Πανεπιστήμιο Πειραιώς
Σχολή Τεχνολογιών Πληροφορικής και Τηλεπικοινωνιών
Τμήμα Ψηφιακών Συστημάτων

Μεταπτυχιακό Πρόγραμμα Σπουδών
Ασφάλεια Ψηφιακών Συστημάτων

Προστασία Προσωπικών Δεδομένων από το Σχεδιασμό και Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας

Επιβλέπον Καθηγητής: κ. Στέφανος Γκρίτζαλης

Δημοπούλου Στέλλα s.dimopoulou@ssl-unipi.gr MTE2007

Πειραιάς
26/06/2022

Προστασία Προσωπικών Δεδομένων από το Σχεδιασμό και Τεχνολογίες Ενίσχυσης Ιδιωτικότητας

Στέλλα Δημοπούλου

Περίληψη

Στη σημερινή εποχή, η συντριπτική πλειονότητα των ανθρώπων χρησιμοποιεί το Διαδίκτυο έτσι ώστε να ικανοποιήσει τις ανάγκες της, καθώς και να εξυπηρετηθεί από τις παρεχόμενες υπηρεσίες που προσφέρονται μέσω αυτού. Η εξάρτηση των ατόμων από τις διαδικτυακές πλατφόρμες και τις εφαρμογές αυξάνεται ολοένα και περισσότερο με την πάροδο των χρόνων, και οι άνθρωποι έχουν αρχίσει να χρησιμοποιούν μια πληθώρα πλατφορμών και υπηρεσιών για πολλούς και διαφορετικούς σκοπούς, συμπεριλαμβανομένης της μάθησης, της ψυχαγωγίας, και της κοινωνικοποίησης. Η αυξανόμενη πρόοδος των συστημάτων πληροφορικής και επικοινωνιών καθιστά τη ζωή και την καθημερινότητα των ατόμων ευκολότερη, ταχύτερη και πιο αποδοτική. Ωστόσο, η ραγδαία τεχνολογική εξέλιξη συχνά επιφέρει τεράστιες προκλήσεις ως προς την ιδιωτικότητα του ατόμου, καθώς πολλοί φορείς, επιχειρήσεις ή οργανισμοί, συλλέγουν, αποθηκεύουν και μοιράζονται προσωπικά δεδομένα με τρίτα μέρη, κυρίως εν αγνοία των ίδιων των κατόχων τους, για να ικανοποιήσουν τους στόχους, καθώς και (σε ορισμένες περιπτώσεις) τα συμφέροντά τους.

Κατά τη διάρκεια των τελευταίων ετών, η συλλογή, η διατήρηση, η χρήση και η διαβίβαση προσωπικών δεδομένων έχουν γίνει ανεξέλεγκτες από υπηρεσίες και επιχειρήσεις. Ο Γενικός Κανονισμός Προστασίας Δεδομένων έχει καθορίσει και θέσει σε ισχύ ορισμένες αρχές ιδιωτικότητας οι οποίες οφείλουν να τηρούνται κατά την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Επιπλέον, για την διασφάλιση της ιδιωτικότητας και την αποφυγή παραβιάσεων στα δεδομένα προσωπικού χαρακτήρα, πρέπει να εφαρμόζονται κατάλληλα μέτρα προστασίας, καθώς και τεχνολογίες ενίσχυσης της ιδιωτικότητας σε συστήματα και υπηρεσίες που αλληλοεπιδρούν με προσωπικά δεδομένα.

Abstract

Nowadays, the vast majority of people use the Internet in order to satisfy their needs, as well as to be benefited from the services provided through it. The individuals' reliance on online platforms and applications has grown increasingly over the years, and people are using a great deal of platforms and services for many different purposes, including learning, entertainment, and socialization. The increasing progress of information and communication systems is making people's lives easier, faster, and more efficient. However, rapid technological development often induces enormous challenges to the privacy of the individuals, as many institutions, businesses or organizations collect, store, and share personal data with third parties, mainly without the knowledge of its owners, to achieve their objectives and their interests.

Over the last few years, the collection, retention, usage, and transmission of personal data have been out of control by services and businesses. The General Data Protection Regulation has stipulated a variety of privacy principles which must be observed when processing personal data. In addition, in order to protect and maintain the privacy of the individuals, and prevent data breach incidents, appropriate privacy measures, as well as privacy-enhancing technologies, should be applied to systems and services that interact with personal data.

Πίνακας Περιεχομένων

Λίστα Πινάκων

Λίστα Εικόνων

Πίνακας Ακρωνυμίων

Πλήρης Όρος	Συντομογραφία
Advanced Encryption Standard	AES
Extensible Markup Language	XML
Internet Protocol	IP
Message-Digest Algorithm	MD5
Platform for Privacy Preferences	P3P
Secure Hash Algorithm 1	SHA-1
World Wide Web Consortium	W3C
Απόδειξη Μηδενικής Γνώσης	ΑΜΓ
Απόκρυψη Χαρακτήρων	ΑΧ
Αριθμός Φορολογικού Μητρώου	ΑΦΜ
Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα	ΑΠΔΠΧ
Ασφαλής Υπολογισμός Πολλών Μερών	ΑΥΠΜ
Γενικός Κανονισμός Προστασίας Δεδομένων	ΓΚΠΔ
Διαφορική Ιδιωτικότητα	ΔΙ
Έμμεσο Αναγνωριστικό	ΕΑ
Επίπεδο Γενίκευσης	ΕΓ
Κάπως Ομομορφική Κρυπτογράφηση	ΚΟΚ
Μερικώς Ομομορφική Κρυπτογράφηση	ΜΟΚ
Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια	ΕΝΙΣΑ
Πλήρως Ομομορφική Κρυπτογράφηση	ΠΟΚ
Προστασία Δεδομένων από το Σχεδιασμό	ΠΔΣ
Προστασία Δεδομένων εξ Ορισμού	ΠΔΟ

Πίνακας Ορολογιών

Ελληνικός Όρος	Αγγλικός Όρος
k-ανωνυμία	k-anonymity
ℓ-διαφορετικότητα	ℓ-diversity
Αναδιοργάνωση Δεδομένων	Shuffling
Αντικατάσταση Δεδομένων	Substitution
Ανώνυμα Διαπιστευτήρια	Anonymous Credentials
Απόδειξη Μηδενικής Γνώσης	Zero-Knowledge Proof
Απόκρυψη Δεδομένων	Suppression
Απόκρυψη Χαρακτήρων	Character Masking
Αριθμητική Διακύμανση και Διακύμανση Ημερομηνίας	Numeric and Date Variance
Ασφάλεια από άκρο σε άκρο – Πλήρης προστασία κύκλου ζωής	End-to-End Security – Full Lifecycle Protection
Ασφαλής Υπολογισμός Πολλών Μερών	Secure Multi-Party Computation
Γενίκευση Δεδομένων	Generalization
Διαδραστική Απόδειξη Μηδενικής Γνώσης	Interactive Zero-Knowledge Proof
Διακριτικό	Token
Διακριτικός Έλεγχος Προσπέλασης	Discretionary Access Control
Διακριτοποίηση	Tokenization
Διαπιστευτήρια βάσει Χαρακτηριστικών	Attribute-Based Credentials
Διαφορική Ιδιωτικότητα	Differential Privacy
Έλεγχος Προσπέλασης βάσει Ρόλου	Role-Based Access Control
Έλεγχος Προσπέλασης βάσει Χαρακτηριστικών	Attribute-Based Access Control
Εναλλαγή Δεδομένων	Swapping
Ενσωματωμένος Πράκτορας Λογισμικού Προστασίας Προσωπικών Δεδομένων	Privacy Incorporated Software Agent

Επίθεση Ασύμμετρης Κατανομής	Skewness Attack
Επίθεση Γνωστικού Υπόβαθρου	Background Knowledge Attack
Επίθεση Ομοιογένειας	Homogeneity Attack
Επίθεση Ομοιότητας Χαρακτηριστικών	Similarity Attack
Κάπως Ομομορφική Κρυπτογράφηση	Somewhat Homomorphic Encryption
Κατακερματισμός	Hashing
Μερικώς Ομομορφική Κρυπτογράφηση	Partially Homomorphic Encryption
Μη συνδεσιμότητα	Unlinkability
Μη-διαδραστική Απόδειξη Μηδενικής Γνώσης	Non-interactive Zero-Knowledge Proof
Ομομορφική Κρυπτογράφηση	Homomorphic Encryption
Πλατφόρμα Προτιμήσεων Ιδιωτικότητας	Platform for Privacy Preferences
Πλήρης λειτουργικότητα	Full Functionality
Πλήρως Ομομορφική Κρυπτογράφηση	Fully Homomorphic Encryption
Προορατική, όχι ως Αντίδραση. Προληπτική, όχι Διορθωτική	Proactive not Reactive; Preventative not Remedial
Προσθήκη Θορύβου	Noise Addition
Προστασία Δεδομένων από το Σχεδιασμό	Privacy by Design
Προστασία Δεδομένων ενσωματωμένη από το Σχεδιασμό	Privacy Embedded into Design
Προστασία Δεδομένων εξ Ορισμού	Privacy by Default
Προστασία Δεδομένων ως Προεπιλεγμένη Ρύθμιση	Privacy as the Default Setting
Σαφήνεια και Διαφάνεια	Visibility and Transparency
Σεβασμός της ιδιωτικότητας των χρηστών	Respect for User Privacy
Συνθετικά Δεδομένα	Synthetic Data
Σχεδόν-Αναγνωριστικό	Quasi-Identifier
Τεχνολογίες Ενίσχυσης Ιδιωτικότητας	Privacy-Enhancing Technologies
Υποχρεωτικός Έλεγχος Προσπέλασης	Mandatory Access Control

Εισαγωγή

Οι ραγδαίες τεχνολογικές εξελίξεις, που έχουν πραγματοποιηθεί τα τελευταία χρόνια, έχουν επηρεάσει τον τρόπο με τον οποίο κοινοποιούνται και υποβάλλονται σε επεξεργασία τα προσωπικά δεδομένα, ενώ παράλληλα έχουν προωθήσει καινούριες τεχνικές και μεθόδους που αποσκοπούν στην ανταλλαγή, επεξεργασία και αποθήκευση κάθε είδους δεδομένων. Η συνεχής εξέλιξη της τεχνολογίας έχει δημιουργήσει νέα μοντέλα επεξεργασίας δεδομένων, τα οποία συμπεριλαμβάνουν και δεδομένα προσωπικού χαρακτήρα, για την εκπλήρωση και την ικανοποίηση των αναγκών του φυσικού προσώπου [1]. Ωστόσο, πέρα από τα οφέλη που αυτή έχει επιφέρει, έχει εισαγάγει επίσης και κάποιες καινούριες απειλές και δυσκολίες προς τον τελικό χρήστη, ο οποίος αδυνατεί να κατανοήσει και να ελέγξει την επεξεργασία των δεδομένων τα οποία έχει στην κατοχή του και τον αφορούν.

Ο όρος «ιδιωτικότητα» θεωρείται ως μια αφηρημένη έννοια, και έχει αποδοθεί πληθώρα ορισμών και εννοιών, οι οποίοι προσπαθούν να την αποτυπώσουν. Το 1890, οι Warren και Brandeis όρισαν την ιδιωτικότητα ως *«το δικαίωμα του να είσαι μόνος»* (the right to be let alone) στο άρθρο τους με τίτλο «Το Δικαίωμα στην Ιδιωτικότητα» [2]. Ύστερα από την απόδοση αυτού του ορισμού ακολούθησαν και άλλοι, αλλά εκείνος που αποτέλεσε βάση για πολλές σύγχρονες αρχές προστασίας της ιδιωτικότητας προτάθηκε από τον Alan Westin στο βιβλίο του με τίτλο «Ιδιωτικότητα και Ελευθερία» [3]. Ο Westin όρισε την ιδιωτικότητα ως *«την απαίτηση των ατόμων, των ομάδων ή των ιδρυμάτων να καθορίζουν οι ίδιοι πότε, πώς και σε ποιο βαθμό οι πληροφορίες σχετικά με αυτά κοινοποιούνται σε άλλους»*, δίνοντας ιδιαίτερη έμφαση στον έλεγχο των υποκειμένων των δεδομένων επί των δεδομένων τους.

Η ιδιωτικότητα είναι μια ευρεία και πολύπλοκη έννοια, καθώς η κατανόηση και η αντίληψή της διαφέρει από άτομο σε άτομο, και η επιβολή της απαιτεί προσπάθειες τόσο από τη νομοθεσία όσο και από τις τεχνολογίες και τα συστήματα που αλληλοεπιδρούν με δεδομένα προσωπικού χαρακτήρα [4]. Οι νόμοι και οι αρχές περί προστασίας της ιδιωτικότητας συμβάλλουν στην επιβολή της συμμόρφωσης και της λογοδοσίας των οργανισμών προς τα υποκείμενα των δεδομένων όσον αφορά την προστασία των προσωπικών δεδομένων. Αντιθέτως, οι Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας υποστηρίζουν τις βασικές αρχές που διέπουν τους νόμους ιδιωτικότητας, και επιτρέπουν την εφαρμογή στρατηγικών και μέτρων προστασίας της ιδιωτικότητας στα συστήματα και τις υπηρεσίες πληροφορικής και επικοινωνιών [4].

Επιπροσθέτως, και σύμφωνα με τα παραπάνω, η ιδιωτικότητα πρέπει να λαμβάνεται υπόψη, και να προστατεύεται, από την αρχή της ανάπτυξης ενός συστήματος και καθ' όλη τη διάρκεια ζωής του, δηλαδή από τα πρώτα στάδια σχεδιασμού έως ότου αυτό να τεθεί σε παραγωγική λειτουργία. Η προσέγγιση αυτή είναι ωφέλιμη όταν πρόκειται για επεξεργασία δεδομένων προσωπικού χαρακτήρα. Ωστόσο, δεν συνοδεύεται από μηχανισμούς που να ενσωματώνουν την ιδιωτικότητα στις διαδικασίες ανάπτυξης ενός συστήματος [5]. Η προσέγγιση της «Προστασίας Δεδομένων από το Σχεδιασμό» εξετάστηκε από την Ευρωπαϊκή Επιτροπή και ενσωματώθηκε στο άρθρο 25 του Γενικού Κανονισμού Προστασίας των Δεδομένων [6]. Το άρθρο 25, που αφορά στην «Προστασία Δεδομένων από το Σχεδιασμό και εξ Ορισμού», υποχρεώνει τις οντότητες που είναι αρμόδιες για την επεξεργασία δεδομένων προσωπικού χαρακτήρα να εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα και διαδικασίες τόσο κατά τον προσδιορισμό των μέσων επεξεργασίας όσο και κατά την διάρκεια της επεξεργασίας αυτής.

Βασικές Έννοιες – Ορισμοί

Σε αυτή την ενότητα αναφέρονται κάποιες βασικές έννοιες και ορισμοί, όπως αυτοί έχουν ορισθεί και περιγραφεί:

- στο πρότυπο ISO 29100:2011 [7] και στον Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ) [6], όσον αφορά την Ιδιωτικότητα (Privacy),
- στο πρότυπο ISO 27000:2018 [8], όσον αφορά την Ασφάλεια (Security),

καθώς και κάποιες επιπρόσθετες έννοιες, οι οποίες χρησιμοποιούνται καθ' όλη τη διάρκεια της παρούσας διπλωματικής εργασίας.

Ιδιωτικότητα

Βάσει του προτύπου ISO 29100:2011 και του Γενικού Κανονισμού Προστασίας Δεδομένων, έχουν ορισθεί οι έννοιες ως ακολούθως:

Δεδομένα προσωπικού χαρακτήρα: Τα δεδομένα προσωπικού χαρακτήρα, ή αλλιώς προσωπικά δεδομένα, αφορούν σε οποιαδήποτε πληροφορία η οποία μπορεί να οδηγήσει, είτε άμεσα είτε έμμεσα, στην ταυτοποίηση ενός φυσικού προσώπου. Παραδείγματα τέτοιων δεδομένων είναι το όνομα, το επώνυμο, ή ο αριθμός δελτίου ταυτότητας, ενός φυσικού προσώπου [6]. Κατά το πρότυπο ISO 29100:2011 τα δεδομένα προσωπικού χαρακτήρα ορίζονται ως αναγνωριστικά στοιχεία ταυτότητας [7].

Υποκείμενο δεδομένων: Υποκείμενο των δεδομένων μπορεί να θεωρηθεί οποιοδήποτε φυσικό πρόσωπο, το οποίο έχει συσχετιστεί με ένα σύνολο από δεδομένα προσωπικού χαρακτήρα τα οποία το περιγράφουν [6] [7].

Υπεύθυνος επεξεργασίας: Ο υπεύθυνος επεξεργασίας είναι οποιοδήποτε φυσικό ή νομικό πρόσωπο, υπηρεσία, φορέας ή δημόσια αρχή, που είναι υπεύθυνο για τον προσδιορισμό του σκοπού και του τρόπου επεξεργασίας των δεδομένων προσωπικού χαρακτήρα των υποκειμένων των δεδομένων. Ο σκοπός, καθώς και τα μέσα της επεξεργασίας δεδομένων, οφείλουν να είναι νόμιμα και να προβλέπονται από την νομοθεσία [6]. Υπό περιπτώσεις, οι υπεύθυνοι επεξεργασίας ενδέχεται να είναι περισσότεροι από έναν, και να έχουν ως αρμοδιότητα την επεξεργασία του ίδιου συνόλου δεδομένων προσωπικού χαρακτήρα, ή την ίδια επεξεργασία δεδομένων η οποία αφορά είτε στον ίδιο είτε σε διαφορετικό σκοπό επεξεργασίας. Σε τέτοιου είδους περιπτώσεις, οι από κοινού υπεύθυνοι επεξεργασίας οφείλουν να συνεργάζονται μεταξύ τους, να διαχωρίζουν τις αρμοδιότητές τους, καθώς και να τηρούν τις αρχές ιδιωτικότητας σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα [7]. Ο υπεύθυνος επεξεργασίας είναι επίσης εκείνος που θα αποφασίσει και θα ορίσει ποιος θα πραγματοποιήσει την επεξεργασία των δεδομένων. Η εν λόγω επεξεργασία μπορεί να ανατεθεί είτε μερικώς είτε εξ' ολοκλήρου σε έναν ή περισσότερους δικαιούχους ιδιωτικότητας [7].

Εκτελών την επεξεργασία: Ο εκτελών την επεξεργασία είναι οποιοδήποτε φυσικό ή νομικό πρόσωπο, υπηρεσία, φορέας ή δημόσια αρχή, που επεξεργάζεται τα δεδομένα προσωπικού χαρακτήρα του υποκειμένου των δεδομένων για λογαριασμό του υπεύθυνου επεξεργασίας. Ειδικότερα, ο εκτελών την επεξεργασία δρα εκ μέρους του υπεύθυνου επεξεργασίας και επεξεργάζεται τα δεδομένα σύμφωνα με τις οδηγίες που εκείνος έχει ορίσει [6].

Ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα: Οι ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα, ή αλλιώς τα ευαίσθητα δεδομένα, αφορούν δεδομένα τα οποία είτε είναι ευαίσθητα στη φύση τους, είτε έχουν σημαντική επίπτωση στα υποκείμενα των

δεδομένων εφόσον αποκαλυφθούν σε τρίτους. Τα ευαίσθητα δεδομένα χρήζουν περισσότερης προσοχής και προστασίας, και πρέπει να είναι εμπιστευτικά και να προστατεύονται από τη μη εξουσιοδοτημένη προσπέλαση. Παραδείγματα τέτοιων δεδομένων είναι οι θρησκευτικές πεποιθήσεις, οι πολιτικές απόψεις, και τα δεδομένα υγείας. Σε αυτό το σημείο αξίζει να σημειωθεί ότι οι ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα έχουν τον ίδιο βαθμό ευαισθησίας, και δεν υφίσταται κάποιος διαχωρισμός μεταξύ αυτών, καθώς όλα θεωρούνται το ίδιο ευαίσθητα [7].

Τα ευαίσθητα δεδομένα θα πρέπει να διατηρούνται ξεχωριστά από τα δεδομένα προσωπικού χαρακτήρα, ενώ παράλληλα απαιτείται παραπάνω προστασία κατά την επεξεργασία των ευαίσθητων δεδομένων, καθώς διακυβεύεται η ελευθερία του ατόμου και υπάρχει μεγάλο ρίσκο για καταπάτηση των ανθρωπίνων δικαιωμάτων [6] [7]. Υπάρχουν περιπτώσεις και περιβάλλοντα, όπου η επεξεργασία ευαίσθητων δεδομένων απαγορεύεται βάσει νόμου, ακόμα και αν το υποκείμενο των δεδομένων έχει συγκατατεθεί για την εν λόγω επεξεργασία. Από την άλλη, υπάρχουν και περιπτώσεις όπου πρέπει να υλοποιούνται σχετικά μέτρα προστασίας όταν πρόκειται για την επεξεργασία τέτοιων δεδομένων, όπως είναι η ανωνυμοποίηση, η ψευδωνυμοποίηση και η κρυπτογράφηση [6] [7].

Επεξεργασία: Ο όρος «επεξεργασία» αναφέρεται σε οποιαδήποτε λειτουργία ή πράξη που μπορεί να εφαρμοστεί στα δεδομένα προσωπικού χαρακτήρα. Παραδείγματα επεξεργασίας είναι η συλλογή, η αποθήκευση, η διαβίβαση, και η καταστροφή δεδομένων, με ή χωρίς τη χρήση αυτοματοποιημένων μέσων [6].

Τρίτο μέρος: Είναι οποιαδήποτε οντότητα, *οποιοδήποτε φυσικό ή νομικό πρόσωπο, υπηρεσία, φορέας ή δημόσια αρχή,* εκτός του υποκειμένου των δεδομένων, του υπεύθυνου επεξεργασίας και του εκτελούντα την επεξεργασία [6].

Πολιτική ιδιωτικότητας: Η πολιτική ιδιωτικότητας περιέχει μια σειρά από κανόνες οι οποίοι έχουν εκφραστεί από τον υπεύθυνο επεξεργασίας και αφορούν στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα [7]. Περιλαμβάνει, μεταξύ άλλων, το σκοπό επεξεργασίας, καθώς και τα προσωπικά δεδομένα τα οποία επρόκειτο να τεθούν υπό επεξεργασία για την επίτευξή του. Η πολιτική ιδιωτικότητας αποτελεί επίσης καθοδήγηση για τον εκτελών την επεξεργασία.

Δικαιούχος ιδιωτικότητας: Ο δικαιούχος ιδιωτικότητας είναι οποιοδήποτε φυσικό ή νομικό πρόσωπο, οργανισμός, φορέας ή δημόσια αρχή, ο όποιος επεξεργάζεται ή επηρεάζεται από την επεξεργασία δεδομένων προσωπικού χαρακτήρα [7]. Οι δικαιούχοι ιδιωτικότητας αναφέρονται και ως ενδιαφερόμενα μέρη, και μπορεί να είναι τα υποκείμενα των δεδομένων ή οι φορείς που επεξεργάζονται τα προσωπικά τους δεδομένα.

Ασφάλεια

Βάσει του προτύπου ISO 27000:2018 έχουν ορισθεί οι παρακάτω έννοιες.

Ταυτοποίηση: Είναι μια διαδικασία κατά την οποία δηλώνει μια οντότητα – *ένας χρήστης* – την ταυτότητά του στο πληροφοριακό σύστημα. Αυτό μπορεί να επιτευχθεί, για παράδειγμα, με το όνομα χρήστη (username) ή κάποιο μοναδικό αναγνωριστικό [8] [9].

Αυθεντικοποίηση: Είναι η διαδικασία επαλήθευσης της ταυτότητας του χρήστη και απαιτεί κάποια επιπλέον πληροφορία που να επιβεβαιώνει την ταυτότητά του [8] [9]. Για παράδειγμα, η αυθεντικοποίηση μπορεί να επιτευχθεί με την ορθή εισαγωγή του κωδικού

πρόσβασης του χρήστη, βάσει του ονόματος χρήστη (username) που είχε δηλώσει προηγουμένως κατά την ταυτοποίησή του στο σύστημα [9].

Εξουσιοδότηση: Μόλις πραγματοποιηθεί η ταυτοποίηση και η αυθεντικοποίηση ενός χρήστη στο πληροφοριακό σύστημα, ο χρήστης θεωρείται πλέον ως εξουσιοδοτημένος χρήστης αυτού του συστήματος. Έτσι, βάσει της ταυτότητάς του, του ρόλου του ή κάποιων χαρακτηριστικών του, ορίζονται τα δικαιώματα που αυτός έχει στο πληροφοριακό σύστημα [9].

Έλεγχος προσπέλασης: Ο έλεγχος προσπέλασης υπαγορεύει ποιος επιτρέπεται να έχει πρόσβαση και σε ποιους υπολογιστικούς ή διαδικτυακούς πόρους ενός πληροφοριακού συστήματος [10] [8]. Έχει ως στόχο να περιορίσει την πρόσβαση των εξουσιοδοτημένων χρηστών σε δεδομένα και πόρους ενός συστήματος, καθώς και να ελαχιστοποιήσει τους κινδύνους ασφαλείας από μη εξουσιοδοτημένη πρόσβαση στα εν λόγω πληροφοριακά συστήματα [11] [12]. Μόνο όσοι έχουν αυθεντικοποιηθεί και είναι εξουσιοδοτημένοι από το σύστημα, θα έχουν τη δυνατότητα πρόσβασης σε δεδομένα του οργανισμού [12] [8].

Εμπιστευτικότητα: Ο όρος «εμπιστευτικότητα» αφορά στην προστασία της πληροφορίας έναντι της μη εξουσιοδοτημένης προσπέλασης ή αποκάλυψής της [8].

Ακεραιότητα: Ο όρος «ακεραιότητα» αφορά στην προστασία της πληροφορίας έναντι της μη εξουσιοδοτημένης τροποποίησής της [8].

Διαθεσιμότητα: Ο όρος «διαθεσιμότητα» αφορά στην διαθεσιμότητα και προσπέλαση συστημάτων ή πληροφοριών από εξουσιοδοτημένους χρήστες, υπό οποιαδήποτε συνθήκη και ανά πάσα χρονική στιγμή [8].

Λοιπές Έννοιες

Σε αυτή την ενότητα παρουσιάζονται επιπρόσθετες – *χρήσιμες* – έννοιες βάσει της σχετικής βιβλιογραφίας που αναγράφεται παρακάτω.

Άμεσα αναγνωριστικά: Ένα άμεσο αναγνωριστικό αφορά σε κάποια συγκεκριμένη πληροφορία που σχετίζεται με ένα μεμονωμένο άτομο, όπως το όνομα, η διεύθυνση ή ο αριθμός δελτίου ταυτότητας [13] [14]. Τα άμεσα αναγνωριστικά επιτρέπουν επί της ουσίας την άμεση ταυτοποίηση ενός φυσικού προσώπου [14]. Ωστόσο, εφόσον τέτοιου είδους αναγνωριστικά δεν είναι απαραίτητα για στατιστικούς ή ερευνητικούς σκοπούς, δεν (πρέπει να) συλλέγονται εξ αρχής από τα υποκείμενα των δεδομένων.

Έμμεσα αναγνωριστικά: Τα έμμεσα αναγνωριστικά (ΕΑ), ή αλλιώς σχεδόν-αναγνωριστικά (quasi-identifiers), αφορούν σε μια ομάδα – *σε ένα ελάχιστο σύνολο* – χαρακτηριστικών, το οποίο ενδέχεται, είτε μεμονωμένα είτε σε συνδυασμό με άλλα χαρακτηριστικά, να ταυτοποιήσει ένα φυσικό πρόσωπο [15] [16]. Παραδείγματα τέτοιων αναγνωριστικών είναι το φύλο και η ηλικία.

Κλάση ισοδυναμίας: Ένα (υπο)σύνολο χαρακτηριστικών ορίζεται ως κλάση ισοδυναμίας όταν όλες οι εγγραφές του συνόλου αυτού έχουν τις ίδιες τιμές στα έμμεσα αναγνωριστικά, δηλαδή στα χαρακτηριστικά τα οποία κατηγοριοποιούνται ως έμμεσα αναγνωριστικά βάσει του προαναφερθέντος ορισμού [16].

Αρχές Ιδιωτικότητας

Οι αρχές ιδιωτικότητας [6] [7] είναι ένα σύνολο από αξίες που διέπουν την προστασία των δεδομένων προσωπικού χαρακτήρα, όταν αυτά γίνονται αντικείμενο επεξεργασίας. Η υλοποίηση των αρχών ιδιωτικότητας έχει ως στόχο την καθοδήγηση του οργανισμού σχετικά με το σχεδιασμό και την ανάπτυξη ενός συστήματος το οποίο αλληλοεπιδρά με δεδομένα προσωπικού χαρακτήρα. Ο υπεύθυνος επεξεργασίας είναι η αρμόδια οντότητα που πρέπει να διασφαλίσει ότι οι αρχές αυτές τηρούνται καθ' όλη τη διάρκεια της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα.

