Διαμοιρασμός προσωπικών δεδομένων υπό το φως των νέων νομοθετικών πράξεων στην ΕΕ: (Τεχνολογικές) προκλήσεις

Δρ. Κωνσταντίνος Λιμνιώτης

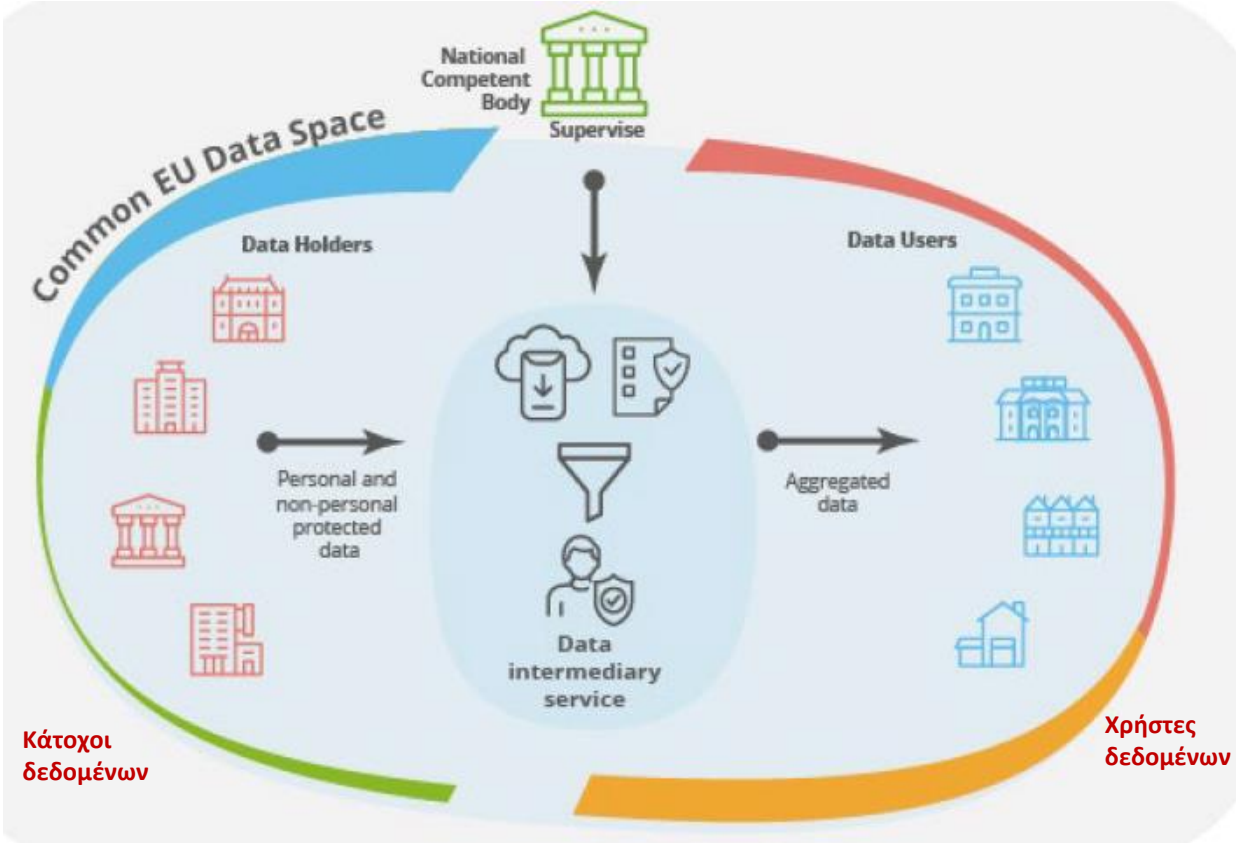
Ειδικός Επιστήμονας Πληροφορικής, Προϊστάμενος Τμήματος Μελετών και Έρευνας, Αρχή Προστασίας Δεδομένων

ΕΠΙΣΤΗΜΟΝΙΚΟ ΣΥΜΒΟΥΛΙΟ για την ΚΟΙΝΩΝΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ
4η Ημερίδα «Πρόσφατες εξελίξεις στην προστασία δεδομένων»
Αθήνα, 27/9/2024

Θέματα που θα συζητηθούν

- Η έννοια του διαμοιρασμού δεδομένων
  - Πράξη για την Διακυβέρνηση των Δεδομένων (DGA)
  - Πράξη για τα Δεδομένα (Data Act)
  - Ευρωπαϊκός Χώρος Δεδομένων για την υγεία (EHDS)
- Ασφαλές περιβάλλον επεξεργασίας
  - Πότε απαιτείται;
  - Πώς υλοποιείται;
- Ο ρόλος των (προηγμένων) κρυπτογραφικών τεχνικών
- Σκέψεις - Συμπεράσματα

Διαμοιρασμός (Κοινοχρησία) δεδομένων μέσω υπηρεσίας διαμεσολάβησης



Πηγή: ENISA, Engineering Data Spaces, 2024

- Προσωπικά δεδομένα διαμοιράζονται, είτε από τα ίδια τα υποκείμενα των δεδομένων είτε από κατόχους δεδομένων (data holders) σε χρήστες δεδομένων (data users), ενδεχομένως μέσω υπηρεσίας διαμεσολάβησης (data intermediation service)
  - Υπό διάφορες προϋποθέσεις (DGA, Data Act, EHDS) και σύμφωνα με τον ΓΚΠΔ
  - **Οι χρήστες δεδομένων κατά κανόνα δεν επιτρέπεται να λάβουν προσωποποιημένες πληροφορίες**
    - Τεχνολογίες προάσπισης της ιδιωτικότητας (ανωνυμοποίηση, ψευδωνυμοποίηση, …..)
    - Ποιος (οφείλει να) τις υλοποιεί; Ποιος ο ρόλος της υπηρεσίας διαμεσολάβησης;

Υπηρεσία διαμεσολάβησης δεδομένων (άρ. 4 DGA)

- *Υπηρεσία που αποσκοπεί στη δημιουργία εμπορικών σχέσεων για τους σκοπούς της κοινοχρησίας δεδομένων μεταξύ απροσδιόριστου αριθμού υποκειμένων των δεδομένων και κατόχων δεδομένων, αφενός, και χρηστών δεδομένων, αφετέρου, με τεχνικά, νομικά ή άλλα μέσα, μεταξύ άλλων για τον σκοπό της άσκησης των δικαιωμάτων των υποκειμένων των δεδομένων σε σχέση με τα δεδομένα προσωπικού χαρακτήρα*

Υπηρεσία διαμεσολάβησης δεδομένων (άρ. 12 DGA)

- *(…) δεν χρησιμοποιεί τα δεδομένα για τα οποία παρέχει τις υπηρεσίες διαμεσολάβησης δεδομένων για άλλους σκοπούς (…)*
- *οι υπηρεσίες (…) μπορούν να περιλαμβάνουν την προσφορά πρόσθετων ειδικών εργαλείων και υπηρεσιών στους κατόχους δεδομένων ή τα υποκείμενα των δεδομένων με συγκεκριμένο σκοπό τη διευκόλυνση της ανταλλαγής δεδομένων, όπως η προσωρινή αποθήκευση, η επιμέλεια, η μετατροπή, η ανωνυμοποίηση και η ψευδωνυμοποίηση, τα οποία εργαλεία χρησιμοποιούνται μόνο κατόπιν ρητού αιτήματος ή έγκρισης του κατόχου των δεδομένων ή του υποκειμένου των δεδομένων (…)*
- *(…) ενεργεί προς το βέλτιστο συμφέρον των υποκειμένων όταν διευκολύνει την άσκηση των δικαιωμάτων τους (…)*

Πότε υπεισέρχεται υπηρεσία διαμεσολάβησης;

- DGA: Ορισμός πλαισίου για την παροχή υπηρεσιών διαμεσολάβησης (εμπορικά – με αντίτιμο) για κατόχους δεδομένων και υποκείμενα των δεδομένων που επιδιώκουν να καταστήσουν διαθέσιμα προσωπικά δεδομένα
- Data Act: Γενική αναφορά στις εισαγωγικές σκέψεις, παραπέμποντας απευθείας στον ορισμό της DGA:
  - Σκέψη 26: *«(…) η εν λόγω κοινοχρησία δεδομένων θα μπορούσε να πραγματοποιείται απευθείας από τον χρήστη, κατόπιν αιτήματος του χρήστη μέσω κατόχου δεδομένων, ή μέσω υπηρεσιών διαμεσολάβησης δεδομένων. Οι υπηρεσίες διαμεσολάβησης δεδομένων (…) μπορούν να στηρίζουν τους χρήστες που ασκούν το δικαίωμά τους να χρησιμοποιούν τα δεδομένα, όπως με τη διασφάλιση της ανωνυμοποίησης των δεδομένων προσωπικού χαρακτήρα ή τη συγκέντρωση της πρόσβασης στα δεδομένα από πολλαπλούς μεμονωμένους χρήστες»*.

Πότε υπεισέρχεται υπηρεσία διαμεσολάβησης;

- EHDS: Ειδική αναφορά για την περίπτωση δευτερογενούς χρήσης δεδομένων
  - Άρθρο 32α: «*Τα κράτη μέλη μπορούν, δυνάμει της εθνικής νομοθεσίας, να προβλέπουν ότι τα καθήκοντα ορισμένων κατηγοριών κατόχων δεδομένων εκπληρώνονται από οντότητες διαμεσολάβησης δεδομένων υγείας*»
- Ωστόσο:
  - Ρόλο κατά μία έννοια αντίστοιχο, με «επαυξημένα εχέγγυα», θα έχουν οι φορείς πρόσβασης σε δεδομένα υγείας (health data access bodies)
    - Δημόσιοι φορείς που ορίζονται από τα Κράτη – Μέλη
    - Αποφασίζουν σχετικά με αιτήσεις πρόσβασης από χρήστες των δεδομένων και, εφόσον εγκρίνουν, επιτρέπουν πρόσβαση (άρθρο 37)
    - Ζητούν τα δεδομένα από τους κατόχους αυτών εφόσον υπάρχει εγκεκριμένο αίτημα χορήγησης δεδομένων
    - Συλλέγουν και επεξεργάζονται περαιτέρω τα δεδομένα από τους κατόχους τους, εφαρμόζοντας τεχνικές ανωνυμοποίησης και ψευδωνυμοποίησης
    - Παρέχουν αναλυτική ενημέρωση σε υποκείμενα των δεδομένων
    - Παρακολουθούν και εποπτεύουν τόσο τους κατόχους όσο και τους χρήστες δεδομένων υγείας
  - Αρμόδιες οι εποπτικές αρχές προστασίας δεδομένων

Φορέας πρόσβασης σε δεδομένα υγείας

Φορέας πρόσβασης σε δεδομένα υγείας

Φορέας πρόσβασης σε δεδομένα υγείας

- Άρθρο 50: Οι φορείς πρόσβασης σε δεδομένα υγείας παρέχουν πρόσβαση σε ηλεκτρονικά δεδομένα υγείας σύμφωνα με άδεια επεξεργασίας δεδομένων μόνο μέσω ασφαλούς περιβάλλοντος επεξεργασίας, με τεχνικά και οργανωτικά μέτρα, καθώς και με απαιτήσεις ασφάλειας και διαλειτουργικότητας.
- Για το ασφαλές περιβάλλον επεξεργασίας, γίνεται αναφορά στον ορισμό στη DGA:
  - *"Το φυσικό ή εικονικό περιβάλλον και τα οργανωτικά μέσα διά των οποίων διασφαλίζεται η συμμόρφωση με το ενωσιακό δίκαιο όπως ο κανονισμός (ΕΕ) 2016/679, ιδίως όσον αφορά τα δικαιώματα των υποκειμένων των δεδομένων (…), την ακεραιότητα και την προσβασιμότητα, καθώς επίσης και με το εφαρμοστέο εθνικό δίκαιο, ενώ παράλληλα δίδεται η δυνατότητα στην οντότητα που παρέχει το ασφαλές περιβάλλον επεξεργασίας να προσδιορίζει και να εποπτεύει όλες τις ενέργειες επεξεργασίας δεδομένων, μεταξύ άλλων την εμφάνιση, αποθήκευση, τηλεφόρτωση, εξαγωγή των δεδομένων και τον υπολογισμό παράγωγων δεδομένων μέσω υπολογιστικών αλγορίθμων"*

