Κεφάλαιο 1ο

1. Εισαγωγή

1.1. Τι είναι η Ψευδωνυμοποίηση;

Η ψευδωνυμοποίηση (pseunonymity) είναι μια διαδικασία που χρησιμοποιείται για την προστασία δεδομένων προσωπικού χαρακτήρα (personal data) / αναγνωριστικά στοιχεία ταυτότητας (Personal Identifiable Information PII), κατά την οποία αντικαθίστανται οι ταυτοποιήσιμες πληροφορίες προσώπων με ψευδώνυμα (pseudonyms) [1]. Με αυτόν τον τρόπο διασφαλίζεται ότι τα άτομα δεν μπορούν να ταυτοποιηθούν άμεσα, παρά μόνο μέσω πρόσθετων πληροφοριών όταν χρειάζεται και ότι διασφαλίζεται η δυνατότητα χρήσιμης επεξεργασίας δεδομένων.

Τα πρότυπα ISO/IEC 20889:2018 και ISO/IEC 29100:2011/2024 παρέχουν κάποιους τεχνικούς ορισμούς που βοηθούν στην περαιτέρω κατανόηση της ψευδωνυμοποίησης. Συγκεκριμένα:

- Κατά το ISO/IEC 20889:2018, ψευδωνυμοποίηση είναι μια τεχνική απόταυτοποίησης (de-identification) που αντικαθιστά ένα αναγνωριστικό (ή αναγνωριστικά) ενός υποκειμένου των δεδομένων με ένα ψευδώνυμο, προκειμένου να αποκρύψει την ταυτότητα του εν λόγω υποκειμένου των δεδομένων.
- Κατά το ISO/IEC 29100:2011, ψευδωνυμοποίηση θεωρείται η αντικατάσταση δεδομένων από ψευδώνυμα στην περίπτωση όπου:
    - τα εναπομείναντα χαρακτηριστικά που συνδέονται με τα ψευδώνυμα δεν επαρκούν για να ταυτοποιήσουν το υποκείμενο δεδομένων, με το οποίο σχετίζονται,

- η διαδικασία απόδοσης ψευδώνυμου δεν μπορεί να αντιστραφεί με λογική προσπάθεια από άλλους δικαιούχους ιδιωτικότητας (privacy stakeholders).

Τα πρότυπα αυτά επισημαίνουν πως τα ψευδώνυμα μπορούν είτε να προκύπτουν από το προσωπικό αναγνωριστικό που χρησιμοποιείται συνήθως, με αναστρέψιμο ή μη αναστρέψιμο τρόπο, είτε να είναι εντελώς άσχετα. Επίσης, ότι για την επαναταυτοποίηση είναι απαραίτητη η διατήρηση μιας συσχέτισης μεταξύ των προσωπικών αναγνωριστικών και των ψευδωνύμων σε κατάλληλα εξουσιοδοτημένα άτομα στον οργανισμό. Αυτή θα πρέπει να είναι ασφαλής και όχι προφανής σε όποιον έχει πρόσβαση στα ψευδωνυμοποιημένα δεδομένα, ώστε να διατηρηθεί ένα ικανοποιητικό επίπεδο ασφάλειας.

Παράλληλα, σύμφωνα με το Άρθρο 4(5) του Γενικού Κανονισμού Προστασίας Δεδομένων – ΓΚΠΔ (General Data Protection Regulation – GDPR), ψευδωνυμοποίηση είναι η επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο ώστε τα δεδομένα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρωματικές πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλιστεί ότι τα δεδομένα δεν μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο.

Ο ΓΚΠΔ τονίζει ότι τα ψευδωνυμοποιημένα δεδομένα δε θα πρέπει να επιτρέπουν την άμεση ή έμμεση ταυτοποίηση υποκειμένων των δεδομένων χωρίς τ χρήση πρόσθετων πληροφοριών. Αυτές οι «πρόσθετες πληροφορίες», παραπέμπουν στη συσχέτιση μεταξύ των αρχικών αναγνωριστικών του υποκειμένου των δεδομένων και των ψευδωνύμων. Επίσης, διευκρινίζεται ότι θα πρέπει να προστατεύονται κατάλληλα – επιπλέον των άμεσων - και τα έμμεσα αναγνωριστικά που αφορούν ένα υποκείμενο των δεδομένων.

1.2. Διαφορές με Ανωνυμοποίηση

1.2.1. Ορισμός Ανωνυμοποίησης

Η ανωνυμοποίηση (anonymisation) είναι μια διαδικασία που χρησιμοποιείται για την προστασία δεδομένων προσωπικού χαρακτήρα, κατά την οποία αφαιρούνται οι ταυτοποιήσιμες πληροφορίες προσώπων [1]. Με αυτόν τον τρόπο, τα δεδομένα καθίστανται ανώνυμα, διασφαλίζοντας ότι τα πρόσωπα που περιγράφουν

δεν μπορούν να αναγνωριστούν, ούτε άμεσα ούτε έμμεσα, με οποιονδήποτε τρόπο.

Σύμφωνα με το ISO/TS 25237:2017, ανωνυμοποίηση είναι μια διαδικασία με την οποία τα δεδομένα προσωπικού χαρακτήρα τροποποιούνται αμετάκλητα με τρόπο που ένα υποκείμενο δεδομένων δεν μπορεί πλέον να αναγνωριστεί άμεσα ή έμμεσα, είτε από τον ίδιο τον υπεύθυνο επεξεργασίας είτε σε συνεργασία με οποιοδήποτε άλλο μέρος.

Παράλληλα, σύμφωνα με τον ΓΚΠΔ, ανωνυμοποίηση είναι η διαδικασία με την οποία τα δεδομένα προσωπικού χαρακτήρα καθίστανται ανώνυμα. Συγκεκριμένα η Αιτιολογική Σκέψη (26) δηλώνει, ότι τα ανώνυμα δεδομένα (anonymous data) είναι πληροφορίες που δε σχετίζονται με κάποιο ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο.

Μια συχνή εσφαλμένη εντύπωση είναι ότι απλά και μόνο με την αφαίρεση των άμεσων αναγνωριστικών (όπως ονομάτων, διευθύνσεων, αριθμών κοινωνικής ασφάλισης κ.λπ.) ενός συνόλου δεδομένων είναι επαρκής για την ανωνυμοποίηση ενός συνόλου δεδομένων. Ωστόσο, η διαδικασία αυτή από μόνη της δεν εγγυάται την ανωνυμία. Ενώ η αφαίρεση των αναγνωριστικών αποτελεί προϋπόθεση για την ανωνυμοποίηση, συχνά αποτυγχάνει να προστατεύσει πλήρως τα πρόσωπα από επαναταυτοποίηση. Για να επιτευχθεί πραγματική ανωνυμοποίηση, απαιτούνται συνήθως πιο περίπλοκες τεχνικές, όπως η τυχαιοποίηση και η γενίκευση.

