ΠΑΝΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΟΙΝΩΝΙΚΩΝ ΚΑΙ ΠΟΛΙΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΣΧΟΛΗ ΕΠΙΣΤΗΜΩΝ ΟΙΚΟΝΟΜΙΑΣ ΚΑΙ ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ
ΤΜΗΜΑ ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ
ΠΜΣ "ΔΙΚΑΙΟ, ΤΕΧΝΟΛΟΓΙΑ ΚΑΙ ΟΙΚΟΝΟΜΙΑ"

Οι νέες ευθύνες του υπεύθυνου επεξεργασίας βάσει του Γενικού Κανονισμού Προστασίας Δεδομένων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της

ΣΤΑΜΑΤΟΠΟΥΛΟΥ ΑΝΝΑΣ του Βασιλείου (Α.Μ. 7116Μ109)

Επιβλέπουσα : Ισμήνη Κριάρη

Πρύτανης Παντείου Πανεπιστημίου

Αθήνα, Νοέμβριος 2017

Περίληψη

Το αντικείμενο της διπλωματικής εργασίας αφορά στις νέες ευθύνες του υπεύθυνου επεξεργασίας (controller of personal data) βάσει του Γενικού Κανονισμού Προστασίας Δεδομένων, ο οποίος τίθεται σε εφαρμογή από τις 25 Μαΐου 2018.

Στο πλαίσιο της εργασίας επιχειρείται μια εισαγωγή στα βασικά σημεία του Γενικού Κανονισμού Προσωπικών Δεδομένων, που ενισχύει τον ρόλο και την ευθύνη του υπεύθυνου επεξεργασίας. Εν συνεχεία ακολουθεί περιγραφή του υφιστάμενου νομικού πλαισίου σε διεθνές, ενωσιακό και εθνικό επίπεδο, εστιάζοντας στις βασικές έννοιες και δικαιώματα των υποκειμένων δεδομένων. Σκόπιμο κρίθηκε ακολούθως να επιχειρηθεί με συνοπτικό τρόπο μια προσέγγιση του ρόλου του υπεύθυνου επεξεργασίας ως έχει σήμερα στο εσωτερικό δίκαιο με το Ν.2472/1997, πριν την έναρξη εφαρμογής του Γενικού Κανονισμού, ώστε από την περαιτέρω ανάλυση να αναδειχθούν οι διαφορές του με τις νέες ευθύνες που αυτός αποκτά από το Μάιο του 2018.

Στον κυρίως κορμό της παρούσας εργασίας γίνεται μια προσπάθεια παράθεσης των βασικότερων ρυθμίσεων του νέου νομοθετικού πλαισίου του Κανονισμού για τα προσωπικά δεδομένα και ειδικότερα για τον υπεύθυνο επεξεργασίας, αφού πρώτα επιχειρείται μια αναφορά στην ιστορική ανάγκη θέσπισής του. Η μεθοδολογία που ακολουθείται είναι η κατ' άρθρο ανάλυση του αναφορικά με το ρόλο και τις νέες ευθύνες του υπεύθυνου επεξεργασίας. Συγκεκριμένα, αναλύονται οι γενικές υποχρεώσεις που έχουν οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία των δεδομένων προσωπικού χαρακτήρα για λογαριασμό αυτών. Παράλληλα, γίνεται αναφορά στα επαγγελματικά προσόντα και, ειδικότερα, την εξειδικευμένη γνώση των νόμων και πρακτικών περί προστασίας των δεδομένων και της ικανότητας εκπλήρωσης των καθηκόντων του υπεύθυνου επεξεργασίας προσωπικών δεδομένων. Έμφαση δίνεται στις περιπτώσεις στις οποίες είναι υποχρεωτικός ο διορισμός του Data Protection Officer (Σ.Σ. Θα διατηρηθεί ο αγγλικός όρος καθώς αποδίδει πληρέστερα την ουσία του συγκεκριμένου όρου) ο οποίος αναλαμβάνει αρμοδιότητες ζωτικής σημασίας.

Στη συνέχεια επιχειρείται μια προσπάθεια καταγραφής των προπαρασκευαστικών ενεργειών που απαιτείται να γίνουν από τους οργανισμούς, τόσο του δημόσιου όσο και του ιδιωτικού τομέα, προκειμένου για την εφαρμογή του Κανονισμού, όπως προαναφέρθηκε, ενόψει του Μαΐου 2018, ημερομηνία κατά την οποία κάθε υπεύθυνος επεξεργασίας των Κρατών-Μελών, θα πρέπει να ενεργεί σε συμμόρφωση με τις διατάξεις του.

Τέλος, επιχειρείται η εξαγωγή συμπερασμάτων για την ανάγκη θεσμοθέτησης του νέου Κανονισμού για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα, ο οποίος πρέπει να προορίζεται να εξυπηρετεί τον άνθρωπο, την εξέταση του τρόπου υλοποίησης στην πράξη των παραπάνω δικαιωμάτων και εν κατακλείδι τον επαυξημένο με νέες αρμοδιότητες θεσμό του υπεύθυνου επεξεργασίας προσωπικών δεδομένων μετά τη θέση σε εφαρμογή του. Μένει μόνο να επιβεβαιωθεί η προσδοκία επιτυχούς εφαρμογής των συντακτών του.

Abstract

The subject of the diploma thesis deals with the new responsibilities of the controller of personal data under the General Data Protection Regulation, which will be in effect from May 25, 2018.

In this context, an introduction to the key points of the General Data Protection Act is being attempted, which reinforces the role and responsibility of the controller of personal data. Following that, there is a description of the existing legal framework at international, EU and national level, focusing on the basic concepts and data rights subject. An approach to the role of the controller currently in effect under national law 2472/1997, before the enforcement of the General Regulation, was then considered to be a concise study, so that from the further analysis his differences can emerge with the new responsibilities he will acquire from May 2018.

The main part of this thesis is an attempt to quote the basic regulations of the new legal framework of the Act on personal data, and more specifically for the controller of personal data, after attempting a reference to the historical need for its adoption. The methodology followed is its breakdown article by article regarding the role and new responsibilities of the controller of personal data. In particular, it analyzes the general obligations of controllers of personal data and processors on their behalf. At the same time, a reference is made to professional qualifications and, in particular, special knowledge of data protection laws and practices and the professional proficiency of the controller. Emphasis is given in cases where the appointment is mandatory for the Data Protection Officer whose role is vital.

An attempt is then made to catalogue the preparatory actions required by public and private organizations to implement the Regulation, as mentioned above, looking ahead to May 2018, the date on which each Member State's the controllers of personal data, should act in accordance with its regulatory arrangements.

Lastly, it is attempted to draw conclusions about the need to establish the new Regulation on the processing of personal data, which should be intended to serve people, to examine the way in which the above rights are actually implemented and, in conclusion, the new institution which empowers the role of the controller of personal data after it's put in effect. It only remains to confirm its editors' expectation of a successful enforcement.

Κατάλογος συντομογραφιών

ΑΠΔΠΧ Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

ΕΔΔΑ Ευρωπαϊκό Δικαστήριο των Δικαιωμάτων του Ανθρώπου

ΕΣΔΑ Ευρωπαϊκή Σύμβαση για τα Δικαιώματα του Ανθρώπου

ΕΕ Ευρωπαϊκή Ένωση

ΕΕΠΔ Ευρωπαίος Επόπτης Προστασίας Δεδομένων

ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2016/679 Γενικός Κανονισμός Προστασίας Δεδομένων

ΜΜΜ Μέσα Μαζικής Μεταφοράς

ΝΠΙΔ Νομικό Πρόσωπο Ιδιωτικού Δικαίου

ΟΟΣΑ Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης

ΣΕΕ Συνθήκη για την Ευρωπαϊκή Ένωση

ΣΛΕΕ Συνθήκη για τη Λειτουργία της Ευρωπαϊκής Ένωσης

ΣΤΕ Συμβούλιο της Επικρατείας

Σύμβαση 108 Σύμβαση για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων (Συμβούλιο της Ευρώπης)

ΥΠΔ Υπεύθυνος για την Προστασία Προσωπικών Δεδομένων

Χάρτης Χάρτης Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης

ΟΟΣΑ Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης

Controller and processor of personal data Υπεύθυνος επεξεργασίας και εκτελών την επεξεργασια

DPIA Αξιολόγηση Αντικτύπου Προστασίας Προσωπικών Δεδομένων (Data Privacy Impact Assessment)

DPO Υπεύθυνος Προστασίας Προσωπικών Δεδομένων

DPWP Ομάδα Εργασίας που συστάθηκε βάσει του άρθρου 29 της οδηγίας 95/46 / ΕΚ για τα προσωπικά δεδομένα προστασίας και ιδιωτικότητας.

FRA Οργανισμός Θεμελιωδών Δικαιωμάτων της ΕΕ

GDPR Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων

IAPP Η μεγαλύτερη και πιο ολοκληρωμένη διεθνώς κοινότητα και πηγή για την προστασία της ιδιωτικής ζωής

IT (Information Technology) Πληροφορίες Τεχνολογίας

PR (Public Relations) Δημόσιες Σχέσεις

SIRENE (Supplementary Information Request at the National Entries) Αίτηση Συμπληρωματικών Πληροφοριών για Εθνικές Καταχωρίσεις

SIS Σύστημα Πληροφοριών Σένγκεν

SWIFT Εταιρία Παγκόσμιων Διατραπεζικών Χρηματοπιστωτικών Τηλεπικοινωνιών

Πίνακας Περιεχομένων

1. Εισαγωγή

Η εισαγωγή του δικαίου των προσωπικών δεδομένων στην έννομη τάξη, που ανέδειξε εντονότερα το θεσμό της λεγόμενης ιδιωτικής σφαίρας, είχε καταλυτικές επιπτώσεις στο νομικό πολιτισμό, αλλά και στην κοινωνική και οικονομική καθημερινότητα. «Η μέριμνα των τραπεζών για πιστοληπτική ικανότητα των πελατών τους, τα όρια της δημοσιογραφικής δραστηριότητας και της επιστημονικής ερευνητικής προσπάθειας σε εργαστήρια και γραφεία στατιστικών μελετών, οι κινήσεις της αστυνομίας και των ιδιωτικών γραφείων ασφαλείας, οι όροι των ασφαλιστηρίων συμβολαίων, ιδίως αναφορικά με το βάρος ενημέρωσης για τις ασθένειες ή τη γενετική προδιάθεση του ασφαλισμένου, η επιτήρηση των δημόσιων και ιδιωτικών χώρων-λ.χ. Εργασίας-, η ιδιότυπη δημοσιότητα των διαδικτυακών ιστοχώρων, ακόμη και οι επιδόσεις δικογράφων, καθώς και οι πτυχές της οικογενειακής ζωής που έχουν εξέλθει της εχεμύθειας του οίκου, προπαντός δε η τρέχουσα πολιτική επικαιρότητα, όλα αυτά επηρεάσθηκαν αποφασιστικά από τη νομοθετική πρωτοβουλία για τη ρύθμιση των πληροφοριών που μπορούν να συνδεθούν με ορισμένο πρόσωπο»[1].

Η προσωπική ζωή των πολιτών και ιδίως τα προσωπικά τους δεδομένα υπήρξαν ανέκαθεν στόχος της δημόσιας και ιδιωτικής εξουσίας, καθότι η διείσδυση σε αυτά, πέραν της ικανοποίησης της γνώσης πασών των πληροφοριών για κάποια πρόσωπα, προσφέρει μεγάλες δυνατότητες οικονομικής κυρίως εκμετάλλευσης τους από τρίτους με νόμιμα (προώθηση προϊόντων) αλλά και παράνομα μέσα (πχ εκβιασμός, απόλυση εργαζομένων)[2]. Η ανάπτυξη της τεχνολογίας αποτέλεσε καταλύτη για την αύξηση των περιπτώσεων τέτοιας παραβίασης των προσωπικών δεδομένων, καθότι από τη μία πλευρά οι κάμερες, οι φωτογραφικές μηχανές και, πλέον, τα κινητά, επιτρέπουν την αποθήκευση προσωπικών στοιχείων, από την άλλη πλευρά η πρόοδος στον τομέα

[1] Σταθόπουλος Μιχάλης, Πρόλογος στο βιβλίο, Δίκαιο προστασίας δεδομένων του καθηγητή Κ. Χρι - στοδούλου Νομική Βιβλιοθήκη 2013, σελ. VII.

[2] Βλ παραδείγματα σε Αραβαντινό Βασίλειο, Η προστασία των στοιχείων προσωπικού χαρακτήρα από την αθέμιτη επεξεργασία μέσω υπολογιστή, Σάκκουλας 1997, σελ 26.

της πληροφορικής επέτρεψε την ταχύτατη και μαζική αποθήκευση και διάδοση των στοιχείων αυτών, δημιουργώντας παράλληλα και τη δυνατότητα για "ηλεκτρονικό φακέλωμα" των πολιτών. Παράλληλα η ανάπτυξη των ιστοσελίδων κοινωνικής δικτυώσεως προσφέρει έτοιμο και δωρεάν υλικό στους τρίτους που επιθυμούν να κάνουν χρήση των δεδομένων που ο κάθε χρήστης τυχόν κοινοποιεί.

Τέλος, η εμφάνιση τηλεοπτικών μορφωμάτων όπως τα "reality shows" και οι "εκπομπές καταγγελίας" καθιέρωσε σταδιακά μια αχόρταγη διάθεση για πληροφορίες. Όπως γλαφυρότατα αναφέρει ο Γέροντας «στη σύγχρονη κοινωνία της πληροφορίας η πληροφορία είναι χρήμα και ο πόλεμος για την απόκτηση της ιερός...το δικαίωμα του ατόμου σε μια ανενόχλητη ιδιωτική ζωή, σ΄ ένα περιβάλλον απαλλαγμένο εξωτερικών ενοχλήσεων, με κατεβασμένα τα ρολά, είναι εκτεθειμένο στους πειρατές του κυβερνοχώρου, σε reality show, αυτόκλητους εξομολογητές, κράχτες του τηλεφωνικού marketing, στους ηδονοβλεψίες της καθημερινής μας ζωής, όπου το άτομο γίνεται έρμαιο της νέας ψηφιακής τεχνολογίας, της ανελέητης γραφειοκρατίας, των απανταχού πλασιέ των ιδιωτικών μας στιγμών, οι οποίου κουρνιάζουν στο προσκεφάλι μας, μηρυκάζουν το όνομα και τη διεύθυνση μας και η ζωή μετουσιώνεται σε ένα ευτελές reality show...»[3]. Ωστόσο, "είναι αδύνατο να υπάρξει δημοκρατική κοινωνία, εάν ο πολίτης δεν ξέρει ποιος, σε ποια χρονική στιγμή και για ποιο στόχο συλλέγει προσωπικά του δεδομένα· η δημοκρατική κοινωνία, δηλαδή, προϋποθέτει την εμπιστοσύνη του πολίτη, ότι δεν είναι αντικείμενο αλλά υποκείμενο και μπορεί ο ίδιος να καθορίζει τα της διάθεσης των προσωπικών του δεδομένων"[4].

Η εξέλιξη των πραγμάτων ανέδειξε την προστασία δεδομένων ως τη μοναδική νομική τροχοπέδη στις σημαντικότερες τεχνολογικές και επιχειρηματικές εξελίξεις μέχρι και σήμερα. Πράγματι, η νομοθεσία περί προστασίας δεδομένων προσωπικού χαρακτήρα επιχείρησε να θέσει περιορισμούς κυρίως στο ηλεκτρονικό εμπόριο, στο στρατηγικό marketing, στη γενετική έρευνα και στις τηλεπικοινωνίες. Οι περιορισμοί αυτοί δεν

[3] Γέροντας Απόστολος, Η προστασία του πολίτη από την ηλεκτρονική επεξεργασία προσωπικών δεδομένων, Εκδ. Σάκκουλα 2002, σελ 43-44.

[4] Αναφορά στην BVerfGE 75, σελ. 1 επ. (Volkszählungsurteil).

έγιναν σχεδόν ποτέ αποδεκτοί από την αγορά, αφού εν τέλει της στερούσαν επικερδείς δραστηριότητες. Έτσι, ενώ η αγορά συνεργάστηκε με τη νομική επιστήμη σε τομείς του δικαίου όπου ο κεντρικός έλεγχος ήταν ευπρόσδεκτος, λ.χ. στην προστασία της πνευματικής ιδιοκτησίας ή στα εγκλήματα χρήσης υπολογιστών, στην περίπτωση της προστασίας δεδομένων προσωπικού χαρακτήρα αναπτύχθηκε αναπόφευκτα μια αντιπαλότητα, η οποία βρίσκεται σήμερα σε έξαρση. Με αφορμή όμως, την αποκάλυψη γεγονότων διαφθοράς στην δημόσια ζωή του τόπου μας αλλά και διεθνώς, έχει ανοίξει μια τεράστια συζήτηση σχετικά με την δήθεν αντίθεση του ατομικού δικαιώματος της προστασίας των προσωπικών δεδομένων που απαντάται στη διάταξη του άρθρου 9^{A} του Συντάγματος και της αρχή της διαφάνειας που απαντάται στη διάταξη του άρθρου 10 παρ. 3 του Συντάγματος για την ελεύθερη και αδιακώλυτη πρόσβαση στα διοικητικά έγγραφα αλλά και στις διατάξεις των άρθρων 14 παρ. 9, 29 παρ. 2 , 102 παρ. 5 και 103 παρ. 7 Σ.

Η ανάπτυξη της «ευρωπαϊκής πολιτικής ψηφιακής οικονομίας» ως επιπλέον παράγοντας ήρθε να προστεθεί στην παραπάνω προβληματική και να καταστήσει αναγκαία την κατάργηση της Οδηγίας 95/46/ΕΚ και επιβεβλημένη την θέσπιση ενός νέου νομικού μορφώματος: «Οι εξελίξεις αυτές απαιτούν ένα ισχυρό και πιο συνεκτικό πλαίσιο προστασίας των δεδομένων στην Ένωση, υποστηριζόμενο από αυστηρή εφαρμογή της νομοθεσίας, δεδομένου ότι είναι σημαντικό να δημιουργηθεί η αναγκαία εμπιστοσύνη που θα επιτρέψει στην ψηφιακή οικονομία να αναπτυχθεί στο σύνολο της εσωτερικής αγοράς. Τα φυσικά πρόσωπα θα πρέπει να έχουν τον έλεγχο των δικών τους δεδομένων προσωπικού χαρακτήρα.Θα πρέπει να ενισχυθούν η ασφάλεια δικαίου και η πρακτική ασφάλεια για τα φυσικά πρόσωπα, τους οικονομικούς παράγοντες και τις δημόσιες αρχές»[5].

[5] Τσολιάς Γρηγόρης, Παρουσίαση με θέμα «Υποχρεώσεις συμμόρφωσης στον Γενικό Κανονισμό Προσωπικών Δεδομένων (GDPR) και ο ρόλος του Υπευθύνου Προστασίας Δεδομένων (DPO)», Δικηγόρος – ΜΔ Ποινικών Επιστημών, Μέλος (αν.) της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, διαθέσιμο στην ιστοσελίδα www.dpa.gr

Απόρροια των παραπάνω ήταν η ψήφιση στις 27 Απριλίου 2016 από το Ευρωπαικό Κοινοβούλιο του Γενικού Κανονισμού Προσωπικών Δεδομένων (Κανονισμός 2016/679), νομοθέτημα άμεσης εφαρμογής σε όλα τα κράτη μέλη της Ευρωπαικής Ενωσης[6], το οποίο θα τεθεί σε ισχύ μετά την παρέλευση της μεταβατικής περιόδου για την προσαρμογή των κρατών δηλαδή στις 25 Μαίου 2018. Το νομοθέτημα αυτό αλλάζει ριζικά το τοπίο στον χώρο της Προστασίας των Προσωπικών Δεδομένων επιβάλλοντας πρόσθετες υποχρεώσεις σε Υπεύθυνους Επεξεργασίας και Εκτελούντες την Επεξεργασία προσωπικών δεδομένων με στόχο μια πιο αποτελεσματική προστασία αυτών.

Ηδη από τον Φεβρούαριο 2016 η Επιτροπή του άρθρου 29 (Article 29 Working Party) η οποία αποτελεί την εποπτεύουσα αρχή των εθνικών Αρχών Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και Συμβουλευτικό Όργανο της Ευρωπαικής Επιτροπής[7] , ανακοίνωσε ότι θα εκδόσει διευκρινιστικές οδηγίες σχετικά με τον ρόλο και την ευθύνη του υπεύθυνου επεξεργασίας προσωπικών δεδομένων, όπως αυτή περιγράφεται στον Κανονισμό. Οι Οδηγίες αυτές εκδόθηκαν στις 16 Δεκεμβρίου 2016 αποσαφήνιζοντας αρκετά – όχι όμως όλα – τα ερωτήματα αναφορικά με τον θεσμό που αποκτά νέα βαρύτητα μετά την εισαγωγή του Κανονισμού.

Τα βασικά σημεία του Γενικού Κανονισμού Προσωπικών Δεδομένων, που ορίζουν τον ρόλο και την ευθύνη του υπεύθυνου επεξεργασίας προσωπικών δεδομένων αποτελούν αντικείμενο ανάπτυξης της παρούσας εργασίας. Σκόπιμο είναι επίσης να επιχειρηθεί και μια συνοπτική παρουσίαση του ρόλου του υπεύθυνου επεξεργασίας πριν την έναρξη εφαρμογής του, ως έχει σήμερα με το Ν.2472/1997, με αυτόν μετά την

[6] Μούσης Νίκος, Ευρωπαϊκή Ένωση: Δίκαιο, Οικονομία, Πολιτική, 13η ενημερωμένη έκδοση, Εκδόσεις Παπαζήση, Αθήνα, 2011.

[7] Αυτή η ομάδα εργασίας (DPWP 29) συστάθηκε βάσει του άρθρου 29 της οδηγίας 95/46 / ΕΚ. Είναι ένα ανεξάρτητο ευρωπαϊκό συμβουλευτικό όργανο για τα προσωπικά δεδομένα προστασίας και ιδιωτικότητας. Τα καθήκοντά της περιγράφονται στο άρθρο 30 της οδηγίας 95/46 / ΕΚ και στο άρθρο 15 της οδηγίας 2002/58 / ΕΚ.

εφαρμογή του Γενικού Κανονισμού, αφού προηγηθεί μια προσπάθεια περιγραφής των βασικών ρυθμίσεων του υφιστάμενου νομικού πλαισίου.

2. Περιγραφή υφιστάμενου νομικού πλαισίου

2.1 Γενικά

Κατ' αρχήν, αυτό που πρέπει να τονιστεί ως γενική παρατήρηση, είναι ότι η νομοθετική παραγωγή, (=οι λεγόμενες από ορισμένους “πηγές του δικαίου”), χωρίζεται σε δύο στάδια, με κομβικότατο σημείο την εισαγωγή της διάταξης του άρθρου 9Α του Συντάγματος το 2001. Να σημειωθεί ότι πριν το 2001 υπήρχε κυρίως ένα μόνο κοινό νομοθετικό κείμενο, ο Ν. 2472/1997, καθώς ο Ν.2774/1999 είναι ειδικότερος και παραπέμπει στις γενικές διατάξεις του 2472/1979, που κάλυπτε το κενό της προστασίας των προσωπικών δεδομένων, ενώ σε συνταγματικό επίπεδο η προστασία αυτή συναγόταν με συστηματική ερμηνεία πολλών συνταγματικών διατάξεων.

Παράλληλα όμως αναφορά στο δικαίωμα αυτό υπήρχε σε πολλά διεθνή κείμενα και κυρίως σε Οδηγίες της Ε.Ε., που αποτέλεσαν και τη βάση για την κατοχύρωση του δικαιώματος αυτού και στην Ελλάδα. Το γεγονός δε ότι η ειδική νομοθεσία (νόμοι, κοινοτικές διατάξεις, διεθνείς συνθήκες) προηγήθηκε της συνταγματικής εκτός από αξιοσημείωτο, αποτελεί σημαντικό στοιχείο για την ερμηνεία της διάταξης αυτής τελεολογικά και συστηματικά, ενώ παράλληλα ενδιαφέρον παρουσιάζει το ζήτημα της συμφωνίας της προϋφιστάμενης νομοθεσίας με το μεταγενέστερο άρθρο του Συντάγματος[8].

[8] Σωτηρόπουλος Βασίλειος, Η Συνταγματική προστασία των προσωπικών δεδομένων, Εκδόσεις Σάκκουλας Α.Ε., 2006.

2.2 Διεθνές και ενωσιακό δίκαιο

Πρώτα ψήγματα σε διεθνές και ευρωπαϊκό επίπεδο, μπορούμε να ανιχνεύσουμε στο Αρ. 8 της Σύμβασης της Ρώμης 4/11/1950 όπου αναφέρεται: "κάθε πρόσωπο έχει δικαίωμα να γίνεται σεβαστή η ιδιωτική οικογενειακή ζωή, κατοικία και αλληλογραφία.

Αρκετά αργότερα, το 1980 ο ΟΟΣΑ, επηρεαζόμενος από τις αρχές του υπήρχαν στο αμερικάνικο Privacy Act του 1974 εξέδωσε το Σεπτέμβριο του 1974 ένα κείμενο που αποτελεί soft law με τίτλο: "Αρχές διέπουσες την προστασία της προσωπικής σφαίρας του ανθρώπου και τις διασυνοριακές ροές προσωπικών στοιχείων" με πρόσκληση προς τις αρχές των κρατών μελών να λάβουν μέτρα για την προστασία του σκληρού πυρήνα του δικαιώματος αυτού.

Για τους περισσότερους όμως, απαρχή της καθιέρωσης του δικαιώματος αυτού, που πλέον βρίσκεται σε πλείστα ευρωπαϊκά συντάγματα[9], αποτελεί η Σύμβαση του Συμβουλίου της Ευρώπης «για την προστασία των ατόμων από την αυτόματη επεξεργασία των προσωπικών πληροφοριών», γνωστή ως Σύμβαση 108[10], η οποία υπεγράφη στο Στρασβούργο, στις 28-01-1981 και κυρώθηκε από την Ελλάδα με τον ν. 2068/1992 και κατέστη νόμος του κράτους με το άρθρο 28Σ. Πρόκειται για το πρώτο διεθνές δεσμευτικό κείμενο που θέτει τις κατευθυντήριες αρχές που πρέπει να ακολουθήσει κάθε κράτος στο ζήτημα αυτό. Περιέχει σειρά εγγυήσεων και δικαιωμάτων των ατόμων από την επεξεργασία των δεδομένων τους μόνο όμως μέσω ηλεκτρονικών υπολογιστών (αυτοματοποιημένα μέσα). Παράλληλα προβλέπεται και η ίδρυση εθνικών αρχών (η οποία στην Ελλάδα ιδρύθηκε 16 χρόνια μετά το 1996) για την εφαρμογή των διατάξεων αυτών. Ωστόσο να σημειωθεί ότι η πρόβλεψη αυτή δεν υπήρχε στο αρχικό κείμενο αλλά προστέθηκε με μεταγενέστερο πρωτόκολλο του 2001.

---

[9] Δόνος Πέτρος, Η συνταγματική κατοχύρωση του δικαιώματος προστασίας του πολίτη από την επεξεργασία των προσωπικών του δεδομένων και της αντίστοιχης ανεξάρτητης αρχής σε: Παπαδημητρίου Γεώργιο (επιμ.), Αναθεώρηση του Συντάγματος και εκσυγχρονισμός των θεσμών, 2000, 109 επ.

[10] Βλ. εδώ το πλήρες κείμενο της Σύμβασης: http://conventions.coe.int/Treaty/FR/Treties/Html/108.htm.

Εξίσου σημαντικό κείμενο αποτελεί η Συνθήκη Σένγκεν (Schengen) που υπογράφηκε στις 14 Ιουνίου 1985 στην ομώνυμη κωμόπολη, με απώτερο στόχο την κατάργηση των ελέγχων στα κοινά συνόρων χωρών-μελών τις συνθήκης, μεταφορά των ελέγχων στα εξωτερικά σύνορα και διευκόλυνση της κυκλοφορίας προσώπων και αγαθών. Το 3ο κεφάλαιο της Σύμβασης αυτής αφορά τη προστασία και την ασφάλεια των προσωπικών δεδομένων. Η συμφωνία αυτή, μαζί με τη μεταγενέστερη Σύμβαση εφαρμογής, κυρώθηκε από την Ελλάδα με τον ν. 2514/1997 και ισχύει από τις 26 Μαρτίου 2000.

Οι δύο αυτές συσχετιζόμενες συμβάσεις προβλέπουν την δημιουργία ενός αποτελεσματικού συστήματος ανταλλαγής πληροφοριών μέσω υπολογιστών με σκοπό τη διαφύλαξη της δημόσιας τάξης[11] ως αντιστάθμισμα για την έλλειψη ελέγχων στα κοινά σύνορα το οποία ονομάστηκε σύστημα Schengen (SIS). Στο σύστημα αυτό καταχωρούνται διοικητικά και αστυνομικά δεδομένα (εντάλματα, άδειες παραμονής κ.α.) των προσώπων, αντικειμένων και οχημάτων των κρατών-μελών που είναι απαραίτητα για την επίτευξη των σκοπών που προβλέπονται στα άρθρα 95-100 της Σύμβασης. Τα δεδομένα αυτά σύμφωνα με το άρθρο 102 μπορούν να χρησιμοποιηθούν μόνο για τους σκοπούς που περιγράφονται και μπορούν να αντιγραφούν μόνο για τεχνικούς σκοπούς (όχι για διοικητικούς). Εκτός από το κεντρικό σύστημα, προβλέπεται και η ύπαρξη εθνικών καθώς και μια αρμόδια εθνική αρχή που μεριμνά για τη σωστή του λειτουργία. Δημιουργείται επίσης μέσω του συστήματος SIRENE ένα δίκτυο συνεργασίας των δικαστικών και αστυνομικών μελών των κρατών-μελών. Ως αντίβαρο σε αυτήν την έντονη επεξεργασία δεδομένων στο SIS, η σύμβαση προβλέπει αυστηρότατες προϋποθέσεις συλλογής και φύλαξης των δεδομένων αυτών. Στην Ελλάδα να σημειωθεί ότι αρμόδια αρχή είναι το Υπουργείο Προστασίας του Πολίτη και η Διεύθυνση Πληροφορικής του Υπουργείου. Τέλος στο άρθρο 82 του Ν. 3386/2005 για την είσοδο, διαμονή και κοινωνική ένταξη υπηκόων τρίτων χωρών στην Ελληνική Επικράτεια προβλέπεται ότι το Υπουργείο Δημοσίας Τάξης (νυν Υπουργείο Προστασίας του Πολίτη) τηρεί κατάλογο ανεπιθύμητων αλλοδαπών.

[11] Άρθρο 92 Σύμβασης Σέγκεν.

Επίσης, στο πεδίο της Ευρωπαϊκής Ένωσης σημαντικότατες για τις περισσότερες εθνικές νομοθεσίες (και για την εγχώρια δημόσια τάξη) είναι οι οδηγίες 95/46/ΕΚ[12] και 97/66/ΕΚ[13] με στόχο της σύγκλιση και εναρμόνιση των εθνικών δικαίων των κρατών μελών ώστε να διασφαλίζεται η "πληροφοριακή αυτοδιάθεση των προσώπων" και αφετέρου η "πληροφοριακή τους ελευθερία", λαμβάνοντας υπόψη (ιδίως η δεύτερη οδηγία) την ανάπτυξη της ψηφιακής τεχνολογίας. Οι οδηγίες αυτές άσκησαν πίεση για τη εκδοσή των δύο αντίστοιχων νόμων που αναφέρθηκα παραπάνω: του Ν. 2472/1997 (νόμος για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα) και του Ν.2774/1999 (προστασία δεδομένων προσωπικού χαρακτήρα στο τηλεπικοινωνιακό τομέα) αντίστοιχα. Πιο πρόσφατα, θεσπίστηκε και ο Ν.3471/2006, ο οποίος κατήργησε τον Ν.2774/1999, κατ' εφαρμογή της οδηγίας 2002/58/ΕΚ[14] και εφαρμόζεται μόνο στις «κατά την επεξεργασία δεδομένων προσωπικού χαρακτήρα και τη διασφάλιση του απορρήτου των επικοινωνιών, στο πλαίσιο της παροχής διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών σε δημόσια δίκτυα ηλεκτρονικών επικοινωνιών» και στον οποίο καθιερώνεται και το απόρρητο αυτών.

Παράλληλα, υπάρχει κι ο Κανονισμός 45/2001 του Ευρωπαϊκού Κοινοβουλίου, στο οποίο γίνεται ξανά προσπάθεια εξισορρόπησης της ανάγκης προστασίας των δεδομένων προσωπικού χαρακτήρα και της κυκλοφορίας των πληροφοριών αυτών μέσα στην Ε.Ε. Ο Κανονισμός αυτός σχετίζεται άμεσα με το Άρθρο 16 της ΣΛΕΕ (πρώην Άρθρο 286 ΣΕΚ) στο οποίο κατοχυρώνεται η προστασία των δεδομένων και ανατίθεται στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο η θέσπιση κανόνων επί του θέματος αυτού. Τέλος, αντίστοιχη πρόβλεψη υπάρχει και στον Χάρτη Θεμελιωδών δικαιωμάτων της Ένωσης όπου στο Άρθρο 8 προβλέπεται ότι «1. Κάθε πρόσωπο έχει

---

[12] Επίσημη Εφημερίδα ΕΕ: αριθ. L 281 της 23/11/1995 σ. 0031 – 0050 http://eur-ex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:el:HTML

[13] http://eur-law.eu/EL/Odegia-97-66-EK-Europaikou-Koinobouliou-Sumbouliou-tes,322993,d .

