ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

«Πολιτικές και Διαδικασίες Προστασίας Δεδομένων Προσωπικού Χαρακτήρα»

Αρ. Συνεδρίασης Συγκλήτου 11/ 12.06.2020

Πίνακας Περιεχομένων

Πίνακας Σχημάτων

Πίνακας Πινάκων

Ακρωνύμια

Ακρωνύμιο	Επεξήγηση
Γενικός Κανονισμός για την Προστασία Δεδομένων (ΓΚΠΔ)	Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ
PIA-CNIL	Μεθοδολογία για την ανάλυση αντικτύπου ιδιωτικότητας της Γαλλικής Αρχής Προστασίας Προσωπικών Δεδομένων – CNIL
ΠΣ	Πληροφοριακό Σύστημα / Πληροφοριακά Συστήματα
ΥΠΔ	Υπεύθυνος Προστασίας Δεδομένων
ΕΟΧ	Ευρωπαϊκός Οικονομικός Χώρος

Επιτελική Σύνοψη

Το παρόν παραδοτέο εντάσσεται στο πλαίσιο μελέτης για τη συμμόρφωση του Πανεπιστημίου Αιγαίου με τον Γενικό Κανονισμό Προστασίας Δεδομένων 2016/679 (ΓΚΠΔ) αναφορικά με τις δραστηριότητες επεξεργασίας που ανήκουν στους σκοπούς επεξεργασίας δεδομένων προσωπικού χαρακτήρα, όπως αυτές αναλύθηκαν στο παραδοτέο Π1.3 «Ανάλυση Αντίκτυπου για την Ιδιωτικότητα και την Προστασία Δεδομένων (Privacy Impact Assessment)».

Η Πολιτική Προστασίας Δεδομένων αποτυπώνει την πρόθεση του Πανεπιστημίου Αιγαίου να προστατέψει τα δεδομένα προσωπικού χαρακτήρα που τελούν υπό επεξεργασία μέσω των δραστηριοτήτων επεξεργασίας που ανήκουν στους σκοπούς επεξεργασίας του. Η Πολιτική Προστασίας Δεδομένων περιγράφει το σύνολο των αρχών και κανόνων που καθορίζουν τον τρόπο με τον οποίο το Πανεπιστήμιο Αιγαίου, ως Υπεύθυνος Επεξεργασίας, και οι εκτελούντες την επεξεργασία για λογαριασμό του Πανεπιστημίου πρέπει να διαχειρίζονται και να προστατεύουν τα δεδομένα προσωπικού χαρακτήρα των εν λόγω δραστηριοτήτων επεξεργασίας, έτσι ώστε να επιτυγχάνεται η συμμόρφωση με τις απαιτήσεις του Γενικού Κανονισμού Προστασίας Δεδομένων 2016/679. Οι στόχοι αυτοί πηγάζουν από τις διατάξεις του Γενικού Κανονισμού Προστασίας Δεδομένων 2016/679, αλλά και από τα αποτελέσματα των μελετών ανάλυσης αντικτύπου για την προστασία δεδομένων, οι οποίες εκπονήθηκαν και αποτυπώνονται στο παραδοτέο Π1.3.

Το παραδοτέο διακρίνεται σε τρία μέρη. Στο πρώτο μέρος αναπτύσσονται οι γενικές αρχές, οδηγίες, διαδικασίες, κανόνες, ρόλοι και αρμοδιότητες/υπευθυνότητες για την προστασία δεδομένων προσωπικού χαρακτήρα στο πλαίσιο λειτουργίας του Πανεπιστημίου Αιγαίου, στο δεύτερο μέρος παρουσιάζονται οι διαδικασίες εφαρμογής της Πολιτικής Προστασίας Δεδομένων, ενώ στο τρίτο μέρος περιλαμβάνονται κρίσιμα έντυπα προς συμπλήρωση.

Μέρος Α': Πολιτική Προστασίας Δεδομένων

Α.1. Η Πολιτική Προστασίας Δεδομένων

Α.1.1 Εισαγωγή

Η Πολιτική Προστασίας Δεδομένων περιλαμβάνει γενικά τον σκοπό και τους στόχους που θέτει η διοίκηση αναφορικά με την προστασία δεδομένων προσωπικού χαρακτήρα, καθώς και τις οδηγίες, διαδικασίες, κανόνες, ρόλους και υπευθυνότητες που αφορούν στην προστασία των δεδομένων αυτών. Στο παρόν έργο οι οδηγίες, κανόνες και διαδικασίες που περιλαμβάνονται στην Πολιτική Προστασίας Δεδομένων υλοποιούνται με την εφαρμογή των μέτρων προστασίας για το Πανεπιστήμιο Αιγαίου και τα πληροφοριακά συστήματα, τα οποία περιγράφονται στο παραδοτέο Π1.4 «Πλάνο Τεχνικών, Οργανωτικών και Διαδικαστικών Ενεργειών για Συμμόρφωση με τον Ευρωπαϊκό Κανονισμό 2016/679» για το Πανεπιστήμιο Αιγαίου. Η Πολιτική Προστασίας Δεδομένων διατυπώνεται στο τρέχον έγγραφο, το οποίο θα πρέπει να γνωρίζουν και να ακολουθούν όλα τα μέλη του Πανεπιστημίου Αιγαίου αναφορικά με όλες τις δραστηριότητές τους που έχουν σχέση με δεδομένα, επιχειρησιακές διαδικασίες και πληροφοριακά συστήματα που καλύπτει η παρούσα Πολιτική.

Η εφαρμογή της Πολιτικής Προστασίας Δεδομένων έχει δεσμευτικό χαρακτήρα για όλα τα μέλη του Πανεπιστημίου Αιγαίου. Αυτό σημαίνει ότι η τήρηση των διαδικασιών και οδηγιών που προβλέπει είναι υποχρεωτική για όλα τα μέλη του Πανεπιστημίου Αιγαίου που συμμετέχουν άμεσα ή έμμεσα σε επιχειρησιακές διεργασίες που περιλαμβάνουν επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Α.1.2 Σκοπός και στόχοι της Πολιτικής Προστασίας Δεδομένων

Η Πολιτική Προστασίας Δεδομένων περιγράφει το σύνολο των κανόνων που καθορίζουν τον τρόπο με τον οποίο το Πανεπιστήμιο Αιγαίου προστατεύει τα προσωπικά δεδομένα, έτσι ώστε να συμμορφώνεται με τον Γενικό Κανονισμό για την Προστασία Δεδομένων (εφεξής «ΓΚΠΔ» ή «Κανονισμός») και να προστατεύεται η ιδιωτικότητα των Υποκειμένων των Δεδομένων. Σκοπός της Πολιτικής Προστασίας Δεδομένων είναι να παράσχει στρατηγική καθοδήγηση στη διοίκηση του Πανεπιστημίου Αιγαίου και στο προσωπικό για την προστασία των προσωπικών δεδομένων κατά την επεξεργασία τους.

Με τη βοήθεια της Πολιτικής Προστασίας Δεδομένων το Πανεπιστήμιο Αιγαίου επιδιώκει να επιτύχει τους ακόλουθους στόχους:

- Την προστασία των φυσικών προσώπων των οποίων τα προσωπικά δεδομένα επεξεργάζεται το Πανεπιστήμιο Αιγαίου.
- Την αναγνώριση των κινδύνων που ενέχει η επεξεργασία προσωπικών δεδομένων που πραγματοποιεί το Πανεπιστήμιο Αιγαίου και την εφαρμογή αντιμέτρων για τον μετριασμό των εν λόγω κινδύνων.

- Την εφαρμογή κανόνων και τεχνικών ώστε να ικανοποιούνται τα νόμιμα δικαιώματα των φυσικών προσώπων, των οποίων τα προσωπικά δεδομένα επεξεργάζεται το Πανεπιστήμιο Αιγαίου.

- Τη συμμόρφωση με τις απαιτήσεις που απορρέουν από την ελληνική Νομοθεσία.

Η Πολιτική Προστασίας Δεδομένων επιχειρεί να ορίσει κοινά αποδεκτές αρχές, τρόπους και αρμοδιότητες που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Ο χαρακτήρας της Πολιτικής Προστασίας Δεδομένων δεν αφορά μόνο τεχνικά ή οργανωτικά θέματα, αλλά αντιμετωπίζει με την ίδια προσοχή και τις δύο κατηγορίες.

Α.1.3 Εμβέλεια εφαρμογής

Η Πολιτική Προστασίας Δεδομένων αφορά στο σύνολο των δεδομένων προσωπικού χαρακτήρα που επεξεργάζεται το Πανεπιστήμιο Αιγαίου, με αυτοματοποιημένα ή μη αυτοματοποιημένα μέσα, σύμφωνα με τα οριζόμενα στο Άρθρο 4 του Γενικού Κανονισμού για την Προστασία Δεδομένων 2016/679. Η Πολιτική Προστασίας Δεδομένων αφορά στο σύνολο των επιχειρησιακών διεργασιών που περιλαμβάνουν επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Η Πολιτική Προστασίας Δεδομένων εφαρμόζεται από όλα τα μέλη του Πανεπιστημίου Αιγαίου που μετέχουν άμεσα ή έμμεσα στην επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Α.2. Διαδικασίες Διαχείρισης της Πολιτικής Προστασίας Δεδομένων

Α.2.1 Έγκριση Πολιτικής

Η Πολιτική Προστασίας Δεδομένων εγκρίνεται από την Ανώτερη Διοίκηση του Πανεπιστημίου Αιγαίου και κοινοποιείται σε όλους τους υπαλλήλους και τους αρμόδιους συνεργάτες.

Α.2.2 Ρόλοι και αρμοδιότητες για τη διαχείριση της Πολιτικής

Το Πανεπιστήμιο Αιγαίου θα αναπτύξει και υλοποιήσει ένα οργανωτικό πλαίσιο, σύμφωνα με το οποίο θα υπάρχουν ρόλοι με αρμοδιότητες για την προστασία προσωπικών δεδομένων. Το πλαίσιο θα περιλαμβάνει τουλάχιστον τους ακόλουθους ρόλους:

- Υπεύθυνος Προστασίας Δεδομένων

- Υπεύθυνος Ανάπτυξης Πληροφοριακών Συστημάτων

- Υπεύθυνος Διαχείρισης Πληροφοριακών Συστημάτων

- Υπεύθυνος Επιθεώρησης Πληροφοριακών Συστημάτων.

Οι συγκεκριμένες αρμοδιότητες που αναλαμβάνει ο κάθε ρόλος για την προστασία προσωπικών δεδομένων και η εφαρμογή αυτής της Πολιτικής θα πρέπει να απονέμονται από τη διοίκηση και να καταγράφονται.

Α.2.3 Αναθεώρηση Πολιτικής

Η Πολιτική Προστασίας Δεδομένων δεν πρέπει να είναι στατική, αλλά να τηρείται κατά το δυνατόν επίκαιρη και να προσαρμόζεται ακολουθώντας τις τροποποιήσεις των πληροφοριακών συστημάτων και του τεχνικο-κοινωνικού περιβάλλοντος. Η Πολιτική Προστασίας Δεδομένων επικαιροποιείται τουλάχιστον ετησίως. Επίσης, επικαιροποιείται στην περίπτωση σημαντικών αλλαγών στο Πανεπιστήμιο Αιγαίου ή τα πληροφοριακά συστήματά του. Η ανώτερη διοίκηση του Πανεπιστημίου Αιγαίου αναθέτει την αρμοδιότητα αναθεώρησης της Πολιτικής Προστασίας Δεδομένων στον Υπεύθυνο Προστασίας Δεδομένων.

Α.2.4 Εποπτεία εφαρμογής Πολιτικής

Η εφαρμογή της Πολιτικής Προστασίας Δεδομένων και οι κανόνες που απορρέουν από αυτήν αξιολογούνται από κατάλληλες διαδικασίες ελέγχου που ορίζει ο Υπεύθυνος Προστασίας Δεδομένων (εφεξής «ΥΠΔ»).

Α.2.5 Εσωτερική επιθεώρηση

Το Πανεπιστήμιο Αιγαίου οφείλει να πραγματοποιεί σε ετήσια βάση εσωτερική επιθεώρηση των πληροφοριακών συστημάτων και των οργανωτικών, διαδικαστικών και τεχνικών αντιμέτρων που περιγράφει η Πολιτική Προστασίας Δεδομένων. Σκοπός της εσωτερικής επιθεώρησης είναι να εξακριβώνεται η συμμόρφωση με την Πολιτική και η αποτελεσματικότητα της Πολιτικής για την προστασία δεδομένων προσωπικού χαρακτήρα. Αρμόδιος για την οργάνωση της εσωτερικής επιθεώρησης είναι ο Υπεύθυνος Επιθεώρησης Πληροφοριακών Συστημάτων. Ο Υπεύθυνος Επιθεώρησης Πληροφοριακών Συστημάτων σχεδιάζει το πλάνο της εσωτερικής επιθεώρησης με εύρος όλες τις επιχειρησιακές διεργασίες που περιλαμβάνουν επεξεργασία προσωπικών δεδομένων, προδιαγράφει τα κριτήρια της επιθεώρησης και εξασφαλίζει ότι τα αποτελέσματα της εσωτερικής επιθεώρησης θα είναι διαθέσιμα για την επόμενη αναθεώρηση της Πολιτικής. Η διοίκηση του Πανεπιστημίου Αιγαίου επιλέγει την ομάδα επιθεωρητών και αναθέτει αρμοδιότητες στους επιθεωρητές.

Α.3. Εκτίμηση Αντικτύπου σχετικά με την Προστασία Δεδομένων

Α.3.1 Υλοποίηση Εκτίμησης Αντικτύπου για την Προστασία Δεδομένων

Το Πανεπιστήμιο Αιγαίου οφείλει να σχεδιάσει την προστασία των δεδομένων προσωπικού χαρακτήρα λαμβάνοντας υπόψη τον κίνδυνο που ενέχει η επεξεργασία για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας. Ο ΥΠΔ επιλέγει και καθορίζει μέθοδο εκτίμησης αντικτύπου για την προστασία δεδομένων, η οποία να ικανοποιεί τις ακόλουθες προδιαγραφές:

- Διασφαλίζει ότι επαναλαμβανόμενες εκτιμήσεις αντικτύπου οδηγούν σε συνεπή και συγκρίσιμα αποτελέσματα.
- Εντοπίζει κινδύνους σχετικά με τη μη εξουσιοδοτημένη πρόσβαση, τροποποίηση και διαγραφή προσωπικών δεδομένων.
- Υπολογίζει επίπεδα κινδύνων λαμβάνοντας υπόψη την πιθανότητα εμφάνισης της απειλής και τον ενδεχόμενο αντίκτυπο από την πραγματοποίηση του κινδύνου.

Το Πανεπιστήμιο Αιγαίου καταγράφει σε επίσημο έγγραφο την αναλυτική περιγραφή της μεθόδου που εφαρμόζεται για την ανάλυση αντικτύπου. Ο ΥΠΔ εφαρμόζει τη μέθοδο και το Πανεπιστήμιο Αιγαίου καταγράφει σε διακριτό έγγραφο τα αποτελέσματα της εφαρμογής.

Α.3.2 Συχνότητα και εναύσματα εκπόνησης

Ο ΥΠΔ καθορίζει κριτήρια και εναύσματα επανάληψης της εκτίμησης αντικτύπου, ώστε να εκπονείται κάθε φορά που υπάρχουν σημαντικές εξελίξεις και αλλαγές στη λειτουργία του Πανεπιστημίου Αιγαίου ή στις τεχνικές επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

Επιπλέον, η εκτίμηση αντικτύπου για την προστασία δεδομένων πραγματοποιείται σε περιοδική βάση. Ο ΥΠΔ καθορίζει τη συχνότητα επανάληψης, αλλά αυτή δεν μπορεί να ξεπερνά το ένα έτος.

Α.4. Οργανωτική Δομή

Α.4.1 Υπεύθυνος Προστασίας Δεδομένων

Η ανώτερη διοίκηση ορίζει ως ΥΠΔ αρμόδιο άτομο που αναφέρεται απευθείας στην ανώτερη διοίκηση χωρίς να λαμβάνει εντολές για την άσκηση των καθηκόντων του ως ΥΠΔ. Η ανώτερη διοίκηση διασφαλίζει ότι ο ΥΠΔ δεν απολύεται ούτε υφίσταται κυρώσεις λόγω της εκτέλεσης των καθηκόντων του.

Ο ΥΠΔ πρέπει να έχει άμεση πρόσβαση στην ανώτερη διοίκηση και τα υποκείμενα των προσωπικών δεδομένων να έχουν ξεκάθαρη πρόσβαση στον Υπεύθυνο Προστασίας Δεδομένων.

Ο ΥΠΔ μπορεί να έχει και άλλες αρμοδιότητες αλλά το Πανεπιστήμιο Αιγαίου εξασφαλίζει ότι δεν δημιουργείται «σύγκρουση συμφερόντων» εξαιτίας των πρόσθετων αυτών επαγγελματικών καθηκόντων και υποχρεώσεων.

Ο ΥΠΔ έχει αρμοδιότητα για όλα τα θέματα που αφορούν στην προστασία προσωπικών δεδομένων στο Πανεπιστήμιο Αιγαίου. Για τον λόγο αυτό, πρέπει να έχει πρόσβαση σε όλες τις βάσεις δεδομένων προσωπικού χαρακτήρα και στα συστήματα του Πανεπιστημίου Αιγαίου που φιλοξενούν προσωπικά δεδομένα. Ο ΥΠΔ δεσμεύεται από όρους εμπιστευτικότητας.

Α.4.1.1 Γνώσεις και Δεξιότητες του Υπεύθυνου Προστασίας Δεδομένων

Ο ΥΠΔ θα πρέπει να έχει τις ακόλουθες γνώσεις και δεξιότητες:

- Εξειδικευμένη γνώση νομικού πλαισίου προστασίας δεδομένων προσωπικού χαρακτήρα σε εθνικό και ευρωπαϊκό επίπεδο.
- Βασική γνώση στοιχείων Ασφάλειας Πληροφοριών και Πληροφοριακών Συστημάτων, ώστε να μπορεί να κατανοήσει, να σχεδιάσει και να εποπτεύσει την εφαρμογή ενός προγράμματος προστασίας δεδομένων προσωπικού χαρακτήρα.
- Επικοινωνιακές ικανότητες και πειθώ, ώστε να είναι σε θέση να αναφέρεται απευθείας στην ανώτερη διοίκηση και να τους πείθει να υποστηρίζουν το πρόγραμμα συμμόρφωσης και προστασίας των δεδομένων προσωπικού χαρακτήρα.

- Απαιτούμενη εμπειρία για να συντονίζει την τυχόν εσωτερική ομάδα που ασχολείται με το πρόγραμμα προστασίας δεδομένων προσωπικού χαρακτήρα, ως επικεφαλής ομάδας.

Ο ΥΠΔ θα πρέπει να διαθέτει αποδείξεις ως προς την επάρκεια της ειδικής και εξειδικευμένης γνώσης και πείρας του/της στον τομέα της προστασίας προσωπικών δεδομένων.

Α.4.1.2 Αρμοδιότητες του Υπεύθυνου Προστασίας Δεδομένων

Το Πανεπιστήμιο Αιγαίου αναθέτει στον ΥΠΔ τις ακόλουθες αρμοδιότητες:

- Να εκπροσωπεί το Πανεπιστήμιο Αιγαίου έναντι των Αρχών, εθνικών και ευρωπαϊκών.

- Να συμβουλεύει την ανώτερη διοίκηση σε θέματα προστασίας δεδομένων προσωπικού χαρακτήρα.

- Να εισηγείται απευθείας στην ανώτερη διοίκηση τις κατάλληλες πολιτικές προστασίας των δεδομένων.

- Να παρακολουθεί και να εναρμονίζει τη λειτουργία του Υπεύθυνου Επεξεργασίας ή του Εκτελούντα την Επεξεργασία σε ό,τι αφορά τις πολιτικές, πρακτικές και μεθοδολογίες επεξεργασίας, αποθήκευσης και μεταφοράς δεδομένων προσωπικού χαρακτήρα.

- Να προστατεύει τον Υπεύθυνο Επεξεργασίας ή τον Εκτελούντα την Επεξεργασία από τους κινδύνους επιβολής των σημαντικότατων και βαρύτατων διοικητικών προστίμων που προβλέπονται ρητά από τον Κανονισμό.

- Να μεριμνά για την εξασφάλιση της υποστήριξης της ανώτερης διοίκησης και να αιτείται εγκαίρως τον απαιτούμενο προϋπολογισμό για την εφαρμογή του προγράμματος προστασίας των δεδομένων.

- Να καταρτίζει το πρόγραμμα και την πολιτική προστασίας δεδομένων και να εποπτεύει την εφαρμογή τους, να αξιολογεί τον βαθμό συμμετοχής και την επιτυχία του και να προβαίνει στις αναγκαίες διορθώσεις, όπου απαιτείται.

- Να καταρτίζει Ευρετήριο Προσωπικών Δεδομένων που αφορά στο είδος των προσωπικών δεδομένων, τον τρόπο αποθήκευσης και επεξεργασίας τους, τον επιτρεπόμενο χρόνο αποθήκευσής τους και τη μεθοδολογία διαγραφής ή καταστροφής τους.

- Να εκτιμά και να συμβουλεύει για την κατά περίπτωση αναγκαιότητα κατάρτισης Εκτίμησης Αντικτύπου και να καταρτίζει πρότυπο υποδείγματος Εκτίμησης Αντικτύπου.

- Να συντονίζει τη διατμηματική συνεργασία με τις διευθύνσεις και τμήματα Ανθρώπινου Δυναμικού, Ασφάλειας Πληροφοριών και Πληροφοριακών Συστημάτων, Νομικής και Κανονιστικής Συμμόρφωσης, Προώθησης και Προμηθειών για τη δημιουργία μίας διαρκούς εταιρικής κουλτούρας προστασίας των δεδομένων ως πολύτιμου περιουσιακού στοιχείου του Πανεπιστημίου.

- Να σχεδιάζει και να πραγματοποιεί εσωτερικά εκπαιδευτικά προγράμματα και να τηρεί τα απαιτούμενα αρχεία ολοκλήρωσης των εκπαιδεύσεων ανά τμήμα/ομάδα εργαζομένων.

A.4.2 Οργανόγραμμα

Η οργανωτική δομή του Πανεπιστημίου Αιγαίου θα πρέπει να αποτυπώνει τον διακριτό ρόλο του ΥΠΔ.

A.5. Νομιμότητα της Επεξεργασίας

A.5.1 Έλεγχος νομιμότητας επεξεργασίας

Το Πανεπιστήμιο Αιγαίου οφείλει να αναπτύξει διαδικασία αναγνώρισης του τύπου των δεδομένων (προσωπικά, ειδικών κατηγοριών, καταδίκες) και να είναι σε θέση να αποδείξει ότι ο τρόπος επεξεργασίας τους συντάσσεται με τις οδηγίες περί επεξεργασίας των διαφόρων τύπων.

Υπάρχουν έξι εναλλακτικοί τρόποι με τους οποίους μπορεί να θεσπιστεί η νομιμότητα επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

Συγκατάθεση: Όπου απαιτείται, το Πανεπιστήμιο Αιγαίου θα αποκτά ρητή συγκατάθεση του υποκειμένου για τη συλλογή και επεξεργασία των δεδομένων του. Διαφανείς πληροφορίες σχετικά με τη χρήση των προσωπικών δεδομένων θα παρέχονται στα υποκείμενα δεδομένων τη στιγμή που θα αποκτηθεί η συγκατάθεση και θα εξηγηθούν τα δικαιώματά τους όσον αφορά στα δεδομένα τους, όπως το δικαίωμα ανάκλησης της συναίνεσης. Οι πληροφορίες αυτές θα παρέχονται σε προσιτή μορφή, χωρίς δαπάνη και θα είναι αποτυπωμένες σε σαφή γλώσσα.

Εκτέλεση σύμβασης: Όταν τα δεδομένα προσωπικού χαρακτήρα που συλλέγονται και υποβάλλονται σε επεξεργασία αφορούν εκτέλεση σύμβασης με το Υποκείμενο των Δεδομένων, δεν απαιτείται ρητή συγκατάθεση.

Έννομη υποχρέωση: Εάν τα προσωπικά δεδομένα πρέπει να συλλεχθούν και να υποβληθούν σε επεξεργασία σύμφωνα με την εθνική και ευρωπαϊκή νομοθεσία, τότε δεν απαιτείται ρητή συγκατάθεση. Αυτό μπορεί να συμβαίνει για ορισμένα στοιχεία που σχετίζονται με την απασχόληση και τη φορολογία, καθώς και την τήρηση στοιχείων των φοιτητών και φοιτητριών και των πτυχιούχων του Πανεπιστημίου.

Ζωτικά συμφέροντα του υποκειμένου των δεδομένων: Σε περίπτωση που τα προσωπικά δεδομένα απαιτούνται για την προστασία των ζωτικών συμφερόντων του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου, τότε αυτό μπορεί να χρησιμοποιηθεί ως νόμιμη βάση για τη επεξεργασία. Το Πανεπιστήμιο Αιγαίου θα διατηρήσει λογικές και τεκμηριωμένες αποδείξεις ότι αυτό συμβαίνει, όποτε αυτός ο λόγος χρησιμοποιείται ως νόμιμη βάση για την επεξεργασία προσωπικών δεδομένων.

Επεξεργασία δεδομένων για το Δημόσιο Συμφέρον: Όταν το Πανεπιστήμιο Αιγαίου χρειάζεται να εκτελεί καθήκον, το οποίο θεωρεί ότι είναι προς το δημόσιο συμφέρον ή ως μέρος ενός υπηρεσιακού καθήκοντος, τότε δεν θα ζητηθεί η συγκατάθεση του υποκειμένου των δεδομένων. Η αξιολόγηση του δημόσιου συμφέροντος ή του επίσημου καθήκοντος θα τεκμηριωθεί και θα τεθεί ως αποδεικτικό στοιχείο, εφόσον απαιτείται.

Έννομο ενδιαφέρον: Εάν η επεξεργασία συγκεκριμένων προσωπικών δεδομένων είναι προς το έννομο συμφέρον του Πανεπιστημίου Αιγαίου και κρίνεται ότι δεν θίγει σημαντικά τα δικαιώματα

και τις ελευθερίες του υποκειμένου των δεδομένων, αυτό μπορεί να οριστεί ως ο νόμιμος λόγος για τη επεξεργασία. Ωστόσο και πάλι, η συλλογιστική για αυτή την άποψη θα τεκμηριωθεί με σαφήνεια.

Α.5.2 Συγκατάθεση ως βάση για την Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα

Το Πανεπιστήμιο Αιγαίου πρέπει να καταγράφει τη νομική βάση για την επεξεργασία των δεδομένων. Όταν η συγκατάθεση αποτελεί τη νομική βάση για τη μεταφορά/αποθήκευση προσωπικών δεδομένων, αυτή πρέπει να παρέχεται από το Υποκείμενο των Δεδομένων ελεύθερα, να είναι συγκεκριμένη, ξεκάθαρη και να έπεται της απαιτούμενης σχετικής ενημέρωσης. Τόσο ο Υπεύθυνος Επεξεργασίας όσο και ο Εκτελών την Επεξεργασία, πρέπει να είναι σε θέση να λογοδοτήσει για το είδος των δεδομένων που επεξεργάζεται, για τον σκοπό της επεξεργασίας και σε ποιες χώρες και τρίτα μέρη διαβιβάζονται τα δεδομένα.

Α.5.3 Πληροφόρηση Υποκειμένων των Δεδομένων

Πριν τη διαδικασία λήψης συγκατάθεσης, ο Υπεύθυνος Επεξεργασίας οφείλει να ενημερώσει το Υποκείμενο των Δεδομένων, κατ' ελάχιστο για όλα τα ουσιαστικά στοιχεία της επεξεργασίας:

- Για την ταυτότητα και τα στοιχεία επικοινωνίας του Υπεύθυνου Επεξεργασίας.
- Για την ταυτότητα και τα στοιχεία επικοινωνίας του ΥΠΔ.
- Για την ταυτότητα και τα στοιχεία επικοινωνίας που αφορούν τρίτους και αποδέκτες που ενδεχομένως εμπλέκονται στην επεξεργασία των δεδομένων.
- Για τους σκοπούς και τη νομική βάση της επεξεργασίας.
- Για το χρονικό διάστημα τήρησης των δεδομένων.
- Για την πρόθεση διασυνοριακής διαβίβασης.
- Για τα δικαιώματα του Υποκειμένου των Δεδομένων.

Επιπλέον, η ενημέρωση πρέπει να είναι εύκολα προσβάσιμη, αναγνώσιμη και κατανοητή, ώστε το Υποκείμενο των Δεδομένων να έχει πραγματική επιλογή.

Α.5.3.1 Διαχείριση Συγκαταθέσεων

Η διαδικασία συγκατάθεσης πρέπει να είναι φιλική προς τον χρήστη, προς αποφυγή ασαφειών. Η δυνατότητα απόσυρσης της συγκατάθεσης πρέπει να μπορεί να διεξάγεται ανά πάσα στιγμή από το Υποκείμενο των Δεδομένων.

Πρόσβαση: Πρέπει να διασφαλιστεί ότι τα Υποκείμενα των Δεδομένων έχουν πρόσβαση στην τρέχουσα κατάσταση της συγκατάθεσής τους ανά πάσα στιγμή και μπορούν να αλλάξουν τις ρυθμίσεις τους ή να αποσύρουν πλήρως τη συγκατάθεση.

Ανανέωση: Μετά την πρώτη είσοδο του Υποκειμένου των Δεδομένων στο εκάστοτε σύστημα, η συγκατάθεση πρέπει να ανανεώνεται ανά δώδεκα (12) μήνες.

A.5.3.2 Αρχείο Συγκαταθέσεων

Ο Υπεύθυνος Επεξεργασίας πρέπει να είναι σε θέση να αποδείξει ότι έχει καταγράψει τη συγκατάθεση των Υποκειμένων των Δεδομένων αναφορικά με την επεξεργασία των προσωπικών τους δεδομένων. Προτείνεται η δημιουργία και διατήρηση αρχείου συγκαταθέσεων, το οποίο θα καταγράφει την αλληλεπίδραση στη συγκατάθεση μεταξύ του Υποκειμένου των Δεδομένων και του Υπεύθυνου Επεξεργασίας, αναφέροντας:

- Την ταυτότητα του Υποκειμένου των Δεδομένων
- Τον χρόνο λήψης της συγκατάθεσης
- Τη θέση και το περιεχόμενο της συγκατάθεσης μεταξύ αυτών των μερών, σε συνδυασμό με τους όρους της συγκατάθεσης που επιτρέπουν την απόδειξη (ή μη) της συμβατότητας με τον ΓΚΠΔ.

Το αρχείο καταγραφής της συγκατάθεσης των Υποκειμένων των Δεδομένων πρέπει να αποθηκεύεται με ασφαλή τρόπο και να μπορεί χρησιμοποιηθεί σε περίπτωση ελέγχου.

A.5.3.3 Λήψη συγκατάθεσης μέσω ιστοτόπου του Πανεπιστημίου Αιγαίου

Το Πανεπιστήμιο Αιγαίου παρέχει επίσης δυνατότητα λήψης συγκατάθεσης μέσω του ιστοτόπου του. Το Πανεπιστήμιο Αιγαίου πρέπει να μεριμνήσει ώστε να παρέχει, μέσω του ιστοτόπου του, εύχρηστο μηχανισμό αιτήματος συγκατάθεσης, ώστε τα Υποκείμενα των Δεδομένων να μπορούν να εκφράσουν σαφώς τη συγκατάθεση ή την άρνησή τους στην επεξεργασία των δεδομένων τους. Μέσω του μηχανισμού αυτού, το Πανεπιστήμιο Αιγαίου οφείλει να επεξηγεί την αναγκαιότητα της επεξεργασίας των δεδομένων (π.χ. cookies[1]) και το όφελος των ψηφιακών λειτουργιών.

Σε περίπτωση εμπλοκής τρίτων, το Πανεπιστήμιο Αιγαίου οφείλει να παρέχει συνδέσμους (links) που θα οδηγούν στις Πολιτικές Προστασίας Δεδομένων των εμπλεκόμενων τρίτων.

A.5.4 Πληροφόρηση και Διαχείριση Συγκαταθέσεων

Το Πανεπιστήμιο Αιγαίου οφείλει να υλοποιήσει διαδικασία μέσω της οποίας θα ενημερώνει το Υποκείμενο των Δεδομένων σε περίπτωση που τα δεδομένα που κατέχει δεν έχουν συλλεγεί από το Υποκείμενο των Δεδομένων.

A.5.5 Δευτερεύουσα χρήση δεδομένων

Το Πανεπιστήμιο Αιγαίου οφείλει να υλοποιήσει διαδικασία μέσω της οποίας θα ενημερώνει το Υποκείμενο των Δεδομένων και θα λαμβάνει τη συγκατάθεσή του για χρήση των δεδομένων άλλη από αυτή του σκοπού για τον οποίο συλλέχθηκαν τα δεδομένα.

---

[1] Η χρήση των cookies πρέπει να γίνεται με εμφανή τρόπο και να δίνεται η δυνατότητα στα Υποκείμενα των Δεδομένων να γνωρίζουν πώς χρησιμοποιούνται τα δεδομένα τους.

Α.5.6 Συγκατάθεση παιδιών

Το Πανεπιστήμιο Αιγαίου οφείλει να υλοποιήσει διαδικασία μέσω της οποίας θα λαμβάνει τη συγκατάθεση, όταν το Υποκείμενο των Δεδομένων είναι ανήλικος.

Α.5.7 Διατήρηση της Ποιότητας των Δεδομένων

Το Πανεπιστήμιο Αιγαίου οφείλει να αναπτύξει διαδικασία για τη διατήρηση της ποιότητας των δεδομένων.

Α.5.8 Ελαχιστοποίηση Δεδομένων

Το Πανεπιστήμιο Αιγαίου οφείλει να αναπτύξει διαδικασία για να ελέγχει ότι τα δεδομένα που επεξεργάζεται πράγματι απαιτούνται για την ολοκλήρωση των σκοπών επεξεργασίας.

Α.5.9 Χρονικό Διάστημα Διατήρησης Δεδομένων

Κατά την ανάπτυξη ενός Πληροφοριακού Συστήματος και ενώ έχει οριστεί ο σκοπός επεξεργασίας δεδομένων, το Πανεπιστήμιο Αιγαίου οφείλει να ελέγξει/καθορίσει το χρονικό διάστημα κατά το οποίο θα τηρεί τα δεδομένα τα οποία κατέχει.

Α.5.10 Διαδικασία για τη Διαχείριση Αρχείου Δραστηριοτήτων Επεξεργασίας

Το Πανεπιστήμιο Αιγαίου οφείλει να διατηρεί αρχείο δραστηριοτήτων επεξεργασίας για τις οποίες είναι υπεύθυνο. Προτείνεται η ανάπτυξη εκτενούς καταλόγου εταιρικών πληροφοριακών πόρων (data inventory) και η εφαρμογή κατάλληλου σχήματος διαβάθμισης δεδομένων (data classification). Οι πληροφορίες που πρέπει να τηρούνται περιλαμβάνουν στοιχεία επικοινωνίας του Υπεύθυνου Επεξεργασίας, τους σκοπούς επεξεργασίας, περιγραφή των κατηγοριών Υποκειμένων των Δεδομένων, περιγραφή των κατηγοριών δεδομένων προσωπικού χαρακτήρα και γενική περιγραφή των τεχνικών και οργανωτικών μέτρων ασφάλειας που έχει λάβει το Πανεπιστήμιο Αιγαίου.

Α.6. Ικανοποίηση Δικαιωμάτων των Υποκειμένων των Δεδομένων

Α.6.1 Δικαίωμα Ενημέρωσης

Εφόσον τα δεδομένα των φυσικών προσώπων έχουν συλλεγεί από το Υποκείμενο των Δεδομένων, το Πανεπιστήμιο Αιγαίου υποχρεούται να υλοποιήσει διαδικασία μέσω της οποίας οι χρήστες θα ενημερώνονται για:

- Την ταυτότητα και τα στοιχεία επικοινωνίας του Υπεύθυνου Επεξεργασίας (ή εκπροσώπου αυτού).
- Τα στοιχεία επικοινωνίας του ΥΠΔ.
- Τους σκοπούς επεξεργασίας για τους οποίους προορίζονται τα δεδομένα.
- Τη νομική βάση για την επεξεργασία.
- Τα έννομα συμφέροντα που επιδιώκονται από τον Υπεύθυνο Επεξεργασίας, ή από τρίτο.

- Τους αποδέκτες, ή τις κατηγορίες αποδεκτών των δεδομένων.
- (Κατά περίπτωση) Την πρόθεση του Υπεύθυνου Επεξεργασίας να διαβιβάσει τα δεδομένα σε τρίτη χώρα ή διεθνή οργανισμό.
- Το χρονικό διάστημα διατήρησης των δεδομένων, ή τα κριτήρια που καθορίζουν αυτό το διάστημα.
- Την ύπαρξη δικαιώματος των χρηστών υποβολής αιτήματος στον Υπεύθυνο Επεξεργασίας αναφορικά με την άσκηση των δικαιωμάτων τους (πρόσβαση, διόρθωση, διαγραφή, περιορισμό επεξεργασίας, αντίταξη στην επεξεργασία, φορητότητα δεδομένων).
- Το δικαίωμα ανάκλησης της συγκατάθεσης.
- Το δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή.
- Τη νομική ή συμβατική υποχρέωση, ή απαίτηση για σύναψη σύμβασης που (πιθανόν να) υποχρεώνει το Υποκείμενο των Δεδομένων να παρέχει τα δεδομένα του και τις ενδεχόμενες συνέπειες που φέρει η μη παροχή.
- Την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων (συμπεριλαμβανομένης της κατάρτισης προφίλ).

Επιπλέον, εάν ο Υπεύθυνος Επεξεργασίας προτίθεται να χρησιμοποιήσει τα δεδομένα που έχει συλλέξει για σκοπούς άλλους από αυτούς για τους οποίους τα δεδομένα συλλέχθηκαν, οφείλει να παρέχει στο Υποκείμενο των Δεδομένων πληροφορίες για τον σκοπό αυτόν.

Εφόσον τα δεδομένα των φυσικών προσώπων δεν έχουν συλλεγεί από τα ίδια τα φυσικά πρόσωπα, το Πανεπιστήμιο Αιγαίου, εκτός των ανωτέρω σημείων, υποχρεούται, σε εύλογο χρονικό διάστημα από τη συλλογή αλλά το αργότερο εντός ενός μηνός, να εντάξει στην παραπάνω διαδικασία ενημέρωσης πληροφορίες για:

- Την πηγή από την οποία προέρχονται τα δεδομένα (κατά περίπτωση, αναφορά εάν η εν λόγω πηγή είναι προσβάσιμη από το κοινό).

Α.6.2 Δικαίωμα Πρόσβασης

Το Πανεπιστήμιο Αιγαίου δεσμεύεται να έχει στον ιστότοπό του ή σε όλα τα υπόλοιπα συστήματά του, κατάλληλο μηχανισμό με τον οποίο θα επιβεβαιώνεται στο Υποκείμενο των Δεδομένων κατά πόσο ή όχι τα δεδομένα προσωπικού χαρακτήρα που το αφορούν υφίστανται επεξεργασία. Εφόσον τα δεδομένα του Υποκειμένου υφίστανται επεξεργασία, το Πανεπιστήμιο Αιγαίου οφείλει να παρέχει στο Υποκείμενο των Δεδομένων πληροφορίες που αφορούν:

1. Στους σκοπούς της επεξεργασίας.
2. Στις σχετικές κατηγορίες δεδομένων.
3. Στους αποδέκτες των κατηγοριών αυτών.

4. Στο χρονικό διάστημα για το οποίο θα αποθηκευτούν τα δεδομένα προσωπικού χαρακτήρα.

5. Στην ύπαρξη δικαιώματος υποβολής αιτήματος στον Υπεύθυνο Επεξεργασίας για διόρθωση ή διαγραφή των δεδομένων ή περιορισμό της επεξεργασίας των δεδομένων που αφορούν το Υποκείμενο των Δεδομένων.

6. Στο δικαίωμα υποβολής καταγγελίας στην εποπτική αρχή.

7. Στην προέλευση των δεδομένων, όταν αυτά δεν έχουν συλλεγεί από το Υποκείμενο των Δεδομένων.

8. Εφόσον υπάρχει, στην ύπαρξη αυτοματοποιημένης λήψης αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ.

Α.6.3 Δικαίωμα Διόρθωσης

Το Πανεπιστήμιο Αιγαίου υποχρεούται να υλοποιήσει διαδικασία μέσω της οποίας οι χρήστες θα μπορούν να διορθώνουν ή να ζητούν τη διόρθωση, χωρίς κόστος, για τα προσωπικά δεδομένα που το Πανεπιστήμιο Αιγαίου διατηρεί για εκείνους.

Α.6.4 Δικαίωμα Διαγραφής

Το Πανεπιστήμιο Αιγαίου υποχρεούται να υλοποιήσει διαδικασία μέσω της οποίας οι χρήστες θα μπορούν να διαγράφουν, ή να ζητούν τη διαγραφή, χωρίς κόστος, για τα προσωπικά δεδομένα που το Πανεπιστήμιο Αιγαίου διατηρεί για εκείνους.

Α.6.5 Δικαίωμα Περιορισμού Επεξεργασίας

Το Πανεπιστήμιο Αιγαίου υποχρεούται να υλοποιήσει διαδικασία μέσω της οποίας οι χρήστες θα μπορούν να αιτηθούν περιορισμό της επεξεργασίας. Όταν η επεξεργασία έχει περιοριστεί, το Πανεπιστήμιο Αιγαίου πρέπει να προδιαγράψει διαδικασία λήψης συγκατάθεσης από τα Υποκείμενα των Δεδομένων προκειμένου να συνεχίσει την επεξεργασία. Σε περίπτωση άρσης του περιορισμού της επεξεργασίας, το Πανεπιστήμιο Αιγαίου οφείλει να ενημερώσει το Υποκείμενο των Δεδομένων.

Α.6.6 Δικαίωμα Φορητότητας Δεδομένων

Το Πανεπιστήμιο Αιγαίου υποχρεούται να υλοποιήσει διαδικασία μέσω της οποίας οι χρήστες θα μπορούν να μεταβιβάζουν, ή να ζητούν τη μεταβίβαση, χωρίς κόστος, των προσωπικών δεδομένων τους σε άλλον φορέα.

Α.6.7 Δικαίωμα Εναντίωσης

Το Πανεπιστήμιο Αιγαίου υποχρεούται να υλοποιήσει διαδικασία μέσω της οποίας οι χρήστες θα μπορούν να δηλώσουν την εναντίωσή τους όσον αφορά στην επεξεργασία των δεδομένων τους, συμπεριλαμβανομένης της κατάρτισης προφίλ των χρηστών.

Α.6.8 Διαδικασία για τη Διαχείριση Αιτημάτων Φυσικών Προσώπων

Το Πανεπιστήμιο Αιγαίου οφείλει να έχει σε ευκρινές σημείο, είτε στις εγκαταστάσεις του, είτε στον ιστότοπό του, φόρμα την οποία μπορεί να χρησιμοποιήσει το Υποκείμενο των Δεδομένων ώστε να υποβάλει αίτημα που εμπίπτει στα δικαιώματά του (ενότητες 6.1 – 6.7).

Α.6.9 Ρόλοι και αρμοδιότητες για τα δικαιώματα των Υποκειμένων των Δεδομένων

Ο ΥΠΔ διαχειρίζεται τα αιτήματα των Υποκειμένων των Δεδομένων. Το Πανεπιστήμιο Αιγαίου οφείλει να παράσχει στο Υποκείμενο των Δεδομένων όλες τις πληροφορίες που απαιτούνται για την απάντηση του αιτήματος, χωρίς καθυστέρηση, και σε κάθε περίπτωση εντός μηνός από την παραλαβή του αιτήματος (ή δύο μήνες αργότερα εφόσον απαιτείται, ανάλογα με την πολυπλοκότητα του αιτήματος και τον αριθμό των αιτημάτων).