Σε αυτή την ενότητα παρουσιάζονται οι αρχές ιδιωτικότητας όπως αυτές έχουν ορισθεί κατά το πρότυπο ISO 29100:2011 [7], και πρέπει να εφαρμόζονται όταν πρόκειται για επεξεργασία δεδομένων προσωπικού χαρακτήρα. Οι έντεκα αρχές ιδιωτικότητας του προτύπου αντιστοιχούν στις επτά αρχές του Γενικού Κανονισμού Προστασίας Δεδομένων [6], και αναφέρονται στο πέμπτο άρθρο του δευτέρου κεφαλαίου του κανονισμού (Πίνακας 1).

Γενικός Κανονισμός Προστασίας Δεδομένων	Πρότυπο ISO 29100:2011
Νομιμότητα, αντικειμενικότητα και διαφάνεια	Ανοιχτότητα, διαφάνεια και γνωστοποίηση
Περιορισμός του σκοπού	Συγκατάθεση και επιλογή
	Νομιμότητα του σκοπού
	Συμμόρφωση με την ιδιωτικότητα
Ελαχιστοποίηση των δεδομένων	Περιορισμός της συλλογής
	Ελαχιστοποίηση δεδομένων
Ακρίβεια	Ακρίβεια και ποιότητα
	Ατομική συμμετοχή και πρόσβαση
Περιορισμός της περιόδου αποθήκευσης	Περιορισμός χρήσης, διατήρησης, και αποκάλυψης
Ακεραιότητα και εμπιστευτικότητα	Ασφάλεια πληροφοριών
Λογοδοσία	Λογοδοσία

Πίνακας 1: Αντιστοίχιση Αρχών Ιδιωτικότητας

Συγκατάθεση και επιλογή

Η αρχή της συγκατάθεσης αναφέρεται στο δικαίωμα επιλογής που οφείλει να έχει το υποκείμενο των δεδομένων σχετικά με το αν θα επιτρέψει ή θα απορρίψει την εν λόγω επεξεργασία στα δεδομένα προσωπικού χαρακτήρα που το αφορούν. Οι μόνες περιπτώσεις όπου το υποκείμενο των δεδομένων δεν θα ερωτάται σχετικά με το αν επιθυμεί να συγκατατεθεί, είναι εκείνες που βάσει της ισχύουσας νομοθεσίας τα δεδομένα προσωπικού χαρακτήρα απαιτούνται για την ικανοποίηση ενός συγκεκριμένου σκοπού χωρίς να υπάρχει η ανάγκη ή η απαίτηση για συγκατάθεση. Παρόλα αυτά, ο υπεύθυνος επεξεργασίας οφείλει να ενημερώνει τα υποκείμενα των δεδομένων, σχετικά με την επεξεργασία την οποία έχουν

υποστεί τα δεδομένα τους, καθώς επίσης πρέπει να τους γνωστοποιεί τόσο το σκοπό όσο και τα μέσα επεξεργασίας αυτών.

Το υποκείμενο των δεδομένων θα πρέπει πρωτίστως να έχει πληροφορηθεί σχετικά με τα δεδομένα που θα χρειαστεί να παραχωρήσει για την εν λόγω επεξεργασία, τον σκοπό, καθώς και τον τρόπο της επεξεργασίας αυτής, και ύστερα, αν και εφόσον το επιθυμεί, να δώσει τη συγκατάθεσή του. Η ενημέρωση του υποκειμένου των δεδομένων οφείλει να γίνεται πριν τη λήψη της συγκατάθεσης, με τρόπο απλό και κατανοητό για το ίδιο το υποκείμενο, έτσι ώστε να είναι σε θέση να κατανοήσει πλήρως το κείμενο με το οποίο πρόκειται να συναινέσει. Επιπλέον, πρέπει να του παρέχεται και σχετική επεξήγηση αναφορικά με τις επιπτώσεις που ενδέχεται να υπάρχουν σε περίπτωση αποδοχής ή άρνησης παραχώρησης της συγκατάθεσής του.

Η λήψη της συγκατάθεσης πρέπει να γίνεται μέσω της διαδικασίας «opt-in», κατά την οποία η προεπιλεγμένη τιμή σχετικά με το αν επιθυμεί το υποκείμενο των δεδομένων να συγκατατεθεί είναι «όχι». Βάσει αυτού, δίνεται η δυνατότητα στο υποκείμενο των δεδομένων να συγκατατεθεί ρητά για τη συλλογή και επεξεργασία των δεδομένων του, εφόσον έχει πληροφορηθεί καταλλήλως όπως αναφέρθηκε προηγουμένως. Η εν λόγω συγκατάθεση δεν ζητείται σε περιπτώσεις όπου η νομοθεσία προβλέπει την επεξεργασία των δεδομένων προσωπικού χαρακτήρα χωρίς τη συγκατάθεση του φυσικού προσώπου. Πέρα από την opt-in συγκατάθεση, η οποία πρέπει να γίνεται με εύκολο τρόπο ως προς το υποκείμενο των δεδομένων, η διαδικασία άρσης της συγκατάθεσης θα πρέπει να είναι εξίσου εύκολη και να μην υπόκειται σε κάποιο κόστος. Σε περιπτώσεις άρσης της συγκατάθεσης, τα δεδομένα θα πρέπει να εξαιρούνται από κάθε επεξεργασία, εκτός αν υπάρχει κάποια νομική βάση η οποία να ισχυρίζεται το αντίθετο.

Νομιμότητα του σκοπού

Η αρχή της νομιμότητας του σκοπού αφορά κυρίως στη σύννομη και θεμιτή επεξεργασία δεδομένων προσωπικού χαρακτήρα. Για την τήρηση αυτής της αρχής θα πρέπει να πληρούνται κάποιες προϋποθέσεις, όπως αυτές αναγράφονται παρακάτω.

1. Πρέπει να διασφαλίζεται ότι ο σκοπός επεξεργασίας στηρίζεται σε κάποια νομική βάση και συμμορφώνεται με την ισχύουσα νομοθεσία.
2. Το υποκείμενο των δεδομένων πρέπει να είναι πλήρως ενημερωμένο για τα δεδομένα προσωπικού χαρακτήρα που επρόκειτο να συλλεχθούν, πριν να γίνει η συλλογή τους, καθώς και για τους σκοπούς και τα μέσα επεξεργασίας αυτών των δεδομένων.
3. Ο τρόπος με τον οποίο θα γίνει η ενημέρωση του υποκειμένου των δεδομένων θα πρέπει να είναι πλήρως κατανοητός, σαφής και κατάλληλα περιγεγραμμένος, με σχετικές σαφείς επεξηγήσεις όπου αυτό απαιτείται (π.χ. όταν πρόκειται για επεξεργασία ευαίσθητων δεδομένων).
4. Η επεξεργασία ευαίσθητων δεδομένων χρήζει περισσότερης προσοχής, και ο σκοπός επεξεργασίας οφείλει να στηρίζεται σε κάποια νομική βάση, καθώς αν η επεξεργασία δεν είναι σύμφωνη με την ισχύουσα νομοθεσία, δεν θα μπορέσει να εφαρμοστεί οποιουδήποτε είδους επεξεργασία στα δεδομένα αυτά.

Περιορισμός της συλλογής

Η αρχή του περιορισμού της συλλογής αφορά στη συλλογή μόνο των απαραίτητων ελάχιστων δεδομένων προσωπικού χαρακτήρα για την ικανοποίηση κάποιου νόμιμου σκοπού επεξεργασίας. Βάσει αυτής της αρχής, απαγορεύεται να συλλέγονται παραπάνω

δεδομένα από τα ελάχιστα δυνατά για την ικανοποίηση του εκάστοτε σκοπού επεξεργασίας. Ο περιορισμός της συλλογής αναφέρεται τόσο στον περιορισμό της ποσότητας όσο και στον περιορισμό του είδους των δεδομένων προσωπικού χαρακτήρα. Είναι πολύ σημαντικό, να προσδιορίζουν οι οργανισμοί από νωρίς, ποιο θα είναι το σύνολο των δεδομένων προσωπικού χαρακτήρα που θα χρειαστούν για την εκπλήρωση του σκοπού επεξεργασίας, πριν να γίνει η συλλογή αυτού. Μαζί με τα δεδομένα προσωπικού χαρακτήρα, πρέπει να καταγράφεται και ο τύπος των δεδομένων, καθώς και ο λόγος συλλογής τους.

Σε περίπτωση που ο υπεύθυνος επεξεργασίας θελήσει να συλλέξει κάποια επιπλέον δεδομένα, για κάποιο διαφορετικό σκοπό από αυτό που είχε συμφωνήσει το υποκείμενο των δεδομένων για την παροχή της εκάστοτε υπηρεσίας, ο υπεύθυνος επεξεργασίας οφείλει να ενημερώσει εκ νέου το υποκείμενο των δεδομένων για τα δεδομένα τα οποία επιθυμεί να χρησιμοποιήσει, και για το σκοπό αυτής της συλλογής, και να ζητήσει εκ νέου τη συγκατάθεσή του. Το υποκείμενο των δεδομένων θα πρέπει να έχει τη δυνατότητα να επιλέξει αν επιθυμεί να συγκατατεθεί ή όχι, εφόσον έχει ενημερωθεί πλήρως για τους σκοπούς και τα μέσα επεξεργασίας των δεδομένων, και μόνο αν δώσει ρητά τη συγκατάθεσή του θα μπορέσει ο υπεύθυνος επεξεργασίας να προβεί σε επεξεργασία των δεδομένων του.

Ελαχιστοποίηση δεδομένων

Η αρχή του περιορισμού της συλλογής, προηγουμένως, είχε να κάνει με την ελαχιστοποίηση των δεδομένων αυτών κάθε αυτών, έτσι ώστε να μην συλλέγονται παραπάνω δεδομένα από τα ελάχιστα δυνατά για την παροχή μιας υπηρεσίας. Η αρχή της ελαχιστοποίησης σε αυτή την περίπτωση, ασχολείται με την ελαχιστοποίηση των διαδικασιών επεξεργασίας που υφίστανται τα δεδομένα, καθώς και τον περιορισμό των δικαιούχων ιδιωτικότητας και των ατόμων που έχουν πρόσβαση σε αυτά και τα επεξεργάζονται. Βάσει αυτού, πρέπει να γίνεται υιοθέτηση της αρχής «need-to-know» και άρα τα άτομα, στα οποία δεν υπάρχει λόγος να αποκαλυφθούν τα δεδομένα προσωπικού χαρακτήρα του υποκειμένου των δεδομένων, να μην έχουν δικαίωμα προσπέλασης αυτών των δεδομένων. Μόνο ο υπεύθυνος και ο εκτελών την επεξεργασία θα μπορούν να προσπελάζουν τα προσωπικά δεδομένα, για την πραγματοποίηση μιας επεξεργασίας, η οποία υπόκειται σε κάποιο συγκεκριμένο σκοπό. Επιπλέον, τα δεδομένα προσωπικού χαρακτήρα θα πρέπει να διαγράφονται όταν περατωθεί ο σκοπός επεξεργασίας, ή μόλις εκπνεύσει το χρονικό διάστημα διατήρησης των δεδομένων, και εφόσον δεν υπάρχει κάποια νομική βάση η οποία να απαιτεί τη διατήρησή τους.

Περιορισμός χρήσης, διατήρησης, και αποκάλυψης

Η αρχή του περιορισμού της χρήσης, διατήρησης και αποκάλυψης αναφέρεται μόνο σε δεδομένα προσωπικού χαρακτήρα τα οποία απαιτούνται για την εκπλήρωση ενός σαφώς καθορισμένου και νόμιμου σκοπού επεξεργασίας. Ειδικότερα,

- Ο περιορισμός της χρήσης των δεδομένων προσωπικού χαρακτήρα αφορά μόνο στην απαραίτητη επεξεργασία που τα δεδομένα αυτά θα υποστούν, και η οποία έχει προσδιοριστεί από τον υπεύθυνο επεξεργασίας πριν τα δεδομένα συλλεχθούν από το υποκείμενο των δεδομένων, για την ικανοποίηση ενός συγκεκριμένου σκοπού επεξεργασίας. Μόνο σε περιπτώσεις όπου η νομοθεσία το επιβάλλει, μπορεί να γίνει χρήση αυτών των δεδομένων για κάποιο διαφορετικό σκοπό επεξεργασίας.
- Η διατήρηση των δεδομένων προσωπικού χαρακτήρα πρέπει να υφίσταται μόνο για το χρονικό περιθώριο το οποίο έχει συμφωνηθεί με το υποκείμενο των δεδομένων κατά την παραχώρηση της συγκατάθεσής του. Μόλις εκπληρωθεί ο σκοπός για τον οποίο τα δεδομένα αυτά συλλέχθηκαν, τα δεδομένα προσωπικού χαρακτήρα θα

πρέπει να εξαιρούνται από οποιαδήποτε επεξεργασία και να διαγράφονται με ασφαλή τρόπο ή να ανωνυμοποιούνται (αν και εφόσον αυτό προβλέπεται βάσει του κειμένου της συγκατάθεσης). Σύμφωνα με το άρθρο 89, παράγραφος 1, του Γενικού Κανονισμού Προστασίας Δεδομένων [6], ενδέχεται να απαιτείται η διατήρηση των δεδομένων για περισσότερο χρονικό διάστημα από το προβλεπόμενο. Σε τέτοιες περιπτώσεις, τα δεδομένα αυτά θα πρέπει να διατηρούνται και να αποθηκεύονται με ασφάλεια, και να επεξεργάζονται μόνο για τους προβλεπόμενους σκοπούς.

- Σε περίπτωση όπου υπάρχει διαβίβαση των δεδομένων σε κάποια άλλη χώρα, ο υπεύθυνος επεξεργασίας οφείλει να ενημερώνεται για τις απαιτήσεις που αφορούν τις διασυνοριακές διαβιβάσεις. Ειδικότερα, όταν τα δεδομένα διαβιβάζονται σε χώρες εκτός Ευρωπαϊκής Ένωσης, ο υπεύθυνος επεξεργασίας θα πρέπει να είναι ενήμερος για την νομοθεσία η οποία εφαρμόζεται στη χώρα αυτή, έτσι ώστε να μην πλήττεται η ασφάλεια και να μη διακυβεύεται η προστασία των δεδομένων.

Ακρίβεια και ποιότητα

Η αρχή της ακρίβειας και ποιότητας των δεδομένων προσωπικού χαρακτήρα σχετίζεται με τη διασφάλιση ότι τα δεδομένα που υφίστανται επεξεργασία είναι πλήρη, ακριβή, ενημερωμένα και κατάλληλα, βάσει του σκοπού επεξεργασίας που έχει ορισθεί. Μόνο σε περιπτώσεις όπου υπάρχει κάποια νομική βάση, η οποία απαιτεί τη διατήρηση μη επικαιροποιημένων δεδομένων, μπορούν να τηρούνται τέτοιου είδους δεδομένα για κάποιο σκοπό επεξεργασίας. Επιπλέον, όταν τα δεδομένα συλλέγονται από κάποια άλλη πηγή, και όχι απευθείας από το υποκείμενο των δεδομένων, τότε αυτά θα πρέπει να ελέγχονται, έτσι ώστε να διασφαλίζεται η αξιοπιστία τους πριν να υποστούν οποιουδήποτε είδους επεξεργασία.

Για να γίνει έλεγχος ορθότητας και να επιβεβαιωθεί η πληρότητα και ακρίβεια των δεδομένων προσωπικού χαρακτήρα, όπως αυτή έχει ορισθεί παραπάνω, πρέπει να γίνει χρήση σχετικών μέσων που θα επιβεβαιώνουν ότι τα δεδομένα που έχει υποβάλει και ισχυριστεί το υποκείμενο των δεδομένων, ή τα δεδομένα που έχουν προέλθει από κάποια άλλη πηγή, είναι πράγματι έγκυρα. Επιπλέον, όταν γίνεται οποιαδήποτε τροποποίηση των δεδομένων από το υποκείμενο των δεδομένων, πρέπει να γίνεται σχετικός έλεγχος πριν τα δεδομένα ενημερωθούν στην εκάστοτε υπηρεσία, έτσι ώστε να διασφαλίζεται ότι οι τροποποιήσεις είναι πράγματι έγκυρες και δεν έχει γίνει κάποια μη εξουσιοδοτημένη ενέργεια, ούτε εσκεμμένη ψευδής τροποποίηση. Ιδιαίτερα σημαντική είναι αυτή η αρχή, ιδίως για περιπτώσεις όπου τα εσφαλμένα ή ανακριβή δεδομένα μπορεί να οδηγήσουν σε παραχώρηση ή στέρηση προνομίων σε ένα φυσικό πρόσωπο.

Ανοιχτότητα, διαφάνεια και γνωστοποίηση

Η αρχή της ανοιχτότητας, διαφάνειας και γνωστοποίησης έχει ως κύριο στόχο την σαφή και πλήρη ενημέρωση του υποκειμένου των δεδομένων, σχετικά με όλες τις ενέργειες στις οποίες θα προβεί ο υπεύθυνος επεξεργασίας, στα δεδομένα προσωπικού χαρακτήρα που το αφορούν. Η γνωστοποίηση και η πληροφόρηση του υποκειμένου των δεδομένων πρέπει να είναι επαρκής και σαφής, και να γίνεται απαραιτήτως πριν να συγκατατεθεί το υποκείμενο των δεδομένων. Έτσι, η γνωστοποίηση πρέπει να περιλαμβάνει:

i. τα δεδομένα που πρόκειται να υποστούν επεξεργασία
ii. τον σκοπό επεξεργασίας και συλλογής των δεδομένων
iii. όλους τους εμπλεκόμενους, οι οποίοι επρόκειτο να αλληλοεπιδράσουν και να επεξεργαστούν τα δεδομένα, για την ικανοποίηση του καθορισμένου σκοπού

iv. πληροφορίες για τον ίδιο τον υπεύθυνο επεξεργασίας και στοιχεία επικοινωνίας αυτού (εφόσον είναι υπαίτιος για οτιδήποτε συμβεί στα δεδομένα του υποκειμένου των δεδομένων)
v. τους μηχανισμούς συλλογής, επικοινωνίας και αποθήκευσης των δεδομένων
vi. όλα τα φυσικά πρόσωπα, τα οποία θα εμπλέκονται στην εν λόγω επεξεργασία και θα μπορούν να προσπελάζουν τα δεδομένα
vii. λοιπές πληροφορίες σχετικά με την προσπέλαση, διαγραφή, διόρθωση και επεξεργασία των δεδομένων

Η ανωτέρω γνωστοποίηση πρέπει να γίνεται με διαφανή τρόπο ως προς τα υποκείμενα των δεδομένων, και να υπάρχει επαρκής πληροφόρηση σχετικά με την επεξεργασία των προσωπικών τους δεδομένων, ειδικά αν η εν λόγω επεξεργασία μπορεί να επιφέρει επιπτώσεις στα υποκείμενα των δεδομένων.

Ατομική συμμετοχή και πρόσβαση

Η αρχή της ατομικής συμμετοχής και πρόσβασης αφορά στη δυνατότητα προσπέλασης και επανεξέτασης των δεδομένων προσωπικού χαρακτήρα του υποκειμένου των δεδομένων. Τα υποκείμενα των δεδομένων μπορούν, εφόσον αυθεντικοποιηθούν στο σύστημα και αν η προσπέλαση των δεδομένων προβλέπεται από τη νομοθεσία, να προσπελάζουν και να επανεξετάζουν τα δεδομένα τους, έτσι ώστε να τηρείται η ανωτέρω αρχή της ακρίβειας και ποιότητας των δεδομένων, και έτσι να είναι τα δεδομένα πλήρη και έγκυρα. Σε περιπτώσεις όπου αυτό προβλέπεται, τα υποκείμενα των δεδομένων μπορούν επίσης να διαγράφουν και να τροποποιούν τα δεδομένα τους. Η εν λόγω επανεξέταση πρέπει να γίνεται με τρόπο απλό και αποδοτικό, χωρίς να υπάρχει καθυστέρηση ή κόστος ως προς το υποκείμενο των δεδομένων.

Ο υπεύθυνος επεξεργασίας οφείλει να διασφαλίζει ότι δικαίωμα προσπέλασης στα δεδομένα προσωπικού χαρακτήρα έχουν μόνο τα υποκείμενα των δεδομένων τα οποία τα αφορούν και κανένας άλλος. Στην περίπτωση που το υποκείμενο των δεδομένων δεν είναι σε θέση να ασκήσει το δικαίωμα προσπέλασης στα δεδομένα του, δίνεται η δυνατότητα σε κάποιο άλλο εξουσιοδοτημένο φυσικό πρόσωπο να τα προσπελάσει για λογαριασμό του.

Λογοδοσία

Η αρχή της λογοδοσίας έχει ως στόχο να προστατέψει τόσο το υποκείμενο των δεδομένων όσο και τον υπεύθυνο επεξεργασίας από τυχόν παραβιάσεις ιδιωτικότητας ή αποποίηση ευθυνών. Σε περίπτωση που υπάρξει κάποια παραβίαση ιδιωτικότητας, τα υποκείμενα των δεδομένων πρέπει να ενημερώνονται τόσο για την παραβίαση αυτή καθ' αυτή όσο και για τα μέτρα που λήφθηκαν για την αντιμετώπισή της. Ο λόγος για τον οποίο γίνεται αυτή η πληροφόρηση είναι ότι οι παραβιάσεις ιδιωτικότητας μπορεί να προκαλέσουν σημαντική ζημία στα υποκείμενα των δεδομένων. Η προκαλούμενη ζημία πρέπει να αποκαθίσταται και να αντιμετωπίζεται, και σε περιπτώσεις όπου η αποκατάσταση αυτής είναι αδύνατη, θα πρέπει να υπάρχουν αντίστοιχες διαδικασίες επανόρθωσης ή αποζημίωσης του φυσικού προσώπου. Τα μέτρα αντιμετώπισης των παραβιάσεων ιδιωτικότητας πρέπει να είναι ανάλογα των κινδύνων που εγκυμονούν και πρέπει να υλοποιούνται το συντομότερο δυνατόν από τη χρονική στιγμή που έγινε αντιληπτή η εκάστοτε παραβίαση.

Η διαδικασία επανόρθωσης, είναι μια διαδικασία όπου καλούνται οι υπεύθυνοι επεξεργασίας να λογοδοτήσουν στα υποκείμενα των δεδομένων σχετικά με την κακή χρήση την οποία υπέστησαν τα δεδομένα τους και η οποία οδήγησε σε παραβίαση της ιδιωτικότητας. Μέσω αυτής της διαδικασίας προστατεύονται τα υποκείμενα των δεδομένων,

ενώ παράλληλα δίνεται η δυνατότητα αποκατάστασής τους σε περιπτώσεις κλοπής ταυτότητας, πλήγματος της φήμης ή κακής διαχείρισης και τροποποίησης των δεδομένων προσωπικού χαρακτήρα τους. Οι διαδικασίες αυτές δίνουν, επιπλέον, το αίσθημα της ασφάλειας στα υποκείμενα των δεδομένων και τα παροτρύνουν να συμμετάσχουν σε τέτοιου είδους δράσεις που συσχετίζονται με τα δεδομένα τους.

Σε περιπτώσεις όπου τα δεδομένα προσωπικού χαρακτήρα διαβιβάζονται σε κάποιο τρίτο φορέα, θα πρέπει να διασφαλίζεται ότι αυτός παρέχει στα δεδομένα το αντίστοιχο επίπεδο προστασίας της ιδιωτικότητας, με αυτό του οργανισμού από τον οποίο προήλθαν. Τα μέσα για την προστασία των δεδομένων, τα οποία θα εφαρμόζονται, πρέπει να εγγράφονται σε σχετική σύμβαση μεταξύ του οργανισμού και του τρίτου φορέα.

Ο υπεύθυνος επεξεργασίας, οφείλει από πλευράς του, πέρα από την πλήρη ενημέρωση του υποκειμένου των δεδομένων, να διατηρεί και τη συγκατάθεση που το υποκείμενο του έχει παραχωρήσει, έτσι ώστε να είναι σε θέση, εφόσον του ζητηθεί, να αποδείξει ότι το εκάστοτε υποκείμενο των δεδομένων έχει συναινέσει για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν.

Ασφάλεια πληροφοριών

Η αρχή της ασφάλειας των πληροφοριών αφορά στην προστασία των δεδομένων προσωπικού χαρακτήρα του υποκειμένου των δεδομένων. Πιο συγκεκριμένα, πρέπει να γίνεται λήψη των κατάλληλων μέτρων, έτσι ώστε να διασφαλίζεται η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των δεδομένων αυτών. Επιπλέον, πρέπει να διασφαλίζεται η προστασία των δεδομένων από κινδύνους, όπως η μη εξουσιοδοτημένη προσπέλαση, χρήση, τροποποίηση, διαγραφή κ.λπ.

Ο υπεύθυνος επεξεργασίας οφείλει να επιλέξει καταρτισμένους εκτελούντες επεξεργασίας, οι οποίοι να κατέχουν επαρκείς γνώσεις και να παρέχουν επαρκείς εγγυήσεις σχετικά με τα μέτρα που αφορούν στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα.

Τόσο τα μέτρα ασφάλειας όσο και η υλοποίηση αυτών, εξαρτώνται από:

i. την πιθανότητα εκδήλωσης ενός περιστατικού,
ii. τη σημαντικότητα των επιπτώσεων που αυτό θα επιφέρει,
iii. τον τύπο των δεδομένων (δεδομένα προσωπικού χαρακτήρα ή ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα),
iv. τον αριθμό των υποκειμένων των δεδομένων, τα οποία εμπλέκονται και θα επηρεαστούν σε περίπτωση παραβίασης, και
v. το πλαίσιο διεξαγωγής της επεξεργασίας

Όπως αναφέρθηκε και στην αρχή της ελαχιστοποίησης, πρόσβαση σε δεδομένα προσωπικού χαρακτήρα θα έχουν μόνο όσοι αλληλοεπιδρούν με αυτά – μόνο όσοι τα επεξεργάζονται για κάποιο συγκεκριμένο σκοπό.

Επιπλέον, τυχόν κίνδυνοι και ευπάθειες που παρουσιάζονται, θα πρέπει να καταγράφονται κατά τη διαδικασία αποτίμησης της επικινδυνότητας, ενώ παράλληλα θα πρέπει βάσει αυτών να εντάσσονται νέα μέτρα ασφάλειας, τα οποία θα επαναποτιμούνται και θα ελέγχονται για τη διατήρηση μιας συνεχούς διαδικασίας διαχείρισης της επικινδυνότητας.

Συμμόρφωση με την ιδιωτικότητα

Η αρχή της συμμόρφωσης με την ιδιωτικότητα έχει ως στόχο να διασφαλίσει ότι οι φορείς και οι οργανισμοί, οι οποίοι επεξεργάζονται δεδομένα προσωπικού χαρακτήρα, συμμορφώνονται με τις απαιτήσεις προστασίας των δεδομένων και διασφάλισης της ιδιωτικότητας, και δεν αποκλίνουν του ορισμένου και νόμιμου σκοπού επεξεργασίας. Για την επίτευξη της συμμόρφωσης πραγματοποιούνται συστημικοί έλεγχοι επιθεώρησης, είτε εσωτερικά (εσωτερικοί έλεγχοι μέσα σε έναν οργανισμό), είτε εξωτερικά (εξωτερικοί έλεγχοι μέσω έμπιστων τρίτων φορέων). Και στις δύο περιπτώσεις, γίνονται έλεγχοι αξιοπιστίας των ελεγκτών και των επιθεωρητών για να διασφαλιστεί ότι η κρίση τους είναι αμερόληπτη. Βάσει αυτών των ελέγχων, διασφαλίζεται η συμμόρφωση του οργανισμού με την ισχύουσα νομοθεσία, καθώς και με τις πολιτικές και τις διαδικασίες για την ασφάλεια και την προστασία της ιδιωτικότητας των προσωπικών δεδομένων.

Επιπλέον, πρέπει να αξιολογείται το κατά πόσο τα προγράμματα και οι πρωτοβουλίες παροχής υπηρεσιών που αλληλοεπιδρούν με δεδομένα προσωπικού χαρακτήρα, και τα επεξεργάζονται, συμμορφώνονται με τις απαιτήσεις της ιδιωτικότητας και της προστασίας των δεδομένων. Βάσει νομοθεσίας, ορίζονται μια ή περισσότερες αρχές, όπως είναι η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, οι οποίες φέρουν ευθύνη και είναι υπεύθυνες για την παρακολούθηση και τήρηση της συμμόρφωσης του οργανισμού με την τρέχουσα νομοθεσία των δεδομένων προσωπικού χαρακτήρα. Έτσι, ο οργανισμός οφείλει, στα πλαίσια τήρησης των αρχών προστασίας ιδιωτικότητας, να έχει άρτια συνεργασία με τις εποπτικές αρχές, και να συμμορφώνεται και να ακολουθεί τις οδηγίες που αυτές θα του υποδεικνύουν.