[14] Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών (Επίσημη Εφημερίδα ΕΕ: αριθ. L 281 της 23/11/1995 σ. 0031 – 0050).

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

2.3 Η expressis verbis συνταγματική κατοχύρωση στο εθνικό δίκαιο

Με τη ριζική συνταγματική αναθεώρηση του 2001, εισήχθη ρητώς πλέον στην Ελληνική Συνταγματική έννομη τάξη το δικαίωμα της προστασίας των προσωπικών δεδομένων, στο νέο άρθρο 9Α[15]. Το ακριβές κείμενο έχεις ως εξής: "Καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων, όπως νόμος ορίζει. Η προστασία των προσωπικών δεδομένων διασφαλίζεται από ανεξάρτητη αρχή, που συγκροτείται και λειτουργεί, όπως νόμος ορίζει".

Ο αναθεωρητικός νομοθέτης του 2001 επέλεξε να αναγάγει το δικαίωμα αυτό στο επίπεδο της συνταγματικής έννομης τάξης, κατοχυρώνοντάς το ρητώς, για να επισφραγιστεί με αυτόν τον τρόπο η πορεία της ελληνικής έννομης τάξης που ξεκίνησε με την υπογραφή της Σύμβασης 108/1981 και συνεχίστηκε με την εναρμόνιση προς την κοινοτική οδηγία 95/46/ΕΚ και την ψήφιση των νόμων 2472/1997 και 2774/1999. Επίσης, η ρητή συνταγματική κατοχύρωση ήταν αναγκαία για να διασφαλιστεί η συνταγματικότητα του "μεροληπτικού" κατά κάποιους υπέρ των πολιτών νόμου 2472/1997 (παρά την πρωτοφανή στήριξη της συνταγματικότητας αυτού από το σύνολο της θεωρίας). Παράλληλα, η κατοχύρωση αυτή συνδυάστηκε με την καθιέρωση της διαπροσωπικής ενέργειας των δικαιωμάτων με το άρθρο 25 παρ.1 γ (τριτενέργεια)[16], στοιχείο απαραίτητο αν αναλογιστούμε το ότι οι παραβάσεις των προσωπικών δεδομένων γίνονται κατά κύριο λόγο από ιδιώτες. Η προστασία των δεδομένων γίνεται από κοινός, θεμελιώδης κανόνας, καθότι παρά τις αντίθετες απόψεις, είναι δύσκολο να θεωρήσουμε ότι υπάρχουν θεμελιώδεις συνταγματικές διατάξεις εκτός συντάγματος[17]. Ταυτόχρονα, θεμελιώνεται με το δεύτερο εδάφιο η συνταγματικότητα της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (εφεξής ΑΠΔΠΧ) ως ανεξάρτητης αρχής σε συνδυασμό με το άρθρο 101Α Σ. Τέλος κατά το Σωτηρόπουλο[18], με την παράλληλη θέσπιση των διατάξεων 5Α και 19 παρ. 3 στην αναθεώρηση του 2001, δημιουργείται ένα πλέγμα προστασίας των προσωπικών δεδομένων και μπορούμε πλέον να μιλήσουμε για ένα τεκμήριο ¨εν αμφιβολία υπέρ

[15] Με το Ψήφισμα της 6/4/2001 με ψήφους 277 υπέρ (σχεδόν ομοφώνως).

[16] Βλ. Χρυσόγονος Κώστας, Ατομικά και Κοινωνικά Δικαιώματα, Νομική Βιβλιοθήκη, 3η εκδ.,σελ 214.

[17] Βλ. Δημητρόπουλος Ανδρέας, Συνταγματικά δικαιώματα, Τόμος Γ΄, Εκδόσεις Σάκκουλα, Αθήνα-Θεσ/κη, 2005, σελ 169.

[18] Σωτηρόπουλος Βασίλης, ό.π., Η Συνταγματική προστασία των προσωπικών δεδομένων, Εκδόσεις Σάκκουλας Α.Ε., 2006.

της προστασίας των προσωπικών δεδομένων". Επομένως η διάταξη δεν έχει απλά "συμβολικό" χαρακτήρα, αλλά κατοχυρώνει ένα αναγκαίο και ασφαλές επίπεδο προστασίας του ατόμου.

2.4 Ο νόμος 2472/97- Βασικές Έννοιες και δικαιώματα υποκειμένου δεδομένων

Στο άρθρο 2 του Ν. 2472/97 υπάρχει ένας κατάλογος ορισμών (όπως συμβαίνει σε πολλά αντίστοιχα πρόσφατα νομοθετήματα) διαφόρων εννοιών που σχετίζονται με το δικαίωμα και που περιλαμβάνονται στο νόμο και συνακόλουθα στην συνταγματική διάταξη. Οι ορισμοί αυτοί αποτελούν δεσμευτικό δίκαιο (ius cogens) και επομένως δε μπορούν να μεταβληθούν με διαφορετική ερμηνεία της ιδιωτικής βούλησης, όμως η ΑΠΔΠΧ έχει επιφυλάξει στον εαυτό της την αρμοδιότητα να τους ερμηνεύει επισήμως, όπως έκανε και στην Οδηγία 115/2001 σχετικά με τη προστασία των προσωπικών δεδομένων στο χώρο εργασίας.

Προστατευόμενο αγαθό του δικαιώματος είναι τα **προσωπικά δεδομένα**[19] (παρόλο που στο σύνταγμα νομοθετικός ορισμός δεν υπάρχει): "Δεδομένα[20] προσωπικού χαρακτήρα, είναι κάθε πληροφορία που αναφέρεται στο υποκείμενο των δεδομένων. Στο συνταγματικό κείμενο αναφέρεται επίσης η προστασία των δεδομένων από την συλλογή, την επεξεργασία και την χρήση.

Η **συλλογή** αποτελεί στο στάδιο που προηγείται της επεξεργασία των δεδομένων και αφορά τη αναζήτηση, συγκέντρωση και λήψη των δεδομένων αυτών. Παρότι το Σύνταγμα τα διαχωρίζει, στο Νόμο φαίνεται η συλλογή να αποτελεί μέρος της επεξεργασίας. Πρόκειται κατά τον Σωτηρόπουλο[21] για πλάσμα δικαίου, που σκοπό έχει την εφαρμογή των διατάξεων της επεξεργασίας και στο στάδιο της συλλογής. Πάντως και ο ίδιος ο νόμος φαίνεται να τα διαχωρίζει, αναφερόμενος σε διάφορα σημεία σε "συλλογή ή/και επεξεργασία". Θα μπορούσαμε ίσως να μιλήσουμε για μια επεξεργασία εν ευρεία εννοία και εν στενή, όπου η πρώτη θα περιλαμβάνει την επέμβαση του δράστη της επεξεργασίας στο περιβάλλον της πληροφορίας, ενώ η δεύτερη της επέμβαση στο πυρήνα και τον περιεχόμενο αυτής. Πάντως αυτή η συζήτηση μόνο θεωρητική αξία έχει αφού ο νόμος κατά βάση προβλέπει κοινές

[19] Εναλλακτικά χρησιμοποιούνται και οι όροι "πληροφορίες" (βλ Απόφαση ΤΕΙΡΕΣΙΑΣ 11/2002),"προσωπικά δεδομένα", "ατομικά δεδομένα (βλ.Αρ.8 Ν. 3144/2003) ή προσωπικά στοιχεία.

[20] Ο όρος δεδομένα προέρχεται από το ρήμα "δίδωμι" και είναι μεταφραστικό δάνειο του αγγλικού data και η μετοχή παρακειμένου προσδίδει ακριβώς ότι πρόκειται για στοιχείο που έχει ήδη δοθεί, από πριν. Επίσης δεν είναι τυχαίος ο πληθυντικός αριθμός, ο οποίος υποδηλώνει ότι οι πληροφορίες γύρω από ένα άτομο δε μπορούν να είναι μεμονωμένες αλλά ειδομένες μόνο ως σύνολο. Απαιτούνται πάντα τουλάχιστον 2 στοιχεία: το δεδομένο αναφοράς και το δεδομένο προσδιορισμού (το πρόσωπο).

[21] Βλ. Σωτηρόπουλο Βασίλη, ο.π., σελ 16.

διατάξεις, εκτός των περιπτώσεων της διασύνδεσης αρχείων και της διασυνοριακής μεταβίβασης πληροφοριών.

Επεξεργασία ή έλεγχος της επεξεργασίας αποτελεί το δεύτερο και κυριότερο στάδιο προστασίας των δεδομένων προσωπικού χαρακτήρα. Η σημασία της προστασίας των δεδομένων από αυτή ακριβώς τη διαδικασία προκύπτει, εκτός από την αναφορά στο Σύνταγμα, από τον ίδιο τον τίτλο του Ν. 2472/97: "Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Σκοπός του νομοθέτη είναι, δίνοντας ένας γενικό και σχετικά αόριστο ορισμό, να εξασφαλίσει ένα ευρύ πεδίο προστασίας των προσωπικών δεδομένων, εντάσσοντας και ενδεχόμενες νέες μορφές που θα προκύψουν στην διαρκώς μεταβαλλόμενη και εξελισσόμενη τα οποία μπορούν να διενεργήσουν την επεξεργασία αυτή ("από το Δημόσιο ή από νομικό πρόσωπο δημοσίου δικαίου ή ιδιωτικού δικαίου ή ένωση προσώπων ή φυσικό πρόσωπο"). Τα πρόσωπα αυτά ονομάζονται στο νόμο ως "**Υπεύθυνος επεξεργασίας**", (περίπτωση ζ "οποιοσδήποτε καθορίζει τον σκοπό και τον τρόπο επεξεργασίας των δεδομένων προσωπικού χαρακτήρα, όπως φυσικό ή νομικό πρόσωπο, δημόσια αρχή ή υπηρεσία ή οποιοσδήποτε άλλος οργανισμός. Όταν ο σκοπός και ο τρόπος της επεξεργασίας καθορίζονται με διατάξεις νόμου ή κανονιστικές διατάξεις εθνικού ή κοινοτικού δικαίου, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια βάσει των οποίων γίνεται η επιλογή του καθορίζονται αντίστοιχα από το εθνικό ή το κοινοτικό δίκαιο"), ως "**Εκτελών την επεξεργασία**", (περίπτωση η, "οποιοσδήποτε επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό υπεύθυνου επεξεργασίας, όπως φυσικό ή νομικό πρόσωπο, δημόσια αρχή ή υπηρεσία ή οποιοσδήποτε άλλος οργανισμός") ή ως "Τρίτος" (περίπτωση θ, "κάθε φυσικό ή νομικό πρόσωπο, δημόσια αρχή ή υπηρεσία, ή οποιοσδήποτε άλλος οργανισμός, εκτός από το υποκείμενο των δεδομένων, τον υπεύθυνο επεξεργασίας και τα πρόσωπα που είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα, εφόσον ενεργούν υπό την άμεση εποπτεία ή για λογαριασμό του υπεύθυνου επεξεργασίας"). Πάντως και εδώ ο κατάλογος των προσώπων είναι ενδεικτικός και πραγματοποιούντες την επεξεργασία μπορεί να άλλα πρόσωπα που δε περιλαμβάνονται στη διάταξη[22].

[22] Βλ. Σωτηρόπουλο Βασίλη, ό.π.,σελ 15.

3. Αρμοδιότητες υπεύθυνου επεξεργασίας με βάση το υφιστάμενο νομικό πλαίσιο

3.1 Εισαγωγικές διαπιστώσεις

Η σημαντικότερη συνέπεια που απορρέει από την ιδιότητα του υπεύθυνου επεξεργασίας, με βάση το ισχύον νομικό πλαίσιο, είναι η νομική ευθύνη για την εκπλήρωση των υποχρεώσεων που προβλέπονται από το δίκαιο για την προστασία των δεδομένων. Ως εκ τούτου, οι εν λόγω θέσεις καταλαμβάνονται μόνον από πρόσωπα στα οποία μπορούν να καταλογιστούν ευθύνες βάσει της ισχύουσας νομοθεσίας. Στον ιδιωτικό τομέα, συνήθως πρόκειται για φυσικό ή νομικό πρόσωπο, ενώ στον δημόσιο τομέα συνήθως πρόκειται για αρχή. Άλλες οντότητες, όπως φορείς ή όργανα χωρίς νομική προσωπικότητα, μπορούν να ενεργούν ως υπεύθυνοι επεξεργασίας ή εκτελούντες την επεξεργασία μόνο στις περιπτώσεις που αυτό προβλέπεται από ειδικές νομικές διατάξεις.

Βάσει του δικαίου της ΕΕ, ως υπεύθυνος επεξεργασίας ορίζεται το πρόσωπο το οποίο «μόνο ή από κοινού με άλλους καθορίζει τους στόχους και τον τρόπο της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα». Η απόφαση του υπεύθυνου επεξεργασίας ορίζει γιατί και πώς θα γίνεται η επεξεργασία των δεδομένων. Βάσει του δικαίου του ΣτΕ, στον ορισμό του «υπεύθυνου επεξεργασίας» αναφέρεται επιπρόσθετα ότι ο υπεύθυνος επεξεργασίας αποφασίζει ποιες κατηγορίες προσωπικών δεδομένων θα αποθηκεύονται.

Η Σύμβαση 108, στον ορισμό του «υπεύθυνου επεξεργασίας», αναφέρεται σε μία ακόμη πτυχή της ιδιότητάς του η οποία απαιτείται να λαμβάνεται υπόψη. Ο ορισμός αυτός αναφέρεται στο ζήτημα των προσώπων τα οποία μπορούν σύννομα να επεξεργαστούν συγκεκριμένα δεδομένα για συγκεκριμένο σκοπό. Παρά ταύτα, όταν αναζητείται ο υπεύθυνος επεξεργασίας για να λογοδοτήσει για εικαζόμενη παράνομη επεξεργασία, υπεύθυνος επεξεργασίας θα θεωρείται το πρόσωπο ή η οντότητα, π.χ. εταιρία ή αρχή, που έλαβε την απόφαση για την επεξεργασία των δεδομένων, ασχέτως αν είχε από τον νόμο το δικαίωμα να το πράξει. Ως εκ τούτου, τα αιτήματα διαγραφής πρέπει να απευθύνονται πάντα στον «πραγματικό» υπεύθυνο επεξεργασίας.

Βάσει του δικαίου του ΣτΕ, ισχύει προαναφερόμενη ερμηνεία της έννοιας του υπευθύνου επεξεργασίας και αντίστοιχα της έννοιας του εκτελούντος την επεξεργασία, όπως φαίνεται και από τις συστάσεις που εκδόθηκαν δυνάμει της Σύμβασης 108.

Πιο συγκεκριμένα οι βασικές υποχρεώσεις του υπεύθυνου επεξεργασίας από την τήρηση προσωπικών δεδομένων συνοψίζονται στις παρακάτω:

α. Κάθε υπεύθυνος επεξεργασίας προσωπικών δεδομένων υποχρεούται να γνωστοποιήσει στην Αρχή τη σύσταση και λειτουργία αρχείου ή την έναρξη της επεξεργασίας. Σε περίπτωση τήρησης αρχείου που περιλαμβάνει ευαίσθητα προσωπικά δεδομένα, η γνωστοποίηση επέχει θέση αιτήσεως για χορήγησης άδειας επεξεργασίας ευαίσθητων δεδομένων. Στην αίτηση/ άδεια προσδιορίζεται και ο σκοπός της επεξεργασίας.

β. Σε περίπτωση επέλευσης αλλαγής σε οποιεσδήποτε από τις πληροφορίες που γνωστοποιούνται στην ΑΠΔΠΧ σχετικά με το αρχείο (π.χ. διεύθυνση τήρησης αρχείου) υποβάλλει γνωστοποίηση της τροποποίησης. Το ίδιο καλό είναι να πράττει και σε περίπτωση κατάργησης του αρχείου (αλλά δεν συνιστά εκ του νόμου επιβαλλόμενη υποχρέωση).

γ. Κατά το στάδιο της συλλογής των προσωπικών δεδομένων, ο υπεύθυνος επεξεργασίας οφείλει να **ενημερώνει** το υποκείμενο για: την ταυτότητά του, τον σκοπό επεξεργασίας, τους αποδέκτες των δεδομένων, την ύπαρξη των δικαιωμάτων του (πρόσβασης και αντίρρησης), να **παρέχει** στο υποκείμενο των προσωπικών δεδομένων, χωρίς καθυστέρηση, και κατά τρόπο εύληπτο και σαφή πληροφορίες σχετικές με τα προσωπικά του δεδομένα που υπόκεινται σε επεξεργασία, εφόσον το ζητήσει. Τέλος, ο υπεύθυνος επεξεργασίας έχει την υποχρέωση να απαντήσει εγγράφως **επί των αντιρρήσεων** μέσα σε αποκλειστική προθεσμία δεκαπέντε (15) ημερών, εφόσον το υποκείμενο, οποτεδήποτε, ζητήσει τη διόρθωση, διαγραφή, τροποποίηση ή εκφράσει οποιαδήποτε άλλη αντίρρηση στην επεξεργασία των προσωπικών του δεδομένων.

δ. Υποχρεούται σε επεξεργασία προσωπικών δεδομένων μόνο για τους σκοπούς που έχουν γνωστοποιηθεί στην ΑΠΔΠΧ και διατήρηση των δεδομένων μόνο για την χρονική διάρκεια που απαιτείται για τους σκοπούς αυτούς.

ε. Οφείλει να λαμβάνει όλα τα κατάλληλα οργανωτικά και τεχνικά μέτρα για την ασφάλεια των δεδομένων και την προστασία τους από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας.

3.2 Αξιολόγηση – κριτική του θεσμού του υπεύθυνου επεξεργασίας με βάση το υφιστάμενο νομικό πλαίσιο

Η έννοια του υπευθύνου της επεξεργασίας και η αλληλεπίδρασή της με την έννοια του εκτελούντος την επεξεργασία διαδραματίζουν κρίσιμο ρόλο στην εφαρμογή της οδηγίας 95/46/ΕΚ, καθώς καθορίζουν ποιος είναι υπεύθυνος για τη συμμόρφωση προς τους κανόνες προστασίας των δεδομένων, με ποιον τρόπο τα πρόσωπα στα οποία αναφέρονται τα δεδομένα μπορούν να ασκήσουν τα δικαιώματά τους, ποιο είναι το εφαρμοστέο εθνικό δίκαιο και πώς μπορούν να λειτουργήσουν αποτελεσματικά οι αρχές προστασίας δεδομένων. Η έννοια του υπευθύνου της επεξεργασίας είναι αυτόνομη, υπό την έννοια ότι πρέπει να ερμηνεύεται κυρίως σύμφωνα με το κοινοτικό δίκαιο για την προστασία των δεδομένων, και λειτουργική, υπό την έννοια ότι προορίζεται να κατανείμει αρμοδιότητες εκεί όπου βρίσκεται η πραγματολογική επιρροή και, επομένως, βασίζεται μάλλον σε πραγματολογική παρά σε τυπική ανάλυση. Ο ορισμός της οδηγίας περιέχει τρία κύρια συστατικά μέρη: την προσωπική πτυχή («*το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή οποιοσδήποτε άλλος φορέας*»)· το ενδεχόμενο πολλαπλού ελέγχου («*που μόνος ή από κοινού με άλλους*»)· και τα βασικά στοιχεία για τη διάκριση του υπευθύνου της επεξεργασίας από άλλους παράγοντες («*καθορίζει τους στόχους και τον τρόπο της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα*»). Η ανάλυση των ως άνω συστατικών μερών οδηγεί στα ακόλουθα κύρια συμπεράσματα:

α. Η ικανότητα να «*καθορίζει* τους στόχους και τον τρόπο....» μπορεί να πηγάζει από διάφορες νομικές ή/και πραγματικές περιστάσεις: μια ρητή νομική αρμοδιότητα, όταν ο νόμος διορίζει τον υπεύθυνο της επεξεργασίας ή απονέμει ένα καθήκον ή μια υποχρέωση συλλογής και επεξεργασίας ορισμένων δεδομένων· διατάξεις του κοινού δικαίου ή υφιστάμενοι παραδοσιακοί ρόλοι οι οποίοι συνεπάγονται κατά κανόνα ορισμένη ευθύνη εντός ορισμένων οργανισμών (για παράδειγμα, ο εργοδότης σε σχέση με τα δεδομένα των υπαλλήλων του)· πραγματικές περιστάσεις και άλλα στοιχεία (όπως συμβατικές σχέσεις, πραγματικός έλεγχος από ένα μέρος, προβολή έναντι των προσώπων στα οποία αναφέρονται τα δεδομένα κ.λπ.). Εάν δεν εφαρμόζεται καμία από τις κατηγορίες αυτές, ο διορισμός ενός υπευθύνου της επεξεργασίας πρέπει να θεωρείται «άκυρος». Πράγματι, ένας φορέας ο οποίος δεν διαθέτει ούτε νομική ούτε πραγματολογική επιρροή καθορισμού του τρόπου επεξεργασίας δεδομένων προσωπικού χαρακτήρα δεν μπορεί να θεωρηθεί υπεύθυνος της επεξεργασίας. Ο καθορισμός του «στόχου» της επεξεργασίας συνεπάγεται τον χαρακτηρισμό του (*de facto*) υπευθύνου της επεξεργασίας. Αντίθετα, ο καθορισμός του «τρόπου» της επεξεργασίας μπορεί να μεταβιβασθεί από τον υπεύθυνο της επεξεργασίας, όσον αφορά τεχνικά ή οργανωτικά ζητήματα. Ωστόσο,

ουσιαστικά ζητήματα τα οποία είναι σημαντικά για την αξιολόγηση της νομιμότητας της επεξεργασίας –όπως τα δεδομένα που πρόκειται να υποβληθούν σε επεξεργασία, η διάρκεια της αποθήκευσης, η πρόσβαση κ.λπ.– πρέπει να καθορίζονται από τον υπεύθυνο της επεξεργασίας.

β. Η *προσωπική* πτυχή του ορισμού παραπέμπει σε ευρύ φάσμα υποκειμένων, τα οποία μπορούν να διαδραματίσουν τον ρόλο του υπευθύνου της επεξεργασίας. Ωστόσο, στη στρατηγική οπτική της κατανομής αρμοδιοτήτων, είναι προτιμότερο να θεωρείται υπεύθυνος της επεξεργασίας η εταιρεία ή ο φορέας παρά ένα συγκεκριμένο πρόσωπο εντός της εταιρείας ή του φορέα. Η εταιρεία ή ο φορέας θα θεωρηθούν τελικά υπεύθυνοι για την επεξεργασία των δεδομένων και τις υποχρεώσεις που απορρέουν από τη νομοθεσία για την προστασία των δεδομένων, εκτός εάν υπάρχουν σαφή στοιχεία που υποδεικνύουν ότι υπεύθυνο είναι ένα φυσικό πρόσωπο, για παράδειγμα όταν ένα φυσικό πρόσωπο το οποίο εργάζεται σε μια εταιρεία ή έναν δημόσιο φορέα χρησιμοποιεί δεδομένα για δικούς του στόχους, εκτός των δραστηριοτήτων της εταιρείας.

γ. Το ενδεχόμενο *πολλαπλού* ελέγχου λαμβάνει υπόψη τον αυξανόμενο αριθμό περιπτώσεων στις οποίες διαφορετικά μέρη ενεργούν ως υπεύθυνοι της επεξεργασίας. Η αξιολόγηση του κοινού αυτού ελέγχου πρέπει να αντικατοπτρίζει την αξιολόγηση του «ενιαίου» ελέγχου υιοθετώντας μια ουσιαστική και λειτουργική προσέγγιση, επικεντρωμένη στο κατά πόσον οι στόχοι και τα ουσιώδη στοιχεία του τρόπου καθορίζονται από περισσότερα του ενός μέρη. Η συμμετοχή των μερών στον καθορισμό των στόχων και του τρόπου επεξεργασίας στο πλαίσιο του κοινού ελέγχου μπορεί να προσλάβει διάφορες μορφές και δεν είναι υποχρεωτικό να είναι επιμερισμένη εξίσου. Στην παρούσα γνώμη παρέχονται πολλά παραδείγματα διάφορων ειδών και βαθμών κοινού ελέγχου. Διαφορετικοί βαθμοί ελέγχου μπορεί να συνεπάγονται διαφορετικούς βαθμούς αρμοδιότητας και ευθύνης, και, βεβαίως, δεν μπορεί να θεωρηθεί ότι υπάρχει «αλληλέγγυος και εις ολόκληρον» ευθύνη σε όλες τις περιπτώσεις. Επιπλέον, είναι πολύ πιθανό σε πολύπλοκα συστήματα με πολλαπλούς εμπλεκόμενους φορείς, η πρόσβαση στα δεδομένα προσωπικού χαρακτήρα και η άσκηση των δικαιωμάτων άλλων προσώπων στα οποία αναφέρονται τα δεδομένα να μπορεί να διασφαλισθεί επίσης σε διαφορετικά επίπεδα από διαφορετικούς φορείς.

Η ύπαρξη του εκτελούντος την επεξεργασία εξαρτάται από απόφαση που λαμβάνει ο υπεύθυνος της επεξεργασίας, ο οποίος μπορεί να αποφασίσει είτε να επεξεργάζεται τα δεδομένα εντός του οργανισμού του είτε να μεταβιβάσει το σύνολο ή μέρος των δραστηριοτήτων επεξεργασίας σε εξωτερικό οργανισμό. Επομένως, δύο βασικές προϋποθέσεις για τον χαρακτηρισμό κάποιου ως εκτελούντος την επεξεργασία είναι αφενός να πρόκειται για χωριστή νομική οντότητα σε σχέση με τον υπεύθυνο της

επεξεργασίας και, αφετέρου, να επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας. Η δραστηριότητα επεξεργασίας μπορεί να περιορίζεται σε ένα πολύ συγκεκριμένο καθήκον ή πλαίσιο, ή μπορεί να περιλαμβάνει κάποιον βαθμό διακριτικής ευχέρειας όσον αφορά την εξυπηρέτηση των συμφερόντων του υπευθύνου της επεξεργασίας, επιτρέποντας στον εκτελούντα την επεξεργασία να επιλέξει τα καταλληλότερα τεχνικά και οργανωτικά μέσα. Επιπλέον, ο ρόλος του εκτελούντος την επεξεργασία δεν απορρέει από τη φύση ενός παράγοντα που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα, αλλά από τις συγκεκριμένες δραστηριότητές του σε ένα συγκεκριμένο πλαίσιο και σε σχέση με συγκεκριμένα σύνολα δεδομένων ή εργασιών. Ορισμένα κριτήρια μπορεί να είναι χρήσιμα για τον καθορισμό του χαρακτηρισμού των διάφορων παραγόντων που συμμετέχουν στην επεξεργασία: το επίπεδο των προηγούμενων εντολών από τον υπεύθυνο της επεξεργασίας· η παρακολούθηση από τον υπεύθυνο της επεξεργασίας του επιπέδου της υπηρεσίας· η προβολή απέναντι στα πρόσωπα στα οποία αναφέρονται τα δεδομένα· η εμπειρογνωμοσύνη των μερών· η εξουσία αυτόνομης λήψης αποφάσεων που διαθέτουν τα διάφορα μέρη.

Η εναπομένουσα κατηγορία των «τρίτων» ορίζεται ως οποιοσδήποτε παράγοντας ο οποίος δεν διαθέτει ειδική νομιμοποίηση ή εξουσιοδότηση –η οποία θα μπορούσε να απορρέει, για παράδειγμα, από τον ρόλο του ως υπευθύνου της επεξεργασίας, εκτελούντος την επεξεργασία ή υπαλλήλου αυτών– για την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Από τα παραπάνω εμφαίνονται οι δυσκολίες στην εφαρμογή των ορισμών της οδηγίας σε ένα πολύπλοκο περιβάλλον, όπου μπορεί να προβλεφθούν πολλά σενάρια με υπευθύνους της επεξεργασίας και εκτελούντες την επεξεργασία, μόνοι ή από κοινού με άλλους, με διαφορετικούς βαθμούς αυτονομίας και αρμοδιότητας. Αδήριτη προβάλλει η αναγκαιότητα κατανομής των αρμοδιοτήτων κατά τρόπο ώστε να διασφαλίζεται επαρκώς στην πράξη η συμμόρφωση προς τους κανόνες προστασίας των δεδομένων.

Από την άνωθεν παράθεση των υποχρεώσεων του υπεύθυνου επεξεργασίας προσωπικών δεδομένων, με βάση το ισχύον νομικό πλαίσιο, συγκριτικά με τα όσα θα αναπτυχθούν παρακάτω για τις ευθύνες και υποχρεώσεις του με βάση το Γενικό Κανονισμό, διαπιστώνεται ότι οι αρμοδιότητές του είναι περιορισμένες, όπως και το ίδιο το κείμενο της οδηγίας 95/46/ΕΚ, η παρέμβαση του είναι στις πλείστες των περιπτώσεων κατασταλτική, ενώ η επιλογή ύπαρξης εκτελούντος την εργασία ανήκει στην αποκλειστική κρίση του, χωρίς σαφώς καθορισμένες προϋποθέσεις από το Ν. 2472/1997. Επιπλέον, η υποχρέωση λογοδοσίας του εξαντλείται στην αναφορά του άρθρου 23 περί αστικής ευθύνης του για παράνομη επεξεργασία προσωπικών

δεδομένων. Στο παραπάνω άρθρο, προβλέπεται η δυνατότητα αποζημίωσης για περιουσιακή ζημία και χρηματική ικανοποίηση ηθικής βλάβης υποκειμένου δεδομένων προσωπικού χαρακτήρα [23] . Πρόκειται για τη δημιουργία ενός ειδικού αστικού αδικήματος, το οποίο όμως δεν φαίνεται να έχει απασχολήσει ευρέως την ελληνική σχετική βιβλιογραφία και νομολογία. Παρ' όλα αυτά, το ειδικό αυτό αστικό αδίκημα παρουσιάζει ιδιαίτερο ενδιαφέρον καταρχήν θεωρητικό, αλλά και πρακτικό, καθώς μπορεί να θεμελιώσει ευθύνη προς αποζημίωση περιουσιακής ζημίας, αλλά και τυχόν χρηματική ικανοποίηση ηθικής βλάβης η οποία μάλιστα ορίζεται τουλάχιστον στο ποσό των 5.860,40 ευρώ. Είναι βέβαιο ότι η αστική ευθύνη λόγω παράνομης επεξεργασίας προσωπικών δεδομένων παρουσιάζει σημαντικό ενδιαφέρον, παρότι εξ αρχής, ίσως φαίνεται ο Ν 2472/1997 δύσκολος στην κατανόησή του και ξένος, μέσα στο αστικό δίκαιο τουλάχιστον, ως προς την ορολογία του. Από την άλλη μεριά, ο νόμος, όπως επιχειρήθηκε να αποδειχθεί, καλύπτει ένα πολύ μεγάλο φάσμα περιπτώσεων ευθύνης, καθώς είναι πολλές και πολύ διαφορετικές μεταξύ τους οι συμπεριφορές που μπορεί να θεωρηθεί ότι εντάσσονται στο πραγματικό των κανόνων του.

Η οργανωτική διαφοροποίηση στον δημόσιο και στον ιδιωτικό τομέα, καθώς και η παγκοσμιοποίηση της επεξεργασίας δεδομένων αυξάνουν την πολυπλοκότητα του τρόπου επεξεργασίας των δεδομένων προσωπικού χαρακτήρα, γι΄ αυτό και οδήγησαν σε ριζικές αλλαγές και την υιοθέτηση ενός νέου νομικού πλαισίου, προκειμένου να διασφαλίζεται αποτελεσματική εφαρμογή και συμμόρφωση στην πράξη, το οποίο αναλύεται στην επόμενη ενότητα της παρούσας εργασίας.

[23] Απόφαση 4244/2016 του Διοικητικού Πρωτοδικείου Αθηνών.

