ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΗΛΕΚΤΡΙΚΩΝ ΒΙΟΜΗΧΑΝΙΚΩΝ ΔΙΑΤΑΞΕΩΝ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΑΠΟΦΑΣΕΩΝ

Μελέτη του γενικού κανονισμού για την προστασία των δεδομένων (GDPR) και διερεύνηση του πλαισίου συμμόρφωσης τεχνολογικών υλοποιήσεων Blockchain με τις διατάξεις του

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της

ΜΑΡΙΑΣ ΜΠΟΥΜΗ

Επιβλέπων : Δημήτριος Ασκούνης
Καθηγητής Ε.Μ.Π.

Αθήνα, Μάρτιος 2022

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ
ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΗΛΕΚΤΡΙΚΩΝ ΒΙΟΜΗΧΑΝΙΚΩΝ ΔΙΑΤΑΞΕΩΝ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΑΠΟΦΑΣΕΩΝ

Μελέτη του γενικού κανονισμού για την προστασία των δεδομένων (GDPR) και διερεύνηση του πλαισίου συμμόρφωσης τεχνολογικών υλοποιήσεων Blockchain με τις διατάξεις του

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της

ΜΑΡΙΑΣ ΜΠΟΥΜΗ

Επιβλέπων : Δημήτριος Ασκούνης
Καθηγητής Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή της 8ης Μαρτίου 2022.

.....	.....	.....
Δημήτριος Ασκούνης	Ιωάννης Ψαρράς	Χρυσόστομος Δούκας
Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.

Αθήνα, Μάρτιος 2022

.....

ΜΑΡΙΑ ΜΠΟΥΜΗ

Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

Περίληψη

Ο GDPR (Γενικός Κανονισμός για την Προστασία Δεδομένων) τέθηκε σε ισχύ στις 25 Μαΐου 2018 και σχεδιάστηκε για να ενισχύσει τα δικαιώματα των κατοίκων της ΕΕ σχετικά με τον τρόπο με τον οποίο οι οργανισμοί επεξεργάζονται και χρησιμοποιούν τα προσωπικά τους δεδομένα. Από τότε που τέθηκε σε ισχύ ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR), έχουν προκύψει πολλά ερωτήματα σχετικά με τη δυνατότητα εφαρμογής του στην τεχνολογία blockchain. Οι εφαρμογές που βασίζονται σε blockchain σχεδιάστηκαν για να λειτουργούν με αποκεντρωμένο τρόπο, με πολλούς φορείς και συμμετέχοντες σε ένα ευρέως κατανεμημένο δίκτυο. Η μη γραμμική λειτουργία των εφαρμογών που βασίζονται σε blockchain, προκαλεί αρκετές εντάσεις σε σχέση με τον GDPR. Η κύρια εστίαση αυτής της μελέτης είναι ο εντοπισμός των βασικών χαρακτηριστικών της τεχνολογίας blockchain που ενδέχεται να αποτελέσουν πρόκληση για τις απαιτήσεις του GDPR, ιδίως για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων. Επιπλέον, θα διερευνήσουμε πώς μπορούν να χρησιμοποιηθούν εφαρμογές που βασίζονται σε blockchain για να βοηθήσουν στην επίτευξη των στόχων του GDPR.

Λέξεις Κλειδιά: GDPR, blockchain, δικαιώματα, προσωπικά δεδομένα, συμμόρφωση

Abstract

GDPR (General Data Protection Regulation) entered into force on 25 May 2018 and is designed to strengthen the rights of EU citizens regarding the way in which organizations process and use their personal data. Since the entry into force of the General Data Protection Regulation (GDPR), many questions have arisen about its applicability to blockchain technology. Blockchain-based applications are designed to operate in a decentralized manner, with multiple players and participants in a widely distributed network. The non-linear operation of blockchain-based applications is causing considerable tension in relation to the GDPR. The main focus of this study is to identify the key features of blockchain technology that may challenge the requirements of the GDPR, in particular the rights and freedoms of data subjects. In addition, we will explore how blockchainbased applications can be used to help achieve GDPR goals.

Keywords: GDPR, blockchain, rights, personal data, compliance

Ευχαριστίες

Με την ολοκλήρωση της διπλωματικής μου εργασίας αισθάνομαι την ιδιαίτερη υποχρέωση να εκφράσω τις θερμότερες ευχαριστίες μου στον επιβλέποντα και καθηγητή του ΕΜΠ κ. Δημήτρη Ασκούνη, για την επίβλεψη της παρούσας διπλωματικής εργασίας και για την ευκαιρία που μου έδωσε να την εκπονήσω στο εργαστήριο Συστημάτων Αποφάσεων και Διοίκησης.

Στη συνέχεια, θα ήθελα να ευχαριστήσω ιδιαιτέρως τον συνεργάτη του εργαστηρίου Συστημάτων Αποφάσεων και Διοίκησης και υποψήφιο διδάκτωρ κ. Χρήστο Κοντζίνο για την εξαιρετική συνεργασία και καθοδήγηση σε όλη την πορεία της διπλωματικής. Η βοήθεια και οι συμβουλές του ήταν καταλυτικής σημασίας για την επιτυχή ολοκλήρωσή της και ελπίζω να μου δοθεί ξανά η ευκαιρία συνεργασίας μαζί του στο μέλλον.

Τέλος θα ήθελα να ευχαριστήσω την οικογένεια και τους φίλους μου που με στήριξαν σε πολλά επίπεδα κατά τη φοίτησή μου στο Εθνικό Μετσόβιο Πολυτεχνείο, όπως και όλους τους καθηγητές της σχολής Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών που με καθοδήγησαν και με εισήγαγαν στον ευρύ και ξεχωριστό κόσμο του ηλεκτρολόγου μηχανικού.

1. Εισαγωγή

1.1. Ορισμός του Blockchain

Το Blockchain εισήχθη για πρώτη φορά το 2008 με τη μορφή του peer-to-peer κρυπτονομίσματος Bitcoin. Ένα άτομο (ή μια ομάδα) που έγραφε με το ψευδώνυμο Satoshi Nakamoto δημοσίευσε μια αναφορά (white paper) με τίτλο «Bitcoin: A Peer-to-Peer Electronic Cash System» [NAKAMOTO2008]. Σε αυτή την αναφορά, το Bitcoin εμφανίζεται ως μια «καθαρά peer-to-peer έκδοση ηλεκτρονικών μετρητών», που χρησιμοποιεί ένα αποκεντρωμένο δίκτυο για να επιτρέψει μη αναστρέψιμες συναλλαγές. Σε αυτό το νέο σύστημα νομισμάτων ανοιχτού κώδικα, οι συναλλαγές μπορούν να πραγματοποιηθούν μεταξύ των κατόχων του νομίσματος απευθείας μεταξύ τους, χωρίς να περάσουν από μεσάζοντες, όπως χρηματοπιστωτικά ιδρύματα.

Καθώς αυτό το σύστημα δεν βασίζεται σε τρίτα μέρη για την επικύρωση, τη διαφύλαξη και τη διατήρηση των συναλλαγών, οι πληρωμές μπορούν να πραγματοποιηθούν αμέσως και χωρίς τις πρόσθετες χρεώσεις που συνήθως αυξάνουν το κόστος. Επιπλέον, το Bitcoin καθιστά δυνατές μη αναστρέψιμες πληρωμές.

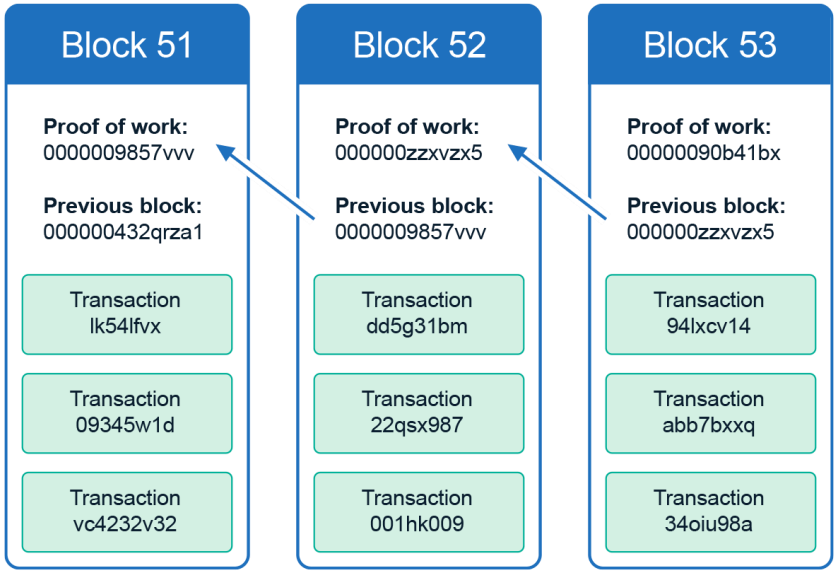
Με το Blockchain, τα δεδομένα διανέμονται μεταξύ όλων των συμμετεχόντων (κόμβων) στο δίκτυο. Τα δεδομένα αποθηκεύονται ως συναλλαγές, και πολλές συναλλαγές συνοψίζονται σε ένα μόνο μπλοκ. Κάθε μπλοκ έχει μια αναφορά στο προηγούμενό του. Μπλοκ μπορούν να προστεθούν μόνο στο τέλος του Blockchain, πράγμα που οδηγεί σε μια δομή δεδομένων που δέχεται μόνο προσαυξήσεις.

Το ιδιαίτερο χαρακτηριστικό του Blockchain είναι ότι οι συμμετέχοντες στο δίκτυο δεν χρειάζεται να εμπιστεύονται πλήρως ο ένας τον άλλον, επειδή η τεχνολογία διασφαλίζει ότι κάθε συμμετέχων συμφωνεί σε μια κοινή συναίνεση. Αυτό επιτυγχάνεται με τους λεγόμενους αλγόριθμους συναίνεσης.

Η τεχνολογία Blockchain μπορεί να χωριστεί σε τρεις κύριους τύπους:

- Public Blockchain: Εντελώς αποκεντρωμένο και ανοιχτό σε όλους
- Ιδιωτικό Blockchain: Εντελώς συγκεντρωμένο και μόνο επιλεγμένοι συμμετέχοντες μπορούν να διαβάζουν και να δημιουργούν συναλλαγές
- Consortium Blockchain: Μερικώς αποκεντρωμένη και διαχειριζόμενη από διάφορους οργανισμούς

Η σύνδεση μεταξύ δύο μπλοκ δημιουργείται από τον κρυπτογραφικό κατακερματισμό (cryptographic hash) ενός μπλοκ που αποθηκεύεται στο διάδοχό του. Το ακόλουθο σχήμα παρέχει μια επισκόπηση αυτής της διαδικασίας.



Σχήμα: Απλοποιημένη αναπαράσταση μιας αλυσίδας μπλοκ (blockchain).

Το γεγονός ότι κάθε μπλοκ συνδέεται με τον πρόδρομό του μέσω του κρυπτογραφικού κατακερματισμού του οδηγεί στο αμετάβλητο ενός Blockchain. Κάθε αλλαγή μιας συναλλαγής, η οποία είναι ήδη αποθηκευμένη στην αλυσίδα, θα τροποποιούσε τον κατακερματισμό κάθε μπλοκ μετά από αυτό και ως εκ τούτου τις τιμές κατακερματισμού ολόκληρου του Blockchain.

Αν και το Bitcoin δεν ήταν η πρώτη εκδήλωση της ιδέας ενός ψηφιακού νομίσματος, ήταν η πρώτη υλοποίηση αυτής της ιδέας και το πρώτο ψηφιακό σύστημα πληρωμών που επέτρεψε με επιτυχία στους συμμετέχοντες του να πραγματοποιούν απευθείας ηλεκτρονικές συναλλαγές, χωρίς να χρειάζεται να έχουν εμπιστοσύνη σε μια κεντρική αρχή, και επίσης έλυσε το πρόβλημα της «διπλής δαπάνης» χωρίς να βασίζεται σε ένα αξιόπιστο τρίτο μέρος.

Αν τα ψηφιακά αρχεία που αντιπροσωπεύουν ένα κρυπτονόμισμα μπορούν να αντιγραφούν ή να παραποιηθούν, με αποτέλεσμα να μπορούν να χρησιμοποιηθούν περισσότερες από μία φορές, αυτό το ελάττωμα ονομάζεται διπλή δαπάνη.

Γενικότερα, **η σημασία του Bitcoin έγκειται στην τεχνολογική δομή, καθώς υλοποιεί την πρώτη χρήση της τεχνολογίας blockchain**. Για αυτόν τον λόγο, οι δύο έννοιες συχνά συγχέονται μεταξύ τους, αν και διαφέρουν σε πολλές άλλες πτυχές. Για παράδειγμα, **το Bitcoin είναι ένα κρυπτονόμισμα** που δημιουργήθηκε βασικά για να απλοποιήσει και να αυξήσει την ταχύτητα των συναλλαγών, χωρίς να βασίζεται στην παρέμβαση ενός κεντρικού οργανισμού ή ενός τρίτου μέρους. Συνολικά, μπορούμε να πούμε ότι **το blockchain είναι η τεχνολογία κορμού (backbone) του Bitcoin**.

Η **τεχνολογία blockchain δεν περιορίζεται στις συναλλαγές κρυπτονομισμάτων, καθώς μπορεί να χρησιμοποιηθεί για τη μεταφορά, επαλήθευση και επικύρωση οποιουδήποτε τύπου δεδομένων ή πληροφοριών**.

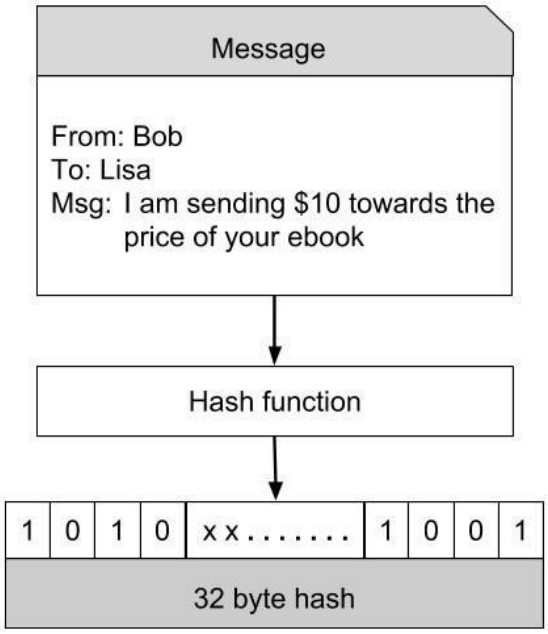
Ωστόσο, ο ορισμός της έννοιας της τεχνολογίας blockchain δεν είναι μια απλή εργασία. Ελλείψει ενός μοναδικού και συναινετικού ορισμού στη βιβλιογραφία του blockchain, πολλοί συγγραφείς τείνουν να χρησιμοποιούν διαφορετικά κριτήρια για να ορίσουν την τεχνολογία blockchain. Για παράδειγμα, ορισμένοι συγγραφείς ορίζουν το blockchain τονίζοντας τα τεχνικά χαρακτηριστικά και τα βασικά του στοιχεία. Άλλοι, με βάση έναν γενικό ορισμό του Bitcoin-Blockchain, εισάγουν μερικές από τις πιο πρόσφατες εξελίξεις αυτής της τεχνολογίας.

Για να οριστεί και να εξηγηθεί τι είναι το blockchain, πρέπει να αναγνωριστεί ότι σύμφωνα με τη βιβλιογραφία δεν υπάρχει μία ενιαία τεχνολογία blockchain, αλλά, αντίθετα, **υπάρχει μια ολόκληρη κατηγορία τεχνολογιών που παρουσιάζουν διαφορετικές τεχνικές και δομές διακυβέρνησης**. Έτσι, οποιαδήποτε προσπάθεια ορισμού της έννοιας του blockchain, εάν υπερβαίνει τα βασικά στοιχεία που είναι κοινά σε όλες τις ποικιλίες αυτής της τεχνολογίας, θα αποτύχει να αναγνωρίσει την ύπαρξη άλλων τύπων blockchain.

Ως απλό παράδειγμα, ο τυπικός ορισμός του blockchain περιλαμβάνει μια αναφορά στον μηχανισμό συναίνεσης (consensus mechanism), ο οποίος χρησιμοποιείται από τους εξορύκτες (miners) για την επικύρωση συνόλων δεδομένων σε εκκρεμότητα και τη δημιουργία μπλοκ ειδήσεων (news blocks) στην αλυσίδα. Αν και αυτή η δυνατότητα είναι κοινή μεταξύ των **DLT** (**Distributed Ledgers Technology** -- τεχνολογία κατανεμημένων λογιστικών βιβλίων), δεν μπορεί να ειπωθεί το ίδιο για άλλα κεντρικά (centralized) αξιόπιστα μοντέλα, όπως οι εφαρμογές που βασίζονται σε blockchain, στις οποίες υπάρχει μόνο μία οντότητα που διαχειρίζεται ολόκληρο το blockchain.

Το blockchain μπορεί γενικά να περιγραφεί ως ένας συγκεκριμένος τύπος βάσης δεδομένων που χρησιμοποιεί ορισμένες κρυπτογραφικές συναρτήσεις (μαθηματικές συναρτήσεις/αλγόριθμοι που χρησιμοποιούνται στην κρυπτογραφία, π.χ. μελέτη και κατασκευή πρωτοκόλλων που εμποδίζουν τρίτα μέρη από πρόσβαση σε ιδιωτικές επικοινωνίες και συναλλαγές) **για την επίτευξη των απαιτήσεων της ακεραιότητας των δεδομένων (data integrity) και του ελέγχου ταυτότητας (identity authentication)**. Αυτά τα δύο στοιχεία της επιτρέπουν να δημιουργεί μια μόνιμη και διαφανή καταγραφή του συνόλου δεδομένων και να πιστοποιεί τα μέρη που συνδέονται με αυτό.

Μια **συνάρτηση κατακερματισμού** (hash function) αντιστοιχίζει τα δεδομένα οποιουδήποτε αυθαίρετου μεγέθους σε δεδομένα σταθερού μεγέθους. Το Bitcoin χρησιμοποιεί συνάρτηση κατακερματισμού SHA-256 που παράγει κατακερματισμό (έξοδο) μεγέθους 256 bit (32 byte), όπως φαίνεται στο σχήμα.



Σχήμα: Hashing.

Ο Bob, ενώ κάνει μια παραγγελία στη Lisa, δημιουργεί ένα μήνυμα παρόμοιο με αυτό που φαίνεται παραπάνω. Αυτό το μήνυμα κατακερματίζεται μέσω μιας συνάρτησης κατακερματισμού που παράγει ένα hash 32 byte. Η ομορφιά αυτού του hash είναι ότι το hash (ο αριθμός 256 bit) θεωρείται μοναδικό για το περιεχόμενο του μηνύματος. Εάν το μήνυμα τροποποιηθεί, η τιμή κατακερματισμού θα αλλάξει. Δεδομένης μιας τιμής κατακερματισμού, είναι αδύνατο να αναδημιουργηθεί το αρχικό μήνυμα.

1.2. Αντικείμενο της διπλωματικής

Ο GDPR (Γενικός Κανονισμός για την Προστασία Δεδομένων) τέθηκε σε ισχύ στις 25 Μαΐου 2018 και σχεδιάστηκε για να ενισχύσει τα δικαιώματα των κατοίκων της ΕΕ σχετικά με τον τρόπο με τον οποίο οι οργανισμοί επεξεργάζονται και χρησιμοποιούν τα προσωπικά τους δεδομένα.

Αυτά τα δικαιώματα συνοψίζονται ουσιαστικά σε δύο βασικά σημεία:

Πρώτον, οι οργανισμοί πρέπει να έχουν σαφή σκοπό για τη συλλογή προσωπικών πληροφοριών και να δίνουν στα άτομα τη δυνατότητα να αναθεωρούν, να τροποποιούν ή να αμφισβητούν τις πρακτικές επεξεργασίας δεδομένων.

Δεύτερον, οι οργανισμοί πρέπει να εφαρμόζουν μέτρα ασφαλείας για την προστασία των προσωπικών δεδομένων από παραβίαση ή κακή χρήση και πρέπει να αποκαλύπτουν τυχόν περιστατικά ασφαλείας που αφορούν αυτά τα δεδομένα.

Από τότε που τέθηκε σε ισχύ ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR), έχουν προκύψει πολλά ερωτήματα σχετικά με τη δυνατότητα εφαρμογής του στην τεχνολογία blockchain. Εκ πρώτης όψεως, αυτή η καινοτόμος κατηγορία νέων τεχνολογιών φαίνεται να μην μπορεί να συμμορφωθεί με τις απαιτήσεις του GDPR, λόγω της αμετάβλητης, αποκεντρωμένης και βασισμένης στη διαφάνεια φύσης της, περιορίζοντας έτσι τη δική της ανάπτυξη και, κατά συνέπεια, θέτοντας σε κίνδυνο την ευρωπαϊκή ψηφιακή αγορά και την τεχνολογική της ανάπτυξη.

Ταυτόχρονα, δεδομένου ότι ο σεβασμός των ανθρωπίνων δικαιωμάτων αποτελεί μια από τις σημαντικότερες βασικές αξίες της Ευρωπαϊκής Ένωσης, η προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα καθιερώνεται ρητώς στα πιο σχετικά μέσα της Ευρωπαϊκής Ένωσης , συγκεκριμένα σύμφωνα με το άρθρο 8 παράγραφος 1 του Χάρτη των Θεμελιωδών Δικαιωμάτων και το άρθρο 16 παράγραφος 1 της Συνθήκης για τη Λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ). Από αυτή την άποψη, η ανάπτυξη της εσωτερικής αγοράς και η προώθηση των ανθρωπίνων δικαιωμάτων πρέπει να βρουν μια δίκαιη ισορροπία, επιτρέποντας στην Ευρωπαϊκή Ένωση να επιτύχει τους οικονομικούς της στόχους, χωρίς να θυσιάζει την προστασία των ανθρωπίνων δικαιωμάτων, και αντιστρόφως.

Όπως θα παρατηρήσουμε μέσω αυτής της μελέτης, ο GDPR υποθέτει σιωπηρά ότι τα δεδομένα ελέγχονται ή υποβάλλονται σε επεξεργασία από αναγνωρίσιμους φορείς, με συγκεντρωτικό τρόπο. Αντίθετα, οι εφαρμογές που βασίζονται σε blockchain σχεδιάστηκαν για να λειτουργούν με αποκεντρωμένο τρόπο, με πολλούς φορείς και συμμετέχοντες σε ένα ευρέως κατανεμημένο δίκτυο. Η μη γραμμική λειτουργία των εφαρμογών που βασίζονται σε blockchain, σε σχέση με τον GDPR, προκαλεί αρκετές εντάσεις, οι οποίες οδήγησαν στην ιδέα ότι η δική τους είναι μια ασυμβίβαστη σχέση.

Προκειμένου να δοθεί λεπτομέρεια στη φύση αυτών των εντάσεων, η κύρια εστίαση αυτής της μελέτης είναι ο εντοπισμός των βασικών χαρακτηριστικών της τεχνολογίας blockchain που ενδέχεται να αποτελέσουν πρόκληση για την απαίτηση του GDPR, ιδίως για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων. Επιπλέον, θα διερευνήσουμε πώς μπορούν να χρησιμοποιηθούν εφαρμογές που βασίζονται σε blockchain για να βοηθήσουν στην επίτευξη των στόχων του GDPR.

Αφού προσδιορίσουμε τα κύρια στοιχεία των εφαρμογών που βασίζονται σε blockchain, θα εξετάσουμε τους διαφορετικούς τύπους blockchain και τους ρόλους που μπορούν να αναλάβουν οι συμμετέχοντες σε κάθε μία από αυτές. Στη συνέχεια, θα μελετήσουμε λεπτομερέστερα τις υπάρχουσες πολυπλοκότητες και αβεβαιότητες που εισάγει αυτή η τεχνολογία σε σχέση με τις απαιτήσεις του GDPR. Τέλος, διερευνούμε τις τεχνολογικές λύσεις που μπορούν να

ενσωματωθούν σε εφαρμογές που βασίζονται σε blockchain για να συμμορφωθούν με τον GDPR και να βοηθήσουν στην επίτευξη των στόχων του GDPR.

Η συμμόρφωση με τον GDPR δεν αφορά την ίδια την τεχνολογία, αλλά μάλλον τον τρόπο με τον οποίο χρησιμοποιείται η τεχνολογία. Παρά την αναγνώριση της ανάγκης διεξαγωγής ανάλυσης κατά περίπτωση, αυτή η μελέτη στοχεύει να παράσχει μια γενική επισκόπηση της εφαρμογής των απαιτήσεων του GDPR στους διάφορους τύπους εφαρμογών που βασίζονται σε blockchain.

Για να ολοκληρώσουμε αυτήν την ανάλυση, θα παρέχουμε πρώτα μια επισκόπηση της τεχνολογίας blockchain, επισημαίνοντας τα κύρια χαρακτηριστικά της τόσο από τεχνική όσο και από νομική άποψη.

1.2.1. Συνεισφορά στην έρευνα

Εποπτικά, η συγκεκριμένη διπλωματική βοήθησε στην εξερεύνηση και ανάλυση της νέας ευρωπαϊκής νομοθεσίας για την προστασία των προσωπικών δεδομένων, του κανονισμού GDPR καθώς και ο αντίκτυπος που έχει στην καινοτόμα τεχνολογία blockchain. Συγκεκριμένα, η συνεισφορά της διπλωματικής μπορεί να εντοπιστεί στα επόμενα σημεία:

- Ανάλυση της Ευρωπαϊκής νομοθεσίας για την προστασία των προσωπικών δεδομένων, της έννοιας των προσωπικών δεδομένων και των βασικών διατάξεων του GDPR.
- Ανάλυση των ηθικών διατάξεων που διέπουν την υλοποίηση λύσεων υπό το πρίσμα του GDPR και διασφαλίζουν την ασφάλεια των δεδομένων καθώς και τα δικαιώματα των χρηστών επί των προσωπικών τους δεδομένων.
- Θεωρητική ανάλυση της τεχνολογίας blockchain υπό το πλαίσιο του κανονισμού GDPR και παρουσίαση του αντικτύπου που είχε ο GDPR σε λύσεις blockchain.
- Βιβλιογραφική ανασκόπηση και παρουσίαση ερευνητικών προσεγγίσεων που επιχειρούν να παράξουν/υλοποιήσουν λύσεις blockchain, οι οποίες συμμορφώνονται με τις διατάξεις του GDPR.
- Δημιουργία μίας ενοποιημένης μεθοδολογίας για την παραγωγή λύσεων blockchain οι οποίες υπακούν τις διατάξεις του GDPR και μπορούν να αποτελέσουν οδηγό για μελλοντικές λύσεις blockchain.

1.3. Οργάνωση κειμένου

Το παρόν κείμενο είναι οργανωμένο ως εξής:

Το κεφάλαιο 1 αποτελεί την εισαγωγή της διπλωματικής, όπου παρουσιάζεται συνοπτικά η τεχνολογία blockchain, ενώ περιλαμβάνονται επίσης, το αντικείμενο της διπλωματικής, η συνεισφορά της στην έρευνα και η οργάνωση του κειμένου.

Το κεφάλαιο 2 πραγματοποιεί μία ιστορική αναδρομή στο ιστορικό της Ευρωπαϊκής νομοθεσίας για την προστασία των προσωπικών δεδομένων.

Το κεφάλαιο 3 παρουσιάζει το θεωρητικό υπόβαθρο της έννοιας των προσωπικών δεδομένων.

Στο κεφάλαιο 4 παρουσιάζεται ο κανονισμός GDPRκαι οι πιο σημαντικές του διατάξεις.

Το κεφάλαιο 5 περιλαμβάνει σημαντικές ηθικές διατάξεις που πρέπει να ακολουθούνται υπό το πρίσμα του GDPR για την παραγωγή λύσεων, οι οποίες υπακούν το GDPR και σέβονται τα προσωπικά δεδομένα των χρηστών και τα λοιπά δικαιώματά τους.

Το κεφάλαιο 6 αποτελεί την εισαγωγή και το θεωρητικό υπόβαθρο της τεχνολογίας blockchain.

Στο κεφάλαιο 7 παρουσιάζεται ο αντίκτυπος του κανονισμού στο blockchainκαι οι διάφορες εντάσεις ανάμεσα στις διατάξεις του κανονισμού και τα τεχνικά χαρακτηριστικά του blockchain.

Το κεφάλαιο 8 αποτελεί ανασκόπηση της ερευνητικής βιβλιογραφίας σχετικά με την ανάπτυξη λύσεων blockchain, οι οποίες υπακούν τις διατάξεις του GDPR.

Στο κεφάλαιο 9, παρουσιάζεται ενοποιημένη μεθοδολογία, η οποία αποτελείται από διακριτά βήματα, τα οποία, εφόσον ακολουθηθούν, μπορούν να οδηγήσουν στην παραγωγή νομικά και ηθικά συναινετικών λύσεων.

Στο κεφάλαιο 10 παρουσιάζονται τα συμπεράσματα της παρούσας διπλωματικής και οι μελλοντικές προοπτικές της.

Το κεφάλαιο 11 περιλαμβάνει τη βιβλιογραφία της διπλωματικής.

2. Η Ευρωπαϊκή νομοθεσία

2.1. Η Ιδιωτική ζωή (privacy)

Το δίκαιο της ΕΕ αποτελείται από το πρωτογενές δίκαιο της ΕΕ, δηλαδή τη Συνθήκη για την Ευρωπαϊκή Ένωση (ΣΕΕ) [ΣΕΕ2007], και τη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ - Συνθήκη της Λισαβόνας) [ΣΛΕΕ2009], και το παράγωγο δίκαιο της ΕΕ, δηλαδή κανονισμούς, οδηγίες και αποφάσεις της ΕΕ.

Η ιδιωτική ζωή και η προστασία δεδομένων, αν και συνδέονται, αναγνωρίζονται κοινώς σε όλο τον κόσμο ως δύο ξεχωριστά δικαιώματα. Στην Ευρώπη, θεωρούνται ζωτικής σημασίας στοιχεία για μια βιώσιμη δημοκρατία.

Στην ΕΕ, η ανθρώπινη αξιοπρέπεια αναγνωρίζεται ως απόλυτο θεμελιώδες δικαίωμα. Σε αυτήν την έννοια της αξιοπρέπειας, της ιδιωτικής ζωής ή του δικαιώματος στην ιδιωτική ζωή, η αυτονομία, ο έλεγχος των πληροφοριών παίζει καθοριστικό ρόλο.

Ιστορικά, σε άλλα μέρη του κόσμου, όπως οι Η.Π.Α., η ιδιωτική ζωή έχει συχνά θεωρηθεί ως στοιχείο ελευθερίας, του δικαιώματος να είσαι απαλλαγμένος από εισβολές από το κράτος.

Οι πρόσφατες καινοφανείς εξελίξεις στο πεδίο της πληροφορικής και επικοινωνιακής τεχνολογίας προκαλούν προβληματισμό όσον αφορά τον έλεγχο του ατόμου επί των προσωπικών του πληροφοριών. Το άτομο έρχεται αντιμέτωπο με απειλές του ιδιωτικού του βίου οι οποίες προέρχονται τόσο από το κράτος όσο και από την ιδιωτική αγορά, τα ΜΜΕ, τις επιχειρήσεις. Αστυνομικές αρχές, ιδιωτικές και δημόσιες τράπεζες δεδομένων αξιοποιούν τις σύγχρονες δυνατότητες της τεχνολογίας προκειμένου να συλλέξουν, να αποθηκεύσουν και να επεξεργαστούν προσωπικά δεδομένα για να εξυπηρετήσουν διωκτικούς σκοπούς, σκοπούς δημόσιας ασφάλειας ή ακόμη και εμπορικούς, καταναλωτικούς στόχους.

Η πρόκληση της προστασίας των προσωπικών δεδομένων είναι στο πλαίσιο αυτό διεθνής, χωρίς αυτό να σημαίνει ότι έχουμε αυτή τη στιγμή κάποια κοινά διεθνή standard προστασίας. Περισσότερο αυτό που παρατηρείται είναι μια αποσπασματική εικόνα, η οποία ανταποκρίνεται σε επιμέρους εθνικές πολιτικές. Το συνταγματικό και νομοθετικό ενωσιακό πλαίσιο επιτυγχάνει να ενσωματώσει βασικές αξίες του ευρωπαϊκού νομικού πολιτισμού, όπως η προστασία της αξιοπρέπειας, της προσωπικότητας και της ιδιωτικότητας του ατόμου.

2.2. Η Ιδιωτική ζωή ως θεμελιώδες δικαίωμα

Σχεδόν κάθε χώρα στον κόσμο αναγνωρίζει την ιδιωτικότητα με κάποιο τρόπο, είτε πρόκειται για το σύνταγμά τους είτε για άλλες διατάξεις. Επιπλέον, ιδιωτική ζωή αναγνωρίζεται ως παγκόσμιο ανθρώπινο δικαίωμα ενώ η προστασία δεδομένων όχι – τουλάχιστον όχι ακόμη. Το δικαίωμα στην ιδιωτική ζωή κατοχυρώνεται στην Οικουμενική Διακήρυξη των Ανθρωπίνων Δικαιωμάτων -- Universal Declaration of Human Rights (άρθρο 12) [ΟΙΚΟΥΜΕΝΙΚΗ1948], στην Ευρωπαϊκή Σύμβαση Ανθρωπίνων Δικαιωμάτων -- European Convention of Human Rights (άρθρο 8) [ΕΥΡΩΠΑΙΚΗ1950], και στον Ευρωπαϊκό Χάρτη Θεμελιωδών Δικαιωμάτων European Charter of Fundamental Rights

(άρθρο 7) [ΕΥΡΩΠΑΙΚΟΣ2000].

Η προστασία των προσωπικών δεδομένων αναγνωρίζεται στην ΕΕ στο συνταγματικό επίπεδο, ως πτυχή της προστασίας της ιδιωτικότητας σύμφωνα με το άρθρο 8 της ΕΣΑΔ στην προστασία των δικαιωμάτων της οποίας παραπέμπει το άρθρο 6 § 3 της ΣΕΕ, όπου τονίζεται η δεσμευτικότητα των θεμελιωδών δικαιωμάτων που απορρέουν από την ΕΣΑΔ και από τις συνταγματικές παραδόσεις των κρατών-μελών για την ΕΕ. Η "συνταγματική" αυτή υποχρέωση τονίζεται και στο προοίμιο (σημείο 6) της βασικής, για την προστασία των προσωπικών δεδομένων στην ΕΕ, Οδηγίας 95/46, όπου και ορίζεται ότι ο στόχος των κρατών μελών κατά την εφαρμογή της νομοθεσίας σχετικά με την προστασία των προσωπικών δεδομένων είναι η προστασία της ιδιωτικότητας, όπως αυτή αναγνωρίζεται στο άρθρο 8 §1 ΕΣΑΔ.

Η θετική υποχρέωση των οργάνων αλλά και των κρατών-μελών της ΕΕ να προστατεύουν τα προσωπικά δεδομένα αναγνωρίζεται ρητά και στο άρθρο 16 της Συνθήκης της Λισαβόνας, το οποίο επιβάλει την προστασία των προσωπικών δεδομένων, οριζόντια στο σύνολο των ενωσιακών πολιτικών. Ωστόσο, σε συνταγματικό επίπεδο, η σημαντικότερη σε επίπεδο ΕΕ εξέλιξη είναι η κατοχύρωση του δικαιώματος στην προστασία των προσωπικών δεδομένων ως αυτόνομου, θεμελιώδους δικαιώματος στο άρθρο 8 της Χάρτας Θεμ. Δικαιωμάτων της ΕΕ (πέρα από την κατοχύρωση του δικαιώματος στην ιδιωτική και οικογενειακή ζωή. Η κατοχύρωση αυτή, το κατατάσσει στα θεμελιώδη δικαιώματα νέας γενιάς τα οποία παράγει η παγκοσμιοποίηση και η τεχνολογία. Περαιτέρω, στη Χάρτα την οποία η Συνθήκη της Λισαβόνας έχει καταστήσει δεσμευτική, κατοχυρώνονται και μια σειρά από αρχές που εγγυώνται περαιτέρω την προστασία των προσωπικών δεδομένων, όπως η νόμιμη και δικαιολογημένη από σκοπούς δημοσίου συμφέροντος επεξεργασία τους, η ανάγκη συναίνεσης του υποκειμένου τους και προστασίας του από Αν. Αρχή.

2.3. Η Ευρωπαϊκή Νομολογία για το Δικαίωμα στην Προστασία Δεδομένων

Το απόρρητο και η προστασία δεδομένων είναι δύο δικαιώματα που κατοχυρώνονται στις Συνθήκες της ΕΕ και στον Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ. Ο Χάρτης περιέχει ρητό δικαίωμα στην προστασία των προσωπικών δεδομένων (άρθρο 8) το οποίο έχει ως εξής: « 1. Κάθε πρόσωπο έχει δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν. 2. Η επεξεργασία αυτών των δεδομένων πρέπει να γίνεται νομίμως, για καθορισμένους σκοπούς και με βάση τη συγκατάθεση του ενδιαφερομένου ή για άλλους θεμιτούς λόγους που προβλέπονται από το νόμο. Κάθε πρόσωπο δικαιούται να έχει πρόσβαση στα συλλεγέντα δεδομένα που το αφορούν και να επιτυγχάνει τη διόρθωσή τους. 3. Ο σεβασμός των κανόνων αυτών υπόκειται στον έλεγχο ανεξάρτητης αρχής. »

Η έναρξη ισχύος της Συνθήκης της Λισαβόνας το 2009 έδωσε στον Χάρτη των Θεμελιωδών Δικαιωμάτων την ίδια νομική αξία με τις συνταγματικές συνθήκες της ΕΕ. Επομένως, τα θεσμικά όργανα και οι οργανισμοί της ΕΕ και τα κράτη μέλη δεσμεύονται από αυτήν.

Επιπλέον, το άρθρο 16 της Συνθήκης για τη Λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ) υποχρεώνει την ΕΕ να θεσπίσει κανόνες προστασίας δεδομένων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Η ΕΕ είναι μοναδική στο να προβλέπει μια τέτοια υποχρέωση στο σύνταγμά της.

Το θεμελιώδες αυτό δικαίωμα συνδέεται εξάλλου ευθέως με το δικαίωμα στον σεβασμό της ιδιωτικής και οικογενειακής ζωής, το οποίο καθιερώνεται στο άρθρο 7 του Χάρτη. Το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα προβλέπεται επίσης στο άρθρο 16, παράγραφος 1, της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ), το οποίο διαδέχθηκε συναφώς το άρθρο 286 ΣΕΚ.

Όσον αφορά το παράγωγο δίκαιο, από τα μέσα της δεκαετίας του 1990 ο νομοθέτης της τότε Ευρωπαϊκής Κοινότητας είχε εκδώσει διάφορες πράξεις με σκοπό να διασφαλίσει την προστασία των δεδομένων προσωπικού χαρακτήρα. Η οδηγία 95/46/ΕΚ για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών, η οποία εκδόθηκε βάσει του άρθρου 100 Α ΣΕΚ, αποτελούσε τη βασική νομική πράξη της Ένωσης στον εν λόγω τομέα. Όριζε υπό ποιες γενικώς προϋποθέσεις επιτρεπόταν η επεξεργασία των δεδομένων αυτών, καθώς και ποια ήταν τα δικαιώματα των ενδιαφερόμενων προσώπων, και προέβλεπε ειδικότερα τη σύσταση ανεξάρτητων αρχών ελέγχου στα κράτη μέλη.

Ακολούθως, η οδηγία 2002/58/ΕΚ συμπλήρωσε την οδηγία 95/46/ΕΚ, εναρμονίζοντας τις διατάξεις της νομοθεσίας των κρατών μελών για την προστασία της ιδιωτικής ζωής, όσον αφορά ιδίως την επεξεργασία των δεδομένων προσωπικού χαρακτήρα στον τομέα των ηλεκτρονικών επικοινωνιών . Σημειωτέον ότι πρόθεση του νομοθέτη της Ένωσης είναι να επανεξεταστεί η ως άνω οδηγία.

Ειδικότερα, η Επιτροπή υπέβαλε, στις 10 Ιανουαρίου 2017, πρόταση για την αντικατάσταση της οδηγίας αυτής με κανονισμό για την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες.

Επιπλέον, στο πλαίσιο του χώρου ελευθερίας, ασφάλειας και δικαιοσύνης (πρώην άρθρα 30 και 31 ΣΕΕ), η απόφασηπλαίσιο 2008/977/ΔΕΥ ρύθμιζε, έως τον Μάιο του 2018, την προστασία των δεδομένων προσωπικού χαρακτήρα στους τομείς της αστυνομικής και δικαστικής συνεργασίας σε ποινικές υποθέσεις.

Το 2016 η Ευρωπαϊκή Ένωση μεταρρύθμισε το όλο νομικό πλαίσιο στον τομέα αυτό. Προς τούτο, εξέδωσε, αφενός, τον κανονισμό (ΕΕ) 2016/679 σχετικά με την προστασία των δεδομένων, ο οποίος καταργεί την οδηγία 95/46/ΕΚ και ισχύει από τις 25 Μαΐου 2018, και, αφετέρου, την οδηγία (ΕΕ) 2016/680 για την προστασία των εν λόγω δεδομένων σε ποινικές υποθέσεις, η οποία καταργεί την απόφαση-πλαίσιο 2008/977/ΔΕΥ και θα πρέπει να μεταφερθεί από τα κράτη μέλη στο εθνικό τους δίκαιο έως τις 6 Μαΐου 2018.

Τέλος, στο πλαίσιο της επεξεργασίας από τα όργανα και τους οργανισμούς της ΕΕ, η προστασία των δεδομένων προσωπικού χαρακτήρα διασφαλιζόταν, αρχικώς, από τον κανονισμό (ΕΚ) 45/2001. Στον κανονισμό αυτό βασίστηκε, ειδικότερα, η δημιουργία, το 2004, του θεσμού του Ευρωπαίου Επόπτη Προστασίας Δεδομένων.

Το 2018 η Ευρωπαϊκή Ένωση απέκτησε νέο νομικό πλαίσιο στον συγκεκριμένο τομέα, ειδικότερα μέσω της έκδοσης του κανονισμού (ΕΕ) 2018/1725, ο οποίος καταργεί τον κανονισμό 45/2001 και την απόφαση 1247/2002/ΕΚ 10 και εφαρμόζεται από τις 11 Δεκεμβρίου 2018. Για την προαγωγή συνεκτικής προσέγγισης στην προστασία των δεδομένων προσωπικού χαρακτήρα σε ολόκληρη την Ένωση, σκοπός του νέου αυτού κανονισμού είναι η ευθυγράμμιση, στο μέτρο του δυνατού, των σχετικών κανόνων με το καθεστώς που θέσπισε ο κανονισμός (ΕΕ) 2016/679.

2.4. Η Οικουμενική Διακήρυξη Ανθρωπίνων Δικαιωμάτων των Ηνωμένων Εθνών (UDHR)

Για πρώτη φορά, το δικαίωμα στην προστασία της ιδιωτικής σφαίρας ενός ατόμου καθιερώθηκε στο άρθρο 12 της Οικουμενικής Διακήρυξης των Ανθρωπίνων Δικαιωμάτων των Ηνωμένων Εθνών (UDHR) του 1948 για το σεβασμό της ιδιωτικής και οικογενειακής ζωής [ΟΙΚΟΥΜΕΝΙΚΗ1948]. Η Διακήρυξη υιοθετήθηκε από τη Γενική Συνέλευση των Ηνωμένων Εθνών το 1948, και ήταν το αποτέλεσμα των συνεπειών του Β΄ Παγκοσμίου Πολέμου. Οι ηγέτες του κόσμου αποφάσισαν να συμπληρώσουν τον Χάρτη των Ηνωμένων Εθνών με ένα οδικό χάρτη που θα εγγυάτο τα δικαιώματα για όλους τους ανθρώπους παντού στον κόσμο. Το τελικό κείμενο ολοκληρώθηκε σε λιγότερο από δύο χρόνια. Στις 10 Δεκεμβρίου 1948 η Οικουμενική Διακήρυξη των Δικαιωμάτων του Ανθρώπου υιοθετείται από τη Γενική Συνέλευση του ΟΗΕ. Είναι σημαντικό ότι καμία από τις χώρες που αντιπροσωπεύονταν στην Γενική Συνέλευση δεν ψήφισε ενάντια στη Διακήρυξη και ότι ακόμη και αυτές που απείχαν από την τελική ψηφοφορία, είχαν συμμετάσχει και συνεργαστεί στις ενδιάμεσες διαδικασίες σύνταξης. Σε μια εποχή όπου κόσμος είχε χωριστεί στο Δυτικό και Ανατολικό μπλοκ, το να βρεθεί ένας κοινός τόπος επί της ουσίας του κειμένου αποδεικνύει ότι ήταν ένα τεράστιο επίτευγμα.

Η αναγνώριση της σύμφυτης αξιοπρέπειας καθώς και των ίσων και αναπαλλοτρίωτων δικαιωμάτων όλων των μελών της ανθρώπινης οικογένειας αποτελεί το θεμέλιο της ελευθερίας, της δικαιοσύνης και της ειρήνης στον κόσμο. Η παραγνώριση και η περιφρόνηση των δικαιωμάτων του ανθρώπου οδήγησαν σε πράξεις βαρβαρότητας που εξεγείρουν την ανθρώπινη συνείδηση, και η προοπτική ενός κόσμου όπου οι άνθρωποι θα απολαμβάνουν την ελευθερία του λόγου και της πίστης, λυτρωμένοι από τον τρόμο και την αθλιότητα, έχει διακηρυχθεί ως η πιο υψηλή επιδίωξη του ανθρώπου. Εχει ουσιαστική σημασία να προστατεύονται τα ανθρώπινα δικαιώματα από ένα καθεστώς δικαίου, ώστε το άτομο να μην αναγκάζεται να προσφεύγει, ως έσχατο καταφύγιο, στην εξέγερση κατά της τυραννίας και της καταπίεσης. Έχει ουσιαστική σημασία να προωθηθεί η ανάπτυξη φιλικών σχέσεων ανάμεσα στα έθνη. Οι λαοί των Ηνωμένων Εθνών, με τον Καταστατικό Χάρτη, διακήρυξαν και πάλι την πίστη τους στα θεμελιώδη δικαιώματα του ατόμου, στην αξιοπρέπεια και την αξία της ανθρώπινης προσωπικότητας, στην ισότητα δικαιωμάτων ανδρών και γυναικών, και έδειξαν πως είναι

αποφασισμένοι να προωθήσουν την κοινωνική πρόοδο και καλύτερες συνθήκες ζωής στο πλαίσιο μιας ευρύτερης ελευθερίας. Η Γενική Συνέλευση ανακηρύσσει την παρούσα Οικουμενική Διακήρυξη των Δικαιωμάτων του Ανθρώπου ως κοινό ιδανικό.