Προστασία Δεδομένων από το Σχεδιασμό και εξ Ορισμού

Ο Γενικός Κανονισμός Προστασίας Δεδομένων εισήγαγε μεταξύ άλλων μια νομική υποχρέωση για τους υπευθύνους επεξεργασίας η οποία αναφέρεται στο άρθρο 25 ως «Προστασία Δεδομένων από το Σχεδιασμό και εξ Ορισμού» [6] [17].

Προστασία Δεδομένων από το Σχεδιασμό: Η Προστασία Δεδομένων από το Σχεδιασμό (ΠΔΣ) (Privacy by Design) αφορά στην έννοια της ενσωμάτωσης των μέτρων προστασίας της ιδιωτικότητας και των τεχνολογιών ενίσχυσης της ιδιωτικότητας απευθείας κατά το σχεδιασμό των τεχνολογιών και των συστημάτων πληροφορικής [18] [19]. Οργανισμοί οι οποίοι αλληλοεπιδρούν ή επεξεργάζονται προσωπικά δεδομένα θα πρέπει να καταβάλουν προσπάθεια έτσι ώστε να αναπτύξουν τα κατάλληλα μέτρα προστασίας προσωπικών δεδομένων κατά τη φάση του σχεδιασμού των συστημάτων επεξεργασίας προσωπικών δεδομένων και να μην προσθέτουν τα μέτρα αυτά εκ των υστέρων σε μεταγενέστερο στάδιο του κύκλου ζωής των συστημάτων [7] [19]. Επιπλέον, ο καθορισμός των απαιτήσεων προστασίας της ιδιωτικότητας πρέπει να προηγείται του σχεδιασμού του εκάστοτε συστήματος πληροφορικής και επικοινωνιών το οποίο επεξεργάζεται προσωπικά δεδομένα.

Προστασία Δεδομένων εξ Ορισμού: Η Προστασία Δεδομένων εξ Ορισμού (ΠΔΟ) (Privacy by Default) αναφέρεται σε προκαθορισμένες ρυθμίσεις των συστημάτων πληροφορικής και επικοινωνιών, οι οποίες στοχεύουν στην παροχή του υψηλότερου επιπέδου προστασίας της ιδιωτικότητας [19] [20]. Η Προστασία Δεδομένων εξ Ορισμού είναι μια προληπτική αρχή προστασίας των προσωπικών δεδομένων, που εφαρμόζεται μέσα σε έναν οργανισμό, και διασφαλίζει ότι ο υπεύθυνος επεξεργασίας επεξεργάζεται μόνο τα δεδομένα προσωπικού χαρακτήρα τα οποία είναι απαραίτητα για τον εκάστοτε σκοπό επεξεργασίας [21] [19]. Με λίγα λόγια, προσφέρει μια προεπιλεγμένη ρύθμιση που σέβεται την ιδιωτικότητα των υποκειμένων των δεδομένων, ενώ παράλληλα μπορεί να αλλάξει από τα ίδια τα υποκείμενα σύμφωνα με τις προτιμήσεις τους [19].

Η αρχή Προστασίας Δεδομένων από το Σχεδιασμό και εξ Ορισμού απαιτεί από τον υπεύθυνο επεξεργασίας να εφαρμόζει αποτελεσματικά τα κατάλληλα τεχνικά και οργανωτικά μέτρα που αποσκοπούν στην εφαρμογή των αρχών ιδιωτικότητας κατά την επεξεργασία των δεδομένων προσωπικού χαρακτήρα [17].

Η έννοια της Προστασία των Δεδομένων από το Σχεδιασμό αποτελεί θεμελιώδη προϋπόθεση για την αποτελεσματική προστασία των δεδομένων των υποκειμένων των δεδομένων [17]. Επί της ουσίας, η Προστασία Δεδομένων από το Σχεδιασμό απαιτεί από τους υπεύθυνους επεξεργασίας να λαμβάνουν υπόψη τις αρχές και τις απαιτήσεις ιδιωτικότητας στο στάδιο του σχεδιασμού οποιουδήποτε συστήματος πληροφορικής και επικοινωνιών, υπηρεσίας ή προϊόντος και καθ' όλη τη διάρκεια του κύκλου ζωής των προσωπικών δεδομένων, και να ενσωματώνουν κατάλληλα τεχνικά και οργανωτικά μέτρα για την εφαρμογή των απαιτήσεων προστασίας των δεδομένων [19] [20].

Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας

Παρόλο που η χρήση μέτρων ασφαλείας, τα οποία στοχεύουν στην αποφυγή της μη εξουσιοδοτημένης πρόσβασης σε δεδομένα προσωπικού χαρακτήρα, αποτελεί βάση για την προστασία των προσωπικών δεδομένων και της ιδιωτικότητας, η ασφάλεια αυτή καθ’ αυτή δεν μπορεί να προστατεύσει αποτελεσματικά την ιδιωτικότητα των φυσικών προσώπων. Εν αντιθέτως, πρέπει να εφαρμόζονται και να υλοποιούνται επιπλέον μέτρα προστασίας από πλευράς ιδιωτικότητας, συμπεριλαμβανομένης της εφαρμογής των Τεχνολογιών Ενίσχυσης

της Ιδιωτικότητας. Η οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[1] και, κατά συνέπεια, η εθνική νομοθεσία περί προστασίας της ιδιωτικότητας αποδίδουν ευθύνες στους φορείς ανάπτυξης συστημάτων τα οποία αλληλοεπιδρούν με προσωπικά δεδομένα [22]. Οι αρχές ιδιωτικότητας, που αναφέρονται στην δεύτερη ενότητα, πρέπει να εφαρμόζονται αποτελεσματικά σε έναν οργανισμό, προκειμένου να παρέχεται κατάλληλη υποστήριξη στα δικαιώματα του φυσικού προσώπου όσον αφορά τα δεδομένα προσωπικού χαρακτήρα και την διαφύλαξή τους [22]. Είναι σημαντικό να αναπτύσσονται κατάλληλα συστήματα που να εφαρμόζουν διαδικασίες και μέτρα προστασίας για την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Από τη δεκαετία του 1980 έχουν προταθεί τεχνολογίες με ενσωματωμένα χαρακτηριστικά και λειτουργίες που στοχεύουν στην προστασία της ιδιωτικότητας [5]. Το 1995, προτάθηκε η ιδέα για διαμόρφωση των τεχνολογιών σύμφωνα με τις αρχές προστασίας της ιδιωτικότητας [5]. Ο όρος «Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας» (Privacy-Enhancing Technologies) έχει ως στόχο την ελαχιστοποίηση της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα στο ελάχιστο δυνατό, καθώς και την προστασία της ταυτότητας των φυσικών προσώπων μέσω πληθώρας τεχνικών, όπως η ανωνυμοποίηση και η ψευδωνυμοποίηση δεδομένων [23]. Πιο συγκεκριμένα, οι Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας έχουν οριστεί ως τεχνολογίες πληροφορικής και επικοινωνιών, οι οποίες προστατεύουν την ιδιωτικότητα των χρηστών τους απαλείφοντας ή μειώνοντας τα δεδομένα προσωπικού χαρακτήρα ή αποτρέποντας την περιττή ή ανεπιθύμητη επεξεργασία των δεδομένων προσωπικού χαρακτήρα, χωρίς να παρεμποδίζεται ή να μειώνεται η λειτουργικότητα του συστήματος [22]. Με τη χρήση των Τεχνολογιών Ενίσχυσης της Ιδιωτικότητας, οι κίνδυνοι για παραβίαση της ιδιωτικότητας των υποκειμένων των δεδομένων μειώνονται, και οι νομικές υποχρεώσεις προστασίας δεδομένων των αρμόδιων οντοτήτων, που είναι υπεύθυνες για την επεξεργασία των προσωπικών δεδομένων, ικανοποιούνται ευκολότερα.

Οι Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας δεν είναι ευρέως χρησιμοποιούμενες, ούτε λαμβάνονται υπόψη κατά το σχεδιασμό του συστήματος [5]. Ωστόσο, σύμφωνα με το άρθρο 25 του ΓΚΠΔ, τόσο οι εταιρίες όσο και οι οργανισμοί υποχρεούνται να ακολουθούν την αρχή της Προστασίας Δεδομένων από το Σχεδιασμό, η οποία συμβάλλει στο σχεδιασμό και την ανάπτυξη συστημάτων και υπηρεσιών, φιλικών προς την ιδιωτικότητα και προς τα υποκείμενα των δεδομένων [5] [24]. Δεδομένου ότι ένα προϊόν πληροφορικής κατασκευάζεται, συνήθως, χρησιμοποιώντας προϋπάρχοντα δομικά στοιχεία και τεχνολογίες, η ανάπτυξη και ενσωμάτωση των Τεχνολογιών Ενίσχυσης της Ιδιωτικότητας διαδραματίζει σημαντικό ρόλο στην υλοποίηση συστημάτων τα οποία υποστηρίζουν την ΠΔΣ [24].

Αρχές Προστασίας Προσωπικών Δεδομένων από το Σχεδιασμό

Η Προστασία Δεδομένων από το Σχεδιασμό παρουσιάστηκε για πρώτη φορά από την Ann Cavoukian [25] [26] και αφορά στην ενσωμάτωση των Μέτρων Προστασίας και των Τεχνολογιών Ενίσχυσης της Ιδιωτικότητας απευθείας από το σχεδιασμό των τεχνολογιών και των συστημάτων πληροφορικής [27]. Για την αποφυγή της προσθήκης δομικών στοιχείων σε ένα ήδη υπάρχον σύστημα, και για την ορθή εφαρμογή της αρχής Προστασίας Δεδομένων από το Σχεδιασμό, η Ann Cavoukian εισήγαγε επτά θεμελιώδεις αρχές, οι οποίες απαιτούν

[1] Η οδηγία 95/46/ΕΚ έπαψε να έχει ισχύ από τις 25 Μαΐου 2018 σύμφωνα με το άρθρο 94 του ΓΚΠΔ. Οι παραπομπές στην οδηγία 95/46/ΕΚ θεωρούνται παραπομπές στον ΓΚΠΔ.

την ενσωμάτωση της ιδιωτικότητας ως προληπτικό μέτρο κατά τον σχεδιασμό των συστημάτων [25] [5] [26].

Προορατική, όχι ως Αντίδραση. Προληπτική, όχι Διορθωτική

Η προσέγγιση της Προστασίας των Δεδομένων από το Σχεδιασμό χαρακτηρίζεται από προληπτικά μέτρα και όχι από μέτρα αντίδρασης. Προβλέπει και αποτρέπει τα συμβάντα παραβίασης της ιδιωτικότητας πριν να συμβούν [17]. Η ΠΔΣ δεν «περιμένει» να πραγματοποιηθούν περιστατικά παραβίασης της ιδιωτικότητας, ούτε προσφέρει διορθωτικά μέτρα για την επίλυση των παραβιάσεων εφόσον συμβούν. Εν αντιθέτως, έχει ως στόχο να αποτρέψει εξ αρχής την πραγματοποίησή τους [25] [26].

Προστασία Δεδομένων ως Προεπιλεγμένη Ρύθμιση

Η Προστασία Δεδομένων από το Σχεδιασμό επιδιώκει να παρέχει τον μέγιστο βαθμό προστασίας της ιδιωτικότητας στα υποκείμενα των δεδομένων διασφαλίζοντας ότι τα προσωπικά τους δεδομένα προστατεύονται αυτομάτως σε οποιοδήποτε σύστημα πληροφορικής, χωρίς να απαιτείται κάποια ενέργεια από πλευράς τους. Με λίγα λόγια, δεν απαιτείται καμία ενέργεια από την πλευρά του υποκειμένου των δεδομένων για την προστασία των προσωπικών του δεδομένων, καθώς η προστασία της ιδιωτικότητας είναι ενσωματωμένη στο σύστημα από προεπιλογή [25] [26]. Ειδικότερα, η διαφάνεια, η ελαχιστοποίηση των δεδομένων, ο περιορισμός του σκοπού, η εμπιστευτικότητα, και η διατήρηση δεδομένων, είναι εξ ορισμού ενσωματωμένα στα συστήματα πληροφορικής και επικοινωνιών, προστατεύοντας τα προσωπικά δεδομένα χωρίς να χρειάζεται να δραστηριοποιηθούν τα ίδια τα υποκείμενα των δεδομένων [17].

Προστασία Δεδομένων ενσωματωμένη από το Σχεδιασμό

Η Προστασία των Δεδομένων από το Σχεδιασμό είναι ενσωματωμένη στο σχεδιασμό και την αρχιτεκτονική των συστημάτων πληροφορικής και επικοινωνιών, και δεν προστίθεται εκ των υστέρων ως επιπλέον χαρακτηριστικό του συστήματος [17]. Το αποτέλεσμα αυτής της αρχής είναι ότι η προστασία της ιδιωτικότητας γίνεται ένα βασικό δομικό στοιχείο για την λειτουργία του συστήματος και αποτελεί αναπόσπαστο μέρος του συστήματος, χωρίς να μειώνεται η λειτουργικότητά του [25] [26].

Πλήρης λειτουργικότητα

Η Προστασία των Δεδομένων από το Σχεδιασμό επιδιώκει να ικανοποιήσει όλα τα έννομα συμφέροντα και τους στόχους ενός οργανισμού με θετικό «win-win» τρόπο, και όχι μέσω μιας παρωχημένης προσέγγισης όπου γίνονται περιττές αντισταθμίσεις, π.χ. μεταξύ ιδιωτικότητας και ασφάλειας [25] [26]. Πιο συγκεκριμένα, πρέπει να εξυπηρετούνται όλα τα έννομα συμφέροντα και οι στόχοι για την προστασία της ιδιωτικότητας, χωρίς συμβιβασμούς, και χωρίς να τίθενται ζητήματα λειτουργικότητας ενός συστήματος έναντι ιδιωτικότητας ενός φυσικού προσώπου [17]. Η Προστασία των Δεδομένων από το Σχεδιασμό δεν σχετίζεται μόνο με τους στόχους για την προστασία της ιδιωτικότητας, αλλά αποφεύγει τέτοιου είδους αντισταθμίσεις, αποδεικνύοντας ότι είναι εφικτό και πολύ πιο επιθυμητό να υφίστανται υλοποιήσεις που να επιτρέπουν την πολύ-λειτουργικότητα των συστημάτων [25] [26].

Ασφάλεια από άκρο σε άκρο – Πλήρης προστασία κύκλου ζωής

Τα δεδομένα προσωπικού χαρακτήρα πρέπει να προστατεύονται συνεχώς από την αρχή μέχρι το τέλος της επεξεργασίας τους, και καθ' όλη τη διάρκεια του κύκλου ζωής τους. Τα δεδομένα προσωπικού χαρακτήρα προφυλάσσονται, ανάλογα με το επίπεδο ευαισθησίας

τους, από τη συλλογή και καθ' όλη τη διάρκεια του κύκλου ζωής τους, με ισχυρά τεχνικά και οργανωτικά μέτρα, όπως κατάλληλη κρυπτογράφηση, ισχυροί έλεγχοι προσπέλασης και μέθοδοι καταγραφής [17]. Η αρχή της ασφάλειας έχει ιδιαίτερη σημασία, διότι χωρίς ισχυρά μέτρα ασφαλείας, δεν θα μπορέσει να υπάρξει ούτε η έννοια της ιδιωτικότητας [25]. Επιπλέον εξασφαλίζει ότι όλα τα δεδομένα διατηρούνται με ασφάλεια και στη συνέχεια καταστρέφονται εγκαίρως, και με ασφάλεια, στο τέλος της εκάστοτε διαδικασίας [25] [26]. Έτσι, η Προστασία των Δεδομένων από το Σχεδιασμό εξασφαλίζει την – *ασφαλή* – διαχείριση των πληροφοριών από άκρη σε άκρη.

Σαφήνεια και Διαφάνεια

Η Προστασία των Δεδομένων από το Σχεδιασμό έχει ως στόχο να διαβεβαιώσει όλα τα ενδιαφερόμενα μέρη ότι ανεξάρτητα από την τεχνολογία ή το σύστημα που εμπλέκεται στην επεξεργασία των προσωπικών δεδομένων, η εν λόγω επεξεργασία λειτουργεί σύμφωνα με τους δηλωθέντες στόχους και σκοπούς του οργανισμού [25] [26]. Οι διαδικασίες και οι λειτουργίες που σχετίζονται με την επεξεργασία προσωπικών δεδομένων παραμένουν προσβάσιμες και διαφανείς προς τα υποκείμενα των δεδομένων, ενώ οι αρχές της «ανοιχτότητας, διαφάνειας και γνωστοποίησης», της «λογοδοσίας» και της «συμμόρφωσης με την ιδιωτικότητα», συμβάλλουν στην εδραίωση της εμπιστοσύνης από τα υποκείμενα των δεδομένων προς τους υπεύθυνους επεξεργασίας [17].

Σεβασμός της ιδιωτικότητας των χρηστών

Η Προστασία των Δεδομένων από το Σχεδιασμό απαιτεί από τους σχεδιαστές και τους (δια)χειριστές των συστημάτων να διατηρούν τα συμφέροντα των υποκειμένων των δεδομένων, προσφέροντάς τους μέτρα όπως ισχυρές προεπιλογές προστασίας των δεδομένων τους, κατάλληλη ενημέρωση, και αύξηση των φιλικών-προς-το-χρήστη επιλογών τους [17]. Τα καλύτερα συστήματα είναι συνήθως αυτά που σχεδιάζονται συνειδητά γύρω από τα ενδιαφέροντα και τις ανάγκες των χρηστών, οι οποίοι έχουν το μεγαλύτερο έννομο συμφέρον από τη διαχείριση των προσωπικών τους δεδομένων [25] [26].

Στρατηγικές Προστασίας Δεδομένων από το Σχεδιασμό

Οι στρατηγικές σχεδιασμού αποτελούν στρατηγικές, οι οποίες εφαρμόζονται στα δεδομένα προσωπικού χαρακτήρα από το σχεδιασμό, με σκοπό την επίτευξη ενός συγκεκριμένου – *και επιθυμητού* – επιπέδου προστασίας της ιδιωτικότητας [28]. Κάθε στρατηγική σχεδιασμού καθορίζει και θέτει ένα διαφορετικό στόχο σχετικά με την Προστασία των Δεδομένων από το Σχεδιασμό, ο οποίος επιτυγχάνεται με την υλοποίηση των εκάστοτε μεθόδων (tactics) που αντιστοιχούν σε κάθε στρατηγική [29] [28].

Οι Στρατηγικές ΠΔΣ χωρίζονται σε δύο διαφορετικές κατηγορίες: α) τις στρατηγικές οι οποίες είναι προσανατολισμένες στα προσωπικά δεδομένα, και β) τις στρατηγικές οι οποίες είναι προσανατολισμένες στην επεξεργασία των δεδομένων [29]. Οι στρατηγικές που είναι προσανατολισμένες στα δεδομένα επικεντρώνονται στην φιλική προς την ιδιωτικότητα επεξεργασία των δεδομένων, ενώ οι στρατηγικές που είναι προσανατολισμένες στην επεξεργασία επικεντρώνονται στις διαδικασίες επεξεργασίας που αφορούν τα δεδομένα προσωπικού χαρακτήρα.

Στην παρούσα ενότητα περιγράφεται κάθε μία από τις στρατηγικές σχεδιασμού, καθώς και οι επί μέρους μέθοδοι εφαρμογής τους.

Στρατηγική 1: Ελαχιστοποίηση

Η πιο βασική στρατηγική σχεδιασμού είναι η ***ελαχιστοποίηση των δεδομένων***, και αναφέρει ότι ο όγκος των προσωπικών δεδομένων που υποβάλλονται σε επεξεργασία θα πρέπει να περιορίζεται στο ελάχιστο δυνατό [5] [29]. Διασφαλίζοντας ότι δεν συλλέγονται ή δεν επεξεργάζονται περιττά ή επιπρόσθετα δεδομένα, οι πιθανές επιπτώσεις από τη χρήση ενός συστήματος που επεξεργάζεται προσωπικά δεδομένα είναι περιορισμένες. Η εφαρμογή της στρατηγικής της ελαχιστοποίησης σημαίνει ότι η επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι ανάλογη του σκοπού επεξεργασίας και δεν υπάρχουν άλλοι τρόποι ή μέσα για την επίτευξη του ίδιου σκοπού με χρήση μικρότερου συνόλου δεδομένων [5]. Μερικές φορές μια εντελώς διαφορετική προσέγγιση ενδέχεται να απαιτεί συλλογή μικρότερου συνόλου δεδομένων ή μπορεί να μην απαιτεί καθόλου προσωπικά δεδομένα [29], και τέτοιου είδους προσεγγίσεις θεωρούνται οι πλέον κατάλληλες για την επίτευξη της ελαχιστοποίησης των δεδομένων.

Μέθοδοι

Η ελαχιστοποίηση των προσωπικών δεδομένων μπορεί να επιτευχθεί είτε με τη συλλογή δεδομένων από λιγότερα άτομα είτε με τη συλλογή λιγότερων δεδομένων – μικρότερου συνόλου δεδομένων.

- **Επιλογή** [29]: Επιλογή μόνο των σχετικών ατόμων και των σχετικών χαρακτηριστικών. Πρέπει να καθοριστεί εκ των προτέρων το πλήθος των ατόμων που θα εμπλακούν, και των χαρακτηριστικών που θα συλλεχθούν. Επιπλέον πρέπει να τεθούν σε επεξεργασία μόνο τα δεδομένα που είναι απολύτως απαραίτητα και που συνάδουν με τον ορισμένο σκοπό επεξεργασίας.
- **Εξαίρεση** [29]**:** Εξαίρεση ατόμων ή χαρακτηριστικών εκ των προτέρων. Εκ των προτέρων προσδιορισμός των ατόμων ή των χαρακτηριστικών τα οποία αποκλίνουν από τους σκοπούς επεξεργασίας, και άρα πρέπει να εξαιρούνται της επεξεργασίας. Σε περιπτώσεις που ένας οργανισμός λάβει τέτοιου είδους δεδομένα, θα πρέπει απευθείας να τα διαγράψει με ασφαλή τρόπο και να μην τα επεξεργαστεί.
- **Διαγραφή** [29]**:** Διαγραφή δεδομένων από τη στιγμή που αυτά θα σταματήσουν να είναι απαραίτητα για τον οργανισμό. Ο χρόνος διατήρησης και επεξεργασίας των δεδομένων πρέπει να είναι καθορισμένος εξαρχής, και τα δεδομένα αυτά θα πρέπει να διαγράφονται κατά το πέρας της ορισμένης χρονικής περιόδου με ασφαλή τρόπο. Οι αλλαγές στην οργάνωση, τις διαδικασίες ή τις υπηρεσίες ενδέχεται να καταστήσουν ορισμένα σύνολα δεδομένων περιττά, πριν από την χρονική περίοδο λήξης τους.
- **Καταστροφή** [29]**:** Ολική διαγραφή/καταστροφή των προσωπικών δεδομένων μόλις αυτά πάψουν να σχετίζονται με τους σκοπούς επεξεργασίας. Η ανάκτηση των δεδομένων αυτών, ύστερα από τη μέθοδο της καταστροφής, θα πρέπει να είναι μη εφικτή, ανεξαρτήτως του τρόπου ανάκτησης. Τα προσωπικά δεδομένα θα πρέπει επίσης να καταργηθούν από τα αντίγραφα ασφαλείας, ενώ παράλληλα θα πρέπει να χρησιμοποιηθούν ασφαλείς τρόποι για την απομάκρυνσή τους από σκληρούς δίσκους.

Στρατηγική 2: Απόκρυψη

Η δεύτερη στρατηγική σχεδιασμού, ***η στρατηγική της απόκρυψης***, δηλώνει ότι όλα τα δεδομένα προσωπικού χαρακτήρα, και οι αλληλεξαρτήσεις τους, θα πρέπει να μην

αποκαλύπτονται σε τρίτους. Η σκέψη πίσω από αυτή τη στρατηγική είναι ότι η απόκρυψη προσωπικών δεδομένων δεν μπορεί εύκολα να οδηγήσει στην καταχρηστική χρήση τους. Η στρατηγική δεν αναφέρει άμεσα από ποιον πρέπει να αποκρύπτονται τα δεδομένα. Σε ορισμένες περιπτώσεις, όπου η στρατηγική χρησιμοποιείται για την απόκρυψη πληροφοριών που προκύπτουν από τη χρήση ενός συστήματος, σκοπός είναι η απόκρυψη των πληροφοριών από οποιονδήποτε [5]. Σε άλλες περιπτώσεις, όπου οι πληροφορίες συλλέγονται, αποθηκεύονται ή υποβάλλονται σε νόμιμη επεξεργασία από ένα μέρος, π.χ. έναν οργανισμό, σκοπός είναι η απόκρυψη των πληροφοριών από οποιοδήποτε άλλο μέρος πλην του εκάστοτε οργανισμού. Στην περίπτωση αυτή, η στρατηγική αντιστοιχεί στη διασφάλιση της εμπιστευτικότητας [29].

Παρόλο που η στρατηγική της απόκρυψης είναι σημαντική, συχνά παραβλέπεται. Στο παρελθόν, πολλά συστήματα είχαν σχεδιαστεί χρησιμοποιώντας αναγνωριστικά που αργότερα αποδείχθηκαν καταστροφικά ως προς την προστασία των προσωπικών δεδομένων [5]. Παραδείγματα τέτοιων αναγνωριστικών είναι τα αναγνωριστικά σε ετικέτες RFID (Radio-Frequency Identification), τα αναγνωριστικά ασύρματου δικτύου, ακόμη και διευθύνσεις IP (Internet Protocol – IP). Η στρατηγική της απόκρυψης επανεξετάζει τη χρήση τέτοιου είδους αναγνωριστικών. Στην ουσία, η στρατηγική αυτή στοχεύει στην εμπιστευτικότητα, τη μη συνδεσιμότητα και τη δυνατότητα μη παρατήρησης των προσωπικών δεδομένων [29]. Η μη συνδεσιμότητα διασφαλίζει ότι ακόμα και αν τα δεδομένα είναι γνωστά, κανείς δεν μπορεί να καταλήξει στο άτομο στο οποίο ανήκουν, ενώ η μη παρατήρηση καθιστά την ύπαρξη των δεδομένων εντελώς άγνωστη [30].

Μέθοδοι

Η στρατηγική της απόκρυψης περιέχει τις ακόλουθες μεθόδους.

- **Περιορισμός** [29]**:** Περιορισμός πρόσβασης σε προσωπικά δεδομένα. Πρέπει να διασφαλίζεται ότι τα προσωπικά δεδομένα προστατεύονται με ορθό τρόπο, π.χ. μέσω μιας αυστηρής πολιτικής ελέγχου προσπέλασης. Μόνο όσοι χρειάζονται πράγματι πρόσβαση στα δεδομένα προσωπικού χαρακτήρα θα επιτρέπεται να τα προσπελαύνουν βάσει της αρχής «need-to-know». Η μέθοδος αυτή καθιστά δύσκολη την διαρροή προσωπικών δεδομένων.
- **Κρυπτογράφηση** [29]**:** Πρέπει να αποτρέπεται η ανάγνωση των προσωπικών δεδομένων από μη εξουσιοδοτημένες οντότητες. Κρυπτογράφηση των δεδομένων προσωπικού χαρακτήρα έτσι ώστε να μην γίνονται κατανοητά – *να μην είναι αναγνώσιμα* – χωρίς το κλειδί κρυπτογράφησης. Σε άλλες περιπτώσεις ενδέχεται να εισέλθουν τα προσωπικά δεδομένα σε μια συνάρτηση κατακερματισμού, π.χ. για τη δημιουργία ψευδωνύμου.
- **Διαχωρισμός** [5] [29]**:** Κατάργηση της συσχέτισης μεταξύ γεγονότων, προσώπων και δεδομένων. Η μη συνδεσιμότητα διασφαλίζει ότι δύο γεγονότα δεν μπορούν να συσχετιστούν μεταξύ τους. *(Ως γεγονότα μπορούν να θεωρηθούν οι ενέργειες των υποκειμένων των δεδομένων, καθώς και σύνολα δεδομένων που προκύπτουν ως αποτέλεσμα από ένα γεγονός.)* Κατάργηση των άμεσων αναγνωριστικών στοιχείων ταυτότητας.
- **Ανακάτεμα** [29]**:** Ανακάτεμα προσωπικών δεδομένων με σκοπό την απόκρυψη της πηγής προέλευσής τους ή των αλληλεξαρτήσεών τους. Ανωνυμοποίηση δεδομένων. Απόκρυψη δεδομένων σε ένα νέφος (cloud) που περιέχει διαφορετικά δεδομένα – διαφορετικού είδους δεδομένα. Κατάργηση της συσχέτισης μεταξύ δύο γεγονότων.