1.2.2. Διαφορά Ψευδωνυμοποίησης και Ανωνυμοποίησης

Η ψευδωνυμοποίηση και η ανωνυμοποίηση συχνά συγχέονται, με μια συχνή παρεξήγηση να είναι η αντιμετώπιση των ψευδωνυμοποιημένων δεδομένων ως ανώνυμων. Όμως, όπως φαίνεται και από τους παραπάνω ορισμούς, η ψευδωνυμοποίηση προϋποθέτει την ύπαρξη συσχέτισης μεταξύ προσωπικών αναγνωριστικών και ψευδωνύμων, ενώ στην ανωνυμοποίηση δε πρέπει να υπάρχει πλέον καμία τέτοια συσχέτιση.

Συνεπώς, δεδομένου ότι η ψευδωνυμοποίηση επιτρέπει την επαναταυτοποίηση ατόμων, τα ψευδωνυμοποιημένα δεδομένα εξακολουθούν να θεωρούνται δεδομένα προσωπικού χαρακτήρα, σε αντίθεση με τα ανωνυμοποιημένα. Αυτό συνεπάγεται ότι τα ψευδωνυμοποιημένα δεδομένα υπόκεινται στους κανονισμούς του ΓΚΠΔ, ενώ τα ανωνυμοποιημένα όχι.

1.3. Βιβλιογραφικές Αναφορές

[1] ENISA, "Recommendations on shaping technology according to GDPR provisions" διαθέσιμο στο https://op.europa.eu/en/publication-detail/-/publication/0e1ca64f-29c7-11e9-8d04-01aa75ed71a1/language-en (2018)

2. Βασικά Στοιχεία Ψευδωνυμοποίησης

2.1. Ορολογία

Δεδομένα προσωπικού χαρακτήρα (Personal data): κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («**υποκείμενο των δεδομένων (data subject)**»)· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου (ΓΚΠΔ, άρθρο 4(1)),

Υπεύθυνος επεξεργασίας (Data controller): το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα· όταν οι σκοποί και ο τρόπος της επεξεργασίας αυτής καθορίζονται από το δίκαιο της Ευρωπαϊκής Ένωσης (ΕΕ) ή το δίκαιο κράτους μέλους της ΕΕ, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια για τον διορισμό του μπορούν να προβλέπονται από το δίκαιο της ΕΕ ή το δίκαιο κράτους μέλους (ΓΚΠΔ, άρθρο 4(7)),

Εκτελών την επεξεργασία (Data processor): το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας (ΓΚΠΔ, άρθρο 4(8)),

Αναγνωριστικό (Identifier *Id*) [1]: μια τιμή που προσδιορίζει ένα στοιχείο σε ένα σύστημα ταυτοποίησης. Ένα μοναδικό αναγνωριστικό συνδέεται με ένα μόνο στοιχείο.

Ψευδώνυμο (επίσης γνωστό ως κρυπτώνυμο) **(Pseudonym)** [1]: μια πληροφορία που σχετίζεται με ένα αναγνωριστικό ενός ατόμου ή με οποιοδήποτε άλλο είδος δεδομένων προσωπικού χαρακτήρα (π.χ. δεδομένα θέσης). Τα ψευδώνυμα μπορεί να έχουν διαφορετικούς βαθμούς συνδεσιμότητας (με τα αρχικά αναγνωριστικά). Ο βαθμός συνδεσιμότητας των διαφόρων τύπων ψευδωνύμων είναι σημαντικός και πρέπει να εξετάζεται για την αξιολόγηση της ισχύος των ψευδωνύμων, αλλά και για τον σχεδιασμό ψευδώνυμων συστημάτων (pseudonymous systems) όπου μπορεί να είναι επιθυμητός ένας ορισμένος βαθμός συνδεσιμότητας (π.χ. κατά την ανάλυση ψευδώνυμων αρχείων καταγραφής (pseudonymous log files) ή για συστήματα φήμης (reputation systems)).

Συνάρτηση ψευδωνυμοποίησης (συμβολίζεται με *P*) **(Pseudonymisation function)** [1]: μια συνάρτηση που αντικαθιστά ένα αναγνωριστικό *Id* με ένα ψευδώνυμο *pseudonym*.

Μυστικό ψευδωνυμοποίησης (συμβολίζεται με *s*) **(Pseudonymisation secret)** [1]: μια (προαιρετική) παράμετρος μιας συνάρτησης ψευδωνυμοποίησης *P*. Η συνάρτηση *P* δεν μπορεί να εκτιμηθεί/υπολογιστεί εάν το *s* είναι άγνωστο.

Συνάρτηση επαναφοράς (συμβολίζεται με *R*) **(Recovery function)** [1]: μια συνάρτηση που αντικαθιστά ένα ψευδώνυμο *pseudo* με το αναγνωριστικό *Id* χρησιμοποιώντας το μυστικό ψευδωνυμοποίησης *s*. Ουσιαστικά, αντιστρέφει τη συνάρτηση ψευδωνυμοποίησης *P*.

Πίνακας αντιστοίχισης ψευδωνυμοποίησης (Pseudonymisation mapping table) [1]: μια αναπαράσταση της ενέργειας της συνάρτησης ψευδωνυμοποίησης. Συνδέει κάθε αναγνωριστικό με το αντίστοιχο ψευδώνυμο. Ανάλογα με τη συνάρτηση ψευδωνυμοποίησης *P*, ο πίνακας αντιστοίχισης ψευδωνυμοποίησης μπορεί να είναι το μυστικό ψευδωνυμοποίησης ή μέρος αυτού.

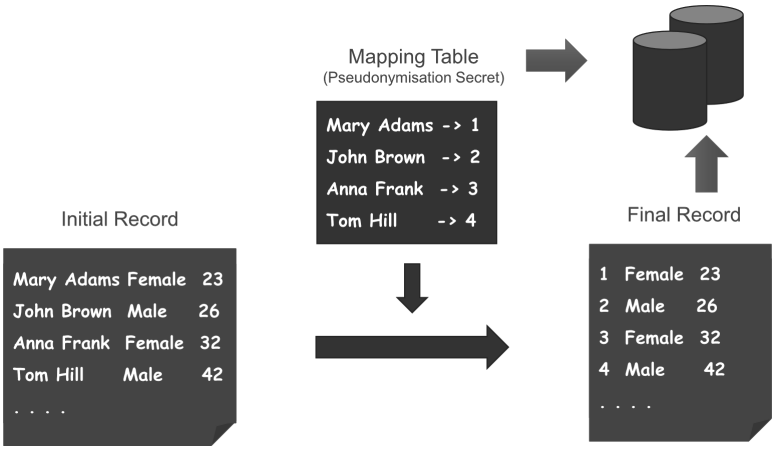
Οντότητα ψευδωνυμοποίησης (Pseudonymisation entity) [1]: είναι η οντότητα που είναι υπεύθυνη για τη μετατροπή των αναγνωριστικών σε ψευδώνυμα χρησιμοποιώντας τη συνάρτηση ψευδωνυμοποίησης. Μπορεί να είναι ένας υπεύθυνος επεξεργασίας δεδομένων, ένας εκτελών την επεξεργασία δεδομένων που εκτελεί ψευδωνυμοποίηση για λογαριασμό ενός υπεύθυνου επεξεργασίας, ένα έμπιστο τρίτο μέρος ή ένα υποκείμενο των δεδομένων, ανάλογα με το σενάριο ψευδωνυμοποίησης.