Α.7. Διαβίβαση Δεδομένων Προσωπικού Χαρακτήρα σε τρίτες χώρες

Το Πανεπιστήμιο Αιγαίου επιτρέπεται να μεταβιβάσει τα δεδομένα σε άλλους φορείς σε τρίτες χώρες ή σε διεθνείς οργανισμούς οι οποίοι είναι συμμορφωμένοι με τον ΓΚΠΔ, σε εκείνους που εμπίπτουν σε δικαιοδοσίες που θεωρούνται «επαρκείς», ή σε εκείνους που επαρκούν βάσει εταιρικών κανόνων, που πρέπει να έχουν εγκριθεί από την αντίστοιχη εποπτική αρχή.

Το Πανεπιστήμιο Αιγαίου, εφόσον προτίθεται να μεταβιβάσει τα δεδομένα που επεξεργάζεται σε τρίτες χώρες, πρέπει να αποθηκεύσει τα δεδομένα σε βάση με τέτοιο τρόπο ώστε να είναι εξαγώγιμα στα συνήθη πρότυπα (π.χ. xml/json/excel table, κ.λπ.).

Α.8. Διαχείριση Τρίτων – Εκτελούντων Επεξεργασία Προσωπικών Δεδομένων

Εφόσον το Πανεπιστήμιο Αιγαίου προτίθεται να χρησιμοποιήσει Εκτελούντες την Επεξεργασία, επιλέγει εκείνους που παρέχουν επαρκείς διαβεβαιώσεις για την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων ώστε η επεξεργασία να πληροί τις απαιτήσεις του ΓΚΠΔ. Η μεταξύ τους σύμβαση εργασίας ρυθμίζει τις υποχρεώσεις του κάθε μέρους.

Α.9. Προστασία δεδομένων κατά τη διαβίβαση ή κοινοποίηση

Το Πανεπιστήμιο Αιγαίου οφείλει να υλοποιήσει διαδικασία κατά την οποία (είτε ως Υπεύθυνος Επεξεργασίας είτε ως Εκτελών την Επεξεργασία) ελέγχει τη συμμόρφωση των εμπλεκόμενων στην επεξεργασία των δεδομένων συνεργατών του. Η συμμόρφωση των εμπλεκομένων ακολουθεί κατευθύνσεις που ορίζει το Πανεπιστήμιο Αιγαίου.

Α.10. Ενσωμάτωση Προδιαγραφών Προστασίας Δεδομένων από τον Σχεδιασμό και Εξ' Ορισμού

Α.10.1 Προδιαγραφές Προστασίας Δεδομένων κατά τον Σχεδιασμό Συστημάτων και εξ' Ορισμού

Το Πανεπιστήμιο Αιγαίου μεριμνά κατά την ανάπτυξη νέων πληροφοριακών συστημάτων για την αναγνώριση και καταγραφή τεχνικών προδιαγραφών για την προστασία των δεδομένων

προσωπικού χαρακτήρα. Ο Υπεύθυνος Ανάπτυξης Πληροφοριακών Συστημάτων συμβουλεύεται τον ΥΠΔ και επιλέγει μέθοδο ανάπτυξης συστημάτων που επιτρέπει την αναγνώριση και μοντελοποίηση των προδιαγραφών και απαιτήσεων προστασίας δεδομένων, κατά την ανάλυση των συνολικών προδιαγραφών κάθε νέου συστήματος και πριν την υλοποίηση του συστήματος αυτού (by design).

Επίσης, θα πρέπει ο Υπεύθυνος Ανάπτυξης Πληροφοριακών Συστημάτων να εξασφαλίσει ότι εξ ορισμού υφίστανται επεξεργασία μόνο τα δεδομένα προσωπικού χαρακτήρα που είναι απαραίτητα για τον εκάστοτε σκοπό επεξεργασίας και ταυτόχρονα είναι απαραίτητο οι «προ-καθορισμένες» (by-default) ρυθμίσεις των εφαρμογών να είναι οι κατά το δυνατόν πιο φιλικές προς την ιδιωτικότητα.

Α.10.2 Διαδικασίες για την Προμήθεια Συστημάτων

Το Πανεπιστήμιο Αιγαίου μεριμνά κατά την προμήθεια νέων συστημάτων για την αναγνώριση και διασφάλιση προδιαγραφών προστασίας δεδομένων προσωπικού χαρακτήρα. Ο Υπεύθυνος Ανάπτυξης Πληροφοριακών Συστημάτων συμβουλεύεται τον ΥΠΔ και διασφαλίζει ότι κάθε προκήρυξη προμήθειας νέου πληροφοριακού συστήματος περιλαμβάνει στις υποχρεώσεις του αναδόχου υλοποίησης την αναγνώριση και μοντελοποίηση προδιαγραφών και απαιτήσεων προστασίας προσωπικών δεδομένων και την ενσωμάτωση των προδιαγραφών στο νέο σύστημα κατά την ανάπτυξη.

Οι προμηθευτές Πληροφοριακών Συστημάτων ενός φορέα πρέπει να αποδείξουν ότι έχουν εφαρμόσει τις αρχές που επιτάσσει ο νόμος στις λύσεις που θα χρησιμοποιήσει το Πανεπιστήμιο Αιγαίου. Αυτό απαιτεί ιδιαίτερη προσοχή κατά την καταγραφή προδιαγραφών και κριτηρίων αξιολόγησης για την απόκτηση ενός νέου Πληροφοριακού Συστήματος.

Α.11. Αντιμετώπιση Περιστατικών Παραβίασης Δεδομένων Προσωπικού Χαρακτήρα

Ο Υπεύθυνος Επεξεργασίας οφείλει να διατηρεί:

- Σχέδιο αντιμετώπισης περιστατικών παραβίασης δεδομένων προσωπικού χαρακτήρα
- Σχέδιο ενημέρωσης των Υποκειμένων και των αρμόδιων Αρχών
- Περιβάλλον καταγραφής περιστατικών παραβίασης δεδομένων προσωπικού χαρακτήρα.

Ο Υπεύθυνος Επεξεργασίας θεωρείται ότι λαμβάνει γνώση μιας παραβίασης δεδομένων όταν έχει επιβεβαιωθεί ότι έχει συμβεί κάποιο γεγονός που έχει ως αποτέλεσμα την παραβίαση χρήσης προσωπικών δεδομένων. Κατά την αρχική διερεύνηση του συμβάντος, η οποία πρέπει να ξεκινήσει το συντομότερο δυνατόν, ο Υπεύθυνος Επεξεργασίας δεν θεωρείται ότι έχει γνώση της παραβίασης. Είτε είναι αμέσως σαφές ότι διακυβεύονται προσωπικά δεδομένα είτε το συμπέρασμα αυτό απαιτεί κάποιο χρονικό διάστημα για να εξαχθεί, πρέπει να δοθεί έμφαση στην άμεση δράση για τη διερεύνηση του περιστατικού προκειμένου να διαπιστωθεί εάν όντως υπήρξε παραβίαση προσωπικών δεδομένων.

Μόλις περάσει η σύντομη περίοδος έρευνας και ο Υπεύθυνος Επεξεργασίας έχει επιβεβαιώσει το περιστατικό, θεωρείται ενήμερος και τότε απαιτείται κοινοποίηση στην εποπτική Αρχή.

Α.11.1 Γνωστοποίηση στην Εποπτική Αρχή

Όταν εντοπιστεί πιθανή παραβίαση δεδομένων και εφόσον υπάρχει κίνδυνος για φυσικά πρόσωπα, ο Υπεύθυνος Επεξεργασίας δεδομένων πρέπει να ενημερώσει την αρμόδια εποπτική αρχή «αμελλητί και, εφόσον είναι δυνατόν, το αργότερο εντός 72 ωρών από τη στιγμή που την αντελήφθη».

Εφόσον η παραβίαση έχει εντοπιστεί από τον Εκτελούντα την Επεξεργασία θα πρέπει να ειδοποιεί «αμελλητί» τους Υπεύθυνους Επεξεργασίας σχετικά με τις παραβιάσεις. Αυτή η ειδοποίηση πρέπει να είναι «άμεση» για να βοηθήσει τον Υπεύθυνο Επεξεργασίας να τηρήσει τις χρονικές δεσμεύσεις. Εάν ο Εκτελών την Επεξεργασία προσφέρει υπηρεσίες σε περισσότερους από έναν Υπεύθυνο Επεξεργασίας, ο Εκτελών την Επεξεργασία πρέπει να αναφέρει το περιστατικό και λεπτομέρειες σχετικά με αυτό σε καθέναν από αυτούς.

Α.11.2 Διαδικασίες που επιτρέπουν την έγκαιρη γνωστοποίηση

Το Πανεπιστήμιο Αιγαίου οφείλει να σχεδιάσει διαδικασίες που θα περιγράφουν τον τρόπο επικοινωνίας του με την εποπτική Αρχή και τις πληροφορίες που θα της κοινοποιήσει. Το Πανεπιστήμιο Αιγαίου οφείλει να αναφέρει:

- Τη φύση της παραβίασης, συμπεριλαμβάνοντας, αν είναι εφικτό, τις κατηγορίες και τον αριθμό των επηρεαζόμενων Υποκειμένων των Δεδομένων και τις κατηγορίες των δεδομένων.
- Το όνομα και τα στοιχεία επικοινωνίας του ΥΠΔ.
- Τις ενδεχόμενες συνέπειες που μπορεί να επιφέρει η παραβίαση.
- Τα ληφθέντα ή προτεινόμενα προς λήψη μέτρα για την αντιμετώπιση της παραβίασης.

Α.11.3 Ανακοίνωση σε Υποκείμενα των Δεδομένων

Το Πανεπιστήμιο Αιγαίου οφείλει να ενημερώσει τα Υποκείμενα των Δεδομένων για την παραβίαση των δεδομένων τους εφόσον το περιστατικό παραβίασης δεδομένων ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες τους.

Το Πανεπιστήμιο Αιγαίου οφείλει να σχεδιάσει διαδικασίες που θα περιγράφουν τον τρόπο επικοινωνίας του με τα Υποκείμενα των Δεδομένων και τις πληροφορίες που θα τους κοινοποιήσει. Η ενημέρωση αυτή πρέπει να είναι συνοπτική, διαφανής, κατανοητή και σε εύκολα προσβάσιμη μορφή. Το Πανεπιστήμιο Αιγαίου οφείλει να χρησιμοποιεί σαφή και απλή διατύπωση, ιδίως όταν η ενημέρωση αφορά σε παιδιά.

Οι διαδικασίες πρέπει να περιλαμβάνουν παροχή πληροφοριών μέσω εντύπων, ηλεκτρονικά, ή και προφορικά εφόσον, όμως, έχει επιβεβαιωθεί η ταυτότητα του Υποκειμένου των Δεδομένων.

Α.11.4 Διαδικασία για τη Διαχείριση Αστοχιών

Με χρήση κατάλληλων τεχνολογιών, το Πανεπιστήμιο Αιγαίου παρακολουθεί τα κρίσιμης σημασίας πληροφοριακά του συστήματα που διαχειρίζονται προσωπικά δεδομένα. Σε περίπτωση που υπάρξει κάποιο περιστατικό διαρροής δεδομένων που οφείλεται σε αστοχία πληροφοριακών συστημάτων του, το Πανεπιστήμιο Αιγαίου πρέπει να ακολουθήσει κατάλληλη διαδικασία ώστε να μπορεί να αιτιολογήσει/τεκμηριώσει τους μηχανισμούς ασφάλειας που έχει εφαρμόσει.

Α.11.5 Διαδικασία για τη Διαχείριση Καταγγελιών

Το Πανεπιστήμιο Αιγαίου οφείλει να σχεδιάσει διαδικασία για τη διαχείριση καταγγελιών στην εποπτική αρχή που μπορεί να δεχθεί από τα Υποκείμενα των Δεδομένων, εάν αυτά θεωρούν ότι η επεξεργασία των δεδομένων που τους αφορά παραβαίνει τον ΓΚΠΔ.

Α.11.6 Ρόλοι και αρμοδιότητες για τη διαχείριση περιστατικών παραβίασης

Το Πανεπιστήμιο Αιγαίου οφείλει να δημιουργήσει εσωτερική ομάδα αντιμετώπισης παραβιάσεων, η οποία πρέπει να είναι αντιπροσωπευτική από όλες τις περιοχές του. Η ομάδα αυτή είναι υπεύθυνη για τον περιορισμό, την αντιμετώπιση και την ανάκτηση λειτουργίας του Πανεπιστημίου Αιγαίου.

Οι ρόλοι και οι αρμοδιότητες των συμμετεχόντων πρέπει να είναι ξεκάθαροι. Ο ΥΠΔ προτείνεται να είναι ο επικεφαλής διοίκησης της ομάδας.

Η ομάδα οφείλει να καταγράψει τα αποδεικτικά στοιχεία ενός περιστατικού.

Α.12. Εκπαίδευση και Ενημερότητα του Προσωπικού

Το Πανεπιστήμιο Αιγαίου πρέπει να παρέχει σε περιοδική βάση επαρκείς και κατάλληλες δράσεις ενημερότητας στο προσωπικό, το οποίο αξιοποιεί ή διαχειρίζεται προσωπικά δεδομένα φυσικών προσώπων, ανάλογα με τον ρόλο του κάθε υπαλλήλου. Οι χρήστες των αντίστοιχων πληροφοριακών συστημάτων πρέπει να είναι εφοδιασμένοι με τα απαραίτητα μέσα (π.χ. εγχειρίδια, εργαλεία) για την ορθή και ασφαλή χρήση των πληροφοριακών συστημάτων που διαχειρίζονται προσωπικά δεδομένα. Το Πανεπιστήμιο Αιγαίου πρέπει επίσης να παρέχει σε περιοδική βάση εκπαίδευση στο εξειδικευμένο προσωπικό (ιδιαίτερα το προσωπικό πληροφορικής και επικοινωνιών) προκειμένου να αναπτύσσουν, χρησιμοποιούν και συντηρούν το λογισμικό, τις εφαρμογές και τον υλικό εξοπλισμό για την προστασία των δεδομένων και τη συμμόρφωση με τον ΓΚΠΔ.

Α.12.1 Ενημερότητα Προσωπικού

Το Πανεπιστήμιο Αιγαίου πρέπει να μεριμνά ώστε το προσωπικό που εργάζεται στον οργανισμό να είναι ενήμερο για την τρέχουσα εκδοχή της Πολιτικής Προστασίας Δεδομένων, για τις προσωπικές τους αρμοδιότητες αναφορικά με την εφαρμογή της Πολιτικής, καθώς και για τις κυρώσεις που επιβάλλονται σε περίπτωση παραβίασης αυτής.

Α.12.2 Εκπαίδευση Εξειδικευμένου Προσωπικού

Το Πανεπιστήμιο Αιγαίου πρέπει να διασφαλίζει ότι το προσωπικό του οργανισμού κατέχει τις γνώσεις και τις δεξιότητες για την εφαρμογή της Πολιτικής Προστασίας Δεδομένων και να

αξιολογεί τακτικά (τουλάχιστον ετησίως) τις σχετικές γνώσεις και δεξιότητες. Το Πανεπιστήμιο Αιγαίου πρέπει να μεριμνά για την παροχή δράσεων κατάρτισης και εκπαίδευσης, όπου απαιτείται, και να αξιολογεί την αποτελεσματικότητα των δράσεων αυτών στην επίδοση του εξειδικευμένου προσωπικού.

Α.13. Παρακολούθηση και Μέτρηση Απόδοσης

Α.13.1 Διαδικασίες Παρακολούθησης και Συμμόρφωσης με τη Νομοθεσία και το Κανονιστικό Πλαίσιο

Το Πανεπιστήμιο Αιγαίου οφείλει να αποδείξει ότι έχει ενεργοποιήσει τους κατάλληλους μηχανισμούς ώστε να παρακολουθεί συνεχώς το επίπεδο συμμόρφωσής του με τις απαιτήσεις του νόμου. Τόσο το Νομικό τμήμα του Πανεπιστημίου Αιγαίου, όσο και ο Υπεύθυνος Ανάπτυξης Πληροφοριακών Συστημάτων, οφείλουν να παρακολουθούν τις πολιτικές και τις διαδικασίες που έχουν αναπτυχθεί και τις τεχνολογίες που επιτρέπουν τη συνεχή παρακολούθηση και αξιολόγηση αδυναμιών ασφάλειας.

Α.13.2 Συμμόρφωση με τις υποχρεώσεις ως Υπεύθυνος Επεξεργασίας Δεδομένων

Το Πανεπιστήμιο Αιγαίου οφείλει να συμμορφώνεται με τις υποχρεώσεις που ορίζει ο ΓΚΠΔ για τον Υπεύθυνο Επεξεργασίας Δεδομένων. Η συμμόρφωση με τις υποχρεώσεις εξασφαλίζεται ως ακολούθως:

Υποχρέωση Υπεύθυνου Επεξεργασίας Δεδομένων	Διαδικασίες
Να έχει υλοποιήσει τα απαραίτητα τεχνικά και οργανωτικά μέτρα, ώστε να εξασφαλίζει την άσκηση των δικαιωμάτων του Υποκειμένου των Δεδομένων	Κεφάλαιο Α.6 Υποκεφάλαιο Β.1.2
Να γνωστοποιεί πράξεις που αφορούν σε διόρθωση ή διαγραφή δεδομένων προσωπικού χαρακτήρα ή τον περιορισμό της επεξεργασίας	Υποκεφάλαιο Α.6.1
Να αναγνωρίσει την ευθύνη του Υπεύθυνου Επεξεργασίας • Διαμόρφωση της ευθύνης σε περίπτωση ενός Υπεύθυνου Επεξεργασίας • Διαμόρφωση της ευθύνης σε περίπτωση από κοινού Υπευθύνων Επεξεργασίας	Κεφάλαιο Α.13
Να προστατεύει τα δεδομένα ήδη από τον σχεδιασμό των συστημάτων επεξεργασίας (data protection by design): Με κατάλληλες τεχνολογίες ιδιωτικότητας και προστασία προσωπικών δεδομένων κατά τον σχεδιασμό συστήματος/επεξεργασίας, και όχι εκ των υστέρων, λαμβάνοντας υπόψη τις τελευταίες εξελίξεις της τεχνολογίας, το κόστος εφαρμογής των μέτρων, τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας και την ελαχιστοποίηση της πιθανότητας κινδύνων που διακυβεύουν τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων από την επεξεργασία.	Κεφάλαιο Α.10

Υποχρέωση Υπεύθυνου Επεξεργασίας Δεδομένων	Διαδικασίες
Το Πανεπιστήμιο Αιγαίου καλείται να επιλέξει μία μεθοδολογία data protection by design σε κάθε προϊόν λογισμικού.	Κεφάλαιο Α.10
Οι «προκαθορισμένες» ρυθμίσεις θα πρέπει να είναι πιο φιλικές προς την ιδιωτικότητα – Ο Υπεύθυνος Πληροφορικής θα πρέπει να κάνει τους απαραίτητους ελέγχους ώστε τα προϊόντα να είναι συμβατά με τις αρχές της ιδιωτικότητας εξ ορισμού.	Κεφάλαιο Α.10
Οφείλει να τηρεί αρχεία σχετικά με τις δραστηριότητες επεξεργασίας. Η υποχρέωση αυτή δεν ισχύει για φορέα που απασχολεί λιγότερους από 250 εργαζόμενος, εκτός εάν: ● Η διενεργούμενη επεξεργασία ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες του Υποκειμένου των Δεδομένων. ● Η επεξεργασία δεν είναι περιστασιακή. ● Η επεξεργασία περιλαμβάνει ειδικές κατηγορίες δεδομένων. ● Η επεξεργασία περιλαμβάνει δεδομένα προσωπικού χαρακτήρα που αφορούν σε ποινικές καταδίκες και αδικήματα.	Υποκεφάλαιο Α.5.10
Οφείλει να συνεργάζεται με την εποπτική αρχή αναφορικά με: ● Κατευθυντήριες γραμμές, συστάσεις, βέλτιστες πρακτικές ● Κανονιστικές πράξεις ● Κώδικες δεοντολογίας ● Πιστοποιήσεις ● Αρχεία δραστηριοτήτων ● Εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων ● Διαβιβάσεις ● Περιστατικά παραβίασης ● Ελέγχους ● Διορθωτικές εξουσίες	Κεφάλαιο Α.4
Οφείλει να διασφαλίσει το απόρρητο και την ασφάλεια της επεξεργασίας: ● Με χρήση κατάλληλων τεχνικών και οργανωτικών μέτρων όπως είναι: a. Η ψευδωνυμοποίηση και η κρυπτογράφηση. Η διασφάλιση του απορρήτου, της ακεραιότητας, της διαθεσιμότητας και της αξιοπιστίας b. Η αποκατάσταση της διαθεσιμότητας και της πρόσβασης σε περίπτωση συμβάντος. Η δοκιμή, εκτίμηση και η διαρκής αξιολόγηση της αποτελεσματικότητας των μέτρων ● Με χρήση εγκεκριμένου κώδικα δεοντολογίας ή μηχανισμού πιστοποίησης	Παραδοτέο Π1.4: «Πλάνο Τεχνικών, Οργανωτικών και Διαδικαστικών Ενεργειών για Συμμόρφωση με τον Ευρωπαϊκό Κανονισμό 2016/679»

Υποχρέωση Υπεύθυνου Επεξεργασίας Δεδομένων	Διαδικασίες
Οφείλει να γνωστοποιήσει, εντός 72 ωρών από τη στιγμή που θα αποκτήσει γνώση του γεγονότος, την παραβίαση των δεδομένων προσωπικού χαρακτήρα στην Εποπτική Αρχή, εκτός και αν η παραβίαση αυτή δεν ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων.	Κεφάλαιο Α.11.1
Οφείλει να διενεργήσει εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων και προηγούμενη διαβούλευση ● Αναφορικά με την εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων, ο Υπεύθυνος Επεξεργασίας οφείλει: a. Να έχει περιγράψει συστηματικά τις προβλεπόμενες πράξεις επεξεργασίας, τους σκοπούς της επεξεργασίας και τη νομική βάση αυτών b. Να εκτιμήσει την αναγκαιότητα και την αναλογικότητα των πράξεων επεξεργασίας c. Να εκτιμήσει τους κινδύνους για τα δικαιώματα και τις ελευθερίες των Υποκειμένων των Δεδομένων d. Να έχει ορίσει τα προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων ● Εφόσον, μετά την εκπόνηση της εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων, προκύπτει ακόμη «υψηλός κίνδυνος», ο Υπεύθυνος Επεξεργασίας οφείλει να προχωρήσει σε διαβούλευση με την Εποπτική Αρχή	Κεφάλαιο Α.3 Παραδοτέο Π1.3: «Ανάλυση Αντίκτυπου για την Ιδιωτικότητα και την Προστασία Δεδομένων (Privacy Impact Assessment)»
Οφείλει να ορίσει Υπεύθυνο Προστασίας Δεδομένων, εφόσον: ● Η επεξεργασία των δεδομένων διενεργείται από δημόσια αρχή ή φορέα. ● Οι βασικές δραστηριότητες του Υπεύθυνου Επεξεργασίας απαιτούν τακτική και συστηματική παρακολούθηση των Υποκειμένων των Δεδομένων σε μεγάλη κλίμακα. ● Οι βασικές δραστηριότητες του Υπεύθυνου Επεξεργασίας συνιστούν μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα και δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα	Κεφάλαιο Α.4

Πίνακας 1: Παρακολούθηση των υποχρεώσεων του Πανεπιστημίου ως Υπεύθυνου Επεξεργασίας Δεδομένων

Α.13.3 Συμμόρφωση με τις υποχρεώσεις ως Εκτελούντος την Επεξεργασία Δεδομένων

Εφόσον το Πανεπιστήμιο Αιγαίου αναθέτει σε εξωτερικό φορέα να επεξεργαστεί δεδομένα προσωπικού χαρακτήρα για λογαριασμό του Πανεπιστημίου Αιγαίου, ο εξωτερικός φορέας θεωρείται Εκτελών την Επεξεργασία και οι υποχρεώσεις του ρυθμίζονται από τη μεταξύ τους σύμβαση. Η συμμόρφωση με τις υποχρεώσεις εξασφαλίζεται ως ακολούθως:

Υποχρέωση Εκτελούντων την Επεξεργασία Δεδομένων	Διαδικασίες
Οφείλει να βοηθά τον Υπεύθυνο της Επεξεργασίας στην εκτέλεση των υποχρεώσεων του ΓΚΠΔ.	Κεφάλαιο Α.8
Για καθέναν από τους σκοπούς της επεξεργασίας, ο Εκτελών την Επεξεργασία: ● Οφείλει να προχωρεί σε επεξεργασία αποκλειστικά πάνω στη βάση των καταγεγραμμένων εντολών του Υπεύθυνου Επεξεργασίας. ● Εφόσον η επεξεργασία γίνεται για άλλο σκοπό, με πρωτοβουλία του Εκτελούντος, τον καθιστά Υπεύθυνο Επεξεργασίας και αποτελεί παραβίαση. ● Τα πρόσωπα που είναι εξουσιοδοτημένα, έχουν αναλάβει δέσμευση τήρησης εμπιστευτικότητας.	Κεφάλαιο Α.8
Οφείλει να ενημερώνει τον Υπεύθυνο της Επεξεργασίας ότι τους ζητείται παράνομη ενέργεια.	Κεφάλαιο Α.8
Οφείλει να διατηρεί αρχεία δραστηριοτήτων	Υποκεφάλαιο Α.5.10
Οφείλει να ορίσει ΥΠΔ, εφόσον: ● Η επεξεργασία των δεδομένων διενεργείται από δημόσια αρχή ή φορέα. Οι βασικές δραστηριότητες του Υπεύθυνου Επεξεργασίας απαιτούν τακτική και συστηματική παρακολούθηση των Υποκειμένων των Δεδομένων σε μεγάλη κλίμακα. ● Οι βασικές δραστηριότητες του Υπεύθυνου Επεξεργασίας συνιστούν μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων και δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα	Κεφάλαιο Α.4
Σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα, οφείλει να ενημερώσει τον Υπεύθυνο Επεξεργασίας αμέσως μόλις αντιληφθεί παραβίαση δεδομένων.	Κεφάλαιο Α.11
Οφείλει να συνεργάζεται με τις Αρχές.	Κεφάλαιο Α.4

Πίνακας 2: Παρακολούθηση των υποχρεώσεων των Εκτελούντων την Επεξεργασία Δεδομένων για λογαριασμό του Πανεπιστημίου

Α.13.4 Διαδικασίες Μέτρησης Απόδοσης

Το Πανεπιστήμιο Αιγαίου οφείλει να σχεδιάσει πλάνο παρακολούθησης και αξιολόγησης της αποτελεσματικότητας της Πολιτικής Προστασίας Δεδομένων. Το πλάνο πρέπει να περιλαμβάνει:

- Μετρικές απόδοσης, αναφορικά με την ικανοποίηση των δικαιωμάτων των υποκειμένων δεδομένων και τη συμμόρφωση με τον ΓΚΠΔ.
- Μεθόδους και τεχνικές για την παρακολούθηση και τη συλλογή δεδομένων.
- Συχνότητα μετρήσεων, ανάλυσης των δεδομένων και αξιολόγησης.

Μέρος Β': Διαδικασίες Εφαρμογής της Πολιτικής Προστασίας Δεδομένων του Πανεπιστημίου Αιγαίου

Β.1. Πολιτική Προστασίας Δεδομένων του Πανεπιστημίου Αιγαίου

Σε αυτή την ενότητα ορίζονται οι πολιτικές που οφείλει να ακολουθήσει το Πανεπιστήμιο Αιγαίου, ως Υπεύθυνος Επεξεργασίας, καθώς και οι Εκτελούντες την Επεξεργασία για λογαριασμό του Πανεπιστημίου, προκειμένου να προστατεύσει τα δεδομένα των χρηστών των ΠΣ και να συμμορφωθεί με τον ΓΚΠΔ. Οι διαδικασίες που περιγράφονται αφορούν τις δραστηριότητες επεξεργασίας που ανήκουν στους σκοπούς επεξεργασίας δεδομένων προσωπικού χαρακτήρα του Πανεπιστημίου όπως αυτοί αναλύθηκαν στο παραδοτέο Π1.3.

Β.1.1. Νομιμότητα της επεξεργασίας

Β.1.1.1 Διαδικασία της λήψης συγκατάθεσης των Υποκειμένων των Δεδομένων

Προκειμένου να είναι έγκυρη η συγκατάθεση που λαμβάνεται από τα υποκείμενα των δεδομένων θα πρέπει να πληρούνται οι ακόλουθες προϋποθέσεις σύμφωνα με τον ΓΚΠΔ:

- να παρέχεται ελεύθερα,
- να είναι συγκεκριμένη, δηλαδή το Υποκείμενο των Δεδομένων να συμφωνεί στην επεξεργασία αναφορικά με έναν συγκεκριμένο σκοπό επεξεργασίας και όχι γενικά και αόριστα,
- να είναι ρητή, δηλαδή το Υποκείμενο των Δεδομένων να συμφωνεί στην επεξεργασία κατά τρόπο ρητό, με σαφή θετική ενέργεια,
- να συνοδεύεται από την κατάλληλη ενημέρωση.

Πιο συγκεκριμένα, η συγκατάθεση θα πρέπει να παρέχεται με σαφή θετική ενέργεια, η οποία να συνιστά ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει ένδειξη της συμφωνίας του υποκειμένου των δεδομένων υπέρ της επεξεργασίας των δεδομένων που το αφορούν. Θεωρείται ότι η συγκατάθεση δόθηκε ελεύθερα, αν το Υποκείμενο των Δεδομένων έχει «πραγματική» επιλογή ή αν είναι σε θέση να αρνηθεί ή να αποσύρει τη συγκατάθεσή του χωρίς να ζημιωθεί. Επιπλέον, για να έχει δοθεί ελεύθερα θα πρέπει να μην συνδέεται με την αποδοχή όρων ή προϋποθέσεων για την εκτέλεση μιας σύμβασης ή παροχής υπηρεσιών, όπως και με την ενημέρωση του Πανεπιστημίου για την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

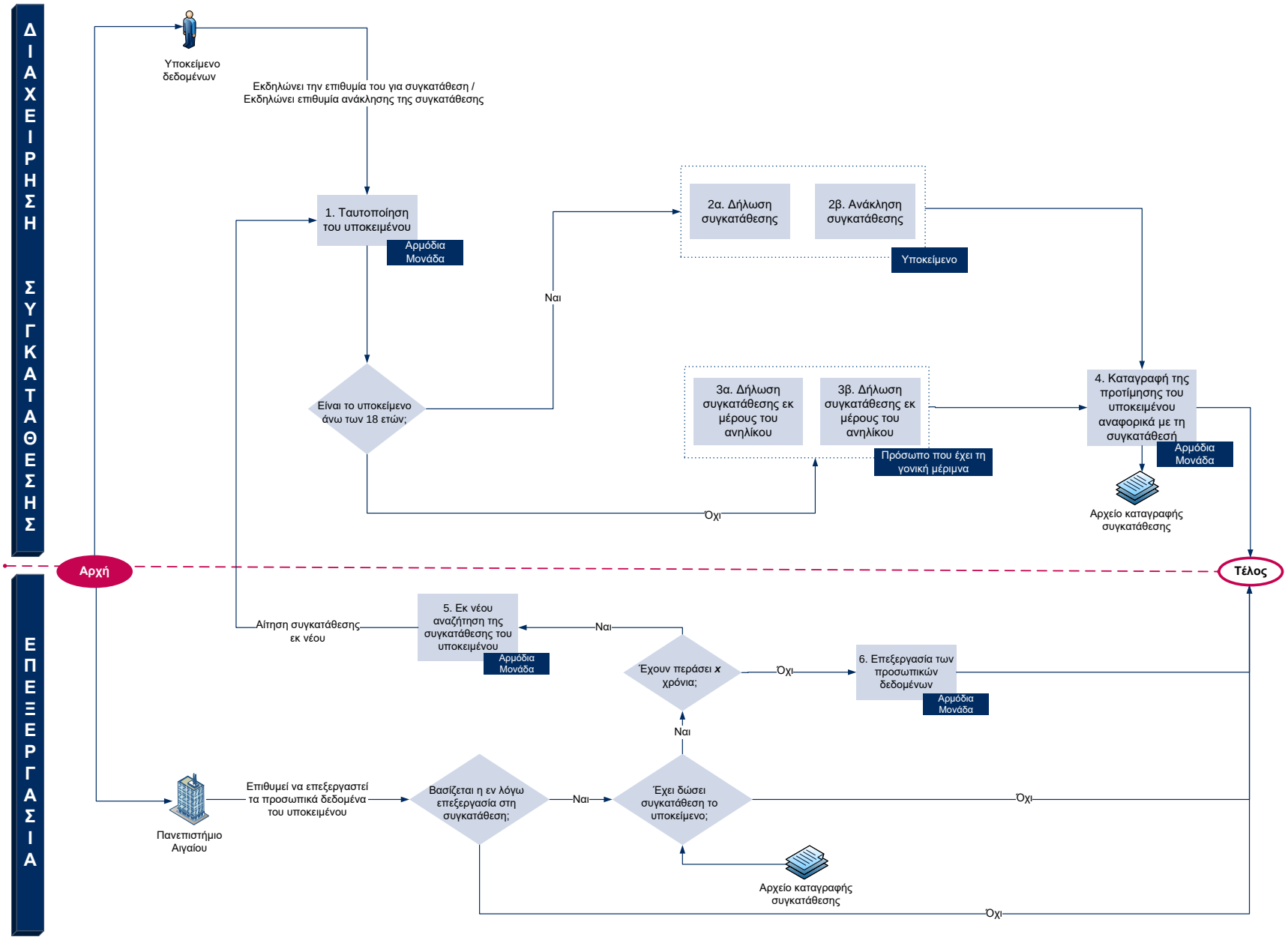
Περαιτέρω, το κείμενο μέσω του οποίου παρέχεται η συγκατάθεση πρέπει είναι συνοπτικό και να περιλαμβάνει τουλάχιστον τα ακόλουθα στοιχεία: i) την «ταυτότητα» του Πανεπιστημίου Αιγαίου (όνομα και στοιχεία επικοινωνίας), ii) τον σκοπό / τους σκοπούς της (κάθε) επεξεργασίας για την οποία ζητείται η συγκατάθεση του Υποκειμένου, iii) τα δεδομένα (ή τις κατηγορίες δεδομένων) προσωπικού χαρακτήρα που συλλέγονται και χρησιμοποιούνται για τον σκοπό της επεξεργασίας, iv) ενημέρωση σχετικά με το δικαίωμα ανάκλησης της συγκατάθεσης, v) σε περίπτωση που το Υποκείμενο υπόκειται σε απόφαση που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης

επεξεργασίας των δεδομένων του, λεπτομέρειες σχετικά με αυτήν, vi) σε περίπτωση διαβίβασης των δεδομένων του σε τρίτες χώρες ή διεθνείς οργανισμούς χωρίς να υπάρχουν οι κατάλληλες εγγυήσεις ή απόφαση επάρκειας, αναφορά των πιθανών κινδύνων από τη διαβίβαση αυτή.

Η δήλωση συγκατάθεσης θα πρέπει να παρέχεται σε χρόνο πρότερο της επεξεργασίας. Ως εκ τούτου, το Πανεπιστήμιο θα πρέπει να παρέχει εκ των προτέρων το αίτημα για τη συγκατάθεση στο Υποκείμενο των Δεδομένων και όχι εκ των υστέρων.

B.1.1.1.1 Σχηματική απεικόνιση της διαδικασίας

Στο παρακάτω Σχήμα φαίνεται η διαδικασία που θα πρέπει να ακολουθηθεί προκειμένου να ληφθεί η συγκατάθεση από τα Υποκείμενα των Δεδομένων που διαχειρίζεται το Πανεπιστήμιο Αιγαίου με σκοπό την παροχή υπηρεσιών.



Σχήμα 1: Σχηματική απεικόνιση της διαδικασίας της λήψης συγκατάθεσης των Υποκειμένων των Δεδομένων

B.1.1.1.2 Περιγραφή των βημάτων της διαδικασίας

Σε αυτή την ενότητα περιγράφονται τα βήματα της διαδικασίας της λήψης συγκατάθεσης των Υποκειμένων των Δεδομένων που θα πρέπει να ακολουθηθούν.

Το Υποκείμενο των Δεδομένων εκδηλώνει, μέσω των διαθέσιμων καναλιών, την επιθυμία του να παράσχει ή να ανακαλέσει τη συγκατάθεσή του για κάποια υπηρεσία που προσφέρει το Πανεπιστήμιο ή για κάποια επεξεργασία που εκτελεί επί των δεδομένων προσωπικού χαρακτήρα που το αφορούν και βασίζεται στη συγκατάθεση ως νόμιμη βάση.

Βήμα 1: Ταυτοποίηση του υποκειμένου

Μόλις το Υποκείμενο των Δεδομένων εκδηλώσει την επιθυμία του για παροχή ή ανάκληση της συγκατάθεσής του, το Πανεπιστήμιο οφείλει, προτού προχωρήσει στην όποια ενέργεια, να το ταυτοποιήσει. Επομένως, η Μονάδα του Πανεπιστημίου που είναι αρμόδια για την εν λόγω ενέργεια, είναι υπεύθυνη για τη διεξαγωγή των απαιτουμένων ελέγχων για την ταυτοποίηση του Υποκειμένου.

Ο Πίνακας 3 παρουσιάζει τον τρόπο και τις ελάχιστες απαιτούμενες πληροφορίες για την ταυτοποίηση του Υποκειμένου των Δεδομένων ανάλογα με το δίαυλο επικοινωνίας που χρησιμοποιείται.

Κανάλι επικοινωνίας	Ταυτοποίηση υποκειμένου	Στοιχεία ταυτοποίησης
Φυσική παρουσία	Η Γραμματεία του εκάστοτε Τμήματος ή το τμήμα Διοικητικού ταυτοποιεί το υποκείμενο βάσει της υφιστάμενης διαδικασίας	Ταυτότητα, πάσο, διαβατήριο, κ.λπ.
Ιστοσελίδα εκάστοτε Τμήματος, με σύνδεση στην ιστοσελίδα	Το υποκείμενο συνδέεται στην ιστοσελίδα του Τμήματος χρησιμοποιώντας τα στοιχεία αυθεντικοποίησής του.	Username, password, URL, κ.λπ.

Πίνακας 3: Ταυτοποίηση Υποκειμένου των Δεδομένων

Σε περίπτωση που το Υποκείμενο των Δεδομένων είναι άνω των 18 ετών, η διαδικασία συνεχίζεται στο **βήμα 2.** Διαφορετικά, η διαδικασία συνεχίζεται στο **βήμα 3**.

Σε περίπτωση δε, που δεν είναι δυνατόν να επαληθευτεί η ταυτότητα του Υποκειμένου των Δεδομένων από το Πανεπιστήμιο, τότε το Υποκείμενο δεν μπορεί να δώσει ή να ανακαλέσει τη συγκατάθεσή του.

Βήμα 2: Δήλωση / ανάκληση της συγκατάθεσης

α) Το Υποκείμενο των Δεδομένων, αφού ταυτοποιηθεί από το Πανεπιστήμιο, μπορεί να προχωρήσει σε δήλωση της συγκατάθεσής του προκειμένου τα δεδομένα προσωπικού χαρακτήρα που το αφορούν να αποτελέσουν αντικείμενο επεξεργασίας. Η εν λόγω ενέργεια επιτυγχάνεται μέσω των παρακάτω διαθέσιμων καναλιών επικοινωνίας του Πανεπιστημίου Αιγαίου, μέσω των οποίων το υποκείμενο δύναται να δηλώσει τη συγκατάθεσή του:

- Φυσική Παρουσία: Το Υποκείμενο των Δεδομένων συμπληρώνει στη Γραμματεία Φοιτητών και Φοιτητριών του Τμήματος εάν είναι φοιτητής ή φοιτήτρια ή απόφοιτος, ή στο τμήμα Διοικητικού εάν είναι καθηγητής ή καθηγήτρια ή υπάλληλος του Πανεπιστημίου, το τυποποιημένο έντυπο που βρίσκεται στο «Γ.2 Έντυπο δήλωσης συγκατάθεσης».

- Ιστοσελίδα εκάστοτε Τμήματος: Το Υποκείμενο των Δεδομένων αφού επισκεφτεί και συνδεθεί στην ιστοσελίδα κάποιου Τμήματος του Πανεπιστημίου Αιγαίου, συμπληρώνει την ηλεκτρονική φόρμα προκειμένου να δηλώσει τη συγκατάθεσή του. Προσχέδιο της εν λόγω ηλεκτρονικής φόρμας βρίσκεται στο Παράρτημα «Γ.2 Έντυπο δήλωσης συγκατάθεσης».

Η διαδικασία συνεχίζεται στο **βήμα 4**.

β) Αντίστοιχα, το Υποκείμενο των Δεδομένων, αφού ταυτοποιηθεί από το Πανεπιστήμιο, μπορεί να ανακαλέσει τη συγκατάθεση που έχει δώσει σε προγενέστερο χρόνο. Η εν λόγω ενέργεια επιτυγχάνεται συμπληρώνοντας το έντυπο στο Παράρτημα «Γ.1 Έντυπο αίτησης ανάκλησης συγκατάθεσης των Υποκειμένων των Δεδομένων».

Η δυνατότητα ανάκλησης της συγκατάθεσης παρέχεται από το Πανεπιστήμιο ανά πάσα στιγμή και πρέπει να είναι εξίσου εύκολη με την παροχή της συγκατάθεσης. Το Υποκείμενο των Δεδομένων θα πρέπει να μπορεί να ανακαλέσει τη συγκατάθεσή του χωρίς να υποστεί κάποια ζημία. Σημειώνεται ότι μόλις το Υποκείμενο ανακαλέσει τη συγκατάθεσή του, το Πανεπιστήμιο οφείλει να σταματήσει άμεσα την όποια επεξεργασία επί των προσωπικών του δεδομένων που βασιζόταν στη συγκατάθεση. Οι πράξεις επεξεργασίας που έλαβαν χώρα πριν την ανάκληση της συγκατάθεσης, παραμένουν νόμιμες. Σε κάθε περίπτωση, το Υποκείμενο των Δεδομένων έχει το δικαίωμα να ζητήσει με αίτησή του την ανάκληση της συγκατάθεσής του.

Η διαδικασία συνεχίζεται στο **βήμα 4**.

Βήμα 3: Δήλωση / ανάκληση της συγκατάθεσης εκ μέρους ανηλίκου

α) Σε περίπτωση που το Υποκείμενο των Δεδομένων δεν έχει συμπληρώσει το 18ο έτος της ηλικίας του, το Πανεπιστήμιο οφείλει να ζητήσει την έγκριση ή την παροχή της συγκατάθεσης από το πρόσωπο που έχει τη γονική μέριμνα του ανηλίκου. Η εν λόγω ενέργεια δύναται να πραγματοποιηθεί μέσω των διαθέσιμων καναλιών, με τους παρακάτω τρόπους:

- Φυσική Παρουσία: Το πρόσωπο που έχει τη γονική μέριμνα του ανηλίκου, αφού ταυτοποιηθεί, συμπληρώνει στη Γραμματεία Φοιτητών και Φοιτητριών του Τμήματος του Υποκειμένου το τυποποιημένο έντυπο που βρίσκεται στο Παράρτημα «Γ.2 Έντυπο δήλωσης συγκατάθεσης», ή εγκρίνει, παρουσία υπαλλήλου της Γραμματείας, τη συγκατάθεση του ανηλίκου.

- Ιστοσελίδα εκάστοτε Τμήματος: Το πρόσωπο που έχει τη γονική μέριμνα του ανηλίκου, συμπληρώνει την ηλεκτρονική φόρμα (Παράρτημα «Γ.2 Έντυπο δήλωσης συγκατάθεσης») για τη συγκατάθεση και μαζί επισυνάπτει βεβαίωση προκειμένου να δηλώσει ότι εγκρίνει ή παρέχει τη συγκατάθεση εκ μέρους του ανηλίκου. Επιπλέον, δηλώνει κάποιο τηλέφωνο επικοινωνίας ώστε να τον/την καλέσει σε δεύτερο χρόνο η αρμόδια Μονάδα του Πανεπιστημίου προκειμένου να επιβεβαιώσει τη δήλωσή του/της.