Στρατηγική 3: Διαχωρισμός

Η τρίτη στρατηγική σχεδιασμού, ***η στρατηγική του διαχωρισμού***, αφορά στο διαχωρισμό της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ορίζει, ότι τα δεδομένα προσωπικού χαρακτήρα θα πρέπει να υποβάλλονται σε επεξεργασία με κατανεμημένο τρόπο, σε ξεχωριστά τμήματα, όποτε αυτό είναι εφικτό [5] [29]. Η εφαρμογή της στρατηγικής αυτής καθιστά δυσκολότερο τον συνδυασμό ή τη συσχέτιση δεδομένων προσωπικού χαρακτήρα [29]. Επιπλέον, διαχωρίζοντας την επεξεργασία ή την αποθήκευση των προσωπικών δεδομένων που ανήκουν στο ίδιο φυσικό πρόσωπο, καθίσταται ανέφικτη η δημιουργία ολοκληρωμένων προφίλ ενός ατόμου [5].

Ο διαχωρισμός είναι μια καλή μέθοδος για την επίτευξη του περιορισμού του σκοπού. Η στρατηγική του διαχωρισμού απαιτεί κατανεμημένη επεξεργασία αντί για κεντρικές λύσεις. Ειδικότερα, τα δεδομένα που προέρχονται από διαφορετικές πηγές θα πρέπει να αποθηκεύονται σε χωριστές βάσεις δεδομένων και οι εν λόγω βάσεις δεδομένων δεν θα πρέπει να συνδέονται μεταξύ τους. Τα δεδομένα θα πρέπει να υποβάλλονται σε τοπική επεξεργασία, και να αποθηκεύονται σε τοπικό επίπεδο, αν αυτό είναι εφικτό [5]. Οι πίνακες της βάσης δεδομένων θα πρέπει να είναι όσο το δυνατόν περισσότερο κατανεμημένοι, ενώ οι γραμμές – *ή αλλιώς πλειάδες* – σε αυτούς τους πίνακες θα πρέπει να είναι δύσκολο να συνδεθούν μεταξύ τους, για παράδειγμα καταργώντας τυχόν αναγνωριστικά ή χρησιμοποιώντας ψευδώνυμα σε επίπεδο πίνακα.

Μέθοδοι

Η στρατηγική του διαχωρισμού περιέχει τις ακόλουθες μεθόδους.

- **Απομόνωση** [29]**:** Συλλογή και επεξεργασία προσωπικών δεδομένων σε διαφορετικές βάσεις δεδομένων ή εφαρμογές. Αυτές οι βάσεις δεδομένων ή εφαρμογές είτε διαχωρίζονται λογικά είτε εκτελούνται σε διαφορετικό υλικό (hardware).
- **Κατανομή** [29]**:** Κατανομή της συλλογής και επεξεργασίας δεδομένων προσωπικού χαρακτήρα σε διαφορετικές φυσικές τοποθεσίες χρησιμοποιώντας βάσεις δεδομένων και συστήματα που δεν βρίσκονται υπό τον έλεγχο μιας μεμονωμένης οντότητας. Χρήση αποκεντρωμένων ή ακόμη και κατανεμημένων αρχιτεκτονικών συστημάτων αντί για κεντρικών.

Στρατηγική 4: Συγκέντρωση – Συνάθροιση

Η τέταρτη στρατηγική σχεδιασμού, ***η στρατηγική της συνάθροισης***, αναφέρει ότι τα προσωπικά δεδομένα πρέπει να υποβάλλονται σε επεξεργασία στο υψηλότερο επίπεδο συγκέντρωσης – *δηλαδή να συναθροίζονται όσο το δυνατόν περισσότερα δεδομένα* – και με τη μικρότερη δυνατή λεπτομέρεια κατά την οποία να παραμένουν χρήσιμα.

Η συγκέντρωση πληροφοριών σε ομάδες χαρακτηριστικών ή ομάδες ατόμων περιορίζει το επίπεδο λεπτομέρειας στα προσωπικά δεδομένα που διατηρούνται [5] [29]. Συνεπώς, τα δεδομένα αυτά γίνονται λιγότερο «ευαίσθητα» αν οι πληροφορίες είναι προσεγγιστικές και το μέγεθος της ομάδας επί της οποίας συγκεντρώνονται τα προσωπικά δεδομένα είναι αρκετά μεγάλο. Τα κατά προσέγγιση δεδομένα αφορούν σε προσωπικά δεδομένα τα οποία είναι αρκετά γενικά, και οι πληροφορίες που αποθηκεύονται ισχύουν για πολλά άτομα, που σημαίνει ότι ελάχιστες πληροφορίες μπορούν να αποδοθούν σε ένα μεμονωμένο άτομο [5]. Με αυτό τον τρόπο επιτυγχάνεται κατ’ επέκταση η προστασία της ιδιωτικότητας του φυσικού

προσώπου. Συνεπώς, όσο πιο γενικευμένο είναι ένα σύνολο προσωπικών δεδομένων, τόσο μικρότερος είναι ο κίνδυνος παραβίασης της ιδιωτικότητας [29].

Μέθοδοι

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα με περιορισμένο επίπεδο λεπτομέρειας μπορεί να πραγματοποιηθεί τόσο σε επίπεδο υποκειμένου των δεδομένων όσο και σε επίπεδο χαρακτηριστικού.

- **Σύνοψη** [29]**:** Σύνοψη, ή αλλιώς γενίκευση, των λεπτομερών χαρακτηριστικών σε πιο γενικά χαρακτηριστικά. Για παράδειγμα, χρήση ενός ηλικιακού εύρους αντί για μια ημερομηνία γέννησης, ή χρήση μιας πόλης διαμονής αντί για μια πλήρη διεύθυνση.
- **Ομαδοποίηση** [29]**:** Επεξεργασία συγκεντρωτικών πληροφοριών που αφορούν σε μια ομάδα ατόμων έναντι της επεξεργασίας προσωπικών πληροφοριών για κάθε άτομο στην ομάδα ξεχωριστά. Δημιουργία προφίλ μιας ομάδας με μέσες πληροφορίες σχετικά με τα μέλη της ομάδας.
- **Σύγχυση** [29]**:** Πρέπει να αποτρέπεται η επεξεργασία των ακριβή δεδομένων προσωπικού χαρακτήρα και να χρησιμοποιείται μια προσέγγιση της αρχικής τιμής. Εναλλακτικά είναι ωφέλιμη και η προσθήκη κάποιου τυχαίου θορύβου στην αρχική τιμή των δεδομένων. Για παράδειγμα, αντί να γίνει χρήση της ακριβούς τοποθεσίας ενός ατόμου, μπορεί να χρησιμοποιηθεί μια άλλη τοποθεσία, η οποία απέχει κατά κάποια τυχαία απόσταση από την πραγματική τοποθεσία του.

Αξίζει να σημειωθεί ότι ακόμη και τα συγκεντρωτικά δεδομένα ενέχουν κινδύνους για παραβίαση της ιδιωτικότητας όταν μεμονωμένα άτομα μπορούν εύκολα να κατηγοριοποιηθούν σε μια συγκεκριμένη ομάδα ατόμων – (όπως άτομα με συγκεκριμένη ιατρική πάθηση ή με συγκεκριμένο οικονομικό προφίλ).

Στρατηγική 5: Πληροφόρηση

Η ***στρατηγική της πληροφόρησης*** αντιστοιχεί στην έννοια της διαφάνειας *(βλέπε την αρχή της «ανοιχτότητας, διαφάνειας και γνωστοποίησης» της ενότητας 2)*. Τα υποκείμενα των δεδομένων θα πρέπει να ενημερώνονται επαρκώς κάθε φορά που υποβάλλονται σε επεξεργασία τα δεδομένα προσωπικού χαρακτήρα που τα αφορούν [29]. Όταν τα υποκείμενα των δεδομένων χρησιμοποιούν ένα σύστημα, θα πρέπει να ενημερώνονται σχετικά με τα δεδομένα προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία, το σκοπό και τα μέσα της επεξεργασίας αυτής [5] [29]. Η ενημέρωση των υποκειμένων των δεδομένων πρέπει να περιλαμβάνει πληροφορίες σχετικά με τους τρόπους προστασίας των προσωπικών τους δεδομένων, και με το δικαίωμα πρόσβασης στα δεδομένα τους [5]. Η διαφάνεια σχετικά με το επίπεδο ασφάλειας του συστήματος είναι εξίσου σημαντική καθώς επιτρέπει στους χρήστες να λαμβάνουν τεκμηριωμένες αποφάσεις σχετικά με τη χρήση, ή μη, του συστήματος [29]. Μια καλή πρακτική είναι η παροχή πρόσβασης σε σαφή τεκμηρίωση του σχεδιασμού του συστήματος. Τα υποκείμενα των δεδομένων θα πρέπει επίσης να ενημερώνονται σχετικά με τρίτα μέρη στα οποία κοινοποιούνται τα προσωπικά τους δεδομένα.

Μέθοδοι

Η πληροφόρηση των υποκειμένων των δεδομένων μπορεί να επιτευχθεί με τις ακόλουθες πρακτικές.

- **Παροχή** [29]**:** Παροχή πληροφοριών σχετικά με το ποια προσωπικά δεδομένα υποβάλλονται σε επεξεργασία, με ποιο τρόπο υποβάλλονται σε επεξεργασία και για ποιο σκοπό. Σαφής προσδιορισμός της διάρκεια διατήρησης των προσωπικών δεδομένων, και του τρόπου διαγραφής τους. Καταγραφή όλων των τρίτων μερών με τα οποία διαμοιράζεται ο οργανισμός τα προσωπικά δεδομένα των υποκειμένων των δεδομένων, και επιβολή όρων και κανόνων υπό τους οποίους μπορούν τα τρίτα μέρη να επεξεργάζονται αυτά τα δεδομένα. Δυνατότητα επικοινωνίας με κάποιον αρμόδιο υπάλληλο του οργανισμού έτσι ώστε να μπορούν οι χρήστες – *τα υποκείμενα των δεδομένων* – να εκφράζουν ερωτήσεις σχετικά με την ιδιωτικότητά τους.
- **Επεξήγηση** [29]**:** Επεξήγηση και αιτιολόγηση του σκοπού επεξεργασίας των προσωπικών δεδομένων, με τρόπο σαφή και κατανοητό, λαμβάνοντας υπόψη ότι τα υποκείμενα των δεδομένων ενδέχεται να μην έχουν πρότερη γνώση σε θέματα ιδιωτικότητας και να μην μπορούν να κατανοήσουν εύκολα τόσο την ορολογία όσο και το πλαίσιο επεξεργασίας των προσωπικών τους δεδομένων.
- **Ενημέρωση** [29]**:** Ενημέρωση των υποκειμένων των δεδομένων – *σε πραγματικό χρόνο* – τη στιγμή που υποβάλλονται σε επεξεργασία τα προσωπικά τους δεδομένα, διαμοιράζονται σε τρίτους ή μόλις γίνει αντιληπτή μια διαρροή δεδομένων [5]. Η ενημέρωση των υποκειμένων των δεδομένων πρέπει να πραγματοποιείται με σαφείς και σύντομες διαδικασίες ως προς αυτό.

Στρατηγική 6: Έλεγχος

Κατά τη ***στρατηγική του ελέγχου*** δίνεται η δυνατότητα στα υποκείμενα των δεδομένων να επιβλέπουν και να επιθεωρούν τις ενέργειες που αφορούν στην επεξεργασία των προσωπικών τους δεδομένων [5].

Η στρατηγική του ελέγχου είναι αντίστοιχη, ή αλλιώς συμπληρωματική, της στρατηγικής πληροφόρησης. Αν δεν υπάρχουν εύλογα μέσα ελέγχου της επεξεργασίας των προσωπικών δεδομένων ενός φυσικού προσώπου, η απλή ενημέρωση των υποκειμένων των δεδομένων, σχετικά με το γεγονός ότι συλλέγονται προσωπικά δεδομένα, δεν είναι ωφέλιμη ως προς τα ίδια τα υποκείμενα. Φυσικά ισχύει και το αντίθετο. Χωρίς την κατάλληλη πληροφόρηση των υποκειμένων των δεδομένων, η δήλωση συγκατάθεσης για την επεξεργασία προσωπικών δεδομένων χάνει την αξία της [5]. Η νομοθεσία περί προστασίας προσωπικών δεδομένων συχνά παρέχει στο υποκείμενο των δεδομένων το δικαίωμα να βλέπει, να ενημερώνει/ τροποποιεί ή ακόμη και να ζητά τη διαγραφή των προσωπικών δεδομένων που συλλέγονται σχετικά με αυτό [6]. Επιπλέον, ο έλεγχος των προσωπικών δεδομένων είναι πιθανό να διορθώσει τυχόν σφάλματα ή ελλείψεις στα δεδομένα, και να βελτιώσει την ποιότητα των δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία.

Μέθοδοι

Η στρατηγική του ελέγχου περιέχει τις ακόλουθες μεθόδους.

- **Συγκατάθεση** [29]**:** Αίτημα συγκατάθεσης για την επεξεργασία προσωπικών δεδομένων από τον οργανισμό προς τα υποκείμενα των δεδομένων. Τα υποκείμενα των δεδομένων πρέπει να ενημερώνονται εκ των προτέρων για το σύνολο των προσωπικών δεδομένων που θα υποβληθούν σε επεξεργασία, το είδος, τον τρόπο, και τα μέσα της επεξεργασίας *(βλέπε την αρχή της «συγκατάθεσης» της ενότητας 2 και τη στρατηγική πληροφόρησης της ενότητας 3)*. Επιπλέον, θα πρέπει να δίνεται η δυνατότητα άρσης της συγκατάθεσης.

- **Ενημέρωση** [29]**:** Πρέπει να παρέχονται τα κατάλληλα μέσα στα υποκείμενα των δεδομένων έτσι ώστε να μπορούν να ελέγχουν και να ενημερώνουν τα προσωπικά τους δεδομένα.
- **Ανάκληση** [29]**:** Τα υποκείμενα των δεδομένων πρέπει να είναι σε θέση να διαγράφουν, ή να κάνουν αίτημα για διαγραφή, των προσωπικών τους δεδομένων.

Στρατηγική 7: Επιβολή

Η έβδομη στρατηγική, ***η στρατηγική της επιβολής***, αναφέρει ότι πρέπει να εφαρμόζεται μια πολιτική ιδιωτικότητας (privacy policy), η οποία να είναι συμβατή με τις νομικές απαιτήσεις. Αυτή η στρατηγική σχετίζεται με την αρχή της «λογοδοσίας», καθώς και με την αρχή του «περιορισμού του σκοπού» [5] *(βλέπε ενότητα 2)*.

Η στρατηγική της επιβολής διασφαλίζει την ύπαρξη της πολιτική ιδιωτικότητας, και αποτελεί δέσμευση για επεξεργασία προσωπικών δεδομένων με τρόπο που να σέβεται την ιδιωτικότητα των υποκειμένων των δεδομένων [5] [29]. Το επίπεδο προστασίας της ιδιωτικότητας εξαρτάται από την πολιτική, η οποία θα πρέπει να είναι κατ' ελάχιστο συμβατή με τις νομικές απαιτήσεις. Η πολιτική ιδιωτικότητας πρέπει να εφαρμόζεται στα πλαίσια ενός οργανισμού, και να υλοποιούνται τα κατάλληλα μέτρα προστασίας της ιδιωτικότητας, έτσι ώστε να αποτρέπονται οι εν δυνάμει κίνδυνοι για παραβίασή της [5]. Ωστόσο, η προστασία των δεδομένων δεν πρέπει να διασφαλίζεται μόνο με τεχνικά μέτρα, αλλά και με οργανωτικά. Πιο συγκεκριμένα, η ιδιωτικότητα, θα πρέπει να αποτελεί μέρος της κουλτούρας του οργανισμού, και να μεταδίδεται από την ανώτατη διοίκηση προς όλους τους εργαζομένους. Διαφορετικά θα χαθεί το αίσθημα της υπευθυνότητας ως προς την επεξεργασία και προστασία των προσωπικών δεδομένων [29]. Μια σαφής πολιτική ιδιωτικότητας θα παρέχει πεδίο εφαρμογής και καθοδήγηση. Η στρατηγική της επιβολής είναι προσανατολισμένη εσωτερικά προς τον ίδιο τον οργανισμό.

<u>Μέθοδοι</u>

Η στρατηγική της επιβολής περιέχει τις ακόλουθες μεθόδους.

- **Δημιουργία** [29]**:** Ο οργανισμός θα πρέπει να δεσμευτεί ως προς την προστασία της ιδιωτικότητας των φυσικών προσώπων, να δημιουργήσει μια πολιτική ιδιωτικότητας, και να εκχωρήσει πόρους και μέτρα για την υλοποίηση αυτής της πολιτικής. Επιπλέον, για κάθε διαδικασία, θα πρέπει να προσδιοριστεί ο σκοπός επεξεργασίας και η νομική βάση στην οποία υπόκειται η εν λόγω επεξεργασία (π.χ. έννομο συμφέρον ή απαίτηση για συγκατάθεση).
- **Διατήρηση** [29]**:** Διατήρηση της πολιτικής με την υλοποίηση όλων των απαραίτητων τεχνικών και οργανωτικών μέτρων. Ανάθεση αρμοδιοτήτων. Ευαισθητοποίηση και εκπαίδευση του προσωπικού. Συμμόρφωση των υπεύθυνων και των εκτελούντων την επεξεργασία, καθώς και των τρίτων μερών, με την πολιτική ιδιωτικότητας.
- **Τήρηση** [29]**:** Δεδομένου ότι η δραστηριότητα ενός οργανισμού ενδέχεται να αλλάξει, ή ενδέχεται να τεθεί σε εφαρμογή ένας καινούριος κανονισμός – *όπως για παράδειγμα η εφαρμογή του Γενικού Κανονισμού Προστασίας Δεδομένων το 2018* – πρέπει να γίνεται επαλήθευση της πολιτικής ιδιωτικότητας, και επιπλέον, ανά τακτά χρονικά διαστήματα, πρέπει να ελέγχονται και τα μέτρα υλοποίησης αυτής της πολιτικής.

Στρατηγική 8: Επίδειξη

Η τελευταία στρατηγική, ***η στρατηγική της επίδειξης***, απαιτεί από τον υπεύθυνο επεξεργασίας να είναι σε θέση να αποδείξει τη συμμόρφωση του οργανισμού με την πολιτική ιδιωτικότητας και τις ισχύουσες νομικές απαιτήσεις [5]. Η στρατηγική αυτή έχει υποστηρικτικό ρόλο στην αρχή της «λογοδοσίας» της δεύτερης ενότητας.

Η στρατηγική της επίδειξης μπορεί να θεωρηθεί ως επέκταση της στρατηγικής της επιβολής, καθώς απαιτεί από τον υπεύθυνο επεξεργασίας να αποδείξει ότι έχει τον έλεγχο των προσωπικών δεδομένων [5]. Ειδικότερα, απαιτείται από τον υπεύθυνο επεξεργασίας να είναι σε θέση να δείξει τον τρόπο με τον οποίο εφαρμόζεται, αποτελεσματικά, η πολιτική ιδιωτικότητας στα συστήματα πληροφορικής. Σε περίπτωση παραπόνων ή προβλημάτων, ο υπεύθυνος επεξεργασίας θα πρέπει να είναι άμεσα σε θέση να προσδιορίσει την έκταση παραβίασης της ιδιωτικότητας.

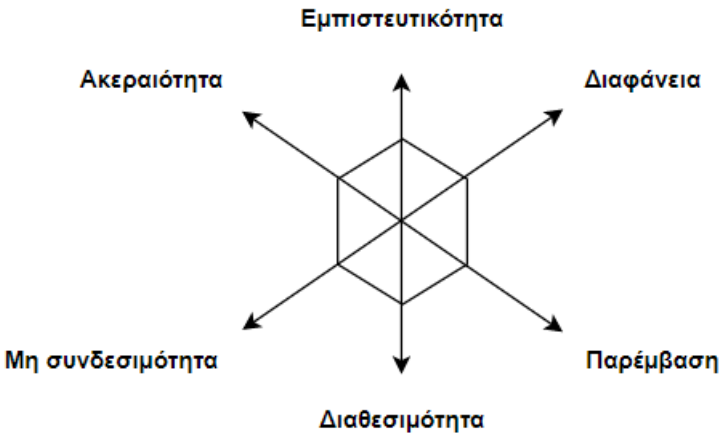
Μέθοδοι

Οι παρακάτω μέθοδοι βοηθούν τους οργανισμούς να επιδείξουν συμμόρφωση.

- **Καταγραφή** [29]**:** Συλλογή αρχείων καταγραφής του συστήματος.
- **Έλεγχος** [29]**:** Τακτικός έλεγχος των αρχείων καταγραφής. Έλεγχος των διαδικασιών και του τρόπου επεξεργασίας των προσωπικών δεδομένων εντός του οργανισμού.
- **Αναφορά** [29]**:** Αναφορά των αποτελεσμάτων των εν λόγω ελέγχων στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ). Είναι ωφέλιμο ο οργανισμός να συμβουλεύεται την ΑΠΔΠΧ όποτε αυτό είναι εφικτό ή κρίνεται απαραίτητο.

Στόχοι Προστασίας της Ιδιωτικότητας

Η ασφάλεια των πληροφοριών στα συστήματα πληροφορικής και επικοινωνιών επιτυγχάνεται με την ικανοποίηση τριών βασικών στόχων προστασίας της ασφάλειας, που είναι η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα, όπως έχουν ορισθεί στην πρώτη ενότητα [5] [31]. Αυτό το τρίπτυχο, όπως αποκαλείται, θεωρείται βασικής σημασίας για την αξιολόγηση των συνθηκών ασφαλείας ενός συστήματος πληροφορικής, καθώς και για τον εντοπισμό των κινδύνων και την επιλογή των κατάλληλων μέτρων προστασίας [31]. Ενώ έχουν προταθεί αρκετές επεκτάσεις και βελτιώσεις, αυτοί οι βασικοί στόχοι προστασίας παρέμειναν σταθεροί και έχουν χρησιμοποιηθεί ως βάση για πολλές μεθοδολογίες που αφορούν στην ασφάλεια των πληροφοριών [5]. Οι τρεις παραπάνω στόχοι προστασίας της ασφάλειας συμπληρώνονται με τρεις περαιτέρω στόχους προστασίας της ιδιωτικότητας, οι οποίοι προτάθηκαν το 2009, με σκοπό τη δημιουργία ενός πλήρους μοντέλου προστασίας δεδομένων και από τις δύο πτυχές, της Ασφάλειας και της Ιδιωτικότητας [31].



Εικόνα 1: Στόχοι προστασίας της ιδιωτικότητας

Μη συνδεσιμότητα

Η μη συνδεσιμότητα (unlinkability) αποσκοπεί στον διαχωρισμό των δεδομένων και των διαδικασιών [32]. Ειδικότερα, η μη συνδεσιμότητα διασφαλίζει ότι τα προσωπικά δεδομένα προστατεύονται και δεν μπορούν να συνδεθούν μεταξύ τομέων (domain) που απαρτίζουν ένα κοινό σκοπό και πλαίσιο επεξεργασίας, και αυτό σημαίνει ότι οι διαδικασίες πρέπει να λειτουργούν με τέτοιο τρόπο ώστε τα προσωπικά δεδομένα να μην είναι συνδεδεμένα με οποιοδήποτε άλλο σύνολο δεδομένων που βρίσκεται εκτός του εκάστοτε τομέα [5] [31] [32]. Με αυτό τον τρόπο, οποιοσδήποτε τρίτος, ο οποίος έχει πρόσβαση σε δυο σύνολα δεδομένων, δεν θα μπορεί να διαχωρίσει αν τα σύνολα αυτά σχετίζονται μεταξύ τους ή αν είναι τελείως ανεξάρτητα [30]. Σκοπός αυτού του στόχου προστασίας της ιδιωτικότητας είναι η ελαχιστοποίηση των κινδύνων σχετικά με την εσφαλμένη χρήση ή την κατάχρηση προσωπικών δεδομένων. Δεδομένου ότι η μη συνδεσιμότητα διαχωρίζει τα προσωπικά δεδομένα από τα συσχετιζόμενα υποκείμενα των δεδομένων, αποτελεί βασικό στοιχείο για την ελαχιστοποίηση των δεδομένων. Επιπλέον, ο διαχωρισμός των συνόλων δεδομένων που ικανοποιούν διαφορετικούς σκοπούς επεξεργασίας υποστηρίζει την αρχή του «περιορισμού του σκοπού» [32]. Υπάρχει πληθώρα μηχανισμών προστασίας της ιδιωτικότητας που στοχεύουν στην επίτευξη ή την υποστήριξη της μη συνδεσιμότητας και περιλαμβάνουν, μεταξύ άλλων, την μείωση δεδομένων, την γενίκευση, την κρυπτογράφηση, τη χρήση διαφορετικών αναγνωριστικών στοιχείων, τον έλεγχο προσπέλασης, την ανωνυμοποίηση και ψευδωνυμοποίηση, την απόκρυψη, τον διαχωρισμό, και την έγκαιρη διαγραφή δεδομένων [5] [31] [32]. Επιπλέον, αξίζει να σημειωθεί ότι η μη συνδεσιμότητα θα πρέπει να λαμβάνεται υπόψη σε πρώιμα στάδια ανάπτυξης των συστημάτων, διότι διαφορετικά οι μεταγενέστερες αποφάσεις σχεδιασμού ενδέχεται να εμποδίζουν την ορθή υλοποίηση του συστήματος [31].

Διαφάνεια

Η διαφάνεια διασφαλίζει ότι όλες οι διαδικασίες επεξεργασίας προσωπικών δεδομένων, συμπεριλαμβανομένων των νομικών, τεχνικών και οργανωτικών προϋποθέσεων και ρυθμίσεων που καθιστούν εφικτή αυτή την επεξεργασία, μπορούν να γίνουν κατανοητές και να ανακατασκευαστούν ανά πάσα στιγμή [5] [31]. Οι πληροφορίες σχετικά με την επεξεργασία δεδομένων πρέπει να είναι διαθέσιμες πριν, κατά τη διάρκεια και μετά από την εκάστοτε επεξεργασία. Έτσι, η διαφάνεια δεν πρέπει να καλύπτει μόνο την επεξεργασία αυτή καθ' αυτή, αλλά και την προγραμματισμένη επεξεργασία – *αυτή που επρόκειτο να πραγματοποιηθεί* – (εκ των προτέρων διαφάνεια), καθώς και τα αποτελέσματα που έχουν προκύψει από την εκάστοτε επεξεργασία (εκ των υστέρων διαφάνεια) [5] [31].

Οι υπεύθυνοι επεξεργασίας πρέπει να είναι πλήρως ενημερωμένοι και να γνωρίζουν επακριβώς τον τρόπο με τον οποίο χειρίζονται οι εκτελούντες την επεξεργασία τα προσωπικά δεδομένα για λογαριασμό τους *(για λογαριασμό των υπεύθυνων επεξεργασίας)*. Από πλευράς υποκειμένων των δεδομένων, τα υποκείμενα των δεδομένων πρέπει να ενημερώνονται πλήρως σχετικά με τα προσωπικά τους δεδομένα και με τον τρόπο επεξεργασίας τους [32]. Αυτή η ενημέρωση περιλαμβάνει τους σκοπούς επεξεργασίας, τα δεδομένα που υποβάλλονται σε επεξεργασία, το χρονικό διάστημα τήρησης και επεξεργασίας τους, τους αποδέκτες οι οποίοι ενδεχομένως θα αλληλοεπιδρούν με τα δεδομένα, καθώς και τις πιθανές συνέπειες ή κινδύνους που ενδέχεται να προκύψουν από την εν λόγω επεξεργασία. Όλα τα μέρη θα πρέπει να γνωρίζουν τους κινδύνους ιδιωτικότητας και να διαθέτουν επαρκείς γνώσεις και κατάρτιση σχετικά με τα αντίμετρα, τον τρόπο με τον οποίο αυτά χρησιμοποιούνται και τους περιορισμούς που έχουν [32].

Η διαφάνεια σχετίζεται με την αρχής της «ανοιχτότητας, διαφάνειας και γνωστοποίησης» και αποτελεί προϋπόθεση για τη «λογοδοσία» [5] [31]. Οι μηχανισμοί για την επίτευξη ή την υποστήριξη της διαφάνειας περιλαμβάνουν την καταγραφή και την υποβολή εκθέσεων, την τεκμηρίωση της επεξεργασίας δεδομένων (η οποία περιέχει, μεταξύ άλλων, την τεχνολογία, τις αρμοδιότητες, τον πηγαίο κώδικα, τις πολιτικές ιδιωτικότητας και τις κοινοποιήσεις των δεδομένων) και την ενημέρωση των υποκειμένων των δεδομένων.

