ΑΡΙΣΤΟΤΕΛΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ
ΘΕΣΣΑΛΟΝΙΚΗΣ

# Προκαταρτικός οδηγός για την Προστασία των Προσωπικών Δεδομένων στο πλαίσιο Επιστημονικής Έρευνας

Έκδοση 1.0 Σεπτέμβριος 2020

# Contents

# 1. Εισαγωγή

Το παρόν κείμενο αποτελεί μια πρώτη προσπάθεια για μια σύντομη διερεύνηση των θεμάτων που πρέπει να έχει υπόψη της ένας Φορέας Έρευνας και αφορούν ένα επιστημονικό ερευνητικό έργο που τα προσωπικά δεδομένα αποτελούν μεγάλο ή μικρό μέρος της έρευνας.

Η προστασία των προσωπικών δεδομένων και της ιδιωτικότητας των φυσικών προσώπων είναι μια υποχρέωση που επιβάλλεται από εθνικές και ευρωπαϊκές νομοθεσίες και που εκφράζονται σήμερα κατά κύριο λόγο μέσα από τον Γενικό Κανονισμός Προστασίας Δεδομένων (ΕΕ 679/2016 ή ΓΚΠΔ εφ' εξής), τον ν. 4624/2019, τον 3471/2006 που ενσωματώνει στο εθνικό δίκαιο την Οδηγία 2002/58/ΕΚ (ePrivacy) για την προστασία της ιδιωτική ζωής στο τομέα των ηλεκτρονικών επικοινωνιών και άλλες νομικές διατάσεις.

Για τα επιστημονικά ερευνητικά προγράμματα με επίκεντρο τον άνθρωπο και όχι μόνο και κυρίως με τα θέματα της υγείας του, της βιολογικής και γενετικής του υπόστασης, τέθηκαν ηθικά θέματα για τα οποία καθορίστηκαν κώδικες συμπεριφοράς και δεοντολογίας σε διάφορα επίπεδα.

*Η διάκριση μεταξύ, αφενός, της γνήσιας έρευνας για το κοινό καλό και, αφετέρου, της έρευνας που εξυπηρετεί κυρίως ιδιωτικούς ή εμπορικούς σκοπούς, γίνεται όλο και πιο θολή. Υπάρχει μια ακμάζουσα αγορά για υπηρεσίες γενετικών δοκιμών απευθείας στους καταναλωτές που προσφέρουν την πρόβλεψη ιατρικών παραγόντων κινδύνου και την αποκάλυψη καταγωγής ή γενεαλογίας. Αυτό το ίδιο δεν είναι έρευνα, αλλά μια στρατηγική για τη συλλογή δεδομένων με βάση τη συγκατάθεση που μπορεί στη συνέχεια να χρησιμοποιηθεί περαιτέρω για έρευνα ή άλλους σκοπούς, συμπεριλαμβανομένης της επιβολής του νόμου*[1].

Επομένως η σημαντική προϋπόθεση για την επιτυχία αυτών των ερευνητικών προσπαθειών είναι η εμπιστοσύνη την οποία θα επιδείξουν τα φυσικά πρόσωπα. Οι άνθρωποι πρέπει να έχουν τη βεβαιότητα ότι διασφαλίζεται η συμμόρφωση με τα θεμελιώδη δικαιώματα τους και ότι τα προσωπικά τους δεδομένα θα χρησιμοποιηθούν μόνο για τους συγκεκριμένα καθορισμένους σκοπούς, ότι δεν θα χρησιμοποιηθούν για μαζική παρακολούθηση και ότι οι ίδιοι θα διατηρούν τον έλεγχο των δεδομένων τους. Αυτή η αξίωση εκφράζεται μέσα από τις σχετικές ευρωπαϊκές και εθνικές νομοθεσίες που απαιτούν για τα προσωπικά δεδομένα να εφαρμόζονται συγκεκριμένες αρχές που εξασφαλίζουν την νομιμότητα και την αντικειμενικότητα για τη χρήση των προσωπικών δεδομένων με όρους διαφάνειας προς τα φυσικά πρόσωπα, που υποχρεώνει τους χρήστη να οργανώσει τους πραγματικούς του σκοπούς και να χρησιμοποιήσει μόνο τα αναγκαία και πρόσφορα προσωπικά δεδομένα και που οφείλει να λάβει τα κατάλληλα οργανωτικά και τεχνικά μέτρα για την προστασία τους αλλά και να μπορεί να το αποδεικνύει.

[1] A Preliminary Opinion on data protection and scientific research from EDPS
https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf

Στα επόμενα κεφάλαια, αρχικά θα δοθούν για εύκολη χρήση μερικοί χρήσιμοι ορισμοί των εννοιών γύρω από τα προσωπικά δεδομένα όπως αυτοί αποτυπώθηκα στον ΓΚΠΔ, θα παρουσιαστεί η αρχιτεκτονική εφαρμογής του ΓΚΠΔ σε ένα Φορέα Έρευνας, θα ξεκαθαριστούν οι αρχές του ΓΚΠΔ και τα δικαιώματα των φυσικών προσώπων που ορίζει και στο τέλος θα περιγραφούν τα τεχνικά και στη συνέχεια τα οργανωτικά μέτρα που θα πρέπει να ληφθούν υπόψη ώστε η επιστημονική έρευνα να συμμορφώνεται με τον ΓΚΠΔ.

**Τα προσωπικά δεδομένα των φυσικών προσώπων θα πρέπει να αντιληφθούμε ότι αποτελούν περιουσιακό τους στοιχείο που όταν το έχουμε στην κατοχή μας θα πρέπει να το σεβόμαστε και να το προστατεύουμε**.

## 2. Ορισμοί

Σύμφωνα με το άρθρο 4 του ΓΚΠΔ:

1. **«δεδομένα προσωπικού χαρακτήρα ή προσωπικά δεδομένα ή ΠΔ»**: κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»)· 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,

2. **«επεξεργασία»:** κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή,

3. **«κατάρτιση προφίλ»**: οποιαδήποτε μορφή αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα που συνίσταται στη χρήση δεδομένων προσωπικού χαρακτήρα για την αξιολόγηση ορισμένων προσωπικών πτυχών ενός φυσικού προσώπου, ιδίως για την ανάλυση ή την πρόβλεψη πτυχών που αφορούν την απόδοση στην εργασία, την οικονομική κατάσταση, την υγεία, τις προσωπικές προτιμήσεις, τα ενδιαφέροντα, την αξιοπιστία, τη συμπεριφορά, τη θέση ή τις μετακινήσεις του εν λόγω φυσικού προσώπου,

4. **«ψευδωνυμοποίηση»**: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 δεν μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο,

5. **«υπεύθυνος επεξεργασίας»**: 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 Ένωσης ή το δίκαιο κράτους μέλους, ο υπεύθυνος

επεξεργασίας ή τα ειδικά κριτήρια για τον διορισμό του μπορούν να προβλέπονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους,

6. **«Από κοινού Υπεύθυνοι Επεξεργασίας – Joint Controllers»**: Σύμφωνα με το άρθρο 26 παράγραφος 1 του ΓΚΠΔ όπου δύο ή περισσότεροι υπεύθυνοι επεξεργασίας καθορίζουν από κοινού τους σκοπούς και τα μέσα επεξεργασίας δεδομένων προσωπικού χαρακτήρα, πρέπει να είναι από κοινού υπεύθυνοι επεξεργασίας,

7. **«εκτελών την επεξεργασία»**: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας,

8. **«αποδέκτης»**: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας, στα οποία κοινολογούνται τα δεδομένα προσωπικού χαρακτήρα, είτε πρόκειται για τρίτον είτε όχι. Ωστόσο, οι δημόσιες αρχές που ενδέχεται να λάβουν δεδομένα προσωπικού χαρακτήρα στο πλαίσιο συγκεκριμένης έρευνας σύμφωνα με το δίκαιο της Ένωσης ή κράτους μέλους δεν θεωρούνται ως αποδέκτες· η επεξεργασία των δεδομένων αυτών από τις εν λόγω δημόσιες αρχές πραγματοποιείται σύμφωνα με τους ισχύοντες κανόνες προστασίας των δεδομένων ανάλογα με τους σκοπούς της επεξεργασίας,

9. **«τρίτος»**: οποιοδήποτε φυσικό ή νομικό πρόσωπο, δημόσια αρχή, υπηρεσία ή φορέας, με εξαίρεση το υποκείμενο των δεδομένων, τον υπεύθυνο επεξεργασίας, τον εκτελούντα την επεξεργασία και τα πρόσωπα τα οποία, υπό την άμεση εποπτεία του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα,

10. **«συγκατάθεση»** του υποκειμένου των δεδομένων: κάθε ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει, με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν,

11. «**παραβίαση δεδομένων προσωπικού χαρακτήρα**»: η παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία,

12. **«ειδικής κατηγορίας δεδομένα ή ευαίσθητα δεδομένα»** ( άρθρο 9 ΓΚΠΔ): προσωπικά δεδομένα που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, ή αφορούν γενετικά δεδομένα, βιομετρικά δεδομένα με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένα που αφορούν την υγεία ή δεδομένων που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό.
    Σύμφωνα με την αιτιολογική σκέψη 51 του ΓΚΠΔ, τα δεδομένα προσωπικού χαρακτήρα τα οποία είναι εκ φύσεως ιδιαίτερα ευαίσθητα σε σχέση με θεμελιώδη δικαιώματα και ελευθερίες χρήζουν ειδικής προστασίας, καθότι το πλαίσιο της επεξεργασίας τους θα μπορούσε να δημιουργήσει σημαντικούς κινδύνους για τα θεμελιώδη δικαιώματα και τις ελευθερίες.

13. **«γενετικά δεδομένα»**: τα δεδομένα προσωπικού χαρακτήρα που αφορούν τα γενετικά χαρακτηριστικά φυσικού προσώπου που κληρονομήθηκαν ή αποκτήθηκαν, όπως προκύπτουν, ιδίως, από ανάλυση βιολογικού δείγματος του εν λόγω φυσικού προσώπου και τα οποία παρέχουν μοναδικές πληροφορίες σχετικά με την φυσιολογία ή την υγεία του εν λόγω φυσικού προσώπου,

14. **«βιομετρικά δεδομένα»**: δεδομένα προσωπικού χαρακτήρα τα οποία προκύπτουν από ειδική τεχνική επεξεργασία συνδεόμενη με φυσικά, βιολογικά ή συμπεριφορικά χαρακτηριστικά φυσικού προσώπου και τα οποία επιτρέπουν ή επιβεβαιώνουν την αδιαμφισβήτητη ταυτοποίηση του εν λόγω φυσικού προσώπου, όπως εικόνες προσώπου ή δακτυλοσκοπικά δεδομένα,

15. **«δεδομένα που αφορούν την υγεία**»: δεδομένα προσωπικού χαρακτήρα τα οποία σχετίζονται με τη σωματική ή ψυχική υγεία ενός φυσικού προσώπου, περιλαμβανομένης της παροχής υπηρεσιών υγειονομικής φροντίδας, και τα οποία αποκαλύπτουν πληροφορίες σχετικά με την κατάσταση της υγείας του.

    Τα δεδομένα υγείας, που ως ευαίσθητα δεδομένα χρήζουν υψηλότερης προστασίας, μπορούν να προέρχονται από διαφορετικές πηγές, για παράδειγμα:

    α) Πληροφορίες που συλλέγονται από πάροχο υπηρεσιών υγείας σε αρχείο ασθενών (όπως ιατρικό ιστορικό και αποτελέσματα εξετάσεων και θεραπειών).
    β) Πληροφορίες που γίνονται δεδομένα υγείας με παραπομπή με άλλα δεδομένα, αποκαλύπτοντας έτσι την κατάσταση των κινδύνων για την υγεία ή την υγεία (όπως η υπόθεση ότι ένα άτομο έχει υψηλότερο κίνδυνο να υποστεί καρδιακές προσβολές με βάση την υψηλή αρτηριακή πίεση που μετράται για μια ορισμένη χρονική περίοδο).

