

ΟΔΗΓΟΣ ΔΙΑΧΕΙΡΙΣΗΣ ΚΑΙ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΟΥ ΣΥΛΛΕΓΟΝΤΑΙ ΓΙΑ ΕΡΕΥΝΗΤΙΚΟΥΣ ΣΚΟΠΟΥΣ

1. Εισαγωγή

Ο παρών οδηγός έχει ως στόχο την παροχή βοήθειας στο ερευνητικό προσωπικό και τους/τις φοιτητές/φοιτήτριες, των οποίων η έρευνα διενεργείται με συμμετοχή ανθρώπων και περιλαμβάνει συλλογή δεδομένων προσωπικού χαρακτήρα, όπως αυτά ορίζονται στον Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR).

Για πληροφορίες σχετικά με την Προστασία Δεδομένων Προσωπικού Χαρακτήρα που συλλέγονται για ερευνητικούς σκοπούς, ανατρέξτε στον Κώδικα Ηθικής και Δεοντολογίας της Επιστημονικής Έρευνας του Πανεπιστημίου Μακεδονίας. Μπορείτε, ακόμα, να επικοινωνήσετε με τον/την Υπεύθυνο/η Προστασίας Δεδομένων (DPO) του Πανεπιστημίου Μακεδονίας στην ηλεκτρονική διεύθυνση: dpo@uom.edu.gr.

2. Συγκατάθεση κατόπιν ενημέρωσης

Πριν την εκκίνηση της εκπόνησης μιας τέτοιας έρευνας, οι συμμετέχοντες/ουσες πρέπει να είναι πλήρως ενημερωμένοι/ες για τον τρόπο διαχείρισης των δεδομένων τους από τον/την ερευνητή/τρια. Για παράδειγμα, πρέπει να είναι σαφές:

- ποια δεδομένα συλλέγονται (π.χ. αναφορά σε απλά ή ευαίσθητα προσωπικά δεδομένα)
- πώς θα συλλεχθούν/ μεταφερθούν/υποστούν επεξεργασία μετά τη διενέργεια συνεντεύξεων
- πώς θα αποχαρακτηριστούν ως προσωπικά (εάν εφαρμόζεται τεχνική ανωνυμοποίησης)
- ποιος θα έχει πρόσβαση σε αυτά
- πού θα αποθηκευτούν (και για πόσο καιρό)
- ποια η πιθανή χρήση των δεδομένων (π.χ. κοινή χρήση με άλλους, δημοσίευση, χρήση για μελλοντική έρευνα)

Οι ερευνητές/τριες πρέπει να αποφεύγουν να δίνουν υποσχέσεις, που ενδέχεται να είναι δύσκολο να τηρηθούν, π.χ., ότι μόνο ο/η επιστημονικά υπεύθυνος/η θα έχει πρόσβαση στα δεδομένα, ή ότι θα καταστραφούν με την ολοκλήρωση του έργου. Είναι πιθανό ότι μέλη άλλων ερευνητικών ομάδων και στελέχη τεχνικής/πληροφορικής υποστήριξης θα έχουν πρόσβαση στα ερευνητικά δεδομένα, επομένως, κρίνεται σκόπιμο να αποφευχθεί σχετική μνεία, εκτός εάν υπάρχουν σοβαροί λόγοι για κάτι τέτοιο.

Ως μέγιστη περίοδος διατήρησης των ερευνητικών δεδομένων έχει καθοριστεί αυτή των πέντε (5) ετών μετά την ολοκλήρωση της έρευνας, η οποία υπολογίζεται με την κατάθεση ή υποβολή του ερευνητικού έργου στον αρμόδιο ερευνητικό ή ακαδημαϊκό φορέα, όπως κάθε φορά ορίζεται.¹

3. Ασφαλής συλλογή και αποθήκευση δεδομένων

Κατά τη συλλογή δεδομένων, οι φορητές συσκευές που περιέχουν δεδομένα του Πανεπιστημίου πρέπει να προστατεύονται με κρυπτογράφηση εφόσον κρίνεται ότι η όποια μορφής διαρροή ή απώλειά τους θα δημιουργήσει πρόβλημα. Το Τμήμα Στατιστικής, Μηχανοργάνωσης και Πληροφορικής διαθέτει μία cloud υπηρεσία για την αποθήκευση δεδομένων έρευνας σε επίπεδο χρήστη η οποία κρυπτογραφεί τα αρχεία κατά την αποθήκευσή τους. Η διακίνηση των δεδομένων από και προς την υπηρεσία γίνεται με κρυπτογράφηση ενώ η αποθήκευσή τους πραγματοποιείται σε διακομιστές που στεγάζονται εντός του Ιδρύματος με υλοποίηση που περιλαμβάνει λογισμικά ανοιχτού κώδικα. Η χωρητικότητα του κάθε λογαριασμού ανέρχεται στα 5GB και η πρόσβαση υλοποιείται με τον ιδρυματικό λογαριασμό των χρηστών (uRegister).