Παρέμβαση

Αυτός ο στόχος προστασίας της ιδιωτικότητας δίνει τη δυνατότητα στα ενδιαφερόμενα μέρη, τα οποία εμπλέκονται σε κάποια επεξεργασία δεδομένων, να παρεμβαίνουν στις διαδικασίες επεξεργασίας που αφορούν δεδομένα προσωπικού χαρακτήρα [5] [31] [32]. Σκοπός της παρέμβασης (intervenability) είναι η εφαρμογή διορθωτικών μέτρων, όπου αυτό κρίνεται αναγκαίο. Για παράδειγμα, η παρέμβαση σχετίζεται με τις αρχές που αφορούν τα δικαιώματα των φυσικών προσώπων, όπως τα δικαιώματα διόρθωσης και διαγραφής δεδομένων, και το δικαίωμα άρσης της συγκατάθεσής τους. Επιπλέον, η παρέμβαση, είναι σημαντική και για άλλα ενδιαφερόμενα μέρη, όπως οι υπεύθυνοι επεξεργασίας, οι οποίοι είναι απαραίτητο να είναι σε θέση να ελέγχουν τόσο τους εκτελούντες την επεξεργασία όσο και τα χρησιμοποιούμενα συστήματα τα οποία αλληλοεπιδρούν με προσωπικά δεδομένα, έτσι ώστε να εμποδίσουν ή να επηρεάσουν την επεξεργασία που υφίστανται τα προσωπικά δεδομένα ανά πάσα στιγμή [5] [31] [32]. Οι εποπτικές αρχές μπορούν επίσης να παρεμβαίνουν ζητώντας ή επιβάλλοντας τη διαγραφή ή την καταστροφή δεδομένων ή ακόμη και την απενεργοποίηση του εκάστοτε συστήματος [32]. Οι μηχανισμοί για την επίτευξη ή την υποστήριξη της παρέμβασης περιλαμβάνουν διαδικασίες για τον ολικό ή μερικό περιορισμό της επεξεργασίας προσωπικών δεδομένων, την αποτροπή αυτοματοποιημένων αποφάσεων και την εγκαθίδρυση ενιαίων σημείων επικοινωνίας για αιτήματα παρέμβασης των υποκειμένων των δεδομένων σχετικά με τα προσωπικά τους δεδομένα [31] [32].

Τεχνολογίες Ενίσχυσης Ιδιωτικότητας και Μέτρα Προστασίας Προσωπικών Δεδομένων

Όπως αναφέρθηκε και προηγουμένως, η έννοια της Προστασίας των Δεδομένων από το Σχεδιασμό αφορά στην ενσωμάτωση των Μέτρων Προστασίας και των Τεχνολογιών Ενίσχυσης της Ιδιωτικότητας απευθείας από το σχεδιασμό του λογισμικού ή του συστήματος [4]. Για τη διατήρηση του επιπέδου ιδιωτικότητας και την αποφυγή μη εξουσιοδοτημένης επεξεργασίας, ο υπεύθυνος ή ο εκτελών την επεξεργασία θα πρέπει να κάνουν αξιολόγηση των κινδύνων που υπάρχουν από την επεξεργασία προσωπικών δεδομένων, και να εφαρμόσουν τα κατάλληλα μέτρα και τεχνικές για την μείωση των κινδύνων αυτών στο ελάχιστο δυνατό. Για να γίνει αυτό, πρέπει να ληφθούν υπόψη οι κίνδυνοι που υπάρχουν, η φύση των δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία, η πιθανότητα εμφάνισης ενός περιστατικού, καθώς και ο αντίκτυπος από την ενδεχόμενη παραβίαση προσωπικών δεδομένων.

Σύμφωνα με τις στρατηγικές Προστασίας Δεδομένων από το Σχεδιασμό *(βλέπε ενότητα 3)*, η παρακάτω ενότητα επικεντρώνεται σε μια σειρά Μέτρων και Τεχνολογιών Ενίσχυσης της Ιδιωτικότητας που μπορούν να χρησιμοποιηθούν για την εφαρμογή αυτών των στρατηγικών και την διασφάλιση της ιδιωτικότητας [27]. Οι τεχνολογίες και τα μέτρα προστασίας περιλαμβάνουν, μεταξύ άλλων, την αυθεντικοποίηση, τα διαπιστευτήρια που βασίζονται σε χαρακτηριστικά, την Κρυπτογράφηση [6] [33], την Ανωνυμοποίηση [6] [7] και την Ψευδωνυμοποίηση [6] [7] Δεδομένων.

Κρυπτογράφηση Δεδομένων

Η κρυπτογράφηση δεδομένων προσωπικού χαρακτήρα πρέπει να πραγματοποιείται πριν τα δεδομένα να αποθηκευτούν ή να αποσταλούν σε κάποια άλλη οντότητα. Ειδικότερα, όταν η μετάδοση των δεδομένων προσωπικού χαρακτήρα πραγματοποιείται πάνω από ένα δημόσιο δίκτυο, τα δεδομένα αυτά θα πρέπει πρωτίστως να έχουν κρυπτογραφηθεί, ιδίως αν πρόκειται για ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα.

Η κρυπτογράφηση δεδομένων θεωρείται απαραίτητη, καθώς μέσω αυτής διασφαλίζεται η εμπιστευτικότητα των δεδομένων, και έτσι μπορεί να αποφευχθεί η μη εξουσιοδοτημένη προσπέλαση στα δεδομένα προσωπικού χαρακτήρα. Τα κρυπτογραφημένα δεδομένα μειώνουν τον κίνδυνο παραβίασης της ασφάλειας, καθώς αν κάποιος μη εξουσιοδοτημένος χρήστης αποκτήσει πρόσβαση σε αυτά, δεν θα μπορέσει να τα αναγνώσει και να κατανοήσει το περιεχόμενό τους. Αυτός είναι και ο λόγος που τα κλειδιά κρυπτογράφησης δεν πρέπει να αποθηκεύονται μαζί με τα κρυπτογραφημένα δεδομένα, αλλά ξεχωριστά, καθώς έτσι διασφαλίζεται ότι αν κάποιος παραβιάσει το σύστημα όπου αυτά είναι αποθηκευμένα, δεν θα έχει στην κατοχή του και το αντίστοιχο κλειδί για να τα αποκρυπτογραφήσει.

Ανεξαρτήτως από την τοποθεσία αποθήκευσης του κλειδιού, θα πρέπει επίσης να διασφαλίζεται ότι το μέγεθός του είναι κατάλληλο και επαρκές, έτσι ώστε βάσει των υπολογιστικών πόρων που είναι διαθέσιμοι την παρούσα χρονική περίοδο, καθώς και στο κοντινό μέλλον, να μην μπορεί κάποιος μη εξουσιοδοτημένος χρήστης να οδηγηθεί σε αποκάλυψη του κλειδιού κρυπτογράφησης.

Ομομορφική Κρυπτογράφηση

Η Ομομορφική Κρυπτογράφηση (Homomorphic Encryption) είναι μια μέθοδος κρυπτογράφησης κατά την οποία εκτελούνται μαθηματικές πράξεις σε δεδομένα τα οποία είναι ήδη κρυπτογραφημένα [34]. Έτσι, τα κρυπτογραφημένα δεδομένα επεξεργάζονται και

αναλύονται σαν να είναι σε απλή μορφή, χωρίς όμως να αποκρυπτογραφηθούν [35]. Με αυτό τον τρόπο, τα προσωπικά δεδομένα των υποκειμένων των δεδομένων παραμένουν εμπιστευτικά καθ' όλη τη διάρκεια της επεξεργασίας τους, δίνοντας την δυνατότητα επεξεργασίας σε τρίτους, χωρίς να είναι γνωστές οι πραγματικές – *αρχικές* – τιμές του συνόλου δεδομένων. Αυτή είναι επί της ουσίας και η βασική ιδιότητα της Ομομορφικής Κρυπτογράφησης [34]. Σε αυτό το σημείο, αξίζει να σημειωθεί ότι η έξοδος που θα προκύψει από την αποκρυπτογράφηση του αποτελέσματος – *ύστερα από την εκτέλεση των εκάστοτε πράξεων* – θα είναι η ίδια με αυτή που θα προέκυπτε αν είχαν εφαρμοστεί οι ίδιες μαθηματικές πράξεις στα αρχικά – *μη κρυπτογραφημένα* – δεδομένα.

Η Ομομορφική Κρυπτογράφηση επιτρέπει δύο υπολογιστικές πράξεις στο κρυπτογραφημένο κείμενο: την πράξη της πρόσθεσης και την πράξη του πολλαπλασιασμού [35]. Οποιαδήποτε άλλη αλγεβρική πράξη, μπορεί να υπολογιστεί ή συνίσταται, από το συνδυασμό των πράξεων της πρόσθεσης και του πολλαπλασιασμού.

Βάσει του αριθμού των υπολογιστικών πράξεων που εφαρμόζονται στα κρυπτογραφημένα δεδομένα, η Ομομορφική Κρυπτογράφηση κατηγοριοποιείται στους παρακάτω τύπους.

- **Πλήρως Ομομορφική Κρυπτογράφηση (ΠΟΚ) (Fully Homomorphic Encryption)** [36]**:** Ένα σύστημα ΠΟΚ υποστηρίζει απεριόριστο αριθμό υπολογιστικών πράξεων, πρόσθεσης και πολλαπλασιασμού, στα κρυπτογραφημένα δεδομένα.
- **Μερικώς Ομομορφική Κρυπτογράφηση (ΜΟΚ) (Partially Homomorphic Encryption)** [36]**:** Ένα σύστημα ΜΟΚ επιτρέπει απεριόριστο αριθμό μια συγκεκριμένης υπολογιστικής πράξης, είτε πρόσθεσης, είτε πολλαπλασιασμού, και δεν υποστηρίζει και τους δύο τύπους αλγεβρικών πράξεων.
- **Κάπως Ομομορφική Κρυπτογράφηση (ΚΟΚ) (Somewhat Homomorphic Encryption)** [36]**:** Ένας αλγόριθμος ΚΟΚ υποστηρίζει πεπερασμένο αριθμό υπολογιστικών πράξεων, πρόσθεσης ή/και πολλαπλασιασμού, στα κρυπτογραφημένα δεδομένα.

Ασφαλής Υπολογισμός Πολλών Μερών

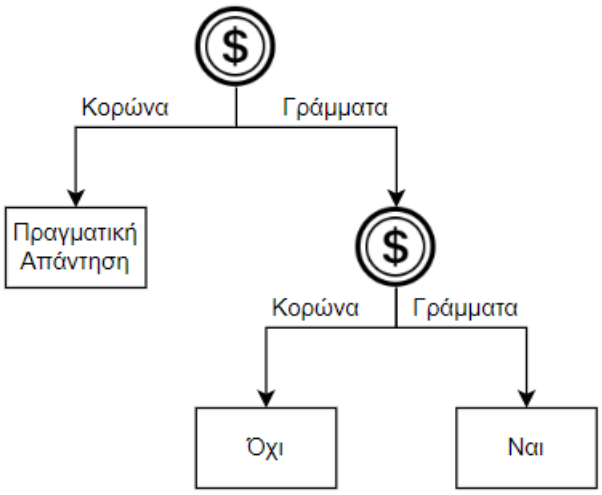
Η έννοια του Ασφαλούς Υπολογισμού Πολλών Μερών (ΑΥΠΜ) (Secure Multi-Party Computation) στοχεύει στην επίλυση προβλημάτων αμοιβαίας εμπιστοσύνης μεταξύ ενός συνόλου μερών, δίνοντάς τους την δυνατότητα του από κοινού υπολογισμού στα δεδομένα [1]. Πιο συγκεκριμένα, ο ΑΥΠΜ στοχεύει στην δημιουργία μεθόδων, με τις οποίες θα μπορούν τα μεμονωμένα μέρη να εκτελούν από κοινού υπολογισμούς στα δεδομένα εισόδου, διατηρώντας τα δεδομένα αυτά ιδιωτικά – εμπιστευτικά ως προς τα υπόλοιπα μέρη [37] [38]. Με αυτό τον τρόπο, κανένα μεμονωμένο μέρος δεν θα μπορεί να δει τα δεδομένα των άλλων μερών ενώ διανέμει τα δεδομένα σε πολλά μέρη [1] [38]. Τα πρωτόκολλα Ασφαλούς Υπολογισμού Δύο Μερών, για παράδειγμα, μπορούν να υπολογίζουν πράξεις ή λειτουργίες στα δεδομένα εισόδου δύο μερών, χωρίς να αποκαλύπτουν τα δεδομένα εισόδου του ενός μέρους στο άλλο [1]. Ανάλογα με το πρωτόκολλο που έχει επιλεχθεί, ο Ασφαλής Υπολογισμός Πολλών Μερών υποστηρίζει τους στόχους για προστασία της ιδιωτικότητας, διασφαλίζοντας την εμπιστευτικότητα των δεδομένων, καθώς τα δεδομένα των άλλων μερών δεν αποκαλύπτονται, και την ακεραιότητα, καθώς καθιστά δύσκολο στους επιτιθέμενους να τροποποιήσουν την έξοδο που θα προκύψει.

Διαφορική Ιδιωτικότητα

Η Διαφορική Ιδιωτικότητα (ΔΙ) (Differential Privacy) μπορεί να θεωρηθεί ως ένας μαθηματικός ορισμός της ιδιωτικότητας. Στην απλούστερη μορφή της, αναλύει ένα σύνολο

δεδομένων και υπολογίζει στατιστικά στοιχεία σχετικά με αυτό, όπως ο μέσος όρος, η διακύμανση και η διάμεσος. Ένας αλγόριθμος ΔΙ μπορεί να θεωρηθεί ως διαφορικά ιδιωτικός αν εξετάζοντας την έξοδό του (το αποτέλεσμα που προέκυψε από την επεξεργασία των δεδομένων), δεν μπορεί κανείς να διαχωρίσει και να καταλάβει αν τα δεδομένα οποιουδήποτε ατόμου συμπεριλήφθηκαν στο αρχικό σύνολο δεδομένων (στα δεδομένα εισόδου) [39]. Επιπλέον, οι αλγόριθμοι Διαφορικής Ιδιωτικότητας διασφαλίζουν ότι μετά την ανάλυση ενός συνόλου δεδομένων, το οποίο αποτελείται από πολλά άτομα, το αποτέλεσμα της ανάλυσης δεν θα επηρεαστεί και θα παραμείνει το ίδιο, ακόμη και αν τα δεδομένα οποιουδήποτε ατόμου (μέχρι κάποιο όριο ε) δεν έχουν συμπεριληφθεί στο σύνολο δεδομένων [1].

Η Διαφορική Ιδιωτικότητα επιτρέπει στους ερευνητές και τους αναλυτές μιας βάσης δεδομένων να εξάγουν χρήσιμες πληροφορίες από τις βάσεις δεδομένων, οι οποίες περιέχουν τα προσωπικά στοιχεία των μεμονωμένων ατόμων, χωρίς να αποκαλύπτουν την προσωπική τους ταυτότητα [40]. Παρέχει εγγύηση ότι δεν διαρρέουν οι προσωπικές πληροφορίες των συμμετεχόντων της βάσης δεδομένων και προστατεύει τα δεδομένα των ατόμων που ανήκουν στο εκάστοτε σύνολο δεδομένων [39]. Ωστόσο, αξίζει να σημειωθεί ότι η Διαφορική Ιδιωτικότητα δεν αποτελεί από μόνη της τεχνική ανωνυμοποίησης, αλλά ένα μοντέλο στο οποίο μπορούν να εφαρμοστούν τεχνικές ανωνυμοποίησης [1].



Εικόνα 2: Αλγόριθμος Διαφορικής Ιδιωτικότητας

Παράδειγμα: Έστω μια έρευνα που αφορά το κάπνισμα και κατά πόσο αυτό προκαλεί καρκίνο. Η ερώτηση που τίθεται στα πλαίσια αυτής της έρευνας αφορά στο αν πάσχει το εκάστοτε άτομο από καρκίνο, και οι πιθανές απαντήσεις είναι είτε «Ναι» είτε «Όχι». Αφού συλλεχθούν οι απαντήσεις όλων των ανθρώπων που συμμετέχουν σε αυτή την έρευνα, αντί να χρησιμοποιηθούν απευθείας για την εξαγωγή ενός συμπεράσματος, θα εισέρθουν ως είσοδοι στον αλγόριθμο ΔΙ (*βλέπε Εικόνα 2*), ο οποίος εισάγει θόρυβο στις ήδη υπάρχουσες τιμές των δεδομένων. Έστω ότι ο Νίκος έχει απαντήσει «Ναι» στην προαναφερθείσα ερώτηση της έρευνας και άρα πάσχει από καρκίνο. Πριν να σταλεί η απάντησή του στο διακομιστή (server) που συγκεντρώνει όλες τις απαντήσεις των ατόμων, ο αλγόριθμος ΔΙ θα γυρίσει ένα νόμισμα και ανάλογα με το αν η πλευρά του νομίσματος είναι κορώνα ή γράμματα θα πράξει αναλόγως. Ειδικότερα, αν η όψη του νομίσματος είναι κορώνα, τότε θα στείλει στο διακομιστή την πραγματική απάντηση που υπέβαλε ο Νίκος, δηλαδή την απάντηση «Ναι». Διαφορετικά, αν είναι γράμματα, ο αλγόριθμος ΔΙ θα γυρίσει ξανά ένα

νόμισμα. Αν η όψη του νομίσματος είναι κορώνα, θα εκχωρήσει την τιμή «Όχι» ως απάντηση, ενώ αν είναι γράμματα θα εκχωρήσει την τιμή «Ναι», ανεξαρτήτως από την πραγματική τιμή που είχε εκχωρηθεί από τον Νίκο [41]. Με αυτό τον τρόπο αντιμετωπίζει η Διαφορική Ιδιωτικότητα το παράδοξο του να μην μαθαίνει κανείς τίποτα για ένα μεμονωμένο άτομο, ενώ μαθαίνει χρήσιμες πληροφορίες για έναν πληθυσμό, καθώς οι πιθανότητες λαμβάνονται πάνω από τυχαίες επιλογές που γίνονται από τον αλγόριθμο ΔΙ [42].

Ανωνυμοποίηση και Ψευδωνυμοποίηση Δεδομένων

Η ανωνυμοποίηση και η ψευδωνυμοποίηση δεδομένων είναι δύο από τις πιο κλασικές και ευρέως διαδεδομένες μεθόδους που χρησιμοποιούνται για την εφαρμογή και υλοποίηση των αρχών ιδιωτικότητας στα δεδομένα προσωπικού χαρακτήρα [1]. Η ψευδωνυμοποίηση αναφέρεται επίσης ρητά στον ΓΚΠΔ ως μια μέθοδος που μπορεί να υποστηρίξει την Προστασία Δεδομένων από το Σχεδιασμό *(άρθρο 25 του ΓΚΠΔ)*, και την ασφαλή επεξεργασία δεδομένων προσωπικού χαρακτήρα *(άρθρο 32 του ΓΚΠΔ)* [6]. Ωστόσο, παρόλο που υπάρχει μια σημαντική διαφορά ανάμεσα σε αυτές τις δυο τεχνικές προστασίας δεδομένων, συχνά συγχέονται. Όπως έχει ήδη επισημανθεί από την ομάδα εργασίας του άρθρου 29 για την προστασία των δεδομένων (working party 29) [43] και σύμφωνα με την αιτιολογική σκέψη 26 (recital) του ΓΚΠΔ [6], οι ανώνυμες πληροφορίες αφορούν σε πληροφορίες που δεν σχετίζονται με κάποιο ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο και έτσι, τα ανωνυμοποιημένα δεδομένα δεν θεωρούνται δεδομένα προσωπικού χαρακτήρα. Αντιθέτως, σύμφωνα με το άρθρο 4 παράγραφος 5 του ΓΚΠΔ [6] [7], τα ψευδωνυμοποιημένα δεδομένα, τα οποία μπορούν να επαναταυτοποιήσουν κάποιο φυσικό πρόσωπο – *με τη χρήση πρόσθετων πληροφοριών* –, είναι δεδομένα προσωπικού χαρακτήρα και οι αρχές προστασίας δεδομένων του ΓΚΠΔ έχουν ισχύ σε αυτά.

Τα τελευταία χρόνια, ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ΕΝΙΣΑ) έχει δημοσιεύσει ορισμένες – *διαφορετικές* – τεχνικές και μεθόδους ανωνυμοποίησης [1] και ψευδωνυμοποίησης δεδομένων [44], καθώς και κάποιες περιπτώσεις χρήσης κατά τις οποίες εφαρμόζεται τόσο η ανωνυμοποίηση όσο και η ψευδωνυμοποίηση δεδομένων στην πράξη. Η παρούσα ενότητα εστιάζει στην έννοια, το ρόλο, και τις βασικές διαφορές των δύο αυτών τεχνικών, βάσει του ΓΚΠΔ, και στην συνέχεια παρουσιάζει εν συντομία ορισμένες τεχνικές και μεθόδους που αποσκοπούν στην προστασία των δεδομένων προσωπικού χαρακτήρα.

Ανωνυμοποίηση Δεδομένων

Η ανωνυμοποίηση δεδομένων μπορεί να θεωρηθεί ως ένα πρόβλημα βελτιστοποίησης μεταξύ δύο αντικρουόμενων παραμέτρων: α) της χρησιμότητας και χρηστικότητας των δεδομένων, και β) της προστασίας έναντι του επαναπροσδιορισμού της ταυτότητας ενός φυσικού προσώπου [1]. Στην πράξη, η ανωνυμοποίηση των δεδομένων επιτυγχάνεται μέσω πληθώρας τεχνικών όπως η προσθήκη θορύβου (noising) ή η γενίκευση (generalization).

Η ανωνυμοποίηση είναι μια διαδικασία, κατά την οποία όλα τα αναγνωριστικά στοιχεία ταυτότητας διαγράφονται ή τροποποιούνται με τέτοιο τρόπο, έτσι ώστε τα δεδομένα που θα προκύψουν από την επεξεργασία αυτή, να μην μπορούν να οδηγήσουν σε ταυτοποίηση του υποκειμένου των δεδομένων με κανένα δυνατό τρόπο. Από τα ανωνυμοποιημένα δεδομένα που θα προκύψουν, ούτε ο υπεύθυνος επεξεργασίας δεν θα μπορεί να καταλήξει στο φυσικό πρόσωπο στο οποίο ανήκουν, ούτε άμεσα, ούτε έμμεσα.

Η διαδικασία της ανωνυμοποίησης είναι μονόδρομη και έτσι κανένας δεν είναι σε θέση να εξακριβώσει την ταυτότητα του υποκειμένου των δεδομένων και να ανακαλύψει ποιο είναι

το φυσικό πρόσωπο στο οποίο ανήκουν τα ανωνυμοποιημένα δεδομένα. Αν κάποιος τρίτος καταφέρει να οδηγηθεί στην αποκάλυψη ενός φυσικού προσώπου, αυτό σημαίνει ότι η ανωνυμοποίηση δεν έχει πραγματοποιηθεί με ορθό τρόπο, πράγμα το οποίο αποτελεί παραβίαση των δεδομένων προσωπικού χαρακτήρα του υποκειμένου των δεδομένων.

Κάθε μια από τις περιπτώσεις χρήσης και επεξεργασίας δεδομένων προσωπικού χαρακτήρα πρέπει να αντιστοιχεί στην εφαρμογή μιας διαφορετικής μεθόδου ανωνυμοποίησης, και δεν θα πρέπει να υπάρχει μια γενική μέθοδος για όλες τις περιπτώσεις, καθώς δεν θα παρέχεται επαρκής προστασία στα δεδομένα προσωπικού χαρακτήρα [1]. Έτσι, η επιλογή της μεθόδου ανωνυμοποίησης πρέπει να γίνεται ανά περίπτωση και ανάλογα με τον τύπο των δεδομένων – *προσωπικά ή ευαίσθητα δεδομένα* –, τον τρόπο και το πλαίσιο επεξεργασίας, καθώς και τις πιθανές επιθέσεις που ενδέχεται να πραγματοποιηθούν στο εκάστοτε σύστημα.

Οι δύο παρακάτω ενότητες περιέχουν μια γρήγορη επισκόπηση των πιο γνωστών τεχνικών και μεθόδων ανωνυμοποίησης.

Τεχνικές Ανωνυμοποίησης Δεδομένων

Απόκρυψη Χαρακτήρων

Αποκρύπτει – *αντικαθιστά* – κάποιο τμήμα των δεδομένων με τυχαίους χαρακτήρες ή άλλα δεδομένα. Η μορφή των δεδομένων διατηρείται, δηλαδή τα δεδομένα διατηρούν ορισμένες ιδιότητες των αρχικών δεδομένων, αλλά ένα μέρος της τιμής τους αντικαθίσταται με κάποιο χαρακτήρα μάσκας, συνήθως « x » ή « * » [45] [46].

Παράδειγμα: Έστω ότι το αρχικό σύνολο δεδομένων (Πίνακας 2) αποτελείται από τις παρακάτω εγγραφές. Αν η τεχνική της Απόκρυψης Χαρακτήρων (ΑΧ) εφαρμοστεί στο έμμεσο αναγνωριστικό «Ταχυδρομικός Κώδικας», τότε η ΑΧ μπορεί να επιτευχθεί όπως απεικονίζεται στον Πίνακα 3.

Ταχυδρομικός Κώδικας	Φύλο	Ηλικία	Ασθένεια
29045	Γυναίκα	45	Καρκίνος
29201	Γυναίκα	23	Γρίπη
29045	Άνδρας	38	Καρκίνος
29063	Γυναίκα	42	Παχυσαρκία
29204	Άνδρας	34	HIV
29201	Άνδρας	28	Γρίπη

Πίνακας 2: Αρχικό σύνολο δεδομένων

Ταχυδρομικός Κώδικας	Φύλο	Ηλικία	Ασθένεια
29***	Γυναίκα	45	Καρκίνος
29***	Γυναίκα	23	Γρίπη
29***	Άνδρας	38	Καρκίνος
29***	Γυναίκα	42	Παχυσαρκία
29***	Άνδρας	34	HIV
29***	Άνδρας	28	Γρίπη

Πίνακας 3: Ανωνυμοποίηση με Απόκρυψη Χαρακτήρων

Γενίκευση Δεδομένων

Μετατροπή μίας τιμής, ενός έμμεσου αναγνωριστικού, σε έναν λιγότερο συγκεκριμένο – *πιο γενικό* – όρο. Η τεχνική της γενίκευσης μπορεί να εφαρμοστεί είτε σε επίπεδο χαρακτηριστικού (attribute generalization) είτε σε επίπεδο μιας τιμής ενός χαρακτηριστικού (cell generalization) [47] [48] [49].

- Γενίκευση Χαρακτηριστικού: Κάθε μια από τις τιμές ενός συγκεκριμένου χαρακτηριστικού – *μιας συγκεκριμένης στήλης του πίνακα* – συνοψίζεται σε ένα επίπεδο γενίκευσης.
- Γενίκευση Τιμής Χαρακτηριστικού: Εφαρμόζεται σε κάποιο κελί του πίνακα. Ο πίνακας μπορεί να περιέχει για μια στήλη διαφορετικά επίπεδα γενίκευσης, δηλαδή διαφορετικές τιμές χαρακτηριστικού.

Κάθε χαρακτηριστικό ΕΑ μπορεί να είναι είτε συνεχές είτε κατηγορικό. Ένα συνεχές χαρακτηριστικό είναι αριθμητικό και μπορεί να λάβει πραγματικές τιμές (π.χ. «Ηλικία» στον Πίνακα 4). Ένα κατηγορικό χαρακτηριστικό λαμβάνει μια τιμή από ένα περιορισμένο σύνολο και οι τιμές του συνόλου εκφράζουν τάξεις ή κατηγορίες (π.χ. «Φύλο» στον Πίνακα 4) [15] [50].

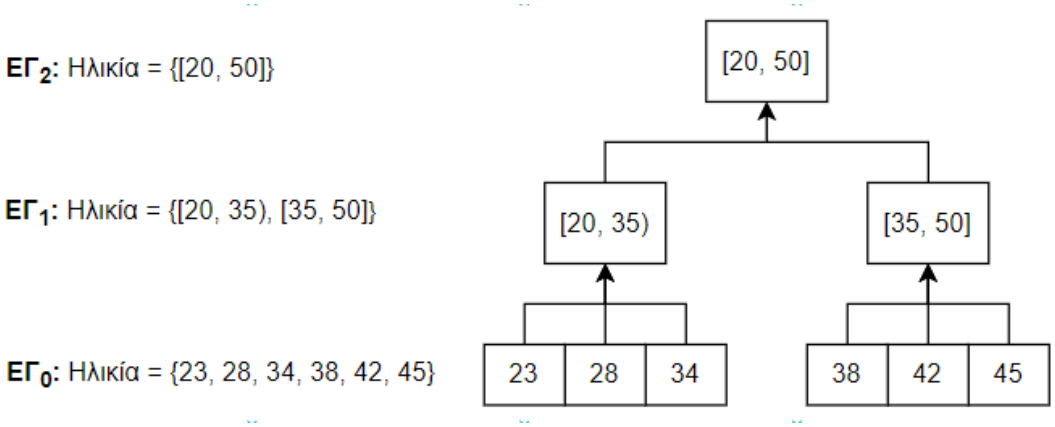
Φύλο	Ηλικία
Γυναίκα	45
Γυναίκα	23
Άνδρας	38
Γυναίκα	42
Άνδρας	34
Άνδρας	28

Πίνακας 4: Αρχικό Σύνολο Δεδομένων

Φύλο	Ηλικία
Άτομο	[35, 50]
Άτομο	[20, 35)
Άτομο	[35, 50]
Άτομο	[35, 50]
Άτομο	[20, 35)
Άτομο	[20, 35)

Πίνακας 5: Γενικευμένο Σύνολο Δεδομένων

Η τεχνική της γενίκευσης απαιτεί τον ορισμό μιας ιεραρχίας γενίκευσης για κάθε χαρακτηριστικό ΕΑ. Κάθε ιεραρχία περιέχει τουλάχιστον δύο επίπεδα γενίκευσης (ΕΓ). Στο υψηλότερο επίπεδο γενίκευσης βρίσκεται η πιο γενική τιμή, ενώ στο χαμηλότερο επίπεδο βρίσκονται οι αρχικές τιμές δεδομένων. Για παράδειγμα, το «δέντρο» της Εικόνας 3 αντιπροσωπεύει μια ιεραρχία γενίκευσης του χαρακτηριστικού «Ηλικία» [15] [50].