Ασφαλές περιβάλλον επεξεργασίας (Σκέψη 54, EHDS)

- Κάθε πρόσβαση στα ζητούμενα ηλεκτρονικά δεδομένα υγείας για δευτερογενή χρήση θα πρέπει να πραγματοποιείται μέσω ασφαλούς περιβάλλοντος επεξεργασίας
- Η επεξεργασία δεδομένων προσωπικού χαρακτήρα σε ένα τέτοιο ασφαλές περιβάλλον θα πρέπει να συμμορφώνεται με τον κανονισμό (ΕΕ) 2016/679, συμπεριλαμβανομένων, όταν το ασφαλές περιβάλλον τελεί υπό τη διαχείριση τρίτου, των απαιτήσεων του άρθρου 28 και, κατά περίπτωση, του κεφαλαίου V.
- Το εν λόγω ασφαλές περιβάλλον επεξεργασίας θα πρέπει να μειώνει τους κινδύνους για την ιδιωτική ζωή που σχετίζονται με τις εν λόγω δραστηριότητες επεξεργασίας και να αποτρέπει τη διαβίβαση των ηλεκτρονικών δεδομένων υγείας απευθείας στους χρήστες των δεδομένων
- Από το εν λόγω ασφαλές περιβάλλον επεξεργασίας οι χρήστες δεδομένων θα πρέπει να εξάγουν μόνο μη προσωπικά ηλεκτρονικά δεδομένα υγείας που δεν περιέχουν ηλεκτρονικά δεδομένα υγείας.

Ασφαλές περιβάλλον επεξεργασίας (Άρθρο 50, EHDS)

- Περιορίζει την πρόσβαση στα εξουσιοδοτημένα ***φυσικά*** πρόσωπα που απαριθμούνται στην αντίστοιχη άδεια επεξεργασίας δεδομένων
- Ελαχιστοποιεί τον κίνδυνο μη εξουσιοδοτημένης ανάγνωσης, αντιγραφής, τροποποίησης ή αφαίρεσης ηλεκτρονικών δεδομένων υγείας με σύγχρονα ***τεχνικά και οργανωτικά μέτρα***
- Περιορίζει την εισαγωγή ηλεκτρονικών δεδομένων υγείας και την επιθεώρηση, τροποποίηση ή διαγραφή ηλεκτρονικών δεδομένων υγείας σε περιορισμένο αριθμό εξουσιοδοτημένων ταυτοποιήσιμων ατόμων
- Διασφαλίζει ότι οι χρήστες των δεδομένων *υγείας* έχουν πρόσβαση μόνο στα ηλεκτρονικά δεδομένα υγείας που καλύπτονται από την άδεια επεξεργασίας, μέσω ατομικών και μοναδικών ταυτοτήτων χρήστη και μόνο με εμπιστευτικούς τρόπους πρόσβασης
- Τηρεί ταυτοποιήσιμα αρχεία καταγραφής πρόσβασης και δραστηριοτήτων για το χρονικό διάστημα που απαιτείται για την επαλήθευση και τον έλεγχο όλων των πράξεων επεξεργασίας στο εν λόγω περιβάλλον.

Ασφαλές περιβάλλον επεξεργασίας: Τι συνεπάγεται πρακτικά

- Υλοποίηση κατάλληλων οργανωτικών και τεχνικών μέτρων για την επίτευξη όλων των προαναφερθεισών απαιτήσεων
- Σε περίπτωση υλοποίησής/υποστήριξής του από εκτελούντα την επεξεργασία, ενδεχομένως ανακύπτουν ακόμα μεγαλύτερες προκλήσεις
  - Τι είδους δεδομένα θα λαμβάνει ο εκτελών;
    - Ανώνυμα; Ψευδωνυμοποιημένα; ….
  - Πώς διασφαλίζεται ότι ο εκτελών παρέχει πράγματι ένα ασφαλές περιβάλλον επεξεργασίας;
- Άξιο αναφοράς ότι στην DGA δεν τίθεται ρητά ως υποχρέωση για τους παρόχους υπηρεσιών διαμεσολάβησης
  - Αναφέρεται μόνο ως «δυνατότητα» των δημόσιων φορέων να επιτρέπουν την πρόσβαση στα δεδομένα που τηρούν για περαιτέρω χρήση μόνο μέσω ενός τέτοιου περιβάλλοντος

Πότε έχουμε ένα ασφαλές περιβάλλον επεξεργασίας;

- Δεν (φαίνεται να) υπάρχει κοινά αποδεκτός τρόπος υλοποίησης ενός τέτοιου περιβάλλοντος
  - Βλ. Report from the Workshop on Secure Processing Environments, 19-20 June 2023 (DOI: 10.5281/zenodo.8341642)
  - Έμφαση δίνεται στην ασφαλή απομακρυσμένη εξουσιοδοτημένη πρόσβαση των χρηστών (π.χ. μέσω Εικονικών Ιδιωτικών Δικτύων - VPNs)
- **Συμμόρφωση με το ΓΚΠΔ => Τήρηση της αρχής της ελαχιστοποίησης των δεδομένων**
  - Η ελαχιστοποίηση των δεδομένων πρέπει επίσης να είναι παρούσα σε όλες τις φάσεις επεξεργασίας (και) σε ένα τέτοιο περιβάλλον
  - Μέχρι τώρα, δεν φαίνεται να λαμβάνεται υπόψη ο όγκος και η φύση των προσωπικών δεδομένων που θα συλλέγει η υπηρεσία διαμεσολάβησης ή ο φορέας πρόσβασης σε δεδομένα υγείας

Ο ρόλος των (προηγμένων) κρυπτογραφικών τεχνικών

- Ασφαλές περιβάλλον επεξεργασίας κατά κανόνα συνεπάγεται «ασφαλείς υπολογισμούς» (secure computations)
- Η κρυπτογραφία παρέχει εργαλεία για ασφαλείς υπολογισμούς
  - Οι ιδιότητές τους είναι απόλυτα συμβατές με τις επιθυμητές ιδιότητες μίας τέτοιας επεξεργασίας
- Ενδεικτικά παραδείγματα:
  - Επανα-κρυπτογράφηση μέσω διαμεσολαβητή
  - Ομομορφική κρυπτογραφία
  - Πολυμορφική κρυπτογραφία
  - Ψευδωνυμοποίηση χωρίς γνώση

Ο ρόλος των (προηγμένων) κρυπτογραφικών τεχνικών

- Ασφαλές περιβάλλον επεξεργασίας κατά κανόνα συνεπάγεται «ασφαλείς υπολογισμούς» (secure computations)
- Η κρυπτογραφία παρέχει εργαλεία για ασφαλείς υπολογισμούς
  - Οι ιδιότητές τους είναι απόλυτα συμβατές με τις επιθυμητές ιδιότητες μίας τέτοιας επεξεργασίας
- Ενδεικτικά παραδείγματα:
  - Επανα-κρυπτογράφηση μέσω διαμεσολαβητή
  - Ομομορφική κρυπτογραφία
  - Πολυμορφική κρυπτογραφία
  - Ψευδωνυμοποίηση χωρίς γνώση

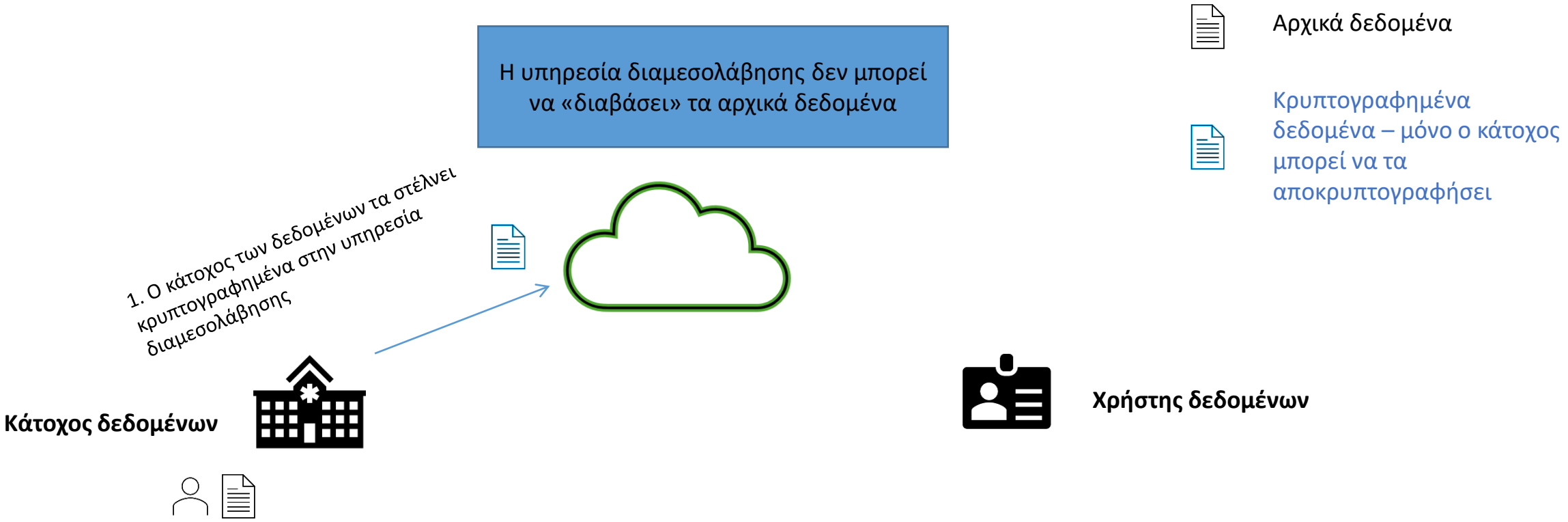
Κατάλληλα για κάθε διαμεσολάβηση, **ανεξαρτήτως του αν υλοποιηθεί ασφαλές περιβάλλον επεξεργασίας ή όχι**

Ο ρόλος των (προηγμένων) κρυπτογραφικών τεχνικών

- Ασφαλές περιβάλλον επεξεργασίας κατά κανόνα συνεπάγεται «ασφαλείς υπολογισμούς» (secure computations)
- Η κρυπτογραφία παρέχει εργαλεία για ασφαλείς υπολογισμούς
  - Οι ιδιότητές τους είναι απόλυτα συμβατές με τις επιθυμητές ιδιότητες μίας τέτοιας επεξεργασίας
- Ενδεικτικά παραδείγματα:
  - Επανα-κρυπτογράφηση μέσω διαμεσολαβητή
  - Ομομορφική κρυπτογραφία
  - Πολυμορφική κρυπτογραφία
  - Ψευδωνυμοποίηση χωρίς γνώση

Βέβαια, **για ασφαλή περιβάλλοντα επεξεργασίας**, ενδεχομένως μία διαχείριση κινδύνων να (πρέπει να) καταστήσει **υποχρεωτική την υλοποίησή τους**

Επανα-κρυπτογράφηση μέσω διαμεσολαβητή (Proxy re-encryption)



Επανα-κρυπτογράφηση μέσω διαμεσολαβητή (Proxy re-encryption)