Επιτιθέμενος (Adversary) [1]: μια οντότητα που προσπαθεί να παραβιάσει την ψευδωνυμοποίηση και να συνδέσει ένα ψευδώνυμο ή ένα ψευδωνυμοποιημένο σύνολο δεδομένων με τον κάτοχο ή τους κατόχους του ψευδωνύμου.

2.2. Βασική Ψευδωνυμοποίηση

Παρακάτω φαίνεται η βασική μορφή ψευδωνυμοποίησης, κατά την οποία αντικαθίστανται τα δεδομένα προσωπικού χαρακτήρα των προσώπων με άμεσα αναγνωριστικά (ψευδώνυμα). Συγκεκριμένα:

- Το αρχικό αρχείο (Initial Record): είναι το αρχικό σύνολο δεδομένων που περιέχει δεδομένα προσωπικού χαρακτήρα, όπως όνομα, φύλο και άλλα δεδομένα (π.χ. ηλικία).
- Ο πίνακας αντιστοίχισης (μυστικό ψευδωνυμοποίησης) (Mapping Table (Pseudonymisation Secret)) δημιουργείται για την καταγραφή της απόδοσης των αναγνωριστικών (π.χ. 1, 2, 3) σε κάθε υποκείμενο δεδομένων που υπάρχει στις αρχικές εγγραφές. Δηλαδή, λειτουργεί ως κλειδί για τη σύνδεση των ψευδωνυμοποιημένων δεδομένων με τα αρχικά δεδομένα και διατηρείται ασφαλής και χωριστά.
- Το τελικό αρχείο (Final Record) είναι το ψευδωνυμοποιημένο σύνολο δεδομένων που προκύπτει από την αντικατάσταση των δεδομένων προσωπικού χαρακτήρα (π.χ. ονομάτων) με τα μοναδικά ψευδώνυμα (π.χ. 1, 2, 3). Έτσι, διασφαλίζεται ότι τα άτομα δεν είναι άμεσα αναγνωρίσιμα, ενώ διατηρείται η χρηστικότητα των δεδομένων, π.χ. για ανάλυση ή άλλους σκοπούς επεξεργασίας.



Εικόνα 1

2.3. Πλεονεκτήματα και Στόχοι Ψευδωνυμοποίησης

Η ψευδωνυμοποίηση είναι μια ισχυρή τεχνική προστασίας δεδομένων που έχει σχεδιαστεί για την ενίσχυση της ιδιωτικότητας, ενώ παράλληλα συμβάλλει στη συμμόρφωση με νομικά και κανονιστικά πλαίσια, όπως ο ΓΚΠΔ. Οι στόχοι και τα πλεονεκτήματά της είναι πολλά [1] [2] [3], καλύπτοντας τόσο τις ανάγκες των υπευθύνων επεξεργασίας και των εκτελούντων την επεξεργασία, όσο και τα δικαιώματα των υποκειμένων των δεδομένων. Ακολούθως παρατίθενται οι βασικοί στόχοι και τα πλεονεκτήματα της ψευδωνυμοποίησης:

Στόχοι της ψευδωνυμοποίησης:

- Προστασία της ταυτότητας του υποκειμένου των δεδομένων: Ο βασικός στόχος της ψευδωνυμοποίησης είναι να αποτραπεί η αποκάλυψη των άμεσων αναγνωριστικών των υποκειμένων των δεδομένων. Με την αντικατάσταση των αναγνωριστικών με ψευδώνυμα, η ταυτότητα των υποκειμένων των δεδομένων παραμένει κρυφή, ιδίως από τρίτους, ενώ παράλληλα επιτρέπει την αξιοποίηση των δεδομένων για νόμιμους σκοπούς.
- Μετριασμός των κινδύνων σε περίπτωση μη εξουσιοδοτημένης πρόσβασης: Σε περίπτωση παραβίασης δεδομένων (data breach) ή μη εξουσιοδοτημένης πρόσβασης (unauthorized access), η ψευδωνυμοποίηση μειώνει σημαντικά τους κινδύνους παραβίασης της εμπιστευτικότητας. Δεδομένου ότι η συσχέτιση των αρχικών και των ψευδωνυμοποιημένων δεδομένων (ή άλλες πρόσθετες πληροφορίες) προστατεύεται και διατηρείται χωριστά από τα ψευδωνυμοποιημένα δεδομένα, τα εκτεθειμένα δεδομένα δεν μπορούν εύκολα να αποκαλύψουν τα υποκείμενα των δεδομένων.
- Προστασία δεδομένων από τον σχεδιασμό (Data protection by design): Ένας άλλος βασικός στόχος της ψευδωνυμοποίησης είναι να δώσει τη δυνατότητα στους υπευθύνους επεξεργασίας να επιτύχουν τους σκοπούς της επεξεργασίας τους χρησιμοποιώντας τα ελάχιστα δεδομένα προσωπικού χαρακτήρα που απαιτούνται για αυτή (π.χ. χωρίς να γνωρίζουν τις πραγματικές ταυτότητες των υποκειμένων των δεδομένων).

Πλεονεκτήματα της ψευδωνυμοποίησης:

- Απόκρυψη ταυτοτήτων των υποκειμένων: Όπως φαίνεται και από τους στόχους της ψευδωνυμοποίησης, ένα από τα κύρια πλεονεκτήματά της είναι η προστασία της ταυτότητας των υποκειμένων των δεδομένων. Διατηρώντας

ασφαλή και χωριστά τις πρόσθετες πληροφορίες από τα ψευδωνυμοποιημένα δεδομένα, μειώνεται σημαντικά ο κίνδυνος μη εξουσιοδοτημένης επαναταυτοποίησης των υποκειμένων των δεδομένων.

- Μη συνδεσιμότητα (unlinkability): Η ψευδωνυμοποίηση ενισχύει τη μη συνδεσιμότητα, δηλαδή μειώνει τον κίνδυνο σύνδεσης δεδομένων προσωπικού χαρακτήρα μεταξύ διαφορετικών τομέων (domains) επεξεργασίας δεδομένων. Αυτό είναι αποτέλεσμα της δυσκολίας που έχει η σύνδεση ψευδωνυμοποιημένων δεδομένων με άλλα δεδομένα προσωπικού χαρακτήρα, που ενδέχεται να αφορούν το ίδιο υποκείμενο δεδομένων, χωρίς τη χρήση πρόσθετων πληροφοριών. Η μη συνδεσιμότητα σχετίζεται με τις βασικές αρχές της προστασίας δεδομένων, της αναγκαιότητας και της ελαχιστοποίησης των δεδομένων (necessity and data minimisation).
- Ακρίβεια δεδομένων (data accuracy): Διαχωρίζοντας το αρχικό σύνολο δεδομένων σε ψευδωνυμοποιημένα δεδομένα και πρόσθετες πληροφορίες, διασφαλίζεται η ακεραιότητά (integrity) του, καθώς μπορεί να ανακατασκευαστεί μόνο με τη χρήση αμφοτέρων των συνιστωσών. Έτσι ενισχύεται η αξιοπιστία των δεδομένων και ικανοποιείται η αρχή της ακρίβειας (principle of accuracy).

