**Σύντομη οδηγία**

**Προσωπικά Δεδομένα και έρευνα στο ΑΠΘ**

Η οδηγία αποτελεί μια σύνοψη του ***προκαταρτικού οδηγού για την Προστασία των Προσωπικών Δεδομένων στο πλαίσιο Επιστημονικής Έρευνας*** ( ***αρχείο: Προστασία Δεδομένων στο πλαίσιο της Έρευνας***) οργανωμένη από άλλη οπτική γωνία.

Το ΑΠΘ συνήθως συμμετέχει σε μια χρηματοδοτούμενη έρευνα, σε συνεργασία με άλλους φορείς (κοινοπραξία - consortium) με τους εξής ρόλους:

* **Project Coordinator** της κοινοπραξίας
* **Μέλος** της κοινοπραξίας
* **Υπεργολάβος** , συνεργαζόμενος με ένα μέλος της της κοινοπραξίας

Για τους σκοπούς της παρούσας οδηγίας, τα προσωπικά δεδομένα θα αναφέρονται σε αυτά των υποκειμένων της έρευνας.

Οι κύριες υποχρεώσεις του ΑΠΘ, ως προς την προστασία των προσωπικών δεδομένων που διατηρεί και επεξεργάζεται, παραμένουν ίδιες ανεξάρτητα του ρόλου του. Τα τεχνικά και οργανωτικά μέτρα που προτείνονται να λαμβάνονται κατά την διάρκεια της έρευνας, περιγράφονται αναλυτικά στον προκαταρτικό οδηγό.

Οι επιπλέον υποχρεώσεις που απορρέουν από τον ρόλο που έχει το ΑΠΘ, αφορούν τις σχέσεις που διαμορφώνει με τα υπόλοιπα μέλη της κοινοπραξίας ως προς τα προσωπικά δεδομένα και μπορεί να θεωρείται:

* **υπεύθυνος επεξεργασίας**, που διατηρεί και επεξεργάζεται μόνο δικά του δεδομένα
* **από κοινού υπεύθυνος επεξεργασίας** με άλλα μέλη της κοινοπραξίας για τα προσωπικά δεδομένα που διαμοιράζονται τα μέλη.
* **Εκτελών την επεξεργασία** (υπεργολάβος) όταν επεξεργάζεται δεδομένα κατ΄ εντολή μέλους της κοινοπραξίας χωρίς να μετέχει σε αυτή.

Εκτελών την επεξεργασία, θα πρέπει να θεωρείται και κάθε ανεξάρτητος ερευνητής με σύμβαση έργου τον οποίο χρησιμοποιεί μέλος της κοινοπραξίας.

Στη συνέχεια θα εξετάσουμε τις υποχρεώσεις του ΑΠΘ με βάση τον ρόλο που αναλαμβάνει.

# **Project Coordinator (PC)**

Στα πλαίσια των ευθυνών αυτού του ρόλου είναι και η διαχείριση των πόρων και των σχέσεων μεταξύ των μελών της κοινοπραξίας, τα οποία εξειδικεύοντας στα προσωπικά δεδομένα, περιλαμβάνουν:

1. Τη διαχείριση ερευνητικών δεδομένων μέσα στη κοινοπραξία (οργανωτικά μέτρα)
2. Την κάλυψη των τεχνικών μέτρων ασφάλειας και προστασίας των δεδομένων
3. Εκτίμηση αντικτύπου σχετική με τη προστασία των δεδομένων (DPIA)

Ο Project Coordinator θα πρέπει να γνωρίζει τι σχέσεις των μελών μεταξύ τους και κυρίως τον τρόπο που θα διαβιβάζονται και θα διαμοιράζονται τα ερευνητικά δεδομένα ελέγχοντας και προτείνοντας τα κατάλληλα μέτρα προστασίας που μειώνουν τους κινδύνους παραβίασης.

Είναι σημαντικό να γίνει κατανοητή η νομική ευθύνη των από κοινού υπευθύνων επεξεργασίας της κοινοπραξίας, όταν υφίσταται αυτή η σχέση, και το πως τα μέλη επηρεάζονται από αυτή.

Επίσης μια υποχρέωση του Project Coordinator είναι η αναζήτηση ή η δημιουργία των κατάλληλων πρότυπων αρχείων για την οργάνωση των παρακάτω μέτρων. Αυτά βρίσκονται στους αντίστοιχους φακέλους του Προγράμματος Προστασίας Δεδομένων που έχει εκπονήσει το ΑΠΘ.

