



# ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

## *Πολιτική Ιδιωτικότητας και Προστασίας Δεδομένων*

Ιούνιος 2019

## Πίνακας Περιεχομένων

<b>A.1. Η ΠΟΛΙΤΙΚΗ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΚΑΙ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ .....</b>	<b>6</b>
A1.1. Εισαγωγή.....	6
A1.2. Σκοπός και στόχοι της Πολιτικής Προστασίας Δεδομένων .....	6
A1.3. Εμβέλεια εφαρμογής .....	6
<b>A.2. ΔΙΑΔΙΚΑΣΙΕΣ ΔΙΑΧΕΙΡΙΣΗΣ ΤΗΣ ΠΟΛΙΤΙΚΗΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ .....</b>	<b>7</b>
A2.1. Έγκριση Πολιτικής .....	7
A2.2. Ρόλοι και αρμοδιότητες για τη διαχείριση της Πολιτικής .....	7
A2.3. Αναθεώρηση Πολιτικής .....	7
A2.4. Εποπτεία εφαρμογής Πολιτικής .....	8
A2.5. Εσωτερική επιθεώρηση .....	8
<b>A.3. ΕΚΤΙΜΗΣΗ ΑΝΤΙΚΤΥΠΟΥ ΣΧΕΤΙΚΑ ΜΕ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ .....</b>	<b>8</b>
A3.1. Υλοποίηση Εκτίμησης Αντικτύπου για την Προστασία Δεδομένων .....	8
A3.2. Συχνότητα και εναύσματα εκπόνησης.....	8
<b>A.4. ΟΡΓΑΝΩΤΙΚΗ ΔΟΜΗ.....</b>	<b>9</b>
A4.1. Υπεύθυνος Προστασίας Δεδομένων.....	9
A4.2. Οργανόγραμμα .....	10
<b>A.5. ΝΟΜΙΜΟΤΗΤΑ ΤΗΣ ΕΠΕΞΕΡΓΑΣΙΑΣ .....</b>	<b>10</b>
A5.1. Έλεγχος νομιμότητας επεξεργασίας .....	10
A5.2. Νομική Βάση Επεξεργασίας .....	10
A5.3. Συγκατάθεση ως βάση για την Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα .....	11
A5.4. Δευτερεύουσα χρήση δεδομένων .....	13
A5.5. Διατήρηση της Ποιότητας των Δεδομένων .....	13
A5.6. Ελαχιστοποίηση Δεδομένων .....	13
A5.7. Χρονικό Διάστημα Διατήρησης Δεδομένων .....	13
A5.8. Διαδικασία για τη Διαχείριση Αρχείου Δραστηριοτήτων Επεξεργασίας.....	13
<b>A.6. ΙΚΑΝΟΠΟΙΗΣΗ ΔΙΚΑΙΩΜΑΤΩΝ ΤΩΝ ΥΠΟΚΕΙΜΕΝΩΝ ΤΩΝ ΔΕΔΟΜΕΝΩΝ .....</b>	<b>13</b>
A6.1. Δικαίωμα Ενημέρωσης.....	13
A6.2. Δικαίωμα Πρόσβασης .....	14
A6.3. Δικαίωμα Διόρθωσης .....	15
A6.4. Δικαίωμα Διαγραφής .....	15
A6.5. Δικαίωμα Περιορισμού Επεξεργασίας .....	15