2.5. Η Ευρωπαϊκή Σύμβαση για τα Ανθρώπινα Δικαιώματα (1950)

Το Συμβούλιο της Ευρώπης, όπως συγκροτήθηκε στον απόηχο του Β' Παγκοσμίου Πολέμου, υιοθέτησε την Ευρωπαϊκή Σύμβαση για την Προστασία των Δικαιωμάτων του Ανθρώπου και των Θεμελιωδών Ελευθεριών (Ευρωπαϊκή Σύμβαση για τα Ανθρώπινα Δικαιώματα - ΕΣΔΑ) το 1950, η οποία τέθηκε σε ισχύ το 1953 [ΕΥΡΩΠΑΙΚΗ1950]. Η ΕΣΔΑ ορίζει μια σειρά από θεμελιώδη δικαιώματα και ελευθερίες (δικαίωμα στη ζωή, απαγόρευση βασανιστηρίων, απαγόρευση της δουλείας και της καταναγκαστικής εργασίας, δικαίωμα στην ελευθερία και ασφάλεια, δικαίωμα σε δίκαιη δίκη, καμία τιμωρία χωρίς νόμο, δικαίωμα σεβασμού της ιδιωτικής ζωής και της οικογένειας ζωή, ελευθερία σκέψης, συνείδησης και θρησκείας, ελευθερία έκφρασης, ελευθερία του συνέρχεσθαι και του συνεταιρίζεσθαι, δικαίωμα γάμου, δικαίωμα αποτελεσματικής ένδικης προστασίας, απαγόρευση των διακρίσεων). Περισσότερα δικαιώματα παρέχονται από πρόσθετα πρωτόκολλα στη Σύμβαση. Αξίζει να σημειωθεί ότι, βάσει της Συνθήκης της Λισαβόνας, τα θεμελιώδη δικαιώματα, όπως κατοχυρώνονται από την ΕΣΔΑ και όπως απορρέουν από τις συνταγματικές παραδόσεις των κρατών μελών, αποτελούν τις γενικές αρχές του δικαίου της Ένωσης.

Σύμφωνα με την ΕΣΔΑ, το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα κατοχυρώνεται στο άρθρο 8 ως μέρος του δικαιώματος σεβασμού της ιδιωτικής και οικογενειακής ζωής, της κατοικίας και της αλληλογραφίας και καθορίζει τους όρους υπό τους οποίους επιτρέπονται περιορισμοί αυτού του δικαιώματος, όπως όταν με το νόμο και προς τα συμφέροντα.

2.6. Σύμβαση του Συμβουλίου της Ευρώπης για την προστασία των ατόμων (1981)

Σε ανάγκη ανάπτυξης πιο λεπτομερών κανόνων για την προστασία των ατόμων με την προστασία των προσωπικών τους δεδομένων και ακολουθώντας μια σειρά ψηφισμάτων που εγκρίθηκαν από την Επιτροπή Υπουργών του Συμβουλίου της Ευρώπης, το 1981 η Σύμβαση για την προστασία των ατόμων έναντι της αυτόματης επεξεργασίας δεδομένων προσωπικού χαρακτήρα (Σύμβαση 108) άνοιξε για υπογραφή [ΠΡΟΣΤΑΣΙΑ1981]. Η Σύμβαση 108 εφαρμόζεται σε κάθε επεξεργασία δεδομένων που πραγματοποιείται τόσο από τον ιδιωτικό όσο και από τον δημόσιο τομέα, συμπεριλαμβανομένων των δικαστικών αρχών και των αρχών επιβολής του νόμου και επιδιώκει να ρυθμίσει τη διασυνοριακή ροή δεδομένων προσωπικού χαρακτήρα. Καθορίζει αρχές για τη συλλογή και επεξεργασία δεδομένων προσωπικού χαρακτήρα για την προστασία των ατομικών καταχρήσεων φόρμας κατά τη διάρκεια αυτής της διαδικασίας, δηλαδή δίκαιη και νόμιμη συλλογή και αυτόματη επεξεργασία δεδομένων, αποθήκευση για καθορισμένους νόμιμους σκοπούς (νομιμότητα) και για τον απαραίτητο και κατάλληλο χρόνο και χρήση συμβατή με τους νόμιμους σκοπούς.

Τα δεδομένα που υποβάλλονται σε επεξεργασία πρέπει να είναι επαρκή, συναφή, ανάλογα με το σκοπό και ακριβή (ποιότητα δεδομένων, αναλογικότητα). Ταυτόχρονα, τα «ευαίσθητα δεδομένα», όπως η φυλή, η πολιτική, η υγεία, η θρησκεία, η σεξουαλική ζωή ή το ποινικό μητρώο ενός ατόμου εξαιρούνται από τη συλλογή και την επεξεργασία, εκτός εάν πληρούνται οι απαραίτητες νομικές απαιτήσεις. Επιπλέον, σύμφωνα με τη Σύμβαση, το άτομο έχει το δικαίωμα να γνωρίζει ότι αποθηκεύονται πληροφορίες σε αυτό και, εάν είναι απαραίτητο, να αντιδράσει (διαφάνεια και ελεύθερη, συγκεκριμένη και ενημερωμένη συναίνεση). Περιορισμοί στα παρεχόμενα δικαιώματα είναι δυνατοί μόνο σε περίπτωση που διακυβεύονται υπέρτατα συμφέροντα, όπως η κρατική ασφάλεια ή η άμυνα.

Το 2017 η Συμβουλευτική Επιτροπή της Σύμβασης για την Προστασία των Ατόμων σε σχέση με την αυτόματη επεξεργασία δεδομένων προσωπικού χαρακτήρα εξέδωσε τις κατευθυντήριες γραμμές για την προστασία των ατόμων έναντι της επεξεργασίας προσωπικών δεδομένων σε έναν κόσμο μεγάλων δεδομένων. Αυτές αποτελούνται από συστάσεις προς τα κράτη μέρη της Σύμβασης, τους υπεύθυνους επεξεργασίας και τους εκτελούντες την επεξεργασία να λάβουν μέτρα σχετικά με την προστασία δεδομένων για την πρόληψη πιθανών αρνητικών επιπτώσεων της χρήσης Big Data στην ανθρώπινη αξιοπρέπεια, τα ανθρώπινα δικαιώματα και τις θεμελιώδεις ελευθερίες.

2.7. Η Οδηγία 95/46/ΕΚ για την προστασία των προσωπικών δεδομένων (1995)

Η προστασία δεδομένων (data protection) αφορά την προστασία οποιασδήποτε πληροφορίας που σχετίζεται με ταυτοποιημένο ή αναγνωρίσιμο φυσικό (ζωντανό) πρόσωπο, συμπεριλαμβανομένων ονομάτων, ημερομηνιών γέννησης, φωτογραφιών, βίντεο, διευθύνσεων ηλεκτρονικού ταχυδρομείου και αριθμών τηλεφώνου. Άλλες πληροφορίες, όπως διευθύνσεις IP και περιεχόμενο επικοινωνίας - που σχετίζονται ή παρέχονται από τελικούς χρήστες υπηρεσιών επικοινωνιών - θεωρούνται επίσης προσωπικά δεδομένα.

Η έννοια της προστασίας δεδομένων πηγάζει από το δικαίωμα στην ιδιωτική ζωή και αμφότερα είναι καθοριστικά για τη διατήρηση και την προώθηση θεμελιωδών αξιών και δικαιωμάτων· όπως η ελευθερία του λόγου ή το δικαίωμα του συνέρχεσθαι.

Η προστασία δεδομένων έχει ακριβείς στόχους για τη διασφάλιση της δίκαιης επεξεργασίας (συλλογή, χρήση, αποθήκευση) προσωπικών δεδομένων τόσο από τον δημόσιο όσο και από τον ιδιωτικό τομέα.

Στο επίκεντρο του νομοθετικού πλαισίου της ΕΕ τίθεται η Οδηγία 95/46/ΕΚ η οποία συνιστά ακόμη και σήμερα το πρώτο, σημαντικότερο νομοθετικό εργαλείο της ΕΕ για την προστασία των προσωπικών δεδομένων, καθώς και το ηγετικό κείμενο για την οικουμενικοποίηση της προστασίας τους διεθνώς [ΟΔΗΓΙΑ1995]. Οι πενταετείς διαπραγματεύσεις οι οποίες οδήγησαν στην υιοθέτηση της Οδηγίας είναι χαρακτηριστικές για το πνεύμα του νομοθετικού τριγώνου της ΕΕ.

Έτσι, ενώ το Ευρ. Κοινοβούλιο είχε ήδη από το '70 υιοθετήσει μια προσέγγιση υπέρ των θεμελιωδών δικαιωμάτων, η Επιτροπή και το Συμβούλιο υπερασπίζονταν την "βιομηχανία επεξεργασίας προσωπικών δεδομένων". Με πρωτοβουλία του Κοινοβουλίου, η Επιτροπή εκπόνησε το '90 το πρώτο σχέδιο της Οδηγίας, βαθιά επηρεασμένο από τη γερμανο-γαλλική νομοθεσία προστασίας των προσωπικών δεδομένων και γι΄αυτό και ιδιαίτερα δικαιωματοκεντρικό. Η Οδηγία υπογράφτηκε στις 2 Οκτωβρίου 1995, παρέχοντας μια τριετή προθεσμία συμμόρφωσης στα κράτη-μέλη (Ελλάδα 2472/1997). Η Οδηγία στοχεύει στην εναρμόνιση των επιμέρους εθνικών νομοθεσιών για την προστασία προσωπικών των δεδομένων, διασφαλίζοντας ταυτόχρονα την ελεύθερη κυκλοφορία τους.

Βασικά σημεία της Οδηγίας είναι η έννοια της αυτοματοποιημένης "επεξεργασίας" των προσωπικών δεδομένων, η οποία αποτελεί και το πεδίο εφαρμογής της και συνίσταται στη συλλογή, αποθήκευση, μεταβολή, χρήση, αποκάλυψη, ταυτοποίηση, αναπαραγωγή τους κλπ, η έννοια των προσωπικών δεδομένων ως "επώνυμων" δεδομένων, τα οποία μπορούν να συνδεθούν με ένα αναγνωρίσιμο υποκείμενο, φυσικό πρόσωπο. Η Οδηγία επίσης, ρητά εξαιρεί από την εφαρμογή της την επεξεργασία για σκοπούς που εκφεύγουν του δικαίου της ΕΕ, όπως η προστασία της δημόσιας ασφάλειας, άμυνας ή η επεξεργασία για σκοπούς ποινικής δίωξης, καθώς και την επεξεργασία τους για καθαρά προσωπικούς, οικογενειακούς λόγους. Πρόκειται για σημεία-όρους, που εμφανίζουν ευρύτητα, αοριστία και ως εκ τούτου εμφανίζουν διχογνωμία στη θεωρία, η οποία επιχειρεί να τα συγκεκριμενοποιήσει και να τα εξειδικεύσει.

Ωστόσο, οι εγγυήσεις που απορρέουν από την Οδηγία, αντισταθμίζουν τις αβεβαιότητες αυτές. Σε πολλές περιπτώσεις μάλιστα υπερβαίνουν την Σύμβαση (CETS 108/1985) του Συμβουλίου της Ευρώπης σχετικά με την προστασία του ατόμου από την αυτόματη επεξεργασία προσωπικών δεδομένων. Ειδικότερα, η Οδηγία επιβάλει την δίκαιη και νόμιμη επεξεργασία των δεδομένων, τη συλλογή τους για συγκεκριμένους, ξεκάθαρους και νόμιμους σκοπούς με τρόπο αναγκαίο, κατάλληλο και όχι δυσανάλογο προς την προστασία των δικαιωμάτων, τη βραχυπρόθεσμη διατήρηση τους σε σχέση πάντα με τους σκοπούς που αυτή εξυπηρετεί. Επιπλέον, η Οδηγία εισάγει την έννοια των ευαίσθητων δεδομένων, δεδομένων που συνδέονται με τη φυλετική, εθνική καταγωγή, τις πολιτικές, φιλοσοφικές απόψεις, τον σεξουαλικό προσανατολισμό και την υγεία του ατόμου, ιδιότητες οι οποίες μπορούν να δώσουν έδαφος σε αδικαιολόγητες εναντίον του διακρίσεις. Η Οδηγία περαιτέρω εγγυάται την επανόρθωση του υποκειμένου, την προστασία του δικαιώματος στα προσωπικά δεδομένα από ανεξάρτητη αρχή, καθώς και τη δημιουργία ενός ανεξάρτητου συμβουλευτικού Οργάνου, της Ομάδας 29 (αποτελούμενο από αντιπροσώπους των Αρχών Προστασίας Προσωπικών Δεδομένων και από τον Ευρωπαίο Επόπτη, εξυπηρετεί στην ενοποίηση και αποτελεσματική εφαρμογή του σχετικού δικαίου στα κράτη-μέλη).

2.8. Ο Χάρτης των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (2000)

Το 2000 ο Χάρτης των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (Χάρτης) ψηφίστηκε στην Ε.Ε [ΕΥΡΩΠΑΙΚΟΣ2000]. Ως σκληρό πολιτικό έγγραφο στην αρχή, ο Χάρτης έγινε νομικά δεσμευτικός ως πρωτογενές δίκαιο της ΕΕ με την έναρξη ισχύος της Συνθήκης της Λισαβόνας το 2009.

Τα δικαιώματα που κατοχυρώνονται στον Χάρτη χωρίζονται σε έξι ενότητες: αξιοπρέπεια, ελευθερίες, ισότητα, αλληλεγγύη, δικαιώματα των πολιτών και δικαιοσύνη. Ο Χάρτης εγγυάται τον σεβασμό της ιδιωτικής και οικογενειακής ζωής και ανεβάζει ρητά το επίπεδο προστασίας των δεδομένων σε αυτό θεμελιώδους δικαιώματος στο δίκαιο της ΕΕ θεσπίζοντας το δικαίωμα στην προστασία δεδομένων. Αναφέρεται σε βασικές αρχές προστασίας δεδομένων, όπως η δίκαιη επεξεργασία και για συγκεκριμένο σκοπό, η συναίνεση του ατόμου ή που βασίζεται σε άλλη νομική βάση, και διασφαλίζει ότι μια ανεξάρτητη αρχή θα ελέγχει την εφαρμογή αυτών των αρχών.

2.9. GDPR: Ο Νόμος για την Προστασία των Δεδομένων (2016)

Για δεκαετίες, η ΕΕ τηρεί υψηλά πρότυπα νομοθεσίας περί προστασίας δεδομένων. Ο νόμος δίνει το δικαίωμα στα άτομα να ασκούν συγκεκριμένα δικαιώματα προστασίας δεδομένων και υποχρεώνει τους οργανισμούς (δημόσιου ή ιδιωτικού τομέα) που επεξεργάζονται τα δεδομένα τους να σέβονται αυτά τα δικαιώματα.

Τον Απρίλιο του 2016, η ΕΕ ενέκρινε ένα νέο νομικό πλαίσιο - τον Γενικό Κανονισμό για την Προστασία Δεδομένων -- the General Data Protection Regulation (GDPR) και την Οδηγία για την Προστασία Δεδομένων για τον τομέα επιβολής του νόμου και της αστυνομίας, [GDPR2016].

Πλήρως εφαρμόσιμος σε ολόκληρη την ΕΕ τον Μάιο του 2018, ο GDPR είναι η πιο ολοκληρωμένη και προοδευτική νομοθεσία για την προστασία δεδομένων στον κόσμο, η οποία ενημερώθηκε για να αντιμετωπίσει τις επιπτώσεις της ψηφιακής εποχής.

Ισχύει για οργανισμούς ή εταιρείες που δεν είναι εγκατεστημένοι στην ΕΕ που προσφέρουν αγαθά και υπηρεσίες σε ιδιώτες στην ΕΕ ή παρακολουθούν τη συμπεριφορά τους. Δημιουργεί νέα δικαιώματα για τα άτομα στο ψηφιακό περιβάλλον και αρκετές νέες και λεπτομερείς υποχρεώσεις συνεργασίας.

Σε παγκόσμιο επίπεδο, παρατηρείται μια αυξανόμενη ανάπτυξη στους νόμους περί προστασίας δεδομένων (που μερικές φορές αναφέρεται ως προστασία της ιδιωτικής ζωής δεδομένων σε χώρες εκτός ΕΕ). Πολλοί από αυτούς τους νόμους επηρεάζονται έντονα από τους κανόνες της ΕΕ, οι οποίοι θεωρούνται εδώ και καιρό ο χρυσός κανόνας στη νομοθεσία περί προστασίας δεδομένων.

Πάνω από 100 χώρες σε όλο τον κόσμο έχουν πλέον θεσπίσει νόμους για την προστασία δεδομένων: λιγότερες από τις μισές από αυτές τις χώρες βρίσκονται στην Ευρώπη (28 κράτη μέλη της ΕΕ και άλλα). Η πλειονότητα των νόμων για την προστασία δεδομένων έχει εγκριθεί εκτός Ευρώπης, με την ταχύτερη ανάπτυξη να παρατηρείται στις αφρικανικές χώρες.

2.9.1. Προστασία δεδομένων στην πράξη

Στις περισσότερες χώρες, οι εθνικές Αρχές Προστασίας Δεδομένων (ΑΠΔ) -- Data Protection Authorities (DPAs) ή Ρυθμιστικές Αρχές -- Regulators, έχουν συσταθεί ως θεματοφύλακες της προστασίας δεδομένων. Για να είναι αποτελεσματική η επιβολή της νομοθεσίας περί προστασίας δεδομένων, δίνεται στις DPAs η εξουσία να ερευνούν, να εντοπίζουν και να τιμωρούν τις παραβιάσεις, καθώς και την ευθύνη να ευαισθητοποιούν τα δικαιώματα και τις υποχρεώσεις προστασίας δεδομένων γενικά.

Στην ΕΕ, αυτή η αποτελεσματικότητα ενισχύεται από την απαίτηση οι ΑΠΔ να είναι ανεξάρτητες από οποιαδήποτε πολιτική, κυβερνητική ή άλλη επιρροή.

2.9.2. Προστασία δεδομένων στον ψηφιακό κόσμο

Στον ψηφιακό κόσμο, παρατηρούμε μια τεράστια ανισορροπία ισχύος μεταξύ των οντοτήτων επεξεργασίας δεδομένων, οι οποίες καθορίζουν τι και πώς γίνεται η επεξεργασία των δεδομένων, και των ατόμων των οποίων τα δεδομένα διακυβεύονται, δηλαδή, των οποίων η ζωή μπορεί να επηρεαστεί από αποφάσεις που βασίζονται σε αυτοματοποιημένη ανάλυση δεδομένων ή λόγω αποτυχίας επαρκούς προστασίας των προσωπικών πληροφοριών. Ως εκ τούτου, ειδικά στον ψηφιακό κόσμο, η προστασία της ιδιωτικής ζωής διαδραματίζει κρίσιμο ρόλο. Ωστόσο, όταν χρησιμοποιούν μια συγκεκριμένη υπηρεσία, πολλά άτομα συχνά αγνοούν την επεξεργασία δεδομένων και τις συνέπειές της. Τέλος, οι κυρώσεις για παραβάσεις των νομικών υποχρεώσεων προστασίας δεδομένων συνήθως τίθενται σε ισχύ μόνο εκ των υστέρων, δηλαδή εάν έχει ήδη σημειωθεί παραβίαση ή κακή χρήση δεδομένων.

Ταυτόχρονα, η κοινωνία μας εξαρτάται όλο και περισσότερο από την αξιόπιστη λειτουργία των τεχνολογιών πληροφοριών και επικοινωνιών (ΤΠΕ). Οι δυνατότητες επεξεργασίας, αποθήκευσης, και δικτύωσης έχουν αυξηθεί, και η επεξεργασία προσωπικών δεδομένων έχει ενταθεί. Ουσιαστικά, σχεδόν όλοι οι τομείς της ζωής συνδέονται με την υποστήριξη ΤΠΕ και, ως εκ τούτου, θα επηρεάζονταν εάν δεν μπορεί να διατηρηθεί η αξιοπιστία. Στην αρνητική πλευρά αυτής της εξέλιξης είναι οι ασαφείς ευθύνες και η έλλειψη διαφάνειας για τους χρήστες και τους ρυθμιστικούς φορείς, καθώς και οι ελλείψεις σε μεγάλο βαθμό εγγυήσεων για το απόρρητο και τα χαρακτηριστικά ασφαλείας. Στην πράξη, οι Ευρωπαϊκές Αρχές Προστασίας Δεδομένων δεν έχουν την ικανότητα να παρακολουθούν αποτελεσματικά και συστηματικά την επεξεργασία των δεδομένων ή να τιμωρούν εκ προμελέτης ή εξ αμελείας παράπτωμα.

2.9.3. Ανεξαρτησία

Στην ΕΕ, η απαίτηση οι ΑΠΔ να είναι ανεξάρτητες ορίζεται νομοθετικά: άρθρο 16 παράγραφος 2 της Συνθήκης για τη λειτουργία της ΕΕ (ΣΛΕΕ) -- Treaty on the Functioning of the EU (TFEU) και άρθρο 8 παράγραφος 3 του Χάρτη Θεμελιωδών Δικαιωμάτων της ΕΕ.

Το Δικαστήριο της Ευρωπαϊκής Ένωσης έχει επανειλημμένα τονίσει ότι ο έλεγχος από ανεξάρτητη αρχή αποτελεί ουσιαστικό στοιχείο του δικαιώματος στην προστασία των δεδομένων και έχει θέσει τα κριτήρια για μια τέτοια ανεξαρτησία. Ειδικότερα, η εποπτική αρχή πρέπει να ενεργεί με πλήρη ανεξαρτησία, πράγμα που συνεπάγεται εξουσία λήψης αποφάσεων ανεξάρτητη από οποιαδήποτε άμεση ή έμμεση εξωτερική επιρροή.

Ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR) τονίζει επίσης τη σημασία της ανεξαρτησίας. Το Κεφάλαιο VI του GDPR παρέχει λεπτομερείς κανόνες για τη σύσταση και τη λειτουργία ανεξάρτητων εποπτικών αρχών, συμπεριλαμβανομένων διατάξεων σχετικά με τους πόρους που απαιτούνται για την αποτελεσματική εκτέλεση των καθηκόντων και των εξουσιών τους.

Η Ευρωπαϊκή Αρχή Εποπτείας Προσωπικών Δεδομένων (ΕΕΠΔ) -- European Data Protection Supervisor (EDPS) είναι μια ανεξάρτητη εποπτική αρχή υπεύθυνη για τη διασφάλιση της συμμόρφωσης των θεσμικών οργάνων και οργανισμών της ΕΕ με τη νομοθεσία περί προστασίας δεδομένων κατά την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

2.9.4. Διασυνοριακή προστασία δεδομένων

Οι νόμοι περί προστασίας δεδομένων είναι εθνικοί, αλλά στο διαδικτυακό περιβάλλον, τα δεδομένα δεν σέβονται τα σύνορα.

Η διασυνοριακή συνεργασία και οι συμφωνίες για την παροχή αποτελεσματικής προστασίας δεδομένων είναι ουσιαστικής σημασίας, ιδίως εάν η ΕΕ θέλει να διατηρήσει τις αξίες της και να τηρήσει τις αρχές της.

Για να επιτευχθεί αυτό, ο ΕΕΠΔ αλληλεπιδρά τακτικά με τις ΑΠΔ και τις ρυθμιστικές αρχές της ΕΕ και τις διεθνείς αρχές για να επηρεάσει και να αναπτύξει τη διασυνοριακή επιβολή.

2.9.5. Ιδιωτική ζωή, προστασία δεδομένων και ασφάλεια

Στην ΕΕ, η προστασία της ιδιωτικής ζωής και των δεδομένων δεν είναι απόλυτα δικαιώματα και μπορούν να περιοριστούν υπό ορισμένες προϋποθέσεις σύμφωνα με τον Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ.

Τα δικαιώματα στην ιδιωτική ζωή και στην προστασία δεδομένων μπορεί να χρειαστεί να εξισορροπηθούν με άλλες αξίες της ΕΕ, ανθρώπινα δικαιώματα ή δημόσια και ιδιωτικά συμφέροντα, όπως τα θεμελιώδη δικαιώματα στην ελευθερία της έκφρασης, την ελευθερία του Τύπου ή την ελευθερία πρόσβασης στις πληροφορίες.

Τα δικαιώματα στην προστασία της ιδιωτικής ζωής και των δεδομένων ενδέχεται επίσης να πρέπει να σταθμίζονται με άλλα δημόσια συμφέροντα, όπως η εθνική ασφάλεια. Τα κράτη μέλη της ΕΕ θεσπίζουν μέτρα για την καταπολέμηση των

τρομοκρατικών απειλών, αλλά γενικότερα για την ενίσχυση της δικαστικής και αστυνομικής συνεργασίας σε ποινικές υποθέσεις στον τομέα της ελευθερίας, της ασφάλειας και της δικαιοσύνης.

Στην ΕΕ, η εθνική ασφάλεια αποτελεί αποκλειστική ευθύνη κάθε κράτους μέλους και περιγράφεται στη Συνθήκη για τη λειτουργία της ΕΕ (άρθρο 4.2 ΣΛΕΕ).

Ωστόσο, τα δικαστήρια μέσω της ειδικής νομικής διάταξης για τη διατήρηση δεδομένων, διερευνούν τώρα τα όρια αυτής της αρμοδιότητας: σύμφωνα με το Δικαστήριο της ΕΕ (ΔΕΕ), ακόμη και μέτρα που παρεκκλίνουν από το δίκαιο της ΕΕ υπόκεινται στον Χάρτη των Θεμελιωδών δικαιώματα.

Σε κάθε περίπτωση, η κλίμακα συλλογής, αποθήκευσης και διασυνοριακής ανταλλαγής δεδομένων προσωπικού χαρακτήρα μεταξύ των κρατών μελών σε θέματα εγκλήματος και τρομοκρατίας είναι τεράστια.

Η αυξημένη πρόσβαση σε ευρωπαϊκές βάσεις δεδομένων καθώς και σε εμπορικά δεδομένα για σκοπούς επιβολής του νόμου αμφισβητούν την ισορροπία μεταξύ ιδιωτικότητας και ασφάλειας.

Οι αρχές προστασίας δεδομένων γενικά έχουν να διαδραματίσουν καθοριστικό ρόλο στη διασφάλιση αυτής της ισορροπίας μεταξύ της ιδιωτικής ζωής και άλλων συμφερόντων, συμπεριλαμβανομένου του ευαίσθητου τομέα της ασφάλειας όπου ο ρόλος τους επεκτείνεται· Για παράδειγμα, την 1η Μαΐου 2017, ο ΕΕΠΔ ανέλαβε την εποπτεία προστασίας δεδομένων της Europol, του οργάνου της ΕΕ που συνεργάζεται ενεργά με τις αρχές επιβολής του νόμου για την καταπολέμηση του διεθνούς εγκλήματος και της τρομοκρατίας.

Ο ρόλος του ΕΕΠΔ ως ανεξάρτητου συμβούλου στα θεσμικά όργανα της ΕΕ σχετίζεται με όλα τα θέματα που αφορούν την επεξεργασία δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων των πρωτοβουλιών για τη βελτίωση της ασφάλειας στην ΕΕ και των νέων εργαλείων ανταλλαγής δεδομένων για τις υπηρεσίες επιβολής του νόμου.

Πράγματι, ο ΕΕΠΔ έχει εκδώσει πολυάριθμες γνωμοδοτήσεις σχετικά με πρωτοβουλίες για την επέκταση της ανταλλαγής πληροφοριών για σκοπούς επιβολής του νόμου εντός της ΕΕ, συμπεριλαμβανομένου του συστήματος εισόδου/εξόδου και του συστήματος PNR της ΕΕ - αλλά και εκτός Ευρώπης, όπως η συμφωνία Umbrella με τις ΗΠΑ και συμφωνίες PNR με μη -Χώρες της ΕΕ.

3. Προσωπικά Δεδομένα

3.1. Ορισμός των Προσωπικών Δεδομένων

Ο ορισμός των προσωπικών δεδομένων καθορίζει το εύρος εφαρμογής του GDPR και συνεπώς είναι υψίστης σημασίας. Ο κανονισμός ισχύει μόνο για δεδομένα που θεωρούνται «προσωπικής φύσης». Ωστόσο, «τι συνιστά δεδομένα προσωπικού χαρακτήρα είναι μία από τις κεντρικές αιτίες αμφιβολίας» στο ισχύον καθεστώς προστασίας δεδομένων. Η δυσκολία προσδιορισμού του τι μετράει ως προσωπικά δεδομένα βασίζεται σε διάφορους παράγοντες. Πρώτον, οι συνεχείς τεχνικές εξελίξεις καθιστούν ευκολότερο τον εντοπισμό ατόμων με βάση δεδομένα που μπορεί να μην είναι προσωπικά. Δεύτερον, ο ευρύς ορισμός των προσωπικών δεδομένων του GDPR περιλαμβάνει όλο και περισσότερα σημεία δεδομένων. Τρίτον, μεγάλη αβεβαιότητα αφορά τις έννοιες της ψευδωνυμοποίησης και της ανωνυμοποίησης στον GDPR. και τέλος, παρά τον εναρμονιστικό στόχο του GDPR παραμένουν σημαντικές αποκλίσεις στην εθνική νομοθεσία και πολιτική που έχουν προσθέσει σύγχυση σε αυτόν τον τομέα του δικαίου.

Ο κανονισμός υιοθετεί μια δυαδική προοπτική μεταξύ προσωπικών δεδομένων και μη προσωπικών δεδομένων και υπαγάγει μόνο τα πρώτα στο πεδίο εφαρμογής του. Σύμφωνα με την αιτιολογική σκέψη 26 του GDPR, ο κανονισμός δεν εφαρμόζεται σε ανώνυμα δεδομένα. Σε αντίθεση με αυτή τη δυαδική νομική προοπτική, η πραγματικότητα λειτουργεί σε ένα φάσμα μεταξύ δεδομένων που είναι σαφώς προσωπικά, δεδομένων που είναι σαφώς ανώνυμα (ένα αδιαμφισβήτητο παράδειγμα θα πρέπει να είναι αυτό των κλιματικών δεδομένων από το διάστημα που δεν αποκαλύπτουν πληροφορίες για εκείνους που τα συνέλεξαν) και οτιδήποτε ενδιάμεσο.

Σήμερα, μεγάλη οικονομική αξία προκύπτει από δεδομένα που δεν είναι προσωπικά, αλλά μπορούν να γίνουν προσωπικά εάν καταβληθεί επαρκής προσπάθεια. Το τρέχον πεδίο μάχης για τον ορισμό των προσωπικών δεδομένων σχετίζεται με «δεδομένα που όταν συλλέγονται και υποβάλλονται σε επεξεργασία έχουν τη δυνατότητα να έχουν αντίκτυπο στο προσωπικό απόρρητο συγκεκριμένων χρηστών, ίσως συμπεριλαμβανομένης της οικονομικής και συναισθηματικής ευημερίας τους, από δεδομένα που σίγουρα δεν έχουν τέτοιες δυνατότητες. Πέρα από αυτό, υπάρχει μια συνεχής συζήτηση σχετικά με το εάν τα προσωπικά δεδομένα μπορούν να παραποιηθούν για να καταστούν ανώνυμα, η οποία είναι πολύ σημαντική σε περιβάλλοντα όπου χρησιμοποιούνται κρυπτογράφηση και κατακερματισμός, όπως συμβαίνει με το DLT.

Το άρθρο 4 παράγραφος 1 του ΓΚΠΔ ορίζει τα προσωπικά δεδομένα ως εξής: κάθε πληροφορία που σχετίζεται με ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο δεδομένων»)· ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο που μπορεί να αναγνωριστεί, άμεσα ή έμμεσα, ιδίως με αναφορά σε ένα αναγνωριστικό όπως ένα όνομα, ένας αριθμός αναγνώρισης, δεδομένα τοποθεσίας, ένα διαδικτυακό αναγνωριστικό ή σε έναν ή περισσότερους παράγοντες ειδικούς για το φυσικό, φυσιολογικό, γενετική, ψυχική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα αυτού του φυσικού προσώπου, [GDPR2016].

Το άρθρο 4 παράγραφος 1 του ΓΚΠΔ υπογραμμίζει ότι δεδομένα προσωπικού χαρακτήρα είναι δεδομένα που σχετίζονται άμεσα ή έμμεσα με ταυτοποιημένο ή αναγνωρίσιμο φυσικό πρόσωπο. Η αναφορά σε ένα «αναγνωριζόμενο» πρόσωπο υπογραμμίζει ότι το υποκείμενο των δεδομένων δεν χρειάζεται να έχει ήδη ταυτοποιηθεί προκειμένου τα δεδομένα να χαρακτηριστούν δεδομένα προσωπικού χαρακτήρα. Αρκεί και μόνο η δυνατότητα ταυτοποίησης. Η ομάδα εργασίας του άρθρου 29 έχει εκδώσει οδηγίες σχετικά με τον τρόπο με τον οποίο πρέπει να είναι τα τέσσερα συστατικά στοιχεία της δοκιμής στο άρθρο 4 παράγραφος 1 του ΓΚΠΔ – «οποιεσδήποτε πληροφορίες», «σχετικά με», «αναγνωρισμένο ή αναγνωρίσιμο» και «φυσικό πρόσωπο» ερμηνεύεται.

Οι πληροφορίες πρέπει να ερμηνεύονται ευρέως και περιλαμβάνουν τόσο αντικειμενικές πληροφορίες (όπως ένα όνομα ή την παρουσία μιας δεδομένης ουσίας στο αίμα κάποιου) όσο και υποκειμενική ανάλυση όπως πληροφορίες, απόψεις και αξιολογήσεις. Σημειώστε, ωστόσο, ότι το Ευρωπαϊκό Δικαστήριο διευκρίνισε εν τω μεταξύ ότι ενώ οι πληροφορίες που περιέχονται στην αίτηση για άδεια διαμονής και τα δεδομένα που περιέχονται στη νομική ανάλυση χαρακτηρίζονται ως προσωπικά δεδομένα, η σχετική νομική ανάλυση δεν πληροί τις προϋποθέσεις. Οι πληροφορίες που χαρακτηρίζονται ως προσωπικά δεδομένα μπορεί να περιλαμβάνουν πληροφορίες που δεν σχετίζονται με την ιδιωτική ζωή κάποιου, υπογραμμίζοντας τη διάκριση μεταξύ των εννοιών της προστασίας δεδομένων και της ιδιωτικής ζωής. Τα προσωπικά δεδομένα μπορούν επίσης να λάβουν οποιαδήποτε μορφή, είτε πρόκειται για αλφαβητικά είτε αριθμητικά δεδομένα, βίντεο και εικόνες. Το Δικαστήριο επιβεβαίωσε πράγματι ότι «η εικόνα ενός ατόμου που καταγράφηκε από κάμερα» συνιστά προσωπικά δεδομένα.

Δεύτερον, τα δεδομένα μπορούν να θεωρηθούν ότι «αφορούν» ένα υποκείμενο των δεδομένων «όταν πρόκειται για αυτό το άτομο». Αυτό περιλαμβάνει προφανώς πληροφορίες που βρίσκονται στο αρχείο ενός ατόμου, αλλά μπορεί επίσης να περιλαμβάνει δεδομένα οχήματος που αποκαλύπτουν πληροφορίες σχετικά με ένα δεδομένο υποκείμενο δεδομένων, όπως έναν οδηγό ή επιβάτη. Ένα άτομο θεωρείται ότι είναι «αναγνωρισμένο» ή «αναγνωριζόμενο» όπου μπορεί να «διακριθεί» από άλλα. Αυτό δεν απαιτεί να μπορεί να βρεθεί το όνομα του ατόμου. Σύμφωνα με το Δικαστήριο, η ταυτοποίηση ατόμων «με το όνομά τους ή με άλλα μέσα, για παράδειγμα δίνοντας τον αριθμό τηλεφώνου τους ή πληροφορίες σχετικά με τις συνθήκες εργασίας και τα χόμπι τους, συνιστά επεξεργασία δεδομένων προσωπικού χαρακτήρα». Ως εκ τούτου, τα προσωπικά δεδομένα είναι «πληροφορίες, λόγω του περιεχομένου, του σκοπού ή του αποτελέσματός τους, που συνδέονται με ένα συγκεκριμένο άτομο».

Τα προσωπικά δεδομένα σχετίζονται με ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο. Όταν τα δεδομένα αφορούν προφανώς ένα φυσικό πρόσωπο, όπως συμβαίνει με το πλήρες όνομα του υποκειμένου των δεδομένων, το συμπέρασμα ότι τα δεδομένα αυτά είναι προσωπικά δεδομένα φαίνεται αδιαμφισβήτητο. Ωστόσο, το άρθρο 4 παράγραφος 1 του ΓΚΠΔ παρέχει επίσης παραδείγματα δεδομένων τοποθεσίας ή αναγνωριστικού ως δεδομένα προσωπικού χαρακτήρα. Αυτό υπογραμμίζει ότι δεδομένα, όπως δεδομένα υγείας, που δεν σχετίζονται με ταυτοποιημένο αλλά ταυτοποιήσιμο φυσικό

πρόσωπο εξακολουθούν να εμπίπτουν σε αυτό το πεδίο εφαρμογής. Πράγματι, η έννοια των προσωπικών δεδομένων θα πρέπει να ερμηνεύεται ευρέως – όπως έχει επιβεβαιωθεί πλέον ευρέως στη σχετική νομολογία.

Στην υπόθεση "Peter Nowak vs. Data Protection Commissioner", το Ευρωπαϊκό Δικαστήριο (European Court of Justice -- ECJ) κατέληξε στο συμπέρασμα ότι οι εξετάσεις από ιδρύματα περαιτέρω εκπαίδευσης αποτελούν προσωπικά δεδομένα. Εξήγησε ότι η έκφραση «οποιαδήποτε πληροφορία» αντικατοπτρίζει «τον στόχο του νομοθέτη της ΕΕ να δώσει ευρύ πεδίο εφαρμογής στην έννοια αυτή, η οποία δεν περιορίζεται σε ευαίσθητες ή ιδιωτικές πληροφορίες, αλλά δυνητικά περιλαμβάνει όλα τα είδη πληροφοριών, όχι μόνο αντικειμενικές αλλά επίσης υποκειμενικό, υπό μορφή γνωμών και αξιολογήσεων, υπό τον όρο ότι «αφορά» το υποκείμενο των δεδομένων». Καθώς οι γραπτές απαντήσεις αντικατοπτρίζουν τις γνώσεις και τις ικανότητες ενός υποψηφίου σε ένα δεδομένο πεδίο και περιέχουν τη γραφή του, χαρακτηρίζονται ως προσωπικά δεδομένα. Τα γραπτά σχόλια του εξεταστή θεωρήθηκαν προσωπικά δεδομένα τόσο του υποψηφίου όσο και του εξεταστή.

Με την απόφαση "Digital Rights Ireland" του 2014 (υποθέσεις C-293/12 και C-594/12), το Ευρωπαϊκό Δικαστήριο έκρινε ότι τα μεταδεδομένα (όπως δεδομένα τοποθεσίας ή διευθύνσεις IP) που επιτρέπουν μόνο την έμμεση ταυτοποίηση του υποκειμένου των δεδομένων μπορούν επίσης να είναι προσωπικά δεδομένα καθώς «μπορεί να επιτρέψουν την εξαγωγή πολύ ακριβών συμπερασμάτων σχετικά με την ιδιωτική ζωή των τα άτομα των οποίων τα δεδομένα έχουν διατηρηθεί, όπως οι συνήθειες της καθημερινής ζωής, οι μόνιμοι ή προσωρινοί τόποι διαμονής, οι καθημερινές ή άλλες μετακινήσεις, οι δραστηριότητες που πραγματοποιούνται, οι κοινωνικές σχέσεις αυτών των προσώπων και τα κοινωνικά περιβάλλοντα στα οποία συχνάζουν».

Ο ευρύς ορισμός των προσωπικών δεδομένων οδήγησε ορισμένους να παρατηρήσουν ότι ο νόμος περί προστασίας δεδομένων έχει γίνει ο «νόμος των πάντων», καθώς στο εγγύς μέλλον όλα τα δεδομένα μπορεί να είναι προσωπικά δεδομένα και επομένως να υπόκεινται στις απαιτήσεις του GDPR. Αυτό συμβαίνει επειδή «η τεχνολογία κινείται γρήγορα προς την τέλεια ταυτοποίηση των πληροφοριών. Η πληροφόρηση δεδομένων και η πρόοδος στην ανάλυση δεδομένων κάνουν τα πάντα (περιέχουν) πληροφορίες. και σε ολοένα και πιο «έξυπνα» περιβάλλοντα, οποιαδήποτε πληροφορία είναι πιθανό να σχετίζεται με ένα άτομο σε σκοπό ή αποτέλεσμα». Η ομάδα εργασίας του άρθρου 29 προειδοποίησε επίσης ότι «η ανωνυμοποίηση είναι ολοένα και πιο δύσκολο να επιτευχθεί με την πρόοδο της σύγχρονης τεχνολογίας υπολογιστών και την πανταχού παρούσα διαθεσιμότητα πληροφοριών».

Τέλος, προσωπικά δεδομένα είναι μόνο δεδομένα που αφορούν φυσικό πρόσωπο. Ως πλαίσιο θεμελιωδών δικαιωμάτων, ο GDPR δεν εφαρμόζεται συνεπώς σε νομικά πρόσωπα. Ομοίως, ο κανονισμός δεν εφαρμόζεται σε δεδομένα που αφορούν τον αποθανόντα. Ωστόσο, αυτό δεν σημαίνει ότι τα δεδομένα που σχετίζονται με ένα αποθανόν δεν αποτελούν προσωπικά δεδομένα ενός σχετικού υποκειμένου δεδομένων, όπως ενός μέλος της οικογένειας.

3.2. Χάραξη της γραμμής μεταξύ προσωπικών και μη προσωπικών δεδομένων

Η χάραξη της διαχωριστικής γραμμής μεταξύ προσωπικών και μη προσωπικών δεδομένων είναι γεμάτη αβεβαιότητα λόγω του ευρέος πεδίου των προσωπικών δεδομένων και της τεχνικής δυνατότητας εξαγωγής πληροφοριών σχετικά με τα υποκείμενα των δεδομένων από σημεία δεδομένων (datapoints) που φαινομενικά δεν σχετίζονται με αυτά. Αυτό δεν οφείλεται μόνο στην εκτεταμένη ερμηνευτική στάση του Δικαστηρίου, αλλά και στη δυσκολία προσδιορισμού του εάν τα δεδομένα που τροποποιούνται για να αποτρέψουν την ταυτοποίηση (identification) μπορούν στην πραγματικότητα να θεωρηθούν ως ανώνυμα δεδομένα για το GDPR. Συγκεκριμένα, έχει δημιουργηθεί η έννοια της ψευδωνυμοποίησης στον Κανονισμό, η οποία προκαλεί αβεβαιότητα. Αυτός ο περίπλοκος τομέας του νόμου εισάγεται για πρώτη φορά για να ορίσει τις βασικές αρχές πριν αντιστοιχιστεί σε blockchains.

Το άρθρο 4 παράγραφος 5 του ΓΚΠΔ εισάγει την **ψευδωνυμοποίηση** ως την επεξεργασία δεδομένων προσωπικού χαρακτήρα με τέτοιο τρόπο ώστε τα προσωπικά δεδομένα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο δεδομένων χωρίς τη χρήση πρόσθετων πληροφοριών, υπό την προϋπόθεση ότι αυτές οι πρόσθετες πληροφορίες τηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα για να διασφαλιστεί ότι τα προσωπικά δεδομένα δεν αποδίδονται σε αναγνωρισμένο ή αναγνωρίσιμο φυσικό πρόσωπο.

Η έννοια της ψευδωνυμοποίησης είναι μια από τις καινοτομίες του GDPR σε σύγκριση με την Οδηγία για την Προστασία Δεδομένων του 1995. Σε αυτό το στάδιο, υπάρχει μια συνεχής συζήτηση σχετικά με τις επιπτώσεις του άρθρου 4 παράγραφος 5 του ΓΚΠΔ στη νομοθεσία της ΕΕ για την προστασία δεδομένων. Ειδικότερα, συζητείται εάν η διάταξη δημιουργεί την τρίτη κατηγορία δεδομένων (πέρα από τα προσωπικά και τα ανώνυμα δεδομένα) και εάν ναι, εάν τα ψευδώνυμα δεδομένα χαρακτηρίζονται ως προσωπικά δεδομένα ή αν μπορούν να ανταποκριθούν στο όριο ανωνυμοποίησης.

Ωστόσο, μια κυριολεκτική ερμηνεία αυτής της διάταξης αποκαλύπτει ότι το άρθρο 4 παράγραφος 5 του GDPR αφορά μια μέθοδο και όχι ένα αποτέλεσμα επεξεργασίας δεδομένων. Ορίζει την **ψευδωνυμοποίηση** ως την «επεξεργασία» προσωπικών δεδομένων με τέτοιο τρόπο ώστε τα δεδομένα να μπορούν να αποδοθούν σε ένα υποκείμενο των δεδομένων μόνο με τη βοήθεια πρόσθετων πληροφοριών. **Δεν προβλέπονται ακριβείς μέθοδοι**, σύμφωνα με το τεχνολογικά ουδέτερο πνεύμα του κανονισμού.

Τα ψευδωνυμοποιημένα δεδομένα παραμένουν προσωπικά δεδομένα, σύμφωνα με τη διαπίστωση της ομάδας εργασίας του άρθρου 29 ότι «**η ψευδωνυμοποίηση δεν είναι μέθοδος ανωνυμοποίησης**. Απλώς μειώνει τη δυνατότητα σύνδεσης ενός συνόλου δεδομένων με την αρχική ταυτότητα ενός υποκειμένου των δεδομένων και, κατά συνέπεια, είναι ένα χρήσιμο μέτρο ασφαλείας».

Ο GDPR πράγματι ενθαρρύνει ρητά την ψευδωνυμοποίηση ως μέτρο διαχείρισης κινδύνου. Η ψευδωνυμοποίηση μπορεί να θεωρηθεί ως απόδειξη συμμόρφωσης με την υποχρέωση ασφάλειας του υπευθύνου επεξεργασίας σύμφωνα με το άρθρο 5(στ) GDPR. Η αιτιολογική σκέψη 28 του GDPR προβλέπει περαιτέρω ότι «ηεφαρμογή ψευδωνυμοποίησης σε δεδομένα προσωπικού χαρακτήρα μπορεί να μειώσει τους κινδύνους για τα ενδιαφερόμενα υποκείμενα των δεδομένων και να βοηθήσει τους υπεύθυνους επεξεργασίας και τους εκτελούντες την επεξεργασία να εκπληρώσουν τις υποχρεώσεις τους για την προστασία των δεδομένων».

Σύμφωνα με την αιτιολογική σκέψη 30, τα υποκείμενα των δεδομένων μπορεί να «σχετίζονται με διαδικτυακά αναγνωριστικά που παρέχονται από τις συσκευές, τις εφαρμογές, τα εργαλεία και τα πρωτόκολλά τους, όπως διευθύνσεις πρωτοκόλλου Διαδικτύου, αναγνωριστικά cookie ή άλλα αναγνωριστικά, όπως ετικέτες αναγνώρισης ραδιοσυχνοτήτων». Ενώ αυτά τα αναγνωριστικά είναι ψευδώνυμου χαρακτήρα, μπορούν ωστόσο να επιτρέπουν την έμμεση ταυτοποίηση ενός υποκειμένου δεδομένων καθώς αφήνουν ίχνη τα οποία «ιδίως όταν συνδυάζονται με μοναδικά αναγνωριστικά και άλλες πληροφορίες που λαμβάνονται από τους διακομιστές, μπορούν να χρησιμοποιηθούν για τη δημιουργία προφίλ των φυσικών προσώπων». Παρακάτω, θα φανεί ότι τα δημόσια κλειδιά που λειτουργούν ως αναγνωριστικά σε blockchain μπορούν να χαρακτηριστούν ως τέτοια αναγνωριστικά και ότι ως τέτοια χαρακτηρίζονται ως προσωπικά δεδομένα.