2.4. Απαιτήσεις Ασφάλειας που Ικανοποιεί η Ψευδωνυμοποίηση

Η ψευδωνυμοποίηση είναι μια πολύ χρήσιμη τεχνική που συμβάλλει στην ικανοποίηση πολλών απαιτήσεων (requirements) προστασίας δεδομένων του ΓΚΠΔ [3].

Καταρχάς, η ψευδωνυμοποίηση μπορεί να χρησιμοποιηθεί για την ικανοποίηση της αρχής της ελαχιστοποίησης δεδομένων (data minimisation), επιτρέποντας ακόμη και στους υπευθύνους επεξεργασίας να επεξεργάζονται δεδομένα χωρίς να επαναταυτοποιούν άτομα, παρά μόνο εάν και όποτε είναι απολύτως απαραίτητο. Παράλληλα, ενισχύεται η εμπιστευτικότητα (confidentiality), διασφαλίζοντας ότι τα ψευδωνυμοποιημένα δεδομένα δεν μπορούν εύκολα να συνδεθούν με τα υποκείμενα των δεδομένων χωρίς πρόσθετες πληροφορίες που διατηρούνται χωριστά και προστατεύονται δεόντως.

Μια άλλη αρχή που ικανοποιείται, είναι ο περιορισμός του σκοπού (purpose limitation), καθώς η ψευδωνυμοποίηση περιορίζει τη χρήση των δεδομένων σε συγκριμένους σκοπούς, γεγονός που είναι ιδιαίτερα χρήσιμο κατά την κοινοποί-

ηση δεδομένων σε εξωτερικούς παραλήπτες. Έτσι, αποτρέπεται η μη εξουσιοδοτημένη σύνδεση δεδομένων, η χρήση δεδομένων για μη συμφωνημένους σκοπούς και η μη εξουσιοδοτημένη επεξεργασία γενικότερα.

Επιπλέον, η ψευδωνυμοποίηση μπορεί να επιβάλλεται για συγκεκριμένους τύπους δεδομένων, είτε από ευρωπαϊκούς είτε από εθνικούς νόμους, για να είναι νόμιμη η επεξεργασία των δεδομένων (αρχή νομιμότητας (lawfulness)). Οι νόμοι αυτοί αποβλέπουν στη μείωση των κινδύνων για τα δικαιώματα των υποκειμένων των δεδομένων και των πιθανών συνεπειών της επιδιωκόμενης περαιτέρω επεξεργασίας (Άρθρο 6(4), ΓΚΠΔ).

Οι αρχές της δικαιοσύνης (fairness) και της ακρίβειας (accuracy), επίσης ενισχύονται με την ψευδωνυμοποίηση. Συγκεκριμένα, όσον αφορά τη δικαιοσύνη, η ψευδωνυμοποίηση συμβάλλει στην προστασία της ταυτότητας των ατόμων επιτρέποντας ταυτόχρονα την απαραίτητη επεξεργασία δεδομένων με διαφανή τρόπο. Ενώ όσον αφορά την ακρίβεια, μειώνει τον κίνδυνο σφαλμάτων, όπως η εσφαλμένη απόδοση πληροφοριών, διασφαλίζοντας ότι τα δεδομένα παραμένουν αξιόπιστα και σωστά ανατεθειμένα.

Σύμφωνα με το Άρθρο 32(1) του ΓΚΠΔ, η ψευδωνυμοποίηση μπορεί να χρησιμοποιηθεί για τη διασφάλιση ενός επιπέδου ασφαλείας ανάλογου με τον κίνδυνο της δραστηριότητας επεξεργασίας δεδομένων. Ακόμη και μετά την ψευδωνυμοποίηση πρέπει να διατηρείται ένα κατάλληλο επίπεδο ασφάλειας ανάλογο των εναπομεινάντων κινδύνων (residual risks) που ενέχει η επεξεργασία των ψευδωνυμοποιημένων δεδομένων. Ειδικά οι εκτελούντες την επεξεργασία, σύμφωνα με το Άρθρο 28(1) του ΓΚΠΔ, πρέπει να είναι σε θέση να αποδείξουν ότι τηρούνται τα κατάλληλα τεχνικά και οργανωτικά μέτρα για τη διασφάλιση αυτού του επιπέδου ασφάλειας.

Μια εύρωστη εφαρμογή ψευδωνυμοποίησης μπορεί να μειώσει σημαντικά τον αντίκτυπο παραβιάσεων δεδομένων, οπότε πρέπει να εξεταστεί κατά τον καθορισμό των υποχρεώσεων του υπεύθυνου επεξεργασίας σύμφωνα με τα Άρθρα 33 και 34 του ΓΚΠΔ. Δηλαδή, μπορεί να χρησιμεύσει ως τεχνικό και οργανωτικό μέτρο που περιορίζει τις συνέπειες μιας παραβίασης σύμφωνα με το Άρθρο 34(3)(α) του ΓΚΠΔ. Ωστόσο, σε περίπτωση παραβίασης – ή γενικότερα μη εξουσιοδοτημένης πρόσβασης στα δεδομένα αυτά – να εξεταστεί κατά πόσον η μείωση του κιν-

δύνου είναι επαρκής για να αποφευχθεί η ειδοποίηση των επηρεαζόμενων υποκειμένων των δεδομένων σύμφωνα με το Άρθρο 34(1) και (2) του ΓΚΠΔ.

Η ψευδωνυμοποίηση μπορεί να αποτελέσει συμπληρωματικό μέτρο για την ικανοποίηση των απαιτήσεων του ΓΚΠΔ σχετικά με τη διαβίβαση δεδομένων σε τρίτες χώρες, που διατυπώνονται στα Άρθρα 44 και 46(1). Έτσι διασφαλίζεται ότι ακόμη και δημόσιες αρχές στη δικαιοδοσία του εκάστοτε παραλήπτη δεν μπορούν να αποδώσουν τα ψευδωνυμοποιημένα δεδομένα σε συγκεκριμένα άτομα με λογική προσπάθεια. Βέβαια αυτό ισχύει με την προϋπόθεση ότι οι πρόσθετες πληροφορίες που απαιτούνται για την επαναταυτοποίηση προστατεύονται αναλόγως και από αυστηρά συμβατικά και τεχνικά αντίμετρα. Με τον ίδιο τρόπο, μπορεί να αποτελέσει κατάλληλο μέτρο προστασίας σύμφωνα με το Άρθρο 49(1) του ΓΚΠΔ, το οποίο επιτρέπει διαβιβάσεις δεδομένων εάν ο κίνδυνος για τα υποκείμενα των δεδομένων μειώνεται επαρκώς και πληρούνται οι υπόλοιπες απαιτήσεις της διάταξης.