## Διαχείριση ερευνητικών δεδομένων μέσα στη κοινοπραξία (οργανωτικά μέτρα)

Τα ερευνητικά δεδομένα που καλείται να επεξεργαστεί η κοινοπραξία μπορεί να αποτελούνται από προσωπικά δεδομένα ή και από ανώνυμα δεδομένα που μπορεί να συλλέγονται απευθείας από τα φυσικά πρόσωπα ή να είναι ιστορικά δεδομένα (αναδρομικές μελέτες).

Ο διαμοιρασμός των ερευνητικών δεδομένων στη κοινοπραξία δημιουργεί δύο νέους ρόλους: τον **Πάροχο (provider)** και τον **Παραλήπτη (recipient)** δεδομένων που εγείρουν με την σειρά τους συγκριμένες αξιώσεις για τις μεταξύ τους σχέσεις πάνω στα δεδομένα.

Τα οργανωτικά μέτρα που θα πρέπει να έχει υπόψη του ο Project Coordinator κατά την εκτέλεση των καθηκόντων του περιλαμβάνουν:

### **Σύμβαση διαμοιρασμού δεδομένων (Joint Controller**/**Data Sharing Agreement)**

Οι υποχρεώσεις και τα δικαιώματα για τον διαμοιρασμό των ερευνητικών δεδομένων είναι πολύ πιθανόν να μην καλύπτονται από την κύρια σύμβαση (Grand Agreement) γιατί δεν αφορά όλους.

Σαν επέκταση της κύριας σύμβασης θα πρέπει να υπογραφεί μεταξύ των μερών σύμβαση διαμοιρασμού δεδομένων (Joint Controller/Data Sharing Agreement). Είναι πρακτικό, να αποτυπωθούν στην ορολογία του συμβατικού κειμένου οι ρόλοι του Παρόχου και του Παραλήπτη δεδομένων λόγω των διαφορετικών απαιτήσεων του ενός έναντι του άλλου.

Ο Πάροχος διατηρεί ερευνητικά δεδομένα τα οποία μπορεί να διαβιβάζει στον/στους Παραλήπτη/ες ή τον/τους παρέχει πρόσβαση σε αυτά ως προσωπικά δεδομένα ή ως ανώνυμα δεδομένα.

Στην πρώτη περίπτωση Πάροχος και Παραλήπτες θεωρούνται από κοινού Υπεύθυνοι επεξεργασίας και το Joint Controller/Data Sharing Agreement θα πρέπει να λαμβάνει υπόψη και τον Γενικό Κανονισμό Προστασίας Δεδομένων (EU 2016/679 - ΓΚΠΔ) όταν εξειδικεύουν τις μεταξύ τους υποχρεώσεις και δικαιώματα.

Αν κάποιος Παραλήπτης βρίσκεται σε χώρα εκτός ΕΟΧ (Ευρωπαϊκού οικονομικού Χώρου) τότε κατά τον ΓΚΠΔ θεωρείται διαβίβαση προσωπικών δεδομένων σε τρίτες χώρες ή διεθνής οργανισμούς. Ο Project Coordinator θα πρέπει να εξετάσει αν υπάρχει επαρκές επίπεδο προστασίας για την χώρα υποδοχής των προσωπικών δεδομένων ή διαφορετικά να υπογραφεί ξεχωριστό Joint Controller/Data Sharing Agreement μεταξύ Παρόχου και Παραλήπτη που να περιέχει τυποποιημένες συμβατικές ρήτρες εγκεκριμένες από την ΕΕ (βλέπε κεφάλαιο 7.3 του προκαταρτικού οδηγού).

Στη δεύτερη περίπτωση, Πάροχος και Παραλήπτες υπογράφουν το Joint Controller/Data Sharing Agreement χωρίς να λαμβάνουν υπόψη τον ΓΚΠΔ.

Σύμβαση από κοινού υπεύθυνων επεξεργασίας Joint Controller/Data Sharing Agreement που αφορά προσωπικά δεδομένα στα [Ελληνικά](5α%20Σύμβαση%20από%20κοινού%20υπεύθυνων%20επεξεργασίας%20GR.docx) και [Αγγλικά](5β%20Joint%20Controller-Data%20Sharing%20Agreement%20EN.docx).