4. Νέος Ευρωπαϊκός Γενικός Κανονισμός για τα Προσωπικά Δεδομένα

Όπως αναφέρθηκε εισαγωγικά στις 14 Απριλίου 2016 το Ευρωπαϊκό Κοινοβούλιο ενέκρινε το Γενικό Κανονισμό για τα Προσωπικά δεδομένα (ΕΕ 2016/679/General Data Protection Regulation)[24]. Ο νέος Γενικός Κανονισμός Προστασίας Δεδομένων της ΕΕ αποτελεί τη μεγαλύτερη αλλαγή στην νομοθεσία περί προστασίας των δεδομένων τα τελευταία σχεδόν 20 χρόνια. Ο κανονισμός αυτός καταργεί την οδηγία 95/46/ΕΚ που ισχύει μέχρι σήμερα, βάσει της οποίας έχει προκύψει ο Νόμος 2472/1997 του Ελληνικού κράτους, η ανομοιόμορφη μεταφορά της οποίας στα κράτη μέλη της ΕΕ και εφαρμογή της είχε ως αποτέλεσμα τον κατακερματισμό της εφαρμογής των κανόνων προστασίας των δεδομένων, την ανασφάλεια δικαίου και την αντίληψη ότι δεν υπάρχει ουσιαστική προστασία, ιδιαίτερα στο ψηφιακό περιβάλλον. Αναμένεται να τεθεί σε ισχύ την άνοιξη του 2016 και θα αρχίσει να εφαρμόζεται την άνοιξη του 2018. Ο Κανονισμός απέκτησε τυπική ισχύ 20 ημέρες μετά την δημοσίευσή του στην Επίσημη Εφημερίδα της ΕΕ και θα ισχύει στα κράτη μέλη 2 χρόνια μετά, δηλαδή το 2018[25]. Καταργεί επίσης την Οδηγία 95/46 που ήταν εδώ και 20 χρόνια το βασικό νομοθέτημα για την προστασία προσωπικών δεδομένων σε επίπεδο Ευρωπαϊκών Κοινοτήτων.

Παράλληλα, δημοσιεύθηκαν στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης δύο ακόμα σημαντικές νομοθετικές πράξεις, οι οποίες στην ουσία αλλάζουν σταδιακά αλλά και ριζικά το νομικό καθεστώς προστασίας δεδομένων προσωπικού χαρακτήρα στην Ευρωπαϊκή Ένωση, η Οδηγία 2016/680 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και η Οδηγία 2016/681 σχετικά με τη χρήση των δεδομένων που περιέχονται στις καταστάσεις ονομάτων επιβατών για την πρόληψη, ανίχνευση, διερεύνηση και δίωξη τρομοκρατικών και σοβαρών εγκλημάτων. Η τελευταία Οδηγία αντικαθιστώντας την σχετική Απόφαση - Πλαίσιο του 2008, πρέπει να εισαχθεί στα κράτη μέλη με την εθνική νομοθεσία, δύο χρόνια μετά την δημοσίευση της στην Επίσημη Εφημερίδα. Για την Ελλάδα, η συγκεκριμένη Οδηγία παίζει σημαντικό ρόλο, καθώς ο ισχύων Ν.2472/1997, όπως τροποποιήθηκε το 2008, εξαιρεί από την προστασία προσωπικών

[24] Επίσημη ιστοσελίδα του GDPR www.eugdpr.org, όπου και το πρωτότυπο κείμενό του.

[25] Άρθρο 99 του GDPR.

δεδομένων τις δικαστικές - εισαγγελικές αρχές και τις αστυνομικές και άλλες αντίστοιχες υπηρεσίες. Έτσι, με την Οδηγία, η ελληνική νομοθεσία θα πρέπει να επαναφέρει την εφαρμογή της προστασίας προσωπικών δεδομένων και στις αστυνομικές και εισαγγελικές υπηρεσίες.

4.1 Λόγοι που οδήγησαν στην ανάγκη δημιουργίας νέου νομοθετικού πλαισίου για τα προσωπικά δεδομένα

Όπως είχε επισημανθεί εδώ και καιρό, το νέο αυτό πλαίσιο σχηματίστηκε έπειτα από διαβουλεύσεις ετών, με έντονο lobbying από τα εμπλεκόμενα μέρη, αλλά και σημαντικές επιρροές από τις τρομοκρατικές επιθέσεις στο Παρίσι και τις Βρυξέλλες. Καθώς το μοντέλο παραγωγής μεταβάλλεται και οι κοινωνικές δομές και σχέσεις τίθενται εν αμφιβόλω, η τεχνονομική και οικονομική προσαρμογή στη ψηφιακή πραγματικότητα και στις υψηλές τεχνολογίες, σε συνδυασμό με την καλλιέργεια αντίστοιχης κουλτούρας, καθίσταται επιβεβλημένη. Έχοντας διανύσει πολύ δρόμο, σήμερα βρισκόμαστε ήδη στο Web 3.0 και το σημασιολογικό ιστό, όπου πλέον ενεργό ρόλο στην ανταλλαγή, επεξεργασία και επανανοηματοδότηση της πληροφορίας αποκτούν οι ίδιες οι μηχανές.

Στο σύγχρονο αυτό οικοσύστημα, κινητήριος δύναμη αποτελούν τα ψηφιακά δεδομένα. Τα ψηφιακά δεδομένα ισοδυναμούν με πρωτογενή και ακατέργαστη πληροφορία, η οποία είναι δεκτική ανάγνωσης, κατανόησης και επεξεργασίας από τις μηχανές. Και καθώς οι μηχανές αποκτούν ολοένα και πιο ενεργό ρόλο στις δράσεις της καθημερινότητας, προκύπτει ότι κάθε πράξη της σύγχρονης καθημερινότητας προϋποθέτει συλλογή, αποθήκευση, επεξεργασία και ανταλλαγή δεδομένων. Πίσω ωστόσο από το κάθε δεδομένο που δημιουργείται, βρίσκονται άτομα. Τα ασύλληπτα σε όγκο, ταχύτητα και ποικιλία σύνολα δεδομένων, τα οποία παράγονται κάθε δευτερόλεπτο που περνά, εμπεριέχουν άτομα. Η ταξινόμηση της πραγματικότητας σε σύνολα δεδομένων εμπεριέχει άτομα. Η αποτελεσματικότερη δυνατή προάσπιση επομένως της προστασίας των προσωπικών δεδομένων και της ιδιωτικότητας των ατόμων, είναι βασικό ζητούμενο και πρόκληση στη σύγχρονη πραγματικότητα των εφαρμογών, των έξυπνων συσκευών, των αισθητήρων και κάθε λογής τεχνολογίας που επικοινωνεί με το διαδίκτυο και απομακρυσμένους υπολογιστές.

Αυτήν την πρόκληση φιλοδοξεί στην Ευρώπη να αντιμετωπίσει ο ιδιαίτερα μακροσκελής Γενικός Κανονισμός Προστασίας Δεδομένων θέτοντας κατάλληλους μηχανισμούς προληπτικής προστασίας των προσωπικών δεδομένων όλων των ευρωπαίων πολιτών. Αποτέλεσμα μίας μακράς και έντονης διαβούλευσης[26], ο

[26] Βλέπε ενδεικτικά Proposal for GPDR EL, Βρυξέλλες25.1.2012, Πρόταση «ΚΑΝΟΝΙΣΜΟΣ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ»για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών (γενικός κανονισμός για την προστασία δεδομένων), COM (2012) 9 τελικό.

Κανονισμός, έρχεται με πλήρη και δεσμευτική ισχύ για όλα τα Κράτη-Μέλη, να δώσει κατευθυντήριες οδηγίες με αναλυτικό τρόπο για τον τρόπο με τον οποίο οι οργανισμοί συλλέγουν, αποθηκεύουν, χαρακτηρίζουν και ταξινομούν τα δεδομένα, καθώς επίσης και για τον τρόπο, με τον οποίο οι οργανισμοί προστατεύουν τα προσωπικά δεδομένα και διασφαλίζουν τα θεμελιώδη δικαιώματα των φυσικών προσώπων κατά την επεξεργασία των δεδομένων τους. Προς ενίσχυση των παραπάνω, ο Κανονισμός θέτει πολύ ψηλά στην ατζέντα την υποχρέωση λογοδοσίας των οργανισμών απέναντι, τόσο στα φυσικά πρόσωπα των οποίων τα δεδομένα επεξεργάζονται, όσο και στις αρμόδιες

ανεξάρτητες αρχές, με σκοπό την:

α. οικονομική και κοινωνική πρόοδο

β. ενίσχυση και σύγκλιση των οικονομιών εντός της εσωτερικής αγοράς

γ. ευημερία των φυσικών προσώπων

δ. καλλιέργεια αισθήματος εμπιστοσύνης που θα συμβάλει στην ανάπτυξη της ψηφιακής οικονομίας και

ε. άρση των εμποδίων που στρεβλώνουν τον υγιή ανταγωνισμό.

Σε έναν κόσμο που τρέφεται από τα δεδομένα, η συμμόρφωση με τον Κανονισμό είναι η μία όψη του νομίσματος. Η άλλη αφορά στη σωστή ανάγνωση των δεδομένων, έτσι ώστε να αναδείξει τις ευκαιρίες που υποκρύπτονται στην εκάστοτε αγορά (επιχειρηματική, ερευνητική, κοινωνική, πολιτική, ανθρωπολογική κοκ) σε συνδυασμό με τα δεδομένα που βρίσκονται διαθέσιμα ως ανοιχτά. Σε αυτές τις αγορές τα προσωπικά δεδομένα αποτελούν συναλλακτικό αγαθό. Προκειμένου λοιπόν η ανάγνωση των δεδομένων να είναι ουσιαστική και να μην ικανοποιεί απλώς το γράμμα του Κανονισμού, απαιτείται μία βαθιά κατανόηση του τρόπου που η τεχνολογία, η κοινωνία και φυσικά η αγορά συνδέονται και αλληλεπιδρούν. Απαιτείται ο εντοπισμός του μοναδικού σημείου που όλα αυτά συναντώνται. Ο Υπεύθυνος Επεξεργασίας με νέο ενισχυμένο ρόλο έρχεται να βοηθήσει τους οργανισμούς να ανακαλύψουν το δικό τους «μοναδικό σημείο βρασμού»[27] και να συντελέσει από την πλευρά του στην ικανοποίηση όλων των παραπάνω στόχων, με σκοπό να βελτιωθούν τα κακώς κείμενα του παρελθόντος.

[27]Βλ. Νούσια Αλέξανδρο, Άρθρο «Καλώς ήρθατε στο Web 3.0.! Ο Γενικός Κανονισμός Προστασίας Δεδομένων και ο Ρόλος του Υπευθύνου Επεξεργασίας Δεδομένων»,25 Ιανουαρίου 2017 στην ιστοσελίδα www.opendata. ellak.gr

4.2 Περιγραφή νέου νομικού πλαισίου

Το νέο πλαίσιο προστασίας προσωπικών δεδομένων, όπως προαναφέρθηκε, συνδιαμορφώνεται από έναν κανονισμό και δύο νέες οδηγίες, ενώ επίκειται και η τροποποίηση μίας ακόμη οδηγίας, σχετικά με την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες.

Να σημειωθεί ότι οι κανονισμοί είναι δεσμευτικές νομοθετικές πράξεις και η εφαρμογή τους σε όλες τις χώρες της ΕΕ είναι υποχρεωτική[28]. Από την άλλη, οι οδηγίες ορίζουν έναν στόχο τον οποίο πρέπει να επιτύχουν όλες οι χώρες της ΕΕ, ωστόσο, εναπόκειται σε κάθε χώρα να θεσπίσει τους δικούς της νόμους για την επίτευξη των στόχων αυτών.

Ο Κανονισμός, που τέθηκε σε ισχύ την άνοιξη του 2016 και θα αρχίσει να εφαρμόζεται την άνοιξη του 2018, περιγράφει τα δικαιώματα του υποκειμένου των δεδομένων, δηλαδή του ατόμου του οποίου τα προσωπικά δεδομένα υποβάλλονται σε επεξεργασία. Αποτελεί προϊόν χρονοβόρων διαδικασιών, και ισχυρών πιέσεων, οι οποίες διήρκησαν περισσότερο από τέσσερα χρόνια. Ο Κανονισμός αυτός αντικαθιστά την ισχύουσα οδηγία για την προστασία των δεδομένων, η οποία δεν ανταποκρινόταν επαρκώς στις ανάγκες μίας εποχής με smartphones, social media, internet banking.

Στόχος των συντακτών του Κανονισμού ήταν να διαμορφωθεί με τρόπο που θα ανταποκρίνεται στις σύγχρονες ανάγκες των πολιτών με ενιαίο τρόπο (τουλάχιστον τους πολίτες και τις επιχειρήσεις εντός ΕΕ). Οι νέος γενικός κανονισμός αποτελείται από 99 άρθρα και έχει κωδικοποιηθεί πλήρως από τη συντακτική ομάδα του Lawspot[29].

Στο άρθρο 1 περιγράφεται το αντικείμενο του που είναι να “θεσπίζει κανόνες που αφορούν την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και κανόνες που αφορούν την ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα και προστατεύει θεμελιώδη δικαιώματα και ελευθερίες των φυσικών προσώπων και ειδικότερα το δικαίωμά τους στην προστασία των δεδομένων προσωπικού χαρακτήρα. Η ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα εντός της Ένωσης δεν περιορίζεται ούτε απαγορεύεται για λόγους που σχετίζονται με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα”. Με βάση το άρθρο 2

[28]Βλ. ό.π., Μούσης Νίκος, Ευρωπαϊκή Ένωση: Δίκαιο, Οικονομία, Πολιτική, 13η ενημερωμένη έκδοση, Εκδόσεις Παπαζήση, Αθήνα, 2011.

[29] https://www.lawspot.gr

ουσιαστικό πεδίο εφαρμογής του αποτελεί, εν όλω ή εν μέρει, αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα, καθώς και στη μη αυτοματοποιημένη επεξεργασία τέτοιων δεδομένων τα οποία περιλαμβάνονται ή πρόκειται να περιληφθούν σε σύστημα αρχειοθέτησης.

Ο Κανονισμός δεν τυγχάνει εφαρμογής στην επεξεργασία δεδομένων προσωπικού χαρακτήρα:

α. στο πλαίσιο δραστηριότητας η οποία δεν εμπίπτει στο πεδίο εφαρμογής του δικαίου της Ένωσης,

β. από τα κράτη μέλη κατά την άσκηση δραστηριοτήτων που εμπίπτουν στο πεδίο εφαρμογής του κεφαλαίου 2 του τίτλου V της ΣΕΕ[30],

γ. από φυσικό πρόσωπο στο πλαίσιο αποκλειστικά προσωπικής ή οικιακής δραστηριότητας,

δ. από αρμόδιες αρχές για τους σκοπούς της πρόληψης, της διερεύνησης, της ανίχνευσης ή της δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων, συμπεριλαμβανομένης της προστασίας και πρόληψης έναντι κινδύνων που απειλούν τη δημόσια ασφάλεια.

Για την επεξεργασία δεδομένων προσωπικού χαρακτήρα από τα θεσμικά όργανα, φορείς, υπηρεσίες και οργανισμούς της Ένωσης, εφαρμόζεται ο κανονισμός ΕΚ 45/2001. Ο κανονισμός ΕΚ 45/2001 και άλλες νομικές πράξεις της Ένωσης εφαρμοστέες σε μια τέτοια επεξεργασία δεδομένων προσωπικού χαρακτήρα προσαρμόζονται στις αρχές και τους κανόνες του Κανονισμού σύμφωνα με το άρθρο 98.

Σύμφωνα με το άρθρο 3 το πεδίο εφαρμογής του Κανονισμού είναι «η επεξεργασία δεδομένων προσωπικού χαρακτήρα στο πλαίσιο των δραστηριοτήτων μιας εγκατάστασης ενός υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία στην Ένωση, ανεξάρτητα από το κατά πόσο η επεξεργασία πραγματοποιείται εντός της Ένωσης».

[30] Διατάξεις σχετικές με μια κοινή εξωτερική πολιτική και πολιτική ασφαλείας.

Είναι δυνατόν να εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα υποκειμένων των δεδομένων που βρίσκονται στην Ένωση από υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία μη εγκατεστημένο στην Ένωση, εάν οι δραστηριότητες επεξεργασίας σχετίζονται με:

α. την προσφορά αγαθών ή υπηρεσιών στα εν λόγω υποκείμενα των δεδομένων στην Ένωση, ανεξαρτήτως εάν απαιτείται πληρωμή από τα υποκείμενα των δεδομένων,

β. ή την παρακολούθηση της συμπεριφοράς τους, στον βαθμό που η συμπεριφορά αυτή λαμβάνει χώρα εντός της Ένωσης.

Επίσης, καινοτομία του Κανονισμού είναι ότι εφαρμόζεται για την επεξεργασία δεδομένων προσωπικού χαρακτήρα και από υπεύθυνο επεξεργασίας μη εγκατεστημένο στην Ένωση, αλλά σε τόπο όπου εφαρμόζεται το δίκαιο κράτους μέλους δυνάμει του δημόσιου διεθνούς δικαίου. Έχει εφαρμογή σε όλους τους φορείς (ιδιωτικές και δημόσιες επιχειρήσεις, κρατικές αρχές, συλλόγους, κλπ.) που διαχειρίζονται, επεξεργάζονται, αποθηκεύουν και διακινούν δεδομένα προσωπικού χαρακτήρα, είτε έχουν έδρα και δραστηριότητα σε χώρα της Ευρωπαϊκής Ένωσης είτε όχι, εφόσον τα δεδομένα αφορούν Ευρωπαίους πολίτες ή σχετίζονται με οποιουδήποτε είδους υπηρεσίες και αγαθά προς Ευρωπαίους πολίτες. Στην πραγματικότητα, υιοθετείται «η αρχή του τόπου εγκατάστασης της επιχείρησης, αλλά και του υποκειμένου των δεδομένων»[31], ενώ επιδιώκεται παράλληλα και η τήρηση της ομοιομορφίας κατά την εφαρμογή του Κανονισμού. Ο νέος κανονισμός εξουσιοδοτεί τις εκάστοτε Αρχές Προστασίας Προσωπικών Δεδομένων στην Ευρώπη, να επιβάλουν για σοβαρές παραβάσεις πρόστιμα σε ύψος έως και 4% του ετήσιου παγκόσμιου κύκλου εργασιών τους ή 20 εκατομμύρια ευρώ, ανάλογα πάντα με το ποιο είναι το μεγαλύτερο.

Το άρθρο 35 του GDPR εισάγει την έννοια της αξιολόγησης αντικτύπου προστασίας δεδομένων (Data Privacy Impact Assessment-DPIA), καθώς και της οδηγίας 2016/6802[32]. Η DPIA είναι μια διαδικασία που αποσκοπεί στην περιγραφή της επεξεργασίας, στην εκτίμηση της αναγκαιότητας και της αναλογικότητας μιας επεξεργασίας και στη διευκόλυνση της διαχείρισης των κινδύνων για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων που προκύπτουν από την επεξεργασία δεδομένων προσωπικού χαρακτήρα (αξιολογώντας τα και προσδιορίζοντας τα μέτρα

[31] Βλ. Παναγοπούλου-Κουτνατζή Φερενίκη, Ο Γενικός Κανονισμός για την προστασία δεδομένων 679/2016/ΕΕ, Εκδόσεις Σάκκουλα,2017.

[32] Βλ. Παράρτημα Α της παρούσας.

αντιμετώπισης τους). Αποτελεί σημαντικό εργαλείο λογοδοσίας, καθώς βοηθά τους υπεύθυνους επεξεργασίας όχι μόνο να συμμορφώνονται με τις απαιτήσεις του GDPR αλλά και να αποδείξουν ότι έχουν ληφθεί τα κατάλληλα μέτρα για να διασφαλιστεί η συμμόρφωση με τον κανονισμό (βλ. επίσης άρθρο 24). Με άλλα λόγια, μια DPIA είναι μια διαδικασία για την οικοδόμηση και την επίδειξη συμμόρφωσης.

Σύμφωνα με το GDPR, η μη συμμόρφωση με τις απαιτήσεις DPIA μπορεί να οδηγήσει σε πρόστιμα που επιβάλλονται από την αρμόδια εποπτική αρχή. Μη εφαρμογή DPIA όταν η επεξεργασία υπόκειται σε DPIA (άρθρο 35 παράγραφοι 1 και 3), που εκτελεί DPIA με εσφαλμένο τρόπο (άρθρο 35 παράγραφοι 2 και 7 έως 9) ή ελλείψει διαβουλεύσεων με την αρμόδια εποπτική αρχή, όταν απαιτείται (άρθρο 36 παράγραφος 3 στοιχείο ε), μπορεί να οδηγήσει σε διοικητικό πρόστιμο έως 10 εκατομμύρια ευρώ ή, σε περίπτωση επιχείρησης, έως και 2% τον ετήσιο κύκλο εργασιών του προηγούμενου οικονομικού έτους, όποιο είναι υψηλότερο.

Σημείωση: Ο όρος "εκτίμηση των επιπτώσεων στην ιδιωτική ζωή" (PIA) χρησιμοποιείται συχνά σε άλλα πλαίσια για να αναφέρεται στην ίδια έννοια.

Ο κανονισμός προβλέπει επίσης τον διορισμό υπευθύνου για την προστασία δεδομένων (DPO) σε κάθε θεσμικό όργανο και τον διορισμό ευρωπαίου επόπτη προστασίας δεδομένων (ΕΕΠΔ) σε ευρωπαϊκό επίπεδο. Επιπλέον, στο πλαίσιο μιας διασυνοριακής επεξεργασίας-συνεργασίας των κρατών-μελών της Ένωσης μέσω ενός μηχανισμού συνεκτικότητας[33] , δημιουργείται το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων, προκειμένου να συμβάλλει στη συνεκτική εφαρμογή του Κανονισμού στο σύνολο της Ένωσης, με στόχο οι εποπτικές αρχές να συνεργάζονται μεταξύ τους και, εφόσον απαιτείται, με την Επιτροπή.

Σύμφωνα με το άρθρο 99, ο Κανονισμός, ο οποίος δημοσιεύθηκε στις Μαΐου 2016, τίθεται σε εφαρμογή από τις 25 Μαΐου 2018. Το διάστημα αυτό των δύο ετών αποτελεί περίοδο προσαρμογής για τα εμπλεκόμενα μέρη. Συγκεκριμένα, πρόκειται για μια περίοδο κατά την οποία οι εταιρείες θα πρέπει να εξασφαλίσουν ότι θα συμμορφώνονται με το νέο σύνολο κανόνων, ενώ οι εθνικές αρχές προστασίας δεδομένων, η ομάδα εργασίας του άρθρου 29 αλλά και ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων θα πρέπει να εκδίδουν και γνωμοδοτήσεις, προκειμένου να βοηθήσουν τα εμπλεκόμενα μέρη στο πλαίσιο της προετοιμασίας τους.

[33] Βλ. Άρθρα 63 έως 76 GDPR.

Οι βασικότερες καινοτομίες του νέου Κανονισμού συνοψίζονται στις εξής:

α. Δικαίωμα διαγραφής (δικαίωμα στη λήθη)

Σύμφωνα με το άρθρο 17 του Κανονισμού, το υποκείμενο των δεδομένων έχει το δικαίωμα να ζητήσει από τον υπεύθυνο επεξεργασίας τη διαγραφή δεδομένων προσωπικού χαρακτήρα που το αφορούν χωρίς αδικαιολόγητη καθυστέρηση και ο υπεύθυνος επεξεργασίας υποχρεούται να διαγράψει δεδομένα προσωπικού χαρακτήρα χωρίς αδικαιολόγητη καθυστέρηση, εάν ισχύει ένας από τους προβλεπόμενους στον Κανονισμό λόγους.

β. Σαφής συγκατάθεση

Σύμφωνα με το άρθρο 7 του Κανονισμού, τίθενται αυστηρές προϋποθέσεις αναφορικά με τη συγκατάθεση από το ενδιαφερόμενο πρόσωπο για την επεξεργασία των προσωπικών του δεδομένων, την οποία έχει δικαίωμα να ανακαλέσει ανά πάσα στιγμή.

γ. Ανακοίνωση παραβίασης δεδομένων

Σύμφωνα με το άρθρο 34 του Κανονισμού, όταν η παραβίαση δεδομένων προσωπικού χαρακτήρα ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων ο υπεύθυνος επεξεργασίας ανακοινώνει αμελλητί την παραβίαση των δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων.

δ. Σαφής και κατανοητή γλώσσα στις πολιτικές απορρήτου

Σύμφωνα με το άρθρο 12 του Κανονισμού, ο υπεύθυνος επεξεργασίας λαμβάνει τα κατάλληλα μέτρα για να παρέχει στο υποκείμενο των δεδομένων κάθε απαιτούμενη από το νόμο πληροφορία σχετικά με την επεξεργασία σε συνοπτική, διαφανή, κατανοητή και εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή διατύπωση, ιδίως όταν πρόκειται για πληροφορία απευθυνόμενη ειδικά σε παιδιά.

ε. Αυστηρότερη εφαρμογή του νόμου και πρόστιμα στις επιχειρήσεις που τον παραβιάζουν

Το άρθρο 83 του Κανονισμού προβλέπει τους γενικούς όρους επιβολής διοικητικών προστίμων[34]. Υπό συγκεκριμένες προϋποθέσεις, ορισμένες παραβάσεις επισύρουν διοικητικά πρόστιμα έως και 20 εκατομμύρια ευρώ ή, σε περίπτωση επιχειρήσεων, έως το 4% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου

[34] Βλ. Παναγοπούλου Φερενίκη, Πώς θα επιβάλλει η ΑΠΔΠΧ τα πρόστιμα στις ασφαλιστικές από το 2018;,συνέντευξη στη Βίκυ Γερασίμου, Insurance Daily News, 17 Μαρ 2017.

οικονομικού έτους, ανάλογα με το ποιο είναι υψηλότερο, όπως αναφέρθηκε και εισαγωγικά.

Με την υιοθέτηση από το Κανονισμό νέων ενισχυμένων δικαιωμάτων, παρέχεται στα άτομα μεγαλύτερος έλεγχος επί των προσωπικών τους δεδομένων, μεταξύ άλλων μέσω:

α. της ανάγκης ύπαρξης σαφούς συγκατάθεσης του ενδιαφερομένου για την επεξεργασία των προσωπικών του δεδομένων.

β. της ευκολότερης πρόσβασης του ενδιαφερομένου στα προσωπικά του δεδομένα.

γ. των δικαιωμάτων διόρθωσης, διαγραφής και «λήθης».

δ. του δικαιώματος εναντίωσης, μεταξύ άλλων στη χρησιμοποίηση των δεδομένων προσωπικού χαρακτήρα για την «κατάρτιση προφίλ».

ε. του δικαιώματος φορητότητας των δεδομένων από πάροχο σε πάροχο.

Επιπλέον αναγνωρίζει το δικαίωμα των υποκειμένων των δεδομένων να υποβάλλουν καταγγελία σε εποπτική αρχή καθώς και το δικαίωμά τους για δικαστική προσφυγή και αποζημίωση[35]. Έτσι οι εταιρίες είναι εκτεθειμένες σε αγωγές από τρίτους των οποίων χάθηκαν τα προσωπικά τους δεδομένα.

Μαζί με το Γενικό Κανονισμό για για την προστασία δεδομένων, δημοσιεύθηκε στην Επίσημη Εφημερίδα της ΕΕ, η Οδηγία για την επεξεργασία δεδομένων από αρμόδιες αρχές για τους σκοπούς που σχετίζονται με ποινικά αδικήματα[36]. Η οδηγία δεν αφορά μόνο στη διασυνοριακή μεταφορά δεδομένων εντός της ΕΕ, αλλά θεσπίζει για πρώτη φορά ελάχιστα πρότυπα για την επεξεργασία δεδομένων από τις αστυνομικές και δικαστικές αρχές στο εσωτερικό κάθε κράτους-μέλους.Σύμφωνα με τους εισηγητές της, η θέσπιση κοινών προτύπων θα συντελέσει στην αντιμετώπιση ενός βασικού και επίκαιρου προβλήματος σχετικά με τη διερεύνηση τρομοκρατικών ενεργειών και άλλων διασυνοριακών εγκλημάτων, το οποίο αφορά στη δυσκολία και την καθυστέρηση στην ανταλλαγή πληροφοριών. Η νέα ευρωπαϊκή οδηγία αποσκοπεί στην προστασία των ατόμων, είτε αυτοί είναι θύματα ή μάρτυρες, είτε εγκληματίες, ορίζοντας σαφή δικαιώματα και περιορισμούς για τις διαβιβάσεις δεδομένων που στόχο έχουν την πρόληψη, διερεύνηση, ανίχνευση ή δίωξη ποινικών αδικημάτων ή την εκτέλεση

[35] Άρθρα 77 επ. GDPR.

[36] Οδηγία (ΕΕ) 2016/680 της 27ης Απριλίου 2016

ποινικών κυρώσεων. Ταυτόχρονα θα διευκολύνει την ομαλή και αποτελεσματική συνεργασία μεταξύ των εθνικών αρχών επιβολής του νόμου.

Τέλος, το «πακέτο» των τροποποιήσεων ολοκληρώνεται, τουλάχιστον επί του παρόντος, με την Οδηγία σχετικά με τη χρήση των δεδομένων που περιέχονται στις καταστάσεις ονομάτων επιβατών για την πρόληψη, ανίχνευση, διερεύνηση και δίωξη τρομοκρατικών και σοβαρών εγκλημάτων[37]. Ορισμένα από τα βασικά σημεία της οδηγίας είναι ότι τα κράτη μέλη θα πρέπει να ιδρύσουν ή να ορίσουν μια αρχή αρμόδια για την πρόληψη, ανίχνευση, διερεύνηση και δίωξη τρομοκρατικών και σοβαρών εγκλημάτων, η οποία θα είναι αρμόδια για τη συλλογή και διαχείριση των δεδομένων αυτών από τους αερομεταφορείς και τη μεταβίβασή τους στις αρχές (Μονάδα Στοιχείων Επιβατών ή ΜΣΕ). Οι πληροφορίες αυτές θα διατηρούνται σε βάση δεδομένων για περίοδο 5 ετών, αλλά μετά από 6 μήνες, όλα τα δεδομένα θα "ανωνυμοποιούνται" με την κάλυψη των στοιχείων που μπορούν να χρησιμεύσουν στην άμεση ταυτοποίηση του επιβάτη στον οποίο αναφέρονται (πχ. όνομα, διεύθυνση και στοιχεία επικοινωνίας). Τα κράτη μέλη θα μπορούν να συλλέγουν και να επεξεργάζονται αυτά τα δεδομένα και από οικονομικούς φορείς που δεν είναι μεταφορείς, όπως ταξιδιωτικά γραφεία και διοργανωτές ταξιδιών που παρέχουν σχετιζόμενες με ταξίδια υπηρεσίες, συμπεριλαμβανομένων των κρατήσεων πτήσεων.

[37] Οδηγία (ΕΕ) 2016/681 της 27ης Απριλίου 2016

4.3 Στόχοι Γενικού Κανονισμού

Ο Κανονισμός GDPR έχει ως στόχο να διευρύνει την προστασία των δεδομένων στην εποχή των big data και του cloud computing, εξασφαλίζοντας ότι η προστασία των δεδομένων αποτελεί θεμελιώδες βασικό δικαίωμα[38], το οποίο θα ρυθμίζεται με συνέπεια σε όλη την Ευρώπη, ενισχύοντας ουσιαστικά τον ρόλο του υπεύθυνου επεξεργασίας.

Ο κανονισμός περιγράφει τα δικαιώματα του υποκειμένου των δεδομένων, δηλαδή του ατόμου του οποίου τα προσωπικά δεδομένα υποβάλλονται σε επεξεργασία. Αυτά τα ενισχυμένα δικαιώματα παρέχουν στα άτομα μεγαλύτερο έλεγχο επί των προσωπικών τους δεδομένων, μέσω της ανάγκης ύπαρξης σαφούς συγκατάθεσης του ενδιαφερομένου για την επεξεργασία των προσωπικών του δεδομένων, της ευκολότερης πρόσβασης του ενδιαφερομένου στα προσωπικά του δεδομένα, των δικαιωμάτων διόρθωσης, διαγραφής και «λήθης», του δικαιώματος εναντίωσης, μεταξύ άλλων στη χρησιμοποίηση των δεδομένων προσωπικού χαρακτήρα για την «κατάρτιση προφίλ», του δικαιώματος φορητότητας των δεδομένων από πάροχο σε πάροχο, που απαριθμήθηκαν παραπάνω.

Από την άλλη πλευρά θέτει μία σειρά περιορισμών και νέων υποχρεώσεων στις επιχειρήσεις σχετικά με την επεξεργασία των προσωπικών δεδομένων σε όλο τον κύκλο ζωής τους, από τη συλλογή έως και την καταστροφή τους, τη δυνατότητα μεταφοράς τους σε άλλες χώρες, την προστασία των δικαιωμάτων των φυσικών προσώπων, την ασφάλεια (εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα) των προσωπικών δεδομένων και τις ενέργειες γνωστοποίησης που οφείλει να κάνει η επιχείρηση σε περίπτωση παραβίασης.

Σκοπός του κανονισμού είναι η προστασία των θεμελιωδών ελευθεριών και δικαιωμάτων των προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα στα πλαίσια των θεσμικών οργάνων και των οργανισμών της ΕΕ. Ορίζει τις αρχές και υποχρεώσεις που οφείλουν να τηρούν τα θεσμικά όργανα της ΕΕ κατά την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Ορίζει τις υποχρεώσεις των προσώπων που επεξεργάζονται δεδομένα προσωπικού χαρακτήρα (υπεύθυνοι επεξεργασίας δεδομένων) και τα δικαιώματα των ατόμων των οποίων τα δεδομένα

[38] Βλ. Ζωγραφόπουλο Δημήτριο, «Το νομικό πλαίσιο προστασίας θεμελιωδών δικαιωμάτων – και ιδίως της ιδιωτικής ζωής- των προσώπων από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, Αθήνα, 23 Ιουν 2016.