Επικοινωνήστε με το ΚΥΔ του Πανεπιστημίου Μακεδονίας στην ηλεκτρονική διεύθυνση: help@uom.edu.gr για συμβουλές σχετικά με τις κατάλληλες πλατφόρμες αποθήκευσης και κοινής χρήσης δεδομένων μεγάλου όγκου.

Επίσης, είναι γενικά καλή πρακτική να χρησιμοποιείτε έναν κωδικό αριθμό για την επισήμανση όλων των έντυπων, υλικών (π.χ. ηχογραφήσεις, CD) και ηλεκτρονικών αρχείων (ακόμη και συζητήσεων μέσω email), με το κλειδί των κωδικών αυτών να αποθηκεύεται σε διαφορετικό σημείο.

Τα δεδομένα προσωπικού χαρακτήρα πρέπει να μεταφέρονται και στη συνέχεια να αποθηκεύονται με τη μεγαλύτερη δυνατή ασφάλεια, είτε σε ασφαλείς φυσικούς χώρους (κλειδωμένο δωμάτιο, έπιπλα γραφείου που κλειδώνουν, κ.ο.κ.), είτε σε κρυπτογραφημένα αρχεία σε συστήματα αποθήκευσης, όπως το Google Drive

Προτείνεται ο ερευνητικός σας σχεδιασμός να περιλαμβάνει το πλαίσιο σύμφωνα με το οποίο όλα τα παραπάνω επιτυγχάνονται.

4. Ανωνυμοποίηση προσωπικών δεδομένων

Γενικά, η διαχείριση και η χρήση των δεδομένων πρέπει να γίνεται με τέτοιο τρόπο, ώστε να προστατεύεται η εμπιστευτικότητα. Διευκρινίζεται ότι οι αρχές της προστασίας δεδομένων δεν εφαρμόζονται σε ανώνυμες πληροφορίες, δηλαδή πληροφορίες που δεν σχετίζονται με ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο, ή σε δεδομένα προσωπικού χαρακτήρα, που έχουν καταστεί ανώνυμα κατά τρόπο ώστε η ταυτότητα του υποκειμένου των δεδομένων να μην μπορεί, ή να μην μπορεί πλέον, να εξακριβωθεί. Αυτό είναι ιδιαίτερα σημαντικό στις περιπτώσεις δεδομένων, όπου ο/η συμμετέχων/ουσα δεν επιθυμεί τη γνωστοποίηση των αποτελεσμάτων που προέκυψαν από την έρευνα σε άλλους. Η ανωνυμοποίηση είναι η μία επιλογή (η άλλη είναι ο περιορισμός της πρόσβασης στα δεδομένα) και πρέπει να πραγματοποιείται σύμφωνα με τις απαιτήσεις του έργου και τις προσδοκίες των συμμετεχόντων/ουσών. Σε κάθε περίπτωση, τα πλεονεκτήματα και τα μειονεκτήματα της ανωνυμοποίησης πρέπει να εξετάζονται σε σχέση με την ασφάλεια και την ποιότητα των δεδομένων που πρόκειται να συλλεχθούν.

5. Επίπεδα ανωνυμοποίησης

Το επίπεδο ανωνυμοποίησης εξαρτάται από την έρευνα. Το σημαντικό είναι ότι στην περίπτωση, κατά την οποία τα δεδομένα δεν δύναται να ανωνυμοποιηθούν απολύτως, οι συμμετέχοντες/ουσες πρέπει να το γνωρίζουν και να δίνουν τη συγκατάθεσή τους

¹ Ανατρέξτε στην ενότητα «Διατήρηση δεδομένων» για περισσότερες πληροφορίες. (Δείτε, επίσης, τα έγγραφα της Ε.Η.Δ.Ε. για την ενημέρωση των συμμετεχόντων/ουσών).