Επανα-κρυπτογράφηση μέσω διαμεσολαβητή (Proxy re-encryption)

Επανα-κρυπτογράφηση μέσω διαμεσολαβητή (Proxy re-encryption)

4. Η υπηρεσία διαμεσολάβησης αξιοποιεί το κλειδί για να επανα-κρυπτογραφήσει το ήδη κρυπτογραφημένο μήνυμα σε ένα άλλο που μπορεί να αποκρυπτογραφήσει μόνο ο χρήστης

Χρήστης δεδομένων

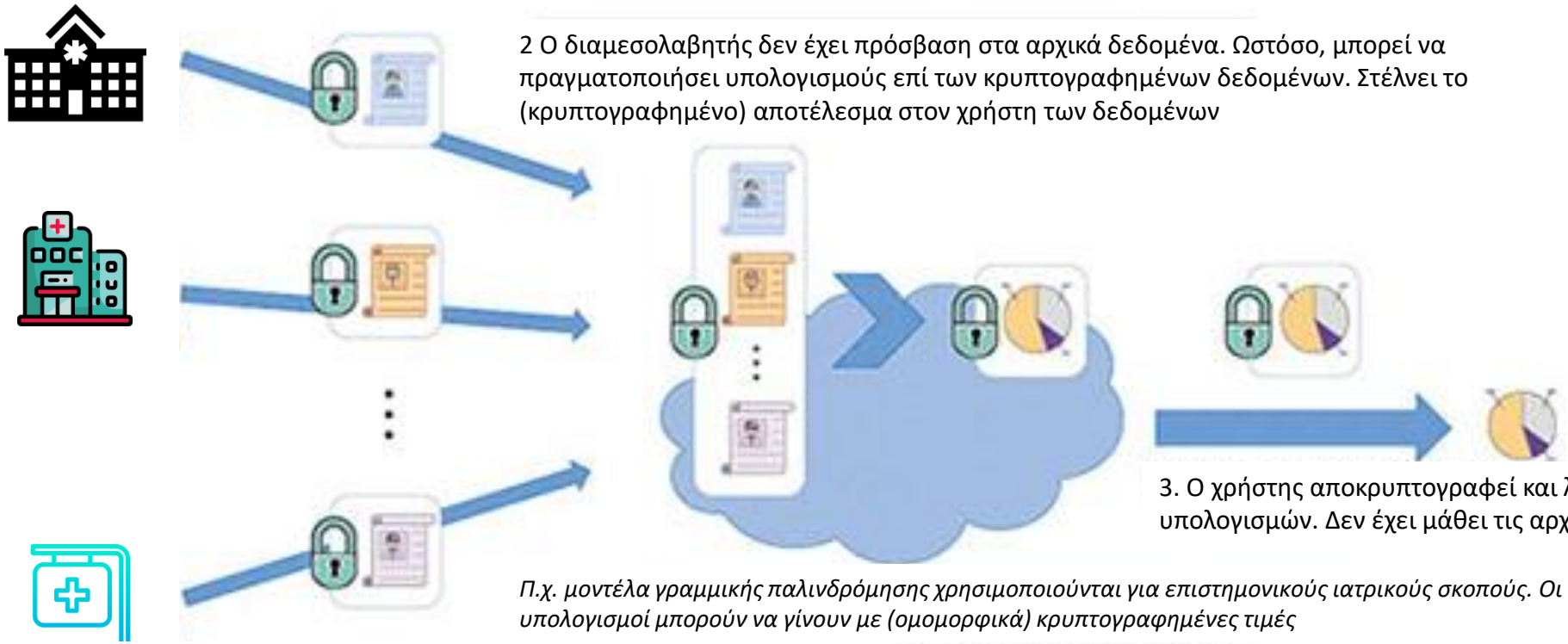
Κάτοχος δεδομένων

Αρχικά δεδομένα

Κρυπτογραφημένα δεδομένα – μόνο ο κάτοχος μπορεί να τα αποκρυπτογραφήσει

Κρυπτογραφημένα δεδομένα – μόνο ο χρήστης μπορεί να τα αποκρυπτογραφήσει

Ομομορφική κρυπτογραφία (Homomorhic encryption)



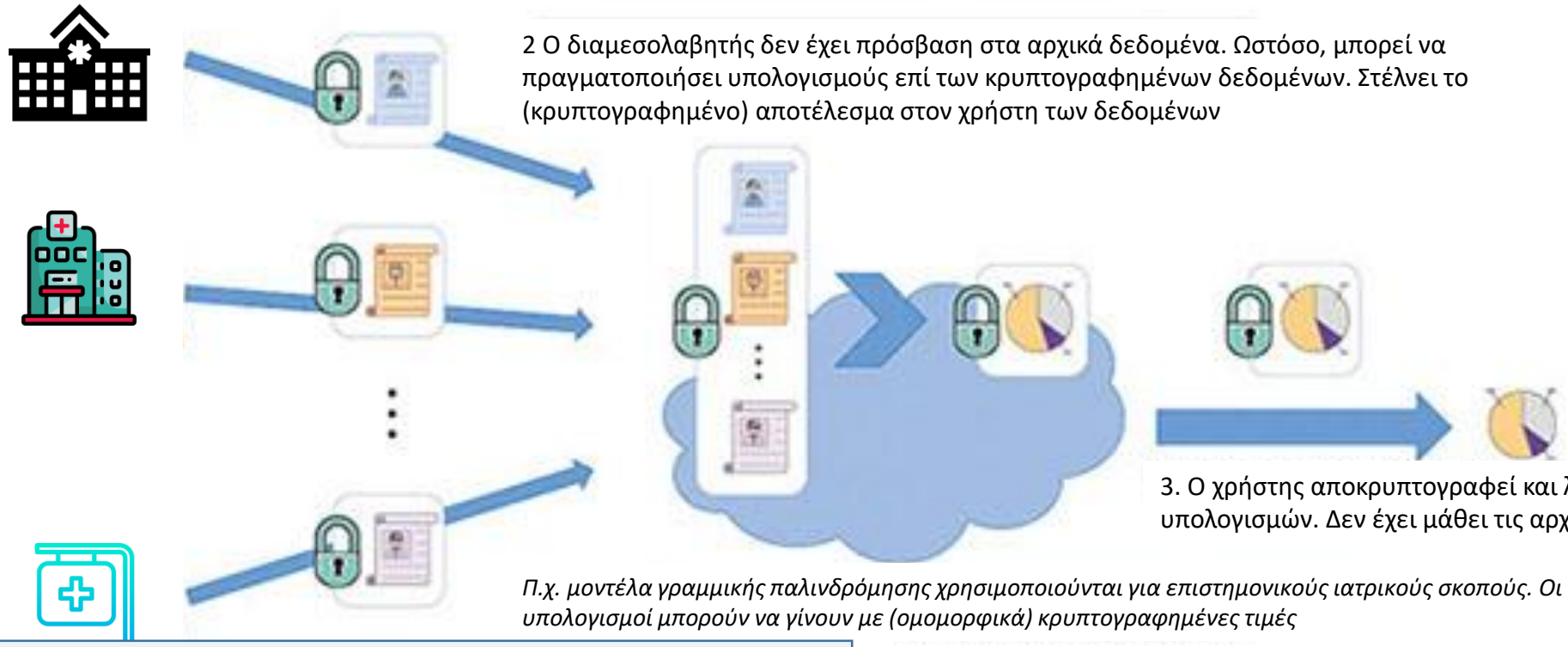
2 Ο διαμεσολαβητής δεν έχει πρόσβαση στα αρχικά δεδομένα. Ωστόσο, μπορεί να πραγματοποιήσει υπολογισμούς επί των κρυπτογραφημένων δεδομένων. Στέλνει το (κρυπτογραφημένο) αποτέλεσμα στον χρήστη των δεδομένων

3. Ο χρήστης αποκρυπτογραφεί και λαμβάνει το αποτέλεσμα των υπολογισμών. Δεν έχει μάθει τις αρχικές τιμές

Π.χ. μοντέλα γραμμικής παλινδρόμησης χρησιμοποιούνται για επιστημονικούς ιατρικούς σκοπούς. Οι υπολογισμοί μπορούν να γίνουν με (ομομορφικά) κρυπτογραφημένες τιμές

1. Οι κάτοχοι δεδομένων στέλνουν κρυπτογραφημένα δεδομένα στον διαμεσολαβητή, τα οποία μόνο ο χρήστης μπορεί να αποκρυπτογραφήσει

Ομομορφική κρυπτογραφία (Homomorhic encryption)



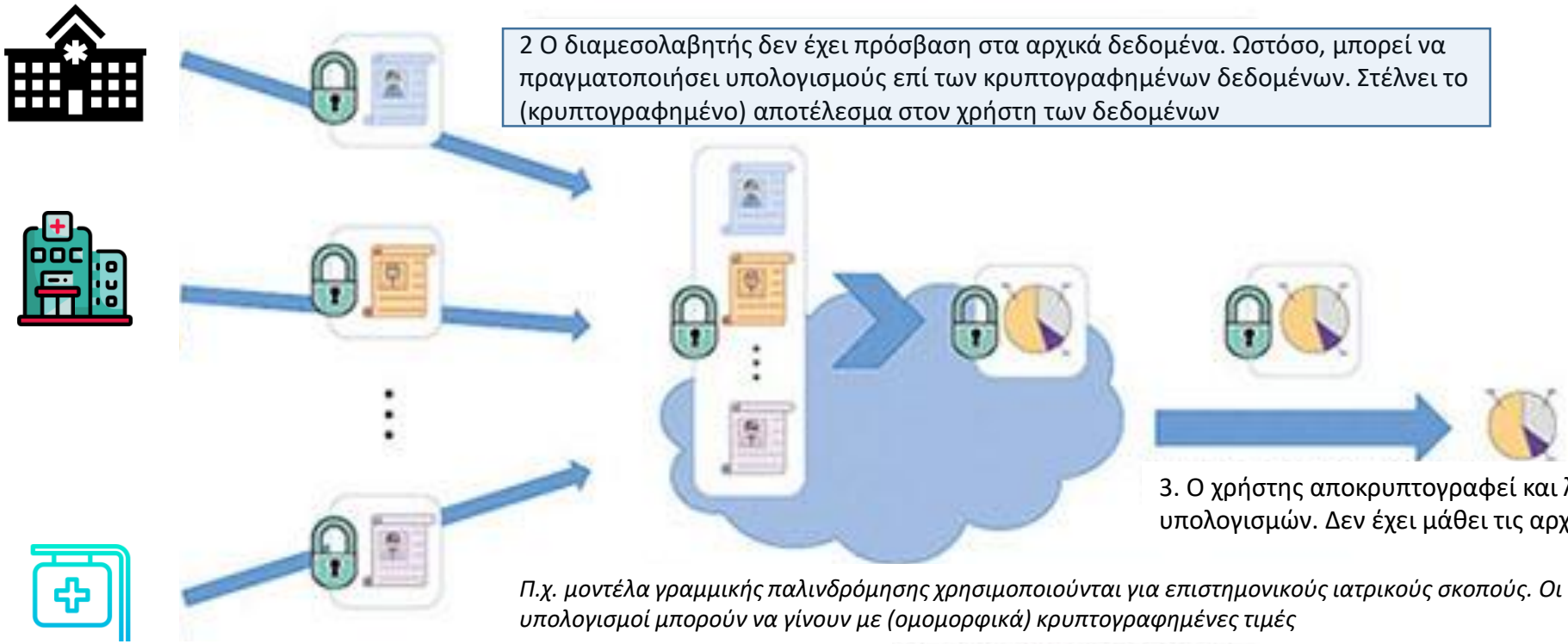
2 Ο διαμεσολαβητής δεν έχει πρόσβαση στα αρχικά δεδομένα. Ωστόσο, μπορεί να πραγματοποιήσει υπολογισμούς επί των κρυπτογραφημένων δεδομένων. Στέλνει το (κρυπτογραφημένο) αποτέλεσμα στον χρήστη των δεδομένων