Θα πρέπει να τονιστεί ότι παρόλο που τα ψευδώνυμα δεδομένα ενδέχεται να μην χαρακτηρίζονται ως ανώνυμα δεδομένα, ενδέχεται να εμπίπτουν στο άρθρο 11 GDPR, σύμφωνα με το οποίο ο υπεύθυνος επεξεργασίας δεν υποχρεούται να διατηρεί, να αποκτά ή να επεξεργάζεται πρόσθετες πληροφορίες για την αναγνώριση του υποκειμένου των δεδομένων προκειμένου να συμμορφώνονται με τον Κανονισμό. Ως εκ τούτου, στο κείμενο του GDPR αναγνωρίζεται επαρκώς ότι **η ψευδωνυμοποίηση είναι μια πολύτιμη προσέγγιση ελαχιστοποίησης του κινδύνου**, αλλά ότι ταυτόχρονα δεν πρέπει να θεωρείται ως τεχνική ανωνυμοποίησης.

3.3. Μετατροπή προσωπικών δεδομένων σε ανώνυμα δεδομένα

Η αρχή που πρέπει να χρησιμοποιείται για να καθοριστεί εάν τα δεδομένα είναι προσωπικά δεδομένα ή όχι είναι αυτή της εύλογης πιθανότητας ταυτοποίησης, η οποία κατοχυρώνεται στην **αιτιολογική σκέψη 26 του GDPR** σύμφωνα με την οποία:

"Οι αρχές της προστασίας δεδομένων θα πρέπει να εφαρμόζονται σε κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο. Προσωπικά δεδομένα που έχουν υποστεί ψευδωνυμοποίηση, τα οποία θα μπορούσαν να αποδοθούν σε φυσικό πρόσωπο με τη χρήση πρόσθετων πληροφοριών θα πρέπει να θεωρούνται πληροφορίες για ένα αναγνωρίσιμο φυσικό πρόσωπο. Για να εξακριβωθεί εάν είναι πιθανό να χρησιμοποιηθούν για την ταυτοποίηση του φυσικού προσώπου, θα πρέπει να λαμβάνονται υπόψη όλοι οι αντικειμενικοί παράγοντες, όπως το κόστος και ο χρόνος που απαιτείται για την ταυτοποίηση, λαμβάνοντας υπόψη τη διαθέσιμη τεχνολογία τη στιγμή της επεξεργασίας και τις

τεχνολογικές εξελίξεις. Ως εκ τούτου, οι αρχές της προστασίας δεδομένων δεν θα πρέπει να ισχύουν για ανώνυμες πληροφορίες. Συνεπώς, ο παρών κανονισμός δεν αφορά την επεξεργασία τέτοιων ανώνυμων πληροφοριών, μεταξύ άλλων για στατιστικούς ή ερευνητικούς σκοπούς."

Η αιτιολογική σκέψη 26 του GDPR υπενθυμίζει αρχικά ότι τα ψευδώνυμα δεδομένα χαρακτηρίζονται ως προσωπικά δεδομένα σύμφωνα με το άρθρο 4 παράγραφος 5 του GDPR. Στη συνέχεια, διατυπώνει το τεστ που πρέπει να χρησιμοποιηθεί για να προσδιοριστεί εάν τα δεδομένα είναι προσωπικά δεδομένα ή όχι, δηλαδή εάν ο υπεύθυνος επεξεργασίας ή άλλο άτομο είναι σε θέση να αναγνωρίσει το υποκείμενο των δεδομένων χρησιμοποιώντας όλα τα «μέσα που είναι εύλογα πιθανό να χρησιμοποιηθούν». Όπου τα προσωπικά δεδομένα δεν είναι πλέον πιθανό να «αποδίδονται εύλογα σε φυσικό πρόσωπο με τη χρήση πρόσθετων πληροφοριών», δεν πρόκειται πλέον για προσωπικά δεδομένα.

Επομένως, ο GDPR είναι σαφής ότι, είναι δυνατός ο χειρισμός των προσωπικών δεδομένων κατά τρόπο που αφαιρεί την εύλογη πιθανότητα ταυτοποίησης ενός υποκειμένου δεδομένων. Η αιτιολογική σκέψη 26 του ΓΚΠΔ προβλέπει ρητά ότι μπορεί να υπάρχουν σενάρια όπου τα δεδομένα προσωπικού χαρακτήρα «καθίσταται ανώνυμα με τέτοιο τρόπο ώστε το υποκείμενο των δεδομένων να μην είναι ή να μην είναι πλέον αναγνωρίσιμο». Όταν μια τέτοια προσπάθεια αποδειχθεί επιτυχής, τα προσωπικά δεδομένα έχουν μετατραπεί σε ανώνυμα δεδομένα που παρακάμπτουν το πεδίο εφαρμογής του κανονισμού.

Ουσιαστικά, η αιτιολογική σκέψη 26 του GDPR επιβάλλει επομένως μια προσέγγιση βάσει κινδύνου για να καθοριστεί εάν τα δεδομένα πληρούν τις προϋποθέσεις ως δεδομένα προσωπικού χαρακτήρα. Όπου υπάρχει εύλογος κίνδυνος ταυτοποίησης, τα δεδομένα θα πρέπει να αντιμετωπίζονται ως προσωπικά δεδομένα και, ως εκ τούτου, υπόκεινται στον GDPR. Όταν ο κίνδυνος είναι μικρός (δηλαδή ότι η ταυτοποίηση δεν είναι πιθανή μέσω της εξάρτησης από όλα τα μέσα που είναι εύλογα πιθανό να χρησιμοποιηθούν), μπορεί θεωρηθούν ως ανώνυμα δεδομένα, παρόλο που η ταυτοποίηση δεν μπορεί να αποκλειστεί με απόλυτη βεβαιότητα.

Το σχετικό κριτήριο για να καθοριστεί εάν τα δεδομένα είναι προσωπικά δεδομένα είναι αυτό της ταυτοποίησης. Επιπλέον, το προοίμιο του GDPR παρέχει έναν κατάλογο στοιχείων που πρέπει να ληφθούν υπόψη για τον προσδιορισμό της πιθανότητας ταυτοποίησης με όλα τα μέσα που είναι εύλογα πιθανό να χρησιμοποιηθούν. Σε αυτούς περιλαμβάνονται «όλοι οι αντικειμενικοί παράγοντες, όπως το κόστος και ο χρόνος που απαιτείται για την ταυτοποίηση, λαμβάνοντας υπόψη τη διαθέσιμη τεχνολογία τη στιγμή της επεξεργασίας και τις τεχνολογικές εξελίξεις».

Με την πάροδο του χρόνου, οι εθνικές εποπτικές αρχές και τα δικαστήρια διαπίστωσαν ότι δεδομένα που κάποτε ήταν προσωπικά είχαν ξεπεράσει αυτό το όριο για να γίνουν ανώνυμα δεδομένα. Για παράδειγμα, το Ανώτατο Δικαστήριο του Ηνωμένου Βασιλείου έκρινε το 2011 ότι τα δεδομένα για ορισμένες αμβλώσεις που είχαν μετατραπεί σε στατιστικές πληροφορίες ήταν ανώνυμα δεδομένα που μπορούσαν να δημοσιοποιηθούν. Ομοίως, το Γραφείο του Επιτρόπου

Πληροφοριών του Ηνωμένου Βασιλείου (η Βρετανική Αρχή Προστασίας Δεδομένων -- ICO) υιοθέτησε μια σχετικιστική αντίληψη της αιτιολογικής σκέψης 26 του GDPR, τονίζοντας ότι το σχετικό κριτήριο δεν είναι αυτό της δυνατότητας ταυτοποίησης αλλά μάλλον του «ταυτοποίηση ή πιθανή ταυτοποίηση» ενός υποκειμένου των δεδομένων.

Ενώ ορισμένοι επομένως ευνοούν μια προσέγγιση βασισμένη στον κίνδυνο, η ομάδα εργασίας του άρθρου 29 έκλινε προς μια προσέγγιση μηδενικού κινδύνου. Σημείωσε στις κατευθυντήριες γραμμές του 2014 για τις τεχνικές ανωνυμοποίησης και ψευδωνυμοποίησης ότι «η ανωνυμοποίηση προκύπτει από την επεξεργασία προσωπικών δεδομένων που οδηγεί στο να αποτραπεί αμετάκλητα η ταυτοποίηση». Πράγματι, στην καθοδήγησή της για το θέμα, η ομάδα εργασίας φαίνεται να εφαρμόζει τον έλεγχο βάσει κινδύνου που είναι εγγενής στη νομοθεσία, ενώ ταυτόχρονα προσθέτει τον δικό της – αυστηρότερο – έλεγχο. Αυτή ήταν η πηγή πολλής σύγχυσης. Θα φανεί ότι αυτές οι κατευθυντήριες γραμμές αποκλίνουν από την αιτιολογική σκέψη 26 του GDPR.

3.4. Τα κριτήρια της αναγνωρισιμότητας

Σύμφωνα με την ομάδα εργασίας του άρθρου 29, πρέπει να ληφθούν υπόψη **τρία διαφορετικά κριτήρια για να καθοριστεί εάν η αποταυτοποίηση είναι «μη αναστρέψιμη»** ή «τόσο μόνιμη όσο η διαγραφή», δηλαδή εάν (i) είναι ακόμη δυνατό να ξεχωρίσουμε ένα άτομο. (ii) εξακολουθεί να είναι δυνατή η σύνδεση αρχείων που σχετίζονται με ένα άτομο και (iii) εάν μπορούν να εξακολουθήσουν να συνάγονται πληροφορίες που αφορούν ένα άτομο. Όπου η απάντηση σε αυτές τις τρεις ερωτήσεις είναι αρνητική, τα δεδομένα μπορούν να θεωρηθούν ανώνυμα.

Το **"singing out"** αναφέρεται στη «δυνατότητα απομόνωσης ορισμένων ή όλων των εγγραφών που προσδιορίζουν ένα άτομο στο σύνολο δεδομένων». Ένα παράδειγμα θα ήταν ένα σύνολο δεδομένων που περιέχει ιατρικές πληροφορίες που επιτρέπει την ταυτοποίηση ενός συγκεκριμένου υποκειμένου δεδομένων, για παράδειγμα μέσω ενός συνδυασμού ιατρικών πληροφοριών (όπως η παρουσία μιας σπάνιας ασθένειας) και πρόσθετων δημογραφικών παραγόντων (όπως η ημερομηνία γέννησής του).

Η **δυνατότητα σύνδεσης** (linkability) υποδηλώνει τον κίνδυνο που δημιουργείται όταν τουλάχιστον δύο σύνολα δεδομένων περιέχουν πληροφορίες για το ίδιο υποκείμενο δεδομένων. Εάν σε τέτοιες περιπτώσεις ένας «επιτιθέμενος μπορεί να αποδείξει (π.χ. μέσω ανάλυσης συσχέτισης) ότι δύο εγγραφές έχουν εκχωρηθεί σε μια ίδια ομάδα ατόμων, αλλά δεν μπορεί να ξεχωρίσει άτομα σε αυτήν την ομάδα», τότε η χρησιμοποιούμενη τεχνική παρέχει μόνο αντίσταση κατά του singing out, αλλά όχι ενάντια στη δυνατότητα σύνδεσης.

Τέλος, η **εξαγωγή συμπερασμάτων** (inference) μπορεί να εξακολουθήσει να είναι δυνατή ακόμη και όταν δεν είναι δυνατά το "singing out" και η συνδεσιμότητα. Πρόκειται για «τη δυνατότητα να συναχθεί, με σημαντική πιθανότητα, η τιμή ενός χαρακτηριστικού από τις τιμές ενός συνόλου άλλων χαρακτηριστικών». Για παράδειγμα, όταν ένα σύνολο

δεδομένων δεν αναφέρεται στην Άνγκελα Μέρκελ, αλλά σε μια γυναίκα Γερμανίδα καγκελάριο στις αρχές της δεκαετίας του 2000, η ταυτότητά της θα ήταν εύλογα δυνατό να συναχθεί.

Ο μετασχηματισμός των προσωπικών δεδομένων με τρόπο που αποκλείει το "singing out", τη δυνατότητα σύνδεσης και την εξαγωγή συμπερασμάτων είναι δύσκολη. Αυτό επιβεβαιώνεται από την ανάλυση της ομάδας εργασίας για τις πιο συχνά χρησιμοποιούμενες μεθόδους «ανωνυμοποίησης», οι οποίες την οδηγούν στο συμπέρασμα ότι καθεμία από αυτές αφήνει έναν υπολειπόμενο κίνδυνο αναγνώρισης. Η αυξανόμενη αφθονία δεδομένων διευκολύνει την αποανωνυμοποίηση δεδομένων σημείων δεδομένων μέσω του συνδυασμού διαφόρων συνόλων δεδομένων. Ως εκ τούτου, είναι συχνά εύκολο να εντοπιστούν τα υποκείμενα των δεδομένων με βάση υποτιθέμενα ανώνυμα δεδομένα.
Ορισμένοι επιστήμονες υπολογιστών έχουν μάλιστα προειδοποιήσει ότι η αποαναγνώριση προσωπικών δεδομένων είναι ένας «ανέφικτος στόχος».

Σε μια απόφαση του Δεκεμβρίου 2018, η Αυστριακή Αρχή Προστασίας Δεδομένων επιβεβαίωσε επιπλέον ότι δεν υπάρχει ανάγκη η ανωνυμοποίηση να είναι μη αναστρέψιμη – τουλάχιστον σε περιπτώσεις όπου η ανωνυμοποίηση χρησιμοποιείται για να ενεργοποιήσει τη «διαγραφή» δεδομένων σύμφωνα με το άρθρο 17 GDPR. Ωστόσο, δεν είναι σαφές εάν οι εποπτικές αρχές σε ολόκληρη την ΕΕ θα τηρήσουν αυτή τη στάση.

Τα ψευδώνυμα δεδομένα (pseudonymous data) σε μια αλυσίδα μπλοκ μπορούν, καταρχήν, να σχετίζονται με ένα αναγνωρισμένο ή αναγνωρίσιμο φυσικό πρόσωπο. Για να δώσουμε ένα παράδειγμα, μπορούμε να φανταστούμε μια κατάσταση όπου δύο άτομα, η Α και η Β, πίνουν καφέ μαζί και η Α βλέπει ότι η Β αγοράζει τον καφέ της μέσω ενός κρυπτονομίσματος που βασίζεται σε μια δημόσια και χωρίς άδεια blockchain. Καθώς αυτή η συναλλαγή καταγράφεται στο δημόσιο λογιστικό βιβλίο (public ledger) μαζί με πληροφορίες σχετικά με το ποσό που καταβλήθηκε και μια χρονική σήμανση (timestamp), μπορεί η Α (ή πιθανώς ένας τρίτος παρατηρητής όπως ο ταμίας) να βρει αυτήν τη συναλλαγή σε μια αλυσίδα μπλοκ και κατά συνέπεια να αποκτήσει γνώση του ψευδώνυμου δημόσιου κλειδιού της Β. Εάν δεν χρησιμοποιείται νέο κλειδί για κάθε συναλλαγή, μπορεί επίσης να είναι δυνατή η ανίχνευση όλων των συναλλαγών που έχει πραγματοποιήσει ποτέ η Β χρησιμοποιώντας αυτό το κρυπτονόμισμα.

3.5. Τα δημόσια κλειδιά ως προσωπικά δεδομένα

Στο πλαίσιο της αλυσίδας μπλοκ, τα δημόσια κλειδιά χρησιμεύουν ως το είδος των αναγνωριστικών που αναφέρονται στην αιτιολογική σκέψη 30 του GDPR. Οι αλυσίδες μπλοκ βασίζονται σε μια διαδικασία επαλήθευσης δύο σταδίων με

ασύμμετρη κρυπτογράφηση. Κάθε χρήστης έχει ένα **δημόσιο κλειδί** (μια συμβολοσειρά γραμμάτων και αριθμών που αντιπροσωπεύουν τον χρήστη), το οποίο θεωρείται καλύτερα ως ένας αριθμός λογαριασμού που μοιράζεται με άλλους για να ενεργοποιηθούν οι συναλλαγές. Επιπλέον, κάθε χρήστης έχει ένα **ιδιωτικό κλειδί** (επίσης μια συμβολοσειρά γραμμάτων και αριθμών), το οποίο θεωρείται καλύτερα ως κωδικός πρόσβασης που δεν πρέπει ποτέ να κοινοποιείται σε άλλους. Και τα δύο κλειδιά έχουν μια μαθηματική σχέση, χάρη στην οποία το ιδιωτικό κλειδί μπορεί να αποκρυπτογραφήσει δεδομένα που έχουν κρυπτογραφηθεί μέσω του δημόσιου κλειδιού.

Τα δημόσια κλειδιά αποκρύπτουν έτσι την ταυτότητα του ατόμου, εκτός εάν συνδέονται με πρόσθετα αναγνωριστικά. Αυτό ισχύει μόνο όταν το δημόσιο κλειδί αφορά ένα φυσικό πρόσωπο. Υπάρχουν περιπτώσεις χρήσης όπου τα δημόσια κλειδιά δεν σχετίζονται με φυσικά πρόσωπα. Για παράδειγμα, όταν τα χρηματοπιστωτικά ιδρύματα χρησιμοποιούν μια αλυσίδα μπλοκ για τον διακανονισμό διατραπεζικών πληρωμών στο τέλος της ημέρας για τους δικούς τους λογαριασμούς, τα δημόσια κλειδιά θα σχετίζονται με αυτά τα ιδρύματα και όχι με φυσικά πρόσωπα, πράγμα που σημαίνει ότι δεν θα θεωρούνται προσωπικά δεδομένα που υπόκεινται το GDPR.

Δημόσιο κλειδί είναι τα δεδομένα που «δεν μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο δεδομένων» εκτός εάν αντιστοιχιστούν με «πρόσθετες πληροφορίες», όπως όνομα, διεύθυνση ή άλλες πληροφορίες αναγνώρισης, και επομένως ψευδώνυμα δεδομένα σύμφωνα με το άρθρο 4 παράγραφος 5 του GDPR.

Σύμφωνα με την ομάδα εργασίας του άρθρου 29, η ψευδωνυμοποίηση είναι «η διαδικασία απόκρυψης ταυτοτήτων» που ακριβώς κάνουν τα δημόσια κλειδιά, αλλά όχι με μη αναστρέψιμο τρόπο. Η πρακτική αποκαλύπτει ότι τα δημόσια κλειδιά μπορούν να επιτρέψουν την ταυτοποίηση ενός συγκεκριμένου φυσικού προσώπου. Υπήρξαν περιπτώσεις όπου τα υποκείμενα των δεδομένων έχουν συνδεθεί με δημόσια κλειδιά μέσω της εθελοντικής αποκάλυψης του δημόσιου κλειδιού τους για τη λήψη κεφαλαίων, με παράνομα μέσα ή όταν συλλέγονται πρόσθετες πληροφορίες σύμφωνα με ρυθμιστικές απαιτήσεις καταπολέμησης της νομιμοποίησης εσόδων από παράνομες δραστηριότητες.

Οι υπηρεσίες πορτοφολιού ή τα ανταλλακτήρια μπορεί πράγματι να χρειάζεται να αποθηκεύουν την πραγματική ταυτότητα των μερών προκειμένου να συμμορφώνονται με τις απαιτήσεις για την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες, ενώ οι αντισυμβαλλόμενοι ενδέχεται να το πράξουν και για δικούς τους εμπορικούς σκοπούς. Ο συνδυασμός τέτοιων εγγραφών με το δημόσιο κλειδί θα μπορούσε έτσι να αποκαλύψει την ταυτότητα του πραγματικού κόσμου που κρύβεται πίσω από μια διεύθυνση blockchain.

Πέρα από αυτά, τα δημόσια κλειδιά μπορεί επίσης να αποκαλύπτουν ένα μοτίβο συναλλαγών με γνωστές στο κοινό διευθύνσεις που θα μπορούσαν να «χρησιμοποιηθούν για να ξεχωρίσουν έναν μεμονωμένο χρήστη», όπως μέσω της ανάλυσης γραφημάτων συναλλαγών. Στο Bitcoin blockchain, τα κρυπτογραφημένα δεδομένα έχουν αποδειχθεί ικανά να αποκαλύψουν έναν χρήστη και δεσμός συναλλαγών που επιτρέπει την ανίχνευση των συναλλαγών στους χρήστες.

Η ακαδημαϊκή έρευνα έχει επίσης επιβεβαιώσει ότι τα δημόσια κλειδιά μπορούν να εντοπιστούν στις διευθύνσεις IP, βοηθώντας στην αναγνώριση. Όταν ένας χρήστης μεταδίδει μια συναλλαγή στο δίκτυο, συνήθως συνδέεται απευθείας στο δίκτυο και αποκαλύπτει τη διεύθυνση IP του. Οι υπηρεσίες επιβολής του νόμου σε όλο τον κόσμο έχουν επίσης εντοπίσει άτομα μέσω των δημόσιων κλειδιών τους μέσω τεχνικών ανάλυσης εγκληματολογικών αλυσίδων για τον εντοπισμό υπόπτων εγκληματιών με βάση τα δημόσια κλειδιά τους, και έχει εμφανιστεί μια σειρά επαγγελματιών παρόχων υπηρεσιών που παρέχουν σχετικές υπηρεσίες.

Υπό το φως των παραπάνω, δεν προκαλεί έκπληξη το γεγονός ότι οι σχολιαστές έχουν σημειώσει ότι τα δημόσια κλειδιά μπορεί να αποτελούν προσωπικά δεδομένα σύμφωνα με τον GDPR. Οι Berberich και Steiner έχουν τονίσει ότι «ακόμα και αν τα προσωπικά στοιχεία περιλαμβάνουν μόνο αριθμούς αναγνώρισης αναφοράς, τέτοια αναγνωριστικά είναι συνήθως μοναδικά για ένα συγκεκριμένο άτομο. Ενώ σε όλες αυτές τις περιπτώσεις ενδέχεται να απαιτούνται πρόσθετες πληροφορίες για την απόδοση πληροφοριών στο υποκείμενο των δεδομένων, αυτές οι πληροφορίες θα είναι απλώς ψευδώνυμες και θα υπολογίζονται ως προσωπικές πληροφορίες». . Στο ίδιο συμπέρασμα κατέληξε και η έκθεση του Παρατηρητηρίου και του Φόρουμ Blockchain της Ευρωπαϊκής Ένωσης, η οποία τόνισε τον κίνδυνο συνδεσιμότητας.

Ενώ υπάρχει ανάγκη για προσεκτική ανάλυση κατά περίπτωση σε κάθε περίπτωση, είναι προφανές από τα παραπάνω ότι τα δημόσια κλειδιά που σχετίζονται άμεσα ή έμμεσα με ταυτοποιημένο ή αναγνωρίσιμο φυσικό πρόσωπο χαρακτηρίζονται ως δεδομένα προσωπικού χαρακτήρα σύμφωνα με την ΕΕ. Η ξεχωριστή σύνδεση, η δυνατότητα σύνδεσης και ακόμη και το συμπέρασμα μπορούν να επιτρέψουν τη σύνδεση δημόσιων κλειδιών με ένα αναγνωρισμένο ή αναγνωρίσιμο φυσικό πρόσωπο, και αυτό σε δημόσιες και χωρίς άδεια και ιδιωτικές και επιτρεπόμενες αλυσίδες μπλοκ. Επιπλέον, σύμφωνα με τις οδηγίες της Ομάδας Εργασίας, φαίνεται ότι όταν ένα δημόσιο κλειδί χρησιμεύει ρητά για την αναγνώριση ενός υποκειμένου δεδομένων, η ταξινόμησή του ως δεδομένα προσωπικού χαρακτήρα είναι πάντα δεδομένη.

Σε κάθε περίπτωση, οι οντότητες που χρησιμοποιούν κατανεμημένα λογιστικά βιβλία θα πρέπει να επιδιώκουν να βασίζονται σε μέτρα που σκόπιμα καθιστούν απίθανο το δημόσιο κλειδί να μπορεί να σχετίζεται με ένα αναγνωρισμένο ή αναγνωρίσιμο φυσικό πρόσωπο (όπως τεχνικά και οργανωτικά μέτρα που το κάνουν να δημιουργεί σκληρούς φραγμούς μεταξύ της αλυσίδας μπλοκ και άλλες βάσεις δεδομένων που ενδέχεται να περιέχουν πρόσθετες πληροφορίες για την ενεργοποίηση της σύνδεσης). Η χρήση δημόσιων κλειδιών μιας χρήσης εμφανίζεται επίσης ως καλή πρακτική από αυτή την άποψη. Αυτό μπορεί να είναι ευκολότερο να γίνει σε ιδιωτικές και εξουσιοδοτημένες αλυσίδες μπλοκ παρά σε δημόσια και χωρίς άδεια λογιστικά βιβλία, λόγω των υπαρχόντων μηχανισμών διακυβέρνησης και των θεσμικών δομών που επιτρέπουν έναν τέτοιο σχεδιασμό.

3.6. Δεδομένα συναλλαγών ως προσωπικά δεδομένα

«Δεδομένα συναλλαγών» (transactional data) είναι η ορολογία που χρησιμοποιείται για την αναφορά σε άλλες κατηγορίες δεδομένων που μπορούν να χρησιμοποιηθούν σε blockchains αλλά δεν είναι δημόσια κλειδιά. Αυτά είναι δεδομένα σχετικά με τη συναλλαγή αυτή καθαυτή. Σύμφωνα με τη Γαλλική Αρχή Προστασίας Δεδομένων, αυτό υποδηλώνει δεδομένα που «περιέχονται «εντός» μιας συναλλαγής (π.χ.: δίπλωμα, τίτλος ιδιοκτησίας)». Για παράδειγμα, τα προσωπικά δεδομένα συναλλαγής θα μπορούσαν να είναι ένα όνομα, διεύθυνση ή ημερομηνία γέννησης που περιέχονται στο ωφέλιμο φορτίο μιας δεδομένης συναλλαγής.

Για να προσδιοριστεί εάν τα δεδομένα συναλλαγών πληρούν τον ορισμό των προσωπικών δεδομένων του GDPR, θα πρέπει να πραγματοποιηθεί ανάλυση κατά περίπτωση. Σε ορισμένες περιπτώσεις, τα δεδομένα συναλλαγών σαφώς δεν θεωρούνται προσωπικά δεδομένα. Για παράδειγμα, όπου τα blockchains χρησιμεύουν ως υποδομή δεδομένων που χρησιμοποιείται για την κοινή χρήση δεδομένων κλιματικών αισθητήρων, αυτά μπορεί να μην είναι προσωπικά δεδομένα. Επιπλέον, ένα κρυπτοστοιχείο που μεταφέρεται από το Α στο Β είναι απίθανο να πληροί τις προϋποθέσεις ως προσωπικά δεδομένα. Σε άλλες περιπτώσεις, τα δεδομένα αυτά θα θεωρούνται προσωπικά δεδομένα. Αυτό θα μπορούσε να συμβαίνει όταν μια ομάδα τραπεζών χρησιμοποιεί το blockchain για να μοιράζεται τα δεδομένα του "Know Your Customer".

Κατά την αξιολόγηση του κατά πόσον τα δεδομένα συναλλαγής πληρούν τις προϋποθέσεις ως δεδομένα προσωπικού χαρακτήρα, θα πρέπει να ληφθεί υπόψη ότι σύμφωνα με τη νομοθεσία της ΕΕ για την προστασία δεδομένων, θα πρέπει να ενσωματωθεί ένας ευρύς ορισμός της έννοιας των προσωπικών δεδομένων προκειμένου να διασφαλιστεί η πλήρης και πλήρης προστασία των υποκειμένων των δεδομένων. Τα δεδομένα συναλλαγών αποτελούν πράγματι δεδομένα προσωπικού χαρακτήρα όταν σχετίζονται άμεσα ή έμμεσα με ταυτοποιημένο ή αναγνωρίσιμο φυσικό πρόσωπο. Δεδομένου ότι τα κατανεμημένα λογιστικά βιβλία χρησιμοποιούνται συχνά για την παρακολούθηση περιουσιακών στοιχείων (ουσιαστικά ως λογιστικός μηχανισμός), αξίζει να τονιστεί ότι η Αρχή Προστασίας Δεδομένων του Ηνωμένου Βασιλείου έκρινε ότι κατά την εφαρμογή της δοκιμής παρακινούμενων εισβολέων, θα πρέπει να αναγνωριστεί ότι τα οικονομικά δεδομένα είναι ιδιαίτερα ελκυστικά για τους εισβολείς, πράγμα που σημαίνει ότι οι εισβολείς θα πρέπει να θεωρούνται ότι έχουν ιδιαίτερα κίνητρα.

Σε κάθε περίπτωση, είναι προφανές ότι τα δεδομένα συναλλαγών μπορεί να είναι προσωπικά δεδομένα. Τόσο τα δημόσια κλειδιά όσο και τα δεδομένα συναλλαγών μπορούν να χρησιμοποιηθούν σε απλό κείμενο, σε κρυπτογραφημένη μορφή ή κατακερματισμένα όταν τοποθετούνται στο blockchain. Όπου τα προσωπικά δεδομένα χρησιμοποιούνται σε απλό

κείμενο, αναμφίβολα παραμένουν προσωπικά δεδομένα και συνεπώς δεν απαιτείται ειδική εξέταση αυτού του σεναρίου εδώ. Παρακάτω, εξετάζεται εάν η κρυπτογράφηση ή ο κατακερματισμός είναι μέθοδοι ικανές να μετατρέψουν προσωπικά δεδομένα σε ανώνυμα δεδομένα. Πράγματι, ενώ σε τεχνικούς κύκλους υπάρχει συχνά η υπόθεση ότι τέτοιες διεργασίες καθιστούν ανώνυμα δεδομένα, αυτό το συμπέρασμα δεν δίνεται βάσει του GDPR.

3.6.1. Κρυπτογράφηση

Όπου τα δεδομένα είναι κρυπτογραφημένα, ο κάτοχος του κλειδιού μπορεί ακόμα να αναγνωρίσει εκ νέου κάθε υποκείμενο δεδομένων μέσω αποκρυπτογράφησης, δεδομένου ότι τα προσωπικά δεδομένα εξακολουθούν να υπάρχουν στο σύνολο δεδομένων που έχει κρυπτογραφηθεί. Κατά συνέπεια, τα κρυπτογραφημένα δεδομένα παραμένουν προσωπικά δεδομένα – τουλάχιστον για τον κάτοχο του κλειδιού που μπορεί να αναγνωρίσει τέτοια δεδομένα. Η ομάδα εργασίας του άρθρου 29 διευκρίνισε πράγματι στη γνώμη της για το cloud computing ότι, παρόλο που η κρυπτογράφηση «μπορεί να συμβάλει σημαντικά στην εμπιστευτικότητα των προσωπικών δεδομένων εάν εφαρμοστεί σωστά», δεν «καθιστά τα προσωπικά δεδομένα μη αναστρέψιμα ανώνυμα». Οι σχολιαστές έχουν προτείνει ότι «τα επαρκώς καλά κρυπτογραφημένα δεδομένα, όπου ο πάροχος δεν έχει πρόσβαση στο κλειδί, δεν πρέπει να είναι «προσωπικά δεδομένα», και ομοίως με επαρκώς ανώνυμα δεδομένα». Αυτό σημαίνει ότι μπορεί να πρέπει να γίνει διάκριση μεταξύ αυτών που έχουν πρόσβαση στο ιδιωτικό κλειδί και εκείνων που δεν έχουν πρόσβαση. Το εάν συμβαίνει αυτό θα πρέπει να διευκρινιστεί με περαιτέρω ρυθμιστικές οδηγίες σχετικά με αυτό το θέμα.

3.6.2. Hash Functions

Ένας κρυπτογραφικός κατακερματισμός (cryptographic hash) είναι μια μαθηματική συνάρτηση που τροφοδοτείται με μια τιμή εισόδου που μετατρέπεται σε μια τιμή εξόδου σταθερού μήκους. Για να κατανοήσουμε τις συναρτήσεις κατακερματισμού, είναι επιτακτική ανάγκη να σημειωθεί ότι η ίδια είσοδος παράγει πάντα την ίδια έξοδο (που σημαίνει ότι είναι ντετερμινιστικές). Επιπλέον, δεν είναι δυνατό να συναχθεί η είσοδος κατακερματισμού από την έξοδο κατακερματισμού.

Οι συναρτήσεις κατακερματισμού χρησιμοποιούνται συχνά για την αφαίρεση προσωπικών αναγνωριστικών (όπως ένα όνομα ή τον αριθμό πελάτη) και την αντικατάστασή τους με ένα ψευδώνυμο που είναι δύσκολο να αντιστραφεί. Για

παράδειγμα, όταν εκτελώ το όνομά μου μέσω του κοινού αλγόριθμου κατακερματισμού SHA256, αυτό μου δίνει '0F0D284D20C3198C5769E7B19CA37EF5061BEB9FA9BD7C021B4177F06BC54F66 ότι δεν αποκαλύπτω πρώτα τίποτα σχετικά με τον εαυτό μου. Ωστόσο, αυτό δεν μετατρέπει απαραίτητα τον κατακερματισμό σε ανώνυμα δεδομένα. Παρόλο που είναι αδύνατο να εκτελεστεί αυτή η συνάρτηση προς τα πίσω (για να εξαχθεί η είσοδος από την έξοδο), όποιος γνωρίζει ότι το όνομά μου περιέχεται σε ένα σύνολο δεδομένων μπορεί απλώς να εισαγάγει το όνομά μου στο SHA256 ή σε άλλες κοινώς χρησιμοποιούμενες συναρτήσεις κατακερματισμού κρυπτογράφησης για να δει τι κατακερματισμός αποκαλύπτεται (καθώς η ίδια είσοδος αποδίδει πάντα την ίδια έξοδο). Επιπλέον, η δυνατότητα σύνδεσης μεταξύ αυτού του συνόλου δεδομένων και των πρόσθετων πληροφοριών παραμένει πάντα ένα ζήτημα που πρέπει να προσδιορίζεται προσεκτικά κατά περίπτωση.

Η ευκολία συσχέτισης ενός κατακερματισμού με ένα υποκείμενο δεδομένων δεν πρέπει να υποτιμάται. Πρόσφατα προτάθηκε ότι ο κατακερματισμός όλων των υπαρχουσών διευθύνσεων email παγκοσμίως – περίπου 5 δισεκατομμύρια – θα διαρκούσε περίπου δέκα χιλιοστά του δευτερολέπτου και θα κόστιζε λιγότερο από το ένα εκατοστό του δολαρίου ΗΠΑ. Όταν μια διεύθυνση ηλεκτρονικού ταχυδρομείου είναι γνωστή (μέσω παραβίασης δεδομένων ή αγοράστηκε ως μέρος μιας λίστας αλληλογραφίας μάρκετινγκ), μπορεί να κατακερματιστεί και να συγκριθεί με «ανώνυμες» διευθύνσεις email. Καθώς το πέρασμα μιας διεύθυνσης email μέσω του ίδιου αλγόριθμου κατακερματισμού θα έχει πάντα το ίδιο αποτέλεσμα, τα αποτελέσματα μπορούν να οδηγήσουν σε γνωστές εισόδους. Έτσι, για να είναι ο κατακερματισμός μη αναστρέψιμος, ο αριθμός των πιθανών εισόδων πρέπει να είναι αρκετά μεγάλος και απρόβλεπτος ώστε να αποτρέπεται η επιλογή δοκιμής όλων των πιθανών συνδυασμών.

Λόγω της αυξανόμενης ισχύος και του μειωμένου κόστους των υπολογιστών, αυτό είναι δύσκολο να επιτευχθεί. Αυτό οδήγησε τον Edward Felten να υποστηρίξει ότι «ο κατακερματισμός είναι πολύ υπερτιμημένος ως τεχνική «ανωνυμοποίησης». Έδειξε ότι είναι στην πραγματικότητα αρκετά εύκολο να εξακριβωθεί η ταυτότητα κάποιου με βάση τις συναρτήσεις κατακερματισμού που έχουν προκύψει από αριθμούς κοινωνικής ασφάλισης, απλά έχοντας έναν υπολογιστή να μαντέψει όλους τους πιθανούς αριθμούς κοινωνικής ασφάλισης για μια χώρα.

Το εάν τα κατακερματισμένα δεδομένα παραμένουν πάντα προσωπικά δεδομένα για τους σκοπούς του GDPR είναι θέμα συνεχούς συζήτησης. Από τα παραπάνω θα πρέπει να είναι προφανές ότι η απλή χρήση μιας συνάρτησης κατακερματισμού δεν θα μετατρέψει αυτόματα τα προσωπικά δεδομένα σε ανώνυμα δεδομένα. Η ομάδα εργασίας του άρθρου 29 προειδοποίησε ότι «η ψευδωνυμοποίηση ως διαδικασία που «συνίσταται στην αντικατάσταση ενός χαρακτηριστικού (συνήθως ενός μοναδικού χαρακτηριστικού) σε μια εγγραφή από ένα άλλο. Ως εκ τούτου, το φυσικό πρόσωπο εξακολουθεί να είναι πιθανό να ταυτοποιηθεί. Συνεπώς, η ψευδωνυμοποίηση όταν χρησιμοποιείται μόνη της δεν θα έχει ως αποτέλεσμα μια ανώνυμη βάση δεδομένων».

Ο κατακερματισμός συχνά δημιουργεί ψευδώνυμα και όχι ανώνυμα δεδομένα. Ενώ ο κίνδυνος αντιστροφής που είναι εγγενής στην κρυπτογράφηση δεν ισχύει για τον κατακερματισμό, υπάρχει ωστόσο ο κίνδυνος ότι "αν είναι γνωστό το εύρος τιμών εισόδου της συνάρτησης κατακερματισμού, μπορούν να αναπαραχθούν ξανά μέσω της συνάρτησης κατακερματισμού προκειμένου να εξαχθεί η σωστή τιμή για μια συγκεκριμένη εγγραφή. Κατά συνέπεια, η ομάδα εργασίας προειδοποίησε ότι ενώ οι συναρτήσεις κατακερματισμού μπορούν να μειώσουν «τη δυνατότητα σύνδεσης ενός συνόλου δεδομένων με την αρχική ταυτότητα ενός υποκειμένου δεδομένων· Ως εκ τούτου, είναι ένα χρήσιμο μέτρο ασφαλείας αλλά όχι μια μέθοδος ανωνυμοποίησης".

Υπάρχουν, ωστόσο, συναρτήσεις κατακερματισμού με ισχυρότερες εγγυήσεις απορρήτου που ενδέχεται να αντιστέκονται στη δοκιμή «μέσα που είναι εύλογα πιθανό να χρησιμοποιηθούν» σύμφωνα με την αιτιολογική σκέψη 26 του GDPR. Ο κατακερματισμός λειτουργεί πράγματι σε ένα φάσμα και ορισμένες από τις τεχνικές μπορούν να βοηθήσουν πολύ στην «αποπροσωποποίηση» των προσωπικών δεδομένων. Αυτό οδήγησε ορισμένους συγγραφείς να δηλώσουν ότι «τα ισχυρά κρυπτογραφημένα «προσωπικά δεδομένα» θα πρέπει ήδη να θεωρούνται «ανώνυμα» στα χέρια ενός παρόχου χωρίς πρόσβαση κλειδιού».

Υπάρχει επίσης αβεβαιότητα ως προς το εάν η χρήση αλατισμένων και πιπερωμένων hashes θα μπορούσε να καταστήσει την ταυτοποίηση του υποκειμένου των δεδομένων απίθανη. Ένας **αλατισμένος κατακερματισμός** (salted hash) μπορεί να μειώσει «την πιθανότητα εξαγωγής της τιμής εισόδου». Ωστόσο, η ομάδα εργασίας τόνισε κατηγορηματικά ότι δεν είναι σε θέση να παράγει ανώνυμα δεδομένα δεδομένου ότι «ο υπολογισμός της αρχικής τιμής χαρακτηριστικού που κρύβεται πίσω από το αποτέλεσμα μιας συνάρτησης αλατισμένης κατακερματισμού μπορεί να είναι ακόμα δυνατός εντός λογικών μέσων».

Σε αντίθεση με τα αλατισμένα hashes, οι **πιπερωμένοι κατακερματισμοί (**peppered hashes) βασίζονται σε ένα μυστικό κλειδί (το «πιπέρι») ως πρόσθετη είσοδο. Ωστόσο, ενώ η Ομάδα Εργασίας προέβλεψε την επιλογή των πιπερωμένων κατακερματισμών, δεν υποδεικνύει σαφώς εάν αυτά είναι ικανά να ανωνυμοποιούν δεδομένα για τους σκοπούς του GDPR. Αυτό πρέπει να προσδιορίζεται ανάλογα κατά περίπτωση, λαμβάνοντας υπόψη τη δοκιμή του GDPR «όλα τα μέσα που είναι εύλογα πιθανό να χρησιμοποιηθούν».

Η ομάδα εργασίας εξέδωσε συγκεκριμένα κριτήρια που πρέπει να ληφθούν υπόψη για να καθοριστεί εάν η ταυτοποίηση είναι δυνατή με βάση τα μέσα που είναι εύλογα πιθανό να χρησιμοποιηθούν: (i) signling out, (ii) σύνδεση και (iii) συμπεράσματα. Ακόμη και με πιπερωμένους κατακερματισμούς, το άτομο εξακολουθεί να προσδιορίζεται από ένα μοναδικό χαρακτηριστικό που είναι το αποτέλεσμα της συνάρτησης ψευδωνυμοποίησης. Ομοίως, η συνδεσιμότητα μπορεί να εξακολουθεί να είναι δυνατή μέσω άλλων χαρακτηριστικών. Αυτό θα μπορούσε να είναι το παράδειγμα βιομετρικών δεδομένων ή διευθύνσεων που αποθηκεύονται με ψευδώνυμο. Τέλος, τα συμπεράσματα παραμένουν επίσης

μια λογική επιλογή όταν ένα ίδιο σύνολο δεδομένων ή διαφορετικές βάσεις δεδομένων χρησιμοποιούν το ίδιο χαρακτηριστικό για το ίδιο υποκείμενο δεδομένων.

Συνεπάγεται ότι, εκτός εάν τέτοιοι μηχανισμοί συνδυάζονται με πρόσθετες εγγυήσεις απορρήτου, οι κατακερματισμοί παραμένουν προσωπικά δεδομένα καθώς υπάρχει κίνδυνος συνδεσιμότητας αφού τα υποκείμενα των δεδομένων ενδέχεται να εξακολουθούν να αναγνωρίζονται μέσω έμμεσων αναγνωριστικών, συμπεριλαμβανομένων άλλων πληροφοριών στο σύνολο δεδομένων ή από άλλες πηγές. Αξίζει να σημειωθεί ότι στο συγκεκριμένο πλαίσιο του blockchain, υπάρχουν πολυάριθμες τεχνικές εξελίξεις που επιδιώκουν να προσφέρουν ισχυρότερες εγγυήσεις ανωνυμίας.

4. Γενικός Κανονισμός για την Προστασία των Δεδομένων -- GDPR

4.1. Ορισμός και σκοπός της νομοθεσίας

Ο GDPR τέθηκε σε ισχύ στις 25 Μαΐου 2018 και αντικατέστησε την υπάρχουσα Οδηγία για την Προστασία Δεδομένων από το 1995 [GDPR2016]. Ο GDPR είναι σχετικός για κάθε αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων στην ΕΕ ή από υποκείμενα που βρίσκονται εντός της ΕΕ. Ορίζει τα προσωπικά δεδομένα ως: "κάθε πληροφορία που σχετίζεται με ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο". Φυσικό πρόσωπο με δυνατότητα ταυτοποίησης είναι εκείνο που μπορεί να αναγνωριστεί, άμεσα ή έμμεσα, ιδίως με αναφορά σε αναγνωριστικό, όπως όνομα ή αριθμό αναγνώρισης.

Η επεξεργασία προσωπικών δεδομένων πρέπει να πληροί ορισμένες απαιτήσεις. Ο GDPR ορίζει ότι κάθε επεξεργασία πρέπει να υπακούει στις «αρχές που σχετίζονται με την επεξεργασία δεδομένων προσωπικού χαρακτήρα». Αυτές οι αρχές αναφέρουν, μεταξύ άλλων, ότι τα προσωπικά δεδομένα πρέπει να είναι σωστά, ενημερωμένα και ότι τα εσφαλμένα δεδομένα πρέπει να διαγράφονται αμέσως. Επιπλέον, τα δεδομένα θα πρέπει να αποθηκεύονται μόνο για όσο διάστημα είναι απαραίτητο. Ο GDPR επιτρέπει στο υποκείμενο των δεδομένων να διορθώσει λανθασμένα προσωπικά δεδομένα. Το δικαίωμα στη λήθη παρέχει το δικαίωμα (υπό ορισμένες προϋποθέσεις) στο υποκείμενο των δεδομένων να ζητήσει τη διαγραφή των προσωπικών του δεδομένων.

Ο GDPR απαιτεί κατάλληλα τεχνικά και οργανωτικά μέτρα για να εγγυηθούν τις αρχές της επεξεργασίας προσωπικών δεδομένων. Αυτά τα μέτρα είναι, μεταξύ άλλων, η χρήση κρυπτογράφησης και ψευδωνυμοποίησης, καθώς και μέθοδοι διασφάλισης της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των προσωπικών δεδομένων.

Τέλος, ο GDPR διαχειρίζεται τη μεταφορά προσωπικών δεδομένων σε τρίτες χώρες. Η διαβίβαση αυτών των ειδών δεδομένων επιτρέπεται, γενικά, μόνο όταν η χώρα υποδοχής διασφαλίζει το κατάλληλο επίπεδο προστασίας. Εάν δεν συμβαίνει αυτό, υπάρχουν ορισμένες πρόσθετες προϋποθέσεις που επιτρέπουν τη μεταφορά. Σύμφωνα με το άρθ. 49 του GDPR αυτό μπορεί να είναι για παράδειγμα η ρητή συγκατάθεση του υποκειμένου των δεδομένων.

Η κύρια νομική πράξη της ΕΕ για την προστασία δεδομένων είναι ο κανονισμός (ΕΕ) 2016/279 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων (Γενικός Κανονισμός Προστασίας Δεδομένων – GDPR). Είναι ένας κανονισμός στην νομοθεσία της ΕΕ για την προστασία των δεδομένων και την ιδιωτικότητα στην Ευρωπαϊκή Ένωση (ΕΕ) και στον Ευρωπαϊκό Οικονομικό Χώρο (ΕΟΧ). Αναφέρεται επίσης στη μεταφορά προσωπικών δεδομένων εκτός των χωρών της ΕΕ και του ΕΟΧ. Ο πρωταρχικός στόχος του GDPR είναι να δώσει στα άτομα τον έλεγχο των προσωπικών τους δεδομένων και να απλοποιήσει το ρυθμιστικό περιβάλλον για τις διεθνείς επιχειρήσεις ενοποιώντας τον κανονισμό εντός της Ευρωπαϊκής Ένωσης. Συμπληρώνοντας την Οδηγία Προστασίας Δεδομένων 95/46/ΕΚ, ο εν λόγω κανονισμός περιέχει διατάξεις και απαιτήσεις που σχετίζονται με την επεξεργασία προσωπικών δεδομένων ατόμων (που ονομάζονται επίσημα υποκείμενα δεδομένων στον ΓΚΠΔ) που βρίσκονται στον ΕΟΧ και ισχύει για οποιαδήποτε επιχείρηση - ανεξάρτητα από την τοποθεσία, την υπηκοότητα ή την κατοικία των υποκειμένων των δεδομένων - που επεξεργάζεται τις προσωπικές πληροφορίες των ατόμων εντός του ΕΟΧ.