προσωπικού χαρακτήρα υφίστανται επεξεργασία (υποκείμενα των δεδομένων) μέσα σε καθεστώς που διέπεται αυστηρά από τις παρακάτω αρχές της νόμιμης επεξεργασίας[39]:

α. Αρχή της νομιμότητας, αντικειμενικότητας και διαφάνειας της επεξεργασίας (lawfulness, fairness and transparency).

β. Αρχή του περιορισμού του σκοπού (purpose limitation): τα προσωπικά δεδομένα πρέπει να συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και να μην υφίστανται περαιτέρω επεξεργασία με τρόπο ασύμβατο προς αυτούς τους σκοπούς. Ο Κανονισμός προβλέπει ότι περαιτέρω επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς δεν θεωρείται ασύμβατη με τους αρχικούς σκοπούς, εφόσον πληρούνται συγκεκριμένες προϋποθέσεις.

γ. Αρχή της ελαχιστοποίησης των δεδομένων (data minimisation): τα δεδομένα που τυγχάνουν επεξεργασίας περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους έχουν αρχικά συλλεγεί.

δ. Αρχή της ακρίβειας (accuracy) : λήψη μέτρων που διασφαλίζουν ότι τα προσωπικά δεδομένα που είναι ανακριβή, λαμβάνοντας υπόψη τους σκοπούς για τους οποίους αυτά υφίστανται επεξεργασία, διαγράφονται ή διορθώνονται χωρίς καθυστέρηση.

ε. Αρχή του περιορισμού της περιόδου αποθήκευσης: (storage limitation) τα δεδομένα διατηρούνται σε μορφή που επιτρέπει την ταυτοποίηση των υποκείμενων μόνο για το διάστημα που απαιτείται για να πραγματοποιηθεί ο σκοπός της επεξεργασίας. Ωστόσο, η αποθήκευση των δεδομένων επιτρέπεται για μεγαλύτερα χρονικά διαστήματα στην περίπτωση που τα προσωπικά δεδομένα αποθηκεύονται μόνο για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς.

στ.Αρχή της ακεραιότητας και εμπιστευτικότητας:(integrity and confidentiality) τα προσωπικά δεδομένα πρέπει να υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ασφάλεια των δεδομένων.

ζ. Αρχή της Λογοδοσίας (accountability): ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και πρέπει να αποδεικνύει τη συμμόρφωση με όλες τις πιο πάνω αρχές.

[39] Άρθρο 5 GDPR.

Ιδιαίτερη μνεία γίνεται στο προοίμιο του Κανονισμού στα παιδιά[40], τα οποία απαιτούν ειδική προστασία όσον αφορά τα δεδομένα τους προσωπικού χαρακτήρα, καθώς μπορεί να έχουν μικρότερη επίγνωση των σχετικών κινδύνων, συνεπειών και εγγυήσεων και των δικαιωμάτων τους σε σχέση με την επεξεργασία δεδομένων προσωπικού χαρακτήρα, όπως επίσης και στους ηλικιωμένους. Αυτή η ειδική προστασία θα πρέπει να ισχύει ιδίως στη χρήση των δεδομένων προσωπικού χαρακτήρα με σκοπό την εμπορία ή τη δημιουργία προφίλ προσωπικότητας ή προφίλ χρήστη και τη συλλογή δεδομένων προσωπικού χαρακτήρα όσον αφορά παιδιά κατά τη χρήση υπηρεσιών που προσφέρονται άμεσα σε ένα παιδί. Η συγκατάθεση του γονέα ή κηδεμόνα δεν θα πρέπει να είναι απαραίτητη σε συνάρτηση με υπηρεσίες πρόληψης ή παροχής συμβουλών που προσφέρονται άμεσα σε ένα παιδί. Ερώτημα ανακύπτει αν το δικαίωμα προστασίας για τα παιδιά θα πρέπει να είναι «επαυξημένο» [41] έναντι του «κανονικού» για όλους τους άλλους, δικαίωμα δύο ταχυτήτων δηλαδή. Η απάντηση είναι ότι η ενισχυμένη προστασία θα πρέπει να αφορά όλους, καθώς δεν είναι λίγοι οι «διαδικτυακά» αναλφάβητοι ενήλικες.

[40] Βλ. Σκέψη 38 προοιμίου GDPR.

[41] Βλ. Μελέτη της Φερενίκης Παναγοπούλου-Κουτνατζή με τίτλο «Τα νέα δικαιώματα για τους πολίτες βάσει του Γενικού Κανονισμού Προστασίας Δεδομένων: μια πρώτη αποτίμηση και συνταγματική αξιολόγηση», δημοσιευμένη στην Εφημ ΔΔ-1/2017.

5. Ο ρόλος και οι νέες ευθύνες του Υπεύθυνου Επεξεργασίας

5.1 Οι γενικές υποχρεώσεις του Υπεύθυνου Επεξεργασίας

Ο υπεύθυνος επεξεργασίας είναι το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα· όταν οι σκοποί και ο τρόπος της επεξεργασίας αυτής καθορίζονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια για τον διορισμό του μπορούν να προβλέπονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους[42]. Σύμφωνα με το άρθρο 24 του Κανονισμού, οφείλει να εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα, προκειμένου να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με αυτόν. Τα εν λόγω μέτρα επανεξετάζονται και επικαιροποιούνται όταν κρίνεται απαραίτητο. Σύμφωνα με το ισχύον δίκαιο της ΕΕ για την προστασία των δεδομένων, η προσέγγιση τους διαφέρει από το ένα κράτος μέλος στο άλλο. Ο Νέος Κανονισμός ορίζει αναλυτικά τις γενικές υποχρεώσεις που έχουν οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία των δεδομένων προσωπικού χαρακτήρα για λογαριασμό αυτών, οι οποίες συμπυκνώνονται στις παρακάτω:

α. Λήψη συγκατάθεσης για ανήλικους κάτω των 16 σε σχέση με τις υπηρεσίες της κοινωνίας των πληροφοριών (Άρθρο 8 GDPR)

Για ανήλικους κάτω των 16 ετών δεν αρκεί η συγκατάθεση τους για την επεξεργασία προσωπικών τους δεδομένων αλλά χρειάζεται και η συγκατάθεση του κηδεμόνα τους.

β. Φέρει το βάρος της αποδείξεως όσον αφορά στην παροχή συγκατάθεσης (Άρθρο 7 GDPR)

Η δήλωση συγκατάθεσης για την επεξεργασία προσωπικών δεδομένων πρέπει να είναι διατυπωμένη εκ των προτέρων από τον υπεύθυνο επεξεργασίας σε απλή και κατανοητή γλώσσα.

[42] Άρθρο 4 GDPA.

γ. Υποχρέωση κατασκευαστών στο στάδιο του σχεδιασμού και εξ΄ορισμού (privacy by default and by design-Άρθρο 25 GDPR)

Οι κατασκευαστές πρέπει να λαμβάνουν μέτρα προστασίας των χρηστών στο στάδιο του σχεδιασμού και εξ' ορισμού. Για παράδειγμα, οι κατασκευαστές έξυπνων συσκευών θα πρέπει να διασφαλίζουν ότι, διατηρείται η ανωνυμία των προσώπων που αγοράζουν τις συσκευές τους και οι σχεδιαστές εφαρμογών (applications) θα συλλέγουν πληροφορίες για τους χρήστες, μόνο στο βαθμό που επιτρέπει ο Κανονισμός.

δ. Υποχρέωση γνωστοποίησης παραβιάσεων ασφάλειας (notification of a personal data breach (Άρθρο 33 GDPR)

Όταν ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία γνωρίζει την παραβίαση της ασφάλειας του συστήματος οφείλει να ειδοποιήσει το Γραφείο της Επιτρόπου. Η Γνωστοποίηση πρέπει να γίνεται και στο ίδιο το υποκείμενο.

ε. Νομική ευθύνη έχει ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία σε περίπτωση παραβίασης (Άρθρο 26 GDPR)

Ο Κανονισμός τους «βλέπει» ως συναδικοπραγούντες, με αποτέλεσμα ο καθένας να ευθύνεται εις ολόκληρο για την ζημιά την οποία υπέστη το υποκείμενο των δεδομένων.

στ. Ασφάλεια της επεξεργασίας (security of processing- Άρθρο 25 GDPR)

1/ Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα για να διασφαλίζεται το επίπεδο ασφάλειας, έναντι των κινδύνων.

2/ Γίνεται εκτίμηση του ενδεδειγμένου επιπέδου ασφαλείας, λαμβάνοντας υπόψη τους κινδύνους που απορρέουν από την επεξεργασία (π.χ. από παράνομη καταστροφή, απώλεια κ.λ.π.).

3/ Τηρείται εγκεκριμένος κώδικας δεοντολογίας ή εγκεκριμένος μηχανισμός πιστοποίησης.

ζ. Εκτίμηση αντικτύπου (impact assessment - Άρθρο 30 GDPR)

1/ Όταν ένα είδος επεξεργασίας (ιδίως με τη χρήση νέων τεχνολογιών) ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας διενεργεί πριν από την επεξεργασία, εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας.

2/ Καταρτίζει και δημοσιοποιεί κατάλογο με τα είδη των πράξεων επεξεργασίας για τα οποία απαιτείται εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων. Επίσης, καταρτίζει και δημοσιοποιεί κατάλογο με τα είδη των πράξεων επεξεργασίας για τα οποία δεν απαιτείται εκτίμηση αντικτύπου.

3/ Σε περίπτωση που έχει οριστεί σε ένα οργανισμό DPO, ο υπεύθυνος επεξεργασίας ζητά τη γνώμη του πριν από την επεξεργασία, όταν η εκτίμηση αντικτύπου υποδεικνύει ότι η επεξεργασία θα έθετε σε κίνδυνο τα δικαιώματα και τις ελευθερίες φυσικών προσώπων.

η. Τήρηση αρχείων των δραστηριοτήτων της επεξεργασίας (records of processing activities- Άρθρο 30 παρ.5 GDPR)

Κάθε υπεύθυνος επεξεργασίας και εκτελών την επεξεργασία τηρεί αρχείο των δραστηριοτήτων επεξεργασίας που περιλαμβάνει πληροφορίες όπως π.χ. τους σκοπούς της επεξεργασίας και τους αποδέκτες των δεδομένων. Η εν λόγω υποχρέωση δεν ισχύει για επιχείρηση/οργανισμό που απασχολεί κάτω από 250 άτομα, εκτός εάν η επεξεργασία ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα/ελευθερίες των υποκειμένων, δεν είναι περιστασιακή και περιλαμβάνει ειδικές κατηγορίες προσωπικών δεδομένων (π.χ. δεδομένα υγείας) και δεδομένα που αφορούν ποινικές καταδίκες.

ζ. Τήρηση κώδικα δεοντολογίας (code of conduct-Άρθρο 40 GDPR)

Ενώσεις και άλλοι φορείς που εκπροσωπούν κατηγορίες υπεύθυνων επεξεργασίας ή εκτελούντων την επεξεργασία μπορούν να εκπονούν κώδικες δεοντολογίας ή να τροποποιούν υφιστάμενους με σκοπό τη συμμόρφωση με τον Κανονισμό όσον αφορά στη θεμιτή και με διαφάνεια επεξεργασία, στη συλλογή προσωπικών δεδομένων, στην άσκηση των δικαιωμάτων των υποκειμένων κ.λ.π. Ανεξάρτητος φορέας που διαθέτει το ενδεδειγμένο επίπεδο εμπειρογνωμοσύνης σε σχέση με το αντικείμενο του κώδικα δεοντολογίας μπορεί να παρακολουθεί τη συμμόρφωση με αυτόν, δεδομένου ότι είναι διαπιστευμένος για το σκοπό αυτό από τον Επίτροπο Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Ο φορέας θεωρείται ότι είναι διαπιστευμένος εφόσον πληροί συγκεκριμένα κριτήρια που θέτει το άρθρο 41 του Κανονισμού. Σε περίπτωση παράβασης του κώδικα, π.χ. ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία δεν έχει ορίσει DPO, ο φορέας λαμβάνει ανάλογα μέτρα και ενημερώνει σχετικά τον Επίτροπο Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

η. Πιστοποίηση (Certification- Άρθρο 42 GDPR)

Ο υπεύθυνος επεξεργασίας/εκτελών την επεξεργασία θεσπίζει, εάν επιθυμεί, μηχανισμούς πιστοποίησης της προστασίας δεδομένων, σφραγίδες και σήματα με σκοπό την απόδειξη συμμόρφωσης με τον Κανονισμό. Η πιστοποίηση χορηγείται από τους φορείς πιστοποίησης (certification bodies) ή τον Επίτροπο Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Οι φορείς πιστοποίησης είναι διαπιστευμένοι βάσει κριτηρίων που εγκρίνονται από τον Επίτροπο για μέγιστη περίοδο 5 ετών και μπορεί να ανανεωθεί. Είναι υπεύθυνοι για την ορθή εκτίμηση που οδηγεί στην πιστοποίηση ή στην ανάκληση της πιστοποίησης.

Ο GDPR θα εισάγει λοιπόν σημαντικές νέες υποχρεώσεις και θα εφαρμόσει επίσης ένα πολύ πιο επίσημο πλαίσιο γύρω από τους ρόλους και τις ευθύνες του υπεύθυνου επεξεργασίας. Από το άρθρο 24 παράγραφος 1 του GDPR προκύπτει επιπλέον η υποχρέωση των επιχειρήσεων να αποδείξουν ότι συμμορφώνονται με τις απαιτήσεις του.

Θα υπάρξει αναμφισβήτητα κάποια διακύμανση όσον αφορά τον τρόπο με τον οποίο οι εταιρείες σε όλο τον κόσμο θα συμμορφώνονται με τον Κανονισμό, ειδικά αν δεν έχουν ακόμη δημιουργήσει ένα επίσημο γραφείο προστασίας προσωπικών δεδομένων κάποιου είδους. Το απόρρητο παραμένει "νέο" σε πολλά μέρη του κόσμου. Αλλά ακόμα και όπου είναι πιο εδραιωμένο, τα οργανωτικά τμήματα της ιδιωτικής ζωής εξακολουθούν να είναι σχετικά πρόσφατες εφευρέσεις. Όπως μάθαμε στην έκθεση για τη διακυβέρνηση της ιδιωτικής ζωής στο 2016 του IAPP-EY[43], το μέσο γραφείο για την προστασία της ιδιωτικής ζωής είναι μόλις πάνω από έξι χρόνια, και ακόμη και όσοι αναφέρουν ότι είναι "ώριμοι" μπορεί να έχουν μέσο όρο ηλικίας μόλις 11 ετών.

[43] Βλ. Ιστοσελίδα https://iapp.org

5.2 Επαγγελματική Κατάρτιση των Υπεύθυνων Επεξεργασίας

Οι υπεύθυνοι επεξεργασίας θα πρέπει να διαθέτουν εμπειρογνωμοσύνη σε εθνικούς και ευρωπαίους νόμους και πρακτικές για την προστασία των δεδομένων, συμπεριλαμβανομένης της σε βάθος κατανόησης του GDPR, κατανόηση των εργασιών επεξεργασίας που πραγματοποιήθηκαν και των τεχνολογιών των πληροφοριών και της ασφάλειας των δεδομένων, γνώση του επιχειρηματικού τομέα και του οργανισμού, ικανότητα να προωθήσει μια κουλτούρα προστασίας δεδομένων εντός του οργανισμού.

Για να μπορέσουν οι επαγγελματίες του χώρου των προσωπικών δεδομένων να ανταποκριθούν στις αυξήμενες υποχρεώσεις και σοβαρότατη ευθύνη του ρόλου του υπεύθυνου επεξεργασίας απαιτείται η ουσιαστική επιμόρφωση και εκπαίδευση τους, τόσο σε ότι αφορά τον Γενικό Κανονισμό Προσωπικών Δεδομένων, αλλά και σε ειδικά θέματα προσωπικών δεδομένων, όπως η κατάρτιση DPIA, που αναφέρθηκε παραπάνω, σε περίπτωση εισαγωγής νέων υπηρεσιών ή προϊόντων που συνεπάγονται την επεξεργασία σε μεγάλη κλίμακα προσωπικών δεδομένων ή διαχειρίζονται ειδικά προσωπικά δεδομένα, την κατάρτιση ενός Προγράμματος/Πλαισίου Προσωπικών Δεδομένων εντός της Επιχείρησης/Εταιρίας, ο καθορισμός και η επικοινωνία Πολιτικής Προστασίας /Κανονισμού Προστασίας Προσωπικών Δεδομένων και η Κοινοποίηση του στην Εθνική Αρχή Προστασία Δεδομένων Προσωπικού Χαρακτήρα και άλλα αντίστοιχα θέματα.

5.3 Οι κατευθυντήριες γραμμές του προοιμίου του GDPR

5.3.1 Στο επίκεντρο της επεξεργασίας ο άνθρωπος και τα θεμελιώδη δικαιώματά του

Στο προοίμιο του Γενικού Κανονισμού ορίζεται σαφώς ότι η επεξεργασία των δεδομένων προσωπικού χαρακτήρα θα πρέπει να προορίζεται να εξυπηρετεί τον άνθρωπο, σεβόμενη όλα τα θεμελιώδη δικαιώματα και να τηρεί τις ελευθερίες και αρχές που αναγνωρίζονται στον Χάρτη όπως κατοχυρώνονται στις Συνθήκες[44], ιδίως τον σεβασμό της ιδιωτικής και οικογενειακής ζωής, της κατοικίας και των επικοινωνιών, την προστασία των δεδομένων προσωπικού χαρακτήρα, την ελευθερία σκέψης, συνείδησης και θρησκείας, την ελευθερία έκφρασης και πληροφόρησης, την επιχειρηματική ελευθερία, το δικαίωμα πραγματικής προσφυγής και αμερόληπτου δικαστηρίου και την πολιτιστική, θρησκευτική και γλωσσική πολυμορφία[45]. Οι εθνικές αρχές των κρατών μελών καλούνται από το δίκαιο της Ένωσης να συνεργάζονται και να ανταλλάσσουν δεδομένα προσωπικού χαρακτήρα προκειμένου να μπορούν να εκτελούν τις υποχρεώσεις τους ή να ασκούν καθήκοντα για λογαριασμό αρχής άλλου κράτους μέλους. Ο Κανονισμός παρέχει επίσης περιθώρια χειρισμού στα κράτη μέλη, ώστε να εξειδικεύσουν τους κανόνες του, συμπεριλαμβανομένων αυτών που αφορούν την επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα («ευαίσθητα δεδομένα»). Σε αυτόν τον βαθμό, ο παρών κανονισμός δεν αποκλείει το δίκαιο των κρατών μελών να προσδιορίζει τις περιστάσεις ειδικών καταστάσεων επεξεργασίας, μεταξύ άλλων τον ακριβέστερο καθορισμό των προϋποθέσεων υπό τις οποίες η επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι σύννομη.

5.3.2 Ενίσχυση και λεπτομερής καθορισμός των δικαιωμάτων των υποκειμένων των δεδομένων

Η αποτελεσματική προστασία των δεδομένων προσωπικού χαρακτήρα σε ολόκληρη την Ένωση απαιτεί την ενίσχυση και τον λεπτομερή καθορισμό των δικαιωμάτων των

---

[44] Άρθρο 8 παράγραφος 1 του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης («Χάρτης») και άρθρο 16 παράγραφος 1 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ).

[45] Σκέψη 4 Προοιμίου GDPR.

υποκειμένων των δεδομένων, καθώς και των υποχρεώσεων όσων επεξεργάζονται και καθορίζουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα, καθώς και των αντίστοιχων εξουσιών παρακολούθησης και διασφάλισης της συμμόρφωσης προς τους κανόνες προστασίας των δεδομένων προσωπικού χαρακτήρα και των αντίστοιχων κυρώσεων για τις παραβιάσεις στα κράτη μέλη. Για την ομαλή λειτουργία της εσωτερικής αγοράς, η ελεύθερη κυκλοφορία δεδομένων προσωπικού χαρακτήρα εντός της Ένωσης δεν πρέπει να περιορίζεται, ούτε να απαγορεύεται για λόγους που σχετίζονται με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

Οι προσωπικές ή οικιακές δραστηριότητες θα μπορούσαν να περιλαμβάνουν την αλληλογραφία και την τήρηση αρχείου διευθύνσεων ή την κοινωνική δικτύωση και την επιγραμμική δραστηριότητα που ασκείται στο πλαίσιο τέτοιων δραστηριοτήτων. Ωστόσο, ο παρών κανονισμός εφαρμόζεται σε υπευθύνους επεξεργασίας ή εκτελούντες την επεξεργασία οι οποίοι παρέχουν τα μέσα επεξεργασίας δεδομένων προσωπικού χαρακτήρα για τέτοιες προσωπικές ή οικιακές δραστηριότητες. Η προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, της διερεύνησης, της ανίχνευσης ή της δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων, συμπεριλαμβανομένης της διασφάλισης έναντι των απειλών κατά της δημόσιας ασφάλειας και της πρόληψής τους και της ελεύθερης κυκλοφορίας των δεδομένων αυτών, αποτελεί το αντικείμενο ειδικής ενωσιακής νομικής πράξης. Ο Κανονισμός δεν θα πρέπει συνεπώς να εφαρμόζεται σε δραστηριότητες επεξεργασίας για τους σκοπούς αυτούς.

Όταν η επεξεργασία δεδομένων προσωπικού χαρακτήρα από ιδιωτικούς φορείς εμπίπτει στο πεδίο εφαρμογής του Κανονισμού, ο κανονισμός θα πρέπει να προβλέπει τη δυνατότητα των κρατών μελών να περιορίζουν διά νόμου, υπό ειδικές συνθήκες, ορισμένες υποχρεώσεις και δικαιώματα, όταν ο περιορισμός αυτός συνιστά αναγκαίο και αναλογικό μέτρο σε μια δημοκρατική κοινωνία για να διασφαλιστούν ειδικά σημαντικά συμφέροντα, μεταξύ άλλων η δημόσια ασφάλεια και η πρόληψη, διερεύνηση, ανίχνευση και δίωξη ποινικών αδικημάτων ή η εκτέλεση ποινικών κυρώσεων, συμπεριλαμβανομένης της διασφάλισης έναντι των απειλών κατά της δημόσιας ασφάλειας και της πρόληψής τους. Αυτό έχει σημασία, για παράδειγμα, στο πλαίσιο του αγώνα ενάντια στο ξέπλυμα χρήματος ή των δραστηριοτήτων των εγκληματολογικών εργαστηρίων. Ενώ ο παρών κανονισμός εφαρμόζεται, μεταξύ άλλων, στις δραστηριότητες των δικαστηρίων και άλλων δικαστικών αρχών, το δίκαιο της Ένωσης ή των κρατών μελών θα μπορούσε να εξειδικεύει τις πράξεις και διαδικασίες επεξεργασίας σε σχέση με την επεξεργασία δεδομένων προσωπικού

χαρακτήρα από δικαστήρια και άλλες δικαστικές αρχές. Η αρμοδιότητα των εποπτικών αρχών δεν θα πρέπει να καλύπτει την επεξεργασία δεδομένων προσωπικού χαρακτήρα, όταν τα δικαστήρια ενεργούν υπό τη δικαιοδοτική τους ιδιότητα, προκειμένου να διασφαλίζεται η ανεξαρτησία των δικαστικών λειτουργών κατά την άσκηση των δικαιοδοτικών τους καθηκόντων, περιλαμβανομένης της λήψης αποφάσεων. Η εποπτεία των εν λόγω πράξεων επεξεργασίας δεδομένων θα πρέπει να μπορεί να ανατεθεί σε ειδικούς φορείς στο πλαίσιο του δικαστικού συστήματος του κράτους μέλους, το οποίο θα πρέπει ιδίως να διασφαλίζει τη συμμόρφωση με τους κανόνες του παρόντος κανονισμού, να ευαισθητοποιεί μέλη των δικαστικών λειτουργών όσον αφορά τις υποχρεώσεις τους βάσει του παρόντος κανονισμού και να επιλαμβάνεται καταγγελιών σε σχέση με τις εν λόγω διαδικασίες επεξεργασίας δεδομένων.

Για να διασφαλιστεί ότι τα φυσικά πρόσωπα δεν στερούνται την προστασία που δικαιούνται βάσει του παρόντος κανονισμού, η επεξεργασία των δεδομένων προσωπικού χαρακτήρα υποκειμένων που βρίσκονται στην Ένωση από υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία μη εγκατεστημένο στην Ένωση θα πρέπει να διέπεται από τον παρόντα κανονισμό, εφόσον οι δραστηριότητες επεξεργασίας σχετίζονται με την παροχή αγαθών ή υπηρεσιών στα εν λόγω υποκείμενα των δεδομένων, ανεξάρτητα από το εάν συνδέονται με πληρωμή. Για να κριθεί εάν ένας τέτοιος υπεύθυνος επεξεργασίας ή εκτελών την επεξεργασία προσφέρει αγαθά ή υπηρεσίες σε υποκείμενα των δεδομένων που βρίσκονται στην Ένωση, θα πρέπει να εξακριβωθεί αν ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία προδήλως αποσκοπεί να παράσχει υπηρεσίες στα υποκείμενα των δεδομένων σε ένα ή περισσότερα κράτη μέλη της Ένωσης. Ενώ η απλή προσβασιμότητα στην ιστοσελίδα του υπευθύνου επεξεργασίας, του εκτελούντος την επεξεργασία ή ενός μεσάζοντος στην Ένωση ή στη διεύθυνση ηλεκτρονικού ταχυδρομείου και σε άλλα στοιχεία επικοινωνίας ή η χρήση γλώσσας που χρησιμοποιείται συνήθως στην τρίτη χώρα όπου ο υπεύθυνος επεξεργασίας είναι εγκατεστημένος δεν αρκεί για να τεκμηριωθεί τέτοια πρόθεση, παράγοντες όπως η χρήση γλώσσας ή νομίσματος που χρησιμοποιούνται συνήθως σε ένα ή περισσότερα κράτη μέλη, με δυνατότητα παραγγελίας προϊόντων και υπηρεσιών σε αυτήν την άλλη γλώσσα, ή η αναφορά σε πελάτες ή χρήστες που βρίσκονται στην Ένωση μπορούν να καταστήσουν πρόδηλο ότι ο υπεύθυνος επεξεργασίας προτίθεται να προσφέρει αγαθά ή υπηρεσίες σε υποκείμενα των δεδομένων στην Ένωση[46].

[46] Σκέψη 23 Προοιμίου GDPR.

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα προσώπων που βρίσκονται στην Ένωση από υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία μη εγκατεστημένο στην Ένωση θα πρέπει επίσης να διέπεται από τον παρόντα κανονισμό, εφόσον αφορά την παρακολούθηση της συμπεριφοράς των εν λόγω υποκειμένων των δεδομένων στον βαθμό που η συμπεριφορά τους λαμβάνει χώρα εντός της Ένωσης. Για τον καθορισμό του κατά πόσον μια δραστηριότητα επεξεργασίας μπορεί να θεωρηθεί ότι παρακολουθεί τη συμπεριφορά υποκειμένου των δεδομένων, θα πρέπει να εξακριβωθεί κατά πόσον φυσικά πρόσωπα παρακολουθούνται στο Διαδίκτυο, συμπεριλαμβανομένης της δυνητικής μετέπειτα χρήσης τεχνικών επεξεργασίας δεδομένων προσωπικού χαρακτήρα οι οποίες συνίστανται στη διαμόρφωση του «προφίλ» ενός φυσικού προσώπου, ιδίως με σκοπό να ληφθούν αποφάσεις που το αφορούν ή να αναλυθούν ή να προβλεφθούν οι προσωπικές προτιμήσεις, οι συμπεριφορές και οι νοοτροπίες του[47].

5.3.3 Αναγκαιότητα σύννομης επεξεργασίας και έννομα συμφέροντα υπεύθυνου επεξεργασίας

Επιπλέον, στο προοίμιο του Κανονισμού επισημαίνεται ότι η επεξεργασία θα πρέπει να είναι σύννομη[48], εφόσον είναι αναγκαία στο πλαίσιο σύμβασης ή πρόθεσης σύναψης σύμβασης. Η αρχή αυτή απαιτεί κάθε πληροφορία και ανακοίνωση σχετικά με την επεξεργασία των εν λόγω δεδομένων προσωπικού χαρακτήρα να είναι εύκολα προσβάσιμη και κατανοητή και να χρησιμοποιεί σαφή και απλή γλώσσα. Αυτή η αρχή αφορά ιδίως την ενημέρωση των υποκειμένων των δεδομένων σχετικά με την ταυτότητα του υπευθύνου επεξεργασίας και τους σκοπούς της επεξεργασίας και την περαιτέρω ενημέρωση ώστε να διασφαλιστεί δίκαιη και διαφανής επεξεργασία σε σχέση με τα εν λόγω φυσικά πρόσωπα και το δικαίωμά τους να λαμβάνουν επιβεβαίωση και να επιτυγχάνουν ανακοίνωση των σχετικών με αυτά δεδομένων προσωπικού χαρακτήρα που υπόκεινται σε επεξεργασία. Θα πρέπει να γνωστοποιείται στα φυσικά πρόσωπα η ύπαρξη κινδύνων, κανόνων, εγγυήσεων και δικαιωμάτων σε σχέση με την επεξεργασία δεδομένων προσωπικού χαρακτήρα και πώς να ασκούν τα δικαιώματά τους σε σχέση με την επεξεργασία αυτή.

[47] Σκέψη 24 Προοιμίου GDPR.

[48] Σκέψη 39 Προοιμίου GDPR.

Όταν η επεξεργασία διενεργείται σύμφωνα με νομική υποχρέωση την οποία υπέχει ο υπεύθυνος επεξεργασίας ή όταν είναι αναγκαία για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας, η επεξεργασία θα πρέπει να έχει βάση στο δίκαιο της Ένωσης ή κράτους μέλους. Ο Κανονισμός δεν απαιτεί συγκεκριμένο νόμο για κάθε μεμονωμένη επεξεργασία. Μπορεί να αρκεί ένας μόνο νόμος ως βάση για περισσότερες από μία πράξεις επεξεργασίας με βάση νομική υποχρέωση στην οποία υπόκειται ο υπεύθυνος επεξεργασίας ή εάν η επεξεργασία είναι αναγκαία για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας. Επίσης, ο καθορισμός του σκοπού της επεξεργασίας θα πρέπει να εναπόκειται στο δίκαιο της Ένωσης ή κράτους μέλους.

Σε κάθε περίπτωση τα έννομα συμφέροντα του υπευθύνου επεξεργασίας, περιλαμβανομένων εκείνων ενός υπευθύνου επεξεργασίας στον οποίο μπορούν να κοινολογηθούν τα δεδομένα προσωπικού χαρακτήρα ή τρίτων, μπορεί να παρέχουν τη νομική βάση για την επεξεργασία, υπό τον όρο ότι δεν υπερισχύουν των συμφερόντων ή των θεμελιωδών δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων, λαμβάνοντας υπόψη τις θεμιτές προσδοκίες των υποκειμένων των δεδομένων βάσει της σχέσης τους με τον υπεύθυνο επεξεργασίας. Τέτοιο έννομο συμφέρον θα μπορούσε λόγου χάρη να υπάρχει όταν υφίσταται σχετική και κατάλληλη σχέση μεταξύ του υποκειμένου των δεδομένων και του υπευθύνου επεξεργασίας, όπως αν το υποκείμενο των δεδομένων είναι πελάτης του υπευθύνου επεξεργασίας ή βρίσκεται στην υπηρεσία του. Εν πάση περιπτώσει η ύπαρξη έννομου συμφέροντος θα χρειαζόταν προσεκτική αξιολόγηση, μεταξύ άλλων ως προς το κατά πόσον το υποκείμενο των δεδομένων, κατά τη χρονική στιγμή και στο πλαίσιο της συλλογής των δεδομένων προσωπικού χαρακτήρα, μπορεί εύλογα να αναμένει ότι για τον σκοπό αυτό μπορεί να πραγματοποιηθεί επεξεργασία. Ειδικότερα, τα συμφέροντα και τα θεμελιώδη δικαιώματα του υποκειμένου των δεδομένων θα μπορούσαν να υπερισχύουν των συμφερόντων του υπευθύνου επεξεργασίας, όταν τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία σε περιπτώσεις κατά τις οποίες το υποκείμενο των δεδομένων δεν αναμένει ευλόγως περαιτέρω επεξεργασία των δεδομένων του. Δεδομένου ότι εναπόκειται στον νομοθέτη να παρέχει διά νόμου τη νομική βάση για την επεξεργασία δεδομένων προσωπικού χαρακτήρα από τις δημόσιες αρχές, η εν λόγω νομική βάση δεν θα πρέπει να εφαρμόζεται στην επεξεργασία από τις δημόσιες αρχές κατά την εκπλήρωση των καθηκόντων τους. Η επεξεργασία δεδομένων προσωπικού χαρακτήρα, στον βαθμό που είναι αυστηρά αναγκαία για τους σκοπούς πρόληψης της απάτης, συνιστά επίσης έννομο συμφέρον του ενδιαφερόμενου υπευθύνου επεξεργασίας. Η επεξεργασία δεδομένων

προσωπικού χαρακτήρα για σκοπούς άμεσης εμπορικής προώθησης μπορεί να θεωρηθεί ότι διενεργείται χάριν έννομου συμφέροντος.