3. Ο χρήστης αποκρυπτογραφεί και λαμβάνει το αποτέλεσμα των υπολογισμών. Δεν έχει μάθει τις αρχικές τιμές

Π.χ. μοντέλα γραμμικής παλινδρόμησης χρησιμοποιούνται για επιστημονικούς ιατρικούς σκοπούς. Οι υπολογισμοί μπορούν να γίνουν με (ομομορφικά) κρυπτογραφημένες τιμές

1. Οι κάτοχοι δεδομένων στέλνουν κρυπτογραφημένα δεδομένα στον διαμεσολαβητή, τα οποία μόνο ο χρήστης μπορεί να αποκρυπτογραφήσει

Ομομορφική κρυπτογραφία (Homomorhic encryption)



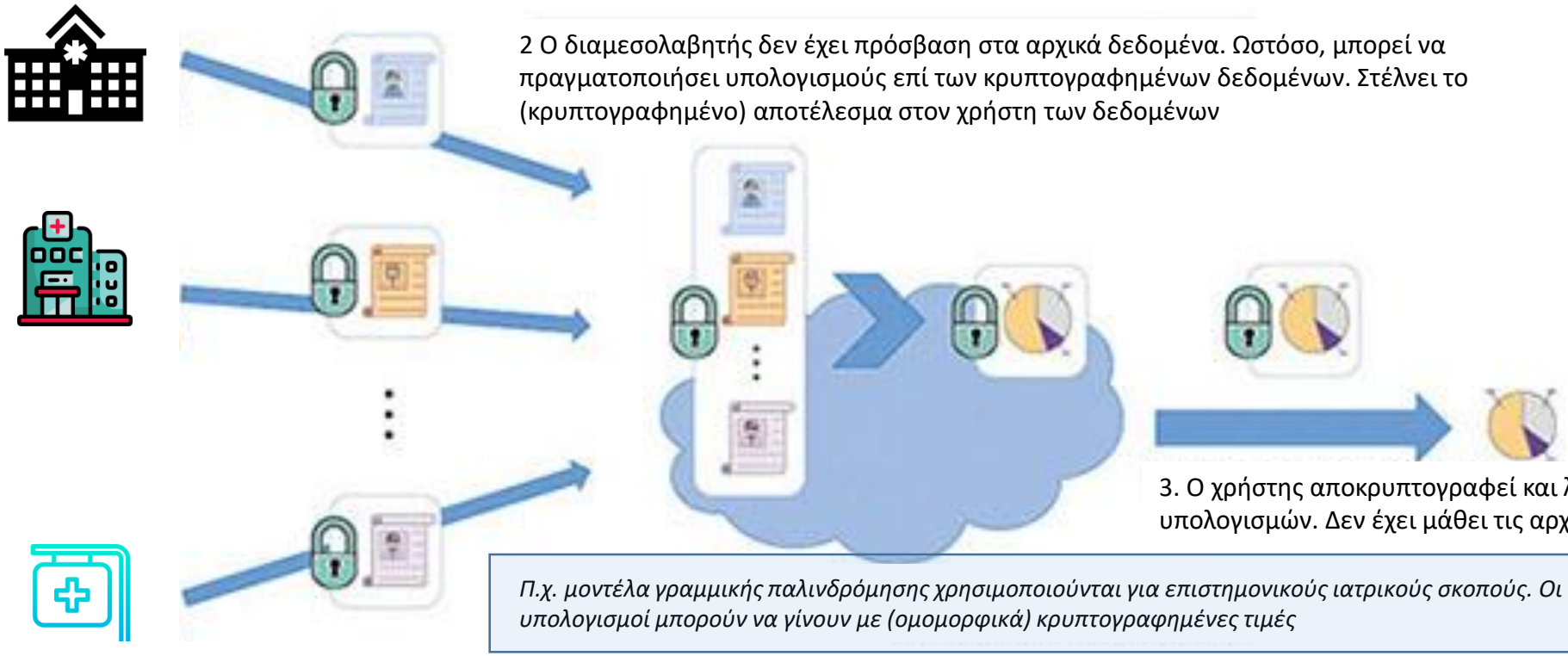
2 Ο διαμεσολαβητής δεν έχει πρόσβαση στα αρχικά δεδομένα. Ωστόσο, μπορεί να πραγματοποιήσει υπολογισμούς επί των κρυπτογραφημένων δεδομένων. Στέλνει το (κρυπτογραφημένο) αποτέλεσμα στον χρήστη των δεδομένων

3. Ο χρήστης αποκρυπτογραφεί και λαμβάνει το αποτέλεσμα των υπολογισμών. Δεν έχει μάθει τις αρχικές τιμές

Π.χ. μοντέλα γραμμικής παλινδρόμησης χρησιμοποιούνται για επιστημονικούς ιατρικούς σκοπούς. Οι υπολογισμοί μπορούν να γίνουν με (ομομορφικά) κρυπτογραφημένες τιμές

1. Οι κάτοχοι δεδομένων στέλνουν κρυπτογραφημένα δεδομένα στον διαμεσολαβητή, τα οποία μόνο ο χρήστης μπορεί να αποκρυπτογραφήσει

Ομομορφική κρυπτογραφία (Homomorhic encryption)



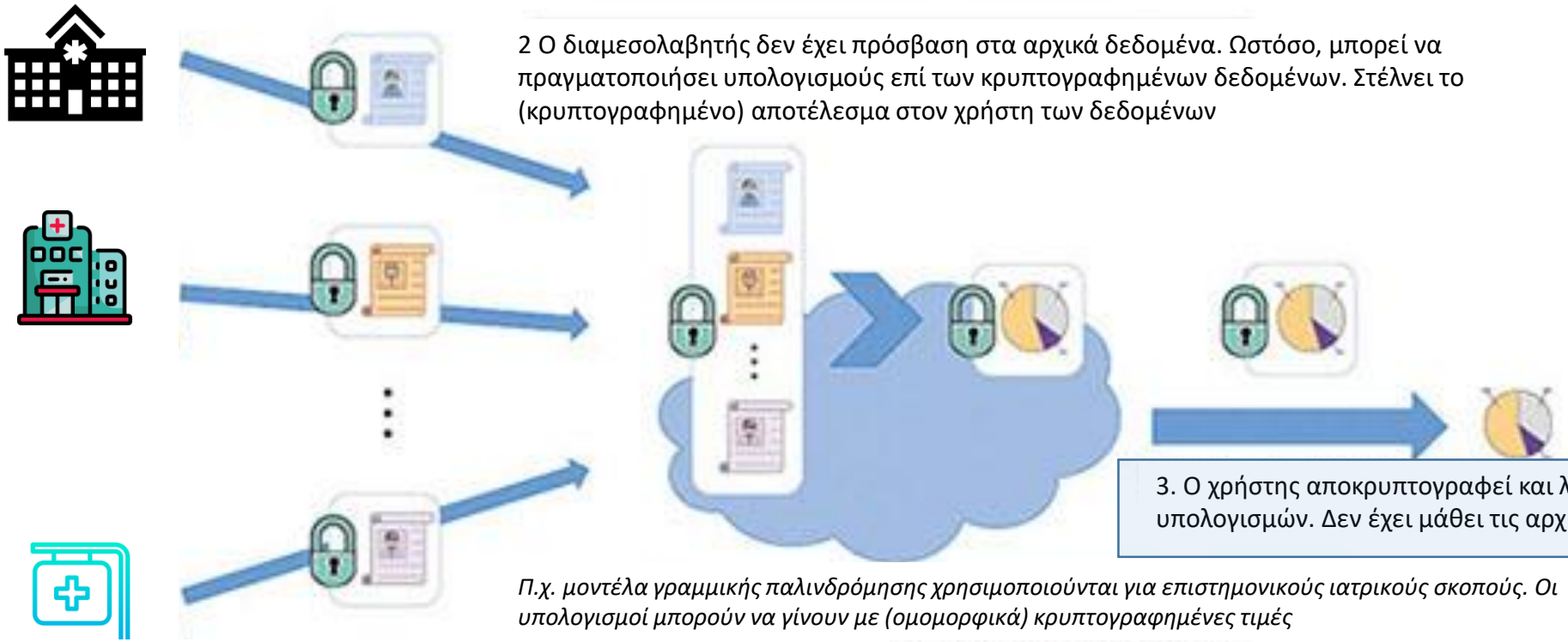
2 Ο διαμεσολαβητής δεν έχει πρόσβαση στα αρχικά δεδομένα. Ωστόσο, μπορεί να πραγματοποιήσει υπολογισμούς επί των κρυπτογραφημένων δεδομένων. Στέλνει το (κρυπτογραφημένο) αποτέλεσμα στον χρήστη των δεδομένων

3. Ο χρήστης αποκρυπτογραφεί και λαμβάνει το αποτέλεσμα των υπολογισμών. Δεν έχει μάθει τις αρχικές τιμές

Π.χ. μοντέλα γραμμικής παλινδρόμησης χρησιμοποιούνται για επιστημονικούς ιατρικούς σκοπούς. Οι υπολογισμοί μπορούν να γίνουν με (ομομορφικά) κρυπτογραφημένες τιμές

1. Οι κάτοχοι δεδομένων στέλνουν κρυπτογραφημένα δεδομένα στον διαμεσολαβητή, τα οποία μόνο ο χρήστης μπορεί να αποκρυπτογραφήσει

Ομομορφική κρυπτογραφία (Homomorhic encryption)



2 Ο διαμεσολαβητής δεν έχει πρόσβαση στα αρχικά δεδομένα. Ωστόσο, μπορεί να πραγματοποιήσει υπολογισμούς επί των κρυπτογραφημένων δεδομένων. Στέλνει το (κρυπτογραφημένο) αποτέλεσμα στον χρήστη των δεδομένων

3. Ο χρήστης αποκρυπτογραφεί και λαμβάνει το αποτέλεσμα των υπολογισμών. Δεν έχει μάθει τις αρχικές τιμές