Ο GDPR θεσπίζει κανόνες για την προστασία των φυσικών προσώπων, ανεξαρτήτως ιθαγένειας ή διαμονής, σχετικά με την επεξεργασία των προσωπικών τους δεδομένων και κανόνες σχετικά με την ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα (άρθρο 1). Ιδιαίτερα, ισχύει για την επεξεργασία δεδομένων προσωπικού χαρακτήρα εν όλω ή εν μέρει με αυτοματοποιημένα μέσα (άρθρο 2). Επιπλέον, όσον αφορά το εδαφικό πεδίο εφαρμογής του GDPR, εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα από εγκατάσταση υπεύθυνου επεξεργασίας ή εκτελούντος την επεξεργασία στην Ένωση.

Αξίζει να σημειωθεί ότι οι ανώνυμες πληροφορίες, συγκεκριμένα πληροφορίες που δεν μπορούν να αποδοθούν σε αναγνωρισμένο ή ταυτοποιήσιμο φυσικό πρόσωπο ή προσωπικά δεδομένα που κατέστησαν ανώνυμα καθιστώντας το υποκείμενο των δεδομένων μη ταυτοποιήσιμο, ακόμη και για στατιστικούς ή ερευνητικούς σκοπούς, δεν ρυθμίζονται από τον GDPR.

Αρχεία ή σύνολα αρχείων, καθώς και τα εξώφυλλά τους, τα οποία δεν είναι δομημένα σύμφωνα με συγκεκριμένα κριτήρια, δεν εμπίπτουν στο πεδίο εφαρμογής του GDPR.

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα από ιδιώτες μόνο για προσωπικούς ή οικιακούς σκοπούς δεν εμπίπτει επίσης στο πεδίο εφαρμογής του παρόντος κανονισμού (εξαίρεση νοικοκυριών).

Ο GDPR δεν ισχύει για την επεξεργασία των προσωπικών δεδομένων από τα θεσμικά όργανα, τους φορείς και τα γραφεία και τους οργανισμούς της Ένωσης, καθώς αυτό εμπίπτει στο πεδίο εφαρμογής του Κανονισμού (ΕΚ) 45/2001.

Επιπλέον, όσον αφορά τη διεκπεραίωση από τις δικαστικές αρχές και τις αρχές επιβολής του νόμου σχετικά με την πρόληψη, τη διερεύνηση, τον εντοπισμό ή τη δίωξη ποινικών αδικημάτων ή την εκτέλεση ποινικών κυρώσεων, συμπεριλαμβανομένης της διασφάλισης και της πρόληψης απειλών για τη δημόσια ασφάλεια, η οδηγία (ΕΕ) 2016/680 ισχύει.

4.2. Το πεδίο εφαρμογής του GDPR

Όπως ορίζεται στις αιτιολογικές σκέψεις του GDPR, ενώ πρέπει να διασφαλίζεται υψηλό επίπεδο προστασίας των φυσικών προσώπων με όσον αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα, αυτή θα πρέπει να εξισορροπηθεί με άλλα θεμελιώδη δικαιώματα σύμφωνα με την αρχή της αναλογικότητας. Οι τεχνολογικές εξελίξεις και η επέκταση της επεξεργασίας και της ανταλλαγής δεδομένων κατέστησαν επιτακτική για τα όργανα της Ένωσης τη θέσπιση ενός ισχυρού και πιο συνεκτικού πλαισίου προστασίας δεδομένων.

Ο κανονισμός General Data Protection Regulation ή GDPR 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.

Ο κανονισμός προστατεύει θεμελιώδη δικαιώματα και ελευθερίες των φυσικών προσώπων και ειδικότερα το δικαίωμά τους στην προστασία των δεδομένων προσωπικού χαρακτήρα.

Ο κανονισμός εφαρμόζεται στην 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 εφαρμόζεται εάν οι δραστηριότητες επεξεργασίας σχετίζονται με:

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

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

4.3. Ορισμοί

Προσωπικά δεδομένα (personal data)

Κάθε πληροφορία που αφορά ταυτοποιημένο φυσικό πρόσωπο (υποκείμενο των δεδομένων).

Επεξεργασία (processing)

Κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή.

Κατάρτιση προφίλ (profiling)

Οποιαδήποτε μορφή αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα που συνίσταται στη χρήση δεδομένων προσωπικού χαρακτήρα για την αξιολόγηση ορισμένων προσωπικών πτυχών ενός φυσικού προσώπου, ιδίως για την ανάλυση ή την πρόβλεψη πτυχών που αφορούν την απόδοση στην εργασία, την οικονομική κατάσταση, την υγεία, τις προσωπικές προτιμήσεις, τα ενδιαφέροντα, την αξιοπιστία, τη συμπεριφορά, τη θέση ή τις μετακινήσεις του εν λόγω φυσικού προσώπου.

Ψευδωνυμοποίηση (pseudonymisation)

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο ώστε τα δεδομένα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρωματικές πληροφορίες διατηρούνται χωριστά.

Σύστημα αρχειοθέτησης (filing system)

Κάθε διαρθρωμένο σύνολο δεδομένων προσωπικού χαρακτήρα τα οποία είναι προσβάσιμα με γνώμονα συγκεκριμένα κριτήρια.

Υπεύθυνος επεξεργασίας (controller)

Το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

Εκτελών την επεξεργασία (processor)

Το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας.

Αποδέκτης (recipient)

Το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας, στα οποία κοινολογούνται τα δεδομένα προσωπικού χαρακτήρα, είτε πρόκειται για τρίτον είτε όχι. Ωστόσο, οι δημόσιες αρχές που ενδέχεται να λάβουν δεδομένα προσωπικού χαρακτήρα στο πλαίσιο συγκεκριμένης έρευνας σύμφωνα με το δίκαιο της Ένωσης ή κράτους μέλους δεν θεωρούνται ως αποδέκτες.

Τρίτος (third party)

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

Συγκατάθεση του υποκειμένου των δεδομένων (consent of the data subject)

Κάθε ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει, με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν.

Παραβίαση δεδομένων προσωπικού χαρακτήρα (personal data breach)

Η παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα.

Γενετικά δεδομένα (genetic data)

Τα δεδομένα προσωπικού χαρακτήρα που αφορούν τα γενετικά χαρακτηριστικά φυσικού προσώπου που κληρονομήθηκαν ή αποκτήθηκαν, όπως προκύπτουν, ιδίως, από ανάλυση βιολογικού δείγματος του εν λόγω φυσικού προσώπου και τα οποία παρέχουν μοναδικές πληροφορίες σχετικά με την φυσιολογία ή την υγεία του εν λόγω φυσικού προσώπου.

Βιομετρικά δεδομένα (biometric data)

Δεδομένα προσωπικού χαρακτήρα τα οποία προκύπτουν από ειδική τεχνική επεξεργασία συνδεόμενη με φυσικά, βιολογικά ή συμπεριφορικά χαρακτηριστικά φυσικού προσώπου και τα οποία επιτρέπουν ή επιβεβαιώνουν την αδιαμφισβήτητη ταυτοποίηση του εν λόγω φυσικού προσώπου, όπως εικόνες προσώπου ή δακτυλοσκοπικά δεδομένα.

Κύρια εγκατάσταση (main establishment)

α) όταν πρόκειται για υπεύθυνο επεξεργασίας με εγκαταστάσεις σε περισσότερα του ενός κράτη μέλη, ο τόπος της κεντρικής του διοίκησης στην Ένωση.

β) όταν πρόκειται για εκτελούντα την επεξεργασία με εγκαταστάσεις σε περισσότερα του ενός κράτη μέλη, ο τόπος της κεντρικής του διοίκησης στην Ένωση.

Εκπρόσωπος (representative)

Φυσικό ή νομικό πρόσωπο εγκατεστημένο στην Ένωση, το οποίο ορίζεται εγγράφως από τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία βάσει του άρθρου 27 και εκπροσωπεί τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία ως προς τις αντίστοιχες υποχρεώσεις τους δυνάμει του παρόντος κανονισμού.

Επιχείρηση (enterprise)

Φυσικό ή νομικό πρόσωπο που ασκεί οικονομική δραστηριότητα, ανεξάρτητα από τη νομική του μορφή, περιλαμβανομένων των προσωπικών εταιρειών ή των ενώσεων που ασκούν τακτικά οικονομική δραστηριότητα.

Όμιλος επιχειρήσεων (group of undertakings)

Μια ελέγχουσα επιχείρηση και οι ελεγχόμενες από αυτήν επιχειρήσεις.

Δεσμευτικοί εταιρικοί κανόνες (binding corporate rules)

Οι πολιτικές προστασίας δεδομένων προσωπικού χαρακτήρα τις οποίες ακολουθεί ένας υπεύθυνος επεξεργασίας ή εκτελών την επεξεργασία για διαβιβάσεις δεδομένων προσωπικού χαρακτήρα σε υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία.

Εποπτική αρχή (supervisory authority)

Ανεξάρτητη δημόσια αρχή που συγκροτείται από κράτος μέλος σύμφωνα με το άρθρο 51.

Ενδιαφερόμενη εποπτική αρχή (supervisory authority concerned)

Εποπτική αρχή την οποία αφορά η επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Διασυνοριακή επεξεργασία (cross-border processing)

α) η επεξεργασία δεδομένων προσωπικού χαρακτήρα η οποία γίνεται στο πλαίσιο των δραστηριοτήτων διάφορων εγκαταστάσεων σε περισσότερα του ενός κράτη μέλη ή

β) η επεξεργασία δεδομένων προσωπικού χαρακτήρα η οποία ενδέχεται να επηρεάσει ουσιωδώς υποκείμενα των δεδομένων σε περισσότερα του ενός κράτη μέλη,

Σχετική και αιτιολογημένη ένσταση (relevant and reasoned objection)

Ένσταση σε ένα σχέδιο απόφασης ως προς την ύπαρξη παράβασης του παρόντος κανονισμού, η οποία καταδεικνύει σαφώς τη σημασία των κινδύνων που εγκυμονεί το σχέδιο απόφασης όσον αφορά τα θεμελιώδη δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων και, κατά περίπτωση, την ελεύθερη κυκλοφορία δεδομένων προσωπικού χαρακτήρα εντός της Ένωσης.

Υπηρεσία της κοινωνίας των πληροφοριών (information society service)

Υπηρεσία κατά την έννοια του άρθρου 1 παράγραφος 1 στοιχείο β) της οδηγίας (ΕΕ) 2015/1535 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (19).

Διεθνής οργανισμός (international organisation)

Οργανισμός και οι υπαγόμενοι σε αυτόν φορείς που διέπονται από το δημόσιο διεθνές δίκαιο ή οποιοσδήποτε άλλος φορέας που έχει ιδρυθεί δυνάμει ή επί τη βάσει συμφωνίας μεταξύ δύο ή περισσότερων χωρών.

4.4. Βασικές αρχές επεξεργασίας προσωπικών δεδομένων

Νομιμότητα, αντικειμενικότητα και διαφάνεια – Τα προσωπικά δεδομένα υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων.

Περιορισμός σκοπού – προσωπικά δεδομένα που συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς. Η 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.

Ελαχιστοποίηση δεδομένων – είναι κατάλληλα, συναφή και περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία.

Ακρίβεια –τα προσωπικά δεδομένα είναι ακριβή και, όταν είναι αναγκαίο, επικαιροποιούνται· πρέπει να λαμβάνονται όλα τα εύλογα μέτρα για την άμεση διαγραφή ή διόρθωση δεδομένων προσωπικού χαρακτήρα τα οποία είναι ανακριβή, σε σχέση με τους σκοπούς της επεξεργασίας.

Περιορισμός αποθήκευσης – Τα προσωπικά δεδομένα θα διατηρούνται σε μορφή που να επιτρέπει την ταυτοποίηση του υποκειμένου των δεδομένων μόνο για το χρόνο που είναι απαραίτητος για τον σκοπό για τον οποίο υποβάλλονται σε επεξεργασία.

Ακεραιότητα και εμπιστευτικότητα – υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλεια των δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά, με τη χρησιμοποίηση κατάλληλων τεχνικών ή οργανωτικών μέτρων.

Λογοδοσία – Ο υπεύθυνος επεξεργασίας είναι υπεύθυνος και σε θέση να αποδείξει τη συμμόρφωση με τις προαναφερθείσες αρχές.

Η αρχή της νομιμότητας απαιτεί τα δεδομένα προσωπικού χαρακτήρα να υποβάλλονται σε επεξεργασία με βάση τη συναίνεση του συγκεκριμένου υποκειμένου των δεδομένων ή κάποια άλλη νόμιμη βάση.

Άλλη νόμιμη βάση, μπορεί να είναι:

- αναγκαιότητα συμμόρφωσης με τη νομική υποχρέωση στην οποία υπόκειται ο υπεύθυνος επεξεργασίας.
- αναγκαιότητα εκτέλεσης μιας σύμβασης στην οποία το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή ως βήμα πριν από τη σύναψη σύμβασης κατόπιν αιτήματος του υποκειμένου των δεδομένων.
- αναγκαιότητα προστασίας των ζωτικών συμφερόντων του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου45.
- αναγκαιότητα σύμφωνα με τα έννομα συμφέροντα που επιδιώκονται από τον υπεύθυνο επεξεργασίας ή από τρίτο μέρος, εκτός εάν υπερβαίνουν τα συμφέροντα ή τα θεμελιώδη δικαιώματα του υποκειμένου των δεδομένων, ιδίως όταν είναι παιδί, τα οποία απαιτούν προστασία προσωπικών δεδομένων.

Με βάση τη νομολογία του Ευρωπαϊκού Δικαστηρίου Ανθρωπίνων Δικαιωμάτων, ο **περιορισμός** του θεμελιώδους δικαιώματος στην προστασία των δεδομένων προσωπικού χαρακτήρα πρέπει να είναι απολύτως απαραίτητος. «Η

αναγκαιότητα δικαιολογείται βάσει αντικειμενικών αποδεικτικών στοιχείων και αποτελεί το πρώτο βήμα πριν από την αξιολόγηση της αναλογικότητας του περιορισμού». Επιπλέον, τα μέσα επεξεργασίας, οι κατηγορίες των δεδομένων που υποβάλλονται σε επεξεργασία και η διάρκεια αποθήκευσης είναι πάντα απαραίτητα για το σκοπό της επεξεργασίας.

Η **αναλογικότητα** απαιτεί τα μειονεκτήματα της μη πλήρους άσκησης του δικαιώματος προστασίας δεδομένων να μην υπερισχύουν των πλεονεκτημάτων που οφείλονται στον περιορισμό του δικαιώματος, δηλαδή ο περιορισμός πρέπει να αιτιολογείται και να συνοδεύεται από μέτρα διασφάλισης.

Οι **σκοποί της επεξεργασίας προσωπικών δεδομένων** θα πρέπει να είναι συμβατοί με τους σκοπούς για τους οποίους συλλέχθηκαν αρχικά τα προσωπικά δεδομένα και επομένως η κοινή νομική βάση καλύπτει και τις δύο περιπτώσεις. Εάν η επεξεργασία είναι απαραίτητη για το δημόσιο συμφέρον, η νομοθεσία της ΕΕ ή η εθνική νομοθεσία καθορίζει και προσδιορίζει τα καθήκοντα και τους σκοπούς για τους οποίους η περαιτέρω επεξεργασία θα πρέπει να θεωρείται ως συμβατή και νόμιμή.

Όταν το υποκείμενο των δεδομένων έχει δώσει τη **συγκατάθεσή** του ή η επεξεργασία βασίζεται στο ενωσιακό ή εθνικό δίκαιο και αποτελεί αναγκαίο και αναλογικό μέτρο σε μια δημοκρατική κοινωνία για τη διασφάλιση, ιδίως, σημαντικών στόχων γενικού δημόσιου συμφέροντος, ο υπεύθυνος επεξεργασίας θα πρέπει να έχει τη δυνατότητα να επεξεργάζεται περαιτέρω τα προσωπικά δεδομένα ανεξάρτητα από τη συμβατότητα των σκοπών.

Περαιτέρω επεξεργασία για σκοπούς αρχειοθέτησης προς το **δημόσιο συμφέρον**, επιστημονικούς ή ιστορικούς σκοπούς έρευνας ή στατιστικούς σκοπούς θα πρέπει να θεωρούνται συμβατές νόμιμες πράξεις επεξεργασίας. Ωστόσο, θα πρέπει να υπάρχουν κατάλληλες διασφαλίσεις, για παράδειγμα η ψευδωνυμοποίηση.

Η **αρχή της διαφάνειας** απαιτεί κάθε πληροφορία που απευθύνεται στο κοινό ή στο υποκείμενο των δεδομένων να είναι συνοπτική, εύκολα προσβάσιμη και κατανοητή, και να χρησιμοποιείται σαφής και απλή γλώσσα ή ακόμη και οπτικοποίηση, ειδικά για πληροφορίες που απευθύνονται σε ένα παιδί. Οι πληροφορίες πρέπει να παρέχονται γραπτώς ή με άλλα μέσα, συμπεριλαμβανομένων των ηλεκτρονικών μέσων. Όταν οι πληροφορίες παρέχονται προφορικά, η ταυτότητα αυτού του υποκειμένου των δεδομένων πρέπει να αποδεικνύεται με άλλα μέσα.

Η **λογοδοσία** αντιστοιχεί στην ενεργή εφαρμογή μέτρων από τους υπευθύνους επεξεργασίας για την προώθηση και τη διασφάλιση της προστασίας δεδομένων κατά τις εργασίες επεξεργασίας τους. Οι υπεύθυνοι επεξεργασίας είναι υπεύθυνοι για τη συμμόρφωση των δραστηριοτήτων επεξεργασίας τους με τον GDPR και θα πρέπει να είναι σε θέση ανά πάσα στιγμή να αποδείξουν τη συμμόρφωσή τους στο ευρύ κοινό και στις εποπτικές αρχές.

4.5. Πότε η επεξεργασία προσωπικών δεδομένων είναι νόμιμη

Η επεξεργασία είναι σύννομη μόνο εάν και εφόσον ισχύει τουλάχιστον μία από τις ακόλουθες προϋποθέσεις:

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

β) η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή για να ληφθούν μέτρα κατ' αίτηση του υποκειμένου των δεδομένων πριν από τη σύναψη σύμβασης,

γ) η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση του υπευθύνου επεξεργασίας,

δ) η επεξεργασία είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου,

ε) η επεξεργασία είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας,

στ) η επεξεργασία είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, εκτός εάν έναντι των συμφερόντων αυτών υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων που επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα, ιδίως εάν το υποκείμενο των δεδομένων είναι παιδί.

4.6. Τα δικαιώματα των πολιτών

Ένας από τους στόχους του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR) είναι να ενδυναμώσει τα άτομα και να τους δώσει τον έλεγχο των προσωπικών τους δεδομένων. Ο GDPR έχει ένα κεφάλαιο για τα δικαιώματα των υποκειμένων των δεδομένων (άτομα). Ο GDPR ενισχύει τα υπάρχοντα δικαιώματα, προβλέπει νέα δικαιώματα και δίνει στους πολίτες περισσότερο έλεγχο στα προσωπικά τους δεδομένα. Αυτά περιλαμβάνουν:

- ευκολότερη πρόσβαση στα δεδομένα τους — συμπεριλαμβανομένης της παροχής περισσότερων πληροφοριών σχετικά με τον τρόπο επεξεργασίας αυτών των δεδομένων και της διασφάλισης ότι αυτές οι πληροφορίες είναι διαθέσιμες με σαφή και κατανοητό τρόπο.
- δικαίωμα στη φορητότητα δεδομένων — διευκολύνει τη μετάδοση προσωπικών δεδομένων μεταξύ παρόχων υπηρεσιών.
- Δικαίωμα διαγραφής («δικαίωμα στη λήθη») — όταν ένα άτομο δεν θέλει πλέον να υποβάλλονται σε επεξεργασία τα δεδομένα του και δεν υπάρχει νόμιμος λόγος να τα διατηρήσει, τα δεδομένα θα διαγραφούν.
- δικαίωμα να γνωρίζουν πότε έχουν παραβιαστεί τα προσωπικά τους δεδομένα — οι εταιρείες και οι οργανισμοί θα πρέπει να ενημερώνουν τα άτομα αμέσως για σοβαρές παραβιάσεις δεδομένων. Θα πρέπει επίσης να ενημερώσουν την αρμόδια εποπτική αρχή προστασίας δεδομένων.

Όλοι οι κανόνες, οι περιορισμοί και οι απαιτήσεις που τίθενται στον GDPR μοιράζονται τον στόχο της προστασίας των υποκειμένων των δεδομένων (ή των χρηστών) και της προάσπισης των δικαιωμάτων τους. Το Κεφάλαιο 3 του GDPR καταγράφει αυτά τα δικαιώματα ως Δικαιώματα του Υποκειμένου των Δεδομένων. Περιγράφει οκτώ διακριτά δικαιώματα που δικαιούνται όλοι οι Ευρωπαίοι και τα οποία κάθε οργανισμός πρέπει να υποστηρίζει. Τα οκτώ δικαιώματα χρήστη είναι:

- Το Δικαίωμα στην Πληροφόρηση
- Το Δικαίωμα Πρόσβασης
- Το Δικαίωμα στη Διόρθωση
- Το δικαίωμα στη Διαγραφή
- Το Δικαίωμα στον Περιορισμό της Επεξεργασίας
- Το Δικαίωμα στη Φορητότητα Δεδομένων
- Το δικαίωμα στην Αντίρρηση
- Το Δικαίωμα Αποφυγής Αυτοματοποιημένης Λήψης Αποφάσεων

4.7. Κανόνες για τις επιχειρήσεις

Ο GDPR έχει σχεδιαστεί για τη δημιουργία επιχειρηματικών ευκαιριών και την τόνωση της καινοτομίας μέσω μιας σειράς βημάτων που περιλαμβάνουν:

• ένα **ενιαίο σύνολο κανόνων** σε όλη την ΕΕ. ένας υπεύθυνος προστασίας δεδομένων, υπεύθυνος για την προστασία δεδομένων, θα οριστεί από τις δημόσιες αρχές και από τις επιχειρήσεις που επεξεργάζονται δεδομένα σε μεγάλη κλίμακα·

- **one-stop-shop** — οι επιχειρήσεις πρέπει να συναλλάσσονται μόνο με μία μόνο εποπτική αρχή (στη χώρα της ΕΕ στην οποία εδρεύουν κυρίως).

- Κανόνες της ΕΕ για **εταιρείες εκτός ΕΕ** — οι εταιρείες που εδρεύουν εκτός ΕΕ πρέπει να εφαρμόζουν τους ίδιους κανόνες όταν προσφέρουν υπηρεσίες ή αγαθά ή παρακολουθούν τη συμπεριφορά ατόμων εντός της ΕΕ.

- **κανόνες φιλικοί προς την καινοτομία** — εγγύηση ότι οι διασφαλίσεις προστασίας δεδομένων ενσωματώνονται σε προϊόντα και υπηρεσίες από το αρχικό στάδιο ανάπτυξης (προστασία δεδομένων από τον σχεδιασμό και από προεπιλογή).

- Τεχνικές **φιλικές προς το απόρρητο**, όπως η ψευδωνυμοποίηση (όταν τα πεδία αναγνώρισης σε μια εγγραφή δεδομένων αντικαθίστανται από ένα ή περισσότερα τεχνητά αναγνωριστικά) και η κρυπτογράφηση (όταν τα δεδομένα κωδικοποιούνται με τέτοιο τρόπο ώστε μόνο εξουσιοδοτημένα μέρη να μπορούν να τα διαβάσουν).

- **κατάργηση ειδοποιήσεων** — οι νέοι κανόνες προστασίας δεδομένων θα καταργήσουν τις περισσότερες υποχρεώσεις κοινοποίησης και το κόστος που σχετίζεται με αυτές. Ένας από τους στόχους του κανονισμού για την προστασία δεδομένων είναι η άρση των εμποδίων στην ελεύθερη ροή προσωπικών δεδομένων εντός της ΕΕ. Αυτό θα διευκολύνει την επέκταση των επιχειρήσεων.

- **εκτιμήσεις επιπτώσεων** — οι επιχειρήσεις θα πρέπει να διενεργούν εκτιμήσεις επιπτώσεων όταν η επεξεργασία δεδομένων μπορεί να οδηγήσει σε υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των ατόμων.

- **τήρηση αρχείων** — Οι MME25 δεν υποχρεούνται να τηρούν αρχεία σχετικά με τις δραστηριότητες επεξεργασίας, εκτός εάν η επεξεργασία είναι τακτική ή ενδέχεται να θέσει σε κίνδυνο τα δικαιώματα και τις ελευθερίες του ατόμου του οποίου τα δεδομένα υφίστανται επεξεργασία.

4.7.1. Ισχύει ο GDPR για τις μικρές επιχειρήσεις;

Όταν τέθηκε σε ισχύ ο GDPR, υπήρχε μια εσφαλμένη αντίληψη ότι ίσχυε μόνο για τις πολυεθνικές και ότι οι ιδιοκτήτες μικρών επιχειρήσεων δεν χρειαζόταν να ασχοληθούν με αυτό.

Η αλήθεια είναι ότι ο κανονισμός ισχύει για όλους τους οργανισμούς που επεξεργάζονται προσωπικά δεδομένα κατοίκων της ΕΕ, είτε είναι ατομικοί έμποροι, είτε μικρές επιχειρήσεις είτε όμιλοι ετερογενών δραστηριοτήτων.

Ωστόσο, υπάρχει εξαίρεση για οργανισμούς που απασχολούν λιγότερα από 250 άτομα. Εάν ο οργανισμός σας πληροί αυτό το κριτήριο, χρειάζεται μόνο να τεκμηριώσετε δραστηριότητες επεξεργασίας που:

- Είναι κάτι περισσότερο από ένα μεμονωμένο περιστατικό ή κάτι που κάνετε σπάνια.
- Είναι πιθανό να οδηγήσουν σε κίνδυνο για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων· και
- Περιλαμβάνουν ειδικές κατηγορίες προσωπικών δεδομένων ή δεδομένα ποινικής καταδίκης και αδικήματος.

4.7.2. Συγκατάθεση

Σε αντίθεση με ό,τι μπορεί να έχετε ακούσει, δεν χρειάζεστε απαραίτητα συγκατάθεση για την επεξεργασία προσωπικών δεδομένων.

Όταν βασίζεστε στη συγκατάθεση, να θυμάστε ότι το υποκείμενο των δεδομένων πρέπει να παράσχει μια σαφή καταφατική ενέργεια για να είναι έγκυρη. Αυτό σημαίνει ότι δεν υπάρχουν προεπιλεγμένα πλαίσια ή συμφωνίες κρυμμένες σε άλλα αιτήματα.

Παραδείγματα σαφούς καταφατικής ενέργειας περιλαμβάνουν την υπογραφή μιας δήλωσης συναίνεσης σε μια έντυπη φόρμα, το κλικ σε ένα κουμπί ή σύνδεσμο συμμετοχής και την επιλογή τεχνικών ρυθμίσεων ή προτιμήσεων σε έναν πίνακα εργαλείων.

4.7.3. Εμπορία

Μπορείτε να προωθήσετε πληροφορίες απευθείας σε οποιονδήποτε, υπό την προϋπόθεση ότι η επεξεργασία πληροί ορισμένες απαιτήσεις.

Πρέπει να λάβετε τις πληροφορίες του υποκειμένου των δεδομένων χρησιμοποιώντας νόμιμες βάσεις, και ο τρόπος με τον οποίο χρησιμοποιείτε αυτές τις πληροφορίες πρέπει να έχει ελάχιστο αντίκτυπο στο απόρρητό του και πρέπει να είστε εύλογα σίγουροι ότι δεν θα εναντιωθεί σε αυτό που κάνετε.

Εάν η επεξεργασία υπόκειται επίσης στον PECR (Κανονισμοί Απορρήτου και Ηλεκτρονικών Επικοινωνιών), πρέπει επίσης να ενημερώσετε το υποκείμενο των δεδομένων ότι χρησιμοποιείτε τα δεδομένα του για σκοπούς μάρκετινγκ.
Εάν αντιταχθεί, θα πρέπει να σταματήσετε την επεξεργασία των προσωπικών τους δεδομένων.

4.7.4. Δικαίωμα πρόσβασης του υποκειμένου των δεδομένων

Ο GDPR δίνει στα άτομα το δικαίωμα να ελέγχουν τα προσωπικά τους δεδομένα που επεξεργάζεται ένας οργανισμός.

Η διαδικασία με την οποία το κάνουν αυτό είναι γνωστή ως DSAR (αίτημα πρόσβασης στο υποκείμενο δεδομένων) – και μόλις ληφθούν, οι οργανισμοί έχουν στη διάθεσή τους ένα μήνα για να απαντήσουν.

4.7.5. Αναφορά παραβίασης δεδομένων

Οι οργανισμοί πρέπει να ειδοποιήσουν την εποπτική τους αρχή για μια παραβίαση δεδομένων εντός 72 ωρών από τη στιγμή που την αντιλήφθηκαν. Με τον όρο «παραβίαση», δεν αναφερόμαστε απλώς σε επιθέσεις στον κυβερνοχώρο. Μπορεί να είναι οποιοδήποτε περιστατικό που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, τροποποίηση, μη εξουσιοδοτημένη αποκάλυψη ή πρόσβαση σε δεδομένα προσωπικού χαρακτήρα. Όπως υποδηλώνει αυτός ο ορισμός, οι παραβιάσεις δεδομένων είναι μόνο λίγες φορές το αποτέλεσμα ενός εγκληματία χάκερ που εισβάλλει στα συστήματά σας. Είναι εξίσου πιθανό να συμβεί όταν ένας υπάλληλος στέλνει κατά λάθος προσωπικές πληροφορίες σε λάθος άτομο, χάσει έναν φορητό υπολογιστή που περιέχει προσωπικά δεδομένα ή αποτυγχάνει να προστατεύσει με κωδικό πρόσβασης μια ηλεκτρονική βάση δεδομένων.

4.8. Η σημασία της συγκατάθεσης

Όταν η επεξεργασία βασίζεται σε συγκατάθεση, ο υπεύθυνος επεξεργασίας είναι σε θέση να αποδείξει ότι το υποκείμενο των δεδομένων συγκατατέθηκε για την επεξεργασία των δεδομένων του προσωπικού χαρακτήρα.

Εάν η συγκατάθεση του υποκειμένου των δεδομένων παρέχεται στο πλαίσιο γραπτής δήλωσης η οποία αφορά και άλλα θέματα, το αίτημα για συγκατάθεση υποβάλλεται κατά τρόπο ώστε να είναι σαφώς διακριτό από τα άλλα θέματα, σε κατανοητή και εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή διατύπωση. Κάθε τμήμα της δήλωσης αυτής το οποίο συνιστά παράβαση του παρόντος κανονισμού δεν είναι δεσμευτικό.

Το υποκείμενο των δεδομένων έχει δικαίωμα να ανακαλέσει τη συγκατάθεσή του ανά πάσα στιγμή. Η ανάκληση της συγκατάθεσης δεν θίγει τη νομιμότητα της επεξεργασίας που βασίστηκε στη συγκατάθεση προ της ανάκλησής της. Πριν την παροχή της συγκατάθεσης, το υποκείμενο των δεδομένων ενημερώνεται σχετικά. Η ανάκληση της συγκατάθεσης είναι εξίσου εύκολη με την παροχή της.

Η συναίνεση, όπως εξετάστηκε παραπάνω, αποτελεί, σε πολλές περιπτώσεις, τη νομική βάση για τη νόμιμη επεξεργασία δεδομένων. Η συγκατάθεση πρέπει να είναι ελεύθερη, ενημερωμένη, συγκεκριμένη και σαφής. θα πρέπει να είναι μια σαφή καταφατική πράξη που υποδηλώνει την αποδοχή από το υποκείμενο των δεδομένων της προτεινόμενης επεξεργασίας των προσωπικών του δεδομένων, με τη μορφή γραπτής δήλωσης ή ηλεκτρονικής φόρμας ή προφορικής δήλωσης (π.χ. σημειώνοντας ένα πλαίσιο κατά την επίσκεψη σε ιστότοπο, επιλογή τεχνικής ρυθμίσεις για τις υπηρεσίες της κοινωνίας της πληροφορίας). Ειδικά όταν η επεξεργασία βασίζεται στη συγκατάθεση, ο υπεύθυνος επεξεργασίας πρέπει να μπορεί να αποδείξει ότι το υποκείμενο των δεδομένων έχει συναινέσει στην επεξεργασία των προσωπικών του δεδομένων. Ως εκ τούτου, μια δήλωση συναίνεσης που έχει εκ των προτέρων διατυπωθεί από τον υπεύθυνο επεξεργασίας θα πρέπει να παρέχεται σε κατανοητή και εύκολα προσβάσιμη μορφή, με σαφή και απλή γλώσσα και δεν πρέπει να περιέχει αθέμιτους όρους, διασφαλίζοντας ότι το υποκείμενο των δεδομένων γνωρίζει και ιδιαίτερα τον βαθμό στον οποίο δίνεται η συγκατάθεση. Επιπλέον, σε περίπτωση γραπτής δήλωσης που περιλαμβάνει και άλλα θέματα, το αίτημα συναίνεσης υποβάλλεται με τρόπο που να διακρίνεται σαφώς από τα άλλα θέματα».
Οποιοδήποτε εξάρτημα συμμορφώνεται με τους κανόνες GDPR δεν είναι δεσμευτικό.

Για να ενημερωθεί η συναίνεση, το υποκείμενο των δεδομένων θα πρέπει να γνωρίζει τουλάχιστον την ταυτότητα του υπεύθυνου επεξεργασίας και τους σκοπούς της επεξεργασίας. Ταυτόχρονα, η συγκατάθεση δεν θα πρέπει να θεωρείται ότι παρέχεται ελεύθερα, εκτός εάν το υποκείμενο των δεδομένων έχει πραγματική ή ελεύθερη επιλογή ή είναι σε θέση να αρνηθεί ή να ανακαλέσει τη συγκατάθεσή του χωρίς να ζημιωθεί. Το υποκείμενο των δεδομένων θα πρέπει να ενημερωθεί πριν δώσει τη συγκατάθεσή του ότι μπορεί να αποσυρθεί ανά πάσα στιγμή. η διαδικασία θα πρέπει να είναι τόσο εύκολη όσο η παροχή συγκατάθεσης. Επιπλέον, για να παρέχεται η συναίνεση ελεύθερα, απαιτεί να επιτρέπει τη χωριστή συναίνεση για διαφορετικές λειτουργίες επεξεργασίας προσωπικών δεδομένων. Επιπλέον, σε περίπτωση εκτέλεσης της σύμβασης ή παροχής υπηρεσιών, αυτά δεν πρέπει να υπόκεινται στη συγκατάθεση για επεξεργασία, εάν αυτό δεν αποτελεί προϋπόθεση για την εκτέλεση της σύμβασης ή της υπηρεσίας. Όταν υπάρχει σαφής ανισορροπία μεταξύ του υπευθύνου της επεξεργασίας και του υποκειμένου των δεδομένων, θα πρέπει να τεκμαίρεται ότι η συγκατάθεση δεν παρέχεται ελεύθερα και επομένως η συγκατάθεση πρέπει να αποτελεί τη νομική βάση για την επεξεργασία.

Σύμφωνα με τον GDPR, αναγνωρίζεται ότι τα παιδιά πρέπει να τυγχάνουν ειδικής προστασίας όσον αφορά τα προσωπικά τους δεδομένα, καθώς ενδέχεται να γνωρίζουν λιγότερο τους κινδύνους, τις συνέπειες και τις διασφαλίσεις που διακυβεύονται, καθώς και τα δικαιώματά τους όσον αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα. . Αυτό είναι ιδιαίτερα εμφανές όσον αφορά τον τομέα του μάρκετινγκ και των υπηρεσιών της κοινωνίας της πληροφορίας. Για το λόγο αυτό, ένα παιδί πρέπει να είναι τουλάχιστον 16 ετών για να θεωρήσει τη συγκατάθεσή του νόμιμη. Για παιδιά ηλικίας κάτω των 16 ετών, η συγκατάθεση παρέχεται ή εξουσιοδοτείται από τον κάτοχο της γονικής μέριμνας του παιδιού και ο υπεύθυνος επεξεργασίας θα πρέπει να καταβάλει εύλογες προσπάθειες για να το επαληθεύσει. Αντίθετα, στο πλαίσιο των προληπτικών ή συμβουλευτικών υπηρεσιών που προσφέρονται απευθείας σε ένα παιδί, δεν θα πρέπει να απαιτείται η συγκατάθεση του δικαιούχου της γονικής μέριμνας.

4.9. Επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα

Υπάρχει μια ειδική κατηγορία προσωπικών δεδομένων που είναι αφιερωμένη σε ευαίσθητες πληροφορίες. Αποτελείται από πληροφορίες που σχετίζονται με:

- Φυλετική ή εθνική καταγωγή.
- Πολιτικές απόψεις;
- Θρησκευτικές ή φιλοσοφικές πεποιθήσεις.
- Συνδικαλιστική ένταξη; • Γενετικά δεδομένα; και
- Βιομετρικά δεδομένα (όπου υποβάλλονται σε επεξεργασία για τη μοναδική ταυτοποίηση κάποιου).
- δεδομένα που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό

Η αρχή αυτή δεν εφαρμόζεται στις ακόλουθες περιπτώσεις:

α) το υποκείμενο των δεδομένων έχει παράσχει ρητή συγκατάθεση για την επεξεργασία αυτών των δεδομένων προσωπικού χαρακτήρα για έναν ή περισσότερους συγκεκριμένους σκοπούς,

β) η επεξεργασία είναι απαραίτητη για την εκτέλεση των υποχρεώσεων και την άσκηση συγκεκριμένων δικαιωμάτων του υπευθύνου επεξεργασίας ή του υποκειμένου των δεδομένων στον τομέα του εργατικού δικαίου και του δικαίου κοινωνικής ασφάλισης και κοινωνικής προστασίας,

γ) η επεξεργασία είναι απαραίτητη για την προστασία των ζωτικών συμφερόντων του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου, εάν το υποκείμενο των δεδομένων είναι σωματικά ή νομικά ανίκανο να συγκατατεθεί,

δ) η επεξεργασία διενεργείται, με κατάλληλες εγγυήσεις, στο πλαίσιο των νόμιμων δραστηριοτήτων ιδρύματος, οργάνωσης ή άλλου μη κερδοσκοπικού φορέα με πολιτικό, φιλοσοφικό, θρησκευτικό ή συνδικαλιστικό στόχο και υπό την προϋπόθεση ότι η επεξεργασία αφορά αποκλειστικά τα μέλη ή τα πρώην μέλη του φορέα ή πρόσωπα τα οποία έχουν τακτική επικοινωνία μαζί του,

ε) η επεξεργασία αφορά δεδομένα προσωπικού χαρακτήρα τα οποία έχουν προδήλως δημοσιοποιηθεί από το υποκείμενο των δεδομένων,

στ) η επεξεργασία είναι απαραίτητη για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων ή όταν τα δικαστήρια ενεργούν υπό τη δικαιοδοτική τους ιδιότητα,

ζ) η επεξεργασία είναι απαραίτητη για λόγους ουσιαστικού δημόσιου συμφέροντος, βάσει του δικαίου της Ένωσης ή κράτους μέλους, το οποίο είναι ανάλογο προς τον επιδιωκόμενο στόχο, σέβεται την ουσία του δικαιώματος στην προστασία των δεδομένων και προβλέπει κατάλληλα και συγκεκριμένα μέτρα για τη διασφάλιση των θεμελιωδών δικαιωμάτων και των συμφερόντων του υποκειμένου των δεδομένων,

η) η επεξεργασία είναι απαραίτητη για σκοπούς προληπτικής ή επαγγελματικής ιατρικής, εκτίμησης της ικανότητας προς εργασία του εργαζομένου, ιατρικής διάγνωσης, παροχής υγειονομικής ή κοινωνικής περίθαλψης ή θεραπείας ή διαχείρισης υγειονομικών και κοινωνικών συστημάτων και υπηρεσιών βάσει του ενωσιακού δικαίου ή του δικαίου κράτους μέλους ή δυνάμει σύμβασης με επαγγελματία του τομέα της υγείας,

θ) η επεξεργασία είναι απαραίτητη για λόγους δημόσιου συμφέροντος στον τομέα της δημόσιας υγείας, όπως η προστασία έναντι σοβαρών διασυνοριακών απειλών κατά της υγείας ή η διασφάλιση υψηλών προτύπων ποιότητας και ασφάλειας της υγειονομικής περίθαλψης και των φαρμάκων ή των ιατροτεχνολογικών προϊόντων

ι) η επεξεργασία είναι απαραίτητη για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς, οι οποίοι είναι ανάλογοι προς τον επιδιωκόμενο στόχο, σέβονται την ουσία του δικαιώματος στην προστασία των δεδομένων και προβλέπουν κατάλληλα και συγκεκριμένα μέτρα για τη διασφάλιση των θεμελιωδών δικαιωμάτων και των συμφερόντων του υποκειμένου των δεδομένων.

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα που αφορούν **ποινικές καταδίκες** και αδικήματα ή σχετικά μέτρα ασφάλειας διενεργείται μόνο υπό τον έλεγχο επίσημης αρχής ή εάν η επεξεργασία επιτρέπεται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους το οποίο προβλέπει επαρκείς εγγυήσεις για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων. Πλήρες ποινικό μητρώο τηρείται μόνο υπό τον έλεγχο επίσημης αρχής.

4.10. Ανάλυση ευθυνών στο πλαίσιο μιας GDPR-compliant τεχνολογικής λύσης

4.10.1. Ευθύνη του υπεύθυνου επεξεργασίας

Ο υπεύθυνος επεξεργασίας είναι υπεύθυνος για την εφαρμογή των κατάλληλων τεχνικών και οργανωτικών μέτρων για τη διασφάλιση και τη δυνατότητα να αποδείξει ότι η επεξεργασία πραγματοποιείται σύμφωνα με τον GDPR λαμβάνοντας υπόψη το πλαίσιο και τον σκοπό της επεξεργασίας καθώς και τον αντίκτυπο που μπορεί να έχει στα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Τα μέτρα αυτά μπορεί να περιλαμβάνουν πολιτικές προστασίας δεδομένων ή την

εφαρμογή εγκεκριμένων κωδίκων δεοντολογίας ή μηχανισμών πιστοποίησης. Όταν δύο ή περισσότεροι ελεγκτές ορίζουν μαζί τον σκοπό και τα μέσα της επεξεργασίας, είναι από κοινού ελεγκτές με συγκεκριμένες ευθύνες συμμόρφωσης με τον GDPR. Αυτή η ρύθμιση θα πρέπει να είναι διαθέσιμη και για το υποκείμενο των δεδομένων.

Όταν ο υπεύθυνος επεξεργασίας αναθέτει σε έναν εκτελούντα την επεξεργασία να εκτελέσει την επεξεργασία δεδομένων προσωπικού χαρακτήρα και να ενεργήσει για λογαριασμό του υπεύθυνου επεξεργασίας, ο τελευταίος πρέπει να χρησιμοποιεί μόνο εκτελούντες την επεξεργασία που παρέχουν επαρκείς εγγυήσεις για την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων σύμφωνα με τον GDPR και σε σχέση με το υποκείμενο των δεδομένων δικαιώματα.

Κάθε υπεύθυνος επεξεργασίας ή εκπρόσωπος υπεύθυνου επεξεργασίας στην ΕΕ, όσον αφορά επιχειρήσεις ή οργανισμούς που απασχολούν περισσότερα από 250 άτομα, είναι υπεύθυνος για την τήρηση αρχείου των εργασιών επεξεργασίας, γραπτώς, συμπεριλαμβανομένης της ηλεκτρονικής μορφής. Αυτό το αρχείο είναι διαθέσιμο κατόπιν αιτήματος της εποπτικής αρχής. Η υποχρέωση τήρησης αρχείου ισχύει για οργανισμούς με λιγότερους από 250 υπαλλήλους, όπου η επεξεργασία είναι πιθανό να οδηγήσει σε κίνδυνο για τα δικαιώματα του υποκειμένου των δεδομένων, η επεξεργασία δεν είναι περιστασιακή ή περιλαμβάνει προσωπικά δεδομένα που αποκαλύπτουν ευαίσθητες πληροφορίες για ένα άτομο ή σχετίζονται με ποινικές καταδίκες.

Ο υπεύθυνος επεξεργασίας αναμένεται να συνεργαστεί με την εποπτική αρχή κατόπιν αιτήματος. Ωστόσο, σε περίπτωση παραβίασης προσωπικών δεδομένων, ο υπεύθυνος επεξεργασίας πρέπει να ενημερώσει την εποπτική αρχή εντός 72 ωρών από τη στιγμή που έλαβε γνώση της παραβίασης, αναμένοντας παραβιάσεις που είναι απίθανο να οδηγήσουν σε κίνδυνο για τα δικαιώματα του υποκειμένου των δεδομένων. Εάν η κοινοποίηση λάβει χώρα μετά από 72 ώρες, οι λόγοι για αυτό πρέπει να γνωστοποιούνται.

Στην κοινοποίηση θα πρέπει να περιγράφεται «η φύση της παραβίασης δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων, όπου είναι δυνατόν, των κατηγοριών και του κατά προσέγγιση αριθμού των σχετικών υποκειμένων των δεδομένων και των σχετικών κατηγοριών και κατά προσέγγιση αριθμού αρχείων δεδομένων προσωπικού χαρακτήρα». θα πρέπει να κοινοποιούνται «το όνομα και τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων ή άλλου σημείου επαφής όπου μπορούν να ληφθούν περισσότερες πληροφορίες».·Θα πρέπει να περιγράφονται· «οι πιθανές συνέπειες της παραβίασης προσωπικών δεδομένων» καθώς και «τα μέτρα που λαμβάνονται ή προτείνονται να ληφθούν από τον υπεύθυνο επεξεργασίας για την αντιμετώπιση της παραβίασης προσωπικών δεδομένων, συμπεριλαμβανομένων, όπου ενδείκνυται, μέτρων για τον μετριασμό των πιθανών δυσμενών συνεπειών της. Ο υπεύθυνος επεξεργασίας είναι υπεύθυνος για την τεκμηρίωση τυχόν παραβιάσεων προσωπικών δεδομένων (γεγονότα που σχετίζονται με την παραβίαση, επιπτώσεις και διορθωτικά μέτρα που ελήφθησαν) προκειμένου η εποπτική αρχή να επαληθεύσει τη συμμόρφωση με τις διατάξεις του GDPR.