Το Πανεπιστήμιο Αιγαίου, στην προσπάθεια του να επαληθεύσει την ταυτότητα του προσώπου που δίνει τη συγκατάθεση εκ μέρους του ανηλίκου, χρησιμοποιεί και επεξεργάζεται μόνο τα απολύτως απαραίτητα για αυτόν τον σκοπό δεδομένα (π.χ. στοιχεία επικοινωνίας, ονοματεπώνυμο, Α.Δ.Τ. κ.λπ.).

Η διαδικασία συνεχίζεται στο **βήμα 4**.

β) Αντίστοιχα, το πρόσωπο που έχει τη γονική μέριμνα του ανηλίκου, μπορεί να ανακαλέσει τη συγκατάθεση που έχει δώσει σε προγενέστερο χρόνο εκ μέρους του. Η εν λόγω ενέργεια επιτυγχάνεται μέσω των προαναφερθέντων καναλιών επικοινωνίας του Πανεπιστημίου Αιγαίου.

Η διαδικασία συνεχίζεται στο **βήμα 4**.

Σημειώνεται ότι μόλις το Υποκείμενο των Δεδομένων συμπληρώσει το 18ο έτος της ηλικίας του, έχει πλέον τον πλήρη έλεγχο επί της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα που το αφορούν. Επομένως, το Υποκείμενο μπορεί να τροποποιήσει την επιλογή του γονέα ή κηδεμόνα σχετικά με τη συγκατάθεση. Το Πανεπιστήμιο Αιγαίου θα πρέπει να ενημερώσει τα εν λόγω Υποκείμενα για αυτή τους τη δυνατότητα. Σε περίπτωση που το Υποκείμενο δεν προβεί σε κάποια ενέργεια, τότε συνεχίζει να ισχύει η δήλωση του κηδεμόνα του.

Βήμα 4: Αποθήκευση της προτίμησης του Υποκειμένου σχετικά με τη συγκατάθεση

Το Πανεπιστήμιο πρέπει να είναι σε θέση να αποδείξει ανά πάσα στιγμή ότι η συγκατάθεση του Υποκειμένου στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν έχει ληφθεί νόμιμα, σε συμμόρφωση με τις απαιτήσεις του ΓΚΠΔ. Για τον λόγο αυτό, η δήλωση συγκατάθεσης του Υποκειμένου καταγράφεται και αποθηκεύεται σε ένα αρχείο, στο «Αρχείο Καταγραφής Συγκατάθεσης». Το εν λόγω αρχείο το τηρεί η Διεύθυνση Σπουδών ή η Γραμματεία εκάστου Τμήματος και έχει καταγεγραμμένες και συγκεντρωμένες τις δηλώσεις συγκατάθεσης όλων των προπτυχιακών φοιτητών και φοιτητριών, των μεταπτυχιακών φοιτητών και φοιτητριών και των αποφοίτων του Τμήματος. Το ίδιο ισχύει και για τις περιπτώσεις όπου το Υποκείμενο δεν είναι φοιτητής ή φοιτήτρια του Πανεπιστημίου αλλά έχει άλλου είδους σχέση με αυτό (π.χ. εργαζόμενος, συνεργάτης), με μόνη διαφορά ότι το προαναφερθέν αρχείο τηρείται από το τμήμα Διοικητικού του Πανεπιστημίου Αιγαίου.

Στο «Αρχείο Καταγραφής Συγκατάθεσης» πρέπει να είναι καταγεγραμμένες πληροφορίες σχετικά με τα παρακάτω:

- Το όνομα του υποκειμένου, ή κάποιο άλλο αναγνωριστικό ταυτότητας αυτού (π.χ. Αριθμός Μητρώου Φοιτητή, username στην ιστοσελίδα του Τμήματος, Α.Δ.Τ)

- Η ημερομηνία που το Υποκείμενο δήλωσε τη συγκατάθεσή του.

- Το κανάλι μέσω του οποίου το υποκείμενο δήλωσε τη συγκατάθεση του, ήτοι ηλεκτρονική φόρμα στην ιστοσελίδα του Τμήματος, τυποποιημένο έντυπο στη Γραμματεία του Τμήματος του ή στο τμήμα Διοικητικού.

- Αντίγραφο της δήλωσης συγκατάθεσης που κοινολογήθηκε στο Υποκείμενο, καθώς και αντίγραφο της ενημέρωσης που του είχε δοθεί σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα.

- Πληροφορίες σχετικά με το εάν το Υποκείμενο έχει ανακαλέσει τη συγκατάθεσή του και αν ναι, η ημερομηνία της ανάκλησης.

Η εκάστοτε αρμόδια μονάδα του Πανεπιστημίου πρέπει να τηρεί τα παραπάνω «αποδεικτικά στοιχεία» για όσο χρονικό διάστημα επεξεργάζεται δεδομένα βάσει της συγκατάθεσης.

Βήμα 5: Ενημέρωση του Υποκειμένου για τη λήψη νέας συγκατάθεσης

Σε αυτό το στάδιο της διαδικασίας, η μονάδα του Πανεπιστημίου που θέλει να επεξεργαστεί δεδομένα προσωπικού χαρακτήρα που αφορούν Υποκείμενο του οποίου η συγκατάθεση έχει ξεπεράσει το διάστημα των Χ χρόνων, αναζητεί εκ νέου τη συγκατάθεση του Υποκειμένου. Για τον λόγο αυτό, ενημερώνει τη Γραμματεία του Τμήματος στο οποίο φοιτά, πρόκειται να φοιτήσει ή φοιτούσε το Υποκείμενο των Δεδομένων ή το τμήμα Διοικητικού, που είναι η αρμόδια Μονάδα για τη λήψη της συγκατάθεσης από Υποκείμενο διαφορετικής «ταυτότητας» (π.χ. εργαζόμενος, συνεργάτης), ώστε να αιτηθεί εκ νέου τη συγκατάθεσή του.

Προκειμένου να ακολουθηθούν όλα τα απαραίτητα βήματα για τη λήψη έγκυρης συγκατάθεσης, η διαδικασία ξεκινάει από την αρχή (**βήμα 1**).

Βήμα 6: Παροχή Υπηρεσιών

Εφόσον ολοκληρωθούν τα παραπάνω βήματα της διαδικασίας, σε αυτό το βήμα τα Υποκείμενα των Δεδομένων έχουν τη δυνατότητα να χρησιμοποιήσουν τις υπηρεσίες του Πανεπιστημίου.

Η διαδικασία ολοκληρώνεται.

Β.1.1.2 Διαδικασία Ενημέρωσης Αρχείου Δραστηριοτήτων Επεξεργασίας

Ο ΓΚΠΔ υποχρεώνει με το Άρθρο 30 τους περισσότερους Υπεύθυνους Επεξεργασίας, καθώς και τους Εκτελούντες την Επεξεργασία, να τηρούν αρχείο με αναλυτική περιγραφή όλων των πράξεων επεξεργασίας που διενεργούν επί των δεδομένων προσωπικού χαρακτήρα.

Πιο συγκεκριμένα, κάθε Υπεύθυνος Επεξεργασίας ή Εκτελών την Επεξεργασία που απασχολεί περισσότερα από 250 άτομα υποχρεούται να τηρεί αρχείο δραστηριοτήτων επεξεργασίας. Το ίδιο ισχύει και για κάθε δραστηριότητα επεξεργασίας που εκτελείται από Υπεύθυνους ή Εκτελούντες την Επεξεργασία που απασχολούν λιγότερα από 250 άτομα και η οποία:

- Γίνεται σε συστηματική βάση, ή
- Αφορά ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα (άρθ. 9 παρ. 1 ΓΚΠΔ) ή δεδομένα ποινικών καταδικών και αδικημάτων (άρθ. 10 ΓΚΠΔ), ή
- Ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των Υποκειμένων των Δεδομένων.

Επομένως, το Πανεπιστήμιο Αιγαίου, έχοντας τον ρόλο του Υπεύθυνου Επεξεργασίας αλλά και, σε ορισμένες περιπτώσεις του Εκτελούντα την Επεξεργασία, οφείλει να αναπτύξει και να τηρεί δύο ξεχωριστά κεντρικά αρχεία δραστηριοτήτων επεξεργασίας, στα οποία θα αντικατοπτρίζονται όλες οι πράξεις επεξεργασίας δεδομένων προσωπικού χαρακτήρα που εκτελεί είτε για δικούς του σκοπούς ή για λογαριασμό τρίτων. Επιπλέον, κάθε μονάδα του Πανεπιστημίου που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα πρέπει να τηρεί τα δικά της αρχεία δραστηριοτήτων, στα οποία θα καταγράφονται οι δραστηριότητες επεξεργασίας που την αφορούν. Τα εν λόγω αρχεία είναι αρκετά σημαντικά, καθώς αφενός αποτελούν υποχρέωση του ΓΚΠΔ ως εργαλείο λογοδοσίας και αφετέρου συνδράμουν στην αποτελεσματική οργάνωση των δραστηριοτήτων επεξεργασίας δεδομένων προσωπικού χαρακτήρα που διενεργούνται από το Πανεπιστήμιο.

Σημειώνεται ότι το Πανεπιστήμιο Αιγαίου χρησιμοποιεί τα υποδείγματα των αρχείων δραστηριοτήτων που παρέχονται από την ελληνική Εποπτική Αρχή (ΑΠΔΠΧ). Περισσότερες πληροφορίες σχετικά με τα υποδείγματα της ΑΠΔΠΧ παρέχονται στο Παράρτημα Γ.8 (Υποδείγματα Αρχείων Δραστηριοτήτων Επεξεργασίας).

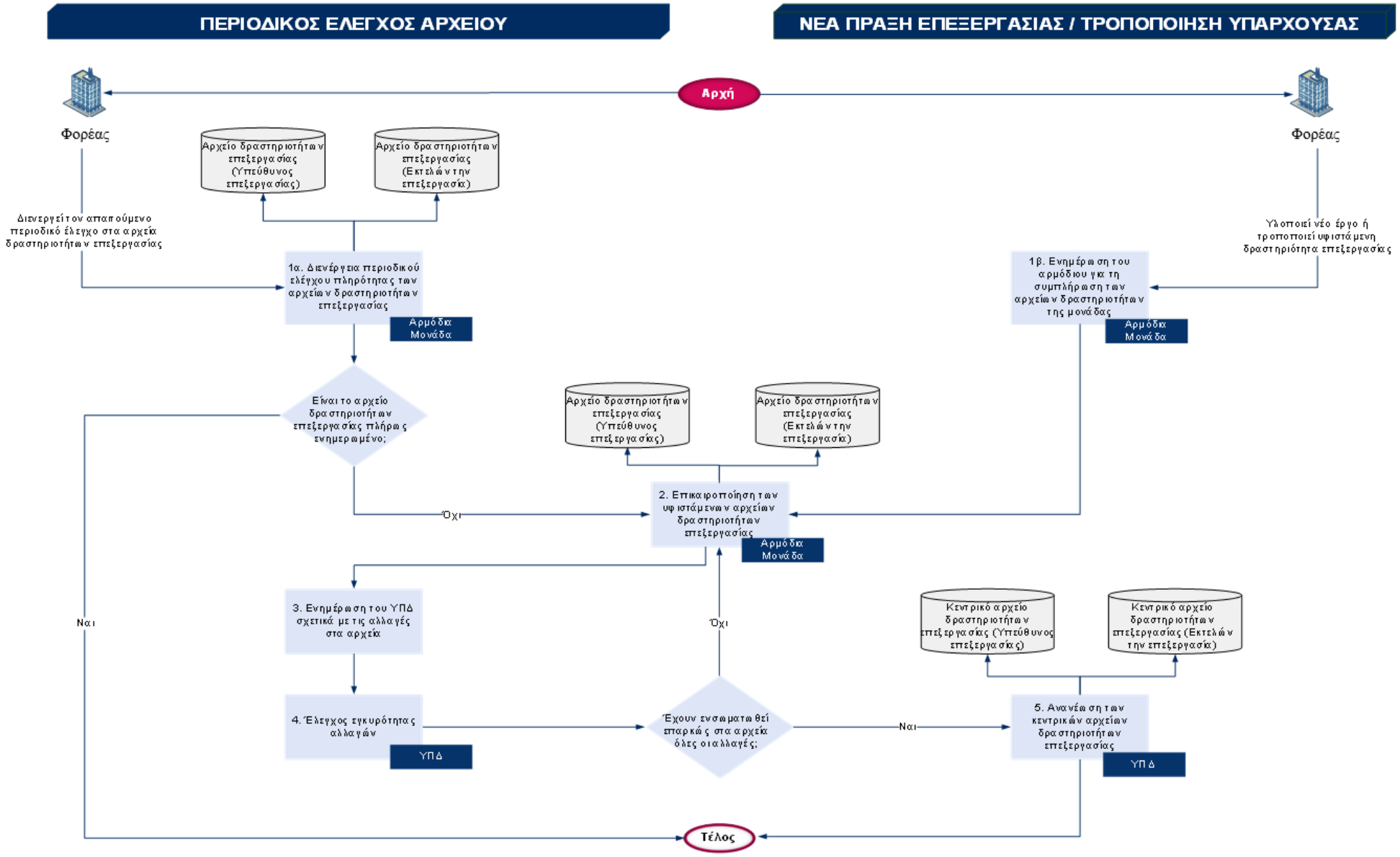
Στόχος της παρούσας διαδικασίας είναι να εξασφαλίσει ότι τα αρχεία δραστηριοτήτων επεξεργασίας που τηρούνται από το Πανεπιστήμιο Αιγαίου είναι πάντοτε ενημερωμένα με τις πληροφορίες που απαιτούνται από το Άρθρο 30 του ΓΚΠΔ και ευθυγραμμίζονται πλήρως με την υφιστάμενη κατάσταση του Πανεπιστημίου αναφορικά με τις δραστηριότητες επεξεργασίας δεδομένων προσωπικού χαρακτήρα που λαμβάνουν χώρα σε αυτό.

Η παρούσα διαδικασία δύναται να εκκινήσει σε δύο περιπτώσεις. Η πρώτη (1α) αφορά στην περίπτωση που οι μονάδες του Πανεπιστημίου διενεργούν τον απαιτούμενο περιοδικό έλεγχο πληρότητας των αρχείων δραστηριοτήτων επεξεργασίας που τηρούν. Ο εν λόγω έλεγχος διενεργείται από τις μονάδες του Πανεπιστημίου που επεξεργάζονται δεδομένα προσωπικού χαρακτήρα μία φορά το χρόνο. Η δεύτερη (1β) αφορά στην περίπτωση που ολοκληρωθεί ένα νέο

έργο ή τροποποιηθεί (ακόμη και εάν παύσει ή καταργηθεί) μία υφιστάμενη δραστηριότητα επεξεργασίας.

B.1.1.2.1 Σχηματική απεικόνιση της διαδικασίας

Στο παρακάτω Σχήμα φαίνεται η διαδικασία που θα πρέπει να ακολουθηθεί προκειμένου να ενημερωθεί το Αρχείο Δραστηριοτήτων Επεξεργασίας.



Σχήμα 2: Σχηματική απεικόνιση της διαδικασίας ενημέρωσης του Αρχείου Δραστηριοτήτων Επεξεργασίας

B.1.1.2.2 Περιγραφή των βημάτων της διαδικασίας

Σε αυτή την ενότητα περιγράφονται τα βήματα της διαδικασίας ενημέρωσης του αρχείου δραστηριοτήτων επεξεργασίας που θα πρέπει να ακολουθηθεί.

Βήμα 1α: Διενέργεια περιοδικού ελέγχου πληρότητας των αρχείων δραστηριοτήτων επεξεργασίας

Κάθε μονάδα του Πανεπιστημίου που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα είναι υπεύθυνη για τον περιοδικό έλεγχο των αρχείων δραστηριοτήτων επεξεργασίας που τηρεί. Ο ετήσιος αυτός έλεγχος έχει ως σκοπό να εντοπίσει τυχόν τροποποιήσεις που δεν έχουν συμπεριληφθεί στα αρχεία δραστηριοτήτων και κατ' επέκταση να διασφαλίσει την πληρότητα των υφιστάμενων αρχείων σε σχέση με τις δραστηριότητες επεξεργασίας που λαμβάνουν χώρα στην αντίστοιχη μονάδα. Στον παρακάτω πίνακα παρουσιάζονται ορισμένοι από τους παράγοντες που πρέπει να αξιολογούνται κατά τη διενέργεια του εν λόγω ελέγχου.

Ενδεικτικοί παράγοντες αξιολόγησης
Ύπαρξη νέων σκοπών επεξεργασίας.
Καταγεγραμμένοι σκοποί επεξεργασίας, οι οποίοι δεν ισχύουν πλέον.
Αλλαγές στα δεδομένα προσωπικού χαρακτήρα που υπόκεινται σε επεξεργασία (π.χ. κάποια δεδομένα μπορεί να μην υπόκεινται πλέον σε επεξεργασία).
Αλλαγή εκτελούντος την επεξεργασία (π.χ. την επεξεργασία τη διενεργεί πλέον το ίδιο το Πανεπιστήμιο ή κάποια διαφορετική οντότητα για λογαριασμό του Πανεπιστημίου).
Διαβίβαση των δεδομένων προσωπικού χαρακτήρα σε τρίτη χώρα, η οποία πρότερα δεν λάμβανε χώρα.

Πίνακας 4: Περιοδικός έλεγχος πληρότητας

Σε περίπτωση που τα αρχεία δραστηριοτήτων επεξεργασίας της μονάδας είναι πλήρως ενημερωμένα, δηλαδή δεν εντοπιστεί κάποια παρέκκλιση από την υφιστάμενη κατάσταση της μονάδας αναφορικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα που εκτελεί ως Υπεύθυνος Επεξεργασίας ή ως Εκτελών την Επεξεργασία, ο έλεγχος ολοκληρώνεται, όπως και η παρούσα διαδικασία. Διαφορετικά, η διαδικασία συνεχίζεται στο **βήμα 2**.

Βήμα 1β: Ενημέρωση του αρμόδιου για τη συμπλήρωση των αρχείων δραστηριοτήτων επεξεργασίας της μονάδας

Κάθε μονάδα του Πανεπιστημίου Αιγαίου ενημερώνει τον αρμόδιο υπάλληλό της για τη συμπλήρωση των αρχείων δραστηριοτήτων της, σε περίπτωση που:

- Ολοκληρωθεί η υλοποίηση κάποιου νέου έργου που αφορά ή εμπεριέχει δεδομένα προσωπικού χαρακτήρα,
- Τροποποιηθεί κάποια υφιστάμενη δραστηριότητα επεξεργασίας που διενεργείται επί των δεδομένων προσωπικού χαρακτήρα, ή
- Καταργηθεί ή παύσει κάποια υφιστάμενη δραστηριότητα επεξεργασίας.

Η διαδικασία συνεχίζεται στο **βήμα 2**.

Βήμα 2: Επικαιροποίηση των υφιστάμενων αρχείων δραστηριοτήτων επεξεργασίας

Ο υπάλληλος της μονάδας που είναι αρμόδιος για τη συμπλήρωση των αρχείων δραστηριοτήτων της, επικαιροποιεί τα υφιστάμενα αρχεία βάσει των αποκλίσεων που εντοπίστηκαν από τον περιοδικό έλεγχο ή βάσει των αλλαγών που έχουν προκύψει στις δραστηριότητες επεξεργασίας δεδομένων προσωπικού χαρακτήρα που διενεργεί η μονάδα.

Τα αρχεία δραστηριοτήτων επεξεργασίας, τόσο αυτό που αφορά στη μονάδα του Πανεπιστημίου ως Υπεύθυνη Επεξεργασίας, όσο και αυτό που αφορά στη μονάδα ως Εκτελούσα την Επεξεργασία, πρέπει να επικαιροποιηθούν ανάλογα με τις αλλαγές που έχουν διαπιστωθεί στα προηγούμενα βήματα της παρούσας διαδικασίας.

Αναλυτικότερα, οι αλλαγές που πρέπει να γίνουν στα αρχεία δραστηριοτήτων επεξεργασίας είναι οι ακόλουθες:

- Τροποποίηση του αντίστοιχου πεδίου ή των αντίστοιχων πεδίων του αρχείου που αφορούν στην υφιστάμενη δραστηριότητα επεξεργασίας όπου εντοπίστηκε η αλλαγή.
- Προσθήκη νέας ροής (γραμμής) στο κατάλληλο αρχείο δραστηριοτήτων, η οποία θα περιγράφει τη νέα πράξη επεξεργασίας που διενεργείται από τη μονάδα επί των δεδομένων προσωπικού χαρακτήρα.
- Αφαίρεση της ροής του αρχείου που αντιστοιχεί στη δραστηριότητα επεξεργασίας δεδομένων προσωπικού χαρακτήρα που έχει καταργηθεί.

Η διαδικασία συνεχίζεται στο **βήμα 3**.

Βήμα 3: Ενημέρωση του ΥΠΔ σχετικά με τις αλλαγές στα αρχεία δραστηριοτήτων επεξεργασίας

Κάθε μονάδα του Πανεπιστημίου, με το πέρας των ανωτέρω ενεργειών στα αρχεία δραστηριοτήτων επεξεργασίας που τηρεί, οφείλει να ενημερώσει τον ΥΠΔ σχετικά με τις αλλαγές που προέκυψαν και ενσωματώθηκαν στα αρχεία της. Επομένως, αποστέλλει στον ΥΠΔ τα εν λόγω αρχεία συνοδευόμενα από σχετική περιγραφή των αλλαγών αυτών.

Η διαδικασία συνεχίζεται στο **βήμα 4**.

Βήμα 4: Έλεγχος εγκυρότητας αλλαγών

Ο ΥΠΔ αξιολογεί τις αλλαγές στα αρχεία δραστηριοτήτων επεξεργασίας που λαμβάνει, επιβεβαιώνοντας την εγκυρότητα και την ορθότητά τους, προκειμένου να διασφαλιστεί ότι η καταγραφή απεικονίζει επακριβώς τις υφιστάμενες δραστηριότητες επεξεργασίας της εκάστοτε μονάδας του Πανεπιστημίου.

Στον παρακάτω πίνακα παρουσιάζονται όσα πρέπει να ελέγξει ο ΥΠΔ στα αρχεία ανάλογα με το είδος της αλλαγής.

Αλλαγή	Έλεγχος αρχείου
Υλοποίηση νέου έργου / νέας δραστηριότητας επεξεργασίας	Εάν έχει προστεθεί νέα ροή (γραμμή) στο κατάλληλο αρχείο δραστηριοτήτων και εάν έχει καταγραφεί επαρκώς όλη η πληροφορία που υπάρχει αναφορικά με αυτήν τη νέα δραστηριότητα επεξεργασίας.
Τροποποίηση υφιστάμενης δραστηριότητας επεξεργασίας	Εάν έχουν καταγραφεί επαρκώς οι αλλαγές της ροής που αφορά στη συγκεκριμένη δραστηριότητα επεξεργασίας και εάν έχουν τροποποιηθεί κατάλληλα τα αντίστοιχα πεδία (κελιά) του αρχείου.
Κατάργηση (ή παύση) υφιστάμενης δραστηριότητας επεξεργασίας	Εάν η ροή που αφορά στην καταργηθείσα δραστηριότητα επεξεργασίας δεδομένων προσωπικού χαρακτήρα έχει αφαιρεθεί από το αρχείο δραστηριοτήτων.

Πίνακας 5: Έλεγχος εγκυρότητας αλλαγών

Σε περίπτωση που εντοπιστεί ότι κάποια αλλαγή δεν έχει καταγραφεί ή δεν έχει ενσωματωθεί σωστά στα αρχεία δραστηριοτήτων της μονάδας, η διαδικασία συνεχίζεται στο **βήμα 2**. Διαφορετικά, δηλαδή σε περίπτωση που όλες οι αλλαγές έχουν καταχωριστεί σωστά στα αρχεία δραστηριοτήτων, η διαδικασία συνεχίζεται στο **βήμα 5**.

Βήμα 5: Ανανέωση των κεντρικών αρχείων δραστηριοτήτων επεξεργασίας

Ο ΥΠΔ επικαιροποιεί τα κεντρικά αρχεία δραστηριοτήτων, τόσο αυτό που αφορά στο Πανεπιστήμιο ως Υπεύθυνο Επεξεργασίας, όσο και αυτό που αφορά στο Πανεπιστήμιο ως Εκτελούντα την Επεξεργασία, με βάση τις αλλαγές που έχουν ενσωματωθεί στα αρχεία δραστηριοτήτων της εκάστοτε μονάδας.

Σκοπός της ενέργειας αυτής είναι τα κεντρικά αρχεία δραστηριοτήτων του Πανεπιστημίου Αιγαίου να αντικατοπτρίζουν με ακρίβεια, ανά πάσα στιγμή, την υφιστάμενη κατάσταση του Πανεπιστημίου, όσον αφορά στις δραστηριότητες επεξεργασίας δεδομένων προσωπικού χαρακτήρα που διενεργούνται από όλες τις μονάδες του.

Η διαδικασία ολοκληρώνεται.

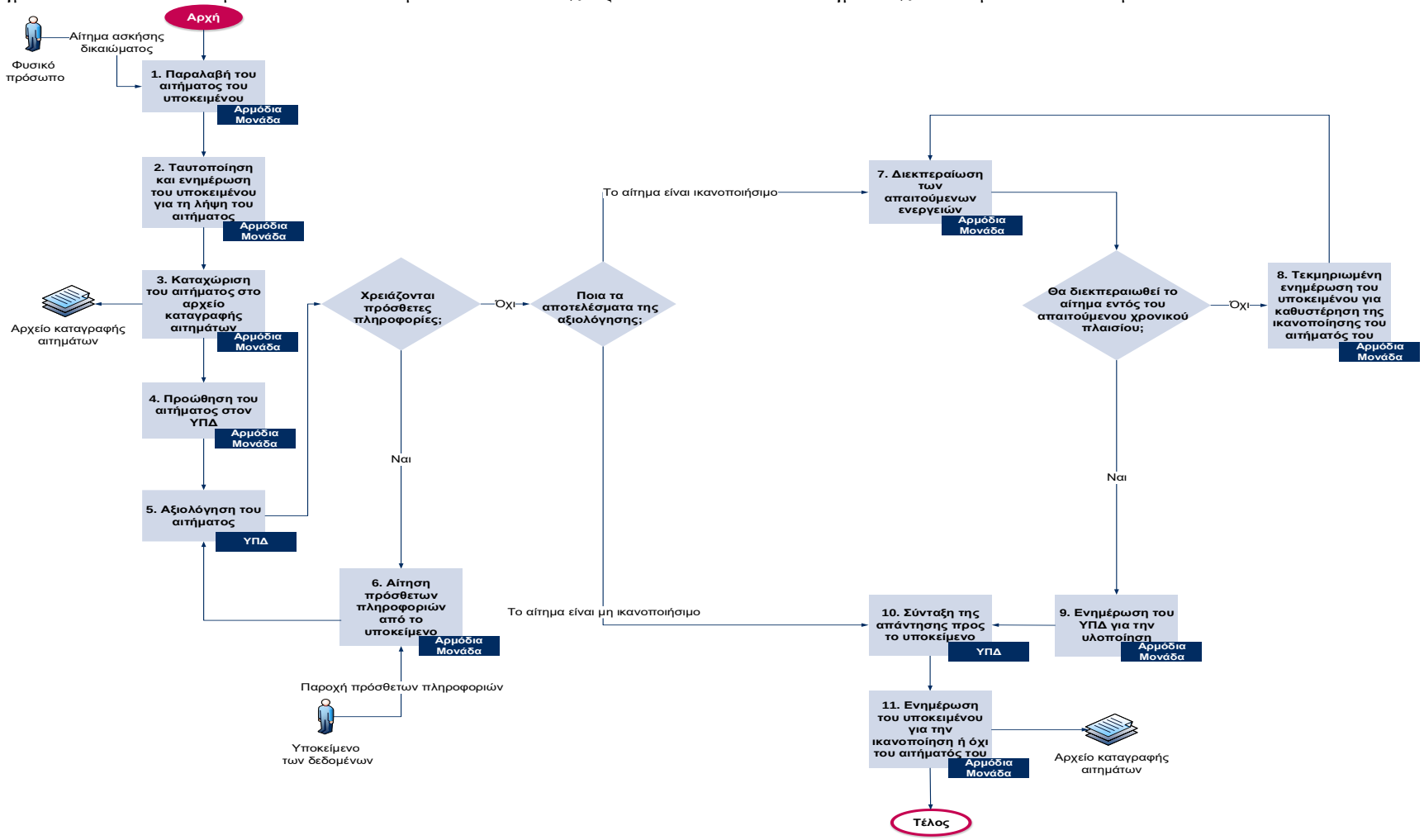
Β.1.2. Διαδικασία Ικανοποίησης δικαιωμάτων Υποκειμένων των Δεδομένων

Σύμφωνα με την ενότητα Α.6 του Α' Μέρους, προκειμένου το Πανεπιστήμιο να μπορεί να διαχειρίζεται αιτήματα των Υποκειμένων των Δεδομένων που αφορούν στην άσκηση των δικαιωμάτων τους, οφείλει να ακολουθήσει μία συγκεκριμένη διαδικασία. Αρχικά, θα πρέπει να ταυτοποιήσει τα στοιχεία των Υποκειμένων των Δεδομένων, στη συνέχεια, να αξιολογήσει τα αιτήματά τους και τέλος, είτε να τα ικανοποιήσει, είτε όχι, ενημερώνοντας παράλληλα τους χρήστες.

Στις παρακάτω ενότητες περιγράφεται η διαδικασία που θα πρέπει να ακολουθηθεί.

B.1.2.1 Σχηματική απεικόνιση της διαδικασίας

Στο παρακάτω Σχήμα φαίνεται η διαδικασία που θα πρέπει να ακολουθηθεί προκειμένου να διεκπεραιωθεί η διαχείριση των αιτημάτων των Υποκειμένων των Δεδομένων που διαχειρίζεται το Πανεπιστήμιο σχετικά με τα δικαιώματά τους.



Σχήμα 3: Σχηματική απεικόνιση της διαδικασίας διαχείρισης αιτημάτων που αφορούν στα δικαιώματα των Υποκειμένων των Δεδομένων

Β.1.2.2 Περιγραφή των βημάτων της διαδικασίας

Σε αυτή την ενότητα περιγράφονται τα βήματα της διαδικασίας διαχείρισης αιτημάτων που αφορούν στα δικαιώματα των Υποκειμένων των Δεδομένων που διαχειρίζεται το Πανεπιστήμιο.

Βήμα 1: Παραλαβή του αιτήματος του Υποκειμένου

Το Υποκείμενο των Δεδομένων καταθέτει, μέσω των διαθέσιμων καναλιών, το αίτημά του σχετικά με τα δεδομένα προσωπικού χαρακτήρα που το αφορούν, προκειμένου να ασκήσει το αντίστοιχο δικαίωμά/δικαιώματά του. Τα κανάλια επικοινωνίας μέσω των οποίων το Υποκείμενο δύναται να αιτηθεί την άσκηση των δικαιωμάτων του στο Πανεπιστήμιο Αιγαίου είναι τα ακόλουθα:

- **Φυσική Παρουσία:** Το Υποκείμενο των Δεδομένων συμπληρώνει στη Γραμματεία Φοιτητών και Φοιτητριών του Τμήματός του αν είναι υφιστάμενος φοιτητής ή φοιτήτρια, υποψήφιος φοιτητής ή φοιτήτρια, ή απόφοιτος του Πανεπιστημίου, είτε στο τμήμα Διοικητικού αν είναι καθηγητής ή καθηγήτρια ή υπάλληλος του Πανεπιστημίου, το τυποποιημένο έντυπο στο Παράρτημα Γ.4 (Έντυπο Άσκησης των Δικαιωμάτων των Υποκειμένων).

- **Ιστοσελίδα εκάστοτε Τμήματος:** Το Υποκείμενο των Δεδομένων, αφού επισκεφτεί την ιστοσελίδα κάποιου Τμήματος του Πανεπιστημίου Αιγαίου, συμπληρώνει την ηλεκτρονική φόρμα για την άσκηση δικαιωμάτων των Υποκειμένων. Προσχέδιο της εν λόγω ηλεκτρονικής φόρμας βρίσκεται στο Παράρτημα Γ.4 (Έντυπο Άσκησης των Δικαιωμάτων των Υποκειμένων) της παρούσας διαδικασίας.

- **Ταχυδρομείο (φυσικό ή ηλεκτρονικό):** Το Υποκείμενο των Δεδομένων μπορεί να ασκήσει κάποιο από τα δικαιώματά του συντάσσοντας ελεύθερο κείμενο και αποστέλλοντάς το στην αρμόδια μονάδα, ήτοι Γραμματεία Φοιτητών και Φοιτητριών, τμήμα Διοικητικού, μέσω ταχυδρομείου ή μέσω ηλεκτρονικού ταχυδρομείου (e-mail).

Επομένως, ο παραλήπτης των εν λόγω αιτημάτων του Υποκειμένου διαφέρει ανάλογα με το κανάλι μέσω του οποίου στάλθηκε το αίτημα στο Πανεπιστήμιο και ανάλογα με την κατηγορία Υποκειμένων (π.χ. φοιτητής ή φοιτήτρια, καθηγητής ή καθηγήτρια, απόφοιτος) στην οποία ανήκει το φυσικό πρόσωπο που άσκησε το αίτημα.

Περαιτέρω, σημειώνεται ότι ένα αίτημα μπορεί να κατατεθεί από τρίτο πρόσωπο για λογαριασμό ενός Υποκειμένου των Δεδομένων με την προσκόμιση κατάλληλης εξουσιοδότησης.

Η διαδικασία συνεχίζεται στο βήμα 2**.**

Βήμα 2: Ταυτοποίηση και ενημέρωση του Υποκειμένου για τη λήψη του αιτήματος

Κατά τη λήψη του αιτήματος, η Μονάδα του Πανεπιστημίου που το παραλαμβάνει οφείλει, εντός εύλογου χρονικού διαστήματος, να προχωρήσει στην ταυτοποίηση του Υποκειμένου των Δεδομένων που έχει καταθέσει το αίτημα, καθώς και στην επικαιροποίηση των παρεχόμενων στοιχείων επικοινωνίας σε περίπτωση που το αίτημα έχει κατατεθεί μέσω του τυποποιημένου εντύπου. Επομένως, η Μονάδα που έχει λάβει το αίτημα είναι υπεύθυνη για τη διεξαγωγή όποιων ελέγχων απαιτούνται για την ταυτοποίηση του Υποκειμένου. Ο παρακάτω πίνακας περιγράφει τις ελάχιστες απαιτούμενες πληροφορίες για την ταυτοποίηση του Υποκειμένου των Δεδομένων:

Κανάλι επικοινωνίας	Στοιχεία ταυτοποίησης
Φυσική παρουσία	Ταυτότητα, ακαδημαϊκή ταυτότητα (πάσο), διαβατήριο, κ.λπ.
Ιστοσελίδα εκάστοτε Τμήματος, με σύνδεση στην ιστοσελίδα	Τακτοποιείται μέσω στοιχείων αυθεντικοποίησης (όνομα χρήστη, URL, κ.λπ.) που χρησιμοποιεί κατά τη σύνδεσή του στην ιστοσελίδα του Τμήματος
Ιστοσελίδα εκάστοτε Τμήματος χωρίς σύνδεση σε αυτή (δηλ. το αίτημα ασκείται από κάποιον τρίτο προς το Πανεπιστήμιο)	Τηλεφωνική επικοινωνία και ταυτοποίηση του Υποκειμένου
Ταχυδρομείο (φυσικό ή ηλεκτρονικό)	Τηλεφωνική επικοινωνία και ταυτοποίηση βάση του Υποκειμένου

Πίνακας 6: Στοιχεία ταυτοποίησης του Υποκειμένου των Δεδομένων

Συγχρόνως, η ίδια Μονάδα του Πανεπιστημίου ενημερώνει το Υποκείμενο ότι το αίτημά του έχει παραληφθεί επιτυχώς και έχει αρχίσει η αξιολόγησή του. Η εν λόγω ενέργεια είναι απαραίτητη για την αποτελεσματική παρακολούθηση του χρονικού πλαισίου που πρέπει να τηρηθεί μέχρι την περάτωση του αιτήματος, καθώς και για την αποφυγή αδικαιολόγητων καθυστερήσεων.

Σημειώνεται ότι από το στιγμή που ταυτοποιηθεί το Υποκείμενο των Δεδομένων, το Πανεπιστήμιο οφείλει να διαχειριστεί το αίτημά του και να του απαντήσει εντός τριάντα (30) ημερών, με δυνατότητα παράτασης επιπλέον εξήντα (60) ημερών. Σε περίπτωση δε, που δεν είναι δυνατόν να επαληθευτεί η ταυτότητα του Υποκειμένου των Δεδομένων από το Πανεπιστήμιο σύμφωνα με τον παραπάνω πίνακα, τότε δύναται να απορριφθεί αίτημα του Υποκειμένου.

Η διαδικασία συνεχίζεται στο **βήμα 3**.

Βήμα 3: Καταχώριση του αιτήματος στο αρχείο καταγραφής αιτημάτων

Στη συνέχεια, η Μονάδα του Πανεπιστημίου που έχει λάβει το αίτημα του Υποκειμένου των Δεδομένων, ήτοι Γραμματεία Φοιτητών και Φοιτητριών του εκάστοτε Τμήματος, τμήμα Διοικητικού, το καταχωρίζει στο «Αρχείο Καταγραφής Αιτημάτων». Το εν λόγω αρχείο έχει καταγεγραμμένα και συγκεντρωμένα όλα τα αιτήματα που έχει λάβει το Πανεπιστήμιο, στο σύνολό τους, σχετικά με δικαιώματα των Υποκειμένων των Δεδομένων.

Για κάθε αίτημα πρέπει να καταχωρίζονται στο αρχείο οι παρακάτω πληροφορίες:

- Στοιχεία ταυτοποίησης του Υποκειμένου των Δεδομένων (π.χ. ταυτότητα, διαβατήριο, άδεια οδήγησης, ακαδημαϊκή ταυτότητα κ.λπ.), εκτός εάν ενεργεί κάποιος τρίτος για λογαριασμό του Υποκειμένου των Δεδομένων.

- Το είδος του δικαιώματος που ασκήθηκε (π.χ. δικαίωμα πρόσβασης, δικαίωμα διόρθωσης, δικαίωμα διαγραφής κ.λπ.).

- Το κανάλι μέσω του οποίου το Πανεπιστήμιο παρέλαβε το αίτημα του Υποκειμένου.

- Σε περίπτωση που το Υποκείμενο των Δεδομένων επιθυμεί να λάβει την απάντηση στο αίτημά του μέσω συγκεκριμένου καναλιού επικοινωνίας, το κανάλι αυτό μέσω του οποίου το Πανεπιστήμιο θα απαντήσει στο αίτημα.

- Χρήσιμες λεπτομέρειες και πληροφορίες σχετικά με το αίτημα του Υποκειμένου των Δεδομένων.

- Σε περίπτωση που το αίτημα του Υποκειμένου έχει αξιολογηθεί ως υπερβολικό ή αβάσιμο, τους λόγους οι οποίοι οδήγησαν σε αυτό το αποτέλεσμα.

- Την ημερομηνία παραλαβής του αιτήματος από την αρμόδια Μονάδα του Πανεπιστημίου.

- Την ημερομηνία που πραγματοποιήθηκε η ταυτοποίηση του Υποκειμένου.

- Την ημερομηνία έκδοσης της απάντησης από το Πανεπιστήμιο.

- Το κανάλι μέσω του οποίου στάλθηκε η απάντηση στο Υποκείμενο των Δεδομένων.

Το «Αρχείο Καταγραφής Αιτημάτων» ενημερώνεται συνεχώς, καθώς οι προαναφερθείσες πληροφορίες συμπληρώνονται καθ' όλη τη διάρκεια της παρούσας διαδικασίας.

Η διαδικασία συνεχίζεται στο **βήμα 4**.

Βήμα 4: Προώθηση του αιτήματος στο Υπεύθυνο Προστασίας Δεδομένων

Όλα τα αιτήματα των υποκειμένων που λαμβάνονται από οποιοδήποτε Τμήμα του Πανεπιστημίου Αιγαίου, ανεξάρτητα από το κανάλι μέσω του οποίου στάλθηκαν σε αυτό και από τη μονάδα του Πανεπιστημίου που το παρέλαβε, πρέπει να αποστέλλονται στον ΥΠΔ. Επομένως, οποιαδήποτε μονάδα του Πανεπιστημίου λαμβάνει αίτημα που αφορά άσκηση δικαιώματος υποκειμένου, οφείλει να το προωθεί στον ΥΠΔ, έτσι ώστε να λάβει χώρα η αξιολόγησή του και να γίνουν οι περαιτέρω απαραίτητες ενέργειες.

Η διαδικασία συνεχίζεται στο **βήμα 5.**

Βήμα 5: Αξιολόγηση του αιτήματος

Σε αυτό το στάδιο της διαδικασίας ο ΥΠΔ, αφού λάβει το αίτημα του Υποκειμένου, είναι υπεύθυνος να το αξιολογήσει ενδελεχώς ώστε να αποφασίσει εάν θα προχωρήσει ή όχι στην ικανοποίησή του. Αφού, αρχικά, αναλύσει, σε συνεργασία με τις αρμόδιες μονάδες, όλες τις διαθέσιμες πληροφορίες,

κρίνει εάν οι εν λόγω πληροφορίες είναι επαρκείς ή εάν χρειάζονται πρόσθετες πληροφορίες από το Υποκείμενο προκειμένου να αξιολογηθεί αποτελεσματικά το αίτημά του.

Σε περίπτωση που οι διαθέσιμες πληροφορίες κριθούν ελλιπείς και χρειάζονται πρόσθετες πληροφορίες από το Υποκείμενο των Δεδομένων, η διαδικασία συνεχίζεται στο **βήμα 6**.

Διαφορετικά, δηλαδή σε περίπτωση που οι πληροφορίες που έχει στην κατοχή του ο ΥΠΔ είναι επαρκείς, τότε είναι σε θέση να προχωρήσει στην περαιτέρω αξιολόγηση του αιτήματος του υποκειμένου σχετικά με το δικαίωμα / τα δικαιώματά του.

Για την περαιτέρω αξιολόγηση του αιτήματος, ο ΥΠΔ οφείλει, μεταξύ άλλων, να αναζητήσει τις απαραίτητες πληροφορίες μέσω των πληροφοριακών συστημάτων που έχει στη διάθεσή του και να επικοινωνήσει με τις μονάδες του Πανεπιστημίου οι οποίες ενδέχεται να σχετίζονται με το αίτημα του Υποκειμένου των Δεδομένων.

Επιπλέον, το Αρχείο των Δραστηριοτήτων Επεξεργασίας, στο οποίο βρίσκονται καταγεγραμμένες όλες οι πράξεις επεξεργασίας δεδομένων προσωπικού χαρακτήρα για τις οποίες είναι υπεύθυνο το Πανεπιστήμιο, δύναται να χρησιμοποιηθεί ως σημείο αναφοράς για την αξιολόγηση, καθώς προσφέρει στον ΥΠΔ σημαντικές πληροφορίες όπως:

- Τον σκοπό της επεξεργασίας
- Τους αποδέκτες των εν λόγω δεδομένων εντός και εκτός του Πανεπιστημίου.
- Τη νομική βάση της επεξεργασίας (για περισσότερες πληροφορίες: Πίνακας 8: Νομική βάση και Άσκηση δικαιωμάτων των Υποκειμένων των Δεδομένων).
- Τα πληροφοριακά συστήματα που εμπλέκονται στην επεξεργασία των εν λόγω δεδομένων.

Έχοντας διαθέσιμες όλες αυτές τις πληροφορίες ο ΥΠΔ μπορεί να αξιολογήσει αποτελεσματικά το αίτημα του Υποκειμένου σχετικά με τα δικαιώματά του και να το χαρακτηρίσει ως «Ικανοποιήσιμο» ή «Μη ικανοποιήσιμο». Ο Νομικός Σύμβουλος του Πανεπιστημίου δύναται να συνδράμει και να υποστηρίζει τον ΥΠΔ κατά τη διάρκεια της εν λόγω αξιολόγησης.

