετωπίζονται σε επίπεδο αρχείων και με κύριο προσανατολισμό τα δίκτυα προστασίας των δεδομένων προσωπικού χαρακτήρα. Ειδικότερα, θα εξεταστούν οι έννοιες και οι σχετικοί ορισμοί που αποδίδονται στα αρχεία και τα προσωπικά δεδομένα σε συνάρτηση με το νομικό πλαίσιο, όπως αυτό διαμορφώνεται από τον Γενικό Κανονισμό της ΕΕ (2016/679), τη νομοθεσία στην Ελλάδα για τα Γ.Α.Κ. (ν.4610/2019) αλλά και το ν.4624/2019 περί δεδομένων προσωπικού χαρακτήρα.

Λέξεις - κλειδιά: αρχείο, προσωπικά δεδομένα, ταυτοποίηση, προστασία, Γενικός Κανονισμός 2016/679, ν.4624/2019, δίκτυο, ψηφιακή εποχή

Abstract

The aim of this paper is to examine the major issue of personal data, in terms of their processing and management as they are treated at the file level and with a focus on personal data protection networks. In particular, we will define terms and meanings related to archives, such as files and records, and personal data in relation to the legal framework formulated by the EU General Regulation (2016/679), the legislation in Greece for General Archives and also the greek law 4624/2019 for protecting personal data.

Key - words: file, record, personal data, protection, identifiable living individual, network, EU General Regulation (2016/679), greek law 4610/2019 for General Archives, and 4624/2019 for protecting personal data.

Ευχαριστίες

Θα ήθελα να προσφέρω τις θερμές μου ευχαριστίες στην υπεύθυνη καθηγήτριά μου κυρία Μαρία Κανελλοπούλου - Μπότη για την πολύτιμη βοήθειά της και τον πολύτιμο χρόνο που μου διέθεσε. Οι σημαντικές υποδείξεις και συμβουλές της, με κατεύθυναν σε ένα σωστό τρόπο σκέψης και μου προσέφεραν σημαντικά εφόδια για τη μετέπειτα πορεία μου. Επιπλέον, θα ήθελα να ευχαριστήσω την οικογένειά μου και τους φίλους μου, που σε όλο αυτό το διάστημα των μεταπτυχιακών σπουδών μου συνέχιζαν να ήταν δίπλα μου και να με στηρίζουν.

1. Εισαγωγή

Η παρούσα διπλωματική εργασία εκπονείται στα πλαίσια του Μεταπτυχιακού προγράμματος του Τμήματος Αρχειονομίας, Βιβλιοθηκονομίας και Μουσειολογίας με τίτλο «Διαχείριση και Ανάδειξη Πολιτιστικής Πληροφορίας». Ο τίτλος της είναι *Αρχεία και δίκτυα προστασίας προσωπικών δεδομένων* και φιλοδοξεί να περιγράψει το πλαίσιο που σχηματίζεται μεταξύ των αρχείων και του τρόπου λειτουργίας τους σε συνάρτηση με το μείζον ζήτημα της προστασίας των δεδομένων προσωπικού χαρακτήρα και πιο συγκεκριμένα τα δίκτυα επιστημόνων που δημιουργούνται και λειτουργούν ως πυλώνες προστασίας και διεκδίκησης της ασφάλειας της ιδιωτικής ζωής μέσα στο χαώδη κυκλώνα του διαδικτύου και των νέων τεχνολογιών.

Είναι γεγονός πως η σύγχρονη εποχή την οποία διανύουμε χαρακτηρίζεται έντονα από την έξαρση της επιστήμης της πληροφορίας (Information Science) και της επιστήμης της πληροφόρησης (Library and Information Science) αντίστοιχα, έννοιες που συχνά συγχέονται. Η μεν πρώτη αφορά στην επιστήμη που ερευνά τις ιδιότητες και τη συμπεριφορά της πληροφορίας, τις δυνάμεις που διέπουν τη ροή και τα μέσα επεξεργασίας της για την εξασφάλιση της καλύτερης δυνατής πρόσβασης και χρήσης της. Η δε δεύτερη λειτουργεί ως το απαραίτητο επιστημονικό εργαλείο προσέγγισης, κατανόησης, διαχείρισης και αξιοποίησης του κυρίαρχου συστατικού στοιχείου της ραγδαία αναπτυσσόμενης «Κοινωνίας της Πληροφορίας». Κοινός, λοιπόν, τόπος είναι ότι ως επιστημονικά πεδία περιλαμβάνουν ζητήματα τα οποία αφορούν στην ανάκτηση και ευρετηρίαση των πληροφοριών, με έμφαση αρχικά στα ίδια τα συστήματα και στη συνέχεια στους χρήστες αυτών των συστημάτων.

Από το παραπάνω καθίσταται σαφές ότι η πληροφορία αποτελεί κρίσιμο παράγοντα της ανθρώπινης δραστηριότητας, όπως άλλωστε συνέβαινε και παλιότερα. Όμως, η ειδοποιός διαφορά του σήμερα με το χτες είναι η ραγδαία και συνεχής παραγωγή πληροφορίας σε συνάρτηση με την ακόρεστη ζήτησή της. Η δυναμική εισβολή της τεχνολογίας και του διαδικτύου επέφερε ποικίλες μεταβολές στις υπηρεσίες πληροφόρησης με αποτέλεσμα τη διαμόρφωση ενός νέου πληροφοριακού «γίγνεσθαι». Οι άνωθι, λοιπόν, επιστήμες καλούνται να εργαστούν πάνω στη θεματική της παραγωγής, διανομής, χρήσης, ενσωμάτωσης και διαχείρισης ενός υπέρογκου όγκου δεδομένων, από τα οποία τελικά παράγεται η πληροφορία.

Η χαοτική εξέλιξη και οι τεράστιες δυνατότητες των νέων τεχνολογιών δημιουργίας και επεξεργασίας της πληροφορίας έχουν θέσει δύο σημαντικά ζητήματα «επί τάπητος»: από τη μια την επιστημονική και τεχνολογική επάρκεια όσων εργάζονται σε θέσεις ευθύνης οργάνωσης και διαχείρισης, όπως οι αρχειονόμοι ή/και βιβλιοθηκονόμοι, ώστε να καταστήσουν δυνατή την πρόσβαση στην πληροφορία και από την άλλη η κατοχύρωση του νομικού πλαισίου ώστε να προστατευθεί το υποκείμενο της πληροφορίας ή πιο αναλυτικά των δεδομένων συχνά προσωπικού χαρακτήρα. Στην εποχή των κοινωνικών δικτύων, των ανοιχτών λογισμικών, της πειρατείας πνευματικών έργων, των on-line πλατφορμών πρόσβασης σε αρχεία ποικίλου υποστρώματος έχει αναχθεί ιδιαίτερα το ζήτημα της προστασίας και ασφάλειας των δεδομένων προσωπικού χαρακτήρα και της πνευματικής ιδιοκτησίας.

Στην παρούσα θα δοθεί ιδιαίτερη βάση στο πρώτο ζήτημα, όπως άλλωστε δηλώνεται και στον τίτλο, δηλαδή την προστασία των προσωπικών δεδομένων σε σχέση με τα Αρχεία. Η αφορμή πηγάζει από την έκδοση του Γενικού Κανονισμού περί Προστασίας Προσωπικών Δεδομένων (General Data Protection Regulation, GDPR) το 2016 από την Ευρωπαϊκή Επιτροπή και η περαιτέρω νομική προέκταση και εφαρμογή του ανά κράτος μέλος. Επίσης, ιδιαίτερο ενδιαφέρον παρουσιάζει η δημιουργία των δικτύων των επιστημόνων πληροφόρησης που οργανώθηκαν με στόχο να υποστηρίζουν έργα που ενσωματώνουν την ιδιωτικότητα σε καθημερινά εργαλεία, αναπτύσσουν νέα εργαλεία που μπορούν αποτελεσματικά να προστατεύσουν και να ενισχύσουν το απόρρητο. Εξ' ου λοιπόν και ο συνδυασμός των δύο θεματικών στον τίτλο της διπλωματικής.

Σε ό,τι αφορά τη δομή της εν λόγω εργασίας να σημειωθεί ότι το σύνθετο ζήτημα των Αρχείων και των Δικτύων προστασίας των δεδομένων προσωπικού χαρακτήρα θα χωριστεί σε έξι επιμέρους ενότητες μετά την εισαγωγή. Προτού όμως συμβεί αυτό θα υπάρχει μια αναφορά στη μεθοδολογία της έρευνας και μια συνοπτική βιβλιογραφική ανασκόπηση των πηγών που αξιοποιήθηκαν για τη συγγραφή της παρούσας. Εν συνεχεία, λαμβάνει χώρα το τρίτο κεφάλαιο όπου θα εξεταστούν τα αρχεία σε συνδυασμό με το δίκαιο. Πιο συγκεκριμένα, σε αυτήν την ενότητα θα γίνει λόγος για τα είδη των αρχείων και πως αυτά χωρίζονται καθώς και στη νομική τους προστασία τόσο από το ελλαδικό νομικό πλαίσιο όσο και το διεθνές. Ζητήματα όπως ο κύκλος ζωής των αρχείων, η σχέση τους με τα δεδομένα της πληροφορίας καθώς και τα υποστρώματα που αξιοποιούνται σήμερα είναι ενδεικτικά μόνο στοιχεία του περιεχομένου της εν λόγω ενότητας.

Με την ολοκλήρωση της τελευταίας θα ακολουθήσει το τέταρτο κεφάλαιο υπό τον τίτλο *Βασικές Αρχές Προστασίας Προσωπικών Δεδομένων*. Εκεί θα παρουσιαστεί εξ ολοκλήρου ο Γενικός Κανονισμός, οι έννοιες των προσωπικών δεδομένων, η ανάγκη δημιουργίας του νέου Κανονισμού, η δυναμική του καθώς και το πεδίο εφαρμογής. Επιπλέον, αναφέρονται τα βασικά δικαιώματα, οι αρχές που το διέπουν, οι βασικοί υπεύθυνοι τήρησής του καθώς και τυχόν κυρώσεις που δύναται να επιβληθούν.

Εν συνεχεία, ακολουθεί το πέμπτο κεφάλαιο με τίτλο *Προσωπικά Δεδομένα και Ιδιωτικότητα*. Σε αυτό το σημείο θα αναλυθεί η έννοια του όρου προσωπικά δεδομένα βάσει της ισχύουσας νομοθεσίας και κυρίως δίνοντας ιδιαίτερη βαρύτητα στον σχετικά πρόσφατο κανονισμό της Ευρωπαϊκής Ένωσης από όπου αφορμάται και η επιμέρους νομοθεσία των κρατών μελών. Εν συντομία εδώ να σημειωθεί ότι ως δεδομένα προσωπικού χαρακτήρα λογίζονται όλα εκείνα τα στοιχεία που δύναται να οδηγήσουν σε ταυτοποίηση ενός ατόμου, το οποίο πολλές φορές ονομάζεται ως υποκείμενο δεδομένων, ανεξάρτητα από το αν βρίσκεται εν ζωή ή όχι. Αντίστοιχα, θα οριοθετηθεί και ο όρος της ιδιωτικότητας, μιας και αποτελεί ένα από τα κύρια δικαιώματα του ατόμου και η αχανής λειτουργία του διαδικτύου επιφυλάσσει ποικίλης ισχύος κινδύνους έκθεσης και αναστολής του απορρήτου και της ιδιωτικής ζωής. Καλό είναι σε αυτό το σημείο να αναφερθεί επίσης πως η προστασία του απορρήτου σε οποιαδήποτε μορφή επικοινωνίας αποτελεί ένα συνταγματικά κατοχυρωμένο δικαίωμα βάση του άρ. 19 του Συντάγματος που προστατεύεται τόσο από την εγχώρια νομοθεσία όσο και από τις Οδηγίες και τους Κανονισμούς της Ευρωπαϊκής Ένωσης.

Τα αμέσως επόμενα κεφάλαια έρχονται σε συνάρτηση με τα παραπάνω και κυρίως θα επιχειρηθεί η σύνδεση των προσωπικών δεδομένων με τα Αρχεία, την επεξεργασία τους και την ασφάλεια τους. Ειδικότερα, εφόσον έχουν προσδιοριστεί οι τύποι των αρχείων και των δεδομένων που εκείνα εμπεριέχουν θα προχωρήσουμε σε ένα περαιτέρω προσδιορισμό των προσωπικών δεδομένων που βρίσκονται στις αρχειακές συλλογές και πως εκείνα είναι εφικτό να προστατευτούν κατά τη διάρκεια της συγκέντρωσης, της επεξεργασίας καθώς και της διατήρησής τους. Περιλαμβάνει δηλαδή, ένα σχολιασμό των όρων και των προϋποθέσεων ασφαλείας κατά την επεξεργασία δεδομένων προσωπικού χαρακτήρα, όπως αυτά διατυπώνονται στον Γενικό Κανονισμό και τις Οδηγίες των Ομάδων πληροφόρησης της Ευρώπης.

Στο προτελευταίο κεφάλαιο θα γίνει λόγος για τα δίκτυα προστασίας προσωπικών δεδομένων. Συγκεκριμένα, ως τέτοια ορίζονται οι ομάδες συνεργασίας ευρωπαϊκού ή εθνικού επιπέδου των επιστημόνων της πληροφόρησης και πληροφορικής που ασχολούνται με την τεχνολογία και τεχνογνωσία των μέσων ή/και μέτρων ασφαλείας που εν συνεχεία οι υπεύθυνοι επεξεργασίας των Αρχείων καλούνται να αξιοποιήσουν εξ ορισμού και εκ σχεδιασμού στις υπηρεσίες τους ώστε να επιτευχθούν οι όροι ασφάλειας, ακεραιότητας και διαφάνειας. Στην κατακλείδα της παρούσας θα υπάρχουν τα συμπεράσματα, τα οποία θα φέρουν την μορφή επιλόγου. Στις τελευταίες σελίδες ο αναγνώστης θα είναι σε θέση να αντικρίσει συγκεντρωτικά όλη τη βιβλιογραφία και δικτυογραφία που χρησιμοποιήθηκε προκειμένου να στοιχειοθετηθεί η παρούσα διπλωματική.

2. Βιβλιογραφική Επισκόπηση

Η συγγραφή της παρούσας συνέπεσε με την πρωτόγνωρη συνθήκη της έξαρσης της πανδημίας Covid-19. Οι αλληπάλληλοι αποκλεισμοί και περιορισμοί στην κυκλοφορία και τις δραστηριότητες επέφεραν εμπόδια και κωλύματα στην παραδοσιακή μορφή έρευνας, που είναι αναζήτηση της βιβλιογραφίας και η εξέταση της σε φυσικό περιβάλλον, όπως οι βιβλιοθήκες και τα αναγνωστήρια. Δεν υπήρξε δηλαδή η άμεση δυνατότητα αξιοποίησης των πανεπιστημιακών και άλλων ιδιωτικών ή δημόσιων βιβλιοθηκών, καθώς και άλλων οργανισμών διαχείρισης αρχείων γεγονός που περιόρισε κατά πολύ την πρόσβαση στην παρεχόμενη βιβλιογραφία, χωρίς αυτό να σημαίνει βέβαια ότι δεν χρησιμοποιήθηκε όσο αυτό ήταν εφικτό. Ωστόσο, η ύπαρξη του διαδικτύου και τα ψηφιακά αποθετήρια των πανεπιστημιακών βιβλιοθηκών απάλυνε μερικώς τις απώλειες καθότι σε ένα μεγάλο μέρος τους παρείχαν τη δυνατότητα πρόσβασης στα αρχεία τους.

Σε ό,τι αφορά τη μεθοδολογία που ακολουθήθηκε και με δεδομένη την κύρια χρήση του διαδικτύου για την εύρεση πηγών μελέτης να σημειωθεί ότι αρχικά δόθηκε ιδιαίτερη βάση στην αναζήτηση με λέξεις και όρους κλειδιά σχετικούς με τη θεματική της παρούσας. Ειδικότερα χρησιμοποιήθηκαν κατά κόρον οι λέξεις: αρχεία, ιστορία των αρχείων, δίκτυα, προστασία προσωπικών δεδομένων, ιδιωτικότητα, Ελλάδα, νομοθεσία, Κανονισμός, Ευρωπαϊκή Ένωση, τεχνολογίες πληροφορίας, μέτρα προστασίας, εποχή της πληροφόρησης και συναφείς όρους σχετικά με την επιστήμη της πληροφόρησης. Αντίστοιχα χρησιμοποιήθηκαν οι αγγλικοί όροι records, archives, networks, computer systems, data protection laws, measures for personal data protection. Η αναζήτησή μας είχε αχανή μεν αποτελέσματα όμως οι χρονικοί περιορισμοί βοήθησαν στη περαιτέρω κατηγοριοποίηση και τελική επιλογή των αποτελεσμάτων.

Πιο αναλυτικά, σχετικά με τα βιβλιογραφικά αποτελέσματα, επιλέχθηκαν εν προκειμένω να σχολιαστούν τόσο αυτά που εμφανίζονται περισσότερο στις επόμενες σελίδες όσο και εκείνα που καθόρισαν με τον τρόπο τους τη δομή της παρούσας. Συγκεκριμένα, τέθηκε άτυπα ένας περιορισμός στις νομικές ρυθμίσεις και τις πολιτικές που προβλέπονται από τον πρόσφατο Γενικό Κανονισμό της Ευρωπαϊκής Ένωσης, που αποτέλεσε και το βασικό κείμενο μελέτης για τη συγγραφή του αρκετών κεφαλαίων σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα. Από

το κείμενο του Κανονισμού ήταν εφικτό να κατανοηθούν περαιτέρω οι όροι προσωπικά δεδομένα, προστασία και ασφάλεια ώστε να γίνει δυνατή η απόδοση, το εννοιολογικό και νομικό πλαίσιο που σχετίζεται με τέτοιας φύσης ζητήματα.

Επικουρικά με τον Γενικό Κανονισμό Προσωπικών Δεδομένων (ΓΚΠΔ) (eng: General Data Protection Regulation GDPR) το βιβλίο της Παναγοπούλου – Κούταντζη Φερηνίκη, *Ο Γενικός Κανονισμός για την Προστασία Δεδομένων 679/2016/EE: Εισαγωγή και Προστασία Δικαιωμάτων* καθώς και εκείνο της Μήτρου Λίλιαν, *Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων. Νέο Δίκαιο – Νέες Υποχρώσεις – Νέα Δικαιώματα*, ήταν αναμφισβήτητα κατευθυντήρια και ιδιαίτεως βοηθητικά έτσι ώστε να καταστεί δυνατή η ανάλυση και η εμβάθυνση στον Γενικό Κανονισμό. Επιπροσθέτως, αξιοποιήθηκαν τα κείμενα των οδηγιών τα οποία έχουν εκδοθεί από την Ευρωπαϊκή Επιτροπή και τις Ομάδες πληροφορικής της Ευρωπαϊκής Ένωσης.

Πιο ειδικά, μελετήθηκε το *Handbook on security of personal data processing* το οποίο έχει εκδοθεί από τον Ευρωπαϊκό Οργανισμό για την Ασφάλεια στον Κυβερνοχώρο, από όπου συγκεντρώθηκαν επιπλέον κατευθυντήριες σχετικά με την ασφάλεια, τα μέτρα και τα επίπεδα των κινδύνων που ελλοχεύουν στις ποικίλες εργασίες επεξεργασίας αρχείων και δεδομένων. Στην ίδια βάση μελετήθηκε το κείμενο *Guidance on data protection for archive services: EAG guidelines on the implementation of the General Data Protection Regulation in the archive sector* των European Archives Group, από όπου ελήφθησαν πληροφορίες σχετικά με το πώς εφαρμόζονται οι όροι του Κανονισμού στον τομέα των Αρχείων.

Υπήρχαν, δηλαδή, μέσα στοιχεία που σχολίαζαν την εφαρμογή των κανόνων ασφαλείας, ακεραιότητας και προσβασιμότητας στα πλαίσια των εργασιών ενός Αρχείου, όπως η συγκέντρωση, η ανάλυση και η περιγραφή του υλικού. Με τη λογική της μελέτης του νομικού πλαισίου σε Ευρώπη και Ελλάδα αξιοποιήθηκαν εξίσου οι ιστοσελίδες Ευρωπαϊκής Επιτροπής, της Αρχής Προστασίας Προσωπικών Δεδομένων και της Τράπεζας Πληροφοριών Νομοθεσίας αντίστοιχα. Επιπλέον, σε ό,τι αφορά το διαδίκτυο σημαντικές θεωρούμε τις επίσημες ιστοσελίδες των δικτύων CSIRT και IPEN, όπου επικουρικά συλλέχθηκαν στοιχεία σχετικά με το ρόλο λειτουργίας, το σκοπό και τη δράση τους. Αντίστοιχα λειτούργησε και η ιστοσελίδα της CERT-EU.

Πέραν των διαδικτυακών πηγών υπάρχει και ένας αξιόλογος αριθμός βιβλιογραφίας που αξιοποιήθηκε στην παρούσα. Ξεκινώντας από το έργο της

Κανελλοπούλου Μπότη να σημειωθεί ότι το βιβλίο *Αρχεία και Δίκαιο: Προσωπικά δεδομένα, Πνευματική ιδιοκτησία, Πολιτιστική κληρονομιά* συνδυαστικά με το άρθρο *Privacy and Surveillance: Current aspects and future perspectives* στάθηκαν επάξιοι αρωγοί προς την κατανόηση τόσο του νομικού και εννοιολογικού πλαισίου περί πληροφορίας, προσωπικών δεδομένων, διαχείρισης και ιδιωτικότητας. Πιο συγκεκριμένα, το πρώτο, παρέχει ένα ιδιαίτερα χρήσιμο επεξηγηματικό πλαίσιο σχετικά με τη νομική αντιμετώπιση του τρόπου λειτουργίας των Αρχείων σε σχέση με τον Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ-GDPR), του ελληνικού εφαρμοστικού ν.4624/2019 αλλά και του νέου νόμου ν.4610/2019 για τα Γενικά Αρχεία του Κράτους επιχειρώντας μια σύγχρονη και πολύπλευρη ερμηνεία υπαγωγής της συνήθους δραστηριότητας των Αρχείων στο πλαίσιο προστασίας προσωπικών δεδομένων. Επικουρικά με τα υπόλοιπα κεφάλαια του βιβλίου περί σύνδεσης των Αρχείων με την πνευματική ιδιοκτησία αλλά και πολιτιστική κληρονομιά αλλά και το δεύτερο άρθρο στην αγγλική περί ιδιωτικότητας και παρακολούθησης θα λέγαμε ότι επιχειρείται μια πλουραλιστική προσέγγιση των Αρχείων και συλλογής ή/ και διάθεσης των δεδομένων προσωπικού χαρακτήρα τοποθετημένη στο πολυσύνθετο κλίμα προστασίας του δικαιώματος στην ιδιωτική ζωή.

Από πλευράς βιβλιογραφίας, συνέβαλε ακόμη ιδιαίτερα και το τεκμήριο της Κολυβά Μαριάννας *Εγχειρίδιο Αρχειονομίας: Θεωρητικές προσεγγίσεις. Οργάνωση και σκοποί. Σύγχρονες προκλήσεις*: κυρίως μας κατατόπισε ως προς τη μελέτη και την ανάλυση των όρων και των εννοιών που σχετίζονται με τα αρχεία και τη διαχείριση τους. Πιο συγκεκριμένα, λειτούργησε ως εισαγωγικό τεκμήριο μελέτης περί της επιστήμης της αρχειονομίας, της επιστήμης που μελετά τη διαδικασία γένεσης και παραγωγής των αρχείων, αλλά και που θέτει τους κανόνες επεξεργασίας, πρόσβασης και διασφάλισής τους. Για την ίδια θεματική αξιοποιήθηκε και το βιβλίο του Μπάγια Α. *Αρχειονομία: Βασικές έννοιες και αρχές. Η Οργάνωση των αρχείων για τη διοίκηση και την έρευνα*, όπως επίσης και τον πολύτιμο και ευκρινή οδηγό των Γιαννακόπουλου– Μπουντούρη, *Εισαγωγή στην Αρχειονομία*. Ειδικά, για το τελευταίο να σημειωθεί ότι αποσκοπεί να διευκρινίσει βασικά θέματα γύρω από την επιστήμη της Αρχειονομίας αλλά και των επιστημών πληροφόρησης εν γένει, επιχειρώντας να απαντήσει σε ερωτήματα όπως: τί είναι αρχείο; πως και γιατί δημιουργείται; γιατί τηρούμε τα αρχεία; ποιός ο ρόλος τους στην καθημερινή κοινωνική δραστηριότητα, σε ατομικό και συλλογικό επίπεδο; ποια η σημασία τους για την μελέτη του παρελθόντος;. Εξαιτίας της άμεσης και δομημένης φύσης του

θεωρούμε ότι αποτελεί βασικό συστατικό μιας εργασίας που μελετά ζητήματα τεκμηρίων και αρχείων, όπως η παρούσα.

3. Αρχεία: Ορισμός και Δίκαιο

Από την αρχαιότητα έως και τις μέρες μας παρατηρείται η τάση συγκέντρωσης και φύλαξης δεδομένων που αφορούν στην ανθρώπινη δραστηριότητα αλλά και το περιβάλλον γύρω μας. Με άλλα λόγια, από τη στιγμή που οι κοινωνίες δημιούργησαν θεσμικές και οργανωτικές δομές προέκυψε η ανάγκη καταγραφής των δραστηριοτήτων τους ώστε να εξασφαλιστεί η πρόσβαση στη μνήμη και η διατήρηση στοιχείων που θα βοηθήσουν στην κάλυψη των τρεχουσών αναγκών μιας κοινωνίας. Έτσι υπάρχουν ήδη από την αρχαία Ελλάδα, τη Ρώμη και μετέπειτα τους Μεσαιωνικούς αλλά και τους νεότερους χρόνους της παγκόσμιας ιστορίας στοιχεία σχετικά με τη διαχείριση αρχείων ως απόρροια της γραφής σε φθαρτό υλικό, όπως ο πάπυρος ή το χαρτί.¹ Η γραφή και η τεχνολογία η οποία συνδέεται με αυτή² αποτέλεσε όχι μόνο το μέσο επικοινωνίας (πχ. αλληλογραφία) και συνδιαλλαγής (πχ. συμβόλαια) μεταξύ των συγχρόνων μιας κοινωνίας αλλά συνέβαλε εξίσου και στη διατήρηση της γνώσης από τη μια γενιά στην επόμενη μέσα από τη διαχείριση των ποικίλων παραγόμενων εντύπων.