A6.6.	Δικαίωμα Φορητότητας Δεδομένων .....	15
A6.7.	Δικαίωμα Εναντίωσης .....	15
A6.8.	Διαδικασία για τη Διαχείριση Αιτημάτων Φυσικών Προσώπων .....	15
A6.9.	Ρόλοι και αρμοδιότητες για τα δικαιώματα των Υποκειμένων των Δεδομένων .....	15
<b>A.7.</b>	<b>ΔΙΑΒΙΒΑΣΗ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ ΣΕ ΤΡΙΤΕΣ ΧΩΡΕΣ.....</b>	<b>16</b>
<b>A.8.</b>	<b>ΔΙΑΧΕΙΡΙΣΗ ΤΡΙΤΩΝ – ΕΚΤΕΛΟΥΝΤΩΝ ΕΠΕΞΕΡΓΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ</b>	<b>16</b>
<b>A.9.</b>	<b>ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ ΚΑΤΑ ΤΗ ΔΙΑΒΙΒΑΣΗ Η ΚΟΙΝΟΠΟΙΗΣΗ .....</b>	<b>16</b>
<b>A.10.</b>	<b>ΕΝΣΩΜΑΤΩΣΗ ΠΡΟΔΙΑΓΡΑΦΩΝ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΑΠΟ ΤΟ ΣΧΕΔΙΑΣΜΟ ΚΑΙ ΕΞ’ ΟΡΙΣΜΟΥ .....</b>	<b>16</b>
A10.1.	Προδιαγραφές Προστασίας Δεδομένων κατά το Σχεδιασμό Συστημάτων και εξ’ Ορισμού .....	16
A10.2.	Διαδικασίες για την Προμήθεια Συστημάτων.....	17
<b>A.11.</b>	<b>ΑΝΤΙΜΕΤΩΠΙΣΗ ΠΕΡΙΣΤΑΤΙΚΩΝ ΠΑΡΑΒΙΑΣΗΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ .....</b>	<b>17</b>
A11.1.	Γνωστοποίηση στην Εποπτική Αρχή .....	17
A11.2.	Διαδικασίες που επιτρέπουν την έγκαιρη γνωστοποίηση .....	18
A11.3.	Ανακοίνωση σε Υποκείμενα των Δεδομένων .....	18
A11.4.	Διαδικασία για τη Διαχείριση Αστοχιών.....	18
A11.5.	Διαδικασία για τη Διαχείριση Καταγγελιών .....	18
A11.6.	Ρόλοι και αρμοδιότητες για τη διαχείριση περιστατικών παραβίασης .....	19
<b>A.12.</b>	<b>ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΕΝΗΜΕΡΟΤΗΤΑ ΤΟΥ ΠΡΟΣΩΠΙΚΟΥ .....</b>	<b>19</b>
A12.1.	Ενημερότητα Προσωπικού .....	19
A12.2.	Εκπαίδευση Εξειδικευμένου Προσωπικού .....	19
<b>A.13.</b>	<b>ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΚΑΙ ΜΕΤΡΗΣΗ ΑΠΟΔΟΣΗΣ .....</b>	<b>19</b>

## Εισαγωγή

Η Πολιτική Ιδιωτικότητας και Προστασίας Δεδομένων αποτυπώνει την πρόθεση του Πανεπιστημίου Πειραιώς να προστατέψει τα δεδομένα προσωπικού χαρακτήρα που συλλέγει και επεξεργάζεται στο πλαίσιο των σκοπών επεξεργασίας που επιτελεί.

Η Πολιτική Ιδιωτικότητας και Προστασίας Δεδομένων περιγράφει το σύνολο των αρχών και κανόνων που καθορίζουν τον τρόπο με τον οποίο το Πανεπιστήμιο Πειραιώς, ως υπεύθυνος επεξεργασίας, διαχειρίζεται και προστατεύει 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 (γνωστός και ως ΓΚΠΔ ή GDPR). Ο ΓΚΠΔ θέτει το πλαίσιο βάσει του οποίου το Πανεπιστήμιο Πειραιώς εκτελεί δραστηριότητες σχετικές με την επεξεργασία δεδομένων. Σε περίπτωση που υπάρξει παραβίαση του Κανονισμού, ο οποίος είναι σχεδιασμένος για να προστατεύει τα δεδομένα προσωπικού χαρακτήρα όσων βρίσκονται στην Ευρωπαϊκή Ένωση, είναι πιθανό να επιβληθούν σημαντικά πρόστιμα. Είναι πολιτική του Πανεπιστημίου Πειραιώς να εξασφαλίσει ότι η συμμόρφωσή με το ΓΚΠΔ και άλλες σχετικές νομοθεσίες είναι ξεκάθαρη και μπορεί να αποδειχτεί ανά πάσα στιγμή.

Οι πλέον σημαντικοί ορισμοί του ΓΚΠΔ που σχετίζονται με τη συγκεκριμένη πολιτική του Πανεπιστημίου Πειραιώς ακολουθούν στη συνέχεια.

**Ως δεδομένα Προσωπικού Χαρακτήρα** χαρακτηρίζεται: κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»): το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου.

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

«**Υπεύθυνος επεξεργασίας**» σημαίνει: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα: όταν οι σκοποί και ο τρόπος της επεξεργασίας αυτής καθορίζονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια για τον διορισμό του μπορούν να προβλέπονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους.