Εικόνα 3: Ιεραρχία Γενίκευσης για το χαρακτηριστικό «Ηλικία»

Με την χρήση των ιεραρχιών γενίκευσης δίνεται η δυνατότητα εφαρμογής διαφορετικών στρατηγικών γενίκευσης ανά περίπτωση χρήσης [48] [50]. Ωστόσο, αξίζει να σημειωθεί ότι η

γενίκευση των δεδομένων πρέπει να γίνεται με τέτοιο τρόπο έτσι ώστε να υπάρχει όσο το δυνατόν λιγότερη απώλεια πληροφορίας, χωρίς να υπονομεύεται η ιδιωτικότητα των φυσικών προσώπων.

Απόκρυψη Δεδομένων

Αφαίρεση/διαγραφή των δεδομένων από το σύνολο δεδομένων. Ορισμένες τιμές των χαρακτηριστικών αντικαθίστανται από έναν αστερίσκο ή διαγράφονται τελείως [47] [48]. Η τεχνική της απόκρυψης δεδομένων μπορεί να εφαρμοστεί σε μια εγγραφή του πίνακα (tuple suppression), σε ένα χαρακτηριστικό (attribute suppression), ή σε μια μεμονωμένη τιμής ενός χαρακτηριστικού (cell suppression) [50].

- Απόκρυψη Εγγραφής: Εφαρμόζεται σε μια εγγραφή – *πλειάδα* – του πίνακα.
- Απόκρυψη Χαρακτηριστικού: Εφαρμόζεται σε κάθε μια από τις τιμές μιας στήλης του πίνακα.
- Απόκρυψη Τιμής Χαρακτηριστικού: Εφαρμόζεται σε κάποιο κελί του πίνακα.

Η απόκρυψη δεδομένων μπορεί να θεωρηθεί ως ειδική περίπτωση γενίκευσης όπου όλες οι ιεραρχίες έχουν επίπεδο ίσο με 1 [50].

Παράδειγμα: Έστω το αρχικό σύνολο δεδομένων όπως απεικονίζεται στον Πίνακα 2. Αν η τεχνική της απόκρυψης δεδομένων εφαρμοστεί στο έμμεσο αναγνωριστικό «Φύλο», τότε τα δεδομένα αναπαρίστανται στον Πίνακα 6 ως ακολούθως.

Ταχυδρομικός Κώδικας	Φύλο	Ηλικία	Ασθένεια
29045	*	45	Καρκίνος
29201	*	23	Γρίπη
29045	*	38	Καρκίνος
29063	*	42	Παχυσαρκία
29204	*	34	HIV
29201	*	28	Γρίπη

Πίνακας 6: Ανωνυμοποίηση με Απόκρυψη Δεδομένων

Προσθήκη Θορύβου

Τροποποίηση των χαρακτηριστικών του συνόλου δεδομένων έτσι ώστε να είναι λιγότερο ακριβή, διατηρώντας παράλληλα τη συνολική κατανομή του συνόλου δεδομένων [43] [51]. Κατά την τεχνική της προσθήκης θορύβου προστίθεται θόρυβος σε κάποιο χαρακτηριστικό του συνόλου δεδομένων. Πιο συγκεκριμένα, η τεχνική αυτή ανωνυμοποιεί τα προσωπικά δεδομένα με την προσθήκη ή τον πολλαπλασιασμό ενός στοχαστικού ή τυχαίου αριθμού σε κάποιο ποσοτικό χαρακτηριστικό του συνόλου δεδομένων. Η στοχαστική τιμή επιλέγεται από μια κανονική κατανομή με μέση τιμή μ=0 και τυπική απόκλιση σ^2 [52].

Παράδειγμα: Έστω το αρχικό σύνολο δεδομένων όπως απεικονίζεται στον Πίνακα 2. Αν η τεχνική της προσθήκης θορύβου εφαρμοστεί στο έμμεσο αναγνωριστικό «Ηλικία», και οι ηλικίες των υποκειμένων των δεδομένων ανωνυμοποιηθούν με μια τυχαία προσθήκη ή αφαίρεση ενός αριθμού από το 1 έως το 9, τότε τα δεδομένα που προκύπτουν αναπαρίστανται στον Πίνακα 7 ως ακολούθως.

Ταχυδρομικός Κώδικας	Φύλο	Ηλικία	Ασθένεια
29045	Γυναίκα	42	Καρκίνος
29201	Γυναίκα	30	Γρίπη
29045	Άνδρας	34	Καρκίνος
29063	Γυναίκα	46	Παχυσαρκία
29204	Άνδρας	26	HIV
29201	Άνδρας	30	Γρίπη

Πίνακας 7: Ανωνυμοποίηση με Προσθήκη Θορύβου

Σε αυτό το σημείο αξίζει να σημειωθεί ότι η τεχνική της προσθήκης θορύβου συνήθως συνδυάζεται και με άλλες τεχνικές ανωνυμοποίησης. Γενικότερα, κατά την ανωνυμοποίηση των δεδομένων, μπορούν να συνδυάζονται και να χρησιμοποιούνται παραπάνω από μια τεχνικές ανωνυμοποίησης στο ίδιο σύνολο δεδομένων. Για παράδειγμα μπορεί να εφαρμόζεται μια διαφορετική τεχνική ανά χαρακτηριστικό.

Αριθμητική Διακύμανση και Διακύμανση Ημερομηνίας

Τροποποίηση της αρχικής τιμής – *της τιμής του χαρακτηριστικού* – κατά μια συγκεκριμένη διακύμανση που αντιπροσωπεύει ένα τυχαίο ποσοστό, ή αριθμό, της αρχικής τιμής [53]. Είναι χρήσιμη σε αριθμητικά δεδομένα ή δεδομένα που αφορούν ημερομηνίες [54]. Για παράδειγμα, η στήλη που περιέχει τις ηλικίες μπορεί να έχει μια τυχαία διακύμανση ±5 χρόνια και άρα, τα ανωνυμοποιημένα δεδομένα, *οι τιμές του χαρακτηριστικού «Ηλικία»*, θα κυμαίνονται μεταξύ ενός αυθαίρετου εύρους το οποίο θα είναι ±5 των αρχικών τιμών. Ύστερα από την εφαρμογή αυτής της τεχνικής στα δεδομένα, κάποιες από τις τιμές θα είναι υψηλότερες και κάποιες θα είναι χαμηλότερες από τις αρχικές τιμές, αλλά δεν θα απέχουν αρκετά από το αρχικό εύρος [53].

Παράδειγμα: Έστω το αρχικό σύνολο δεδομένων όπως απεικονίζεται στον Πίνακα 2. Αν η διακύμανση που προσθαφαιρείται από την εκάστοτε αρχική τιμή του συνόλου δεδομένων είναι ίση με 5, τότε τα δεδομένα που θα προκύψουν αναπαρίστανται στον Πίνακα 8 ως ακολούθως.

Ταχυδρομικός Κώδικας	Φύλο	Ηλικία	Ασθένεια
29045	Γυναίκα	40	Καρκίνος
29201	Γυναίκα	28	Γρίπη
29045	Άνδρας	33	Καρκίνος
29063	Γυναίκα	37	Παχυσαρκία
29204	Άνδρας	39	HIV
29201	Άνδρας	23	Γρίπη

Πίνακας 8: Ανωνυμοποίηση με Διακύμανση τιμών δεδομένων

Αναδιοργάνωση/Εναλλαγή Δεδομένων

Η αναδιοργάνωση (shuffling), ή αλλιώς εναλλαγή (swapping), δεδομένων αναδιατάσσει τυχαία τις τιμές μέσα σε μία στήλη του συνόλου δεδομένων, διατηρώντας παράλληλα τη σειρά των εγγραφών στις υπόλοιπες στήλες [53] [54]. Ωστόσο, η αναδιοργάνωση των δεδομένων μπορεί να εφαρμοστεί και σε παραπάνω στήλες του συνόλου δεδομένων [54]. Με άλλα λόγια, τα δεδομένα μιας στήλης ανακατεύονται τυχαία μέσα σε αυτή, και οι τιμές που προκύπτουν είναι επί της ουσίας οι αρχικές τιμές που αντιστοιχούν πλέον σε κάποια διαφορετική εγγραφή του πίνακα. Η τεχνική της αναδιοργάνωσης είναι χρήσιμη όταν είναι

απαραίτητο να διατηρηθούν οι συγκεντρωτικές τιμές στην αρχική τους μορφή [53]. Τα δεδομένα μετατίθενται σε επίπεδο στήλης μέχρις ότου να μην υπάρχει πιθανή συσχέτιση στα δεδομένα μεταξύ των γραμμών του συνόλου δεδομένων [53]. Ωστόσο, υπάρχει κίνδυνος κατά τη χρήση της τεχνικής αυτής, καθώς τα αρχικά δεδομένα εξακολουθούν να υπάρχουν στον ανωνυμοποιημένο πίνακα.

Παράδειγμα: Έστω το αρχικό σύνολο δεδομένων όπως απεικονίζεται στον Πίνακα 2. Αν η τεχνική της αναδιοργάνωσης δεδομένων εφαρμοστεί σε όλα τα έμμεσα αναγνωριστικά, δηλαδή στα χαρακτηριστικά «Ταχυδρομικός Κώδικας», «Φύλο» και «Ηλικία», τότε τα δεδομένα που προκύπτουν αναπαρίστανται στον Πίνακα 9 ως ακολούθως.

Ταχυδρομικός Κώδικας	Φύλο	Ηλικία	Ασθένεια
29201	Άνδρας	45	Καρκίνος
29045	Άνδρας	23	Γρίπη
29045	Γυναίκα	42	Καρκίνος
29201	Γυναίκα	38	Παχυσαρκία
29204	Γυναίκα	28	HIV
29063	Άνδρας	34	Γρίπη

Πίνακας 9: Ανωνυμοποίηση με Αναδιοργάνωση

Αντικατάσταση Δεδομένων

Αντικατάσταση των τιμών σε ένα σύνολο δεδομένων με τυχαίο τρόπο, ή μέσω ενός καταλόγου δεδομένων παρόμοιων με τις αρχικές τιμές του συνόλου δεδομένων [55]. Τα δεδομένα που επρόκειτο να αντικατασταθούν θα επιλεγούν από μια δεδομένη λίστα που περιέχει ψεύτικες – *μη αυθεντικές* – τιμές [53]. Η τεχνική της αντικατάστασης είναι ιδιαίτερα χρήσιμη σε περιπτώσεις όπου η ανωνυμοποίηση στοχεύει να διατηρήσει το αίσθημα της ύπαρξης αυθεντικών δεδομένων [55]. Ωστόσο, η δημιουργία ενός μεγάλου συνόλου ψεύτικων πληροφοριών, οι οποίες θα χρησιμοποιούνται για κάθε αντικατάσταση, αποτελεί πρόκληση για την εφαρμογή της παρούσας τεχνικής [53].

Παράδειγμα: Έστω το αρχικό σύνολο δεδομένων όπως απεικονίζεται στον Πίνακα 2. Αν η τεχνική της αντικατάστασης δεδομένων εφαρμοστεί στο έμμεσο αναγνωριστικό «Ταχυδρομικός Κώδικας», και αντικατασταθούν όλες οι τιμές του με μια τυχαία ακολουθία αριθμών, τότε τα δεδομένα που προκύπτουν αναπαρίστανται στον Πίνακα 10 ως ακολούθως.

Ταχυδρομικός Κώδικας	Φύλο	Ηλικία	Ασθένεια
25389	Γυναίκα	45	Καρκίνος
34747	Γυναίκα	23	Γρίπη
47505	Άνδρας	38	Καρκίνος
69923	Γυναίκα	42	Παχυσαρκία
55077	Άνδρας	34	HIV
28768	Άνδρας	28	Γρίπη

Πίνακας 10: Ανωνυμοποίηση με Αντικατάσταση

Συνθετικά Δεδομένα

Το συνθετικό σύνολο δεδομένων δημιουργείται βάσει των στατιστικών στοιχείων που προέρχονται από το αρχικό σύνολο δεδομένων και αντικατοπτρίζουν τα δεδομένα του πραγματικού κόσμου. Οι τιμές των συνθετικών δεδομένων (synthetic data) δημιουργούνται

με τέτοιο τρόπο ώστε οι στατιστικές πληροφορίες του συνθετικού συνόλου δεδομένων να μην διαφέρουν σε μεγάλο βαθμό από αυτές του πραγματικού συνόλου δεδομένων [56]. Τα συνθετικά δεδομένα παράγονται από κάποιον αλγόριθμο, σε αντίθεση με τα αρχικά δεδομένα που βασίζονται στις προσωπικές πληροφορίες των φυσικών προσώπων. Έχουν πολλά κοινά στοιχεία με τα πραγματικά δεδομένα, όπως τη μορφή και τις σχέσεις μεταξύ των χαρακτηριστικών των δεδομένων. Το συνθετικό σύνολο δεδομένων μοιάζει και συμπεριφέρεται παρόμοια με τα πραγματικά δεδομένα.

Επί της ουσίας, η ιδέα γύρω από τη δημιουργία συνθετικών δεδομένων είναι να λαμβάνει ένας υπολογιστής μια αρχική πηγή δεδομένων – *ένα σύνολο δεδομένων* – και να δημιουργεί καινούρια, τεχνητά δεδομένα, με παρόμοιες στατιστικές ιδιότητες όπως αυτό [57]. Η διατήρηση των στατιστικών ιδιοτήτων σημαίνει ότι όποιος αναλύει τα συνθετικά δεδομένα θα πρέπει να είναι σε θέση να εξάγει τα ίδια στατιστικά συμπεράσματα με αυτά που θα εξήγαγε αν είχε λάβει υπόψη του τα πραγματικά – *πρωτότυπα* – δεδομένα.

Μέθοδοι Ανωνυμοποίησης Δεδομένων

k-ανωνυμία

Η μέθοδος της k-ανωνυμίας (k-anonymity) στοχεύει στο συνδυασμό, ή αλλιώς τη συνάθροιση, προσωπικών δεδομένων με παρόμοια χαρακτηριστικά [1]. Ένα σύνολο δεδομένων μπορεί να θεωρηθεί ως k-ανώνυμο όταν υπάρχει ένας αριθμός από τουλάχιστον k άτομα τα οποία έχουν τις ίδιες τιμές χαρακτηριστικών – *τις ίδιες προσωπικές πληροφορίες* – στο σύνολο δεδομένων [58].

Διαδικασία: Η διαδικασία αυτής της μεθόδου αποτελείται από τα ακόλουθα βήματα [1] [58] [59] [60].

1) Όλα τα άμεσα αναγνωριστικά – *όλες οι μεμονωμένες πληροφορίες που μπορούν να ταυτοποιήσουν ανεξάρτητα ένα φυσικό πρόσωπο* – θα πρέπει να αφαιρεθούν από το σύνολο δεδομένων.
2) Όλα τα χαρακτηριστικά που μπορούν να ταυτοποιήσουν έμμεσα ένα άτομο – *όλα τα έμμεσα αναγνωριστικά ή σχεδόν-αναγνωριστικά* – θα πρέπει να τροποποιηθούν και να γενικευθούν σε ευρύτερες κατηγορίες, έτσι ώστε να έχουν τις ίδιες τιμές για τουλάχιστον k άτομα.
3) Τα υπόλοιπα χαρακτηριστικά που αποτελούν ευαίσθητα δεδομένα θα παραμείνουν τα ίδια εντός του συνόλου δεδομένων.

Αποτέλεσμα: Τα δεδομένα προσωπικού χαρακτήρα ενός υποκειμένου των δεδομένων δεν μπορούν να διακριθούν από τουλάχιστον k – 1 δεδομένα των υποκειμένων των δεδομένων που ανήκουν στην ίδια ομάδα – *στο ίδιο σύνολο* – δεδομένων [1] [58].

Δεδομένου ότι η πιθανότητα επαναπροσδιορισμού της ταυτότητας ενός ατόμου εντός του συνόλου δεδομένων σχετίζεται με την τιμή k, η τιμή αυτή διαδραματίζει βασικό ρόλο κατά την εφαρμογή της k-ανωνυμίας σε ένα σύνολο δεδομένων, ιδίως αν το σύνολο αυτό σχετίζεται με ευαίσθητα δεδομένα όπως τα δεδομένα υγείας [1]. Επί της ουσίας, η μέθοδος αυτή, στοχεύει στην αντιμετώπιση του κινδύνου επαναταυτοποίησης των υποκειμένων των δεδομένων από τα ανωνυμοποιημένα δεδομένα.

Παράδειγμα: Αν το αρχικό σύνολο δεδομένων (Πίνακας 11) αποτελείται από τις ακόλουθες πλειάδες και k = 3, η 3-ανωνυμία μπορεί να επιτευχθεί όπως απεικονίζεται στον Πίνακα 12 και κάθε ομάδα θα πρέπει να έχει τουλάχιστον τρεις εγγραφές με τις ίδιες τιμές χαρακτηριστικών – έμμεσα αναγνωριστικά.

Όνομα	Ταχυδρομικός Κώδικας	Φύλο	Ηλικία	Ασθένεια
Μαρία	29045	Γυναίκα	45	Καρκίνος
Γιώργος	29201	Άνδρας	23	Γρίπη
Ελένη	29045	Γυναίκα	38	Καρκίνος
Βασιλική	29063	Γυναίκα	42	Παχυσαρκία
Δημήτρης	29204	Άνδρας	34	HIV
Γιάννης	29201	Άνδρας	28	Γρίπη

Πίνακας 11: Αρχικό σύνολο δεδομένων

Για την ανωνυμοποίηση των δεδομένων του Πίνακα 11 θα εφαρμοστούν οι τεχνικές της απόκρυψης και της γενίκευσης δεδομένων. Ειδικότερα, σε αυτό το παράδειγμα, το χαρακτηριστικό «Φύλο» δεν θα τροποποιηθεί, καθώς θεωρείται σημαντικό για τη μελέτη των ιατρικών ασθενειών. Επιπλέον, ο «Ταχυδρομικός Κώδικας» της διεύθυνσης των ατόμων, καθώς και η «Ηλικία» τους θα γενικευτούν διατηρώντας τα τρία πρώτα ψηφία του Ταχυδρομικού Κώδικα – *επίπεδο δύο της τεχνικής γενίκευσης* – και χρησιμοποιώντας διαστήματα των ετών για την Ηλικία των ατόμων, αντίστοιχα. Το χαρακτηριστικό «Όνομα» θα διαγραφεί τελείως, καθώς θεωρείται άμεσο αναγνωριστικό του συνόλου δεδομένων.

Ταχυδρομικός Κώδικας	Φύλο	Ηλικία	Ασθένεια
290**	Γυναίκα	[35, 50]	Καρκίνος
292**	Άνδρας	[20, 35)	Γρίπη
290**	Γυναίκα	[35, 50]	Καρκίνος
290**	Γυναίκα	[35, 50]	Παχυσαρκία
292**	Άνδρας	[20, 35)	HIV
292**	Άνδρας	[20, 35)	Γρίπη

Πίνακας 12: Ανωνυμοποιημένο σύνολο δεδομένων (k = 3)

Ωστόσο, η k-ανωνυμία είναι ευαίσθητη σε επιθέσεις [1]. Πιο συγκεκριμένα, αν ένας επιτιθέμενος έχει κάποια πρότερη γνώση για το υποκείμενο των δεδομένων, τότε μπορεί να συμπεράνει την ταυτότητα του φυσικού προσώπου μέσω των παρακάτω επιθέσεων.

Επίθεση Ομοιογένειας (Homogeneity Attack) [61]**:** Η επίθεση αυτή εκμεταλλεύεται περιπτώσεις κατά τις οποίες όλες οι εγγραφές – *πλειάδες* – που ανήκουν σε μια κλάση ισοδυναμίας του k-ανώνυμου πίνακα έχουν την ίδια ή παρόμοια τιμή στο ευαίσθητο χαρακτηριστικό (π.χ. την ίδια ασθένεια). Για παράδειγμα, ο επιτιθέμενος που γνωρίζει ότι η Ελένη είναι 38 χρονών και μένει στην περιοχή με Ταχυδρομικό Κώδικα 29045, μπορεί να συμπεράνει ότι η Ελένη πάσχει από καρκίνο, εφόσον όλες οι πλειάδες με Ηλικία [35, 50] και Ταχυδρομικό Κώδικα 290** έχουν καρκίνο.

Ταχυδρομικός Κώδικας	Φύλο	Ηλικία	Ασθένεια
290**	Γυναίκα	[35, 50]	Καρκίνος
292**	Άνδρας	[20, 35)	Γρίπη
290**	Γυναίκα	[35, 50]	Καρκίνος
290**	Γυναίκα	[35, 50]	Καρκίνος
292**	Άνδρας	[20, 35)	HIV
292**	Άνδρας	[20, 35)	Παχυσαρκία

Πίνακας 13: Επίθεση Ομοιογένειας

Επίθεση Γνωστικού Υπόβαθρου (Background Knowledge Attack) [61]**:** Η επίθεση αυτή αξιοποιεί την ύπαρξη μιας συσχέτισης μεταξύ ενός ή περισσοτέρων χαρακτηριστικών ΕΑ με το ευαίσθητο χαρακτηριστικό, έτσι ώστε να περιορίσει το σύνολο των πιθανών τιμών που αντιστοιχούν στο ευαίσθητο χαρακτηριστικό. Για παράδειγμα, έστω ότι ο επιτιθέμενος γνωρίζει ότι η Μαρία είναι 45 χρονών και μένει στην περιοχή με Ταχυδρομικό Κώδικα 29045, τότε μπορεί να συμπεράνει ότι η Μαρία είτε πάσχει από καρκίνο, είτε πάσχει από παχυσαρκία, εφόσον όλες οι πλειάδες με Ηλικία [35, 50] και Ταχυδρομικό Κώδικα 290** έχουν μια από τις δυο ασθένειες. Επιπλέον, ο επιτιθέμενος γνωρίζει ότι η Μαρία αθλείται καθημερινά, οπότε μπορεί να συμπεράνει ότι δεν έχει πρόβλημα με το βάρος της.

Ταχυδρομικός Κώδικας	Φύλο	Ηλικία	Ασθένεια
290**	Γυναίκα	[35, 50]	Καρκίνος
292**	Άνδρας	[20, 35)	Γρίπη
290**	Γυναίκα	[35, 50]	Καρκίνος
290**	Γυναίκα	[35, 50]	Παχυσαρκία
292**	Άνδρας	[20, 35)	HIV
292**	Άνδρας	[20, 35)	Παχυσαρκία

Πίνακας 14: Επίθεση Γνωστικού Υπόβαθρου

ℓ-διαφορετικότητα

Μια επέκταση της k-ανωνυμίας είναι η μέθοδος ℓ-διαφορετικότητα (ℓ-diversity). Η ℓ-διαφορετικότητα είναι επί της ουσίας ίδια με την k-ανωνυμία, αλλά έχει επιπλέον μια πρόσθετη ιδιότητα. Η μέθοδος της ℓ-διαφορετικότητας ορίζει ως q-block ένα σύνολο εγγραφών που έχουν τις ίδιες τιμές στα χαρακτηριστικά ΕΑ – *αυτή ήταν η λογική πίσω από κάθε ομάδα, ή αλλιώς κλάση ισοδυναμίας, στην k-ανωνυμία της προηγούμενης ενότητας*. Ένα q-block ενός συνόλου δεδομένων θεωρείται ℓ-διαφορετικό αν περιέχει τουλάχιστον ℓ διαφορετικές, διακριτές και καλά-διαμοιρασμένες τιμές στα ευαίσθητα δεδομένα. Συνεπώς, ολόκληρο το σύνολο δεδομένων είναι ℓ-διαφορετικό εφόσον όλα τα q-block είναι ℓ-διαφορετικά [59] [60].

Αποτέλεσμα: Η επίθεση της ομοιογένειας δεν είναι πλέον εφικτή. Επιπλέον, η επίθεση γνωστικού υπόβαθρου γίνεται πιο περίπλοκη [60] [61].

Παράδειγμα: Έστω το αρχικό σύνολο δεδομένων του Πίνακα 15 και ℓ = 3, τότε η 3-διαφορετικότητα μπορεί να επιτευχθεί όπως απεικονίζεται στον Πίνακα 16. Κάθε ομάδα θα πρέπει να έχει τουλάχιστον τρεις εγγραφές με τις ίδιες τιμές χαρακτηριστικών – έμμεσα αναγνωριστικά, όπως στην k-ανωνυμία. Επιπλέον, η στήλη που αντιπροσωπεύει τις ευαίσθητες πληροφορίες – *η στήλη «Ασθένεια»* – θα πρέπει να περιέχει τουλάχιστον τρεις διαφορετικές τιμές ανά ομάδα σε αυτό το χαρακτηριστικό.

Όνομα	Ταχυδρομικός Κώδικας	Φύλο	Ηλικία	Ασθένεια
Μαρία	29045	Γυναίκα	45	Καρκίνος
Ελένη	29201	Γυναίκα	23	HIV
Γιώργος	29045	Άνδρας	38	Γρίπη
Βασιλική	29063	Γυναίκα	42	Παχυσαρκία
Δημήτρης	29204	Άνδρας	34	Γρίπη
Γιάννης	29201	Άνδρας	28	Παχυσαρκία

Πίνακας 15: Αρχικό σύνολο δεδομένων

Για την ανωνυμοποίηση των δεδομένων του Πίνακα 15 θα εφαρμοστούν οι ίδιες τεχνικές και με τον ίδιο τρόπο όπως προηγουμένως, δηλαδή θα εφαρμοστούν οι τεχνικές της απόκρυψης και της γενίκευσης δεδομένων με τον ίδιο τρόπο όπως στην k-ανωνυμία. Επιπλέον, η διαφορά σε αυτό το παράδειγμα είναι ότι θα τροποποιηθεί και το χαρακτηριστικό «Φύλο», και έτσι το σύνολο των τιμών {Άνδρας, Γυναίκα} θα γενικευθεί ως {Άτομο}.

Ταχυδρομικός Κώδικας	Φύλο	Ηλικία	Ασθένεια
290**	Άτομο	[35, 50]	Καρκίνος
292**	Άτομο	[20, 35)	HIV
290**	Άτομο	[35, 50]	Γρίπη
290**	Άτομο	[35, 50]	Παχυσαρκία
292**	Άτομο	[20, 35)	Γρίπη
292**	Άτομο	[20, 35)	Παχυσαρκία

Πίνακας 16: Ανωνυμοποιημένο σύνολο δεδομένων (ℓ = 3)

Επίθεση Ασύμμετρης Κατανομής (Skewness Attack) [60]**:** Η επίθεση αυτή μπορεί να προκύψει όταν η κατανομή των ευαίσθητων δεδομένων σε ένα q-block είναι διαφορετική από ότι είναι στο σύνολο δεδομένων – σε ολόκληρο τον πίνακα. Για παράδειγμα, αν το q-block είναι {290**, Άτομο, [35, 50]}, τότε ο επιτιθέμενος μπορεί να συμπεράνει ότι οποιοδήποτε άτομο ανήκει σε αυτή την ομάδα πάσχει από καρκίνο, με πιθανότητα 66%, ενώ στην πραγματικότητα η πιθανότητα εμφάνισης καρκίνου για ένα άτομο του συνόλου δεδομένων είναι ίση με 33% *(που είναι αισθητά χαμηλότερη)*. Ειδικότερα, αν ο επιτιθέμενος γνωρίζει ότι ο Γιώργος είναι 38 χρονών και μένει στην περιοχή με Ταχυδρομικό Κώδικα 29045, μπορεί να συμπεράνει ότι ο Γιώργος πάσχει από καρκίνο με πιθανότητα 66%.