### **Εκτελών την Επεξεργασία**

Είναι ενδεχόμενο κάποιο μέλος της κοινοπραξίας να επεξεργαστεί τα ερευνητικά δεδομένα, που περιλαμβάνουν προσωπικά δεδομένα, με την συνδρομή υπεργολάβου (Εκτελών την επεξεργασία). Θα πρέπει να προηγείται η αξιολόγηση του εκτελούντα την επεξεργασία, πριν την σύναψη σύμβασης, η οποία θα πρέπει να περιλαμβάνει δεσμεύσεις που θα καλύπτουν θέματα εμπιστευτικότητας και προστασίας των προσωπικών δεδομένων (βλέπε κεφάλαιο 7.2 σχετική παράγραφο του προκαταρτικού οδηγού) και να υπογράφεται η παρακάτω σύμβαση εκτελούντος την επεξεργασία.

Σύμβαση εκτελούντος την επεξεργασία στα [Ελληνικά](6α%20Σύμβαση%20Εκτελούντος%20την%20επεξεργασία%20GR.docx) και [Αγγλικά](6β%20Σύμβαση%20Εκτελούντος%20την%20επεξεργασία%20EN.docx).

### **Συνεργάτες με σύμβαση εξαρτημένης εργασίας**

Για την εκτέλεση ενός ερευνητικού έργου ενδεχομένως να απαιτηθεί από τα μέλη της κοινοπραξίας 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 (NDA). Οι δεσμεύσεις αυτές θα πρέπει να είναι γραπτές και να λαμβάνονται κατά την πρόσληψη του εργαζόμενου.

Σύμβαση Εχεμύθειας, [Εμπιστευτικότητας](7%20Σύμβαση%20Εχεμύθειας-%20Εμπιστευτικότητας%20και%20Προστασίας%20Προσωπικών%20Δεδομένων.docx) και προστασίας Προσωπικών Δεδομένων.

**Συγκατάθεση των υποκειμένων των δεδομένων**

Στην περίπτωση που ο Πάροχος συλλέγει τα ερευνητικά δεδομένα απ’ ευθείας από τα φυσικά πρόσωπα, τότε θα πρέπει να εξασφαλιστεί η ενημερωμένη συγκατάθεση τους με χρήση κατάλληλων εντύπων (περισσότερα για την συγκατάθεση: βλέπε το 5.4 Νομιμότητα της Επεξεργασίας σε μια επιστημονική έρευνα του προκαταρτικού οδηγού).

Γενικές οδηγίες για τη συγκατάθεση εδώ.

Υποδείγματα συγκατάθεσης στα [Ελληνικά](4α%20Πρότυπο%20έντυπο%20Ενημερωμένης%20συγκατάθεσης%20GR.docx) και [Αγγλικά](4β%20Πρότυπο%20έντυπο%20Ενημερωμένης%20συγκατάθεσης%20EN.docx).

### **Συλλογή ερευνητικών δεδομένων από χώρες εκτός ΕΟΧ**

Ο κώδικας δεοντολογίας και ο ΓΚΠΔ ισχύουν και για δεδομένα που συλλέγονται εκτός ΕΟΧ. Επιπλέον θα πρέπει 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 (βλέπε κεφάλαιο 7.4 του προκαταρτικού οδηγού).

### **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 τη συγκατάθεσή τους (βλέπε κεφάλαιο 7.4 του προκαταρτικού οδηγού).

## Τεχνικά μέτρα ασφάλειας και προστασίας των δεδομένων

Η προστασία των ερευνητικών δεδομένων έχει τρεις άξονες (βλέπε κεφάλαιο 6 του προκαταρτικού οδηγού) με τα ελάχιστα προτεινόμενα μέτρα:

1. **Εμπιστευτικότητα**

* **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).

* **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.

* **Κρυπτογράφηση**

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.

1. **Ακεραιότητα**

* **Έλεγχος Προσβάσεων**

Είναι ύψιστης σημασίας να διαβαθμιστούν τα επίπεδα πρόσβασης στις πληροφορίες της έρευνας και να τεθούν εξ αρχής οι απαιτήσεις για τον έλεγχο πρόσβασης σε αυτές. Για την παραχώρηση των δικαιωμάτων πρόσβασης θα πρέπει να εφαρμοστούν οι αρχές του “διαχωρισμού των καθηκόντων” και των “ελάχιστων δικαιωμάτων”.

1. **Διαθεσιμότητα**

* **Λήψη Αντιγράφων Ασφάλειας Συστημάτων και Πληροφοριών**

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.

## Εκτίμηση αντικτύπου σχετική με τη προστασία των δεδομένων (DPIA)

Οι επιστημονικές έρευνες σε θέματα με ευαίσθητα προσωπικά δεδομένα και ειδικά με δεδομένα υγείας, γενετικών και βιομετρικών χαρακτηριστικών θα πρέπει να συνοδεύονται πάντα από μια μελέτη εκτίμησης αντικτύπου (βλέπε κεφάλαιο 7.1 του προκαταρτικού οδηγού).