γ) Πληροφορίες από μια έρευνα ερωτηματολογίου, όπου τα υποκείμενα των δεδομένων απαντούν σε ερωτήσεις που σχετίζονται με την υγεία τους (όπως δηλώσεις συμπτωμάτων).

δ) Πληροφορίες που γίνονται δεδομένα υγείας λόγω της χρήσης τους σε ένα συγκεκριμένο πλαίσιο (όπως πληροφορίες σχετικά με ένα πρόσφατο ταξίδι ή παρουσία σε μια περιοχή που έχει πληγεί από μια επιδημία ( πχ COVID-19) που υποβάλλονται σε επεξεργασία από έναν ιατρό για να κάνει διάγνωση).

# 3. Αρχιτεκτονική του ΓΚΠΔ σε Φορέα Έρευνας

Το επόμενα σχήμα περιγράφει την αρχιτεκτονική συμμόρφωσης του υπεύθυνου επεξεργασίας με τον ΓΚΠΔ.

Στην αρχιτεκτονική αυτή φαίνεται καθαρά η σχέση που αναπτύσσεται μεταξύ των ενδιαφερομένων μερών στο εσωτερικό και εξωτερικό περιβάλλον του υπεύθυνου επεξεργασίας

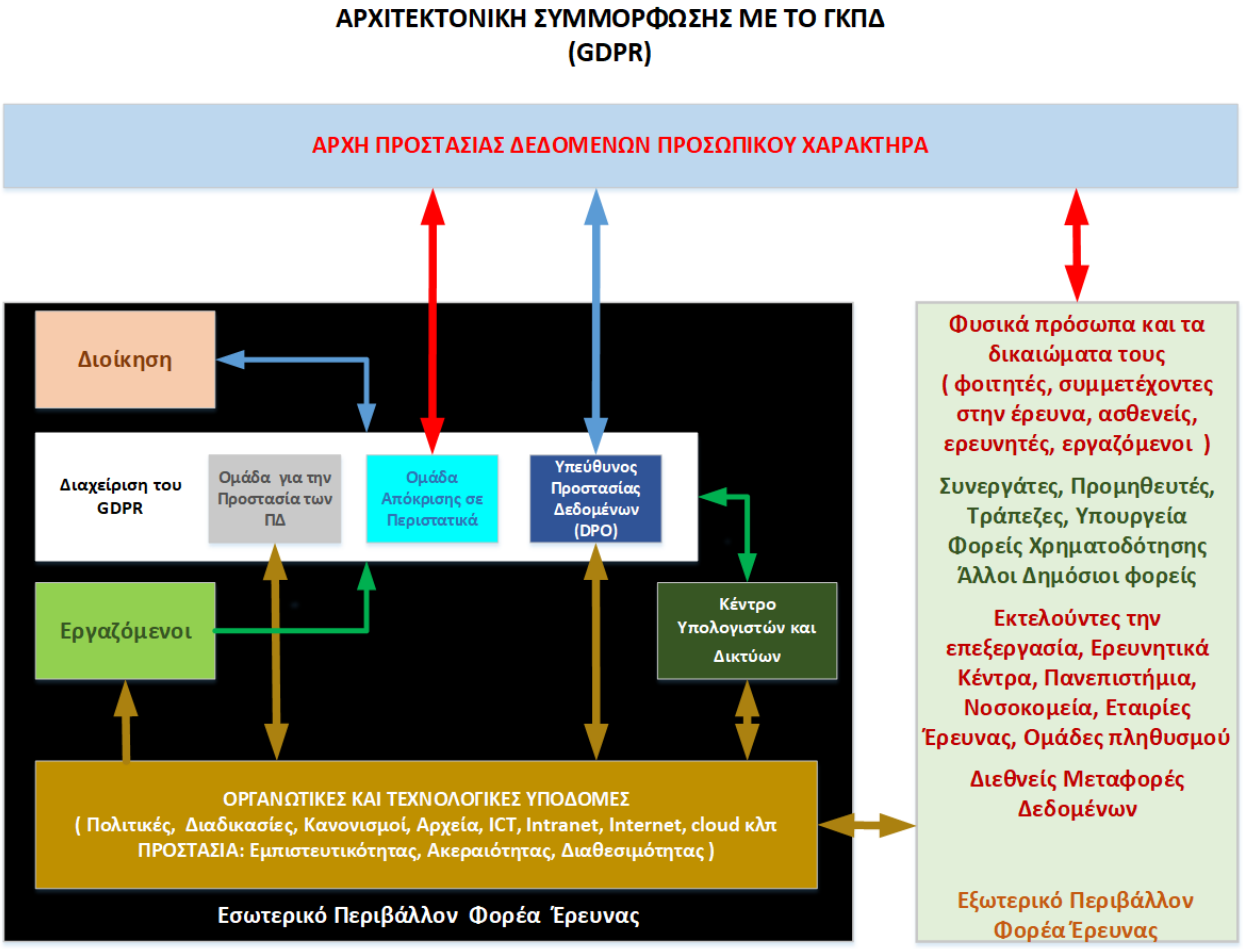


*Figure 1 Αρχιτεκτονική συμμόρφωσης με τον ΓΚΠΔ*

Σε γενικές γραμμές, οι υποχρεώσεις προς τον ΓΚΠΔ δημιουργούν νέες οργανωτικές δομές και τεχνολογικές υποδομές τα οποία οριοθετούν και τις σχέσεις και τις δράσεις μεταξύ των εμπλεκομένων.

Οι σχέσεις και οι δράσεις δημιουργούνται τόσο μεταξύ των μερών στο εσωτερικό περιβάλλον του Υπεύθυνου Επεξεργασίας όσο και μεταξύ του εσωτερικού περιβάλλοντος και του εξωτερικού

περιβάλλοντος του. Στο εξωτερικό περιβάλλον περιλαμβάνεται και η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) η οποία έχει πλέον ρόλο ελεγκτικό.

Στα δομικά στοιχεία του εσωτερικού περιβάλλοντος περιλαμβάνονται και νέες οργανωτικές δομές που αφορούν την συνολική διαχείριση του ΓΚΠΔ και που ανταποκρίνονται στις ανάγκες προστασίας στην καθημερινή λειτουργία του Υπεύθυνου Επεξεργασίας καθώς και στις περιπτώσεις παραβιάσεων.

Οι δομές αυτές περιλαμβάνουν την Ομάδα για την Προστασία των Προσωπικών Δεδομένων και την Ομάδα Απόκρισης σε Περιστατικά. Συνδετικός κρίκος αυτών των ομάδων είναι η πληροφορική και ο Υπεύθυνος Προστασίας Δεδομένων (Data Protection Officer - DPO) τον οποίο υποχρεωτικά πρέπει να ορίσει ο Υπεύθυνος Επεξεργασίας ( άρθρο 37.1α ΓΚΠΔ).

Τα άλλα εσωτερικά δομικά στοιχεία είναι η Διοίκηση, οι Εργαζόμενοι και το οργανωτικό και τεχνολογικό πλαίσιο λειτουργίας. Το τελευταίο υλοποιείται με τα οργανωτικά (πολιτικές, διαδικασίες, κανονισμούς και ρόλους) και τεχνολογικά μέτρα (web site, firewall, VPN, Internet και άλλα) ικανά να παρέχουν την απαιτούμενη προστασία των προσωπικών δεδομένων. Κρίσιμο στοιχείο σε αυτά τα μέτρα αποτελεί η διεπαφή του Υπεύθυνου Επεξεργασίας με το εξωτερικό του περιβάλλον.

Η Ομάδα για την Προστασία των Προσωπικών Δεδομένων και ο Υπεύθυνος Προστασίας Δεδομένων (DPO) εποπτεύουν την συμμόρφωση με το GPDR και τη λειτουργία των μέτρων προστασίας, τα οποία εφαρμόζουν οι εργαζόμενοι στην καθημερινή τους λειτουργία. Οι εργαζόμενοι ανατροφοδοτούν τις Ομάδες για τη λειτουργία των μέτρων ασφαλείας ή τις ενημερώνουν με περιστατικά παραβίασης προσωπικών δεδομένων ανατροφοδοτώντας συνεχώς τον κύκλο εφαρμογής και βελτίωσης των τεχνικών και οργανωτικών μέτρων.

Η συμμετοχή της Διοίκησης στη Διαχείριση του ΓΚΠΔ έχει μεγάλη σημασία για την άμεση γνώση και λήψη οικονομικών αποφάσεων.

Με το εξωτερικό περιβάλλον ο Υπεύθυνος Επεξεργασίας αναπτύσσει διαδικασίες επικοινωνίας, ενημέρωσης και μηχανισμούς για ικανοποίηση των δικαιωμάτων των φυσικών προσώπων και την δέσμευση τρίτων (από κοινού Υπεύθυνοι επεξεργασίας και Εκτελούντες την επεξεργασία) στην προστασία των προσωπικών δεδομένων που κοινοποιούνται εκτός του χώρου εποπτείας τους και εφαρμογής των μέτρων του. Οι διεθνείς μεταφορές καλύπτουν συνεργασίες που μπορεί να αναπτύσσει ο Υπεύθυνος Επεξεργασίας εκτός ΕΟΧ.

Η επικοινωνία με την Αρχή Προστασίας και οι υποχρεώσεις για την ενημέρωσή της αναφέρονται αναλυτικά στον ΓΚΠΔ. Η σχέση με την Αρχή Προστασίας μπορεί να διαμορφώνεται σε επίπεδο ενημερώσεων και διευκρινήσεων, αλλά και σε επίπεδο διαχείρισης παραβιάσεων.

# 4. Επιστημονική Έρευνα και Προσωπικά δεδομένα

Ο παρών προκαταρτικός οδηγός δεν έχει στόχο να εμβαθύνει στα θέματα της επιστημονικής έρευνας, αλλά να προσπαθήσει να καταγράψει την σχέση των προσωπικών δεδομένων με την επιστημονική έρευνα.

Ο όρος «επεξεργασία για σκοπούς επιστημονικής έρευνας» δεν περιέχεται στους ορισμούς του ΓΚΠΔ, όμως στην αιτιολογική σκέψη 159, όπου αναφέρει ότι *«Όταν δεδομένα προσωπικού χαρακτήρα υφίστανται επεξεργασία για σκοπούς επιστημονικής έρευνας, ο παρών κανονισμός θα πρέπει να ισχύει και για την επεξεργασία αυτή»*, αναφέρει επίσης ότι «*η επεξεργασία δεδομένων προσωπικού χαρακτήρα για σκοπούς επιστημονικής έρευνας θα πρέπει να ερμηνεύεται διασταλτικά, δηλαδή να περιλαμβάνει παραδείγματος χάριν τεχνολογική ανάπτυξη και επίδειξη, βασική έρευνα, εφαρμοσμένη έρευνα και ιδιωτικά χρηματοδοτούμενη έρευνα. Επιπλέον, θα πρέπει να λαμβάνει υπόψη τον στόχο της Ένωσης δυνάμει του άρθρου 179 παράγραφος 1 ΣΛΕΕ (Συνθήκη για τη λειτουργία της ΕΕ) για την επίτευξη ενός ευρωπαϊκού χώρου έρευνας. Στους σκοπούς επιστημονικής έρευνας θα πρέπει να περιλαμβάνονται και μελέτες που πραγματοποιούνται για το δημόσιο συμφέρον στον τομέα της δημόσιας υγείας. Για να ληφθούν υπόψη οι ιδιαιτερότητες της επεξεργασίας δεδομένων προσωπικού χαρακτήρα για σκοπούς επιστημονικής έρευνας, θα πρέπει να ισχύουν ειδικοί όροι ιδίως όσον αφορά τη δημοσίευση ή με άλλο τρόπο δημοσιοποίηση δεδομένων προσωπικού χαρακτήρα στο πλαίσιο των σκοπών επιστημονικής έρευνας. Εάν το αποτέλεσμα της επιστημονικής έρευνας ειδικότερα στον τομέα της υγείας αιτιολογεί τη λήψη περαιτέρω μέτρων προς το συμφέρον του υποκειμένου των δεδομένων, ισχύουν οι γενικοί κανόνες του παρόντος κανονισμού όσον αφορά τα μέτρα αυτά.»*

Ωστόσο, η Ομάδα του Άρθρου 29 (WP29)[2] θεωρεί ότι η διασταλτική ερμηνεία της επιστημονικής έρευνας δεν μπορεί να ξεπεράσει το κοινό της νόημα και κατανοεί ότι η επιστημονική έρευνα σε αυτό το πλαίσιο σημαίνει ένα ερευνητικό έργο που καταρτίζεται σύμφωνα με τα μεθοδολογικά και δεοντολογικά πρότυπα (ethics standards) που σχετίζονται με τον συγκεκριμένο τομέα, σύμφωνα με τις ορθές πρακτικές.