Εν ολίγοις, λόγω της πολυπλοκότητας της ανθρώπινης δραστηριότητας δημιουργήθηκε η ανάγκη καταγραφής της δια μέσου έντυπων εγγράφων τα οποία περιλαμβάνουν πληροφορίες και δεδομένα σχετικά με την εκάστοτε δραστηριότητα. Νομικής, εκκλησιαστικής, διοικητικής φύσης τεκμήρια συγκεντρώνονται και διαφυλάσσονται ήδη από τους αρχαίους και μεσαιωνικούς χρόνους ώστε να προστατευθεί η εκάστοτε διατήρηση της τάξης και της εξουσίας.³ Το πλαίσιο αυτό αλλάζει από το 1800 και εξής οπότε και παρατηρείται ο εκμοντερνισμός της κοινωνίας ως απόρροια της Γαλλικής Επανάστασης και η δημιουργία μοντέρνων εθνών-κρατών. Η ανάδυση δηλαδή των εθνικιστικών κινημάτων του 19^{ου} αιώνα και η μετέπειτα σχηματοποίηση των εθνικών κρατών ανέδειξαν μια ανάγκη σύνδεσης με την ιστορία των λαών και την τεκμηρίωση αυτής. Έτσι, σημειώνεται η στροφή προς την ιστορική χρήση και αξιοποίηση των αρχειακών τεκμηρίων, με στόχο την ανεύρεση συνδετικών κρίκων του παρόντος με το παρελθόν στα πλαίσια της νέας

¹ Duchein Michel, (1992), "The history of European archives and the development of the archival profession in Europe", in *The American Archivist*, vol. 55, no. 1, pp. 14–25. Available on www.jstor.org/stable/40293621 (last visited 03.8.2021).

² Γιαννακόπουλος Γιώργος – Μπουντούρη Βασιλική, (2015), *Εισαγωγή στην Αρχειονομία*, Αθήνα: ΣΕΑΒ, σελ. 1.

³ Ό.π., σελ. 4.

επιστημονικής ιστορίας⁴ και εισάγοντας σιγά - σιγά τις αρχές διατήρησης και κατηγοριοποίησης τους που οδηγούν ως τις μέρες μας. Πρόκειται για αιώνα σταθμό στην ιστορία των αρχείων, μιας και εφεξής ιδρύονται εθνικά αρχεία ως θεματοφύλακες της ιστορικής μνήμης⁵ ενώ παράλληλα άνοιξε ο δρόμος για τη συστηματική έρευνα υπέρ της ιστορικής επιστήμης.

Τι ορίζεται όμως ως αρχείο; Ο όρος ενέχει τριπλή χρήση μιας και καλείται ανά περίπτωση να εκφράσει είτε το σύνολο των τεκμηρίων ή εγγραφών (eng:records) μιας συλλογής, είτε την αρχειακή υπηρεσία (eng:Archives or manuscript repositories) είτε το κτίριο όπου διατηρείται μια συλλογή ή το αρχειοστάσιο.⁶ Αναγκαία σημείωση σε αυτό το σημείο είναι η διάκριση των αγγλικών όρων archive και record, όπου ο μεν πρώτος έρχεται να εκφράσει ανά περίπτωση κάποιο από τα τρία παραπάνω ενώ ο δεύτερος με σαφήνεια αφορά στις εγγραφές ή τα τεκμήρια που εντοπίζονται σε ένα οργανισμό ή ίδρυμα ανεξαρτήτως μορφοποίησης.⁷ Εκείνο δηλαδή το οποίο μας ενδιαφέρει δεν είναι το υπόστρωμα της καταγραφής σε ένα τεκμήριο αλλά η πληροφορία που αυτό ενέχει στο εσωτερικό του. Στις μέρες μας, όπως θα φανεί και στη συνέχεια, με την εξέλιξη της τεχνολογίας και την εκτόξευση των ηλεκτρονικών συστημάτων διαφαίνεται η διαφοροποίηση των μορφών που δύναται ένα αρχειακό τεκμήριο να έχει, το οποίο συνδέεται άρρηκτα με τις εξελίξεις της ανθρώπινης δραστηριότητας και τις συνήθειές της. Δεν είναι τυχαίο ότι ζούμε στην εποχή της πληροφορίας, η ζήτηση και παραγωγή της οποίας έχει εκτοξευτεί σε απίστευτους ρυθμούς καθορίζοντας δραστικά την κοινωνία.⁸

Ένας πρώτος ορισμός του αρχείου είναι ότι αφορά στο σύνολο των τεκμηρίων ανεξαρτήτως χρονολογίας, ύλης και σχήματος, το οποίο έχει δεχθεί και παραγάγει ένα φυσικό ή νομικό πρόσωπο, στο πλαίσιο των δραστηριοτήτων του.⁹ Ένας πρόσθετος

⁴ Οι Joan M.Shwartz και Terry Cook μας ενημερώνουν ότι «Historians since the mid-nineteenth century, in pursuing the new scientific history, needed an archive that was a neutral repositories of facts». Βλ. Shwartz Joan M.& Cook Terry (2002), *Archives, records and power: The making of modern memory*, Archival Science 2, p.1. Available on <https://link.springer.com/content/pdf/10.1007/BF02435628.pdf> (last visited 13.8.2021).

⁵ Γιαννακόπουλος Γιώργος – Μπουντούρη Βασιλική (2015), *ό.π.*, σελ. 5

⁶ Maygene F. Daniels (1984), *Archives and records management resources*, National Archives 25.08.2016. Available on <https://www.archives.gov/research/alic/reference/archives-resources/terminology.html> (last visited 03.8.2021).

⁷ *Ο.π.*

⁸ Γιαννακόπουλος Γιώργος – Μπουντούρη Βασιλική (2015), *ό.π.*, σελ.49.

⁹ Μπάγιας Α. (1999), *Αρχειονομία: Βασικές έννοιες και αρχές. Η Οργάνωση των αρχείων για τη διοίκηση και την έρευνα*, Αθήνα: Κριτική, σελ.22.

ορισμός της επιστήμης της αρχειονομίας¹⁰ φανερώνει ότι ως αρχεία νοούνται «τα έγγραφα τα οποία δημιούργησε, παρέλαβε και συγκέντρωσε ένα άτομο ή ένας οργανισμός στο πλαίσιο της άσκησης των δραστηριοτήτων του και τα διατηρεί λόγω της διηνεκούς τους χρησιμότητας».¹¹ Ως τέτοια δύναται να χαρακτηριστούν συμβολαιογραφικές πράξεις ή άλλα διοικητικά έγγραφα, φωτογραφίες, σημειωματάρια, ημερολόγια, χάρτες και γενικότερα οποιοδήποτε υλικό που χρησιμεύει για τη διαχείριση των υποθέσεων ενός φυσικού ή νομικού προσώπου στο παρόν και δύναται να παρέχει στο μέλλον χρήσιμα στοιχεία στην έρευνα.

Συγκεντρωτικά, ως αρχειακό υλικό ενός οργανισμού ή ενός ατόμου ορίζεται το σύνολο των τεκμηρίων που περιλαμβάνει μια συλλογή και έχει τα εξής χαρακτηριστικά:

- Έχουν περιεχόμενο, δομή και δημιουργούνται με φυσικό τρόπο σε κάποιο περιβάλλον.
- Αποτελούν απόδειξη πράξεων ή/και συναλλαγών
- Συνδέονται με την εξέλιξη μιας δραστηριότητας
- Αποτελούν απόδειξη ευθύνης
- Διατηρούνται για μικρό ή μεγάλο χρονικό διάστημα ή ακόμη και για πάντα
- Αποτελούν μέρος της μνήμης του οργανισμού που τα παρήγαγε.¹²

Ακόμη, όπως χαρακτηριστικά αναφέρεται από την Αμερικανική Ένωση Αρχειονόμων, ως αρχεία ορίζονται τα τεκμήρια που διαθέτουν διαχρονική αξία και διατηρούνται πέραν της χρησιμότητας των ατόμων που μπορεί να τα συνέθεσαν και για μελλοντική χρήση από άλλους χρήστες καθότι αποτελούν αδιάσειστα στοιχεία του παρελθόντος που μπορούν κάλλιστα να βοηθήσουν στην κατανόηση του παρόντος ή ακόμα και του μέλλοντος.¹³ Στον ίδιο μήκος κύματος το Διεθνές Συμβούλιο Αρχείων (ICA) ορίζει ότι τα αρχεία είναι τα τεκμηριωμένα υποπροϊόντα της ανθρώπινης δραστηριότητας που διατηρούνται για τη μακροπρόθεσμη αξία τους.¹⁴ Επίσης, για να χαρακτηριστεί κάτι ως αρχείο οφείλει να προέρχεται από μια έμπιστη πηγή που

¹⁰ Η αρχειονομία μελετά τις αρχές, τις μεθόδους, την εξελικτική διαδικασία για την αποκατάσταση των αρχείων όπως και τη νομική ρύθμιση της διαχείρισής τους. Στο Κολυβά Μαριάννα (2011), *Εγχειρίδιο Αρχειονομίας: Θεωρητικές προσεγγίσεις. Οργάνωση και σκοποί. Σύγχρονες προκλήσεις*, Αθήνα: Πατάκης, σελ. 19.

¹¹ Κανελλοπούλου – Μπότη Μαρία (2020), *Αρχεία και Δίκαιο: Προσωπικά δεδομένα, Πνευματική ιδιοκτησία, Πολιτιστική κληρονομιά*, Αθήνα: Νομική Βιβλιοθήκη, σελ., 2.

¹² Γιαννακόπουλος Γιώργος – Μπουντούρη Βασιλική (2015), *ό.π.*, σελ. 22.

¹³ Κανελλοπούλου – Μπότη Μαρία (2020), *ό.π.*, σελ. 5.

¹⁴ (2016), “What are archives,” International Council on Archives, <https://www.ica.org/en/what-archive> (last visited 13.8.2021).

συγχρόνως να χαρακτηρίζεται από αυθεντικότητα, αξιοπιστία, ακεραιότητα και ευχρηστία¹⁵ έτσι ώστε να είναι κανείς σε θέση να διατηρήσει το πλαίσιο του και να κατανοήσει πώς, γιατί και ποιος το δημιούργησε καθώς και το περιεχόμενο και τη μορφή του. Εδώ άλλωστε έγκειται και η αξία ενός αρχείου ως καταγεγραμμένης ανθρώπινης μνήμης μέρος της πολιτιστικής κληρονομιάς, επίσημης ή ανεπίσημης.

Επιπρόσθετα, είναι άξιο να αναγνωριστεί το γεγονός ότι οφείλουμε να λογίζουμε τα αρχεία ως καταγραφές από ένα άτομο ή οργανισμό με συγκεκριμένο επίπεδο συμμετοχής και οπτικής της κοινωνίας και όχι ως απόλυτη αλήθεια σχετικά με μια χρονική περίοδο ή γεγονός. Σε αυτό το σημείο να αναφερθεί πως η πλειονότητα των αρχείων όπως ορίζονται παραπάνω αναφέρεται στα ανενεργά ή ιστορικά, εκείνα δηλαδή τα οποία δεν χρησιμοποιούνται πια αλλά λόγω της αξίας τους δεν απορρίπτονται καθώς φυλάσσονται ως επί το πλείστον σε κάποιο δημόσιο φορέα ή μια ιδιωτική βιβλιοθήκη. Τα τελευταία, δηλαδή, οι χώροι αποθήκευσης των τεκμηρίων μπορούν, όπως φάνηκε και νωρίτερα, επίσης να χαρακτηριστούν ως Αρχεία (eng: Archives) με κεφαλαίο το πρώτο γράμμα αποδίδοντας την έννοια του οργανισμού ο οποίος επιφορτίζεται με το έργο της διατήρησης των αρχείων και διασφαλίζει τις προϋποθέσεις πρόσβασης σε αυτά.¹⁶ Η προβληματική εδώ εντοπίζεται στο ότι συχνά συγχέεται ο χώρος φύλαξης ή/και διατήρησης με αυτό καθεαυτό το αρχείο, γεγονός που είναι πέρα για πέρα λανθασμένος εξαιτίας του περιεχομένου και του σκοπού ύπαρξης του καθενός. Πιο συγκεκριμένα, το αρχείο αφορά στα πρωτότυπα και μοναδικά τεκμήρια (πρωτογενείς πηγές) μιας συλλογής, ενώ το Αρχείο στο χώρο φύλαξης και διατήρησης αυτής της τελευταίας που δύναται να περιέχει αντίτυπα των πρωτογενών πηγών καθώς και δευτερογενείς ή άλλες πηγές.

Σημαντικό να τονιστεί ότι το αρχειακό υλικό νομοτελειακά σχεδόν δημιουργείται από τη στιγμή που ένα νομικό ή φυσικό πρόσωπο καταγράφει δεδομένα της δραστηριότητάς του ως μέσο τεκμηρίωσης και απόδειξης αυτής της ίδιας της ενέργειας εξυπηρετώντας άμεσες λειτουργικές ανάγκες. Πρόκειται για αυτό που στην αρχειονομία ορίζεται ως ενεργό ή τρέχων αρχείο, όπου περιλαμβάνονται τεκμήρια που χρησιμοποιούνται σε καθημερινή βάση.¹⁷ Επιπρόσθετα, συναντώνται τα ημιενεργά αρχεία, τα οποία περιλαμβάνουν τεκμήρια που σπανίως αξιοποιούνται και φυλάσσονται μέχρι την τελική τους απόρριψη ή καταστροφή (ανενεργό αρχείο).

¹⁵ Ibid.

¹⁶ Ο.π., σελ., 7.

¹⁷ Γιαννακόπουλος Γιώργος – Μπουντούρη Βασιλική (2015), ό.π., σελ. 24.

Όλα τα παραπάνω φανερώνουν έναν ενιαίο χαρακτήρα σε ό,τι αφορά το αρχειακό υλικό αποδίδοντας τον κύκλο της ζωής του από τη στιγμή της δημιουργίας έως την καταστροφή. Η θεωρία του κύκλου ζωής ή όπως αναφέρεται στην ελληνική βιβλιογραφία η αρχή των τριών ηλικιών¹⁸ των τεκμηρίων ανάγεται στην αγγλοσαξονική παράδοση διαχείρισης του αρχειακού υλικού και διαφοροποιείται από την ευρωπαϊκή, η οποία ορίζει πως οι κανόνες διαχείρισης καθορίζονται από τις διοικητικές ανάγκες ενός οργανισμού και όχι από τη χρονική ακολουθία των φάσεων ύπαρξης του τεκμηρίου.

Σε επίπεδο Ελλάδας ο νόμος 4610/2019, διατυπώνει ότι ως αρχείο ορίζεται «το σύνολο των τεκμηρίων, μαρτυριών και εγγράφων, αδιακρίτως χρονολογίας, σχήματος, ύλης και υποστρώματος, που σχετίζονται με τη δραστηριότητα του Κράτους, των δημοσίων ή ιδιωτικών οργανισμών ή των νομικών ή φυσικών προσώπων ή ομάδων φυσικών προσώπων ή των λοιπών οντοτήτων».¹⁹ Επιπρόσθετα καθορίζεται πως το αρχειακό υλικό περιλαμβάνει πρωτότυπα ή αντίγραφα οποιασδήποτε ύλης ή τεχνικής, ιδίως:

- α) μεμονωμένα έγγραφα, χειρόγραφα, κατάστιχα, κώδικες και συλλογές αυτών,
- β) απομνημονεύματα και ημερολόγια,
- γ) αλληλογραφία επίσημη και ιδιωτική δημοσίων προσώπων,
- δ) προπαγανδιστικά τεκμήρια, εκκλήσεις, προκηρύξεις, αφίσες, εφήμερο υλικό ή άλλα πληροφοριακά έντυπα,
- ε) ηλεκτρονικά έγγραφα και αρχεία ή σε οποιαδήποτε άλλη μορφή, σύμφωνα με την εξέλιξη της τεχνολογίας. Σε αυτή την κατηγορία περιλαμβάνονται και οι κάθε φύσεως βάσεις δεδομένων του δημοσίου τομέα,
- στ) οπτικοακουστικά αρχεία, ηχητικές και κινούμενες ή στατικές οπτικές αποτυπώσεις,
- ζ) χάρτες, σχέδια, χαρακτηριστικά και έργα εικαστικού ενδιαφέροντος, τα οποία αποτυπώνουν μαρτυρίες σε οπτικές, γραμμικές αποτυπώσεις και απεικονίσεις, τοπογραφικά και υδρογραφικά διαγράμματα, μακέτες, αεροφωτογραφίες, ιχνογραφήματα, χαλκογραφίες λιθογραφίες, ξυλογραφίες, που τεκμηριώνουν πληροφορίες, οι οποίες αναφέρονται στην ιστορία και στην πολιτιστική

¹⁸ Ο.π.

¹⁹ ΥΠΕΠΘ, Νόμος Περί Γενικών Αρχείων του Κράτους, <http://www.opengov.gr/ypepth/?p=4833> (τελευταία επίσκεψη 13.8.2021).

κληρονομιά του ελληνικού έθνους και σε ό τι έχει σχέση με τη διοικητική, οικονομική και κοινωνική ζωή του ελληνικού κράτους.²⁰

Στον ίδιο νόμο γίνεται διάκριση των αρχείων στις εξής κατηγορίες:

α) Δημόσια αρχεία, που παράγονται από την ανώτατη πολιτειακή ηγεσία, τις δημόσιες υπηρεσίες, τις δικαστικές αρχές, τα νομικά πρόσωπα δημόσιου δικαίου, τους οργανισμούς τοπικής αυτοδιοίκησης, τα νομικά πρόσωπα ιδιωτικού δικαίου, καθώς και λοιπούς οργανισμούς και επιχειρήσεις που εμπίπτουν στο δημόσιο τομέα, τα ληξιαρχεία, τα συμβολαιογραφεία, τα υποθηκοφυλακεία, τα εκπαιδευτικά ιδρύματα, τα ιδρύματα του Απόδημου Ελληνισμού.

β) Ιδιωτικά αρχεία, όπου συναντώνται τα αρχεία ιδιωτικού περιεχομένου από τη βυζαντινή περίοδο και εξής, τα προσωπικά αρχεία όσων βρέθηκαν σε θέσεις δημόσιου ή θρησκευτικού λειτουργήματος ή διακρίθηκαν στις τέχνες και τα γράμματα, αρχεία πολιτικών κομμάτων και νομικών προσώπων ιδιωτικού δικαίου, όπως δύναται να είναι οι συνεταιρισμοί και οι σύλλογοι. Επιπρόσθετα, σε αυτή την κατηγορία εντάσσονται τα αρχεία οικογενειών, ομάδων φυσικών προσώπων, εμπορικών οίκων, επιχειρήσεων, τραπεζών, εφόσον το περιεχόμενό τους παρουσιάζει ιδιαίτερο ιστορικό ή πολιτιστικό ενδιαφέρον.

γ) Εκκλησιαστικά αρχεία, όπου περιλαμβάνονται τα αρχεία της Εκκλησίας της Ελλάδος, της Εκκλησίας της Κρήτης, των Ιερών Μητροπόλεων Δωδεκανήσου, της Πατριαρχικής Εξαρχίας Πάτμου, των εκκλησιαστικών αρχών, ιδρυμάτων, ιερών ναών, ιερών μονών, καθώς και τα αρχεία των μονών του Αγίου Όρους. Εδώ συμπεριλαμβάνονται και τα αρχεία θρησκευτικών κοινοτήτων, όπως το Ισραηλιτικό Συμβούλιο και στις Ισραηλιτικές Κοινότητες.²¹

Στην πραγματικότητα αυτό που επιχειρείται εδώ είναι η περιγραφή και ο προσδιορισμός από πλευράς νομοθέτη του συνόλου των δραστηριοτήτων που παράγουν αρχειακό υλικό σε μια χώρα και δύναται να αποτυπώσουν τον τρόπο λειτουργίας της κοινωνίας σε μια συγκεκριμένη ή ευρύτερη συνθήκη.

Σε γενικές γραμμές ωστόσο εκείνο που οφείλει κανείς να συγκρατήσει εν προκειμένω είναι ότι τα αρχεία είναι είτε δημόσιου είτε ιδιωτικού χαρακτήρα²² και

²⁰ Ο.π.

²¹ Ο.π.

²² Κανελλοπούλου – Μπότη Μαρία (2020), *ό.π.*, σελ.9.

δύναται να διακριθούν περαιτέρω βάσει της τεκμηριωτικής αξίας τους σε πρωτογενή ή δευτερογενή.²³ Την ευθύνη συγκέντρωσης, διαχείρισης και διαφύλαξης των αρχείων της χώρας αναλαμβάνουν τα Γενικά Αρχεία του Κράτους (Γ.Α.Κ.) και οι εκάστοτε περιφερειακές υπηρεσίες των Γ.Α.Κ. ανά την Ελλάδα. Πρόκειται για μια αυτοτελή δημόσια υπηρεσία με αποστολή τον εντοπισμό, τη συγκέντρωση και διάσωση του αρχειακού υλικού καθώς και την εποπτεία της απρόσκοπτης και ελεύθερης πρόσβασης σε αυτό. Με άλλα λόγια, τα Γ.Α.Κ. επωμίζονται το ρόλο διαχείρισης του πλούτου των πληροφοριών «για κάθε πτυχή της κοινωνικής, πολιτικής, οικονομικής, επιστημονικής, πολιτιστικής και οποιασδήποτε άλλης δραστηριότητας του έθνους».²⁴

Από τα παραπάνω γίνεται αντιληπτό το γεγονός ότι η εξέλιξη της ανθρώπινης δραστηριότητας διαχώρισε και τα είδη των αρχείων. Επιπλέον, οι ραγδαίες τεχνολογικές εξελίξεις από τη δεκαετία του '60 και εξής είχαν ως απόρροια την έκρηξη της πρόσβασης στην πληροφορία και την παραγωγή αυτής, επιφέροντας έναν ακόμη διαχωρισμό των αρχείων αυτή τη φορά ως προς τη μορφολογία. Συγκεκριμένα, στη σύγχρονη εποχή συναντάμε δύο είδη αρχείων. Από τη μια υπάρχουν τα παραδοσιακά έντυπα ή αλλιώς τα λεγόμενα πλέον αναλογικά αρχεία και από την άλλη τα ψηφιακά. Τα τελευταία αφορούν είτε την ψηφιοποιημένη εκδοχή των εντύπων με χαρακτηριστικό ότι η διαχείριση και η πρόσβαση πραγματοποιείται μέσω των ηλεκτρονικών συστημάτων, όπως οι υπολογιστές και οι σαρωτές (σκάνερ), ενώ φαίνεται να λειτουργούν ως προοίμιο για το πως θα γίνουν τα αρχεία στο μέλλον.

Επίσης, χάριν της πλέον διαδεδομένης ηλεκτρονικής επικοινωνίας και διακυβέρνησης σημειώνεται η δημιουργία αποκλειστικά ηλεκτρονικών τεκμηρίων, εγγράφων ή άλλων τύπων. Εδώ εντοπίζεται και το εξής: αν και το αρχείο παραμένει ως αποθήκη πληροφορίας εν τούτοις οι τεχνολόγοι της πληροφορίας προσθέτουν ένα ακόμη ορισμό στην έννοια αρχείο: πρόκειται για κάτι ουδέτερο και μηχανικό που λειτουργεί για τη συσσώρευση πληροφοριών και την ασφαλή φύλαξη, η οποία σαφώς διακρίνεται από την πρότερη θεωρητική των επιστημών της ιστορίας, κοινωνιολογίας και εν γένει κουλτούρας που ήθελε το αρχείο πηγή γνώσης.²⁵

Είναι λοιπόν, γεγονός, ένα μεγάλο μέρος του αρχειακού υλικού παράγεται πλέον σε ψηφιακή μορφή, σηματοδοτώντας το πέρασμα από τη σταθερότητα του

²³ Γιαννακόπουλος Γιώργος – Μπουντούρη Βασιλική (2015),ό.π., σελ. 25.

²⁴ Γενικά Αρχεία του Κράτους, Αρχειομνήμων, <http://arxeiomnimon.gak.gr/> (τελευταία επίσκεψη 13.8.2021).

²⁵ Shwartz Joan M.& Cook Terry (2002), *ibid*, p.5.

χαρτιού και τη φυσική μορφή του εντύπου στα ευμετάβλητα ηλεκτρονικά υποστρώματα της κοινωνίας της πληροφορίας.²⁶ Θα πρέπει να τονιστεί πως η διατήρηση των αρχείων σε ηλεκτρονική μορφή πέραν του γεγονότος ότι δύναται να προσφέρει ελεύθερη πρόσβαση σε όλους ανά πάσα στιγμή από την ευχέρεια του χώρου τους, συμβάλλει αδιαμφισβήτητα στην διατήρησή τους καθώς τα προστατεύει από την αναπόφευκτη φθορά του χρόνου.²⁷ Η ηλεκτρονική εκδοχή φαίνεται να υπερέχει της έντυπης, εξαιτίας της φύσης του υποστρώματος. Το χαρτί ως υλικό υπόστρωμα γραφής ή άλλης καλλιτεχνικής δημιουργίας διακρίνεται από ευπάθεια μιας και οι αυξημένες ανάγκες παραγωγής του έχουν επιφέρει αλλοιώσεις στην ποιότητα των πρώτων υλών και των τελικών προϊόντων, γεγονός που καθιστά ιδιαίτερα απαιτητική τη συντήρηση και διαφύλαξή του.²⁸ Βέβαια, το να πραγματοποιηθεί η ψηφιοποίηση στον τεράστιο όγκο αρχείων που διαθέτει η χώρα μας αλλά και σε παγκόσμιο επίπεδο είναι σαφώς χρονοβόρο και δε μπορεί να συμβεί εν μία νυκτί.