Ταχυδρομικός Κώδικας	Φύλο	Ηλικία	Ασθένεια
290**	Άτομο	[35, 50]	Καρκίνος
292**	Άτομο	[20, 35)	HIV
290**	Άτομο	[35, 50]	Καρκίνος
290**	Άτομο	[35, 50]	Γρίπη
292**	Άτομο	[20, 35)	Παχυσαρκία
292**	Άτομο	[20, 35)	Γρίπη

Πίνακας 17: Επίθεση Ασύμμετρης Κατανομής

Επίθεση Ομοιότητας Χαρακτηριστικών (Similarity Attack) [60]**:** Η επίθεση αυτή μπορεί να συμβεί όταν ένα q-block αποτελείται από διαφορετικές αλλά σημασιολογικά παρόμοιες τιμές για τα ευαίσθητα δεδομένα. Για παράδειγμα στο q-block με ΕΑ = {290**, Άτομο, [35, 50]}, παρόλο που οι τιμές των ευαίσθητων δεδομένων είναι διαφορετικές, ο επιτιθέμενος μπορεί να εξάγει πληροφορία και να ανακαλύψει από τι πάσχει οποιοδήποτε άτομο της ομάδας αυτής, εφόσον και οι τρεις ασθένειες κατατάσσονται στην ίδια κατηγορία ως «καρκινοπαθείς». Ειδικότερα, αν ο επιτιθέμενος γνωρίζει ότι η Μαρία είναι 45 χρονών και μένει στην περιοχή με Ταχυδρομικό Κώδικα 29045, τότε μπορεί να συμπεράνει ότι η Μαρία πάσχει από καρκίνο.

Ταχυδρομικός Κώδικας	Φύλο	Ηλικία	Ασθένεια
290**	Άτομο	[35, 50]	Καρκίνος Εντέρου
292**	Άτομο	[20, 35)	HIV
290**	Άτομο	[35, 50]	Καρκίνος Στομάχου
290**	Άτομο	[35, 50]	Καρκίνος Νεφρού
292**	Άτομο	[20, 35)	Παχυσαρκία
292**	Άτομο	[20, 35)	Γρίπη

Πίνακας 18: Επίθεση Ομοιότητας Χαρακτηριστικών

Συνοψίζοντας, ο Πίνακας 12 είναι 3-ανώνυμος, αλλά δεν είναι 3-διαφορετικός. Από την άλλη, ο Πίνακας 16 είναι και 3-ανώνυμος και 3-διαφορετικός, δεδομένου ότι υπάρχουν πάντα τουλάχιστον τρεις εγγραφές με ίδιες τιμές στα χαρακτηριστικά ΕΑ *(k = 3)*, και με διαφορετικές τιμές στο χαρακτηριστικό «Ασθένεια» που περιγράφει τα ευαίσθητα δεδομένα.

Ψευδωνυμοποίηση Δεδομένων

Η ψευδωνυμοποίηση είναι μια διαδικασία, κατά την οποία όλα τα αναγνωριστικά στοιχεία ταυτότητας αντικαθίστανται με ψευδώνυμα. Τα δεδομένα που θα προκύψουν από αυτή την επεξεργασία, δεν θα μπορέσουν να οδηγήσουν σε ταυτοποίηση του υποκειμένου των δεδομένων, εκτός αν υπάρχει γνώση συμπληρωματικής (επιπλέον) πληροφορίας. Οι συμπληρωματικές πληροφορίες πρέπει να διατηρούνται ξεχωριστά από τα ψευδωνυμοποιημένα δεδομένα και πρόσβαση σε αυτές οφείλει να έχει μόνο ο υπεύθυνος επεξεργασίας, ο οποίος είναι εξουσιοδοτημένος να αντιστρέψει τη διαδικασία εφόσον αυτό προβλέπεται για κάποιο συγκεκριμένο σκοπό. Οι πληροφορίες αυτές είναι επί της ουσίας ένας πίνακας αντιστοίχισης, ο οποίος διατηρεί τα δεδομένα προσωπικού χαρακτήρα των υποκειμένων των δεδομένων και τα αντίστοιχα ψευδώνυμα αυτών. Τα ψευδώνυμα είναι αναγνωριστικά τα οποία θεωρούνται ως δεδομένα προσωπικού χαρακτήρα, εφόσον σχετίζονται με φυσικά πρόσωπα, και μπορούν να οδηγήσουν στην ταυτοποίηση ενός υποκειμένου των δεδομένων.

Η ψευδωνυμοποίηση δεδομένων πραγματοποιείται έτσι ώστε να περιοριστεί το πλήθος των ατόμων που μπορούν να ταυτοποιήσουν τα υποκείμενα των δεδομένων από τα αντίστοιχα δεδομένα προσωπικού χαρακτήρα τα οποία προσπελάζουν για την εκπλήρωση ενός συγκεκριμένου σκοπού. Μέσω αυτής, τόσο οι υπεύθυνοι όσο και οι εκτελούντες την επεξεργασία, δεν θα γνωρίζουν σε ποιο υποκείμενο των δεδομένων αντιστοιχεί το εκάστοτε σύνολο δεδομένων, καθώς όλες οι πληροφορίες ταυτότητας θα έχουν αντικατασταθεί από ένα ψευδώνυμο. Αυτή η διαδικασία επεξεργασίας είναι πολύ χρήσιμη τόσο σε επεξεργασία δεδομένων προσωπικού χαρακτήρα όσο και σε επεξεργασία ευαίσθητων δεδομένων, καθώς με αυτό τον τρόπο θα διατηρείται μια έμμεση σύνδεση μεταξύ των δεδομένων προσωπικού χαρακτήρα και του φυσικού προσώπου, ενώ παράλληλα μόνο ο υπεύθυνος επεξεργασίας, ο οποίος θα διατηρεί τον πίνακα αντιστοίχισης, θα μπορεί να ταυτοποιήσει το φυσικό πρόσωπο εφόσον αυτό είναι επιθυμητό.

Η ψευδωνυμοποίηση θεωρείται ορθή, όταν τα εναπομείναντα χαρακτηριστικά, με τα αντίστοιχα ψευδώνυμα, δεν μπορούν να συνδεθούν με κάποιο φυσικό πρόσωπο, και η διαδικασία δεν μπορεί να αντιστραφεί, εκτός αν γίνει χρήση επιπρόσθετης πληροφορίας *(του πίνακα αντιστοίχισης)*. Σε οποιαδήποτε άλλη περίπτωση, υπάρχει παραβίαση των δεδομένων προσωπικού χαρακτήρα.

Μέθοδοι Ψευδωνυμοποίησης Δεδομένων

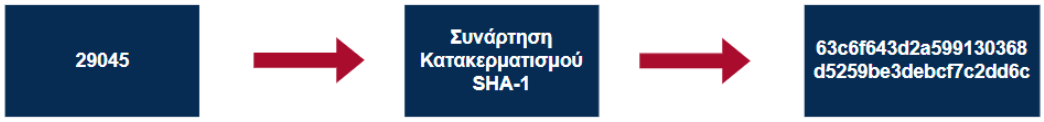
Κρυπτογραφική Συνάρτηση Κατακερματισμού ως Τεχνική Ψευδωνυμοποίησης

Ο κατακερματισμός (hashing) είναι μια μαθηματική έννοια η οποία βρίσκει εφαρμογή, μεταξύ άλλων, στην παραγωγή ψευδώνυμων, καθώς και στην διασφάλιση της ακρίβειας των δεδομένων [44].

Η Κρυπτογραφική Συνάρτηση Κατακερματισμού h(.) είναι μια συνάρτηση που δέχεται ως είσοδο μια τιμή x – *αυθαίρετου μήκους* – και με βάση αυτή την τιμή x δημιουργεί μια έξοδο, την τιμή y = h(x). Για οποιαδήποτε τιμή εισόδου x, θα παράγεται πάντα μια τιμή εξόδου y, η οποία είναι σταθερού μήκους – *το μήκος εξόδου αλλάζει ανάλογα με την επιλογή της συνάρτησης κατακερματισμού* – και είναι ανεξάρτητη από το μέγεθος της τιμής εισόδου. Με αυτό τον τρόπο, κάθε είσοδος έχει μια καθορισμένη έξοδο σταθερού μήκους. Για παράδειγμα, ο αλγόριθμος MD5 (Message-Digest Algorithm) λαμβάνει ως είσοδο ένα μήνυμα αυθαίρετου μήκους και παράγει μια έξοδο μεγέθους 128 bit, δηλαδή 16 χαρακτήρες [44] [62] [53].

Ωστόσο, μια Συνάρτηση Κατακερματισμού θεωρείται ασφαλής όταν ισχύουν οι παρακάτω ιδιότητες:

1. **Μονοδρομικότητα:** Δεδομένου του αποτελέσματος της συνάρτησης κατακερματισμού h(x), είναι υπολογιστικά ανέφικτο να βρεθεί η αρχική τιμή x, καθώς η συνάρτηση h(.) είναι μαθηματικά μη αναστρέψιμη [44] [62].
2. **Ανθεκτικότητα στο δεύτερο προ-είδωλο:** Για οποιαδήποτε δεδομένη τιμή x, δεν μπορεί να βρεθεί μια τιμή y *(τέτοια ώστε y ≠ x)*, που να καταλήγει στην ίδια συνάρτηση κατακερματισμού h(x) = h(y) [44] [62].
3. **Ανθεκτικότητα σε συγκρούσεις:** Δοθείσας μιας τιμής x και μιας τιμής y, τέτοιες ώστε x ≠ y, τα αποτελέσματα των συναρτήσεων κατακερματισμού h(x) και h(y) δεν θα είναι ίδια [44] [62].



Εικόνα 4: Ψευδωνυμοποίηση με χρήση Συνάρτησης Κατακερματισμού

Ωστόσο, η δημιουργία ψευδωνύμων μέσω μιας Συνάρτησης Κατακερματισμού θεωρείται ως μια αδύναμη τεχνική ψευδωνυμοποίησης, καθώς η διαδικασία αυτή μπορεί να αντιστραφεί χωρίς την χρήση πρόσθετων πληροφοριών. Μια αδυναμία αυτής της τεχνικής είναι, ότι καθιστά εύκολη την αντιστοίχιση αναγνωριστικού και ψευδώνυμου, καθώς δίνεται η δυνατότητα σε κάποιον τρίτο, ο οποίος έχει στην κατοχή του ένα δεδομένο αναγνωριστικό, να εκχωρήσει το αναγνωριστικό ως είσοδο στη συνάρτηση κατακερματισμού και στη συνέχεια, να ελέγξει αν υπάρχει αυτό το ψευδώνυμο στο σύνολο δεδομένων. Επιπλέον, μια ακόμα αδυναμία είναι ότι δεν αποτρέπεται η χρήση των ίδιων ψευδώνυμων σε διαφορετικά σύνολα δεδομένων, και σε διαφορετικούς τομείς επεξεργασίας δεδομένων. Αυτό αποτελεί πρόβλημα καθώς η χρήση της ίδιας συνάρτησης κατακερματισμού δημιουργεί σύνδεση μεταξύ δύο διαφορετικών, και μέχρι πρότινος ανεξάρτητων και μη συνδεδεμένων, συνόλων δεδομένων [44]. Για παράδειγμα, έστω δύο πίνακες που περιέχουν τα ακόλουθα δεδομένα

των υποκειμένων των δεδομένων. Το «ΑΦΜ» (Αριθμός Φορολογικού Μητρώου) αποτελεί άμεσο αναγνωριστικό και για τους δύο πίνακες, ενώ ο «Ταχυδρομικός Κώδικας» και η «Ηλικία» είναι τα έμμεσα αναγνωριστικά των Πινάκων 19 και 20 αντίστοιχα. Αν εφαρμοστεί η ίδια Συνάρτηση Κατακερματισμού και στα δυο σύνολα δεδομένων, και πιο συγκεκριμένα στο χαρακτηριστικό «ΑΦΜ», τότε θα αναπαραχθεί το ίδιο ψευδώνυμο και για τα δύο σύνολα δεδομένων, και θα δημιουργηθεί μια σύνδεση μεταξύ αυτών των συνόλων.

ΑΦΜ	Ταχυδρομικός Κώδικας
820501759	29045
603219530	29201
466948956	29045
163897188	29063
703756110	29204
219922166	29201

Πίνακας 19: Σύνολο Δεδομένων Α

ΑΦΜ	Ηλικία
820501759	45
603219530	23
466948956	38
163897188	42
703756110	34
219922166	28

Πίνακας 20: Σύνολο Δεδομένων Β

ΑΦΜ	Ταχυδρομικός Κώδικας
63c6f64…d6c	29045
0922b3e…d09	29201
59e1b8e…229	29045
179234a…14a	29063
0b3d1f1…5cf	29204
f62f900…5a8	29201

Πίνακας 21: Σύνολο Δεδομένων Α'

ΑΦΜ	Ηλικία
63c6f64…d6c	45
0922b3e…d09	23
59e1b8e…229	38
179234a…14a	42
0b3d1f1…5cf	34
f62f900…5a8	28

Πίνακας 22: Σύνολο Δεδομένων Β'

Συμμετρική Κρυπτογράφηση Δεδομένων ως Τεχνική Ψευδωνυμοποίησης

Η Συμμετρική Κρυπτογράφηση των αναγνωριστικών των υποκειμένων των δεδομένων θεωρείται ως μια αποτελεσματική μέθοδος για την δημιουργία ψευδωνύμων. Το άμεσο αναγνωριστικό ενός υποκειμένου των δεδομένων μπορεί να κρυπτογραφηθεί μέσω ενός συμμετρικού αλγορίθμου κρυπτογράφησης, δημιουργώντας έτσι ένα κρυπτοκείμενο που πρόκειται να χρησιμοποιηθεί ως ψευδώνυμο [44] [53]. Στη Συμμετρική Κρυπτογράφηση, το ίδιο μυστικό κλειδί που θα χρησιμοποιηθεί για την δημιουργία του κρυπτοκειμένου – *του ψευδώνυμου* – θα πρέπει να χρησιμοποιηθεί και για την αποκρυπτογράφησή του, όταν θα χρειαστεί να γίνει αντιστροφή της διαδικασίας ψευδωνυμοποίησης.

Εικόνα 5: Ψευδωνυμοποίηση μέσω της Συμμετρικής Κρυπτογράφησης

Η δημιουργία ψευδωνύμου μέσω της Συμμετρικής Κρυπτογράφησης ξεπερνά τα προβλήματα που επιφέρουν οι Συναρτήσεις Κατακερματισμού, εφόσον κανένα τρίτο μέρος, πέρα από τον υπεύθυνο ή τον εκτελούντα την επεξεργασία, δεν έχει πρόσβαση στο μυστικό

κλειδί – στο κλειδί κρυπτογράφησης. Ωστόσο, πρέπει να χρησιμοποιούνται κατάλληλοι αλγόριθμοι κρυπτογράφησης, και το μήκος του κλειδιού κρυπτογράφησης να είναι επαρκές, καθώς η επιλογή του μήκους του κλειδιού αποτελεί βασική προϋπόθεση για την διαφύλαξη και μη εξουσιοδοτημένη αποκάλυψη των δεδομένων [44]. Στους Συμμετρικούς Αλγορίθμους Κρυπτογράφησης, ένα κλειδί μήκους 256 bit θεωρείται, επί του παρόντος, επαρκές για την ασφάλεια των δεδομένων.

Διακριτοποίηση

Η Διακριτοποίηση (Tokenization) [63] αναφέρεται στη διαδικασία της αντικατάστασης των αναγνωριστικών στοιχείων ταυτότητας των υποκειμένων των δεδομένων με τυχαία παραγόμενες τιμές, γνωστές και ως διακριτικά (tokens), τα οποία δεν έχουν καμία σχέση ή συσχέτιση με τα αρχικά δεδομένα. Έτσι, η γνώση ενός διακριτικού δεν έχει καμία χρησιμότητα σε τρίτους, και χρησιμοποιείται συνήθως για την προστασία ευαίσθητων δεδομένων όπως είναι οι οικονομικές συναλλαγές και τα ιατρικά αρχεία [63] [53]. Είναι πολύ σημαντικό, τα συστήματα διακριτοποίησης να είναι σχεδιασμένα καταλλήλως, έτσι ώστε να εξασφαλίζεται ότι πράγματι δεν υπάρχει καμία σύνδεση μεταξύ των ψευδώνυμων και των αρχικών αναγνωριστικών στοιχείων ταυτότητας [44]. Ωστόσο, αξίζει να σημειωθεί ότι παρά την αποτελεσματικότητα της Διακριτοποίησης, η ανάπτυξή της μπορεί να είναι αρκετά δύσκολη κατά περίπτωση, και άρα οι παραπάνω προσεγγίσεις όπως οι αλγόριθμοι κρυπτογράφησης ενδέχεται να είναι προτιμότερες όσον αφορά τη μείωση της πολυπλοκότητας και της αποθήκευσης των δεδομένων [44].

Διαφορές Ανωνυμοποίησης και Ψευδωνυμοποίησης Δεδομένων

Συχνά υπάρχει σύγχυση μεταξύ των εννοιών της ανωνυμοποίησης και ψευδωνυμοποίησης δεδομένων. Ωστόσο, όπως αναφέρεται στην παρακάτω ενότητα, αυτές οι δύο έννοιες είναι διαφορετικές, και θα πρέπει να δοθεί ιδιαίτερη προσοχή κατά την εφαρμογή τους στην πράξη.

Η κύρια διαφορά που διαχωρίζει την ανωνυμοποίηση και την ψευδωνυμοποίηση των δεδομένων υπόκειται στο εξής: Ο Γενικός Κανονισμός Προστασίας Δεδομένων εφαρμόζεται μόνο όταν πρόκειται για επεξεργασία δεδομένων προσωπικού χαρακτήρα, όπου τα δεδομένα σχετίζονται με κάποιο φυσικό πρόσωπο και μπορούν να οδηγήσουν στην άμεση ή έμμεση ταυτοποίηση του υποκειμένου των δεδομένων.

Συνοψίζοντας βάσει των παραπάνω ενοτήτων, η ψευδωνυμοποίηση δεδομένων είναι μια αντιστρέψιμη διαδικασία, καθώς δίνεται η δυνατότητα στον υπεύθυνο επεξεργασίας να οδηγηθεί στην ταυτότητα του φυσικού προσώπου με χρήση του πίνακα αντιστοίχισης. Εφόσον τα ψευδωνυμοποιημένα δεδομένα θεωρούνται ως δεδομένα προσωπικού χαρακτήρα, λόγω της δυνατότητας έμμεσης ταυτοποίησης του φυσικού προσώπου με χρήση του πίνακα αντιστοίχισης, ο Γενικός Κανονισμός Προστασίας Δεδομένων έχει ισχύ και εφαρμόζεται σε αυτά. Επιπλέον, αξίζει να σημειωθεί ότι η μη εξουσιοδοτημένη αντιστροφή αποτελεί παραβίαση προσωπικών δεδομένων, ενώ παράλληλα οποιαδήποτε αντιστροφή πραγματοποιείται, θα πρέπει να προβλέπεται από το σκοπό επεξεργασίας ή τη νομοθεσία.

Από την άλλη, η ανωνυμοποίηση είναι μια μη αντιστρέψιμη διαδικασία, καθώς ύστερα από την εφαρμογή της, παύει να υπάρχει οποιαδήποτε συνδεσιμότητα μεταξύ των ανωνυμοποιημένων δεδομένων και του φυσικού προσώπου. Σε αυτή την περίπτωση, ο Γενικός Κανονισμός Προστασίας Δεδομένων δεν εφαρμόζεται στα ανωνυμοποιημένα δεδομένα, καθώς τα δεδομένα αυτά δεν μπορούν να οδηγήσουν στην αποκάλυψη της ταυτότητας ενός φυσικού προσώπου, εφόσον δεν συνδέονται πλέον με αυτό. Επιπλέον,

βάσει της μη συνδεσιμότητας των δεδομένων, τα ανωνυμοποιημένα δεδομένα μπορούν να κοινοποιηθούν σε τρίτους, χωρίς τη συγκατάθεση του κατόχου τους. Αυτό συμβαίνει, καθώς μόλις τα δεδομένα προσωπικού χαρακτήρα ανωνυμοποιηθούν πλήρως και με ορθό τρόπο, δεν αποτελούν πλέον δεδομένα προσωπικού χαρακτήρα και ο Γενικός Κανονισμός Προστασίας Δεδομένων δεν έχει ισχύ για μεταγενέστερες χρήσεις τους.

Μέτρα Ασφάλειας για την Προστασία της Ιδιωτικότητας

Η αυθεντικοποίηση, η εξουσιοδότηση και ο έλεγχος προσπέλασης, αποσκοπούν στην αποτροπή της μη εξουσιοδοτημένης ή ανεπιθύμητης δραστηριότητας, εφαρμόζοντας ελέγχους και περιορισμούς σχετικά με το τι μπορούν να κάνουν οι χρήστες, ποιους πόρους μπορούν να προσπελαύνουν και ποιες λειτουργίες επιτρέπεται να εκτελούν στα δεδομένα, συμπεριλαμβανομένης της μη εξουσιοδοτημένης προβολής, τροποποίησης ή αντιγραφής [1]. Η αυθεντικοποίηση επιβεβαιώνει την ταυτότητα ενός χρήστη που ζητά πρόσβαση στο σύστημα, ενώ η εξουσιοδότηση καθορίζει ποιες ενέργειες μπορεί να κάνει ένας χρήστης του συστήματος – ένας χρήστης που έχει ήδη αυθεντικοποιηθεί στο σύστημα. Ο έλεγχος προσπέλασης διασφαλίζει ότι μόνο οι εξουσιοδοτημένοι και αυθεντικοποιημένοι χρήστες μπορούν να έχουν πρόσβαση στις πληροφορίες στις οποίες τους έχει εκχωρηθεί το εκάστοτε δικαίωμα. Η αυθεντικοποίηση, η εξουσιοδότηση και ο έλεγχος προσπέλασης είναι τρεις συσχετισμένες έννοιες και η παράλειψη της μίας μπορεί να αποδυναμώσει το επίπεδο προστασίας των δεδομένων.

Μηχανισμοί Ελέγχου Προσπέλασης

Υπάρχει πληθώρα μηχανισμών ελέγχου προσπέλασης που μπορούν να τεθούν σε εφαρμογή. Ωστόσο, η επιλογή του μηχανισμού αυτού καθ’ αυτού εξαρτάται από το πλαίσιο και τις ανάγκες του οργανισμού.

Διακριτικός Έλεγχος Προσπέλασης

Στον Διακριτικό Έλεγχο Προσπέλασης (Discretionary Access Control) οι κάτοχοι ή οι διαχειριστές του πληροφοριακού συστήματος, των δεδομένων, ή των πόρων, είναι αυτοί που ορίζουν τις πολιτικές, οι οποίες καθορίζουν ποια οντότητα είναι εξουσιοδοτημένη για πρόσβαση σε κάποιο πόρο [12] [64]. Τέτοιου είδους συστήματα βασίζονται στους διαχειριστές τους, για να περιορίσουν την εκχώρηση των δικαιωμάτων προσπέλασης [12]. Με αυτό τον τρόπο, δίνεται η δυνατότητα στον κάτοχο ενός αρχείου ή συστήματος να ελέγχει, να εκχωρεί ή να περιορίζει τα δικαιώματα προσπέλασης που έχουν άλλες οντότητες σε αρχεία ή συστήματα που αυτός είναι ιδιοκτήτης [65] [64]. Οι Διακριτικοί Έλεγχοι Προσπέλασης δίνουν μεγάλο βαθμό ελευθερίας ως προς το πλήθος των ενεργειών που μπορούν να πραγματοποιηθούν σε ένα σύστημα, και δεν είναι τόσο περιοριστικοί [65]. Από την άλλη, συγκριτικά με τις μεθόδους που ακολουθούν, θεωρούνται οι λιγότερο ασφαλείς, ενώ παράλληλα είναι ευρέως χρησιμοποιούμενοι από οργανισμούς και εταιρίες [65].

Υποχρεωτικός Έλεγχος Προσπέλασης

Στον Υποχρεωτικό Έλεγχο Προσπέλασης (Mandatory Access Control), τα δικαιώματα πρόσβασης ορίζονται από μια κεντρική αρχή, η οποία αποφασίζει ποιες οντότητες θα έχουν δικαιώματα προσπέλασης και σε ποιους πόρους του συστήματος, βάσει των διαφορετικών επιπέδων ασφαλείας στο οποίο ανήκουν οι πόροι αυτοί [10] [12]. Η διαχείριση τέτοιου είδους συστημάτων είναι αρκετά δύσκολη, καθώς περιορίζει αρκετά τις οντότητες του συστήματος, αλλά η χρήση τους είναι εξαιρετικά σημαντική όταν πρόκειται για την προστασία ευαίσθητων δεδομένων [12]. Σε αντίθεση με την προηγούμενη μέθοδο, του

Διακριτικού Ελέγχου Προσπέλασης, οι κάτοχοι των αρχείων σπάνια μπορούν να αποφασίσουν και να ορίσουν ποιος θα έχει πρόσβαση στα αρχεία τους [65].

Έλεγχος Προσπέλασης βάσει Ρόλου

Κατά τον Έλεγχο Προσπέλασης βάσει Ρόλου (Role-Based Access Control), εκχωρούνται δικαιώματα πρόσβασης σε μια οντότητα *(π.χ. σε έναν χρήστη)* βάσει του ρόλου της, και όχι βάσει της ταυτότητας του μεμονωμένου χρήστη [10] [66]. Με αυτό τον τρόπο, αποτρέπεται η πρόσβαση των χρηστών σε πόρους του συστήματος, εκτός αν οι πόροι αυτοί θεωρούνται απαραίτητοι βάσει του εκάστοτε ρόλου [66]. Έτσι, οι χρήστες θα έχουν δικαιώματα προσπέλασης σε πόρους τους συστήματος βάσει του ρόλου τον οποίο κατέχουν, και εφόσον η προσπέλαση αυτών των πόρων κρίνεται απαραίτητη βάσει αυτού [10] [64]. Σε αντίθεση με τον Διακριτικό Έλεγχο Προσπέλασης, όπου δινόταν η δυνατότητα στους χρήστες του συστήματος να ελέγχουν και να διαχειρίζονται τα δικαιώματα προσπέλασης στους πόρους τους, σε αυτή την περίπτωση, η προσπέλαση ελέγχεται σε επίπεδο συστήματος, και βρίσκεται εκτός του ελέγχου των χρηστών [12].

Έλεγχος Προσπέλασης βάσει Χαρακτηριστικών

Ο Έλεγχος Προσπέλασης βάσει Χαρακτηριστικών (Attribute-Based Access Control) σχετίζει ένα σύνολο χαρακτηριστικών και περιβαλλοντικών συνθηκών με κάθε πόρο και με κάθε χρήστη του συστήματος [10] [66]. Βάσει των χαρακτηριστικών και των συνθηκών τη δεδομένη χρονική στιγμή, γίνεται λήψη απόφασης σχετικά με το αν ο εκάστοτε χρήστης θα μπορεί να προσπελάσει κάποιο πόρο του συστήματος [66]. Τέτοια χαρακτηριστικά ή συνθήκες μπορεί να είναι το ύψος του χρήστη ή η γεωγραφική τοποθεσία, η ημέρα, η ώρα, κ.λπ. [66].

Σε περιπτώσεις όπου οι οργανισμοί διαχειρίζονται και επεξεργάζονται δεδομένα προσωπικού χαρακτήρα ή ευαίσθητα δεδομένα, είναι πολύ σημαντική η επιλογή του μηχανισμού ελέγχου προσπέλασης για να αποφευχθεί η μη εξουσιοδοτημένη προσπέλαση αυτών των δεδομένων [66].

Διαπιστευτήρια βάσει Χαρακτηριστικών

Τα Διαπιστευτήρια βάσει Χαρακτηριστικών (Attribute-Based Credentials), ή αλλιώς τα Ανώνυμα Διαπιστευτήρια (Anonymous Credentials), στοχεύουν στην αυθεντικοποίηση μιας οντότητας με τη χρήση κάποιων ελάχιστων χαρακτηριστικών, χωρίς να αποκαλύπτουν πρόσθετες πληροφορίες που χρησιμοποιούνται συνήθως στην αυθεντικοποίηση και ενδέχεται να αποτελούν προσωπικά δεδομένα [1] [67] [68]. Τα Διαπιστευτήρια βάσει Χαρακτηριστικών επιτρέπουν στους χρήστες – *στα υποκείμενα των δεδομένων* – να λαμβάνουν ψηφιακά πιστοποιητικά, ή αλλιώς διαπιστευτήρια, που πιστοποιούν συγκεκριμένες προσωπικές πληροφορίες [69]. Ένας χρήστης μπορεί να παρουσιάσει τα διαπιστευτήριά του σε έναν ελεγκτή (verifier) με τρόπο που να σέβεται την ιδιωτικότητα του χρήστη, παρέχοντας παράλληλα εγγυήσεις υψηλής αυθεντικότητας στον ελεγκτή [69]. Οι χρήστες λαμβάνουν διαπιστευτήρια από έναν εκδότη (issuer), τα οποία περιλαμβάνουν μια λίστα πιστοποιημένων τιμών χαρακτηριστικών για τον εκάστοτε χρήστη. Με αυτό τον τρόπο, οι χρήστες μπορούν να χρησιμοποιήσουν τα διαπιστευτήριά τους για να αυθεντικοποιηθούν σε επαληθευτές (verifiers), ενώ παράλληλα τους δίνεται η δυνατότητα να αποκαλύψουν μόνο ένα υποσύνολο χαρακτηριστικών τα οποία απαιτούνται κατ' ελάχιστο για την εν λόγω αυθεντικοποίηση [67] [68]. Για παράδειγμα, προκειμένου ένας Πάροχος Υπηρεσιών να επιτρέπει την πρόσβαση σε μια ηλεκτρονική υπηρεσία, ο Πάροχος πρέπει να επαληθεύσει την ηλικία του ατόμου που ζήτησε πρόσβαση στην υπηρεσία αυτή [1]. Αντί να ζητήσει την

ηλικία του ατόμου, ο Πάροχος θα μπορούσε να ζητήσει την τιμή ενός χαρακτηριστικού που υποδεικνύει αν το υποκείμενο των δεδομένων είναι ή δεν είναι άνω των 18 ετών, χωρίς να αποκαλύπτεται η ηλικία του.