σχετικά. Όταν σχεδιάζετε την ανωνυμοποίηση, εξετάστε με ποιους τρόπους είναι δυνατό να ταυτοποιηθούν οι συμμετέχοντες/ουσες (δηλαδή, εάν ένας συνδυασμός λεπτομερειών θα μπορούσε να επιτρέψει την ταυτοποίηση του ατόμου, ή εάν το μέγεθος του δείγματος είναι σχετικά μικρό) και ποιες είναι οι πιθανές συνέπειες αυτής της ταυτοποίησης. Ένας συνδυασμός δεδομένων θα μπορούσε να επιτρέψει την ταυτοποίηση ενός ατόμου. Ο στόχος είναι να μεγιστοποιηθεί η ασφάλεια των δεδομένων και να διασφαλιστεί το απόρρητό τους, ελαχιστοποιώντας ταυτόχρονα τον κίνδυνο απώλειας δεδομένων ή παραβίασής τους. Όταν τα δεδομένα πρόκειται να αρχειοθετηθούν για επιστημονική επαναχρησιμοποίηση, οι συμμετέχοντες/ουσες πρέπει να ενημερωθούν εκ των προτέρων και τα δεδομένα πρέπει να είναι ανωνυμοποιημένα, σε τέτοιο επίπεδο που να διασφαλίζεται ότι οι νέοι χρήστες δεν θα μπορούν να ταυτοποιήσουν τους/τις συμμετέχοντες/ουσες. Τα οπτικοακουστικά σύνολα δεδομένων, που δεν μπορούν εύκολα να ανωνυμοποιηθούν, αρχειοθετούνται για επιστημονική επαναχρησιμοποίηση μόνο κατόπιν ρητής συγκατάθεσης των συμμετεχόντων/ουσών.

Άλλα άμεσα αναγνωριστικά στοιχεία, όπως ταχυδρομικοί κώδικες, αριθμοί τηλεφώνου και ημερομηνίες γέννησης πρέπει, όπου είναι αυτό δυνατόν, να αφαιρούνται από τα δεδομένα μετά την ολοκλήρωση της αρχικής έρευνας. Η διατήρησή τους δικαιολογείται μόνο όταν αυτά τα άμεσα αναγνωριστικά είναι απαραίτητα για την ανάλυση των δεδομένων και οι συμμετέχοντες/ουσες έχουν δώσει εκ των προτέρων τη συγκατάθεσή τους.

6. Πρόσβαση σε δεδομένα

Η πρόσβαση στα ερευνητικά δεδομένα επιτρέπεται σύμφωνα με την κείμενη νομοθεσία και τις υποχρεώσεις του Πανεπιστημίου Μακεδονίας ως υπευθύνου επεξεργασίας δεδομένων. Το βασικό σημείο είναι η εκ των προτέρων ενημέρωση των συμμετεχόντων/ουσών.

7. Αρχειοθέτηση/ Αποθήκευση δεδομένων (και εκ νέου χρήση σε επιστημονική έρευνα)

Δεδομένου ότι πολλοί φορείς χρηματοδότησης ενθαρρύνουν την αρχειοθέτηση των δεδομένων για επιστημονική επαναχρησιμοποίηση, αυτό πρέπει να αποφασίζεται στο αρχικό στάδιο του σχεδιασμού. Προτιμότερη είναι η αναφορά στην ανωνυμοποίηση των δεδομένων (π.χ. αφαιρώντας όλες τις προσωπικές πληροφορίες που θα μπορούσαν να ταυτοποιήσουν άμεσα ένα άτομο) και στην προστασία της εμπιστευτικότητας.

8. Κοινή χρήση δεδομένων

Τα ερευνητικά δεδομένα μπορούν να χρησιμοποιούνται ή να κοινοποιούνται για ερευνητικούς, μόνο, σκοπούς και πρέπει να ζητείται η συγκατάθεση των συμμετεχόντων/ουσών για την κοινή τους χρήση. Εάν οι ερευνητές/τριες πρόκειται να προχωρήσουν σε κοινή χρήση ή να χρησιμοποιήσουν άλλους παρόχους υπηρεσιών για τη συλλογή ή επεξεργασία προσωπικών δεδομένων (τα άλλα μέρη εκτελούν την επεξεργασία δεδομένων), πρέπει να συμβουλευτούν την Ε.Η.Δ.Ε. και τον Ε.Λ.Κ.Ε., έτσι ώστε να συναφθεί ένα συμφωνητικό μεταξύ αυτών των παρόχων και να διασφαλιστεί, με αυτόν τον τρόπο, η επεξεργασία σύμφωνα με τις νομικές υποχρεώσεις του Πανεπιστημίου Μακεδονίας. Για περισσότερες πληροφορίες, είναι σκόπιμο να επικοινωνήσετε με τον/την Υπεύθυνο/η Προστασίας Δεδομένων (DPO) του Πανεπιστημίου Μακεδονίας.