Επιπρόσθετα, είναι αδύνατο να ψηφιοποιηθούν ορισμένα αρχεία που λόγω της παλαιότητας των υλικών τους ή όποια τεχνολογική παρέμβαση μπορεί να κατέλγε σε καταστροφή του αρχείου. Ακόμη, είναι άξιο να σημειωθεί ότι η ηλεκτρονική πραγματικότητα βρίσκεται ακόμη σε καθεστώς επισφάλειας, μιας και η εξάρτηση της από την αντοχή και τη διάρκεια ζωής των ηλεκτρονικών συστημάτων εξαρτάται από τις τεχνολογίες παροχής ρεύματος και δικτύου. Μπορεί παλαιότερα ένας κίνδυνος για τη διαφύλαξη του αρχείου να ήταν η κτιριακή υποδομή που θα απέκλειε κινδύνους φυσικών καταστροφών ωστόσο για τα ηλεκτρονικά αποθετήρια είναι αναγκαία η εξασφάλιση των όρων πρόσβασης σε αυτά, λχ. λειτουργικότητα σέρβερ, αποθήκευση σε περισσότερες τοποθεσίες κτλ. Γι' αυτό άλλωστε και η εποχή μας κρίνεται από τον υβριδικό της χαρακτήρα, όπου η έντυπη και ηλεκτρονική μορφή συνυπάρχουν. Ωστόσο, είναι δεδομένο ότι η πρόκληση του σήμερα αλλά και του μέλλοντος είναι η διαχείριση ενός τεράστιου όγκου πληροφορίας και τεκμηρίων σε ψηφιακή μορφή, που ολοένα και περισσότερο κερδίζει έδαφος έναντι των παραδοσιακών έντυπων.

Ολοκληρώνοντας, είναι σημαντικό να αναφερθεί ότι η αυξημένη παραγωγή πληροφορίας δημιουργεί έναν εξίσου τεράστιο όγκο δεδομένων, ο οποίος εκτινάσσεται και από τον αντίστοιχα τεράστιο όγκο των μεταδεδομένων τους. Τα

²⁶ Γιαννακόπουλος Γιώργος – Μπουντούρη Βασιλική (2015), *ό.π.*, σελ. 50.

²⁷ Κανελλοπούλου – Μόπη Μαρία (2020), *ό.π.*, 11.

²⁸ Ζερβός Σπύρος (2015), *Συντήρηση και διατήρηση χαρτιού, βιβλίων και αρχειακού υλικού*, ΣΕΑΒ, Αθήνα, σελ.27.

τελευταία δεν είναι τίποτε παραπάνω από τα δεδομένα που δημιουργούνται σχετικά με τα αρχικά δεδομένα (data about data): δηλαδή δεδομένα που περιγράφουν, ερμηνεύουν, εντοπίζουν ή διευκολύνουν την ανάκτηση, τη χρήση και τη διαχείριση ενός πληροφοριακού πόρου.²⁹ Η διαχείριση δεδομένων δεν είναι κάτι καινούριο για έναν αρχειονόμο ή την αντίστοιχη υπηρεσία φύλαξης. Ωστόσο, εκείνο που αποτελεί πρόκληση είναι ο τεράστιος όγκος των δεδομένων που δημιουργείται καθημερινά και απαιτεί διαχωρισμό, ταξινόμηση κτλ. Τα μεταδεδομένα άλλωστε δημιουργούνται μέσα από συγκεκριμένα πρότυπα περιγραφής που καθορίζονται από τους επαγγελματίες της πληροφορικής. Οι διάφορες εντολές αυτοματοποίησης των υπολογιστικών συστημάτων λειτουργούν προσθετικά και υπέρ μας, μειώνοντας κάπως το χρόνο καταχώρησης, ευρετηρίασης και οργάνωσης των πληροφοριακών πόρων. Όμως παράλληλα δημιουργείται η πρόκληση της αναγνωσιμότητας των ψηφιακών αρχείων αλλά και η ανάγκη περαιτέρω προστασίας των προσωπικών δεδομένων που αυτά περιέχουν.

²⁹ Society of American Archivists <https://dictionary.archivists.org/entry/metadata.html>

4. Βασικές Αρχές Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένων

Τα προσωπικά δεδομένα αποτελούν ευαίσθητα ατομικά δεδομένα τα οποία δεν θα πρέπει να διοχετεύονται οιοδήποτε εκτός κι αν υπάρχει η συγκατάθεση του εν λόγω προσώπου ή κάποια εισαγγελική παρέμβαση και γι' αυτό το λόγο ακριβώς προστατεύονται από το σύνταγμα αλλά και από διεθνείς συμβάσεις και συνθήκες. Ο Γενικός Κανονισμός της Ευρωπαϊκής Ένωσης 679/2016 ή General Data Protection Regulation (GDPR) φαίνεται να εξελίσσει ένα βήμα παραπάνω τα όσα ίσχυαν μέχρι πρότινος με βάση την προϋπάρχουσα Οδηγία. Αποτελείται από 99 άρθρα στο σύνολό του με τη δυνατότητα κάποια από αυτά να μπορούν να παρεκκλίνουν ανάλογα τις συνθήκες.

Ο νέος νόμος αρχίζει να τίθεται σε εφαρμογή στις 25 Μαΐου του 2018 έχοντας ως κύριο στόχο και μόνο την ακόμη μεγαλύτερη προστασία των προσωπικών δεδομένων των ανθρώπων καθότι η προηγούμενη Οδηγία 95/46/EK αν και ήδη ρηξικέλευθη για την εποχή της δεν έπαυε να υστερεί πλέον λόγω και μόνο του πέρατος των ετών. Άλλωστε έχοντας περάσει περίπου είκοσι χρόνια από την έκδοσή της, η τεχνολογική ανάπτυξη που συνέβη αυτά τα έτη ήταν τεράστια, γεγονός το οποίο δεν μπορούσε να ακολουθήσει. Να αναφερθεί ότι στην Οδηγία 95/46/EK βασίστηκε και ο ελληνικός ν.2472/97, που αποτελεί ορόσημο στην ιστορία της προστασίας προσωπικών δεδομένων.³⁰

Αρχικά, είναι ένα απαραίτητο εργαλείο για την ολοκλήρωση της ευρωπαϊκής εσωτερικής αγοράς. Οι άνθρωποι, τα αγαθά, οι υπηρεσίες, τα κεφάλαια πρέπει να κυκλοφορούν ελεύθερα εντός της Ευρωπαϊκής Ένωσης και οι διαφορετικοί κανόνες για την προστασία των προσωπικών δεδομένων εμποδίζουν αυτήν την ελεύθερη κυκλοφορία. Σημαντική επίσης είναι η ασφάλεια δικαίου για την ενίσχυση της εμπιστοσύνης των πολιτών στην κοινωνία της πληροφορίας και της απελευθέρωσης και εξέλιξης της αγοράς της πληροφορικής και των συναφών υπηρεσιών στην Ευρώπη. Ο Κανονισμός δηλώνει αυτή τη σχέση μεταξύ της προστασίας των προσωπικών δεδομένων από τη μια πλευρά και των αναγκών για ελεύθερη διακίνηση των πληροφοριών από την άλλη. επίσης, εντός της Ευρωπαϊκής Ένωσης η προστασία των ατομικών δικαιωμάτων διαδραματίζει πρωτεύοντα ρόλο από τη στιγμή που η

³⁰ Παναγοπούλου – Κουτναντζή Φερενίκη, (2017), *Ο Γενικός Κανονισμός για την Προστασία Δεδομένων 679/2016/ΕΕ*, Αθήνα: Σάκκουλα, σελ., 23.

κοινή αγορά έχει πάψει να αποτελεί μοναδικό σκοπό της Ευρωπαϊκής Ένωσης και η Συνθήκη του Μάαστριχτ άρχισε να αλλάζει τα δεδομένα στα θεμελιώδη δικαιώματα.³¹

Μέσα σε λίγα χρόνια ανεξαρτήτως κοινωνικού υπόβαθρου ή οικονομικής κατάστασης η πλειονότητα των ανθρώπων διαθέτει κινητό τηλέφωνο το οποίο με τη σειρά του δύναται να έχει πρόσβαση στο διαδίκτυο. Επιπλέον σχεδόν όλοι διαθέτουν ηλεκτρονικό υπολογιστή στις οικίες τους. Συνεπώς, όπως γίνεται αντιληπτό το πρόβλημα με την ασφάλεια των προσωπικών δεδομένων άρχισε να γιγαντώνεται ένεκα της νέας τάξης που εδραιώθηκε και δεν είναι άλλη από την ψηφιακή εποχή. Βέβαια, αξίζει να σημειωθεί ότι όπως κάθε αλλαγή έτσι και αυτή στην αρχή συνάντησε δυσκολίες ως προς την υλοποίησή της διότι το ρυθμιστικό πλαίσιο των εθνικών νομοθεσιών ήταν ήδη υπαρκτό και πολύπλοκο.

Πιο συγκεκριμένα, η κριτική αφορούσε ενστάσεις και επιφυλάξεις καθώς η δεσμευτική ισχύς του Κανονισμού ερχόταν σε αντίθεση με τις εθνικές αντιλήψεις και προτιμήσεις για τον τρόπο προστασίας προσωπικών δεδομένων, θεωρήθηκε ότι βασίζεται σε συγκεντρωτική και μονοπωλιακή νομοθέτηση ενώ άφηνε πολύ μικρά περιθώρια για μελλοντικές διαφορετικές πολιτικές προστασίας των εκάστοτε κρατών μελών της Ε.Ε. Επί παραδείγματι, στη Γερμανία το ομοσπονδιακό συμβούλιο ανέφερε τον κίνδυνο πλήρους αποκλεισμού των εθνικών ρυθμίσεων. Η Αγγλία τότε εξέφραζε φόβο ότι η χώρα τους θα γινόταν λιγότερο ελκυστική για επενδύσεις από εταιρείες των Η.Π.Α λόγω των υποχρεώσεων στον τομέα των προσωπικών δεδομένων.³²

Ο Κανονισμός εξειδίκευσε και συμπλήρωσε τις βασικές αρχές επεξεργασίας προσωπικών δεδομένων με περισσότερες απαιτήσεις και προϋποθέσεις και συνάρτησε το σύννομο χαρακτήρα της επεξεργασίας με τη θεμελίωσή της σε μία από τις περιοριστικά απαριθμούμενες βάσεις επεξεργασίας. Ο κοινοτικός νομοθέτης κατοχύρωσε τα δικαιώματα των προσώπων αλλά παράλληλα αναγνώρισε και τον πρωταρχικό ρόλο των ανεξάρτητων ελεγκτικών αρχών για την αποτελεσματική προστασία των προσωπικών δεδομένων. Η Ευρωπαϊκή Ένωση απέδιδε ιδιαίτερη βαρύτητα στο ζήτημα προστασίας προσωπικών δεδομένων και αυτό αποτυπώθηκε και στην Συνθήκη του Άμστερνταμ (1997) και με το χάρτη θεμελιωδών δικαιωμάτων

³¹ Μήτρου Λίλιαν, (2017), *Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων. Νέο Δίκαιο – Νέες Υποχρεώσεις – Νέα Δικαιώματα*, Αθήνα: Σάκκουλα, σελ., 11-12.

³² Ο.π., σελ., 34.

της Ε.Ε. καθώς και με τη Συνθήκη της Λισσαβόνας (2009) κατά την οποία ο χάρτης κατέστη νομικά δεσμευτικός ως πρωτογενές ενωσιακό δίκαιο. Τα δικαιώματα που κατοχύρωνε ο χάρτης αποτέλεσαν βασικό γνώμονα σε αποφάσεις του ενωσιακού δικαστηρίου με τις οποίες δήλωνε τη βούλησή του να εφαρμόσει αυστηρό έλεγχο σεβασμού της ιδιωτικότητας και της προστασίας προσωπικών δεδομένων σε όλους του τομείς, δημόσιους και ιδιωτικούς εντός και εκτός της Ευρωπαϊκής Ένωσης.³³

Ωστόσο, καίριες αλλαγές στην τεχνολογία σε όλους τους τομείς έκριναν την ανάγκη για περαιτέρω εναρμόνιση του θεσμικού πλαισίου. Πρέπει να αναφερθεί ότι η ανάγκη για τη δημιουργία ενός νέου Κανονισμού δεν οφείλεται μόνο στην τεχνολογική επανάσταση και την ψηφιακή εποχή. Επιπρόσθετοι λόγοι ήταν η άμετρη μεταβίβαση προσωπικών δεδομένων σε τρίτους, η παράνομη πώλησή τους, η μη τήρηση βασικών αρχών ή ακόμα και η έλλειψη μέτρων ασφαλείας, η απόκρυψη περιστατικών παραβίασης, οι διαφορές που υπήρχαν στο νομοθετικό πλαίσιο των υπόλοιπων κρατών μελών της Ευρωπαϊκής Ένωσης κ.ά.

Η σταδιακή εξέλιξη του κόσμου σε μία δικτυωμένη κοινωνία που τα προσωπικά δεδομένα συλλέγονται ανταλλάσσονται, επαναχρησιμοποιούνται καθιστά όλο και περισσότερο σαφές ότι επικοινωνία και προστασία προσωπικών δεδομένων είναι αλληλοεξαρτώμενες διαδικασίες με τους ίδιους τους χρήστες να είναι σημαντικοί «παίκτες» του συστήματος (web2.0, web3.0). Ακόμα, είναι προφανές ότι στην κοινωνία της πληροφορίας η αλματώδης ανάπτυξη τεχνολογιών επικοινωνίας και πληροφορίας αλλάζει άρδην τον τρόπο και την έκταση συλλογής και επεξεργασίας προσωπικών δεδομένων. Η παγκοσμιοποίηση οικονομικών και κοινωνικών δικτύων, η πληροφορία της πληροφορίας που υπερβαίνει τα εδαφικά σύνορα και η τεχνολογική υποδομή των δικτύων καθιστά τη συλλογή και χρήση των πληροφοριών εύκολη και προσιτή οικονομικά. Στο πλαίσιο αυτής της παγκοσμιοποιημένης και ανταγωνιστικής αγοράς τα προσωπικά δεδομένα και η πίεση για την αξιοποίησή τους αποτελούν μείζον διακύβευμα.³⁴

Συνεπώς, ένα από τα βασικά στοιχεία του νέου Κανονισμού αφορά την ιδιαιτερότητα της ψηφιακής εποχής και πώς θα καταφέρει να προστατέψει τους πολίτες από τη διαρροή των δεδομένων τους δίχως τη συγκατάθεσή τους. Η Ευρωπαϊκή Ένωση επέλεξε τη δημιουργία ενός Κανονισμού εγκαταλείποντας τη μέθοδο των Οδηγιών αποβλέποντας στη δημιουργία μιας πιο συνεκτικής ρύθμισης,

³³ Ο.π., σελ., 15.

³⁴ Ο.π., σελ., 25-26, 28-29.

στην εναρμόνιση των εθνικών κανόνων, στην απλούστευση των διαδικασιών και στη μείωση του κόστους συμμόρφωσης κυρίως για εταιρείες που δραστηριοποιούνται σε περισσότερες χώρες της Ε.Ε.

Η εκπόνηση του νέου Κανονισμού υπήρξε διαδικασία μακρόχρονη και επίμονη. Υπήρξε αποτέλεσμα πενταετούς συζήτησης στο πλαίσιο των θεσμών και το συμβούλιο κατέληξε στην υιοθέτηση μιας κοινής θέσης τον Ιούνιο του 2015. Ο Κανονισμός επισφραγίζει τα θεμελιώδη δικαιώματα και ειδικότερα το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα. Διατήρησε την έννοια της επεξεργασίας ως έναν γενικό όρο που περιλαμβάνει κάθε πράξη που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων σε δεδομένα προσωπικού χαρακτήρα, αναφερόμενος σε όλο το κύκλο της ζωής των δεδομένων από τη συλλογή έως την καταστροφή τους με σκοπό να εξασφαλίσει μια ευρεία πλατφόρμα υποδοχής ώστε κάθε μορφή επεξεργασίας να εμπίπτει στο ρυθμιστικό του πλαίσιο.³⁵

Για λόγους ασφάλειας δικαίου και ερμηνείας ορίστηκαν διακριτά τρεις μορφές επεξεργασίας:

1. Περιορισμός της επεξεργασίας.³⁶
2. Κατάρτιση προφίλ.³⁷
3. Ψευδωνυμοποίηση.³⁸

Ο Κανονισμός επίσης, ενσωματώνει την αρχή της λογοδοσίας. Αυτό σημαίνει αυτόματα ότι ο/η υπεύθυνος/η της επεξεργασίας θα πρέπει να είναι σε θέση να αποδείξει ότι έχουν ληφθεί όλα τα απαραίτητα μέτρα για τη διαφύλαξη των προσωπικών δεδομένων. Εν συνεχεία, τα υποκείμενα ή αλλιώς οι ιδιοκτήτες των προσωπικών δεδομένων επιφορτίζονται με επιπλέον δικαιώματα, τα οποία οι

³⁵ Ο.π., σελ., 42.

³⁶ Κανονισμός (ΕΕ) 2016/679, σελ. 33. Διαθέσιμο στο: <https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016R0679&from=EL> (τελευταία επίσκεψη 13.8.2021), άρθρο 4, παρ. 3: «η επισήμανση αποθηκευμένων δεδομένων προσωπικού χαρακτήρα με στόχο τον περιορισμό της επεξεργασίας τους στο μέλλον».

³⁷ Κανονισμός (ΕΕ) 2016/679, άρθρο 4, παρ. 4: «οποιαδήποτε μορφή αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα που συνίσταται στη χρήση δεδομένων προσωπικού χαρακτήρα για την αξιολόγηση ορισμένων προσωπικών πτυχών ενός φυσικού προσώπου, ιδίως για την ανάλυση ή την πρόβλεψη πτυχών που αφορούν την απόδοση στην εργασία, την οικονομική κατάσταση, την υγεία, τις προσωπικές προτιμήσεις, τα ενδιαφέροντα, την αξιοπιστία, τη συμπεριφορά, τη θέση ή τις μετακινήσεις του εν λόγω φυσικού προσώπου».

³⁸ Κανονισμός (ΕΕ) 2016/679, άρθρο 4, παρ. 5: «η επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο ώστε τα δεδομένα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρωματικές πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλιστεί ότι δεν μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο».

υπεύθυνοι επεξεργασίας δεν πρέπει να αμελούν. Η λογοδοσία σε συνδυασμό με την ασφάλεια των προσωπικών δεδομένων δημιουργούν μια διαφορετική αντίληψη ως προς τη σχέση νομικής ρύθμισης, τεχνικής διασφάλισης και ευθύνης όσων επεξεργάζονται τα δεδομένα. Διατηρείται η διάκριση σε κατηγορίες δεδομένων ανάλογα με το είδος τους για τις ατομικές ελευθερίες και την ιδιωτική σφαίρα επιβεβαιώνοντας ότι υπάρχουν ορισμένες κατηγορίες δεδομένων οι οποίες με βάση το περιεχόμενό τους επιφέρουν κίνδυνο προσβολής αυτής της σφαίρας. Στις ειδικές κατηγορίες που υπήρχαν παλαιότερα στην Οδηγία ο Κανονισμός προσθέτει τα γενετικά και βιομετρικά δεδομένα.³⁹ Έτσι λοιπόν, συνδυάζεται η ενίσχυση της λογοδοσίας με απαιτήσεις για περισσότερη διαφάνεια και υποχρέωση αντικτύπου.

Η εφαρμογή του Κανονισμού περιλαμβάνει όλους τους φορείς που μπορεί να υπάρχουν, από ιδιωτικές και δημόσιες επιχειρήσεις έως και τις κρατικές αρχές, καθώς όλοι οι παραπάνω φορείς έχουν τη δυνατότητα να αποθηκεύουν, να επεξεργάζονται και να μεταβιβάζουν προσωπικά δεδομένα είτε οι πολίτες διαμένουν εντός του πλαισίου της Ευρωπαϊκής Ένωσης, είτε εκτός καθότι δεν παύουν να διαθέτουν την ιδιότητα του ευρωπαίου πολίτη. Μία βασική φιλοδοξία του Κανονισμού είναι το εδαφικό πεδίο εφαρμογής του νέου δικαίου με γνώμονα να μην στερούνται τα φυσικά πρόσωπα την προστασία που δικαιούνται βάση του Κανονισμού ακόμη και όταν η επεξεργασία των δεδομένων τους γίνεται από άτομα που δεν είναι στην Ε.Ε.

Αναλύοντας λοιπόν, στο παρόν κεφάλαιο τις βασικές αρχές του Κανονισμού θα πρέπει να γίνει αντιληπτό ότι τα προσωπικά δεδομένα δεν σχετίζονται επ' ουδενί με τον περιορισμό της ελευθερίας της έκφρασης κάτι το οποίο τονίζεται ιδιαίτερα εντός του κειμένου, καθότι με το άρθρο 85Κ κατοχυρώνεται η ελευθερία της έκφρασης καθώς αποτελεί ένα εξίσου θεμελιώδες δικαίωμα. Ο νέος Κανονισμός λοιπόν, έρχεται για να συμβάλει στη διατήρηση των υπαρχόντων δικαιωμάτων αλλά και στη δημιουργία νέων όπου κρίνεται απαραίτητο.

³⁹ Κανονισμός (ΕΕ) 2016/679, άρθρο 4, παρ. 13,14, 15: 13: «γενετικά δεδομένα, τα δεδομένα προσωπικού χαρακτήρα που αφορούν τα 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 την φυσιολογία ή την υγεία του εν λόγω φυσικού προσώπου», 14: «βιομετρικά δεδομένα, δεδομένα προσωπικού χαρακτήρα τα οποία προκύπτουν από ειδική τεχνική επεξεργασία συνδεδεμένη 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», και 15: «δεδομένα που αφορούν την υγεία, δεδομένα προσωπικού χαρακτήρα τα οποία σχετίζονται με τη 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»

Τα βασικότερα δικαιώματα συγκεντρωτικά είναι τα ακόλουθα:

- Δικαίωμα στη λήθη
- Ενίσχυση της παιδικής προστασίας
- Δικαίωμα στη φορητότητα
- Ενημέρωση σε περίπτωση παραβίασεως
- Δικαίωμα στην ανθρώπινη παρέμβαση
- Δικαίωμα περιορισμού της επεξεργασίας.⁴⁰

Αντίστοιχα, οι βασικές υποχρεώσεις του υπεύθυνου επεξεργασίας είναι οι εξής:

- Λήψη κατάλληλων τεχνικών και οργανωτικών μέτρων
- Δημιουργία κατά το σχεδιασμό (privacy by design) και εξ ορισμού κατάλληλης δομής (privacy default)
- Υποχρέωση ενημερώσεως εποπτικής αρχής και υποκειμένου δεδομένων
- Κατάρτιση μελέτης εκτιμήσεως επιπτώσεων
- Κατάρτιση πολιτικής ασφαλείας και κωδίκων δεοντολογίας
- Τήρηση αρχείων δραστηριοτήτων
- Ορισμός υπευθύνου προστασίας δεδομένων.⁴¹

Ένα από τα σημάδια ενίσχυσης των υποχρεώσεων του εκτελούντος την επεξεργασία στον Κανονισμό ως προς την προστασία των δεδομένων είναι η υπογραφή συμβάσεων ανάμεσα στον υπεύθυνο και στον εκτελών καθώς και στην τήρηση εγκεκριμένου κώδικα δεοντολογίας ή ενός εγκεκριμένου μηχανισμού πιστοποιήσεως. Σε περίπτωση που αυτό δεν τηρηθεί στο έπακρο και υπάρχει διαρροή δεδομένων και ο εκτελών αλλά και ο υπεύθυνος υπόκεινται σε κυρώσεις.

Όπως σε κάθε Οδηγία ή Νόμο έτσι και σε αυτήν την περίπτωση του Κανονισμού υπάρχουν βασικά ζητήματα προβληματισμού όπως είναι η καθιέρωση της αρχής του σκοπού επεξεργασίας, το ζήτημα της συγκατάθεσης και το κόστος επιτηρήσεως και ενίσχυση της γραφειοκρατίας.⁴²

Οι βασικές αρχές του Γενικού Κανονισμού στηριζόμενοι στην αρχή της λογοδοσίας είναι οι ακόλουθες:

⁴⁰ Παναγοπούλου – Κουτναντζή Φερενίκη, ό.π., σελ., 28-30.

⁴¹ Όπ., σελ., 32-34.

⁴² Ό.π., σελ., 35.