2.5. Πολιτικές Ψευδωνυμοποίησης

Η εφαρμογή της ψευδωνυμοποίησης δεν εξαρτάται μόνο από την τεχνική που επιλέγεται, αλλά και από την πολιτική ή τον συγκεκριμένο τρόπο ψευδωνυμοποίησης [1]. Η πολιτική καθορίζει τον τρόπο με τον οποίο αντικαθίστανται τα αναγνωριστικά στοιχεία με ψευδώνυμα σε όλα τα σύνολα δεδομένων, επηρεάζοντας την ισορροπία μεταξύ της χρηστικότητας των δεδομένων, της ιδιωτικότητας και της συνέπειας.

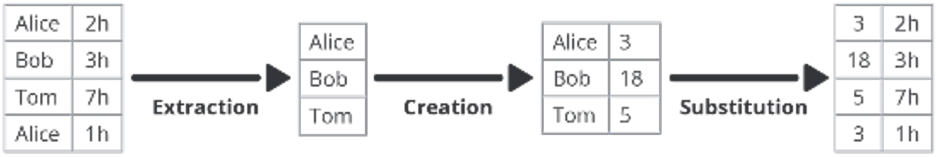
Η ενότητα αυτή παρουσιάζει τις πολιτικές ψευδωνυμοποίησης που εφαρμόζονται σε μια βάση δεδομένων ή ένα έγγραφο που περιέχει k αναγνωριστικά. Αν ένα αναγνωριστικό Id εμφανίζεται πολλές φορές στα σύνολα δεδομένων A και B, μπορεί να ψευδωνυμοποιηθεί χρησιμοποιώντας μία από τις ακόλουθες πολιτικές:

- Αιτιοκρατική ψευδωνυμοποίηση (Deterministic pseudonymisation)
- Τυχαιοποιημένη με τεκμηρίωση ψευδωνυμοποίηση (Document-randomized pseudonymisation)
- Πλήρως τυχαιοποιημένη ψευδωνυμοποίηση (Fully-randomized pseudonymisation)

2.5.1. Αιτιοκρατική Ψευδωνυμοποίηση (Deterministic Pseudonymisation)

Η αιτιοκρατική ψευδωνυμοποίηση [1] ορίζει ότι το αναγνωριστικό *Id* αντικαθίσταται με το ίδιο ψευδώνυμο *pseudo* κάθε φορά που εμφανίζεται σε μία ή περισσότερες βάσεις δεδομένων.

Για την εφαρμογή αυτής της πολιτικής, πρέπει αρχικά να εξαχθεί η λίστα των μοναδικών αναγνωριστικών που υπάρχουν στη βάση δεδομένων. Έπειτα, η λίστα αυτή αντιστοιχίζεται στα ψευδώνυμα και ακολούθως τα αναγνωριστικά αυτά αντικαθίστανται στη βάση με τις τιμές των ψευδωνύμων.

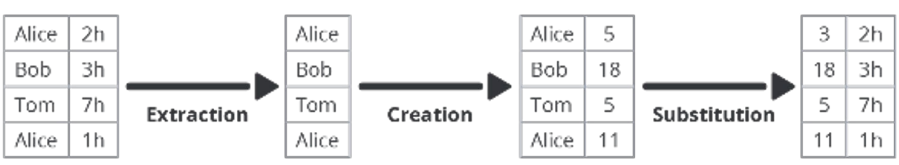


Εικόνα 1: *Αιτιοκρατική ψευδωνυμοποίηση (πηγή: [1])*

2.5.2. Τυχαιοποιημένη με Τεκμηρίωση Ψευδωνυμοποίηση (Document-randomized Pseudonymisation)

Η τυχαιοποιημένη με τεκμηρίωση ψευδωνυμοποίηση [1] ορίζει ότι το αναγνωριστικό *Id* αντικαθίσταται με διαφορετικό ψευδώνυμο ($pseudo_1$, $pseudo_2$,...) κάθε φορά που εμφανίζεται σε μία βάση δεδομένων. Ωστόσο, το *Id* αντιστοιχίζεται στην ίδια συλλογή ψευδωνύμων ($pseudo_1$, $pseudo_2$,...) μεταξύ διαφορετικών συνόλων δεδομένων (π.χ. συνόλων δεδομένων *A* και *B*).

Για την εφαρμογή αυτής της πολιτικής, κάθε αναγνωριστικό αντιμετωπίζεται ανεξάρτητα. Επομένως, ο πίνακας αντιστοίχισης δημιουργείται χρησιμοποιώντας όλα τα αναγνωριστικά που περιέχονται στην βάση δεδομένων.



Εικόνα 2: *Τυχαιοποιημένη με τεκμηρίωση ψευδωνυμοποίηση (πηγή: [1])*

2.5.3. Πλήρως Τυχαιοποιημένη Ψευδωνυμοποίηση (Fully-randomized Pseudonymisation)

Η πλήρως τυχαιοποιημένη ψευδωνυμοποίηση [1] ορίζει ότι το αναγνωριστικό *Id* αντικαθίσταται με διαφορετικό ψευδώνυμο ($pseudo_1$, $pseudo_2$,...) κάθε φορά που εμφανίζεται, δηλαδή ακόμη και εντός του ίδιου συνόλου δεδομένων.

Για την εφαρμογή αυτής της πολιτικής, κάθε αναγνωριστικό αντικαθίσταται από ένα διαφορετικό ψευδώνυμο.

Η διαφορά μεταξύ της τυχαιοποιημένης με τεκμηρίωση ψευδωνυμοποίησης και της πλήρως τυχαιοποιημένης ψευδωνυμοποίησης φαίνεται αν ένα έγγραφο ψευδωνυμοποιηθεί παραπάνω από μία φορά. Συγκεκριμένα, με την τυχαιοποιημένη με τεκμηρίωση ψευδωνυμοποίηση, το ίδιο έγγραφο θα παράγει πάντα το ίδιο αποτέλεσμα, ενώ η πλήρως τυχαιοποιημένη ψευδωνυμοποίηση παράγει εντελώς νέα ψευδώνυμα κάθε φορά, δηλαδή διαφορετικά αποτελέσματα για το ίδιο έγγραφο. Συνεπώς, η τυχαιοποιημένη με τεκμηρίωση ψευδωνυμοποίηση διατηρεί κάποια συνέπεια, ενώ η πλήρως τυχαιοποιημένη ψευδωνυμοποίηση δίνει έμφαση στο μέγιστο επίπεδο ιδιωτικότητας και καταργεί εντελώς τη συνέπεια.