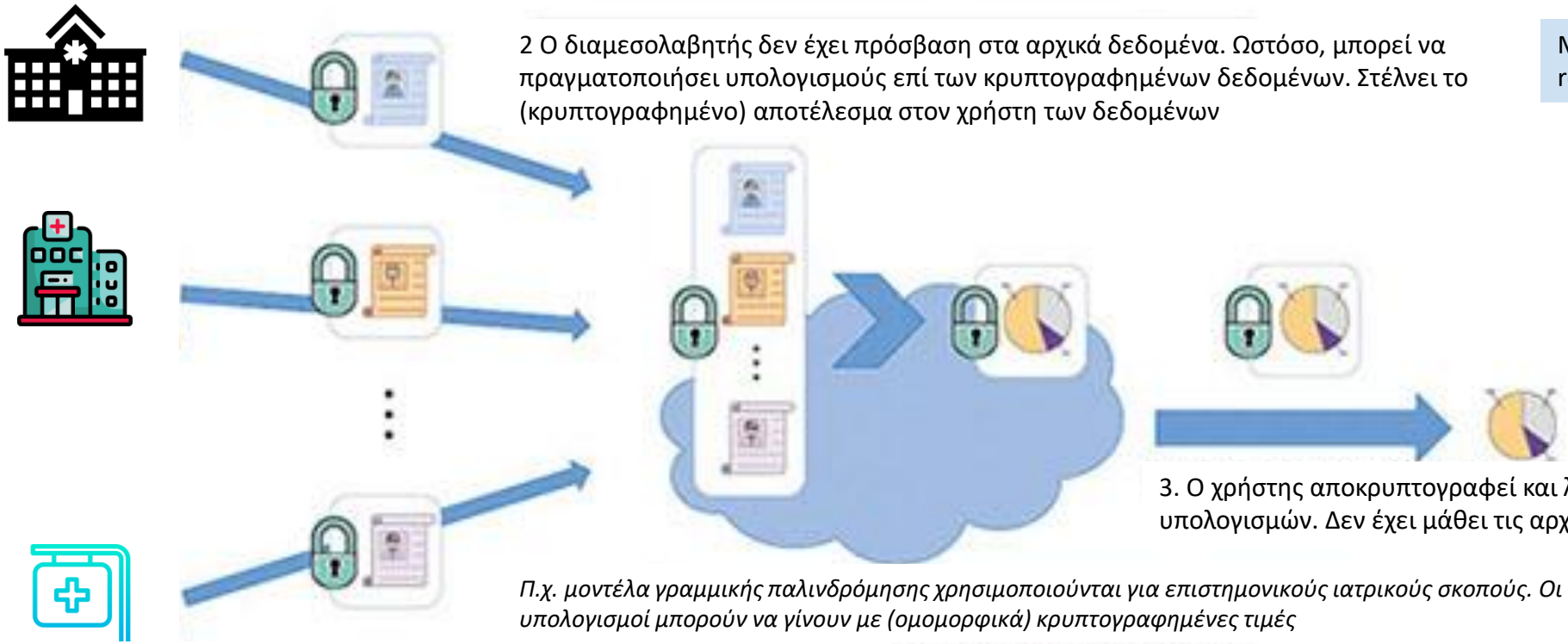
Π.χ. μοντέλα γραμμικής παλινδρόμησης χρησιμοποιούνται για επιστημονικούς ιατρικούς σκοπούς. Οι υπολογισμοί μπορούν να γίνουν με (ομομορφικά) κρυπτογραφημένες τιμές

1. Οι κάτοχοι δεδομένων στέλνουν κρυπτογραφημένα δεδομένα στον διαμεσολαβητή, τα οποία μόνο ο χρήστης μπορεί να αποκρυπτογραφήσει

Ομομορφική κρυπτογραφία (Homomorhic encryption)

Διαθέσιμες βιβλιοθήκες πλήρως ομομορφικής κρυπτογράφησης (π.χ. Zama - https://www.zama.ai/)

Μπορεί να συνδυστεί και με proxy re-encryption λειτουργία



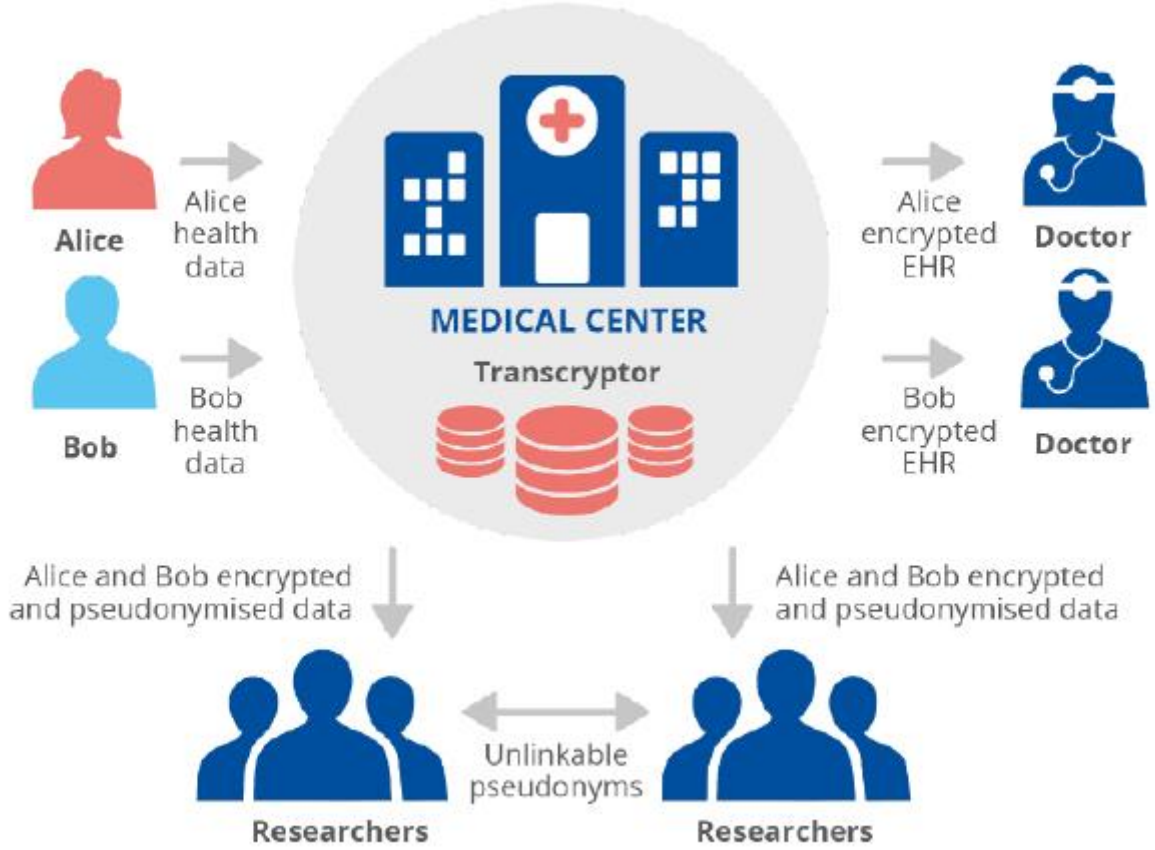
2 Ο διαμεσολαβητής δεν έχει πρόσβαση στα αρχικά δεδομένα. Ωστόσο, μπορεί να πραγματοποιήσει υπολογισμούς επί των κρυπτογραφημένων δεδομένων. Στέλνει το (κρυπτογραφημένο) αποτέλεσμα στον χρήστη των δεδομένων

3. Ο χρήστης αποκρυπτογραφεί και λαμβάνει το αποτέλεσμα των υπολογισμών. Δεν έχει μάθει τις αρχικές τιμές

Π.χ. μοντέλα γραμμικής παλινδρόμησης χρησιμοποιούνται για επιστημονικούς ιατρικούς σκοπούς. Οι υπολογισμοί μπορούν να γίνουν με (ομομορφικά) κρυπτογραφημένες τιμές

1. Οι κάτοχοι δεδομένων στέλνουν κρυπτογραφημένα δεδομένα στον διαμεσολαβητή, τα οποία μόνο ο χρήστης μπορεί να αποκρυπτογραφήσει

Πολυμορφική κρυπτογραφία (Polymorphic encryption)

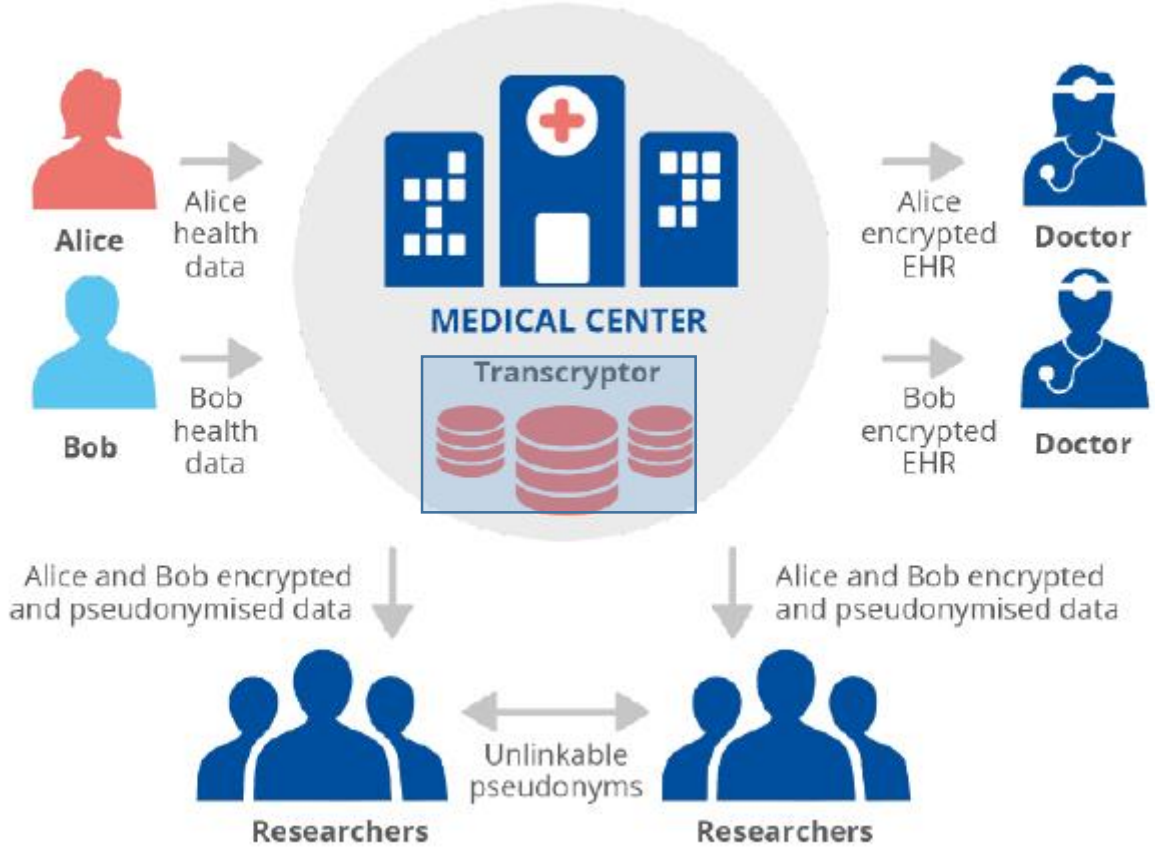


Πηγή: ENISA, Data Sharing Report, 2023

- Δεδομένα τηρούνται κρυπτογραφημένα, χωρίς να είναι εκ των προτέρων γνωστό ποιος θα αποκρυπτογραφήσει
- Εάν κάποιος χρήστης τα αιτηθεί, επανα-κρυπτογραφούνται κατάλληλα ώστε μόνο αυτός να μπορεί να τα αποκρυπτογραφήσει
- Παράλληλα ψευδωνυμοποιούνται, με τρόπο ώστε να προκύπτουν ασυσχέτιστα ψευδώνυμα μεταξύ διαφορετικών χρηστών
- Η οντότητα που επιτελεί αυτές τις λειτουργίες (transcryptor) δεν έχει πρόσβαση στα αρχικά δεδομένα (τις επιτελεί «τυφλά»)
- Ο transcryptor μπορεί να είναι μία ενδιάμεση οντότητα διαμεσολάβησης!
- Η τεχνική αυτή έχει ήδη υλοποιηθεί για συγκεκριμένη επιστημονική μελέτη

B. Gastel et. al., **Data Protection Using Polymorphic Pseudonymisation in a Large-Scale Parkinson's Disease Study,** 2021

Πολυμορφική κρυπτογραφία (Polymorphic encryption)