- Αρχή της λογοδοσίας, όπου ο υπεύθυνος επεξεργασίας και ο εκτελών θα πρέπει να αποδείξουν ότι συμμορφώνονται στα όσα υποστηρίζονται στον Κανονισμό.
- Αρχή νομικής, αντικειμενικής και διαφανούς επεξεργασίας.
- Αρχή του περιορισμού του σκοπού.
- Αρχή ελαχιστοποίησης των δεδομένων, τόσο στον όγκο των δεδομένων όσο και στη διάρκεια διατήρησής τους.
- Αρχή της ακρίβειας των δεδομένων και εν γένει η εγκυρότητα αυτών.
- Αρχή της ακεραιότητας και της εμπιστευτικότητας.
- Αρχή του περιορισμού της περιόδου αποθήκευσης (για ένα μόνο συγκεκριμένο χρονικό διάστημα),
- Αρχή της αναλογικότητας.⁴³

Στο εν λόγω κεφάλαιο δε θα μπορούσε να παραληφθεί να γίνει λόγος για τα κατοχυρωμένα δικαιώματα που προβάλλονται μέσα από τον Γενικό Κανονισμό. Αυτό περιλαμβάνει συνοπτικά τα ακόλουθα -καθότι αναλύονται στις επόμενες σελίδες- :

- Προστασία των δικαιωμάτων των παιδιών. Τα παιδιά αποτελούν μια ευάλωτη κοινωνική ομάδα και συνεπώς έτσι αντιμετωπίζονται. Σε περίπτωση λοιπόν, που κάποιος παραβιάσει τα δικαιώματά τους επιβάλλεται χρηματική ποινή που αγγίζει τα 10.000.000 ευρώ.
- Δικαιώματα ενημέρωσης ή γενική αρχή διαφάνειας, τα οποία περιλαμβάνουν την ενημέρωση του υποκειμένου δεδομένων, την ενημέρωση των αποδεκτών και την ενημέρωση περαιτέρω υπευθύνων επεξεργασίας σε περιπτώσεις διαγραφής δεδομένων.
- Δικαίωμα προσβάσεως.
- Δικαίωμα διορθώσεως.
- Δικαίωμα διαγραφής ή λήθης.
- Δικαίωμα περιορισμού της επεξεργασίας.
- Δικαίωμα φορητότητας δεδομένων, το οποίο για να εφαρμοστεί προϋποθέτει νομική βάση συγκαταθέσεως ή συμβάσεως, αυτοματοποιημένη επεξεργασία, χορήγηση δεδομένων από το υποκείμενο των δεδομένων, μη επέμβαση στα δικαιώματα τρίτων, χορήγηση δεδομένων σε δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα διαλειτουργικό

⁴³ Ο.π. και Μήτρου Λίλιαν, ό.π.

μορφότυπο, ενημέρωση εκ μέρους του υπευθύνου επεξεργασίας, εξακρίβωση της ταυτότητας του υποκειμένου των δεδομένων, προθεσμία ικανοποίησης του δικαιώματος, η ασφάλεια των δεδομένων.

- Δικαίωμα εναντίωσης.
- Δικαίωμα στην ανθρώπινη παρέμβαση.⁴⁴

Κρίνεται σκόπιμο να σταθεί κανείς λίγο παραπάνω στον Υπεύθυνο Επεξεργασίας ο οποίος, υπήρχε και στην προηγούμενη Οδηγία. Εκείνο που προστέθηκε στον νέο Κανονισμό είναι ο Εκτελών την επεξεργασία. Σε περιπτώσεις που παραβιαστούν τα προσωπικά δεδομένα και οι δύο παραπάνω βρίσκονται αντιμέτωποι με νομικές κυρώσεις και χρηματικές αποζημιώσεις έναντι του υποκειμένου. Ο Υπεύθυνος Επεξεργασίας επιφορτίζεται με μια σειρά αρμοδιοτήτων. Συνοπτικά είναι εκείνος που πρέπει να ενημερώσει έγκαιρα την Αρχή σε περίπτωση απώλειας ή εμπιστευτικότητας των δεδομένων. Είναι επιφορτισμένος να παρακολουθεί συνεχώς τις διαδικασίες και τις ροές των δεδομένων. Επιπλέον, ο ίδιος θα πρέπει να ορίζει χρονική διάρκεια όπου με το τέλος της θα διαγράφονται όλα τα δεδομένα.

Από την άλλη ο Εκτελών την Επεξεργασία είναι υποχρεωμένος να φροντίσει να υπάρχει ικανοποιητικό επίπεδο της προστασίας των δεδομένων που επεξεργάζονται. Συνεπώς, δύναται να επιλέξει τα μέτρα εκείνα που θεωρεί ότι θα μπορέσουν να διατηρήσουν την ασφάλεια. Επιπλέον, δε θα πρέπει να αμελεί το γεγονός πως όσα μέτρα κι αν έχει λάβει πάντοτε υπάρχει η πιθανότητα να υπάρξει απώλεια ή πρόσβαση από τρίτους. Ακόμα, σε περίπτωση που αντιληφθεί κίνδυνο διαρροής ή οτιδήποτε άλλο θα πρέπει αμέσως να ενημερώσει τον Υπεύθυνο Επεξεργασίας δίχως όμως να ορίζεται επακριβώς το χρονικό περιθώριο που μπορεί να το κάνει.

Ο νέος Κανονισμός έχει εισάγει αρχές που στην προηγούμενη Οδηγία δεν υπήρχαν όπως είναι η αρχή της λογοδοσίας και η μετατόπιση των ευθυνών στον εκτελούντα και υπεύθυνο επεξεργασίας. Για τη διασφάλιση αυτής της αρχής δημιουργήθηκε ο Υπεύθυνος Προστασίας Δεδομένων. Στην προκειμένη περίπτωση ο υπεύθυνος αυτός ορίζεται είτε από τον υπεύθυνο επεξεργασίας είτε από τον εκτελούντα. Διαθέτει συγκεκριμένα καθήκοντα με βασικότερο να επιτηρεί τη συμμόρφωση με τα όσα γράφονται στον Κανονισμό. Επιπροσθέτως, επιφορτίζεται με την τήρηση του απορρήτου και της εμπιστευτικότητας όσον αφορά την εκτέλεση των

⁴⁴ Ο.π., σελ., 47-114.

καθηκόντων του. Σε περίπτωση που συμβεί κάτι εκείνος λογοδοτεί αμέσως στην ανώτατη διοίκηση και το προσωπικό μιας επιχείρησης ή ενός οργανισμού αναφορικά με τις υποχρεώσεις τους για την προστασία των προσωπικών τους δεδομένων. Για να υπάρξει Υπεύθυνος Προστασίας Δεδομένων θα πρέπει να τηρούνται κάποιες προϋποθέσεις όπως ότι θα είναι δημόσιος φορέας ή δημόσια αρχή και θα πρέπει να προβλέπεται από το δίκαιο ενός κράτους μέλους.

Αναφορικά με τα προηγούμενα ο Κανονισμός προβλέπει τη δυνατότητα επιβολής κυρώσεων για την ενίσχυση των κανόνων του. Οι κυρώσεις περιλαμβάνουν ιδιαίτερα υψηλά διοικητικά πρόστιμα και ποινικές κυρώσεις. Σύμφωνα με τον Ιγγλεζάκη,⁴⁵ η επιβολή προστίμων είναι στην ευχέρεια της εκάστοτε εποπτική αρχής η οποία μπορεί να επιβάλλει μόνο διορθωτικά μέτρα. Ωστόσο τα διοικητικά πρόστιμα αποτελούν ισχυρό εργαλείο του Κανονισμού και γι' αυτό έχουν απασχολήσει τη δημοσιότητα. Το άρθρο 83 προβλέπει ότι η επιβολή προστίμων πρέπει να είναι για κάθε περίπτωση αποτελεσματική, αναλογική και αποτρεπτική.⁴⁶

Για τη λήψη της σχετικής απόφασης λαμβάνονται υπόψη κριτήρια τα οποία προσδιορίζονται από άρθρο 83, παρ. 2 και αφορούν στη φύση, τη βαρύτητα και τη διάρκεια της παράβασης, στο δόλο ή την αμέλεια, στον βαθμό ευθύνης τους υπεύθυνου, στον τρόπο με τον οποίο η εποπτική αρχή πληροφορήθηκε τη παράβαση, στη τήρηση των εγκεκριμένων κανόνων δεοντολογίας κ.ά. Στο ίδιο άρθρο, στις παραγράφους 4-6 ρυθμίζεται και το ύψος των προστίμων που επιβάλλονται από την εποπτική αρχή. «Πρόστιμα έως 10.000.000 ευρώ ή σε περίπτωση επιχειρήσεων 2% του συνολικού παγκόσμιου κύκλου εργασιών του προηγούμενου οικονομικού έτους ανάλογα με το ποιο είναι υψηλότερο»⁴⁷, ή σε ορισμένες περιπτώσεις έως 20.000.000 ευρώ ή σε περίπτωση επιχειρήσεων το 4% του συνολικού παγκόσμιου κύκλου εργασιών.

Σε κάθε περίπτωση η εποπτική αρχή είναι η κατάλληλη για την επιλογή μείγματος μέτρων λαμβάνοντας υπόψη φυσικά και τα διορθωτικά μέτρα όπως αναφέρεται στον Κανονισμό. Τα πρόστιμα επιβάλλονται ανάλογα με τη περίπτωση

⁴⁵ Ιγγλεζάκης Δ. Ιωάννης, (2018), *Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (Κανονισμός 2016/679. Το νέο Νομικό Πλαίσιο Προστασίας Προσωπικών Δεδομένων*, 2^η έκδοση, Θεσσαλονίκη: Andy's Publishers, σελ., 230.

⁴⁶ Κανονισμός (ΕΕ) 2016/679, άρθρο 83: «Κάθε εποπτική αρχή μεριμνά ώστε η επιβολή διοικητικών προστίμων σύμφωνα με το παρόν άρθρο έναντι παραβάσεων του παρόντος κανονισμού που αναφέρονται στις παραγράφους 4, 5 και 6 να είναι για κάθε μεμονωμένη περίπτωση αποτελεσματική, αναλογική και αποτρεπτική».

⁴⁷ Κανονισμός (ΕΕ) 2016/679, άρθρο 83.

έπειτα από σταθμισμένη προσέγγιση των εποπτικών αρχών χωρίς αυτό να σημαίνει ότι δεν πρέπει να επιβάλλονται χρηματικές ποινές διότι σε διαφορετική περίπτωση δύναται να μειωθεί η αποτελεσματικότητα του Κανονισμού. Δηλαδή, θα μπορούσε να μην επιβληθεί πρόστιμο στην περίπτωση που ο Υπεύθυνος Επεξεργασίας είναι ένα φυσικό πρόσωπο και το πρόστιμο θα αποτελούσε δυσανάλογη επιβάρυνση. Η φύση της παράβασης, η διάρκεια αυτής, ο αριθμός των υποκειμένων που επηρεάστηκαν από την παράβαση, ο δόλος ή η αμέλεια αποτελούν κριτήρια που πρέπει να ληφθούν υπόψη στην επιβολή προστίμου.

Για την αξιολόγηση του βαθμού ευθύνης του Υπευθύνου Επεξεργασίας ή του Εκτελούντος της επεξεργασία πρέπει να λαμβάνεται υπόψη αν είχαν εφαρμοστεί τα τεχνικά μέτρα σύμφωνα με τις αρχές προστασίας δεδομένων ήδη από τον σχεδιασμό, αν είχαν εφαρμοστεί τα οργανωτικά μέτρα ήδη από τον σχεδιασμό σε όλα τα επίπεδα οργάνωσης, αν είχε εξασφαλιστεί το κατάλληλο επίπεδο ασφαλείας, αν ήταν γνωστοί και εφαρμόζονταν οι σχετικοί κανόνες στο κατάλληλο διοικητικό επίπεδο στην οργάνωση. Η εποπτική αρχή λαμβάνει υπόψη της αν ο Υπεύθυνος Επεξεργασίας είναι υπότροπος, δηλαδή, έχει διαπράξει ξανά την ίδια παράβαση, εάν έχει παραβιάσει τον Κανονισμό με τον ίδιο τρόπο λόγω ανεπαρκούς γνώσης ή ακατάλληλης εκτίμησης κινδύνου ή αδικαιολόγητης καθυστέρησης, αν έχει καθυστερήσει ή αμελήσει να ενημερώσει την εποπτική αρχή, αν δεν έχει τηρήσει τον εγκεκριμένο κώδικα δεοντολογίας και τέλος αν αποκόμισε οφέλη από αυτήν την παράβαση.⁴⁸ Στα κράτη μέλη δίνεται η ευχέρεια να καθορίσουν τους κανόνες σχετικά με τις κυρώσεις ιδίως σε περιπτώσεις που δεν αποτελούν αντικείμενο διοικητικών προστίμων (άρ. 84).

Ο Κανονισμός σε γενικές γραμμές έχει σαν στόχο την εναρμόνιση των νομοθεσιών των κρατών μελών. Ωστόσο, παρέχει ένα μικρό περιθώριο στα κράτη μέλη να εκδώσουν ειδικές ρυθμίσεις σε ορισμένα ζητήματα.⁴⁹ Επίσης, το άρθρο 87

⁴⁸ Ιγγλεζάκης Δ. Ιωάννης, *ό.π.*, σελ., 236-239.

⁴⁹ Κανονισμός (ΕΕ) 2016/679, άρθρο 6, παρ. 1: «Η επεξεργασία είναι σύνομη μόνο εάν και εφόσον ισχύει τουλάχιστον μία από τις ακόλουθες προϋποθέσεις: α) το υποκείμενο των δεδομένων έχει συναινέσει στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα του για έναν ή περισσότερους συγκεκριμένους σκοπούς, β) η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή για να ληφθούν μέτρα κατ' αίτηση του υποκειμένου των δεδομένων πριν από τη σύναψη σύμβασης, γ) η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση του υπευθύνου επεξεργασίας, δ) η επεξεργασία είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου, ε) η επεξεργασία είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας, στ) η επεξεργασία είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο

δίνει εξουσιοδότηση στα κράτη μέλη να ρυθμίσουν τις προϋποθέσεις για την επεξεργασία εθνικού αριθμού ταυτότητας ή άλλου αναγνωριστικού ταυτότητας εφόσον αυτό δεν έρχεται σε αντίθεση με τον Κανονισμό. Η θεμελιώδης αρχή παραμένει ότι η συλλογή και επεξεργασία προσωπικών δεδομένων πρέπει να γίνεται με θεμιτά μέσα και με τρόπο που να διασφαλίζει το σεβασμό της αξιοπρέπειας, της προσωπικής ζωής και της ιδιωτικότητας. Θεμελιώδης σημασίας επίσης είναι και οι ρυθμίσεις για την επεξεργασία δεδομένων μέσω κλειστού κυκλώματος τηλεόρασης σε χώρους εργασίας και μεθόδων επιτήρησης και παρακολούθησης μέσω χρήσης συστημάτων γεωεντοπισμού. Το σύστημα της παρακολούθησης και ελέγχου ηλεκτρονικών επικοινωνιών επιτρέπεται εφόσον είναι απολύτως απαραίτητο για τη προστασία προσώπων και αγαθών, την οργάνωση και τον έλεγχο μιας εργασίας.⁵⁰

υπεύθυνος επεξεργασίας ή τρίτος, εκτός εάν έναντι των συμφερόντων αυτών υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων που επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα, ιδίως εάν το υποκείμενο των δεδομένων είναι παιδί.».

⁵⁰ Κανονισμός (ΕΕ) 2016/679, άρθρο 19.

5. Προσωπικά Δεδομένα και Ιδιωτικότητα

Μέχρι στιγμής έχει προσδιοριστεί ο όρος αρχεία και τα εκάστοτε είδη και χαρακτηριστικά τους. Εν προκειμένω, θα εξεταστεί η έννοια των προσωπικών δεδομένων, που τα τελευταία χρόνια εξαιτίας της εξάρσης της ψηφιακής εποχής αλλά και του πρόσφατου κανονισμού της Ευρωπαϊκής Ένωσης περί προστασίας των προσωπικών δεδομένων βρίσκονται στο επίκεντρο των επιστημών της πληροφόρησης, των νομικών και όχι μόνο. Ως, λοιπόν, προσωπικά δεδομένα σύμφωνα με την Ευρωπαϊκή Επιτροπή ορίζονται όλες εκείνες οι πληροφορίες που συνδέονται με ένα ταυτοποιημένο⁵¹ ή αναγνωρίσιμο ζωντανό άτομο, το οποίο πολλές φορές ονομάζεται ως υποκείμενο δεδομένων.⁵² Πρόκειται, δηλαδή, για πληροφορίες που αφορούν αυτό το πρόσωπο και είναι επί παραδείγματι το όνομά, η διεύθυνσή του, ο αριθμός δελτίου της αστυνομικής ταυτότητας, το εισόδημα, το πολιτισμικό προφίλ, το ιατρικό ή δικηγορικό απόρρητο μέχρι και ο κωδικός ή διεύθυνση πρωτοκόλλου του διαδικτύου ευρύτερα γνωστό ως IP (Internet Protocol).

Όπως αναφέρεται χαρακτηριστικά από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) προσωπικά δεδομένα είναι κάθε πληροφορία που αναφέρεται και περιγράφει ένα άτομο⁵³, όπως είναι τα στοιχεία αναγνώρισης (ονοματεπώνυμο, ηλικία, κατοικία κλπ.), τα φυσικά χαρακτηριστικά, η εκπαίδευση, η εργασία (προϋπηρεσία κλπ.), η οικονομική κατάσταση (έσοδα, περιουσιακά στοιχεία κλπ.), τα ενδιαφέροντα, οι δραστηριότητες, οι συνήθειες κτλ.⁵⁴ Η άνωθεν περιγραφή υπήρχε στο άρθρο 2 του νόμου 2472/1997 που αποτέλεσε για χρόνια ο οδηγός για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα (personally identifiable information⁵⁵) όμως καταργήθηκε με επιφυλάξεις και αντικαταστάθηκε από τον ν.4624/2019⁵⁶ σε μια προσπάθεια υιοθέτησης του ενιαίου ευρωπαϊκού νομοθετικού πλαισίου περί προστασίας δεδομένων προσωπικού

⁵¹ Στα αγγλικά συναντάται ο όρος identifiable living individual (Data Protection Act 2018). Βλ. στο <https://www.legislation.gov.uk/ukpga/2018/12/section/3/enacted> (last visited 03.8.2021).

⁵² European Commission, "What is personal?", https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en (last visited 03.8.2021).

⁵³ Νόμος, 2472/1997, https://www.dpa.gr/sites/default/files/201910/2472_97%20%28SEPT2019%29.pdf (τελευταία επίσκεψη 3.8.2021).

⁵⁴ Κανελλοπούλου – Μπότη Μαρία (2020), ό.π., σελ.41.

⁵⁵ National Archives and Records Administration, (2017), <https://www.archives.gov/files/foia/directives/nara1608.pdf> (τελευταία επίσκεψη 23.8.2021)

⁵⁶ <https://www.e-nomothesia.gr/law-news/demosieutheke-sto-pherk-nomos-4624-2019.html> (τελευταία επίσκεψη 3.8.2021).

χαρακτήρα. Στην ουσία, δηλαδή, πρόκειται για την υιοθέτηση των κανόνων του Γενικού Κανονισμού για την Προστασία Δεδομένων (Κανονισμός ΕΕ 2016/679) που συνέταξαν το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο της Ευρωπαϊκής Ένωσης τον Απρίλιο του 2016 και τέθηκε σε εφαρμογή μερικά χρόνια αργότερα και συγκεκριμένα το 2018.

Σύμφωνα με τους ορισμούς που δίνονται στο άρ. 4 του νέου Κανονισμού 2016/679, με τον οποίο θα ασχοληθούμε εκτενέστερα στη συνέχεια, έχουμε ότι ως δεδομένα προσωπικού χαρακτήρα ορίζονται «κάθε πληροφορία η οποία αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο του οποίου η ταυτότητα μπορεί έμμεσα ή άμεσα να εξακριβωθεί μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, σε αριθμό ταυτότητας, σε δεδομένα θέσης ή έναν ή περισσότερους παράγοντες που αφορούν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω προσώπου».⁵⁷ Από τον εν λόγω επικαιροποιημένο ορισμό γίνεται εμφανής η προσπάθεια προσδιορισμού ολόένα και περισσότερων στοιχείων της ευρείας έννοιας των προσωπικών δεδομένων ως απάντηση στην πολυπλοκότητα της ίδιας της ανθρώπινης ύπαρξης, των δικαιωμάτων της που διαρκώς επαναπροσδιορίζονται προσφέροντας, αναγνωρίζοντας ή αναθεωρώντας ελευθερίες και ισότητες, όπως η ισότητα φύλου, το δικαίωμα της σεξουαλικότητας κτλ.

Σε αυτό το σημείο να αναφερθεί πως τα προσωπικά δεδομένα χωρίζονται σε κατηγορίες αντίστοιχες της φύσης της πληροφορίας που παρέχουν, όπως είναι τα ιατρικά, γενετικά, σεξουαλικά, εμφανισιακά ή άλλα δεδομένα που αφορούν ένα άτομο. Η πιο αποδεκτή αν και γενικευμένη κατηγοριοποίηση ορίζει:

- Τα κοινά ή απλά δεδομένα που περιλαμβάνουν στοιχεία προσωπικής ταυτοποίησης, όπως το ονοματεπώνυμο και η διεύθυνση, η εργασιακή ή οικογενειακή συνθήκη, τηλέφωνο κτλ. Για τη συλλογή και την επεξεργασία τους αρκεί η προφορική συγκατάθεση του ατόμου.
- Τα ευαίσθητα ή ειδικής κατηγορίας δεδομένα, όπου περιλαμβάνονται όλες εκείνες οι πληροφορίες ειδικού χαρακτήρα που αφορούν την προσωπικότητα και τη ζωή ενός ατόμου. Τέτοια είναι ο ιατρικός ή δικηγορικός φάκελος, η φυλετική καταγωγή, ο σεξουαλικός προσανατολισμός, τα πολιτικά φρονήματα, η συνδικαλιστική δράση, οι θρησκευτικές πεποιθήσεις όπως και

⁵⁷ Κανονισμός (ΕΕ) 2016/679, σελ. 33.

τα δικαιώματα των ανηλίκων. Εξαιτίας της ευαίσθητης φύσης των εν λόγω πληροφοριών ο νομοθέτης απαγορεύει ρητά την επεξεργασία τους εκτός και αν συντρέχουν ειδικοί λόγοι (Άρθρο 9 του Κανονισμού) που θα αναλυθούν παρακάτω.⁵⁸

Επιπρόσθετα σε επίπεδο δεδομένων προσωπικού χαρακτήρα συναντάμε και:

- Τα δημόσια δεδομένα που σχετίζονται με πληροφορίες που αφορούν το δημόσιο γίνεσθαι⁵⁹ και παράγονται από δημόσιους φορείς ή/και ιδιωτικούς αντίστοιχα και είναι δημοσίου συμφέροντος, έχουν δηλαδή παραχθεί με δημόσιους πόρους ή αφορούν το γενικότερο κοινωνικό σύνολο.⁶⁰
- Τα κυβερνητικά δεδομένα που ως τέτοια ορίζονται το υποσύνολο των δημοσίων δεδομένων που παράγονται από το κράτος, την κυβέρνηση ή κυβερνητικά ελεγχόμενους οργανισμούς, όπως λόγου χάρη είναι οι δαπάνες του δημοσίου.⁶¹
- Συνδυαστικά συχνά γίνεται λόγος και για τα «ανοικτά» κυβερνητικά δεδομένα, τα οποία ως περιεχόμενο δεν διαφοροποιούνται από τα παραπάνω. Ωστόσο, η ειδοποιός διαφορά τους είναι σε επίπεδο πρόσβασης, χρήσης⁶² και επαναδιάθεσης. Με άλλα λόγια πρόκειται για δεδομένα που έχει δοθεί η δυνατότητα να διατίθενται και να χρησιμοποιούνται ελεύθερα.⁶³

Ο μόνος τρόπος προκειμένου να έχει κανείς ελεύθερη πρόσβαση στις πληροφορίες προσωπικών δεδομένων είναι να έχει δοθεί η γραπτή συγκατάθεση του υποκειμένου, χωρίς να τελούνται όροι που αντίκεινται στο νόμο ή τα χρηστά ήθη,

⁵⁸ Σημαντική κατά τη γνώμη μας πρόβλεψη του νομοθέτη είναι και το γεγονός ότι τα κράτη μέλη μπορούν να διατηρούν ή να θεσπίζουν περαιτέρω όρους, μεταξύ άλλων και περιορισμούς, όσον αφορά την επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων ή δεδομένων που αφορούν την υγεία. Ο.π., σελ. 39. Ενδεικτικά και με αφορμή το ξέσπασμα της πανδημίας Covid-19 και τις προσπάθειες περιορισμού και ελέγχου της διασποράς και ελέγχου της έχουμε τα πιστοποιητικά εμβολιασμού με ευαίσθητα προσωπικά δεδομένα υγείας που χρησιμοποιούνται για την είσοδο σε καταστήματα, αγορές, ταξίδια, την εργασία κτλ.

⁵⁹ Κρίσιμο ζήτημα της διαχείρισης των δημοσίων δεδομένων στο πλαίσιο των οραμάτων της δημοκρατίας και της ψηφιακής διακυβέρνησης είναι η ανοιχτή πρόσβαση ή αλλιώς η ανοιχτότητα των δεδομένων και του περιεχομένου. Στο <http://opendefinition.org/> (τελευταία επίσκεψη 13.8.2021).

⁶⁰ Παπαδόπουλος Θεοδωρής (χ.χ.), *Ανοιχτά δημόσια δεδομένα*, Αθήνα: Ε.Κ.Δ.Δ.Α., σελ. 26.

⁶¹ Ο.π., σελ.27.

⁶² Το ζητούμενο εδώ είναι πως ο σκοπός της επαναχρησιμοποίησης δεδομένων διαφέρει από τον αρχικό για τον οποίο παρήχθησαν υπό τον όρο να γίνεται αναφορά στους δημιουργούς και να διατίθενται, με τη σειρά τους, υπό τους ίδιους όρους. Βλ. περισσότερα στο <https://okfn.gr/what-is-open/> (τελευταία επίσκεψη 13.8.2021).

⁶³ Τριανταφυλλίδου Βικτώρια (2018), *Η επεξεργασία των προσωπικών δεδομένων στον χώρο των ηλεκτρονικών επικοινωνιών: Νομικές πτυχές*, Θεσσαλονίκη: ΠΑΜΑΚ, σελ., 6 [διπλωματική εργασία] Διαθέσιμο στο: <https://dspace.lib.uom.gr/bitstream/2159/21653/4/TriantafyllidouViktoriaMsc2018.pdf> (τελευταία επίσκεψη 3.8.2021).