Οι υπεύθυνοι επεξεργασίας που είναι μέλη ομίλου επιχειρήσεων ή ιδρυμάτων που συνδέονται με κεντρικό φορέα ενδέχεται να έχουν έννομο συμφέρον να διαβιβάζουν δεδομένα προσωπικού χαρακτήρα εντός του ομίλου επιχειρήσεων για εσωτερικούς διοικητικούς σκοπούς, συμπεριλαμβανομένης της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα πελατών ή εργαζομένων. Οι γενικές αρχές της διαβίβασης δεδομένων προσωπικού χαρακτήρα, εντός ομίλου επιχειρήσεων, προς επιχείρηση εγκατεστημένη σε τρίτη χώρα δεν θίγονται.

5.3.4 Αρχή της αλλαγής του σκοπού επεξεργασίας

Ο Κανονισμός επιτρέπει, πέραν των όσων καθορίζονται παραπάνω την αλλαγή του σκοπού επεξεργασίας, όταν η επεξεργασία γίνεται για σκοπό άλλο από αυτόν για τον οποίο έχουν συλλεγεί τα δεδομένα προσωπικού χαρακτήρα και δεν βασίζεται στη συγκατάθεση του υποκειμένου των δεδομένων[49]. Η αρχή αυτή καθιερώνει αναγκαίο και αναλογικό μέτρο σε μια δημοκρατική κοινωνία ο υπεύθυνος επεξεργασίας, προκειμένου να εξακριβωθεί κατά πόσο η επεξεργασία για άλλο σκοπό είναι συμβατή με τον σκοπό για τον οποίο συλλέγονται αρχικώς τα δεδομένα προσωπικού χαρακτήρα να λαμβάνει υπόψη, μεταξύ άλλων:

α. τυχόν σχέση μεταξύ των σκοπών για τους οποίους έχουν συλλεχθεί τα δεδομένα προσωπικού χαρακτήρα και των σκοπών της επιδιωκόμενης περαιτέρω επεξεργασίας,

β. το πλαίσιο εντός του οποίου συλλέχθηκαν τα δεδομένα προσωπικού χαρακτήρα, ιδίως όσον αφορά τη σχέση μεταξύ των υποκειμένων των δεδομένων και του υπευθύνου επεξεργασίας,

γ. τη φύση των δεδομένων προσωπικού χαρακτήρα, ιδίως για τις ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία, σύμφωνα με το άρθρο 9, ή κατά πόσο δεδομένα προσωπικού χαρακτήρα που σχετίζονται με ποινικές καταδίκες και αδικήματα υποβάλλονται σε επεξεργασία, σύμφωνα με το άρθρο 10,

[49] Βλ. ό.π., Παναγοπούλου-Κουτνατζή Φερενίκη, Ο Γενικός Κανονισμός για την προστασία δεδομένων 679/2016/ΕΕ, Κεφ. VIII, Εκδόσεις Σάκκουλα,2017

δ. τις πιθανές συνέπειες της επιδιωκόμενης περαιτέρω επεξεργασίας για τα υποκείμενα των δεδομένων,

ε. την ύπαρξη κατάλληλων εγγυήσεων, που μπορεί να περιλαμβάνουν κρυπτογράφηση ή ψευδωνυμοποίηση.

5.3.5 Επεξεργασία κατά την άσκηση δημόσιας εξουσίας

Σε αυτήν την περίπτωση, δεν απαιτείται νομική βάση χωριστή από εκείνη που επέτρεψε τη συλλογή των δεδομένων προσωπικού χαρακτήρα. Εάν η επεξεργασία είναι αναγκαία για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας[50], το δίκαιο της Ένωσης ή κράτους μέλους μπορεί να καθορίζει και να προσδιορίζει τα καθήκοντα και τους σκοπούς για τους οποίους πρέπει να θεωρείται συμβατή και σύννομη η περαιτέρω επεξεργασία. Η περαιτέρω επεξεργασία για λόγους αρχειοθέτησης που άπτονται του δημόσιου συμφέροντος, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς θα πρέπει να θεωρείται συμβατή σύννομη πράξη επεξεργασίας. Η νομική βάση που προβλέπεται από το δίκαιο της Ένωσης ή κράτους μέλους για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα μπορεί επίσης να συνιστά τη νομική βάση για την περαιτέρω επεξεργασία. Για να εξακριβωθεί αν ο σκοπός της περαιτέρω επεξεργασίας είναι συμβατός με τον σκοπό της αρχικής συλλογής των δεδομένων προσωπικού χαρακτήρα, ο υπεύθυνος επεξεργασίας, εφόσον πληροί όλες τις απαιτήσεις για τη νομιμότητα της αρχικής επεξεργασίας, θα πρέπει να λάβει υπόψη, μεταξύ άλλων: τυχόν συνδέσμους μεταξύ των σκοπών αυτών και των σκοπών της επιδιωκόμενης περαιτέρω επεξεργασίας, το πλαίσιο στο οποίο έχουν συλλεγεί τα δεδομένα προσωπικού χαρακτήρα, ιδίως τις εύλογες προσδοκίες του υποκειμένου των δεδομένων βάσει της σχέσης του με τον υπεύθυνο επεξεργασίας ως προς την περαιτέρω χρήση τους, τη φύση των δεδομένων προσωπικού χαρακτήρα· τις συνέπειες της επιδιωκόμενης περαιτέρω επεξεργασίας για τα υποκείμενα των δεδομένων και την ύπαρξη κατάλληλων εγγυήσεων τόσο για τις αρχικές όσο και τις σκοπούμενες πράξεις περαιτέρω επεξεργασίας.

[50] Σκέψη 52 Προοιμίου GDPR.

5.3.6 Δικαίωμα προβολής αντιρρήσεων και η αρχή της αναλογικότητας

Όταν το υποκείμενο των δεδομένων παρέσχε τη συναίνεσή του ή η επεξεργασία βασίζεται στο δίκαιο της Ένωσης ή κράτους μέλους που συνιστά αναγκαίο και αναλογικό μέτρο σε μια δημοκρατική κοινωνία για τη διασφάλιση, ειδικότερα, σημαντικών σκοπών στο πλαίσιο γενικού δημόσιου συμφέροντος, θα πρέπει να επιτρέπεται στον υπεύθυνο επεξεργασίας να προβαίνει στην περαιτέρω επεξεργασία των δεδομένων προσωπικού χαρακτήρα, ανεξάρτητα από τη συμβατότητα των σκοπών[51]. Σε κάθε περίπτωση, θα πρέπει να διασφαλίζεται η εφαρμογή των αρχών που καθορίζονται Κανονισμό και, ιδίως, η ενημέρωση του υποκειμένου των δεδομένων σχετικά με τους άλλους αυτούς σκοπούς και σχετικά με τα δικαιώματά του, συμπεριλαμβανομένου του δικαιώματος προβολής αντιρρήσεων και η αρχή της αναλογικότητας[52], προκειμένου να διασφαλισθεί ότι η συγκατάθεση δόθηκε ελεύθερα. Η επισήμανση πιθανών εγκληματικών πράξεων ή απειλών κατά της δημόσιας ασφάλειας από τον υπεύθυνο επεξεργασίας και η διαβίβαση των σχετικών δεδομένων προσωπικού χαρακτήρα σε αρμόδια αρχή σε μία μεμονωμένη υπόθεση ή σε περισσότερες από μία υποθέσεις που αφορούν την ίδια αξιόποινη πράξη ή τις ίδιες απειλές για τη δημόσια ασφάλεια θα πρέπει να θεωρείται ως εμπίπτουσα στο πλαίσιο του θεμιτού συμφέροντος που επιδιώκει ο υπεύθυνος επεξεργασίας. Ωστόσο, η διαβίβαση αυτή στο πλαίσιο του θεμιτού συμφέροντος του υπευθύνου επεξεργασίας ή η περαιτέρω επεξεργασία δεδομένων προσωπικού χαρακτήρα θα πρέπει να απαγορεύεται, εάν η επεξεργασία δεν είναι συμβατή με νομική, επαγγελματική ή άλλη δεσμευτική υποχρέωση τήρησης απορρήτου.

5.3.7 Ειδικά και κατάλληλα μέτρα για την προστασία των θεμελιωδών δικαιωμάτων

Το δίκαιο της Ένωσης ή των κρατών μελών θα πρέπει να προβλέπει ειδικά και κατάλληλα μέτρα για την προστασία των θεμελιωδών δικαιωμάτων και των δεδομένων προσωπικού χαρακτήρα των φυσικών προσώπων. Τα κράτη μέλη θα πρέπει να μπορούν να διατηρούν ή να θεσπίζουν περαιτέρω όρους, μεταξύ άλλων και περιορισμούς, όσον αφορά την επεξεργασία γενετικών δεδομένων, βιομετρικών

[51] Σκέψη 50 Προοιμίου GDPR.

[52] Άρθρο 25 παρ.1 Σ.

δεδομένων ή δεδομένων που αφορούν την υγεία. Ωστόσο, αυτό δεν θα πρέπει να εμποδίζει την ελεύθερη κυκλοφορία δεδομένων προσωπικού χαρακτήρα εντός της Ένωσης, όταν οι όροι αυτοί εφαρμόζονται στη διασυνοριακή επεξεργασία των δεδομένων αυτών. Η επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα μπορεί να είναι απαραίτητη για λόγους δημόσιου συμφέροντος στους τομείς της δημόσιας υγείας, χωρίς τη συναίνεση του υποκειμένου των δεδομένων. Η εν λόγω επεξεργασία θα πρέπει να υπόκειται σε κατάλληλα και ειδικά μέτρα για την προστασία των δικαιωμάτων και ελευθεριών των φυσικών προσώπων. Στο πλαίσιο αυτό, η «δημόσια υγεία» θα πρέπει να ερμηνεύεται ως το σύνολο των στοιχείων που συνδέονται με την υγεία, συγκεκριμένα η κατάσταση της υγείας, περιλαμβανομένων της νοσηρότητας και αναπηρίας, οι καθοριστικοί παράγοντες που επιδρούν στην κατάσταση της υγείας, οι ανάγκες υγειονομικής περίθαλψης, οι πόροι που διατίθενται για την υγειονομική περίθαλψη, η παροχή υγειονομικής περίθαλψης και η πρόσβαση από όλους σε αυτήν, καθώς και οι δαπάνες και η χρηματοδότηση της υγειονομικής περίθαλψης και οι αιτίες θνησιμότητας. Αυτή η επεξεργασία δεδομένων σχετικών με την υγεία για λόγους δημόσιου συμφέροντος δεν θα πρέπει να έχει ως αποτέλεσμα την επεξεργασία δεδομένων προσωπικού χαρακτήρα για άλλους σκοπούς από τρίτους, όπως εργοδότες ή ασφαλιστικές εταιρείες και τράπεζες.

5.4 Οι κατευθυντήριες γραμμές της Ομάδας Εργασίας του Άρθρου 29 (WP29) για τους υπεύθυνους επεξεργασίας

Παράλληλα, η ομάδα εργασίας του άρθρου 29 (εφεξης WP29) εξέδωσε τελικές κατευθυντήριες γραμμές για τους υπεύθυνους επεξεργασίας. Κατά τη σύνοδο ολομέλειας της 5ης Απριλίου, ενέκρινε αναθεωρημένες οδηγίες για την ερμηνεία στοιχείων του γενικού κανονισμού για την προστασία των δεδομένων ("GDPR"). Οι αναθεωρήσεις του σχεδίου καθοδήγησης, το οποίο κυκλοφόρησε αρχικά τον Δεκέμβριο του 2016, ακολούθησαν μια περίοδο ανοιχτής δημόσιας διαβούλευσης που διήρκεσε μέχρι τα τέλη Ιανουαρίου 2017.

Με βάση αυτές, είναι εκ των ων ουκ ανευ απαραίτητο όλοι οι οργανισμοί που με τον έναν ή τον άλλον τρόπο συλλέγουν, αποθηκεύουν και επεξεργάζονται δεδομένα να ακολουθήσουν μία μακρά και μη ξεκάθαρα προσδιορισμένη πορεία προς τη συμμόρφωσή τους με τις διατάξεις του Κανονισμού, η οποία σημειωτέον έχει ως καταληκτική ημερομηνία τις 25 Μαΐου 2018. Στον πυρήνα αυτής της διαδικασίας βρίσκεται ο θεσμός του Υπευθύνου Επεξεργασίας Δεδομένων.

5.4.1 Η συμμόρφωση της προστασίας δεδομένων με το Κανονισμό αποτελεί ευθύνη του υπεύθυνου επεξεργασίας

Ο GDPR καθιστά σαφές ότι ο υπεύθυνος της επεξεργασίας υποχρεούται να εξασφαλίζει και να είναι σε θέση να αποδείξει ότι η επεξεργασία πραγματοποιείται σύμφωνα με τις διατάξεις του, λαμβάνοντας υπόψη 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. Γι΄ αυτό το σκοπό εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα, τα οποία επανεξετάζονται και επικαιροποιούνται όταν κρίνεται απαραίτητο[53]. Η συμμόρφωση της προστασίας δεδομένων με το Κανονισμό αποτελεί ευθύνη του υπεύθυνου επεξεργασίας. Ο υπεύθυνος επεξεργασίας οφείλει να εφαρμόζει μέτρα για να διασφαλίζει ότι, εξ ορισμού, υφίσταται επεξεργασία μόνο για τα δεδομένα προσωπικού χαρακτήρα που είναι απαραίτητα για τον εκάστοτε σκοπό της επεξεργασίας. Αυτή η υποχρεώση ισχύει για το εύρος των δεδομένων προσωπικού χαρακτήρα που συλλέγονται, τον βαθμό της επεξεργασίας τους, την περίοδο

[53] Άρθριο 24 παρ. 1 GDPR.

αποθήκευσης και την προσβασιμότητά τους. Ειδικότερα, τα εν λόγω μέτρα διασφαλίζουν ότι, εξ ορισμού, τα δεδομένα προσωπικού χαρακτήρα δεν καθίστανται προσβάσιμα χωρίς την παρέμβαση του φυσικού προσώπου σε αόριστο αριθμό φυσικών προσώπων. Οι κατευθυντήριες γραμμές παρέχουν επίσης συστάσεις βέλτιστης πρακτικής, αξιοποιώντας την εμπειρία που αποκτήθηκε σε ορισμένα κράτη μέλη της ΕΕ. Η WP29 θα παρακολουθεί την εφαρμογή αυτών των κατευθυντήριων γραμμών και θα μπορεί να τις συμπληρώνει με περαιτέρω λεπτομέρειες, ανάλογα με την περίπτωση.

Ο νέος κανονισμός αφορά οριζόντια κάθε υπεύθυνο επεξεργασίας και, βέβαια, όλες τις επιχειρήσεις που επεξεργάζονται προσωπικά δεδομένα ανεξαρτήτως κλάδου οικονομικής δραστηριότητας και μεγέθους. Ο κανονισμός εφαρμόζεται στις περιπτώσεις που εκτελείται μερική ή ολική, αυτοματοποιημένη ή μη αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα, τα οποία περιλαμβάνονται ή πρόκειται να περιληφθούν σε σύστημα αρχειοθέτησης. Ο νέος κανονισμός αυξάνει σημαντικά τις υποχρεώσεις των επιχειρήσεων αναφορικά με τη διαχείριση των προσωπικών δεδομένων, επομένως και το κόστος επιτήρησης και την αύξηση της γραφειοκρατίας. Σε περιπτώσεις δε μη συμμόρφωσης, το μέγεθος των προβλεπόμενων προστίμων τον τοποθετεί πολύ υψηλά στην καθημερινή ατζέντα της ανώτατης διοίκησης κάθε εταιρείας.

5.4.2 Υπεύθυνοι Επεξεργασίας από κοινού

Στο άρθρο 26 ορίζεται ότι «σε περίπτωση που δύο ή περισσότεροι υπεύθυνοι επεξεργασίας καθορίζουν από κοινού τους σκοπούς και τα μέσα της επεξεργασίας, αποτελούν από κοινού υπευθύνους επεξεργασίας. Αυτοί καθορίζουν με διαφανή τρόπο τις αντίστοιχες ευθύνες τους για συμμόρφωση προς τις υποχρεώσεις που απορρέουν από τον παρόντα κανονισμό, ιδίως όσον αφορά την άσκηση των δικαιωμάτων του υποκειμένου των δεδομένων και τα αντίστοιχα καθήκοντά τους για να παρέχουν τις πληροφορίες που αναφέρονται στα άρθρα 13 και 14, μέσω συμφωνίας μεταξύ τους, εκτός εάν και στον βαθμό που οι αντίστοιχες αρμοδιότητες των υπευθύνων επεξεργασίας καθορίζονται από το δίκαιο της Ένωσης ή το δίκαιο του κράτους μέλους στο οποίο υπόκεινται οι υπεύθυνοι επεξεργασίας. Στη συμφωνία μπορεί να αναφέρεται ένα σημείο επικοινωνίας για τα υποκείμενα των δεδομένων..».Η συμφωνία που αναφέρεται παραπάνω αντανακλά δεόντως τους αντίστοιχους ρόλους και σχέσεις των από κοινού υπευθύνων επεξεργασίας έναντι των υποκειμένων των δεδομένων. Η ουσία της συμφωνίας τίθεται στη διάθεση του υποκειμένου των

δεδομένων. Ανεξάρτητα από τους όρους της συμφωνίας όμως, το υποκείμενο των δεδομένων μπορεί να ασκήσει τα δικαιώματά του δυνάμει του παρόντος κανονισμού έναντι και κατά καθενός από τους υπευθύνους επεξεργασίας. Οι Οδηγίες της WP29 διευκρίνησαν ότι ο υπεύθυνος επεξεργασίας, δεν θα έχει προσωπική ευθύνη, στο πλαίσιο της άσκησης των καθηκόντων του.

Σύμφωνα με τον ορισμό του «υπεύθυνου επεξεργασίας» στην Οδηγία για την προστασία δεδομένων προσωπικού χαρακτήρα, όταν ως υπεύθυνοι επεξεργασίας ενεργούν περισσότερα του ενός αυτοτελή νομικά πρόσωπα, από κοινού μεταξύ τους ή με άλλους, σημαίνει ότι αποφασίζουν από κοινού να επεξεργάζονται δεδομένα για έναν κοινό σκοπό[54]. Από νομικής άποψης, πάντως, αυτό είναι δυνατό μόνο στις περιπτώσεις εκείνες στις οποίες ειδική νομική βάση προβλέπει την από κοινού επεξεργασία των δεδομένων για έναν κοινό σκοπό. Οι διατάξεις δεν αναφέρουν ρητά κατά πόσον απαιτείται ο κοινός σκοπός να είναι ίδιος για κάθε υπεύθυνο επεξεργασίας ή αρκεί να υπάρχει απλώς μερική επικάλυψη των σκοπών. Μέχρι στιγμής, πάντως, δεν υπάρχει συναφής νομολογία σε ευρωπαϊκό επίπεδο ούτε έχουν διευκρινιστεί οι συνέπειες όσον αφορά την αστική ευθύνη. Η WP29 υπεραμύνεται μιας ευρύτερης ερμηνείας της έννοιας των από κοινού υπευθύνων επεξεργασίας, ούτως ώστε να υπάρχει ένα περιθώριο ευελιξίας κατά την αντιμετώπιση της πολυπλοκότητας των τρεχουσών συνθηκών της επεξεργασίας προσωπικών δεδομένων. Η θέση της ομάδας εργασίας αποτυπώνεται με σαφήνεια στην υπόθεση της Εταιρίας Παγκόσμιων Διατραπεζικών Χρηματοπιστωτικών Τηλεπικοινωνιών (SWIFT)[55].

5.4.3 Εκτελών την επεξεργασία

Εκτελών την επεξεργασία βάσει του δικαίου της ΕΕ, είναι το πρόσωπο που επεξεργάζεται τα δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου επεξεργασίας. Οι δραστηριότητες που ανατίθενται στον εκτελούντα την επεξεργασία μπορεί να περιορίζονται σε ένα πολύ συγκεκριμένο καθήκον ή πλαίσιο ή να είναι αρκετά γενικές και εκτενείς. Βάσει του δικαίου του ΣτΕ, η έννοια του εκτελούντα την επεξεργασία είναι ταυτόσημη με αυτήν του ενωσιακού δικαίου. Οι εκτελούντες την επεξεργασία, πέραν της επεξεργασίας δεδομένων που εκτελούν για λογαριασμό

[54] Σκέψη 79 Προοιμίου GDPR.

[55] http://www.kathimerini.gr/60966/article/epikairothta/kosmos/h-ee-diekoye-thn-ereyna-sxetika-me-th-xrhsh-ths-vashs-dedomenwn-swift-gia-kataskopeia

τρίτων, είναι και υπεύθυνοι επεξεργασίας δεδομένων σε σχέση με τις επεξεργασίες που εκτελούν για τους δικούς τους σκοπούς, π.χ. τη διαχείριση των εργαζομένων, των πωλήσεων και των λογιστικών τους.

Όπως είδαμε και στον ορισμό, υπεύθυνος επεξεργασίας είναι το πρόσωπο που καθορίζει τους σκοπούς και τα μέσα της επεξεργασίας. Ακόμη και όταν η αρμοδιότητα καθορισμού των μέσων επεξεργασίας ανατίθεται στον εκτελούντα την επεξεργασία, ο υπεύθυνος επεξεργασίας οφείλει να διατηρεί τη δυνατότητα να παρεμβαίνει στις αποφάσεις του σχετικά με τα μέσα επεξεργασίας. Η γενική ευθύνη συνεχίζει να βαρύνει τον υπεύθυνο επεξεργασίας, ο οποίος οφείλει να ασκεί εποπτεία στους εκτελούντες την επεξεργασία ώστε να διασφαλίζει ότι οι αποφάσεις τους συμμορφώνονται με τους κανόνες για την προστασία των προσωπικών δεδομένων. Ως εκ τούτου, σύμβαση η οποία απαγορεύει στον υπεύθυνο επεξεργασίας να παρεμβαίνει στις αποφάσεις του εκτελούντος την επεξεργασία θα μπορούσε να εκληφθεί ως σύμβαση από κοινού υπευθύνων επεξεργασίας, με τη νομική ευθύνη της επεξεργασίας να βαρύνει αμφότερα τα μέρη.

5.4.4 Ευθύνη προς αποζημίωση στην από κοινού ευθύνη επεξεργασίας

Εξάλλου, εάν ο εκτελών την επεξεργασία δεν τηρεί τους περιορισμούς που έχει θέσει ο υπεύθυνος επεξεργασίας όσον αφορά τη χρήση των δεδομένων, ο εκτελών την επεξεργασία καθίσταται υπεύθυνος επεξεργασίας, τουλάχιστον στο μέτρο που παρέβη τις εντολές του υπευθύνου επεξεργασίας[56]. Η συνέπεια θα είναι, κατά πάσα πιθανότητα, η μετατροπή του εκτελούντος την επεξεργασία σε υπεύθυνο επεξεργασίας ο οποίος ενεργεί παράνομα. Από την άλλη, ο αρχικός υπεύθυνος επεξεργασίας θα κληθεί να δώσει εξηγήσεις για το πώς κατέστη δυνατόν ο εκτελών την επεξεργασία να παραβεί τις εντολές του. Σε τέτοιες περιπτώσεις, μάλιστα, η ομάδα εργασίας του άρθρου 29 συνήθως τεκμαίρει από κοινού ευθύνη επεξεργασίας, δεδομένου ότι έτσι προστατεύονται με τον βέλτιστο δυνατό τρόπο τα συμφέροντα των υποκειμένων των δεδομένων. Μια σημαντική συνέπεια των από κοινού υπευθύνων επεξεργασίας είναι η από κοινού και εις ολόκληρον ευθύνη τους προς αποζημίωση, που παρέχει στα υποκείμενα των δεδομένων ευρύτερο φάσμα ένδικης προστασίας.

Δεν αποκλείεται επίσης να εγείρεται ζήτημα επιμερισμού της ευθύνης, όταν ο υπεύθυνος επεξεργασίας είναι μια μικρή επιχείρηση και ο εκτελών την επεξεργασία

[56] Σκέψη 81 Προοιμίου GDPR.

είναι μια μεγάλη εταιρία μετοχών, ικανή να υπαγορεύει τους όρους με τους οποίους παρέχει τις υπηρεσίες της. Σε μια τέτοια περίπτωση, πάντως, η ομάδα εργασίας του άρθρου 29 υποστηρίζει ότι δεν θα πρέπει να μειώνεται το μέτρο ευθύνης λόγω ανισότητας της οικονομικής ισχύος, αντίθετα θα πρέπει να ισχύει η ίδια αντίληψη για την έννοια του υπευθύνου επεξεργασίας.

Χάριν της σαφήνειας και διαφάνειας, η σχέση μεταξύ υπευθύνου επεξεργασίας και εκτελούντος την επεξεργασία θα πρέπει να αποτυπώνεται λεπτομερώς σε σύμβαση που καταρτίζεται εγγράφως. Η ανυπαρξία έγγραφης σύμβασης συνιστά αθέτηση της υποχρέωσης του υπεύθυνου επεξεργασίας να τεκμηριώνει εγγράφως τις αμοιβαίες υποχρεώσεις και θα μπορούσε να επιφέρει κυρώσεις. Ο εκτελών την επεξεργασία μπορεί να επιθυμεί να αναθέσει ορισμένα καθήκοντα σε τρίτους υπο-εκτελούντες. Αυτό επιτρέπεται από τον νόμο, πλην όμως το πώς θα διευθετηθεί επακριβώς είναι συνάρτηση των συμβατικών όρων που συνομολογήθηκαν ανάμεσα στον υπεύθυνο επεξεργασίας και τον εκτελούντα την επεξεργασία, συμπεριλαμβανομένου του κατά πόσον είναι αναγκαία η έγκριση του υπευθύνου επεξεργασίας σε κάθε περίπτωση ή αρκεί η ενημέρωσή του.

Όταν η επεξεργασία πρόκειται να διενεργηθεί για λογαριασμό υπευθύνου επεξεργασίας, ο υπεύθυνος επεξεργασίας χρησιμοποιεί μόνο εκτελούντες την επεξεργασία που παρέχουν επαρκείς διαβεβαιώσεις για την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων, κατά τρόπο ώστε η επεξεργασία να πληροί τις απαιτήσεις του Κανονισμού και να διασφαλίζεται η προστασία των δικαιωμάτων του υποκειμένου των δεδομένων[57]. Ο εκτελών την επεξεργασία δεν προσλαμβάνει άλλον εκτελούντα την επεξεργασία χωρίς προηγούμενη ειδική ή γενική γραπτή άδεια του υπευθύνου επεξεργασίας. Σε περίπτωση γενικής γραπτής άδειας, ο εκτελών την επεξεργασία ενημερώνει τον υπεύθυνο επεξεργασίας για τυχόν σκοπούμενες αλλαγές που αφορούν την προσθήκη ή την αντικατάσταση των άλλων εκτελούντων την επεξεργασία, παρέχοντας με τον τρόπο αυτό τη δυνατότητα στον υπεύθυνο επεξεργασίας να αντιταχθεί σε αυτές τις αλλαγές[58]. Η επεξεργασία από τον εκτελούντα την επεξεργασία διέπεται από σύμβαση ή άλλη νομική πράξη υπαγόμενη στο δίκαιο της Ένωσης ή του κράτους μέλους, που δεσμεύει τον εκτελούντα την επεξεργασία σε σχέση με τον υπεύθυνο επεξεργασίας και καθορίζει το αντικείμενο και τη διάρκεια της επεξεργασίας, τη φύση και τον σκοπό της επεξεργασίας, το είδος των δεδομένων προσωπικού χαρακτήρα και τις κατηγορίες των υποκειμένων των δεδομένων και τις

[57] Άρθρο 28 παρ.1 GDPR.

[58] Άρθρο 28 παρ.2 GDPR.

υποχρεώσεις και τα δικαιώματα του υπευθύνου επεξεργασίας[59]. Η εν λόγω σύμβαση ή άλλη νομική πράξη προβλέπει ειδικότερα ότι ο εκτελών την επεξεργασία επεξεργάζεται τα δεδομένα προσωπικού χαρακτήρα μόνο βάσει καταγεγραμμένων εντολών του υπευθύνου επεξεργασίας, μεταξύ άλλων όσον αφορά τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτη χώρα ή διεθνή οργανισμό, διασφαλίζει ότι τα πρόσωπα που είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα έχουν αναλάβει δέσμευση τήρησης εμπιστευτικότητας ή τελούν υπό τη δέουσα κανονιστική υποχρέωση τήρησης εμπιστευτικότητας. Λαμβάνει όλα τα απαιτούμενα μέτρα, κατ' επιλογή του υπευθύνου επεξεργασίας, διαγράφει ή επιστρέφει όλα τα δεδομένα προσωπικού χαρακτήρα στον υπεύθυνο επεξεργασίας μετά το πέρας της παροχής υπηρεσιών επεξεργασίας και διαγράφει τα υφιστάμενα αντίγραφα, εκτός εάν το δίκαιο της Ένωσης ή του κράτους μέλους απαιτεί την αποθήκευση των δεδομένων προσωπικού χαρακτήρα, θέτει στη διάθεση του υπευθύνου επεξεργασίας κάθε απαραίτητη πληροφορία προς απόδειξη της συμμόρφωσης προς τις υποχρεώσεις που θεσπίζονται στο παρόν άρθρο και επιτρέπει και διευκολύνει τους ελέγχους, περιλαμβανομένων των επιθεωρήσεων, που διενεργούνται από τον υπεύθυνο επεξεργασίας ή από άλλον ελεγκτή εντεταλμένο από τον υπεύθυνο επεξεργασίας, ενημερώνει αμέσως τον υπεύθυνο επεξεργασίας, εάν, κατά την άποψή του, κάποια εντολή παραβιάζει τον παρόντα κανονισμό ή άλλες ενωσιακές ή εθνικές διατάξεις περί προστασίας δεδομένων.

Όταν ο εκτελών την επεξεργασία προσλαμβάνει άλλον εκτελούντα για τη διενέργεια συγκεκριμένων δραστηριοτήτων επεξεργασίας για λογαριασμό του υπευθύνου επεξεργασίας, οι ίδιες υποχρεώσεις όσον αφορά την προστασία των δεδομένων που προβλέπονται στη σύμβαση ή στην άλλη νομική πράξη μεταξύ υπευθύνου επεξεργασίας και εκτελούντος την επεξεργασία, επιβάλλονται στον άλλον αυτόν εκτελούντα μέσω σύμβασης ή άλλης νομικής πράξης σύμφωνα με το δίκαιο της Ένωσης ή του κράτους μέλους, ιδίως ώστε να παρέχονται επαρκείς διαβεβαιώσεις για την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων, ούτως ώστε η επεξεργασία να πληροί τις απαιτήσεις του Κανονισμού. Όταν ο άλλος εκτελών την επεξεργασία αδυνατεί να ανταποκριθεί στις σχετικές με την προστασία των δεδομένων υποχρεώσεις του, ο αρχικός εκτελών παραμένει πλήρως υπόλογος έναντι του υπευθύνου επεξεργασίας για την εκπλήρωση των υποχρεώσεων του άλλου εκτελούντος την επεξεργασία[60]. Η τήρηση εκ μέρους του εκτελούντος την επεξεργασία

[59] Άρθρο 28 παρ.3 GDPR.

[60] Άρθρο 28 παρ.4 GDPR.

εγκεκριμένου κώδικα δεοντολογίας όπως αναφέρεται στο άρθρο 40 ή εγκεκριμένου μηχανισμού πιστοποίησης όπως αναφέρεται στο άρθρο 42 δύναται να χρησιμοποιηθεί ως στοιχείο για να αποδειχθεί ότι παρέχει επαρκείς διαβεβαιώσεις. Η σύμβαση ή η άλλη νομική πράξη που αναφέρεται στις παραγράφους μπορεί να βασίζεται, εν όλω ή εν μέρει, σε τυποποιημένες συμβατικές ρήτρες, μεταξύ άλλων όταν αποτελούν μέρος πιστοποίησης που χορηγείται στον υπεύθυνο επεξεργασίας ή στον εκτελούντα την επεξεργασία σύμφωνα με τα άρθρα 42 και 43. Η Επιτροπή μπορεί να θεσπίσει τυποποιημένες συμβατικές ρήτρες για τα θέματα αυτά και σύμφωνα με τη διαδικασία εξέτασης που αναφέρεται στο άρθρο 93 παράγραφος 2. Η σύμβαση ή η άλλη νομική πράξη υφίσταται γραπτώς, μεταξύ άλλων σε ηλεκτρονική μορφή. Εάν ο εκτελών την επεξεργασία καθορίσει κατά παράβαση του παρόντος κανονισμού τους σκοπούς και τα μέσα της επεξεργασίας, ο εκτελών την επεξεργασία θεωρείται υπεύθυνος επεξεργασίας για τη συγκεκριμένη επεξεργασία.