Τέλος, οι βασικές αρχές στις οποίες στηρίζεται ο Γενικός Κανονισμός Προστασίας Δεδομένων και τις οποίες το Πανεπιστήμιο Πειραιώς διασφαλίζει ότι συμμορφώνεται, είναι οι παρακάτω:

## 1. Τα Δεδομένα Προσωπικού Χαρακτήρα πρέπει να :

(α) υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων («νομιμότητα, αντικειμενικότητα και διαφάνεια»),

(β) συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς· η περαιτέρω επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς δεν θεωρείται ασύμβατη με τους αρχικούς σκοπούς σύμφωνα με το άρθρο 89 παράγραφος 1 («περιορισμός του σκοπού»),

(γ) είναι κατάλληλα, συναφή και περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία («ελαχιστοποίηση των δεδομένων»),

(δ) είναι ακριβή και, όταν είναι αναγκαίο, επικαιροποιούνται· πρέπει να λαμβάνονται όλα τα εύλογα μέτρα για την άμεση διαγραφή ή διόρθωση δεδομένων προσωπικού χαρακτήρα τα οποία είναι ανακριβή, σε σχέση με τους σκοπούς της επεξεργασίας («ακρίβεια»),

(ε) διατηρούνται υπό μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων μόνο για το διάστημα που απαιτείται για τους σκοπούς της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα· τα δεδομένα προσωπικού χαρακτήρα μπορούν να αποθηκεύονται για μεγαλύτερα διαστήματα, εφόσον τα δεδομένα προσωπικού χαρακτήρα θα υποβάλλονται σε επεξεργασία μόνο για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς, σύμφωνα με το άρθρο 89 παράγραφος 1 και εφόσον εφαρμόζονται τα κατάλληλα τεχνικά και οργανωτικά μέτρα που απαιτεί ο παρών κανονισμός για τη διασφάλιση των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων («περιορισμός της περιόδου αποθήκευσης»),

(στ) υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλεια των δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά, με τη χρησιμοποίηση κατάλληλων τεχνικών ή οργανωτικών μέτρων («ακεραιότητα και εμπιστευτικότητα»).

2. Ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και είναι σε θέση να αποδείξει τη συμμόρφωση με την παράγραφο 1 («λογοδοσία»).

## **A.1. Η Πολιτική Ιδιωτικότητας και Προστασίας Δεδομένων**

### **A1.1. Εισαγωγή**

Η Πολιτική Ιδιωτικότητας και Προστασίας Δεδομένων περιλαμβάνει γενικά τον σκοπό και τους στόχους που θέτει η διοίκηση του Πανεπιστημίου Πειραιώς αναφορικά με την προστασία δεδομένων προσωπικού χαρακτήρα, καθώς και τις οδηγίες, διαδικασίες, κανόνες, ρόλους και υπευθυνότητες που αφορούν στην προστασία των δεδομένων αυτών. Οι οδηγίες, κανόνες και διαδικασίες που περιλαμβάνονται στην Πολιτική Ιδιωτικότητας και Προστασίας Δεδομένων υλοποιούνται με την εφαρμογή των κατάλληλων τεχνικών, οργανωτικών και διαδικαστικών μέτρων προστασίας.

Την Πολιτική Ιδιωτικότητας και Προστασίας Δεδομένων θα πρέπει να γνωρίζουν και να ακολουθούν όλα τα μέλη του φορέα αναφορικά με όλες τις δραστηριότητές τους που έχουν σχέση με δεδομένα, επιχειρησιακές διαδικασίες και πληροφοριακά συστήματα που καλύπτει η Πολιτική.

### **A1.2. Σκοπός και στόχοι της Πολιτικής Προστασίας Δεδομένων**

Σκοπός της Πολιτικής Ιδιωτικότητας και Προστασίας Δεδομένων είναι να παράσχει στρατηγική καθοδήγηση στη διοίκηση του Πανεπιστημίου και στο προσωπικό του για την προστασία των προσωπικών δεδομένων κατά την επεξεργασία τους.

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

- Την προστασία των φυσικών προσώπων των οποίων τα προσωπικά δεδομένα επεξεργάζεται το Πανεπιστήμιο Πειραιώς.
- Την αναγνώριση των κινδύνων που ενέχει η επεξεργασία προσωπικών δεδομένων που πραγματοποιεί το Πανεπιστήμιο Πειραιώς 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 Πειραιώς.
- Τη συμμόρφωση με τις απαιτήσεις που απορρέουν από την ελληνική Νομοθεσία.