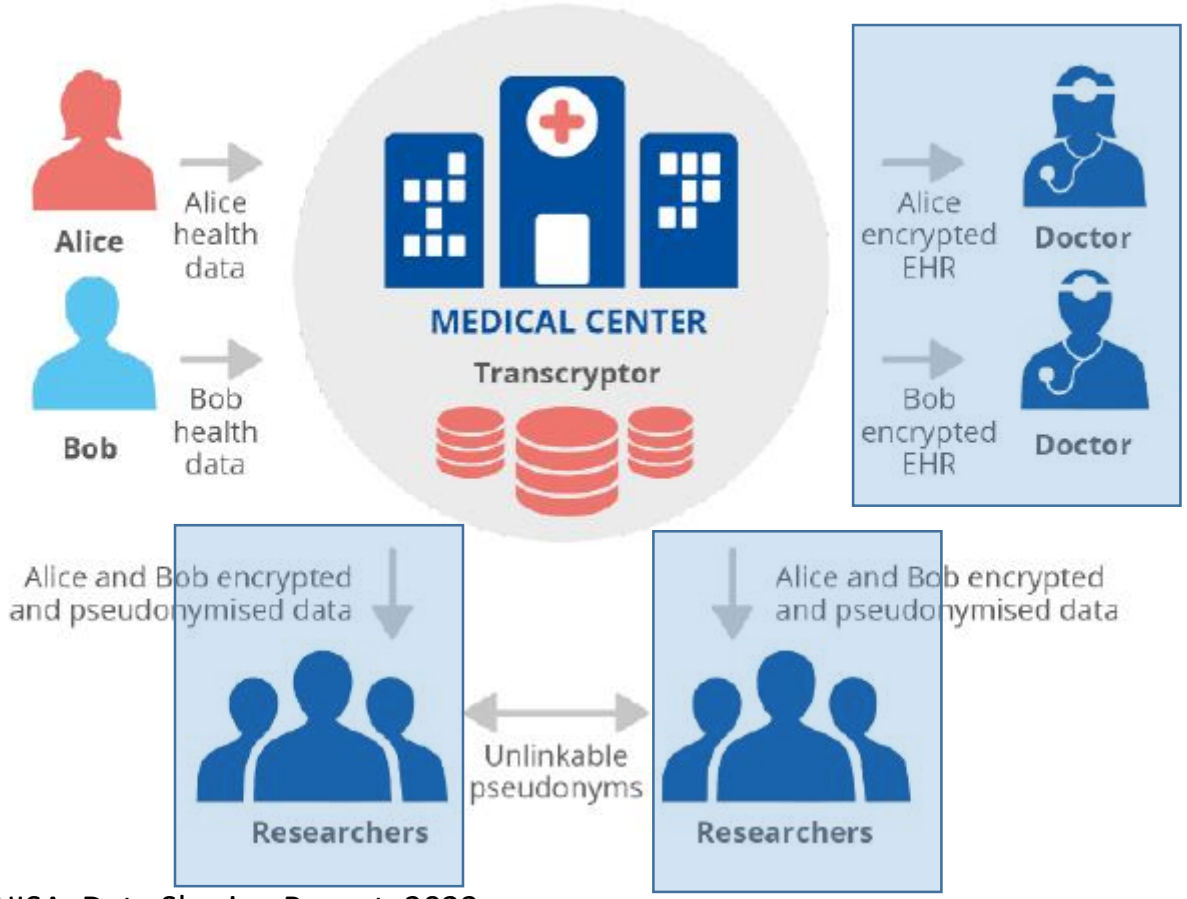


Πηγή: ENISA, Data Sharing Report, 2023

- Δεδομένα τηρούνται κρυπτογραφημένα, χωρίς να είναι εκ των προτέρων γνωστό ποιος θα αποκρυπτογραφήσει
- Εάν κάποιος χρήστης τα αιτηθεί, επανα-κρυπτογραφούνται κατάλληλα ώστε μόνο αυτός να μπορεί να τα αποκρυπτογραφήσει
- Παράλληλα ψευδωνυμοποιούνται, με τρόπο ώστε να προκύπτουν ασυσχέτιστα ψευδώνυμα μεταξύ διαφορετικών χρηστών
- Η οντότητα που επιτελεί αυτές τις λειτουργίες (transcryptor) δεν έχει πρόσβαση στα αρχικά δεδομένα (τις επιτελεί «τυφλά»)
- Ο transcryptor μπορεί να είναι μία ενδιάμεση οντότητα διαμεσολάβησης!
- Η τεχνική αυτή έχει ήδη υλοποιηθεί για συγκεκριμένη επιστημονική μελέτη

B. Gastel et. al., **Data Protection Using Polymorphic Pseudonymisation in a Large-Scale Parkinson's Disease Study,** 2021

Πολυμορφική κρυπτογραφία (Polymorphic encryption)

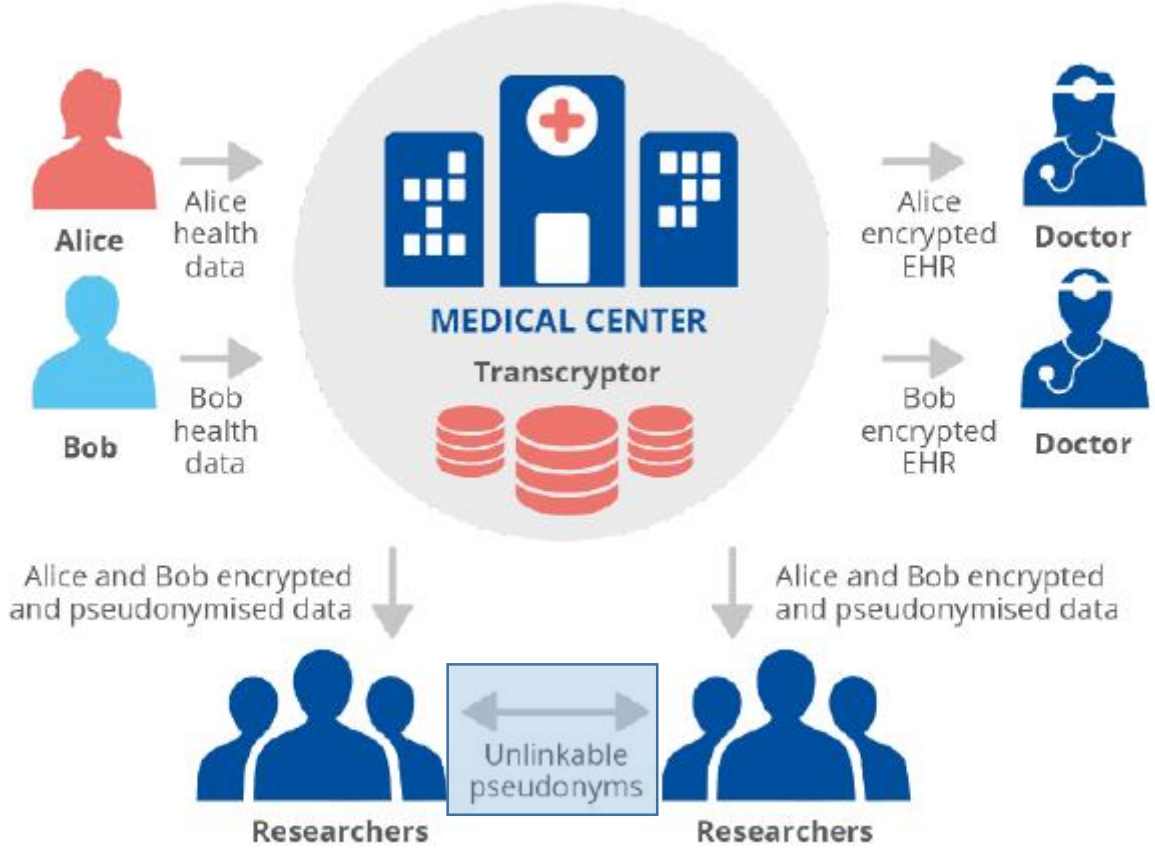


Πηγή: ENISA, Data Sharing Report, 2023

- Δεδομένα τηρούνται κρυπτογραφημένα, χωρίς να είναι εκ των προτέρων γνωστό ποιος θα αποκρυπτογραφήσει
- Εάν κάποιος χρήστης τα αιτηθεί, επανα-κρυπτογραφούνται κατάλληλα ώστε μόνο αυτός να μπορεί να τα αποκρυπτογραφήσει
- Παράλληλα ψευδωνυμοποιούνται, με τρόπο ώστε να προκύπτουν ασυσχέτιστα ψευδώνυμα μεταξύ διαφορετικών χρηστών
- Η οντότητα που επιτελεί αυτές τις λειτουργίες (transcryptor) δεν έχει πρόσβαση στα αρχικά δεδομένα (τις επιτελεί «τυφλά»)
- Ο transcryptor μπορεί να είναι μία ενδιάμεση οντότητα διαμεσολάβησης!
- Η τεχνική αυτή έχει ήδη υλοποιηθεί για συγκεκριμένη επιστημονική μελέτη

B. Gastel et. al., **Data Protection Using Polymorphic Pseudonymisation in a Large-Scale Parkinson's Disease Study,** 2021

Πολυμορφική κρυπτογραφία (Polymorphic encryption)

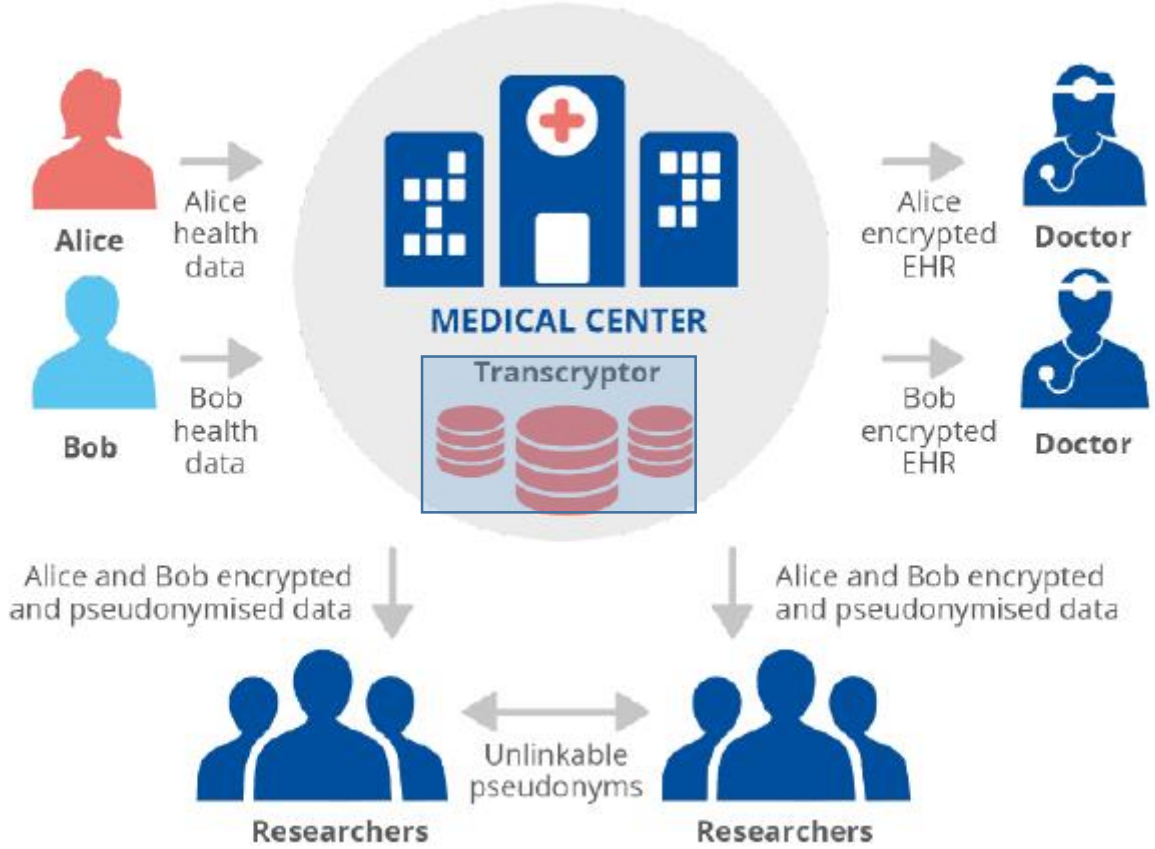


Πηγή: ENISA, Data Sharing Report, 2023

- Δεδομένα τηρούνται κρυπτογραφημένα, χωρίς να είναι εκ των προτέρων γνωστό ποιος θα αποκρυπτογραφήσει
- Εάν κάποιος χρήστης τα αιτηθεί, επανα-κρυπτογραφούνται κατάλληλα ώστε μόνο αυτός να μπορεί να τα αποκρυπτογραφήσει
- Παράλληλα ψευδωνυμοποιούνται, με τρόπο ώστε να προκύπτουν ασυσχέτιστα ψευδώνυμα μεταξύ διαφορετικών χρηστών
- Η οντότητα που επιτελεί αυτές τις λειτουργίες (transcryptor) δεν έχει πρόσβαση στα αρχικά δεδομένα (τις επιτελεί «τυφλά»)
- Ο transcryptor μπορεί να είναι μία ενδιάμεση οντότητα διαμεσολάβησης!
- Η τεχνική αυτή έχει ήδη υλοποιηθεί για συγκεκριμένη επιστημονική μελέτη