9. Έμμεσα αναγνωριστικά / πληροφορίες ιστορικού

Τα παρακάτω αποτελούν παραδείγματα προσωπικών δεδομένων (προσωπικά δεδομένα είναι και πληροφορίες που μπορούν έμμεσα, σε συνδυασμό με άλλες πληροφορίες, να ταυτοποιήσουν ένα φυσικό πρόσωπο): ενδεικτικά, φύλο, ηλικία, εκπαίδευση, επάγγελμα, οικονομική δραστηριότητα, κοινωνικοοικονομική κατάσταση, σύνθεση νοικοκυριού, εισόδημα, οικογενειακή κατάσταση, μητρική γλώσσα, εθνικότητα, θρησκεία, σεξουαλικός προσανατολισμός, ιατρικά δεδομένα, χώρος/ οργανισμός εργασίας, εκπαιδευτικό ίδρυμα, και γεωγραφικά αναγνωριστικά. Τα γεωγραφικά αναγνωριστικά περιλαμβάνουν, για παράδειγμα, τον ταχυδρομικό κώδικα, το προάστιο, τον δήμο, την επαρχία, την περιοχή και τον τόπο όπου μεγάλωσε ο/η ερωτώμενος/η.

Τα (έμμεσα) αναγνωριστικά, όταν συνδέονται με π.χ. γεωγραφικές τοποθεσίες, διευθύνσεις IP, ταχυδρομικούς κώδικες, ονόματα ιδρυμάτων κ.λπ., ενδέχεται να καταστήσουν δυνατή την ταυτοποίηση των συμμετεχόντων/ουσών. Όσο μεγαλύτερος είναι ο αριθμός των έμμεσων αναγνωριστικών τόσο μεγαλύτερος ο κίνδυνος ταυτοποίησης. Ως εκ τούτου, οι ερευνητές/τριες πρέπει να ελαχιστοποιούν τη συλλογή δεδομένων και να προσδιορίζουν τον τρόπο, με τον οποίο θα μετριάζουν τον κίνδυνο ταυτοποίησης των υποκειμένων, έτσι ώστε να είναι η έρευνα σύμφωνη με τους κανόνες ηθικής και δεοντολογίας.

Οι απαντήσεις σε ερωτήσεις ανοιχτού τύπου περιέχουν μερικές φορές αναγνωριστικά που συνδέονται με τους/τις ερωτώμενους/όμενες ή άλλα άτομα, όπως το όνομα ή το επάγγελμα συζύγου. Ο κίνδυνος ταυτοποίησης πρέπει να αξιολογείται κατά περίπτωση και να λαμβάνονται αποφάσεις σχετικά με την αναγκαιότητα επανακωδικοποίησης (re-coding), χρήσης ψευδώνυμων ή διαγραφής κάποιων από τις συλλεχθείσες πληροφορίες για τη διατήρηση της εμπιστευτικότητας.

Το επίπεδο ανωνυμοποίησης, που απαιτείται, εξαρτάται από το εάν ένας συνδυασμός έμμεσων αναγνωριστικών μπορεί να οδηγήσει στην ταυτοποίηση ενός/μίας ερωτώμενου/νης. Οι μεταβλητές μπορούν να επανακωδικοποιηθούν (recoded) ή να διαγραφούν προκειμένου να ~~να~~ αποφευχθεί η ταυτοποίηση: για παράδειγμα, αντί για ημερομηνία γέννησης, θα μπορούσε να χρησιμοποιηθεί η ηλικία· αντί για τον πλήρη ταχυδρομικό κώδικα, θα μπορούσαν να χρησιμοποιηθούν μόνο οι τρεις πρώτοι χαρακτήρες.

10. Τεχνικές και ζητήματα ανωνυμοποίησης/ ψευδωνυμοποίησης

Η αλλαγή των ονομάτων σε κωδικούς ή ψευδώνυμα είναι η πιο δημοφιλής τεχνική ανωνυμοποίησης που χρησιμοποιείται για τη συλλογή δεδομένων ποιοτικών ερευνών. Μια καλή πρακτική είναι η αντικατάσταση των ονομάτων των ερευνητικών υποκειμένων από ψευδώνυμα αμέσως μετά την αποθήκευση και μεταγραφή των δεδομένων. Η πληκτρολόγηση ενός ειδικού χαρακτήρα μπροστά από όλα τα ονόματα στο αρχικό στάδιο μεταγραφής διευκολύνει την ανωνυμοποίηση, αφού όλα τα ονόματα εντοπίζονται εύκολα.