Η Πολιτική Ιδιωτικότητας και Προστασίας Δεδομένων επιχειρεί να ορίσει κοινά αποδεκτές αρχές, τρόπους και αρμοδιότητες που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

### **A1.3. Εμβέλεια εφαρμογής**

Η Πολιτική Ιδιωτικότητας και Προστασίας Δεδομένων αφορά στο σύνολο των δεδομένων προσωπικού χαρακτήρα που επεξεργάζεται το Πανεπιστήμιο Πειραιώς, με αυτοματοποιημένα ή μη αυτοματοποιημένα μέσα, σύμφωνα με τα οριζόμενα στο Άρθρο 4 του Γενικού Κανονισμού

για την Προστασία Δεδομένων 2016/679. Η Πολιτική Ιδιωτικότητας και Προστασίας Δεδομένων αφορά στο σύνολο των επιχειρησιακών διεργασιών που περιλαμβάνουν επεξεργασία δεδομένων προσωπικού χαρακτήρα.

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

## **A.2. Διαδικασίες Διαχείρισης της Πολιτικής Προστασίας Δεδομένων**

### **A2.1. Έγκριση Πολιτικής**

Η Πολιτική Ιδιωτικότητας και Προστασίας Δεδομένων εγκρίνεται από την ανώτερη διοίκηση του Πανεπιστημίου Πειραιώς, κοινοποιείται σε όλους τους υπαλλήλους και τους αρμόδιους συνεργάτες.

### **A2.2. Ρόλοι και αρμοδιότητες για τη διαχείριση της Πολιτικής**

Το Πανεπιστήμιο Πειραιώς υλοποιεί ένα οργανωτικό πλαίσιο σύμφωνα με το οποίο υπάρχουν ρόλοι με αρμοδιότητες για την προστασία προσωπικών δεδομένων. Το πλαίσιο περιλαμβάνει τους εξής 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 την εφαρμογή αυτής της Πολιτικής απονέμονται από τη διοίκηση και καταγράφονται.

### **A2.3. Αναθεώρηση Πολιτικής**

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

## **A2.4. Εποπτεία εφαρμογής Πολιτικής**

Η εφαρμογή της Πολιτικής Ιδιωτικότητας και Προστασίας Δεδομένων και οι κανόνες που απορρέουν από αυτήν αξιολογούνται από κατάλληλες διαδικασίες ελέγχου που ορίζει ο Υπεύθυνος Προστασίας Δεδομένων.

## **A2.5. Εσωτερική επιθεώρηση**

Το Πανεπιστήμιο Πειραιώς οφείλει να πραγματοποιεί σε ετήσια βάση εσωτερική επιθεώρηση των πληροφοριακών συστημάτων και των οργανωτικών, διαδικαστικών και τεχνικών αντιστάσεων που περιγράφει η Πολιτική Ιδιωτικότητας και 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 Πειραιώς επιλέγει την ομάδα επιθεωρητών και αναθέτει αρμοδιότητες στους επιθεωρητές.

## **A.3. Εκτίμηση Αντικτύπου σχετικά με την Προστασία Δεδομένων**

### **A3.1. Υλοποίηση Εκτίμησης Αντικτύπου για την Προστασία Δεδομένων**

Το Πανεπιστήμιο Πειραιώς έχει 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 Υπεύθυνος Προστασίας Δεδομένων μεριμνά ώστε η μέθοδος εκτίμησης αντικτύπου για την προστασία δεδομένων ικανοποιεί τις εξής 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 Πειραιώς καταγράφει σε επίσημο έγγραφο την αναλυτική περιγραφή της μεθόδου που εφαρμόζεται για την ανάλυση αντικτύπου. Ο Υπεύθυνος Προστασίας Δεδομένων εφαρμόζει τη μέθοδο και ο φορέας καταγράφει σε διακριτό έγγραφο τα αποτελέσματα της εφαρμογής.