B. Gastel et. al., **Data Protection Using Polymorphic Pseudonymisation in a Large-Scale Parkinson's Disease Study,** 2021

Πολυμορφική κρυπτογραφία (Polymorphic encryption)

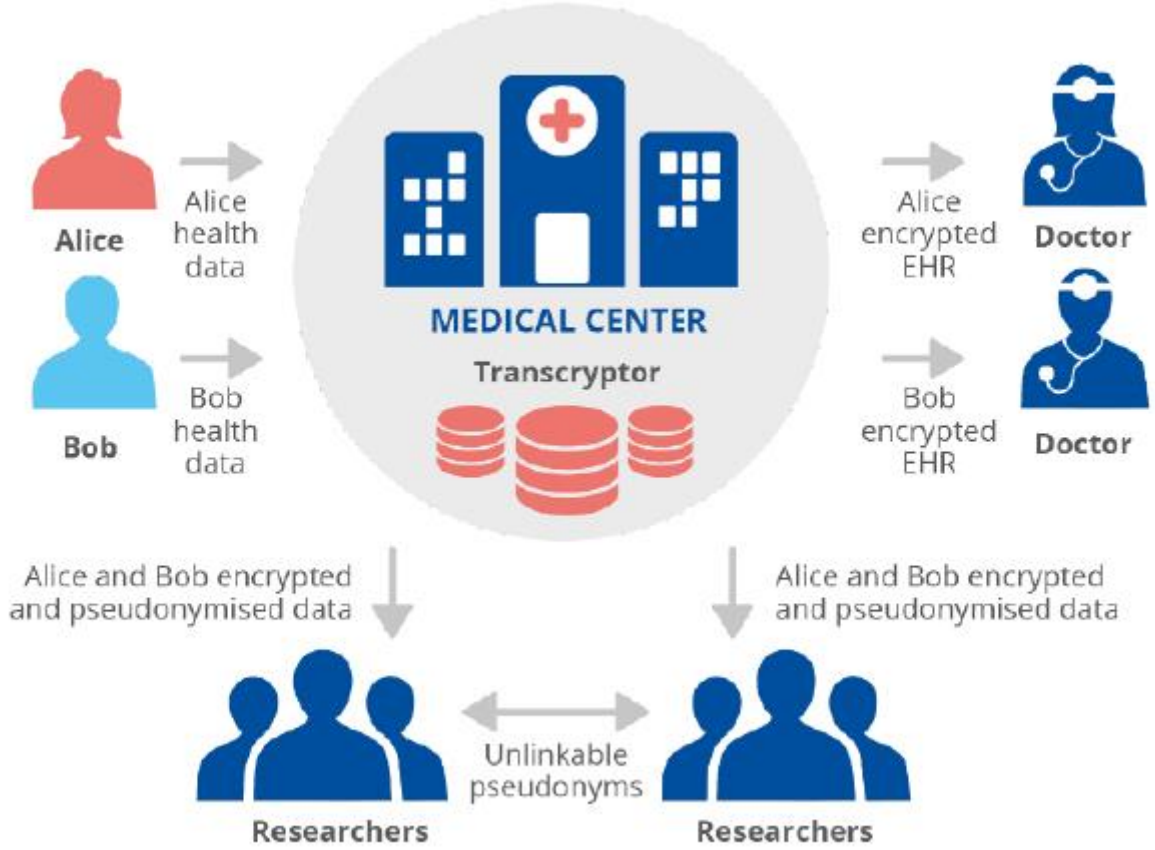


Πηγή: ENISA, Data Sharing Report, 2023

- Δεδομένα τηρούνται κρυπτογραφημένα, χωρίς να είναι εκ των προτέρων γνωστό ποιος θα αποκρυπτογραφήσει
- Εάν κάποιος χρήστης τα αιτηθεί, επανα-κρυπτογραφούνται κατάλληλα ώστε μόνο αυτός να μπορεί να τα αποκρυπτογραφήσει
- Παράλληλα ψευδωνυμοποιούνται, με τρόπο ώστε να προκύπτουν ασυσχέτιστα ψευδώνυμα μεταξύ διαφορετικών χρηστών
- Η οντότητα που επιτελεί αυτές τις λειτουργίες (transcryptor) δεν έχει πρόσβαση στα αρχικά δεδομένα (τις επιτελεί «τυφλά»)
- Ο transcryptor μπορεί να είναι μία ενδιάμεση οντότητα διαμεσολάβησης!
- Η τεχνική αυτή έχει ήδη υλοποιηθεί για συγκεκριμένη επιστημονική μελέτη

B. Gastel et. al., **Data Protection Using Polymorphic Pseudonymisation in a Large-Scale Parkinson's Disease Study,** 2021

Πολυμορφική κρυπτογραφία (Polymorphic encryption)

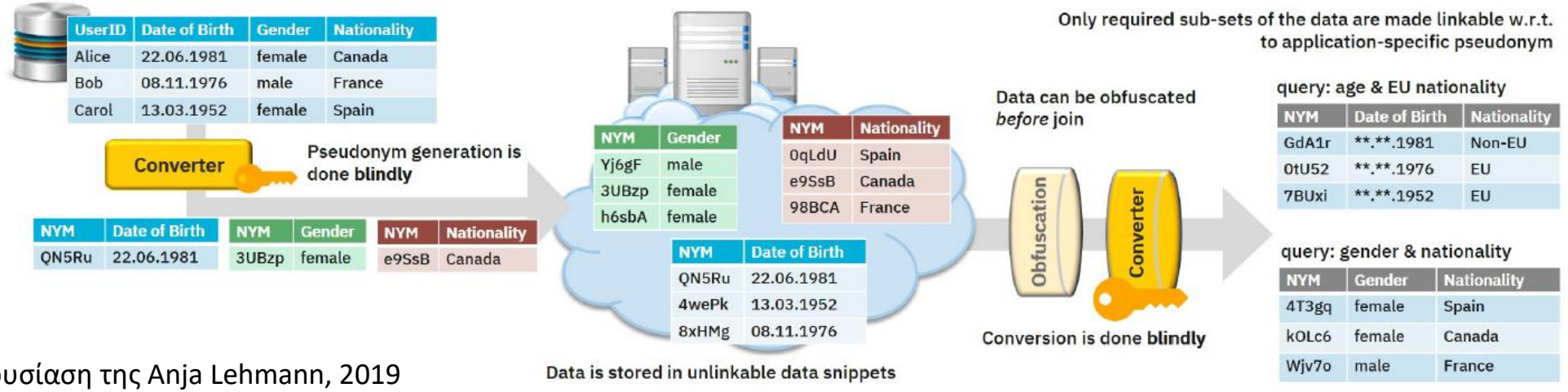


Πηγή: ENISA, Data Sharing Report, 2023

- Δεδομένα τηρούνται κρυπτογραφημένα, χωρίς να είναι εκ των προτέρων γνωστό ποιος θα αποκρυπτογραφήσει
- Εάν κάποιος χρήστης τα αιτηθεί, επανα-κρυπτογραφούνται κατάλληλα ώστε μόνο αυτός να μπορεί να τα αποκρυπτογραφήσει
- Παράλληλα ψευδωνυμοποιούνται, με τρόπο ώστε να προκύπτουν ασυσχέτιστα ψευδώνυμα μεταξύ διαφορετικών χρηστών
- Η οντότητα που επιτελεί αυτές τις λειτουργίες (transcryptor) δεν έχει πρόσβαση στα αρχικά δεδομένα (τις επιτελεί «τυφλά»)
- Ο transcryptor μπορεί να είναι μία ενδιάμεση οντότητα διαμεσολάβησης!
- Η τεχνική αυτή έχει ήδη υλοποιηθεί για συγκεκριμένη επιστημονική μελέτη

  B. Gastel et. al., **Data Protection Using Polymorphic Pseudonymisation in a Large-Scale Parkinson's Disease Study,** 2021

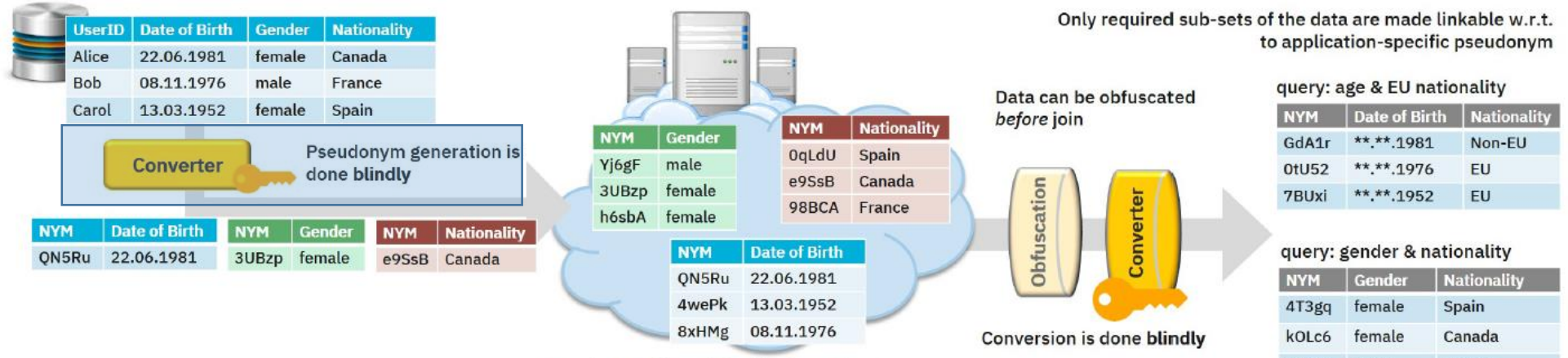
Ψευδωνυμοποίηση χωρίς γνώση (Oblivious pseudonymisation)



Πηγή: Παρουσίαση της Anja Lehmann, 2019

- Η οντότητα που παράγει τα αρχικά ψευδώνυμα (converter) δεν μαθαίνει ποτέ τα αρχικά αναγνωριστικά
- Η οντότητα διαμεσολάβησης τηρεί μόνο ψευδωνυμοποιημένα δεδομένα, με τρόπο που δεν επιτρέπει αναγνώριση χρηστών. Δεν μαθαίνει ποτέ τα αρχικά αναγνωριστικά
- Τα δεδομένα μπορούν να συνδυαστούν και να ψευδωνυμοποιηθούν εκ νέου, για πολλούς διαφορετικούς χρήστες, παράγοντας «ασυσχέτιστα» ψευδώνυμα για τον κάθε χρήστη. Η οντότητα διαμεσολάβησης σε κανένα σημείο της διαδικασίας δεν μαθαίνει τα αρχικά αναγνωριστικά.