Στον ακόλουθο πίνακα παρουσιάζεται ενδεικτικός οδηγός αναφορικά με την αξιολόγηση των αιτημάτων:

ΠΙΝΑΚΑΣ ΑΞΙΟΛΟΓΗΣΗΣ ΑΙΤΗΜΑΤΩΝ		
Αίτημα	**Περιγραφή**	**Παραδείγματα αιτημάτων**
Ικανοποιήσιμο	Αίτημα το οποίο δύναται να υλοποιηθεί εντός του προβλεπόμενου χρονικού πλαισίου (30 μέρες).	• Διόρθωση δεδομένων • Πρόσβαση στα δεδομένα • Περιορισμός επεξεργασίας των δεδομένων
Ικανοποιήσιμο κατόπιν χρέωσης	Αίτημα το οποίο είναι υπερβολικό (π.χ. λόγω του επαναλαμβανόμενου χαρακτήρα του).	• Πολλαπλά αντίγραφα δεδομένων (Χ φορές σε διάστημα Υ μηνών)
Μη ικανοποιήσιμο	Προδήλως αβάσιμο αίτημα ή αίτημα το οποίο είναι υπερβολικό (π.χ. λόγω του επαναλαμβανόμενου χαρακτήρα του).	• Το Υποκείμενο έχει αιτηθεί πρόσβαση στα δεδομένα του, το οποίο όμως θα έχει ως αποτέλεσμα την αποκάλυψη προσωπικών δεδομένων τρίτου φυσικού προσώπου. • Το Υποκείμενο έχει ασκήσει το δικαίωμα στη φορητότητα των δεδομένων του, όμως προηγουμένως έχει αιτηθεί τη διαγραφή των εν λόγω δεδομένων. • Βλ. Πίνακας 8: Νομική βάση και Άσκηση δικαιωμάτων των Υποκειμένων των Δεδομένων

Πίνακας 7: Πίνακας αξιολόγησης αιτημάτων των Υποκειμένων των Δεδομένων

Ο παρακάτω πίνακας παρουσιάζει την ικανότητα άσκησης των δικαιωμάτων των υποκειμένων, η οποία προκύπτει σε σχέση με τη νομική βάση επεξεργασίας. Τα αιτήματα, τα οποία δεν είναι δυνατόν να ικανοποιηθούν για το λόγο αυτό, θεωρούνται προδήλως αβάσιμα.

ΝΟΜΙΚΗ ΒΑΣΗ	ΔΙΚΑΙΩΜΑ ΣΤΗΝ ΠΡΟΣΒΑΣΗ	ΔΙΚΑΙΩΜΑ ΣΤΗ ΔΙΟΡΘΩΣΗ	ΔΙΚΑΙΩΜΑ ΣΤΗ ΔΙΑΓΡΑΦΗ	ΔΙΚΑΙΩΜΑ ΠΕΡΙΟΡΙΣΜΟΥ	ΔΙΚΑΙΩΜΑ ΣΤΗ ΦΟΡΗΤΟΤΗΤΑ	ΔΙΚΑΙΩΜΑ ΕΝΑΝΤΙΩΣΗΣ	ΔΙΚΑΙΩΜΑ ΕΝΑΝΤΙΩΣΗΣ (ΑΠΕΥΘΕΙΑΣ ΕΜΠΟΡΙΚΗ ΠΡΟΩΘΗΣΗ)
Συναίνεση	✓	✓	✓	✓	✓	✗	✓ (ανάκληση συγκαταθέσεως)
Εκτέλεση Σύμβασης	✓	✓	✓	✓	✓	✗	✓
Έννομη Υποχρέωση	✓	✓	✗	✓	✗	✗	✓
Έννομο συμφέρον	✓	✓	✓	✓	✗	✓	✓
Ζωτικό συμφέρον	✓	✓	✗	✓	✗	✗	✓
Δημόσιο συμφέρον	✓	✓	✓	✓	✗	✓	✓

Πίνακας 8: Νομική βάση και Άσκηση δικαιωμάτων των Υποκειμένων των Δεδομένων

Σημειώνεται ότι το έννομο συμφέρον δεν ισχύει ως νομική βάση για επεξεργασίες που διενεργεί το Πανεπιστήμιο Αιγαίου, καθώς ως ανώτατο εκπαιδευτικό ίδρυμα αποτελεί δημόσια αρχή.

Σε περίπτωση που το αίτημα αξιολογηθεί ως «Ικανοποιήσιμο κατόπιν σχετικής χρεώσεως», η διαδικασία συνεχίζεται στο **Βήμα 7** της παρούσας διαδικασίας. Εάν το αίτημα του Υποκειμένου των Δεδομένων αξιολογηθεί ως «Ικανοποιήσιμο» η διαδικασία συνεχίζεται στο **Βήμα 8**. Σε περίπτωση που το αίτημα αξιολογηθεί ως «Μη ικανοποιήσιμο» η διαδικασία συνεχίζεται στο **Βήμα 11** της διαδικασίας.

Ωστόσο, σε κάθε περίπτωση, ο ΥΠΔ ενημερώνει τις αρμόδιες μονάδες του Πανεπιστημίου, ήτοι Γραμματεία Φοιτητών και Φοιτητριών εκάστοτε Τμήματος, τμήμα Διοικητικού, ώστε αυτές με τη σειρά τους να προβούν στις απαραίτητες ενέργειες ή / και ενημερώσεις με βάση τη διαδικασία.

Βήμα 6: Αίτηση πρόσθετων πληροφοριών από το Υποκείμενο των Δεδομένων

Σε περίπτωση που κατά την αξιολόγηση του αιτήματος κριθούν ελλιπείς οι διαθέσιμες πληροφορίες, τότε η αρμόδια μονάδα του Πανεπιστημίου αιτείται πρόσθετες πληροφορίες από το Υποκείμενο των Δεδομένων προκειμένου να αξιολογηθεί αποτελεσματικά το αίτημα σχετικά με την άσκηση των δικαιωμάτων του. Αφού το Υποκείμενο των Δεδομένων παράσχει τις απαραίτητες πληροφορίες η διαδικασία συνεχίζεται στο **βήμα 5.**

Βήμα 7: Ενημέρωση του Υποκειμένου για την εν λόγω χρέωση

Το αρμόδιο Τμήμα του Πανεπιστημίου ενημερώνει το Υποκείμενο ότι το αίτημά του θα διεκπεραιωθεί μόνο αν καταβάλει εύλογο ποσό που αντιστοιχεί στην πολυπλοκότητα του

αιτήματος. Σε περίπτωση που το Υποκείμενο των Δεδομένων αποδεχτεί τη χρέωση, η διαδικασία συνεχίζεται στο **Βήμα 8**. Διαφορετικά, η διαδικασία συνεχίζεται στο **Βήμα 11.**

Βήμα 8: Διεκπεραίωση των απαιτούμενων ενεργειών

Το Πανεπιστήμιο οφείλει να είναι σε θέση να ικανοποιήσει τα δικαιώματα των Υποκειμένων των Δεδομένων. Ανάλογα με τον τρόπο με τον οποίο θα ορίσει το Πανεπιστήμιο, ο ΥΠΔ θα είναι σε θέση να επικοινωνήσει με το Υποκείμενο των Δεδομένων μέσω εντύπων ή ηλεκτρονικών μέσων.

Το Πανεπιστήμιο οφείλει να αναρτήσει το έντυπο Παράρτημα Γ.4 (Έντυπο Άσκησης των Δικαιωμάτων των Υποκειμένων) σε ευκρινές σημείο, τόσο σε έντυπη μορφή στις εγκαταστάσεις του, όσο και σε ηλεκτρονική μορφή στον ιστότοπό του.

Για την ικανοποίηση του δικαιώματος της ενημέρωσης το Πανεπιστήμιο μπορεί να χρησιμοποιήσει τα πρότυπα Παράρτημα Γ.5 (α) Έντυπο Άσκησης του δικαιώματος της ενημέρωσης εφόσον τα δεδομένα των φυσικών προσώπων έχουν συλλεγεί από το Υποκείμενο των Δεδομένων και Παράρτημα Γ.5 (β) Έντυπο Άσκησης του δικαιώματος της ενημέρωσης εφόσον τα δεδομένα των φυσικών προσώπων δεν έχουν συλλεγεί από το Υποκείμενο των Δεδομένων.

Για την ικανοποίηση του δικαιώματος της πρόσβασης, το Πανεπιστήμιο μπορεί να χρησιμοποιήσει το πρότυπο Παράρτημα Γ.6. (Έντυπο Άσκησης του δικαιώματος της πρόσβασης).

Για την ικανοποίηση των δικαιωμάτων της διόρθωσης, της διαγραφής, της εναντίωσης, του περιορισμού της επεξεργασίας, της φορητότητας των δεδομένων, το Πανεπιστήμιο, σε συνεργασία με τον ΥΠΔ, οφείλει να αναπτύξει τεχνικούς μηχανισμούς υποστήριξης των εν λόγω αιτημάτων.

Εφόσον το Πανεπιστήμιο παραλάβει ένα αίτημα άσκησης δικαιώματος, μπορεί να χρησιμοποιήσει το Παράρτημα Γ.7 (Διαχείριση Αιτήματος) και κατόπιν να το καταχωρίσει στο Αρχείο Καταγραφής Αιτημάτων.

Το Πανεπιστήμιο μπορεί να επικοινωνεί τις απαντήσεις στα αιτήματα των Υποκειμένων των Δεδομένων με επιστολή είτε σε έντυπη μορφή, είτε σε ηλεκτρονική, είτε μέσω τηλεφώνου, είτε μέσω τηλεομοιότυπου, εφόσον έχει γίνει ταυτοποίηση του φυσικού προσώπου.

Οι ενέργειες που περιγράφονται παραπάνω, λαμβάνουν χώρα υπό τη συνεχή επίβλεψη του ΥΠΔ, έτσι ώστε να αναγνωρίζονται χωρίς καθυστέρηση περιπτώσεις πολύπλοκων υλοποιήσεων, οι οποίες μπορούν να οδηγήσουν σε καθυστέρηση του αιτήματος. Σε περίπτωση που οι ενέργειες μίας Μονάδας δύνανται να επιφέρουν καθυστερήσεις, η διαδικασία συνεχίζεται στο **βήμα 8**. Διαφορετικά, δηλαδή σε περίπτωση που οι απαραίτητες ενέργειες για την ικανοποίηση του αιτήματος του Υποκειμένου διεκπεραιωθούν εντός του απαιτούμενου χρονικού πλαισίου, η διαδικασία συνεχίζεται στο **βήμα 9.**

Βήμα 9: Τεκμηριωμένη ενημέρωση του Υποκειμένου για καθυστέρηση της ικανοποίησης του αιτήματός του

Η αρμόδια Μονάδα, ήτοι Γραμματεία Φοιτητών και Φοιτητριών του εκάστοτε Τμήματος του Πανεπιστημίου ή τμήμα Διοικητικού, είναι υπεύθυνη να ενημερώσει το Υποκείμενο των

Δεδομένων, σε περίπτωση που το αίτημά του δεν δύναται να ικανοποιηθεί από το Πανεπιστήμιο εντός του ορισμένου, από τον ΓΚΠΔ, χρονικού πλαισίου των τριάντα (30) ημερών. Η εν λόγω ενημέρωση πρέπει να περιέχει τεκμηριωμένους τους λόγους για τους οποίους καθυστέρησε η ικανοποίηση του αιτήματος του Υποκειμένου των Δεδομένων.

Σημειώνεται ότι η ενημέρωση του Υποκειμένου για καθυστέρηση της ικανοποίησης του αιτήματός του μπορεί, εάν είναι απαραίτητο, να αποσταλεί αργότερα κατά τη διάρκεια αυτής της διαδικασίας. Η διαδικασία συνεχίζεται στο **βήμα 10**.

Βήμα 10: Ενημέρωση του Υπεύθυνου Προστασίας Δεδομένων για την υλοποίηση

Μόλις η αρμόδια Μονάδα ή αρμόδιες Μονάδες ολοκληρώσουν όλες τις απαιτούμενες ενέργειες για την ικανοποίηση του αιτήματος του υποκειμένου, οφείλουν να ενημερώσουν τον ΥΠΔ ότι υλοποιήθηκε το αίτημα και ότι δεν απαιτούνται άλλες ενέργειες από τη μεριά τους.

Η διαδικασία συνεχίζεται στο **βήμα 12**.

Βήμα 11: Σύνταξη της απάντησης προς το Υποκείμενο

Ο ΥΠΔ οφείλει να αναλύσει όλες τις διαθέσιμες πληροφορίες, είτε αυτές έχουν ως πηγή το Υποκείμενο των Δεδομένων είτε έχουν προέλθει από τις διεκπεραιωτικές ενέργειες των λοιπών συναρμόδιων τμημάτων του Πανεπιστημίου, καθώς και να συντάξει την απάντηση προς το Υποκείμενο των Δεδομένων. Οι εν λόγω ενέργειες διενεργούνται τόσο σε περίπτωση ικανοποιήσεως όσο και σε περίπτωση μη ικανοποιήσεως του αιτήματός του. Σε κάθε περίπτωση, η απάντηση που θα δοθεί στο Υποκείμενο των Δεδομένων σχετικά με την ικανοποίηση ή μη του αιτήματός του πρέπει να είναι τεκμηριωμένη.

Η διαδικασία συνεχίζεται στο **Βήμα 12**.

Βήμα 12: Ενημέρωση του Υποκειμένου για την ικανοποίηση ή όχι του αιτήματός του

Η Γραμματεία Φοιτητών και Φοιτητριών εκάστου Τμήματος του Πανεπιστημίου Αιγαίου αν ο αιτών / η αιτούσα είναι φοιτητής ή φοιτήτρια, υποψήφιος φοιτητής ή φοιτήτρια, ή απόφοιτος του Τμήματος, είτε το τμήμα Διοικητικού αν ο αιτών / η αιτούσα είναι καθηγητής ή καθηγήτρια ή υπάλληλος του Πανεπιστημίου, πρέπει να ενημερώσει το Υποκείμενο των Δεδομένων κατάλληλα για την ικανοποίηση ή μη του αιτήματός του.

Επομένως, η απάντηση στο Υποκείμενο των Δεδομένων επικοινωνείται από την αρμόδια Μονάδα στο Υποκείμενο των Δεδομένων μέσω του καναλιού επικοινωνίας που έχει επιλέξει. Ενδεικτικά:

- Με επιστολή στη δηλωμένη ταχυδρομική διεύθυνση του Υποκειμένου των Δεδομένων.
- Ηλεκτρονικά, είτε σε περίπτωση που το έχει ζητήσει το Υποκείμενο των Δεδομένων είτε σε περίπτωση που το αίτημα έχει υποβληθεί με ηλεκτρονικά μέσα.
- Προφορικά, σε περίπτωση που το έχει ζητήσει το Υποκείμενο των Δεδομένων.

Ενημερώνει το αρχείο καταγραφής αιτημάτων ώστε το αίτημα να είναι καταχωρισμένο με την κατάλληλη σήμανση και να φαίνεται ότι έχει ολοκληρωθεί (π.χ. ολοκληρωμένο). Σημειώνεται ότι το εν λόγω αρχείο αποδεικνύει ότι το αίτημα του Υποκειμένου έχει ληφθεί εγκαίρως υπόψη και έχουν διενεργηθεί επ' αυτού οι απαιτούμενες ενέργειες, καθώς και ότι το Πανεπιστήμιο Αιγαίου συμμορφώνεται με τις σχετικές απαιτήσεις του ΓΚΠΔ.

Η διαδικασία ολοκληρώνεται.

Β.1.3. Διαδικασία για Διεθνείς διαβιβάσεις δεδομένων προσωπικού χαρακτήρα

Σύμφωνα με την ενότητα Α.7 του Α' Μέρους, προκειμένου το Πανεπιστήμιο να μπορεί να μεταβιβάσει τα δεδομένα σε άλλους φορείς σε τρίτες χώρες ή σε διεθνείς οργανισμούς οι οποίοι είναι συμμορφωμένοι με τον ΓΚΠΔ, οφείλει να ακολουθήσει μία συγκεκριμένη διαδικασία.

Βασικός στόχος του νέου ΓΚΠΔ αποτελεί η ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα εντός του Ευρωπαϊκού Οικονομικού Χώρου, χωρίς περιορισμούς και απαγορεύσεις. Επιπλέον, ο ΓΚΠΔ θεσπίζει αυστηρούς κανόνες που αφορούν στη διαβίβαση δεδομένων προσωπικού χαρακτήρα εκτός των συνόρων του εν λόγου Χώρου.

Ειδικότερα, ο Ευρωπαϊκός Οικονομικός Χώρος (εφεξής «ΕΟΧ») περιλαμβάνει όλες τις χώρες μέλη της Ευρωπαϊκής Ένωσης, καθώς και τις μη ενταγμένες στην Ευρωπαϊκή Ένωση χώρες Ισλανδία, Λιχτενστάιν, Νορβηγία. Μέχρι στιγμής, οι χώρες που ανήκουν στον ΕΟΧ είναι αυτές που παρουσιάζονται στον παρακάτω Πίνακα.

Χώρες Ευρωπαϊκού Οικονομικού Χώρου			
Αυστρία	Βέλγιο	Βουλγαρία	Γαλλία
Γερμανία	Δανία	Δημοκρατία της Τσεχίας	Ελλάδα
Εσθονία	Ηνωμένο Βασίλειο	Ιρλανδία	Ισλανδία
Ισπανία	Ιταλία	Κροατία	Κύπρος
Λετονία	Λιθουανία	Λιχτενστάιν	Λουξεμβούργο
Μάλτα	Νορβηγία	Ολλανδία	Ουγγαρία
Πολωνία	Πορτογαλία	Ρουμανία	Σλοβακία
Σλοβενία	Σουηδία	Φινλανδία	

Πίνακας 9: Χώρες Ευρωπαϊκού Οικονομικού Χώρου (ΕΟΧ)

Όλες οι υπόλοιπες χώρες, οι οποίες δεν ανήκουν στην παραπάνω λίστα, ονομάζονται «τρίτες χώρες». Βάσει του ΓΚΠΔ οι διαβιβάσεις δεδομένων προσωπικού χαρακτήρα προς τρίτες χώρες ή διεθνείς οργανισμούς υπόκεινται σε αυστηρούς κανόνες και προϋποθέσεις, καθώς πρέπει, κάθε φορά, να διασφαλίζεται ότι δεν υπονομεύεται το επίπεδο προστασίας που εγγυάται ο ΓΚΠΔ για τα δεδομένα, τις ελευθερίες και τα δικαιώματα των φυσικών προσώπων.

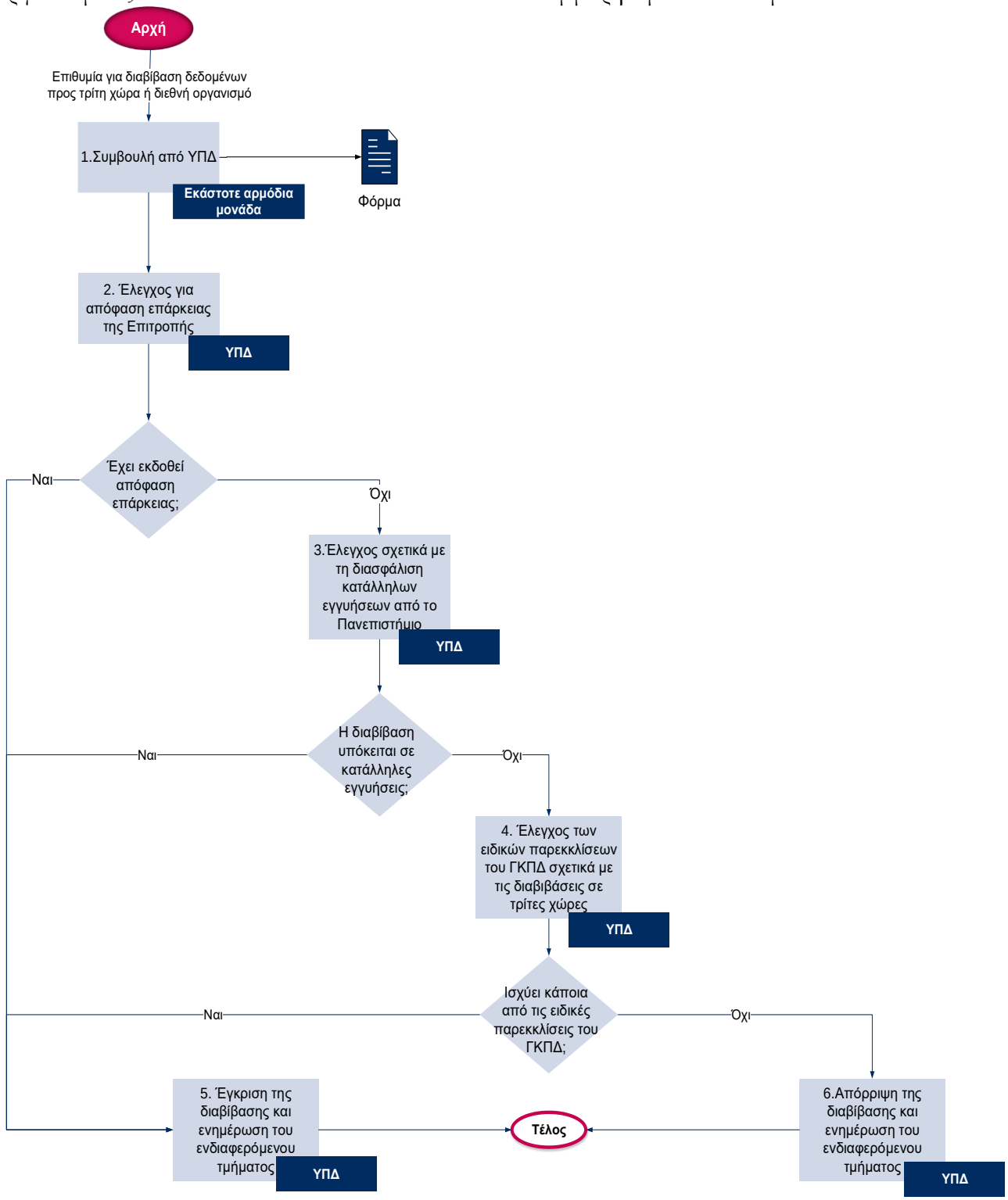
Για να είναι νόμιμη μία τέτοια διαβίβαση, πρέπει να πληρούνται τόσο οι γενικές διατάξεις του ΓΚΠΔ, όπως οι βασικές αρχές που διέπουν την επεξεργασία των δεδομένων, η νομιμότητα της επεξεργασίας, τα ειδικώς ορισμένα για τις ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα, όσο και οι ειδικές προϋποθέσεις και μηχανισμοί που θεσπίζονται στον Κανονισμό, αναφορικά με τις διεθνείς διαβιβάσεις.

Ο ΓΚΠΔ θεμελιώνει σαφή ιεραρχία μεταξύ των εν λόγω μηχανισμών διαβίβασης: Ο ιδανικός μηχανισμός διαβίβασης είναι η απόφαση επάρκειας από την Ευρωπαϊκή Επιτροπή. Εάν η απόφαση επάρκειας δεν είναι διαθέσιμη, τότε η δεύτερη επιλογή μηχανισμού είναι συγκεκριμένες διασφαλίσεις για τα δεδομένα που διαβιβάζονται στις τρίτες χώρες, οι οποίες έχουν εγκριθεί από την Επιτροπή ή από τις εθνικές αρχές προστασίας δεδομένων. Εάν τέτοιες διασφαλίσεις δεν είναι διαθέσιμες, τότε έσχατη λύση του ΓΚΠΔ αποτελεί ένας απαριθμούμενος κατάλογος παρεκκλίσεων που επιτρέπουν περιορισμένες διαβιβάσεις δεδομένων σε τρίτες χώρες.

Η παρούσα διαδικασία εκκινεί κάθε φορά που κάποιο Τμήμα του Πανεπιστημίου επιθυμεί να διαβιβάσει δεδομένα προσωπικού χαρακτήρα προς τρίτες χώρες ή διεθνείς οργανισμούς. Στόχος αυτής είναι να περιγραφούν αναλυτικά οι ενέργειες που πρέπει να γίνονται από το Πανεπιστήμιο Αιγαίου προκειμένου να διασφαλίσει ότι εκάστη διεθνής διαβίβαση δεδομένων προσωπικού χαρακτήρα γίνεται βάσει των ειδικών προϋποθέσεων του ΓΚΠΔ.

Β.1.3.1 Σχηματική απεικόνιση της διαδικασίας

Στο παρακάτω Σχήμα φαίνεται η διαδικασία που θα πρέπει να ακολουθηθεί προκειμένου το Πανεπιστήμιο να μπορεί να μεταβιβάσει δεδομένα σε άλλους φορείς σε τρίτες χώρες ή σε διεθνείς οργανισμούς οι οποίοι είναι συμμορφωμένοι με τον ΓΚΠΔ.



Σχήμα 4: Σχηματική απεικόνιση της διαδικασίας μεταβίβασης δεδομένων σε άλλους φορείς σε τρίτες χώρες ή σε διεθνείς οργανισμούς οι οποίοι είναι συμμορφωμένοι με τον ΓΚΠΔ

Β.1.3.2 Περιγραφή των βημάτων της διαδικασίας

Σε αυτή την ενότητα περιγράφονται τα βήματα της διαδικασίας μεταβίβασης δεδομένων σε άλλους φορείς σε τρίτες χώρες ή σε διεθνείς οργανισμούς οι οποίοι είναι συμμορφωμένοι με τον ΓΚΠΔ.

Βήμα 1: Συμβουλή από τον Υπεύθυνο Προστασίας Δεδομένων σχετικά με τη διαβίβαση

Κάθε φορά που κάποιο Τμήμα του Πανεπιστημίου Αιγαίου επιθυμεί να διαβιβάσει δεδομένα προσωπικού χαρακτήρα προς τρίτη χώρα ή διεθνή οργανισμό, πρέπει πρώτα να ζητά τη γνώμη και τη συμβουλή του ΥΠΔ. Η εν λόγω ενέργεια είναι απολύτως απαραίτητη, καθώς πριν την όποια διαβίβαση σε τρίτη χώρα πρέπει να διερευνηθεί και να εξασφαλιστεί ότι η χώρα αυτή δεν υπονομεύει το αποδεκτό επίπεδο προστασίας για τα φυσικά πρόσωπα.

Επομένως, το εκάστοτε Τμήμα του Πανεπιστημίου επικοινωνεί με τον ΥΠΔ, παρέχοντάς του όλες τις απαραίτητες πληροφορίες σχετικά με τη διεθνή διαβίβαση, προκειμένου στη συνέχεια να λάβει την έγκριση, ή μη, της εν λόγω διαβίβασης δεδομένων.

Η διαδικασία συνεχίζεται στο **βήμα 2**.

Βήμα 2: Έλεγχος για απόφαση επάρκειας από την Επιτροπή

Αρχικά, ο ΥΠΔ ελέγχει τον κατάλογο που έχει δημοσιοποιηθεί από την Επιτροπή με τις τρίτες χώρες για τις οποίες έχει εκδοθεί απόφαση επάρκειας, προκειμένου να διαπιστώσει εάν υπάρχει απόφαση επάρκειας για τη χώρα – παραλήπτη των δεδομένων. Ο εν λόγω κατάλογος είναι δημοσιοποιημένος στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης και στον ιστότοπο της Ευρωπαϊκής Επιτροπής και αφορά όχι μόνο αποφάσεις επάρκειας για διαβιβάσεις σε τρίτες χώρες, αλλά και σε έδαφος ή συγκεκριμένο τομέα εντός της τρίτης χώρας ή σε έναν διεθνή οργανισμό.

Μέχρι στιγμής, οι χώρες για τις οποίες έχει εκδώσει η Επιτροπή απόφαση επάρκειας είναι η Ανδόρα, η Αργεντινή, ο Καναδάς, οι νήσοι Φερόες, το Γκέρνσεϊ, το Ισραήλ, η νήσος του Μαν, το Τζέρσεϊ, η Νέα Ζηλανδία, η Ελβετία, η Ουρουγουάη και οι ΗΠΑ (μόνο στο πλαίσιο της «Ασπίδας Προστασίας Privacy Shield)»), ενώ έχει αρχίσει η διαδικασία έγκρισης της απόφασης επάρκειας για την Ιαπωνία και γίνονται συζητήσεις για τη Νότιο Κορέα.

Όσον αφορά στη διαβίβαση δεδομένων προσωπικού χαρακτήρα στις ΗΠΑ, η απόφαση επάρκειας αφορά μόνο το μηχανισμό της «Ασπίδας Προστασίας». Επομένως, όταν ο παραλήπτης των δεδομένων είναι στις ΗΠΑ πρέπει να γίνεται και δεύτερος έλεγχος ώστε να διαπιστωθεί κατά πόσο η οντότητα που πρόκειται να λάβει τα δεδομένα ανήκει στη λίστα με τις πιστοποιημένες κατά Privacy Shield οντότητες (https://www.privacyshield.gov/list).

Σε περίπτωση που έχει εκδοθεί από την Επιτροπή απόφαση επάρκειας για την τρίτη χώρα ή για το έδαφος ή συγκεκριμένο τομέα εντός της τρίτης χώρας ή για τον διεθνή οργανισμό, η διαδικασία συνεχίζεται στο **βήμα 5**. Διαφορετικά, δηλαδή σε περίπτωση που δεν έχει εκδοθεί απόφαση επάρκειας για τη χώρα – παραλήπτη των δεδομένων, η διαδικασία συνεχίζεται στο **βήμα 3**.

Βήμα 3: Έλεγχος σχετικά με τη διασφάλιση κατάλληλων εγγυήσεων από το Πανεπιστήμιο

Ελλείψει απόφασης επάρκειας της Επιτροπής, το Πανεπιστήμιο όταν επιθυμεί να διαβιβάσει δεδομένα προσωπικού χαρακτήρα πρέπει να λαμβάνει τα απαραίτητα μέτρα προστασίας, προκειμένου να μην υπονομευθεί το επίπεδο προστασίας που εγγυάται ο ΓΚΠΔ για τα φυσικά πρόσωπα από την ελλιπή προστασία δεδομένων στην τρίτη χώρα.

Επομένως, ο ΥΠΔ, σε συνεργασία με τον Νομικό Σύμβουλο του Πανεπιστημίου και το ενδιαφερόμενο Τμήμα, ελέγχει κατά πόσο το Πανεπιστήμιο παρέχει κάποια από τις παρακάτω κατάλληλες εγγυήσεις υπέρ των Υποκειμένων των Δεδομένων.

Πιο συγκεκριμένα, οι εν λόγω κατάλληλες εγγυήσεις παρέχονται μέσω:

- **Νομικά δεσμευτικού και εκτελεστού μέσου μεταξύ δημόσιων αρχών ή φορέων**, δηλαδή οι διαβιβάσεις δεδομένων μεταξύ δημόσιων αρχών (δημόσια αρχή αποτελεί και το Πανεπιστήμιο), δύνανται να πραγματοποιηθούν στο πλαίσιο νομικά δεσμευτικής συμφωνίας μεταξύ τους χωρίς να απαιτείται η έκδοση άδειας από την εποπτική αρχή.

- **Διοικητικών, μη δεσμευτικών, ρυθμίσεων μεταξύ δημοσίων αρχών ή φορέων**, οι οποίες περιλαμβάνουν εκτελεστά και ουσιαστικά δικαιώματα των Υποκειμένων (π.χ. Μνημόνιο Συνεργασίας). Σε αυτή την περίπτωση η **άδεια της εποπτικής αρχής** είναι απαραίτητη, οι ρυθμίσεις αυτού του τύπου είναι νομικά μη δεσμευτικές.

- Εγκεκριμένων από την αρμόδια εποπτική αρχή **δεσμευτικών εταιρικών κανόνων (Binding Corporate Rules – BCRs)**. Ως δεσμευτικοί εταιρικοί κανόνες νοούνται στον ΓΚΠΔ «οι πολιτικές προστασίας δεδομένων προσωπικού χαρακτήρα τις οποίες ακολουθεί ένας Υπεύθυνος Επεξεργασίας ή Εκτελών την Επεξεργασία εγκατεστημένος στο έδαφος κράτους μέλους για διαβιβάσεις ή δέσμη διαβιβάσεων δεδομένων προσωπικού χαρακτήρα σε Υπεύθυνο Επεξεργασίας ή Εκτελούντα την Επεξεργασία σε μία ή περισσότερες τρίτες χώρες εντός ομίλου επιχειρήσεων, ή ομίλου εταιρειών που ασκεί κοινή οικονομική δραστηριότητα».

- Υιοθέτησης **τυποποιημένων συμβατικών ρητρών προστασίας δεδομένων** που έχουν εκδοθεί από την Ευρωπαϊκή Επιτροπή ή έχουν εκδοθεί από την Εθνική Εποπτική Αρχή ΑΠΔΠΧ και εγκριθεί από την Επιτροπή.

- Σύνταξης **συμβατικών ρητρών** μεταξύ του Πανεπιστημίου Αιγαίου και του Υπευθύνου Επεξεργασίας, του Εκτελούντος την Επεξεργασία ή του αποδέκτη των δεδομένων προσωπικού χαρακτήρα στην τρίτη χώρα ή τον διεθνή οργανισμό και υποβολή αυτών **στην αρμόδια εποπτική αρχή προς έγκριση**.

- **Εγκεκριμένων**, από την αρμόδια εποπτική αρχή, **κωδίκων δεοντολογίας**, οι οποίοι θα πρέπει να προσομοιάζουν σε προγράμματα αυτορρύθμισης τα οποία χρησιμοποιούνται για να αποδεικνύουν στις αρχές και στα Υποκείμενα των Δεδομένων ότι το Πανεπιστήμιο τηρεί ορισμένους κανόνες προστασίας των δεδομένων.

  Για να θεωρηθούν οι εν λόγω κώδικες ως επαρκείς και κατάλληλες εγγυήσεις που επιτρέπουν διεθνείς διαβιβάσεις στο πλαίσιο του ΓΚΠΔ, πρέπει να συνοδεύονται από μηχανισμό με τον οποίο καθίστανται νομικά δεσμευτικοί για τους τρίτους που πρόκειται να λάβουν τα δεδομένα (π.χ. σύμβαση μεταξύ του Πανεπιστημίου Αιγαίου και του παραλήπτη

των δεδομένων, όπου ο δεύτερος συμφωνεί να εφαρμόσει τον εγκεκριμένο κώδικα δεοντολογίας).

- **Εγκεκριμένου μηχανισμού πιστοποίησης**, μέσω της οποίας ο παραλήπτης στην τρίτη χώρα διαβεβαιώνει ότι προσφέρει κατάλληλη προστασία στα δεδομένα προσωπικού χαρακτήρα που προέρχονται από χώρα εντός ΕΟΧ. Η εν λόγω πιστοποίηση πρέπει να συνοδεύεται με μία νομική δέσμευση να εφαρμόζει τα πρότυπα πιστοποίησης, μεταξύ άλλων όσον αφορά στα δικαιώματα των υποκειμένων των δεδομένων.

  Σημειώνεται ότι οι πιστοποιήσεις ισχύουν για μέγιστο χρονικό διάστημα τριών ετών από την έκδοσή τους.

Σε περίπτωση, λοιπόν, που αποδειχθεί ότι το Πανεπιστήμιο παρέχει κάποια από τις ανωτέρω κατάλληλες εγγυήσεις σχετικά με τη διαβίβαση των δεδομένων, η διαδικασία συνεχίζεται στο **βήμα 5**. Διαφορετικά, η διαδικασία συνεχίζεται στο **βήμα 4**.

Βήμα 4: Έλεγχος του καταλόγου των ειδικών παρεκκλίσεων του ΓΚΠΔ που επιτρέπουν περιορισμένες διαβιβάσεις δεδομένων σε τρίτες χώρες

Στην περίπτωση που ούτε έχει εκδοθεί απόφαση επάρκειας για την τρίτη χώρα ούτε παρέχονται από το Πανεπιστήμιο οι κατάλληλες εγγυήσεις του **βήματος 3**, η διαβίβαση δεδομένων προσωπικού χαρακτήρα προς τρίτη χώρα ή διεθνή οργανισμό μπορεί να πραγματοποιηθεί μόνο εφόσον ισχύει μία από τις παρακάτω ειδικές παρεκκλίσεις του ΓΚΠΔ:

1. Η διαβίβαση είναι απαραίτητη για σημαντικούς λόγους δημοσίου συμφέροντος.

2. Η διαβίβαση είναι απαραίτητη για τη θεμελίωση, την άσκηση ή την υποστήριξη νομικών αξιώσεων.

3. Η διαβίβαση είναι απαραίτητη για την προστασία των ζωτικών συμφερόντων του Υποκειμένου των Δεδομένων ή άλλων φυσικών προσώπων, εφόσον το Υποκείμενο των Δεδομένων δεν έχει τη φυσική, νοητική ή νομική ικανότητα να παράσχει τη συγκατάθεσή του.

4. Τα διαβιβαζόμενα δεδομένα λαμβάνονται από μητρώο ανοιχτό στο κοινό ή, έπειτα από αίτημα, σε κάθε πρόσωπο που μπορεί να θεμελιώσει το έννομο συμφέρον του στην πρόσβαση στο εν λόγω μητρώο.

Όσον αφορά στις άλλες τρείς περιπτώσεις ειδικών παρεκκλίσεων του ΓΚΠΔ σχετικά με τις διεθνείς διαβιβάσεις, ήτοι:

- το Υποκείμενο έχει ενημερωθεί για τους πιθανούς κινδύνους μιας τέτοιας διαβίβασης και έχει ρητώς συγκατατεθεί στη συγκεκριμένη διαβίβαση

- η διαβίβαση είναι απαραίτητη για την εκτέλεση σύμβασης μεταξύ του Υποκειμένου και του Υπευθύνου Επεξεργασίας ή την εφαρμογή προσυμβατικών μέτρων κατόπιν αιτήματος του Υποκειμένου των Δεδομένων

- η διαβίβαση είναι απαραίτητη για τη σύναψη ή εκτέλεση σύμβασης συναφθείσας προς όφελος του Υποκειμένου,

δεν δύναται να εφαρμόζονται από τα Πανεπιστήμια, όντας δημόσιες αρχές, σε δραστηριότητες που εκτελούν κατά την άσκηση των δημόσιων εξουσιών τους.

Σημειώνεται ότι η προσφυγή στις ανωτέρω παρεκκλίσεις είναι η τελευταία επιλογή μεταξύ των μηχανισμών διαβίβασης και είναι εφαρμοστέα μόνο σε περιορισμένες και ειδικές περιπτώσεις, καθώς οι διαβιβάσεις δεδομένων που γίνονται βάσει αυτών, ενδέχεται να οδηγήσουν σε υψηλούς κινδύνους για τα δικαιώματα και τις ελευθερίες των Υποκειμένων των Δεδομένων.

Επομένως, ο ΥΠΔ, σε συνεργασία με τον Νομικό Σύμβουλο του Πανεπιστημίου και το ενδιαφερόμενο Τμήμα, πρέπει, κάθε φορά, να αξιολογεί κατά πόσο η διαβίβαση που μπορεί να πραγματοποιηθεί με βάση μία από τις ανωτέρω τέσσερις πρώτες παρεκκλίσεις είναι αναγκαία για τον εκάστοτε σκοπό.

Συγκεκριμένα, όσον αφορά στην **πρώτη παρέκκλιση**, τα δημόσια συμφέροντα πρέπει να αναγνωρίζονται είτε από το δίκαιο της Ευρωπαϊκής Ένωσης είτε από τη νομοθεσία της Ελλάδας, η οποία αποτελεί το κράτος – μέλος στο οποίο υπόκειται το Πανεπιστήμιο Αιγαίου. Για παράδειγμα, η εν λόγω παρέκκλιση δεν θα μπορούσε να εφαρμοστεί εάν η δημόσια αρχή μιας τρίτης χώρας ζητούσε τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε αυτή λόγω κάποιου δημόσιου συμφέροντος που ορίζεται στο δίκαιό της, αλλά υπάρχει μόνο σε αφηρημένη έννοια στο δίκαιο της Ε.Ε. ή της Ελλάδας. Αντιθέτως, σε περίπτωση που το εν λόγω δημόσιο συμφέρον συνάγεται από το δίκαιο της Ε.Ε. ή της Ελλάδας, θα μπορούσε να εφαρμοστεί η συγκεκριμένη παρέκκλιση για τη διαβίβαση των δεδομένων. Επιπλέον, όταν η εν λόγω παρέκκλιση ισχύει κατά κανόνα και εφαρμόζεται σε επαναλαμβανόμενη βάση, το Πανεπιστήμιο πρέπει να αναζητήσει κάποιον από τους μηχανισμούς των βημάτων 2 ή 3 (π.χ. μέσω νομικά δεσμευτικού και εκτελεστού μέσου μεταξύ δημοσίων αρχών) για τη διαβίβαση των δεδομένων και να μην στηρίζεται σε αυτή.

Η **δεύτερη παρέκκλιση** πρέπει να εφαρμόζεται μόνο εάν η διαβίβαση των δεδομένων δεν γίνεται συστηματικά και μόνον εφόσον είναι απολύτως αναγκαία. Ενδεικτικό παράδειγμα αποτελεί η διαβίβαση δεδομένων στο πλαίσιο ποινικής ή διοικητικής έρευνας σε τρίτη χώρα, όπου η συγκεκριμένη παρέκκλιση μπορεί να εφαρμοστεί προς υπεράσπιση του Πανεπιστημίου Αιγαίου ή προκειμένου να επιτευχθεί μείωση ή παραίτηση από νόμιμα προβλεπόμενα πρόστιμα. Αντιθέτως, η παρέκκλιση αυτή δεν θα πρέπει να εφαρμόζεται για διαβίβαση δεδομένων λόγω πιθανής εκκίνησης δικαστικής διαδικασίας στο μέλλον.

Η **τρίτη παρέκκλιση**, η οποία αφορά στο ζωτικό συμφέρον των φυσικών προσώπων, πρέπει να εφαρμόζεται μόνο όταν ο επικείμενος κίνδυνος σοβαρής βλάβης του Υποκειμένου υπερτερεί των κινδύνων που ενδέχεται να προκύψουν από τη διαβίβαση σχετικά με την προστασία των δεδομένων. Κάθε φορά που η διαβίβαση δεδομένων πραγματοποιείται βάσει της εν λόγω παρέκκλισης, πρέπει να αποδεικνύεται, αναλόγως με την περίπτωση, η ανικανότητα του Υποκειμένου να συγκατατεθεί. Τέτοια απόδειξη μπορεί να αποτελεί είτε κάποιο ιατρικό πιστοποιητικό που αποδεικνύει τη νοητική ή φυσική ανικανότητα του Υποκειμένου, είτε κάποιο κυβερνητικό έγγραφο που επιβεβαιώνει τη νομική κατάσταση του Υποκειμένου των Δεδομένων (π.χ. ανήλικος). Επιπλέον, σημειώνεται ότι το Υποκείμενο μπορεί να είναι ανίκανο να δώσει τη συγκατάθεσή του λόγω κάποιας φυσικής καταστροφής (π.χ. σεισμός, πυρκαγιά, πλημμύρα).

Η **τέταρτη παρέκκλιση** εφαρμόζεται στην περίπτωση που τα δεδομένα που πρόκειται να διαβιβαστούν ανήκουν σε κάποιο δημόσιο μητρώο, το οποίο ορίζεται σύμφωνα με το δίκαιο της Ε.Ε. ή της Ελλάδας. Το εν λόγω μητρώο προορίζεται για την παροχή πληροφοριών στο κοινό και είναι ανοικτό για αναζήτηση πληροφοριών είτε στο ευρύ κοινό είτε σε οποιοδήποτε πρόσωπο μπορεί να επικαλεστεί έννομο συμφέρον για την πρόσβασή του σε αυτό. Τέτοια μητρώα μπορεί να αποτελούν μητρώα εταιρειών, μητρώα ποινικών καταδικαστέων αποφάσεων, μητρώα δημόσιων οχημάτων, μητρώα τίτλων γης, κ.λπ. Επισημαίνεται ότι η διαβίβαση δεδομένων από τα εν λόγω ανοιχτά στο κοινό μητρώα, μπορεί να πραγματοποιηθεί μόνο εφόσον πληρούνται στην εκάστοτε περίπτωση οι προϋποθέσεις που προβλέπονται στο δίκαιο της Ε.Ε. ή της Ελλάδας για την αναζήτηση πληροφοριών. Επομένως, το Πανεπιστήμιο προτού διαβιβάσει τα δεδομένα εφαρμόζοντας την παρέκκλιση αυτή, αξιολογεί την αναγκαιότητα της διαβίβασης λαμβάνοντας υπόψη τα συμφέροντα, τα δικαιώματα και τις ελευθερίες των Υποκειμένων των Δεδομένων. Σε περίπτωση, δε, που κάποιο φυσικό πρόσωπο έχει επικαλεστεί το έννομο συμφέρον του για αναζήτηση πληροφοριών που υπάρχουν σε αυτά τα μητρώα, η διαβίβαση των δεδομένων πραγματοποιείται μόνο κατόπιν αιτήματος του εν λόγω προσώπου ή μόνο εάν πρόκειται να είναι ο αποδέκτης των δεδομένων. Ο ΓΚΠΔ απαγορεύει τη διαβίβαση του συνόλου των δεδομένων προσωπικού χαρακτήρα ή ολόκληρης κατηγορίας δεδομένων προσωπικού χαρακτήρα που περιέχονται στα μητρώα αυτά.