5.4.5 Υποχρέωση τήρησης αρχείου των δραστηριοτήτων επεξεργασίας και ασφάλεια αυτής

Κάθε υπεύθυνος επεξεργασίας και, κατά περίπτωση, ο εκπρόσωπός του, τηρεί αρχείο των δραστηριοτήτων επεξεργασίας για τις οποίες είναι υπεύθυνος[61]. Το εν λόγω αρχείο περιλαμβάνει όλες τις ακόλουθες πληροφορίες:

α. το όνομα και τα στοιχεία επικοινωνίας του υπευθύνου επεξεργασίας και, κατά περίπτωση, του από κοινού υπευθύνου επεξεργασίας, του εκπροσώπου του υπευθύνου επεξεργασίας και του υπευθύνου προστασίας δεδομένων,

β. τους σκοπούς της επεξεργασίας,

γ. περιγραφή των κατηγοριών υποκειμένων των δεδομένων και των κατηγοριών δεδομένων προσωπικού χαρακτήρα,

δ. τις κατηγορίες αποδεκτών στους οποίους πρόκειται να γνωστοποιηθούν ή γνωστοποιήθηκαν τα δεδομένα προσωπικού χαρακτήρα, περιλαμβανομένων των αποδεκτών σε τρίτες χώρες ή διεθνείς οργανισμούς,

ε. όπου συντρέχει περίπτωση, τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα σε τρίτη χώρα ή διεθνή οργανισμό, συμπεριλαμβανομένων του προσδιορισμού της εν λόγω τρίτης χώρας ή του διεθνούς οργανισμού,

[61] Άρθρο 30 GDPR.

στ. όπου είναι δυνατό, τις προβλεπόμενες προθεσμίες διαγραφής των διάφορων κατηγοριών δεδομένων,

ζ. όπου είναι δυνατό, γενική περιγραφή των τεχνικών και οργανωτικών μέτρων ασφάλειας που αναφέρονται παραπάνω.

Κάθε εκτελών την επεξεργασία και, κατά περίπτωση, ο εκπρόσωπος του εκτελούντος την επεξεργασία τηρούν αντίστοιχο αρχείο όλων των κατηγοριών δραστηριοτήτων επεξεργασίας που διεξάγονται εκ μέρους του υπευθύνου επεξεργασίας, όπως παραπάνω, το οποίο τηρείται και σε ηλεκτρονική μορφή. Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία και, κατά περίπτωση, οι εκπρόσωποί τους συνεργάζονται, κατόπιν αιτήματος, με την εποπτική αρχή για την άσκηση των καθηκόντων της, στη διάθεση της οποίας θέτουν το παραπάνω αρχείο κατόπιν αιτήματος. Οι υποχρεώσεις αυτές δεν ισχύουν για επιχείρηση ή οργανισμό που απασχολεί λιγότερα από 250 άτομα, εκτός εάν η διενεργούμενη επεξεργασία ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων, η επεξεργασία δεν είναι περιστασιακή ή η επεξεργασία περιλαμβάνει ειδικές κατηγορίες δεδομένων ή επεξεργασία αφορά δεδομένα προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες.

Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία οφείλουν κατά την επξεργασία να εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων, περιλαμβανομένων, μεταξύ άλλων, κατά περίπτωση: της ψευδωνυμοποίησης και της κρυπτογράφησης δεδομένων προσωπικού χαρακτήρα, της δυνατότητας διασφάλισης του απορρήτου, της ακεραιότητας, της διαθεσιμότητας και της αξιοπιστίας των συστημάτων και των υπηρεσιών επεξεργασίας σε συνεχή βάση, της δυνατότητας αποκατάστασης της διαθεσιμότητας και της πρόσβασης σε δεδομένα προσωπικού χαρακτήρα σε εύθετο χρόνο σε περίπτωση φυσικού ή τεχνικού συμβάντος, διαδικασίας για την τακτική δοκιμή, εκτίμηση και αξιολόγηση της αποτελεσματικότητας των τεχνικών και των οργανωτικών μέτρων για τη διασφάλιση της ασφάλειας της επεξεργασίας[62]. Τέλος, σύμφωνα με το άρθρο 31, κατά περίπτωση ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία και, κατά περίπτωση, οι εκπρόσωποί τους συνεργάζονται, κατόπιν αιτήματος, με την εποπτική αρχή για την άσκηση των καθηκόντων της.

[62] Άρθρο 32 GDPR.

5.4.6 Παραβίαση δεδομένων προσωπικού χαρακτήρα

Σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα, ο υπεύθυνος επεξεργασίας, με βάση το άρθρο 33, γνωστοποιεί αμελλητί και, αν είναι δυνατό, εντός 72 ωρών από τη στιγμή που αποκτά γνώση του γεγονότος της παραβίασης των δεδομένων προσωπικού χαρακτήρα από την ανακάλυψη του περιστατικού παραβίασης και απώλειας προσωπικών δεδομένων στις αρμόδιες εποπτικές αρχές και στα υποκείμενα των δεδομένων, αν η φύση των δεδομένων που χάθηκαν το απαιτεί, εκτός εάν η παραβίαση δεδομένων προσωπικού χαρακτήρα δεν ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων[63]. Όταν η γνωστοποίηση στην εποπτική αρχή δεν πραγματοποιείται εντός 72 ωρών, συνοδεύεται από αιτιολόγηση για την καθυστέρηση. Για τους υπεύθυνους επεξεργασίας ή τους εκτελούντες την επεξεργασία δεδομένων οι οποίοι παραβιάζουν τους κανόνες για την προστασία των δεδομένων προβλέπονται πολύ αυστηρές κυρώσεις, όπως ορίζει το άρθρο 83 του Κανονισμού. Μπορεί να επιβληθεί πρόστιμο που είναι δυνατό να ανέλθει σε 20 εκατομμύρια ευρώ ή στο 4% του συνολικού ετήσιου κύκλου εργασιών τους. Για την επιβολή διοικητικού προστίμου, καθώς και σχετικά με το ύψος του διοικητικού προστίμου για κάθε μεμονωμένη περίπτωση, λαμβάνονται υπόψη ενδεικτικά τα ακόλουθα:

α. η φύση, η βαρύτητα και η διάρκεια της παράβασης, λαμβάνοντας υπόψη τη φύση, την έκταση ή το σκοπό της σχετικής επεξεργασίας, καθώς και τον αριθμό των υποκειμένων των δεδομένων που έθιξε η παράβαση και το βαθμό ζημίας που υπέστησαν,

β. ο δόλος ή η αμέλεια που προκάλεσε την παράβαση,

γ. οποιεσδήποτε ενέργειες στις οποίες προέβη ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία για να μετριάσει τη ζημία που υπέστησαν τα υποκείμενα των δεδομένων,

δ. ο βαθμός ευθύνης του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, λαμβάνοντας υπόψη τα τεχνικά και οργανωτικά μέτρα που εφαρμόζουν,

ε. τυχόν σχετικές προηγούμενες παραβάσεις του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία,

---

[63] Βλ. Γιαννόπουλο Γεώργιο, Γενικός Κανονισμός Προστασίας Δεδομένων:οι νέες ευθύνες και υποχρεώσεις του υπεύθυνου επεξεργασίας,Εφημ ΔΔ 2017, σελ 199 επ.

στ. ο βαθμός συνεργασίας με την αρχή ελέγχου για την επανόρθωση της παράβασης και τον περιορισμό των πιθανών δυσμενών επιπτώσεών της,

ζ. οι κατηγορίες δεδομένων προσωπικού χαρακτήρα που επηρεάζει η παράβαση,

η. ο τρόπος με τον οποίο η εποπτική αρχή πληροφορήθηκε την παράβαση, ειδικότερα εάν και κατά πόσο ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία κοινοποίησε την παράβαση,

θ. σε περίπτωση που διατάχθηκε προηγουμένως η λήψη των μέτρων που αναφέρονται κατά του εμπλεκόμενου υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία σχετικά με το ίδιο αντικείμενο, η συμμόρφωση με τα εν λόγω μέτρα,

ι. η τήρηση εγκεκριμένων κωδίκων δεοντολογίας ή εγκεκριμένων μηχανισμών πιστοποίησης σύμφωνα και

ια. κάθε άλλο επιβαρυντικό ή ελαφρυντικό στοιχείο που προκύπτει από τις περιστάσεις της συγκεκριμένης περίπτωσης, όπως τα οικονομικά οφέλη που αποκομίστηκαν ή ζημιών που αποφεύχθηκαν, άμεσα ή έμμεσα, από την παράβαση.

Όταν ένα είδος επεξεργασίας, ιδίως με χρήση νέων τεχνολογιών και συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας διενεργεί, πριν από την επεξεργασία, εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα. Σε μία εκτίμηση μπορεί να εξετάζεται ένα σύνολο παρόμοιων πράξεων επεξεργασίας οι οποίες ενέχουν παρόμοιους υψηλούς κινδύνους[64]. Η εκτίμηση περιέχει τουλάχιστον συστηματική περιγραφή των προβλεπόμενων πράξεων επεξεργασίας και των σκοπών της επεξεργασίας, περιλαμβανομένου, κατά περίπτωση, του έννομου συμφέροντος που επιδιώκει ο υπεύθυνος επεξεργασίας, εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας σε συνάρτηση με τους σκοπούς, εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων και τα προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων, περιλαμβανομένων των εγγυήσεων, των μέτρων και μηχανισμών ασφάλειας, ώστε να διασφαλίζεται η προστασία των δεδομένων προσωπικού χαρακτήρα και να αποδεικνύεται η συμμόρφωση προς τον παρόντα κανονισμό, λαμβάνοντας υπόψη τα δικαιώματα και

[64] Άρθρο 35 GDPR.

τα έννομα συμφέροντα των υποκειμένων των δεδομένων και άλλων ενδιαφερόμενων προσώπων.

5.4.7 Κώδικας δεοντολογίας

Στο άρθρο 40, που αναφέρθηκε παραπάνω, προβλέπεται η τήρηση ενός αυστηρού κώδικα δεοντολογίας. Πιο συγκεκριμένα ορίζεται ότι «...1.Τα κράτη μέλη, οι εποπτικές αρχές, το Συμβούλιο Προστασίας Δεδομένων και η Επιτροπή ενθαρρύνουν την εκπόνηση κωδίκων δεοντολογίας που έχουν ως στόχο να συμβάλουν στην ορθή εφαρμογή του παρόντος κανονισμού, λαμβάνοντας υπόψη τα ειδικά χαρακτηριστικά των διάφορων τομέων επεξεργασίας και τις ειδικές ανάγκες των πολύ μικρών, των μικρών και των μεσαίων επιχειρήσεων. 2.Ενώσεις και άλλοι φορείς που εκπροσωπούν κατηγορίες υπευθύνων επεξεργασίας ή εκτελούντων την επεξεργασία μπορούν να εκπονούν κώδικες δεοντολογίας ή να τροποποιούν ή να επεκτείνουν υφιστάμενους κώδικες δεοντολογίας, προκειμένου να προσδιορίσουν την εφαρμογή του παρόντος κανονισμού, όπως όσον αφορά:

α. τη θεμιτή και με διαφάνεια επεξεργασία,

β. τα έννομα συμφέροντα που επιδιώκουν οι υπεύθυνοι επεξεργασίας σε συγκεκριμένα πλαίσια,

γ. τη συλλογή δεδομένων προσωπικού χαρακτήρα,

δ. την ψευδωνυμοποίηση δεδομένων προσωπικού χαρακτήρα,

ε. την ενημέρωση του κοινού και των υποκειμένων των δεδομένων,

στ. την άσκηση των δικαιωμάτων των υποκειμένων των δεδομένων,

ζ. την ενημέρωση και την προστασία των παιδιών και τον τρόπο απόκτησης της συγκατάθεσης του ασκούντος τη γονική μέριμνα του παιδιού,

η. τα μέτρα και τις διαδικασίες που αναφέρονται στα άρθρα 24 και 25 και τα μέτρα για τη διασφάλιση της ασφάλειας της επεξεργασίας που αναφέρεται στο άρθρο 32 του Κανονισμού,

θ. τη γνωστοποίηση παραβιάσεων δεδομένων προσωπικού χαρακτήρα στις εποπτικές αρχές και την ανακοίνωση των εν λόγω παραβιάσεων δεδομένων προσωπικού χαρακτήρα στα υποκείμενα των δεδομένων,

ι. τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες ή διεθνείς οργανισμούς, ή

ια.εξωδικαστικές διαδικασίες και άλλες διαδικασίες επίλυσης διαφορών για την επίλυση διαφορών μεταξύ υπευθύνων επεξεργασίας και υποκειμένων των δεδομένων όσον αφορά την επεξεργασία, με την επιφύλαξη των δικαιωμάτων των υποκειμένων των δεδομένων δυνάμει των άρθρων 77 και 79 του Κανονισμού».

Η τήρηση των κώδικων δεοντολογίας από υπεύθυνους επεξεργασίας ή εκτελούντες την επεξεργασία υπαγόμενους στον κανονισμό έχουν γενική ισχύ βάσει της παραγράφου, μπορούν επίσης να τηρούνται από υπευθύνους επεξεργασίας ή εκτελούντες την επεξεργασία μη υπαγόμενους στον παρόντα κανονισμό σύμφωνα με το άρθρο 3, προκειμένου να παρέχονται οι κατάλληλες εγγυήσεις στο πλαίσιο των διαβιβάσεων δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες ή διεθνείς οργανισμούς. Οι εν λόγω υπεύθυνοι επεξεργασίας ή εκτελούντες την επεξεργασία αναλαμβάνουν δεσμευτικές και εκτελεστές υποχρεώσεις μέσω συμβάσεων ή άλλων νομικά δεσμευτικών πράξεων, προκειμένου να εφαρμόσουν τις εν λόγω κατάλληλες εγγυήσεις, μεταξύ άλλων όσον αφορά τα δικαιώματα των υποκειμένων των δεδομένων. Ο παραπάνω περιγραφόμενος κώδικας δεοντολογίας περιέχει μηχανισμούς που επιτρέπουν στον εκάστοτε φορέα να διενεργεί την υποχρεωτική παρακολούθηση της συμμόρφωσης προς τις διατάξεις του από τους υπευθύνους επεξεργασίας ή τους εκτελούντες την επεξεργασία που έχουν αναλάβει να τον εφαρμόζουν. Ενώσεις και άλλοι φορείς που αναφέρονται στην παράγραφο 2 άρθρου 40 και προτίθενται να εκπονήσουν κώδικα δεοντολογίας ή να τροποποιήσουν ή να επεκτείνουν υφιστάμενο κώδικα υποβάλλουν το σχέδιο κώδικα στην εποπτική αρχή που είναι αρμόδια. Η εποπτική αρχή γνωμοδοτεί ως προς τη συμμόρφωση του σχεδίου κώδικα, της τροποποίησης ή της επέκτασης προς τον παρόντα κανονισμό και εγκρίνει το εν λόγω σχέδιο κώδικα, τροποποίηση ή επέκταση, εάν κρίνει ότι παρέχει επαρκείς κατάλληλες εγγυήσεις. Σε περίπτωση που σχέδιο κώδικα δεοντολογίας αναφέρεται σε δραστηριότητες επεξεργασίας σε διάφορα κράτη μέλη, η εποπτική αρχή που είναι αρμόδια το υποβάλλει, πριν από την έγκριση του σχεδίου κώδικα, της τροποποίησης ή της επέκτασης, με βάση τη διαδικασία που προβλέπεται στο Συμβούλιο Προστασίας Δεδομένων, το οποίο γνωμοδοτεί ως προς τη συμμόρφωση του σχεδίου κώδικα, της τροποποίησης ή της επέκτασης προς τον παρόντα κανονισμό.Σε περίπτωση που η γνωμοδότηση επιβεβαιώνει ότι ο κώδικας, η τροποποίηση ή η επέκταση του είναι σύμφωνα προς τον παρόντα κανονισμό το Συμβούλιο Προστασίας Δεδομένων [65]

[65] Άρθρο 68 GDPR.

διαβιβάζει τη γνώμη του στην Επιτροπή, η οποία μπορεί, μέσω εκτελεστικών πράξεων, να αποφασίζει ότι οι εγκεκριμένοι κώδικες δεοντολογίας και οι τροποποιήσεις ή οι επεκτάσεις που της υποβλήθηκαν δυνάμει της παραγράφου 8 του ιδίου άρθρου έχουν γενική ισχύ εντός της Ένωσης.

5.4.8 Μηχανισμοί πιστοποίησης προστασίας δεδομένων

Επιπλέον διασφάλιση για την προστασία προσωπικών δεδομένων παρέχει το άρθρο 42 που ορίζει ότι τα κράτη μέλη, οι εποπτικές αρχές, το Συμβούλιο Προστασίας Δεδομένων και η Επιτροπή παροτρύνουν, ιδίως σε ενωσιακό επίπεδο, τη θέσπιση μηχανισμών πιστοποίησης προστασίας δεδομένων και σφραγίδων και σημάτων προστασίας δεδομένων, με σκοπό την απόδειξη της συμμόρφωσης προς τον παρόντα κανονισμό των πράξεων επεξεργασίας από τους υπευθύνους επεξεργασίας και τους εκτελούντες την επεξεργασία. Πέραν της εφαρμογής τους από τους υπευθύνους επεξεργασίας ή τους εκτελούντες την επεξεργασία που υπόκεινται στον παρόντα κανονισμό, οι μηχανισμοί πιστοποίησης της προστασίας δεδομένων και οι σφραγίδες και τα σήματα προστασίας δεδομένων μπορούν να θεσπίζονται για τον σκοπό της απόδειξης ότι παρέχονται κατάλληλες εγγυήσεις από τους υπευθύνους επεξεργασίας ή τους εκτελούντες την επεξεργασία που δεν υπόκεινται στον παρόντα κανονισμό, στο πλαίσιο των διαβιβάσεων δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες ή διεθνείς οργανισμούς. [66] Οι εν λόγω υπεύθυνοι επεξεργασίας ή εκτελούντες την επεξεργασία αναλαμβάνουν δεσμευτικές και εκτελεστές υποχρεώσεις μέσω συμβάσεων ή άλλων νομικά δεσμευτικών πράξεων, προκειμένου να εφαρμόσουν τις εν λόγω κατάλληλες εγγυήσεις, μεταξύ άλλων όσον αφορά τα δικαιώματα των υποκειμένων των δεδομένων. Η πιστοποίηση είναι εθελοντική και διαθέσιμη μέσω διαφανούς διαδικασίας, δεν περιορίζει την ευθύνη του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία για συμμόρφωση προς τον παρόντα κανονισμό και δεν θίγει τα καθήκοντα και τις αρμοδιότητες των εποπτικών αρχών που είναι αρμόδιες.

[66] Σύμφωνα με τους όρους που αναφέρονται στο άρθρο 46 παράγραφος 2 στοιχείο στ. του GDPR.

5.4.9 Δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή και δικαστικής προσφυγής

Δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή, σύμφωνα με το άρθρο 77 του Κανονισμού, με την επιφύλαξη τυχόν άλλων διοικητικών ή δικαστικών προσφυγών, έχει κάθε υποκείμενο των δεδομένων ιδίως στο κράτος μέλος στο οποίο έχει τη συνήθη διαμονή του ή τον τόπο εργασίας του ή τον τόπο της εικαζόμενης παράβασης, εάν το υποκείμενο των δεδομένων θεωρεί ότι η επεξεργασία των δεδομένων προσωπικού χαρακτήρα που το αφορά παραβαίνει τον Κανονισμό. Η εποπτική αρχή στην οποία έχει υποβληθεί καταγγελία ενημερώνει τον καταγγέλλοντα για την πρόοδο και για την έκβαση της καταγγελίας, καθώς και για τη δυνατότητα άσκησης δικαστικής προσφυγής σύμφωνα με το άρθρο 78. Δικαίωμα πραγματικής δικαστικής προσφυγής κατά υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία προβλέπεται στο άρθρο 79, με την επιφύλαξη κάθε διαθέσιμης διοικητικής ή μη δικαστικής προσφυγής, συμπεριλαμβανομένου του δικαιώματος υποβολής της παραπάμω καταγγελίας, για έκαστο υποκείμενο των δεδομένων εάν θεωρεί ότι τα δικαιώματά του που απορρέουν από τον Κανονισμό παραβιάστηκαν ως αποτέλεσμα της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα του που το αφορούν κατά παράβαση του παρόντος κανονισμού. Η διαδικασία κατά υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία κινείται ενώπιον των δικαστηρίων του κράτους μέλους στο οποίο ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία έχουν εγκατάσταση. Εναλλακτικά, η εν λόγω διαδικασία μπορεί να κινηθεί ενώπιον των δικαστηρίων του κράτους μέλους στο οποίο το υποκείμενο των δεδομένων έχει τη συνήθη διαμονή του, εκτός εάν ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία είναι δημόσια αρχή κράτους μέλους η οποία ενεργεί κατά την άσκηση των δημόσιων εξουσιών της.

Κάθε πρόσωπο το οποίο υπέστη υλική ή μη υλική ζημία ως αποτέλεσμα παραβίασης του Γενικού Κανονισμού δικαιούται αποζημίωση από τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία για τη ζημία που υπέστη κατά το άρθρο 82[67]. Κάθε υπεύθυνος επεξεργασίας που συμμετέχει στην επεξεργασία είναι υπεύθυνος για τη ζημία που προκάλεσε η εκ μέρους του επεξεργασία που παραβαίνει τον παρόντα κανονισμό. Ο εκτελών την επεξεργασία ευθύνεται για τη ζημία που προκάλεσε η επεξεργασία μόνο εφόσον δεν ανταποκρίθηκε στις υποχρεώσεις του παρόντος κανονισμού που αφορούν ειδικότερα τους εκτελούντες την επεξεργασία ή υπερέβη ή ενήργησε αντίθετα προς τις νόμιμες εντολές του υπευθύνου επεξεργασίας. Ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία απαλλάσσεται από την ευθύνη

[67] Σκέψη 144 Προοιμίου GDPR.

που έχουν εάν αποδεικνύει ότι δεν φέρει καμία ευθύνη για το γενεσιουργό γεγονός της ζημίας. Εάν περισσότεροι του ενός υπεύθυνοι επεξεργασίας ή εκτελούντες την επεξεργασία ή αμφότεροι ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία εμπλέκονται στην ίδια επεξεργασία και είναι υπεύθυνοι για τυχόν ζημία που προκάλεσε η επεξεργασία, κάθε υπεύθυνος επεξεργασίας ή εκτελών την επεξεργασία ευθύνεται για τη συνολική ζημία, προκειμένου να διασφαλιστεί αποτελεσματική αποζημίωση του υποκειμένου των δεδομένων. Εάν ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία έχει καταβάλει, σύμφωνα με την παράγραφο 4 του άρθρου 82, πλήρη αποζημίωση για τη ζημία που προκάλεσε, ο εν λόγω υπεύθυνος ή εκτελών την επεξεργασία δικαιούται να ζητήσει από τους άλλους υπευθύνους επεξεργασίας ή εκτελούντες την επεξεργασία που εμπλέκονται στην ίδια επεξεργασία την ανάκτηση μέρους της αποζημίωσης που αντιστοιχεί στο μέρος της ευθύνης τους λόγω της ζημίας που προκλήθηκε.

Τα κράτη μέλη μπορούν να θεσπίζουν ειδικούς κανόνες για τον καθορισμό των εξουσιών των ελεγκτικών αρχών σε σχέση με υπευθύνους επεξεργασίας ή εκτελούντες την επεξεργασία οι οποίοι υπέχουν, βάσει του δικαίου της Ένωσης ή κράτους μέλους ή των κανόνων που θεσπίζονται από αρμόδιους εθνικούς φορείς, υποχρέωση τήρησης του επαγγελματικού απορρήτου ή άλλες αντίστοιχες υποχρεώσεις τήρησης του απορρήτου, εάν αυτό είναι αναγκαίο και αναλογικό, προκειμένου να συμβιβαστεί το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα με την υποχρέωση τήρησης του απορρήτου. Οι εν λόγω κανόνες εφαρμόζονται μόνο σε σχέση με δεδομένα προσωπικού χαρακτήρα τα οποία ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία έλαβαν ή εξασφάλισαν στο πλαίσιο δραστηριότητας που καλύπτεται από την εν λόγω υποχρέωση απορρήτου σύμφωνα με το άρθρο 90 του Κανονισμού.

5.5 Υποχρεωτικός ο διορισμός του Υπεύθυνου Προστασίας Δεδομένων (DPO)

Σπουδαίος συμπαραστάτης του υπεύθυνου επεξεργασίας καθίσταται με βάση τον Κανονισμό ο Υπεύθυνος Προστασίας Δεδομένων (DPO) [68] . Το άρθρο 37 του Κανονισμού ορίζει το θεσμό του υπεύθυνου προστασίας δεδομένων ως υποχρεωτικό σε τρεις περιπτώσεις, όταν:

α. η επεξεργασία διενεργείται από δημόσια αρχή ή φορέα, εκτός από δικαστήρια που ενεργούν στο πλαίσιο της δικαιοδοτικής τους αρμοδιότητας,

β. οι βασικές δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν πράξεις επεξεργασίας οι οποίες, λόγω της φύσης, του πεδίου εφαρμογής και/ή των σκοπών τους, απαιτούν τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε μεγάλη κλίμακα, ή οι βασικές δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα κατά το άρθρο 9 και δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα που αναφέρονται στο άρθρο 10 και

γ. ο νόμος ενός κράτους μέλους απαιτεί διορισμό ενός DPO (πιθανό σε χώρες όπως η Γερμανία).

Είναι φανερό ότι στις παραπάνω περιπτώσεις απαιτείται περαιτέρω εξειδίκευση των διαφόρων εννοιών, δεδομένου ότι ούτε στον Κανονισμό υπάρχουν σαφείς επεξηγήσεις, ούτε υπάρχει σχετικό νομικό ή/και πρακτικό προηγούμενο. Η έννοια πχ του δημόσιου φορέα εξαρτάται από το αντικείμενο δράσης ενός οργανισμού. Για παράδειγμα, ένα ΝΠΙΔ που σχετίζεται με τα ΜΜΜ, τις δημόσιες οδικές υποδομές ή τις δημόσιες υπηρεσίες ύδρευσης ή παροχής ενέργειας, θα μπορούσε να θεωρηθεί δημόσιος φορέας. Ομοίως, τα κριτήρια της ‘τακτικής’, ‘συστηματικής’, ‘μεγάλης κλίμακας’, τα οποία αφορούν στη νομικά εμποτισμένη πράξη της επεξεργασίας χρίζουν βαθιάς μελέτης και κατανόησης, προκειμένου να μην υπάρξουν αστοχίες στη διάγνωση, που οι δημόσιοι και ιδιωτικοί οργανισμοί θα υποχρεωθούν να κάνουν σχετικά με την ανάγκη

[68] Βλ. Λαζαράκο Γρηγόριο, Ο θεσμός του υπεύθυνου προστασίας προσωπικών δεδομένων (DPO) στο νέο νομοθετικό πλαίσιο των προσωπικών δεδομένων μετά την υιοθέτηση του Κανονισμού ΕΕ/679/2016, Εφαρμογές Δημοσίου Δικαίου 2016, σελ. 243 επ.

ορισμού DPO[69]. Διότι το γεγονός ότι ένας οργανισμός δεν εμπίπτει στις περιπτώσεις του άρθρου 37 του Κανονισμού δε σημαίνει ότι δεν υποχρεούται να συμμορφωθεί με τις διατάξεις του. Και η συμμόρφωση αυτή αποτελεί μία πολύπλοκη, πολυεπίπεδη και διατομεακή διαδικασία, που περιλαμβάνει πολλά στάδια, όπως ταξινόμηση δεδομένων, καταγεγραμμένες διαδικασίες συλλογής, ταξινόμησης, αποθήκευσης, μεταβίβασης και διαμοιρασμού δεδομένων, εκθέσεις αποτίμησης κινδύνου, διαδικασίες αντιμετώπισης κινδύνων, άλλως παραβιάσεων, προστασία της ιδιωτικότητας εξ'ορισμού και από το σχεδιασμό (Privacy by Design / Privacy by Default) κτλ. Η σχετική πρόβλεψη υπάρχει ρητώς στα άρθρα 37-39 του Κανονισμού, αλλά βρίσκεται διάσπαρτη σε πολλά σημεία του. Ο DPO δρα και ενεργεί σε καθεστώς ανεξαρτησίας και ανεξάρτητα από τον ειδικό νομικό χαρακτηρισμό της σύμβασης (δηλαδή σύμβαση εργασίας, σύμβαση ανεξάρτητων υπηρεσιών, έργου κτλ), που το συνδέει με τον εκάστοτε οργανισμό και ανεξάρτητα από το αν ο οργανισμός αυτός λειτουργεί ως υπεύθυνος επεξεργασίας ή ως εκτελών την επεξεργασία. Θεσπίζει επίσης την υποχρέωση των υπεύθυνων επεξεργασίας των δεδομένων να παρέχουν διαφανείς και εύκολα προσβάσιμες πληροφορίες στα υποκείμενα των δεδομένων όσον αφορά την επεξεργασία των δεδομένων τους. Το GDPR αναγνωρίζει τον DPO ως κύριο παράγοντα στο νέο σύστημα διακυβέρνησης δεδομένων και καθορίζει τους όρους για το διορισμό του, τη θέση και τα καθήκοντά του. Στόχος αυτών των κατευθυντήριων γραμμών είναι να διευκρινιστούν οι σχετικές διατάξεις του GDPR προκειμένου να βοηθηθούν οι υπεύθυνοι επεξεργασίας να συμμορφωθούν με το νόμο, αλλά και να βοηθήσουν τους DPO στο ρόλο τους. Οι DPO δεν φέρουν προσωπική ευθύνη σε περίπτωση μη συμμόρφωσης με το GDPR.΄Σε περίπτωση παραβίασης λοιπόν, η ευθύνη βαρύνει αποκλειστικά τον υπεύθυνο επεξεργασίας[70].

Τον Φεβρουάριο του 2016, στο πλαίσιο του σχεδίου δράσης για την εφαρμογή του γενικού κανονισμού για την προστασία των δεδομένων (GDPR), η ομάδα εργασίας του άρθρου 29 (A29WP) δεσμεύτηκε να δημοσιεύσει οδηγίες σχετικά με τη λειτουργία των διατάξεων του GDPR μετά από την απαίτηση με βάση τον Κανονισμό οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία να διορίσουν έναν υπεύθυνο

[69] Βλ. ό.π., Νούσια Αλέξανδρο, Άρθρο «Καλώς ήρθατε στο Web 3.0.! Ο Γενικός Κανονισμός Προστασίας Δεδομένων και ο Ρόλος του Υπευθύνου Επεξεργασίας Δεδομένων»,25 Ιανουαρίου 2017 στην ιστοσελίδα www.opendata.ellak.gr .

[70] Βλ. Βαρβέρη Αλέξανδρο, Τεχνικά και Οργανωτικά θέματα-η ϋποχρεωτική τοποθέτηση υπεύθυνου προστασίας δεδομένων, ΕφημΔΔ 2017, σελ. 206 επ.

προστασίας δεδομένων (DPO). Αυτές οι οδηγίες δημοσιεύθηκαν στις 16 Δεκεμβρίου 2016[71].

Ορισμένα από τα νέα σημεία που τέθηκαν από τη WP29 είναι τα εξής:

α. Η λογοδοσία σημαίνει ότι οι εκτιμήσεις DPO πρέπει να είναι ενημερωμένες και μπορούν να ζητηθούν ανά πάσα στιγμή. Όταν οι ελεγκτές και οι μεταποιητές καθορίζουν εάν απαιτείται ή όχι ένας DPO, θα πρέπει να διατηρούν αντίγραφο της ανάλυσής τους στα αρχεία τους, καθώς η εκτίμηση αυτή εμπίπτει στο πεδίο εφαρμογής των ευρύτερων υποχρεώσεών τους για υποχρέωση λογοδοσίας. Οι τελικές κατευθυντήριες γραμμές προβλέπουν ότι η αξιολόγηση αυτή μπορεί να ζητηθεί ανά πάσα στιγμή από την αρμόδια εποπτική αρχή και πρέπει να επανεξετάζεται κάθε φορά που εξετάζονται νέες δραστηριότητες και υπηρεσίες. Δεδομένων των αυξανόμενων νομικών συνεπειών που θα δημιουργήσει η εν λόγω ανάλυση, οι υπεύθυνοι επεξεργασίας και ο υπεύθυνος επεξεργασίας καλούνται να προχωρήσουν με προσοχή κατά την αξιολόγηση του DPO.