Σύμφωνα με τις αιτιολογικές σκέψεις 156 και 161 του ΓΚΠΔ, η επεξεργασία δεδομένων προσωπικού χαρακτήρα για επιστημονικούς σκοπούς θα πρέπει να συμμορφώνεται επίσης με άλλες σχετικές νομοθεσίες, όπως αυτή για τις κλινικές δοκιμές (Κανονισμός (ΕΕ) αριθ. 536/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου).

Στο πλαίσιο αυτής της προσέγγισης, μόνο η επιστημονική έρευνα που διεξάγεται σε ένα καθορισμένο πλαίσιο δεοντολογίας θα μπορούσε επομένως να χαρακτηριστεί ως δραστηριότητες που εμπίπτουν στο

[2] δες «Οδηγίες για την Συγκατάθεση για τον ΓΚΠΔ» της πρώην Ομάδας του Άρθρου 29 , WP259 rev. 01, § 7.2 Science Research, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

ειδικό καθεστώς προστασίας δεδομένων το οποίο, σύμφωνα με την Γνώμη του EDPS[3], θεωρείται ότι εφαρμόζεται όταν πληρούνται καθένα από τα τρία κριτήρια:

i. τα προσωπικά δεδομένα υποβάλλονται σε επεξεργασία
ii. εφαρμόζονται σχετικά τομεακά πρότυπα μεθοδολογίας και δεοντολογίας (ethics), συμπεριλαμβανομένης της έννοιας της ενημερωμένης συγκατάθεσης, της λογοδοσίας και της εποπτείας
iii. η έρευνα διεξάγεται με στόχο την αύξηση της συλλογικής γνώσης και ευημερίας της κοινωνίας, σε αντίθεση με την εξυπηρέτηση κυρίως ενός ή περισσότερων ιδιωτικών συμφερόντων.

Ένα ενδιαφέρον παράδειγμα κώδικα δεοντολογίας βρίσκεται στο επόμενο link

- Ethics and data protection[4], Ευρωπαϊκή Επιτροπή, 14 Νοεμβρίου 2018

Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων ( EDPB), σε εφαρμογή του άρθρου 40 του ΓΚΠΔ αναπτύσσει (εντός του 2020) Κώδικα Συμπεριφοράς για την Έρευνα για την Υγεία (https://code-of-conduct-for-health-research.eu/), ο οποίος θα έχει σαν στόχο να:

- καθοδηγεί ερευνητές και διοικητικό προσωπικό
- μειώνει τον περιττό φόβο σχετικά με τη συμμόρφωση και
- ενισχύει την ανταλλαγή δεδομένων με σκοπό την τόνωση της προόδου στην έρευνα

## 5. Βασικές έννοιες του ΓΚΠΔ

Κάθε φορέας του ιδιωτικού και του δημόσιου τομέα είναι υπεύθυνος επεξεργασίας δεδομένου ότι έχει εργαζομένους, των οποίων τα προσωπικά δεδομένα χρησιμοποιεί. Οι σχέσεις που αναπτύσσει ο υπεύθυνος επεξεργασίας με τα φυσικά πρόσωπα υπόκεινται συσσωρευτικά από την εθνική και ευρωπαϊκή νομοθεσία η οποία ρυθμίζει τις υποχρεώσεις και τα δικαιώματα των δύο μερών. Οι σχέσεις αυτές είναι σύνθετες και πολύπλευρες που όμως σε κάθε περίπτωση συναλλαγής εξειδικεύονται σε διαδικασίες και ενέργειες που με την σειρά τους καθορίζουν ή πρέπει να καθορίζουν με σαφήνεια τις συμπεριφορές και τις πληροφορίες που είναι απαραίτητες για την συναλλαγή. Επομένως κάθε τέτοια διαδικασία συναλλαγής που υλοποιεί ο υπεύθυνος επεξεργασίας είναι συνυφασμένη με ένα σύνολο

[3] A Preliminary Opinion on data protection and scientific research from EDPS, §3.5, p.12 https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf

[4] https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-data-protection_en.pdf

επεξεργασιών που εκτελούνται πάνω σε πληροφορίες που το πιθανότερο είναι να περιέχουν και προσωπικά δεδομένα, χρησιμοποιώντας την οργάνωση και τα τεχνικά μέσα που διαθέτει.

Είναι σημαντικό να γίνει κατανοητό, ότι η ανάγκη συμμόρφωσης του υπεύθυνου επεξεργασίας στον ΓΚΠΔ και ο τρόπος που αυτός το επιβάλει, του δημιουργεί την ανάγκη της προηγούμενης καλής οργάνωσης του Υπεύθυνου Επεξεργασίας στους τομείς που εμπλέκονται επεξεργασίες προσωπικών δεδομένων ξεκινώντας από την συλλογή τους. Έχοντας αυτό κατά νου, θα ήταν επίσης σημαντικό η τήρηση των υποχρεώσεων του ΓΚΠΔ που αναλύονται στην συνέχεια να μπορεί να συνοδευτεί με αλλαγή κουλτούρας στην αντιμετώπιση των ΠΔ με μεγαλύτερη ευαισθητοποίηση στη προστασία τους.

## 5.1 Οι Αρχές του ΓΚΠΔ ( άρθρο 5)

Σύμφωνα με τον ΓΚΠΔ η επεξεργασία των δεδομένων προσωπικού χαρακτήρα θα πρέπει να τηρεί επτά αρχές οι οποίες καθορίζουν και το πλαίσιο της συμμόρφωσης.

**Νομιμότητα, Αντικειμενικότητα και Διαφάνεια**: Τα δεδομένα προσωπικού χαρακτήρα θα πρέπει να υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων.

**Περιορισμός του Σκοπού:** Τα δεδομένα προσωπικού χαρακτήρα συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς (και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς.

**Ελαχιστοποίηση των Δεδομένων:** Τα δεδομένα προσωπικού χαρακτήρα θα πρέπει να είναι κατάλληλα, συναφή και να περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία.

**Ακρίβεια:** Τα δεδομένα που θα συλλεχθούν θα πρέπει να είναι ακριβή και, όταν είναι αναγκαίο, επικαιροποιούνται. Θα πρέπει να λαμβάνονται όλα τα εύλογα μέτρα για την άμεση διαγραφή ή διόρθωση δεδομένων προσωπικού χαρακτήρα τα οποία είναι ανακριβή, σε σχέση με τους σκοπούς της επεξεργασίας

**Περιορισμός της Περιόδου Αποθήκευσης:** Τα δεδομένα προσωπικού χαρακτήρα θα πρέπει να διατηρηθούν υπό μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων μόνο για το διάστημα που απαιτείται για τους σκοπούς της έρευνα, και εφόσον εφαρμόζονται τα κατάλληλα τεχνικά και οργανωτικά μέτρα που απαιτεί ο ΓΚΠΔ για τη διασφάλιση των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων.

**Ακεραιότητα και Εμπιστευτικότητα:** Τα δεδομένα προσωπικού χαρακτήρα θα πρέπει να υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλεια των δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά, με τη χρησιμοποίηση κατάλληλων τεχνικών ή οργανωτικών μέτρων.

**Λογοδοσία:** Ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και είναι σε θέση να αποδείξει τη συμμόρφωση με τις παραπάνω αρχές.

## 5.2 Προσωπικά δεδομένα

Προσωπικά δεδομένα σημαίνουν οποιαδήποτε πληροφορία ταυτοποιεί ένα φυσικό πρόσωπο που μπορεί να γίνει άμεσα ή έμμεσα ιδίως με αναφορά σε μοναδικό στοιχείο αναγνώρισης (αριθμός Δελτίου Ταυτότητας) ή σε έναν ή περισσότερους παράγοντες που αφορούν τη σωματική, ψυχολογική, γενετική, διανοητική, οικονομική, πολιτιστική ή κοινωνική του ταυτότητα.

- Οποιαδήποτε πληροφορία: περιλαμβάνει κάθε πληροφορία που αφορά ένα φυσικό πρόσωπο. Αυτό καλύπτει «αντικειμενικές» πληροφορίες, όπως η ημερομηνία γέννησης και «υποκειμενικές» πληροφορίες όπως η άποψη, η εκτίμηση. Ο ΓΚΠΔ δεν εφαρμόζεται για τους νεκρούς, για τους οποίους όμως ισχύει ο Αστικός Κώδικας περί προσβολής της μνήμης του νεκρού.
- Άμεσα ταυτοποιημένο ή ταυτοποιήσιμο πρόσωπο: αυτή η έννοια σχετίζεται με τις ελάχιστες από τις διαθέσιμες ήδη πληροφορίες οι οποίες επιτρέπουν να ταυτοποιηθεί μοναδικά το φυσικό πρόσωπο, όπως ο αριθμός διαβατηρίου ή ΑΔΤ, ή το ονοματεπώνυμο σε συνδυασμό με το πατρώνυμο και το μητρώνυμο.
- Έμμεσα ταυτοποιημένο ή ταυτοποιήσιμο πρόσωπο: αυτή η έννοια σχετίζεται συνήθως με την περίπτωση των μοναδικών ή σπάνιων συνδυασμών περισσότερων χαρακτηριστικών. Υπάρχουν περιπτώσεις, στις οποίες εκ πρώτης όψεως το πλήθος των διαθέσιμων χαρακτηριστικών δεν επιτρέπει σε κανέναν να ταυτοποιήσει ένα συγκεκριμένο άτομο, αλλά αυτό το άτομο μπορεί στην πραγματικότητα να είναι ταυτοποιήσιμο, διότι αυτές οι πληροφορίες σε συνδυασμό με άλλες πληροφορίες μπορούν ακόμη να επιτρέπουν τη διάκριση αυτού του ατόμου από άλλους. Επομένως, για να εξακριβωθεί εάν ένα άτομο είναι ταυτοποιήσιμο, θα πρέπει να ελεγχθεί εάν ο συνδυασμός πληροφοριών, που είναι διαθέσιμες στον υπεύθυνο επεξεργασίας ή σε οποιοδήποτε άλλο υπεύθυνο επεξεργασίας, μπορεί να οδηγήσει στην ταυτοποίηση του φυσικού προσώπου.

Ορισμένα χαρακτηριστικά είναι τόσο μοναδικά που κάποιος μπορεί να αναγνωριστεί χωρίς προσπάθεια («ο σημερινός αρχηγός της εθνικής μας ποδοσφαιρικής ομάδας»), όπως επίσης και ένας συνδυασμός χαρακτηριστικών σε διάφορες κατηγορίες πληροφοριών (ημερομηνία γέννησης, τόπος γέννησης και φύλο) μπορεί επίσης να επιτρέψει την ταυτοποίηση ενός φυσικού προσώπου, ιδίως, σε συνδυασμό με άλλες πληροφορίες που αφορούν το φυσικό πρόσωπο.