Σε περίπτωση, λοιπόν, που αξιολογηθεί και αποδειχθεί ότι η διαβίβαση μπορεί να εφαρμοστεί βάσει κάποιας από τις ανωτέρω ειδικές παρεκκλίσεις, η διαδικασία συνεχίζεται στο **βήμα 5**. Διαφορετικά, η διαδικασία συνεχίζεται στο **βήμα 6**.

Βήμα 5: Έγκριση της διαβίβασης και ενημέρωση του ενδιαφερόμενου Τμήματος του Πανεπιστημίου

Ο ΥΠΔ εγκρίνει τη διαβίβαση των δεδομένων προσωπικού χαρακτήρα προς την τρίτη χώρα ή τον διεθνή οργανισμό και ενημερώνει σχετικά το ενδιαφερόμενο τμήμα του Πανεπιστημίου, ώστε να πραγματοποιήσει τη διαβίβαση που επιθυμεί.

Η παρούσα διαδικασία ολοκληρώνεται.

Βήμα 6: Απόρριψη της διαβίβασης και ενημέρωση του ενδιαφερόμενου Τμήματος του Πανεπιστημίου

Ο ΥΠΔ απορρίπτει τη διαβίβαση των δεδομένων προσωπικού χαρακτήρα προς την τρίτη χώρα ή τον διεθνή οργανισμό, καθώς δεν πληροί κάποια από τις ειδικές προϋποθέσεις του ΓΚΠΔ σχετικά με τις διεθνείς διαβιβάσεις και ενημερώνει το ενδιαφερόμενο τμήμα του Πανεπιστημίου προκειμένου να μην προχωρήσει στην πραγμάτωση της συγκεκριμένης διαβίβασης.

Η παρούσα διαδικασία ολοκληρώνεται.

Β.1.4. Διαδικασία Αντιμετώπισης Περιστατικών Παραβίασης Δεδομένων Προσωπικού Χαρακτήρα

Ο ΓΚΠΔ υποχρεώνει τους Υπεύθυνους Επεξεργασίας για γνωστοποίηση της παραβίασης δεδομένων προσωπικού χαρακτήρα στην αρμόδια Εποπτική Αρχή και, σε ορισμένες περιπτώσεις, για ανακοίνωση αυτής στα φυσικά πρόσωπα των οποίων τα δεδομένα προσωπικού χαρακτήρα έχουν επηρεαστεί.

Όλες οι Μονάδες του Πανεπιστημίου Αιγαίου δεσμεύονται να προστατεύουν τα δεδομένα προσωπικού χαρακτήρα που επεξεργάζονται, καθώς και τα Υποκείμενα των εν λόγω Δεδομένων. Επομένως το Πανεπιστήμιο οφείλει να είναι σε θέση να εντοπίζει, να διαχειρίζεται, να αναφέρει και να αντιμετωπίζει τα περιστατικά παραβίασης δεδομένων προσωπικού χαρακτήρα με αποτελεσματικό και αποδοτικό τρόπο, και σύμφωνα, πάντα, με τις απαιτήσεις του υφιστάμενου κανονιστικού πλαισίου.

Ειδικότερα, ως παραβίαση δεδομένων προσωπικού χαρακτήρα ορίζεται «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». Ενδεικτικά παραδείγματα περιστατικών τα οποία σχετίζονται με παραβίαση δεδομένων προσωπικού χαρακτήρα αποτελούν:

- Απώλεια ή κλοπή αποθηκευτικού μέσου (π.χ. USB stick, σκληρός δίσκος) που περιέχει δεδομένα προσωπικού χαρακτήρα υπαλλήλων του Πανεπιστημίου.
- Η μη εξουσιοδοτημένη πρόσβαση, υπαλλήλου ή μη, σε συστήματα που καταχωρίζονται δεδομένα προσωπικού χαρακτήρα φοιτητών και φοιτητριών.
- Η προσωρινή ή η μόνιμη διακοπή πρόσβασης σε δεδομένα προσωπικού χαρακτήρα, π.χ. λόγω διακοπής ρεύματος, λόγω καταστροφής από πυρκαγιά, λόγω επίθεσης άρνησης υπηρεσίας (Denial of Service DOS) στο Πανεπιστήμιο.
- Αποκάλυψη ευαίσθητων ή εμπιστευτικών πληροφοριών σε μη εξουσιοδοτημένο άτομο, π.χ. αποστολή ηλεκτρονικού μηνύματος που περιέχει δεδομένα προσωπικού χαρακτήρα σε λάθος παραλήπτη.

Οποιοδήποτε από τα παραπάνω περιστατικά ενδέχεται να διακυβεύσει την εμπιστευτικότητα, την ακεραιότητα ή/και τη διαθεσιμότητα των δεδομένων προσωπικού χαρακτήρα των Υποκειμένων, είτε αυτά είναι σε ηλεκτρονική είτε σε έντυπη μορφή.

Στόχος της παρούσας διαδικασίας είναι να διασφαλίσει τη γνωστοποίηση των περιστατικών παραβίασης δεδομένων προσωπικού χαρακτήρα στην αρμόδια Εποπτική Αρχή, εντός της προβλεπόμενης προθεσμίας των 72 ωρών, καθώς και την αμελλητί ενημέρωση των επηρεαζόμενων Υποκειμένων των Δεδομένων, σε περίπτωση που αυτό κριθεί απαραίτητο. Σημειώνεται, ότι παράλληλα με την εν λόγω διαδικασία εφαρμόζεται και η υφιστάμενη διαδικασία του Πανεπιστημίου για την αντιμετώπιση περιστατικών ασφάλειας πληροφοριών, καθώς ένα περιστατικό παραβίασης δεδομένων προσωπικού χαρακτήρα αποτελεί πάντα περιστατικό ασφάλειας πληροφοριών.

Β.1.4.1 Ομάδα Χειρισμού Περιστατικών Παραβίασης Δεδομένων Προσωπικού Χαρακτήρα

Ο ΥΠΔ και η Διοίκηση του Πανεπιστημίου είναι αρμόδιοι να συστήσουν την Ομάδα Χειρισμού Περιστατικών Παραβίασης Δεδομένων Προσωπικού Χαρακτήρα. Ο ΥΠΔ αποτελεί μέλος της Ομάδας Χειρισμού Περιστατικών Παραβίασης Δεδομένων Προσωπικού Χαρακτήρα, ενώ τα λοιπά μέλη περιλαμβάνουν προσωπικό κατάλληλα εκπαιδευμένο για την επιτυχή αντιμετώπιση περιστατικών παραβίασης δεδομένων προσωπικού χαρακτήρα και ασφάλειας, όπως διαχειριστές συστημάτων, ιδιοκτήτες συστημάτων κ.λπ.

Β.1.4.2 Περιστατικά Παραβίασης Δεδομένων Προσωπικού Χαρακτήρα

Ως ***περιστατικό παραβίασης δεδομένων προσωπικού χαρακτήρα*** το οποίο χρήζει αντιμετώπισης από το Πανεπιστήμιο ορίζονται περιστατικά παραβίασης της ασφάλειας που οδηγούν 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. Τα είδη των παραβιάσεων δεδομένων προσωπικού χαρακτήρα μπορεί να πλήξουν κάποιες από τις απαιτήσεις ασφάλειας πληροφοριακών συστημάτων, όπως φαίνεται στον παρακάτω πίνακα:

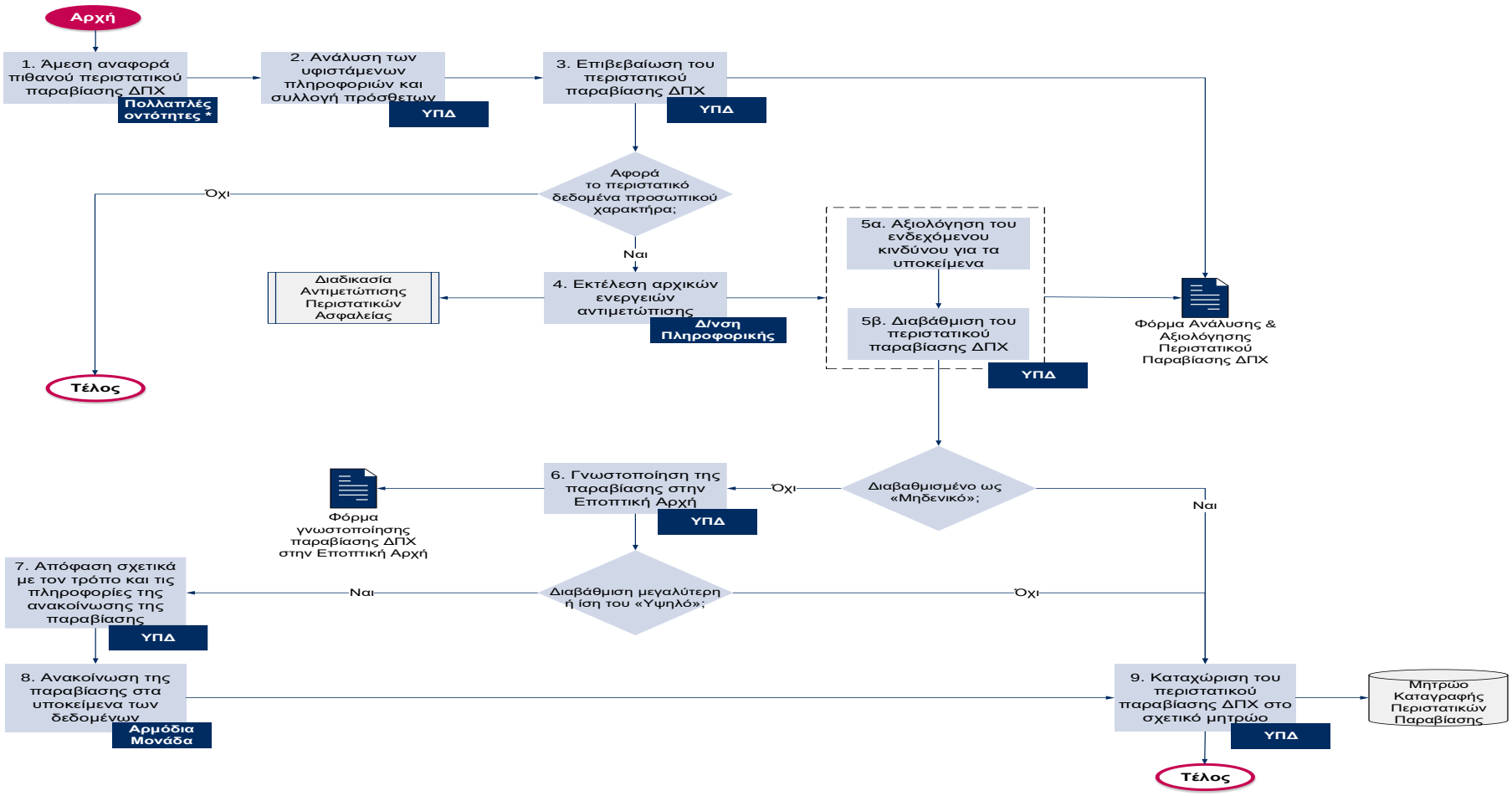
Είδη παραβιάσεων	
Εμπιστευτικότητας	Μη εξουσιοδοτημένη πρόσβαση, άνευ άδειας κοινολόγηση ή τυχαία αποκάλυψη προσωπικών δεδομένων
Διαθεσιμότητας	Τυχαία ή μη εξουσιοδοτημένη πρόσβαση που οδηγεί σε απώλεια ή καταστροφή ή απώλεια προσωπικών δεδομένων
Ακεραιότητας	Μη εξουσιοδοτημένη, ή τυχαία μεταβολή των δεδομένων προσωπικού χαρακτήρα

Πίνακας 10: Είδη παραβιάσεων δεδομένων προσωπικού χαρακτήρα

Β.1.4.3 Διαδικασία αντιμετώπισης περιστατικών παραβίασης δεδομένων προσωπικού χαρακτήρα

Στις παρακάτω ενότητες περιγράφεται η διαδικασία που θα πρέπει να ακολουθηθεί.

B.1.4.3.1 Σχηματική απεικόνιση της διαδικασίας



Σχήμα 5: Σχηματική απεικόνιση της διαδικασίας αντιμετώπισης περιστατικών παραβίασης δεδομένων προσωπικού χαρακτήρα για τον Υπεύθυνο Επεξεργασίας

Β.1.4.3.2 Περιγραφή των βημάτων της διαδικασίας

Σε αυτή την ενότητα περιλαμβάνονται τα βήματα για την αντιμετώπιση των περιστατικών παραβίασης δεδομένων προσωπικού χαρακτήρα στο πλαίσιο διαδικασιών επεξεργασίας από το Πανεπιστήμιο.

Βήμα 1: Αναφορά/Υποψία περιστατικού και ενημέρωση του Υπεύθυνου Προστασίας Δεδομένων

Ως αρμόδιο σημείο επικοινωνίας για την αναφορά περιστατικών παραβίασης δεδομένων προσωπικού χαρακτήρα του Πανεπιστημίου ορίζεται ο ΥΠΔ. Τα στοιχεία επικοινωνίας (τηλέφωνο, διεύθυνση ηλεκτρονικού ταχυδρομείου) του ΥΠΔ γνωστοποιούνται στο προσωπικό και τους συνεργάτες του Πανεπιστημίου. Τα συμβάντα πιθανής παραβίασης δεδομένων προσωπικού χαρακτήρα αναφέρονται στον ΥΠΔ με έναν από τους παρακάτω τρόπους, κατά σειρά προτίμησης:

- Ηλεκτρονικά, μέσω αποστολής μηνύματος ηλεκτρονικού ταχυδρομείου στον ΥΠΔ, το οποίο θα επισυνάπτει το έντυπο Παράρτημα Γ.3 (Έντυπο αναφοράς περιστατικού παραβίασης δεδομένων προσωπικού χαρακτήρα).

- Έντυπα, με χρήση του εντύπου Παράρτημα Γ.3 (Έντυπο αναφοράς περιστατικού παραβίασης δεδομένων προσωπικού χαρακτήρα).

- Τηλεφωνικά, σε εξαιρετικές περιπτώσεις (π.χ. ιδιαίτερα σοβαρά συμβάντα).

Σημειώνεται ότι πιθανά περιστατικά παραβίασης δεδομένων προσωπικού χαρακτήρα ενδέχεται να αναφερθούν στο Πανεπιστήμιο και από τρίτα μέρη που ενεργούν ως Εκτελούντες την Επεξεργασία για λογαριασμό του. Οι Εκτελούντες την Επεξεργασία υποχρεούνται από τις σχετικές συμβατικές ρήτρες να ενημερώνουν άμεσα το Πανεπιστήμιο σχετικά με κάποιο πιθανό περιστατικό παραβίασης δεδομένων.

Όλες οι παραπάνω οντότητες οφείλουν, όταν αναφέρουν πιθανό περιστατικό παραβίασης, να παρέχουν και συμπληρωματικές πληροφορίες στον ΥΠΔ, όπως τα στοιχεία επικοινωνίας τους, τον τύπο του πιθανού περιστατικού παραβίασης, μία συνοπτική περιγραφή αυτού, πληροφορίες σχετικά με την ημερομηνία και την ώρα που εκδηλώθηκε ή εντοπίστηκε το περιστατικό, καθώς και τα εμπλεκόμενα πληροφοριακά συστήματα.

Εφόσον ο ΥΠΔ αξιολογήσει το περιστατικό, μπορεί να συστήσει και να εμπλέξει Ομάδα Διερεύνησης Περιστατικών και να προχωρήσει στο **Βήμα 2**. Διαφορετικά, η διαδικασία ολοκληρώνεται.

Βήμα 2: Ενεργοποίηση της Ομάδας Χειρισμού Περιστατικών Παραβίασης Δεδομένων Προσωπικού Χαρακτήρα

Ο ΥΠΔ αξιοποιεί όλες τις διαθέσιμες πληροφορίες σχετικά με το συμβάν που του έχει γνωστοποιηθεί και συλλέγει επιπλέον πληροφορίες, αν κριθεί απαραίτητο, με σκοπό να τις αναλύσει και να εξακριβώσει, με βάση τις επόμενες ενέργειες, αν το αναφερθέν συμβάν αποτελεί πραγματικό περιστατικό παραβίασης δεδομένων προσωπικού χαρακτήρα. Ο ΥΠΔ ενημερώνει την Ομάδα Χειρισμού Περιστατικών Παραβίασης Δεδομένων Προσωπικού Χαρακτήρα.

Βήμα 3: Επιβεβαίωση περιστατικού παραβίασης δεδομένων προσωπικού χαρακτήρα

Στη συνέχεια, ο ΥΠΔ, με τη συνδρομή της Διεύθυνσης Πληροφορικής και Επικοινωνιών η οποία αποτελεί τη Μονάδα του Πανεπιστημίου που είναι υπεύθυνη για τα περιστατικά ασφαλείας πληροφοριών, πρέπει να εξακριβώσει αν το εν λόγω περιστατικό αφορά δεδομένα προσωπικού χαρακτήρα.

Προκειμένου να επιτευχθεί το παραπάνω, ο ΥΠΔ καταγράφει και αξιολογεί στην Παράρτημα «Γ.9 Φόρμα Ανάλυσης και Αξιολόγησης Περιστατικού Παραβίασης δεδομένων προσωπικού χαρακτήρα» όλες τις απαραίτητες πληροφορίες αναφορικά με το πιθανό περιστατικό παραβίασης. Συγκεκριμένα, τα πεδία που πρέπει να συμπληρωθούν είναι τα πεδία της Ενότητας Α – Πληροφορίες σχετικά με το ύποπτο συμβάν / περιστατικό και της Ενότητας Β – Περιγραφή του ύποπτου συμβάντος / περιστατικού της εν λόγω φόρμας.

Σε περίπτωση που το περιστατικό ασφαλείας / ύποπτο συμβάν δεν αφορά δεδομένα προσωπικού χαρακτήρα, τη διαχείρισή του την αναλαμβάνει αποκλειστικά η Διεύθυνση Πληροφορικής και Επικοινωνιών βάσει της υφιστάμενης διαδικασίας του Πανεπιστημίου για την αντιμετώπιση περιστατικών ασφαλείας πληροφοριών και η παρούσα διαδικασία τερματίζεται. Διαφορετικά, σε περίπτωση που το περιστατικό ασφαλείας / ύποπτο συμβάν αφορά δεδομένα προσωπικού χαρακτήρα, τότε χαρακτηρίζεται ως «περιστατικό παραβίασης δεδομένων προσωπικού χαρακτήρα» και διαδικασία συνεχίζεται στο **βήμα 4**.

Σημειώνεται ότι από τη στιγμή που επιβεβαιωθεί ότι πρόκειται για περιστατικό παραβίασης δεδομένων προσωπικού χαρακτήρα, το Πανεπιστήμιο, μέσω του ΥΠΔ, οφείλει να ενημερώσει την Εποπτική Αρχή εντός 72 ωρών.

Βήμα 4: Εκτέλεση αρχικών ενεργειών αντιμετώπισης του περιστατικού παραβίασης

Αμέσως μετά την επιβεβαίωση του περιστατικού παραβίασης δεδομένων προσωπικού χαρακτήρα από τον ΥΠΔ, διενεργούνται από τη Διεύθυνση Πληροφορικής και Επικοινωνιών, εάν και εφόσον είναι εφικτό, απλές, γρήγορες και αποτελεσματικές αρχικές ενέργειες αντιμετώπισης του περιστατικού, προκειμένου να περιοριστούν, όσο το δυνατόν περισσότερο, οι επιπτώσεις του στα Υποκείμενα των Δεδομένων.

Επιπλέον, προκειμένου να αντιμετωπιστεί πλήρως το περιστατικό, παράλληλα με τα βήματα της παρούσας διαδικασίας, διενεργούνται από τη Διεύθυνση Πληροφορικής και Επικοινωνιών του Πανεπιστημίου ενέργειες για τη διαχείριση και την αντιμετώπισή του, σύμφωνα με τη διαδικασία για την αντιμετώπιση περιστατικών ασφάλειας πληροφοριών.

Η διαδικασία συνεχίζεται στο **βήμα 5.**

Σημειώνεται ότι το **βήμα 4** διενεργείται παράλληλα με το **βήμα 5.**

Βήμα 5: Αξιολόγηση και διαβάθμιση του περιστατικού παραβίασης δεδομένων προσωπικού χαρακτήρα

α. Αξιολόγηση του ενδεχόμενου κινδύνου για τα Υποκείμενα των Δεδομένων

Αμέσως μόλις επιβεβαιωθεί ότι το περιστατικό αφορά παραβίαση δεδομένων προσωπικού χαρακτήρα, ο ΥΠΔ το αξιολογεί και του αποδίδει ένα επίπεδο κινδύνου, με βάση τις πιθανές επιπτώσεις που έχει ή ενδέχεται να έχει στο Υποκείμενο ή τα Υποκείμενα των Δεδομένων. Στην εν λόγω ενέργεια, όπου και όποτε χρειάζεται, συνδράμουν τον ΥΠΔ οι υπόλοιπες μονάδες του Πανεπιστημίου και δη η Διεύθυνση Πληροφορικής και Επικοινωνιών.

Αναλυτικότερα, οι παράγοντες οι οποίοι λαμβάνονται υπόψη για την αξιολόγηση του κινδύνου που ενδέχεται να επιφέρει ένα περιστατικό παραβίασης για τα Υποκείμενα των Δεδομένων, είναι αυτοί που βρίσκονται στη φόρμα Παράρτημα «Γ.9 Φόρμα Ανάλυσης και Αξιολόγησης Περιστατικού Παραβίασης δεδομένων προσωπικού χαρακτήρα». Ενδεικτικά κάποια πεδία της φόρμας περιγράφονται παρακάτω:

- Ο τύπος της παραβίασης δεδομένων. Η φύση της παραβίασης των δεδομένων, δηλαδή αν αποτελεί παραβίαση της εμπιστευτικότητας, παραβίαση της ακεραιότητας, παραβίαση της διαθεσιμότητας, ή οποιονδήποτε συνδυασμό αυτών, επηρεάζει σε σημαντικό βαθμό τη διαβάθμιση του κινδύνου. Για παράδειγμα, μία παραβίαση της ακεραιότητας και της εμπιστευτικότητας των δεδομένων ενδέχεται να επιφέρει μεγαλύτερο κίνδυνο για τα δικαιώματα και τις ελευθερίες των επηρεαζόμενων υποκειμένων, από ότι μία παραβίαση μόνο της εμπιστευτικότητας.

- Η φύση και ο όγκος των δεδομένων προσωπικού χαρακτήρα που έχουν επηρεαστεί από το περιστατικό παραβίασης. Όσο πιο ειδικής κατηγορίας είναι τα δεδομένα, τόσο υψηλότερος είναι ο κίνδυνος να επηρεαστούν αρνητικά τα επηρεαζόμενα από το περιστατικό Υποκείμενα. Επιπλέον, ένα περιστατικό που αφορά συνδυασμό διαφόρων κατηγοριών δεδομένων προσωπικού χαρακτήρα, τις περισσότερες φορές ενδέχεται να προκαλέσει μεγαλύτερη ζημιά από ένα περιστατικό που αφορά μία μόνο κατηγορία δεδομένων προσωπικού χαρακτήρα.

- Η «ταυτότητα» των Υποκειμένων των Δεδομένων που επηρεάστηκαν από το περιστατικό παραβίασης, καθώς και ο εκτιμώμενος αριθμός αυτών. Η «ταυτότητα» των Υποκειμένων είναι η κατηγορία στην οποία ανήκουν τα Υποκείμενα των Δεδομένων, όπως για παράδειγμα φοιτητές και φοιτήτριες άνω των 18 ετών, ανήλικοι φοιτητές και φοιτήτριες, υπάλληλοι του Πανεπιστημίου, απόφοιτοι, κ.λπ. Συγκεκριμένα, το επίπεδο κινδύνου του περιστατικού θα είναι υψηλότερο σε περίπτωση που επηρεαστούν ευάλωτα άτομα ή άτομα που χρήζουν ειδικής μεταχείρισης, όπως παιδιά ή ΑμεΑ. Επιπλέον, μεγάλος αριθμός επηρεαζόμενων Υποκειμένων σημαίνει ότι το επίπεδο του κινδύνου του περιστατικού ενδεχομένως θα είναι υψηλό, ανεξαρτήτως της «ταυτότητας» των επηρεαζόμενων Υποκειμένων.

- Η ευκολία ταυτοποίησης των Υποκειμένων των Δεδομένων. Το επίπεδο του κινδύνου του περιστατικού διαμορφώνεται ανάλογα με το πόσο εύκολα, κάθε φορά, τα δεδομένα προσωπικού χαρακτήρα που έχουν παραβιαστεί, μπορούν να οδηγήσουν στα Υποκείμενα των Δεδομένων και στην ταυτοποίηση αυτών. Όταν η ταυτοποίηση του Υποκειμένου / των Υποκειμένων ενδέχεται να γίνει με μεγάλη ευκολία, τότε το επίπεδο κινδύνου είναι υψηλό.

Αντίθετα, όταν η ταυτοποίηση του Υποκειμένου / των Υποκειμένων είναι αδύνατο να επιτευχθεί τότε το περιστατικό διαβαθμίζεται στα κατώτερα επίπεδα κινδύνου.

- Οι ενδεχόμενες επιπτώσεις για τα Υποκείμενα των Δεδομένων. Η διαβάθμιση του περιστατικού παραβίασης δεδομένων προσωπικού χαρακτήρα εξαρτάται σε σημαντικό βαθμό από τις επιπτώσεις που έχει ή ενδέχεται να έχει το περιστατικό για τα Υποκείμενα των Δεδομένων. Προκειμένου να διαβαθμιστεί αποτελεσματικά το περιστατικό βάσει των εν λόγω επιπτώσεων, πρέπει να εκτιμηθεί τόσο η σοβαρότητα των επιπτώσεων για τα Υποκείμενα των Δεδομένων, όσο και η πιθανότητα να συμβεί στην πραγματικότητα κάποια βλάβη, σωματική, υλική ή μη υλική, στα Υποκείμενα λόγω των επιπτώσεων αυτών.

- Υφιστάμενα μέτρα ασφάλειας, τα οποία εφαρμόζονται από το Πανεπιστήμιο στα συστήματα ή / και στα δεδομένα που έχουν επηρεαστεί από το περιστατικό. Τα εν λόγω μέτρα δεν λειτουργούν αποτρεπτικά, αλλά στοχεύουν στη μέγιστη δυνατή ελαχιστοποίηση των επιπτώσεων που ενδέχεται να έχει το περιστατικό για τα Υποκείμενα των Δεδομένων, ενώ λειτουργούν και αποτρεπτικά στη χρήση των επηρεαζόμενων δεδομένων με κακόβουλο τρόπο. Για παράδειγμα, αν τα δεδομένα που επηρεάστηκαν από την παραβίαση είναι κρυπτογραφημένα με ισχυρό αλγόριθμό, δεν είναι αναγνώσιμα από κάποιον μη εξουσιοδοτημένο ο οποίος δεν γνωρίζει το κλειδί αποκρυπτογράφησής τους, επομένως, ο κίνδυνος για τα Υποκείμενα είναι μικρός.

β. Διαβάθμιση του περιστατικού παραβίασης

Αφού εκτιμηθούν από τους αρμόδιους όλα τα πεδία της φόρμας, ο ΥΠΔ διαβαθμίζει το επίπεδο κινδύνου του περιστατικού παραβίασης δεδομένων προσωπικού χαρακτήρα ως μηδενικό, χαμηλό, μεσαίο, υψηλό, πολύ υψηλό (βλ. Πίνακας 11).

Η σωστή διαβάθμιση του κινδύνου του περιστατικού παραβίασης είναι αρκετά σημαντική, καθώς οι περισσότερες από τις μετέπειτα ενέργειες που θα εκτελεστούν και από τις αποφάσεις που θα ληφθούν εξαρτώνται από αυτή.

ΠΙΝΑΚΑΣ ΔΙΑΒΑΘΜΙΣΗΣ ΚΙΝΔΥΝΟΥ ΠΕΡΙΣΤΑΤΙΚΟΥ ΠΑΡΑΒΙΑΣΗΣ		
Κίνδυνος για τα υποκείμενα	**Περιγραφή επιπτώσεων**	**Απαίτηση γνωστοποίησης**
Πολύ υψηλός	Οι επιπτώσεις για τα Υποκείμενα των Δεδομένων είναι εξαιρετικά σοβαρές και απαιτούνται σημαντικές προσπάθειες για την αντιμετώπισή τους ή ενδέχεται να είναι μη αναστρέψιμες και να μην δύναται να ξεπεραστούν	Στην αρμόδια Εποπτική Αρχή και στα επηρεαζόμενα Υποκείμενα των Δεδομένων

ΠΙΝΑΚΑΣ ΔΙΑΒΑΘΜΙΣΗΣ ΚΙΝΔΥΝΟΥ ΠΕΡΙΣΤΑΤΙΚΟΥ ΠΑΡΑΒΙΑΣΗΣ		
	από τα επηρεαζόμενα Υποκείμενα.	
Υψηλός	Τα Υποκείμενα των Δεδομένων ενδέχεται να αντιμετωπίσουν σημαντικά και σοβαρά προβλήματα, τα οποία θα ξεπεραστούν με δυσκολία.	Στην αρμόδια Εποπτική Αρχή και στα επηρεαζόμενα Υποκείμενα των Δεδομένων
Μεσαίος	Τα Υποκείμενα των Δεδομένων δύναται να αντιμετωπίσουν δυσκολίες ή δυσμενείς επιπτώσεις, οι οποίες, ωστόσο, δεν είναι πολύ σοβαρές και μπορούν να ξεπεραστούν με κάποιο κόστος.	Στην αρμόδια Εποπτική Αρχή
Χαμηλός	Τα Υποκείμενα αντιμετωπίζουν λίγες δυσκολίες ή μικρά προβλήματα, τα οποία μπορούν εύκολα να ξεπεραστούν.	Στην αρμόδια Εποπτική Αρχή
Μηδενικός	Τα Υποκείμενα δεν επηρεάζονται καθόλου από το περιστατικό.	Δεν απαιτείται

Πίνακας 11: Διαβάθμιση περιστατικού παραβίασης

Σε περίπτωση που ο κίνδυνος από το περιστατικό παραβίασης δεν διαβαθμιστεί ως «Μηδενικός», δηλαδή υπάρχει ενδεχόμενος κίνδυνος για τα Υποκείμενα των Δεδομένων, η παρούσα διαδικασία συνεχίζεται στο **βήμα 6**. Διαφορετικά, δηλαδή σε περίπτωση που ο κίνδυνος από το περιστατικό παραβίασης διαβαθμιστεί ως «Μηδενικός», η διαδικασία συνεχίζεται στο **βήμα 9.**

Βήμα 6: Γνωστοποίηση της παραβίασης δεδομένων προσωπικού χαρακτήρα στην αρμόδια Εποπτική Αρχή

Το Πανεπιστήμιο Αιγαίου, έχοντας τον ρόλο του Υπευθύνου της Επεξεργασίας, οφείλει να γνωστοποιήσει το περιστατικό παραβίασης στην αρμόδια Εποπτική Αρχή (ΑΠΔΠΧ) εντός 72 ωρών από τη στιγμή που αποκτά γνώση της παραβίασης. Θεωρείται πως έχει λάβει γνώση της παραβίασης από τη στιγμή που έχει αποκτήσει κάποιο βαθμό βεβαιότητας ότι το αναφερθέν συμβάν αποτελεί περιστατικό παραβίασης δεδομένων προσωπικού χαρακτήρα (βήμα 3 της παρούσας διαδικασίας). Αρμόδιος για την εκτέλεση της εν λόγω ενέργειας είναι ο ΥΠΔ.

Ο ΥΠΔ επιλέγει από την ιστοσελίδα της Εθνικής Εποπτικής Αρχής ΑΠΔΠΧ (http://www.dpa.gr/portal/page?_pageid=33,211142&_dad=portal&_schema=PORTAL) τη φόρμα που απαιτείται για τη γνωστοποίηση της παραβίασης δεδομένων προσωπικού χαρακτήρα και συμπληρώνει τις απαραίτητες πληροφορίες για το περιστατικό παραβίασης. Σημειώνεται ότι η αγγλική έκδοση της φόρμας επιλέγεται μόνο σε περίπτωση που το περιστατικό αφορά διασυνοριακή επεξεργασία. Στη συμπλήρωση της φόρμας της Εποπτικής Αρχής δύνανται να συνδράμουν τον ΥΠΔ, όποτε και όπου απαιτείται, οι λοιπές μονάδες του Πανεπιστημίου.

Έπειτα, ο ΥΠΔ κρυπτογραφεί, με βάση τις οδηγίες της Αρχής, τη συμπληρωμένη φόρμα γνωστοποίησης του περιστατικού παραβίασης δεδομένων προσωπικού χαρακτήρα και την αποστέλλει στην Αρχή μέσω μηνύματος ηλεκτρονικού ταχυδρομείου (e-mail) στην ηλεκτρονική διεύθυνση: databreach@dpa.gr. Σημειώνεται ότι ο ΥΠΔ μπορεί να υποβάλλει τη φόρμα με άλλο τρόπο μόνον σε εξαιρετικές περιπτώσεις, όπου η φόρμα δεν μπορεί να αποσταλεί στην Αρχή μέσω e-mail και σε αυτή την περίπτωση θα πρέπει να τεκμηριώνεται επαρκώς ο λόγος που δεν προτιμήθηκε η ηλεκτρονική υποβολή.

Εάν ο ΥΠΔ δεν γνωστοποιήσει την παραβίαση στην αρμόδια εποπτική Αρχή εντός των 72 ωρών, τότε πρέπει, μαζί με τη γνωστοποίησή της, να αιτιολογήσει επαρκώς τους λόγους για τους οποίους καθυστέρησε. Επιπλέον, σε περίπτωση που η παροχή όλων των πληροφοριών σχετικά με την παραβίαση δεν μπορεί να γίνει ταυτόχρονα, οι πληροφορίες δύνανται να παρέχονται σταδιακά από τον ΥΠΔ στην Εποπτική Αρχή χωρίς αδικαιολόγητη καθυστέρηση.

Σε περίπτωση που ο κίνδυνος από το περιστατικό παραβίασης έχει διαβαθμιστεί ως «Πολύ Υψηλός» ή «Υψηλός», η διαδικασία συνεχίζεται στο **βήμα 7**. Διαφορετικά, η διαδικασία συνεχίζεται στο **βήμα 9.**

Βήμα 7: Απόφαση σχετικά με τον τρόπο και τις πληροφορίες της ανακοίνωσης της παραβίασης στα Υποκείμενα των Δεδομένων

Ο ΥΠΔ αποφασίζει τον τρόπο που θα πραγματοποιηθεί η απαιτούμενη ανακοίνωση του περιστατικού παραβίασης στα επηρεαζόμενα Υποκείμενα των Δεδομένων, καθώς και τις απαραίτητες πληροφορίες που θα κοινοποιηθούν σε εκείνα σχετικά με την παραβίαση. Η ανακοίνωση στα Υποκείμενα των Δεδομένων πρέπει να γίνει άμεσα από τη στιγμή που το Πανεπιστήμιο Αιγαίου λάβει γνώση του περιστατικού παραβίασης δεδομένων προσωπικού χαρακτήρα.

Αναλυτικότερα, ο ΥΠΔ ανάλογα με το μέγεθος του περιστατικού παραβίασης, την «ταυτότητα» και τον αριθμό των επηρεαζόμενων Υποκειμένων επιλέγει τον πιο αποτελεσματικό τρόπο για την ανακοίνωση της παραβίασης στα Υποκείμενα των Δεδομένων.

Ενδεικτικοί τρόποι για την ανακοίνωση της παραβίασης στους φοιτητές, απόφοιτους, διδακτορικούς, φαίνονται στον παρακάτω πίνακα (Πίνακας 12).

Τρόπος Ανακοίνωσης	Περιγραφή
Τηλεφωνική επικοινωνία	Η αρμόδια μονάδα καλεί τα επηρεαζόμενα Υποκείμενα των Δεδομένων στο τηλέφωνο επικοινωνίας που έχουν δηλώσει στο Πανεπιστήμιο.
E-mail	Η αρμόδια μονάδα αποστέλλει, στη διεύθυνση ηλεκτρονικού ταχυδρομείου που έχουν δηλώσει τα Υποκείμενα στο Πανεπιστήμιο, κείμενο που αφορά στην ανακοίνωση της παραβίασης.

Πίνακας 12: Τρόπος ανακοίνωσης της παραβίασης

Όταν τα επηρεαζόμενα Υποκείμενα των Δεδομένων είναι φοιτητές ή φοιτήτριες ή απόφοιτοι, η ανακοίνωση της παραβίασης γίνεται από τη Διεύθυνση Σπουδών. Σε περίπτωση που η παραβίαση αφορά δεδομένα των καθηγητών ή καθηγητριών ή του λοιπού προσωπικού του Πανεπιστημίου, υπεύθυνη μονάδα για να προβεί στις απαιτούμενες ενέργειες για την ενημέρωση των επηρεαζόμενων Υποκειμένων σχετικά με το περιστατικό παραβίασης είναι το τμήμα Διοικητικού του Πανεπιστημίου.

Σημειώνεται ότι όταν για την ανακοίνωση της παραβίασης στα επηρεαζόμενα Υποκείμενα των Δεδομένων απαιτούνται δυσανάλογες προσπάθειες, το Πανεπιστήμιο πρέπει να προχωρήσει σε δημόσια ανακοίνωση. Επιπλέον, το Πανεπιστήμιο μπορεί να βρει παρόμοιους τρόπους, μέσω των οποίων να καταφέρει να ενημερώνονται τα Υποκείμενα των Δεδομένων με εξίσου αποτελεσματικό τρόπο. Ενδεικτικοί τρόποι ανακοίνωσης της παραβίασης όταν απαιτούνται δυσανάλογες προσπάθειες είναι:

- Η ανάρτηση ανακοίνωσης αναφορικά με το περιστατικό παραβίασης δεδομένων προσωπικού χαρακτήρα στην ιστοσελίδα εκάστου Τμήματος του Πανεπιστημίου.
- Η δημοσιοποίηση του περιστατικού παραβίασης στα Μέσα Μαζικής Ενημέρωσης.

Προκειμένου να ανακοινωθεί με επιτυχία η παραβίαση των δεδομένων προσωπικού χαρακτήρα στα Υποκείμενα, ο ΥΠΔ συντονίζει, καθοδηγεί και παρακολουθεί τις αρμόδιες μονάδες του Πανεπιστημίου σχετικά με τις ενέργειες που πρέπει να εκτελέσουν.

Η διαδικασία συνεχίζεται στο **βήμα 8**.

Βήμα 8: Ανακοίνωση της παραβίασης στα επηρεαζόμενα Υποκείμενα των Δεδομένων

Η αρμόδια μονάδα του Πανεπιστημίου, η οποία έχει επιλεγεί από τον ΥΠΔ στο προηγούμενο βήμα της παρούσας διαδικασίας, ανακοινώνει αμελλητί μέσω του αντίστοιχου καναλιού επικοινωνίας την παραβίαση δεδομένων προσωπικού χαρακτήρα στα επηρεαζόμενα Υποκείμενα.

Ανεξαρτήτως από την αρμόδια μονάδα και τον τρόπο που θα ανακοινωθεί η παραβίαση, πρέπει να παρέχονται στα Υποκείμενα των Δεδομένων συγκεκριμένες πληροφορίες, οι οποίες πρέπει κατ' ελάχιστον να περιλαμβάνουν όσα αναφέρονται ακολούθως: Πίνακας 13.

Πληροφορίες της ανακοίνωσης	Επεξήγηση
Σκοπός της επικοινωνίας	Συνοπτική εισαγωγική παράγραφος αναφορικά με τον σκοπό της εν λόγω επικοινωνίας.
Στοιχεία του ΥΠΔ	Δήλωση των στοιχείων επικοινωνίας του ΥΠΔ, ώστε τα υποκείμενα να έχουν τη δυνατότητα επικοινωνίας με το Πανεπιστήμιο για τυχόν περαιτέρω λεπτομέρειες αναφορικά με την παραβίαση.
Περιγραφή περιστατικού παραβίασης	Συνοπτική περιγραφή του περιστατικού παραβίασης δεδομένων προσωπικού χαρακτήρα.
Επηρεαζόμενα δεδομένα	Αναφορά των δεδομένων ή των κατηγοριών δεδομένων προσωπικού χαρακτήρα που επηρεάστηκαν από την παραβίαση.
Επιπτώσεις της παραβίασης	Περιγραφή των επιπτώσεων που έχει ή ενδέχεται να έχει η παραβίαση για τα Υποκείμενα των Δεδομένων.
Υφιστάμενα και προγραμματισμένα προς λήψη μέτρα προστασίας	Περιγραφή των μέτρων προστασίας που έχει λάβει ή θα λάβει το Πανεπιστήμιο Αιγαίου, προκειμένου να προστατεύσει τα δεδομένα προσωπικού χαρακτήρα και να ελαχιστοποιήσει τις επιπτώσεις για τα Υποκείμενα των Δεδομένων.
Μέτρα προς λήψη από τα ίδια τα Υποκείμενα	Παροχή συμβουλών σχετικά με τις ενέργειες ή με τα μέτρα προστασίας που μπορούν να λάβουν τα Υποκείμενα των Δεδομένων προκειμένου να αυτό-προστατευθούν από τις ενδεχόμενες επιπτώσεις της παραβίασης.

Πίνακας 13: Περιεχόμενα της ανακοίνωσης της παραβίασης στα Υποκείμενα των Δεδομένων

Η διαδικασία συνεχίζεται στο βήμα 9.

<u>Βήμα 9: Καταχώριση του περιστατικού παραβίασης δεδομένων προσωπικού χαρακτήρα στο σχετικό μητρώο</u>

Ο ΥΠΔ καταχωρίζει όλες τις λεπτομέρειες του περιστατικού παραβίασης δεδομένων προσωπικού χαρακτήρα σε ένα μητρώο, το «Μητρώο Καταγραφής Περιστατικών Παραβίασης». Σκοπός του εν λόγω μητρώου είναι να τηρούνται τεκμηριωμένα όλα τα επιβεβαιωμένα περιστατικά παραβίασης δεδομένων προσωπικού χαρακτήρα, ανεξαρτήτως του επιπέδου κινδύνου τους, είτε αυτά

εκδηλώθηκαν εντός του Πανεπιστημίου είτε αναφέρθηκαν σε αυτό από κάποιον εκτελούντα την επεξεργασία ή από κάποιον τρίτο ως προς αυτό.

Η παρούσα διαδικασία ολοκληρώνεται.

Όσον αφορά στην αντιμετώπιση του περιστατικού παραβίασης, οι απαιτούμενες ενέργειες περιγράφονται στην υφιστάμενη διαδικασία του Πανεπιστημίου Αιγαίου για την αντιμετώπιση περιστατικών ασφαλείας πληροφοριών.

Β.1.5. Διαδικασία για την Εκπαίδευση του προσωπικού

Το Πανεπιστήμιο Αιγαίου οφείλει να διασφαλίζει ότι το προσωπικό που είναι αρμόδιο για την τεχνική διαχείριση των ΠΣ του, καθώς και την εγγραφή και υποστήριξη των χρηστών του, κατέχει τις απαιτούμενες γνώσεις και δεξιότητες για την προστασία έναντι παραβιάσεων προσωπικών δεδομένων. Η εκπαίδευση του προσωπικού αφορά τόσο στην αποφυγή σφαλμάτων που θα οδηγήσουν σε παραβιάσεις προσωπικών δεδομένων, όσο και την εφαρμογή αντιμέτρων και την προστασία των δεδομένων και την έγκαιρη ανίχνευση περιστατικών. Η διαδικασία της εκπαίδευσης του προσωπικού είναι διαρκής και περιλαμβάνει τουλάχιστον τα παρακάτω βήματα.