β. Ο διορισμός ενός DPO δεν πρέπει να λαμβάνει χώρα "a la carte", που σημαίνει ότι οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία διορίζουν έναν DPO (είτε σε υποχρεωτική είτε σε εθελοντική βάση), το πρόσωπο αυτό είναι υπεύθυνο για όλες τις δραστηριότητες επεξεργασίας που διεξάγονται από τον οργανισμό. Επομένως, δεν θα είναι δυνατόν να οριοθετηθεί ο ρόλος του σε μέρος μόνο των δραστηριοτήτων του οργανισμού και να τον κρατήσει μακριά από τα υπόλοιπα.

γ. Τα big data αποτελούν τώρα ένα παράδειγμα "τακτικής και συστηματικής παρακολούθησης". Όπως σημειώθηκε αρχικά, όλες οι μορφές παρακολούθησης και προβολής σε απευθείας σύνδεση καλούνται ως παραδείγματα, μεταξύ άλλων για σκοπούς συμπεριφορικής διαφήμισης και επαναπροσανατολισμού ηλεκτρονικού ταχυδρομείου. Οι τελικές κατευθυντήριες γραμμές πηγαίνουν ένα βήμα παραπέρα και προσθέτουν μια αναφορά σε «δραστηριότητες προώθησης με βάση δεδομένα», ώστε να εντοπίζονται, για παράδειγμα, μεγάλες διαδικασίες τύπου big data δεδομένων.

δ. Κατά προτίμηση, ο DPO πρέπει να βρίσκεται εντός της ΕΕ. Οι τελικές κατευθυντήριες γραμμές υποδηλώνουν ότι αυτός είναι πράγματι ο τρόπος για τους υπεύθυνους επεξεργασίας και τους εκτελούντες την επεξεργασία να εξασφαλίσουν ότι

[71] Βλ. A29WP, Guidelines on Data Protection Officers (‘DPOs’), 16/EN WP 243 rev.01, τελευταία επικαιροποίηση 5.4.17.

είναι εύκολα προσβάσιμος (εκτός αν οι εν λόγω οργανώσεις δεν έχουν παρουσία στην ΕΕ και οι δραστηριότητες τους θα διεξαχθούν καλύτερα εκτός της ΕΕ).

ε. Αν και οι τελικές οδηγίες επιβεβαιώνουν ότι μπορεί να οριστεί μόνο ένας DPO (αποτρέποντας την «εικονικοποίηση» του ρόλου μεταξύ διαφόρων ατόμων), αυτό το άτομο μπορεί να λάβει βοήθεια και υποστήριξη από μια ομάδα. Αυτό διασαφηνίζεται σε ένα σημείο του αρχικού σχεδίου κατευθυντήριων γραμμών, το οποίο προέβλεπε ότι ο υπεύθυνος προστασίας δεδομένων πρέπει να είναι σε θέση να επικοινωνεί αποτελεσματικά με τα υποκείμενα των δεδομένων και να συνεργάζεται με τις εποπτικές αρχές στη γλώσσα ή τις γλώσσες που χρησιμοποιούν οι εποπτικές αρχές και τα εμπλεκόμενα πρόσωπα στα οποία αναφέρονται τα δεδομένα. Αυτό το σημείο είχε προκαλέσει επικρίσεις, καθώς φάνηκε να σημαίνει ότι ο DPO πρέπει να μιλά όλες τις γλώσσες της ΕΕ. Οι τροποποιημένες κατευθυντήριες γραμμές καθιστούν σαφές ότι αυτές οι επικοινωνίες στις διάφορες γλώσσες της ΕΕ μπορούν να γίνουν από τον "με τη βοήθεια μιας ομάδας εάν είναι απαραίτητο".

στ. Υποχρέωση τήρησης του απορρήτου των επικοινωνιών μεταξύ του DPO και των υπαλλήλων Οι τελικές κατευθυντήριες γραμμές επιβεβαιώνουν την ανάγκη δημιουργίας «ασφαλών μέσων επικοινωνίας» μεταξύ των εργαζομένων και του (εσωτερικού ή εξωτερικού) DPO, ώστε να διασφαλίζεται η εμπιστευτικότητα των ανταλλαγών τους. Αυτό, για παράδειγμα, θα εξασφαλίζεται από τη φυσική παρουσία του στις εγκαταστάσεις των εργαζομένων ή τη δημιουργία μιας ανοικτής τηλεφωνικής γραμμής. Η πρόταση εδώ είναι ότι τα ασφαλή μέσα επικοινωνίας πρέπει να είναι απαλλαγμένα από τεχνολογίες παρακολούθησης.

ζ. Τα ανώτερα διευθυντικά στελέχη, συμπεριλαμβανομένου του Προϊσταμένου των Ανθρώπινων Δικαιωμάτων, του Μάρκετινγκ ή των ατόμων πληροφορικής, δεν μπορούν να υπηρετούν ως DPO. Ο GDPR δεν δεσμεύει τους DPO από την κατοχή άλλων θέσεων, αλλά απαιτεί ρητά ότι οι υπεύθυνοι επεξεργασίας και ο υπεύθυνος επεξεργασίας εξασφαλίζουν ότι αυτά τα άλλα καθήκοντα δεν δημιουργούν σύγκρουση συμφερόντων. Οι τελικές κατευθυντήριες γραμμές προσδιορίζουν δύο ομάδες καταστάσεων που ενδέχεται να προκαλέσουν σύγκρουση συμφερόντων:

1/ Εσωτερικός διορισμός: Οι DPO που έχουν ανώτερες διευθυντικές θέσεις (π.χ. Διευθύνων Σύμβουλος, COO, CFO, Διευθυντές Ιατρικών Υπηρεσιών, Προϊστάμενος Μάρκετινγκ, Ανθρώπινου Δυναμικού ή Πληροφορικής) δεν θα μπορούν να διοριστούν σε θέσεις DPO. Το ίδιο ισχύει και για τους ανθρώπους που έχουν μικρότερο ρόλο στην οργάνωση της επιχείρησης, εάν οι ρόλοι τους οδηγούν στον καθορισμό των σκοπών και των μέσων επεξεργασίας και

2/ Εξωτερικός διορισμός: Εάν ένας εξωτερικός συνεργάτης λειτουργεί ως υπεύθυνος επεξεργασίας δεδομένων (π.χ. δικηγόρος) παρέχοντας καθημερινές υπηρεσίες DPO σε υπεύθυνους επεξεργασίας και εκτελούντες την επεξεργασία, αυτό μπορεί να εμποδίσει το συγκεκριμένο άτομο να εκπροσωπεί τις εν λόγω οντότητες ενώπιον των δικαστηρίων σε περιπτώσεις που αφορούν ζητήματα προστασίας προσωπικών δεδομένων.

η. Ο GDPR δεν εμποδίζει τον υπεύθυνο προστασίας δεδομένων να τηρεί αρχεία επεξεργασίας Σύμφωνα με τον GDPR, ο DPO δεν είναι υπεύθυνος για την τήρηση αρχείων των δραστηριοτήτων επεξεργασίας, ενώ αυτό αποτελεί σημαντικό μέρος των τρεχόντων καθηκόντων του βάσει των τοπικών νόμων για την προστασία των δεδομένων στη Γαλλία και τη Γερμανία. Οι τροποποιημένες κατευθυντήριες γραμμές προβλέπουν πλέον ότι τίποτα δεν εμποδίζει τον υπεύθυνο επεξεργασίας και τον εκτελούντα την επεξεργασία να αναθέτει στον υπεύθυνο προστασίας δεδομένων την υποχρέωση να τηρεί τα αρχεία των εργασιών επεξεργασίας υπό την ευθύνη τους. Οι τροποποιημένες κατευθυντήριες γραμμές προβλέπουν επίσης ότι τα εν λόγω αρχεία πρέπει να θεωρούνται ως ένα από τα μέσα που επιτρέπουν στον υπεύθυνο προστασίας δεδομένων να εκτελεί τα καθήκοντά του ενημέρωσης και παροχής συμβουλών στον ελεγκτή ή τον μεταποιητή και την παρακολούθηση της συμμόρφωσης με τον κανονισμό.

Οι κατευθυντήριες οδηγίες της Επιτροπής του άρθρου 29 εστιάζουν στην διασαφήνιση της έννοιας «βασικές δραστηριότητες» (Core Activities), οι οποίος περιγράφονται ως «αναπόσπαστο τμήμα της επίδιωξης των εταιρικών σκοπών του Υπευθύνου ή Εκτελούντος την Επεξεργασία όπως για παράδειγμα οι δραστηριότητες παρακολούθησης μιας εταιρίας παροχής υπηρεσιών ασφαλείας, με τις οποίες ελέγχει/παρακολουθεί έναν δημόσιο ή ιδιωτικό χώρο , οι δραστηριότητες επεξεργασίας ιατρικών φακέλων ασθενών που νοσηλεύονται σε ένα νοσοκομείο καθώς και οι δραστηριότητες επεξεργασίας προσωπικών δεδομένων υπαλλήλων από έναν εξωτερικό συνεργάτη που διαχειρίζεται την μισθοδοσία του προσωπικού μιας εταιρίας.

Η έννοια «Συστηματική» και «Τακτική» Παρακολούθηση των υποκειμένων σε μεγάλη κλίμακα (regular and systematic monitoring) στην οποία εντάσσονται όλες οι μορφες on line παρακολούθησης όπως για παράδειγμα η παρακολούθηση των μετακινήσεων του υποκειμένου (location tracking) η επεξεργασία που στοχεύει στον καθορισμό της καταναλωτικής συμπεριφοράς και συνηθειών του υποκειμένου για διαφημιστιούς σκοπούς (behavioral advertising) καθώς και ο καθορισμός του Προφίλ του υποκειμένου με βάση συγκεκριμένα προσωπικά δεδομένα που αφορούν την καταναλωτική του ταυτότητα, τις προτιμήσεις του, επισκεψιμότητα σε συγκεκριμένα καταστήματα, (Profiling). Άλλα ενδιαφέροντα παραδείγματα που παρατίθενται

περιλαμβάνουν τη βαθμολόγηση (π.χ. για βαθμολόγηση πιστώσεων, πρόληψη απάτης ή για τον καθορισμό ασφαλίστρων), τον εντοπισμό τοποθεσίας, την καταλληλότητα και παρακολούθηση δεδομένων για την υγεία και την επεξεργασία από συνδεδεμένες συσκευές (έξυπνοι μετρητές, έξυπνα αυτοκίνητα κ.λπ.).

Η επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα (των «Ευαίσθητων Προσωπικών Δεδομένων της Οδηγίας 96/45) σε «μεγάλη κλίμακα», όπως δεδομένων που αφορουν την θρησκεία, πολιτικές πεποιθήσεις, σεξουαλικό προσανατολισμό, συμμετοχή σε συνδικαλιστικές οργανώσεις αλλά και Γενετικα Δεδομένων ή Υλικό όπως και Βιομετρικά Στοιχεία τα οποία ορίζονται ως «Ειδικά Προσωπικά Δεδομένα» με το Νέο Κανονισμό. Η ομάδα του A29WP δεν ενδιαφέρεται επί του παρόντος για ακριβείς αριθμούς που χρησιμοποιούνται ως σημείο αναφοράς για τον όρο αυτό, αν και σημειώνει ότι τα σχέδια πρέπει να δημοσιεύσουν κατώτατα όρια. Αντίθετα, η Καθοδήγηση παραθέτει κάποιους αρκετά προφανείς παράγοντες που πρέπει να λαμβάνονται υπόψη κατά τον προσδιορισμό της μεγάλης κλίμακας (π.χ. ο αριθμός των προσβεβλημένων ατόμων και η γεωγραφική έκταση της επεξεργασίας). Παραδείγματα επεξεργασίας μεγάλης κλίμακας που αναφέρονται περιλαμβάνουν: μια τράπεζα ή μια ασφαλιστική εταιρεία που επεξεργάζεται δεδομένα πελατών, και επεξεργασία δεδομένων γεωγραφικής θέσης πελάτη της αλυσίδας ταχείας διανομής σε πραγματικό χρόνο για στατιστικούς σκοπούς από ειδικό επεξεργαστή.

Επίσης η ομάδα του άρθρου 29, στις κατευθυντήριες οδηγίες της, επιβεβαιώνει ότι, όταν ένας DPO διορίζεται σε εθελοντική βάση, θα ισχύουν για αυτούς οι ίδιες απαιτήσεις όπως αυτές που ορίζονται από το GDPR στους υποχρεωτικούς (π.χ. όσον αφορά την ανεξαρτησία, την απαλλαγή από την άδικη απόλυση, την υποχρέωση δημοσίευσης των στοιχείων επικοινωνίας κλπ.). Είναι ενδιαφέρον το γεγονός ότι η Ομάδα συνιστά ότι ένας οργανισμός που αποφασίζει να μην ορίσει εθελοντικά ένα έγγραφο προστασίας δεδομένων GDPR γιατί πιστεύει ότι δεν υπόκειται στα υποχρεωτικά κριτήρια ορισμού του DPO (όπως συνοψίζονται παραπάνω). Όμως οι υπεύθυνοι προστασίας δεδομένων στην περίπτωση αυτή δε θα ευθύνονται προσωπικά εάν η οργάνωσή τους δεν συμμορφωθεί με το GDPR. Επίσης αναγνωρίζεται η δυνατότητα διορισμού ένας εξωτερικού DPO, εφόσον εφαρμόζονται οι απαιτήσεις του GDPR, συμπεριλαμβανομένης της αμεροληψίας, της γνώσης του οργανισμού στον οποίο διορίζεται και της προσβασιμότητας. Υπογραμμίζεται ότι οι όροι εξωτερικού διορισμού του πρέπει να ορίζονται σαφώς σε σύμβαση παροχής υπηρεσιών και να συμφωνείται σαφώς ο τίτλος, το καθεστώς, η θέση και τα καθήκοντα του. Επιπλέον, μια ομάδα εταιρειών δύναται να ορίσει έναν ενιαίο DPO τηρουμένων των προϋποθέσεων του GDPR.

Η Ομάδα του άρθρου 29 κάνει ένα ενδιαφέρον σχόλιο σε σχέση με την προσβασιμότητα. Οι DPO πρέπει να είναι εύκολα προσβάσιμοι στα υποκείμενα των δεδομένων και στις ρυθμιστικές αρχές. Αυτό δεν θα είναι δυνατό εκτός εάν ο DPO μπορεί να επικοινωνήσει στις γλώσσες στις οποίες τα πρόσωπα στα οποία αναφέρονται τα δεδομένα (για παράδειγμα οι πελάτες και το προσωπικό) και οι ρυθμιστικές αρχές που ενδέχεται να μιλήσουν οι οργανώσεις τις οποίες εκπροσωπεί. Φαίνεται ότι το A29WP αναμένει ότι οι DPO σε πολυεθνικές εταιρείες θα είναι εξειδικευμένοι σε ζητήματα που άπτονται την προστασία των δεδομένων και πολυγλωσσολόγοι (ή τουλάχιστον θα έχουν πρόσβαση σε μηχανισμούς καλής μετάφρασης). Απαραίτητη κρίνεται η δημοσίευση των στοιχείων επικοινωνίας του DPO με βάση τον GDPR. Δεν απαιτείται να δημοσιοποιείται το όνομα του DPO, αλλά θα πρέπει να δημοσιεύεται σε όλες τις αρμόδιες ρυθμιστικές αρχές και τα μέλη του προσωπικού. Οι πολίτες χρειάζονται μόνο επαρκείς πληροφορίες για την εύκολη επικοινωνία με τον DPO, π.χ. μια αποκλειστική διεύθυνση ηλεκτρονικού ταχυδρομείου που δημοσιεύεται σε έναν ιστότοπο.

Σε περίπτωση που ο διορισμός ενός DPO καθυστερήσει μέχρι την έναρξη εφαρμογής του GDPR, η επιχείρηση δύναται να ανακοινώσει ότι δεν υπάρχουν διαθέσιμοι κατάλληλοι υποψήφιοι. Εν τω μεταξύ, η κυβέρνηση του Ηνωμένου Βασιλείου, παρά την αβεβαιότητα σχετικά με την Brexit, επιβεβαίωσε ότι το GDPR θα εφαρμοστεί στο Ηνωμένο Βασίλειο από τις 25 Μαΐου 2018. Αυτό σημαίνει ότι οι επιχειρήσεις του Ηνωμένου Βασιλείου θα υπόκεινται στην υποχρέωση διορισμού του, όπως προαναφέρθηκε. Η White & Case δημιούργησε ένα λεπτομερές Εγχειρίδιο GDPR[72] που παρέχει πρακτικές οδηγίες σχετικά με τον αντίκτυπο αυτής της νομοθεσίας στις επιχειρήσεις. Σύμφωνα με τη μελέτη η παγκόσμια εμβέλεια του GDPR απαιτεί τουλάχιστον 75.000 DPO παγκοσμίως. Ο κανονισμός ρυθμίζει τις πρακτικές απορρήτου οποιασδήποτε εταιρείας που χειρίζεται δεδομένα πολιτών της ΕΕ, είτε αυτή η εταιρεία βρίσκεται στην ΕΕ είτε όχι. Επειδή τα 28 κράτη μέλη της ΕΕ αντιπροσωπεύουν από κοινού τη μεγαλύτερη οικονομία στον κόσμο και τον κορυφαίο εμπορικό εταίρο για 80 χώρες, πολλές εταιρείες σε όλο τον κόσμο αγοράζουν και πωλούν αγαθά στους πολίτες της ΕΕ και επομένως υπόκεινται στον GDPR. Νωρίτερα, η μελέτη του IAPP[73] έτους 2016 εκτιμά συντηρητικά ότι, από την έναρξη ισχύος του GDPR, τουλάχιστον 28.000 DPO θα χρειαστούν στην Ευρώπη και μόνο στις Ηνωμένες Πολιτείες. Εφαρμόζοντας μια παρόμοια μεθοδολογία, εκτιμούμε τώρα ότι θα

[72] https://www.whitecase.com/publications/alert/unlocking-eu-general-data-protection-regulation

[73] Βλ. ιστοσελίδα https://iapp.org ,ο.π.

δημιουργηθούν έως και 75.000 θέσεις DPO ως απάντηση στο GDPR σε όλο τον κόσμο. Η απαίτηση του ΥΠΔ δανείζεται από ένα παρόμοιο πρόγραμμα που είχε στη διάθεσή της η Γερμανία για μια δεκαετία και άλλες οικονομίες, όπως η Γαλλία και η Σουηδία, έχουν, για παράδειγμα, καλά εδραιωμένη την έννοια και την ανάγκη διορισμού του.

Για τα ώριμα προγράμματα, η απαίτηση DPO του GDPR πρέπει να παρουσιάζει ελάχιστα προβλήματα. Σύμφωνα με το έγγραφο του Ευρωπαίου Επόπτη Προστασίας Δεδομένων σχετικά με τα "Επαγγελματικά Πρότυπα για τους Υπεύθυνους Προστασίας Δεδομένων", η πιο σχετική πιστοποίηση για έναν DPO είναι "αυτή που παρέχεται από τη Διεθνή Ένωση Επαγγελματιών Προστασίας Προσωπικών Δεδομένων". Παρομοίως, ο Eric Lachaud, στο άρθρο του "Θα έπρεπε ο DPO να πιστοποιηθεί ;" για το περιοδικό International Data Privacy Law του Πανεπιστημίου της Οξφόρδης[74], καταλήγει στο συμπέρασμα ότι η καταλληλότερη πιστοποίηση για τον DPO είναι ένας συνδυασμός του Πιστοποιητικού IAPP επαγγελματίες (CIPP / E) και Certified Privacy Manager (CIPM). Το IAPP προσφέρει επίσης τις διαπιστευτήριες πιστοποιήσεις CIPT (Certified Privacy Technologist), καθώς και μια έκδοση του CIPP για τις Ηνωμένες Πολιτείες και μία για την ομοσπονδιακή κυβέρνηση του Καναδά και των ΗΠΑ.

Ο ρόλος του DPO, ως εξειδικευμένου, λειτουργικά ανεξάρτητου, στελέχους δεν περιορίζεται μόνο στην υποχρεωτική, κατά το Νέο Κανονισμό, παρουσία του σε μία εταιρία με την έννοια της τυπικής πλήρωσης μιας θέσης εργασίας (tick box) όπως αντίστοιχα ο Ιατρός Εργασίας ή ο Τεχνικός Ασφαλείας. Αναλαμβάνει ουσιαστικά να εκπροσωπήσει την Επιχείρηση έναντι των Αρχών, Εθνικών και Ευρωπαικών, να διασφαλίσει την εναρμόνιση της λειτουργίας της επιχείρησης σε ότι αφορά τις πολιτικές πρακτικές και μεθοδολογία επεξεργασίας, αποθήκευσης και μεταφοράς Δεδομένων Προσωπικού Χαρακτήρα με το νέο αυστηρό νομοθετικό πλαίσιο και να προστατέψει την επιχείρηση από τους κινδύνους επιβολής των σημαντικότατων και βαρύτατων διοικητικών προστίμων που προβλέπει ο Κανονισμός τα οποία εκκινούν από 10.000.000 Ευρώ ή το 2% του παγκόσμιου τζίρου εαν πρόκειται για διεθνή όμιλο και φτάνουν σε περίπτωση παράβασης βασικών διατάξεων του κανονισμού σε 20.000.000 ή στο 4% του παγκόσμιου τζίρου.

[74] https://academic.oup.com/idpl/article-abstract/4/3/189/2549069

5.6 Αξιολόγηση – κριτική του θεσμού του Υπεύθυνου Επεξεργασίας

Από την παραπάνω ανάλυση προκύπτει ότι η ενίσχυση των δικαιωμάτων των πολιτών επιτυγχάνεται μέσω της επιβολής ενισχυμένων υποχρεώσεων στους υπεύθυνους επεξεργασίας. Η επαυξημένη ευθύνη του αποτελεί καινοτομία του Κανονισμού, καθώς το άρθρο 23 παρ. 2 της Οδηγίας 95/46/ΕΚ τον απαλλάσσει αν αποδείξει ότι δεν ευθύνεται, ενώ ο Κανονισμός με το ίδιο λεκτικό ορίζει ότι οφείλει να εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα και πολιτικές, προκειμένου να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τον Κανονισμό (Άρθρο 24 παρ.1)[75]. Επομένως, ο υπεύθυνος επεξεργασίας θα πρέπει ανά πάσα στιγμή να είναι σε θέση να αποδεικνύει ότι δεν φταίει, αλλά κινείται εντός των ορίων που θέτει η νομοθεσία.

Προς διασφάλιση της τηρήσεως των υποχρεώσεων του υπεύθυνου επεξεργασίας επιβάλλονται πολύ υψηλά πρόστιμα που μπορούν να φτάσον τα 20 εκατομμύρια Ευρώ ή το 4% του παγκόσμιου ετήσιου κύκλου εργασιών μιας εταιρείας. Γι' αυτό το λόγο ο υπεύθυνος επεξεργασίας, θα πρέπει, κατά την άποψη μου, να λειτουργήσει ως επικεφαλής μιας ομάδας ειδικών (Task Force) που θα τον πλαισιώνει και θα περιλαμβάνει μέλη του IT, PR, Legal/Compliance και Information Security (Νομική / Συμμόρφωση και Ασφάλεια Πληροφοριών), δημιουργώντας μια εύελικτη ομάδα που θα αντιμετωπίσει επιτυχώς όλες τις προκλήσεις που θα ανακύψουν κατά την εφαρμογή του νέου αυστηρού νομοθετικου πλαισίου στον χώρο των προσωπικών δεδομένων. Λαμβάνοντας υπόψη 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, ο υπεύθυνος επεξεργασίας εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα που επανεξετάζονται και επικαιροποιούνται όταν κρίνεται απαραίτητο. Η τήρηση εγκεκριμένων κωδίκων δεοντολογίας όπως αναφέρεται στο άρθρο 40 ή εγκεκριμένου μηχανισμού πιστοποίησης όπως αναφέρεται στο άρθρο 42 του Κανονισμού δύναται να χρησιμοποιηθεί ως στοιχείο για την απόδειξη της συμμόρφωσης με τις υποχρεώσεις του υπευθύνου επεξεργασίας.

[75] Βλ. όπως παραπάνω Παναγοπούλου Φερενίκη, Πώς θα επιβάλλει η ΑΠΔΠΧ τα πρόστιμα στις ασφαλιστικές από το 2018;,συνέντευξη στη Βίκυ Γερασίμου, Insurance Daily News, 17 Μαρ 2017.

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 από την επεξεργασία, σύμφωνα με το άρθρο 25 του Κανονισμού ο υπεύθυνος επεξεργασίας καλείται να εφαρμόζει αποτελεσματικά, τόσο κατά τη στιγμή του καθορισμού των μέσων επεξεργασίας όσο και κατά τη στιγμή της επεξεργασίας, κατάλληλα τεχνικά και οργανωτικά μέτρα, όπως η ψευδωνυμοποίηση, σχεδιασμένα για την εφαρμογή αρχών προστασίας των δεδομένων, όπως η ελαχιστοποίηση των δεδομένων, και την ενσωμάτωση των απαραίτητων εγγυήσεων στην επεξεργασία κατά τρόπο ώστε να πληρούνται οι απαιτήσεις του παρόντος κανονισμού και να προστατεύονται τα δικαιώματα των υποκειμένων των δεδομένων.

Σε περίπτωση που δύο ή περισσότεροι υπεύθυνοι επεξεργασίας καθορίζουν από κοινού τους σκοπούς και τα μέσα της επεξεργασίας, αποτελούν από κοινού υπευθύνους επεξεργασίας. Αυτοί καθορίζουν με διαφανή τρόπο τις αντίστοιχες ευθύνες τους για συμμόρφωση προς τις υποχρεώσεις που απορρέουν από τον παρόντα κανονισμό, ιδίως όσον αφορά την άσκηση των δικαιωμάτων του υποκειμένου των δεδομένων και τα αντίστοιχα καθήκοντά τους για να παρέχουν τις απαραίτητες πληροφορίες μέσω συμφωνίας μεταξύ τους, εκτός εάν και στον βαθμό που οι αντίστοιχες αρμοδιότητες των υπευθύνων επεξεργασίας καθορίζονται από το δίκαιο της Ένωσης ή το δίκαιο του κράτους μέλους στο οποίο υπόκεινται οι υπεύθυνοι επεξεργασίας. Στη συμφωνία μπορεί να αναφέρεται ένα σημείο επικοινωνίας για τα υποκείμενα των δεδομένων.

Αναλόγως του μεγέθους και της διάρθρωσης της οργάνωσης, μπορεί να χρειαστεί να δημιουργηθεί μια ομάδα προστασίας προσωπικών δεδομένων, ικανή να ενισχύσει το έργο του υπεύθυνου επεξεργασίας (ένας DPO και το προσωπικό του / της). Σε τέτοιες περιπτώσεις, η εσωτερική δομή της ομάδας και τα καθήκοντα και οι αρμοδιότητες κάθε μέλους της πρέπει να καταρτίζονται σαφώς. Ομοίως, όταν η λειτουργία του ασκείται από εξωτερικό πάροχο υπηρεσιών, μια ομάδα ατόμων που εργάζονται για αυτήν την οντότητα μπορεί να διεκπεραιώσει αποτελεσματικά τα καθήκοντα ενός DPO ως ομάδα για τον πελάτη.

Σε γενικές γραμμές, όσο πιο σύνθετες και/ή ευαίσθητες είναι οι διαδικασίες επεξεργασίας, τόσο περισσότεροι πόροι πρέπει να παρέχονται στον DPO. Η λειτουργία προστασίας δεδομένων πρέπει να είναι αποτελεσματική και να διαθέτει επαρκείς πόρους σε σχέση με την επεξεργασία δεδομένων που πραγματοποιείται. Σε αντίθετη περίπτωση υπάρχει σοβαρότατος κίνδυνος επιβολής εξοντωτικών για τις επιχειρήσεις διοικητικών προστίμων, αλλά πέραν αυτών, κίνδυνος αναστολής της

επεξεργασίας ή μεταφοράς συγκεκριμένων προσωπικών δεδομένων από τις εταιρίες που πρακτικά μπορεί να σημαίνει αναστολής της δραστηριότητας της επιχείρησης με τις αντίστοιχες συνέπειες. Κατά συνέπεια, ο οργανισμός πρέπει να διασφαλίσει, για παράδειγμα, ότι DPO καλείται να συμμετέχει τακτικά σε συνεδριάσεις ανώτερων και μεσαίων στελεχών. Συνιστάται η παρουσία του όταν λαμβάνονται αποφάσεις με συνέπειες προστασίας δεδομένων. Όλες οι σχετικές πληροφορίες πρέπει να διαβιβάζονται έγκαιρα σε αυτόν προκειμένου να του επιτρέψουν να παρέχει επαρκείς συμβουλές. Πρέπει πάντοτε να λαμβάνεται υπόψη η γνώμη του. Σε περίπτωση διαφωνίας, το WP29 συνιστά, ως ορθή πρακτική, να τεκμηριωθούν οι λόγοι για τους οποίους δεν ακολουθήθηκε η συμβουλή του.

Σκόπιμο θα ήταν να προσδιοριστεί ο χρόνος που απαιτείται για την εκτέλεση της λειτουργίας, το κατάλληλο επίπεδο προτεραιότητας για τα καθήκοντα DPO και αυτός με τη σειρά του (ή ο οργανισμός) να καταρτίσει ένα σχέδιο εργασίας, που περιλαμβάνει τους οικονομικούς πόρους, την υποδομή (χώρους, εγκαταστάσεις, εξοπλισμό) και το προσωπικό, όπου ενδείκνυται. Απαραίτητη κρίνεται να έχει προηγηθεί επίσημη ανακοίνωση σχετικά με τον διορισμό του σε όλο το προσωπικό ώστε να διασφαλιστεί ότι η ύπαρξη και η λειτουργία τους είναι γνωστές στον οργανισμό.

Επιπλέον απαραίτητη είναι η πρόσβαση του σε άλλες υπηρεσίες, όπως οι ανθρώπινοι πόροι, η νομική, η πληροφορική, η ασφάλεια κ.λπ., ώστε να μπορεί να λαμβάνει ουσιαστική υποστήριξη και πληροφορίες από αυτές τις άλλες υπηρεσίες και η συνεχής εκπαίδευση του με ενημέρωσή του σχετικά με τις εξελίξεις στον τομέα της προστασίας δεδομένων. Στόχος θα πρέπει να είναι η συνεχής αύξηση του επιπέδου εμπειρογνωμοσύνης του και η συνεχής κατάρτισή του σχετικά με την προστασία των δεδομένων και άλλες μορφές επαγγελματικής ανάπτυξης, όπως η συμμετοχή σε φόρουμ για την προστασία της ιδιωτικής ζωής, σε εργαστήρια κλπ.

Είναι αναγκαία η αφύπνιση και η δραστηριόποιηση της αγοράς ώστε στον χρόνο που απομένει μέχρι την έναρξη ισχύος του Γενικού Κανονισμού οι οργανισμοί να προετοιμασθούν κατάλληλα και επαρκώς για να αντιμετώπισουν τα νέα δεδομένα, και στους επαγγελματίες των Προσωπικών Δεδομένων να επικαιροποιήσουν και εξειδικεύσουν την γνώση τους ώστε να μπορέσουν να αναλάβουν υπεύθυνα και ουσιαστικά τα καθήκοντα τους.

6. Προετοιμασία για συμμόρφωση με ορίζοντα το 2018

Ο Κανονισμός 2016/679 θα εφαρμοστεί, όπως προαναφέρθηκε, από τις 24 Μαΐου 2018. Κατά την ημερομηνία αυτή, κάθε υπεύθυνος επεξεργασίας των Κρατών -Μελών, θα πρέπει να ενεργεί σε συμμόρφωση με τις διατάξεις του Κανονισμού. Μέχρι την ημερομηνία αυτή, θα πρέπει να ετοιμαστεί και να προωθηθεί η υιοθέτηση Νομοσχεδίου για την καλύτερη εφαρμογή ορισμένων διατάξεων του Κανονισμού. Παράλληλα, σε συνεργασία με τις Αρχές Προστασίας Προσωπικών Δεδομένων των άλλων Κρατών Μελών, θα υιοθετηθούν και θα δημοσιευτούν Καθοδηγητικές Γραμμές και Κώδικες Πρακτικής για συμμόρφωση με τις διατάξεις του Κανονισμού. Οι οργανισμοί, τόσο του δημόσιου όσο και του ιδιωτικού τομέα, θα πρέπει να αξιοποιήσουν το χρονικό διάστημα που απομένει μέχρι την εφαρμογή του για να είναι έτοιμοι να τον εφαρμόσουν στις 24 Μαΐου 2018.

Για την καλύτερη προετοιμασία των υπεύθυνων επεξεργασίας θα πρέπει να προηγηθεί[76]:

α. Ενημέρωση και μελέτη του κανονισμού, ώστε να εντοπιστούν οι πτυχές που μπορεί να επηρεάζουν τον Οργανισμό-Υπηρεσία εκάστου εξετάζοντας θέματα προσωπικού ή τεχνικά θέματα μηχανογράφησης ή διαχείρισης βάσεων δεδομένων.