2.6. Βιβλιογραφικές Αναφορές

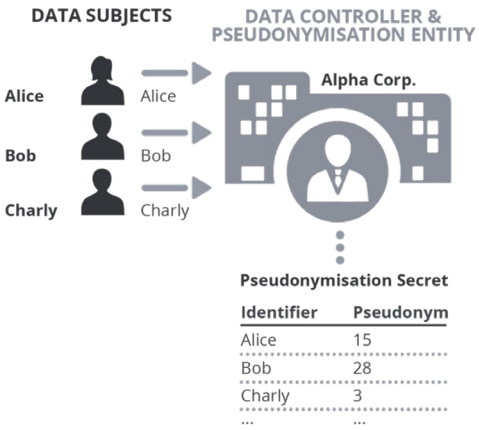
[1] ENISA, “Pseudonymisation techniques and best practices” διαθέσιμο στο https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices (2019)

[2] ENISA, “Recommendations on shaping technology according to GDPR provisions” διαθέσιμο στο https://op.europa.eu/en/publication-detail/-/publication/0e1ca64f-29c7-11e9-8d04-01aa75ed71a1/language-en (2018)

[3] EDPB, “Guidelines 01/2025 on Pseudonymisation” διαθέσιμο στο https://www.edpb.europa.eu/system/files/2025-01/edpb_guidelines_202501_pseudonymisation_en.pdf (2025)

3. Σενάρια

Σε αυτό το κεφάλαιο παρουσιάζονται τα βασικά σενάρια ψευδωνυμοποίησης [1] που μπορούν να συναντηθούν στην πράξη, περιγράφοντας τους βασικούς εμπλεκόμενους φορείς και τους στόχους της ψευδωνυμοποίησης σε κάθε περίπτωση. Οι



διαφορές μεταξύ των σεναρίων αφορούν τον φορέα που αναλαμβάνει τον ρόλο της οντότητας ψευδωνυμοποίησης (pseudonymisation entity) και τους άλλους πιθανούς φορείς που ενδέχεται να συμμετέχουν, καθώς και τους ρόλους τους.

3.1. Σενάριο Ψευδωνυμοποίησης 1

Ένα σύνηθες σενάριο ψευδωνυμοποίησης αποτελεί η συλλογή δεδομένων απευθείας από τα υποκείμενα των δεδομένων και η ψευδωνυμοποίησή τους από τον υπεύθυνο επεξεργασίας πριν χρησιμοποιηθούν για εσωτερική επεξεργασία [1].

Όπως φαίνεται στην Εικόνα 4, ο υπεύθυνος επεξεργασίας (Alpha Corp.) ενεργεί ως οντότητα ψευδωνυμοποίησης που συλλέγει τα δεδομένα των υποκειμένων και επιλέγει και αποδίδει ψευδώνυμα στα αναγνωριστικά. Αξίζει να σημειωθεί, ότι τα υποκείμενα των δεδομένων δεν γνωρίζουν απαραίτητα τα ψευδώνυμα που τους αποδίδονται, καθώς το μυστικό ψευδωνυμοποίησης (π.χ. ο πίνακας αντιστοίχισης στο παρόν παράδειγμα) είναι γνωστό μόνο στην Alpha Corp.

Ο βασικός σκοπός της ψευδωνυμοποίησης σε αυτό το σενάριο είναι η ενίσχυση της ασφάλειας των δεδομένων προσωπικού χαρακτήρα, είτε για εσωτερική χρήση (π.χ. κοινολόγηση μεταξύ διαφορετικών τμημάτων του υπεύθυνου επεξεργασίας) είτε ως μέτρο προστασίας σε περίπτωση συμβάντος ασφαλείας.

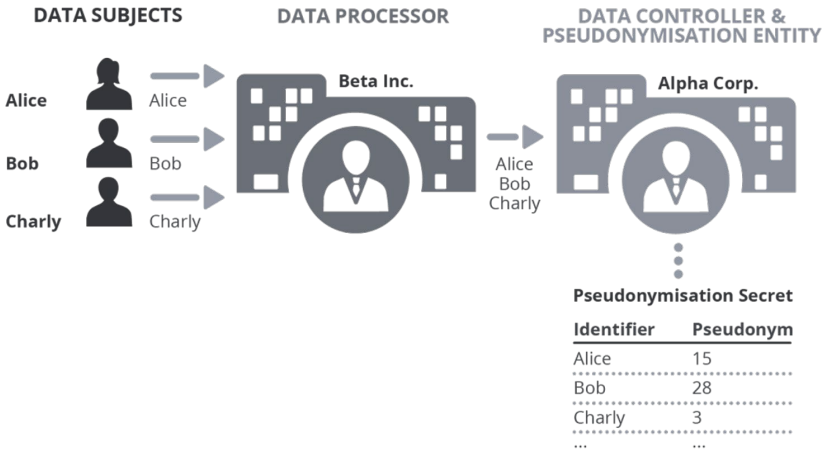
Εικόνα 3: *Σενάριο ψευδωνυμοποίησης 1 (πηγή: [1])*

3.2. Σενάριο Ψευδωνυμοποίησης 2

Μια παραλλαγή του παραπάνω σεναρίου αποτελεί η συλλογή των αναγνωριστικών των υποκειμένων των δεδομένων από έναν εκτελούντα την επεξεργασία εκ μέρους του υπεύθυνου επεξεργασίας, καθώς η ψευδωνυμοποίηση εξακολουθεί να πραγματοποιείται από τον υπεύθυνο επεξεργασίας πριν από οποιαδήποτε περαιτέρω επεξεργασία [1].

Όπως φαίνεται στην Εικόνα 5, ο εκτελών την επεξεργασία (Beta Inc.) είναι υπεύθυνος για τη συλλογή αναγνωριστικών από τα υποκείμενα των δεδομένων και την προώθησή τους στον υπεύθυνο επεξεργασίας (Alpha Corp.), ο οποίος στη συνέχεια πραγματοποιεί την ψευδωνυμοποίηση, δηλαδή ενεργεί ως οντότητα ψευδωνυμοποίησης.

Ο σκοπός της ψευδωνυμοποίησης σε αυτό το σενάριο παραμένει ο ίδιος με του σεναρίου ψευδωνυμοποίησης 1, με τη διαφορά ότι σε αυτή την περίπτωση, στη διαδικασία συμμετέχει διαμεσολαβώντας και ένας εκτελών την επεξεργασία.



Εικόνα 4: *Σενάριο ψευδωνυμοποίησης 2 (πηγή: [1])*

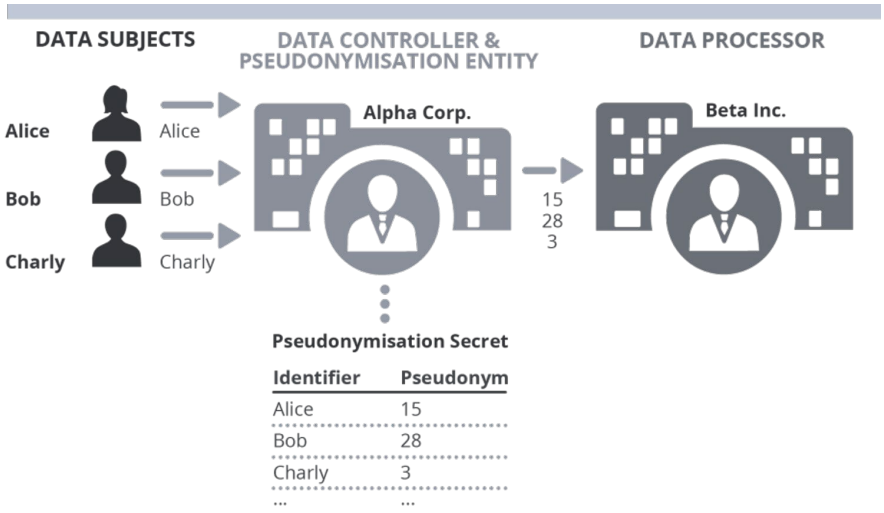
3.3. Σενάριο ψευδωνυμοποίησης 3

Ένα σενάριο ψευδωνυμοποίησης που έρχεται σε αντίθεση με το προηγούμενο, αποτελεί η συλλογή δεδομένων των υποκειμένων δεδομένων από τον υπεύθυνο επεξεργασίας, η ψευδωνυμοποίησή τους και έπειτα η κοινοποίηση των δεδομένων αυτών σε έναν εκτελούντα την επεξεργασία για περαιτέρω επεξεργασία [1].