Η ταυτοποίηση με το ονοματεπώνυμο είναι η πιο κοινή περίπτωση στην πράξη, αλλά το ίδιο το όνομα μπορεί σε κάθε περίπτωση να μην είναι απαραίτητο για την ταυτοποίηση του ατόμου.

Παραδείγματα πιθανών αναγνωριστικών: αριθμός τηλεφώνου, αριθμός/οι μητρώου/ων, φυσικά χαρακτηριστικά, ψευδώνυμα, επάγγελμα, διεύθυνση, ταυτότητα του κατοικίδιου, γεωγραφική θέση κ.λπ.

Ωστόσο, εάν η ταυτοποίηση ενός υποκειμένου των δεδομένων συνεπάγεται υπερβολική προσπάθεια, το άτομο δεν θεωρείται «αναγνωρίσιμο» (βλέπε παρακάτω περί «ανωνυμοποίησης»).

Τα προσωπικά δεδομένα μπορεί να διατηρούνται σε έντυπα ή ηλεκτρονικά μέσα και να περιέχονται σε μορφή κειμένων, αριθμών, εικόνων, φωτογραφιών, ήχων κλπ.

### Κατηγοριοποιήσεις σε επίπεδο ΠΔ:

Έχοντας υπόψη τις διαμορφωμένες σχέσεις του υπεύθυνου επεξεργασίας με τα φυσικά πρόσωπα που συναλλάσσεται, είναι χρήσιμο για την καλύτερη αντίληψη των αναγκών οργάνωσης των μέτρων προστασίας των ΠΔ, να υπάρχει μια ξεκάθαρη εικόνα των ομάδων τόσο των φυσικών προσώπων όσο και των και προσωπικών τους δεδομένων που επεξεργάζεται ο υπεύθυνος επεξεργασίας, όπως:

- Κατηγορίες προσωπικών δεδομένων
    - Απλά ΠΔ (όνομα, τηλέφωνο, διεύθυνση κατοικίας και email, ΑΔΤ, μισθός κλπ)
    - Ειδικής κατηγορίας ή ευαίσθητα ΠΔ ( θέματα υγείας, εθνοτική και φυλετική καταγωγή, γενετικές και βιομετρικές πληροφορίες κλπ)
    - Προσωπικά δεδομένα που διαθέτει ήδη ο υπεύθυνος επεξεργασίας

Η παραπάνω κατηγοριοποίηση εξυπηρετεί στην διαφοροποίηση κυρίως των μέτρων προστασίας που θα πρέπει να εφαρμοστούν ώστε να μην παραβιαστούν τα δεδομένα, με ενίσχυσή τους στη περίπτωση των ευαίσθητων ΠΔ.

- Ενδεικτικές κατηγορίες φυσικών προσώπων που συμμετέχουν σε μια έρευνα
    - Ασθενείς
    - Εθελοντές (για τη συλλογή δεδομένων, ερευνητές κλπ)

- Εργαζόμενοι (ερευνητές, διοικητικοί, ορισμένου χρόνου)
- Εξωτερικοί συνεργάτες
- Παιδιά κάτω των 15 ετών
- Άτομα με ειδικές ανάγκες
- Επισκέπτες / προσκεκλημένοι

Μια τέτοια κατηγοριοποίηση βοηθά να γίνουν αντιληπτές κυρίως οι διαφορετικές διαδικασίες συναλλαγών που πρέπει να εφαρμοστούν κατά περίπτωση και τον τρόπο που αυτές θα καταστούν νόμιμες σύμφωνα με τον ΓΚΠΔ.

**Σημαντικό: Για τις προφορικές πληροφορίες που περιέχουν προσωπικά δεδομένα και που δεν πρόκειται να περιληφθούν σε σύστημα αρχειοθέτησης, δεν εφαρμόζεται ο ΓΚΠΔ.**

## 5.3 Ο σκοπός και η αντικειμενικότητα της επεξεργασίας

Ο σκοπός μιας επεξεργασίας ΠΔ εμπεριέχεται στην αρχή αντικειμενικότητας η οποία διέπει πρωτίστως τη σχέση μεταξύ του υπευθύνου επεξεργασίας και του φυσικού προσώπου. *Οι πράξεις επεξεργασίας δεν πρέπει να διενεργούνται μυστικά, και τα φυσικά πρόσωπα θα πρέπει να έχουν επίγνωση των δυνητικών κινδύνων. Εάν ο σκοπός της επεξεργασίας είναι επαρκώς συγκεκριμένος και σαφής, τα άτομα γνωρίζουν τί να περιμένουν και αυξάνονται η διαφάνεια και η ασφάλεια δικαίου*[5].

*Επιπλέον, στο μέτρο που είναι εφικτό, οι υπεύθυνοι επεξεργασίας πρέπει να ενεργούν κατά τρόπο που συμμορφώνεται άμεσα με τις επιθυμίες του υποκειμένου των δεδομένων, ιδίως όταν η συγκατάθεση αυτού αποτελεί τη νομική βάση για την επεξεργασία τους. Ταυτόχρονα, η σαφής οριοθέτηση του σκοπού είναι σημαντική προϋπόθεση ώστε τα υποκείμενα των δεδομένων να μπορούν να ασκούν αποτελεσματικά τα δικαιώματά τους, όπως το δικαίωμα εναντίωσης στην επεξεργασία.*

*Σε κάθε περίπτωση, η αρχή της αντικειμενικότητας προχωρά πέραν από τις υποχρεώσεις της διαφάνειας και θα μπορούσε επίσης να συνδέεται με την επεξεργασία δεδομένων προσωπικού χαρακτήρα με δεοντολογικό τρόπο.* ***Ο σκοπός επεξεργασίας θα πρέπει να είναι δίκαιος και νόμιμος****.*

*Τα κύρια σημεία της σχέσης του σκοπού με την επεξεργασία είναι:*

- *Ο σκοπός της επεξεργασίας δεδομένων πρέπει να καθορίζεται προτού ξεκινήσει η επεξεργασία.*

[5] για περισσότερα δες στο Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων, §3.1,2, §3.2, έκδοση 2018

- *Δεν επιτρέπεται περαιτέρω επεξεργασία των δεδομένων κατά τρόπο ασύμβατο προς τον αρχικό σκοπό, παρότι ο ΓΚΠΔ προβλέπει εξαιρέσεις από τον κανόνα αυτό για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς. Οι εξαιρέσεις αναλύονται στην συνέχεια.*
- *Κατ' ουσία, η αρχή του περιορισμού του σκοπού σημαίνει ότι κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα πρέπει να πραγματοποιείται για συγκεκριμένο, καλά καθορισμένο σκοπό και μόνο για πρόσθετους, συγκεκριμένους σκοπούς οι οποίοι είναι συμβατοί προς τον αρχικό*.
- Ένας καλά καθορισμένος σκοπό μιας επεξεργασίας καθορίζει επίσης και την ορθή τήρηση και των άλλων αρχών του ΓΚΠΔ:
- Υπάρχει ορθή ενημέρωση των φυσικών προσώπων (αρχή της Διαφάνειας)
- συλλέγονται μόνο τα δεδομένα που είναι πρόσφορα, σχετικά και όχι περισσότερα για την επίτευξη του στόχου (αρχή της Ελαχιστοποίησης)
- προσδιορίζεται ο χρόνος διατήρησης που εξυπηρετεί καλύτερα τους σκοπούς (αρχή του Περιορισμού της Περιόδου Αποθήκευσης)

Σε σχέση με τους σκοπούς επεξεργασίας, υπάρχουν δύο τύποι χρήσης δεδομένων σε μια επιστημονική έρευνα[6]:

*α) Έρευνα σε προσωπικά δεδομένα που συλλέγονται απευθείας για σκοπούς επιστημονικής έρευνας («πρωτογενής χρήση»).*

*β) Έρευνα σε προσωπικά δεδομένα που συνίσταται στην περαιτέρω επεξεργασία δεδομένων που συλλέχθηκαν αρχικά για άλλο σκοπό («δευτερεύουσα χρήση»). Μια τέτοια χρήση είναι νόμιμη αν πριν από την εν λόγω επεξεργασία το φυσικό πρόσωπο είχε παράσχει συγκατάθεση κατά την συλλογή των ΠΔ ή έχει δώσει ξεχωριστή συγκατάθεση ή επιτρέπεται από το εθνικό ή ευρωπαϊκό δίκαιο.*

*Παράδειγμα 1: Για τη διεξαγωγή κλινικής δοκιμής σε άτομα που είναι ύποπτα ότι έχουν μολυνθεί από έναν ιό, συλλέγονται δεδομένα για την υγεία και χρησιμοποιούνται ερωτηματολόγια. Πρόκειται για μια περίπτωση «πρωτογενούς χρήσης» δεδομένων υγείας όπως ορίζεται παραπάνω.*

*Παράδειγμα 2: Ένα φυσικό πρόσωπο έχει επισκεφτεί ως ασθενής ένα πάροχο υπηρεσιών υγείας σχετικά με τα συμπτώματα π.χ. του SARS-CoV-2. Εάν τα δεδομένα υγείας που καταγράφονται από τον πάροχο*

[6] Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak, EDPB, 21 April, 2020

*υπηρεσιών υγείας χρησιμοποιηθούν αργότερα για σκοπούς επιστημονικής έρευνας, αυτή η χρήση αξιολογείται ως περαιτέρω επεξεργασία δεδομένων υγείας (δευτερεύουσα χρήση) που έχουν συλλεχθεί για άλλο αρχικό σκοπό*.

Σε μια επεξεργασία ΠΔ η διάκριση με βάση την πρωτογενή ή δευτερογενή χρήση τους είναι σημαντική όταν εξετάζεται η νομική βάση της επεξεργασίας και οι υποχρεώσεις πληροφόρησης του φυσικού προσώπου, όπως θ' αναλυθεί στη συνέχεια.

## 5.4 Νομιμότητα της Επεξεργασίας σε μια επιστημονική έρευνα

Κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα για σκοπούς επιστημονικής έρευνας, συμπεριλαμβανομένης και της έρευνας σε θέματα ευαίσθητων προσωπικών δεδομένων, πρέπει να συμμορφώνεται με τις αρχές του ΓΚΠΔ και με μια από τις νομικές βάσεις και τις ειδικές παρεκκλίσεις που αναφέρονται αντίστοιχα στα άρθρα 6 και 9 του ΓΚΠΔ για να είναι νόμιμη.

Ο ΓΚΠΔ αναγνωρίζει την ανάγκη της επιστημονικής έρευνας μέσα μέσα από την αιτιολογική σκέψη 33 του ΓΚΠΔ :

*«Συχνά, δεν είναι δυνατόν να προσδιορίζεται πλήρως ο σκοπός της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα για σκοπούς επιστημονικής έρευνας κατά τον χρόνο συλλογής των δεδομένων. Ως εκ τούτου, τα υποκείμενα των δεδομένων θα πρέπει να μπορούν να δώσουν τη συγκατάθεσή τους για ορισμένους τομείς της επιστημονικής έρευνας, όταν ακολουθούνται τα αναγνωρισμένα πρότυπα δεοντολογίας για την επιστημονική έρευνα. Τα υποκείμενα των δεδομένων θα πρέπει να έχουν τη δυνατότητα να παρέχουν τη <u>συναίνεσή</u> τους μόνο σε ορισμένους τομείς της έρευνας ή μόνο σε μέρη προγραμμάτων έρευνας, στον βαθμό που επιτρέπεται από τον επιδιωκόμενο σκοπό*.»