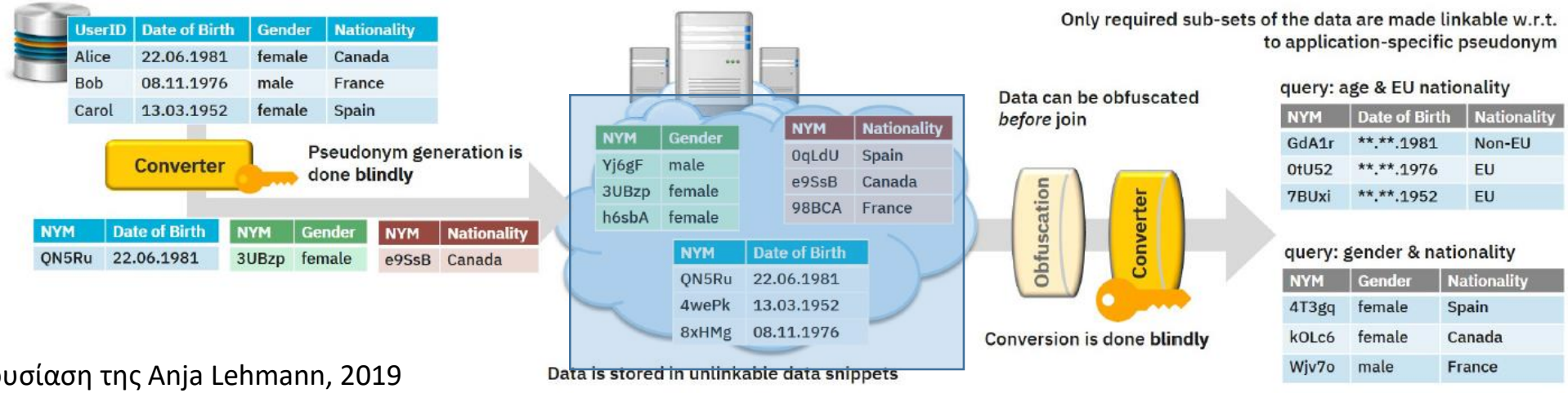
Ψευδωνυμοποίηση χωρίς γνώση (Oblivious pseudonymisation)



Πηγή: Παρουσίαση της Anja Lehmann, 2019

- Η οντότητα που παράγει τα αρχικά ψευδώνυμα (converter) δεν μαθαίνει ποτέ τα αρχικά αναγνωριστικά
- Η οντότητα διαμεσολάβησης τηρεί μόνο ψευδωνυμοποιημένα δεδομένα, με τρόπο που δεν επιτρέπει αναγνώριση χρηστών. Δεν μαθαίνει ποτέ τα αρχικά αναγνωριστικά
- Τα δεδομένα μπορούν να συνδυαστούν και να ψευδωνυμοποιηθούν εκ νέου, για πολλούς διαφορετικούς χρήστες, παράγοντας «ασυσχέτιστα» ψευδώνυμα για τον κάθε χρήστη. Η οντότητα διαμεσολάβησης σε κανένα σημείο της διαδικασίας δεν μαθαίνει τα αρχικά αναγνωριστικά.

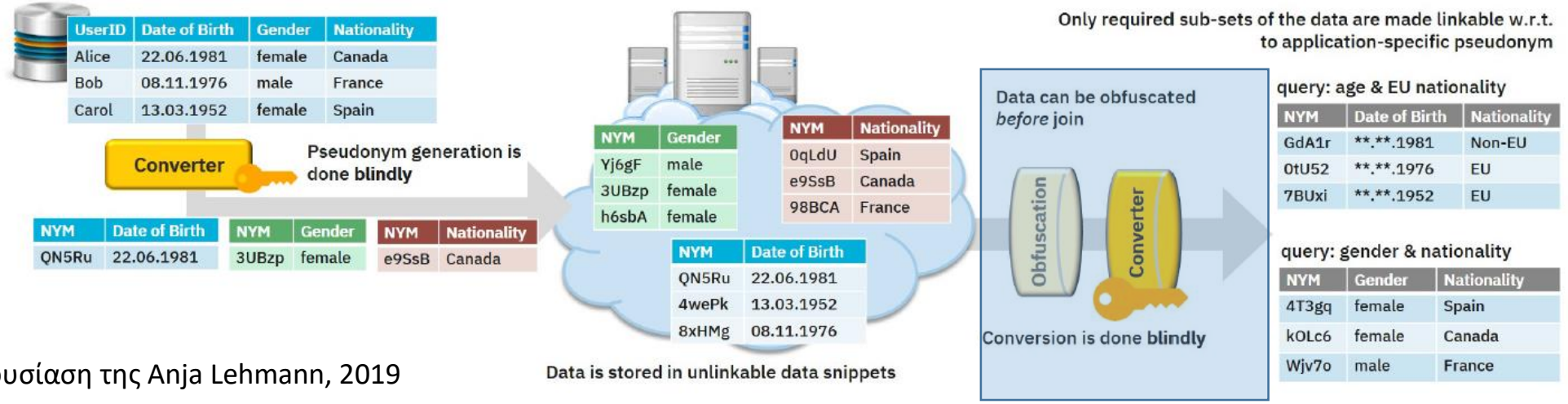
Ψευδωνυμοποίηση χωρίς γνώση (Oblivious pseudonymisation)



Πηγή: Παρουσίαση της Anja Lehmann, 2019

- Η οντότητα που παράγει τα αρχικά ψευδώνυμα (converter) δεν μαθαίνει ποτέ τα αρχικά αναγνωριστικά
- Η οντότητα διαμεσολάβησης τηρεί μόνο ψευδωνυμοποιημένα δεδομένα, με τρόπο που δεν επιτρέπει αναγνώριση χρηστών. Δεν μαθαίνει ποτέ τα αρχικά αναγνωριστικά
- Τα δεδομένα μπορούν να συνδυαστούν και να ψευδωνυμοποιηθούν εκ νέου, για πολλούς διαφορετικούς χρήστες, παράγοντας «ασυσχέτιστα» ψευδώνυμα για τον κάθε χρήστη. Η οντότητα διαμεσολάβησης σε κανένα σημείο της διαδικασίας δεν μαθαίνει τα αρχικά αναγνωριστικά.

Ψευδωνυμοποίηση χωρίς γνώση (Oblivious pseudonymisation)



Πηγή: Παρουσίαση της Anja Lehmann, 2019

- Η οντότητα που παράγει τα αρχικά ψευδώνυμα (converter) δεν μαθαίνει ποτέ τα αρχικά αναγνωριστικά
- Η οντότητα διαμεσολάβησης τηρεί μόνο ψευδωνυμοποιημένα δεδομένα, με τρόπο που δεν επιτρέπει αναγνώριση χρηστών. Δεν μαθαίνει ποτέ τα αρχικά αναγνωριστικά
- Τα δεδομένα μπορούν να συνδυαστούν και να ψευδωνυμοποιηθούν εκ νέου, για πολλούς διαφορετικούς χρήστες, παράγοντας «ασυσχέτιστα» ψευδώνυμα για τον κάθε χρήστη. Η οντότητα διαμεσολάβησης σε κανένα σημείο της διαδικασίας δεν μαθαίνει τα αρχικά αναγνωριστικά.

Συμπεράσματα - Σκέψεις

- Οι οντότητες διαμεσολάβησης μπορούν να συλλέγουν μεγάλο όγκο (ευαίσθητων) προσωπικών δεδομένων
  - Είτε πρόκειται για υπηρεσίες διαμεσολάβησης κατά την DGA είτε για άλλους «ενισχυμένων διασφαλίσεων» φορείς όπως ο φορέας πρόσβασης δεδομένων υγείας
- Ένα ασφαλές περιβάλλον επεξεργασίας είναι απαραίτητο, όμως… πότε το έχουμε πραγματικά;
  - Κίνδυνοι από αυτό καθ’ αυτό το γεγονός ότι οι οντότητες αυτές τηρούν τα δεδομένα
  - Κίνδυνοι που επιτείνονται αν υπεισέλθει και εκτελών την επεξεργασία
- Προηγμένες κρυπτογραφικές τεχνικές φαίνεται να δίνουν απαντήσεις σε (κάποιες) σχεδιαστικές απαιτήσεις
  - Δεν είναι πανάκεια μεν, αλλά πρέπει να λαμβάνονται υπόψη, βάσει και των κινδύνων
  - Ρεαλιστική η υλοποίησή τους
- Με ποιον τρόπο θα δρομολογήσουν οι αρμόδιοι φορείς την υιοθέτηση τέτοιων τεχνικών;
  - Ανάγκη κατάρτισης προτύπων;

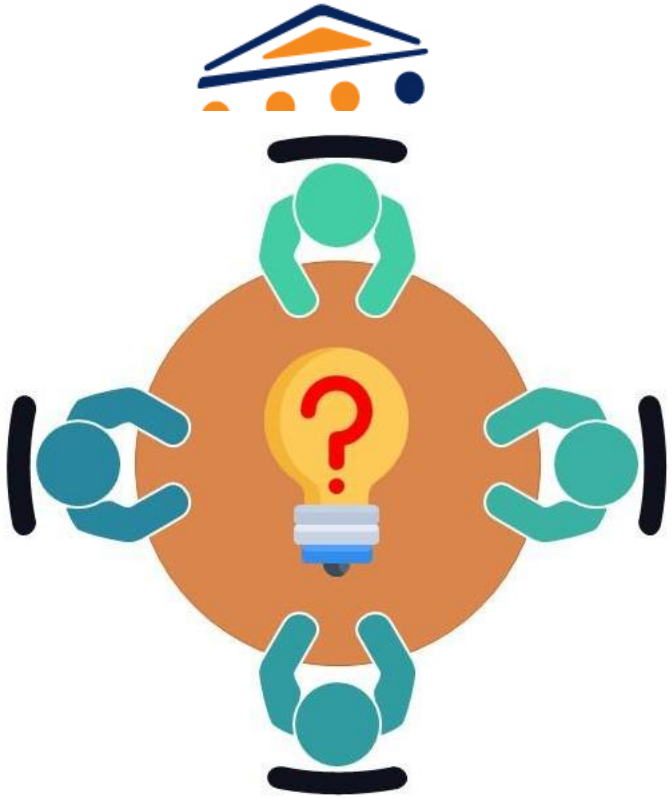
Χρήσιμες πηγές

- ENISA, “Engineering personal data protection in EU Data Spaces”, 2024.
- ENISA, “Engineering personal data sharing – Emerging use cases and technologies”, 2023.
- M.R. Albrecht, A. Davidson, A. Deo, D. Gardham, “Crypto Dark Matter on the Torus: Oblivious PRFs from shallow PRFs and TFHE”. EUROCRYPT 2024.
- A. Lehmann, “ScrambleDB: Oblivious (Chameleon) Pseudonymization-as-a-Service“, Proc. of PETs Symposium, 2019
- Eric Verheul, Bart Jacobs, Carlo Meijer, Mireille Hildebrandt, and Joeri de Ruiter, “Polymorphic encryption and pseudonymisation”, Cryptology ePrint Archive, Report 2016/411, 2016.
- B. Gastel, “Data Protection Using Polymorphic Pseudonymisation in a Large-Scale Parkinson’s Disease Study”, 2021
- K. Limniotis, “Cryptography as the means to protect fundamental human rights‘’, Cryptography, vol. 5, no. 4, 2021.

«Cryptography is about the right to privacy, freedom of speech, freedom of political association, freedom of the press, freedom from unreasonable search and seizure, freedom to be left alone».

Phil Zimmermann

Σας ευχαριστώ για την προσοχή σας!



Συζήτηση / Ερωτήσεις;