Ο υπεύθυνος επεξεργασίας είναι υπεύθυνος για την κοινοποίηση μιας παραβίασης προσωπικών δεδομένων στο υποκείμενο των δεδομένων, χρησιμοποιώντας μια σαφή και απλή γλώσσα, εάν είναι πιθανό να επηρεάσει αρνητικά τα δικαιώματα του φυσικού προσώπου. Εάν έχουν ληφθεί μέτρα, όπως κρυπτογράφηση ή άλλα, που είτε καθιστούν τα προσωπικά δεδομένα κατανοητά είτε ο κίνδυνος δεν υφίσταται πλέον, ο υπεύθυνος επεξεργασίας δεν χρειάζεται να ενημερώσει το υποκείμενο των δεδομένων. Σε περίπτωση που απαιτεί δυσανάλογη προσπάθεια προσέγγισης του υποκειμένου/των δεδομένων που επηρεάζεται, τότε θα πρέπει να χρησιμοποιείται δημόσια επικοινωνία ή παρόμοιο μέτρο.

Ο υπεύθυνος επεξεργασίας είναι υπεύθυνος για οποιαδήποτε ζημία προκληθεί από μια επεξεργασία που παραβίαζε τον GDPR, εκτός εάν ο υπεύθυνος επεξεργασίας αποδείξει ότι δεν είναι υπεύθυνος για την αιτία της ζημίας.

4.10.2. Ευθύνη του εκτελούντα την επεξεργασία

Ο εκτελών την επεξεργασία πρέπει να δεσμεύεται από σύμβαση ή άλλη νομική πράξη σύμφωνα με το δίκαιο της ΕΕ ή το εθνικό δίκαιο όσον αφορά τον υπεύθυνο επεξεργασίας και να ενεργεί σύμφωνα με τις πράξεις επεξεργασίας. Σε αυτό καθορίζονται «το αντικείμενο και η διάρκεια της επεξεργασίας, η φύση και ο σκοπός της επεξεργασίας, το είδος των προσωπικών δεδομένων και οι κατηγορίες των υποκειμένων των δεδομένων και η υποχρέωση και τα δικαιώματα του υπευθύνου επεξεργασίας». Σύμφωνα με το άρθρο 28 παράγραφος 3 του ΓΚΠΔ, προβλέπονται ειδικές ρήτρες που αποτελούν μέρος της σύμβασης ή της νομικής πράξης, όπως ότι

(α) η επεξεργασία πραγματοποιείται μόνο με τεκμηριωμένες οδηγίες του υπεύθυνου επεξεργασίας, εκτός εάν ο εκτελών την επεξεργασία υποχρεούται να ενεργήσει έτσι από την ΕΕ ή εθνικό δίκαιο·

(β) ο εκτελών την επεξεργασία διασφαλίζει ότι τα εξουσιοδοτημένα πρόσωπα για την επεξεργασία δεδομένων προσωπικού χαρακτήρα δεσμεύονται από την υποχρέωση εμπιστευτικότητας·

(γ) ο εκτελών την επεξεργασία λαμβάνει όλα τα απαραίτητα τεχνικά και οργανωτικά μέτρα για να εξασφαλίσει την προστασία των προσωπικών δεδομένων του υποκειμένου των δεδομένων·

(δ) ο εκτελών την επεξεργασία δεν μπορεί να δεσμεύσει άλλους εκτελούντες την επεξεργασία εκτός εάν υπάρχει προηγούμενη γραπτή εξουσιοδότηση του υπεύθυνου επεξεργασίας - σε περίπτωση που η εξουσιοδότηση είναι γενική, ο εκτελών την επεξεργασία πρέπει να ενημερώσει τον υπεύθυνο επεξεργασίας για τυχόν επιδιωκόμενες αλλαγές σχετικά με τους εμπλεκόμενους επεξεργαστές.

(δ) ο εκτελών την επεξεργασία βοηθά τον υπεύθυνο επεξεργασίας να ανταποκρίνεται σε αιτήματα υποκειμένων των δεδομένων που ασκούν τα δικαιώματά τους βάσει του GDPR·

(ε) ο εκτελών την επεξεργασία, εάν ζητηθεί από τον υπεύθυνο επεξεργασίας, θα διαγράψει ή θα επιστρέψει όλα τα προσωπικά δεδομένα στον υπεύθυνο επεξεργασίας έως το τέλος της παροχής των υπηρεσιών και θα διαγράψει αντίγραφα, εκτός εάν απαιτείται διαφορετικά από το δίκαιο της ΕΕ ή την εθνική νομοθεσία·

(στ) ο εκτελών την επεξεργασία παρέχει τις απαραίτητες πληροφορίες στον υπεύθυνο επεξεργασίας ώστε ο τελευταίος να διαπιστώσει τη συμμόρφωση του πρώτου με την υποχρέωση που ορίζεται στο άρθρο 28 του ΓΚΠΔ και να συμβάλει σε ελέγχους και επιθεωρήσεις που διενεργούνται από τον υπεύθυνο επεξεργασίας. Εάν, κατά τη γνώμη του εκτελούντος την επεξεργασία, η εντολή του υπεύθυνου επεξεργασίας παραβιάζει τον GDPR, ο εκτελών την επεξεργασία πρέπει να ενημερώσει αμέσως τον υπεύθυνο επεξεργασίας. Τυπικές συμβατικές ρήτρες για τα προαναφερθέντα θέματα μπορούν να θεσπιστούν από την Ευρωπαϊκή Επιτροπή ή την εποπτική αρχή. Σε κάθε περίπτωση, η σύμβαση ή άλλη νομική πράξη πρέπει να είναι γραπτή, συμπεριλαμβανομένης της ηλεκτρονικής μορφής.

Εάν ο εκτελών την επεξεργασία δεσμεύσει άλλον εκτελούντα την επεξεργασία για να εκτελέσει συγκεκριμένες δραστηριότητες επεξεργασίας για λογαριασμό του υπεύθυνου επεξεργασίας, οι ίδιες υποχρεώσεις προστασίας δεδομένων πρέπει να προβλέπονται σε παρόμοια σύμβαση ή άλλη νομική πράξη. Επαρκείς εγγυήσεις για την εφαρμογή των κατάλληλων τεχνικών και οργανωτικών μέτρων κατά τρόπο που η επεξεργασία να πληροί τις απαιτήσεις του GDPR μπορεί να αποδεικνύονται από τη συμμόρφωση του εκτελούντος την επεξεργασία σε έναν εγκεκριμένο κώδικα δεοντολογίας ή μηχανισμό πιστοποίησης.

Κάθε εκτελών την επεξεργασία ή ο εκπρόσωπος ενός εκτελούντος την επεξεργασία στην ΕΕ είναι υπεύθυνος για την τήρηση αρχείου όλων των κατηγοριών εργασιών επεξεργασίας που εκτελούνται για λογαριασμό του υπεύθυνου επεξεργασίας, γραπτώς, συμπεριλαμβανομένης της ηλεκτρονικής μορφής. Αυτό το αρχείο είναι διαθέσιμο στην εποπτική αρχή κατόπιν αιτήματος. Ισχύουν τα ίδια κριτήρια για την υποχρέωση τήρησης αρχείου σε σχέση με το μέγεθος μιας επιχείρησης ή οργανισμού, όπως και για τον υπεύθυνο επεξεργασίας. Σε κάθε περίπτωση, ο εκτελών την επεξεργασία αναμένεται να συνεργαστεί με την εποπτική αρχή, κατόπιν αιτήματος.

Ο εκτελών την επεξεργασία μόλις αντιληφθεί παραβίαση προσωπικών δεδομένων πρέπει να ενημερώσει τον υπεύθυνο επεξεργασίας.

Ο εκτελών την επεξεργασία είναι υπεύθυνος για ζημίες που προκύπτουν από μια επεξεργασία μόνο όταν έχει ενεργήσει αντίθετα ή εκτός των υποχρεώσεων που απορρέουν από τον GDPR ή τις νόμιμες οδηγίες του υπεύθυνου επεξεργασίας. Ο εκτελών την επεξεργασία απαλλάσσεται από την ευθύνη, εάν αποδείξει ότι δεν ευθύνεται για την αιτία της ζημίας.

4.10.3. Ο ρόλος του υπεύθυνου προστασίας δεδομένων

Ο υπεύθυνος προστασίας δεδομένων (data protection officer -- DPO) πρέπει να ορίζεται από τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία, εάν: (α) η επεξεργασία πραγματοποιείται από δημόσια αρχή ή φορέα, (β) στο πλαίσιο της επεξεργασίας, τακτικής και συστηματικής παρακολούθησης των υποκειμένων των δεδομένων λαμβάνει χώρα μεγάλη κλίμακα, (γ) λαμβάνει χώρα επεξεργασία προσωπικών δεδομένων σε μεγάλη κλίμακα που αποκαλύπτουν ευαίσθητες πληροφορίες για άτομα ή ποινικές καταδίκες. Εκτός από τις προαναφερθείσες περιπτώσεις, ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία θα πρέπει να ορίσει έναν υπεύθυνο προστασίας δεδομένων, όπου απαιτείται από τη νομοθεσία της ΕΕ ή την εθνική νομοθεσία. Ένας υπεύθυνος προστασίας δεδομένων μπορεί να εξυπηρετεί περισσότερους υπευθύνους επεξεργασίας ή εκτελούντες την επεξεργασία. Πρέπει να έχει εξειδικευμένες γνώσεις σχετικά με τη νομοθεσία και τις πρακτικές προστασίας δεδομένων και την ικανότητα να εκτελεί καθήκοντα που προβλέπονται στο πλαίσιο του GDPR. Μπορεί να είναι μέλος του προσωπικού του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία ή να έχει προσληφθεί με σύμβαση παροχής υπηρεσιών. Τα στοιχεία επικοινωνίας του
ΥΠΔ δημοσιεύονται και κοινοποιούνται επίσης στην εποπτική αρχή.

Ο ΥΠΔ εμπλέκεται σε όλα τα ζητήματα που αφορούν την προστασία των προσωπικών δεδομένων και αναφέρεται απευθείας στο ανώτατο διοικητικό επίπεδο του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία. Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία υποστηρίζουν τον ΥΠΔ στην εκτέλεση των καθηκόντων του βάσει του GDPR (πόροι, πρόσβαση σε δραστηριότητες επεξεργασίας δεδομένων προσωπικού χαρακτήρα, συνεχής εκπαίδευση) και δεν τον/την δίνουν οδηγίες. Ωστόσο, ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία διασφαλίζει ότι δεν υπάρχει σύγκρουση συμφερόντων, εάν ο ΥΠΔ απασχολείται σε πολλές θέσεις. Σε κάθε περίπτωση, ο ΥΠΔ πρέπει να δεσμεύεται από το απόρρητο ή το απόρρητο όσον αφορά τα καθήκοντά του/της. Τέλος, ο ΥΠΔ θα πρέπει να είναι διαθέσιμος στα υποκείμενα των δεδομένων για να επικοινωνήσουν μαζί του σχετικά με τα προσωπικά τους δεδομένα.

Σύμφωνα με το άρθρο 39 παράγραφος 1 του ΓΚΠΔ στον ΥΠΔ ανατίθενται συγκεκριμένα καθήκοντα, και συγκεκριμένα

(α) «να ενημερώνει και να συμβουλεύει τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία και τους υπαλλήλους που διεκπεραιώνουν τις υποχρεώσεις τους σύμφωνα με» τον ΓΚΠΔ και προς άλλες ΕΕ ή εθνικές διατάξεις προστασίας δεδομένων·

(β) «να παρακολουθεί τη συμμόρφωση με» τον GDPR, με άλλες κοινοτικές ή εθνικές «διατάξεις προστασίας δεδομένων» και με τις πολιτικές του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία σε σχέση με την προστασία των προσωπικών δεδομένων, συμπεριλαμβανομένης της ανάθεσης ευθυνών, της ευαισθητοποίησης και της εκπαίδευσης του προσωπικού που συμμετέχει στις εργασίες επεξεργασίας και στους σχετικούς ελέγχους».

(γ) «να παρέχει συμβουλές όπου ζητείται σχετικά με την εκτίμηση επιπτώσεων στην προστασία δεδομένων και να παρακολουθεί την απόδοσή της σύμφωνα με το άρθρο 35» του GDPR·

(δ) να συνεργάζεται με την εποπτική αρχή·

(ε) να ενεργεί ως το σημείο επαφής της εποπτικής αρχής σε θέματα που σχετίζονται με την επεξεργασία, συμπεριλαμβανομένης της προηγούμενης διαβούλευσης που αναφέρεται στο άρθρο 36» του ΓΚΠΔ, «και να διαβουλεύεται, όπου χρειάζεται, για οποιοδήποτε άλλο θέμα».

Κατά την εκτέλεση των καθηκόντων του, ο ΥΠΔ πρέπει να λαμβάνει υπόψη τους κινδύνους που απορρέουν από τις δραστηριότητες επεξεργασίας, συμπεριλαμβανομένης της φύσης, του πεδίου εφαρμογής, του πλαισίου και των σκοπών της επεξεργασίας.

4.11. Εγγυήσεις προστασίας δεδομένων

4.11.1. Πληροφορίες που πρέπει να παρέχονται, όταν έχουν συλλεχθεί προσωπικά δεδομένα από το υποκείμενο των δεδομένων

Μόλις ληφθούν προσωπικά δεδομένα από το υποκείμενο των δεδομένων και εφόσον το υποκείμενο των δεδομένων δεν γνωρίζει ήδη, **ο υπεύθυνος επεξεργασίας πρέπει να παράσχει ορισμένες πληροφορίες**, όπως

(α) την ταυτότητα και τα στοιχεία επικοινωνίας του υπευθύνου επεξεργασίας ή του εκπροσώπου του υπευθύνου επεξεργασίας,

(β) τα στοιχεία επικοινωνίας του υπεύθυνου προστασίας δεδομένων, κατά περίπτωση,

(γ) ο σκοπός της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και η νομική βάση για αυτήν,

(δ) εάν η επεξεργασία βασίζεται στο έννομο συμφέρον του υπεύθυνου επεξεργασίας, τότε αυτά θα πρέπει γνωστοποιούνται

(ε) οι αποδέκτες των δεδομένων προσωπικού χαρακτήρα, εάν υπάρχουν (στ) όπου ισχύει, η πρόθεση μεταφοράς δεδομένων.

Εκτός από τα προαναφερθέντα, ο υπεύθυνος επεξεργασίας παρέχει **περαιτέρω πληροφορίες** σχετικά με

(α) τη χρονική περίοδο αποθήκευσης δεδομένων,

(β) την ύπαρξη του δικαιώματος αίτησης πρόσβασης και διόρθωσης ή διαγραφής δεδομένων προσωπικού χαρακτήρα ή περιορισμού της επεξεργασίας,

(γ) όταν η επεξεργασία βασίζεται στη συγκατάθεση του υποκειμένου των δεδομένων, το δικαίωμα ανάκλησης της συγκατάθεσης ανά πάσα στιγμή, χωρίς να επηρεάζεται η νομιμότητα της επεξεργασίας πριν από την ανάκλησή της,

(δ) το δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή,

(ε) εάν η παροχή προσωπικών δεδομένων αποτελεί νομική ή συμβατική απαίτηση ή απαίτηση απαραίτητη για τη σύναψη σύμβασης, καθώς και εάν το υποκείμενο των δεδομένων υποχρεούται να παράσχει τα προσωπικά δεδομένα και οι πιθανές συνέπειες της μη παροχής τους,
(στ) η ύπαρξη αυτοματοποιημένης λήψης αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ, η λογική που εμπλέκεται και η σημασία ή η πιθανή συνέπεια αιτίες αυτής της επεξεργασίας για το υποκείμενο των δεδομένων.

4.11.2. Πληροφορίες που πρέπει να παρέχονται, όταν δεν έχουν συλλεχθεί προσωπικά δεδομένα από το υποκείμενο των δεδομένων

Σε περίπτωση που τα προσωπικά δεδομένα δεν έχουν ληφθεί από το υποκείμενο των δεδομένων και το τελευταίο δεν το γνωρίζει ήδη, ο υπεύθυνος επεξεργασίας έχει την ίδια υποχρέωση να ενημερώσει το υποκείμενο των δεδομένων εντός εύλογου χρονικού διαστήματος από τη λήψη των προσωπικών δεδομένων, αλλά τουλάχιστον εντός ενός μήνα ή εάν ισχύει στην πρώτη επικοινωνία με το υποκείμενο των δεδομένων ή εάν ισχύει κατά την πρώτη αποκάλυψη των δεδομένων σε άλλον παραλήπτη. Εκτός από τα προαναφερθέντα, ο υπεύθυνος επεξεργασίας πρέπει να ενημερώσει περαιτέρω το υποκείμενο των δεδομένων σχετικά με τις σχετικές κατηγορίες προσωπικών δεδομένων και τις πηγές από τις οποίες προέρχονται τα δεδομένα και εάν αυτές οι πηγές πρόσβασης στο κοινό. Οι πληροφορίες πρέπει να παρέχονται δωρεάν. Δεν αποτελεί υποχρέωση του υπεύθυνου επεξεργασίας να ενημερώσει το υποκείμενο των δεδομένων, εάν αυτό αποδειχθεί αδύνατο ή συνεπάγεται δυσανάλογη προσπάθεια ή ενδέχεται να μην εξυπηρετεί τους στόχους της επεξεργασίας. Η δημοσιοποίηση των πληροφοριών θα μπορούσε να εξισορροπήσει τα συμφέροντα και των δύο πλευρών. Επιπλέον, όταν η απόκτηση ή η αποκάλυψη παρέχεται απευθείας από το δίκαιο της ΕΕ ή το εθνικό δίκαιο, λαμβάνοντας υπόψη τις απαραίτητες εγγυήσεις προστασίας δικαιωμάτων ή όταν τα δεδομένα πρέπει να παραμένουν εμπιστευτικά (νομική υποχρέωση απορρήτου), ο υπεύθυνος επεξεργασίας δεν παρέχει καμία πληροφορία στο υποκείμενο των δεδομένων.

4.11.3. Προστασία δεδομένων από σχεδιασμό και από προεπιλογή

Με το σχεδιασμό της επεξεργασίας και της εφαρμογής του, ο υπεύθυνος επεξεργασίας πρέπει να εφαρμόζει τεχνικά και οργανωτικά μέτρα για την αποτελεσματική διασφάλιση των αρχών προστασίας δεδομένων. Επιπλέον, εξ ορισμού, η ποσότητα των συλλεγόμενων προσωπικών δεδομένων, η έκταση της επεξεργασίας τους, η περίοδος αποθήκευσης και η προσβασιμότητά τους πρέπει να ρυθμίζονται κατά τρόπο ώστε να διασφαλίζονται όλες οι αρχές.

4.11.4. Ασφάλεια επεξεργασίας

Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία πρέπει να λάβουν όλα τα απαραίτητα τεχνικά και οργανωτικά μέτρα για να διασφαλίσουν την προστασία των δεδομένων και να απαγορεύσουν τις παραβιάσεις προσωπικών δεδομένων

ή οποιουσδήποτε άλλους πιθανούς κινδύνους για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Η ψευδωνυμοποίηση και η κρυπτογράφηση εισάγονται ως μέτρα που θα μπορούσαν να εφαρμοστούν για τη μείωση αυτών των κινδύνων. Σε περίπτωση ψευδωνυμοποίησης, ορίζεται ότι οι πρόσθετες πληροφορίες που θα μπορούσαν να καταστήσουν ταυτοποιήσιμο ένα φυσικό πρόσωπο θα πρέπει να τηρούνται χωριστά. Επιπλέον, για να εξασφαλιστεί ένα επίπεδο ασφάλειας έναντι τέτοιων κινδύνων, μέτρα που διασφαλίζουν τη συνεχή εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα και ανθεκτικότητα των συστημάτων και υπηρεσιών επεξεργασίας ή που αποκαθιστούν τη διαθεσιμότητα και την πρόσβαση σε προσωπικά δεδομένα εγκαίρως σε περίπτωση φυσικού τεχνικό περιστατικό. Σε αυτό, προβλέπεται η καθιέρωση διαδικασίας τακτικού ελέγχου, αξιολόγησης και αξιολόγησης της αποτελεσματικότητας των μέτρων ασφαλείας. Πρόσθετες διασφαλίσεις μπορεί να είναι η τήρηση ενός εγκεκριμένου κώδικα δεοντολογίας ή ενός εγκεκριμένου μηχανισμού πιστοποίησης. Σε κάθε περίπτωση, κατά την αξιολόγηση του επιπέδου ασφάλειας, οι κίνδυνοι που πρέπει να λαμβάνονται υπόψη θα πρέπει να είναι αυτοί που προέρχονται από «τυχαία ή παράνομη καταστροφή, απώλεια, τροποποίηση, μη εξουσιοδοτημένη αποκάλυψη ή πρόσβαση σε προσωπικά δεδομένα που μεταδίδονται, αποθηκεύονται ή υποβάλλονται με άλλο τρόπο σε επεξεργασία».

4.11.5. Κώδικες δεοντολογίας

Ενθαρρύνεται να συνταχθούν κώδικες δεοντολογίας για να συμβάλουν στην ορθή εφαρμογή του GDPR από τα κράτη μέλη, τις εποπτικές αρχές, το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων και την Ευρωπαϊκή Επιτροπή. «Οι ενώσεις και άλλοι φορείς που εκπροσωπούν κατηγορίες υπευθύνων επεξεργασίας ή εκτελούντες την επεξεργασία μπορούν να καταρτίσουν κώδικες συμπεριφοράς ή να τροποποιήσουν ή να επεκτείνουν αυτούς τους κώδικες» για να προσδιορίσουν την εφαρμογή του GDPR, όσον αφορά τα ιδιαίτερα χαρακτηριστικά της διαδικασίας επεξεργασίας και τις αρχές για την προστασία και την επεξεργασία δεδομένων (π.χ. δίκαιη και διαφανής επεξεργασία, έννομο συμφέρον του υπευθύνου επεξεργασίας, συλλογή προσωπικών δεδομένων, ψευδωνυμοποίηση, παροχή πληροφοριών στα υποκείμενα των δεδομένων).

4.11.6. Επεξεργασία που δεν απαιτεί ταυτοποίηση

Σε περίπτωση που ο υπεύθυνος επεξεργασίας δεν είναι σε θέση να προσδιορίσει ένα υποκείμενο δεδομένων από τα προσωπικά δεδομένα που υποβλήθηκαν σε επεξεργασία, τότε ο υπεύθυνος επεξεργασίας δεν θα πρέπει να υποχρεούται να λάβει πρόσθετες πληροφορίες για την ταυτοποίηση του υποκειμένου των δεδομένων, εκτός εάν αυτό είναι προσφέρεται από το υποκείμενο των δεδομένων προκειμένου να βοηθήσει το τελευταίο να ασκήσει τα δικαιώματά του. Σε μια τέτοια περίπτωση, ένας μηχανισμός ελέγχου ταυτότητας θα μπορούσε να εφαρμοστεί ως ψηφιακή ταυτοποίηση του υποκειμένου των δεδομένων (π.χ. σύνδεση στην ηλεκτρονική υπηρεσία).

4.11.7. Εκτίμηση επιπτώσεων στην προστασία δεδομένων και προηγούμενη διαβούλευση

Όταν υπάρχει η πιθανότητα ότι ένας τύπος επεξεργασίας, ιδίως με τη χρήση νέων τεχνολογιών, θα μπορούσε να οδηγήσει σε υψηλό κίνδυνο για τα δικαιώματα των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας θα πρέπει να διενεργεί εκ των προτέρων εκτίμηση των επιπτώσεων των σκοπούμενων εργασιών επεξεργασίας στην προστασία προσωπικών δεδομένων. Αυτό θα απαιτηθεί ιδιαίτερα σε περίπτωση

(α) συστηματικής και εκτενούς αξιολόγησης των προσωπικών πτυχών των φυσικών προσώπων, με βάση την αυτοματοποιημένη επεξεργασία, συμπεριλαμβανομένης της κατάρτισης προφίλ, και η οποία περαιτέρω γίνεται λόγος για αποφάσεις που παράγουν έννομα αποτελέσματα για το φυσικό πρόσωπο ή το επηρεάζουν σημαντικά/ της,

(β) επεξεργασία σε μεγάλη κλίμακα ειδικών κατηγοριών δεδομένων που αποκαλύπτουν ευαίσθητες πληροφορίες για ένα φυσικό πρόσωπο ή προσωπικών δεδομένων που σχετίζονται με ποινικές καταδίκες και αδικήματα·

(γ) συστηματική παρακολούθηση μιας δημόσιας προσβάσιμης περιοχής σε μεγάλη κλίμακα. Παρόμοιες εργασίες επεξεργασίας που παρουσιάζουν τον ίδιο υψηλό κίνδυνο θα μπορούσαν να αντιμετωπιστούν με μία ενιαία αξιολόγηση. Τέτοιες περιπτώσεις επεξεργασίας θα πρέπει να αναφέρονται από την εποπτική αρχή, καθώς και οι περιπτώσεις όπου δεν απαιτείται εκτίμηση επιπτώσεων. Όπου η επεξεργασία βασίζεται στη νομοθεσία της ΕΕ ή των κρατών μελών βάσει ειδικών ρητρών στις οποίες υπόκειται ο υπεύθυνος επεξεργασίας, έχει ήδη πραγματοποιηθεί εκτίμηση επιπτώσεων στην προστασία των δεδομένων στο πλαίσιο της υιοθέτησης αυτής της νομικής βάσης.

Σύμφωνα με το άρθρο 35 παρ. 7 του ΓΚΠΔ, προβλέπεται το **ελάχιστο περιεχόμενο αξιολόγησης**. Κατά συνέπεια, η αξιολόγηση πρέπει να περιέχει τουλάχιστον:

(α) συστηματική περιγραφή των αναμενόμενων εργασιών επεξεργασίας και των σκοπών της, συμπεριλαμβανομένου, κατά περίπτωση, του έννομου συμφέροντος που επιδιώκει ο υπεύθυνος επεξεργασίας,

(β) αξιολόγηση της αναγκαιότητας και της αναλογικότητας των επεξεργασία σε σχέση με τους σκοπούς,

(γ) εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων και

(δ) τα μέτρα που προβλέπονται για την αντιμετώπιση των κινδύνων, συμπεριλαμβανομένων διασφαλίσεων, μέτρων ασφαλείας και μηχανισμών για τη διασφάλιση της προστασίας των δεδομένων προσωπικού χαρακτήρα και να αποδείξει τη συμμόρφωση με τον GDPR λαμβάνοντας υπόψη τα δικαιώματα και τα έννομα συμφέροντα των υποκειμένων των δεδομένων και άλλων ενδιαφερομένων προσώπων. Για την αξιολόγηση θα ληφθεί υπόψη η συμμόρφωση με τους εγκεκριμένους κώδικες δεοντολογίας.

Όταν μια εκτίμηση επιπτώσεων στην προστασία δεδομένων δείχνει ότι η επεξεργασία θα είχε ως αποτέλεσμα υψηλό κίνδυνο, εάν δεν ληφθούν μέτρα από τον υπεύθυνο επεξεργασίας για τον μετριασμό του κινδύνου, ο υπεύθυνος επεξεργασίας πρέπει να συμβουλευτεί την εποπτική αρχή πριν από την επεξεργασία.

4.12. Δικαιώματα χρηστών πάνω στα προσωπικά τους δεδομένα

Ο GDPR προβλέπει τα δικαιώματα του υποκειμένου των δεδομένων σε σχέση με την επεξεργασία των προσωπικών του δεδομένων. Ο υπεύθυνος επεξεργασίας θα πρέπει να διευκολύνει την άσκηση των δικαιωμάτων του υποκειμένου των δεδομένων παρέχοντας τρόπους, όπως εύκολα προσβάσιμους και δωρεάν μηχανισμούς για την υποβολή του αιτήματος.

4.12.1. Δικαίωμα πρόσβασης από το υποκείμενο των δεδομένων

Το υποκείμενο των δεδομένων διατηρεί το δικαίωμα να λάβει επιβεβαίωση σχετικά με το εάν τα προσωπικά του δεδομένα υποβάλλονται σε επεξεργασία ή όχι και, όπου συμβαίνει αυτό, για πληροφορίες όπως ο σκοπός της επεξεργασίας, οι εν λόγω κατηγορίες δεδομένων προσωπικού χαρακτήρα, οι αποδέκτες ότι δεδομένα έχουν αποκαλυφθεί ή πρόκειται να αποκαλυφθούν, την ύπαρξη του δικαιώματος διόρθωσης ή διαγραφής δεδομένων προσωπικού χαρακτήρα ή περιορισμού της επεξεργασίας ή του δικαιώματος αντίρρησης στην επεξεργασία, το δικαίωμα υποβολής καταγγελίας· τις πηγές από τις οποίες ο υπεύθυνος επεξεργασίας συνέλεξε τα δεδομένα, την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων. Επιπλέον, ο υπεύθυνος επεξεργασίας παρέχει αντίγραφο των υπό επεξεργασία δεδομένων προσωπικού χαρακτήρα. Είναι σημαντικό ότι ο υπεύθυνος επεξεργασίας θα πρέπει να επαληθεύει την ταυτότητα ενός υποκειμένου των δεδομένων πριν δώσει πρόσβαση.

4.12.2. Δικαίωμα διόρθωσης

Το υποκείμενο των δεδομένων έχει το δικαίωμα να απαιτήσει από τον υπεύθυνο επεξεργασίας να διορθώσει ανακριβή προσωπικά δεδομένα. Εάν τα δεδομένα είναι ελλιπή, το υποκείμενο των δεδομένων έχει το δικαίωμα να τα συμπληρώσει.

4.12.3. Δικαίωμα στη διαγραφή («δικαίωμα στη λήθη»)

Υπό ορισμένες προϋποθέσεις, το υποκείμενο των δεδομένων έχει το δικαίωμα να απαιτήσει από τον υπεύθυνο επεξεργασίας τη διαγραφή των προσωπικών δεδομένων χωρίς αδικαιολόγητη καθυστέρηση. Αυτές οι **προϋποθέσεις** περιορίζονται στα ακόλουθα:

(α) η αρχή της αναγκαιότητας δεν πληρούται πλέον σε σχέση με τους σκοπούς για τους οποίους τα δεδομένα προσωπικού χαρακτήρα συλλέχθηκαν ή υποβλήθηκαν αρχικά σε επεξεργασία·

(β) όταν η συγκατάθεση ήταν η μόνη νομική βάση για την επεξεργασία δεδομένων προσωπικού χαρακτήρα και το υποκείμενο των δεδομένων αποσύρει τη συγκατάθεσή του·

(γ) το υποκείμενο των δεδομένων αντιτίθεται στην επεξεργασία στο πλαίσιο της εκτέλεσης καθηκόντων του υπεύθυνου επεξεργασίας προς το δημόσιο συμφέρον ή για τα έννομα συμφέροντα του υπευθύνου επεξεργασίας ·

(δ) τα προσωπικά δεδομένα έχουν υποστεί παράνομη επεξεργασία·

(ε) τα δεδομένα προσωπικού χαρακτήρα πρέπει να διαγραφούν για συμμόρφωση με νομική υποχρέωση της ενωσιακής ή εθνικής νομοθεσίας στην οποία υπόκειται ο υπεύθυνος επεξεργασίας·

(στ) τα προσωπικά δεδομένα έχουν συλλεχθεί από άτομο ηλικίας κάτω των 18 ετών στο πλαίσιο των υπηρεσιών της κοινωνίας της πληροφορίας.

Σε περίπτωση προσωπικών δεδομένων που δημοσιοποιούνται από τον υπεύθυνο επεξεργασίας και ο τελευταίος υποχρεούται να διαγράψει τα προσωπικά δεδομένα, ο υπεύθυνος επεξεργασίας πρέπει να λάβει όλα τα εύλογα μέτρα για να ενημερώσει τους υπεύθυνους επεξεργασίας που επεξεργάζονται και αυτά τα προσωπικά δεδομένα, ότι το υποκείμενο των δεδομένων έχει ζητήσει τη διαγραφή «οποιωνδήποτε συνδέσμων προς ή αντιγραφή ή αναπαραγωγή αυτών των προσωπικών δεδομένων».

Ωστόσο, το δικαίωμα διαγραφής εξισορροπείται με άλλα δικαιώματα, νομικές υποχρεώσεις ή λόγους και, στον βαθμό που η επεξεργασία είναι απαραίτητη για τον σεβασμό αυτών, μπορεί να εφαρμοστεί μόνο εν μέρει. Τέτοιες περιπτώσεις είναι το δικαίωμα στην ελευθερία έκφρασης και πληροφόρησης, η νομική υποχρέωση συμμόρφωσης με το ενωσιακό ή εθνικό δίκαιο ή η άσκηση δημόσιας εξουσίας για την εκτέλεση καθήκοντος προς το δημόσιο συμφέρον, όπου σε όλες τις προηγούμενες περιπτώσεις απαιτείται επεξεργασία, το δημόσιο συμφέρον για λόγους που σχετίζονται με τη δημόσια υγεία, σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, «σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς.

4.12.4. Δικαίωμα περιορισμού επεξεργασίας

Όσον αφορά την προσωρινή προστασία, το υποκείμενο των δεδομένων έχει το δικαίωμα να λάβει από τον υπεύθυνο επεξεργασίας περιορισμό της επεξεργασίας υπό συγκεκριμένες συνθήκες, οι οποίες είναι: όταν η ακρίβεια των προσωπικών δεδομένων αμφισβητείται από το υποκείμενο των δεδομένων (για τον απαραίτητο χρόνο στον υπεύθυνο επεξεργασίας για την επαλήθευση της ακρίβειας) η επεξεργασία είναι παράνομη και το υποκείμενο των δεδομένων ζητά περιορισμό της επεξεργασίας και όχι διαγραφή των προσωπικών δεδομένων· τα προσωπικά δεδομένα δεν είναι πλέον απαραίτητα για τους σκοπούς της επεξεργασίας, αλλά το υποκείμενο των δεδομένων τα χρειάζεται για να θεμελιώσει, να ασκήσει ή να υπερασπιστεί νομικές αξιώσεις· το υποκείμενο των δεδομένων έχει αντιταχθεί στα έννομα συμφέροντα του υπεύθυνου επεξεργασίας και οι αξιώσεις εξετάζονται. Σε αυτές τις περιπτώσεις, τα προσωπικά δεδομένα δεν μπορούν να υποβληθούν σε επεξεργασία εκτός εάν με τη συγκατάθεση του υποκειμένου των δεδομένων ή με σκοπό τη θεμελίωση,

άσκηση ή υπεράσπιση νομικών αξιώσεων ή για την προστασία των δικαιωμάτων άλλου φυσικού ή νομικού προσώπου για λόγους σημαντικού δημόσιου συμφέροντος της ΕΕ ή ένα κράτος μέλος. Εάν πρόκειται να αρθεί ο περιορισμός, ο υπεύθυνος επεξεργασίας πρέπει να ενημερώσει εκ των προτέρων το υποκείμενο των δεδομένων.

4.12.5. Δικαίωμα φορητότητας δεδομένων

Όταν η επεξεργασία των προσωπικών δεδομένων βασίζεται στη συγκατάθεση του υποκειμένου των δεδομένων και πραγματοποιείται με αυτοματοποιημένα μέσα, το υποκείμενο των δεδομένων έχει το δικαίωμα να λαμβάνει τα προσωπικά του δεδομένα από τον υπεύθυνο επεξεργασίας που του παρείχε τα δεδομένα, «σε δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμη από μηχανή μορφή» και να διαβιβάσει αυτά τα δεδομένα σε άλλον ελεγκτή. Αυτό το δικαίωμα δεν ισχύει «στην επεξεργασία που είναι απαραίτητη για την εκτέλεση καθηκόντων που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση επίσημης εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας» ή όταν επηρεάζει σημαντικά τα δικαιώματα και τις ελευθερίες άλλων.

4.12.6. Δικαίωμα αντίρρησης

Υπό ορισμένες προϋποθέσεις, το υποκείμενο των δεδομένων έχει το δικαίωμα να αντιταχθεί ανά πάσα στιγμή στην επεξεργασία των προσωπικών του δεδομένων, που είναι έννομα συμφέροντα του υπεύθυνου επεξεργασίας. Εκτός εάν ο υπεύθυνος επεξεργασίας αποδείξει ότι υπάρχουν συμφέροντα που υπερισχύουν των δικαιωμάτων του υποκειμένου των δεδομένων ή ότι η επεξεργασία είναι απαραίτητη για την άσκηση νομικών αξιώσεων, ο υπεύθυνος επεξεργασίας δεν επεξεργάζεται πλέον τα προσωπικά δεδομένα. Μέχρι την πρώτη επικοινωνία με το υποκείμενο των δεδομένων, ο υπεύθυνος επεξεργασίας οφείλει να ενημερώσει ρητά το υποκείμενο των δεδομένων σχετικά με αυτό το δικαίωμα. Επιπλέον, «όταν τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς σύμφωνα με το άρθρο 89 παράγραφος 1, το υποκείμενο των δεδομένων, για λόγους που σχετίζονται με την ιδιαίτερη κατάστασή του, έχει το δικαίωμα να αντιταχθεί στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που τον αφορούν, εκτός εάν η επεξεργασία είναι απαραίτητη για την εκτέλεση εργασίας που εκτελείται για λόγους δημοσίου συμφέροντος».

4.12.7. Δικαίωμα να μην υπόκεινται σε απόφαση που βασίζεται αποκλειστικά στην αυτοματοποιημένη επεξεργασία

Το υποκείμενο των δεδομένων έχει το δικαίωμα να μην υπόκειται σε απόφαση που βασίζεται στην αξιολόγηση προσωπικών πτυχών που έχουν υποστεί αυτόματη επεξεργασία, δηλαδή δημιουργία προφίλ, και η οποία έχει νομικά αποτελέσματα πάνω του ή το επηρεάζει σημαντικά. Το δικαίωμα δεν ισχύει σε περίπτωση που μια τέτοια απόφαση είναι (α) απαραίτητη για τη σύναψη ή την εκτέλεση σύμβασης μεταξύ του υπευθύνου επεξεργασίας και του υποκειμένου των δεδομένων,
(β) είναι εξουσιοδοτημένη από το δίκαιο της ΕΕ ή το εθνικό δίκαιο και ο υπεύθυνος επεξεργασίας τηρεί αυτήν π.χ. παρακολούθηση απάτης και φοροδιαφυγής) και η οποία προβλέπει κατάλληλες διασφαλίσεις για τα δικαιώματα του υποκειμένου των δεδομένων,
(γ) βασίζεται στη ρητή συναίνεση του υποκειμένου των δεδομένων.

4.12.8. Περιορισμοί

Περιορισμοί στα δικαιώματα του υποκειμένου των δεδομένων και αντίστοιχες υποχρεώσεις του υπευθύνου επεξεργασίας μπορούν να επιβληθούν από το δίκαιο της ΕΕ ή το εθνικό δίκαιο, εφόσον αυτά σέβονται τα θεμελιώδη δικαιώματα και ελευθερίες και αποτελούν αναγκαίο και αναλογικό μέτρο για τη διασφάλιση: εθνική ασφάλεια. άμυνα; ηβική ασφάλεια? πράξεις που σχετίζονται με ποινικά αδικήματα ή την εκτέλεση ποινικών κυρώσεων· άλλους σημαντικούς στόχους δημοσίου συμφέροντος της ΕΕ ή ενός κράτους μέλους· την προστασία της δικαστικής ανεξαρτησίας και των δικαστικών διαδικασιών· την πρόληψη/διερεύνηση/εντοπισμό/ δίωξη παραβιάσεων της δεοντολογίας για νομοθετικά κατοχυρωμένα επαγγέλματα· παρακολούθηση, επιθεώρηση ή ρυθμιστική λειτουργία που σχετίζεται με την άσκηση επίσημης εξουσίας· την προστασία των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων ή άλλων· την επιβολή εάν αξιώνει το αστικό δίκαιο (ΓΚΠΔ, άρθρο 23, παρ. 1). Το εν λόγω νομοθετικό μέτρο περιλαμβάνει ελάχιστη ειδική διάταξη όπως ορίζεται στην παράγραφο 2 του άρθρου 23 του ΓΚΠΔ.

4.12.9. Δικαίωμα αποκατάστασης

Κάθε υποκείμενο των δεδομένων έχει το δικαίωμα να υποβάλει καταγγελία ενώπιον της αρμόδιας εποπτικής αρχής. Σε περίπτωση που η εποπτική αρχή δεν χειριστεί την καταγγελία ή δεν ενημερώσει το υποκείμενο εντός τριών μηνών σχετικά με την πρόοδο ή την έκβαση της καταγγελίας, το υποκείμενο των δεδομένων έχει το δικαίωμα σε αποτελεσματική δικαστική προσφυγή. Περαιτέρω, κάθε φυσικό ή νομικό πρόσωπο έχει δικαίωμα σε αποτελεσματικό ένδικο μέσο κατά νομικά δεσμευτικής απόφασης εποπτικής αρχής που το αφορά. Το υποκείμενο των δεδομένων, το οποίο θεωρεί ότι τα

δικαιώματά του βάσει του GDPR έχουν παραβιαστεί από τον υπεύθυνο επεξεργασίας λόγω επεξεργασίας κατά μη συμμόρφωση με τον GDPR, έχει, επιπλέον, το δικαίωμα σε αποτελεσματική δικαστική προσφυγή (άμεσα). Σε περίπτωση που οι υπεύθυνοι επεξεργασίας ήταν δύο ή περισσότεροι, το υποκείμενο των δεδομένων μπορεί να ασκήσει τα δικαιώματά του βάσει του GDPR έναντι καθενός από τους υπευθύνους επεξεργασίας. Εάν μια τέτοια παραβίαση του GDPR έχει προκαλέσει υλικές ή μη υλικές ζημιές σε ένα άτομο, τότε ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία πρέπει να αποζημιώσει το άτομο.

5. Ηθικές διατάξεις

5.1. Συμμόρφωση με εθνικές νομοθεσίες

Σε εθνικό επίπεδο, κάθε εταιρία ή πλατφόρμα θα πρέπει να ευθυγραμμίζεται με την εθνική νομοθεσία σχετικά με τη διαχείριση προσωπικών δεδομένων. Αυτή η σχετική νομοθεσία θα παρουσιαστεί στο πλαίσιο του D1.1 POPD – Απαίτηση No2, όπου θα παρουσιαστεί το εθνικό νομικό πλαίσιο των χωρών των πιλοτικών εταίρων. Επιπλέον, θα ληφθεί υπόψη η νομοθεσία της ΕΕ και η διεθνής νομοθεσία προκειμένου να αποφευχθεί οποιαδήποτε κατάχρηση δεδομένων. Για να διασφαλιστεί η ευθυγράμμιση με την ισχύουσα νομοθεσία, συνάπτονται οι ακόλουθες συμφωνίες:

Η νομοθεσία που πρέπει να ακολουθείται σε περιπτώσεις που περισσότερες από μία χώρες εμπλέκονται σε μια διαδικασία επαλήθευσης

Ορισμένες περιπτώσεις περιλαμβάνουν την επαλήθευση πτυχίου μεταξύ δύο διαφορετικών χωρών της ΕΕ. Σε τέτοιες περιπτώσεις, όπου η επαλήθευση ενός πτυχίου ή ενός τίτλου σπουδών αφορά περισσότερες από μία χώρες, θα πρέπει να προαποφασιστεί ποια νομοθεσία επικρατεί σχετικά με τα προσωπικά δεδομένα των εμπλεκόμενων μερών στο πλαίσιο της πλατφόρμας. Θα πρέπει, δηλαδή, να προαποφασιστεί εάν θα ισχύει η νομοθεσία της χώρας προέλευσης του χρήστη ή η νομοθεσία της χώρας όπου ο χρήστης έστειλε το πτυχίο του ή η σχετική νομοθεσία της ΕΕ και της διεθνούς προστασίας δεδομένων.

Το επίπεδο πρόσβασης των αρχών που ζητούν δεδομένα-προσωπικά αναγνωριστικά

Οι χρήστες που ενεργούν κυρίως ως πηγές πληροφοριών αλλά αποτελούν και υποκείμενα δεδομένων μπορούν να είναι εγγεγραμμένοι αναγνωρίσιμοι χρήστες, εγγεγραμμένοι χρήστες χωρίς προσωπικά αναγνωριστικά ή ολόκληροι οργανισμοί (δημόσιοι ή ιδιωτικοί). Το επίπεδο πρόσβασης στα προσωπικά δεδομένα αυτών των ομάδων χρηστών θα πρέπει να είναι

σαφώς προκαθορισμένο για την αποφυγή κάθε είδους παραβίασης απορρήτου και ταυτόχρονα η πλατφόρμα να λειτουργεί σύμφωνα με το νόμο.

Παρά το γεγονός ότι καποιοι χρήστες δεν είναι εγγεγραμμένοι, ορισμένες βασικές πληροφορίες ενδέχεται να συλλέγονται και να αποθηκευτούν αυτόματα στον διακομιστή όπου φιλοξενείται μια πλατφόρμα, όταν οι χρήστες χρησιμοποιούν την πλατφόρμα (όπως το όνομα του τομέα διαδικτύου εάν χρησιμοποιούν ιδιωτικό λογαριασμό πρόσβασης στο Διαδίκτυο, τη διεύθυνση του Πρωτοκόλλου Διαδικτύου (IP), την ημερομηνία, την ώρα που χρησιμοποίησαν την πλατφόρμα).

5.2. Δεοντολογικές πτυχές που σχετίζονται με την πλατφόρμα

Το Privacy by design είναι μια τεχνική προσέγγιση ενός κοινωνικού προβλήματος. Όσον αφορά τα όρια της ιδιωτικότητας από το σχεδιασμό, υπάρχει μια προειδοποίηση: σημαντικό μέρος της παραβίασης της ιδιωτικής ζωής χαμηλού επιπέδου είναι το άμεσο αποτέλεσμα της εσωτερικής λειτουργίας των τεχνικών συστημάτων. Έτσι, ενώ τα κίνητρα και η βούληση για παραβίαση της ιδιωτικής ζωής μπορεί να είναι κοινωνικά προβλήματα, η πραγματική δυνατότητα να γίνει κάτι τέτοιο είναι τεχνικό πρόβλημα σε πολλές περιπτώσεις. Επομένως, η αντιμετώπισή του σε τεχνολογικό επίπεδο είναι απαραίτητη.

5.2.1. Εφαρμογή αρχών σχεδιασμού απορρήτου-διασφάλιση κατάλληλου επιπέδου προστασίας ευαίσθητων προσωπικών δεδομένων

Η οδηγία 2002/58/ΕΚ (οδηγία για την προστασία της ιδιωτικής ζωής ηλεκτρονικών επικοινωνιών) [ΟΔΗΓΙΑ2002] μπορεί να ερμηνευθεί ως έκκληση για προστασία της ιδιωτικής ζωής από το σχεδιασμό, ενώ η νομοθεσία της ΕΕ για την προστασία δεδομένων, άρθρο 29. Η Ομάδα Εργασίας για την Προστασία Δεδομένων ζητά και αναφέρεται στο απόρρητο βάσει σχεδιασμού. εκεί, επισημαίνονται επίσης πρακτικές πτυχές: «Στην πράξη, η εφαρμογή της αρχής της ιδιωτικότητας βάσει σχεδιασμού θα απαιτήσει την αξιολόγηση πολλών, συγκεκριμένων πτυχών ή στόχων. Ειδικότερα, κατά τη λήψη αποφάσεων σχετικά με το σχεδιασμό ενός συστήματος επεξεργασίας, την απόκτησή του και τη λειτουργία ενός τέτοιου συστήματος, θα πρέπει να τηρούνται οι ακόλουθες γενικές πτυχές / στόχοι: Ελαχιστοποίηση δεδομένων, Ελεγχσιμότητα, Διαφάνεια, Συστήματα φιλικά προς τον χρήστη, Εμπιστευτικότητα δεδομένων, Ποιότητα δεδομένων και Περιορισμός χρήσης».