Μια διαγνωσθείσα σοβαρή ασθένεια μπορεί να μετατραπεί σε έναν άλλο, παρόμοιο τύπο της ασθένειας, εάν αυτό δεν μειώνει υπερβολικά τη χρησιμότητα των δεδομένων. Μια άλλη επιλογή είναι η κατηγοριοποίηση των πληροφοριών με τον ίδιο τρόπο

όπως στα ποσοτικά δεδομένα. Για παράδειγμα, το «AIDS» θα μπορούσε να αλλάξει σε «σοβαρή μακροχρόνια ασθένεια» και στη συνέχεια να αναφέρεται ως «ασθένεια», υπό την προϋπόθεση ότι ο αναγνώστης θα μπορεί να συμπεράνει ότι η «ασθένεια» αναφέρεται στη «σοβαρή μακροχρόνια ασθένεια» που αναφέρθηκε στην αρχή.

Γενικά στις ποιοτικές έρευνες, η πλήρης ανωνυμοποίηση των προσωπικών δεδομένων χωρίς ταυτόχρονη μείωση της αξίας τους αποτελεί μια δύσκολη εργασία. Αποφασίστε εάν θα χρησιμοποιήσετε πλήρη ανωνυμοποίηση ή ψευδωνυμοποίηση, τόσο στην αίτησή σας προς την Ε.Η.Δ.Ε., όσο και στις πληροφορίες για τους/τις συμμετέχοντες/ουσες και στα έντυπα συγκατάθεσης. Στις περισσότερες περιπτώσεις, η ψευδωνυμοποίηση είναι η πιο πρακτική και ρεαλιστική επιλογή, αν και η πλήρης ανωνυμοποίηση μπορεί να είναι απαραίτητη, όταν ο κίνδυνος αναγνώρισης των συμμετεχόντων/ουσών (και των ερευνητών/τριών) είναι υπαρκτός.

Παραδείγματα:

- Αναγνωρίσιμα/προσωπικά δεδομένα: «Μαίρη, 35, 2 παιδιά, Θεσσαλονίκη»
- Ψευδωνυμοποιημένα δεδομένα: «Αναστασία (ψευδώνυμο), ηλικίας 35 ετών, 2 παιδιά, Θεσσαλονίκη»
- Ανωνυμοποιημένα δεδομένα: «γονέας δύο παιδιών»

11. Περαιτέρω συμβουλές ανωνυμοποίησης

Πρέπει να τηρούνται λεπτομερή αρχεία καταγραφής όλων των πραγματοποιούμενων ενεργειών ανωνυμοποίησης. Ανάλογα με τη φύση του ερευνητικού έργου, η συμμόρφωση με τον GDPR ενδέχεται να μην είναι μία απλή υπόθεση (π.χ. σε ορισμένα έργα Κοινωνικής Ανθρωπολογίας και Εθνογραφίας μπορεί να είναι πολύ εύκολο να αναγνωριστούν τα χωριά ή/και οι συμμετέχοντες/ουσες).

12. Διατήρηση δεδομένων

Ως μέγιστη περίοδος διατήρησης των ερευνητικών δεδομένων έχει καθοριστεί αυτή των πέντε (5) ετών μετά την ολοκλήρωση της έρευνας, η οποία υπολογίζεται με την κατάθεση ή υποβολή του ερευνητικού έργου στον αρμόδιο ερευνητικό ή ακαδημαϊκό φορέα, όπως κάθε φορά ορίζεται.

Στην περίπτωση που οι φορείς χρηματοδότησης και οι ρυθμιστικές αρχές απαιτούν μεγαλύτερες περιόδους διατήρησης δεδομένων, το Πανεπιστήμιο Μακεδονίας δύναται να διατηρεί και να επιτρέπει την πρόσβαση στα ερευνητικά δεδομένα σύμφωνα με τις νομικές απαιτήσεις και τις απαιτήσεις χρηματοδότησης και λαμβάνοντας δεόντως υπόψη την ισχύουσα νομοθεσία.

Σε κάθε περίπτωση, η περίοδος διατήρησης, ή τουλάχιστον η βάση και το σκεπτικό με το οποίο αυτή ορίζεται (αν όχι η ακριβής περίοδος), πρέπει να κοινοποιούνται στους/στις συμμετέχοντες/ουσες στην έρευνα προκειμένου να ικανοποιείται η περί διαφάνειας απαίτηση του GDPR.

13. Καταστροφή δεδομένων

Τα αρχεία σε έντυπη μορφή πρέπει να καταστρέφονται με ασφαλή τρόπο (ενδεικτικά σε καταστροφέα εγγράφων).

Τα ηλεκτρονικά αρχεία πρέπει να διαγράφονται με εξειδικευμένα λογισμικά, κατάλληλα να αφαιρέσουν όλα τα δεδομένα από το υλικό.