Βήμα 1: Καταγραφή γνώσεων και δεξιοτήτων

Το προσωπικό του Πανεπιστημίου πρέπει να γνωρίζει την παρούσα πολιτική προστασίας δεδομένων. Επιπρόσθετα, το προσωπικό τεχνικής διαχείρισης πρέπει να κατέχει γνώσεις σχετικές με την τεχνική διαχείριση των πληροφοριακών συστημάτων του Πανεπιστημίου.

Βήμα 2: Διαχωρισμός (τυχόν) ομάδων αποδεκτών

Σε περίπτωση που κρίνεται απαραίτητο, το προσωπικό διαχωρίζεται σε ομάδες αποδεκτών. Κριτήρια για τον διαχωρισμό είναι: α) προηγούμενες αξιολογήσεις και διαφοροποίηση επιδόσεων, β) έτη προϋπηρεσίας, γ) εξειδικευμένες γνώσεις που απαιτούνται από συγκεκριμένα στελέχη.

Βήμα 3: Σχεδιασμός εκπαιδευτικού πλάνου και μετρικών αξιολόγησης

Σε αυτό το βήμα σχεδιάζεται το εκπαιδευτικό πλάνο, το οποίο περιλαμβάνει τουλάχιστον τα ακόλουθα στοιχεία:

- Θεματικές ενότητες εκπαίδευσης και εκπαιδευτικό περιεχόμενο (π.χ. εκπαίδευση στη διαχείριση συστημάτων ανίχνευσης παρεισφρήσεων)
- Αντιστοίχιση του εκπαιδευτικού περιεχομένου με τις καταγεγραμμένες γνώσεις και δεξιότητες
- Μέσα εκπαίδευσης (π.χ. webinars, απομακρυσμένη μάθηση, διαλέξεις)
- Μετρικές και μέσα αξιολόγησης (π.χ. τεστ, προσομοιώσεις)

Βήμα 4: Υλοποίηση εκπαιδεύσεων

Σε αυτό το βήμα υλοποιούνται οι εκπαιδεύσεις σύμφωνα με το εκπαιδευτικό πλάνο του **Βήματος 3**.

Βήμα 5: Αξιολόγηση εκπαίδευσης

Σε αυτό το βήμα υλοποιείται η αξιολόγηση της εκπαίδευσης με στόχο την αποτίμηση της ικανότητας του προσωπικού να εφαρμόζει τα ισχύοντα τεχνικά αντίμετρα για την προστασία της υποδοχής και την ευαισθητοποίηση στην προστασία προσωπικών δεδομένων και τη συμμόρφωση με τον ΓΚΠΔ.

Η διαδικασία ολοκληρώνεται.

Β.1.6. Διαδικασία για την Ενημερότητα του προσωπικού

Το Πανεπιστήμιο οφείλει να διασφαλίζει ότι το προσωπικό του είναι ευαισθητοποιημένο σε θέματα προστασίας προσωπικών δεδομένων, καθώς διαχειρίζεται τις προσωπικές πληροφορίες των χρηστών των Πληροφοριακών Συστημάτων. Η διαδικασία της ευαισθητοποίησης του προσωπικού του Πανεπιστημίου είναι διαρκής και περιλαμβάνει τουλάχιστον τα παρακάτω βήματα.

Βήμα 1: Αναγνώριση αποδεκτών και διαχωρισμός (τυχόν) ομάδων αποδεκτών

Το προσωπικό του Πανεπιστημίου ενδέχεται να διαφέρει αναφορικά με τις ανάγκες ευαισθητοποίησης σε θέματα προστασίας προσωπικών δεδομένων. Σε αυτή την περίπτωση συστήνεται ο διαχωρισμός ομάδων αποδεκτών. Ενδεικτικά κριτήρια αποτελούν α) το είδος των προσωπικών δεδομένων που διαχειρίζεται ο υπάλληλος (π.χ. στην περίπτωση που το Πανεπιστήμιο αποδώσει διαφορετικούς ρόλους στο προσωπικό του), β) τα έτη προϋπηρεσίας (π.χ. οι ανάγκες ευαισθητοποίησης νέων εργαζομένων είναι διαφορετικές από αυτές των ήδη υπηρετούντων).

Βήμα 2: Σχεδιασμός πλάνου ενημερότητας προστασίας προσωπικών δεδομένων

Σε αυτό το βήμα σχεδιάζεται το πρόγραμμα ενημερότητας, το οποίο περιλαμβάνει τουλάχιστον τα ακόλουθα στοιχεία:

- Θεματικές ενότητες. Κατ' ελάχιστον το πρόγραμμα ενημερότητας πρέπει να περιλαμβάνει θέματα:
    - του ΓΚΠΔ (ορισμός και αναγνώριση προσωπικών δεδομένων, αναγνώριση σκοπού επεξεργασίας των Πληροφοριακών Συστημάτων του Πανεπιστημίου, επίγνωση δικαιωμάτων των υποκειμένων των δεδομένων),
    - πολιτικής προστασίας δεδομένων του Πανεπιστημίου και σχετικές πρακτικές εργασίας
    - προστασίας λογαριασμού χρήστη
    - κοινωνικής μηχανικής, μη επιθυμητής αλληλογραφίας, ηλεκτρονικής αλίευσης και απάτης
    - προστασίας από κακόβουλο και ιομορφικό λογισμικό
    - φυσικής ασφάλειας.
- Κανάλια επικοινωνίας. Η επιλογή καναλιών επικοινωνίας εξαρτάται από τον αριθμό του προσωπικού που απασχολείται στο Πανεπιστήμιο και μπορεί να περιλαμβάνει κοινωνικά μέσα, προωθητικά μέσα (π.χ. αντικείμενα με μηνύματα για την προστασία προσωπικών δεδομένων, αφίσες, φυλλάδια, κ.λπ.) ή ενημερωτικά μέσα (π.χ. newsletters, εκδηλώσεις).

Βήμα 3: Υλοποίηση δράσεων ενημερότητας προστασίας προσωπικών δεδομένων

Σε αυτό το βήμα υλοποιούνται οι δράσεις ενημερότητας και ευαισθητοποίησης που έχουν σχεδιαστεί στο **Βήμα 2**.

Βήμα 4: Αξιολόγηση προγράμματος ενημερότητας

Η υλοποίηση των δράσεων ενημερότητας είναι διαρκείς, προκειμένου να επιφέρουν μακροπρόθεσμο αποτέλεσμα. Παρόλα αυτά, συστήνεται η περιοδική αξιολόγηση της επίδρασης του προγράμματος ενημερότητας (π.χ. ετησίως) στο προσωπικό του Πανεπιστημίου. Η αξιολόγηση μπορεί να υλοποιηθεί με προκαθορισμένες μετρικές, όπως ο αριθμός συμμετεχόντων στις εκδηλώσεις του προγράμματος, ο αριθμός περιστατικών αποκάλυψης προσωπικών δεδομένων λόγω ανθρώπινου λάθους, επιδόσεις σε ασκήσεις αξιολόγησης, κ.ά.

Η διαδικασία ολοκληρώνεται.

Β.1.7. Πλαίσιο αναφορικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα για ερευνητικούς σκοπούς

Η έρευνα έχει προνομιακή θέση στον ΓΚΠΔ. Για τον λόγο αυτό υπάρχουν αρκετές παρεκκλίσεις και εξαιρέσεις αναφορικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα για ερευνητικούς σκοπούς. Οι εν λόγω εξαιρέσεις δεν ισχύουν κατά γενικό κανόνα, αλλά κάθε φορά εξετάζεται, κατά περίπτωση, κατά πόσο δύνανται να εφαρμοστούν. Συγκεκριμένα, οι παρεκκλίσεις και οι εξαιρέσεις που αφορούν στην επεξεργασία δεδομένων για ερευνητικούς σκοπούς, ισχύουν μόνο όταν:

- Η επεξεργασία υπόκειται σε κατάλληλες τεχνικές και οργανωτικές εγγυήσεις σχετικά με την προστασία των δεδομένων, όπως η αρχή της ελαχιστοποίησης, η ψευδωνυμοποίηση, ο έλεγχος λογικής πρόσβασης.

- Η επεξεργασία δεν πρόκειται να οδηγήσει σε λήψη μέτρων ή αποφάσεων που θα επηρεάσουν τα φυσικά πρόσωπα.

- Η επεξεργασία δεν δύναται να προκαλέσει κάποια σημαντική βλάβη ή κίνδυνο για το Υποκείμενο των Δεδομένων.

- Η εφαρμογή των προβλεπόμενων από τον ΓΚΠΔ απαιτήσεων ενδέχεται να καταστήσει αδύνατη ή να βλάψει σε μεγάλο βαθμό την επίτευξη των σκοπών της έρευνας.

Οι εξαιρέσεις σχετικά με την επιστημονική έρευνα αφορούν τις παρακάτω θεματικές ενότητες του ΓΚΠΔ.

Περιορισμός του σκοπού: Η περαιτέρω επεξεργασία δεδομένων προσωπικού χαρακτήρα για σκοπούς επιστημονικής έρευνας δεν θεωρείται ασύμβατη με τους σκοπούς για τους οποίους αρχικά συλλέχθηκαν τα δεδομένα. Επομένως τα δεδομένα προσωπικού χαρακτήρα που έχουν συλλεχθεί από το Πανεπιστήμιο μπορούν να χρησιμοποιηθούν και για ερευνητικούς σκοπούς, εφόσον παρέχονται κατάλληλες εγγυήσεις για τα δικαιώματα και τις ελευθερίες των Υποκειμένων των Δεδομένων.

Περιορισμός της περιόδου αποθήκευσης: Τα δεδομένα προσωπικού χαρακτήρα που χρησιμοποιούνται για ερευνητικούς σκοπούς απαλλάσσονται από την απαίτηση του ΓΚΠΔ αναφορικά με την τήρησή τους μόνο για το χρονικό διάστημα που είναι αναγκαίο για την εκπλήρωση του σκοπού της επεξεργασίας ή από τον νόμο. Επομένως, τα δεδομένα μπορούν να αποθηκεύονται για μεγαλύτερες χρονικές περιόδους, εφόσον υποβάλλονται σε επεξεργασία για σκοπούς επιστημονικής έρευνας και εφαρμόζονται κατάλληλα μέτρα και εγγυήσεις για τη διασφάλιση των δικαιωμάτων και ελευθεριών των Υποκειμένων.

Επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα: Η επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα, δηλαδή των δεδομένων των Άρθρων 9 και 10 του ΓΚΠΔ, είναι κατ' εξαίρεση δυνατή για ερευνητικούς σκοπούς, οι οποίοι είναι ανάλογοι με τον επιδιωκόμενο σκοπό και σέβονται το κατοχυρωμένο από το Σύνταγμα δικαίωμα στην προστασία των δεδομένων.

Διαφανής ενημέρωση του υποκειμένου των δεδομένων: Οι παρεκκλίσεις του ΓΚΠΔ που αφορούν τη διαφανή ενημέρωση είναι δύο.

Η πρώτη αφορά στην περίπτωση που τα δεδομένα που έχουν συλλεγεί από το ίδιο το Υποκείμενο και πρόκειται να χρησιμοποιηθούν για κάποιον άλλο σκοπό από εκείνον για τον οποίο αρχικά συλλέχθηκαν. Όταν ο νέος σκοπός επεξεργασίας αφορά σκοπούς επιστημονικής έρευνας, τότε υπάρχει μία ελαστικότητα σχετικά με τη διαφανή ενημέρωση του σκοπού της επεξεργασίας και το Υποκείμενο μπορεί να συγκατατεθεί είτε στον ερευνητικό σκοπό με γενικότερο τρόπο είτε μόνο για συγκεκριμένους τομείς / στάδια της επιστημονικής έρευνας. Αυτό συμβαίνει διότι τις περισσότερες φορές είναι αρκετά δύσκολο να προσδιοριστεί από την αρχή, πλήρως, ο σκοπός της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα για τους σκοπούς της επιστημονικής έρευνας.

Η δεύτερη παρέκκλιση αφορά στην περίπτωση όπου τα δεδομένα προσωπικού χαρακτήρα του Υποκειμένου έχουν συλλεγεί μέσω κάποιου άλλου (π.χ. δημόσια πηγή, άλλη δημόσια αρχή) και όχι από το ίδιο το Υποκείμενο των Δεδομένων. Στη συγκεκριμένη περίπτωση, ο ερευνητής / η ερευνήτρια δεν υποχρεούται από τον Κανονισμό να ενημερώσει τα Υποκείμενα των Δεδομένων όταν η ενέργεια αυτή αποδεικνύεται αδύνατη ή απαιτεί δυσανάλογες προσπάθειες, καθώς και όταν η εν λόγω ενημέρωση ενδέχεται να καταστήσει αδύνατη ή να βλάψει σε μεγάλο βαθμό την επίτευξη των σκοπών της έρευνας. Πάρα ταύτα, οι απαιτούμενες πληροφορίες πρέπει να είναι διαθέσιμες στο κοινό και ο ερευνητής / η ερευνήτρια οφείλει να λαμβάνει κατάλληλα μέτρα για την προστασία των δεδομένων των Υποκειμένων.

Δικαιώματα των Υποκειμένων των Δεδομένων: Όταν η επεξεργασία των δεδομένων προσωπικού χαρακτήρα εκτελείται για ερευνητικούς σκοπούς, ο ΓΚΠΔ παρέχει τη δυνατότητα στα κράτη μέλη της Ε.Ε. να προβλέπουν παρεκκλίσεις από τα δικαιώματα που μπορούν να ασκήσουν τα Υποκείμενα των Δεδομένων. Συγκεκριμένα, οι εν λόγω παρεκκλίσεις δύναται να αφορούν το δικαίωμα πρόσβασης, το δικαίωμα διόρθωσης, το δικαίωμα του περιορισμού της επεξεργασίας και το δικαίωμα εναντίωσης. Οι παρεκκλίσεις είναι εφαρμόσιμες μόνο εάν τα εν λόγω δικαιώματα μπορεί να καταστήσουν αδύνατη την επιστημονική έρευνα ή να παρεμποδίσουν την επίτευξη των σκοπών της. Επιπροσθέτως, ο ΓΚΠΔ ρητώς αναφέρει ότι σε περίπτωση που η επεξεργασία των δεδομένων είναι απαραίτητη για σκοπούς επιστημονικής έρευνας το δικαίωμα της διαγραφής δεν είναι ικανοποιήσιμο.

Στόχος του παρόντος πλαισίου είναι να διασφαλίσει ότι η επεξεργασία των δεδομένων προσωπικού χαρακτήρα για ερευνητικές δραστηριότητες γίνεται σύμφωνα με τα όσα ορίζονται στον ΓΚΠΔ. Στο έγγραφο αυτό αναλύονται οι ενέργειες που πρέπει να γίνονται κάθε φορά, σε περίπτωση που στο πλαίσιο κάποιας επιστημονικής έρευνας του Πανεπιστημίου χρησιμοποιούνται δεδομένα προσωπικού χαρακτήρα. Επιπλέον, μέσω αυτού παρέχεται εκτενής καθοδήγηση στους ερευνητές του Πανεπιστημίου Αιγαίου σχετικά με τις υποχρεώσεις τους πριν, κατά τη διάρκεια, και μετά το πέρας της επιστημονικής τους έρευνας.

Β.1.7.1 Οδηγίες για τους ερευνητές αναφορικά με την προστασία δεδομένων προσωπικού χαρακτήρα

Οι παρακάτω οδηγίες πρέπει να εφαρμόζονται από οποιονδήποτε σκοπεύει να πραγματοποιήσει κάποια επιστημονική έρευνα, η οποία πρόκειται να περιλαμβάνει συλλογή και κατ' επέκταση επεξεργασία δεδομένων προσωπικού χαρακτήρα. Οι οδηγίες αποτελούνται από εννέα (9) βήματα που πρέπει να γίνονται πριν ξεκινήσει ένας ερευνητής / μία ερευνήτρια μία τέτοια έρευνα.

Βήμα 1: Προσδιορισμός του σκοπού ή των σκοπών επεξεργασίας

Αρχικά, ο ερευνητής / η ερευνήτρια πρέπει να εντοπίσει και να προσδιορίσει τον σκοπό ή τους σκοπούς της επεξεργασίας των δεδομένων στο πλαίσιο της επιστημονικής έρευνας. Καθότι αρκετές φορές είναι αρκετά δύσκολο να προσδιοριστούν εξαρχής οι εν λόγω σκοποί, ο ερευνητής / η ερευνήτρια πρέπει, τουλάχιστον, να περιγράφει σε γενικότερο επίπεδο τον σκοπό της έρευνας.

Βήμα 2: Δυνατότητα χρήσης ανωνυμοποιημένων δεδομένων στην έρευνα

Ο ερευνητής / Η ερευνήτρια πρέπει να εξακριβώσει εάν για την εκπλήρωση της επιστημονικής του έρευνας χρειάζεται να γνωρίζει την ταυτότητα των συμμετεχόντων φυσικών προσώπων. Σε περίπτωση που η έρευνα μπορεί να πραγματοποιηθεί με την επεξεργασία ανωνυμοποιημένων δεδομένων, τότε η εκπλήρωση των σκοπών της πρέπει να γίνεται κατ' αυτόν τον τρόπο.

Στη νομοθεσία περί προστασίας δεδομένων προσωπικού χαρακτήρα, ανωνυμοποιημένα νοούνται τα δεδομένα εκείνα που δεν μπορούν αντιστοιχηθούν, από κανέναν, σε κάποιο συμμετέχοντα στην έρευνα. Επομένως, όταν τα δεδομένα είναι ανωνυμοποιημένα το φυσικό πρόσωπο που το αφορούν δεν μπορεί να ταυτοποιηθεί ούτε από τον υπεύθυνο ερευνητή, ούτε από κάποιον άλλο που εργάζεται χρησιμοποιώντας αυτά τα δεδομένα, ούτε κάποιον τρίτον στον οποίο ενδέχεται να ανήκει το εργαλείο που χρησιμοποιείται για τη συλλογή των δεδομένων, ούτε από κάποιον στον οποίο ενδέχεται να αποσταλούν τα δεδομένα.

Σημειώνεται ότι η επεξεργασία ανωνυμοποιημένων δεδομένων δεν εντάσσεται στο πεδίο εφαρμογής του ΓΚΠΔ και σε αυτή την περίπτωση δεν απαιτείται ο ερευνητής / η ερευνήτρια να ακολουθήσει τα υπόλοιπα βήματα του παρόντος εγγράφου.

Βήμα 3: Προσδιορισμός της νομικής βάσης

Σύμφωνα με τον ΓΚΠΔ, για να είναι σύννομη μία επεξεργασία δεδομένων προσωπικού χαρακτήρα, πρέπει να βασίζεται σε μία από τις νομικές βάσεις του Άρθρου 6.1. Η επεξεργασία δεδομένων από το Πανεπιστήμιο, το οποίο αποτελεί δημόσια αρχή, για σκοπούς επιστημονικής έρευνας δύναται να βασίζεται είτε στη συγκατάθεση του Υποκειμένου είτε στην εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί σε αυτό.

Πιο συγκεκριμένα, τα δεδομένα μπορούν να επεξεργαστούν για ερευνητικούς σκοπούς όταν:

- το Υποκείμενο έχει δώσει τη συγκατάθεσή του,

- το Υποκείμενο έχει ήδη συγκατατεθεί από κάποια προηγούμενη έρευνα στην περαιτέρω χρήση των δεδομένων του ή στη χρήση τους για παρεμφερείς σκοπούς,

- τα δεδομένα προσωπικού χαρακτήρα που αφορούν στο Υποκείμενο προέρχονται από κάποια δημόσια προσβάσιμη πηγή,

- η επεξεργασία είναι απαραίτητη για τους σκοπούς της έρευνας και ο ερευνητής / η ερευνήτρια μπορεί να αποδείξει ότι οι σκοποί της επιστημονικής έρευνας υπερισχύουν των συμφερόντων και των δικαιωμάτων του Υποκειμένου των Δεδομένων.

Ωστόσο, είναι σημαντικό να σημειωθεί ότι η συγκατάθεση των Υποκειμένων ως νομική βάση της επεξεργασίας για ερευνητικούς σκοπούς δεν προτείνεται και πρέπει να αποτελεί την τελευταία επιλογή του ερευνητή, καθώς κάθε έρευνα που βασίζεται στη συγκατάθεση υπόκειται σε πρόσθετες απαιτήσεις βάσει του ΓΚΠΔ (π.χ. ανάκληση της συγκατάθεσης), οι οποίες ενδέχεται να έχουν ζημιογόνο αντίκτυπο στην έρευνα.

Επιπροσθέτως, όταν τα δεδομένα προσωπικού χαρακτήρα ανήκουν σε ειδική κατηγορία δεδομένων (Άρθρα 9 και 10 του ΓΚΠΔ), ο σκοπός της έρευνας πρέπει να είναι ανάλογος του πρόσθετου κινδύνου που συνεπάγεται η επεξεργασία τέτοιου είδους δεδομένων προσωπικού χαρακτήρα.

Σημείωση:

Σε περίπτωση που η επεξεργασία για τους σκοπούς της επιστημονικής έρευνας αφορά ειδική κατηγορία δεδομένων, τότε το Πανεπιστήμιο μπορεί να ορίσει ΥΠΔ μόνο για τις ανάγκες της εν λόγω έρευνας και για όσο χρονικό διάστημα αυτή διαρκέσει.

Βήμα 4: Διασφάλιση των κατάλληλων εγγυήσεων

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα για ερευνητικούς σκοπούς πρέπει, βάσει του ΓΚΠΔ, να υπόκειται σε κατάλληλες εγγυήσεις για τα δικαιώματα και τις ελευθερίες των Υποκειμένων των Δεδομένων. Οι εν λόγω εγγυήσεις θα πρέπει να διασφαλίζουν ότι έχουν υλοποιηθεί από τον ερευνητή ποικίλα αποτελεσματικά τεχνικά και οργανωτικά μέτρα. Εκτενής καταγραφή των μέτρων αυτών γίνεται στο παρόν πλαίσιο (Πίνακας 14).

Ωστόσο, προκειμένου να χρησιμοποιηθούν τα δεδομένα προσωπικού χαρακτήρα για τους σκοπούς της έρευνας, πρέπει να εφαρμοστούν οπωσδήποτε μέτρα τα οποία θα εξασφαλίζουν την αρχή της «ελαχιστοποίησης των δεδομένων». Πιο αναλυτικά, ο ερευνητής / η ερευνήτρια πρέπει να μεριμνά για τα ακόλουθα:

i. **Τι δεδομένα προσωπικού χαρακτήρα πραγματικά χρειάζεται.**

   Ο ερευνητής / Η ερευνήτρια πρέπει να συλλέγει και να επεξεργάζεται μόνο τα δεδομένα εκείνα που είναι αναγκαία και συναφή προς τους ειδικούς σκοπούς της εκάστοτε επιστημονικής έρευνας. Επιπλέον, πριν τη συλλογή των δεδομένων, πρέπει να λαμβάνει υπόψη τη φύση και τους σκοπούς της έρευνας προκειμένου να αξιολογήσει κατά πόσον απαιτούνται γενικές πληροφορίες ή συγκεκριμένα δεδομένα για την εκπλήρωσή τους. Για παράδειγμα, εάν η επιστημονική έρευνα μπορεί να εκπληρωθεί μόνο με το έτος γέννησης ή

την ηλικία των συμμετεχόντων, ο ερευνητής / η ερευνήτρια δεν χρειάζεται να γνωρίζει την πλήρη ημερομηνία γέννησής τους.

ii. **Τη δυνατότητα ψευδωνυμοποίησης των δεδομένων.**

Ο ερευνητής / Η ερευνήτρια πρέπει να εφαρμόσει μέτρα που περιλαμβάνουν τη χρήση ψευδωνύμων (ψευδωνυμοποίηση), εφόσον οι σκοποί της έρευνας μπορούν να εκπληρωθούν κατ' αυτόν τον τρόπο. Τα ψευδώνυμα πρέπει να τηρούνται σε ξεχωριστό φυσικό ή ηλεκτρονικό αρχείο από τα δεδομένα προσωπικού χαρακτήρα, στο οποίο θα έχουν δικαίωμα πρόσβασης μόνο εξουσιοδοτημένα άτομα της ερευνητικής ομάδας. Με αυτόν τον τρόπο, το Πανεπιστήμιο μπορεί να ελαχιστοποιήσει τον ενδεχόμενο κίνδυνο διαρροής πληροφορίας και ταυτοποίησης των συμμετεχόντων φυσικών προσώπων από συνεργαζόμενα τρίτα μέρη, καθώς και από οποιονδήποτε άλλο δεν έχει πρόσβαση στο αρχείο με τα δεδομένα προσωπικού χαρακτήρα.

iii. **Ποιος θα έχει πρόσβαση στα δεδομένα.**

Το Πανεπιστήμιο πρέπει να εξασφαλίζει ότι πρόσβαση στα δεδομένα προσωπικού χαρακτήρα, όπως και στα ψευδώνυμα, των συμμετεχόντων έχουν μόνο όσοι είναι αναγκαίο να τα γνωρίζουν. Για παράδειγμα, αρκετές φορές προκειμένου να εκπληρωθούν οι σκοποί της εκάστοτε έρευνας δεν χρειάζεται όλα τα μέλη της ερευνητικής ομάδας να γνωρίζουν την ταυτότητα των συμμετεχόντων. Αντίστοιχα, τα δεδομένα προσωπικού χαρακτήρα πρέπει να αποστέλλονται μόνο στα τρίτα μέρη που είναι απαραίτητα για τις ανάγκες της έρευνας.

Βήμα 5: Αναγνώριση των εμπλεκόμενων τρίτων μερών

Πριν την έναρξη της επιστημονικής έρευνας πρέπει να εντοπιστούν όλα τα εμπλεκόμενα μέρη. Πιο συγκεκριμένα:

- Σε περίπτωση που τον σκοπό και τον τρόπο με τον οποίο θα διεξαχθεί η επιστημονική έρευνα, τους καθορίζει το προσωπικό του Πανεπιστημίου Αιγαίου (καθηγητές και καθηγήτριες, ερευνητές και ερευνήτριες κ.λπ.) ή οι φοιτητές και φοιτήτριες που εργάζονται υπό την καθοδήγησή τους, τότε υπεύθυνος επεξεργασίας είναι το Πανεπιστήμιο.

- Σε περίπτωση που τον σκοπό ή / και τον τρόπο διεξαγωγής της έρευνας δύναται να τον καθορίσουν και άλλοι συνεργάτες, τότε το Πανεπιστήμιο και οι εν λόγω συνεργάτες ερευνητές και ερευνήτριες δρουν ως από κοινού Υπεύθυνοι Επεξεργασίας.

- Σε περίπτωση που συνεργάτες ερευνητές και ερευνήτριες επεξεργάζονται δεδομένα προσωπικού χαρακτήρα συμμετεχόντων στην έρευνα υπό την καθοδήγηση και υπό τις εντολές του προσωπικού ή των φοιτητών και φοιτητριών του Πανεπιστημίου Αιγαίου, τότε οι συνεργάτες ερευνητές και ερευνήτριες δρουν ως Εκτελούντες την Επεξεργασία. Επιπλέον, οποιοσδήποτε άλλος (φυσικό ή νομικό πρόσωπο) επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του Πανεπιστημίου, είναι Εκτελών την Επεξεργασία. Ενδεικτικά παραδείγματα αποτελούν οργανισμοί οι οποίοι ενδέχεται να συλλέγουν τα δεδομένα των συμμετεχόντων για λογαριασμό του Πανεπιστημίου ή φορείς που ενδέχεται να παρέχουν στο Πανεπιστήμιο κάποιο διαδικτυακό εργαλείο για έρευνα (online survey tool).

Για οποιαδήποτε από τις ανωτέρω περιπτώσεις, όπου τα δεδομένα γνωστοποιούνται ή επεξεργάζονται από εμπλεκόμενα στην έρευνα τρίτα μέρη, το Πανεπιστήμιο πρέπει να καλύπτεται από σύμβαση στην οποία θα ορίζονται οι υποχρεώσεις του εκάστοτε συνεργαζόμενου τρίτου (από κοινού Υπεύθυνος Επεξεργασίας, Εκτελών την Επεξεργασία) σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα. Για τον λόγο αυτό, ο υπεύθυνος ερευνητής ή ερευνήτρια πρέπει να ζητάει τη γνώμη του ΥΠΔ σχετικά με τον τρίτο με τον οποίο επιθυμεί να συνεργαστεί, ώστε να τον διαβεβαιώσει ότι πληροί τα απαιτούμενα κριτήρια αναφορικά με την προστασία και την ασφάλεια των δεδομένων. Επιπλέον, ο ερευνητής και η ερευνήτρια πρέπει, κάθε φορά, να ζητά την αρωγή του Νομικού Συμβούλου του Ειδικού Λογαριασμού Κονδυλίων Έρευνας του Πανεπιστημίου προκειμένου να καταρτιστεί η εκάστοτε σύμβαση.

Βήμα 6: Απόφαση για τη διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων

Προτού αρχίσει η έρευνα, ο ερευνητής / η ερευνήτρια πρέπει να αξιολογήσει κατά πόσο η επεξεργασία των δεδομένων προσωπικού χαρακτήρα ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των Υποκειμένων.

Συγκεκριμένα, τα μέλη της ερευνητικής ομάδας πρέπει να αξιολογήσουν κατά πόσο η επεξεργασία εμπεριέχεται στον κατάλογο της Αρχής (ΑΠΔΠΧ) με τα είδη των πράξεων επεξεργασίας που υπόκεινται στην απαίτηση για διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων (εφεξής «ΕΑΠΔ»). Σε περίπτωση που η επεξεργασία δεν ανήκει στον ανωτέρω κατάλογο, πρέπει, στη συνέχεια, ο ερευνητής / η ερευνήτρια να ελέγξει εάν πληροί κάποια από τα παρακάτω κριτήρια:

- Αξιολόγηση ή βαθμολόγηση, μεταξύ άλλων και της κατάρτισης προφίλ φυσικών προσώπων.
- Λήψη αυτοματοποιημένων αποφάσεων που παράγουν έννομα αποτελέσματα σχετικά με το φυσικό πρόσωπο ή αποτελέσματα που το επηρεάζουν σημαντικά κατ' ανάλογο τρόπο.
- Η επεξεργασία «εμποδίζει τα Υποκείμενα των Δεδομένων να ασκήσουν κάποιο δικαίωμα ή να χρησιμοποιήσουν μία υπηρεσία ή σύμβαση».
- Συστηματική παρακολούθηση των Υποκειμένων των Δεδομένων, συμπεριλαμβανομένης της παρακολούθησης μέσω δικτύων και της «συστηματικής παρακολούθησης δημοσίως προσβάσιμου χώρου».
- Επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα (Άρθρο 9 ΓΚΠΔ) ή / και δεδομένων προσωπικού χαρακτήρα που αφορούν σε ποινικές καταδίκες ή αδικήματα (Άρθρο 10 ΓΚΠΔ).
- Επεξεργασία δεδομένων που αφορούν ευάλωτα φυσικά πρόσωπα, όπως παιδιά, εργαζόμενοι, ΑμεΑ, κ.λπ.
- Αντιστοίχιση ή συνδυασμός δύο ή περισσότερων διαφορετικών συνόλων δεδομένων.
- Μεγάλης κλίμακας επεξεργασία δεδομένων προσωπικού χαρακτήρα.

- Καινοτόμος χρήση ή εφαρμογή νέων τεχνολογικών ή οργανωτικών λύσεων, όπως το «διαδίκτυο των πραγμάτων» (Internet of Things), βιομετρικές τεχνολογίες κ.λπ.

Εάν η επεξεργασία είναι μία από αυτές του καταλόγου της ΑΠΔΠΧ ή εάν πληρούνται τουλάχιστον δύο από τα ανωτέρω κριτήρια, τότε απαιτείται η διενέργεια ΕΑΠΔ. Ο υπεύθυνος ερευνητής / ερευνήτρια πρέπει να ενημερώσει τον ΥΠΔ του Πανεπιστημίου αναφορικά με την ανάγκη της ΕΑΠΔ, προκειμένου ο τελευταίος να συμμετέχει εποπτικά στην εν λόγω διεργασία.

Βήμα 7: Υλοποίηση επιπλέον τεχνικών και οργανωτικών μέτρων

Είναι ζωτικής σημασίας για το Πανεπιστήμιο τα δεδομένα της έρευνας που αφορούν σε δεδομένα προσωπικού χαρακτήρα να συλλέγονται, να τηρούνται, να διαβιβάζονται και να καταστρέφονται με ασφάλεια. Για τον λόγο αυτό, η εκάστοτε ερευνητική ομάδα του Πανεπιστημίου, είτε επειδή εντοπίστηκε η ανάγκη πρόσθετων μέτρων για τον μετριασμό των κινδύνων που αναγνωρίστηκαν στην ΕΑΠΔ, είτε επειδή κρίνει ότι απαιτείται η λήψη μέτρων προστασίας, εφαρμόζει τα απαραίτητα, κάθε φορά, τεχνικά και οργανωτικά μέτρα.

Ειδικότερα, προκειμένου να προστατεύονται τα δικαιώματα και οι ελευθερίες των Υποκειμένων, αλλά και τα δεδομένα προσωπικού χαρακτήρα που αφορούν σε αυτά από μη εξουσιοδοτημένη πρόσβαση/χρήση, από μη εξουσιοδοτημένη τροποποίηση, από τυχαία ή μη απώλεια, καταστροφή ή βλάβη, εφαρμόζεται από την ερευνητική ομάδα ένα εύρος τεχνικών και οργανωτικών μέτρων προστασίας (Πίνακας 14).

ΕΝΔΕΙΚΤΙΚΑ ΤΕΧΝΙΚΑ ΚΑΙ ΟΡΓΑΝΩΤΙΚΑ ΜΕΤΡΑ
Οργανωτικά μέτρα
• Σχεδιασμός και εφαρμογή πλαισίου αναφορικά με την προστασία δεδομένων προσωπικού χαρακτήρα (πολιτικές, διαδικασίες, οδηγίες) αναφορικά με: o τις βασικές αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα, o τη διαχείριση των αιτημάτων των Υποκειμένων σχετικά με τα δικαιώματά τους, o τη λήψη και τη διαχείριση της συγκατάθεσης των Υποκειμένων, o τη συντήρηση του αρχείου δραστηριοτήτων επεξεργασίας, o τη διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία των δεδομένων, o τη διαβίβαση των δεδομένων σε χώρες εκτός Ε.Ο.Χ, o την προστασία δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού, o τη γνωστοποίηση και την αντιμετώπιση παραβιάσεων δεδομένων προσωπικού χαρακτήρα κ.λπ.
• Προσδιορισμός του χρόνου τήρησης των δεδομένων προσωπικού χαρακτήρα και εφαρμογή διαδικασίας αναφορικά με την ασφαλή καταστροφή των δεδομένων, τόσο σε έγχαρτη όσο και σε ηλεκτρονική μορφή.
• Προσδιορισμός της νομικής βάσης των πράξεων επεξεργασίας.

ΕΝΔΕΙΚΤΙΚΑ ΤΕΧΝΙΚΑ ΚΑΙ ΟΡΓΑΝΩΤΙΚΑ ΜΕΤΡΑ
• Έλεγχος της αναγκαιότητας κάθε προσωπικού δεδομένου που συλλέγεται από ηλεκτρονικές φόρμες, αιτήσεις ή λοιπά έντυπα του Πανεπιστημίου.
• Ανάπτυξη υλικού και υλοποίηση προγραμμάτων εκπαίδευσης και ευαισθητοποίησης σχετικά με την προστασία δεδομένων προσωπικού χαρακτήρα.
• Εφαρμογή διαδικασίας αναφορικά με τη διαχείριση των κινδύνων ασφάλειας πληροφοριών.
• Εφαρμογή ενός πλαισίου για τη διαβάθμιση των πληροφοριών (π.χ. εσωτερικής χρήσης, εμπιστευτικό, απόρρητο).
• Περιορισμός προσβάσεων στα δεδομένα προσωπικού χαρακτήρα βάσει ρόλων και αρμοδιοτήτων.
• Εφαρμογή αυστηρής πολιτικής σχετικά με τους κωδικούς πρόσβασης.
Τεχνικά μέτρα
• Μηχανισμοί που αφορούν την ικανοποίηση νομικών υποχρεώσεων του Πανεπιστημίου, όπως εφαρμογή για τη διαχείριση αιτημάτων και συγκαταθέσεων υποκειμένων.
• Μηχανισμοί ανάθεσης συγκεκριμένης περιόδου τήρησης σε κάθε δεδομένο (π.χ. μέσω μεταδεδομένων) και αυτόματης διαγραφής δεδομένων των οποίων έχει παρέλθει η καθορισμένη περίοδος τήρησής τους.
• Έλεγχος λογικής πρόσβασης σε φακέλους, αρχεία, βάσεις, συστήματα, εφαρμογές που περιέχουν δεδομένα προσωπικού χαρακτήρα.
• Μηχανισμοί επαλήθευσης στοιχείων και εξουσιοδότησης χρηστών.
• Μηχανισμοί για αποτροπή ταυτοποίησης ή αναγνώρισης του Υποκειμένου των Δεδομένων (π.χ. ανωνυμοποίηση, ψευδωνυμοποίηση, masking)
• Κρυπτογράφηση των δεδομένων προσωπικού χαρακτήρα που είναι αποθηκευμένα στα συστήματα / βάσεις του Πανεπιστημίου, ειδικά εάν αυτά ανήκουν σε ειδική κατηγορία.
• Κρυπτογράφηση των ψηφιακών καναλιών επικοινωνίας, ώστε να διαβιβάζονται με ασφάλεια τα δεδομένα προσωπικού χαρακτήρα.
• Καταγραφή της δραστηριότητας στα συστήματα μέσω αρχείων καταγραφής ελέγχου (logs).
• Δημιουργία αντιγράφων ασφαλείας για τα δεδομένα που είναι αποθηκευμένα σε ηλεκτρονική μορφή.
• Αποθήκευση δεδομένων προσωπικού χαρακτήρα σε υπολογιστικό νέφος (cloud) υπό την προϋπόθεση ότι παρέχει αποδεκτό επίπεδο προστασίας για τα δεδομένα και έχει εγκριθεί από το Πανεπιστήμιο.

ΕΝΔΕΙΚΤΙΚΑ ΤΕΧΝΙΚΑ ΚΑΙ ΟΡΓΑΝΩΤΙΚΑ ΜΕΤΡΑ
• Ασφαλής αποθήκευση εγγράφων σε φυσική μορφή (π.χ. πυρασφαλείς χώροι, χώροι περιορισμένης πρόσβασης)
• Έλεγχος φυσικής πρόσβασης στους χώρους όπου τηρούνται δεδομένα προσωπικού χαρακτήρα (π.χ. ασφαλισμένοι χώροι και πόρτες, συνοδεία επισκεπτών)

Πίνακας 14: Ενδεικτικά μέτρα προστασίας

Ο υπεύθυνος ερευνητής / ερευνήτρια πρέπει να συμβουλεύεται τον ΥΠΔ ή / και τις λοιπές κατάλληλες Διευθύνσεις του Πανεπιστημίου σχετικά με τα μέτρα προστασίας που πρέπει ή επιθυμεί να λάβει. Για παράδειγμα, ο ερευνητής / η ερευνήτρια επικοινωνεί με τη Διεύθυνση Πληροφορικής και Επικοινωνιών για καθοδήγηση σχετικά με τις αποδεκτές από το Πανεπιστήμιο υπηρεσίες για αποθήκευση και διαβίβαση δεδομένων προσωπικού χαρακτήρα, καθώς και για βοήθεια σχετικά με τα δικαιώματα πρόσβασης και την κρυπτογράφηση. Επίσης, ο ερευνητής / η ερευνήτρια σε περίπτωση που χρειάζεται έναν ασφαλή χώρο για την αποθήκευση έγχαρτων εγγράφων δύναται να επικοινωνήσει με τη Διεύθυνση του Πανεπιστημίου που είναι αρμόδια για τη διαχείριση εγγράφων.

<u>Βήμα 8: Δημιουργία εντύπου ενημέρωσης σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και δήλωσης συγκατάθεσης</u>

Αφού γίνουν τα ανωτέρω βήματα, ο ερευνητής / η ερευνήτρια πρέπει να σχεδιάσει ένα έντυπο σχετικά με την επεξεργασία που διενεργείται στο πλαίσιο της έρευνας επί των δεδομένων προσωπικού χαρακτήρα. Το έντυπο ενημέρωσης θα πρέπει να διασφαλίζει ότι τα υποκείμενα των δεδομένων έχουν λάβει όλη την απαραίτητη πληροφορία σχετικά με την επεξεργασία των δεδομένων τους.

Ο **Πίνακας 15** παρουσιάζει πληροφορίες που πρέπει να γνωστοποιούνται στα υποκείμενα των δεδομένων, βάσει του ΓΚΠΔ (Άρθρα 13 και 14), αναλόγως εάν τα δεδομένα προσωπικού χαρακτήρα που τα αφορούν έχουν συλλεγεί απευθείας από εκείνα ή όχι.

Τι πρέπει να περιλαμβάνει το έντυπο της ενημέρωσης:	Όταν τα δεδομένα συλλέγονται απευθείας από το Υποκείμενο	Όταν τα δεδομένα <u>δεν</u> συλλέγονται απευθείας από το Υποκείμενο
Την ταυτότητα και τα στοιχεία επικοινωνίας του Υπευθύνου Επεξεργασίας και του ΥΠΔ.	✓	✓
Τη δραστηριότητα επεξεργασίας και τη νομική βάση αυτής.	✓	✓
Τον σκοπό ή τους σκοπούς της επεξεργασίας.	✓	✓

Τι πρέπει να περιλαμβάνει το έντυπο της ενημέρωσης:	Όταν τα δεδομένα συλλέγονται απευθείας από το Υποκείμενο	Όταν τα δεδομένα δεν συλλέγονται απευθείας από το Υποκείμενο
Τις κατηγορίες των δεδομένων προσωπικού χαρακτήρα.		✓
Τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων, εφόσον υπάρχουν.	✓	✓
Πληροφορίες σχετικά με τη διαβίβαση των δεδομένων σε τρίτη χώρα και τις κατάλληλες εγγυήσεις, εφόσον υφίστανται.	✓	✓
Το χρονικό διάστημα αποθήκευσης των δεδομένων ή τα κριτήρια που το καθορίζουν.	✓	✓
Πληροφορίες σχετικά με τα δικαιώματα του Υποκειμένου βάσει του ΓΚΠΔ.	✓	✓
Ενημέρωση σχετικά με την ύπαρξη του δικαιώματος ανάκλησης της συγκατάθεσής του οποτεδήποτε, εφόσον υφίσταται.	✓	✓
Ενημέρωση σχετικά με την ύπαρξη του δικαιώματος υποβολής καταγγελίας στην ΑΠΔΠΧ.	✓	✓
Την πηγή από την οποία προέρχονται τα δεδομένα προσωπικού χαρακτήρα και εάν τα δεδομένα προήλθαν από δημόσια προσβάσιμες πηγές.		✓
Την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ.	✓	✓

Πίνακας 15: Περιεχόμενο εντύπου ενημέρωσης

Επιπλέον, η ενημέρωση σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα πρέπει, βάσει των διεθνών προτύπων δεοντολογίας, να περιλαμβάνει γενικές πληροφορίες σχετικά με την επιστημονική έρευνα (π.χ. τίτλο, διάρκεια, αντικείμενο, κ.λπ.), διευκρινίσεις σχετικά με πιθανούς κινδύνους ή οφέλη που υπάρχουν ή δύναται να ανακύψουν από την έρευνα, καθώς και μία σαφή δήλωση ότι η συμμετοχή είναι εντελώς εθελοντική και ότι οι συμμετέχοντες μπορούν να αποχωρήσουν από την έρευνα, ανά πάσα στιγμή, χωρίς να επηρεαστούν.