Πριν από την κυκλοφορία της πλατφόρμας, θα πρέπει να διασφαλιστεί ότι οι πολιτικές ασφαλείας έχουν ρυθμιστεί κατάλληλα και ότι τα σωστά μέτρα για την προστασία των δεδομένων που μοιράζονται οι χρήστες με την πλατφόρμα. Μερικές ενδεικτικές συμβουλές για τους προγραμματιστές σχετικά με την ασφάλεια ιστού περιλαμβάνουν, μεταξύ άλλων, την αναθεώρηση δεδομένων για τη συλλογή και τη διατήρηση και τη δημιουργία ασφαλών διαπιστευτηρίων χρηστών (όνομα χρήστη και κωδικοί πρόσβασης).

5.2.2. Διασφάλιση της αποτροπής κακής χρήσης πλατφόρμας (από οποιονδήποτε πιθανό ενδιαφερόμενο φορέα της πλατφόρμας)

Η πρόκληση για τους προγραμματιστές μιας πλατφόρμας ΤΠΕ είναι να προβλέψουν την κακή χρήση και να σχεδιάσουν για να την αποτρέψουν. Υπό την προϋπόθεση ότι η ασχολείται με προσωπικά δεδομένα, θα πρέπει να διασφαλίζεται ότι εφαρμόζονται τα απαραίτητα πρότυπα και κανονισμοί προκειμένου να αποφευχθεί οποιαδήποτε κακή χρήση της εφαρμογής. Θα πρέπει να διερευνηθούν τρόποι για την αποτροπή της κατάχρησης δεδομένων μέσω της πλατφόρμας (όπως παρακολούθηση της πρόσβασης σε δεδομένα, παρακολούθηση ενεργειών διάφορων ενδιαφερομένων/χρηστών και διασφάλιση ότι το σύστημα είναι καλά προστατευμένο, καθώς η κατάχρηση δεδομένων θεωρείται παραβίαση ασφάλειας και πρωτίστως αποτελεί ανησυχία για την ασφάλεια).

5.2.3. Διαφανής διαχείριση αρχείων καταγραφής (περιεχόμενο, προστασία, πρόσβαση, καταστροφή)

Το πρώτο ηθικό δίλημμα που αναφέρεται σε ένα δημοφιλές άρθρο στο InfoWorld211 αφορά τα αρχεία καταγραφής, τι να αποθηκεύσετε και πώς να τα χειριστείτε. Σημειώνεται ότι οι προγραμματιστές συχνά κρατούν αρχεία για τα πάντα, γιατί αυτός είναι ο μόνος τρόπος εντοπισμού σφαλμάτων ενός συστήματος. Τα αρχεία καταγραφής, ωστόσο, μπορούν να αποκαλύψουν πληροφορίες που οι χρήστες θέλουν να κρατηθούν μυστικές. Η απλή ύπαρξη αρχείων καταγραφής εγείρει πολλά ηθικά ερωτήματα. Προστατεύονται επαρκώς; Ποιος έχει πρόσβαση; Όταν λέμε ότι καταστρέφουμε τα αρχεία, καταστρέφονται πραγματικά; Το κρίσιμο σημείο, που ισχύει και για την πλατφόρμα QualiChain, είναι να αποφασίσετε ποιες πληροφορίες αξίζει να κρατήσετε, δεδομένων των ηθικών κινδύνων που συνεπάγεται κάτι τέτοιο.

5.2.4. Πτυχές της συντήρησης της πλατφόρμας

Θα πρέπει να καθοριστεί η διαδικασία παρακολούθησης και η μεθοδολογία για τη διασφάλιση της εύρυθμης λειτουργίας της πλατφόρμας καθώς και ο υπεύθυνος οργανισμός/αρχή που θα αναλάβει την παρακολούθηση και κατά συνέπεια την αναφορά στον εκτελούντα την επεξεργασία.

5.3. Πολιτική απορρήτου

Μια εταιρία ή μια διαδικτυακή πλατφόρμα μπορεί να συλλέγει, να αποθηκεύει και να μοιράζεται προσωπικά δεδομένα (π.χ. ονόματα, διευθύνσεις email, εκπαιδευτικούς τίτλους, δεξιότητες, ενδιαφέροντα κ.λπ.) μαθητών και επαγγελματιών καθώς και άλλων ομάδων χρηστών και, ως εκ τούτου, η πολιτική απορρήτου είναι υποχρεωτική, καθώς και οι δύο παραπάνω οδηγίες είναι επιτακτικοί νόμοι, δεδομένου ότι τα δικαιώματα του ατόμου είναι μη μεταβιβάσιμα και δεν υπόκεινται σε συμβατική παραίτηση.

Ως εκ τούτου, θα συνταχθεί μια εύκολα προσβάσιμη πολιτική απορρήτου για την ενημέρωση των χρηστών τουλάχιστον σχετικά με τα ακόλουθα:

- στοιχεία ταυτότητας και επικοινωνίας
- ποια προσωπικά δεδομένα συλλέγει και επεξεργάζεται η πλατφόρμα και γιατί αυτό είναι απαραίτητο (σκοπός)
- εάν τα προσωπικά δεδομένα θα γνωστοποιηθούν σε τρίτους (εάν ναι, συγκεκριμένα σε ποιον)
- ποια είναι τα δικαιώματά τους (των χρηστών), όσον αφορά την ανάκληση της συγκατάθεσης και τη διαγραφή δεδομένων

Το περιεχόμενο της πολιτικής απορρήτου θα μπορούσε να δομηθεί ως εξής:

- Πληροφορίες που συλλέγονται από την πλατφόρμα
- Κοινή χρήση πληροφοριών με τρίτα μέρη
- cookies
- Ασφάλεια
- Ερωτήσεις

Σε διάφορες υπηρεσίες, ο χρήστης πρέπει να μπορεί να προσαρμόσει τις ρυθμίσεις απορρήτου, ώστε να ελέγχετε τα στοιχεία που συλλέγονται και τον τρόπο με τον οποίο αυτά χρησιμοποιούνται.

5.3.1. Διασφάλιση του απορρήτου των χρηστών και του απορρήτου των προσωπικών δεδομένων

Η κάθε εταιρία θα πρέπει να ακολουθεί τις απαραίτητες διαδικασίες για να διασφαλίσει ότι όλο το προσωπικό και οι άλλοι που έχουν πρόσβαση σε οποιεσδήποτε προσωπικές πληροφορίες που κατέχει η Πλατφόρμα, γνωρίζουν πλήρως και τηρούν τα καθήκοντα και τις ευθύνες τους σύμφωνα με το κύριο νομικό πλαίσιο της ΕΕ. Τα καθήκοντα και οι ευθύνες θα μπορούσαν να περιγραφούν είτε ως μέρος των Όρων Χρήσης των κύριων ομάδων ενδιαφερομένων ή σε ξεχωριστό έγγραφο «Πολιτική Προστασίας Δεδομένων και Εμπιστευτικότητας».

Απαιτούνται μηχανισμοί προστασίας από τυχόν μη εξουσιοδοτημένη πρόσβαση, παραποίηση, αποκάλυψη ή καταστροφή των πληροφοριών, όπως:

- Κρυπτογράφηση, για να διατηρηθούν απόρρητα τα δεδομένα κατά τη μεταφορά τους
- Διάφορες λειτουργίες ασφαλείας, όπως η Ασφαλής περιήγηση, ο Έλεγχος ασφαλείας και η Επαλήθευση σε 2 βήματα
- Περιορισμός της πρόσβασης στα προσωπικά στοιχεία μόνο σε υπαλλήλους, αναδόχους και αντιπροσώπους της εταιρίας. Οποιοσδήποτε έχει τέτοια πρόσβαση πρέπει να υπόκειται σε αυστηρές συμβατικές υποχρεώσεις

εμπιστευτικότητας και ενδεχομένως σε πειθαρχικές διαδικασίες ή σε απόλυση, εάν δεν ανταποκριθεί σε αυτές τις υποχρεώσεις.

5.3.2. Δημιουργία προφίλ χρήστη

Κατά τη δημιουργία ενός Λογαριασμού (προφίλ χρήστη), παρέχονται ορισμένα προσωπικά στοιχεία στα οποία περιλαμβάνονται το όνομα και ο κωδικός πρόσβασης. Μπορεί επίσης να προστεθεί ένας αριθμός τηλεφώνου, στοιχεία πληρωμής, ή μια διεύθυνση ηλεκτρονικού ταχυδρομείου. Οι εταιρίες συλλέγουν επίσης το περιεχόμενο που δημιουργεί, ανεβάζει ή λαμβάνει από άλλους χρήστες. Αυτό μπορεί να περιλαμβάνει μηνύματα ηλεκτρονικού ταχυδρομείου, φωτογραφίες και βίντεο, έγγραφα και υπολογιστικά φύλλα. Στους λογαριασμούς που δημιουργούνται στα κινητά τηλέφωνα, οι πληροφορίες περιλαμβάνουν στοιχεία όπως τύπο συσκευής, όνομα εταιρείας κινητής τηλεφωνίας, αναφορές σφαλμάτων, καθώς και εφαρμογές που έχετε εγκαταστήσει.

Στις μηχανές αναζήτησης, οι πληροφορίες δραστηριότητας που συλλέγονται ενδέχεται να περιλαμβάνουν:

- Όρους αναζήτησης
- Βίντεο που παρακολουθεί ο χρήστης
- Προβολές και αλληλεπιδράσεις με περιεχόμενο και διαφημίσεις
- Πληροφορίες φωνής και ήχου
- Αγοραστική δραστηριότητα
- Άτομα με τα οποία ο χρήστης επικοινωνεί ή μοιράζεται περιεχόμενο
- Ιστορικό περιήγησης

5.3.3. Επεξεργασία Δεδομένων με Analytics engine

Οι εταιρίες χρησιμοποιούν δεδομένα για αναλύσεις και μετρήσεις ώστε να κατανοήσουν πώς χρησιμοποιούνται οι υπηρεσίες τους. Για παράδειγμα, αναλύουν δεδομένα σχετικά με τις επισκέψεις στους ιστότοπους, για ενέργειες όπως η βελτιστοποίηση του σχεδιασμού προϊόντων. Επίσης χρησιμοποιούν δεδομένα σχετικά με τις διαφημίσεις με τις οποίες αλληλεπιδρούν οι χρήστες, για να βοηθήσουν τους διαφημιζόμενους να κατανοήσουν την απόδοση των διαφημιστικών καμπανιών τους. Όταν οι χρήστες επισκέπτονται έναν ιστότοπο που χρησιμοποιεί κάποια Analytics engine, ένας πελάτης της μπορεί να δει πληροφορίες σχετικά με τη δραστηριότητά σας στον συγκεκριμένο ιστότοπο.

5.3.4. Αυτοματοποιημένη Λήψη Αποφάσεων (ADM)

Η αυτοματοποιημένη λήψη αποφάσεων (ή ADM) είναι η λήψη αποφάσεων με τεχνολογικά μέσα, όπως ένας αλγόριθμος ή ένας υπολογιστής. Ο GDPR απαγορεύει σε άτομα να υποβάλλονται σε αποφάσεις «που βασίζονται αποκλειστικά σε αυτοματοποιημένη επεξεργασία». Αυτό σημαίνει σε ορισμένες περιπτώσεις εταιρείες, αρχές και άλλες οντότητες δεν μπορούν να λαμβάνουν αποφάσεις για άτομα που χρησιμοποιούν μόνο τεχνολογία και καμία ανθρώπινη παρέμβαση.

Τα δεδομένα που χρησιμοποιούνται σε ένα σύστημα ADM μπορούν να συλλεχθούν με διαφορετικούς τρόπους: απευθείας από τα άτομα π.χ. μέσω ερωτηματολογίου, παρατηρώντας τα άτομα, συλλέγοντας δεδομένα τοποθεσίας από μια εφαρμογή στο τηλέφωνο ή αντλώντας δεδομένα από ένα προφίλ.

Παραδείγματα: (α) μια τράπεζα αρνείται ένα δάνειο με βάση έναν αλγόριθμο σε ένα πρόγραμμα υπολογιστή, (β) ένας πάροχος τηλεπικοινωνιών δεν αποδέχεται κάποιον ως πελάτη επειδή ένας οργανισμός πιστοληπτικής ικανότητας επέστρεψε αρνητικό αποτέλεσμα.

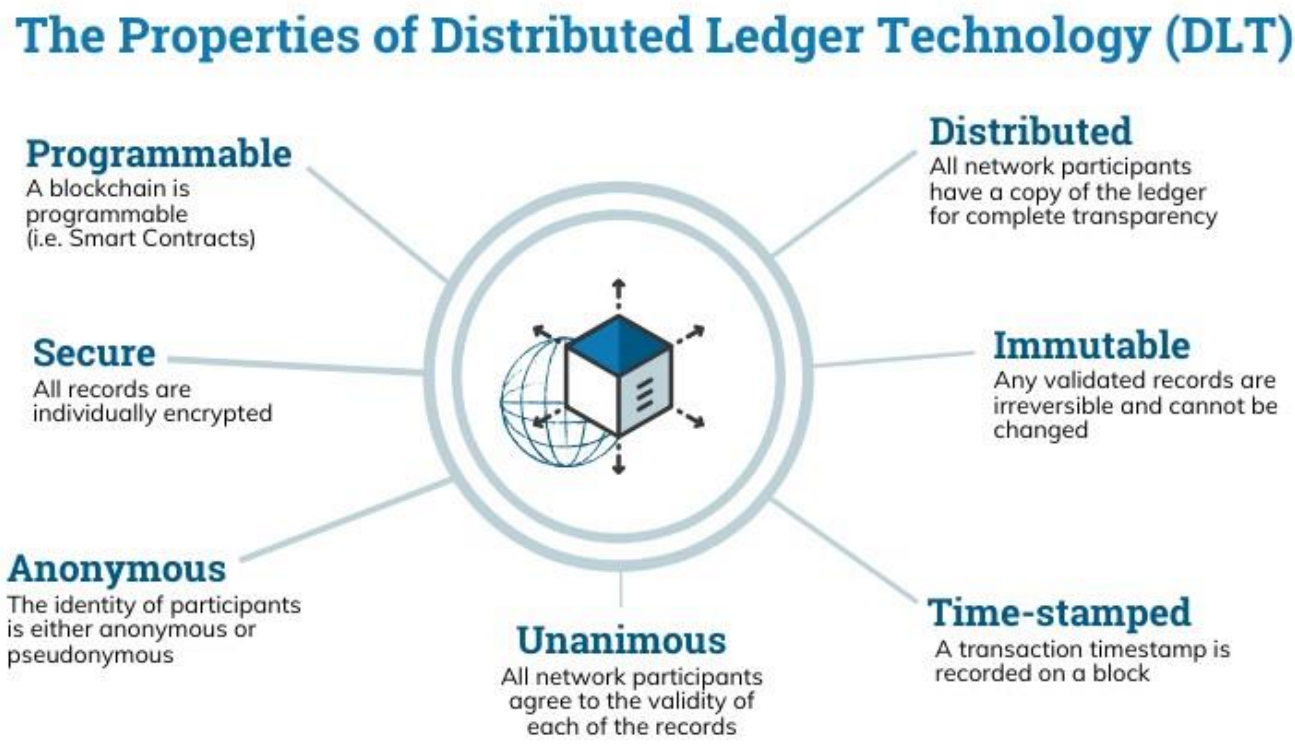
6. Blockchain

6.1. Η δομή του Blockchain

Το Blockchain είναι ένα σύστημα καταγραφής πληροφοριών με τρόπο που καθιστά δύσκολη ή αδύνατη την αλλαγή, την παραβίαση ή την εξαπάτηση του συστήματος.

Ένα blockchain είναι ουσιαστικά ένα ψηφιακό λογιστικό βιβλίο συναλλαγών που αντιγράφεται και διανέμεται σε ολόκληρο το δίκτυο υπολογιστικών συστημάτων που ανήκουν στους συμμετέχοντες. Κάθε μπλοκ στην αλυσίδα περιέχει έναν αριθμό συναλλαγών και κάθε φορά που πραγματοποιείται μια νέα συναλλαγή, μια εγγραφή αυτής της συναλλαγής προστίθεται στο λογιστικό βιβλίο κάθε συμμετέχοντα. Η αποκεντρωμένη βάση δεδομένων που διαχειρίζονται πολλοί συμμετέχοντες είναι γνωστή ως Τεχνολογία Κατανεμημένης Λογιστικής (Distributed Ledger Technology -- DLT).

Το Blockchain είναι ένας τύπος DLT στο οποίο οι συναλλαγές καταγράφονται με μια αμετάβλητη κρυπτογραφική υπογραφή που ονομάζεται hash.



6.2. Ακεραιότητα δεδομένων

Οι πρώιμες εφαρμογές του blockchain, όπως το Bitcoin, δημιουργήθηκαν για να λειτουργούν σε ένα περιβάλλον χωρίς εμπιστοσύνη, όπου το blockchain δεν θα πρέπει να διαχειρίζεται κανένα κεντρικό μέρος, αλλά αντίθετα να αποθηκεύεται με τρόπο κατανεμημένο σε όλο το δίκτυο peer-to-peer, στο οποίο κάθε κόμβος διατηρεί ένα ενημερωμένο αντίγραφο του καθολικού συναλλαγών.

6.2.1. Οι συναρτήσεις κατακερματισμού (hashes)

Με τον ίδιο τρόπο που το κατανεμημένο δίκτυο peer-to-peer είναι απαραίτητο για την υπέρβαση της ανυπαρξίας μιας κεντρικής οντότητας, οι κρυπτογραφικές συναρτήσεις κατακερματισμού είναι απαραίτητες για τη διασφάλιση της ακεραιότητας των συναλλαγών. Στην πράξη, οι συναρτήσεις κατακερματισμού όχι μόνο δημιουργούν μια καταγεγραμμένη κατακερματισμένη εγγραφή των συναλλαγών, αλλά εγγυώνται επίσης ότι είναι «υπολογιστικά μη πρακτικό να αντιστραφούν». Το Bitcoin και άλλες εφαρμογές blockchain χρησιμοποιούν συναρτήσεις κατακερματισμού για να δημιουργήσουν μια μοναδική τιμή κατακερματισμού στο στοιχείο δεδομένων εισόδου. που αποτελείται από μια συμβολοσειρά ψηφίων με σταθερό μήκος. Η τιμή κατακερματισμού χρησιμοποιείται για να αποδείξει την ακεραιότητα ενός στοιχείου δεδομένων, καθώς οποιαδήποτε αλλαγή στο αρχικό στοιχείο δεδομένων θα δημιουργήσει

ένα διαφορετική και άσχετη τιμή κατακερματισμού που επιτρέπει στους συμμετέχοντες του blockchain να ανιχνεύουν εάν έχει συμβεί οποιαδήποτε προσπάθεια παραβίασης των δεδομένων. Για αυτόν τον συγκεκριμένο λόγο, λέγεται συνήθως ότι η τιμή κατακερματισμού ενός στοιχείου δεδομένων λειτουργεί ως το δακτυλικό του αποτύπωμα, καθώς αυτή η τιμή είναι μοναδική.

Εκτός από αυτό το συγκεκριμένο χαρακτηριστικό, οι συναρτήσεις κατακερματισμού είναι μη αναστρέψιμες, με την έννοια ότι δεν είναι δυνατή η χρήση την τιμή κατακερματισμού για την αναδημιουργία της αρχικής εισαγωγής ενός συγκεκριμένου στοιχείου δεδομένων. Επανεξετάζοντας τη μεταφορά του τρένου, οι συναρτήσεις κατακερματισμού λειτουργεί, στο συγκεκριμένο πλαίσιο, ως ένας τρόπος επαλήθευσης ότι οι επιβάτες έχουν έγκυρο εισιτήριο εισόδου στο τρένο και ότι το εισιτήριο δεν παραποιήθηκε ή παραποιήθηκε με κανέναν τρόπο, καθώς είναι μοναδικό και μπορεί να χρησιμοποιηθεί μόνο από τους συγκεκριμένους επιβάτες.

6.2.2. Τα μπλοκ

Πέρα από τις μεμονωμένες συναλλαγές και τα στοιχεία δεδομένων, οι συναρτήσεις κατακερματισμού διαδραματίζουν επίσης σημαντικό ρόλο στη δημιουργία μεγάλων δομών δεδομένων, οι οποίες περιέχουν πολλαπλές συναλλαγές ή στοιχεία δεδομένων, προφανείς για παραβιάσεις, χρησιμοποιώντας δείκτες κατακερματισμού. Στο blockchain, αυτές οι δομές είναι κοινώς γνωστές ως μπλοκ και **κάθε μπλοκ περιέχει μια εγγραφή πολυάριθμων μεμονωμένων συναλλαγών ή άλλων στοιχείων δεδομένων**. Προκειμένου να αποδειχθεί η ακεραιότητα των μπλοκ, συμπεριλαμβανομένου του περιεχομένου και της ακολουθίας τους, οι δείκτες κατακερματισμού συνδέουν τα μπλοκ μεταξύ τους, βάζοντας σε μια συνάρτηση κατακερματισμού το συνδυασμό των δεδομένων κάθε μπλοκ με την τιμή κατακερματισμού του προηγούμενου μπλοκ. Αυτό δημιουργεί την τιμή κατακερματισμού ενός μπλοκ που θα συμπεριληφθεί στο επόμενο μπλοκ μαζί με μια λίστα συναλλαγών ή συνόλων δεδομένων και άλλα μεταδεδομένα. Το αποτέλεσμα είναι μια αλυσίδα μπλοκ, στην οποία οποιαδήποτε προσπάθεια τροποποίησης του περιεχομένου ενός μπλοκ θα σπάσει τη σύνδεση μεταξύ των μπλοκ, επιτρέποντας τον εύκολη εντοπισμό τυχόν δόλιας παρέμβασης.

6.2.3. Τα δέντρα Merkle

Οι πρώτες εφαρμογές blockchain θεωρήθηκαν πρακτικά αμετάβλητες και μη αναστρέψιμες, καταγράφοντας και συνδέοντας όλες τις συναλλαγές σε μια αλυσίδα μπλοκ. Από πρώιμο στάδιο, προέκυψε μια ανησυχία σχετικά με τον αποθηκευτικό χώρο, καθώς όσο περισσότερες συναλλαγές πραγματοποιούνται, τόσο περισσότερο μεγαλώνει η βάση δεδομένων. Η χρήση ενός δέντρου Merkle παρείχε μια λύση τόσο στον αποθηκευτικό χώρο όσο και στην επαλήθευση δεδομένων. Γενικά, ένα δέντρο Merkle είναι μια δομή δεδομένων που βασίζεται σε κατακερματισμό που περιέχει το συνδυασμό των τιμών κατακερματισμού των μεμονωμένων συναλλαγών. Στην πράξη, οι τιμές κατακερματισμού των

μεμονωμένων συναλλαγών ζευγαρώνονται και τοποθετούνται σε μια συνάρτηση κατακερματισμού προκειμένου να δημιουργηθούν νέες τιμές κατακερματισμού. Αυτή η διαδικασία επαναλαμβάνεται διαδοχικά μέχρι να βρεθεί η τελευταία τιμή κατακερματισμού – επίσης γνωστή ως ρίζα Merkle –. Κάθε μπλοκ περιέχει μια ρίζα Merkle, η οποία αντιπροσωπεύει μια σύνοψη όλων των συναλλαγών που διατηρεί ένα μπλοκ. Εκτός από την απαίτηση λιγότερου χώρου για την αποθήκευση δεδομένων και τη χρήση λιγότερους πόρους, το σύστημα δέντρου Merkle διευκολύνει την επαλήθευση της ακεραιότητας των συναλλαγών και τον έλεγχο εάν μια συναλλαγή έχει συμπεριληφθεί σε ένα μπλοκ χωρίς να χρειάζεται να κατεβάσετε ολόκληρο το βιβλίο συναλλαγών.

6.3. Μπορούν να εντοπιστούν οι συμμετέχοντες στα blockchain;

Όπως αναφέρθηκε προηγουμένως, η ταξινόμηση (δηλαδή η δομή) των εφαρμογών blockchain έχει διαφορετικό αντίκτυπο στις εξουσίες, τα δικαιώματα, τις άδειες και τους περιορισμούς των συμμετεχόντων σε μια συγκεκριμένη πλατφόρμα. Συνήθως, οποιοσδήποτε συμμετέχων, ή ακόμα και το κοινό, μπορεί να συμβουλευτεί ολόκληρο το αρχείο blockchain μιας δημόσιας και χωρίς άδεια (public and permissionless) blockchain εφαρμογής. Αντίθετα, στις εφαρμογές blockchain κοινοπραξίας, οι άδειες ανάγνωσης των αρχείων μπορούν να περιοριστούν σε συγκεκριμένο αριθμό συμμετεχόντων, ενώ σε ιδιωτικές και με άδεια (permissioned) εφαρμογές blockchain, η πρόσβαση στα αρχεία blockchain μπορεί να μην επιτρέπεται ή να περιοριστεί σε μερικά μπλοκ ή ορισμένες καταχωρίσεις δεδομένων.

Αυτό εγείρει αμέσως δύο βασικά ερωτήματα: μπορούν να εντοπιστούν οι συμμετέχοντες στις πλατφόρμες blockchain; Εάν ναι, μπορεί οποιοσδήποτε άλλος συμμετέχων να έχει πρόσβαση στα δεδομένα και το ιστορικό των συναλλαγών του;

Όπως αναφέρθηκε παραπάνω, οι εφαρμογές blockchain χρησιμοποιούν ένα PKI για τον έλεγχο ταυτότητας των συμμετεχόντων τους. Γενικά, το δημόσιο και το ιδιωτικό κλειδί δεν αποκαλύπτουν την ταυτοποίηση των συμμετεχόντων στον πραγματικό κόσμο. Οι πρώιμες εφαρμογές blockchain, όπως το Bitcoin, έλαβαν υπόψη αυτές τις ανησυχίες και, όπως εξηγεί ο Nakamoto [NAKAMOTO2008]: «το απόρρητο μπορεί ακόμα να διατηρηθεί διακόπτοντας τη ροή πληροφοριών σε άλλο μέρος: διατηρώντας τα δημόσια κλειδιά ανώνυμα. Το κοινό μπορεί να δει ότι κάποιος στέλνει ένα ποσό σε κάποιον άλλο, αλλά χωρίς πληροφορίες που συνδέουν τη συναλλαγή με κανέναν». Επιπλέον, οι χρήστες μπορούν να δημιουργήσουν ένα νέο ζεύγος ιδιωτικού και δημόσιου κλειδιού για κάθε νέα συναλλαγή. Αυτό το επίπεδο ψευδωνυμοποίησης διασφαλίζει ότι ακόμη και στα δημόσια blockchain, όπου ο καθένας μπορεί να συμβουλευτεί το αρχείο blockchain, κανείς δεν θα μπορεί να προσδιορίσει την πραγματική ταυτότητα των μερών που εμπλέκονται σε μια συγκεκριμένη συναλλαγή.

Ωστόσο, η ταυτότητα των χρηστών μπορεί να αποκαλυφθεί σε εθελοντική βάση, εάν οι χρήστες αποφασίσουν να αποκαλύψουν την ταυτότητά τους στον πραγματικό κόσμο, ή σε ακούσια βάση, όπως συμβαίνει με κακόβουλες επιθέσεις

σε διαδικτυακά πορτοφόλια, στα οποία ο εισβολέας έχει αποκτήσει πρόσβαση σε πληροφορίες χρήστη. Με τον ίδιο τρόπο, η πραγματική ταυτότητα ενός χρήστη μπορεί να αποκαλυφθεί έμμεσα με τη σύνδεση διαφορετικών στοιχείων δεδομένων.

Για παράδειγμα, εάν ένας χρήστης χρησιμοποιεί το bitcoin ως μέθοδο πληρωμής για να αγοράσει αγαθά ή υπηρεσίες, το άλλο μέρος μπορεί να χρειαστεί το όνομα, τη διεύθυνση email, την ταχυδρομική διεύθυνση και άλλες προσωπικές πληροφορίες του πελάτη που μπορεί να οδηγήσουν στην αναγνώριση του χρήστη. Οι διευθύνσεις IP μπορούν επίσης να χρησιμοποιηθούν ως τρόπος προσδιορισμού της ταυτότητας των χρηστών, συνδέοντας το ζεύγος ιδιωτικού και δημόσιου κλειδιού των χρηστών με την τοποθεσία από την οποία δημιουργήθηκε η συναλλαγή.

Παρόλο που η υποδομή δημόσιου κλειδιού (public key infrastructure -- PKI) διασφαλίζει ένα ορισμένο επίπεδο προστασίας της ταυτότητας των χρηστών, μόλις αποκαλυφθεί η πραγματική τους ταυτότητα, οποιοσδήποτε μπορεί να έχει πρόσβαση σε ολόκληρο το ιστορικό συναλλαγών που σχετίζεται με αυτόν τον χρήστη, ειδικά σε περιπτώσεις όπου το ζεύγος ιδιωτικού και δημόσιου κλειδιού δεν έχει αλλάξει. Αν και τα ιδιωτικά blockchain και οι κοινοπραξίες λειτουργούν κανονικά σε ένα περιβάλλον όπου μπορεί να βρεθεί εμπιστοσύνη μεταξύ των συμμετεχόντων και όπου μερικές φορές οι συμμετέχοντες γνωρίζονται μεταξύ τους, αυτοί οι τύποι blockchain μπορούν να περιορίσουν το επίπεδο πρόσβασης στο αρχείο blockchain, διασφαλίζοντας ότι η ταυτότητα των χρηστών παραμένει κατάλληλα προστατευμένη.

6.4. Έλεγχος ταυτότητας

Επί του παρόντος, ένας μεγάλος αριθμός συναλλαγών που σχετίζονται με τις πιο διαφορετικές οικονομικές δραστηριότητες εξακολουθούν να εκτελούνται με τη χρήση χρηματοπιστωτικών διαμεσολαβητών, όπως ένα χρηματοπιστωτικό ίδρυμα ή μια τράπεζα. Σε αυτό το πλαίσιο, ένα από τα κύρια καθήκοντα ενός χρηματοπιστωτικού ιδρύματος είναι να προσδιορίζει σωστά τα μέρη που εμπλέκονται σε μια συναλλαγή και να διασφαλίζει ότι το περιεχόμενο της συναλλαγής είναι ακριβές. Όπως αναφέρθηκε παραπάνω, οι πρώιμες εφαρμογές του blockchain, όπως το Bitcoin, σχεδιάστηκαν για να λειτουργούν σε περιβάλλον χωρίς εμπιστοσύνη, δηλαδή χωρίς την παρέμβαση ενός αξιόπιστου τρίτου μέρους. Ωστόσο, το blockchain πρέπει ακόμα να εντοπίσει και να πιστοποιήσει τα μέρη που εμπλέκονται σε οποιαδήποτε συναλλαγή, πριν την αποθηκεύσει σε ένα μπλοκ. Για την επίτευξη αυτού του σκοπού, η τεχνολογία blockchain βασίζεται σε μια μέθοδο ασφαλείας γνωστή ως υποδομή δημόσιου κλειδιού (public key infrastructure -- PKI). Αυτή η μέθοδος ασφαλείας χρησιμοποιείται για την εφαρμογή ισχυρού ελέγχου ταυτότητας δημιουργώντας ένα ζεύγος κλειδιών που περιέχει ένα δημόσιο και ένα ιδιωτικό κλειδί, έναν αλγόριθμο υπογραφής και λειτουργία επικύρωσης που ελέγχει την εγκυρότητα των ψηφιακών υπογραφών.

Καθώς όλες οι εγγραφές συναλλαγών στο blockchain υπογράφονται πριν συμπεριληφθούν σε μπλοκ, το PKI χρησιμοποιείται κυρίως για τον καθορισμό της ψηφιακής ταυτότητας ενός χρήστη και για τη δημιουργία ψηφιακών υπογραφών. Το δημόσιο και το ιδιωτικό κλειδί μπορούν να χρησιμοποιηθούν για την κρυπτογράφηση και αποκρυπτογράφηση δεδομένων που έχουν κρυπτογραφηθεί ή αποκρυπτογραφηθεί αντίστοιχα χρησιμοποιώντας ένα από αυτά τα κλειδιά. Έτσι, για να αποδείξει την ταυτότητά του ή για να υπογράψει μια συναλλαγή ή οποιοδήποτε άλλο στοιχείο δεδομένων, ένας χρήστης μπορεί να κρυπτογραφήσει τα δεδομένα χρησιμοποιώντας το ιδιωτικό του κλειδί και να παρέχει στο συνδεδεμένο μέρος το δημόσιο κλειδί. Εάν το συνδεδεμένο μέρος μπορεί με επιτυχία να αποκρυπτογραφήσει τα δεδομένα χρησιμοποιώντας το δημόσιο κλειδί που παρέχεται από τον χρήστη, μπορεί να είναι βέβαιο ότι η συναλλαγή ή οποιοδήποτε άλλο στοιχείο δεδομένων προέρχεται από τον συγκεκριμένο χρήστη.

6.5. Ιδιωτικά και δημόσια blockchain

Στο ιστορικό τους πλαίσιο, τα κρυπτονομίσματα ήταν η πρώτη εφαρμογή της τεχνολογίας blockchain, η οποία εμφανίστηκε για να ξεπεράσει τις «εγγενείς αδυναμίες του μοντέλου που βασίζεται στην εμπιστοσύνη», δηλαδή το ποσοστό απάτης που γίνεται αποδεκτό ως αναπόφευκτο σε ένα τέτοιο μοντέλο και, πιο συγκεκριμένα, τη χρονική διάρκεια και το κόστος των συναλλαγών που υποστηρίζουν οι πελάτες όταν χρησιμοποιούν τρίτα μέρη για την επεξεργασία ηλεκτρονικών πληρωμών. Ως εκ τούτου, οι πρώτες εφαρμογές της τεχνολογίας blockchain σχεδιάστηκαν για να λειτουργούν χωρίς αξιόπιστο τρίτο μέρος. Ωστόσο, ένα σημαντικό ερώτημα προκύπτει από αυτό το παράδειγμα: ποιος ελέγχει το blockchain;

Η ερώτηση μπορεί να χωριστεί στις ακόλουθες δύο ερωτήσεις: ποιος μπορεί να αποθηκεύσει αντίγραφα του blockchain και ποιος μπορεί να προτείνει νέα μπλοκ που θα προστεθούν στο blockchain; Καθώς μπορούν να δοθούν διαφορετικές απαντήσεις, ο σχεδιασμός των πλατφορμών που χρησιμοποιούν τεχνολογία blockchain μπορεί να ποικίλλει Σημαντικά, δημιουργώντας διαφορετικούς τύπους εφαρμογών blockchain.
Αν και ο σχεδιασμός του blockchain μπορεί να παρουσιάσει ένα ευρύ φάσμα, για να γίνει πιο κατανοητή η ιδέα, οι τύποι blockchain συνήθως κατατμούνται σε ιδιωτικές ή δημόσιες και χωρίς άδεια ή βάσεις δεδομένων.

Το κριτήριο για τη διαφοροποίηση των ιδιωτικών ή δημόσιων blockchain μπορεί να βρεθεί παρατηρώντας τον τρόπο με τον οποίο οι συμμετέχοντες εντάσσονται στο δίκτυο. Από αυτή την άποψη, ενώ οι δημόσιες αλυσίδες μπλοκ είναι ανοιχτές σε οποιοδήποτε άτομο ή οντότητα που επιθυμεί να ενταχθεί στο δίκτυο peer-to-peer, από την άλλη πλευρά, τα ιδιωτικά blockchain επιτρέπουν μόνο σε προεπιλεγμένους συμμετέχοντες να ενταχθούν στο ομότιμο δίκτυο. Το προεπιλεγμένο κριτήριο χρησιμοποιείται επίσης για τη διαφοροποίηση των μπλοκ αλυσίδων χωρίς άδεια και των αδειοδοτημένων. Στην πρώτη, οποιοδήποτε πρόσωπο ή οντότητα μπορεί να συμμετάσχει στον μηχανισμό συναίνεσης, έχοντας τη δυνατότητα να προσθέσει νέα μπλοκ στην αλυσίδα. Στις επιτρεπόμενες αλυσίδες μπλοκ, μόνο οι προεπιλεγμένες οντότητες εξουσιοδοτούνται να προσθέτουν νέα μπλοκ στην αλυσίδα.

6.6. Έλεγχος και διακυβέρνηση του Blockchain

Ποιος ελέγχει την πλατφόρμα blockchain; Ποιος μπορεί να αλλάξει τον σχεδιασμό της πλατφόρμας και σε ποιο βαθμό; Αυτές οι ερωτήσεις είναι σημαντικές όχι μόνο για να ολοκληρώσουμε την εισαγωγή μας στην τεχνολογία blockchain, αλλά είναι επίσης κρίσιμες, όπως θα δούμε στις επόμενες ενότητες, για να προσδιορίσουμε ποιος μπορεί να θεωρηθεί ως ελεγκτής ή/και επεξεργαστής από την άποψη του GDPR.

Κάθε πλατφόρμα blockchain έχει τους δικούς της κανόνες διακυβέρνησης και το δικό της σχέδιο και δομή. Οι **προγραμματιστές** είναι υπεύθυνοι για την παραγωγή του λογισμικού που χρησιμοποιείται από κόμβους και εξορύκτες για την υποστήριξη της αλυσίδας μπλοκ.

Για παράδειγμα, ορισμένες δημόσιες πλατφόρμες blockchain, όπως το Bitcoin και το Ethereum, αναπτύχθηκαν χρησιμοποιώντας έναν κώδικα ανοιχτού κώδικα, ο οποίος θα μπορούσε να χρησιμοποιηθεί από άλλους προγραμματιστές και όχι από τους βασικούς προγραμματιστές, για να γράψουν μια νέα έκδοση του λογισμικού και να το κάνουν διαθέσιμο για τους συμμετέχοντες στο δίκτυο P2P. Συνήθως, εκτός από τις διορθώσεις σφαλμάτων, οι αλλαγές που εισάγονται στο λογισμικό blockchain προορίζονται για την επίτευξη άλλων λειτουργιών ή την τροποποίηση της ικανότητας του λογισμικού.

Οι **κόμβοι** (nodes) διατηρούν ένα πλήρες αντίγραφο του blockchain. Περιέχει το πλήρες ιστορικό συναλλαγών όλων των προηγούμενων συναλλαγών. Οι κόμβοι διασφαλίζουν ότι ο αποστολέας μιας συναλλαγής δεν ξοδεύει το ίδιο BTC (νόμισμα) δύο φορές και δεν το δημιούργησε "από τον αέρα".

Μόλις οι κόμβοι επικυρώσουν μια συναλλαγή, αυτή εμφανίζεται σε κατάσταση "εκκρεμότητας" έως ότου ένας εξειδικευμένος κόμβος, γνωστός ως **εξορύκτης** (miner), ή μια ομάδα εξορυκτών (ομάδα εξόρυξης), παραλάβει τη συναλλαγή. Οι εξορύκτες Bitcoin βρίσκονται σε όλο τον κόσμο και ανταγωνίζονται για να επιβεβαιώσουν τις εκκρεμείς συναλλαγές. Η μετάβαση από κατάσταση "εκκρεμότητας" σε "επιβεβαιωμένη" σημαίνει ότι η συναλλαγή έχει προστεθεί στο σύστημα καθολικής λογιστικής (blockchain) και δίνει τη δυνατότητα στον παραλήπτη της συναλλαγής να τη στείλει σε άλλο χρήστη.

Μόλις εισαχθούν στο δίκτυο P2P, οι κόμβοι και οι εξορύκτες μπορούν να αποφασίσουν ποια έκδοση λογισμικού θέλουν να τρέξουν. Σε περίπτωση που κάποιος προγραμματιστής έπεισε επιτυχώς τους εξορύκτες και τους κόμβους να υιοθετήσουν μια νέα έκδοση του λογισμικού, θα δημιουργηθεί ένα fork στο blockchain, το οποίο θα δημιουργεί δύο διαφορετικές αλυσίδες μπλοκ, στις οποίες θα προστεθούν στη συνέχεια νέα μπλοκ. Στο πλαίσιο του Bitcoin, όταν μια νέα έκδοση του λογισμικού υιοθετείται από κόμβους και εξορύκτες, δημιουργείται ένα fork, που δημιουργεί νέες αλυσίδες μπλοκ, μια που συνεχίζει να παρακολουθεί τα bitcoin και μια νέα που παρακολουθεί τώρα ένα νέο κρυπτονόμισμα.

Αντίθετα, σε ιδιωτικές και κοινοπραξίες blockchain, οι νέες εκδόσεις του λογισμικού που υποστηρίζει το blockchain μπορούν να υπόκεινται σε συμβατικές διατάξεις που αποτέλεσαν αντικείμενο διαπραγμάτευσης μεταξύ των μερών που εμπλέκονται στη δημιουργία και την ανάπτυξη μιας συγκεκριμένης πλατφόρμας blockchain. Σε τέτοιες περιπτώσεις, μπορεί να υποστηριχθεί ότι ο ρόλος των προγραμματιστών περιορίζεται στην εκτέλεση συμβατικών υποχρεώσεων, καθώς συνήθως δεν έχουν τη δύναμη ή τα μέσα να αλλάξουν την έκδοση λογισμικού με δική τους πρωτοβουλία.

Τέλος, υπάρχει μια ακόμη ομάδα παρέμβασης στο περιβάλλον blockchain: οι **πάροχοι υπηρεσιών**. Κανονικά, οι πάροχοι υπηρεσιών παρεμβαίνουν σε πλατφόρμες blockchain είτε προσφέροντας υπηρεσίες που σχετίζονται με διαδικτυακά πορτοφόλια είτε προσφέροντας «Blockchain-as-a-Service». Αυτό είναι μια υπηρεσία που επιτρέπει στον πελάτη να αξιοποιήσει λύσεις που βασίζονται σε σύννεφο για να δημιουργήσει τις δικές του εφαρμογές blockchain. Η προσφορά των παρόχων υπηρεσιών περιλαμβάνει ένα ευρύ φάσμα εργασιών και δραστηριοτήτων που μπορεί να περιλαμβάνουν τη διαχείριση της πλατφόρμας, τη φιλοξενία ορισμένου αριθμού κόμβων ή ακόμη και τη διαχείριση ελέγχου ταυτότητας. Δεδομένου ότι οι πάροχοι υπηρεσιών έχουν άμεση εμπλοκή στη δημιουργία και τον έλεγχο της πλατφόρμας blockchain, αυτό μπορεί να εγείρει ορισμένα ερωτήματα σχετικά με τον βαθμό ισχύος και τον έλεγχο που έχουν οι πάροχοι υπηρεσιών στο blockchain. Όπως θα αναλύσουμε παρακάτω, αυτά τα ερωτήματα είναι σημαντικά για τον προσδιορισμό της φύσης

των παρόχων υπηρεσιών στο πλαίσιο του GDPR, δηλαδή για την αξιολόγηση του εάν οι πάροχοι υπηρεσιών μπορούν να καθορίσουν τους σκοπούς και τα μέσα επεξεργασίας των προσωπικών δεδομένων.

6.7. Προσωπικά Δεδομένα στο Blockchain

Σύμφωνα με την αιτιολογική σκέψη 26 του GDPR, οι αρχές της προστασίας δεδομένων θα πρέπει να ισχύουν μόνο για οποιαδήποτε πληροφορία που αφορά ένα αναγνωρισμένο ή αναγνωρίσιμο φυσικό πρόσωπο, το οποίο υποδηλώνει ότι η εφαρμογή του GDPR στις εφαρμογές που βασίζονται σε blockchain και στους χειριστές τους εξαρτάται, σε κάθε περίπτωση, από τον χαρακτηρισμό των δεδομένων που αποθηκεύονται και υποβάλλονται σε επεξεργασία στο blockchain ως προσωπικά δεδομένα.

Το άρθρο 4 παράγραφος 1 του GDPR ενσωματώνει έναν ευρύ ορισμό των «προσωπικών δεδομένων». Περιλαμβάνει κάθε πληροφορία που σχετίζεται άμεσα ή έμμεσα με ταυτοποιημένο ή αναγνωρίσιμο φυσικό πρόσωπο. Προκειμένου να καθοριστεί εάν ένα φυσικό πρόσωπο είναι αναγνωρίσιμο, η αιτιολογική σκέψη 26 του GDPR αναφέρει ότι θα πρέπει να λαμβάνονται υπόψη όλα τα μέσα που είναι εύλογα πιθανό να χρησιμοποιηθούν για την άμεση ή έμμεση ταυτοποίηση του φυσικού προσώπου. Για να εξακριβωθεί ποια είναι τα εύλογα μέσα που είναι πιθανό να χρησιμοποιηθούν, θα πρέπει να ληφθούν υπόψη αντικειμενικοί παράγοντες. Η αιτιολογική σκέψη 26 του GDPR τονίζει ορισμένους από αυτούς τους παράγοντες, οι οποίοι περιλαμβάνουν: i) το κόστος και το χρόνο που απαιτείται για την ταυτοποίηση. ii) την τεχνολογία που είναι διαθέσιμη κατά τη στιγμή της επεξεργασίας· και iii) τις τεχνολογικές εξελίξεις.

Στην υπόθεση Digital Rights Ireland, το Ευρωπαϊκό Δικαστήριο έχει καθορίσει ότι ο ορισμός των «προσωπικών δεδομένων» είναι αρκετά ευρύς ώστε να χαρακτηρίζει τα μεταδεδομένα (π.χ. τοποθεσία εξοπλισμού κινητής επικοινωνίας, διεύθυνση IP, κ.λπ.) ως προσωπικά δεδομένα. Η χρήση αυτού του τύπου δεδομένων καθιστά δυνατή την ταυτοποίηση ενός ατόμου και «μπορεί να επιτρέψει την εξαγωγή πολύ ακριβών συμπερασμάτων σχετικά με την ιδιωτική ζωή των προσώπων των οποίων τα δεδομένα έχουν διατηρηθεί».

Τα διαδικτυακά αναγνωριστικά που παρέχονται από τις συσκευές, τις εφαρμογές, τα εργαλεία και τα πρωτόκολλα των υποκειμένων των δεδομένων, **μπορούν επίσης να χρησιμοποιηθούν για την άμεση ή έμμεση ταυτοποίησή τους**. Όπως αναγνωρίζει η αιτιολογική σκέψη 30 του GDPR, τα διαδικτυακά αναγνωριστικά «μπορεί να αφήνουν ίχνη τα οποία, ιδίως όταν συνδυάζονται με μοναδικά αναγνωριστικά και άλλες πληροφορίες που λαμβάνονται από τους διακομιστές, μπορούν να χρησιμοποιηθούν για τη δημιουργία προφίλ των φυσικών προσώπων και την αναγνώρισή τους».