όπως δύναται να είναι ο εκβιασμός ή/και εξαναγκασμός.⁶⁴ Ωστόσο, αναγνωρίζονται και ορισμένες ειδικές συνθήκες επεξεργασίας των προσωπικών δεδομένων και συγκεκριμένα εκείνων που ανήκουν στις ευαίσθητες κατηγορίες (άρθρο 22). Αυτές είναι όταν:

- α) τα προσωπικά δεδομένα είναι αναγκαία για την τήρηση συμβατικής υποχρέωσης έναντι του υποκειμένου των δεδομένων ή αφορά σε προστασία ζωτικών συμφερόντων του τελευταίου ή προβλεπόμενου από το νόμο συμφέροντος τρίτου, εάν το υποκείμενο τελεί σε φυσική ή νομική αδυναμία να δώσει τη συγκατάθεσή του
- β) τα προσωπικά δεδομένα απαιτούνται για την εκπλήρωση τυχόν νομικής υποχρέωσης ή υπεράσπιση δικαιώματος ενώπιον δικαστηρίου ή πειθαρχικού οργάνου,
- γ) η επεξεργασία των προσωπικών δεδομένων κρίνεται απαραίτητη για τη διεκπεραίωση αποστολής δημοσίου συμφέροντος.⁶⁵

Ο έλληνας νομοθέτης κατά παρέκκλιση του Κανονισμού (άρθρο 9, παρ. 1) ορίζει ως εξαιρέσεις (άρθρο 22, παρ. 1 και 2) επεξεργασίας ειδικών προσωπικού χαρακτήρα δεδομένων όταν είναι απαραίτητη:

- α) για την άσκηση δικαιωμάτων που απορρέουν από το δικαίωμα κοινωνικής ασφάλισης και κοινωνικής προστασίας και για την εκπλήρωση των συναφών υποχρεώσεων,
- β) για λόγους προληπτικής ιατρικής, για την εκτίμηση της ικανότητας προς εργασία του εργαζομένου, για ιατρική διάγνωση, για την παροχή υγείας ή κοινωνικής περίθαλψης ή για τη διαχείριση των συστημάτων και υπηρεσιών υγείας ή κοινωνικής περίθαλψης ή δυνάμει σύμβασης με επαγγελματία του τομέα υγείας ή άλλου προσώπου που δεσμεύεται από το επαγγελματικό απόρρητο ή είναι υπό την εποπτεία του,
- γ) για λόγους δημοσίου συμφέροντος στον τομέα της δημόσιας υγείας, όπως σοβαρών διασυννοριακών απειλών κατά της υγείας ή για την εξασφάλιση υψηλών προδιαγραφών ποιότητας και ασφάλειας της υγειονομικής περίθαλψης και των φαρμάκων ή των ιατροτεχνολογικών προϊόντων,
- δ) για λόγους ουσιώδους δημοσίου συμφέροντος,

⁶⁴ «Προστασία δεδομένων στο πλαίσιο του ΓΚΠΔ», https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_el.htm (τελευταία επίσκεψη 03.8.2021).

⁶⁵ Ο.π..

ε) για την αποτροπή σημαντικής απειλής για την εθνική ασφάλεια ή τη δημόσια ασφάλεια,

στ) για τη λήψη ανθρωπιστικών μέτρων, και στις περιπτώσεις αυτές το συμφέρον για την επεξεργασία είναι υπέρτερο του συμφέροντος του υποκειμένου των δεδομένων.

Τα προσωπικά δεδομένα εμπίπτουν σε στοιχεία που αφορούν την ιδιωτικότητα ενός ατόμου, η οποία αποτελεί θεμελιώδες δικαίωμα κατοχυρωμένο ήδη από το 1948 και την Οικουμενική Διακήρυξη των Δικαιωμάτων του Ανθρώπου αλλά και τα δημοκρατικά συντάγματα πολλών χωρών, μιας και θεωρείται κύρια προϋπόθεση της ατομικής ελευθερίας και της κοινωνικής προόδου. Σύμφωνα με τους Brandeis και Warren ως δικαίωμα ιδιωτικότητας ορίζεται το δικαίωμα των ανθρώπων να προστατεύουν την ιδιωτική τους ζωή από την ανεπιθύμητη διανομή πληροφοριών και ιδιαίτερα τη δημοσίευσή τους.⁶⁶ Έτσι υπάρχει στο άρθρο 12 της Οικουμενικής Διακήρυξης ότι «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 υπόληψης του. Καθένας έχει το δικαίωμα να τον προστατεύουν οι νόμοι από επεμβάσεις και προσβολές αυτού του είδους».⁶⁷

Ακόμη, σε επίπεδο της ελληνικής νομικής πραγματικότητας υπάρχει από το Σύνταγμα της μεταπολίτευσης η ρητή κατοχύρωση του απαραβίαστου της ιδιωτικής και οικογενειακής ζωής του ατόμου. Ειδικότερα, στο άρθρο 2 παρ. 1 χαρακτηριστικά αναγράφεται: «ο σεβασμός και η προστασία της αξίας του ανθρώπου αποτελούν πρωταρχική υποχρέωση της Πολιτείας».⁶⁸ Προσθετικά, στην αναθεώρηση του Συντάγματος το 2001 με το Άρθρο 9 κατοχυρώνεται το δικαίωμα της προστασίας των προσωπικών δεδομένων ως πυλώνας προστασίας του δικαιώματος της ιδιωτικότητας του ατόμου.

Η τελευταία σύμφωνα με το νόμο παρέχει στο άτομο αρνητική, αμυντική προστασία από κάθε εισβολή ή παρέμβαση στον ιδιωτικό του χώρο που πιθανά θα

⁶⁶ Warren and Brandeis (1890), *The right to privacy*, Harvard Law Review, vol.IV, http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html (last visited 03.8.2021).

⁶⁷ Οικουμενική Διακήρυξη για τα Ανθρώπινα Δικαιώματα, 10 Δεκεμβρίου 1948, https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/grk.pdf (τελευταία επίσκεψη 03.8.2021).

⁶⁸ Βουλή των Ελλήνων, <https://www.hellenicparliament.gr/Vouli-ton-Ellinon/To-Politevma/Syntagma/article-2/> (τελευταία επίσκεψη 3.8.2021).

περιορίσει την προσωπικότητα και την αυτονομία του.⁶⁹ Έτσι διαβάζουμε, λοιπόν, ότι ο: «Καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών δεδομένων, όπως ο νόμος ορίζει. Η προστασία των προσωπικών δεδομένων διασφαλίζεται από ανεξάρτητη Αρχή, που συγκροτείται και λειτουργεί σύμφωνα με το νόμο».⁷⁰ Η Αρχή αυτή δεν είναι άλλη από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Ως τέτοια ορίζεται η συνταγματικά κατοχυρωμένη ανεξάρτητη δημόσια Αρχή, που έχει ως σκοπό την εποπτεία της εφαρμογής του Γενικού Κανονισμού Προστασίας Δεδομένων του ν. 4624/2019, του ν. 3471/2006 καθώς και άλλων διατάξεων που στοχεύουν στην προστασία του ατόμου από την επεξεργασία των δεδομένων προσωπικού χαρακτήρα.⁷¹

Τα όσα αφορούν τα προσωπικά δεδομένα έχουν στις μέρες μας κατοχυρωθεί από τον Γενικό Κανονισμό Προσωπικών Δεδομένων (ΓΚΠΔ) στο Ευρωπαϊκό Κοινοβούλιο τον Απρίλιο του 2016 και ισχύουν σε όλες τις χώρες της Ευρωπαϊκής Ένωσης από τις 25 Μαΐου 2018. Ωστόσο, η ανάγκη διαμόρφωσης διεθνούς νομικού πλαισίου περί προστασίας προσωπικών δεδομένων είχε προκύψει και νωρίτερα. Έτσι από το 1981 υπάρχει από το Συμβούλιο της Ευρώπης η έκδοση της Ευρωπαϊκής Σύμβασης για την Προστασία από την Αυτοματοποιημένη Επεξεργασία των Προσωπικών Δεδομένων ή αλλιώς γνωστή ως Σύμβαση 108. Πρόκειται για το πρώτο νομικά δεσμευτικό διεθνές κείμενο του ευρωπαϊκού χώρου με σκοπό την προστασία των προσωπικών δεδομένων, που η χώρα μας επικύρωσε δώδεκα χρόνια μετά, με την ψήφιση του Νόμου 2068/1992.

Ακολούθως, το Ευρωπαϊκό Κοινοβούλιο εκδίδει την Οδηγία 95/46/EK πάνω στην οποία στηρίχθηκε ο παλιός δικός μας Ν.2472/1997 που στόχευσε στην προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων αυτών και εξυπηρέτησε καλώς το σκοπό του μέχρι πρόσφατα. Η συνεχής ανανέωση των όρων των παραπάνω ευρωπαϊκών συμβάσεων επιτεύχθηκε με πλήθος οδηγιών, νέων συμφωνιών και υιοθέτησης ρυθμιστικών κανόνων που μας έφεραν στο σήμερα και τον Γενικό Κανονισμό Προσωπικών Δεδομένων.

⁶⁹ Ακριβοπούλου, Χριστίνα Μ., (2011), «Το δικαίωμα στην προστασία των προσωπικών δεδομένων μέσα από τον φακό του δικαιώματος στην ιδιωτική ζωή», στο: *Θεωρία και Πράξη Διοικητικού Δικαίου*, τχ 7, Αθήνα, σελ., 681.

⁷⁰ Βουλή των Ελλήνων, <https://www.hellenicparliament.gr/Vouli-ton-Ellinon/To-Politevma/Syntagma/article-9a/> (τελευταία επίσκεψη 3.8.2021).

⁷¹ Αρχή Προστασίας Δεδομένων, <https://www.dpa.gr/> (τελευταία επίσκεψη 3.8.2021).

Περί της ιστορικής εξέλιξης της νομοθεσίας και του ζητήματος των προσωπικών δεδομένων, να σημειωθεί ότι πέρα από τα ευρωπαϊκά όρια στις ΗΠΑ υποστηρίζεται σχετικά με την προστασία των προσωπικών δεδομένων ότι το άτομο και μόνο αυτό θα πρέπει να έχει το δικαίωμα να παρακολουθεί και να ελέγχει τις προσωπικές του πληροφορίες. Παράλληλα, υποστηρίζεται και η εκδοχή ότι η επιλογή των ατόμων να διατηρούν μερικές πληροφορίες για ιδιωτική τους χρήση και να αποκαλύπτουν μόνο όσες επιθυμούν είναι ο πυλώνας για την διασφάλιση της ανεξαρτησίας και της ελευθερίας της επιλογής στην ζωή τους.⁷² Να τονιστεί βέβαια ότι όπως και στον Καναδά έτσι και στις ΗΠΑ ισχύει το δικαίωμα της αυτορρύθμισης στον ιδιωτικό τομέα ενώ η προστασία των δεδομένων στον δημόσιο τομέα φαίνεται να ακολουθεί την ευρωπαϊκή πολιτική.

Επιστρέφοντας στο Γενικό Κανονισμό Προσωπικών Δεδομένων είναι σημαντικό να σημειωθεί ότι ως στόχος ορίζεται η προστασία των προσωπικών δεδομένων ανεξάρτητα από την τεχνολογία η οποία χρησιμοποιείται για την επεξεργασία τους.⁷³ Όπως φάνηκε, η ανάπτυξη της τεχνολογίας και η ολοένα και μεγαλύτερη χρήση αυτής στην καθημερινότητά μας, από τα δίκτυα κοινωνικής δικτύωσης μέχρι και τις οικονομικές συναλλαγές δημιουργούν πιο έντονα το αίσθημα της αναγκαιότητας για ασφάλεια και της προστασία των προσωπικών δεδομένων των ανθρώπων. Αυτή η τεχνολογική εξέλιξη έχει κάνει πολλές κυβερνήσεις ανά τον κόσμο να θεσπίσουν καινούργιους νόμους οι οποίοι θα έχουν ως σκοπό τη διασφάλιση της ιδιωτικότητας με οτιδήποτε αυτή συνεπάγεται. Ειδικότερα, λοιπόν, με βάση τον Ευρωπαϊκό Γενικό Κανονισμό στόχος είναι η προστασία των προσωπικών δεδομένων ανεξάρτητα από την τεχνολογία που χρησιμοποιείται.⁷⁴

Ακόμη σύμφωνα με τον ίδιο Κανονισμό τα υποκείμενα δεδομένων έχουν τα εξής τα δικαιώματα⁷⁵:

- **Δικαίωμα ενημέρωσης και διαφάνεια (άρθρα 12-14):** Πρόκειται για το δικαίωμα του ατόμου να γνωρίζει ποιος επεξεργάζεται τα δεδομένα του, ποια δεδομένα είναι αυτά και για ποιον λόγο. Επιπλέον, ο οποιοσδήποτε

⁷² Bottis Maria (2012), *Privacy and Surveillance: Current aspects and future perspectives*, Αθήνα: Νομική Βιβλιοθήκη, σελ. 216.

⁷³ Ως επεξεργασία δεδομένων ορίζεται η διαδικασία προσθήκης αξίας σε αυτά δια μέσου οργάνωσης, μαθηματικής ή στατιστικής ανάλυσης, διόρθωση λαθών ή συμπίεση καταλήγοντας στην παραγωγή πληροφορίας. Βλ στο Παπαδόπουλος Θεοδωής ό.π., σελ.24.

⁷⁴ European Commission, "What is personal?" https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en (τελευταία επίσκεψη 3.8.2021).

⁷⁵ Κανονισμός (ΕΕ) 2016/679, ό.π., σελ. 39-46.

οργανισμός προχωρά σε επεξεργασία δεδομένων καλείται να παρέχει σαφείς πληροφορίες καταγεγραμμένες σε απλή γλώσσα.

- **Δικαίωμα πρόσβασης του υποκειμένου των δεδομένων (άρθρο 15):** Ο καθένας που έχει δώσει τη δυνατότητα να επεξεργαστούν τα δεδομένα του έχει δικαίωμα να ζητήσει χωρίς κάποιο κώλυμα να έχει πρόσβαση στα δεδομένα του που διαθέτει κάποιος οργανισμός.
- **Δικαίωμα διόρθωσης (άρθρο 16):** Σε περίπτωση που υπάρχουν εσφαλμένα στοιχεία υπάρχει το δικαίωμα να ζητήσει κανείς τη διόρθωση των ανακριβών προσωπικών δεδομένων καθώς και της συμπλήρωσης των ελλিপών στοιχείων.
- **Δικαίωμα διαγραφής («δικαίωμα στη λήθη») (άρθρο 17):** Το υποκείμενο δεδομένο έχει το δικαίωμα να ζητήσει τη διαγραφή των προσωπικών του δεδομένων, υπό ορισμένες προϋποθέσεις, όπως όταν τα δεδομένα δεν είναι πλέον απαραίτητα ή έχει ανακαλέσει τη συγκατάθεσή του και πόσο μάλλον δε όταν τα δεδομένα έχουν υποβληθεί σε παράνομη επεξεργασία, κ.ο.κ.
- **Δικαίωμα περιορισμού της επεξεργασίας (άρθρο 18):** Το άτομο έχει το δικαίωμα να ζητήσει τον περιορισμό της επεξεργασίας των δεδομένων του όταν αμφισβητείται η ακρίβειά τους, η επεξεργασία είναι παράνομη, τα δεδομένα δεν χρειάζονται πλέον στον υπεύθυνο επεξεργασίας, έχετε αντιρρήσεις ως προς την αυτοματοποιημένη επεξεργασία.
- **Δικαίωμα στη φορητότητα των δεδομένων (άρθρο 20):** Δύναται κανείς να ζητήσει τη μεταφορά των δεδομένων του σε άλλον υπεύθυνο επεξεργασίας.
- **Δικαίωμα εναντίωσης (άρθρο 21):** Υπάρχει το δικαίωμα να εναντιωθεί κάποιος στην επεξεργασία των προσωπικών του δεδομένων από έναν οργανισμό, υπό την προϋπόθεση ότι δεν θίγεται το δημόσιο συμφέρον.
- **Δικαίωμα στη μη αυτοματοποιημένη ατομική λήψη αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ (άρθρο 22):** Μπορεί κανείς να προβάλλει αντιρρήσεις όταν μια απόφαση που τον αφορά βασίζεται αποκλειστικά σε αυτοματοποιημένη επεξεργασία, συμπεριλαμβανομένης της κατάρτισης προφίλ, και η απόφαση αυτή παράγει έννομα αποτελέσματα ή τον επηρεάζει σημαντικά.

Πέραν των δικαιωμάτων όμως των υποκείμενων δεδομένων ο Γενικός Κανονισμός έθεσε και κάποιες προϋποθέσεις στις οποίες επιβάλλονται οι υπεύθυνοι επεξεργασίας. Αυτές οι προϋποθέσεις είναι οι ακόλουθες⁷⁶:

- **Ευθύνη (άρθρο 24):** Ο υπεύθυνος επεξεργασίας θα πρέπει να αποδεικνύει ότι διαθέτει όλα τα κατάλληλα οργανωτικά και τεχνικά μέτρα προστασίας των προσωπικών δεδομένων και κυρίως ότι συμμορφώνεται με τον Γενικό Κανονισμό.
- **Προστασία δεδομένων κατά τον σχεδιασμό («Data protection by design», άρθρα 25):** Ο Γενικός Κανονισμός επιβάλλει την εφαρμογή προϊόντων και υπηρεσιών (ηλεκτρονικών ή μη) που κατά τον αρχικό σχεδιασμό τους δημιουργούν φιλικές συνθήκες για την προστασία των δεδομένων. Ενδεικτικά, στις υπηρεσίες της κοινωνικής δικτύωσης (social media) θα πρέπει να παρέχεται η δυνατότητα να επιλέγει κανείς τις ρυθμίσεις οι οποίες θα προστατεύουν όλο και περισσότερο τα προσωπικά μας δεδομένα.
- **Προστασία δεδομένων εξ ορισμού («Data protection by default», άρθρο 25):** Επιβάλλεται η εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων που να διασφαλίζουν ότι εξ ορισμού υφίστανται επεξεργασία μόνο τα δεδομένα που είναι απαραίτητα για τον σκοπό της επεξεργασίας.
- **Αρχεία των δραστηριοτήτων επεξεργασίας (άρθρο 30):** κάθε υπεύθυνος επεξεργασίας ή ο εκπρόσωπός του τηρεί αρχείο των δραστηριοτήτων για τις οποίες είναι υπεύθυνος, όπου σημειώνεται: το όνομα και τα στοιχεία του υπευθύνου επεξεργασίας και υπευθύνου προστασίας των δεδομένων, οι σκοποί της επεξεργασίας, προθεσμίες, αποδέκτες γνωστοποίησης των προσωπικών δεδομένων ακόμη και αν πρόκειται για τρίτες χώρες ή διεθνείς οργανισμούς.
- **Ασφάλεια επεξεργασίας (άρθρο 32):** Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία πρέπει να εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το ενδεδειγμένο επίπεδο ασφάλειας.
- **Γνωστοποίηση παραβιάσεων δεδομένων (άρθρο 33):** Ο υπεύθυνος επεξεργασίας έχει την υποχρέωση αμέσως μόλις αντιληφθεί παραβίαση, να

⁷⁶ Ο.π., σελ. 47-48, 50-59.

ενημερώσει τις αρμόδιες εποπτικές Αρχές και καθώς και το υποκείμενο δεδομένο, εφόσον η παραβίαση μπορεί να τον θέσει σε σοβαρό κίνδυνο.

- **Εκτίμηση αντικτύπου και προηγούμενη διαβούλευση (άρθρο 35):** Όταν η επεξεργασία ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα των ατόμων, ιδίως επειδή είναι συστηματική, μεγάλης κλίμακας, αφορά ειδικές κατηγορίες δεδομένων και βασίζεται στη χρήση νέων τεχνολογιών, ο υπεύθυνος επεξεργασίας πρέπει να διενεργήσει εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων (Data protection impact assessment). Όταν βάσει της διενεργηθείσας εκτίμησης αντικτύπου και παρά την πρόβλεψη μέτρων προστασίας παραμένει υψηλή επικινδυνότητα της επεξεργασίας, ο υπεύθυνος επεξεργασίας υποχρεούται να προβεί σε προηγούμενη διαβούλευση με την εποπτική Αρχή.
- **Υπεύθυνος προστασίας δεδομένων (άρθρα 37, 38 και 39):** Προβλέπεται, υπό προϋποθέσεις, ο ορισμός «υπευθύνου προστασίας δεδομένων» ο οποίος έχει εχέγγυα ανεξαρτησίας και παρακολουθεί τη συμμόρφωση με τον νόμο αποτελώντας, συγχρόνως, το σημείο επαφής με την εποπτική Αρχή.
- **Κώδικες δεοντολογίας (άρθρο 40):** Ενθαρρύνεται η εκπόνηση κωδίκων δεοντολογίας -χωρίς να είναι υποχρεωτικοί- από τους υπευθύνους επεξεργασίας, οι οποίοι υποβάλλονται προς έγκριση στην εποπτική Αρχή. Σε περίπτωση διευρωπαϊκής δραστηριότητας ζητείται και η γνώμη του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων.
- **Πιστοποίηση (άρθρο 42):** Ενθαρρύνεται η θέσπιση μηχανισμών πιστοποίησης, σφραγίδων και σημάτων προστασίας δεδομένων για την απόδειξη της συμμόρφωσης προς τον ΓΚΠΔ ή για την απόδειξη παροχής κατάλληλων εγγυήσεων κατά την επεξεργασία. Η πιστοποίηση έχει προαιρετικό χαρακτήρα και είναι εθελοντική.

6. Αρχεία και Επεξεργασία Προσωπικών Δεδομένων

Μέχρι στιγμής έχουν εξεταστεί οι έννοιες αρχεία και προσωπικά δεδομένα ξεχωριστά επιχειρώντας έτσι να σκιαγραφηθεί τόσο το εννοιολογικό όσο και το νομοθετικό πλαίσιο που τα προσδιορίζει. Ποια είναι όμως η μεταξύ τους σχέση; Έγινε γνωστό ότι ως αρχεία λογίζονται ποικίλης μορφής ή υποστρώματος τεκμήρια που δημιουργούνται με σκοπό την καταγραφή της δραστηριότητας ενός ατόμου, ενός οργανισμού, μιας κυβέρνησης κ.ο.κ. Από αυτό γίνεται κατανοητό ότι περιλαμβάνουν δεδομένα και μάλιστα συχνά προσωπικού χαρακτήρα. Δηλαδή, στην εποχή της υπερβάλλουσας παραγωγής και διάθεσης δεδομένων προσωπικού χαρακτήρα, απλής ή πιο ειδικής φύσεως, όλοι όσοι δημιουργούν, διαχειρίζονται και συμβουλεύονται αρχεία πρέπει να λαμβάνουν υπόψη τη νομοθεσία σχετικά με την προστασία των προσωπικών δεδομένων. Επομένως, κατά την επεξεργασία και διαχείριση ενός αρχείου αλλά και στη γενικότερη οργάνωση και λειτουργία των Αρχείων ως φορείς στην ουσία προκύπτει ζήτημα επεξεργασίας προσωπικών δεδομένων δημιουργώντας την περαιτέρω ανάγκη οριοθέτησης του νομικού πλαισίου.

Να σημειωθεί εδώ ότι ως επεξεργασία προσωπικών δεδομένων σύμφωνα με τον Κανονισμό ορίζεται κάθε πράξη που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων σε δεδομένα προσωπικού χαρακτήρα.⁷⁷ Πιο συγκεκριμένα, ως επεξεργασία ορίζεται η συλλογή, καταχώριση, οργάνωση, διάρθρωση, αποθήκευση, προσαρμογή ή μεταβολή, ανάκτηση, αναζήτηση πληροφοριών, χρήση, κοινολόγηση με διαβίβαση, διάδοση ή κάθε άλλη μορφή διάθεσης, συσχέτιση ή συνδυασμό, περιορισμό, διαγραφή ή καταστροφή των δεδομένων. Επιπρόσθετα, σε επίπεδο ελληνικού δικαίου οι διατάξεις του ν.4624/2019 εφαρμόζονται στο σύνολο ή σε μέρη της αυτοματοποιημένης ή μη επεξεργασίας των δεδομένων προσωπικού χαρακτήρα, ανεξάρτητα από τη μορφή και το υπόστρωμα των αρχείων (βάση δεδομένων, εικόνα, φιλμ, χαρτί κτλ.). Να αναφερθεί ότι ο ν.3471/2006 ορίζει ως αρχείο δεδομένων προσωπικού χαρακτήρα κάθε διαρθρωμένο σύνολο δεδομένων προσωπικού χαρακτήρα τα οποία είναι προσιτά βάσει συγκεκριμένων κριτηρίων.⁷⁸

⁷⁷ Κανονισμός (ΕΕ) 2016/679 ό.π., σελ. 33.

⁷⁸ Βρεττού Χριστίνα Αντ. (2017), *Η τροποποίηση της έννοιας του αρχείου δεδομένων προσωπικού χαρακτήρα με τον ν.3471/2006 και οι συνέπειες της εφαρμογής του ν.2472/1997 στα δημοσιογραφικά αρχεία*, Ένωση Ελλήνων Νομικών. Διαθέσιμο <https://bit.ly/2Z7fVVB> (τελευταία επίσκεψη 27.8.2021).