### Ενημερωμένη Συγκατάθεση

Η συγκατάθεση ως νομική βάση και ως προς τους όρους που μπορεί να παρασχεθεί προβλέπονται στα άρθρα του ΓΚΠΔ 6(1)(α), 9(2)(α), 7, και το 8 που αναφέρεται στα παιδιά. Να σημειωθεί ότι με βάση τον ν.4624/2019, τα παιδιά στην Ελλάδα πάνω από τα 15 έτη μπορούν να παράσχουν τα ίδια συγκατάθεση για τα ΠΔ.

Πριν την λήψη της συγκατάθεσης, πρέπει να παρασχεθούν στο φυσικό πρόσωπο όλες οι πληροφορίες με σαφή και συνοπτικό τρόπο, λαμβάνοντας υπόψη και τις αντιληπτικές του δεξιότητες, ώστε να γνωρίζει και να καταλαβαίνει τα θέματα της επεξεργασίας των προσωπικών του δεδομένων. Στο άρθρο 13 και 14 τον ΓΚΠΔ αναφέρονται αναλυτικά όλες οι πληροφορίες που θα πρέπει να το παρασχεθούν.

Αναλυτική περιγραφή για την κατανόηση της συγκατάθεσης παραθέτει στον αντίστοιχο οδηγό της η πρώην Ομάδα του Άρθρου 29[7].

Ο Ευρωπαίος Επίτροπος Προστασίας Δεδομένων (EDPS) συνοψίζει τα θέματα της συγκατάθεσης στην προκαταρτική του γνώμη που εξέδωσε για την έρευνα[8] και το Ευρωπαϊκό πανεπιστημιακό ίδρυμα με τον οδηγό Καλών πρακτικών Προστασίας Δεδομένων στην Έρευνα[9] παρέχει χρήσιμες συμβουλές στη σύνταξη μια ενημερωμένης συγκατάθεσης.

Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (EDPB) επικεντρώνεται στη συγκατάθεση για την έρευνα στην υγεία[10] με αφορμή την πανδημία COVID-19.

Θα πρέπει να σημειωθεί ότι τα φυσικά πρόσωπα που συμμετέχουν σε μια επιστημονική έρευνα, έχουν το δικαίωμα να ανακαλέσουν την συγκατάθεσή τους ανά πάσα στιγμή. Η ανάκληση της συγκατάθεσης δε θίγει τη νομιμότητα της επεξεργασίας που βασίστηκε σε αυτή και έγινε πριν της ανάκλησής της.

### Εθνική νομοθεσία

Ο εφαρμοστικός νόμος για την προστασία των προσωπικών δεδομένων ν.4624/2019, με το άρθρο 30 *«Επεξεργασία δεδομένων προσωπικού χαρακτήρα για σκοπούς επιστημονικής ή ιστορικής έρευνας ή συλλογής και τήρησης στατιστικών στοιχείων»,* για τα ευαίσθητα προσωπικά δεδομένα ορίζει ότι:

«*Κατά παρέκκλιση από το άρθρο 9 παράγραφος 1 του ΓΚΠΔ η επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα, με την έννοια της παραγράφου 1 του άρθρου 9 του ΓΚΠΔ, επιτρέπεται χωρίς τη συγκατάθεση του υποκειμένου, όταν η επεξεργασία είναι απαραίτητη για σκοπούς επιστημονικής ή ιστορικής έρευνας ή συλλογής και τήρησης στατιστικών στοιχείων και το συμφέρον του υπεύθυνου επεξεργασίας είναι υπέρτερο του συμφέροντος του υποκειμένου να μην τύχουν επεξεργασίας τα δεδομένα προσωπικού του χαρακτήρα. Ο υπεύθυνος επεξεργασίας υποχρεούται να λαμβάνει κατάλληλα και συγκεκριμένα μέτρα για την προστασία των εννόμων συμφερόντων του υποκειμένου των δεδομένων*.»

Θεσπίζει σύμφωνα με το άρθρο 89 (1) του ΓΚΠΔ τις κατάλληλες εγγυήσεις ορίζοντας τα ελάχιστα τεχνικά και οργανωτικά μέτρα που πρέπει να λαμβάνει ο υπεύθυνος επεξεργασίας για να διασφαλιστούν τα δικαιώματα και οι ελευθερίες των φυσικών προσώπων, και τα οποία είναι:

α) περιορισμοί πρόσβασης των υπεύθυνων επεξεργασίας και εκτελούντων την επεξεργασία·

---

[7] δες «Οδηγίες για την Συγκατάθεση για τον ΓΚΠΔ» της πρώην Ομάδας του Άρθρου 29 , WP259 rev. 01, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

[8] A Preliminary Opinion on data protection and scientific research from EDPS, §6.3, p.17 https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf

[9] https://www.eui.eu/Documents/ServicesAdmin/DeanOfStudies/ResearchEthics/Guide-Data-Protection-Research.pdf , European University Institute, p.9

[10] Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak, EDPB, 21 April, 2020

β) ψευδωνυμοποίηση των δεδομένων προσωπικού Χαρακτήρα

γ) κρυπτογράφηση των δεδομένων προσωπικού χαρακτήρα

δ) ορισμός ΥΠΔ

ε) ανωνυμοποίηση των δεδομένων μόλις το επιτρέψουν οι επιστημονικοί ή στατιστικοί σκοποί, εκτός εάν αυτό είναι αντίθετο προς το έννομο συμφέρον του υποκειμένου των δεδομένων.

Για τη νομιμοποίηση της επεξεργασίας για επιστημονικούς σκοπούς επιπλέον πρέπει να τηρείται και η ελάχιστη προϋπόθεση που θέτει το άρθρο 89(1) του ΓΚΠΔ που αφορά την ελαχιστοποίηση των προσωπικών δεδομένων.

Μια τέτοια προϋπόθεση μπορεί να θεωρηθεί ότι καλύπτεται με την ανωνυμοποίηση των δεδομένων αν και στην αιτιολογική σκέψη του νόμου 4624/2019 δεν υπονοείται κάτι ανάλογο.

Αξίζει επίσης να σημειωθεί ότι στη Γνωμοδότηση 1/2020 της Αρχής Προστασίας για την αξιολόγηση του παραπάνω εφαρμοστικού νόμου, δεν γίνεται καμία παρατήρηση για το συγκεκριμένο άρθρο 30, γεγονός που αποτελεί μια απόδειξη συμμόρφωση του άρθρου με τις διατάξεις του ΓΚΠΔ.

# 6. Τεχνικά Μέτρα

Η ασφάλεια των προσωπικών δεδομένων ακολουθεί στην πράξη τις γενικές αρχές της ασφάλειας των πληροφοριών και της διαχείρισης κινδύνων ασφάλειας των πληροφοριών, όπως αυτές παρουσιάζονται στις προηγούμενες παραγράφους. Ωστόσο, τα προσωπικά δεδομένα έχουν ορισμένες ιδιαιτερότητες που πρέπει να λαμβάνονται υπόψη κατά την ανάλυση των κινδύνων ασφάλειας και την υιοθέτηση μέτρων ασφαλείας.

Είναι σημαντικό να υιοθετηθούν κατάλληλα μέτρα ασφάλειας και πολιτικές εμπιστευτικότητας, διασφαλίζοντας ότι τα προσωπικά δεδομένα δεν αποκαλύπτονται σε μη εξουσιοδοτημένα μέρη. Τα μέτρα που εφαρμόζονται για τη διαχείριση της τρέχουσας έκτακτης ανάγκης και της υποκείμενης διαδικασίας λήψης αποφάσεων πρέπει να τεκμηριώνονται κατάλληλα.

Αν και τον ΓΚΠΔ δεν παρέχει άμεση αναφορά σε τεχνολογίες ενίσχυσης της προστασίας της ιδιωτικής ζωής, εξετάζει συγκεκριμένα την ψευδωνυμοποίηση και την κρυπτογράφηση ως βασικά μέτρα προστασίας για την ασφάλεια των προσωπικών δεδομένων. Το σημείο αυτό συνδέεται με τις διατάξεις του ΓΚΠΔ για την προστασία των δεδομένων από το σχεδιασμό και από προεπιλογή (άρθρο 25), οι οποίες δίνουν έμφαση στη σχεδίαση των απαιτήσεων προστασίας της ιδιωτικής ζωής στα συστήματα και στις υπηρεσίες ΤΠ, πέρα από την «παραδοσιακή» κατανόηση της ασφάλειας. Ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) εκπόνησε μια ενδιαφέρουσα εργασία για την ιδιωτικότητα και προστασία των δεδομένων από τον σχεδιασμό (Privacy and Data Protection by Design – from policy to engineering) *που συμβάλλει στη γεφύρωση του χάσματος μεταξύ του νομικού πλαισίου και των διαθέσιμων τεχνολογικών μέτρων εφαρμογής, παρέχοντας έναν κατάλογο των υπαρχουσών προσεγγίσεων, των στρατηγικών σχεδιασμού της ιδιωτικής ζωής και των τεχνικών δομικών στοιχείων για διάφορους βαθμούς ωριμότητας από την έρευνα και την ανάπτυξη*[11].

Επίσης και το EDPB εξέδωσε τις οδηγίες 4/2019 για το άρθρο 25 που *καλύπτουν στοιχεία που πρέπει να λάβουν υπόψη οι υπεύθυνοι επεξεργασίας κατά το σχεδιασμό της επεξεργασίας. Τα κριτήρια της «τελευταίας τεχνολογίας» απαιτούν από τους υπεύθυνους επεξεργασίας να ενημερώνονται σχετικά με την τεχνολογική πρόοδο προκειμένου να διασφαλίζεται η συνεχής αποτελεσματική εφαρμογή των αρχών προστασίας δεδομένων. Το «κόστος υλοποίησης» απαιτεί από τον υπεύθυνο επεξεργασίας να λαμβάνει υπόψη το κόστος και τους πόρους που απαιτούνται για την αποτελεσματική εφαρμογή και τη συνεχή συντήρηση όλων των αρχών προστασίας δεδομένων καθ 'όλη τη διάρκεια της επεξεργασίας. Άλλα στοιχεία που πρέπει να λάβουν υπόψη οι υπεύθυνοι επεξεργασίας είναι η φύση, το πεδίο εφαρμογής, το*

[11]Privacy and Data Protection by Design – from policy to engineering
https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design

*πλαίσιο και ο σκοπός της επεξεργασίας και ο κίνδυνος διαφορετικής πιθανότητας και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων που θέτει η επεξεργασία*[12]

Η ασφάλεια των πληροφοριών περιλαμβάνει όλα τα μέτρα που λαμβάνονται για την προστασία των πληροφοριών από μη εξουσιοδοτημένη πρόσβαση, χρήση, αποκάλυψη, διακοπή, τροποποίηση, εξέταση, επιθεώρηση, καταγραφή ή καταστροφή. Το πιο χρησιμοποιούμενο μοντέλο για την καθοδήγηση της ανάπτυξης και της εφαρμογής ενός πλαισίου για τη διαχείριση της ασφάλειας των πληροφοριών αντιπροσωπεύεται από την αποκαλούμενη τριάδα της CIA: Εμπιστευτικότητα (Confidentiality) , Ακεραιότητα (Integrity) και Διαθεσιμότητα (Availability) πληροφοριών.