Ο ευρύς ορισμός των προσωπικών δεδομένων περιλαμβάνει επίσης τα προσωπικά δεδομένα που έχουν υποστεί **ψευδωνυμοποίηση**. Σε αντίθεση με την ανωνυμοποίηση, η εφαρμογή της ψευδωνυμοποίησης σε δεδομένα προσωπικού χαρακτήρα θεωρείται ως μέτρο ασφαλείας που συμβάλλει στον μετριασμό των κινδύνων για τα υποκείμενα των δεδομένων σε σχέση με την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Στην πραγματικότητα, η ομάδα εργασίας

του άρθρου 29 (στο εξής WP29) αναγνωρίζει ότι «η ψευδωνυμοποίηση δεν είναι μέθοδος ανωνυμοποίησης. Απλώς μειώνει τη δυνατότητα σύνδεσης ενός συνόλου δεδομένων με την αρχική ταυτότητα ενός υποκειμένου των δεδομένων και, κατά συνέπεια, αποτελεί χρήσιμο μέτρο ασφαλείας».

Υπό αυτή την έννοια, **η χρήση κρυπτογραφημένων και κατακερματισμένων τεχνικών** για την αποθήκευση και επεξεργασία δεδομένων σε εφαρμογές που βασίζονται σε blockchain θεωρείται ότι **χαρακτηρίζεται ως συγκεκριμένη μέθοδος ψευδωνυμοποίησης**, λαμβάνοντας υπόψη ότι ένας σημαντικός παράγοντας για τον χαρακτηρισμό των δεδομένων ως ανώνυμων είναι ότι η επεξεργασία των -η ταυτοποίηση ενός φυσικού προσώπου πρέπει να είναι μη αναστρέψιμη. Λαμβάνοντας υπόψη τον ευρύ ορισμό των προσωπικών δεδομένων, οι εφαρμογές που βασίζονται σε blockchain είναι πιθανό να επεξεργάζονται, τουλάχιστον, δύο τύπους προσωπικών δεδομένων: δημόσια κλειδιά και δεδομένα συναλλαγών.

Σε εφαρμογές που βασίζονται σε blockchain, τα δημόσια κλειδιά χρησιμοποιούνται κυρίως για σκοπούς αναγνώρισης, ενώ τα ιδιωτικά κλειδιά χρησιμοποιούνται κυρίως για σκοπούς ελέγχου ταυτότητας και κρυπτογράφησης. Το ζεύγος ιδιωτικού και δημόσιου κλειδιού, που αντιπροσωπεύεται από μια σειρά γραμμάτων και αριθμών, χρησιμοποιείται για την απόκρυψη της πραγματικής ταυτότητας των φυσικών προσώπων. Όπως υποστηρίζει το WP29, η «ψευδωνυμοποίηση είναι η διαδικασία συγκάλυψης ταυτοτήτων. Ο στόχος μιας τέτοιας διαδικασίας είναι να μπορεί να συλλέγει πρόσθετα δεδομένα που αφορούν το ίδιο άτομο χωρίς να χρειάζεται να γνωρίζει την ταυτότητά του». θα μπορούσε να υποστηριχθεί ότι το ζεύγος ιδιωτικού και δημόσιου κλειδιού είναι πιθανό να χαρακτηριστεί ως μέθοδος ψευδωνυμοποίησης, καθώς η ταυτότητα και άλλα προσωπικά δεδομένα δεν μπορούν πλέον να αποδοθούν σε ένα συγκεκριμένο υποκείμενο δεδομένων χωρίς τη χρήση πρόσθετων πληροφοριών. Όπως αναγνωρίζει ρητά το WP29, η χρήση ψευδωνύμου σημαίνει ότι είναι ακόμα δυνατό, υπό ορισμένες συνθήκες, να υποχωρήσουν τα άτομα και να ανακαλύψουν την ταυτότητά τους.

Πράγματι, **υπάρχουν ορισμένες πρακτικές και μέθοδοι για τον προσδιορισμό της ταυτότητας των κατόχων ενός ζεύγους ιδιωτικού και δημόσιου κλειδιού**. Εκτός από την εθελοντική αποκάλυψη του ζεύγους ιδιωτικών και δημόσιων κλειδιών, είναι δυνατός ο εντοπισμός ενός φυσικού προσώπου όταν συλλέγονται πρόσθετες πληροφορίες σύμφωνα με άλλες κανονιστικές απαιτήσεις – όπως είναι το παράδειγμα των καθηκόντων για την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες – και στη συνέχεια, σε συνδυασμό με ότι, το συγκεκριμένο ζεύγος ιδιωτικού και δημόσιου κλειδιού. Στην πλατφόρμα του Bitcoin, είναι επίσης δυνατός ο προσδιορισμός της ταυτότητας ενός υποκειμένου δεδομένων συνδέοντας το δημόσιο κλειδί του με τη διεύθυνση IP του. Το μοτίβο των συναλλαγών μπορεί επίσης να χρησιμοποιηθεί για να ξεχωρίσει ένα συγκεκριμένο υποκείμενο δεδομένων χρησιμοποιώντας την τεχνική «ανάλυση γραφήματος συναλλαγών», η οποία επιτρέπει τον προσδιορισμό της ταυτότητας ενός συγκεκριμένου άγνωστου χρήστη αναλύοντας τη συναλλακτική του δραστηριότητα με έναν γνωστό χρήστη μιας συγκεκριμένης εφαρμογής που βασίζεται σε blockchain. Σε αυτό το πλαίσιο, μπορεί κανείς να υποστηρίξει ότι το ζεύγος ιδιωτικού και δημόσιου κλειδιού θα πρέπει

να θεωρείται ως δεδομένα προσωπικού σύμφωνα με το άρθρο 4 παράγραφος 1 του GDPR, καθώς θα μπορούσε ενδεχομένως να οδηγήσει σε άμεση ή έμμεση ταυτοποίηση σύσταση φυσικού προσώπου.

Σε πολλές περιπτώσεις, το αντικείμενο των συναλλαγών –ή τα δεδομένα συναλλαγών– μπορούν επίσης να θεωρηθούν προσωπικά δεδομένα, καθώς τα δεδομένα αυτού του τύπου μπορούν να συνδεθούν με μια πραγματική ταυτότητα. Εκτός από το ζεύγος ιδιωτικού και δημόσιου κλειδιού, τα δεδομένα συναλλαγής περιλαμβάνουν όλες τις άλλες κατηγορίες δεδομένων που μπορεί να περιέχει μια συναλλαγή. Για παράδειγμα, εάν μια ομάδα τραπεζών χρησιμοποιεί μια εφαρμογή που βασίζεται σε blockchain κοινοπραξίας για να μοιράζεται τις πληροφορίες Know Your Client, τα δεδομένα που περιέχονται σε αυτές τις συναλλαγές θεωρούνται ως προσωπικά δεδομένα, καθώς αυτά τα δεδομένα αφορούν φυσικά πρόσωπα που έχουν ταυτοποιηθεί ή ταυτοποιηθούν. Τα δεδομένα συναλλαγής μπορούν να χρησιμοποιηθούν σε απλό κείμενο, σε κρυπτογραφημένη μορφή ή μπορούν να κατακερματιστούν.

Όταν τα δεδομένα συναλλαγών χρησιμοποιούνται σε απλό κείμενο, που περιέχουν οποιεσδήποτε πληροφορίες που σχετίζονται με ταυτοποιημένο ή αναγνωρίσιμο φυσικό πρόσωπο, δεν υπάρχει αμφιβολία ως προς τον χαρακτηρισμό τους ως προσωπικά δεδομένα.

Όσον αφορά την **κρυπτογράφηση**, όπως περιγράφει σωστά το WP29, είναι μία από τις πιο χρησιμοποιούμενες τεχνικές ψευδωνυμοποίησης. Όπως αναφέρθηκε παραπάνω, αν και αυτή η τεχνική συμβάλλει στη μείωση της δυνατότητας σύνδεσης ενός συγκεκριμένου συνόλου δεδομένων με την ταυτότητα ενός υποκειμένου δεδομένων, είναι μια χρήσιμη ασφάλεια. μέτρο, αλλά δεν μπορεί να θεωρηθεί μέθοδος ανωνυμοποίησης. Πράγματι, ο κάτοχος του ζεύγους ιδιωτικού και δημόσιου κλειδιού μπορεί ακόμα να αναγνωριστεί εκ νέου μέσω των διαδικασιών αποκρυπτογράφησης. Σε αυτό το πλαίσιο, μπορεί κανείς να υποστηρίξει ότι τα προσωπικά δεδομένα εξακολουθούν να αποθηκεύονται σε ένα σύνολο δεδομένων που έχει κρυπτογραφηθεί και, επομένως, τα κρυπτογραφημένα δεδομένα πρέπει να χαρακτηρίζονται ως προσωπικά δεδομένα.

Σε αντίθεση με τη χρήση τεχνικών κρυπτογράφησης, οι **συναρτήσεις κατακερματισμού** δεν μπορούν να αντιστραφούν, πράγμα που σημαίνει ότι όταν τα δεδομένα έχουν τεθεί μέσω ενός αλγόριθμου κατακερματισμού – όπως ο SHA-256 – που έχει μετατρέψει την τιμή εισόδου σε τιμή εξόδου με σταθερό μήκος, Η συνάρτηση κατακερματισμού δεν μπορεί να εκτελεστεί προς τα πίσω. Ωστόσο, αυτό δεν σημαίνει αυτόματα ότι οι συναρτήσεις κατακερματισμού είναι μια μέθοδος ανωνυμοποίησης, καθώς μπορεί ακόμα να βρεθεί η δυνατότητα σύνδεσης μεταξύ ενός συγκεκριμένου συνόλου δεδομένων και της τιμής εξόδου της συνάρτησης κατακερματισμού. Όπως επιβεβαιώνει το WP29, σε περίπτωση που είναι γνωστό το εύρος μιας τιμής εισόδου, μπορεί να αναπαραχθεί ξανά μέσω μιας συνάρτησης κατακερματισμού, προκειμένου να επιτευχθεί η ακριβής τιμή ενός συγκεκριμένου συνόλου δεδομένων. Για τη Michèle Finck, μια μη αναστρέψιμη συνάρτηση κατακερματισμού πρέπει να διασφαλίζει ότι οι πιθανές εισροές είναι αρκετά μεγάλες και απρόβλεπτες για να αποτρέψουν την επιλογή να δοκιμάσουμε όλους τους πιθανούς συνδυασμούς, αλλά όπως αναγνωρίζει ο συγγραφέας, αυτό

είναι δύσκολο να επιτευχθεί, ειδικά αν λάβουμε υπόψη την αυξανόμενη ισχύ και το μειωμένο κόστος των υπολογιστών. Επομένως, σύμφωνα με τη γνώμη του WP29, ο κατακερματισμός θα παράγει δεδομένα με ψευδώνυμα στις περισσότερες περιπτώσεις, ακόμη και όταν χρησιμοποιούνται συναρτήσεις κατακερματισμού με ισχυρότερες εγγυήσεις απορρήτου (π.χ. κ.λπ.).

Θα μπορούσε να υποστηριχθεί ότι η κρυπτογράφηση και οι συναρτήσεις κατακερματισμού είναι συγκεκριμένες μέθοδοι ψευδωνυμοποίησης που δεν αποκλείουν την εφαρμογή του GDPR, λαμβάνοντας υπόψη τη δοκιμή της αιτιολογικής σκέψης 26 και το άρθρο 4 παράγραφοι 1 και 5 του το GDPR.

7. Blockchain και GDPR

7.1. Blockchain και GDPR

Με βάση τα πρόσφατα γεγονότα, τα άτομα συνειδητοποιούν περισσότερο τις απειλές παραβίασης δεδομένων και τη χρήση των προσωπικών τους δεδομένων σχετικά με εμπορικούς σκοπούς. Ο GDPR (Γενικός Κανονισμός για την Προστασία Δεδομένων) επιδιώκει να δημιουργήσει μια εναρμονισμένη νομοθεσία για την προστασία των δεδομένων σε ολόκληρη την Ευρωπαϊκή Ένωση και στοχεύει στην επιστροφή του ελέγχου των προσωπικών δεδομένων στους ίδιους τους κατόχους των δεδομένων. Με τον GDPR, ακόμη και οργανισμοί χωρίς φυσική παρουσία στην ΕΕ ευποχρεώνονται να συμμορφωθούν με τον GDPR εάν ο οργανισμός προσφέρει αγαθά ή υπηρεσίες επί πληρωμή ή μη σε άτομα που βρίσκονται στην ΕΕ ή εάν ο οργανισμός παρακολουθεί τη συμπεριφορά ατόμων εντός της ΕΕ.

Επιπλέον, εάν ένας οργανισμός συνεργάζεται με προμηθευτές ή συνεργάτες που δραστηριοποιούνται στην ΕΕ, θα περιμένουν από τον οργανισμό να συμμορφωθεί με τον GDPR προκειμένου να περιορίσει τον δικό του κίνδυνο. Με απλά λόγια, η συμμόρφωση με τον GDPR θεωρείται ως προϋπόθεση για τη διεξαγωγή συναλλαγών με υποκείμενα δεδομένων της ΕΕ. Με την επιβολή να έχει ξεκινήσει από τις 25 Μαΐου 2018, οι οργανισμοί πρέπει πλέον να λαμβάνουν υπόψη τα βήματα που απαιτούνται για την ετοιμότητα σε ολόκληρο τον οργανισμό τους, που να περιλαμβάνει άτομα, διαδικασίες, δεδομένα και τεχνολογία.

Το Blockchain είναι ένα κοινό, αμετάβλητο λογιστικό βιβλίο για την καταγραφή του ιστορικού των συναλλαγών. Προωθεί μια νέα γενιά εφαρμογών συναλλαγών που συμβάλλουν στη δημιουργία λογοδοσίας και διαφάνειας. Το Blockchain παρέχει ένα απαράμιλλο επίπεδο λογοδοσίας για τον τρόπο διαχείρισης των δεδομένων με βάση την ανθεκτική αποθήκευση δεδομένων και τον μηχανισμό συναίνεσης που χρησιμοποιείται για την τροποποίηση των δεδομένων. Κατά βάση, τα δεδομένα blockchain προστατεύονται από το σχεδιασμό (privacy by design). Το Blockchain δεν είναι ακόμα

ευρέως διαδεδομένο σε τομείς πέρα από τα κρυπτονομίσματα, αλλά διαθέτει αξιόλογα δίκτυα που παρέχουν ήδη αξία, όπως η ασφάλεια των τροφίμων και το παγκόσμιο εμπόριο.

Ενώ το blockchain και το GDPR ξεκίνησαν με πολύ διαφορετικούς στόχους - τη δημιουργία ενός νομίσματος ανεξάρτητου από μια κεντρική αρχή έναντι της εισαγωγής νόμων περί απορρήτου δεδομένων - οι δύο πρωτοβουλίες ευθυγραμμίζονται με τις αρχές των ασφαλών και αυτοκυριαρχικών δεδομένων (άτομα που είναι υπεύθυνα για τα δεδομένα τους). Για παράδειγμα, το Ίδρυμα Αποκεντρωμένης Ταυτότητας που ανακοινώθηκε πρόσφατα καθορίζει τους πυλώνες για αποκεντρωμένες ταυτότητες που στηρίζονται στο blockchain.

Τα τελευταία δύο χρόνια, το blockchain αναδύθηκε και δημιούργησε αξία σε τομείς όπως η εφοδιαστική αλυσίδα, η προέλευση, η συμμόρφωση, η ασφάλεια των τροφίμων και η ψηφιακή ταυτότητα. Το Blockchain προσθέτει υπευθυνότητα και διαφάνεια για τους συμμετέχοντες που εμπλέκονται στην αλυσίδα αξίας, διατηρώντας παράλληλα το απόρρητο και την εμπιστευτικότητα. Το πιο σημαντικό, το blockchain μπορεί να βοηθήσει στην άρση των σημείων τριβής που υπήρχαν στις παραδοσιακές επιχειρηματικές διαδικασίες. Το blockchain δεν αποτελεί λύση για όλες τις προκλήσεις του GDPR, αλλά μπορεί να θεωρηθεί ως ένας μηχανισμός που βοηθά στον έλεγχο της χρήσης προσωπικών δεδομένων.

7.2. Νομικές εντάσεις μεταξύ της τεχνολογίας blockchain και του GDPR

Ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR) της Ευρωπαϊκής Ένωσης τέθηκε σε ισχύ τον Μάιο του 2016 και έγινε νομικά δεσμευτικός τον Μάιο του 2018, αντικαθιστώντας την Οδηγία για την Προστασία Δεδομένων του 1995. Ο GDPR θεσπίζει ένα ομοιογενές νομοθετικό πλαίσιο σε όλη την Ευρωπαϊκή Ένωση, διασφαλίζοντας προστασία υψηλού επιπέδου των φυσικών προσώπων και την άρση των εμποδίων στη ροή δεδομένων προσωπικού χαρακτήρα μεταξύ όλων των κρατών μελών.

Ο GDPR είναι ένα καινοτόμο νομικό πλαίσιο που άλλαξε τον τρόπο με τον οποίο γίνεται αντιληπτή η προστασία των δεδομένων και ο τρόπος με τον οποίο η επεξεργασία των δεδομένων προσωπικού χαρακτήρα πρέπει να ρυθμίζεται από το νόμο. Η μεταρρύθμιση του νομικού πλαισίου της Ευρωπαϊκής Ένωσης για την προστασία δεδομένων έχει επηρεάσει τη χρήση και την ανάπτυξη νέων τεχνολογιών όπως το blockchain. Σε αυτό το πλαίσιο, εμφανίζεται μια κοινή κριτική μεταξύ των συντακτών προστασίας δεδομένων, οι οποίοι βεβαιώνουν ότι ο Ευρωπαίος νομοθέτης δεν έχει λάβει δεόντως υπόψη την εμφάνιση νέων τεχνολογιών, ιδίως τεχνολογιών που ήταν υπό ανάπτυξη κατά την επεξεργασία του σχεδίου GDPR.

Στην πραγματικότητα, έχουν εντοπιστεί αρκετές εντάσεις μεταξύ GDPR και blockchain, αποκαλύπτοντας τη δυσκολία που έχει το GDPR στο να συμβαδίσει με την τεχνολογία blockchain. Με την επιφύλαξη άλλων παραγόντων, οι εντάσεις μεταξύ GDPR και blockchain εμφανίζονται σε δύο βασικά επίπεδα: πρώτον, ο GDPR σιωπηρά προϋποθέτει ότι τα δεδομένα ελέγχονται ή υποβάλλονται σε επεξεργασία από αναγνωρίσιμους φορείς· και δεύτερον, προϋποθέτει επίσης ότι τα προσωπικά δεδομένα των υποκειμένων των δεδομένων μπορούν να διορθωθούν ή να διαγραφούν σε κάθε περίπτωση, προκειμένου να συμμορφωθούν με τις νομικές απαιτήσεις που ορίζονται στα άρθρα 16 και 17 του GDPR.

7.3. Δυνατότητα εφαρμογής του GDPR σε πλατφόρμες που βασίζονται σε Blockchain

Λαμβάνοντας υπόψη τον στόχο της διασφάλισης συνεπούς και ομοιογενούς προστασίας των φυσικών προσώπων όσον αφορά την επεξεργασία των προσωπικών τους δεδομένων, το υλικό και εδαφικό πεδίο εφαρμογής του GDPR είναι ευρύ, καλύπτοντας ένα ευρύ φάσμα περιπτώσεων που περιλαμβάνουν επίσης τις δραστηριότητες επεξεργασίας δεδομένων που λαμβάνουν χώρα εκτός της επικράτειας της Ευρωπαϊκής Ένωσης.

Όσον αφορά το εδαφικό του πεδίο εφαρμογής, το άρθρο 3 παράγραφος 1 του GDPR ορίζει ότι ο κανονισμός ισχύει για όλους τους υπεύθυνους επεξεργασίας και επεξεργασίας δεδομένων που είναι εγκατεστημένοι στην Ευρωπαϊκή Ένωση, ανεξάρτητα από το αν η επεξεργασία πραγματοποιείται στην Ένωση ή όχι. Η αιτιολογική σκέψη του GDPR διευκρινίζει ότι η ίδρυση υπεύθυνου επεξεργασίας ή εκτελούντος την επεξεργασία «συνεπάγεται την αποτελεσματική και πραγματική

άσκηση δραστηριότητας μέσω σταθερών ρυθμίσεων», γεγονός που υποδηλώνει ότι η έννοια της εγκατάστασης δεν περιορίζεται στα τυπικά στοιχεία της, αλλά, αντιθέτως, περιλαμβάνει λειτουργικά στοιχεία επίσης. Σε συμφωνία με αυτή την προσέγγιση είναι η νομολογία του Ευρωπαϊκού Δικαστηρίου (ΔΕΚ), το οποίο εξήγησε ότι «ο βαθμός σταθερότητας των ρυθμίσεων και η αποτελεσματική άσκηση των δραστηριοτήτων πρέπει να ερμηνευθεί υπό το πρίσμα της ειδικής φύσης των σχετικών οικονομικών δραστηριοτήτων και της παροχής υπηρεσιών». Είναι πιθανό το εδαφικό πεδίο εφαρμογής του GDPR να εκπληρωθεί για το μεγαλύτερο μέρος των παρόχων blockchain που είναι εγκατεστημένοι στην Ένωση, εκτός εάν ισχύει η εξαίρεση των νοικοκυριών σύμφωνα με το άρθρο 2 παράγραφος 2 στοιχείο γ) του GDPR.

Σε περίπτωση που το κριτήριο θέσπισης δεν ενεργοποιεί την εφαρμογή του GDPR, το άρθρο 2 στοιχεία α) και β) του GDPR επεκτείνει το εδαφικό του πεδίο εφαρμογής σε υπευθύνους επεξεργασίας δεδομένων και εκτελούντες την επεξεργασία που δεν είναι εγκατεστημένοι στην Ένωση, όπου οι δραστηριότητες επεξεργασίας σχετίζονται με την προσφορά αγαθών ή υπηρεσιών προς τα υποκείμενα των δεδομένων που βρίσκονται στην Ένωση, και την παρακολούθηση της συμπεριφοράς των υποκειμένων των δεδομένων, εφόσον η συμπεριφορά τους λαμβάνει χώρα εντός της Ένωσης.

Λόγω του ευρέος εδαφικού του πεδίου, ο GDPR είναι πολύ πιθανό να εφαρμοστεί σε ένα ευρύ φάσμα πλατφορμών που βασίζονται σε blockchain και στους χειριστές του. Για παράδειγμα, ο GDPR θα ισχύει σε σχέση με όλους τους φορείς εκμετάλλευσης blockchain που είναι εγκατεστημένοι εκτός της επικράτειας της Ένωσης, όποτε προσφέρουν υπηρεσίες σε υποκείμενα δεδομένων που βρίσκονται στην Ένωση. Με τον ίδιο τρόπο, οι χειριστές ανοιχτών και χωρίς άδεια πλατφορμών που βασίζονται σε blockchain υπόκεινται επίσης σε συμμόρφωση με τους κανόνες GDPR, καθώς θα μπορούσε να υποστηριχθεί ότι αυτοί οι τύποι πλατφορμών προσφέρουν υπηρεσίες σε υποκείμενα δεδομένων που βρίσκονται στην Ένωση. Αυτή είναι η περίπτωση του Bitcoin, μιας πλατφόρμας που προσφέρει ηλεκτρονική μέθοδο πληρωμής στα υποκείμενα των δεδομένων στην Ένωση.

Σύμφωνα με το άρθρο 2 παράγραφος 1 του GDPR, ο κανονισμός εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα εν όλω ή εν μέρει με αυτοματοποιημένα μέσα, καθώς και στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που βασίζεται σε μη αυτοματοποιημένα μέσα, αλλά αποτελεί μέρος ή προορίζεται να είναι μέρος ενός συστήματος πλήρωσης. Σύμφωνα με το άρθρο 4 παράγραφος 2 του GDPR, επεξεργασία προσωπικών δεδομένων είναι «κάθε λειτουργία ή σύνολο λειτουργιών που εκτελείται σε προσωπικά δεδομένα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, είτε με αυτοματοποιημένα μέσα είτε όχι». Ο γενικός ορισμός της «επεξεργασίας» περιλαμβάνει τη «συλλογή, καταγραφή, οργάνωση, δομή, αποθήκευση, προσαρμογή ή τροποποίηση, ανάκτηση, διαβούλευση, χρήση, αποκάλυψη μέσω μετάδοσης, διάδοσης ή με άλλο τρόπο διάθεσης, ευθυγράμμιση ή συνδυασμό, περιορισμό, διαγραφή ή καταστροφή». των προσωπικών δεδομένων. Ωστόσο, σύμφωνα με τη νομολογία του, ιδίως στην υπόθεση Bodil Lindqvist, το Ευρωπαϊκό Δικαστήριο παρατήρησε ότι πρόκειται απλώς για παραδείγματα επεξεργασίας δεδομένων προσωπικού χαρακτήρα, καθώς η έννοια της «επεξεργασίας» προορίζεται να ερμηνεύεται ευρέως.

Σε αυτό το πλαίσιο, μπορεί κανείς να υποστηρίξει ότι οι κύριες λειτουργίες των πλατφορμών που βασίζονται σε blockchain είναι ακριβώς η μετάδοση, αποθήκευση και καταγραφή προσωπικών δεδομένων με αυτοματοποιημένα μέσα. Για αυτόν τον λόγο, θα μπορούσε να ειπωθεί ότι οι συμμετέχοντες στο blockchain ασχολούνται αναμφίβολα με την επεξεργασία προσωπικών δεδομένων, η οποία ενεργοποιεί την εφαρμογή του GDPR, εκτός ισχύει κάποια εξαίρεση.

7.4. Blockchain και δικαιώματα των υποκειμένων των δεδομένων στην ΕΕ

Ο GDPR θα δώσει στα άτομα καλύτερο έλεγχο των προσωπικών τους δεδομένων (οποιαδήποτε πληροφορία που σχετίζεται με ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο) και θα θεσπίσει έναν ενιαίο κανονισμό προστασίας δεδομένων σε όλη την ΕΕ: ευκολότερη πρόσβαση στα προσωπικά δεδομένα, δικαίωμα διόρθωσης, σαφέστερο δικαίωμα διαγραφής («δικαίωμα στη λήθη»), ένα νέο δικαίωμα στη φορητότητα των δεδομένων, δικαίωμα συναίνεσης και δικαίωμα ενημέρωσης για παραβίαση προσωπικών δεδομένων όταν αυτή η παραβίαση έχει δυνητικά μεγάλο αντίκτυπο στα δικαιώματα και τις ελευθερίες κάποιου. Η κατοχή προσωπικών δεδομένων σε πολλά μέρη για τον ίδιο σκοπό καθιστά δύσκολη την επιβολή αυτών των δικαιωμάτων. Οι λύσεις που βασίζονται στο blockchain μπορούν να σας βοηθήσουν να απλοποιήσετε καθώς εκπληρώνετε αυτούς τους κανόνες.

Η εφαρμογή ενός κοινόχρηστου blockchain "Know Your Customer" (KYC) βοηθά τις εταιρείες καθώς ικανοποιούν την απαίτηση φορητότητας δεδομένων (επιτρέποντας στα άτομα να αποκτούν και να επαναχρησιμοποιούν τα προσωπικά τους δεδομένα για δικούς τους σκοπούς σε διάφορες υπηρεσίες). Για παράδειγμα, η Crédit Mutuel Arkéa δημιούργησε ένα δίκτυο blockchain με άδεια λειτουργίας που παρέχει μια άποψη της ταυτότητας του πελάτη για να επιτρέψει τη συμμόρφωση με τις απαιτήσεις του KYC. Το πιλοτικό προσφέρει μια πλήρη εικόνα των εγγράφων των πελατών σε όλο το κατανεμημένο δίκτυο της τράπεζας [IBM2017].

Σύμφωνα με την International Airlines Group, οι ταξιδιώτες είναι μόνο 50 τοις εκατό ακριβείς όταν συμπληρώνουν τις πληροφορίες που απαιτούνται για να πετάξουν. Αυτό μπορεί να διορθωθεί με διαδικασίες στο αεροδρόμιο, αλλά αυτές προσθέτουν χρόνο, πολυπλοκότητα και τριβή, δημιουργώντας μια κακή ταξιδιωτική εμπειρία. Για να αντιμετωπίσει αυτές τις προκλήσεις, η VEChain Tech ανέπτυξε μια λύση, η οποία χρησιμοποίησε το blockchain για να παρέχει ψηφιακή ταυτότητα ως υπηρεσία για να βοηθήσει τις αεροπορικές εταιρείες να μοιράζονται δεδομένα με ασφάλεια όταν επιβάτες επιβιβάζονται σε πτήσεις ανταπόκρισης [VECHAIN2019]. Το Blockchain θα παρέχει μια ψηφιακή επαλήθευση των δεδομένων των επιβατών για αεροπορικές εταιρείες χωρίς έκθεση δεδομένων.

Τα παραπάνω παραδείγματα δείχνουν τη δυνατότητα εφαρμογής του blockchain για την υποστήριξη των δικαιωμάτων GDPR των υποκειμένων των δεδομένων. Ορισμένες προειδοποιήσεις, ωστόσο, θα πρέπει να εφαρμόζονται κατά τη χρήση του blockchain. Το Blockchain είναι ένα σύστημα «μόνο προσάρτησης» και η αμεταβλητότητα είναι βασικό και

επιθυμητό χαρακτηριστικό της αρχιτεκτονικής. Έχοντας αυτό υπόψη, μια εταιρεία που πρέπει να συμμορφωθεί με το «δικαίωμα διαγραφής» του GDPR μπορεί να αμφισβητηθεί. Για τη συμμόρφωση με το δικαίωμα διαγραφής, τα προσωπικά δεδομένα θα πρέπει να διατηρούνται ιδιωτικά από το blockchain σε ένα κατάστημα δεδομένων «εκτός αλυσίδας», με μόνο τα αποδεικτικά στοιχεία του (κρυπτογραφικό κατακερματισμό) εκτεθειμένα στην αλυσίδα. Χρησιμοποιώντας αυτήν την τεχνική, τα προσωπικά δεδομένα μπορούν να διαγραφούν όταν χρειάζεται χωρίς περαιτέρω επιπτώσεις. Η αμετάβλητη αλυσίδα μπλοκ μπορεί να χρησιμοποιηθεί για να βοηθήσει στην εφαρμογή της διαχείρισης συναίνεσης και να αποδείξει τη συμμόρφωση με την καθορισμένη διαδικασία της εταιρείας και να βοηθήσει στην επιβολή του δικαιώματος διαγραφής.

Ένα άλλο θέμα που πρέπει να εξεταστεί συνοψίζεται στην ερώτηση: ποιος είναι ο Υπεύθυνος Προστασίας Δεδομένων (Data Protection Officer -- DPO) των συλλεγόμενων προσωπικών δεδομένων; Σε πολλές περιπτώσεις, οι εταιρείες δημιουργούν κοινοπραξίες (μια ξεχωριστή νομική οντότητα) για την ιδιοκτησία και τη διαχείριση της λύσης blockchain. Αυτό το θέμα δεν πρέπει να υποτιμάται κατά τη σύναψη της συμφωνίας μεταξύ διαφορετικών μερών. Και, όπως θα εξηγήσουμε, δεν θα πρέπει να αποθηκεύονται προσωπικά δεδομένα στο ίδιο το blockchain.

7.5. Ασφάλεια επεξεργασίας στο Blockchain

Σύμφωνα με το άρθρο 32 του GDPR, οι υπεύθυνοι επεξεργασίας και οι υπεύθυνοι επεξεργασίας δεδομένων υποχρεούνται να εφαρμόζουν «κατάλληλα τεχνικά και οργανωτικά μέτρα για να διασφαλίσουν ένα επίπεδο ασφάλειας κατάλληλο για τον κίνδυνο...» Ειδικότερα, το άρθρο αυτό αναφέρεται στον κίνδυνο βλάβης του υποκειμένου των δεδομένων, μαζί με ένα σύνολο παραδειγμάτων και κατευθυντήριων γραμμών για την εφαρμογή της ασφάλειας των προσωπικών δεδομένων, όπως η ψευδωνυμοποίηση και η κρυπτογράφηση, η εμπιστευτικότητα, η ακεραιότητα, η διαθεσιμότητα και η ανθεκτικότητα των συστημάτων και υπηρεσιών. Στη συνέχεια δηλώνει ότι η τυχαία ή παράνομη καταστροφή, απώλεια, τροποποίηση, μη εξουσιοδοτημένη αποκάλυψη ή πρόσβαση θα πρέπει επίσης να λαμβάνεται υπόψη όταν λαμβάνεται υπόψη το κατάλληλο επίπεδο ασφάλειας ανάλογα με τον κίνδυνο.

Το GDPR σχεδιάστηκε για να είναι τεχνολογικά αγνωστικιστικό και αρκετά ευέλικτο ώστε να επιτρέπει καινοτομίες όπως το blockchain. Πιστεύουμε ότι πολλές από τις εγγενείς δυνατότητες του blockchain προσφέρονται για την υποστήριξη της ασφάλειας της επεξεργασίας, καλύπτοντας την τριάδα ασφάλειας πληροφοριών εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας. Το Blockchain χρησιμοποιεί κρυπτογραφία για να υποστηρίξει το απόρρητο των συναλλαγών μαζί με ελέγχους πρόσβασης για να αποτρέψει τη μη εξουσιοδοτημένη χρήση. Επιπλέον, δεδομένου ότι τα δεδομένα δεν αποθηκεύονται κεντρικά όλα σε ένα μέρος, μπορούμε να περιορίσουμε τον κίνδυνο να έχουμε ένα κεντρικό honeypot για να στοχεύουν οι επιτιθέμενοι. Οι δυνατότητες του blockchain περιλαμβάνουν ίχνη ελέγχου και ιχνηλασιμότητα, τη χρήση μηχανισμών συναίνεσης για τη δέσμευση συναλλαγών και την αμετάβλητη συναλλαγή. Ομοίως, το blockchain μπορεί να βελτιώσει τη διαθεσιμότητα εξαλείφοντας μεμονωμένα σημεία αποτυχίας. Το καθολικό και η εκτέλεση της έξυπνης σύμβασης διανέμονται και εάν δεν είναι διαθέσιμος ένας κόμβος, το δίκτυο μπορεί να συνεχίσει να λειτουργεί και τα δεδομένα είναι ακόμα προσβάσιμα.

Το SecureKey αξιοποιεί το blockchain για την υλοποίηση ενός δικτύου επαλήθευσης ταυτότητας στον Καναδά. Ως καταναλωτής, μπορεί κανείς να χρησιμοποιήσει το δίκτυο για να επαληθεύσει την ταυτότητά του όταν αγοράζει αγαθά ή υπηρεσίες. Τα χαρακτηριστικά ταυτότητας κάποιου διανέμονται σε όλο το δίκτυο blockchain αντί να βρίσκονται όλα σε ένα μέρος. Η εμπιστευτικότητα υποστηρίζεται από το blockchain μέσω "triple blind": ο πάροχος χαρακτηριστικών ταυτότητας δεν γνωρίζει σε ποιον παρέχει τα χαρακτηριστικά. ο καταναλωτής δεν γνωρίζει ποιος παρείχε το χαρακτηριστικό· και το SecureKey δεν γνωρίζει για την ανταλλαγή χαρακτηριστικών. Επίσης, με αυτό το δίκτυο, ο καταναλωτής είναι υπεύθυνος για την ταυτότητά του και αποφασίζει ποια χαρακτηριστικά ταυτότητας μοιράζεται, πότε τα μοιράζεται και με ποιον τα μοιράζεται. Αυτό αναφέρεται ως ταυτότητα αυτοκυριαρχίας.

Το B3i είναι μια κοινοπραξία αφιερωμένη στην ανάπτυξη πλατφορμών συναλλαγών σε ολόκληρη την ασφαλιστική αλυσίδα αξίας χρησιμοποιώντας τεχνολογίες που βασίζονται σε blockchain [B3I2019]. Κάθε οργανισμός-μέλος του B3i έχει ένα ιδιωτικό βιβλίο για την αποθήκευση των δικών του στοιχείων και δεδομένων ασφαλιστικής σύμβασης. Στη

συνέχεια, όλοι οι οργανισμοί συμμετέχουν επίσης σε δύο κοινόχρηστα καθολικά: Το κοινό βασικό καθολικό δεδομένων περιέχει κοινά και συμφωνημένα κύρια δεδομένα, συμπεριλαμβανομένων πληροφοριών δημόσιας εταιρείας και ρήτρες κοινών συμβολαίων. Το κοινόχρηστο καθολικό επικοινωνίας είναι κρυπτογραφικά ασφαλισμένο και αποθηκεύει την επικοινωνία που χρησιμοποιείται για την παροχή συναίνεσης σχετικά με την κατάσταση των λογιστικών βιβλίων του ιδιωτικού οργανισμού. Μόνο οι αντισυμβαλλόμενοι μπορούν να δουν το περιεχόμενο και τον προορισμό της επικοινωνίας.

Παρά το γεγονός ότι το blockchain είναι αμετάβλητο από το σχεδιασμό, εξακολουθούν να υπάρχουν κίνδυνοι για την ασφάλεια ακόμη και με ιδιωτικά δίκτυα blockchain με άδεια. Για παράδειγμα, μια ευάλωτη εφαρμογή που συνδέεται με το δίκτυο εξακολουθεί να έχει τη δυνατότητα μη εξουσιοδοτημένης πρόσβασης στο καθολικό, είτε απευθείας στον δίσκο της είτε μέσω του δικτύου. Ως εκ τούτου, οι οργανισμοί πρέπει να περιορίζουν και να παρακολουθούν την πρόσβαση στο δίκτυο και να αποτρέπουν τη μη εξουσιοδοτημένη πρόσβαση. Τα κλειδιά κρυπτογράφησης θα μπορούσαν επίσης να παραβιαστούν ή ακόμα και να χαθούν ή να κλαπούν, εμποδίζοντας την πρόσβαση. Τέλος, η ταυτότητα των συμμετεχόντων στο blockchain πρέπει να επαληθευτεί για να αποτραπεί η μίμηση έγκυρων χρηστών από τους φορείς απειλής. Η χρήση συγκεκριμένων αρχιτεκτονικών blockchain όπως το Hyperledger και πλατφορμών όπως η πλατφόρμα IBM Blockchain βοηθά στον μετριασμό των κινδύνων.

7.6. Blockchain, Νομιμότητα και Συναίνεση

Σύμφωνα με τους όρους του GDPR, η επεξεργασία προσωπικών δεδομένων επιτρέπεται μόνο εάν υπάρχει νόμιμη βάση για τέτοια επεξεργασία. Μια τέτοια νόμιμη βάση είναι η συγκατάθεση του υποκειμένου των δεδομένων σε τέτοια επεξεργασία. Η διασφάλιση της συναίνεσης των υποκειμένων των δεδομένων πριν από την επεξεργασία των δεδομένων τους θα γίνει πιθανότατα πολύ πιο δύσκολη από ό,τι στο παρελθόν. Για να θεωρηθεί έγκυρη η συγκατάθεση πρέπει να δίνεται ελεύθερα, συγκεκριμένη, ενημερωμένη και ξεκάθαρη. Σε περιπτώσεις όπως η υγειονομική περίθαλψη, όπου είναι πιο πιθανό να γίνει χειρισμός ειδικών κατηγοριών προσωπικών δεδομένων, πρέπει επίσης να είναι ρητή. Περιπλέκοντας περαιτέρω τα ζητήματα, η συγκατάθεση μπορεί να ανακληθεί από το υποκείμενο των δεδομένων ανά πάσα στιγμή.

Το Blockchain μπορεί να χρησιμοποιηθεί για την παρακολούθηση και τη διαχείριση της συναίνεσης μεταξύ των υποκειμένων των δεδομένων, των υπευθύνων επεξεργασίας και των ελεγκτών. Η αναπαραγωγιμότητα, η κοινή χρήση δεδομένων, οι ανησυχίες για το απόρρητο των προσωπικών δεδομένων και η εγγραφή ασθενών σε κλινικές δοκιμές αποτελούν τεράστιες ιατρικές προκλήσεις για τη σύγχρονη κλινική έρευνα. Η APHP και η Inserm διερεύνησαν πώς μια ροή εργασίας συναίνεσης με δυνατότητα blockchain θα επέτρεπε τη συλλογή της ενημερωμένης συγκατάθεσης των ασθενών στο πλαίσιο κλινικών δοκιμών. Διαπίστωσαν ότι η τεχνολογία εξασφαλίζει λεπτομερή έλεγχο των δεδομένων, της ασφάλειάς τους και των παραμέτρων που μπορούν να κοινοποιηθούν, για έναν ασθενή ή ομάδα ασθενών ή ενδιαφερόμενους φορείς κλινικών δοκιμών.

Ομοίως, η IBM Watson Health έχει υπογράψει μια ερευνητική πρωτοβουλία με τον Οργανισμό Τροφίμων και Φαρμάκων (FDA) με στόχο τον καθορισμό μιας ασφαλούς, αποτελεσματικής και επεκτάσιμης ανταλλαγής δεδομένων υγείας χρησιμοποιώντας τεχνολογία blockchain. Η IBM και ο FDA διερευνούν την ανταλλαγή δεδομένων που διαμεσολαβούνται από τον ιδιοκτήτη από διάφορες πηγές, όπως ηλεκτρονικά ιατρικά αρχεία (EMR), κλινικές δοκιμές, γονιδιωματικά δεδομένα και δεδομένα υγείας από κινητές συσκευές, φορητές συσκευές και το Διαδίκτυο των πραγμάτων. Διατηρώντας μια διαδρομή ελέγχου όλων των συναλλαγών σε ένα αμετάβλητο κατανεμημένο καθολικό, η τεχνολογία blockchain θα δημιουργήσει υπευθυνότητα και διαφάνεια στη διαδικασία ανταλλαγής δεδομένων.

Όπως αναφέρθηκε προηγουμένως, δεν πρέπει να αποθηκεύονται προσωπικά δεδομένα στο blockchain.

7.7. Λογοδοσία συμμόρφωσης στο Blockchain

Ως υπεύθυνος επεξεργασίας ή εκτελών την επεξεργασία δεδομένων, ένας οργανισμός πρέπει να είναι σε θέση να αποδείξει τη συμμόρφωση με τις υποχρεώσεις του GDPR — ή τουλάχιστον να τεκμηριώσει πως προχωρά προς τη συμμόρφωση. Τα βήματα για την επίτευξη συμμόρφωσης μπορεί να περιλαμβάνουν εκτιμήσεις κινδύνου, εκτιμήσεις επιπτώσεων στην προστασία δεδομένων, καθιέρωση μοντέλου διακυβέρνησης και κώδικα δεοντολογίας σε επίπεδο επιχείρησης και σχεδιασμό και εφαρμογή συστήματος τήρησης αρχείων που επισημοποιεί και τεκμηριώνει τα εφαρμοσμένα μέτρα προστασίας δεδομένων και έλεγχο μονοπάτια.

Με την παραδοσιακή τήρηση αρχείων, οι πληροφορίες μπορούν να συλλεχθούν, να μην είναι επαληθεύσιμες και να ξεπεραστούν γρήγορα. Αυτά τα χαρακτηριστικά καθιστούν τα δεδομένα αναξιόπιστα και σαφώς μη διορατικά. Η χρήση του blockchain προσφέρει την ευκαιρία να αυξηθεί το επίπεδο λογοδοσίας και διορατικότητας στα δεδομένα και να βοηθήσει μια εταιρεία να αποδείξει τη συμμόρφωση με συγκεκριμένους κανονισμούς.

Το Blockchain έχει τεθεί σε λειτουργία για να ενεργοποιήσει δυνατότητες προέλευσης δεδομένων, όπως η ασφάλεια των τροφίμων. Η προέλευση της παρακολούθησης είναι δυνατή επειδή το blockchain όχι μόνο παρακολουθεί την τρέχουσα κατάσταση των δεδομένων («παγκόσμια κατάσταση»), αλλά και όλες τις αλλαγές που έχουν γίνει ποτέ στο καθολικό (την αλυσίδα των μπλοκ). Επιπλέον, χάρη στον μηχανισμό συναίνεσης του blockchain, τα δεδομένα στο blockchain μπορούν να αλλάξουν μόνο όταν οι βασικοί συμμετέχοντες με μερίδιο στα δεδομένα καταλήξουν σε συναίνεση.

Δεν αποτελεί έκπληξη ότι οι ρυθμιστικές αρχές του κλάδου έχουν έντονο ενδιαφέρον για το blockchain, όπως είναι προφανές στον τομέα των χρηματοπιστωτικών υπηρεσιών. Για παράδειγμα, στις κεφαλαιαγορές, η Northern Trust χρησιμοποίησε το blockchain για να ψηφιοποιήσει τον παραδοσιακά χειροκίνητο και βαρύ κόσμο της διαχείρισης ιδιωτικών επενδυτικών κεφαλαίων. Η Επιτροπή Χρηματοοικονομικών Υπηρεσιών του Guernsey με έδρα το Ηνωμένο

Βασίλειο ήταν ένας από τους συμμετέχοντες στην κατασκευή του Minimal Viable Product (MVP). Αντί να βασίζονται σε έντυπες αναφορές, το blockchain τους έδωσε άμεση και σχεδόν σε πραγματικό χρόνο πρόσβαση στα δεδομένα του καθολικού που έπρεπε να δουν.

Όταν αντιμετωπίζουμε δυνητικά χιλιάδες κανονισμούς και εκατομμύρια αρχεία που πρέπει να τηρούνται σύμφωνα με τον GDPR, η αυτοματοποίηση είναι ζωτικής σημασίας. Εδώ μπορούν να βοηθήσουν οι δυνατότητες έξυπνων συμβάσεων του blockchain. Για παράδειγμα, η Everledger Ltd. χρησιμοποιεί blockchain για να παρακολουθεί την προέλευση αγαθών υψηλής αξίας, όπως τα διαμάντια.

Συγκεκριμένα, πήρε τις υποχρεώσεις του εμπορίου διαμαντιών από τη διαδικασία Kimberley των Ηνωμένων Εθνών και τις κωδικοποίησε ως έξυπνα συμβόλαια blockchain. Αυτή η λύση επιτρέπει στα διαμάντια που διαχειρίζεται το blockchain να ελέγχονται αυτόματα για συμμόρφωση — και να ενεργοποιούνται ειδοποιήσεις ή ροές εργασίας ως αποτέλεσμα συμβάντος μη συμμόρφωσης. Για τον GDPR, μια παρόμοια έννοια θα μπορούσε να χρησιμοποιηθεί για τη διαχείριση συμφωνιών υπευθύνου επεξεργασίας/εκτελών την επεξεργασία με μια τεκμηριωμένη αλυσίδα όρων συμβολαίου.

Σε αυτήν την ενότητα, χρησιμοποιήσαμε παραδείγματα έργων blockchain για να δείξουμε πώς το blockchain εφαρμόζεται στη λογοδοσία του GDPR ως προς τη συμμόρφωση. Συγκεκριμένα, κάναμε τους ακόλουθους τρεις ισχυρισμούς:

- Τα χαρακτηριστικά προέλευσης και συναίνεσης του Blockchain συμβάλλουν στη δημιουργία λογοδοσίας και αμετάβλητης.
- Το blockchain βοηθά στη βελτίωση της διαφάνειας.
- Τα έξυπνα συμβόλαια blockchain βοηθούν τις εταιρείες καθώς αυτοματοποιούν τους ελέγχους συμμόρφωσης.