Όπως φαίνεται στην Εικόνα 6, ο υπεύθυνος επεξεργασίας (Alpha Corp.) συλλέγει τα δεδομένα των υποκειμένων και πραγματοποιεί την ψευδωνυμοποίηση, δηλαδή ενεργεί ως οντότητα ψευδωνυμοποίησης, πριν καν προωθήσει τα ψευδωνυμοποιημένα δεδομένα σε έναν εκτελούντα την επεξεργασία (Beta Inc.). Σε αντίθεση με τα προηγούμενα σενάρια, ο εκτελών την επεξεργασία δε συμμετέχει στη διαδικασία ψευδωνυμοποίησης, αλλά μόνο λαμβάνει και επεξεργάζεται τα ψευδωνυμοποιημένα δεδομένα, όπως για στατιστική ανάλυση ή μακροχρόνια αποθήκευση.

Ο βασικός σκοπός της ψευδωνυμοποίησης σε αυτό το σενάριο είναι να ενισχυθεί η ασφάλεια των δεδομένων διασφαλίζοντας ότι η Beta Inc. δεν έχει πρόσβαση στα αρχικά αναγνωριστικά των υποκειμένων των δεδομένων, αποτρέποντας την άμεση επαναταυτοποίηση, υπό την προϋπόθεση ότι δεν υπάρχουν άλλα χαρακτηριστικά που να την επιτρέπουν. Με τον τρόπο αυτό, η ψευδωνυμοποίηση προστατεύει την ασφάλεια των δεδομένων των υποκειμένων των δεδομένων από τον εκτελούντα την επεξεργασία, αλλά και τον υπεύθυνο επεξεργασίας από τυχόν πράξεις του εκτελούντος που θα οδηγούσαν σε διακινδύνευση προσωπικά δεδομένα των υποκειμένων της επεξεργασίας.

Μια παραλλαγή αυτού του σεναρίου θα μπορούσε να περιλαμβάνει την προώθηση των ψευδωνυμοποιημένων δεδομένων σε έναν άλλο υπεύθυνο επεξεργασίας, αντί για έναν εκτελούντα την επεξεργασία.



Εικόνα 5: *Σενάριο ψευδωνυμοποίησης 3 (πηγή: [1])*

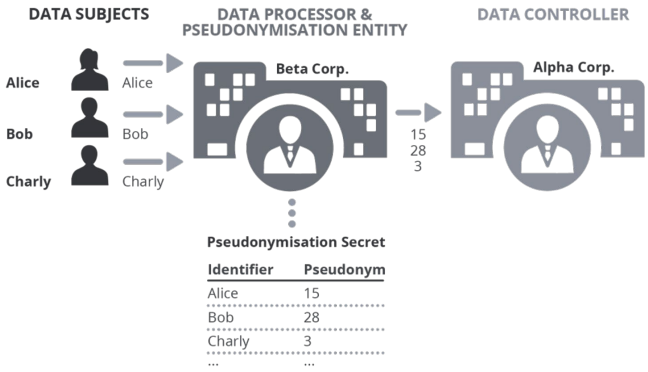
3.4. Σενάριο Ψευδωνυμοποίησης 4

Ένα άλλο σενάριο ψευδωνυμοποίησης αποτελεί η ανάθεση της ψευδωνυμοποίησης από τον υπεύθυνο επεξεργασίας σε έναν εκτελούντα την επεξεργασία, ο οποίος διαχειρίζεται το μυστικό της ψευδωνυμοποίησης και τις απαραίτητες τεχνικές υποδομές [1].

Όπως φαίνεται στην Εικόνα 7, τα υποκείμενα των δεδομένων αποστέλλουν τα δεδομένα προσωπικού χαρακτήρα τους σε έναν εκτελούντα την επεξεργασία (Beta Inc.), ο οποίος πραγματοποιεί την ψευδωνυμοποίηση, δηλαδή ενεργεί ως οντότητα ψευδωνυμοποίησης εκ μέρους του υπεύθυνου επεξεργασίας (Alpha Corp.). Στη συνέχεια, τα ψευδωνυμοποιημένα δεδομένα προωθούνται στον υπεύθυνο επεξεργασίας, διασφαλίζοντας ότι μόνο ψευδωνυμοποιημένα δεδομένα αποθηκεύονται από πλευράς του υπεύθυνου επεξεργασίας.

Ο βασικός σκοπός της ψευδωνυμοποίησης σε αυτό το σενάριο είναι να ενισχυθεί η ασφάλεια στο επίπεδο του υπεύθυνου επεξεργασίας, ελαχιστοποιώντας τον κίνδυνο έκθεσης σε περίπτωση παραβίασης δεδομένων. Ωστόσο, ο υπεύθυνος επεξεργασίας διατηρεί τη δυνατότητα επαναταυτοποίησης των υποκειμένων των δεδομένων μέσω του εκτελούντος την επεξεργασία, καθιστώντας την ασφάλεια στο επίπεδο του εκτελούντος την επεξεργασία εξαιρετικά σημαντική.

Μια παραλλαγή αυτού του σεναρίου θα μπορούσε να περιλαμβάνει τη συμμετοχή πολλών διαφορετικών εκτελούντων την επεξεργασία στη διαδικασία ψευδωνυμοποίησης ως ακολουθία οντοτήτων ψευδωνυμοποίησης (αλυσίδα εκτελούντων την επεξεργασία).