## 6.1 Εμπιστευτικότητα (Confidentiality)

Τα δεδομένα θα πρέπει να προστατεύονται από μη εξουσιοδοτημένη αποκάλυψή (ανάγνωση) τους. Ενδεικτικά κατάλληλα μέτρα προς την κατεύθυνση αυτή είναι:

### Ανωνυμοποίηση

*Η ανωνυμοποίηση είναι μια διαδικασία με την οποία τα προσωπικά δεδομένα τροποποιούνται αμετάκλητα με τέτοιο τρόπο ώστε ένα υποκείμενο των δεδομένων να μην μπορεί πλέον να αναγνωριστεί άμεσα ή έμμεσα, είτε από τον Υπεύθυνο Επεξεργασίας μόνο του είτε σε συνεργασία με οποιοδήποτε άλλο μέρος* (ISO / TS 25237: 2017)

Στην αιτιολογική σκέψη 26 εξετάζονται και άλλοι παράγοντες για τον χαρακτηρισμό των πληροφοριών ως ανώνυμων. Σύμφωνα με αυτή, *για να κριθεί κατά πόσον ένα φυσικό πρόσωπο είναι ταυτοποιήσιμο, θα πρέπει να λαμβάνονται υπόψη όλα τα μέσα τα οποία είναι ευλόγως πιθανό ότι θα χρησιμοποιηθούν, όπως για παράδειγμα ο διαχωρισμός του, είτε από τον υπεύθυνο επεξεργασίας είτε από τρίτο για την άμεση ή έμμεση εξακρίβωση της ταυτότητας του φυσικού προσώπου. Για να διαπιστωθεί κατά πόσον κάποια μέσα είναι ευλόγως πιθανό ότι θα χρησιμοποιηθούν για την εξακρίβωση της ταυτότητας του φυσικού προσώπου, θα πρέπει να λαμβάνονται υπόψη όλοι οι αντικειμενικοί παράγοντες, όπως τα έξοδα και ο χρόνος που απαιτούνται για την ταυτοποίηση, λαμβανομένων υπόψη της τεχνολογίας που είναι διαθέσιμη κατά τον χρόνο της επεξεργασίας και των εξελίξεων της τεχνολογίας. Οι αρχές της προστασίας δεδομένων δεν θα πρέπει συνεπώς να εφαρμόζονται σε ανώνυμες πληροφορίες, δηλαδή πληροφορίες που δεν σχετίζονται προς ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο ή σε δεδομένα προσωπικού*

[12] Guidelines 4/2019 on Article 25 Data Protection by Design and by Default https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en

*χαρακτήρα που έχουν καταστεί ανώνυμα κατά τρόπο ώστε η ταυτότητα του υποκειμένου των δεδομένων να μην μπορεί ή να μην μπορεί πλέον να εξακριβωθεί*.

Τεχνικές ανωνυμοποίησης περιλαμβάνουν:

- Τυχαιοποίηση των προσωπικών δεδομένων, όπου τα στοιχεία αναγνώρισης αντικαθίστανται από πληροφορίες που αυξάνουν τον βαθμό αβεβαιότητας
- Γενίκευση των προσωπικών δεδομένων με την δημιουργία μεγαλύτερων συνόλων φυσικών προσώπων που αντιπροσωπεύουν. Για παράδειγμα αναφορά σε μεγαλύτερη περιοχή κατοικίας αντί συγκεκριμένη διεύθυνση ή εύρος ηλικίας αντί συγκεκριμένης ηλικίας. Σημαντικό είναι ότι πρέπει το πλήθος, των φυσικών προσώπων από τομή των συνόλων ανά χαρακτηριστικό, να είναι μεγάλο ώστε να μην είναι ευλόγως πιθανόν να χρησιμοποιηθούν κάποια μέσα για την εξακρίβωση της ταυτότητας.

Με την ανωνυμία επιτυγχάνεται η πλήρη αποδέσμευση από τις υποχρεώσεις του ΓΚΠΔ , αφού πλέον δεν υπάρχει αντικείμενο εφαρμογής.

### Ψευδωνυμοποίηση

Η ψευδωνυμοποίηση, σύμφωνα με τον ορισμό της, είναι μια τεχνική διαχωρισμού των πληροφοριών με παράλληλη χρήση τεχνικών και οργανωτικών μέτρων για την διασφάλιση ότι οι πληροφορίες αυτές δεν μπορούν να αποδοθούν σε ένα φυσικό πρόσωπο. Ο ΓΚΠΔ επιβεβαιώνει στην αιτιολογική σκέψη 26 ότι τα ψευδώνυμοποιημένα δεδομένα πρέπει να αντιμετωπίζονται ως προσωπικά δεδομένα (σύμφωνα με την προηγούμενη γνώμη της ομάδας εργασίας του άρθρου 29). Αυτή η θέση προκύπτει από την αυξημένη ευπάθεια των υποκειμένων των δεδομένων που θα μπορούσαν ενδεχομένως να ταυτοποιηθούν σε σύγκριση με την προστασία που τους παρείχε πραγματική ανωνυμοποίηση - εάν ο κωδικός κλειδιού παραβιαστεί, τότε όλα τα δεδομένα μπορούν να συνδεθούν με ένα άτομο για άλλη μια φορά.

Βασικό χαρακτηριστικό που διαφοροποιεί την ανωνυμοποίηση από την ψευδωνυμοποίηση είναι ότι στην δεύτερη υπάρχει μια πρόσθεση πληροφορία η οποία επιτρέπει την αντιστοίχιση των ψευδωνύμων με τα πραγματικά δεδομένα (αναγνωριστικά) , ο πίνακας ψευδωνυμοποίησης (pseudonymisation secret).

**Τεχνικές ψευδωνυμοποίησης με αντικατάσταση του αναγνωριστικού από:**

- Σειριακό μετρητή
- Γεννήτρια τυχαίων τιμών από ένα σύνολο με ίδια πιθανότητα επιλογής (Random number generator (RNG))
- μια κρυπτογραφική συνάρτηση κατακερματισμού που χρησιμοποιεί το αναγνωριστικό (Cryptographic hash function)

- Κώδικας Αυθεντικοποίησης μηνύματος (Message authentication code (MAC))
- Κρυπτογράφηση των αναγνωριστικών

Ισοδύναμη των τεχνικών ψευδωνυμοποίησης είναι και ο τρόπος (πολιτική) για την πρακτική εφαρμογής τους και την υλοποίηση του αντίστοιχου πίνακα ψευδωνυμοποίησης. Τέτοιες πολιτικές είναι:

- Αιτιοκρατική ψευδωνυμοποίηση (Deterministic pseudonymisation), όπου το κάθε αναγνωριστικό αντικαθίσταται από ένα συγκεκριμένο ψευδώνυμο.
- Τυχαιοποιημένη με τεκμηρίωση ψευδωνυμοποίηση (Document-randomized pseudonymisation), όπου κάθε αναγνωριστικό αντιστοιχίζεται σε σύνολο διαφορετικών ψευδωνύμων ανά dataset, αλλά το ίδιο για κάθε dataset.
- Πλήρως τυχαιοποιημένη ψευδωνυμοποίηση ( Fully-randomized pseudonymisation), όπου κάθε αναγνωριστικό αντιστοιχίζεται σε τυχαία κάθε φορά ψευδώνυμα.

Τις παραπάνω τεχνικές και πολιτικές ψευδωνυμοποίησης, καθώς και περισσότερες πληροφορίες γύρω από την ψευδωνυμοποίηση, καθώς και τεχνικές λύσεις που μπορούν να υποστηρίξουν την εφαρμογή της στην πράξη, υπάρχουν την αντίστοιχη έκθεση της ENISA **Pseudonymisation techniques and best practices**[13]**.**

### Κρυπτογράφηση

Κάθε πληροφοριακό σύστημα είναι ευάλωτο σε θέματα ασφάλειας και απαιτεί ιδιαίτερη προσοχή. Στην περίπτωση των ιατρικών δεδομένων και άλλων ατομικών δεδομένων, απαιτείται αυστηρώς η διασφάλισή τους καθώς η έκθεσή τους σε μη εξουσιοδοτημένα πρόσωπα, ενδέχεται να πλήξει τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Η κρυπτογράφηση των δεδομένων αποτελεί βασική προϋπόθεση, ώστε ακόμα και να μπορέσει κάποιος να αποσπάσει τα δεδομένα, να μην είναι σε θέση να τα αναγνώσει. Η σύσταση προς την κατεύθυνση αυτή είναι η κρυπτογράφηση να είναι σύμφωνα με τους τελευταίους αλγορίθμους.

## 6.2 Ακεραιότητα (Integrity)

Τα δεδομένα θα πρέπει να προστατεύονται από μη εξουσιοδοτημένη μεταβολή (τροποποίηση ή διαγραφή) τους.

### Έλεγχος Προσβάσεων

Είναι ύψιστης σημασίας να διαβαθμιστούν τα επίπεδα πρόσβασης στις πληροφορίες της έρευνας και τεθούν εξ αρχής οι απαιτήσεις για τον έλεγχο πρόσβασης σε αυτές. Για την παραχώρηση των

[13] https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices

δικαιωμάτων πρόσβασης θα πρέπει να εφαρμοστούν οι αρχές του “διαχωρισμού των καθηκόντων” και των “ελάχιστων δικαιωμάτων”.

Ο έλεγχος των προσβάσεων επίσης ενισχύεται με την διαχείριση των κωδικών πρόσβασης σε υπολογιστικά συστήματα, αλλά και πρόσβασης σε χώρους.

### 6.3 Διαθεσιμότητα (Availability)

Τα δεδομένα θα πρέπει να είναι προσβάσιμα (από τους εξουσιοδοτημένους χρήστες) χωρίς εμπόδια ή καθυστέρηση.

#### Λήψη Αντιγράφων Ασφάλειας Συστημάτων και Πληροφοριών

Για την προστασία της διαθεσιμότητας των δεδομένων, είναι καίρια η τακτική λήψη αντιγράφων ασφάλειας των κρίσιμων συστημάτων, εφαρμογών και αρχείων της υπολογιστικής και δικτυακής υποδομής με τρόπο ώστε να διασφαλιστεί ότι σε περίπτωση ανεπανόρθωτης βλάβης είτε του λειτουργικού συστήματος είτε των διαφόρων προγραμμάτων ή αρχείων είτε των διαφόρων υλικών του συστήματος, ελαχιστοποιείται η περίοδος διακοπής της ομαλής λειτουργίας.

Επιπλέον θα πρέπει να διασφαλιστεί, ότι ο εξοπλισμός που χρησιμοποιείται στο πλαίσιο της έρευνας, μπορεί να ανακτήσει τη λειτουργία του εντός μιας λογικής χρονικής περιόδου μετά από οποιαδήποτε ζημιά που μπορεί να οφείλεται σε κακόβουλες επιθέσεις ή τυχόν ατυχήματα στον εξοπλισμό.

## 7. Οργανωτικά μέτρα

### 7.1 Εκτίμηση αντικτύπου σχετικά με την προστασία ερευνητικών δεδομένων

Σύμφωνα με τον ΓΚΠΔ, όταν το είδος επεξεργασίας, ιδίως με χρήση νέων τεχνολογιών και συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, θα πρέπει να διενεργηθεί, πριν από την επεξεργασία, εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα. Σε μία εκτίμηση μπορεί να εξετάζεται ένα σύνολο παρόμοιων πράξεων επεξεργασίας οι οποίες ενέχουν παρόμοιους υψηλούς κινδύνους.

Οι επιστημονικές έρευνες σε θέματα με ευαίσθητα προσωπικά δεδομένα και ειδικά με δεδομένα υγείας, γενετικών και βιομετρικών χαρακτηριστικών θα πρέπει θα συνοδεύονται πάντα από μια μελέτη εκτίμησης αντικτύπου.

Σκοπός της εκτίμησης αυτής είναι να διασφαλιστεί ότι η επεξεργασία των προσωπικών δεδομένων γίνεται πλήρως κατανοητή, ότι οι κίνδυνοι για τις ελευθερίες και τα δικαιώματα των υποκειμένων των δεδομένων αυτών εξετάζονται προσεκτικά και ότι θεσπίζονται όλα τα κατάλληλα μέτρα για την προστασία τους και τον μετριασμό των κινδύνων κατά τη διάρκεια του κύκλου ζωής των προσωπικών δεδομένων.

Οι μελέτες εκτίμησης αντικτύπου μιας επεξεργασίας αποτελούν την απόδειξη συμμόρφωσης της με τον ΓΚΠΔ.