Απόδειξη Μηδενικής Γνώσης

Η Απόδειξη Μηδενικής Γνώσης (ΑΜΓ) (Zero-Knowledge Proof) είναι μια μαθηματική τεχνική που στοχεύει στην επαλήθευση των πληροφοριών χωρίς να αποκαλύπτεται η ίδια η πληροφορία [70]. Στην Κρυπτογραφία, η ΑΜΓ συνιστά ένα τρόπο αυθεντικοποίησης των χρηστών, χωρίς να γίνει χρήση ή ανταλλαγή κάποιου μυστικού κωδικού πρόσβασης [71]. Η ΑΜΓ αυθεντικοποίηση επιτυγχάνεται όταν μια οντότητα Α (prover) πείθει μια οντότητα Β (verifier) ότι έχει στην κατοχή της ένα μυστικό αναγνώρισης, χωρίς να αποκαλύπτει το μυστικό αυτό καθ' αυτό [72] [73]. Πιο συγκεκριμένα, κατά την διαδικασία αυθεντικοποίησης, η οντότητα Α πρέπει να πείσει την οντότητα Β ότι έχει εκτελέσει σωστά κάποιον υπολογισμό στα μυστικά δεδομένα, χωρίς να του αποκαλύψει τα δεδομένα αυτά [73].

Απόδειξη Μηδενικής Γνώσης στην Ιδιωτικότητα: Η Απόδειξη Μηδενικής Γνώσης μπορεί να χρησιμοποιηθεί για να εφαρμόσει τις αρχές της εμπιστευτικότητας και ελαχιστοποίησης δεδομένων του ΓΚΠΔ. Επιπλέον, βάσει όσων αναφέρθηκαν προηγουμένως, δίνει την δυνατότητα σε ένα υποκείμενο των δεδομένων να αποδείξει στον υπεύθυνο επεξεργασίας ότι γνωρίζει κάποια μυστική πληροφορία χωρίς να αποκαλύψει τίποτα σχετικά με την πληροφορία αυτή [1].

Υπάρχουν δύο βασικοί τύποι Απόδειξης της Μηδενικής Γνώσης.

- **Διαδραστική Απόδειξη Μηδενικής Γνώσης (Interactive Zero-Knowledge Proof)**: Σε αυτή την περίπτωση, οι οντότητες Α και Β αλληλοεπιδρούν αρκετές φορές, και η αλληλεπίδραση πρέπει να γίνεται σε πραγματικό χρόνο. Ειδικότερα, η οντότητα Β (verifier) κάνει συνεχώς – *μέχρι να πειστεί* – μια σειρά από ερωτήσεις σχετικά με τη «γνώση» που κατέχει η οντότητα Α (prover) [70] [74].
- **Μη-διαδραστική Απόδειξη Μηδενικής Γνώσης (Non-interactive Zero-Knowledge Proof):** Σε αυτή την περίπτωση, η απόδειξη που θα διανεμηθεί από την οντότητα Α (prover) μπορεί να επαληθευτεί από την οντότητα Β (verifier) μόνο μία φορά, ανά πάσα στιγμή. Αυτός ο τύπος απαιτεί περισσότερη υπολογιστική ισχύ [70] [74].

Έργα που στοχεύουν στην Προστασία της Ιδιωτικότητας

Υπάρχουν πολλά έργα που ερευνούν και αναπτύσσουν τεχνολογίες που ενισχύουν την προστασία της ιδιωτικότητας. Ωστόσο, στην παρακάτω ενότητα παρουσιάζονται δύο από τα πιο γνωστά έργα προστασίας της ιδιωτικότητας.

Πλατφόρμα Προτιμήσεων Ιδιωτικότητας

Η Πλατφόρμα Προτιμήσεων Ιδιωτικότητας (Platform for Privacy Preferences – P3P) αναπτύχθηκε από την Κοινοπραξία του Παγκόσμιου Ιστού (World Wide Web Consortium – W3C), και αφορά σε ένα πρότυπο το οποίο σχεδιάστηκε και αναπτύχθηκε έτσι ώστε να παρέχει στους χρήστες του Διαδικτύου μια σαφή και ολοκληρωμένη επεξήγηση του τρόπου με τον οποίο επρόκειτο να χρησιμοποιηθούν οι προσωπικές τους πληροφορίες από μια συγκεκριμένη ιστοσελίδα [75]. Το P3P έχει σχεδιαστεί για να διευκολύνει και να βελτιώσει την επικοινωνία των χρηστών. Βασίζεται στις προκαθορισμένες πολιτικές ιδιωτικότητας μιας ιστοσελίδας και στον τρόπο με τον οποίο αυτές συγκρίνονται και διαμορφώνονται σύμφωνα με τις πολιτικές προτιμήσεων του εκάστοτε χρήστη. Το πρωτόκολλο P3P διευκολύνει τους

χρήστες του Διαδικτύου να αποφασίσουν εάν και υπό ποιες συνθήκες επιθυμούν να αποκαλύψουν τις προσωπικές τους πληροφορίες. Με αυτό τον τρόπο αυξάνεται, για παράδειγμα, η εμπιστοσύνη των χρηστών στις ηλεκτρονικές συναλλαγές, καθώς παρουσιάζονται στους χρήστες ουσιώδεις πληροφορίες και επιλογές σχετικά με τις πρακτικές ιδιωτικότητας που εφαρμόζονται στην εκάστοτε ιστοσελίδα [75]. Παρόλο που το P3P παρέχει έναν τεχνικό μηχανισμό που διασφαλίζει ότι οι χρήστες μπορούν να ενημερώνονται σχετικά με τις πολιτικές ιδιωτικότητας πριν δημοσιεύσουν τις προσωπικές τους πληροφορίες, δεν παρέχει κάποιο τεχνικό μηχανισμό ο οποίος να διασφαλίζει ότι οι ιστότοποι ενεργούν σύμφωνα με αυτές τις πολιτικές [76]. Το P3P δεν θέτει, δηλαδή, κάποια ελάχιστα πρότυπα που πρέπει να τηρούνται από τις ιστοσελίδες για την προστασία της ιδιωτικότητας, ούτε παρακολουθεί αν οι ιστότοποι συμμορφώνονται με τις δικές τους αναφερόμενες διαδικασίες [75]. Επιπλέον, το P3P δεν περιλαμβάνει μηχανισμούς για την ασφαλή διαβίβαση, μεταφορά ή αποθήκευση των προσωπικών δεδομένων. Ωστόσο, μπορεί να ενσωματωθεί σε εργαλεία που έχουν σχεδιαστεί, για τη διευκόλυνση της μεταφοράς δεδομένων [76].

Το πρωτόκολλο P3P χρησιμοποιεί αρχεία XML (Extensible Markup Language), των οποίων η σημασιολογική έννοια διέπεται από ένα προκαθορισμένο σχήμα XML που παρέχεται από το W3C, για να αναπαριστά τις αναγνώσιμες από τον άνθρωπο πολιτικές ιδιωτικότητας σε μια αναγνώσιμη από τον υπολογιστή μορφή. Όταν οι χρήστες επισκέπτονται μια ιστοσελίδα, τα αρχεία P3P που δημοσιεύονται από την ιστοσελίδα ανακτώνται και συγκρίνονται με τις προσωπικές προτιμήσεις που ορίζονται από τον χρήστη μέσω των πρακτόρων P3P. Η ευθύνη του πράκτορα είναι να ανακτήσει την ισχύουσα πολιτική, να προσδιορίσει αν υπάρχουν συγκρούσεις με τις προτιμήσεις του χρήστη και να τις παρουσιάσει σε μια κατανοητή προς το χρήστη μορφή [76]. Με λίγα λόγια, το P3P παρέχει μια αναγνώσιμη από τον υπολογιστή μορφή της πολιτικής ιδιωτικότητας μιας ιστοσελίδας, και ένας πράκτορας πρέπει να αναλύσει το περιεχόμενο αυτής της πολιτικής και να το παρουσιάσει με τρόπο κατανοητό ως προς το χρήστη.

Οι πολιτικές P3P περιλαμβάνουν τα στοιχεία επικοινωνίας της εκάστοτε ιστοσελίδας, και υποδεικνύουν τους τύπους δεδομένων που συλλέγει ένας ιστότοπος, τους σκοπούς για τους οποίους επρόκειτο να χρησιμοποιηθούν τα δεδομένα, και τις πολιτικές διαμοιρασμού και διατήρησης των δεδομένων [77]. Οι πολιτικές P3P υποδεικνύουν επίσης πότε είναι διαθέσιμες οι επιλογές συμμετοχής («opt-in») ή εξαίρεσης («opt-out») και παρέχουν πληροφορίες σχετικά με τον τρόπο άσκησης αυτών των επιλογών.

Ενσωματωμένος Πράκτορας Λογισμικού Προστασίας Προσωπικών Δεδομένων

Το έργο Privacy Incorporated Software Agent (Ενσωματωμένος Πράκτορας Λογισμικού Προστασίας Προσωπικών Δεδομένων) παρουσιάζει την Τεχνολογία Ενίσχυσης της Ιδιωτικότητας ως μια ασφαλή τεχνική λύση για την προστασία της ιδιωτικότητας των φυσικών προσώπων όταν χρησιμοποιούν εφαρμογές ή υπηρεσίες που υλοποιούνται μέσω ευφυών πρακτόρων λογισμικού (intelligent software agents), όπως είναι το ηλεκτρονικό εμπόριο (e-commerce) ή το κινητό ηλεκτρονικό εμπόριο (m-commerce) [75] [78] [79]. Οι ευφυείς πράκτορες λογισμικού είναι ένα τμήμα λογισμικού το οποίο εκτελεί εργασίες για λογαριασμό του εκάστοτε χρήστη, διατηρώντας παράλληλα την ιδιωτικότητά του ή, κατ' ελάχιστο, το επίπεδο προστασίας που καθορίζεται από το ίδιο το φυσικό πρόσωπο [78] [80]. Ο πράκτορας προστατεύει επί της ουσίας τα προσωπικά δεδομένα των χρηστών, τα οποία είναι αποθηκευμένα σε αυτόν, και ελέγχει την εσωτερική επεξεργασία (internal processing) των προσωπικών δεδομένων, καθώς και την ανταλλαγή τους με εξουσιοδοτημένες οντότητες

(χρήστες ή πράκτορες), βάσει της ισχύουσας νομοθεσίας [78]. Ο πράκτορας θα πρέπει, επίσης, να είναι σε θέση να διακρίνει ποιες πληροφορίες θα πρέπει να ανταλλάσσονται, υπό ποιες συνθήκες και σε ποιο τρίτο μέρος. Η πρόκληση εδώ αφορά στην εφαρμογή της νομοθεσίας για την προστασία της ιδιωτικότητας, και πιο συγκεκριμένα στην εφαρμογή του Γενικού Κανονισμού Προστασίας Δεδομένων που αποτελεί το υψηλότερο πρότυπο προστασίας της ιδιωτικότητας την δεδομένη στιγμή [80]. Οι λύσεις που έχουν αναπτυχθεί λαμβάνουν υπόψη τις οδηγίες του Ευρωπαϊκού Κοινοβουλίου σχετικά με την ιδιωτικότητα [78], ενώ παράλληλα θα πρέπει να υπάρχουν κατάλληλοι (κρυπτογραφικοί) μηχανισμοί προστασίας για τη διασφάλιση της ασφάλειας των δεδομένων και την αποφυγή της διαρροής τους σε τρίτους [80].

Συμπεράσματα

Η ραγδαία άνοδος και εξέλιξη των συστημάτων και των τεχνολογιών πληροφορικής και επικοινωνιών εγείρει πολλές ανησυχίες σχετικά με την προστασία της ιδιωτικότητας και των δεδομένων προσωπικού χαρακτήρα, καθώς τα συστήματα και οι τεχνολογίες συλλέγουν, επεξεργάζονται και αλληλοεπιδρούν με προσωπικά δεδομένα για την εκπλήρωση ορισμένων σκοπών και την παροχή συγκεκριμένων υπηρεσιών. Η προστασία της ιδιωτικότητας του ατόμου είναι μία από τις σημαντικότερες ανησυχίες κατά την κοινοποίηση ή τον διαμοιρασμό προσωπικών δεδομένων με τρίτους, δεδομένου ότι ενδέχεται να αποκαλυφθεί η ταυτότητα του φυσικού προσώπου ή ακόμη και να παραβιαστούν τα δικαιώματά του. Για τη μη αποκάλυψη της ταυτότητας των υποκειμένων των δεδομένων, *π.χ. όταν τα προσωπικά τους δεδομένα κοινοποιούνται σε τρίτους*, καθώς και για τη μείωση των κινδύνων παραβίασης της ιδιωτικότητας, εφαρμόζονται τα κατάλληλα, ανά περίπτωση, μέτρα προστασίας της ιδιωτικότητας, καθώς και τεχνολογίες ενίσχυσής της, όπως είναι η ανωνυμοποίηση, η ψευδωνυμοποίηση, οι μηχανισμοί ελέγχου προσπέλασης, και η κρυπτογράφηση.

Ο Γενικός Κανονισμός Προστασίας Δεδομένων μπορεί να μετριάσει πολλούς από τους κινδύνους που θέτει η επεξεργασία δεδομένων προσωπικού χαρακτήρα, με την εφαρμογή των κατάλληλων αρχών, και την ικανοποίηση των απαραίτητων απαιτήσεων και στόχων, για την προστασία της ιδιωτικότητας. Τόσο οι αρχές όσο και οι στρατηγικές ιδιωτικότητας, εξηγούν και αναλύουν τον τρόπο με τον οποίο οι ευρωπαίοι νομοθέτες οραματίζονται δίκαιη, διαφανή και νόμιμη επεξεργασία δεδομένων. Μια από τις νομικές υποχρεώσεις του ΓΚΠΔ αφορά στην Προστασία Δεδομένων από το Σχεδιασμό και εξ Ορισμού, μια έννοια η οποία αποτελεί θεμελιώδη προϋπόθεση και συμβάλλει αποτελεσματικά στην προστασία των προσωπικών δεδομένων. Η αρχή αυτή πρέπει να εφαρμόζεται και να ενσωματώνεται από το στάδιο του σχεδιασμού του εκάστοτε συστήματος, υπηρεσίας ή προϊόντος που αλληλοεπιδρά με προσωπικά δεδομένα, ενώ παράλληλα πρέπει να υποστηρίζεται καθ' όλη τη διάρκεια του κύκλου ζωής των δεδομένων. Δεδομένου ότι τα συστήματα πληροφορικής ενδέχεται να συγκρούονται, και να μην συμμορφώνονται, με πολλές από τις αρχές ιδιωτικότητας, ο ΓΚΠΔ αποτελεί σημαντική πρόκληση για τους προγραμματιστές, τους κατασκευαστές και τους παρόχους υπηρεσιών, και η εφαρμογή του αποτελεί απαίτηση για όλους του οργανισμούς και φορείς που επεξεργάζονται προσωπικά δεδομένα.

Βιβλιογραφικές Αναφορές

[1] European Union Agency for Cybersecurity, "Data Protection Engineering," 2022.

[2] S. D. Warren and L. D. Brandeis, "The Right to Privacy," *Harvard Law Review,* vol. 4, no. 5, pp. 193-220, 1890.

[3] A. F. Westin, Privacy And Freedom, 1968.

[4] C. Li and B. Palanisamy, "Privacy in internet of things: From principles to technologies.," *IEEE Internet of Things Journal,* pp. 488-505, 2018.

[5] European Union Agency for Cybersecurity, "Privacy and Data Protection by Design," 2015.

[6] European Commission, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC," 2016.

[7] International Organization for Standardization, "Information technology — Security techniques — Privacy framework," 2011.

[8] International Organization for Standardization, "Information technology — Security techniques — Information security management systems — Overview and vocabulary," 2018.

[9] D. Gibson, "Identification, Authentication, and Authorization," [Online]. Available: https://blogs.getcertifiedgetahead.com/identification-authentication-authorization/. [Accessed 2022].

[10] "What is access control?," [Online]. Available: https://www.citrix.com/solutions/secure-access/what-is-access-control.html. [Accessed 2022].

[11] B. Lutkevich, "access control," [Online]. Available: https://searchsecurity.techtarget.com/definition/access-control. [Accessed 2022].

[12] A. T. Tunggal and K. Sen, "What is Access Control? The Essential Cybersecurity Practice," [Online]. Available: https://www.upguard.com/blog/access-control. [Accessed 2022].

[13] European Union Agency for Cybersecurity, "10 MISUNDERSTANDINGS RELATED TO ANONYMISATION," 2021.

[14] . A. Gkoulalas-Divanis, G. Loukides and J. Sun, "Publishing data from electronic health records while preserving privacy: A survey of algorithms," *Journal of biomedical informatics,* vol. 50, pp. 4-19, 2014.

[15] F. B. Fredj, N. Lammari and I. Comyn-Wattiau, "Abstracting anonymization techniques: a prerequisite for selecting a generalization algorithm," *Procedia computer science,* vol. 60, pp. 206-215, 2015.

[16] J. Zhang, X. Gong, Z. Han and S. Feng, "An improved algorithm for k-anonymity," in *International Conference on E-business Technology and Strategy*, 2012, pp. 352-360.

[17] D. F. Masoch, "Implementing privacy by design in practice," 2019.

[18] European Union Agency for Cybersecurity, "ENISA: Privacy by Design," [Online]. Available: https://www.enisa.europa.eu/topics/data-protection/privacy-by-design. [Accessed 2022].

[19] European Union Agency for Cybersecurity, "Privacy and Security in Personal Data Clouds," 2017.

[20] European Data Protection Board, "Guidelines 4/2019 on Article 25 Data Protection by Design and by Default," 2020.

[21] EUROPEAN DATA PROTECTION SUPERVISOR, "Privacy by Default," [Online]. Available: https://edps.europa.eu/data-protection/our-work/subjects/privacy-default_en. [Accessed 2022].

[22] J. J. Borking and C. Raab, "Laws, PETs and other technologies for privacy protection," *Journal of Information, Law and Technology,* vol. 1, pp. 1-14, 2001.

[23] R. Hes and J. Borking, "Privacy-Enhancing Technologies: The Path to Anonymity," 1995.

[24] European Union Agency for Cybersecurity, "Privacy Enhancing Technologies: Evolution and State of the Art," 2017.

[25] A. Cavoukian, "Privacy by design: The 7 foundational principles.," *Information and privacy commissioner of Ontario, Canada,* 2009.

[26] A. Cavoukian, "Operationalizing privacy by design: A guide to implementing," 2012.

[27] European Union Agency for Cybersecurity, "Privacy by design in big data," 2015.

[28] M. Colesky, J.-H. Hoepman and C. Hillen, "A critical analysis of privacy design strategies.," *2016 IEEE security and privacy workshops (SPW),* pp. 33-40, 2016.

[29] J. H. Hoepman, "Privacy design strategies (the little blue book)," 2018.

[30] A. Pfitzmann and M. Hansen, "Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management-a consolidated proposal for terminology.," 2008.

[31] M. Hansen, M. Jensen and M. Rost, "Protection goals for privacy engineering," in *2015 IEEE Security and Privacy Workshops*, IEEE, 2015, pp. 159-166.

[32] M. Hansen, "Top 10 mistakes in system design from a privacy perspective and privacy protection goals," in *IFIP primelife international summer school on privacy and identity management for life*, Springer, 2011, pp. 14-31.

[33] International Organization for Standardization, "Information technology — Security techniques — Privacy architecture framework," 2018.

[34] V. F. Rocha, J. López and V. F. D. Rocha, "An Overview on Homomorphic Encryption Algorithms," 2019.

[35] R. Challa, "Homomorphic Encryption: Review and Applications.," *Advances in Data Science and Management,* pp. 273-281, 2020.

[36] R. Yackel, "What is homomorphic encryption?," 2021. [Online]. Available: https://www.keyfactor.com/blog/what-is-homomorphic-encryption/#:~:text=Partially%20homomorphic%20encryption%20algorithms%20allow,sum%20of%20the%20two%20plaintexts. [Accessed 2022].

[37] Ε. Καρατσιώλης και Μ. Λουκίδη-Παπανικολή, «Μελέτη εργαλείων Secure Multiparty Computation με έμφαση στο πρωτόκολλο SPDZ,» 2018.

[38] C. Zhao, S. Zhao, M. Zhao, Z. Chen, C.-Z. Gao, H. Li and Y.-a. Tan, "Secure multi-party computation: theory, practice and applications," *Information Sciences,* vol. 476, pp. 357-372, 2019.

[39] "Differential Privacy," [Online]. Available: https://privacytools.seas.harvard.edu/differential-privacy. [Accessed 2022].

[40] N. Tyagi, "What is Differential Privacy and how does it work?," 2021. [Online]. Available: https://www.analyticssteps.com/blogs/what-differential-privacy-and-how-does-it-work. [Accessed 2022].

[41] "Differential Privacy - Simply Explained," 2018. [Online]. Available: https://www.youtube.com/watch?v=gI0wk1CXlsQ. [Accessed 2022].

[42] C. Dwork and A. Roth, "The algorithmic foundations of differential privacy," *Foundations and Trends® in Theoretical Computer Science,* vol. 9, no. 3-4, pp. 211-407, 2014.

[43] European Commission, "ARTICLE 29 DATA PROTECTION WORKING PARTY," 2014. [Online]. Available: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf. [Accessed 2022].

[44] European Union Agency for Cybersecurity, "Recommendations on shaping technology according to GDPR provisions - An overview on data pseudonymisation," 2019.

[45] Z. Aslanyan and M. Boesgaard, "Privacy Analysis of Format-Preserving Data-Masking Techniques," 2019, pp. 1-6.

[46] O. O. Ajayi and T. O. Adebiyi, "Application of Data Masking in Achieving Information Privacy," *IOSR Journal of Engineering,* vol. 4, pp. 13-21, 2014.

[47] C. Eyupoglu, M. A. Aydin, A. H. Zaim and A. Sertbas, "An efficient big data anonymization algorithm based on chaos and perturbation techniques," *Entropy,* vol. 20, 2018.

[48] L. Sweeney, "Achieving k-anonymity privacy protection using generalization and suppression," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems,* vol. 10, pp. 571-588, 2002.

[49] S. Hajian, J. Domingo-Ferrer and O. Farràs, "Generalization-based privacy preservation and discrimination prevention in data publishing and mining," *Data Mining and Knowledge Discovery,* vol. 28, pp. 1158-1188, 2014.

[50] V. Ciriani, S. D. Capitani di Vimercati, S. Foresti and P. Samarati, "κ-anonymity," in *Secure data management in decentralized systems*, Springer, 2007, pp. 323-353.

[51] J. F. Marques and J. Bernardino, "Analysis of Data Anonymization Techniques," in *KEOD*, 2020, pp. 235-241.

[52] K. Mivule, "Utilizing noise addition for data privacy, an overview," 2013.

[53] Z. El Ouazzani and H. El Bakkali, "A classification of non-cryptographic anonymization techniques ensuring privacy in big data," *International Journal of Communication Networks and Information Security,* vol. 12, pp. 142-152, 2020.

[54] T. Križan, M. Brakus and D. Vukelić, "In-situ anonymization of big data," in *2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, IEEE, 2015, pp. 292-298.

[55] K. Sharmila, S. B. A. Catherine and V. Sreeja, "A comprehensive Study of Data Masking Techniques on cloud," *International Journal of Pure and Applied Mathematics,* vol. 119, pp. 3719-3728, 2018.

[56] A. Majeed and S. Lee, "Anonymization techniques for privacy preserving data publishing: A comprehensive survey," *IEEE access,* vol. 9, pp. 8512-8545, 2020.

[57] EUROPEAN DATA PROTECTION SUPERVISOR, "Synthetic Data," [Online]. Available: https://edps.europa.eu/press-publications/publications/techsonar/synthetic-data_en. [Accessed 2022].

[58] F. Kohlmayer, F. Prasser, C. Eckert, A. Kemper and K. A. Kuhn, "Flash: efficient, stable and optimal k-anonymity," in *2012 International Conference on Privacy, Security, Risk and Trust and 2012 International Confernece on Social Computing*, IEEE, 2012, pp. 708-717.

[59] I. E. Olatunji, J. Rauch, M. Katzensteiner and M. Khosla, "A review of anonymization for healthcare data," *Big Data,* 2022.

[60] N. Li, T. Li and S. Venkatasubramanian, "t-closeness: Privacy beyond k-anonymity and l-diversity," in *2007 IEEE 23rd international conference on data engineering*, IEEE, 2007, pp. 106-115.

[61] C. C. Aggarwal and S. Y. Philip, Privacy-preserving data mining: models and algorithms, Springer Science & Business Media, 2008.

[62] R. Sobti and G. Geetha, "Cryptographic hash functions: a review," *International Journal of Computer Science Issues (IJCSI),* vol. 9, p. 461, 2012.

[63] «Tokenization (ασφάλεια δεδομένων),» [Ηλεκτρονικό]. Available: https://wikipredia.net/el/Tokenization_(data_security). [Πρόσβαση 2022].

[64] Β. Καλουδάς, «Υλοποίηση RBAC, με χρήση AzMan, σε περιβάλλον Windows,» 2013.

[65] C. Crane, "The Role of Access Control in Information Security," 2020. [Online]. Available: https://securityboulevard.com/2020/11/the-role-of-access-control-in-information-security/. [Accessed 2022].

[66] J. A. Martin, "What is access control? A key component of data security," 2019. [Online]. Available: https://www.csoonline.com/article/3251714/what-is-access-control-a-key-component-of-data-security.html. [Accessed 2022].

[67] J. Camenisch, A. Lehmann, G. Neven and A. Rial, "Privacy-preserving auditing for attribute-based credentials," in *European Symposium on Research in Computer Security*, 2014, pp. 109-127.

[68] G. Neven, G. Baldini, J. Camenisch and R. Neisse, "Privacy-preserving attribute-based credentials in cooperative intelligent transport systems," in *2017 IEEE Vehicular Networking Conference (VNC)*, 2017, pp. 131-138.

[69] J. Bobolz, F. Eidens, S. Krenn, S. Ramacher and K. Samelin, "Issuer-Hiding Attribute-Based Credentials," in *International Conference on Cryptology and Network Security*, 2021, pp. 158-178.

[70] C. Dilmegani, "Zero-Knowledge Proof: How it Works & Applications in 2022," 2022. [Online]. Available: https://research.aimultiple.com/zero-knowledge-proofs/. [Accessed 2022].

[71] "Zero Knowledge Proof," 2020. [Online]. Available: https://hackernoon.com/eli5-zero-knowledge-proof-78a276db9eff. [Accessed 2022].

[72] J. Kurm and A. Sodhi, "A Survey of Zero-Knowledge Proof for Authentication," *International Journal of Advanced Research in Computer Science and Software Engineering,* vol. 5, no. 1, 2015.

[73] A. Mohr, "A survey of zero-knowledge proofs with applications to cryptography," *Southern Illinois University, Carbondale,* pp. 1-12, 2007.

[74] F. Li and B. McMillin, "Chapter Two - A Survey on Zero-Knowledge Proofs," in *Advances in Computers*, vol. 94, 2014, pp. 25-69.

[75] V. Seničar, B. Jerman-Blažič and T. Klobučar, "Privacy-enhancing technologies—approaches and development," *Computer Standards & Interfaces,* vol. 25, no. 2, pp. 147-158, 2003.

[76] "P3P, The Platform for Privacy Preferences," [Online]. Available: http://www.tireme.fr/glossaire/SPEC-P3P.pdf. [Accessed 2022].

[77] L. Faith Cranor, "Platform for Privacy Preferences (P3P)," in *Encyclopedia of Cryptography and Security*, Boston, MA, Springer US, 2011, pp. 940-941.

[78] H. Debar, "Privacy-Enhancing Technologies," in *Security and Privacy in Advanced Networking Technologies*, 2004, pp. 224-226.

[79] A. Patrick and S. Kenny, "From Privacy Legislation to Interface Design: Implementing Information Privacy in Human-Computer Interactions," in *Privacy Enhancing Technologies*, 2003, pp. 107-124.

[80] J. J. Borking, "Privacy Incorporated Software Agent (PISA): Proposal for Building a Privacy Guardian for the Electronic Age," in *Designing Privacy Enhancing Technologies: International Workshop on Design Issues in Anonymity and Unobservability Berkeley, CA, USA, July 25--26, 2000 Proceedings*, Berlin, Heidelberg, Springer Berlin Heidelberg, 2001, pp. 130-140.