Εφόσον στο [Ερωτηματολόγιο](8%20Ερωτηματολόγιο%20για%20την%20Εκτίμηση%20Αντίκτυπου%20σχετικά%20με%20την%20Προστασία%20Δεδομένων.docx) για ΕΑΠΔ απαντήσετε έστω και σε μία από τις ερωτήσεις 4-17 ΝΑΙ απαιτείται η διενέργεια ΕΑΠΔ.

Η [διαδικασία](9%20Διαδικασία%20Εκτίμησης%20Αντίκτυπου%20σχετικά%20με%20την%20Προστασία%20Δεδομένων.docx) και το Ερωτηματολόγιο [συλλογής](10%20Ερωτηματολόγιο%20συλλογής%20πληροφοριών%20για%20την%20εκτίμηση%20αντικτύπου%20στα%20ΠΔ.DOCX) πληροφοριών για την εκτίμηση αντικτύπου στα ΠΔ.

Η DPIA αποτελεί επίσης την απόδειξη της συμμόρφωσης με τον ΓΚΠΔ για τις συγκεκριμένες επεξεργασίες που αφορούν τον διαμοιρασμό και τις αναλύσεις των προσωπικών δεδομένων.

Προτείνεται να διεξαχθεί DPIA ακόμη και στη περίπτωση που διαμοιράζονται και στην συνέχεια γίνεται επεξεργασία σε ανώνυμα δεδομένα.

[Πρότυπη Έκθεση Εκτίμησης Αντίκτυπου σχετικά με την Προστασία Δεδομένων](11%20Πρότυπη%20Έκθεση%20Εκτίμησης%20Αντίκτυπου%20σχετικά%20με%20την%20Προστασία%20Δεδομένων.docx)

# **Μέλος της κοινοπραξίας**

Το ΑΠΘ σαν μέλος μιας κοινοπραξίας, μπορεί να έχει την ιδιότητα του Παρόχου ή του Παραλήπτη ερευνητικών δεδομένων και επομένως θα πρέπει αρχικά να διαμορφώσει ανάλογα του όρους του Joint Controller/Data Sharing Agreement.

Το ΑΠΘ είναι υπεύθυνος επεξεργασίας για μια σειρά προσωπικών δεδομένων που ήδη διατηρεί και επομένως η συμμόρφωσή του έναντι του ΓΚΠΔ τον υποχρεώνει να υλοποιεί τις αντίστοιχες υποχρεώσεις που εφαρμόζονται και περιγράφονται στο 1.1, 1.2 και 1.3 του παραπάνω κεφαλαίου.

# **Υπεργολάβος (εκτελών την επεξεργασία)**

Αν το ΑΠΘ λειτουργεί σαν υπεργολάβος μέλους της κοινοπραξίας ή άλλου υπεύθυνου επεξεργασίας, η συμβατική σχέση θα πρέπει να περιλαμβάνει υποχρεώσεις εμπιστευτικότητας και σε περίπτωση που περιλαμβάνονται προσωπικά δεδομένα οι όροι προστασίας τους. Οι συγκεκριμένοι όροι μπορούν να αποτελούν μέρος της κύριας σύμβασης ή παράρτημά της. Αναλυτικά για την περίπτωση αυτή μπορείτε να βρείτε στο κεφάλαιο 7.1 του προκαταρτικού οδηγού περί εκτελούντα την επεξεργασία.

Μπορεί ο υπεύθυνος επεξεργασίας να ζητήσει από το ΑΠΘ πληροφορίες για να τον αξιολογήσει σε θέματα προστασίας των δεδομένων πριν την υπογραφή της σύμβασης και τις οποίες θα πρέπει να παράσχει.

Είναι προφανές ότι αν και το ΑΠΘ χρησιμοποιήσει με την σειρά του υπεργολάβο, θα πρέπει να εφαρμόσει την ίδια διαδικασία και να υπογραφεί η παρακάτω σύμβαση εκτελούντος την επεξεργασία.

Σύμβαση εκτελούντος την επεξεργασία στα [Ελληνικά](6α%20Σύμβαση%20Εκτελούντος%20την%20επεξεργασία%20GR.docx) και [Αγγλικά](6β%20Σύμβαση%20Εκτελούντος%20την%20επεξεργασία%20EN.docx).