Επικοινωνήστε με το ΚΥΔ για περισσότερες οδηγίες σχετικά με τη διαγραφή των ηλεκτρονικών αρχείων. Οι ερευνητές/τριες πρέπει να καταγράφουν ποια αρχεία καταστράφηκαν, πότε και με ποιον τρόπο.

14. Ειδικές οδηγίες για τα οπτικοακουστικά δεδομένα/φωτογραφίες

Όταν τα δεδομένα αυτά αφορούν καταγραφή ατόμων με εικόνα ή/και ήχο, είναι ιδιαίτερα σημαντική η προηγούμενη λήψη της ρητής συγκατάθεσής τους για την εγγραφή ήχου/ εικόνας, καθώς επίσης για την περίπτωση κατά την οποία οι συμμετέχοντες/ουσες είναι αναγνωρίσιμοι/ες (π.χ., πρόσωπα, φωνές). Τα οπτικοακουστικά δεδομένα δεν μπορούν να ανωνυμοποιηθούν εύκολα. Εάν στα δεδομένα εμπεριέχονται αναγνωρίσιμες πληροφορίες, τότε διατηρούνται μόνο υπό την προϋπόθεση ρητής συγκατάθεσης των υποκειμένων πριν την καταγραφή τους.

Όπου ενδέχεται να υπάρχει ευαίσθητο περιεχόμενο (π.χ., ο/η συμμετέχων/ουσα μπορεί να εκφράζει προσωπικές πολιτικές, φιλοσοφικές, θρησκευτικές απόψεις ή να επιδεικνύει ανικανότητα ως προς μια εργασία λόγω αναπηρίας), τότε εναπόκειται στον ερευνητή/τρια να λάβει πρόσθετα μέτρα.

Για την πλειονότητα των έργων, τα σημεία που ακολουθούν είναι τα πιο σημαντικά:

α) Πρέπει να λαμβάνεται συγκατάθεση του υποκειμένου κατόπιν ενημέρωσής του, η οποία θα συμμορφώνεται με την πολιτική διαχείρισης δεδομένων που, ενδεχομένως, έχουν τυχόν άλλοι ερευνητικοί συνεργάτες (εάν εφαρμόζεται). Στο έντυπο ενημέρωσης και συγκατάθεσης συμμετεχόντων πρέπει να αναφέρεται ότι στο υλικό έχουν πρόσβαση μόνο μέλη της ερευνητικής ομάδας και άλλοι ακαδημαϊκοί (όχι το κοινό).

β) Τα σχετικά αρχεία πρέπει να φυλάσσονται κατά τρόπο ασφαλή ή, για αντίγραφα σε έντυπη μορφή, σε κλειδωμένο ντουλάπι αρχειοθέτησης.

γ) Σε περίπτωση κατάθεσης ευαίσθητου υλικού σε ένα αρχείο/αποθετήριο, ο/η ερευνητής/τρια πρέπει να συνεργαστεί με το αρχείο/αποθετήριο για να διασφαλίσει ότι λαμβάνονται όλα τα κατάλληλα μέτρα για τον περιορισμό της πρόσβασης σε αυτό το υλικό.

Επιπλέον, πρέπει να ληφθούν υπόψη οι ακόλουθες ενέργειες εάν αυτό κριθεί απαραίτητο:

δ) Οι συμμετέχοντες/ουσες πρέπει να διευκρινίζουν κατά τη διάρκεια των ηχογραφήσεων/βιντεοσκοπήσεων τυχόν τμήματα που είναι «off the record».

ε) Οι ερευνητές/τριες αναλαμβάνουν την υποχρέωση να ελέγχουν την πρόσβαση άλλων στα δεδομένα (ή να ζητούν από το αποθετήριο όπου θα κατατεθούν να αναλάβει αυτόν τον έλεγχο).

στ) Ειδικά μέτρα πρέπει να λαμβάνονται αμέσως για την ασφαλή διαβίβαση των δεδομένων (και την πλήρη διαγραφή τους) και την κρυπτογραφημένη αποθήκευσή τους.

ζ) Όταν χρησιμοποιείτε τεχνικές καταγραφής ήχου και εικόνας, είναι σημαντικό να διασφαλίσετε ότι τα δεδομένα διαβιβάζονται μεταξύ των μερών κατά τρόπο ασφαλή και ότι ο πάροχος της υπηρεσίας θα διαγράψει όλο το οπτικοακουστικό υλικό μόλις παραδώσει τη μεταγραφή. Μία συμφωνία για την παροχή υπηρεσίας πρέπει να έχει συναφθεί προτού διαβιβαστεί οποιοδήποτε υλικό στον πάροχο.