Σε περίπτωση που η επεξεργασία βασίζεται στη συγκατάθεση των συμμετεχόντων στην έρευνα φυσικών προσώπων, ο ερευνητής / η ερευνήτρια πρέπει επιπλέον να σχεδιάσει τη δήλωση της συγκατάθεσης που θα δίδεται στους συμμετέχοντες, βάσει των απαιτήσεων του ΓΚΠΔ (βλ. Παράρτημα Γ.10 Έντυπο δήλωσης συγκατάθεσης για επιστημονική έρευνα) και των αναγνωρισμένων προτύπων δεοντολογίας για την επιστημονική έρευνα (Παράρτημα Γ.10: Έντυπο δήλωσης συγκατάθεσης για επιστημονική έρευνα).

Βήμα 9: Δημοσίευση έρευνας

Μετά το πέρας της έρευνας, σε περίπτωση που ο ερευνητής / η ερευνήτρια επιθυμεί να δημοσιεύσει δεδομένα προσωπικού χαρακτήρα που επεξεργάστηκε κατά την επιστημονική του έρευνα ή τα αποτελέσματά της, συμπεριλαμβανομένων δεδομένων που αφορούν στους συμμετέχοντες, πρέπει να έχει τη ρητή συγκατάθεση των Υποκειμένων. Για τον λόγο αυτό προτείνεται, σε κάθε περίπτωση, ο ερευνητής / η ερευνήτρια να δημιουργεί πριν την ολοκλήρωση της έρευνας μία ανωνυμοποιημένη έκδοση των δεδομένων προσωπικού χαρακτήρα, προκειμένου να μπορεί όποτε επιθυμεί να τα δημοσιεύσει.

Β.1.8. Εσωτερικές πολιτικές ιδιωτικότητας για την προστασία των προσωπικών δεδομένων

Β.1.8.1 Πολιτική «Αποδεκτής χρήσης πληροφοριακών συστημάτων»

Β.1.8.1.1 Σκοπός της Πολιτικής

Αποτελεσματική χρήση Πληροφοριακών Συστημάτων είναι αποτέλεσμα ομαδικής προσπάθειας που περιλαμβάνει τη συμμετοχή και υποστήριξη κάθε εργαζομένου και συνεργάτη του Πανεπιστημίου, οι οποίοι σχετίζονται με πληροφορίες ή Πληροφοριακά Συστήματα. Είναι αρμοδιότητα κάθε εργαζομένου που χρησιμοποιεί υπολογιστή να γνωρίζει τις οδηγίες (guidelines) και να συμμορφώνει τις δραστηριότητές του, σύμφωνα με αυτές.

Σκοπός αυτής της πολιτικής είναι να περιγράψει την αποδεκτή χρήση εξοπλισμού πληροφορικής στο Πανεπιστήμιο. Η πολιτική εφαρμόζεται προκειμένου να προστατευθούν οι εργαζόμενοι και το ίδιο το Πανεπιστήμιο από κάθε τυχαία ή σκόπιμη απειλή. Μη αποδεκτή χρήση των πληροφοριακών πόρων εκθέτει το Πανεπιστήμιο σε κινδύνους, όπως για παράδειγμα ιομορφικό λογισμικό. Αυτή η πολιτική ισχύει για τους εργαζομένους, τους συνεργάτες, τους συμβούλους, τους προσωρινά εργαζόμενους και άλλους υπαλλήλους στο Πανεπιστήμιο, συμπεριλαμβανομένου και όλου του προσωπικού που συνεργάζεται με τρίτους φορείς (third parties). Αυτή η πολιτική εφαρμόζεται σε όλο τον εξοπλισμό υπολογιστών και τηλεπικοινωνιών που ανήκει ή ενοικιάζει το Πανεπιστήμιο.

Β.1.8.1.2 Βασικές Αρχές της Πολιτικής

- **Χρήση και Ιδιοκτησία**
    - Η διαχείριση του δικτύου (network administration) του Πανεπιστημίου επιθυμεί να παρέχει ένα λογικό επίπεδο ιδιωτικότητας στους χρήστες των Πληροφοριακών Συστημάτων. Παρόλα αυτά, οι χρήστες θα πρέπει να είναι ευαισθητοποιημένοι στο γεγονός ότι τα δεδομένα που επεξεργάζονται τα Πληροφοριακά Συστήματα του οργανισμού παραμένουν υπό την ιδιοκτησία του Πανεπιστημίου.
    - Η Ομάδα Ασφάλειας προτείνει οποιαδήποτε πληροφορία, την οποία οι χρήστες θεωρούν ευαίσθητη ή ευπαθή, να κρυπτογραφείται.
- **Εμπιστευτικές Πληροφορίες**
    - Μερικά παραδείγματα εμπιστευτικών πληροφοριών, ενδεικτικά είναι: επιχειρησιακές στρατηγικές, εμπορικά μυστικά, προδιαγραφές, κατάλογοι πολιτών και δεδομένα έρευνας. Οι εργαζόμενοι θα πρέπει να λάβουν μέτρα ώστε να αποφύγουν μη εξουσιοδοτημένη πρόσβαση σε αυτές τις πληροφορίες.
    - Όλος ο εξοπλισμός θα πρέπει να ασφαλίζεται με μηχανισμό για αυτόματο κλείδωμα λογαριασμού χρήστη στα 10 λεπτά ή και λιγότερο, ή μέσω της διαδικασίας κλειδώματος (logging-off) όταν ο χρήστης δεν παρευρίσκεται κοντά στον εξοπλισμό.
- **Μη Αποδεκτή Χρήση**

Δραστηριότητες (activities) που είναι γενικά απαγορευμένες:

- **Χρήση Δικτύου και Συστημάτων**: Παραβιάσεις δικαιωμάτων οποιουδήποτε προσώπου, οργανισμού ή εταιρείας που προστατεύονται από δικαιώματα πνευματικής ιδιοκτησίας (copyright), εμπορικό απόρρητο (trade secret), δίπλωμα ευρεσιτεχνίας (patent) ή οποιαδήποτε άλλη πνευματική ιδιοκτησία ή παρόμοιους νόμους ή κανονισμούς, συμπεριλαμβανομένων, ενδεικτικά, της εγκατάστασης ή διανομής «πειρατικών» ή άλλων προϊόντων λογισμικού που δεν διαθέτουν κατάλληλη άδεια χρήσης (license) από το Πανεπιστήμιο.

- **Χρήση Ηλεκτρονικού Ταχυδρομείου και Τηλεπικοινωνιών**: Απαγορεύεται η αποστολή ανεπιθύμητων μηνυμάτων ηλεκτρονικού ταχυδρομείου, συμπεριλαμβανομένης της αποστολής μηνύματος ανεπιθύμητης αλληλογραφίας («junk mail») ή άλλου διαφημιστικού υλικού σε άτομα που δεν ζήτησαν συγκεκριμένα τέτοιο υλικό (spam email).

- **Ιστολόγια και Κοινωνικά Μέσα**: Οι εργαζόμενοι απαγορεύεται να αποκαλύπτουν σε οποιονδήποτε οργανισμό εμπιστευτικές πληροφορίες ή πληροφορίες σχετικά με την ιδιοκτησία, εμπορικά μυστικά ή οποιοδήποτε άλλο υλικό θεωρείται ευαίσθητο από το Πανεπιστήμιο, όταν ασχολούνται με ιστολόγια, αναρτούν άρθρα και στη γενικότερη επικοινωνία τους στα κοινωνικά δίκτυα.

Β.1.8.2 Πολιτική «Ασφάλεια ηλεκτρονικού ταχυδρομείου»

Β.1.8.2.1 Σκοπός της Πολιτικής

Το ηλεκτρονικό ταχυδρομείο (email) θεωρείται ως μία δημοφιλής, αλλά σταθερά μη ασφαλής μορφή επικοινωνίας. Επιπλέον, το ηλεκτρονικό ταχυδρομείο είναι ένας διαδεδομένος τρόπος που χρησιμοποιείται σε επιθέσεις κοινωνικής μηχανικής (social engineering) με σκοπό την εξάπλωση κακόβουλου λογισμικού (malware) και την απόκτηση πρόσβασης σε διαβαθμισμένες πληροφορίες.

Το ευρύ κοινό βλέπει κάθε μορφή επικοινωνίας που προέρχεται από το Πανεπιστήμιο ως επίσημη δήλωση (official statement) αυτής.

Ο σκοπός αυτής της πολιτικής είναι:

- Να προστατεύσει την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των πληροφοριών και να εξασφαλίσει ότι στις πληροφορίες μπορούν να έχουν πρόσβαση μόνο όσοι έχουν οριστεί στον σκοπό και έχουν εξουσιοδοτηθεί να το κάνουν.
- Να αποτρέψει τη μη εξουσιοδοτημένη ή ακούσια αποκάλυψη εμπιστευτικών πληροφοριών ενός οργανισμού.
- Να αποτρέψει ανεπιθύμητες επιπτώσεις στη δημόσια εικόνα του Πανεπιστημίου.
- Να διασφαλίσει τη σωστή τήρηση των πληροφοριών που ανταλλάσσονται.

Β.1.8.2.2 Βασικές Αρχές της Πολιτικής

- **Εφαρμογή Σήμανση των Μηνυμάτων**
  - Η σήμανση (marking) εμπιστευτικότητας όλων των ηλεκτρονικών μηνυμάτων είναι κρίσιμη για την εφαρμογή των κατάλληλων μέτρων ασφάλειας.
- **Ασφαλής Υποδομή Ηλεκτρονικού Ταχυδρομείου**
  - Η κατάλληλη διαμόρφωση των ρυθμίσεων ηλεκτρονικών μηνυμάτων (π.χ. αποκλεισμός εισερχομένων και εξερχόμενων μηνυμάτων ηλεκτρονικού ταχυδρομείου με προστατευτική σήμανση υψηλότερη από την ταξινόμηση του συστήματος λήψης μηνυμάτων) είναι απαραίτητη για να προστατεύσει από διαρροές δεδομένων ή από πιθανή παρακολούθηση ή έκθεση σε κίνδυνο πληροφοριών.
  - Η εφαρμογή ελέγχων ταυτοποίησης, όπως οι ψηφιακές υπογραφές, μπορούν να βοηθήσουν στην ανίχνευση πλαστογραφημένων μηνυμάτων ηλεκτρονικού ταχυδρομείου που ενδέχεται να περιέχουν κακόβουλο κώδικα σχεδιασμένο να θέτει σε κίνδυνο ένα δίκτυο.

- **Απαγορευμένη Χρήση**

  - Τα συστήματα ανταλλαγής μηνυμάτων ηλεκτρονικού ταχυδρομείου του Πανεπιστημίου δεν θα πρέπει να χρησιμοποιούνται για τη δημιουργία ή τη διανομή οποιουδήποτε ενοχλητικού ή προσβλητικού μηνύματος, συμπεριλαμβανομένων προσβλητικών σχολίων σχετικά με τη φυλή, το φύλο, το χρώμα των μαλλιών, τις αναπηρίες, την ηλικία, τον σεξουαλικό προσανατολισμό, την πορνογραφία, τις θρησκευτικές πεποιθήσεις και πρακτικές, τις πολιτικές πεποιθήσεις ή τις πεποιθήσεις εθνικής προέλευσης.

- **Προσωπική Χρήση**

  - Η εύλογη χρήση των πόρων του Πανεπιστημίου για προσωπική επικοινωνία είναι αποδεκτή, αλλά τα μηνύματα που δεν σχετίζονται με την εργασία πρέπει να αποθηκευτούν σε έναν ξεχωριστό φάκελο από αυτά που σχετίζονται με την εργασία.

  - Οι εργαζόμενοι του Πανεπιστημίου δεν πρέπει να προσδοκούν την τήρηση της ιδιωτικότητας τους, στον βαθμό που επιτρέπεται από τον νόμο, σε οτιδήποτε αποθηκεύουν, στέλνουν ή λαμβάνουν στα ηλεκτρονικά συστήματα μηνυμάτων του Πανεπιστημίου.

  - Το Πανεπιστήμιο μπορεί να παρακολουθεί μηνύματα χωρίς προηγούμενη ειδοποίηση.

  - Το Πανεπιστήμιο δεν είναι υποχρεωμένο να παρακολουθεί μηνύματα ηλεκτρονικού ταχυδρομείου.

  - Το Πανεπιστήμιο δεν παρέχει καμία εκπροσώπηση ή εγγύηση, ρητή ή σιωπηρή, όσον αφορά στην προστασία του απορρήτου των πληροφοριών που αποθηκεύονται, αποστέλλονται ή λαμβάνονται στα ηλεκτρονικά συστήματα μηνυμάτων του.

- **Κατάρτιση και Ευαισθητοποίηση**

  - Οι επιθέσεις κοινωνικής μηχανικής (π.χ. phishing ηλεκτρονική αλίευση) είναι μία από τις κοινές τεχνικές που χρησιμοποιούνται για την εξάπλωση κακόβουλου λογισμικού (malware). Οι χρήστες είναι η τελευταία γραμμή άμυνας για την εξασφάλιση ενός κατάλληλα προστατευμένου συστήματος ηλεκτρονικού ταχυδρομείου. Το Πανεπιστήμιο πρέπει να διασφαλίζει ότι οι χρήστες του γνωρίζουν την απειλή και είναι εκπαιδευμένοι σχετικά με τον τρόπο ανίχνευσης και αναφοράς ύποπτων μηνυμάτων ηλεκτρονικού ταχυδρομείου.

B.1.8.3 Πολιτική «Ασφάλεια φορητών συσκευών πληροφορικής»

B.1.8.3.1 Σκοπός της Πολιτικής

Η παρούσα πολιτική επιβάλλει ορισμένους ελέγχους ασφάλειας πληροφοριών σχετικά με φορητές συσκευές πληροφορικής.

Πολλοί εργαζόμενοι χρησιμοποιούν φορητές συσκευές που παρέχονται από το Πανεπιστήμιο για να εργάζονται τόσο μέσα, όσο και έξω από τους κτιριακούς χώρους. Ενώ οι φορητές υπολογιστικές συσκευές είναι αναμφίβολα βολικές, υπάρχουν αυξημένοι κίνδυνοι ασφάλειας σε σύγκριση με τον εξοπλισμό πληροφορικής που βρίσκεται σε σταθερό γραφείο ως αποτέλεσμα:

- Επιπρόσθετων αδυναμιών λόγω της φορητότητάς τους και του τρόπου μεταφοράς και χρήσης τους (π.χ. απώλεια, κλοπή, σωματική βλάβη, μειωμένες ευκαιρίες για την εφαρμογή ενημερωμένων εκδόσεων ασφαλείας και ενημερώσεων για ιούς).

- Επιπρόσθετων απειλών αν χρησιμοποιούνται σε δημόσιους χώρους, π.χ. ακούγονται ή χρησιμοποιούνται από άτομα που δεν έχουν εξουσιοδοτηθεί να έχουν πρόσβαση στις πληροφορίες, κακόβουλο λογισμικό (π.χ. ιός) μέσω φορητών μέσων ή αναξιόπιστων / μη ασφαλών δικτύων.

- Επιπρόσθετων επιπτώσεων όπως απώλειες ή κλοπές φορητών υπολογιστών και πρόσβαση σε πιστοποιητικά που ενδέχεται να επιτρέπουν μη εξουσιοδοτημένη απομακρυσμένη πρόσβαση στο δίκτυο δεδομένων του Πανεπιστημίου, ενώ τα φορητά αποθηκευτικά μέσα συνήθως φέρουν πληροφορίες που είναι τρέχουσες και ευαίσθητες.

B.1.8.3.2 Βασικές Αρχές της Πολιτικής

- **Προδιαγραφές Χρήσης**

  - Οι φορητές συσκευές θα πρέπει να προστατεύονται επαρκώς οπουδήποτε χρησιμοποιούνται ενώ μεταφέρονται ή αποθηκεύονται.

  - Οι φορητές συσκευές θα επιτρέπεται να εγκαταλείψουν τις εγκαταστάσεις του Πανεπιστημίου μόνο εφόσον προστατεύονται επαρκώς, π.χ. είναι ανθεκτικές και δεν μπορούν να αλλοιωθούν.

- **Προστασία**

  Οι φορητές συσκευές θα πρέπει:

  - Να προστατεύονται από απώλειες, κλοπές, ζημιές και μη εξουσιοδοτημένη πρόσβαση χωρίς να είναι προστατευμένες κατάλληλα, π.χ. χρησιμοποιώντας κλείδωμα, αποθήκευση σε ασφαλή χώρο ή τουλάχιστον απομακρυσμένες από κοινή θέα. Δεν πρέπει να παραμένουν χωρίς επιτήρηση σε δημόσιους χώρους, ξεκλείδωτα γραφεία, οχήματα, δωμάτια ξενοδοχείων, σπίτια κ.λπ.

  - Να προστατεύονται χρησιμοποιώντας προϊόντα ασφαλείας που έχουν εγκριθεί για τον σκοπό αυτό από τον υπεύθυνο ασφάλειας. Πρέπει να προστατεύονται από κακόβουλο

λογισμικό, μη εξουσιοδοτημένη πρόσβαση, μη εξουσιοδοτημένες αλλαγές διαμόρφωσης κ.λπ.

- Τα ευαίσθητα προσωπικά ή εμπιστευτικά δεδομένα που είναι αποθηκευμένα σε φορητές συσκευές και μέσα θα πρέπει να κρυπτογραφούνται χρησιμοποιώντας κατάλληλα προϊόντα και διαδικασίες που έχουν εγκριθεί από την Ομάδα Ασφάλειας Πληροφοριών.

- **Διαχείριση Φορητών Συσκευών**

  - Ο εξοπλισμός πληροφορικής του Πανεπιστημίου, συμπεριλαμβανομένων των φορητών συσκευών και μέσων, θα πρέπει να χρησιμοποιείται μόνο από εξουσιοδοτημένους χρήστες για νόμιμους επιχειρησιακούς σκοπούς.

  - Οι εργαζόμενοι δεν θα πρέπει να παρεμβαίνουν ή να απενεργοποιούν τους ελέγχους ασφαλείας σε συσκευές πληροφορικής του Πανεπιστημίου, συμπεριλαμβανομένων φορητών συσκευών και μέσων.

- **Τερματισμός Χρήσης**

  - Τα πληροφοριακά αγαθά του Πανεπιστημίου, συμπεριλαμβανομένων των φορητών συσκευών και μέσων, πριν μεταβιβαστούν ή διατεθούν σε άλλους χρήστες, θα πρέπει να υπάρχει μέριμνα ώστε οι πληροφορίες που απομένουν να καταστραφούν φυσικά ή να διαγραφούν με ασφάλεια χρησιμοποιώντας διαδικασίες που έχουν εγκριθεί για τον σκοπό αυτό από την Ομάδα Ασφάλειας Πληροφοριών.

- **Διαχείριση Περιστατικών**

  - Οι εργαζόμενοι θα πρέπει να αναφέρουν τα περιστατικά ασφάλειας, συμπεριλαμβανομένων εκείνων που αφορούν φορητά πληροφοριακά αγαθά.

Β.1.8.4 Πολιτική «Bring your Own Device (BYOD)»

Β.1.8.4.1 Σκοπός της Πολιτικής

Οι εξουσιοδοτημένοι εργαζόμενοι και τρίτοι φορείς (third parties) ενδέχεται να θέλουν να χρησιμοποιήσουν τις προσωπικές τους συσκευές (Personal Owned Devices – PODs) για λόγους εργασίας, π.χ. χρησιμοποιώντας τη δική τους υπολογιστική συσκευή για πρόσβαση, ανάγνωση και απάντηση σε μηνύματα ηλεκτρονικού ταχυδρομείου εργασίας ή για εργασία από το σπίτι.

Η πολιτική «Bring Your Own Device (BYOD)» συνδέεται με αρκετούς κινδύνους ασφάλειας πληροφοριών, όπως:

1. Απώλεια, αποκάλυψη ή αλλοίωση των δεδομένων του οργανισμού που βρίσκονται αποθηκευμένα στις προσωπικές φορητές συσκευές.

2. Περιστατικά που περιλαμβάνουν απειλές ή παραβιάσεις της υποδομής των Τεχνολογιών Πληροφορικής και Επικοινωνιών του Πανεπιστημίου και άλλων πληροφοριακών αγαθών (π.χ. malware ή hacking).

3. Μη συμμόρφωση με τους ισχύοντες νόμους, κανονισμούς και υποχρεώσεις (π.χ. ιδιωτικότητα ή πειρατεία).

Μία πολιτική «Bring Your Own Device (BYOD)» επιτρέπει ή ενθαρρύνει τους εργαζομένους να χρησιμοποιούν τις προσωπικές τους φορητές συσκευές, υπό προϋποθέσεις. Υπάρχουν τέσσερις βασικές επιλογές:

1. Απεριόριστη πρόσβαση προσωπικών φορητών συσκευών.

2. Πρόσβαση μόνο σε μη ευαίσθητα συστήματα και δεδομένα.

3. Πρόσβαση σε δεδομένα και συστήματα, αλλά με έλεγχο της Διεύθυνσης Πληροφορικής και Επικοινωνιών του Πανεπιστημίου στην προσωπική συσκευή, τις εφαρμογές και τα αποθηκευμένα δεδομένα.

4. Πρόσβαση σε δεδομένα και συστήματα, αλλά αποτρέποντας την τοπική αποθήκευση δεδομένων σε προσωπικές συσκευές.

Β.1.8.4.2 Βασικές Αρχές της Πολιτικής

- **Διαχείριση Φορητών Συσκευών**

    - Τα δεδομένα του Πανεπιστημίου μπορούν να δημιουργηθούν, να επεξεργαστούν, να αποθηκευτούν και να κοινοποιηθούν μόνο σε προσωπικές συσκευές που εφαρμόζουν την πολιτική ασφάλειας του Πανεπιστημίου. Οι συσκευές που δεν συμμορφώνονται με την πολιτική μπορούν να συνδεθούν μόνο με καθορισμένα δίκτυα επισκεπτών (guest networks) που παρέχουν συνδέσεις στο Διαδίκτυο, αλλά δεν θα έχουν πρόσβαση στο τοπικό δίκτυο του Πανεπιστημίου.

- Κατάλληλο λογισμικό προστασίας από ιούς θα πρέπει να είναι εγκατεστημένο και να λειτουργεί σωστά σε όλες τις προσωπικές φορητές συσκευές.

- **Αυθεντικοποίηση**

  - Οι χρήστες προσωπικών φορητών συσκευών θα πρέπει να χρησιμοποιούν κατάλληλες μορφές ταυτοποίησης που έχουν εγκριθεί από την Ομάδα Ασφάλειας Πληροφοριών, όπως αναγνωριστικά χρήστη, κωδικούς πρόσβασης.

- **Πρόσβαση σε Δεδομένα και Συστήματα**

  - Δεν επιτρέπεται πρόσβαση μέσω προσωπικών φορητών συσκευών στις παρακάτω κλάσεις ή τύπους δεδομένων του Πανεπιστημίου:

    - Οποιαδήποτε πληροφορία υψηλού κινδύνου ή αντικτύπου (high impact).

    - Άλλες πληροφορίες με μικρότερο αντίκτυπο, αλλά εξαιρετικά πολύτιμες ή ευαίσθητες πληροφορίες του Πανεπιστημίου (low impact).

  - Το Πανεπιστήμιο έχει το δικαίωμα να εξετάζει κάθε προσωπική συσκευή που περιέχει ή περιείχε δεδομένα του Πανεπιστημίου όταν αυτό είναι απαραίτητο για σκοπούς έρευνας ή ελέγχου.

- **Τερματισμός Χρήσης**

  - Προτού μία φορητή συσκευή εγκαταλείψει τους χώρους του Πανεπιστημίου (π.χ. όταν ανακυκλώνεται μία παρωχημένη συσκευή), το Πανεπιστήμιο θα πρέπει να διαγράψει τυχόν ευαίσθητα δεδομένα. Επίσης, το Πανεπιστήμιο θα πρέπει να εξετάσει την πλήρη διαγραφή όλων των δεδομένων στη συσκευή αποθήκευσης.

  - Όμοιοι κανόνες θα πρέπει να εφαρμόζονται στην περίπτωση προσωπικών φορητών συσκευών που περιέχουν ή περιείχαν πληροφορίες του Πανεπιστημίου.

- **Ιδιωτικότητα**

  - Οι εργαζόμενοι έχουν την εύλογη προσδοκία για την προστασία της ιδιωτικότητας των προσωπικών τους δεδομένων σχετικά με τον δικό τους εξοπλισμό. Παρόλα αυτά, το Πανεπιστήμιο έχει το δικαίωμα να ελέγχει τα δεδομένα που είναι αποθηκευμένα σε προσωπικές συσκευές και να διαχειρίζεται τις προσωπικές συσκευές, εφόσον έχουν χρησιμοποιηθεί για εργασιακούς σκοπούς. Αυτό μπορεί ενίοτε να έχει ως αποτέλεσμα το προσωπικό τεχνικής υποστήριξης να αποκτά, μη προσδοκώμενα, πρόσβαση σε προσωπικές πληροφορίες των εργαζομένων. Για να μειωθεί η πιθανότητα μιας τέτοιας αποκάλυψης, οι χρήστες των προσωπικών συσκευών ενθαρρύνονται να διατηρούν τα προσωπικά τους δεδομένα ξεχωριστά από τα επιχειρησιακά δεδομένα, σε ξεχωριστούς φακέλους με συγκεκριμένη και σαφή ονοματοδοσία.

- Πρέπει να λαμβάνεται μέριμνα, ώστε να μην παραβιάζονται τα δικαιώματα ιδιωτικότητας π.χ. να μη χρησιμοποιούνται προσωπικές συσκευές για να γίνουν οπτικοακουστικές εγγραφές στον χώρο εργασίας.

Β.1.8.5 Πολιτική «Διαχείρισης Cookies»

Β.1.8.5.1 Αντικείμενο της Πολιτικής «Διαχείρισης Cookies»

Το Πανεπιστήμιο εγγυάται τον σεβασμό του ιδιωτικού απορρήτου των χρηστών του κατά την περιήγησή τους στους διαδικτυακούς ιστοτόπους του.

Η παρούσα Πολιτική «Διαχείρισης Cookies» εξηγεί τι είναι τα cookies και πώς αυτά χρησιμοποιούνται στους ιστότοπους που ανήκουν στο Πανεπιστήμιο και σχετίζονται με τη δραστηριότητα αυτού (π.χ. ιστότοποι Ακαδημαϊκών Τμημάτων κ.λπ.). Επίσης παρέχει πληροφορίες για τους τύπους cookies που χρησιμοποιούνται, τις πληροφορίες που συλλέγονται με αυτά και πώς χρησιμοποιούνται από το Πανεπιστήμιο.

Β.1.8.5.2 Έννοια

Τα αρχεία αναγνώρισης cookies είναι αυτοεγκαθιστώμενα αρχεία κειμένου, με σύντομο περιεχόμενο, που αποθηκεύονται επιτρεπτά στον ηλεκτρονικό υπολογιστή ή άλλες ηλεκτρονικές συσκευές (π.χ. κινητά τηλέφωνα, tablets, κ.λπ.) του χρήστη που επισκέπτεται έναν δικτυακό τόπο. Διευκολύνουν τον διαδικτυακό τόπο να απομνημονεύει πληροφορίες από την επίσκεψη κάθε χρήστη, με σκοπό να τον κάνει πιο χρήσιμο για τον χρήστη κατά την επόμενη επίσκεψή του. Τα αρχεία cookies αποστέλλονται από έναν δικτυακό τόπο προς τον τερματικό εξοπλισμό του χρήστη κατά την πρώτη επίσκεψή του σε αυτόν και ακολουθούν αντίστροφη πορεία κατά τις επόμενες επισκέψεις του χρήστη στον ίδιο δικτυακό τόπο.

Τα cookies που προέρχονται από τους διαδικτυακούς ιστοτόπους του Πανεπιστημίου χρησιμεύουν στην αναγνώριση του χρήστη και, μέσω στατιστικών δεδομένων, στη βελτίωση των παρεχόμενων υπηρεσιών προς αυτόν, όπως με την παροχή εξατομικευμένων υπηρεσιών. Η αβλαβής για τον χρήστη συλλογή μη προσωπικών πληροφοριών και δεδομένων που δεν αποκαλύπτουν σε καμία περίπτωση την ταυτότητά του, συμβάλει στην ταχύτερη και αποτελεσματικότερη λειτουργία του δικτυακού τόπου μέσω στατιστικών αξιολογήσεων και συγκριτικών παρατηρήσεων, στην ταχύτερη διεκπεραίωση των αιτημάτων του χρήστη και στην εν γένει βελτιστοποίηση των υπηρεσιών του δικτυακού τόπου του Πανεπιστημίου.

Η τεχνικής φύσης αποθήκευση αρχείων cookies επιτρέπεται με τη συγκατάθεση του χρήστη, η οποία μπορεί να δίδεται μέσω κατάλληλων ρυθμίσεων στον φυλλομετρητή ιστού (browser) ή μέσω άλλης εφαρμογής, για τους σκοπούς της διαβίβασης μιας επικοινωνίας, της παροχής υπηρεσίας που ρητά έχει ζητήσει ο χρήστης και για συγκεκριμένους σκοπούς επεξεργασίας. Ο χρήστης δύναται να διαγράψει οποτεδήποτε τα αρχεία cookies από τον τερματικό εξοπλισμό του. Εντούτοις, κάτι τέτοιο ενδεχομένως θα έχει συνέπειες στην ευκολία πρόσβασης στην ιστοσελίδα και δύναται να οδηγήσει σε μειωμένη λειτουργικότητά της.

Β.1.8.5.3 Τύποι cookies

Υπάρχουν δύο βασικές κατηγορίες cookies:

1. Τα προσωρινά cookies (cookies συνεδρίας – session cookies) τα οποία διαγράφονται αμέσως μετά το πέρας του προγράμματος περιήγησης ή μετά το κλείσιμο του φυλλομετρητή.

2. Τα μόνιμα cookies (persistent cookies), τα οποία παραμένουν στο πρόγραμμα περιήγησης για ορισμένο χρονικό διάστημα ή μέχρι να διαγραφούν από τους χρήστες.

Επιπλέον, ανάλογα με το εάν τα cookies δημιουργούνται και ελέγχονται από τον χειριστή του ιστοτόπου ή από άλλα μέρη, διακρίνονται σε «ιδιόκτητα» cookies και σε cookies «τρίτων μερών».

B.1.8.5.4 Χρήση cookies

Η ιστοσελίδα του Πανεπιστήμιου έχει πρόσβαση και αποθηκεύει cookies, καθώς και συναφείς τεχνολογίες στον υπολογιστή των χρηστών.

1. Βασικά / απαραίτητα cookies

Τα βασικά cookies είναι ουσιαστικής σημασίας για την ορθή λειτουργία του ιστότοπου, επιτρέπουν στους χρήστες να περιηγούνται και να χρησιμοποιούν τις λειτουργίες του, όπως πρόσβαση σε ασφαλείς περιοχές. Αυτά τα cookies δεν αναγνωρίζουν την ατομική ταυτότητα του χρήστη. Τα cookies αυτά είναι αναγκαία για τη λειτουργία του ιστοτόπου και η απενεργοποίησή τους ενδέχεται να καταστήσει τις υπηρεσίες και τα χαρακτηριστικά μη διαθέσιμα.

Όνομα	Σκοπός	Χρόνος Τήρησης
HSID	Αποκλεισμός πολλών τύπων επίθεσης, όπως απόπειρες απόκρυψης του περιεχομένου των εντύπων που συμπληρώνονται σε ιστοσελίδες.	Έως 2 έτη
SID	Αποκλεισμός πολλών τύπων επίθεσης, όπως απόπειρες απόκρυψης του περιεχομένου των εντύπων που συμπληρώνονται σε ιστοσελίδες.	Έως 2 έτη
PHPSESSID	Για την αποθήκευση του ονόματος χρήστη του συνδεδεμένου χρήστη με ένα κρυπτογραφημένο κλειδί 128bit. Αυτές οι πληροφορίες απαιτούνται για να επιτρέπουν σε έναν χρήστη να παραμείνει συνδεδεμένος σε έναν ιστότοπο χωρίς να χρειάζεται να υποβάλει το όνομα χρήστη και τον κωδικό πρόσβασης για κάθε σελίδα που επισκέπτεται. Χωρίς αυτό το cookie, ένας χρήστης δεν μπορεί να προχωρήσει σε περιοχές της ιστοσελίδας που απαιτούν πιστοποιημένη πρόσβαση.	Προσωρινό
__cfduid	Έχει οριστεί από την υπηρεσία CloudFlare για τον εντοπισμό αξιόπιστης επισκεψιμότητας ιστού. Δεν αντιστοιχεί σε κανένα αναγνωριστικό χρήστη στην εφαρμογή Ιστού ούτε το cookie αποθηκεύει τυχόν προσωπικά αναγνωρίσιμες πληροφορίες.	Έως 1 έτος
SIDCC	Cookie ασφάλειας για την προστασία των δεδομένων των χρηστών από μη εξουσιοδοτημένη πρόσβαση	Έως 90 μέρες

Πίνακας 16: Βασικά/Απαραίτητα Cookies

2. Cookies απόδοσης

Τα cookies αυτά συλλέγουν πληροφορίες για τη χρήση του ιστοτόπου, π.χ. ποιες σελίδες επισκέπτονται οι χρήστες πιο συχνά και εάν λαμβάνουν μηνύματα λάθους από τον ιστότοπο. Αυτά τα cookies δεν συλλέγουν πληροφορίες που ταυτοποιούν τους χρήστες, καθώς τις συλλέγουν με συγκεντρωτικό τρόπο και άρα παραμένουν ανώνυμα. Χρησιμοποιούνται μόνο για στατιστικούς σκοπούς που θα βοηθήσουν τη βελτίωση της λειτουργίας του ιστοτόπου.

Όνομα	**Σκοπός**	**Χρόνος Τήρησης**
HSID	Αποκλεισμός πολλών τύπων επίθεσης, όπως απόπειρες απόκρυψης του περιεχομένου των εντύπων που συμπληρώνονται σε ιστοσελίδες.	Έως 2 έτη
SID	Αποκλεισμός πολλών τύπων επίθεσης, όπως απόπειρες απόκρυψης του περιεχομένου των εντύπων που συμπληρώνονται σε ιστοσελίδες.	Έως 2 έτη
PHPSESSID	Για την αποθήκευση του ονόματος χρήστη του συνδεδεμένου χρήστη με ένα κρυπτογραφημένο κλειδί 128bit. Αυτές οι πληροφορίες απαιτούνται για να επιτρέπουν σε έναν χρήστη να παραμείνει συνδεδεμένος σε έναν ιστότοπο χωρίς να χρειάζεται να υποβάλει το όνομα χρήστη και τον κωδικό πρόσβασης για κάθε σελίδα που επισκέπτεται. Χωρίς αυτό το cookie, ένας χρήστης δεν μπορεί να προχωρήσει σε περιοχές της ιστοσελίδας που απαιτούν πιστοποιημένη πρόσβαση.	Προσωρινό
__cfduid	Έχει οριστεί από την υπηρεσία CloudFlare για τον εντοπισμό αξιόπιστης επισκεψιμότητας ιστού. Δεν αντιστοιχεί σε κανένα αναγνωριστικό χρήστη στην εφαρμογή Ιστού ούτε το cookie αποθηκεύει τυχόν προσωπικά αναγνωρίσιμες πληροφορίες.	Έως 1 έτος
SIDCC	Cookie ασφαλείας για την προστασία των δεδομένων των χρηστών από μη εξουσιοδοτημένη πρόσβαση	Έως 90 μέρες

Πίνακας 17: Cookies απόδοσης

3. Λειτουργικά cookies

Τα cookies αυτά χρησιμοποιούνται για την αποθήκευση των ρυθμίσεων στον ιστότοπο (π.χ. μέσω της απομνημόνευσης των προτιμήσεων των χρηστών όσον αφορά στην ασφαλή αναζήτηση, ή για να διευκολυνθούν οι χρήστες στην περιήγηση του ιστοτόπου, κ.λπ.). Μέσω των cookies αυτών μπορούν να συλλεχθούν πληροφορίες για τους χρήστες, όπως ο τύπος του προγράμματος περιήγησης, ο διακομιστής, η γλώσσα που επιλέγει ο χρήστης, οι προτιμήσεις του, οι αναζητήσεις του και η γεωγραφική θέση του χρήστη.

Στην περίπτωση των υπερσυνδέσμων (links) προς άλλους δικτυακούς τόπους, ο δικτυακός τόπος δεν ευθύνεται για τους όρους διαχείρισης και προστασίας των προσωπικών δεδομένων που αυτοί ακολουθούν.

Όνομα	**Σκοπός**	**Χρόνος Τήρησης**
hide_popup	Ρύθμιση WP για Popups	Έως 14 μέρες
cookieconsent_dismissed	Απομνημόνευση επιλογής popup για πολιτική cookies	Έως 365 μέρες
wp-settings-5	Περιέχουν γενικές πληροφορίες γεωγραφικής τοποθεσίας (π.χ. για την υπενθύμιση ζώνης ώρας)	Έως 365 μέρες
wp-settings-time-5		Έως 2 έτη
CONSENT	Πολιτική cookies	Έως 2 έτη
CONSENT	Πολιτική cookies	Έως 2 έτη

Πίνακας 18: Λειτουργικά cookies

4. Cookies διαφημίσεων

Πληροφορίες που αντλούμε μέσω της τεχνολογίας cookies και παρεμφερούς τεχνολογίας κοινοποιούνται σε τρίτους στο πλαίσιο δημιουργίας μηνυμάτων στοχευμένης διαφήμισης που μπορεί να προβληθούν στον χρήστη κατά την επίσκεψή του σε ιστοσελίδες τρίτων. Επιπλέον, η σχετική τεχνολογία cookies επιτρέπει μετρήσεις που σχετίζονται με τη δραστηριότητα χρήστη σε άλλον ιστότοπο που παρέπεμψε τον χρήστη στους ιστοτόπους του Πανεπιστημίου.

Όνομα	Σκοπός	Χρόνος Τήρησης
SID	Χρησιμοποιείται για την προσαρμογή των διαφημίσεων στις ιδιότητες Google, όπως η Αναζήτηση Google	Έως 2 έτη
SID	Χρησιμοποιείται για την προσαρμογή των διαφημίσεων στις ιδιότητες Google, όπως η Αναζήτηση Google	Έως 2 έτη
IDE	Αυτό το cookie χρησιμοποιείται για επαναπροσδιορισμό, βελτιστοποίηση, αναφορά και κατανομή των διαφημίσεων στο διαδίκτυο.	Έως 365 μέρες
NID	Χρησιμοποιείται για την προσαρμογή των διαφημίσεων στις ιδιότητες Google, όπως η Αναζήτηση Google	Έως 90 μέρες
__gads	Χρησιμοποιείται για τη μέτρηση των αλληλεπιδράσεων με τις διαφημίσεις και εμποδίζονται οι ίδιες διαφημίσεις να εμφανίζονται πολλές φορές.	Έως 2 έτη
1P_JAR	Χρησιμοποιείται από την Google για την προβολή εξατομικευμένων διαφημίσεων σε ιστότοπους Google, βάσει πρόσφατων αναζητήσεων και προηγούμενων αλληλεπιδράσεων.	Έως 30 μέρες
APISID	Χρησιμοποιείται από την Google για την προβολή εξατομικευμένων διαφημίσεων σε ιστότοπους Google, βάσει πρόσφατων αναζητήσεων και προηγούμενων αλληλεπιδράσεων.	Έως 2 έτη
APISID	Χρησιμοποιείται από την Google για την προβολή εξατομικευμένων διαφημίσεων σε ιστότοπους Google, βάσει πρόσφατων αναζητήσεων και προηγούμενων αλληλεπιδράσεων.	Έως 2 έτη
DSID	Αυτό το cookie χρησιμοποιείται για την αναγνώριση ενός συγκεκριμένου χρήστη και περιέχει έναν μοναδικό κωδικό αναγνώρισης	Έως 14 μέρες

Πίνακας 19: Cookies διαφημίσεων

5. Cookies *ασφαλείας*

Cookies ενδέχεται να χρησιμοποιούνται και για σκοπούς ασφάλειας (πρόληψη κυβερνοεπιθέσεων και κάθε άλλης κακόβουλης δραστηριότητας).

Όνομα	Σκοπός	Χρόνος Τήρησης
HSID	Αποκλεισμός πολλών τύπων επίθεσης, όπως απόπειρες απόκρυψης του περιεχομένου των εντύπων που συμπληρώνονται σε ιστοσελίδες.	Έως 2 έτη
HSID	Αποκλεισμός πολλών τύπων επίθεσης, όπως απόπειρες απόκρυψης του περιεχομένου των εντύπων που συμπληρώνονται σε ιστοσελίδες.	Έως 2 έτη
SID	Αποκλεισμός πολλών τύπων επίθεσης, όπως απόπειρες απόκρυψης του περιεχομένου των εντύπων που συμπληρώνονται σε ιστοσελίδες.	Έως 2 έτη
SID	Αποκλεισμός πολλών τύπων επίθεσης, όπως απόπειρες απόκρυψης του περιεχομένου των εντύπων που συμπληρώνονται σε ιστοσελίδες.	Έως 2 έτη
PHPSESSID	Για την αποθήκευση του ονόματος χρήστη του συνδεδεμένου χρήστη με ένα κρυπτογραφημένο κλειδί 128bit. Αυτές οι πληροφορίες απαιτούνται για να επιτρέπουν σε έναν χρήστη να παραμείνει συνδεδεμένος σε έναν ιστότοπο χωρίς να χρειάζεται να υποβάλει το όνομα χρήστη και τον κωδικό πρόσβασης για κάθε σελίδα που επισκέπτεται. Χωρίς αυτό το cookie, ένας χρήστης δεν μπορεί να προχωρήσει σε περιοχές της ιστοσελίδας που απαιτούν πιστοποιημένη πρόσβαση.	Προσωρινό
__cfduid	Έχει οριστεί από την υπηρεσία CloudFlare για τον εντοπισμό αξιόπιστης επισκεψιμότητας ιστού. Δεν αντιστοιχεί σε κανένα αναγνωριστικό χρήστη στην εφαρμογή Ιστού ούτε το cookie αποθηκεύει τυχόν προσωπικά αναγνωρίσιμες πληροφορίες.	Έως 1 έτος
SIDCC	Cookie ασφάλειας για την προστασία των δεδομένων των χρηστών από μη εξουσιοδοτημένη πρόσβαση	Έως 90 μέρες

Πίνακας 20: Cookies ασφάλειας

6. Cookies ανάλυσης

Τα cookies αυτά συλλέγουν στοιχεία για τον χρήστη του ιστοτόπου και επιτρέπουν τη βελτίωση του τρόπου λειτουργίας του. Τα στοιχεία αυτά βοηθούν στην παρακολούθηση των επιδόσεων του ιστοτόπου, τη μέτρηση των επισκέψεων, την παρακολούθηση του τρόπου πρόσβασης στον ιστότοπο, κ.λπ.

Όνομα	**Σκοπός**	**Χρόνος Τήρησης**
DV	Google Analytics Remarketing	Προσωρινό
OTZ	Το cookie της Google Analytics χρησιμοποιείται για πληροφορίες σχετικά με την επισκεψιμότητα του ιστότοπου	Έως 30 μέρες
SAPISID	Cookie από την Google για τη συλλογή πληροφοριών χρηστών για βίντεο που φιλοξενούνται από το YouTube	Έως 2 έτη
SAPISID	Cookie από την Google για τη συλλογή πληροφοριών χρηστών για βίντεο που φιλοξενούνται από το YouTube	Έως 2 έτη
SSID	Cookie από την Google για τη συλλογή πληροφοριών χρηστών για βίντεο που φιλοξενούνται από το YouTube	Έως 2 έτη
SSID	Cookie από την Google για τη συλλογή πληροφοριών χρηστών για βίντεο που φιλοξενούνται από το YouTube	Έως 2 έτη
_ga	Διατήρηση αρχείου στατιστικών επισκεπτών	Έως 2 έτη
_gid	Χρησιμοποιείται για τη διάκριση των χρηστών	Προσωρινό

Πίνακας 21: Cookies ανάλυσης

7. Άλλες τεχνολογίες

Οι άλλες τεχνολογίες μπορεί να χρησιμοποιηθούν για τους ίδιους σκοπούς με τα cookies και επιτρέπουν να γνωρίζουμε πότε ο χρήστης επισκέφτηκε τον ιστότοπο. Μέσω αυτών, τα μη προσωπικά δεδομένα (π.χ. το λειτουργικό σύστημα του χρήστη, το πρόγραμμα περιήγησης του χρήστη) ή συγκεντρωτικά στοιχεία, μπορεί να συλλεχθούν και να χρησιμοποιηθούν για τη βελτίωση της εμπειρίας χρήσης του ιστοτόπου.