### **A3.2. Συχνότητα και εναύσματα εκπόνησης**

Ο Υπεύθυνος Προστασίας Δεδομένων καθορίζει κριτήρια και εναύσματα επανάληψης της εκτίμησης αντικτύπου, ώστε να εκπονείται κάθε φορά που υπάρχουν σημαντικές εξελίξεις και



αλλαγές στη λειτουργία του Πανεπιστημίου Πειραιώς ή στις τεχνικές επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

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

## **A.4. Οργανωτική Δομή**

### **A4.1. Υπεύθυνος Προστασίας Δεδομένων**

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

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

Ο Υπεύθυνος Προστασίας Δεδομένων μπορεί να έχει και άλλες αρμοδιότητες αλλά ο φορέας εξασφαλίζει ότι δεν δημιουργείται «σύγκρουση συμφερόντων» εξαιτίας των πρόσθετων αυτών επαγγελματικών καθηκόντων και υποχρεώσεων.

Ο Υπεύθυνος Προστασίας Δεδομένων έχει αρμοδιότητα για όλα τα θέματα που αφορούν στην προστασία προσωπικών δεδομένων στον φορέα. Για το λόγο αυτό, πρέπει να έχει πρόσβαση σε όλες τις βάσεις δεδομένων και στα συστήματα του φορέα. Ο Υπεύθυνος Προστασίας Δεδομένων δεσμεύεται από όρους εμπιστευτικότητας.

#### **A4.1.1. Αρμοδιότητες του Υπεύθυνου Προστασίας Δεδομένων**

Το Πανεπιστήμιο Πειραιώς αναθέτει στον Υπεύθυνο Προστασίας Δεδομένων τις εξής αρμοδιότητες:

- Να εκπροσωπεί το Πανεπιστήμιο Πειραιώς έναντι των Αρχών, εθνικών και Ευρωπαϊκών.
- Να συμβουλεύει την ανώτερη διοίκηση σε θέματα προστασίας προσωπικών δεδομένων
- 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 σημαντικότερων και βαρύτερων διοικητικών προστίμων που προβλέπονται από τον Κανονισμό.
- Να εξασφαλίζει την υποστήριξη της ανώτερης διοίκησης και τον απαιτούμενο προϋπολογισμό για την εφαρμογή του προγράμματος προστασίας των δεδομένων.
- Να καταρτίζει το πρόγραμμα και την Πολιτική Ιδιωτικότητας και 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 σχεδιάζει και να πραγματοποιεί εσωτερικά εκπαιδευτικά προγράμματα και να τηρεί τα απαιτούμενα αρχεία ολοκλήρωσης των εκπαιδύσεων ανά τμήμα/ομάδα εργαζομένων.

## **A4.2. Οργανόγραμμα**

Η οργανωτική δομή του Πανεπιστημίου Πειραιώς θα πρέπει να αποτυπώνει τον διακριτό ρόλο του Υπεύθυνου Προστασίας Δεδομένων.

## **A.5. Νομιμότητα της Επεξεργασίας**

### **A5.1. Έλεγχος νομιμότητας επεξεργασίας**

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

### **A5.2. Νομική Βάση Επεξεργασίας**

Υπάρχουν έξι εναλλακτικοί τρόποι με τους οποίους μπορεί να θεσπιστεί στο πλαίσιο του ΓΚΠΔ, η νομιμότητα επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

**Συγκατάθεση:** Όπου απαιτείται το Πανεπιστήμιο Πειραιώς 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 τα δεδομένα τους, όπως το δικαίωμα ανάκλησης της συναίνεσης. Οι πληροφορίες αυτές θα παρέχονται σε προσιτή μορφή, γραμμένη σε σαφή γλώσσα και δωρεάν.

**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 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 Πειραιώς 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 Πειραιώς 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 δημοσίου 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 Πειραιώς 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 πίσω από αυτή την άποψη θα τεκμηριωθεί.

### **A5.3. Συγκατάθεση ως βάση για την Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα**

Το Πανεπιστήμιο Πειραιώς 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.

#### **A5.3.1. Πληροφόρηση Υποκειμένων των Δεδομένων**

Πριν τη διαδικασία λήψης συγκατάθεσης, Το Πανεπιστήμιο Πειραιώς 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 Προστασίας Δεδομένων.

- 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 δικαιώματά του.

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

Το Πανεπιστήμιο Πειραιώς οφείλει να ενημερώνει το Υποκείμενο των Δεδομένων σε περίπτωση που τα δεδομένα που κατέχει δεν έχουν συλλεγεί από το Υποκείμενο των Δεδομένων.