η) Η καταγραφή εικόνας ή/και ήχου παιδιών εγείρει δύο (2) επιπλέον ηθικά ζητήματα:

- Οι ερευνητές/τριες πρέπει να γνωρίζουν ότι οι γονείς και οι εκπαιδευτικοί ενδέχεται να ανησυχούν ότι ακόμη και οι πιο ακίνδυνες ηχογραφήσεις/βίντεοσκοπήσεις παιδιών μπορεί να γίνουν αντικείμενο κατάχρησης, επομένως οι ερευνητές/τριες πρέπει να διευκρινίσουν τις ενέργειες στις οποίες θα προβούν για την προστασία των δεδομένων και την ακεραιότητα της έρευνάς τους. Το σημείο (β) πρέπει να τηρείται ακόμη και όταν το περιεχόμενο της ηχογράφησης δεν είναι φαινομενικά «ευαίσθητο».

- Με την πάροδο του χρόνου, ένα παιδί ενδέχεται να μη συμφωνεί πλέον με τη διατήρηση των δεδομένων του. Αυτό είναι πιθανό να συμβεί μόνο στην περίπτωση κατά την οποία ένας ενήλικας παραχώρησε άδεια για τη διάθεση του οπτικοακουστικού/φωτογραφικού υλικού στο ευρύ κοινό, π.χ., ως ενδεικτικό παράδειγμα (case study) σε μια επιστημονική διάλεξη.

Για διαχρονικές μελέτες, όταν τα παιδιά που συμμετέχουν σε οπτικοακουστικό/φωτογραφικό υλικό έχουν φτάσει σε μια ηλικία κατά την οποία μπορούν να δώσουν τη δική τους συγκατάθεση για καταγραφή του ήχου ή της εικόνας τους, τότε η εν λόγω συγκατάθεση πρέπει να λαμβάνεται πριν τη διαβίβαση των δεδομένων σε άτομα εκτός της ερευνητικής ομάδας.

Βεβαιωθείτε ότι έχετε συντάξει τα κατάλληλα ερευνητικά πρωτόκολλα αναφορικά με τη διαχείριση ερευνητικών δεδομένων πριν υποβάλετε αίτηση προς την Ε.Η.Δ.Ε..

15. Παράρτημα Α – Οδηγίες για την απομακρυσμένη εγγραφή ήχου ή/και εικόνας

Με τα παρακάτω προσδιορίζονται συγκεκριμένα σημεία αναφορικά με την προστασία δεδομένων κατά την απομακρυσμένη/διαδικτυακή εγγραφή.

Χρειάζεται να κάνω εγγραφή ήχου ή/και εικόνας;

Υπάρχει πλέον η απαίτηση να είναι δυνατή η διεξαγωγή συνεντεύξεων με τους συμμετέχοντες και η απομακρυσμένη συλλογή δεδομένων με τη χρήση εργαλείων τηλεδιάσκεψης. Ωστόσο, καταρχήν, οι ερευνητές/τριες πρέπει να εξετάσουν, εάν υπάρχει ανάγκη απομακρυσμένης εγγραφής των συμμετεχόντων/ουσών. Η χρήση τεχνικών επεξεργασίας δεδομένων με καταγραφή εικόνας ή/και ήχου πρέπει να δηλώνεται υποχρεωτικά στο ερευνητικό πρωτόκολλο.

Εγγραφή βίντεο

Το ZOOM και το GoogleMeet είναι τα εγκεκριμένα, από μέρους του Πανεπιστημίου, εργαλεία για τις εικονικές συναντήσεις. Οι ερευνητές/τριες πρέπει να λαμβάνουν υπόψη τους κινδύνους καταγραφής μιας εικονικής συνάντησης. Για να μάθετε περισσότερα, επικοινωνήστε με το ΚΥΔ.

Αναγκαιότητα και αναλογικότητα

Η αναγκαιότητα και η αναλογικότητα της καταγραφής ήχου ή και εικόνας πρέπει να λαμβάνονται, επίσης, υπόψη. Για παράδειγμα, εάν μια εγγραφή βίντεο είναι απαραίτητη για την αξιολόγηση ενός/μιας συμμετέχοντος/ουσας, αυτή πρέπει να περιορίζεται μόνο στην ενέργεια της αξιολόγησής του/της, αφού μπορεί να μην είναι απαραίτητη η εγγραφή ολόκληρης της συνάντησης για τους σκοπούς της έρευνας.