7.8. Προστασία δεδομένων από σχεδιασμό και από προεπιλογή

Ο GDPR απαιτεί να σχεδιαστεί η προστασία δεδομένων για την ανάπτυξη επιχειρηματικών διαδικασιών για προϊόντα και υπηρεσίες. Συγκεκριμένα, οι ρυθμίσεις απορρήτου πρέπει να ορίζονται σε υψηλό επίπεδο από προεπιλογή και ο υπεύθυνος επεξεργασίας θα πρέπει να διαθέτει τεχνικά, διαδικαστικά και οργανωτικά μέτρα προκειμένου να αποδείξει τη συμμόρφωση με τον κανονισμό GDPR. Οι υπεύθυνοι επεξεργασίας θα πρέπει επίσης να εφαρμόζουν μηχανισμούς για να διασφαλίζουν ότι τα προσωπικά δεδομένα υφίστανται επεξεργασία μόνο όταν είναι απαραίτητο για κάθε συγκεκριμένο σκοπό. Η ψευδωνυμοποίηση και η κρυπτογράφηση των προσωπικών δεδομένων είναι βασικές τεχνολογίες που προσδιορίζονται στον κανονισμό για να βοηθήσουν στην επίτευξη αυτού του στόχου. Βασισμένο σε προηγμένες τεχνολογίες κρυπτογράφησης, το blockchain μπορεί να βοηθήσει στην εφαρμογή λύσεων συμβατών με τον GDPR.

Το Εσθονικό Ίδρυμα eHealth έφερε επανάσταση στο σύστημα υγειονομικής περίθαλψης με καινοτόμες λύσεις: οι ασθενείς, οι γιατροί, τα νοσοκομεία και η κυβέρνηση επωφελούνται από την άνετη πρόσβαση και την εξοικονόμηση πόρων που προσφέρουν αυτές οι υπηρεσίες. Κάθε άτομο στην Εσθονία που έχει επισκεφθεί γιατρό έχει ένα ηλεκτρονικό αρχείο υγείας που μπορεί να παρακολουθηθεί. Προκειμένου να διατηρούνται οι πληροφορίες υγείας απόλυτα ασφαλείς και ταυτόχρονα προσβάσιμες σε εξουσιοδοτημένα άτομα, το σύστημα ηλεκτρονικής ταυτότητας χρησιμοποιεί τεχνολογία blockchain που παρέχεται από την Guardtime για τη διασφάλιση της ακεραιότητας των δεδομένων και τον μετριασμό των εσωτερικών απειλών για τα δεδομένα.

Κάθε αρχείο αποθηκευμένων δεδομένων συνοδεύεται από ανεξάρτητη απόδειξη ότι τα δεδομένα είναι στην αρχική τους κατάσταση και δεν έχουν υποστεί χειραγώγηση, επομένως καθίσταται δυνατή η παροχή μιας ανεξάρτητης διαδρομής ελέγχου εγκληματολογικής ποιότητας για τον κύκλο ζωής των αρχείων ασθενών. Πιστεύουμε ότι αυτό παρέχει αυξημένη ασφάλεια σε μια χώρα που βρίσκεται υπό σκληρή πίεση από επιθέσεις στον κυβερνοχώρο, και έχει ανάγκη από διαφάνεια, δυνατότητα ελέγχου και ρύθμισης ηλεκτρονικών συστημάτων και διαχείρισης κύκλου ζωής πάνω από ένα εκατομμύριο αρχεία ασθενών.

Η Stampery λειτουργεί ως ψηφιακός συμβολαιογράφος, δεσμεύει και εγγυάται επιχειρηματικές συμβάσεις, διαθήκες και πνευματική ιδιοκτησία [STAMPERY2015]. Η Stampery αξιοποιεί την τεχνολογία blockchain για να εξασφαλίσει την ύπαρξη, την ακεραιότητα και την απόδοση των επικοινωνιών, των διαδικασιών και των δεδομένων. Οι λύσεις πιστοποίησης δεδομένων που βασίζονται σε blockchain δημιουργούν ένα αμετάβλητο αρχείο όλης της δραστηριότητας σε συστήματα διαχείρισης εγγράφων μέσω των οποίων οι καταθέσεις, οι ένορκες βεβαιώσεις ή οι όρκοι ελέγχου, λογιστικών ή νομικών γραφείων μπορούν να πιστοποιηθούν αυτόματα. Τα ακατέργαστα δεδομένα ή το απλό κείμενο δεν δημοσιεύονται ποτέ σε μια δημόσια αλυσίδα μπλοκ, αλλά μόνο μοναδικά κρυπτογραφικά αναγνωριστικά (hashes) προκειμένου να μην αποκαλυφθούν τα αρχικά δεδομένα. Δεδομένου ότι οι κατακερματισμοί είναι μονόδρομοι κρυπτογραφικοί αλγόριθμοι, είναι δυνατό να αποδειχθεί ότι ένας καθορισμένος κατακερματισμός σχετίζεται με ορισμένα δεδομένα, αλλά κανείς δεν θα μπορέσει ποτέ να λάβει τα δεδομένα έχοντας μόνο τον κατακερματισμό του.

Αυτή η λύση εφαρμόζεται σε δημόσιες αλυσίδες μπλοκ προσβάσιμες από οποιονδήποτε στον κόσμο με μηδενικό κόστος. Όλα είναι διαφανή και εξαιρετικά εύκολο να επαληθευτούν, διατηρώντας παράλληλα το απόλυτο απόρρητο. Οι κρυπτογραφικές αποδείξεις που δημιουργούνται είναι όλα όσα χρειάζεται κάποιος για να αποδείξει ή να επαληθεύσει ότι ένα δεδομένο σύνολο δεδομένων υπήρχε σε μια συγκεκριμένη χρονική στιγμή. Επιπλέον, η επαλήθευση των κρυπτογραφικών αποδείξεων μπορεί να γίνει με αυτόματο τρόπο, επιτρέποντας ασφαλείς συναλλαγές από μηχανή σε μηχανή. Καθώς ο GDPR δίνει έμφαση στην επίδειξη συμμόρφωσης, το τελευταίο παράδειγμα δείχνει ότι η ενσωματωμένη «ίχνη ελέγχου» του blockchain μπορεί να βοηθήσει τους οργανισμούς να αποδείξουν ποιος έχει πρόσβαση στα προσωπικά δεδομένα, πού και πότε.

8. Παρούσα κατάσταση σε GDPR-compliant λύσεις

8.1. Βιβλιογραφική επισκόπηση Ευρωπαϊκών ερευνητικών έργων

Η βιβλιογραφική ανασκόπηση που διεξάγαμε εντόπισε τέσσερις πιθανές λύσεις για την επεξεργασία προσωπικών δεδομένων σύμφωνα με το GDPR με χρήση του Blockchain στην ακαδημαϊκή βιβλιογραφία και τις πηγές επαγγελματιών. Ωστόσο, αποκάλυψε έλλειψη επιστημονικών ερευνητικών εργασιών στο συγκεκριμένο ερευνητικό πεδίο. Πολλές από τις πηγές δεν υποβλήθηκαν σε διαδικασία αξιολόγησης από ομοτίμους. Ένας λόγος για αυτό μπορεί να είναι η ταχεία ανάπτυξη της τεχνολογίας Blockchain που τεκμηριώνεται κυρίως σε πηγές διαδικτύου καθώς και η πρόσφατη νομική ισχύς του GDPR [ZEMLER2019].

Η λύση που συζητείται περισσότερο στην αναθεωρημένη βιβλιογραφία είναι το Off-Chain Storage. Με αυτήν την ιδέα, τα προσωπικά δεδομένα αποθηκεύονται εκτός του δικτύου Blockchain και αναφέρονται στο Blockchain μόνο στην τοποθεσία εκτός αλυσίδας. Το πρόβλημα είναι ότι στις περισσότερες περιπτώσεις μια «απόδειξη ορθότητας» διατηρείται στην αλυσίδα και αυτή θα μπορούσε επίσης να είναι προσωπικά δεδομένα. Αυτή η λύση εφαρμόζεται ήδη στην πράξη.

Η δεύτερη αναγνωρισμένη λύση, το Redactable Blockchain, χρησιμοποιεί έναν ειδικό αλγόριθμο κατακερματισμού, ο οποίος επιτρέπει την αλλαγή δεδομένων ενός μπλοκ χωρίς αλλαγή του αντίστοιχου κατακερματισμού του. Αυτό επιτρέπει την αλλαγή και τη διαγραφή δεδομένων στο Blockchain και είναι ενόψει των απαιτήσεων του GDPR μια πολύ ενδιαφέρουσα λύση. Από την άλλη πλευρά, αυτή η έννοια συχνά επικρίνεται ως παραβίαση του αμετάβλητου του Blockchain, ενός από τα θεμελιώδη χαρακτηριστικά του.

Η επόμενη έννοια, Legal Argumentations, χρησιμοποιεί ερμηνείες του GDPR. Από τη μία πλευρά, μπορεί να υποστηριχθεί ότι το δικαίωμα στη λήθη δεν είναι απόλυτο δικαίωμα και ότι τα δεδομένα στο Blockchain θα μπορούσαν να τροποποιηθούν ή να διαγραφούν προσθέτοντας μια νέα συναλλαγή στο μπλοκ που δηλώνει άκυρη την παλιά. Από την άλλη πλευρά, θα μπορούσε να είναι δυνατός ο ισχυρισμός ότι απαιτείται συνεπής επεξεργασία δεδομένων για τη σωστή λειτουργία του Blockchain. Επομένως, κανένα στοιχείο δεν μπορεί να τροποποιηθεί ή να διαγραφεί. Αυτή η επιχειρηματολογία μπορεί να βασίζεται στο άρθρο 17,1 του GDPR.

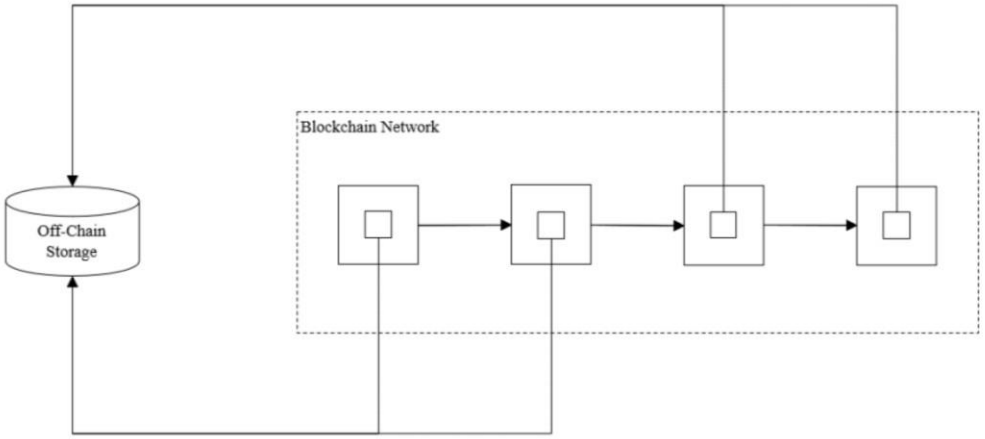
Η τελευταία ιδέα, Κρυπτογράφηση & Διαγραφή Κλειδιού, περιγράφει μια τεχνική κατά την οποία τα προσωπικά δεδομένα κρυπτογραφούνται πριν από την αποθήκευση των δεδομένων στο Blockchain και το κλειδί αποθηκεύεται χωριστά. Εάν τα δεδομένα δεν απαιτούνται πλέον, το κλειδί κρυπτογράφησης απλώς διαγράφεται και ως εκ τούτου τα δεδομένα δεν είναι πλέον προσβάσιμα. Ο κύριος επικριτής αυτής της μεθόδου είναι ότι στο εγγύς μέλλον μπορεί να είναι δυνατή η αποκρυπτογράφηση των δεδομένων χωρίς την ανάγκη του κλειδιού αποκρυπτογράφησης και τα δεδομένα γίνονται ξανά προσβάσιμα.

Σε γενικές γραμμές, αυτή τη στιγμή συνιστάται ανεπιφύλακτα να μην αποθηκεύονται προσωπικά δεδομένα σε ένα Δημόσιο Blockchain. Εάν τα προσωπικά δεδομένα είχαν αποθηκευτεί σε ένα Δημόσιο Blockchain, δεν θα μπορούσαμε να εγγυηθούμε ότι τα δεδομένα παραμένουν εντός του εδαφικού πεδίου εφαρμογής του GDPR και ενδέχεται να παραβιάζουν τις αρχές της μεταφοράς προσωπικών δεδομένων σε τρίτες χώρες. Η έννοια του Legal Argumentation δρα σε γκρίζα ζώνη και έτσι είναι πάντα πιθανό αυτή η μέθοδος να κηρυχθεί παράνομη. Η κατάσταση είναι παρόμοια με την έννοια του Encryption & Key Erasure. Σε αυτήν την ιδέα, τα προσωπικά δεδομένα παραμένουν κρυπτογραφημένα στο Blockchain, για όσο διάστημα υπάρχει το Blockchain. Ακόμα κι αν το κλειδί αποκρυπτογράφησης καταστραφεί, τα δεδομένα μετρώνται επί του παρόντος ως προσωπικά δεδομένα.

8.2. Αποθήκευση εκτός αλυσίδας

Η αποθήκευση εκτός αλυσίδας είναι η πιο πολυσυζητημένη έννοια στην αναθεωρημένη βιβλιογραφία για την επεξεργασία στο Blockchain που είναι συμβατή με το GDPR. Αποθήκευση δεδομένων "εκτός αλυσίδας" σημαίνει, ότι τα προσωπικά δεδομένα δεν διατηρούνται μέσα στο Blockchain, αλλά αποθηκεύονται έξω από αυτό, π.χ., σε μια παραδοσιακή βάση δεδομένων [ESPOSITO2018]. Μόνο μια αναφορά προς τα έξω (για παράδειγμα, μια τιμή κατακερματισμού) αποθηκεύεται στο Blockchain [KATUWAL2018].

Το σχήμα παρέχει μια απλοποιημένη επισκόπηση μιας αρχιτεκτονικής αποθήκευσης εκτός αλυσίδας. Γενικά, η αποθήκευση μεγαλύτερων συνόλων δεδομένων εκτός του Blockchain συνιστάται ιδιαίτερα, γιατί η αποθήκευση σε ένα Blockchain είναι σχετικά δαπανηρή [ZHANGY 2018].



Σχήμα: Αποθήκευση εκτός αλυσίδας [ZEMLER2019].

Πλεονεκτήματα

- Τα προσωπικά δεδομένα αποθηκεύονται εκτός αλυσίδας
- Μόνο μια αναφορά στη θέση αποθήκευσης εκτός αλυσίδας και στον κατακερματισμό των δεδομένων διατηρείται στην αλυσίδα
- Επιτρέπει την επεξεργασία μεγάλων δεδομένων

Μειονεκτήματα

- Μπορεί να απαιτεί την επανεισαγωγή ενός TTP
- Ενδέχεται να απαιτούνται σημαντικές τεχνικές τροποποιήσεις ανάλογα με το πού διατηρούνται τα δεδομένα

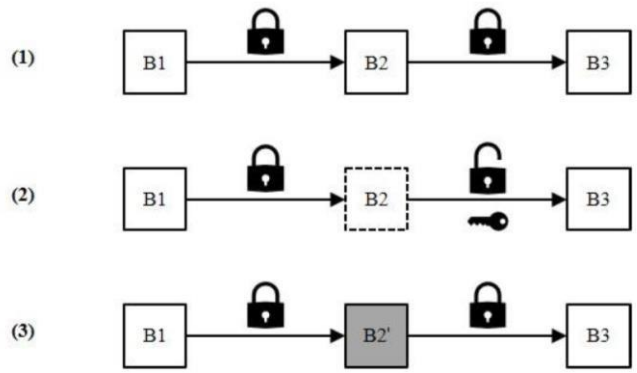
8.3. Διορθώσιμο Blockchain

Το Διορθώσιμο Blockchain (Redactable Blockchain) αναφέρθηκε για πρώτη φορά στο βιβλιογραφία από τους Ateniese et al. [ATENIESE2017] και είναι σχετικά νέα ιδέα. Με τον όρο «διορθώσιμο» εννοούν οι συγγραφείς την επανεγγραφή ενός ή περισσότερων μπλοκ που ήταν ήδη γραμμένα στο Blockchain, τη συμπίεση οποιουδήποτε αριθμού ήδη υπαρχόντων μπλοκ σε μικρότερο αριθμό μπλοκ και την εισαγωγή ενός ή περισσότερων μπλοκ στην υπάρχουσα αλυσίδα.

Αρχικά, αυτό φαίνεται να έρχεται σε αντίθεση με το αμετάβλητο του Blockchain, μια από τις βασικές του έννοιες. Ωστόσο, οι συγγραφείς υποστηρίζουν ότι το αμετάβλητο μπορεί να μην είναι κατάλληλο για όλες τις νέες εφαρμογές που βασίζονται στην τεχνολογία Blockchain. Για παράδειγμα, αυτό μπορεί να γίνει στην αποθήκευση αρχείων ή τη διαχείριση προσωπικών αρχείων υγείας. Αυτά τα δεδομένα θα πρέπει μπορούν να διαγραφούν εάν περιέχουν σφάλματα ή όταν απαιτείται βάσει νόμου.

Για να γίνει το Blockchain μεταβλητό χρειάζεται μια τεχνική που λέγεται «συνάρτηση κατακερματισμού χαμαιλέοντα» (chameleon hash function). Η συνάρτηση κατακερματισμού chameleon λειτουργεί όπως και κάθε άλλη, με τη διαφορά ότι έχει κάτι σαν καταπακτή (trapdoor) που μπορεί να χρησιμοποιηθεί για τη δημιουργία συγκρούσεων (collisions). Αυτές οι συγκρούσεις μπορούν να χρησιμοποιηθούν για να τροποποιηθούν τα δεδομένα των συναλλαγών χωρίς να αλλάξει η αντίστοιχη τιμή κατακερματισμού του μπλοκ ώστε αυτό να διατηρήσει τη σύνδεση με το επόμενό του.

Το σχήμα παρουσιάζει τις τρεις διαφορετικές φάσεις του Redactable Blockchain. Στο (1) το Redactable Blockchain συμπεριφέρεται όπως κάθε άλλο Blockchain και δεν υπάρχει καμία τροποποίηση. Αυτό είναι δυνατό γιατί όλες οι κλειδαριές είναι ασφαλισμένες. Στο (2) η σύνδεση μεταξύ B2 και B3 ανοίγει με το μυστικό κλειδί και είναι δυνατή η τροποποίηση. Στο (3) οι τροποποιήσεις στο B2 τελειώνουν και καταλήγουμε στη μορφή του μπλοκ B2'. Η σύνδεση μεταξύ B2' και B3 είναι ξανά κλειδωμένη και δεν είναι δυνατές περισσότερες τροποποιήσεις.



Το Redactable Blockchain θα μπορούσε να είναι ενδιαφέρουσα λύση. Η ιδέα της απευθείας αφαίρεσης μπλοκ που περιέχουν προσωπικά δεδομένα θα έλυνε πολλά προβλήματα. Ωστόσο, αντιμετωπίζει κάποια προβλήματα. Πρώτον, προσθέτοντας δυνατότητα redactability σε ένα υπάρχον Blockchain δεν είναι δυνατό. Αυτό σημαίνει ότι η απόφαση για

redactability πρέπει να ληφθεί πριν την κατασκευή του Blockchain. Δεύτερον, τα παλιά αντίγραφα του Blockchain θα εξακολουθούν να περιέχουν τα προσωπικά δεδομένα που διαγράφηκαν. Τέλος, υπάρχει πάντα ο κίνδυνος μια πλευρά να διαγράψει δεδομένα από το Blockchain προς όφελός του.

Πλεονεκτήματα

- Παρέχει έναν τρόπο αλλαγής και διαγραφής προσωπικών δεδομένων απευθείας στο Blockchain
- Δεν απαιτεί αλλαγή στον τρόπο χρήσης του Blockchain

Μειονεκτήματα

- Απαιτεί τεχνικές προσαρμογές
- Το Redactability δεν μπορεί να προστεθεί σε ένα υπάρχον Blockchain
- Εάν χαθεί το μυστικό κλειδί, το Blockchain παραμένει αμετάβλητο
- Απαιτούνται κόμβοι για τη διαγραφή παλαιών αντιγράφων των μπλοκ που έχουν υποστεί επεξεργασία
- Οι κόμβοι μπορούν να κάνουν κατάχρηση αυτής της δυνατότητας προς όφελός τους
- Μπορεί να απαιτεί αποθήκευση εκτός αλυσίδας για μεγάλα δεδομένα

8.4. Νομικά επιχειρήματα

Το Legal Argumentation ασχολείται με τον ανακριβή ορισμό ορισμένων τμημάτων του παρόντος κανονισμού. Λόγω του αμετάβλητου της τεχνολογίας Blockchain, είναι μια πραγματική πρόκληση να διαγραφούν τα προσωπικά δεδομένα μόλις αποθηκευτούν στο Blockchain. Από νομική άποψη, η ανασκόπηση της βιβλιογραφίας εντόπισε δύο διαφορετικούς τρόπους επιχειρηματολογίας κατά αυτής της διαδικασίας.

Οι Ibáñez et al. [IBANEZ2018] προβάλλουν ότι το δικαίωμα λήθης δεν είναι απόλυτο δικαίωμα και η έννοια αυτή αφήνει περιθώρια για ερμηνεία. Στο παράδειγμά τους, παρουσιάζουν ότι η διαγραφή ή η τροποποίηση πραγματοποιείται προσθέτοντας μια νέα συναλλαγή στο Blockchain που περιέχει αναφορά στην διεγραμμένη καταχώρηση και την ακυρώνει σημασιολογικά.

Μια άλλη λύση παρουσιάζεται από τους Berberich και Steiner [BERBERICH2016] που επεξηγούν ότι με τη βοήθεια του άρθρου 17 παράγραφος 1β μπορεί να είναι δυνατό να υποστηριχθεί ότι για τα προσωπικά δεδομένα απαιτείται αποθήκευση στην αλυσίδα γιατί Το Blockchain χρειάζεται την αλυσίδα για να λειτουργεί σωστά. Ως εκ τούτου, το δικαίωμα στη λήθη του υποκειμένου των δεδομένων δεν μπορεί να εφαρμοστεί εδώ.

Όλα αυτά τα νομικά επιχειρήματα θα πρέπει επί του παρόντος να είναι αντιμετωπίζονται με προσοχή. Λόγω της έλλειψης κρίσης σε αυτό το πεδίο, αυτή η έννοια λειτουργεί σε γκρίζα περιοχή. Είναι πολύ πιθανό ότι αυτές οι διαδικασίες στο

μέλλον θα μπορούσαν να θεωρούνται παράνομες στο δικαστήριο. Τότε, δεν θα είναι δυνατή η αφαίρεση των προσωπικών δεδομένων από ένα υπάρχον Blockchain, ακόμα κι αν απαιτείται από το νόμο.

Πλεονεκτήματα

- Δεν απαιτούνται αλλαγές στην τεχνολογία Blockchain
- Τα δεδομένα που είναι παρωχημένα μπορούν απλώς να ακυρωθούν με μια νέα συναλλαγή

Μειονεκτήματα

- Το concept πρέπει να αντιμετωπιστεί πολύ προσεκτικά γιατί λειτουργεί σε νόμιμη γκρίζα ζώνη
- Μπορεί να απαιτεί αποθήκευση εκτός αλυσίδας για μεγάλα δεδομένα

8.5. Κρυπτογράφηση και Διαγραφή κλειδιού

Η λύση αυτή αφορά την κρυπτογράφηση δεδομένων σε μια αλυσίδα Blockchain για την επίτευξη συμμόρφωσης με τον GDPR. Ορισμένες μελέτες προτείνουν την κρυπτογράφηση των δεδομένων που είναι αποθηκευμένα σε μια αλυσίδα Blockchain και, όταν πρέπει να διαγραφούν, απλώς να καταστραφεί το κλειδί κρυπτογράφησης [VANGEELKERKEN2017].

Αυτή η ιδέα προϋποθέτει ότι με τη χρήση τεχνικών κρυπτογράφησης αιχμής τα δεδομένα γίνονται απρόσιτα όταν το κλειδί κρυπτογράφησης δεν είναι πλέον διαθέσιμο. Αυτή η διαδικασία πλησιάζει στη διαγραφή δεδομένων.
Λαμβάνοντας υπόψη τον GDPR, αυτή η έννοια πρέπει να αντιμετωπιστεί κριτικά.

Πρώτον, είναι πιθανό οι σημερινοί αλγόριθμοι κρυπτογράφησης να μην θεωρούνται πλέον ασφαλείς στο μέλλον, έτσι ώστε να είναι δυνατή η αποκρυπτογράφηση των δεδομένων χωρίς τη γνώση του αρχικού κλειδιού κρυπτογράφησης.

Δεύτερον, η Ομάδα Εργασίας για την Προστασία Δεδομένων του άρθρου 29 (2014) ορίζει ξεκάθαρα ότι η κρυπτογράφηση πρέπει να θεωρείται ως μορφή ψευδωνυμοποίησης και δεν ανωνυμοποιεί αυτόματα τα δεδομένα. Είναι σημαντικό να σημειωθεί ότι η κρυπτογράφηση εγγυάται την εμπιστευτικότητα μόνο για μια συγκεκριμένη χρονική περίοδο, αλλά η ανωνυμοποίηση θα πρέπει να διαρκεί επ' αόριστον. Σε γενικές γραμμές, μπορεί να ειπωθεί ότι η χρήση κρυπτογράφησης και καταστροφής κλειδιού δεν πρέπει να θεωρείται ως η κύρια τεχνική για μια λύση συμβατή με το GDPR.

Πλεονεκτήματα

- Δεν απαιτούνται αλλαγές στην τεχνολογία Blockchain
- Τα δεδομένα στην αλυσίδα αποθηκεύονται κρυπτογραφημένα
- Όταν τα δεδομένα πρέπει να αφαιρεθούν από το Blockchain, το κλειδί κρυπτογράφησης απλώς καταστρέφεται

Μειονεκτήματα

- Δεν πρέπει να χρησιμοποιείται ως η κύρια ιδέα για τη συμμόρφωση με τον GDPR
- Τα κρυπτογραφημένα προσωπικά δεδομένα πρέπει να αντιμετωπίζονται ως δεδομένα με ψευδώνυμα
- Μπορεί να είναι σε θέση να αποκρυπτογραφήσει δεδομένα στο μέλλον με τη χρήση ενημερωμένης τεχνολογίας
- Μπορεί να απαιτεί αποθήκευση εκτός αλυσίδας για μεγάλα δεδομένα

9. Ενοποιημένη μεθοδολογία συμμόρφωσης τεχνολογικών λύσεων με το GDPR

9.1. Διακριτά βήματα για την επίτευξη συμμόρφωσης

Για την εναρμόνιση με τον Νέο Ευρωπαϊκό Κανονισμό GDPR (General Data Protection Regulation) απαιτούνται μια σειρά από βήματα:

- Να διερευνηθούν τα σημεία απόκλισης της λειτουργίας της εταιρείας ή οργανισμού από τον κανονισμό GDPR.
- Οργάνωση των εσωτερικών διαδικασιών, προτάσεις για την λήψη απαραίτητων μέτρων, και υποστήριξη για την υλοποίηση τους.
- Κατάταξη, προτεραιότητα και τεκμηρίωση στις ενέργειες συμμόρφωσης
- Κατάταξη και χαρτογράφηση δεδομένων
- Διορισμός ενός Υπευθύνου Προστασίας Δεδομένων ("DPO")
- Διαχείριση κινδύνων και αξιολόγηση επιπτώσεων σχετικών με την προστασία δεδομένων.
- Δημιουργία αρχείου δραστηριοτήτων επεξεργασίας προσωπικών δεδομένων.
- Συμμόρφωση με διεθνώς αναγνωρισμένο πρότυπο που προσδιορίζει τις προδιαγραφές για την διαχείριση της ασφάλειας των πληροφοριών (π.χ. το ISO 27001).
- Ανάπτυξη όλων των απαιτούμενων πολιτικών και διαδικασιών προστασίας προσωπικών δεδομένων, σε ενοποιημένο Σύστημα Διαχείρισης Προσωπικών Δεδομένων (π.χ. με το πρότυπο ISO / IEC 27701: 2019).
- Ενημέρωση και συμμετοχή του εμπλεκόμενου προσωπικού στη διαδικασία εναρμόνισης της εταιρείας με τον Κανονισμό GDPR, εκπαιδευτικά σεμινάρια.
- Εκπαίδευση των υπευθύνων στην μεθοδολογία και τις βέλτιστες πρακτικές (best practices) που ακολουθούνται διεθνώς.

- Ανάπτυξη διαδικασιών αντιμετώπισης διαρροής δεδομένων (data leaks) και παραβιάσεων ασφαλείας (security breaches).
- Νομικές Υπηρεσίες GDPR.

9.2. Το πρότυπο ISO 27001: πρότυπο προδιαγραφών για την διαχείριση της ασφάλειας των πληροφοριών

Στις μέρες μας οι επιχειρήσεις βασίζονται όλο και περισσότερο σε συστήματα πληροφοριών για να υποστηρίξουν τις κρίσιμες επιχειρηματικές διαδικασίες τους και αυτό καθιστά της εφαρμογή ενός Συστήματος Ασφάλειας Πληροφοριών απαραίτητο. Η απώλεια αρχείων, δεδομένων και πληροφοριών, η κλοπή εμπιστευτικών δεδομένων και η βλάβη σε κρίσιμα συστήματα και έγγραφα είναι μεταξύ άλλων από τους πιο συνηθισμένους κινδύνους που μπορεί να αντιμετωπίσει μια επιχείρηση οι οποίες οδηγούν σε σοβαρές συνέπειες των εσωτερικών διαδικασιών της, συμπεριλαμβανομένων των οικονομικών επιπτώσεων και την διακινδύνευση της φήμης της.

Το ISO 27001 είναι ένα διεθνώς αναγνωρισμένο πρότυπο το οποίο προσδιορίζει τις προδιαγραφές για την διαχείριση της ασφάλειας των πληροφοριών. Μπορεί να χρησιμοποιηθεί από εταιρίες, που επιθυμούν να εγκαταστήσουν και να βελτιώσουν την ασφαλή διαχείριση των δεδομένων τους και των πελατών τους [ISO27001].

Σκοπός του ISO / IEC 27001: 2013, είναι να εξασφαλίσει την ύπαρξη επαρκών και κατάλληλων ελέγχων σε θέματα εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας της πληροφορίας, προστατεύοντας έτσι τα δεδομένα των ενδιαφερόμενων μερών.

Τα σημαντικότερα οφέλη από την εφαρμογή ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών είναι μεταξύ άλλων:

- Η εκτίμηση και αντιμετώπιση των κινδύνων της ασφάλειας των πληροφοριών, προσαρμοσμένων στις ανάγκες του κάθε οργανισμού
- Η διασφάλιση της ακεραιότητας των πληροφοριών που εισέρχονται και ελέγχονται από μια επιχείρηση.
- Ο εντοπισμός και η καλύτερη κατανόηση των σχετικών νομοθετικών και κανονιστικών απαιτήσεων.
- Η αύξηση εμπιστοσύνης των πελατών και των ενδιαφερόμενων μερών μέσω της απόδειξης ότι τα δεδομένα τους προστατεύονται.
- Η ύπαρξη ενός επίσημου και λειτουργικού συστήματος διαχείρισης ασφάλειας πληροφοριών.
- Η βελτίωση της αξιοπιστίας και της εμπιστευτικότητας της επιχείρησης.
- Η καλύτερη αναγνώριση και αξιολόγηση των κινδύνων.

Μέσω του προτύπου ISO / 27001 **επιτυγχάνεται**:

- Μείωση επιχειρηματικού ρίσκου και κόστους.– Εξασφαλίζει την ύπαρξη ελέγχων τόσο για την μείωση του ρίσκου όσο και για την αποφυγή εκμετάλλευσης τυχόν αδυναμιών του συστήματος. Ακόμα και αν το χειρότερο συμβεί, ο οργανισμός είναι σε θέση να το αντιμετωπίσει και να ανακτήσει τον έλεγχο το συντομότερο δυνατό.
- Βέλτιστη Πρακτική.– Διασφάλιση ότι υπάρχει δέσμευση ως προς την ασφάλεια πληροφοριών από όλους και σε όλα τα επίπεδα του οργανισμού.
- Συμμόρφωση με νομικές και κανονιστικές απαιτήσεις.
- Ανταγωνιστικότητα.– Τόνωση και προβολή της εμπορικής εικόνας. Αύξηση της εμπιστοσύνης των πελατών, συνεργατών και γενικά όλων των ενδιαφερόμενων μερών, με την επίγνωση ότι η διαχείριση των πληροφοριών και των δεδομένων τους είναι ασφαλής.
- Ενιαίο Σύστημα Διαχείρισης.– Βασισμένο στον κύκλο « Σχεδιάζω – εκτελώ – ελέγχω – ενεργώ» το ISO / IEC 27001 έχει αρκετά κοινά με άλλα πρότυπα όπως 9001 και 14001, καθιστώντας ευκολότερη την ανάπτυξη ενός ενιαίου συστήματος διαχείρισης που ικανοποιεί τις απαιτήσεις και άλλων προτύπων.

Οι **απαιτήσεις του προτύπου** είναι λογικές και στις περισσότερες περιπτώσεις αυτονόητες, όπως:

- Προδιαγραφές για υλικά, προϊόντα και υπηρεσίες.
- Μέθοδοι ανταπόκρισης του οργανισμού για τις δεσμεύσεις και προδιαγραφές που δίνει στους πελάτες.
- Οργανόγραμμα, υπευθυνότητες, αρμοδιότητες (ποιος κάνει τι, με τι εξουσιοδότηση).
- Σχεδιασμένες διαδικασίες για τις κρίσιμες ή πολύπλοκες λειτουργίες.
- Καθορισμένος τρόπος επικοινωνίας και διαχείρισης των πληροφοριών.
- Συγκεκριμένοι στόχοι για τη συνεχή βελτίωση του οργανισμού.
- Διαδικασίες ελέγχου και αξιολόγησης των δεδομένων, των μεθόδων και των ανθρώπων.
- Καταγραφή όλων των χρήσιμων και κρίσιμων δεδομένων που χρειάζεται ο οργανισμός για να διασφαλίζει τη καλή λειτουργία του και να χτίζει τη βελτίωσή του.
- Η πιστοποίηση κατά ISO 27001 αποδεικνύει ότι ο οργανισμός εφαρμόζει ένα αποτελεσματικό σύστημα διαχείρισης της Ασφάλειας των Πληροφοριών, που ικανοποιεί τις απαιτήσεις του προτύπου.

9.3. Το πρότυπο ISO 27701 που αφορά την προστασία προσωπικών δεδομένων

Το πρότυπο ISO / IEC 27701: 2019 αφορά την προστασία προσωπικών δεδομένων. Το εν λόγω πρότυπο παρέχει καθοδήγηση σε οργανισμούς και εταιρείες που επιθυμούν να εφαρμόζουν συστήματα που να υποστηρίζουν τη συμμόρφωση με τις απαιτήσεις του Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένων GDPR [ISO27701].

Η εγκατάσταση και η εφαρμογή του συστήματος ISO 27701:2019 μειώνει τον κίνδυνο διαρροής των δεδομένων προσωπικού χαρακτήρα και ενισχύει το υπάρχον σύστημα Διαχείρισης Ασφάλειας Πληροφοριών ISO 27001.

Η πιστοποίηση με το παραπάνω πρότυπο αποτελεί ένα μέσο ώστε να αποδείξει κάθε επιχείρηση/ οργανισμός στους πελάτες, εξωτερικούς και εσωτερικούς φορείς και ενδιαφερόμενους ότι έχει λάβει όλα τα κατάλληλα τεχνικά και οργανωτικά μέτρα για τη στήριξη της συμμόρφωσης με το GDPR και άλλες σχετικές νομοθεσίες περί απορρήτου.

Οι οργανισμοί/ εταιρείες που επιθυμούν να λάβουν πιστοποίηση σύμφωνα με το πρότυπο ISO 27701 προκειμένου να συμμορφωθούν με το GDPR είτε θα πρέπει να διαθέτουν ήδη πιστοποίηση ISO 27001 είτε να εφαρμόσουν το ISO 27001 και το ISO 27701 μαζί ως ένα ενοποιημένο σύστημα διαχείρισης.

Περισσότεροι από 60.000 οργανισμοί παγκοσμίως έχουν πιστοποιηθεί μέχρι σήμερα στο ISO 27001, αποδεικνύοντας ότι η πιστοποίηση αποτελεί ουσιαστικό εφόδιο για τις επιχειρήσεις & οργανισμούς.

Η σημαντική αλληλεπικάλυψη των συστημάτων και των τεχνικών απαιτήσεων μεταξύ ενός συστήματος διαχείρισης πληροφοριών απορρήτου και ενός συστήματος ασφάλειας πληροφοριών αποτελεί μια αναγκαστική υπόθεση για την υιοθέτηση των προτύπων ISO 27001 και ISO 27701.

ΤΟ ISO 27701 εξυπηρετεί την καλύτερη εφαρμογή της νομοθεσίας. Αν και υπάρχει άμεση σχέση με τον GDPR, μιας και αμφότεροι φέρουν ευθύνη για τα δεδομένα που χρησιμοποιούν, ο GDPR εμπεριέχει, έννοιες και αρμοδιότητες σχετιζόμενες με την ασφάλεια των πληροφοριών, αλλά δεν περιλαμβάνει οδηγίες σχετικά με την ασφάλεια αυτών.

Περιλαμβάνοντας ένα σύνολο επιπρόσθετων απαιτήσεων και ελέγχων σε σύγκριση με το ISO 27001, έχει ως στόχο του, να βελτιστοποιήσει το υπάρχον Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ISMS), προκειμένου να προσφέρει μια διεθνή προσέγγιση στην Προστασία των Προσωπικών Δεδομένων.

Καλύπτει κάθε κενό στο κομμάτι της διασφάλισης αυτών και βελτιώνει το σύστημα διαχείρισης πληροφοριών απορρήτου (PIMS), ώστε να μειωθεί ο κίνδυνος καταπάτησης του δικαιώματος απορρήτου των ανθρώπων και να προστατευθεί η ιδιωτικότητά τους από τη διαρροή ή την κακή διαχείριση πληροφοριών.

Πλεονεκτήματα από την εγκατάσταση και εφαρμογή του ISO 27701

- Τεκμηριωμένη απόδειξη συμμόρφωσης με τις απαιτήσεις GDPR
- Διασφάλιση προσωπικών δεδομένων
- Μείωση κινδύνου διαρροής προσωπικών δεδομένων

- Δήλωση δέσμευσης για την ασφάλεια των πληροφοριών/δεδομένων σε πελάτες, προμηθευτές και άλλα ενδιαφερόμενα μέρη
- Η πιστοποίηση αναγνωρίζεται διεθνώς

10. Συμπεράσματα και μελλοντικές προοπτικές

Η παρούσα διπλωματική αποσκοπεί στην ανάλυση του κανονισμού GDPR υπό το πρίσμα της τεχνολογίας blockchain, αποσκοπώντας να διαλευκάνει το τοπίο και τις εντάσεις ανάμεσα στις διατάξεις του κανονισμού και το blockchain και να αποτελέσει οδηγό για μελλοντικές υλοποιήσεις. Η τεχνολογία blockchain εκ πρώτης όψεως διαφωνεί με το GDPR σε βασικά σημεία, το κυριότερο εκ των οποίων αποτελεί το δικαίωμα των χρηστών για τη διαγραφή των δεδομένων τους. Ωστόσο, με περαιτέρω ανάλυση, είναι εύκολο να διαπιστωθεί πως το blockchain πρεσβεύει αρχές παρόμοιες με το GDPR, όπως η προστασία των δεδομένων, η διαφάνεια, η έλλειψη κεντρικής αρχής επεξεργασίας δεδομένων σε ένα σύστημα κ.α. Αυτό γίνεται ορατό και από την πληθώρα λύσεων στην ερευνητική βιβλιογραφία, οι οποίες εκμεταλλεύονται τις εγγενείς ιδιότητες του blockchain για την παραγωγή συστημάτων τα οποία συμμορφώνονται με τις διατάξεις του GDPR. Η ενοποιημένη μεθοδολογία που προέκυψε σε αυτή τη διπλωματική μπορεί να αποτελέσει οδηγό για μελλοντικές υλοποιήσεις και να καθοδηγήσει ερευνητές, προγραμματιστές κτλ. Στην κατανόηση του κανονισμού και στην παραγωγή νόμιμων λύσεων που σέβονται και προστατεύουν τα προσωπικά δεδομένα και την ασφάλεια των χρηστών.

Βασικά συμπεράσματα:

- Ο GDPR είναι αρκετά οριζόντια νομοθεσία
- Υπάρχουν ασάφειες όσον αφορά τον ορισμό της έρευνας και τι καθιστά ερευνητική δραστηριότητα
- Υπάρχουν ασάφειες όσον αφορά το τι καθιστά καινοτόμα τεχνολογία
- Η παρούσα διπλωματική επιχείρησε να καθαρίσει το τοπίο όσον αφορά την τεχνολογία blockchain και το GDPR

- Μελλοντικές ερευνητικές προσπάθειες θα πρέπει να επαναλάβουν τη φιλοσοφία της παρούσας διπλωματικής και για άλλες τεχνολογίες (bigdata, AIetc.) ώστε να δημιουργηθούν κάθετες μεθοδολογίες που μπορούν να οδηγήσουν μία λύση σε νομική συμμόρφωση ανεξάρτητα του τεχνολογικού πεδίου.

11. Βιβλιογραφία

[ATENIESE2017] Ateniese, Giuseppe; Magri, Bernardo; Venturi, Daniele; Andrade, Ewerton (2017): Redactable Blockchain – or – Rewriting history in Bitcoin and friends. In : 2017 IEEE European Symposium on Security and Privacy (EuroS&P). 2017 IEEE European Symposium on Security and Privacy (EuroS&P). Paris, France, 26.04.2017 - 28.04.2017: IEEE, pp. 111–126.

[B3I2019], Accelerating direct collaboration in regulated markets with trust technology—DLT and confidential computing platforms—that delivers irrefutable trust and secure exchange between parties, 2019, https://www.r3.com/

[BERBERICH2016], Berberich, Matthias; Steiner, Malgorzata (2016): Blockchain technology and the GDPR – How to reconcile privacy and distributed ledgers? In European Data Protection Law Review 2 (3), pp. 422–426. DOI: 10.21552/EDPL/2016/3/21.

[ESPOSITO2018] Esposito, Christian; Santis, Alfredo de; Tortora, Genny; Chang, Henry; Choo, Kim-Kwang Raymond (2018): Blockchain: A Panacea for healthcare cloud-based data security and privacy? In IEEE Cloud Comput. 5 (1), pp. 31–37. DOI: 10.1109/MCC.2018.011791712.

[GDPR2016], General Data Protection Regulation - GDPR, official PDF of the Regulation, https://gdpr-info.eu/

[HAQUE2021] A. B. Haque, A. K. M. N. Islam, S. Hyrynsalmi, B. Naqvi and K. Smolander, "GDPR Compliant Blockchains–A Systematic Literature Review," in IEEE Access, vol. 9, pp. 50593-50606, 2021, doi: 10.1109/ACCESS.2021.3069877.

[IBANEZ2018], Ibáñez, Luis-Daniel; O'Hara, Kieron; Simperl, Elena (2018): On Blockchains and the General Data Protection Regulation. Available online at https://eprints.soton.ac.uk/422879/1/BLockchains_G DPR_4.pdf.

[IBM2017], IBM and Crédit Mutuel Arkéa Announce Identity Verification Project Built on Hyperledger Blockchain, 2017, https://www.redchalk.com/feature/ibm-and-credit-mutuel-arkea-announce-identity-verification-project-built-onhyperledger-blockchain/

[ISO27001], ISO/IEC 27001:2013, Information technology — Security techniques — Information security management systems — Requirements, https://www.iso.org/standard/54534.html

[ISO27701], ISO/IEC 27701:2019, Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines, https://www.iso.org/standard/71670.html

[KATUWAL2018], Katuwal, Gajendra J.; Pandey, Sandip; Hennessey, Mark; Lamichhane, Bishal (2018): Applications of Blockchain in healthcare: Current landscape & challenges. Available online at http://arxiv.org/pdf/1812.02776v1.

[NAKAMOTO2008] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System|Satoshi Nakamoto Institute, Oct. 2008, [online] Available: https://nakamotoinstitute.org/bitcoin/.

[STAMPERY2015], Leaders in blockchain-based data certification, 2015, https://stampery.com/

[VANGEELKERKEN2017], van Geelkerken, F.W.J; Konings, K. (2017): Using Blockchain to strengthen the rights granted through the GDPR. In : 7th International youth science forum «Litteris et Artibus». Lviv, Ukraine, pp. 458–461.

[VECHAIN2019], VeChainThor, The public blockchain that derives its value from activities created by members within the ecosystem solving real world economic problems, 2019, https://www.vechain.org/

[ZEMLER2019], Florian Zemler, Concepts for GDPR-Compliant Processing of Personal Data on Blockchain: A Literature Review, December 2019, https://www.researchgate.net/publication/338117615_Concepts_for_GDPR-Compliant_Processing_of_Personal_Data_on_Blockchain_A_Literature_Review

[ZHANGY 2018], Zhangy, Shifa; Kim, Anne; Liu, Dianbo; Nuckchadyy, Sandeep C.; Huangy, Lauren; Masurkary, Aditya et al. (2018): Genie: A secure, transparent sharing and services platform for genetic and health data. Available online at http://arxiv.org/pdf/1811.01431v1.

[ΕΥΡΩΠΑΙΚΗ1950], Ευρωπαϊκή Σύμβαση Ανθρωπίνων Δικαιωμάτων, 1950, https://www.echr.coe.int/documents/convention_ell.pdf

[ΕΥΡΩΠΑΙΚΟΣ2000], Ευρωπαϊκός Χάρτης Θεμελιωδών Δικαιωμάτων, 2000, https://www.europarl.europa.eu/charter/pdf/text_el.pdf

[ΟΔΗΓΙΑ1995], 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, 1995, https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A31995L0046

[ΟΔΗΓΙΑ2002], Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες), 2002, https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32002L0058

[ΟΙΚΟΥΜΕΝΙΚΗ1948], Οικουμενική Διακήρυξη των Ανθρωπίνων Δικαιωμάτων, 1948, https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/grk.pdf

[ΠΡΟΣΤΑΣΙΑ1981], Προστασία των δεδομένων προσωπικού χαρακτήρα, 1981, https://www.europarl.europa.eu/ftu/pdf/el/FTU_4.2.8.pdf

[ΣΕΕ2007], Συνθήκη για την Ευρωπαϊκή Ένωση (ΣΕΕ), 2007, https://eur-lex.europa.eu/legalcontent/EL/TXT/?uri=LEGISSUM:4301855

[ΣΛΕΕ2009], Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ), 2009, https://eur-lex.europa.eu/legalcontent/EL/TXT/?uri=LEGISSUM:4301854