

## ΕΡΓΑΣΙΑ 2

### Τεχνικές και Διαδικασίες Ψευδωνυμοποίησης βάσει του κανονισμού GDPR

#### ΑΣΚΗΣΗ 1<sup>η</sup>

Η Παθολογική Κλινική ενός Νοσοκομείου στο πλαίσιο μια κλινικής μελέτης πρέπει να παραδώσει σε ένα πανεπιστήμιο δεδομένα ασθενών για την εξαγωγή συμπερασμάτων για χρόνια πάσχοντες. Θα πρέπει όμως βάσει του GDPR πριν τα διαβιβάσει να τα προστατεύσει εφαρμόζοντας ψευδωνυμοποίηση. Τα δεδομένα που διαθέτει στη βάση δεδομένων του Πληροφοριακού Συστήματος για συγκεκριμένους ασθενείς περιλαμβάνουν: **Ονοματεπώνυμο ασθενούς, ΑΜΚΑ, τηλέφωνο, διεύθυνση κατοικίας, αποτελέσματα εξετάσεων (βιοχημικές & αιματολογικές), ιστορικό θεραπειών και κλινική διάγνωση.**

#### Ζητούνται:

1. Να εντοπίσετε ποια από αυτά τα στοιχεία αποτελούν **απλά προσωπικά δεδομένα (άμεσα αναγνωριστικά και ποια είναι έμμεσα αναγνωριστικά)**
2. Να εντοπίσετε ποια θεωρούνται **ευαίσθητα προσωπικά δεδομένα**
3. Να προτείνετε έναν κατάλληλο τρόπο ψευδωνυμοποίησης (βάσει του άρθρου 4 του GDPR) για να αντικατασταθούν τα αναγνωριστικά στοιχεία με τεχνητούς κωδικούς (βασιστείτε στις διαφάνειες 45 – 49 της σχετικής διάλεξης για τον κανονισμό του GDPR).
4. Να περιγράψετε πώς πρέπει να αποθηκεύεται με ασφάλεια ο πίνακας αντιστοίχισης (που συνδέει τους κωδικούς με τα πραγματικά στοιχεία) βάσει του άρθρου 32 του GDPR.
5. Να παρουσιάσετε τα βασικά βήματα της διαδικασίας από την εξαγωγή των δεδομένων μέχρι τη διαβίβαση των ψευδωνυμοποιημένων δεδομένων αναφέροντας. Ποιος είναι ο ρόλος του Data Protection Officer σε αυτήν τη διαδικασία, ποιοι άλλοι εργαζόμενοι εμπλέκονται. Να εξηγήσετε γιατί η ψευδωνυμοποίηση μειώνει τον κίνδυνο παραβίασης αλλά και σε ποιες περιπτώσεις μπορεί να μην είναι επαρκής.

**Υποδείξεις:** Ταξινομήστε τα δεδομένα του οργανισμού σε κατηγορίες (άμεσα αναγνωριστικά, έμμεσα αναγνωριστικά, ευαίσθητα δεδομένα), προτείνετε έναν πρακτικό τρόπο με τον οποίο θα μπορούσαν να αντικατασταθούν τα πραγματικά στοιχεία των ασθενών με ψευδώνυμα όπως “PAT001” ή “PAT002”, περιγράψτε πού και πώς θα πρέπει να φυλάσσεται ο πίνακας αντιστοίχισης με τα πραγματικά στοιχεία, παρουσιάστε τη σειρά ενεργειών που πρέπει να ακολουθήσει ο οργανισμός, ώστε να εφαρμόσει σωστά την ψευδωνυμοποίηση πριν στείλει τα δεδομένα, και περιγράψτε γιατί αυτή η διαδικασία μειώνει τον κίνδυνο αποκάλυψης ταυτότητας και σε ποιες περιπτώσεις μπορεί να μην είναι αρκετή από μόνη της. **Το παραδοτέο είναι έγγραφο σε word ή pdf με τις απαντήσεις σας.**

## ΑΣΚΗΣΗ 2"

Ένας οργανισμός θέλει να μοιραστεί δεδομένα πελατών του με έναν εξωτερικό συνεργάτη για τη διεξαγωγή μιας στατιστικής ανάλυσης με βάση το επάγγελμα και την ηλικία. Σύμφωνα με τον κανονισμό του GDPR, πριν αποσταλούν τα δεδομένα των πελατών, θα πρέπει να πραγματοποιηθεί η **ψευδωνυμοποίηση**, δηλαδή η αντικατάσταση των πραγματικών στοιχείων (ονόματα, emails & επαγγέλματος) με τεχνητά αναγνωριστικά, ώστε να μην αποκαλύπτεται η ταυτότητα των ατόμων. Ο αρχικός πίνακας δεδομένων είναι:

```
customers = [  
  
    {"name": "Αννα", "surname": "Παπαδοπούλου", "email": "anna@example.com", "age": 28,  
    "profession": "Ιατρός"},  
  
    {"name": "Κώστας", "surname": "Νικολάου", "email": "kostas@example.com", "age": 35,  
    "profession": "Μηχανικός Η/Υ"},  
  
    {"name": "Ιωάννα", "surname": "Γεωργίου", "email": "ioanna@example.com", "age": 22,  
    "profession": "Καθηγήτρια"}  
]
```

### Ζητούνται:

1. Να αντικαταστήσετε τα στοιχεία που μπορούν να ταυτοποιήσουν άμεσα τον πελάτη (όνομα, email) με ένα ψευδώνυμο της μορφής "USER1", "USER2", "USER3" ή οποιασδήποτε άλλης μορφής χρησιμοποιώντας μία από τις τεχνικές του πίνακα της σελίδας 47 της διάλεξης του GDPR.
2. Να δημιουργήσετε έναν πίνακα αντιστοίχισης (mapping table), όπου θα καταγράφονται τα ψευδώνυμα και τα πραγματικά στοιχεία. Σημείωση: Βάσει του κανονισμού GDPR, ο πίνακας αυτός πρέπει να αποθηκεύεται ξεχωριστά και με αυξημένα τεχνικά μέτρα ασφάλειας.
3. Να εξάγετε:
  - i. τον πίνακα με τα ψευδωνυμοποιημένα δεδομένα,
  - ii. τον πίνακα αντιστοίχισης
4. Να εξηγήσετε με ένα σύντομο σχόλιο μέσα στο πρόγραμμα **γιατί η ψευδωνυμοποίηση βοηθά στην προστασία των προσωπικών δεδομένων**, σύμφωνα με τον GDPR.

**Υποδείξεις:** Θα πρέπει να χρησιμοποιήσετε μια γλώσσα προγραμματισμού της αρεσκείας σας (π.χ. Python, Matlab, Java, C#, κτλ.) για να απαντήσετε στα ερωτήματα. Το παραδοτέο είναι έγγραφο σε word ή pdf με τις απαντήσεις σας και τον κώδικα.