Στην περίπτωση βίντεοσκοπήσης, προκειμένου να καταγραφεί μόνο ο ήχος, όλοι οι συμμετέχοντες/ουσες πρέπει να απενεργοποιήσουν τις κάμερές τους πριν την εκκίνηση της εγγραφής. Αυτό μπορεί να γίνει από τον/την κάθε συμμετέχοντα/ουσα μεμονωμένα. Επομένως, η ευθύνη απενεργοποίησης της κάμερας βαρύνει τον/την συμμετέχοντα/ουσα, καθώς αυτό δεν μπορεί να γίνει από τον/την διοργανωτή/τρια της τηλεδιάσκεψης. Υπάρχει ο κίνδυνος οι συμμετέχοντες/ουσες να ενεργοποιήσουν κατά λάθος την κάμερά τους κατά τη διάρκεια της εγγραφής και ο/η ερευνητής/τρια να καταγράψει ακούσια εικόνα των συμμετεχόντων/ουσών. Για να διασφαλιστεί ότι θα καταγραφεί μόνο ήχος, το ηλεκτρονικό μήνυμα της πρόσκλησης, που θα αποσταλεί, θα μπορούσε να υπενθυμίζει ότι οι κάμερες πρέπει να είναι απενεργοποιημένες πριν την έναρξη της συμμετοχής τους στην τηλεδιάσκεψη. Ταυτόχρονα, οι ερευνητές/τριες πρέπει να το υπενθυμίσουν και να ελέγξουν ότι όλες οι κάμερες είναι απενεργοποιημένες πριν εκκινήσουν την εγγραφή.

Στις περιπτώσεις κατά τις οποίες κρίνεται απαραίτητη μόνο η ηχογράφηση αλλά οι ερευνητές/τριες πρέπει να έχουν τη δυνατότητα να δουν το άτομο κατά τη διάρκεια της εγγραφής, υπάρχει ο κίνδυνος υπερβολικής συλλογής προσωπικών δεδομένων. Οι ερευνητές/τριες πρέπει να εξετάσουν τον τρόπο με τον οποίο μπορούν να μειώσουν αυτόν τον κίνδυνο, για παράδειγμα, με διαγραφή του βίντεο μόλις ολοκληρωθεί η καταγραφή εικόνας και ήχου.

Ασφάλεια

Πριν από την έναρξη της τηλεδιάσκεψης, οι ερευνητές/τριες πρέπει να διασφαλίσουν ότι το εργασιακό περιβάλλον έχει διαμορφωθεί κατάλληλα, ώστε να τηρεί και να προστατεύει το απόρρητο και την εμπιστευτικότητα των συμμετεχόντων/ουσών μέσω, π.χ., χρήσης ακουστικών και αποκλεισμού μη εξουσιοδοτημένων ατόμων από το εν λόγω περιβάλλον.

Μόλις ολοκληρωθούν οι εγγραφές, αποθηκεύονται. Ο/η διοργανωτής/τρια πρέπει να διασφαλίσει ότι έχουν οριστεί τα δικαιώματα αποθήκευσης, ενώ στο περιεχόμενο καταγραφής έχουν πρόσβαση μόνο όσοι/ες χρειάζεται να λάβουν γνώση.

Διατήρηση

Καθώς το οπτικοακουστικό υλικό βρίσκεται στον λογαριασμό του/της διοργανωτή/τριας και όχι σε κάποιον κοινόχρηστο χώρο, συνιστάται η λήψη και η αποθήκευση των ηχογραφήσεων στο πανεπιστημιακό δίκτυο πληροφορικής (για παράδειγμα σε έναν φάκελο περιορισμένης πρόσβασης που θα προστατεύεται με κωδικό πρόσβασης) για λόγους διαθεσιμότητας των δεδομένων και εύκολης διατήρησης. Η εγγραφή θα υπάρχει όσο ο/η κάτοχος τη διατηρεί. Μετά τη λήψη τους, οι εγγραφές πρέπει να διαγράφονται από τον λογαριασμό του/της διοργανωτή/τριας.

Διαφάνεια

Είναι σημαντικό οι συμμετέχοντες/ουσες να ενημερώνονται σχετικά με την προτεινόμενη μέθοδο καταγραφής ή τις αλλαγές στην καταγραφή στο πλαίσιο ερευνητικών έργων που ήδη υλοποιούνται.

Βεβαιωθείτε ότι το εργασιακό περιβάλλον έχει ρυθμιστεί κατάλληλα για να διασφαλιστεί ότι όλα τα μέρη μπορούν να τηρήσουν και να προστατεύσουν το απόρρητο και την εμπιστευτικότητα των δεδομένων.