Με άλλα λόγια, «σπάνια τα αρχεία θα μπορούσαν να επικαλεστούν ότι επεξεργάζονται πληροφορίες για φυσικά πρόσωπα οι οποίες όμως δεν συνιστούν προσωπικά δεδομένα ταυτοποιημένων ή ταυτοποιήσιμων προσώπων ώστε να αποφύγουν την εφαρμογή του νόμου»⁷⁹ είτε πρόκειται για τον ΓΚΠΔ είτε για επιμέρους νομοθετικές ρυθμίσεις του αστικού δικαίου των επιμέρους μελών κρατών, όπως ο δικός μας ν.4624/2019 ή η Πράξη Προστασίας Δεδομένων του 2018 του Ηνωμένου Βασιλείου (Data Protection Act 2018).⁸⁰ Αναλογιζόμενοι μόνο κάποιες από τις βασικές λειτουργίες των αρχείων όπως η ταξινόμηση ή η καταλογογράφηση των τεκμηρίων, η περιγραφή ή εκτίμηση του υλικού, όπως επίσης και η συγκέντρωση ή εκκαθάριση του υλικού καθίσταται σαφές ότι πρόκειται για δραστηριότητες επεξεργασίας προσωπικών δεδομένων.⁸¹

Για όλα τα παραπάνω, η Ευρωπαϊκή Ομάδα Αρχείων έχει εκδώσει πρόσθετες οδηγίες για την εφαρμογή του Κανονισμού από τις υπηρεσίες αρχειοθέτησης, είτε πρόκειται για δημόσια είτε για ιδιωτικά ιδρύματα που διατηρούν αρχεία. Σε πρώτο στάδιο ορίζεται σαφώς η υποχρέωση του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία να γνωρίζει και να υπακούει στις αρχές του Άρθρου 5 του ΓΚΠΔ περί επεξεργασίας δεδομένων προσωπικού χαρακτήρα, όπως είναι η διαφάνεια, η επικαιροποίηση, το ασύμβατο του σκοπού κ.ο.κ.⁸²

Όλοι οι παραπάνω όροι δεσμεύουν σύμφωνα με τον Κανονισμό εξίσου και τους υπαλλήλους που έχουν υπό την ευθύνη τους οι υπεύθυνοι ή εκτελούντες την επεξεργασία. Ως υπεύθυνος επεξεργασίας ορίζεται οποιοσδήποτε καθορίζει από κοινού ή με άλλους το σκοπό και τον τρόπο επεξεργασίας των προσωπικών δεδομένων και κατ' επέκταση φέρει την ευθύνη για την πραγματοποιούμενη επεξεργασία είτε αυτή γίνεται από τον ίδιο ή από άλλον. Για τα αρχεία υπεύθυνος επεξεργασίας είναι το νομικό πρόσωπο που συστήθηκε για την λειτουργία των αρχείων, λόγω χάρη το νομικό πρόσωπο των Γ.Α.Κ. είναι υπεύθυνο για την επεξεργασία του υλικού που συγκεντρώνεται.⁸³ Σύμφωνα με τον ν.4624/2019 στους

⁷⁹ Κανελλοπούλου – Μπότη Μαρία (2020), ό.π., σελ.42.

⁸⁰ Το Ηνωμένο Βασίλειο αν και πλέον βρίσκεται σε διαδικασίες αποχώρησης από την Ευρωπαϊκή Ένωση (Brexit) διατήρησε τους γενικούς κανόνες του Κανονισμού περί προστασίας προσωπικών (UK GDPR) που εφαρμόζεται σε επιχειρήσεις που δραστηριοποιούνται ή συνεργάζονται με την ΕΕ, ενώ για το εσωτερικό της χώρας ισχύει μόνο ο DPA 2018. Βλ. <https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/overview-data-protection-and-the-eu/> (τελευταία επίσκεψη 23.8.2021).

⁸¹ Κανελλοπούλου – Μπότη Μαρία (2020), ό.π σελ 50.

⁸² European Archives Group (2018), *Guidance on data protection for archive services: EAG guidelines on the implementation of the General Data Protection Regulation in the archive sector*, p.8.

⁸³ Κανελλοπούλου – Μπότη Μαρία (2020), ό.π., σελ. 53.

δημόσιους φορείς μπορεί να ορίζεται ένα υπεύθυνος επεξεργασίας, ο οποίος δύναται να λειτουργεί ως τέτοιος σε παραπάνω από έναν δημόσιο φορέα ανάλογα το μέγεθος και την οργανωτική τους δομή (άρθρο 6).

Από την Ευρωπαϊκή Ομάδα υπογραμμίζεται επίσης ότι πρέπει να τηρούνται οι όροι νομιμότητας για την επεξεργασία των προσωπικών δεδομένων όπως ορίζονται στα άρθρα 5 και 6 του Κανονισμού.⁸⁴ Δηλαδή ότι τα δεδομένα προσωπικού χαρακτήρα πρέπει να:

- ο επεξεργάζονται νόμιμα, δίκαια και με διαφάνεια σε σχέση με το υποκείμενο των δεδομένων,
- ο συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και να μην υφίστανται περαιτέρω επεξεργασία κατά τρόπο ασυμβίβαστο με αυτούς τους σκοπούς,
- ο είναι επαρκή, σχετικά και περιορισμένα στο αναγκαίο σε σχέση με το σκοπό που υποβάλλονται σε επεξεργασία,
- ο είναι ακριβή και ενημερωμένα· σε άλλη περίπτωση ανακρίβειας λαμβανομένων των σκοπών επεξεργασίας τα δεδομένα είτε διαγράφονται είτε διορθώνονται,
- ο φυλάσσονται σε μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων ακόμη και για μεγαλύτερο χρονικό διάστημα από εκείνο της εξυπηρέτησης των αρχικών σκοπών της επεξεργασίας στο βαθμό που υποβάλλονται σε αρχειοθέτηση για λόγους δημοσίου συμφέροντος, επιστημονικούς ή ιστορικούς σκοπούς έρευνας,
- ο υποβάλλονται σε επεξεργασία με τρόπο που διασφαλίζει την κατάλληλη ασφάλεια των προσωπικών δεδομένων, συμπεριλαμβανομένης της προστασίας από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και από τυχαία απώλεια, καταστροφή ή ζημιά, χρησιμοποιώντας κατάλληλα τεχνικά ή οργανωτικά μέτρα

και σε σχέση με την επεξεργασία να ισχύουν τα κάτωθι:

- ο το υποκείμενο των δεδομένων έχει συναινέσει στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα του για έναν ή περισσότερους συγκεκριμένους σκοπούς,

⁸⁴ European Archives Group (2018), Ibid.

- η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή για να ληφθούν μέτρα κατ' αίτηση του υποκειμένου των δεδομένων πριν από τη σύναψη σύμβασης,
- η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση του υπευθύνου επεξεργασίας,
- η επεξεργασία είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου,
- η επεξεργασία είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας,
- η επεξεργασία είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων 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 των δεδομένων που επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα, ιδίως εάν το υποκείμενο των δεδομένων είναι παιδί.

Παράλληλα, σημειώνεται και η υποχρέωση της συμμόρφωσης του υπευθύνου επεξεργασίας βάσει του άρθρου 24 περί ευθύνης.⁸⁵ Η τελευταία καθίσταται ένας σημαντικός όρος προς τα Αρχεία ιδιαίτερα, ως φύλακες της μνήμης και διαχειριστές τεράστιου όγκου δεδομένων, μιας και διατυπώνεται ότι η επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι νόμιμη, εάν είναι απαραίτητη για την εκτέλεση μιας εργασίας που εκτελείται προς το δημόσιο συμφέρον, όπως αυτή (ενν. η εργασία) ορίζεται από το δίκαιο της Ένωσης ή του κράτους μέλους. Η έννοια του δημοσίου συμφέροντος δεν καθορίζεται⁸⁶ επακριβώς στον Κανονισμό, αν και επαναλαμβάνεται ουκ ολίγες φορές, ωστόσο πρόκειται για φορές. Παρ' όλα αυτά αποτελεί έννοια «γνώριμη στο δίκαιο [...] και περιλαμβάνει όλες τις πτυχές της δημόσιας σφαίρας

⁸⁵ Ibid.

⁸⁶ Πρόκειται για μια έννοια που εντάσσεται στο πλαίσιο των αόριστων νομικών εννοιών, ενώ χαρακτηρίζεται από τον εκάστοτε χρόνο, τόπο και προϋποθέσεις επίκλησης. Στο Ζώης Θ. Γεώργιος (2017), «Το γενικό συμφέρον και το δημόσιο συμφέρον: Ιστορική διαδρομή και σημερινή λειτουργία της έννοιας», στο *Το Σύνταγμα: Τριμηνιαία Επιθεώρηση Ελληνικής και Ευρωπαϊκής Συνταγματικής Θεωρίας και Πράξης*, Τχ.1/2017, Αθήνα: Εκδόσεις Σάκουλα, σελ. 110.

κάθε μέλους μιας πολιτικά οργανωμένης κοινωνίας»⁸⁷. Εξ' ου, λοιπόν, και η με σαφήνεια αναφορά ότι δημόσιες αρχές και δημόσιοι ή ιδιωτικοί φορείς⁸⁸ που τηρούν αρχεία δημόσιου συμφέροντος θα πρέπει να είναι υπηρεσίες οι οποίες, σύμφωνα με το ενωσιακό δίκαιο ή το δίκαιο κράτους μέλους, υπέχουν εκ του νόμου υποχρέωση να αποκτούν, να διατηρούν, να αξιολογούν, να ταξινομούν, να περιγράφουν, να ανακοινώνουν, να προωθούν, να διαδίδουν και να παρέχουν πρόσβαση σε αρχεία σταθερής αξίας για το γενικό δημόσιο συμφέρον.

Η απαλλαγή δηλαδή από τους περιορισμούς του Κανονισμού λόγω δημοσίου συμφέροντος προκύπτει από τη φύση του οργανισμού που διατηρεί τα αρχεία και όχι από αυτό καθεαυτό το περιεχόμενο των αρχείων. Τέτοιες υπηρεσίες δύναται να είναι τα Εθνικά Αρχεία ή οι φορείς που έχουν σαφή πολιτιστική αποστολή και διατηρούν αρχεία για σκοπούς ιστορικής έρευνας. Επιπρόσθετα, τα κράτη μέλη θα πρέπει να έχουν το δικαίωμα να προβλέπουν περαιτέρω επεξεργασία δεδομένων προσωπικού χαρακτήρα για σκοπούς αρχειοθέτησης, λόγου χάρι με στόχο την παροχή συγκεκριμένων πληροφοριών σχετικών με πολιτική συμπεριφορά σε πρώην απολυταρχικά καθεστώτα, γενοκτονία, εγκλήματα κατά της ανθρωπότητας.⁸⁹ Στην πράξη η αρχειοθέτηση προς το δημόσιο συμφέρον αφορά στην επεξεργασία δεδομένων με σκοπό τη διάθεση και πρόσβαση στην καταγεγραμμένη μνήμη με όρους τεκμηρίωσης και πληροφορίας.

Όμοια με τους όρους και περιορισμούς επεξεργασίας δεδομένων προσωπικού χαρακτήρα για σκοπούς δημοσίου συμφέροντος ο νομοθέτης προέβλεψε δύο ακόμη περιπτώσεις: την επιστημονική και την ιστορική έρευνα (Άρθρο 89 ΓΚΠΔ). Εδώ ισχύουν αντίστοιχα οι προϋποθέσεις και οι εγγυήσεις ως προς τα δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων που συναντάμε σε περιπτώσεις επεξεργασίας δεδομένων περί δημοσίου συμφέροντος, ξεκινώντας από την αρχή της ελαχιστοποίησης και την ακεραιότητα των αρχείων που επιλέγονται για μόνιμη διατήρηση.⁹⁰ Επιπρόσθετα, λόγω της φύσης του σκοπού μιας επιστημονικής ή ιστορικής έρευνας προβλέπεται προσθετικά το μέτρο χρήσης ψευδωνύμων

⁸⁷ Κανελλοπούλου – Μπότη Μαρία (2020), ό.π., σελ. 82-83.

⁸⁸ Στον δικό μας ν.4624/2019 διαβάζουμε ότι ο «ιδιωτικός φορέας» ορίζεται το φυσικό ή νομικό πρόσωπο ή η ένωση προσώπων χωρίς νομική προσωπικότητα, που δεν εμπίπτει στην έννοια του «δημόσιου φορέα». Στο <https://www.e-nomothesia.gr/kat-dedomena-prosopikou-kharaktera/nomos-4624-2019-phke-137a-29-8-2019.html> (τελευταία επίσκεψη 27.8.2021).

⁸⁹ Κανελλοπούλου – Μπότη Μαρία (2020), ό.π..

⁹⁰ Χάρη στην αρχειοθέτηση αρχείων

(ψευδωνυμοποίηση) εφόσον οι εν λόγω σκοποί μπορούν να εκπληρωθούν κατ' αυτόν τον τρόπο.⁹¹

Ξεκινώντας από την αρχή της ελαχιστοποίησης ή αλλιώς αρχή της αναλογικότητας να αναφερθεί ότι πρόκειται για μέθοδο σύμφωνα με την οποία τα δεδομένα θα πρέπει να είναι πρόσφορα, συναφή και αναγκαία για τους επιδιωκόμενους σκοπούς επεξεργασίας. Με λίγα λόγια ο υπεύθυνος επεξεργασίας θα πρέπει να περιορίζεται σε όσα δεδομένα παρουσιάζουν άμεση συνάφεια με το σκοπό της επεξεργασίας, ενώ ταυτόχρονα υπάρχει η οδηγία διατήρησης των δεδομένων για συγκεκριμένο χρονικό διάστημα, το οποίο είναι ισότιμο με το χρόνο που απαιτείται για την επίτευξη των σκοπών της επεξεργασίας. Ένα σημαντικό ζήτημα που έχει προκύψει με αφορμή την αρχή της ελαχιστοποίησης είναι το δικαίωμα του υποκειμένου δεδομένων στη λήθη, το δικαίωμα δηλαδή του ατόμου να ζητήσει την οριστική διαγραφή των προσωπικών του δεδομένων από βάσεις δεδομένων φορέων ή οργανισμών.

Πράγματι σύμφωνα με το άρθρο 17 του Κανονισμού με απώτερο σκοπό τη διαφύλαξη του υποκειμένου των δεδομένων από τους κινδύνους της νέας ψηφιακής πραγματικότητας δίνεται το δικαίωμα το υποκείμενο να αιτηθεί την πλήρη διαγραφή των δεδομένων του από τον υπεύθυνο επεξεργασίας όταν:

1. τα δεδομένα προσωπικού χαρακτήρα δεν είναι πλέον απαραίτητα σε σχέση με τους σκοπούς για τους οποίους συλλέχθηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία,
2. το υποκείμενο των δεδομένων ανακαλεί τη συγκατάθεση επί της οποίας βασίζεται η επεξεργασία,
3. το υποκείμενο των δεδομένων αντιτίθεται στην επεξεργασία σύμφωνα με το άρθρο 21 παράγραφος 1 και δεν υπάρχουν επιτακτικοί και νόμιμοι λόγοι για την επεξεργασία ή το υποκείμενο των δεδομένων αντιτίθεται στην επεξεργασία σύμφωνα με το άρθρο 21 παράγραφος 2,
4. τα δεδομένα προσωπικού χαρακτήρα υποβλήθηκαν σε επεξεργασία παράνομα,
5. τα δεδομένα προσωπικού χαρακτήρα πρέπει να διαγραφούν, ώστε να τηρηθεί νομική υποχρέωση βάσει του ενωσιακού δικαίου ή του δικαίου κράτους μέλους, στην οποία υπόκειται ο υπεύθυνος επεξεργασίας,

⁹¹ Κανονισμός (ΕΕ) 2016/679, ό.π., σελ. 85.

6. τα δεδομένα προσωπικού χαρακτήρα έχουν συλλεχθεί σε σχέση με την προσφορά υπηρεσιών της κοινωνίας των πληροφοριών που αναφέρονται στο άρθρο 8 παρ.1.

Ωστόσο, το εν λόγω δικαίωμα έρχεται σε άμεση αντιδιαστολή με το ρόλο των Αρχείων, που δεν είναι άλλος από τη διατήρηση της μνήμης και άρα δεδομένων, σαφώς και προσωπικού χαρακτήρα, για λόγους δημοσίου συμφέροντος, επιστημονικής και ιστορικής έρευνας και συνεπώς δεν είναι δυνατό να εφαρμοστεί στα αρχεία. Με πιο απλά λόγια, είναι ο σκοπός και η λειτουργία των αρχείων που τα διαχωρίζει από άλλους οργανισμούς ή υπηρεσίες, όπως οι μηχανές αναζήτησης στο διαδίκτυο, και δίνει ισχυρή βάση στα επιχειρήματα, όπως η διαφύλαξη της μνήμης και η προστασία από την επανεγγραφή της ιστορίας.

Σε ό,τι αφορά την ακεραιότητα στην ουσία γίνεται λόγος για το ότι τα δεδομένα πρέπει να υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ασφάλεια και προστασία τους από παράνομη επεξεργασία, απώλεια, καταστροφή ή φθορά τους. Σχετικά με τη μέθοδο χρήσης ψευδωνύμων ουσιαστικά πρόκειται για τη δυνατότητα του υπευθύνου ή εκτελεστή της επεξεργασίας να αλλάξει τα στοιχεία στα αρχεία ώστε να επιτευχθεί η μη ταυτοποίηση του υποκειμένου.

Σε επίπεδο λειτουργίας Αρχείων αυτό σημαίνει την επεξεργασία δεδομένων προσωπικού χαρακτήρα με τέτοιο τρόπο ώστε τα δεδομένα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο δεδομένων χωρίς τη χρήση πρόσθετων πληροφοριών, εφόσον αυτές οι πρόσθετες πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικές και οργανωτικά μέτρα για να διασφαλιστεί η μη απόδοση σε ένα αναγνωρισμένο ή αναγνωρίσιμο άτομο (άρθρο 4 ΓΚΠΔ). Από το ανωτέρω γίνεται κατανοητό ότι η υπηρεσία του Αρχείου φέρει την ευθύνη να διατηρούνται τα αρχικά αρχεία με τα ακριβή δεδομένα, γεγονός που διαφοροποιεί την ψευδονυμοποίηση από εκείνη της ανωνυμοποίησης.⁹²

Τέλος, να σημειωθεί ότι σε επίπεδο επεξεργασίας αρχείων η νομιμότητα του Κανονισμού, όπως και των εκάστοτε εθνικών νόμων⁹³, περί προστασίας των δεδομένων προσωπικού χαρακτήρα απαντά μόνο σε ζώντα υποκείμενα δεδομένων

⁹² “Anonymisation and Pseudonymisation”, <https://www.ucl.ac.uk/data-protection/guidance-staff-students-and-researchers/practical-data-protection-guidance-notices/anonymisation-and> (τελευταία επίσκεψη 27.8.2021).

⁹³ Εξαίρεση αποτελεί η ελληνική νομοθεσία όπου προβλέπεται η προστασία των ανθρώπων που έχουν πεθάνει βάσει της προστασίας της προσωπικότητας, η οποία ωστόσο αναιρείται σε περιπτώσεις όπου η ελευθερία του τύπου ή η ιστορική ελευθερία υπερτερούν. Βλ. ό.π., σελ. 43.

και δεν άπτεται στους θανόντες.⁹⁴ Ενδεικτικά, ισχύει ότι πέραν των εκατό ετών ο υπεύθυνος ή τελών την επεξεργασία μπορεί να θεωρήσει ότι το υποκείμενο των δεδομένων έχει πια πεθάνει. Κάθε κράτος μέλος που δεσμεύεται από τον ΓΚΠΔ έχει τη δυνατότητα να προβλέπει κανόνες σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα θανόντων. Ενδεικτικά το δικό μας δίκαιο έχει τέτοια πρόβλεψη στο νόμο ΑΚ περί προστασίας της προσωπικότητας όπου προστατεύονται τα δεδομένα θανόντων με εξαίρεση περιπτώσεις όπου το αγαθό της ενημέρωσης του κοινού για την ιστορική αλήθεια ή η ελευθερία του τύπου κρίνονται ως υπέρτερα δικαιώματα έναντι της προστασίας προσωπικών δεδομένων.

⁹⁴ Κανονισμός (ΕΕ) 2016/679 *ό.π.*, σελ. 29 και στο European Archives Group (2018), *Ibid*, p. 9.

7. Αρχεία και Ασφάλεια Προσωπικών Δεδομένων

Γίνεται σαφές από όσα προηγήθηκαν ότι από τη μια προκύπτει μεγάλος όγκος δεδομένων χάρη στη ψηφιακή τεχνολογία και από την άλλη ζητήματα προστασίας κατά τη μεταφορά, διαχείριση και εν γένει την επεξεργασία τους. Πιο συγκεκριμένα, σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα στην Ευρώπη ήδη από το 1995 υπήρχε η Οδηγία Προστασίας Δεδομένων (Directive 95/46/EC), όπου διατυπωνόταν ένα κανονιστικό πλαίσιο για την εγγύηση της ασφαλούς και ελεύθερης κυκλοφορίας των προσωπικών δεδομένων πέρα από τα εθνικά σύνορα των χωρών μελών της ΕΕ συνδυαστικά με τον καθορισμό μιας βάσης ασφαλείας για τις προσωπικές πληροφορίες. Αυτό ακριβώς το πλαίσιο ενισχύει ο Γενικός Κανονισμός Προσωπικών Δεδομένων της ΕΕ με την ειδοποιό διαφορά ότι επεκτείνει τη νομική ευθύνη ασφάλειας των δεδομένων προσωπικού χαρακτήρα πέρα από τους υπεύθυνους επεξεργασίας και στους επεξεργαστές των δεδομένων αλλά και στα πρόσωπα που δουλεύουν υπό τις εντολές τους. Όπως ακριβώς, άλλωστε συμβαίνει και με την ευθύνη επεξεργασίας που είδαμε νωρίτερα.

Συγκεκριμένα, λοιπόν, για την ασφάλεια στο Άρθρο 32 του ΓΚΠΔ διαβάζουμε ότι ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων, λαμβάνοντας υπόψη τις τελευταίες εξελίξεις, το κόστος εφαρμογής και τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Στην ουσία επαναλαμβάνονται στο σημείο αυτό οι όροι περί προστασίας των δεδομένων ήδη από το σχεδιασμό και εξ ορισμού, όπως προσδιορίζονται από το νομοθέτη στο άρθρο 25 του ΓΚΠΔ. Επιπρόσθετα, στο άρθρο 32 αναγνωρίζεται πως όσοι λειτουργούν σε δραστηριότητες επεξεργασίας προσωπικών δεδομένων δεσμεύονται και από τον κώδικα δεοντολογίας, όπως αυτός αναπτύσσεται στο άρθρο 40 του Κανονισμού.

Παρενθετικά στο σημείο αυτό να αναφερθεί ότι αν και ο κώδικας δεοντολογίας του Κανονισμού φαίνεται να λειτουργεί δεσμευτικά προς τα κράτη μέλη και τους οργανισμούς που τον ακολουθούν ωστόσο από τη δική μας Αρχή Προστασίας Δεδομένων ισχύει ότι «Οι κώδικες δεοντολογίας δεν είναι υποχρεωτικοί

αλλά προαιρετικοί. Ωστόσο, η Αρχή σαφώς ενθαρρύνει την εκπόνησή τους, υπό την έννοια ότι μπορεί να αποτελούν σύνολο ειδικών κανόνων/πρακτικών προς τη συμμόρφωση με τις συνολικές προϋποθέσεις νόμιμης επεξεργασίας προσωπικών δεδομένων που θέτει ο ΓΚΠΔ, λαμβάνοντας υπόψη τα ειδικά χαρακτηριστικά των διαφόρων τομέων επεξεργασίας».⁹⁵

Επίσης, σημαντικό κατά τη γνώμη μας είναι να σημειωθεί ότι κατά την κατάρτιση ενός κώδικα δεοντολογίας ή κατά την τροποποίηση ή την επέκταση ενός τέτοιου κώδικα, ενώσεις και άλλοι φορείς που εκπροσωπούν κατηγορίες υπευθύνων επεξεργασίας ή εκτελούντων την επεξεργασία θα πρέπει να διαβουλεύονται με τα ενδιαφερόμενα μέρη, μεταξύ άλλων, και με υποκείμενα των δεδομένων, όπου αυτό είναι εφικτό, και να λαμβάνουν υπόψη όσες παρατηρήσεις υποβάλλονται και όσες απόψεις διατυπώνονται στο πλαίσιο αυτών των διαβουλεύσεων.

Επιστρέφοντας στο άρθρο 40 ΓΚΠΔ ορίζεται ότι οι ενώσεις ή άλλοι φορείς που εκπροσωπούν κατηγορίες υπευθύνων ή εκτελούντων επεξεργασία μπορούν να εκπονούν, τροποποιούν ή επεκτείνουν τους υφιστάμενους κώδικες δεοντολογίας ώστε να προσδιορίζουν:

- Τη θεμιτή και με διαφάνεια επεξεργασία,
- Τα έννομα συμφέροντα που επιδιώκουν οι υπεύθυνοι επεξεργασίας στα εκάστοτε πλαίσια,
- Τη συλλογή προσωπικών δεδομένων,
- Τη ψευδωνυμοποίηση των δεδομένων προσωπικού χαρακτήρα,
- Την ενημέρωση του κοινού και των υποκειμένων των δεδομένων,
- Την άσκηση των δικαιωμάτων των υποκειμένων των δεδομένων,
- Την ενημέρωση και την προστασία των παιδιών και τον τρόπο απόκτησης της συγκατάθεσης του ασκούντος τη γονική μέριμνα του παιδιού,
- Τη γνωστοποίηση παραβιάσεων δεδομένων προσωπικού χαρακτήρα στις εποπτικές αρχές και την ανακοίνωση των εν λόγω παραβιάσεων δεδομένων προσωπικού χαρακτήρα στα υποκείμενα των δεδομένων,
- Τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες προκειμένου να παρέχονται οι κατάλληλες εγγυήσεις στο πλαίσιο των

⁹⁵ Αρχή Προστασίας Δεδομένων, «Κώδικες Δεοντολογίας», https://www.dpa.gr/el/foreis/kwdikes_deodologias (τελευταία επίσκεψη 29.8.2021).