Η εκτίμηση αντικτύπου θα πρέπει να περιέχει τουλάχιστον:

- Τη συστηματική περιγραφή των προβλεπόμενων πράξεων επεξεργασίας και των σκοπών της επεξεργασίας, περιλαμβανομένου, κατά περίπτωση, του έννομου συμφέροντος που επιδιώκει ο υπεύθυνος επεξεργασίας,
- Την εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας σε συνάρτηση με τους σκοπούς,
- Την εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων που αναφέρονται στην παράγραφο 1 και
- Τα προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων, περιλαμβανομένων των εγγυήσεων, των μέτρων και μηχανισμών ασφάλειας, ώστε να διασφαλίζεται η προστασία των δεδομένων προσωπικού χαρακτήρα και να αποδεικνύεται η συμμόρφωση προς τον παρόντα κανονισμό, λαμβάνοντας υπόψη τα δικαιώματα και τα έννομα συμφέροντα των υποκειμένων των δεδομένων και άλλων ενδιαφερόμενων προσώπων,
- Λήψη απόφασης (decision) σχετικά με τον τρόπο που θα ικανοποιηθούν οι βασικές αρχές για την προστασία της ιδιωτικότητας και για την αντιμετώπιση των κινδύνων που έχουν εντοπιστεί,
- εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων (υποκειμένων των δεδομένων),
- τα προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων, περιλαμβανομένων των εγγυήσεων, των μέτρων και μηχανισμών ασφάλειας, ώστε να διασφαλίζεται η προστασία των δεδομένων προσωπικού χαρακτήρα και να αποδεικνύεται η συμμόρφωση προς τον κανονισμό, λαμβάνοντας υπόψη τα δικαιώματα και τα έννομα συμφέροντα των υποκειμένων των δεδομένων και άλλων ενδιαφερόμενων προσώπων,
- Διαβούλευση με την ΑΠΔΠΧ σύμφωνα με το άρθρο 36 του Κανονισμού εφόσον κρίνεται ότι ακόμα και με τα προτεινόμενα στην εκτίμηση αντικτύπου μέτρα μετριασμού των κινδύνων, αυτοί παραμένουν υψηλοί.

## 7.2 Συνεργασίες του φορέα έρευνας

Κατά την υλοποίηση μιας επιστημονικής έρευνας φορέας έρευνας μπορεί να λειτουργεί ως υπεύθυνος επεξεργασίας, αλλά και ως εκτελών την επεξεργασία.

Ως υπεύθυνος επεξεργασίας αναπτύσσει συνεργασίες με τρεις κατηγορίες συνεργατών: από κοινού υπεύθυνους επεξεργασίας, εκτελούντες την επεξεργασία και συνεργάτες με σύμβαση εξαρτημένης εργασίας.

### Από κοινού Υπεύθυνοι επεξεργασίας ( Join Controllers)

Από το ορισμό των από κοινού Υπευθύνων Επεξεργασίας μία υποχρέωσή υπεύθυνου επεξεργασίας είναι ότι πρέπει να αποφασίσει με τους άλλους υπεύθυνους επεξεργασίας ποιος θα εκτελέσει και τι από τις δεσμεύσεις του ΓΚΠΔ. Ωστόσο, ανεξάρτητα από αυτές τις ρυθμίσεις, κάθε υπεύθυνος επεξεργασίας παραμένει υπεύθυνος για τη συμμόρφωση με όλες τις υποχρεώσεις των υπευθύνων επεξεργασίας.

Σε ένα χρηματοδοτούμενο ερευνητικό έργο, οι μεταξύ τους σχέσεις των μελών ρυθμίζονται ήδη από μια κύρια σύμβαση (grant agreement) που καθορίζει τις υποχρεώσεις τους ως προς έργο και με βάση τις οποίες στη συνέχεια αναγνωρίζονται οι από κοινού υπεύθυνοι επεξεργασίας.

Για τα προσωπικά δεδομένα σαν αντικείμενο έρευνας που διακινούνται μεταξύ των μελών του έργου, πολλές φορές υπάρχει η ανάγκη να τεθούν ειδικές ρυθμίσεις οι οποίες θα πρέπει να συμπεριλαμβάνονται σε μια σύμβαση (data sharing agreement). Σε αυτή πρέπει να καθορίζονται πιο εξειδικευμένα οι συμφωνημένοι ρόλοι και ευθύνες, όπως, έναντι των φυσικών προσώπων (της ενημέρωσης και τρόπου άσκησης των δικαιωμάτων τους), έναντι των περιπτώσεων παραβίασης, την χρήση των προσωπικών δεδομένων μετά την λήξη του έργου.

Η ενημέρωση των φυσικών προσώπων θα πρέπει να περιλαμβάνει τα κύρια σημεία που τους αφορούν και κυρίως στην περίπτωση της συγκατάθεσης.

Το φυσικό πρόσωπο μπορεί να ασκήσει τα δικαιώματα του και να ζητήσει αποζημίωση έναντι και κατά καθενός από τους υπευθύνους επεξεργασίας. Κάθε από κοινού υπεύθυνος επεξεργασίας θα είναι υπεύθυνος για ολόκληρη τη ζημιά που προκαλείται από την επεξεργασία, εκτός εάν μπορεί να αποδείξει ότι δεν είναι καθόλου υπεύθυνος για το συμβάν που προκαλεί τη ζημία. Η όποια ρύθμιση που γίνεται μεταξύ των υπεύθυνων επεξεργασίας για τον σκοπό αυτό δεν έχει ισχύ.

Εάν ένας από κοινού υπεύθυνος επεξεργασίας χρειάστηκε να αποζημιώσει ένα άτομο, αλλά θεωρεί ότι δεν είναι πλήρως υπεύθυνος για την ζημία, ενδέχεται να μπορεί να διεκδικήσει από έναν άλλο υπεύθυνο επεξεργασίας (ή εκτελούντα την επεξεργασία) το μέρος της αποζημίωσης για την οποία ευθύνονται.

Επιπλέον, όλοι οι από κοινού υπεύθυνοι επεξεργασίας ευθύνονται πλήρως έναντι των εποπτικών αρχών για μη συμμόρφωση με τον ΓΚΠΔ.

Σε ένα ερευνητικό έργο ενδέχεται να μετέχουν και μέλη που δεν ανήκουν στον ΕΟΧ και στα οποία αποστέλλονται προσωπικά δεδομένα. Η περίπτωση αυτή αποτελεί διεθνή διαβίβαση και αντιμετωπίζεται στην επόμενη ενότητα ***7.3 Διεθνή διαβίβαση ερευνητικών*** δεδομένων.

### Εκτελούντες την επεξεργασία (Processors)

Εκτελών την επεξεργασία είναι: «φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας».

Από τον ορισμό είναι φανερό ότι ως εκτελούντες την επεξεργασία μπορούν να θεωρηθούν και οι ερευνητές των οποίων η σχέση με τον υπεύθυνό επεξεργασίας βασίζεται σε σύμβαση έργου όπου *το βασικό αντικείμενο της συμβάσεως είναι το αποτέλεσμα της εργασιακής δραστηριότητας, ήτοι το δημιούργημα (προϊόν) της εργασίας, στην οποία δεν ενδιαφέρει η ανθρώπινη ενέργεια η οποία παράγει το αποτέλεσμα, αλλά αυτό τούτο το αποτέλεσμά της*[14].

Όπως αναφέρθηκε και στην αρχή της ενότητας, ο φορέας έρευνας μπορεί να είναι ο ίδιος εκτελών την επεξεργασία ή να χρησιμοποιεί ως υπεύθυνος επεξεργασίας εκτελούντες την επεξεργασία.

Σε κάθε περίπτωση η σχέση μεταξύ υπεύθυνου επεξεργασίας θα πρέπει να είναι γραπτή, όπου θα πρέπει να περιλαμβάνονται μια σειρά από υποχρεωτικές δεσμεύσεις που θα καλύπτουν θέματα εμπιστευτικότητας και προστασίας των προσωπικών δεδομένων.

Η αξιολόγηση του εκτελούντα την επεξεργασία, πριν την σύναψη σύμβασης, αποτελεί ένα μέτρο ελέγχου που ενισχύει την συμμόρφωση του υπεύθυνου επεξεργασίας.

Για τον έλεγχο του επιπέδου συμμόρφωσης ενός συνεργάτη με τον ΓΚΠΔ ως νομικού προσώπου μπορούν να συλλεχθούν οι απαραίτητες πληροφορίες με χρήση κατάλληλου ερωτηματολογίου, όπου ζητούνται δεδομένα, όπως η οικονομική κατάσταση, πιστοποιήσεις ασφάλειας και πληροφοριών, τήρηση κώδικα δεοντολογίας για την προστασία των ΠΔ, δήλωση συμμόρφωσης με τον ΓΚΠΔ κ.λπ.

---

[14] Διάκριση της σύμβασης εξαρτημένης εργασίας από τη σύμβαση έργου, 2017, Ι. Φωτοπούλου http://efotopoulou.gr/diakrisi-tis-simvasis-exartimenis-ergasias-apo-ti-simvasi-ergou/

Ενδεικτικά στη σύμβαση θα πρέπει να υπάρχουν δεσμεύσεις του εκτελούντα την επεξεργασία όπως:

- **Να εφαρμόζει συγκεκριμένα μέτρα ασφάλειας,** όπως της προστασίας από τυχαία ή παράνομη καταστροφή ή απώλεια, αλλοίωση, μη εξουσιοδοτημένη αποκάλυψη ή πρόσβαση
- **Να εκτελεί επεξεργασίες μόνο με τις οδηγίες του υπευθύνου επεξεργασίας**. Σε περίπτωση παράνομης επεξεργασίας να ενημερώνει τον υπεύθυνο επεξεργασίας. Εάν ο εκτελών την επεξεργασία επεξεργαστεί προσωπικά δεδομένα για άλλους σκοπούς τότε καθίσταται υπεύθυνος για αυτήν την επεξεργασία.
- **Να Επιλέγει υπεργολάβους ή ΥποΕκτελούντες την επεξεργασία μόνο με άδεια του υπεύθυνου επεξεργασίας.** Οποιαδήποτε σύναψη σύμβασης του εκτελούντα την επεξεργασία με υπεργολάβο θα πρέπει να διασφαλίζει τουλάχιστον ισοδύναμο επίπεδο προστασίας για τα προσωπικά δεδομένα με εκείνα της σύμβασης τον υπεύθυνου ελέγχου.
- **Να ενημερώνει για παραβιάσεις ή και πιθανές παραβιάσεις προσωπικών δεδομένων και να λαμβάνει τα κατάλληλα μέτρα.** Ο χρόνος που πρέπει να γίνει η ενημέρωση θα πρέπει να είναι επαρκής, ώστε σε ο υπεύθυνος επεξεργασίας να ενημερώσει την Εποπτική Αρχή σε 72 ώρες και θα συνδράμει τον υπεύθυνο επεξεργασίας για την καταγραφή των παραβιάσεων.
- **Να έχει την έγκριση του υπεύθυνου επεξεργασίας για Διεθνείς διαβιβάσεις.** Οι υποχρεώσεις αναφέρονται στην ενότητα ***7.3 Διεθνή διαβίβαση ερευνητικών*** δεδομένων.
- **Να τηρεί αρχείο επεξεργασίας ΠΔ και γενικά να συμμορφώνεται με ορισμένες υποχρεώσεις λογοδοσίας του ΓΚΠΔ.**
- **Να επιτρέπει τον επιτόπιο έλεγχο των μέτρων ασφάλειας από τον υπεύθυνο επεξεργασίας.** Μπορούν επιπλέον να οριστεί η συχνότητα ελέγχου, όπως και το πεδίο ελέγχου.

Οι υποχρεώσεις του εκτελούντα την επεξεργασία πηγάζουν τόσο από τον ΓΚΠΔ όσο και από τους όρους της σύμβασης.