β. Καταγραφή δραστηριοτήτων του Οργανισμού-Υπηρεσίας που εμπίπτουν στον Κανονισμό. Η καταγραφή αυτή είναι χρήσιμη τόσο για την εσωτερική λειτουργία του οργανισμού όσο και για την εφαρμογή των αρχών της διαφάνειας και της λογοδοσίας, καθώς οι υπεύθυνοι επεξεργασίας θα έχουν υποχρέωση να συμμορφώνονται με τον Κανονισμό αλλά και υποχρέωση να επιδεικνύουν τη συμμόρφωσή τους.

γ. Στον τομέα της επικοινωνίας να γίνει έλεγχος αν η πληροφόρηση που παρέχεται σε πολίτες, πελάτες ή εταίρους του οργανισμού, μέσω εντύπων ή της ιστοσελίδας του, χρειάζεται να διαφοροποιηθεί και προσαρμοστεί ανάλογα. Αν ο οργανισμός έχει Πολιτική Προστασίας της Ιδιωτικής Ζωής (Privacy Policy), να εξεταστεί ποιες πτυχές της χρήζουν εκσυγχρονισμού, σε συμμόρφωση με τον Κανονισμό.

---

[76]Βλ. Λοϊζίδου- Νικολαΐδου Ειρήνη, παρουσίαση με τίτλο «Προστασία Προσωπικών Δεδομένων-Νεοι Ορίζοντες», Επίτροπος Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, διαθέσιμη στην ιστοσελίδα www.icpac.org.cy .

δ. Έλεγχος των δικαιωμάτων των πολιτών που επηρεάζουν τις δραστηριότητες της κάθε Υπηρεσίας, δεδομένου ότι ο Κανονισμός ενισχύει τα υφιστάμενα δικαιώματα των πολιτών και επιπλέον, δημιουργεί και νέα δικαιώματα, και εύρεση των τρόπων με τους οποίους οι πολίτες θα μπορούν να ασκούν τα δικαιώματά τους. Με την εφαρμογή του Κανονισμού, ίσως χρειαστεί να υιοθετηθούν και να γνωστοποιήθούν στο κοινό μια τυποποιημένη διαδικασία για την άσκηση των δικαιωμάτων.

ε. Κάθε δραστηριότητα του οργανισμού θα πρέπει να υπακούει στις προϋποθέσεις για νόμιμη επεξεργασία που καθορίζει ο Κανονισμός, Παρόλο που οι προϋποθέσεις αυτές είναι σε μεγάλο βαθμό όμοιες με τις υφιστάμενες, ο κάθε οργανισμός θα πρέπει να είναι σε θέση να δικαιολογήσει, εφόσον χρειαστεί, τη νομική βάση στην οποία βασίζεται η κάθε δραστηριότητα του.

στ.Ο Κανονισμός, όπως και η υφιστάμενη νομοθεσία, διαχωρίζει μεταξύ της «συγκατάθεσης» και της «ρητής συγκατάθεσης» που λαμβάνεται για την επεξεργασία ευαίσθητων δεδομένων. Σε αντίθεση όμως με την υφιστάμενη νομοθεσία, ο Κανονισμός θέτει συγκεκριμένες προϋπόθεσης για τη λήψη της συγκατάθεσης. Αν οι δραστηριότητες ενός οργανισμού βασίζονται στη συγκατάθεση, θα πρεέπει να δωθεί ιδιαίτερη προσοχή στις σχετικές πρόνοιες του Κανονισμού. Για υπηρεσία της κοινωνίας των πληροφοριών απευθείας σε παιδί, θα πρέπει να λαμβάνεται η συγκατάθεση του προσώπου πού έχει τη γονική μέριμνα του παιδιού.

ζ. Ο οργανισμός πρέπει να λαμβάνει εκσυγχρονισμένα τεχνικά και διαδικαστικά μέτρα για την προστασία των δεδομένων που χειρίζεται. Σε περίπτωση παραβίασης ή υποκλοπής βάσεων δεδομένων, ο οργανισμός ίσως πρέπει να ενημερώσει την Επίτροπο και/ ή τα επηρεαζόμενα πρόσωπα. Να εξεταστεί αν τα μέτρα ασφάλειας που εφαρμόζει ο οργανισμός σας ανταποκρίνονται στις απαιτήσεις του Κανονισμού.

η. Ο Κανονισμός αναγνωρίζει ορισμένες δραστηριότητες ως υψηλού κινδύνου. Οργανισμός που εμπλέκεται σε τέτοιες δραστηριότητες, ενδεχομένως να έχει υποχρέωση διεξαγωγής εκτίμησης κινδύνου για κάθε δραστηριότητα. Ορισμένοι οργανισμοί, λόγω μεγέθους, ή λόγω φύσης δραστηριοτήτων, θα πρέπει να ορίζουν Υπεύθυνους Προστασίας Δεδομένων (DPO). Ο DPO μπορεί να είναι υπάλληλος του οργανισμού ή εξωτερικός συνεργάτης. Οργανισμός που χρησιμοποιεί ή αναπτύσσει/ σχεδιάζει μηχανογραφημένα συστήματα επεξεργασίας δεδομένων ή νέες τεχνολογίες ή εφαρμογές, θα πρέπει να λάβει υπόψη τις πρόνοιες του Κανονισμού, σχετικά με την ενσωμάτωση δικλίδων ασφαλείας (data protection by design and by default).

θ. Οργανισμός που εδρεύει και δραστηριοποιείται σε περισσότερα από ένα Κράτη Μέλη έχει το δικαίωμα να ορίσει το Κράτος Μέλος στο οποίο θα έχει την κύρια έδρα του και, κατά κανόνα, θα συναλλάσσεται με την Αρχή Προστασίας Προσωπικών

Δεδομένων του Κράτους αυτού. Για αποφάσεις που λαμβάνονται από κοινού μεταξύ ξεχωριστών οργανισμών, ο Κανονισμός εισάγει το θεσμό των συνυπεύθυνων επεξεργασίας. Για διασυνοριακές περιπτώσεις που χρήζουν της συνεργασίας των Αρχών, ο Κανονισμός εισάγει το μηχανισμό συνεκτικότητας και καθορίζει το ρόλο της κάθε Αρχής ως «επικεφαλής» ή «αρμόδιας» ή ως «ενδιαφερόμενης» Αρχής.

ι. Ο Κανονισμός καταργεί το υφιστάμενο σύστημα Γνωστοποιήσεων και έκδοσης αδειών Διασύνδεσης αρχείων ή Διαβίβασης δεδομένων σε τρίτες χώρες αλλά, δημιουργεί νέες, αντίστοιχες υποχρεώσεις, με τις οποίες οι οργανισμοί θα πρέπει να είναι έτοιμοι να συμμορφωθούν τον Μάιο του 2018. Τέτοιες υποχρεώσεις είναι, η καταγραφή διαδικασιών, η διεξαγωγή εκτίμησης κινδύνου, οι κώδικες πρακτικής, η πιστοποίηση διαδικασιών και ο DPO. Κάθε οργανισμός θα πρέπει να γνωρίζει σε ποιες από αυτές τις υποχρεώσεις υπόκειται.

7. Συμπερασματικές σκέψεις και προτάσεις

Οι ραγδαίες τεχνολογικές εξελίξεις που δημιουργούν νέες προκλήσεις για την προστασία των δεδομένων προσωπικού χαρακτήρα. Η κλίμακα της ανταλλαγής και της συλλογής δεδομένων έχει αυξηθεί σε μεγάλο βαθμό. Η τεχνολογία επιτρέπει τόσο σε ιδιωτικές επιχειρήσεις όσο και σε δημόσιες αρχές να κάνουν χρήση δεδομένων προσωπικού χαρακτήρα σε πρωτόγνωρο βαθμό για την επιδίωξη των δραστηριοτήτων τους. Τα φυσικά πρόσωπα καθιστούν ολοένα και περισσότερο δημόσια διαθέσιμες προσωπικές πληροφορίες σε παγκόσμιο επίπεδο. Η τεχνολογία έχει αλλάξει τόσο την οικονομία όσο και την κοινωνική ζωή. Η οικοδόμηση εμπιστοσύνης στο επιγραμμικό (online) περιβάλλον είναι καθοριστικής σημασίας για την οικονομική ανάπτυξη. Η έλλειψη εμπιστοσύνης κάνει τους καταναλωτές να διστάζουν να αγοράσουν και να υιοθετήσουν νέες ψηφιακές υπηρεσίες. Αυτό απειλεί να επιβραδύνει την ανάπτυξη καινοτόμων χρήσεων των νέων τεχνολογιών. Επομένως, η προστασία των δεδομένων προσωπικού χαρακτήρα κατέχει κεντρική θέση στο ψηφιακό θεματολόγιο για την Ευρώπη, και γενικότερα στη στρατηγική «Ευρώπη 2020» .

Απόρροια της κατάστασης αυτής, με βάση την αιτιολογική έκθεση της Ευρωπαϊκής Επιτροπής, ήταν η θέσπιση ενός νέου νομικού πλαισίου περί της προστασίας των δεδομένων προσωπικού χαρακτήρα στην ΕΕ, που αποτελείται βασικά από τον Γενικό Κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών (ΕΕ 2016/679/ General Data Protection Regulation), με σκοπό μια συνολικότερη και συνεκτικότερη πολιτική σχετικά με το θεμελιώδες δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα στην ΕΕ, καθώς το ισχύον πλαίσιο παραμένει αναποτελεσματικό όσον αφορά τους στόχους και τις αρχές του, αφού δεν κατάφερε να αποτρέψει τον κατακερματισμό του τρόπου εφαρμογής της προστασίας των δεδομένων προσωπικού χαρακτήρα στην Ένωση, την ανασφάλεια δικαίου και μια διαδεδομένη αντίληψη του κοινού ότι υπάρχουν σημαντικοί κίνδυνοι, οι οποίοι

σχετίζονται ειδικότερα με την επιγραμμική δραστηριότητα. Για τον λόγο αυτό, το νέο νομικό οικοδόμημα έρχεται να θεραπεύσει αυτές τις ατέλειες, υιοθετώντας ένα πιο συνεκτικό πλαίσιο προστασίας των δεδομένων στην ΕΕ, υποστηριζόμενο από ισχυρή επιβολή του νόμου, η οποία θα επιτρέψει στην ψηφιακή οικονομία να αναπτυχθεί σε ολόκληρη την εσωτερική αγορά, θα επιτρέψει στα φυσικά πρόσωπα να ασκούν έλεγχο επί των δεδομένων που τους αφορούν και θα ενισχύσει τη νομική και την πρακτική ασφάλεια για τους οικονομικούς παράγοντες και τις δημόσιες αρχές. Η «αγορακεντρική» αυτή διάσταση απασχολεί ευθέως το νομοθέτη της Ένωσης, προκύπτει δε από τον ίδιο τον τίτλο του Κανονισμού που έχει ως αντικείμενο τόσο την προστασία τους έναντι της επεξεργασίας των δεδομένων, όσο και την «ελεύθερη κυκλοφορία τους»[77]. Γι΄ αυτό και με το νέο αυτό θεσμικό κείμενο επιχειρείται με μια δέσμη λύσεων και εργαλείων, η αποτελεσματικότητά του στη διαμόρφωση ενός επιτυχούς μηχανισμού πρόληψης και αποτροπής της κακής χρήσης τους, μέσα από την υιοθέτηση αναλυτικών διατάξεων αναφορικά με την ευθύνη του παραβάτη-επιχείρησης, την επιβολή κυρώσεων και την αναζήτηση αποζημίωσης, επιβαρύνοντάς τους σημαντικά με υψηλό κόστος και γραφειοκρατικό βάρος επιτήρησης.

Ο Νέος Κανονισμός σέβεται όλα τα θεμελιώδη δικαιώματα και τηρεί τις ελευθερίες και αρχές που αναγνωρίζονται στον Χάρτη όπως κατοχυρώνονται στις Συνθήκες, ιδίως τον σεβασμό της ιδιωτικής και οικογενειακής ζωής, της κατοικίας και των επικοινωνιών, την προστασία των δεδομένων προσωπικού χαρακτήρα, την ελευθερία σκέψης, συνείδησης και θρησκείας, την ελευθερία έκφρασης και πληροφόρησης, την επιχειρηματική ελευθερία, το δικαίωμα πραγματικής προσφυγής και αμερόληπτου δικαστηρίου και την πολιτιστική, θρησκευτική και γλωσσική πολυμορφία. Επιπλέον, αποσαφηνίζοντας ότι τα γενετικά και βιομετρικά δεδομένα χρήζουν ιδιαίτερης προστασίας, τα εντάσσει στις ειδικές κατηγορίες δεδομένων, επιδιώκοντας την μεγαλύτερη δυνατή ασφάλεια δικαίου.

[77] Βλ. Δελλή Γεώργιο, Μελέτη με τίτλο Για μια αποτελεσματική δημόσια προστασία των προσωπικών δεδομένων: Ο «θαυμαστός καινούργιος κόσμος» του Κανονισμού (ΕΕ) 679/2016, ΕφημΔΔ-1/2017

Ο αντίκτυπος της εφαρμογής του Κανονισμού αυτού γίνεται πιο εύκολα καταληπτός αν λάβε κανείς υπόψη τις νέες και πολύ κομβικές ευθύνες των υπεύθυνων επεξεργασίας, όπως αυτές αποτυπώθηκαν στο κύριο σώμα της παρούσας εργασίας, καθώς λόγω του ρόλου και του τρόπου ενέργειάς τους, τόσο οι δημόσιες όσο και οι ιδιωτικές οντότητες θα επωφεληθούν της αυξημένης ασφάλειας δικαίου από την εναρμόνιση και την αποσαφήνιση των κανόνων και των διαδικασιών της ΕΕ για την προστασία των δεδομένων, οι οποίες δημιουργούν ίσους όρους ανταγωνισμού και εξασφαλίζουν συνεκτική επιβολή των κανόνων για την προστασία των δεδομένων, καθώς και σημαντική μείωση του διοικητικού φόρτου. Προκειμένου να διασφαλισθεί δίκαιη και διαφανής επεξεργασία σε σχέση με το υποκείμενο των δεδομένων, λαμβανομένων υπόψη των ειδικών συνθηκών και του πλαισίου εντός του οποίου πραγματοποιείται η επεξεργασία των δεδομένων προσωπικού χαρακτήρα, ο υπεύθυνος επεξεργασίας θα πρέπει να χρησιμοποιεί κατάλληλες μαθηματικές ή στατιστικές διαδικασίες για την κατάρτιση του προφίλ, να εφαρμόζει τεχνικά και οργανωτικά μέτρα, ώστε να διορθώνονται οι παράγοντες που οδηγούν σε ανακρίβειες σε δεδομένα προσωπικού χαρακτήρα και να ελαχιστοποιείται ο κίνδυνος σφαλμάτων, να καθιστά ασφαλή τα δεδομένα προσωπικού χαρακτήρα κατά τρόπο που να λαμβάνει υπόψη τους πιθανούς κινδύνους που συνδέονται με τα συμφέροντα και τα δικαιώματα του υποκειμένου των δεδομένων και κατά τρόπο που να προλαμβάνει, μεταξύ άλλων, τα αποτελέσματα διακρίσεων σε βάρος φυσικών προσώπων βάσει της φυλετικής ή εθνικής καταγωγής, των πολιτικών φρονημάτων, της θρησκείας ή των πεποιθήσεων, της συμμετοχής σε συνδικαλιστικές οργανώσεις, της γενετικής κατάστασης ή της κατάστασης της υγείας ή του γενετήσιου προσανατολισμού, ή μέτρων ισοδύναμου αποτελέσματος.

Η αυτοματοποιημένη λήψη αποφάσεων και κατάρτιση προφίλ που βασίζονται σε ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα θα πρέπει να επιτρέπονται μόνο υπό ειδικές προϋποθέσεις. Τα φυσικά πρόσωπα θα ασκούν καλύτερο έλεγχο στα δεδομένα προσωπικού χαρακτήρα που τα αφορούν και θα μπορούν να εμπιστεύονται το ψηφιακό περιβάλλον διατηρώντας την προστασία τους ακόμη και όταν τα δεδομένα προσωπικού χαρακτήρα που τα αφορούν υποβάλλονται σε επεξεργασία στο εξωτερικό. Θα ενισχυθεί επίσης η λογοδοσία εκείνων που επεξεργάζονται δεδομένα

προσωπικού χαρακτήρα. Ένα συνολικό σύστημα προστασίας των δεδομένων θα καλύπτει επίσης τους τομείς της αστυνομίας και της δικαιοσύνης, ακόμη και πέραν του πρώην τρίτου πυλώνα[78].

Μάλιστα έχουν προσδιορισθεί δείκτες για την παρακολούθηση της υλοποίησης των επιταγών του Κανονισμού που θα αξιολογούνται περιοδικά και θα περιλαμβάνουν τα σημανικά στοιχεία όπως ο χρόνος και το κόστος συμμόρφωσης των υπευθύνων επεξεργασίας δεδομένων προς τη νομοθεσία «άλλων κρατών μελών», τους πόρους που διατίθενται σε αρχές προστασίας δεδομένων, τον ορισμό υπευθύνων επεξεργασίας δεδομένων σε δημόσιους και ιδιωτικούς οργανισμούς, τη χρήση εκτίμησης επιπτώσεων σχετικά με την προστασία δεδομένων, τον αριθμό καταγγελιών από πρόσωπα στα οποία αναφέρονται τα δεδομένα και αποζημίωση που έλαβαν τα πρόσωπα αυτά, τον αριθμό υποθέσεων που είχαν ως αποτέλεσμα τη δίωξη υπευθύνων επεξεργασίας και τα τυχόν επιβληθέντα πρόστιμα σε υπευθύνους επεξεργασίας δεδομένων που κρίθηκαν ένοχοι για παραβιάσεις της προστασίας των δεδομένων.

Ο Κανονισμός θέτει επίσης ως κεντρικό θεσμικό πυλώνα για τη δημόσια εποπτεία στο πεδίο των προσωπικών δεδομένων μια ανεξάρτητη Εποπτική αρχή με αυξημένες εξουσίες και εκτενείς αρμοδιότητες- ελεγκτικές, αδειοδοτικές, συμβουλευτικές, δικαιοπλαστικές και τιμωρητικές. Στο μέτρο μάλιστα που η επεξεργασία δεδομένων έχει έντονο διασυνοριακό χαρακτήρα, λαμβάνεται ιδιαίτερη μέριμνα για την συνεργασία των εθνικών εποπτικών αρχών μεταξύ τους, μέσα από ένα «μηχανισμό συνεκτικότητας».

Ανακεφαλαιώνοντας, με το Γενικό Κανονισμό «βρισκόμαστε ενώπιον ενός νέου διοικητικού δικαίου, στο οποίο το στίγμα της οικονομικής ανάλυσης είναι παραπάνω

[78] Η Αστυνομική και Δικαστική Συνεργασία σε Ποινικές Υποθέσεις (ΑΔΣΠΥ) είναι ο τρίτος από τους Τρεις Πυλώνες της Ευρωπαϊκής Ένωσης, εστιάζει στη συνεργασία της εφαρμογής του νόμου και στην καταπολέμηση του ρατσισμού. Βασίζεται περισσότερο στη διακυβερνητική συνεργασία που σημαίνει ότι τα ιδρύματα της Ένωσης μπορούν να επέμβουν ελάχιστα. Είναι υπεύθυνο για την έκδοση Ευρωπαϊκού Εντάλματος Σύλληψη EUROPA - Glossary - Police and judicial cooperation in criminal matters.

από εμφανές και όπου τα όρια μεταξύ νομικής, οικονομικής και τεχνικής προσέγγισης είναι ρευστά, ενώ η προστασία ενός θεμελιώδους δικαιώματος συνδέεται άρρηκτα με την αποτελεσματική άσκηση των οικονομικών δραστηριοτήτων»[79]. Η επεξεργασία των δεδομένων προσωπικού χαρακτήρα, με τη μορφή μιας μοντέρνας και αποτελεσματικής πάνω από όλα εποπτείας, θα πρέπει να προορίζεται να εξυπηρετεί τον άνθρωπο. Το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα δεν είναι απόλυτο δικαίωμα· πρέπει να εκτιμάται σε σχέση με τη λειτουργία του στην κοινωνία και να σταθμίζεται με άλλα θεμελιώδη δικαιώματα, σύμφωνα με την αρχή της αναλογικότητας (Άρθρο 25 παρ.1 Σ)[80]. Το μεγάλο στοίχημα είναι η εξέταση του τρόπου υλοποίησης στην πράξη των παραπάνω δικαιωμάτων και εν κατακλείδι του επαυξημένου με νέες αρμοδιότητες θεσμού του υπεύθυνου επεξεργασίας προσωπικών δεδομένων μετά τη θέση σε εφαρμογή του, ιδιαίτερα σήμερα σε μια διανυόμενη περίοδο οικονομικής κρίσης.

.

[79] Βλ. Δελλή Γεώργιο, Μελέτη με τίτλο Για μια αποτελεσματική δημόσια προστασία των προσωπικών δεδομένων: Ο «θαυμαστός καινούργιος κόσμος» του Κανονισμού (ΕΕ) 679/2016, ΕφημΔΔ-1/2017

[80]Βλ. Κοντιάδη Ξενοφώντα / Φωτιάδου Αλκμήνη, Κοινωνικά δικαιώματα, αναλογικότητα και δημοσιονομική κρίση.

8. Βιβλιογραφία-Αρθρογραφία

- Αιτιολογική Έκθεση (Proposal for GDPR) για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών, Βρυξέλλες, 25.1.2012

- Αναφορά στην BVerfGE 75, σελ. 1 επ. (Volkszählungsurteil)

- Αραβαντινός Ιωάννης, Η προστασία των στοιχείων προσωπικού χαρακτήρα από την αθέμιτη επεξεργασία μέσω υπολογιστή, Εκδόσεις Σάκκουλας, 1997

- Βαρβέρης Αλέξανδρος, Τεχνικά και Οργανωτικά θέματα - η ϋποχρεωτική τοποθέτηση υπεύθυνου προστασίας δεδομένων, ΕφημΔΔ 2017, σελ. 206 επ.

- Γενικός Κανονισμός Πραστασίας Δεδομένων (ΕΕ 679/2016/GDPR)

- Γέροντας Απόστολος, Η προστασία του πολίτη από την ηλεκτρονική επεξεργασία προσωπικών δεδομένων, Εκδόσεις Σάκκουλα, 2002

- Γιαννόπουλος Γεώργιος, Γενικός Κανονισμός Προστασίας Δεδομένων:οι νέες ευθύνες και υποχρεώσεις του υπεύθυνου επεξεργασίας, ΕφημΔΔ 2017, σελ 199 επ.

- Δόνος Πέτρος, Η συνταγματική κατοχύρωση του δικαιώματος προστασίας του πολίτη από την επεξεργασία των προσωπικών του δεδομένων και της αντίστοιχης ανεξάρτητης αρχής σε: Γ. Παπαδημητρίου (επιμ.), Αναθεώρηση του Συντάγματος και εκσυγχρονισμός των θεσμών, 2000

- Δημητρόπουλος Ανδρέας, Συνταγματικά δικαιώματα, Τόμος Γ΄, Εκδόσεις Σάκκουλα, Αθήνα-Θεσ/κη, 2005

- Δελλής Γεώργιος, Μελέτη με τίτλο Για μια αποτελεσματική δημόσια προστασία των προσωπικών δεδομένων: ο «θαυμαστός καινούργιος κόσμος» του Κανονισμού (ΕΕ) 679/2016, ΕφημΔΔ-1/2017

- Εδώ το πλήρες κείμενο της Σύμβασης108 η Σύμβαση του Συμβουλίου της Ευ-ρώπης «για την προστασία των ατόμων από την αυτόματη επεξεργασία των προσωπικών πληροφοριών» http://conventions.coe.int/Treaty/FR/Treaties/Html/108.htm

- Ελληνική Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα: www.dpa.gr

- Επίσημη Εφημερίδα ΕΕ: αριθ. L 281 της 23/11/1995 σ. 0031 – 0050 http://eur-ex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:el:HTML

- Επίσημη ιστοσελίδα του GDPR www.eugdpr.org , όπου και το πρωτότυπο κείμενό του.

- Ζωγραφόπουλος Δημήτριος, «Το νομικό πλαίσιο προστασίας θεμελιωδών δικαιωμάτων – και ιδίως της ιδιωτικής ζωής- των προσώπων από την επεξεργασία δεδομένωνπροσωπικού χαρακτήρα, Αθήνα, 23 Ιουν 2016.

- Ιστοσελίδα https://academic.oup.com/idpl/article-abstract/4/3/189/2549069

- Ιστοσελίδα http://eur-law.eu/EL/Odegia-97-66-EK-Europaikou-Koinobouliou-Sumbouliou-tes,322993,d

- Ιστοσελίδα https://iapp.org

- Ιστοσελίδα http://www.kathimerini.gr/60966/article/epikairothta/kosmos/h-ee-diekoye-thn-ereyna-sxetika-me-th-xrhsh-ths-vashs-dedomenwn-swift-gia-kataskopeia

- Ιστοσελίδα https://www.lawspot.gr

- Ιστοσελίδα https://www.whitecase.com/publications/alert/unlocking-eu-general-data-protection-regulation

- Κοντιάδης Ξενοφών/ Φωτιάδου Αλκμήνη, Κοινωνικά δικαιώματα, αναλογικότητα και δημοσιονομική κρίση, Εκδόσεις Σάκκουλας, 2006

- Λαζαράκος Γρηγόριος, Ο θεσμός του υπεύθυνου προστασίας προσωπικών δεδομένων (DPO) στο νέο νομοθετικό πλαίσιο των προσωπικών δεδομένων μετά την υιοθέτηση του Κανονισμού ΕΕ/679/2016, Εφαρμογές Δημοσίου Δικαίου 2016

- Λοϊζίδου- Νικολαΐδου Ειρήνη, παρουσίαση με τίτλο «Προστασία Προσωπικών Δεδομένων-Νεοι Ορίζοντες», Επίτροπος Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, διαθέσιμη στην ιστοσελίδα www.icpac.org.cy

- Μούσης Νίκος, Ευρωπαϊκή Ένωση: Δίκαιο, Οικονομία, Πολιτική, 13η ενημερωμένη έκδοση, Εκδόσεις Παπαζήση, Αθήνα, 2011

- Νούσιας Αλέξανδρος, Άρθρο «Καλώς ήρθατε στο Web 3.0.! Ο Γενικός Κανονισμός Προστασίας Δεδομένων και ο Ρόλος του Υπευθύνου Επεξεργασίας Δεδομένων»,25 Ιανουαρίου 2017 στην ιστοσελίδα www.opendata.ellak.gr

- Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών (Επίσημη Εφημερίδα ΕΕ: αριθ. L 281 της 23/11/1995 σ. 0031 – 0050)

- Ομάδα Εργασίας Άρθρου 29, Γνωμοδοτήσεις και Έγγραφα, διαθέσιμα σε: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp117_el.pdf

- Ομάδα εργασίας του άρθρου 29 (2010), Γνώμη 1/2010 σχετικά με τις έννοιες του «υπευθύνου τησεπεξεργασίας» και του «εκτελούντος την επεξεργασία», WP 169, Βρυξέλλες, 16 Φεβρουαρίου 2010

- Ομάδα εργασίας του άρθρου 29 (2010), Guidelines on Data Protection Officers ('DPOs'), 16/EN WP 243 rev.01, τελευταία επικαιροποίηση 5.4.17.

- Παναγοπούλου-Κουτνατζή Φερενίκη, Μελέτη με τίτλο «Τα νέα δικαιώματα για τους πολίτες βάσει του Γενικού Κανονισμού Προστασίας Δεδομένων: μια πρώτη αποτίμηση και συνταγματική αξιολόγηση», δημοσιευμένη στην Εφημ ΔΔ-1/2017.

- Παναγοπούλου-Κουτνατζή Φερενίκη, Ο Γενικός Κανονισμός για την προστασία δεδομένων 679/2016/ΕΕ, Εκδόσεις Σάκκουλα,2017

- Παναγοπούλου Φερενίκη, Πώς θα επιβάλλει η ΑΠΔΠΧ τα πρόστιμα στις ασφαλιστικές από το 2018;,συνέντευξη στη Βίκυ Γερασίμου, Insurance Daily News, 17 Μαρ 2017.

- Πρόταση Κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών (γενικός κανονισμός για την προστασία δεδομένων), διαθέσιμη σε: http://ec.europa.eu/justice/dataprotection/document/review2012, 25 Ιανουαρίου 2012

- Σταθόπουλος Μιχάλης, Πρόλογος στο βιβλίο, Δίκαιο προστασίας δεδομένων του καθηγητή Κ. Χριστοδούλου, Νομική Βιβλιοθήκη, 2013

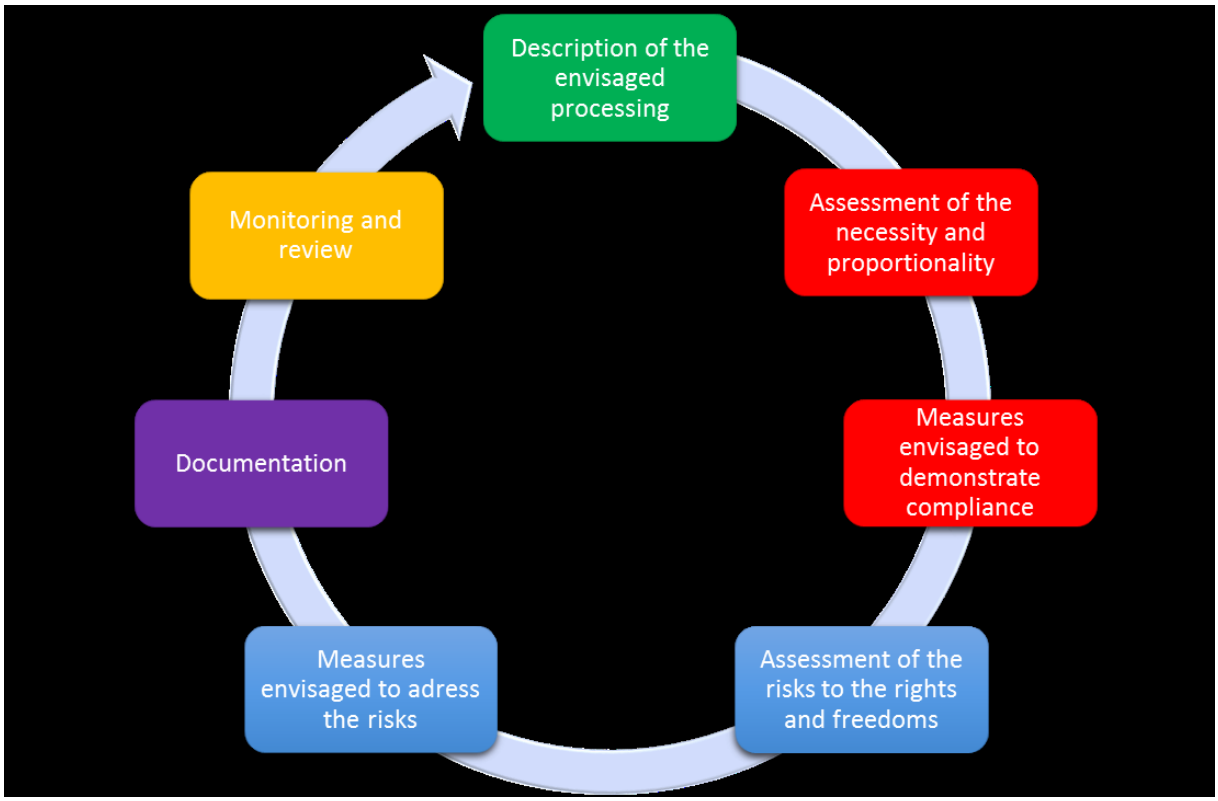
- Σωτηρόπουλος Βασίλης, Η Συνταγματική προστασία των προσωπικών δεδομένων, Εκδόσεις Σάκκουλας, 2006

- Τσολιάς Γρηγόρης, Παρουσίαση με θέμα «Υποχρεώσεις συμμόρφωσης στον Γενικό Κανονισμό Προσωπικών Δεδομένων (GDPR) και ο ρόλος του Υπευθύνου Προστασίας Δεδομένων (DPO)», Δικηγόρος – ΜΔ Ποινικών Επιστημών, Μέλος (αν.) της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, διαθέσιμο στην ιστοσελίδα www.dpa.gr

- Χρυσόγονος Κων/νος, Ατομικά και Κοινωνικά Δικαιώματα, Νομική Βιβλιοθήκη, 3η Έκδοση, 2006

Παράρτημα Α

Το παρακάτω σχήμα απεικονίζει ορίζει τα ελάχιστα χαρακτηριστικά μιας DPIA (άρθρο 35 παράγραφος 7 GDPR και αιτιολογικές σκέψεις 84 και 90):[81]:



[81]Από το ARTICLE 29 DATA PROTECTION WORKING PARTY με τίτλο « **Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679».** Σημείωση: Θα πρέπει να υπογραμμιστεί ότι η διαδικασία που απεικονίζεται εδώ είναι επαναληπτική. Στην πράξη, είναι πιθανό ότι κάθε ένα από τα στάδια επανεξετάζεται πολλές φορές πριν ολοκληρωθεί η DPIA.