διαβιβάσεων σύμφωνα με τους όρους του άρθρου 46 περί διαβιβάσεων που υπόκεινται σε κατάλληλες εγγυήσεις.⁹⁶

Προσθετικά στον κώδικα δεοντολογίας σύμφωνα με τον ΓΚΠΔ αναφέρονται τα μέτρα και οι διαδικασίες στα άρθρα 24 περί ευθύνης του υπευθύνου επεξεργασίας, τα οποία σχολιάστηκαν στο προηγούμενο κεφάλαιο αλλά και οι όροι του άρθρου 25 όπου γίνεται λόγος για την προστασία δεδομένων από το σχεδιασμό και εξ ορισμού, όπως φάνηκε και πρωτίστως. Αξίζει να σημειωθεί σχετικά με το άρθρο 25 ότι υφίστανται επεξεργασία μόνο τα δεδομένα προσωπικού χαρακτήρα που είναι απαραίτητα για τον εκάστοτε σκοπό της επεξεργασίας και η υποχρέωση ισχύει για το εύρος των δεδομένων προσωπικού χαρακτήρα που συλλέγονται, τον βαθμό της επεξεργασίας τους, την περίοδο αποθήκευσης και την προσβασιμότητα τους.

Ενδεικτικά για την περίπτωση των Αρχείων οι εργασίες που καθορίζονται από τους όρους του άρθρου 25 δηλαδή οργανώνονται από το σχεδιασμό και εξ ορισμού είναι όλες εκείνες οι εργασίες που αφορούν στην ανάπτυξη και τη δημιουργία νέων συστημάτων πληροφόρησης. Τέτοια, λόγω χάρη, είναι τα ψηφιακά αποθετήρια, οι τράπεζες δεδομένων σχετικά με αρχεία γεννήσεων ή άλλα στοιχεία που περιέχουν προσωπικές πληροφορίες, τα συστήματα πληροφοριών για τη διαχείριση των υπηρεσιών του αναγνωστήριου αλλά και τα εργαλεία για on-line πρόσβαση, που στις εποχές αποκλεισμού που διανύουμε λόγω πανδημίας προσέφεραν μια χρήσιμη εναλλακτική για την ανεύρεση τεκμηρίων σε βιβλιοθήκες, μουσεία και άλλους πολιτιστικούς ή μη, δημόσιους ή ιδιωτικούς φορείς.

Για παράδειγμα, αν θεωρηθεί ότι οι υπηρεσίες αρχειοθέτησης ενός οργανισμού καλούνται να οργανώσουν και να περιγράψουν μια ομάδα εγγράφων (archive fonds) που περιλαμβάνουν προσωπικά δεδομένα ζωντανών ατόμων σχετικά με την υγεία, τη σεξουαλική ζωή, τις πολιτικές απόψεις και άλλες ειδικές κατηγορίες δεδομένων ή δεδομένα που σχετίζονται με ποινικές καταδίκες, τότε οι υπηρεσίες πρέπει να δημιουργήσουν ένα βοήθημα εύρεσης που να δείχνει πραγματικά ονόματα ώστε να είναι σε θέση να απαντήσουν σε πιθανά αιτήματα πρόσβασης των υποκειμένων δεδομένων και να συμμορφωθούν με τα δικαιώματα άλλων υποκειμένων δεδομένων.

Παράλληλα, έχουν τη δυνατότητα να δημιουργήσουν μια on-line εκδοχή του βοηθήματος ώστε να ικανοποιήσουν τυχόν ανάγκες διαδικτυακής έρευνας όμως τα

⁹⁶ Κανονισμός (ΕΕ) 2016/679, ό.π, σελ. 57.

ονόματα εδώ για λόγους προστασίας των δικαιωμάτων των ζώντων υποκειμένων των δεδομένων θα έχουν υποστεί ψευδωνυμοποίηση. Επομένως, κρίνεται απαραίτητη η ανάπτυξη λογισμικού που να προσφέρει τη δυνατότητα για αρχειακή περιγραφή που να επιτρέπει τη δημιουργία δύο διαφορετικών εκδόσεων ενός βοηθήματος εύρεσης, μία με πραγματικά ονόματα και μία με ψευδώνυμα. Ένα τέτοιο λογισμικό ορίζεται ως ένα εργαλείο συμμόρφωσης με τους όρους του άρθρου 25 διότι πληρούνται οι προϋποθέσεις προστασίας και ασφάλειας των δεδομένων προσωπικού χαρακτήρα.

Εξίσου σημαντικό είναι ότι για τον Κανονισμό τα μέτρα και οι τεχνικές ασφαλείας ισότιμα πρέπει να ορίζουν και το απόρρητο, την ακεραιότητα και τη διαθεσιμότητα των προσωπικών δεδομένων.⁹⁷ Κατά συνέπεια η ασφάλεια οφείλει να γίνεται αντιληπτή ως μια προσέγγιση βάσει κινδύνου: όσο υψηλότερος είναι ο κίνδυνος για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων, τόσο πιο αυστηρά είναι τα μέτρα που πρέπει να λάβει ο υπεύθυνος επεξεργασίας προκειμένου να διαχειριστεί τον κίνδυνο. Για το λόγο αυτό, άλλωστε ο νομοθέτης έχει διατυπώσει στο τμήμα 3 τους όρους εκτίμησης αντικτύπου σχετικά με την προστασία των δεδομένων. Με άλλα λόγια, εκτιμάται από τον υπεύθυνο επεξεργασίας ο κίνδυνος ή και περισσότεροι του ενός προς τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων.

Οι αρχειονόμοι και όσοι απασχολούνται με την επεξεργασία δεδομένων, όπως οι επιστήμονες της πληροφορικής, είναι γνωστό ότι έχουν μια μακρά ιστορία διαχείρισης και διευκόλυνσης της πρόσβασης σε τεκμήρια και αρχεία επομένως έχουν τη δυνατότητα να εφεύρουν οργανωτικές και τεχνικές λύσεις. Ωστόσο, το ηλεκτρονικό περιβάλλον χάριν των νέων τεχνολογιών συνεχώς αναπτύσσεται και άρα προκαλούνται πιο περίπλοκα ζητήματα πρόσβασης λόγω της κλίμακας και της ποικιλίας αυτών των ίδιων των ηλεκτρονικών αρχείων. Σε πολλές περιπτώσεις τα μεγάλα δεδομένα δεν μπορούν να ελεγχθούν και να επαληθευτούν με μη αυτόματο τρόπο πριν από την πρόσβαση, οπότε οι εγγυήσεις και οι έλεγχοι θα πρέπει να αυτοματοποιούνται ολοένα και περισσότερο.⁹⁸

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα, στον βαθμό που είναι αυστηρά αναγκαία και ανάλογη για τους σκοπούς της διασφάλισης της ασφάλειας δικτύων και πληροφοριών, δηλαδή της ικανότητας ενός δικτύου ή ενός συστήματος πληροφοριών να ανθίσταται, σε ένα δεδομένο επίπεδο εμπιστοσύνης, σε τυχαία

⁹⁷ ENISA (December 2017), *Handbook on security of personal data processing*, p.8.

⁹⁸ European Archives Group (2018), *Ibid*, p.24.

γεγονότα ή παράνομες ή κακόβουλες ενέργειες οι οποίες θέτουν σε κίνδυνο τη διαθεσιμότητα, τη γνησιότητα, την ακεραιότητα και την εμπιστευτικότητα αποθηκευμένων ή διαβιβαζόμενων δεδομένων προσωπικού χαρακτήρα, καθώς και της ασφάλειας των σχετικών υπηρεσιών που προσφέρουν τα εν λόγω δίκτυα και συστήματα ή που είναι προσπελάσιμες μέσω των εν λόγω δικτύων και συστημάτων, ή που προσφέρονται από δημόσιες αρχές, από ομάδες αντιμετώπισης έκτακτων αναγκών στην πληροφορική (CERT), από ομάδες παρέμβασης για συμβάντα που αφορούν την ασφάλεια των υπολογιστών (CSIRT), από παρόχους δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών και από παρόχους τεχνολογιών και υπηρεσιών ασφάλειας, αποτελεί έννομο συμφέρον του ενδιαφερόμενου υπευθύνου επεξεργασίας δεδομένων. Αυτό θα μπορούσε να περιλαμβάνει, λόγω χάρη, την αποτροπή ανεξουσιοδότητης πρόσβασης σε δίκτυα ηλεκτρονικών επικοινωνιών και διανομής κακόβουλων κωδικών και την παύση επιθέσεων «άρνησης υπηρεσίας» και ζημιών σε συστήματα πληροφορικής και ηλεκτρονικών επικοινωνιών.

Έχει επανειλημμένα σημειωθεί στην παρούσα ότι η σύγχρονη εποχή χαρακτηρίζεται από την έκρηξη της τεχνολογίας και της επιστήμης της πληροφορικής. Η χρήση των υπολογιστικών συστημάτων έχει προ πολλού ξεπεράσει τους σταθερούς ή φορητούς υπολογιστές περνώντας με μεγάλη επιτυχία και πολλές ακόμη νέες δυνατότητες στα έξυπνα κινητά, τις έξυπνες οικιακές συσκευές που οραματίζονται μια πιο απλή, εύκολη και έξυπνη ζωή στο σπίτι ή το γραφείο. Κοινός τόπος της έξυπνης τεχνολογίας είναι η διασύνδεση των συσκευών και άρα η δυνατότητα αποθήκευσης, μεταφοράς και πρόσβασης αγαπημένων αρχείων, όπως φωτογραφίες ή βίντεο, σε ένα δίκτυο συσκευών απλά με το πάτημα ενός κουμπιού. Ένα ακόμη παράδειγμα της εξέλιξης των υπολογιστικών συστημάτων είναι τα υπολογιστικά νέφη ή αλλιώς γνωστά με την αγγλική ορολογία cloud, όπου μέσω διαδικτύου καθίσταται δυνατή η διάθεση υπολογιστικών πόρων από κεντρικά συστήματα που βρίσκονται απομακρυσμένα από το χρήστη αξιοποιώντας αυτοματοποιημένες διαδικασίες παρέχοντας αυτό που ακριβώς διαφημίζουν: ευκολία και ευελιξία σύνδεσης.

Απομακρυσμένη πρόσβαση, διανεμημένες πληροφοριακές υπηρεσίες και εικονικά περιβάλλοντα είναι η πραγματικότητα του σήμερα και πάνω σε αυτά οφείλουμε να χτίσουμε τις νέες υπηρεσίες πρόσβασης στη γνώση, την πληροφορία και τα δεδομένα. Όλα τα παραπάνω να μην έχουν απλουστεύσει τη διαχείριση αρχείων και όγκου πληροφορίας όμως παράλληλα έχουν δημιουργήσει νέες μορφές

κινδύνων για τη διαρροή δεδομένων, που όπως φάνηκε νωρίτερα στο σύνολό τους αποτελούν δεδομένα προσωπικού χαρακτήρα είτε απλής είτε πιο ειδικής φύσεως.

Για το λόγο αυτό συντάχθηκε ο Γενικός Κανονισμός από την ΕΕ, ώστε να τεθούν οι κανόνες λειτουργίας και διαχείρισης προσωπικών δεδομένων, και γι' αυτό ο Οργανισμός Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) έχει εκδώσει σχετικό οδηγό για την προστασία και την εκτίμηση ενδεχόμενων κινδύνων και παραβιάσεων των συστημάτων πληροφόρησης. Σκοπός και των δύο αυτών δράσεων είναι η ενθάρρυνση των υπευθύνων επεξεργασίας δεδομένων αρχείων και προσωπικών στοιχείων να αναλάβουν δράσεις σχετικές προς τη συμμόρφωση με τους όρους νομικής προστασίας και ασφάλειας τους δικαιώματος της ιδιωτικής ζωής (άρθρο 32 του Κανονισμού).

Στην πράξη αυτό που επιχειρείται είναι κατά την αξιολόγηση του κατάλληλου επιπέδου ασφαλείας να λαμβάνονται υπόψη οι κίνδυνοι που παρουσιάζονται από την επεξεργασία δεδομένων προκαλούμενοι από τυχαία ή παράνομη καταστροφή, απώλεια, τροποποίηση, μη εξουσιοδοτημένη αποκάλυψη ή πρόσβαση σε δεδομένα προσωπικού χαρακτήρα.⁹⁹ Στον οδηγό εκτίμησης λοιπόν κινδύνων της ENISA συναντάμε αρχικά την κατηγοριοποίηση των κινδύνων ανάλογα με το ύψος της επικινδυνότητας ή αλλιώς του αντικτύπου που ενέχει για τα υποκείμενα των δεδομένων: χαμηλό, μεσαίο, υψηλό και πολύ υψηλό.

Στα χαμηλού αντικτύπου ανήκουν παραβιάσεις της προστασίας που προκαλούν χαμηλού μεγέθους ενοχλήσεις στα υποκείμενα των δεδομένων, όπως πχ το να ξοδευτεί χρόνος επανεισαγωγής πληροφοριών σε μια ιστοσελίδα λόγω μπλοκαρίσματος του λειτουργικού της ή μη δυνατότητας επικοινωνίας των σερβερ κατά τη φόρτωση της σελίδας. Ο μεσαίου επιπέδου αντίκτυπος προκαλεί περισσότερες ενοχλήσεις στα υποκείμενα μιας και σχετίζεται συνήθως με την απώλεια ακεραιότητας της υπηρεσίας που επεξεργάζεται τα δεδομένα. Επί παραδείγματι, σε μια διαδικασία αξιολόγησης προσωπικού συχνά καταγράφονται ποσοτικές και ποιοτικές αξίες ενός ή περισσότερων υπαλλήλων με στόχο τη δημιουργία ενός λεπτομερούς επαγγελματικού προφίλ. Παρ' όλο που η αξιολόγηση μπορεί να περιορίζεται στις επιδόσεις της εργασίας, κατά τη διάρκεια της άσκησης, μπορεί να προκύψουν και επιπλέον χαρακτηριστικά του ατόμου, δημιουργώντας έναν οριακό κίνδυνο να επεξεργαστούν επίσης πληροφορίες σχετικά με τη συμπεριφορά,

⁹⁹ ENISA (December 2017), *ibid.*

την προσωπικότητα και τις αξίες οδηγώντας σε ενόχληση ή περιορισμό του υπαλλήλου.¹⁰⁰

Αντίστοιχα, στις υψηλού και πολύ υψηλού επιπέδου παραβιάσεις των μέσων προστασίας και άρα διαρροής των δεδομένων τα υποκείμενα δύναται να αντιμετωπίσουν πιο σοβαρές επιπτώσεις όπως καταστροφή ιδιοκτησίας, απώλεια εργασίας, μακροπρόθεσμα ψυχολογικά προβλήματα κ.α.. Ενδεικτικά, κρίνεται σκόπιμο να αναφερθεί η περίπτωση όπου η συστηματική επεξεργασία δεδομένων καταναλωτικών ή αναγνωστικών προτιμήσεων για την αποστολή διαφημιστικών μηνυμάτων στο κινητό ή το ηλεκτρονικό ταχυδρομείο (newsletter) δεν πραγματοποιείται με όρους ασφάλειας και προστασίας και μπορεί να οδηγήσει σε αποκάλυψη δεδομένων προσωπικού χαρακτήρα που πιθανόν να συνδέονται με πολιτικές απόψεις ή κατάσταση της υγείας του υποκειμένου σε κάποιο τρίτο ενδιαμέσο που δεν έχει καμία άδεια ή συγκατάθεση διαχείρισης και επεξεργασίας των δεδομένων. Τέτοιου είδους διαρροές ειδικών δεδομένων προσωπικού χαρακτήρα χαρακτηρίζονται ως υψηλού και πολύ υψηλού χαρακτήρα ρίσκα.

Η εκτίμηση αντικτύπου και των κινδύνων είναι γνωστή και ως διαδικασία διαχείρισης κινδύνων (Risk management process), που αφορά στη συστηματική εφαρμογή πολιτικών, διαδικασιών διαχείρισης και πρακτικές στις δραστηριότητες επικοινωνίας, διαβούλευσης, καθιέρωσης του πλαισίου και εντοπισμού, ανάλυσης, αξιολόγησης, αντιμετώπισης, παρακολούθησης και επανεξέτασης των κινδύνων.¹⁰¹ Πιο απλά ειπωμένο πρόκειται για τις συντονισμένες δραστηριότητες για την κατεύθυνση και τον έλεγχο ενός οργανισμού σε σχέση με τον κίνδυνο, διαδικασία γνώριμη στους οργανισμούς διαχείρισης και επεξεργασίας των δεδομένων.

Ο ΓΚΠΔ αναφέρεται στη διαδικασία διαχείρισης κινδύνων χωρίς ωστόσο να προτείνει συγκεκριμένα μέτρα ασφαλείας που πρέπει να έχουν ο υπεύθυνος ή τελών την επεξεργασία.¹⁰² Μόνη του απαίτηση είναι η διασφάλιση των κατάλληλων επιπέδων ασφαλείας σύμφωνα με τους πιθανούς κινδύνους του έργου της επεξεργασίας που έχουν αναλάβει, μιας και αναγνωρίζει το πόσο πιθανό και υπαρκτό είναι να προκληθεί παραβίαση ασφαλείας (breach) που θα οδηγήσει πιθανά σε τυχαία ή παράνομη καταστροφή, απώλεια, τροποποίηση, μη εξουσιοδοτημένη αποκάλυψη ή

¹⁰⁰ Ibid, p.24.

¹⁰¹ European Data Protection Supervisor (21 March 2016), *Security measures for professional data processing: Article 22 of Regulation 45/2001*, p.13.

¹⁰² European Archives Group (2018), Ibid, p. 25.

πρόσβαση σε προσωπικά δεδομένα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία (άρθρο 4 παρ. 12)¹⁰³.

¹⁰³ Κανονισμός (ΕΕ) 2016/679, *ό.π.*, σελ. 34.

8. Δίκτυα Προστασίας Προσωπικών Δεδομένων

Συνοψίζοντας όσα έχουν εξεταστεί μέχρι αυτό το σημείο να τονιστεί ότι η ασφάλεια στον καιρό του διαδικτύου και των νέων τεχνολογιών ανάγεται σε καίριο ζήτημα που αποσκοπεί στη διασφάλιση των δικαιωμάτων των ατόμων σχετικά με τη διαχείριση των προσωπικών τους δεδομένων. Σε επίπεδο οργανισμών που διαχειρίζονται αρχεία, οι υπεύθυνοι επεξεργασίας των τελευταίων αλλά και όσοι συνολικά δύναται να απασχολούνται σε τέτοιες εργασίες όπως ο εκτελών την επεξεργασία και οι τυχόν υπάλληλοι ή συνεργάτες του, καθίστανται από το νόμο ως υπεύθυνοι για την ασφάλεια των δεδομένων προσωπικού χαρακτήρα που έχουν στη διάθεσή τους. Επιπρόσθετα, σύμφωνα με τις υπάρχουσες επαγγελματικές πρακτικές, οφείλουν να διασφαλίζουν την ακεραιότητα και την αυθεντικότητά των δεδομένων και να τα προστατεύουν από μη εξουσιοδοτημένη πρόσβαση, αλλοίωση, απώλεια, ζημιά ή καταστροφή.

Συνεπώς γίνεται ευκόλως κατανοητό ότι τα αρχεία πρέπει να αποθηκεύονται με ασφάλεια, ώστε να τηρείται το απόρρητο ανά πάσα στιγμή. Η πρόσβαση πρέπει να παρέχεται μόνο σε όσους έχουν ανάγκη να γνωρίζουν ότι μπορούν να ικανοποιηθούν τα αιτήματα και τα δικαιώματά τους βάσει του ισχύοντος νομικού πλαισίου τόσο σε επίπεδο γενικά της Ευρωπαϊκής Ένωσης όσο και ξεχωριστά σε επίπεδο κράτους μέλους. Το επίπεδο ασφάλειας πρέπει να είναι κατάλληλο και ανάλογο με τη φύση των δεδομένων και τη ζημιά που θα μπορούσε να προκύψει από πιθανή παραβίαση της ασφάλειας. Πρέπει, δηλαδή, με άλλα λόγια να αντικατοπτρίζει τα επαγγελματικά πρότυπα και τη χρήση τεχνικών διαχείρισης κινδύνου για την αξιολόγηση της φύσης, του επιπέδου και του αντίκτυπου των κινδύνων και τα κατάλληλα μέτρα που πρέπει να ληφθούν για την προστασία των δεδομένων.

Η επίτευξη της ασφάλειας καθίσταται υπαρκτή όταν πληρούνται προδιαγραφές που διασφαλίζουν:

- i. την εμπιστευτικότητα, δηλαδή, την πρόληψη μη εξουσιοδοτημένης αποκάλυψης πληροφοριών,
- ii. την ακεραιότητα, δηλαδή, την πρόληψη της μη εξουσιοδοτημένης μεταβολής των πληροφοριών και
- iii. τη διαθεσιμότητα, να είναι δηλαδή οι πληροφορίες διαθέσιμες χωρίς κωλύματα ή καθυστερήσεις από μη εξουσιοδοτημένα άτομα.

Τα πρακτικά μέτρα ασφαλείας, γνώριμα στους επαγγελματίες του είδους όπως οι αρχιονόμοι, που πρέπει να ληφθούν υπόψη περιλαμβάνουν την εγκατάσταση συσκευών φυσικής ασφάλειας, όπως συναγερμούς εισβολέων, περιορισμό της πρόσβασης σε ασφαλείς περιοχές, τήρηση αρχείου επισκεπτών και εποπτεία των δραστηριοτήτων τους στο μέτρο του δυνατού.

Από την άλλη, τα ηλεκτρονικά δεδομένα πρέπει να είναι ασφαλή και για να καταστεί αυτό δυνατό οι υπεύθυνοι επεξεργασίας οφείλουν να συνεργαστούν με τους τεχνικούς των υπολογιστών και λοιπών συστημάτων πληροφόρησης ώστε να διασφαλιστεί η μέγιστη ασφάλεια λειτουργίας των λογισμικών και των δικτύων που αξιοποιούνται από την υπηρεσία. Ως μέσα προστασίας των ανωτέρω λογίζονται τα μέσα προστασίας λογισμικού από ιούς και Trojans, τα γνώριμα μας πια antivirus, και πρόσβαση με έλεγχο κωδικού πρόσβασης μόνο για εξουσιοδοτημένους χρήστες. Τα προσωπικά δεδομένα πρέπει να διαβιβάζονται με ασφάλεια: τα εργαλεία κρυπτογράφησης πρέπει να χρησιμοποιούνται για την ασφαλή μετάδοση ηλεκτρονικών προσωπικών δεδομένων.

Καίριος όρος που συναντά κανείς στη βιβλιογραφία σχετικά με τη διαχείριση των ανωτέρω είναι το σύστημα δικτύου και πληροφοριών. Ως τέτοιο ορίζεται από τη νομοθεσία α) κάθε συσκευή ή ομάδα διασυνδεδεμένων ή σχετιζόμενων συσκευών από τις οποίες μία ή περισσότερες εκτελούν, βάσει προγράμματος, αυτόματη επεξεργασία ψηφιακών δεδομένων και β) ψηφιακά δεδομένα που αποθηκεύονται, υποβάλλονται σε επεξεργασία, ανακτώνται ή μεταδίδονται από στοιχεία που καλύπτονται στα σημεία δικτύου ηλεκτρονικών επικοινωνιών και στις δυνάμει υπαρκτές συσκευές – διασυνδεδεμένες ή σχετιζόμενες – που εκτελούν λειτουργίες επεξεργασίας για τους σκοπούς της λειτουργίας, χρήσης, προστασίας και συντήρησής τους.¹⁰⁴

Επιπρόσθετα, είναι σαφές αν όχι αυτονόητο ότι η διαχείριση περιστατικών (risk management) περιλαμβάνει τον εντοπισμό και την ανταπόκριση σε συμβάντα ασφάλειας υπολογιστών, καθώς και την προστασία κρίσιμων δεδομένων, στοιχείων και συστημάτων για την αποφυγή συμβάντων. Οι ενέργειες που λαμβάνονται για την πρόληψη ή τον μετριασμό τρεχόντων και πιθανών συμβάντων και συμβάντων ασφάλειας υπολογιστών μπορεί να περιλαμβάνουν εργασίες που εκτελούνται από ένα ευρύ φάσμα συμμετεχόντων σε όλη την επιχείρηση, όπως οι αναλυτές ασφάλειας, οι

¹⁰⁴ Κανονισμός (ΕΕ) 2016/679.

χειριστές συμβάντων, οι διαχειριστές δικτύων και συστημάτων, προσωπικό ανθρώπινου δυναμικού και δημόσιων υποθέσεων, προγραμματιστές προϊόντων, ακόμη και τελικοί χρήστες. Μια συγκεκριμένη οργανωτική οντότητα που μπορεί να συσταθεί για να συντονίσει και να διαχειριστεί τη διαδικασία διαχείρισης συμβάντων σε έναν οργανισμό είναι η ομάδα αντιμετώπισης συμβάντων ασφαλείας υπολογιστών (Computer Security Incident Response Teams – CSIRT).