### Συνεργάτες με σύμβαση εξαρτημένης εργασίας

Για την εκτέλεση ενός ερευνητικού έργου ενδεχομένως να απαιτηθεί η πρόσληψη νέων ερευνητών με σχέση εξαρτημένης εργασίας.

Ο ερευνητής/εργαζόμενος επιπλέον είναι υποχρεωμένος να δεσμεύεται και να ακολουθεί τους κανονισμούς, τις πολιτικές και τις οδηγίες που εφαρμόζει ο εργοδότης για την επίτευξη των σκοπών του, όπως επίσης να δεσμεύεται για την τήρηση της εμπιστευτικότητας. Οι δεσμεύσεις αυτές θα πρέπει να είναι γραπτές και να λαμβάνονται κατά την πρόσληψη του εργαζόμενου.

## 7.3 Διεθνή διαβίβαση ερευνητικών δεδομένων

Η διαβίβαση προσωπικών δεδομένων εκτός τη ΕΟΧ (Ευρωπαϊκού οικονομικού Χώρου) αναφέρεται στον ΓΚΠΔ ως διαβίβαση προσωπικών δεδομένων σε τρίτες χώρες ή διεθνής οργανισμούς.

Γενικά ως διαβίβαση δεδομένων θα πρέπει να θεωρούμε την διάθεση, την κοινοποίηση ή την αποκάλυψη τους από τον υπεύθυνο επεξεργασίας σε τρίτον (άλλον υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία ή άλλο φορέα) ανεξάρτητα από το μέσον όπως:

1. Φυσική αποστολή των δεδομένων σε τρίτο μέρος
2. Απομακρυσμένη online πρόσβαση τρίτου στα δεδομένα
3. Μεταφορά μέσω δικτύου ή υπηρεσιών cloud ή email
4. Αποθήκευση σε servers εκτός των χωρών του υπεύθυνου επεξεργασίας

Η διεθνή διαβίβαση τω προσωπικών δεδομένων, σύμφωνα με τον ΓΚΠΔ πρέπει να διασφαλίζεται από συγκεκριμένες εγγυήσεις, δεδομένου ότι το πλαίσιο προστασίας σε κάθε χώρα δεν διασφαλίζει τα δικαιώματα των φυσικών προσώπων. Θα πρέπει να ισχύουν οι παρακάτω προϋποθέσεις που εξασφαλίζουν ότι υφίστανται εκτελεστά δικαιώματα και αποτελεσματικά ένδικα μέσα για τα υποκείμενα των δεδομένων.:

i. **Να υπάρχει επαρκές επίπεδο προστασίας για την χώρα υποδοχής των προσωπικών δεδομένων**[15]

   Η ΕΕ με βάση το άρθρο 45 του ΓΚΠΔ έχει την εξουσία να αποφασίσει εάν μια χώρα εκτός της ΕΕ προσφέρει επαρκές επίπεδο προστασίας δεδομένων και στην ιστοσελίδα [12] υπάρχει ο σχετικός κατάλογος των χωρών.

   Για τις ΗΠΑ υπάρχει η απόφαση επάρκειας σχετικά με την Ασπίδα Προστασίας Προσωπικών Δεδομένων ΕΕ-ΗΠΑ (EU-US Privacy Shield)[16]. Αυτό το πλαίσιο προστατεύει τα θεμελιώδη δικαιώματα οποιουδήποτε στην ΕΕ του οποίου τα προσωπικά δεδομένα μεταφέρονται στις Ηνωμένες Πολιτείες για εμπορικούς σκοπούς. Επιτρέπει την ελεύθερη μεταφορά δεδομένων σε εταιρείες στις ΗΠΑ που είναι πιστοποιημένες σύμφωνα με την Ασπίδα Προστασίας. Καλό είναι ο υπεύθυνος επεξεργασίας να εξετάσει κάθε περίπτωση ξεχωριστά όταν μεταφέρει δεδομένα στις ΗΠΑ.

[15] Κατάλογος των χωρών που υπάρχει απόφαση επάρκειας https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[16] EU-US Privacy Shield: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en

**ii. σύμβαση μεταφοράς δεδομένων που περιέχει τυποποιημένες συμβατικές ρήτρες εγκεκριμένες από την ΕΕ[17]**

Η ΕΕ έχει εκδώσει δύο σύνολα τυποποιημένων συμβατικών ρητρών για τη μεταφορά δεδομένων από υπεύθυνους επεξεργασίας δεδομένων στην ΕΕ σε υπευθύνους επεξεργασίας δεδομένων που είναι εγκατεστημένοι εκτός της ΕΕ ή του Ευρωπαϊκού Οικονομικού Χώρου (ΕΟΧ) καθώς και να σύνολο συμβατικών ρητρών για τη μεταφορά δεδομένων από υπεύθυνους επεξεργασίας στην ΕΕ σε επεξεργαστές εγκατεστημένους εκτός ΕΕ ή ΕΟΧ.

Ο υπεύθυνος επεξεργασίας θα πρέπει να χρησιμοποιήσει αυτές τις συμβατικές ρήτρες σε περίπτωση που δεν υπάρχει απόφαση επάρκειας μεταφοράς δεδομένων στην τρίτη χώρα.

**iii. ρητή συγκατάθεση του φυσικού προσώπου.**

Τελική επιλογή για την διεθνή μεταβίβαση δεδομένων είναι η λήψη συγκατάθεσης από τα φυσικά πρόσωπα.

Τα φυσικά πρόσωπα πρέπει να ενημερώνονται εκ των προτέρων για πιθανούς κινδύνους που εγκυμονούν τέτοιες διαβιβάσεις για το υποκείμενο των δεδομένων λόγω απουσίας απόφασης επάρκειας και κατάλληλων εγγυήσεων.

Σε μία έρευνα, τέτοιες περιπτώσεις μπορεί να συμβούν αν το περιεχόμενο αναρτηθεί σε site ή σε cloud υπηρεσία όπου ο χώρος αποθήκευσης είναι σε χώρα εκτός ΕΕ ή δεν καθορίζεται σαφώς (συνήθως υπηρεσίες χωρίς χρέωση πχ YouTube, facebook, WeTransfer). Τότε θα πρέπει να υποθέσουμε ότι πρόκειται για διεθνή διαβίβαση δεδομένων για την οποία δεν εξασφαλίζεται καμία απόφαση επάρκειας ή/και κατάλληλες εγγυήσεις του παρόχου. Για να συνεχίσει να θεωρείται νόμιμη η συγκατάθεση, θα πρέπει τα φυσικά πρόσωπα να ενημερωθούν για τους πιθανούς κινδύνους που εγκυμονούν τέτοιες διαβιβάσεις προσθέτοντας μια παράγραφο με την εξής ενδεικτική διατύπωση:

« Το αρχείο καταγραφής που αναρτάται στο …..[υπηρεσία, πάροχος] ενδέχεται να αποθηκεύεται σε εξυπηρετητές (servers) που βρίσκονται σε χώρες εκτός του Ευρωπαϊκού Οικονομικού Χώρου (ΕΟΧ), ή σε χώρες που δεν υπάρχει απόφαση επάρκειας από την ΕΕ, ή δεν υπάρχουν οι κατάλληλες εγγυήσεις από τον συγκεκριμένο …..[υπηρεσία, πάροχος] για την υπηρεσία που χρησιμοποιούμε. Αυτό σημαίνει ότι δεν διασφαλίζεται το επίπεδο προστασίας των προσωπικών σας δεδομένων και τα δικαιώματά που εγγυάται ο Γενικός Κανονισμός Προστασίας Δεδομένων

[17] Εγκεκριμένες συμβατικές ρήτρες: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

(ΕΕ 2016/679) και υπάρχει κίνδυνος αθέμητης χρήσης, κοινοποίησης, διάδοσης και τροποποίησης των προσωπικών σας δεδομένων.»

Σημείωση: αν χρησιμοποιούνται υπηρεσίες τύπου WeTransfer για την διαβίβαση του αρχείου καταγραφής, ένα καλό μέτρο προστασίας στην περίπτωση αυτή, που υποβαθμίζει τον κίνδυνο, είναι η ο περιορισμός του χρόνου διατήρησης στην υπηρεσία για μερικές ημέρες και η κρυπτογράφηση του αρχείου με εργαλεία όπως το zip7. Ο κωδικός αποκρυπτογράφησης στέλνεται στα φυσικά πρόσωπα με email.

Αυτές οι απαιτήσεις ισχύουν και για τα ευαίσθητα προσωπικά δεδομένα.

### Συλλογή ερευνητικών δεδομένων από χώρες εκτός ΕΟΧ

Ο κώδικας δεοντολογίας της επιστημονικής έρευνας διασφαλίζει τους ερευνητές ότι συλλογή δεδομένων από χώρες εκτός ΕΟΧ θα πρέπει να αντιμετωπίζεται με παρόμοιο τρόπο.
Οι απαιτήσεις δεοντολογίας της ΕΕ ισχύουν για όλες τις χρηματοδοτούμενες από την ΕΕ έρευνες, ανεξάρτητα από το πού πραγματοποιείται[18].

Οι υποχρεώσεις του ΓΚΠΔ και στην περίπτωση αυτή ισχύουν όπως και η υποχρέωση απόδειξης της συμμόρφωσης λόγω του εδαφικού πεδίου εφαρμογής του *για τις επεξεργασίες προσωπικών δεδομένων στο πλαίσιο των δραστηριοτήτων μιας εγκατάστασης ενός υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία στην Ένωση, ανεξάρτητα από το κατά πόσο η επεξεργασία πραγματοποιείται εντός της Ένωσης* ( άρθρο 3 ( 1) ).

Είναι προφανές ότι θα πρέπει επίσης να ληφθούν οι νομικές δεσμεύσεις των χωρών για την συλλογή και διαβίβαση των δεδομένων και ο υπεύθυνος επεξεργασίας θα πρέπει να λάβει τις κατάλληλες εξουσιοδοτήσεις.

## 7.4 Διατήρηση των ερευνητικών δεδομένων

Ο σκοπός της έρευνας καθορίζει και την περίοδο διατήρησης των προσωπικών δεδομένων και πρέπει να προσδιοριστεί πριν την επεξεργασία ώστε τα φυσικά πρόσωπα που μετέχουν στην έρευνα να διαθέτουν την πληροφορία αυτή πριν δώσουν την συγκατάθεσή τους.

[18] Ethics and Data Protection (https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-data-protection_en.pdf ), 2014

Αν τα προσωπικά δεδομένα δεν είναι πλέον χρήσιμα ή έχει λήξει ο χρόνος διατήρησης τους, θα πρέπει να διαγραφούν ή να καταστραφούν με ασφάλεια ώστε να μην υπάρχει περίπτωση ανάκτησης (πχ διαγραφή αντιγράφων ασφαλείας, καταστροφέας εγγράφων). Η διαγραφή αυτή εφαρμόζεται σε δεδομένα που διατηρεί στους χώρους του ή σε cloud ή σε άλλο πάροχο υπηρεσιών.

Υποχρέωση του υπεύθυνου εργασίας είναι να διασφαλίσει ότι τα δεδομένα που έχουν διαβιβαστεί σε συνεργάτες ή εκτελούντες την επεξεργασία έχουν διαγραφεί, εκτός αν υπάρχει νομική δέσμευση που ορίζει διαφορετικά . Η υποχρέωση αυτή του υπεύθυνου επεξεργασίας μπορεί να διασφαλιστεί και μέσα από τις συμβατικές υποχρεώσεις που συνάπτει με τους συνεργάτες του.

Ο υπεύθυνος επεξεργασίας, έχοντας ήδη εξασφαλίσει την συγκατάθεση των φυσικών προσώπων, μπορεί να ανωνυμοποιήσει τα ερευνητικά προσωπικά δεδομένα μετά την λήξη του χρόνου διατήρησης.