Εικόνα 6: *Σενάριο ψευδωνυμοποίησης 4 (πηγή: [1])*

3.5. Σενάριο Ψευδωνυμοποίησης 5

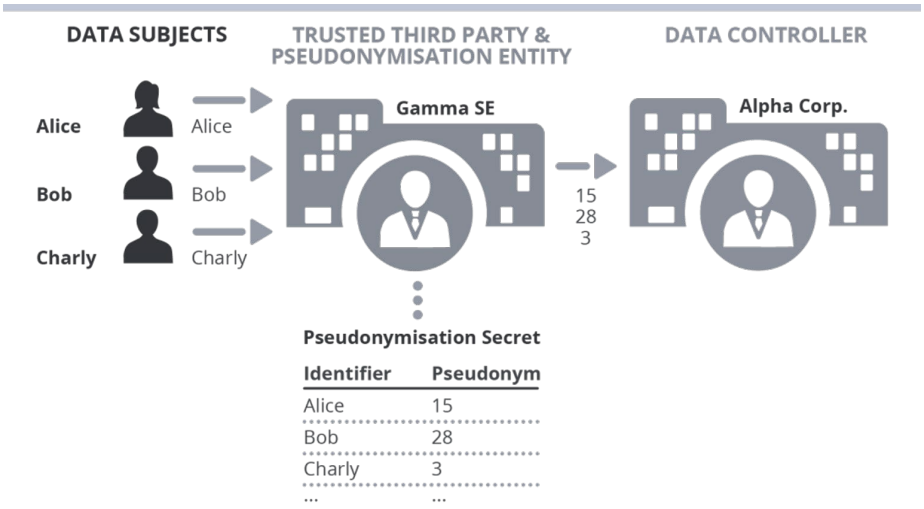
Ένα διαφορετικό σενάριο αποτελεί η πραγματοποίηση της ψευδωνυμοποίησης από ένα τρίτο μέρος και όχι από τον εκτελούντα την επεξεργασία και ακολούθως η προώθηση των ψευδωνυμοποιημένων δεδομένων στον υπεύθυνο επεξεργασίας [1]. Σε αντίθεση με το σενάριο 4, ο υπεύθυνος επεξεργασίας στην περίπτωση αυτή δεν έχει πρόσβαση στα αναγνωριστικά των υποκειμένων των δεδομένων, καθώς το τρίτο μέρος δεν υπόκειται στον έλεγχό του.

Όπως φαίνεται στην Εικόνα 8, τα υποκείμενα των δεδομένων αποστέλλουν τα δεδομένα προσωπικού χαρακτήρα τους σε ένα τρίτο μέρος (Gamma SE), το οποίο αρχικά πραγματοποιεί την ψευδωνυμοποίηση, δηλαδή ενεργεί ως οντότητα ψευδωνυμοποίησης και στη συνέχεια προωθεί τα ψευδωνυμοποιημένα δεδομένα στον υπεύθυνο επεξεργασίας (Alpha Corp.). Σε αυτό το σενάριο, ο υπεύθυνος επεξεργασίας δεν μπορεί να συνδέσει άμεσα ή έμμεσα μεμονωμένες εγγραφές δεδομένων με συγκεκριμένα υποκείμενα των δεδομένων.

Ο βασικός σκοπός της ψευδωνυμοποίησης σε αυτό το σενάριο είναι να ενισχυθεί η ασφάλεια στο επίπεδο του υπεύθυνου επεξεργασίας, σύμφωνα με την αρχή της ελαχιστοποίησης των δεδομένων. Δηλαδή, μπορεί να χρησιμοποιηθεί σε περιπτώσεις που ο υπεύθυνος επεξεργασίας δεν χρειάζεται να έχει πρόσβαση στις ταυτότητες των υποκειμένων των δεδομένων για να πραγματοποιήσει μια επεξεργασία.

Το σενάριο αυτό, μπορεί να είναι ιδιαίτερα σημαντικό σε περιπτώσεις ευθύνης επεξεργασίας (controllership), όπου ένας υπεύθυνος επεξεργασίας ενεργεί ως έμπιστο τρίτο μέρος (trusted third party), που πραγματοποιεί την ψευδωνυμοποίηση πριν από την προώθηση των ψευδωνυμοποιημένων δεδομένων σε άλλον υπεύθυνο επεξεργασίας για περαιτέρω επεξεργασία.

Μια παραλλαγή αυτού του σεναρίου θα μπορούσε να περιλαμβάνει ένα έμπιστο τρίτο μέρος που είναι κατανεμημένο σε περισσότερες από μία οντότητες, οι οποίες μπορούν μόνο από κοινού να δημιουργούν και να επαναφέρουν ψευδώνυμα. Με αυτόν τον τρόπο, δε χρειάζεται να εμπιστεύεται κανείς μόνο μία οντότητα.



Εικόνα 7: *Σενάριο ψευδωνυμοποίησης 5 (πηγή: [1])*

3.6. Σενάριο Ψευδωνυμοποίησης 6

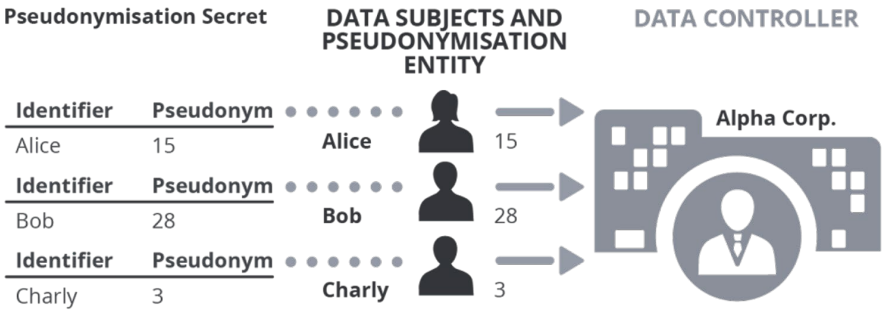
Ένα ειδικό σενάριο ψευδωνυμοποίησης αποτελεί η πραγματοποίηση της ψευδωνυμοποίησης από τα ίδια τα υποκείμενα των δεδομένων που δημιουργούν τα δικά τους ψευδώνυμα, ως μέρος της διαδικασίας ψευδωνυμοποίησης [1].

Όπως φαίνεται στην Εικόνα 9, κάθε άτομο – υποκείμενο των δεδομένων – δημιουργεί το δικό του ψευδώνυμο πριν προωθήσει τα δεδομένα του μαζί με το ψευδώνυμό του στον υπεύθυνο επεξεργασίας. Έτσι διασφαλίζεται, ότι ο υπεύθυνος επεξεργασίας δεν έχει πρόσβαση στα αρχικά αναγνωριστικά των υποκειμένων των δεδομένων, ενώ παράλληλα, επιτρέπεται σε αυτά να διατηρούν τον έλεγχο της διαδικασίας ψευδωνυμοποίησης. Πρέπει να σημειωθεί, ότι η συνολική ευθύνη για τη διατήρηση της ακεραιότητας του συστήματος ψευδωνυμοποίησης εξακολουθεί να ανήκει στον υπεύθυνο επεξεργασίας δεδομένων.

Ένα παράδειγμα αυτής της προσέγγισης συναντάται στα συστήματα blockchain (π.χ. Bitcoin), όπου το δημόσιο κλειδί ενός ζεύγους κλειδιών, χρησιμοποιείται για τη δημιουργία του ψευδωνύμου.

Ομοίως με το σενάριο ψευδωνυμοποίησης 5, το παρόν σενάριο συνάδει με την αρχή της ελαχιστοποίησης των δεδομένων και μπορεί να χρησιμοποιηθεί σε περιπτώσεις που ο υπεύθυνος επεξεργασίας δε χρειάζεται να έχει πρόσβαση στα

αρχικά αναγνωριστικά των υποκειμένων των δεδομένων για να πραγματοποιήσει μια επεξεργασία.



Εικόνα 8: *Σενάριο ψευδωνυμοποίησης 6 (πηγή: [1])*

3.7. Βιβλιογραφικές Αναφορές

[1] ENISA, "Pseudonymisation techniques and best practices" διαθέσιμο στο https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices (2019)