Για τη διασφάλιση ορθής λειτουργίας και ασφάλειας ενός οργανισμού διαχείρισης αρχείων και κατ' επέκταση δεδομένων προσωπικού χαρακτήρα, υπό τη σκέπη του ΓΚΠΔ και των ελάχιστων προδιαγραφών προτείνεται από την Ευρωπαϊκή Ένωση στην οδηγία 2016/1148 άρθρο 12¹⁰⁵ η δημιουργία ενός δικτύου αυτών των αρμόδιων αρχών ή των ομάδων απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών (CSIRT).¹⁰⁶ Πιο συγκεκριμένα, προβλέπεται ότι το δίκτυο CSIRT θα λειτουργεί με σκοπό τη συμβολή στην ανάπτυξη της αξιοπιστίας και της εμπιστοσύνης μεταξύ των κρατών μελών και την προώθηση της ταχείας και αποτελεσματικής επιχειρησιακής συνεργασίας.¹⁰⁷ Το δίκτυο απαρτίζεται από αντιπροσώπους των CSIRT των κρατών μελών και την Ομάδα Ηλεκτρονικής Αντιμετώπισης Έκτακτης Ανάγκης της Ευρωπαϊκής Ένωσης (Computer Emergency Response Team, CERT-EU).

Παρενθετικά για την τελευταία να σημειωθεί ότι μετράει ήδη δέκα χρόνια λειτουργίας και απαρτίζεται από εμπειρογνώμονες ασφαλείας πληροφορικής από τα κύρια θεσμικά όργανα της ΕΕ (Ευρωπαϊκή Επιτροπή, Γενική Γραμματεία του Συμβουλίου, Ευρωπαϊκό Κοινοβούλιο, Επιτροπή των Περιφερειών, Οικονομική και Κοινωνική Επιτροπή) και συνεργάζεται στενά με άλλες CERT στα κράτη μέλη και πέρα από αυτήν, καθώς και με εξειδικευμένες εταιρείες ασφαλείας πληροφορικής. Επιπρόσθετα, ο σκοπός της είναι να συμβάλει στην ασφάλεια της υποδομής των τεχνολογιών πληροφοριών και επικοινωνιών όλων των θεσμικών οργάνων της Ένωσης, φορέων και οργανισμών βοηθώντας στην πρόληψη, τον εντοπισμό, τον μετριασμό και την ανταπόκριση στις κυβερνοεπιθέσεις και ενεργώντας ως κόμβος συντονισμού ανταλλαγής πληροφοριών και ανταπόκρισης συμβάντων στον

¹⁰⁵ Ο.π..

¹⁰⁶ Αντίστοιχες ομάδες επέμβασης φυσικά λειτουργούν και στις ΗΠΑ και τον Καναδά. Βλ. ενδεικτικά <https://us-cert.cisa.gov/bsi/articles/best-practices/incident-management/defining-computer-security-incident-response-teams>

¹⁰⁷ Enisa, “CSIRTs network”, <https://www.enisa.europa.eu/topics/csirts-in-europe/csirts-network> (τελευταία επίσκεψη 5.09.2021).

κυβερνοχώρο για τα συστατικά μέρη.¹⁰⁸ Ομάδες CERT λειτουργούν εξίσου και σε εθνικό επίπεδο κρατών μελών αλλά και οργανισμών όπως οι βιβλιοθήκες, τα πανεπιστήμια και λοιπά ερευνητικά κέντρα, οι οποίες συνεργάζονται μεταξύ τους δημιουργώντας ένα ακόμη δίκτυο συνεργασίας σε τοπικό επίπεδο με σκοπό την προστασία στο διαδίκτυο και την αποφυγή διαρροής δεδομένων. Οι CERTs, με άλλα λόγια, έχουν αναπτυχθεί τόσο στον ιδιωτικό όσο και στον δημόσιο τομέα ως μικρές ομάδες κυβερνοεμπειρογνομόνων συνδεδεμένων στο διαδίκτυο που μπορούν να ανταποκριθούν αποτελεσματικά σε περιστατικά ασφάλειας πληροφοριών και απειλές στον κυβερνοχώρο. Είναι σαφές λοιπόν ότι η μεταξύ τους συνεργασία είτε σε διεθνές είτε σε τοπικό επίπεδο είναι απαραίτητη για την επίτευξη της μέγιστης ασφάλειας και διαφάνειας.

Επιστρέφοντας στο δίκτυο CSIRT να σημειωθεί ότι έχει τα εξής καθήκοντα:

α) ανταλλαγή πληροφοριών σχετικά με τις υπηρεσίες, τις δραστηριότητες και τις δυνατότητες συνεργασίας των CSIRT·

β) κατόπιν αιτήματος του αντιπροσώπου CSIRT κράτους μέλους που ενδέχεται να επηρεάζεται από ένα συμβάν, ανταλλαγή και συζήτηση μη ευαίσθητων από εμπορικής άποψης πληροφοριών που σχετίζονται με το συγκεκριμένο συμβάν και συναφείς κινδύνους· ωστόσο, κάθε κράτος μέλος μπορεί να αρνηθεί να συμβάλει στη συζήτηση αυτή εάν υπάρχει κίνδυνος να θιγεί η διερεύνηση του συμβάντος·

γ) ανταλλαγή και διάθεση σε εθελούσια βάση μη εμπιστευτικών πληροφοριών για μεμονωμένα συμβάντα·

δ) κατόπιν αιτήματος αντιπροσώπου CSIRT κράτους μέλους, συζήτηση και, εφόσον είναι δυνατόν, καθορισμός συντονισμένης απόκρισης για ένα συμβάν που έχει διαπιστωθεί εντός της δικαιοδοσίας του συγκεκριμένου κράτους μέλους·

ε) υποστήριξη των κρατών μελών για την αντιμετώπιση διασυνοριακών συμβάντων βάσει της εθελούσιας αμοιβαίας συνδρομής τους·

στ) συζήτηση, διερεύνηση και καθορισμός περαιτέρω μορφών επιχειρησιακής συνεργασίας, συμπεριλαμβανομένων μεταξύ άλλων και τα σχετικά με:

- i) τις κατηγορίες κινδύνων και συμβάντων·
- ii) τις έγκαιρες προειδοποιήσεις·

¹⁰⁸ <https://cert.europa.eu/static/RFC2350/RFC2350.pdf> (τελευταία επίσκεψη 5.09.2021).

- iii) την αμοιβαία συνδρομή·
- iv) τις αρχές και τις λεπτομέρειες για τον συντονισμό, όταν τα κράτη μέλη παρεμβαίνουν για την αντιμετώπιση διασυνοριακών κινδύνων και συμβάντων·
- ζ) ενημέρωση της ομάδας συνεργασίας σχετικά με τις δραστηριότητές του και τις περαιτέρω μορφές επιχειρησιακής συνεργασίας που συζητούνται σύμφωνα με το στοιχείο στ), και υποβολή αιτήματος για καθοδήγηση ως προς αυτό·
- η) συζήτηση των διδαγμάτων που αντλούνται από ασκήσεις σχετικά με την ασφάλεια συστημάτων δικτύου και πληροφοριών, συμπεριλαμβανομένων μεταξύ άλλων και από εκείνες που οργανώνει ο ENISA·
- θ) κατόπιν αιτήματος μεμονωμένου CSIRT, συζήτηση των δυνατοτήτων και της ετοιμότητας του εν λόγω CSIRT.

Στο σημείο αυτό να αναφερθεί ότι πέρα από με τις ομάδες των CSIRT και CERTs συνήθως σε φορείς ή επιχειρήσεις υπάρχει και λειτουργεί το κέντρο επιχειρήσεων ασφαλείας (security operations center, SOC). Το τελευταίο είναι μια εγκατάσταση όπου το δίκτυο, οι εφαρμογές και τα τελικά σημεία ενός οργανισμού παρακολουθούνται και προστατεύονται από πιθανές επιθέσεις.¹⁰⁹ Λειτουργεί δηλαδή ως τη πρώτη βαθμίδα προάσπισης των δεδομένων ενάντια σε εξωτερικές επιθέσεις σε επίπεδο μιας επιχείρησης, ενώ οι άλλες δύο ομάδες λειτουργούν σε μεγαλύτερο επίπεδο χώρας/-ων, οργανισμών ή βιομηχανιών προσφέροντας ευρύτερο πεδίο δράσης.

Ένα ακόμη δίκτυο που έχει συσταθεί για να φέρει κοντά προγραμματιστές και εμπειρογνώμονες προστασίας δεδομένων με τεχνικό υπόβαθρο από διαφορετικούς τομείς, προκειμένου να ξεκινήσουν και να υποστηρίζουν έργα που ενσωματώνουν την ιδιωτικότητα σε καθημερινά εργαλεία και αναπτύσσουν νέα εργαλεία που μπορούν αποτελεσματικά να προστατεύσουν και να ενισχύσουν το απόρρητο είναι το Δίκτυο Μηχανικής Απορρήτου Διαδικτύου (Internet Privacy Engineering Network, IPEN).¹¹⁰ Σκοπός του εν λόγω δικτύου είναι η προώθηση και εξέλιξη της τελευταίας τεχνολογίας της μηχανικής απορρήτου, υποστηρίζοντας μηχανικούς δικτύων που απασχολούνται σε δομικά στοιχεία, σχέδια σχεδίασης και άλλα αντίστοιχα εργαλεία για επιλεγμένες περιπτώσεις χρήσης του διαδικτύου όπου η προστασία της

¹⁰⁹ “The Complete Guide to CSIRT organization: How to Build an Incident Response Team”, <https://www.exabeam.com/incident-response/csirt/> (τελευταία επίσκεψη 5.09.2021).

¹¹⁰ “IPEN – Internet Privacy Engineering Network”, https://edps.europa.eu/data-protection/ipen-internet-privacy-engineering-network_en (τελευταία επίσκεψη 5.09.2021).

ιδιωτικότητας κρίνεται ιδιαίτερα επισφαλής. Λόγω της φύσης και της ουσίας δράσης του, το IPEN προσκαλεί συμμετέχοντες από διαφορετικούς τομείς, όπως ρυθμιστικές αρχές, ακαδημαϊκούς χώρους, ανοικτού κώδικα ανάπτυξης επιχειρήσεων και άλλα άτομα που έχουν δεσμευτεί να βρίσκουν μηχανικές λύσεις σε προκλήσεις απορρήτου. Ο γενικός στόχος είναι η ενσωμάτωση της προστασίας δεδομένων και της ιδιωτικής ζωής σε όλες τις φάσεις της διαδικασίας ανάπτυξης, από τη φάση των απαιτήσεων έως την παραγωγή, ως πιο κατάλληλη ανάλογα με το μοντέλο ανάπτυξης και το περιβάλλον εφαρμογής.

Καθώς οι οργανισμοί γίνονται πιο περίπλοκοι και δυνατότητες, όπως οι CSIRT και οι CERTs, ενσωματώνονται περισσότερο σε οργανωτικές επιχειρηματικές λειτουργίες, είναι σαφές ότι η διαχείριση συμβάντων δεν είναι μόνο η εφαρμογή τεχνολογίας για την επίλυση συμβάντων ασφάλειας υπολογιστών. Είναι επίσης η ανάπτυξη ενός σχεδίου δράσης, το οποίο είναι ένα σύνολο διαδικασιών που είναι συνεπείς, επαναλαμβανόμενες, υψηλής ποιότητας, μετρήσιμες και κατανοητές εντός της υπηρεσίας, του οργανισμού ή του δικτύου των συνεργαζόμενων φορέων ή επιχειρήσεων. Για να γίνει αυτό, το σχέδιο θα πρέπει να ενσωματωθεί σε υπάρχουσες διαδικασίες και οργανωτικές δομές έτσι ώστε να επιτρέπει παρά να εμποδίζει κρίσιμες επιχειρηματικές λειτουργίες. Το σχέδιο θα πρέπει επίσης να υποστηρίζει, να συμπληρώνει και να παρέχει στοιχεία σε υπάρχουσες πολιτικές επιχειρήσεων και πληροφορικής που επηρεάζουν την ασφάλεια της υποδομής ενός οργανισμού, όπως και κάθε άλλη διαδικασία διαχείρισης περιστατικών.

9. Συμπεράσματα

Η εξέλιξη της τεχνολογίας και η χωρίς επιλογή πλέον είσοδος του ανθρώπου στην Κοινωνία της Πληροφορίας οδήγησε στην όλο και μεγαλύτερη έκθεση της προσωπικότητάς του και στη δημοσιοποίηση των προσωπικών του δεδομένων. Οι παραβιάσεις της ιδιωτικότητας είναι ακόμα πιο εύκολες με συνέπεια να κρίνεται επιτακτική η ανάγκη για την προστασία της. Μόνο όμως η αναγνώριση του προβλήματος δεν είναι αρκετή· θα πρέπει να υπάρξει η άμεση ευαισθητοποίηση και κινητοποίηση όλων των φορέων προκειμένου να προστατευθεί ο πολίτης. Τα συστήματα και οι υπηρεσίες δικτύων και πληροφοριών διαδραματίζουν ζωτικό ρόλο στην κοινωνία. Η αξιοπιστία και η ασφάλειά τους είναι ουσιώδους σημασίας για τις οικονομικές και κοινωνικές δραστηριότητες. Για την επίτευξη και τη διατήρηση υψηλού επιπέδου ασφάλειας των συστημάτων δικτύου και πληροφοριών, κάθε κράτος μέλος θα πρέπει να διαθέτει εθνική στρατηγική ασφάλειας συστημάτων δικτύου και πληροφοριών που να καθορίζει τους στρατηγικούς στόχους και τις συγκεκριμένες δράσεις πολιτικής που πρέπει να εφαρμοστούν.

Η μεγαλύτερη μερίδα των χωρών έχει προχωρήσει ήδη σε προσπάθειες κατοχύρωσης και προστασίας των προσωπικών δεδομένων και της ιδιωτικότητας λόγω της εκτεταμένης έκθεσης των ατόμων στις νέες τεχνολογίες και τα κοινωνικά δίκτυα. Βέβαια, είναι αναμφισβήτητο και το γεγονός ότι όλο και περισσότεροι άνθρωποι έχοντας πρόσβαση στον κυβερνοχώρο παραχωρούν οικειοθελώς μέρος των προσωπικών τους δεδομένων δίχως να αντιλαμβάνονται τους κινδύνους που μπορεί αυτό να ελλοχεύουν. Η επέκταση της «έξυπνης τεχνολογίας» σε ολόένα και περισσότερες πτυχές της ανθρώπινης δραστηριότητας, από τα κινητά και τις έξυπνες συσκευές έως τα έξυπνα δίκτυα στην ενέργεια και τις μεταφορές, δημιουργούν μεν ένα ευρύ πλαίσιο δράσης αυτοματοποιημένων λειτουργιών αλλά και ταυτόχρονα ένα ευρύ πεδίο επιθέσεων και ρίσκων (breach).

Μεταφερόμενοι στα αρχεία θα πρέπει να τονιστεί εκ νέου η σημαίνουσα συμβολή τους στη διατήρηση και διαφύλαξη της μνήμης. Ωστόσο, ενώ οι υπηρεσίες αρχειοθέτησης υπάρχουν για να διατηρούν και να παρέχουν πρόσβαση σε έγγραφα και λοιπά τεκμήρια ή δραστηριότητες, την ίδια στιγμή δεν πρέπει να αποκαλύπτουν έγγραφα που περιέχουν προσωπικά δεδομένα. Τα τελευταία φάνηκε ότι αφορούν σε οποιαδήποτε πληροφορία μπορεί να ταυτοποιήσει ένα υποκείμενο συνεπώς

δημιουργούν ένα λεπτό πεδίο ισορροπίας μεταξύ προσβασιμότητας – κυρίως με ελεύθερους όρους – στα αρχεία ως φορέας και μέσο μνήμης από τη μια και διασφάλισης της ιδιωτικότητας ή/και του δικαιώματος στη λήθη από την άλλη. Έτσι, τα Αρχεία ως φορείς καλούνται να συμβιβάσουν τις απαιτήσεις της έρευνας, είτε ιστορικές είτε τεκμηριωμένες, με τα δικαιώματα και τις θεμελιώδεις ελευθερίες των υποκειμένων των δεδομένων. Η νέα τεχνολογία του διαδικτύου και των υπολογιστών εν γένει έχει δημιουργήσει νέες προοπτικές και εναλλακτικές πρόσβασης και διαχείρισης συμβάλλοντας στον εκσυγχρονισμό του έργου των Αρχείων όμως παράλληλα ενέχουν νέα επίπεδα αλλοίωσης και ρίσκου.

Σε αυτό το πλαίσιο εκσυγχρονισμού και εξέλιξη η Ευρώπη ως Ένωση αλλά και ως μεμονωμένα κράτη μέλη επιχειρεί την αναβάθμιση του νομοθετικού της πλαισίου, με κύρια χαρακτηριστικά τη συνεργασία και την ανταλλαγή των αντίστοιχων ομάδων τεχνογνωσίας ώστε να διασφαλιστεί η ισότιμη και απρόσκοπτη πρόσβαση στη συλλογική μνήμη, με όρους δημοκρατίας, διαφάνειας και ακεραιότητας. Πέραν του ρυθμιστικού ρόλου των επιμέρους νομοθετικών ρυθμίσεων και συνοδευτικών οδηγιών, όπως είναι ο Γενικός Κανονισμός περί Προστασίας Προσωπικών Δεδομένων, η Ευρώπη στοχεύει στην ισορροπία της ιδιωτικότητας και της ελεύθερης κυκλοφορίας των δεδομένων προσωπικού χαρακτήρα, δίνοντας τη σκυτάλη σε κάθε κράτος – μέλος να δημιουργήσει δικούς του φορείς που θα επιφορτιστούν με την εποπτεία της ιδιωτικότητας. Η χώρα μας διαθέτει τους απαραίτητους νόμους προστασίας βαδίζοντας στις ευρωπαϊκές οδηγίες μπορεί όμως να ενστερνιστεί κανείς την άποψη ότι πάσχει από εκτελεστικά όργανα και δομές που θα δύναται να εφαρμόσουν στην πράξη τα όσα ο νόμος υποστηρίζει.

Βιβλιογραφία - Δικτυογραφία

1. Ακριβοπούλου, Χριστίνα Μ., (2011) «Το δικαίωμα στην προστασία των προσωπικών δεδομένων μέσα από τον φακό του δικαιώματος στην ιδιωτική ζωή», στο *Θεωρία και Πράξη Διοικητικού Δικαίου*, τχ 7, Αθήνα.
2. Bottis Maria (ed.) (2012), *Privacy and Surveillance: Current aspects and future perspectives*, Αθήνα: Νομική Βιβλιοθήκη
3. Γιαννακόπουλος Γιώργος – Μπουντούρη Βασιλική (2015), *Εισαγωγή στην Αρχειονομία*, Αθήνα: ΣΕΑΒ
4. ENISA (December 2017), *Handbook on security of personal data processing*
5. European Data Protection Supervisor (21 March 2016), *Security measures for professional data processing: Article 22 of Regulation 45/2001*.
6. (2018), *Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων*.
7. Ζερβός Σπύρος, (2015), *Συντήρηση και διατήρηση χαρτιού, βιβλίων και αρχειακού υλικού*, ΣΕΑΒ, Αθήνα.
8. Ζώης Θ. Γεώργιος, (2017), «Το γενικό συμφέρον και το δημόσιο συμφέρον: Ιστορική διαδρομή και σημερινή λειτουργία της έννοιας», στο *Το Σύνταγμα: Τριμηνιαία Επιθεώρηση Ελληνικής και Ευρωπαϊκής Συνταγματικής Θεωρίας και Πράξης*, τχ.1/2017, Αθήνα: Εκδόσεις Σάκκουλα.
9. Ιγγλεζάκης Δ. Ιωάννης, (2018), *Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (Κανονισμός 2016/679. Το νέο Νομικό Πλαίσιο Προστασίας Προσωπικών Δεδομένων*, 2^η έκδοση, Θεσσαλονίκη: Andy's Publishers.
10. Ιγγλεζάκης Δ. Ιωάννης, (2003), *Ευαίσθητα Προσωπικά Δεδομένα*, Αθήνα: Σάκκουλα.
11. Κανελλοπούλου – Μπότη Μαρία, (2020), *Αρχεία και Δίκαιο: Προσωπικά δεδομένα, Πνευματική ιδιοκτησία, Πολιτιστική κληρονομιά*, Αθήνα: Νομική Βιβλιοθήκη.
12. Κολυβά Μαριάννα, (2011), *Εγχειρίδιο Αρχειονομίας: Θεωρητικές προσεγγίσεις. Οργάνωση και σκοποί. Σύγχρονες προκλήσεις*, Αθήνα: Πατάκης.
13. Μήτρου Λίλιαν, (2017), *Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων. Νέο Δίκαιο – Νέες Υποχρώσεις – Νέα Δικαιώματα*, Αθήνα: Σάκκουλα.

14. Μπάγιας Α., (1999), *Αρχειονομία: Βασικές έννοιες και αρχές. Η Οργάνωση των αρχείων για τη διοίκηση και την έρευνα*, Αθήνα: Κριτική.
15. Παναγοπούλου - Κουτναντζή Φερενίκη, (2017), *Ο Γενικός Κανονισμός για την Προστασία Δεδομένων 679/2016/ΕΕ: Εισαγωγή και Προστασία Δικαιωμάτων*, Αθήνα: Σάκκουλα.
16. Παντελιάδου - Σαατζίδου Ε., (2006), *Το παράδειγμα της νομικής ρύθμισης της ηλεκτρονικής επεξεργασίας των προσωπικών δεδομένων με έμφαση στην επεξεργασία των δεδομένων οικονομικής συμπεριφοράς*, Πανεπιστήμιο Μακεδονίας.
17. Παπαδόπουλος Θωδωρής, (χ.χ.), *Ανοιχτά δημόσια δεδομένα*, Αθήνα: Ε.Κ.Δ.Δ.Α.

Δικτυογραφία

1. Duchein Michel, “The history of European archives and the development of the archival profession in Europe”, in *The American Archivist*, vol. 55, no. 1, 1992, www.jstor.org/stable/40293621
2. Βρεττού Χριστίνα Αντ. (2017), *Η τροποποίηση της έννοιας του αρχείου δεδομένων προσωπικού χαρακτήρα με τον ν.3471/2006 και οι συνέπειες της εφαρμογής του ν.2472/1997 στα δημοσιογραφικά αρχεία*, Ένωση Ελλήνων Νομικών, <https://bit.ly/2Z7fVVB>
3. Κανονισμός (ΕΕ) 2016/679
<https://eurlex.europa.eu/legalcontent/EL/TXT/PDF/?uri=CELEX:32016R0679&from=EL>
4. Maygene F. Daniels, (1984), *Archives and records management resources*, <https://www.archives.gov/research/alic/reference/archivesresources/terminology.html>
5. Shwartz Joan M.& Cook Terry (2002), *Archives, records and power: The making of modern memory*, Archival Science
<https://link.springer.com/content/pdf/10.1007/BF02435628.pdf>
6. Τριανταφυλλίδου Βικτώρια, (2018), *Η επεξεργασία των προσωπικών δεδομένων στον χώρο των ηλεκτρονικών επικοινωνιών: Νομικές πτυχές*, Θεσσαλονίκη: ΠΑΜΑΚ, σελ., 6 [διπλωματική εργασία]

- <https://dspace.lib.uom.gr/bitstream/2159/21653/4/TriantafyllidouViktoriaMsc2018.pdf>
7. National Archives and Records Administration, (2017),
<https://www.archives.gov/files/foia/directives/nara1608.pdf>
 8. Warren and Brandeis, *The right to privacy*, Harvard Law Review, vol.IV, 1890
http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html
 9. Γενικά Αρχεία του Κράτους, Αρχαιομνήμων, <http://arxeiomnimon.gak.gr/>
 10. <https://cert.europa.eu/static/RFC2350/RFC2350.pdf>
 11. Society of American Archivists
<https://dictionary.archivists.org/entry/metadata.html>
 12. «Προστασία δεδομένων στο πλαίσιο του ΓΚΠΔ»,
https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_el.htm
 13. Νόμος, 2472/1997,
<https://www.dpa.gr/sites/default/files/201910/247297%20%28SEPT2019%29.pdf>
 14. Βουλή των Ελλήνων, <https://www.hellenicparliament.gr/Vouli-ton-Ellinon/To-Politevma/Syntagma/article-2/>
 15. Αρχή Προστασίας Δεδομένων, <https://www.dpa.gr/>
 16. Αρχή Προστασίας Δεδομένων, «Κώδικες Δεοντολογίας»,
https://www.dpa.gr/el/foreis/kwdikes_deodologias
 17. Anonymisation and Pseudonymisation”, <https://www.ucl.ac.uk/data-protection/guidance-staff-students-and-researchers/practical-data-protection-guidance-notice/anonymisation-and>
 18. “IPEN – Internet Privacy Engineering Network”, https://edps.europa.eu/data-protection/ipen-internet-privacy-engineering-network_en
 19. Enisa, “CSIRTs network”, <https://www.enisa.europa.eu/topics/csirts-in-europe/csirts-network>
 20. European Commission , “What is personal data?”,
https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en
 21. <https://www.e-nomothesia.gr/kat-dedomena-prosopikou-kharaktera/nomos-4624-2019-pherk-137a-29-8-2019.html>

22. <https://www.e-nomothesia.gr/kat-ekpaideuse/nomos-4610-2019-phek-70a-7-5-2019-2.html>
23. https://epic.org/privacy/intl/eu_data_protection_directive.html
24. “The Complete Guide to CSIRT organization: How to Build an Incident Response Team”, <https://www.exabeam.com/incident-response/csirt/>
25. <https://www.hellenicparliament.gr/Vouli-ton-Ellinon/To-Politevma/Syntagma>
26. (2016), “What are archives,”, International Council on Archives, <https://www.ica.org/en/what-archive>
27. ΥΠΕΠΘ, Νόμος Περί Γενικών Αρχείων του Κράτους, <http://www.opengov.gr/ypepth/?p=4833>
28. <https://www.legislation.gov.uk/ukpga/2018/12/section/3/enacted>
29. <http://opendefinition.org/>
30. <https://okfn.gr/what-is-open/>
31. Οικουμενική Διακήρυξη για τα Ανθρώπινα Δικαιώματα, 10 Δεκεμβρίου 1948, https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/grk.pdf
32. <https://www.ucl.ac.uk/data-protection/guidance-staff-students-and-researchers/practical-data-protection-guidance-notices/anonymisation-and>