Όνομα	Σκοπός	Χρόνος Τήρησης
_ga	Χρησιμοποιείται για τη διάκριση των χρηστών	Έως 2 έτη
OTZ	Το cookie της Google Analytics χρησιμοποιείται για πληροφορίες σχετικά με την επισκεψιμότητα του ιστότοπου	1 μήνας
wp-settings-5	Περιέχουν γενικές πληροφορίες γεωγραφικής τοποθεσίας (π.χ. για την υπενθύμιση ζώνης ώρας)	Έως 1 έτος
wp-settings-time-5	Περιέχουν γενικές πληροφορίες γεωγραφικής τοποθεσίας (π.χ. για την υπενθύμιση ζώνης ώρας)	Έως 1 έτος

Πίνακας 22: Άλλες τεχνολογίες (εκτός cookies)

B.1.8.5.5 Πώς μπορούν οι χρήστες να διαγράψουν τα cookies

Εάν ο χρήστης επιθυμεί να απενεργοποιήσει κάποια cookies, ανάλογα με τον συγκεκριμένο τύπο τους ο ιστότοπος ενδέχεται να μη λειτουργεί σωστά.

Ο χρήστης μπορεί πάντοτε να τροποποιήσει τις επιλογές στο πρόγραμμα περιήγησης για να λαμβάνει ειδοποιήσεις σχετικά με τη χρήση cookies ή για να απορρίπτει τη χρήση cookies. Σε αυτή την περίπτωση, εάν ο χρήστης δεν επιτρέπει τη χρήση cookies για συγκεκριμένες υπηρεσίες, ενδέχεται να μην έχει περαιτέρω πρόσβαση σε αυτές. Ο χρήστης μπορεί να μάθει περισσότερες πληροφορίες, σύμφωνα με το πρόγραμμα περιήγησης, χρησιμοποιώντας τους ακόλουθους συνδέσμους:

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safari
- Opera
- Adobe (flashcookies)

Για να ενημερωθεί ο χρήστης περαιτέρω σχετικά με τους τύπους cookies, μπορεί να επισκεφτεί τον ιστότοπο: http://www.allaboutcookies.org.

Μέρος Γ': Παραρτήματα

Γ.1. Έντυπο αίτησης ανάκλησης συγκατάθεσης των Υποκειμένων των Δεδομένων

Αίτηση Ανάκλησης Συγκατάθεσης

Αριθμός Πρωτοκόλλου: _____

Ημερομηνία Παραλαβής:_____

*Συμπληρώνονται από τον οργανισμό

Προς το Πανεπιστήμιο Αιγαίου

ΣΤΟΙΧΕΙΑ ΑΙΤΟΥΝΤΟΣ:

Όνομα:	Επώνυμο:	
Πατρώνυμο:	Μητρώνυμο:	Ημερ. Γέννησης:
ΑΦΜ:	ΔΟΥ:	ΑΔΤ:

ΔΙΕΥΘΥΝΣΗ ΕΠΙΚΟΙΝΩΝΙΑΣ:

Οδός:	Αριθμός:
Πόλη:	ΤΚ:
Τηλέφωνο:	Κινητό:
Φαξ:	E-mail:

Δήλωση:
Σας επισυνάπτω τα δικαιολογητικά και σας παρακαλώ όπως με βάση τα έγγραφα αυτά προβείτε στην ταυτοποίησή μου καθώς και την ανάκληση της συγκατάθεσής μου σχετικά με τη συλλογή και χρήση των προσωπικών μου δεδομένων (και συγκεκριμένα την αναίρεση .....
.....)
Βεβαιώνω υπευθύνως περί της ακρίβειας και ορθότητας των ανωτέρω αναγραφόμενων στοιχείων.
Αριθμός συνημμένων δικαιολογητικών: _____

Ημερομηνία ___ /___ / ____

Ο / Η αιτ____

Γ.2. Έντυπο δήλωσης συγκατάθεσης

(Παρέχεται από το Πανεπιστήμιο στο Υποκείμενο των Δεδομένων, συμπληρώνεται από το Υποκείμενο των Δεδομένων και αποστέλλεται στο Πανεπιστήμιο)

ΣΥΓΚΑΤΑΘΕΣΗ ΓΙΑ ΕΠΕΞΕΡΓΑΣΙΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ ΑΠΟ ΤΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

Στο πλαίσιο των διατάξεων του Γενικού Κανονισμού για την Προστασία των Δεδομένων (ΓΚΠΔ), το Πανεπιστήμιο Αιγαίου λειτουργεί ως Υπεύθυνος Επεξεργασίας και επεξεργάζεται δεδομένα προσωπικού χαρακτήρα, μεταξύ άλλων και για τον/τους ακόλουθο σκοπό/σκοπούς: *Συμπληρώστε τον σκοπό / τους σκοπούς της επεξεργασίας*.

Για την εκπλήρωση του/των παραπάνω σκοπού/σκοπών ζητάμε τη σύμφωνη γνώμη σας προκειμένου να επεξεργαστούμε τα δεδομένα προσωπικού χαρακτήρα που σας αφορούν *Αναφέρετε τα δεδομένα ή τις κατηγορίες δεδομένων προσωπικού χαρακτήρα που συλλέγονται και επεξεργάζονται για τον/τους ανωτέρω σκοπό/σκοπούς επεξεργασίας*, όπως περιγράφεται παρακάτω:

Περιγράψτε την επεξεργασία που διενεργείται επί των δεδομένων προσωπικού χαρακτήρα.

* Σε περίπτωση που το Υποκείμενο των Δεδομένων υπόκειται σε απόφαση που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας των δεδομένων του, *Καταγράψτε κάποιες λεπτομέρειες σχετικά με την εν λόγω επεξεργασία*.

** Σε περίπτωση διαβίβασης των δεδομένων προσωπικού χαρακτήρα που αφορούν στο υποκείμενο σε τρίτες χώρες ή διεθνείς οργανισμούς χωρίς να υπάρχουν οι κατάλληλες εγγυήσεις ή κάποια απόφαση επάρκειας, *Αναφέρετε όλους τους κινδύνους που ενδέχεται να προκύψουν για το Υποκείμενο των Δεδομένων από την εν λόγω διαβίβαση*.

☐ Δεν Συναινώ ☐ Συναινώ

Δικαίωμα ανάκλησης συγκατάθεσης: Σε περίπτωση που επιθυμείτε να ανακαλέσετε τη συγκατάθεσή σας ή να τροποποιήσετε τη δήλωσή σας, μπορείτε να:

- Επισκεφθείτε ανά πάσα στιγμή την ιστοσελίδα του Τμήματος
- Επισκεφθείτε την αντίστοιχη Γραμματεία ή το τμήμα Διοικητικού (εάν είστε υπάλληλος ή καθηγητής ή καθηγήτρια) στις ώρες λειτουργίας της.

ΣΤΟΙΧΕΙΑ ΦΥΣΙΚΟΥ ΠΡΟΣΩΠΟΥ:

Ονοματεπώνυμο:	Αριθμός Μητρώου (Α.Μ.) Φοιτητή ή Φοιτήτριας / Α.Δ.Τ:
Υπογραφή:	Ημερομηνία:

Σε περίπτωση που συμπληρώνετε τη φόρμα μέσω της ιστοσελίδας του Τμήματος, παρακαλούμε όπως επιλέξετε το παρακάτω τετραγωνίδιο αντί της υπογραφής σας ☐

Για τυχόν απορίες, σχόλια και διευκρινίσεις σε θέματα αναφορικά με τα δεδομένα προσωπικού χαρακτήρα που σας αφορούν, μπορείτε να επικοινωνήσετε με το Πανεπιστήμιο Αιγαίου

στο e-mail:

ή τηλεφωνικώς στο τηλ.:

Γ.3. Έντυπο αναφοράς περιστατικού παραβίασης δεδομένων προσωπικού χαρακτήρα

Αναφορά Περιστατικού Παραβίασης Δεδομένων Προσωπικού Χαρακτήρα

ΟΝΟΜΑΤΕΠΩΝΥΜΟ ΑΝΑΦΕΡΟΝΤΟΣ:		Email / ΤΗΛΕΦΩΝΟ ΑΝΑΦΕΡΟΝΤΟΣ:	
ΤΙΤΛΟΣ / ΡΟΛΟΣ ΑΝΑΦΕΡΟΝΤΟΣ:		ΑΡΙΘΜΟΣ ΠΕΡΙΣΤΑΤΙΚΟΥ:	
ΠΗΓΗ (π.χ. χρήστης, ανώνυμο, υπάλληλος πανεπιστημίου)		ΗΜΕΡΟΜΗΝΙΑ/ ΩΡΑ ΑΝΑΦΟΡΑΣ:	

ΠΛΗΡΟΦΟΡΙΕΣ ΠΕΡΙΣΤΑΤΙΚΟΥ					
ΧΑΡΑΚΤΗΡΙΣΜΟΣ ΠΕΡΙΣΤΑΤΙΚΟΥ:	• Μέγιστης Προτεραιότητας • Σημαντικής Προτεραιότητας • Χαμηλής Προτεραιότητας		ΗΜΕΡΟΜΗΝΙΑ ΠΕΡΙΣΤΑΤΙΚΟΥ:		
Τοποθεσία:					
ΠΟΛΗ:		ΧΩΡΑ:		ΤΚ:	
ΣΥΓΚΕΚΡΙΜΕΝΟ ΣΗΜΕΙΟ ΤΟΠΟΘΕΣΙΑΣ (εάν υπάρχει):					

ΣΥΝΟΠΤΙΚΗ ΑΝΑΦΟΡΑ ΠΕΡΙΣΤΑΤΙΚΟΥ:
Γενικές Πληροφορίες:

- Πλήθος δεδομένων: _____
- Από πού διέρρευσαν: _____
- Γιατί βρίσκονται σε κίνδυνο: _____
- Τα δεδομένα είναι κρυπτογραφημένα; _____

Τύπος δεδομένων	
• Ονόματα • Κωδικοί / passwords • Credit / Debit cards • Τραπεζικοί λογαριασμοί • E-mail διευθύνσεις • Κείμενο σε e-mails • Τηλέφωνα • Διευθύνσεις • Στοιχεία προσωπικού	• ΑΜΚΑ • Ασφαλιστήρια συμβόλαια • Ιατρικά στοιχεία • Αρ. Ταυτότητας / Αρ. Διαβατηρίου • Αρ. Διπλώματος Οδήγησης • Σχέδια της εταιρείας, οικονομικές πληροφορίες, αρχεία • Άλλα ευαίσθητα προσωπικά δεδομένα _____ • Άλλες ευαίσθητες πληροφορίες _____
Τύπος περιστατικού	
• Παραβίαση δικτύου ή Server	• Μη εξουσιοδοτημένη πρόσβαση σε sites που περιέχουν ευαίσθητες πληροφορίες

• Απώλεια ή κλοπή ή παραβίαση Η/Υ ή μέσων αποθήκευσης δεδομένων • Απώλεια, κλοπή, παραβίαση Software hacking σε συστήματα	• Άλλο _____
ΑΙΤΙΕΣ ΠΕΡΙΣΤΑΤΙΚΟΥ:	
ΣΥΝΕΠΕΙΕΣ ΠΕΡΙΣΤΑΤΙΚΟΥ:	
ΕΝΕΡΓΕΙΕΣ ΔΙΑΧΕΙΡΙΣΗΣ ΠΕΡΙΣΤΑΤΙΚΟΥ:	
ΣΥΜΠΕΡΑΣΜΑΤΑ – ΠΕΡΑΙΤΕΡΩ ΠΑΡΑΤΗΡΗΣΕΙΣ:	
Στοιχεία Επικοινωνίας Υπευθύνου	
ΤΗΛ:	
ΔΙΕΥΘΥΝΣΗ:	
E- MAIL:	

Ημερομηνία ___ /___ / ____

Υπογραφή

Γ.4. Έντυπο Άσκησης των Δικαιωμάτων των Υποκειμένων

(Παρέχεται από το Πανεπιστήμιο στο Υποκείμενο των Δεδομένων, συμπληρώνεται από το Υποκείμενο των Δεδομένων και αποστέλλεται στο Πανεπιστήμιο)

Αίτηση Άσκησης των Δικαιωμάτων του Υποκειμένων των Δεδομένων

Αριθμός Πρωτοκόλλου: _____

Ημερομηνία Παραλαβής:_____

*Συμπληρώνονται από το Πανεπιστήμιο

Προς το Πανεπιστήμιο Αιγαίου

ΣΤΟΙΧΕΙΑ ΑΙΤΟΥΝΤΟΣ:

Όνομα:	**Επώνυμο:**	**ΑΔΤ:**
Πατρώνυμο:	**Μητρώνυμο:**	**Ημερ. Γέννησης:**

ΔΙΕΥΘΥΝΣΗ ΕΠΙΚΟΙΝΩΝΙΑΣ:

Οδός:	**Αριθμός:**
Πόλη:	**ΤΚ:**
Τηλέφωνο:	**Κινητό:**
Φαξ:	**E-mail:**

Επιθυμώ να ασκήσω το δικαίωμα[2]:

☐ Της ενημέρωσης
☐ Της πρόσβασης
☐ Της διόρθωσης
☐ Της διαγραφής
☐ Της εναντίωσης
☐ Του περιορισμού της επεξεργασίας
☐ Της φορητότητας των δεδομένων

Αναφορικά με το δικαίωμα της **αυτοματοποιημένης λήψης αποφάσεων**, το Πανεπιστήμιο ενημερώνει/δεσμεύεται πως δεν διενεργεί αυτοματοποιημένη λήψη αποφάσεων χρησιμοποιώντας τα δεδομένα προσωπικού χαρακτήρα που έχει στην κατοχή του, ούτε υποστηρίζει κατάρτιση προφίλ χρηστών.

[2] Για τη διεκπεραίωση του δικαιώματος της διόρθωσης, της διαγραφής, της εναντίωσης, του περιορισμού της επεξεργασίας και της φορητότητας των δεδομένων, το Υποκείμενο των Δεδομένων θα πρέπει να επισυνάψει την απαραίτητη συμπληρωματική πληροφορία.

Σημειώνεται ότι η άσκηση/επίκληση των ανωτέρω δικαιωμάτων σας δεν επιφέρει οποιαδήποτε χρέωση. Περαιτέρω, ενημερώνεστε ότι οι οποιεσδήποτε ενέργειες από το Πανεπιστήμιο οφείλουν να διεκπεραιωθούν εντός ενός μήνα από την ημερομηνία επίκλησης / άσκησης του εκάστοτε δικαιώματός σας, εκτός εάν οι εργασίες που αφορούν την ικανοποίηση του αιτήματος σας χαρακτηρίζονται από ιδιαιτερότητες και/ή περιπλοκές βάσει των οποίων το Πανεπιστήμιο διατηρεί το δικαίωμα να επεκτείνει το χρόνο ολοκλήρωσης των ενεργειών κατά δύο ακόμη μήνες. Σε τέτοια περίπτωση θα ενημερώνεστε εντός ενός μήνα από την υποβολή του αιτήματος σας. Όπου η επίκληση του δικαιώματος σας δεν ικανοποιηθεί, διατηρείτε το δικαίωμα να αποταθείτε στον Υπεύθυνο Προστασίας Δεδομένων του Πανεπιστημίου (dpo@aegean.gr).

Για την άσκηση του εκάστοτε δικαιώματος, μπορείτε να επικοινωνήσετε με το Πανεπιστήμιο Αιγαίου μέσω:

Ταχυδρομείου	*XXX, 81100 Μυτιλήνη*
Τηλεφώνου	*XXXX 0 XXXXX*
Τηλεομοιοτυπίου	*XXXX 0 XXXXX*
Ηλεκτρονικού Ταχυδρομείου	*XXX@aegean.gr*

Ημερομηνία ___ /___ / ____ **Ο / Η αιτ_____**

Γ.5. Έντυπο Άσκησης του δικαιώματος της ενημέρωσης

a) **Εφόσον τα δεδομένα των φυσικών προσώπων έχουν συλλεγεί από το Υποκείμενο των Δεδομένων**
(Συμπληρώνεται από το Πανεπιστήμιο και αποστέλλεται στο Υποκείμενο των Δεδομένων)

Υπεύθυνος Επεξεργασίας			
Όνομα φορέα			
Στοιχεία επικοινωνίας			
Υπεύθυνος Προστασίας Δεδομένων			
Ονοματεπώνυμο			
Στοιχεία επικοινωνίας			
Σκοπός επεξεργασίας			
Δεδομένα		**Σκοπός επεξεργασίας**	
Νομική βάση επεξεργασίας			
Έννομα συμφέροντα που επιδιώκονται από το Πανεπιστήμιο ή τρίτο φορέα			
Αποδέκτες, ή κατηγορίες αποδεκτών των δεδομένων			
Πρόθεση του Πανεπιστημίου να διαβιβάσει τα δεδομένα σε τρίτη χώρα ή διεθνή οργανισμό			
Χρονικό διάστημα διατήρησης των δεδομένων και κριτήρια που καθορίζουν αυτό το διάστημα			

Επιπλέον, το Πανεπιστήμιο σας ενημερώνει για τα ακόλουθα:

1. Έχετε το δικαίωμα να υποβάλετε αίτημα στο Πανεπιστήμιο αναφορικά με την άσκηση των δικαιωμάτων σας (πρόσβαση, διόρθωση, διαγραφή, περιορισμό επεξεργασίας, αντίταξη στην επεξεργασία, φορητότητα δεδομένων).

2. Έχετε το δικαίωμα να ανακαλέσετε τη συγκατάθεσή σας για τους παρακάτω σκοπούς επεξεργασίας:
   _____
   _____

3. Έχετε το δικαίωμα να υποβάλετε καταγγελία στην ΑΠΔΠΧ.

4. Βάσει της _____ [3] καλείστε να παράσχετε στο Πανεπιστήμιο τα προσωπικά σας δεδομένα. Η μη παροχή των δεδομένων αυτών, φέρει τις ακόλουθες συνέπειες:

_____
_____
_____

5. Το Πανεπιστήμιο δεν διενεργεί αυτοματοποιημένη λήψη αποφάσεων χρησιμοποιώντας τα δεδομένα προσωπικού χαρακτήρα που έχει στην κατοχή του, ούτε υποστηρίζει κατάρτιση προφίλ χρηστών.

6. Το Πανεπιστήμιο δεν προτίθεται να χρησιμοποιήσει τα δεδομένα που έχει συλλέξει για σκοπούς άλλους από αυτούς για τους οποίους τα δεδομένα συλλέχθηκαν.

[3] Αναγράφεται από το Πανεπιστήμιο η νομική ή συμβατική υποχρέωση ή απαίτηση για σύναψη σύμβασης που υποχρεώνει το Υποκείμενο των Δεδομένων να παρέχει τα δεδομένα του.

b) Εφόσον τα δεδομένα των φυσικών προσώπων δεν έχουν συλλεγεί από το Υποκείμενο των Δεδομένων

(Συμπληρώνεται από το Πανεπιστήμιο και αποστέλλεται στο Υποκείμενο των Δεδομένων)

Υπεύθυνος Επεξεργασίας			
Όνομα φορέα			
Στοιχεία επικοινωνίας			
Υπεύθυνος Προστασίας Δεδομένων			
Ονοματεπώνυμο			
Στοιχεία επικοινωνίας			
Σκοπός επεξεργασίας			
Δεδομένα		**Σκοπός επεξεργασίας**	
Νομική βάση επεξεργασίας			
Έννομα συμφέροντα που επιδιώκονται από το Πανεπιστήμιο ή τρίτο φορέα			
Αποδέκτες, ή κατηγορίες αποδεκτών των δεδομένων			
Πρόθεση του Πανεπιστημίου να διαβιβάσει τα δεδομένα σε τρίτη χώρα ή διεθνή οργανισμό			
Χρονικό διάστημα διατήρησης των δεδομένων και κριτήρια που καθορίζουν αυτό το διάστημα			
Πηγή συλλογής των δεδομένων[4]			

[4] Κατά περίπτωση, αναφορά εάν η εν λόγω πηγή είναι προσβάσιμη από το κοινό.

Επιπλέον, το Πανεπιστήμιο σας ενημερώνει για τα ακόλουθα:

1. Έχετε το δικαίωμα να υποβάλετε αίτημα στο Πανεπιστήμιο αναφορικά με την άσκηση των δικαιωμάτων σας (πρόσβαση, διόρθωση, διαγραφή, περιορισμό επεξεργασίας, αντίταξη στην επεξεργασία, φορητότητα δεδομένων).

2. Έχετε το δικαίωμα να ανακαλέσετε τη συγκατάθεσή σας για τους παρακάτω σκοπούς επεξεργασίας:
   _____
   _____

3. Έχετε το δικαίωμα να υποβάλετε καταγγελία στην ΑΠΔΠΧ.

4. Βάσει της _____ [5] καλείστε να παράσχετε στο Πανεπιστήμιο τα προσωπικά σας δεδομένα. Η μη παροχή των δεδομένων αυτών, φέρει τις ακόλουθες συνέπειες:
   _____
   _____
   _____

5. Το Πανεπιστήμιο δεν διενεργεί αυτοματοποιημένη λήψη αποφάσεων χρησιμοποιώντας τα δεδομένα προσωπικού χαρακτήρα που έχει στην κατοχή του, ούτε υποστηρίζει κατάρτιση προφίλ χρηστών.

6. Το Πανεπιστήμιο δεν προτίθεται να χρησιμοποιήσει τα δεδομένα που έχει συλλέξει για σκοπούς άλλους από αυτούς για τους οποίους τα δεδομένα συλλέχθηκαν.

[5] Αναγράφεται από τον Πανεπιστήμιο η νομική ή συμβατική υποχρέωση ή απαίτηση για σύναψη σύμβασης που υποχρεώνει το Υποκείμενο των Δεδομένων να παρέχει τα δεδομένα του.

Γ.6. Έντυπο Άσκησης του δικαιώματος της πρόσβασης

(Συμπληρώνεται από το Πανεπιστήμιο και αποστέλλεται στο Υποκείμενο των Δεδομένων)

Σκοπός επεξεργασίας			
Δεδομένα		**Σκοπός επεξεργασίας**	
Κατηγορίες δεδομένων προσωπικού χαρακτήρα που διατηρεί το Πανεπιστήμιο			
Αποδέκτες ή κατηγορίες αποδεκτών στους οποίους έχουν κοινολογηθεί ή πρόκειται να κοινολογηθούν τα δεδομένα προσωπικού χαρακτήρα[6]			
Χρονικό διάστημα για το οποίο θα αποθηκευτούν τα δεδομένα προσωπικού χαρακτήρα[7]			

Επιπλέον, το Πανεπιστήμιο σας ενημερώνει για τα ακόλουθα:

1. Έχετε το δικαίωμα να υποβάλετε αίτημα στο Πανεπιστήμιο για διόρθωση ή διαγραφή των προσωπικών σας δεδομένων ή περιορισμό της επεξεργασίας των προσωπικών σας δεδομένων ή να αντιταχθείτε στην εν λόγω επεξεργασία.
2. Έχετε το δικαίωμα να υποβάλετε καταγγελία στην ΑΠΔΠΧ.
3. Έχετε δικαίωμα να γνωρίζετε την προέλευση των δεδομένων σας[8]
4. Το Πανεπιστήμιο δεν διενεργεί αυτοματοποιημένη λήψη αποφάσεων χρησιμοποιώντας τα δεδομένα προσωπικού χαρακτήρα που έχει στην κατοχή του, ούτε υποστηρίζει κατάρτιση προφίλ χρηστών.
5. Το Πανεπιστήμιο δεν διαβιβάζει δεδομένα προσωπικού χαρακτήρα σε τρίτη χώρα ή σε διεθνή οργανισμό.
6. Το Πανεπιστήμιο μπορεί να σας παρέχει αντίγραφο των προσωπικών σας δεδομένων που υποβάλλονται σε επεξεργασία. Για επιπλέον αντίγραφα, οφείλετε να καταβάλετε στο Πανεπιστήμιο το τέλος των ΧΧ € για διοικητικά έξοδα.
    a. Εάν το αίτημα υποβληθεί με ηλεκτρονικά μέσα, το Πανεπιστήμιο θα σας ενημερώσει με ηλεκτρονικό τρόπο, εκτός εάν αιτηθείτε εναλλακτικό τρόπο αποστολής των στοιχείων.

[6] Ιδίως τους αποδέκτες σε τρίτες χώρες ή διεθνείς οργανισμούς

[7] Όταν είναι αδύνατο να οριστεί σαφώς το χρονικό διάστημα, το Πανεπιστήμιο Αιγαίου αναφέρει τα κριτήρια που καθορίζουν το εν λόγω διάστημα

[8] Όταν τα δεδομένα προσωπικού χαρακτήρα δεν έχουν συλλεχθεί από το Υποκείμενο των Δεδομένων

Γ.7. Διαχείριση Αιτήματος

(Συμπληρώνεται από το Πανεπιστήμιο για λόγους εσωτερικής διαχείρισης)

ΠΑΡΑΛΑΒΗ ΑΙΤΗΜΑΤΟΣ

Ημερομηνία Παραλαβής: ……...…….……

Μονάδα: …….……....……...

Παραλήφθηκε Από: ……..……..……..

Ενέργειες μονάδας

ΔΙΕΚΠΕΡΑΙΩΣΗ ΑΙΤΗΜΑΤΟΣ

Μονάδα: ……..……..

Υπογραφή Λειτουργού Εξυπηρέτησης: ……..…….…….…….

Ημερομηνία: ……..……..

Υπογραφή Προϊστάμενου Μονάδας: …….……

Ημερομηνία: …….

Ενέργειες μονάδας

Γ.8. Υποδείγματα Αρχείων Δραστηριοτήτων Επεξεργασίας

Το Πανεπιστήμιο χρησιμοποιεί τα υποδείγματα των αρχείων δραστηριοτήτων επεξεργασίας που παρέχει η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) στην ιστοσελίδα της (http://www.dpa.gr/portal/page?_pageid=33,211400&_dad=portal&_schema=PORTAL). Τα εν λόγω αρχεία είναι σε μορφή αρχείου Excel.

Στην ιστοσελίδα της ΑΠΔΠΧ υπάρχει υπόδειγμα αρχείου δραστηριοτήτων «Υπεύθυνος Επεξεργασίας», στο οποίο θα καταγράφονται όλες οι δραστηριότητες επεξεργασίας που διενεργούνται για σκοπό του Πανεπιστημίου καθώς και ένα υπόδειγμα αρχείου δραστηριοτήτων «Εκτελών την Επεξεργασία», στο οποίο θα καταγράφονται όλες οι δραστηριότητες επεξεργασίας δεδομένων προσωπικού χαρακτήρα που διενεργούνται για λογαριασμό του Πανεπιστημίου. Στο τέλος κάθε αρχείου υπάρχουν οδηγίες αναφορικά με τα πεδία και τις πληροφορίες που πρέπει να συμπληρωθούν.

Σημειώνεται ότι οι στήλες των αρχείων είναι είτε με πράσινο είτε με γαλάζιο χρώμα. Οι στήλες με πράσινο χρώμα αφορούν τις υποχρεωτικές πληροφορίες που πρέπει να περιλαμβάνει το αρχείο δραστηριοτήτων προκειμένου να συμμορφώνεται με τις απαιτήσεις του ΓΚΠΔ (άρθρο 30). Επίσης, οι στήλες με γαλάζιο χρώμα αφορούν προαιρετικές πληροφορίες που ενδέχεται να βοηθήσουν στη διαδικασία συμμόρφωσης. Όσον αφορά στις γαλάζιες στήλες, είναι στην ευχέρεια του Πανεπιστημίου αν θα τις κρατήσει ή όχι στα αρχεία δραστηριοτήτων που τηρεί.

Γ.9. Φόρμα Ανάλυσης και Αξιολόγησης Περιστατικού Παραβίασης δεδομένων προσωπικού χαρακτήρα

(Συμπληρώνεται από τον Υπεύθυνο Προστασίας Δεδομένων του Πανεπιστημίου)

ΦΟΡΜΑ ΑΝΑΛΥΣΗΣ ΚΑΙ ΑΞΙΟΛΟΓΗΣΗΣ ΤΟΥ ΠΕΡΙΣΤΑΤΙΚΟΥ ΠΑΡΑΒΙΑΣΗΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Η συμπλήρωση της παρούσας φόρμας αποσκοπεί στα ακόλουθα: i) στην ανάλυση του ύποπτου συμβάντος προκειμένου να εξακριβωθεί εάν πρόκειται για παραβίαση δεδομένων προσωπικού χαρακτήρα, ii) στην αξιολόγηση του κινδύνου που ενδέχεται να προκύψει από το περιστατικό παραβίασης για τα υποκείμενα των δεδομένων, iii) στη διαβάθμιση του περιστατικού παραβίασης, ώστε στη συνέχεια να αποφασισθεί ο τρόπος αντιμετώπισής του, καθώς και το κατά πόσον θα ανακοινωθούν στην αρμόδια Εποπτική Αρχή και τα υποκείμενα των δεδομένων.

Περιστατικό Παραβίασης # *Συμπληρώστε τον κωδικό του περιστατικού*

Α – Πληροφορίες σχετικά με το ύποπτο συμβάν / περιστατικό

Αναφέρθηκε από τον / την	*Συμπλήρωσε το ονοματεπώνυμο*
Θέση / Τμήμα:	*Προς συμπλήρωση*
Τηλέφωνο:	*Προς συμπλήρωση*
E-mail:	*Προς συμπλήρωση*

Β – Περιγραφή του ύποπτου συμβάντος / περιστατικού

1. Σχετικές ημερομηνίες:

1α. Εκτιμώμενη ημερομηνία και ώρα κατά την οποία συνέβη το περιστατικό:

ΗΗ/ΜΜ/ΕΕ, ΩΩ:ΛΛ

1β. Ημερομηνία και ώρα κατά την οποία εντοπίστηκε και αναφέρθηκε το περιστατικό:

ΗΗ/ΜΜ/ΕΕ, ΩΩ:ΛΛ

Η ημερομηνία που συνέβη το περιστατικό μπορεί να είναι διαφορετική της ημερομηνίας που εντοπίστηκε.

2. Οντότητα που ανέφερε το περιστατικό:

- ☐ Διεύθυνση Πληροφορικής και Επικοινωνιών του Πανεπιστημίου (εντοπίστηκε από αυτή ή αναφέρθηκε σε αυτή)
- ☐ Φοιτητής ή Φοιτήτρια (προπτυχιακός, μεταπτυχιακός, διδακτορικός)
- ☐ Καθηγητής ή Καθηγήτρια / Υπάλληλος του Πανεπιστημίου
- ☐ Εκτελών την επεξεργασία
- ☐ Τρίτος ως προς το Πανεπιστήμιο (π.χ. φυσικό πρόσωπο, άλλη δημόσια αρχή)
- ☐ Άλλη οντότητα Παρακαλώ συμπληρώστε

3. Τύπος περιστατικού παραβίασης:

- ☐ Παραβίαση της εμπιστευτικότητας: εκούσια ή ακούσια κοινοποίηση των δεδομένων προσωπικού χαρακτήρα ή μη εξουσιοδοτημένη πρόσβαση στα δεδομένα.
- ☐ Παραβίαση της ακεραιότητας: εκούσια ή ακούσια τροποποίηση των δεδομένων προσωπικού χαρακτήρα από μη εξουσιοδοτημένη οντότητα.
- ☐ Παραβίαση της διαθεσιμότητας: εκούσια ή ακούσια καταστροφή των δεδομένων προσωπικού χαρακτήρα ή απώλεια πρόσβασης σε αυτά.

Η παραβίαση μπορεί να αφορά ταυτόχρονα την εμπιστευτικότητα, τη διαθεσιμότητα και την ακεραιότητα των δεδομένων προσωπικού χαρακτήρα, καθώς και οποιονδήποτε συνδυασμό αυτών.

4. Συνοπτική περιγραφή του περιστατικού παραβίασης

Περιγράψτε το περιστατικό

Αποτελεί το παρόν συμβάν περιστατικό παραβίασης δεδομένων προσωπικού χαρακτήρα;

○ Ναι ○ Όχι

Σε περίπτωση που το αναφερθέν συμβάν **δεν** αφορά δεδομένα προσωπικού χαρακτήρα και άρα δεν είναι περιστατικό παραβίασης δεδομένων προσωπικού χαρακτήρα, **δεν** απαιτείται η συμπλήρωση των παρακάτω πεδίων.

Γ– Επηρεαζόμενα δεδομένα προσωπικού χαρακτήρα

	Κατηγορία επηρεαζόμενων δεδομένων	Εκτιμώμενος αριθμός επηρεαζόμενων δεδομένων
☐	Στοιχεία επικοινωνίας (π.χ. e-mail, τηλέφωνο, ταχυδρομική διεύθυνση)	*Προς συμπλήρωση*
☐	Στοιχεία ταυτοποίησης (π.χ. ΑΔΤ, ΑΦΜ, ΑΜΚΑ)	*Προς συμπλήρωση*
☐	Οικονομικά / φορολογικά δεδομένα (π.χ. αριθμός λογαριασμού, εκκαθαριστικό σημείωμα)	*Προς συμπλήρωση*
☐	Δεδομένα υγείας	*Προς συμπλήρωση*
☐	Δεδομένα που αφορούν ποινικές καταδίκες και αδικήματα	*Προς συμπλήρωση*
☐	Λοιπά ευαίσθητα δεδομένα (π.χ. πολιτικά φρονήματα, φυλετική καταγωγή, βιομετρικά) Παρακαλώ συμπληρώστε	*Προς συμπλήρωση*
	Άλλη κατηγορία δεδομένων προσωπικού χαρακτήρα	
☐	Παρακαλώ συμπληρώστε την κατηγορία / τις κατηγορίες δεδομένων	*Προς συμπλήρωση*

Δ– Επηρεαζόμενα υποκείμενα των δεδομένων

1. Κατηγορίες και προσεγγιστικός αριθμός επηρεαζόμενων υποκειμένων

☐	Προπτυχιακοί, μεταπτυχιακοί, διδακτορικοί φοιτητές και φοιτήτριες	*Αριθμός αυτών*
☐	Υποψήφιοι φοιτητές και φοιτήτριες	*Αριθμός αυτών*
☐	Καθηγητές / Καθηγήτριες / Ερευνητές / Υπάλληλοι του Πανεπιστημίου	*Αριθμός αυτών*

☐ Τρίτα μέρη / Συνεργάτες (π.χ. προμηθευτές)	*Αριθμός αυτών*
☐ Άλλη κατηγορία υποκειμένων Παρακαλώ συμπληρώστε	*Αριθμός αυτών*

2. Έχουν επηρεαστεί από την παραβίαση ευπαθείς ομάδες υποκειμένων (π.χ. ανήλικοι φοιτητές και φοιτήτριες, παιδιά, ΑμεΑ); Ναι/ Όχι. *Καταγράψτε τον αριθμό αυτών*.

3. Πόσο εύκολο είναι να ταυτοποιηθούν τα επηρεαζόμενα Υποκείμενα των Δεδομένων;

Αδύνατο / Πολύ δύσκολα / Με μικρή δυσκολία / Εύκολα

Ε– Επιπτώσεις της παραβίασης

1. Επιπτώσεις που προέκυψαν ή ενδέχεται να προκύψουν για τα Υποκείμενα των Δεδομένων από το περιστατικό παραβίασης:

Καταγράψτε όλες τις ενδεχόμενες επιπτώσεις της παραβίασης για τα Υποκείμενα των Δεδομένων

Σοβαρότητα των επιπτώσεων για τα Υποκείμενα	Πιθανότητα να προκληθεί βλάβη στα Υποκείμενα λόγω των επιπτώσεων
☐ Αμελητέα	☐ Αμελητέα
☐ Περιορισμένη	☐ Περιορισμένη
☐ Σημαντική	☐ Σημαντική
☐ Υψηλή	☐ Υψηλή

ΣΤ– Μέτρα Ασφάλειας

Καταγράψτε όλα τα μέτρα ασφάλειας που έχουν ληφθεί από το Πανεπιστήμιο προκειμένου να ελαχιστοποιηθεί ο ενδεχόμενος κίνδυνος από την παραβίαση για τα Υποκείμενα των Δεδομένων (π.χ. κρυπτογράφηση, ανωνυμοποίηση, ψευδωνυμοποίηση)

Καταγράψτε όλα τα υφιστάμενα μέτρα ασφαλείας σχετικά με τα δεδομένα προσωπικού χαρακτήρα

Ζ– Διαβάθμιση Κινδύνου Περιστατικού Παραβίασης

- ☐ Πολύ υψηλός κίνδυνος
- ☐ Υψηλός κίνδυνος
- ☐ Μέτριος κίνδυνος
- ☐ Χαμηλός κίνδυνος
- ☐ Αμελητέος κίνδυνος

Γ.10. Έντυπο δήλωσης συγκατάθεσης για επιστημονική έρευνα

(Συμπληρώνεται από τον υπεύθυνο ερευνητή και αποστέλλεται στο Υποκείμενο των Δεδομένων)

ΔΗΛΩΣΗ ΣΥΓΚΑΤΑΘΕΣΗΣ ΓΙΑ ΣΥΜΜΕΤΟΧΗ ΣΕ ΕΠΙΣΤΗΜΟΝΙΚΗ ΕΡΕΥΝΑ

Καλείστε να συμμετάσχετε σε μία επιστημονική έρευνα του Τμήματος *Συμπληρώστε το Τμήμα του Πανεπιστημίου που διενεργεί την έρευνα* του Πανεπιστημίου Αιγαίου. Ο τίτλος της έρευνας είναι *Συμπληρώστε τον τίτλο της έρευνας*

Σκοπός της εν λόγω επιστημονικής έρευνας είναι *Να συμπληρωθεί το πεδίο από τον υπεύθυνο ερευνητή*

Προτού συμφωνήσετε με τη συμμετοχή σας στην έρευνα, βεβαιωθείτε ότι:

- Έχετε διαβάσει και κατανοήσει το έντυπο ενημέρωσης σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα που σας αφορούν στο πλαίσιο της εν λόγω έρευνας (εφεξής «Έντυπο Ενημέρωσης») και όποιες απορίες είχατε σχετικά με αυτήν απαντήθηκαν σε ικανοποιητικό βαθμό ☐
- Μέσω του Εντύπου Ενημέρωσης λάβατε γνώση σχετικά με τη διάρκεια της έρευνας και τις διαδικασίες της, ήτοι ποια δεδομένα προσωπικού χαρακτήρα που σας αφορούν πρόκειται να επεξεργαστούν στο πλαίσιο της έρευνας, ποια / ποιες πράξεις επεξεργασίας θα διενεργηθούν επί αυτών, σε ποιους πρόκειται να διαβιβαστούν τα δεδομένα σας, πόσο καιρό θα τηρηθούν από τον ερευνητή και πώς εξασφαλίζεται η ασφαλής τήρησή τους ☐
- Έχετε ενημερωθεί, μέσω του Εντύπου Ενημέρωσης, σχετικά με τα δικαιώματά σας, όπως αυτά απορρέουν από τον Γενικό Κανονισμό για την Προστασία Δεδομένων ☐
- Γνωρίζετε ότι η συμμετοχή σας στην εν λόγω επιστημονική έρευνα είναι εθελοντική ☐

Μπορείτε να αποχωρήσετε από την έρευνα ανά πάσα στιγμή, χωρίς καμία συνέπεια/κύρωση, ανακαλώντας τη συγκατάθεσή σας στο e-mail: *Να συμπληρωθεί το πεδίο από τον υπεύθυνο ερευνητή* ή με τη φυσική σας παρουσία στη διεύθυνση *Να συμπληρωθεί το πεδίο από τον υπεύθυνο ερευνητή*.

ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ

Ο ερευνητής / Η ερευνήτρια και το Πανεπιστήμιο δεσμεύεται να τηρεί πλήρη εμπιστευτικότητα για όλες τις πληροφορίες που θα αποκτηθούν στο πλαίσιο της συγκεκριμένης έρευνας και οι οποίες μπορούν να οδηγήσουν στην ταυτοποίησή σας.

Πιο συγκεκριμένα, δεδομένα που σας αφορούν θα δημοσιευτούν μόνο εφόσον υπάρχει η ρητή συγκατάθεσή σας ή είναι πλήρως ανωνυμοποιημένα. Επιπλέον, η επεξεργασία δεδομένων προσωπικού χαρακτήρα για τους σκοπούς της έρευνας υπόκειται σε κατάλληλες εγγυήσεις, ήτοι *Καταγράψτε τα μέτρα προστασίας που εφαρμόζονται στην εν λόγω επεξεργασία, όπως αυτά εντοπίστηκαν στα βήματα 4 και 7 της σχετικής διαδικασίας*

Για τυχόν απορίες σε θέματα αναφορικά με την επιστημονική έρευνα, μπορείτε να επικοινωνήσετε με τον υπεύθυνο ερευνητή (*Να συμπληρωθούν το όνομα και τα πλήρη στοιχεία επικοινωνίας του υπεύθυνου ερευνητή*), καθώς και με τον Υπεύθυνο Προστασίας Δεδομένων (εφεξής «ΥΠΔ») του Πανεπιστημίου για απορίες σχετικά με τα δεδομένα προσωπικού χαρακτήρα που σας αφορούν (*Να συμπληρωθούν το όνομα και τα πλήρη στοιχεία επικοινωνίας του ΥΠΔ*).

Θα σας δοθεί αντίγραφο του Εντύπου Ενημέρωσης και της παρούσας δήλωσης συγκατάθεσης, όταν η τελευταία έχει υπογραφεί.

Έχω διαβάσει τις ανωτέρω αναφερόμενες πληροφορίες και συμφωνώ να συμμετέχω στη συγκεκριμένη επιστημονική έρευνα.

Ονοματεπώνυμο συμμετέχοντος/συμμετέχουσας στην έρευνα: ……

……..……

Ημερομηνία: ……..

Υπογραφή: ……

Σε περίπτωση που ο υπεύθυνος ερευνητής / ερευνήτρια επιθυμεί μετά το πέρας της έρευνας να δημοσιεύσει δεδομένα προσωπικού χαρακτήρα που με αφορούν, ☐ **Συναινώ** ☐ **Δεν Συναινώ** σε αυτή του την ενέργεια.

Γ.11. Περιγραφή συμβόλων σχηματικής απεικόνισης διαδικασιών του ΓΚΠΔ

Στον παρακάτω πίνακα παρουσιάζονται τα σύμβολα και η περιγραφή τους που χρησιμοποιήθηκαν στην σχηματική απεικόνιση των διαδικασιών του ΓΚΠΔ για το Πανεπιστήμιο.

ΣΥΜΒΟΛΟ	ΠΕΡΙΓΡΑΦΗ	ΣΥΜΒΟΛΟ	ΠΕΡΙΓΡΑΦΗ
Αρχή	Δηλώνει την έναρξη της διαδικασίας.	Μητρώο	Δηλώνει την καταχώριση πληροφοριών σε Μητρώο.
Τέλος	Δηλώνει τη λήξη της διαδικασίας		Δηλώνει ότι οι ενέργειες που περικλείει εκτελούνται παράλληλα.
1. Ενέργεια	Δηλώνει ενέργεια σε μία διαδικασία.		Δηλώνει φόρμα.
Απόφαση	Δηλώνει απόφαση σε μία διαδικασία.		Δηλώνει αρχείο καταγραφής.
Οντότητα	Δηλώνει την οντότητα που είναι αρμόδια για την εκτέλεση της σχετικής ενέργειας.		Πανεπιστήμιο Αιγαίου.
1. Ανφορά σε άλλη διαδικασία	Χρησιμοποιείται όταν γίνεται αναφορά σε άλλες διαδικασίες.		Υποκείμενο των Δεδομένων / Φυσικό πρόσωπο.

Πίνακας 23: Περιγραφή συμβόλων σχηματικής απεικόνισης διαδικασιών του ΓΚΠΔ