#### A5.3.2. 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.

#### A5.3.3. Αρχείο Συγκαταθέσεων

Το Πανεπιστήμιο Πειραιώς πρέπει να είναι σε θέση να αποδείξει ότι έχει καταγράψει τη συγκατάθεση των Υποκειμένων των Δεδομένων αναφορικά με την επεξεργασία των προσωπικών τους δεδομένων. Προς αυτή την κατεύθυνση θα δημιουργηθεί αρχείο 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 αποθηκεύεται με ασφαλή τρόπο και μπορεί να χρησιμοποιηθεί σε περίπτωση ελέγχου.

#### **A5.4. Δευτερεύουσα χρήση δεδομένων**

Το Πανεπιστήμιο Πειραιώς οφείλει να ενημερώνει το Υποκείμενο των Δεδομένων και να λαμβάνει τη συγκατάθεσή του, για χρήση των δεδομένων για σκοπό διαφορετικό από αυτόν για τον οποίο συλλέχθηκαν τα δεδομένα.

#### **A5.5. Διατήρηση της Ποιότητας των Δεδομένων**

Το Πανεπιστήμιο Πειραιώς οφείλει να διατηρεί την ποιότητα των δεδομένων.

#### **A5.6. Ελαχιστοποίηση Δεδομένων**

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

#### **A5.7. Χρονικό Διάστημα Διατήρησης Δεδομένων**

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

#### **A5.8. Διαδικασία για τη Διαχείριση Αρχείου Δραστηριοτήτων Επεξεργασίας**

Το Πανεπιστήμιο Πειραιώς οφείλει να διατηρεί αρχείο δραστηριοτήτων επεξεργασίας. 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.

### **A.6. Ικανοποίηση Δικαιωμάτων των Υποκειμένων των Δεδομένων**

#### **A6.1. Δικαίωμα Ενημέρωσης**

Εφόσον τα δεδομένα των φυσικών προσώπων έχουν συλλεγεί από τα ίδια τα Υποκείμενα των Δεδομένων, το Πανεπιστήμιο Πειραιώς οφείλει να ενημερώνει τους χρήστες για τα παρακάτω:

- Την ταυτότητα και τα στοιχεία επικοινωνίας του Υπεύθυνου Επεξεργασίας (ή εκπροσώπου αυτού).
- Τα στοιχεία επικοινωνίας του Υπεύθυνου Προστασίας Δεδομένων.
- 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 (πιθανά 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, ο φορέας, 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).

## **A6.2. Δικαίωμα Πρόσβασης**

Το Πανεπιστήμιο Πειραιώς υποστηρίζει διαδικασία με την οποία 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, παρέχονται 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.

### **A6.3. Δικαίωμα Διόρθωσης**

Το Πανεπιστήμιο Πειραιώς υποστηρίζει διαδικασία με την οποία οι χρήστες θα μπορούν να διορθώνουν ή να ζητούν τη διόρθωση, χωρίς κόστος, για τα προσωπικά δεδομένα που διατηρεί για εκείνους.

### **A6.4. Δικαίωμα Διαγραφής**

Το Πανεπιστήμιο Πειραιώς υποστηρίζει διαδικασία με την οποία οι χρήστες θα μπορούν να διαγράψουν, ή να ζητούν τη διαγραφή, χωρίς κόστος, για τα προσωπικά δεδομένα που διατηρεί για εκείνους.

### **A6.5. Δικαίωμα Περιορισμού Επεξεργασίας**

Το Πανεπιστήμιο Πειραιώς υποστηρίζει διαδικασία με την οποία οι χρήστες θα μπορούν να αιτηθούν περιορισμό της επεξεργασίας.

### **A6.6. Δικαίωμα Φορητότητας Δεδομένων**

Το Πανεπιστήμιο Πειραιώς υποστηρίζει διαδικασία με την οποία οι χρήστες θα μπορούν να μεταβιβάζουν, ή να ζητούν τη μεταβίβαση, χωρίς κόστος, των προσωπικών δεδομένων τους σε άλλον φορέα.

### **A6.7. Δικαίωμα Εναντίωσης**

Το Πανεπιστήμιο Πειραιώς υποστηρίζει διαδικασία με την οποία οι χρήστες θα μπορούν να δηλώσουν την εναντίωσή τους όσον αφορά στην επεξεργασία των δεδομένων τους, συμπεριλαμβανομένης της κατάρτισης προφίλ των χρηστών.

### **A6.8. Διαδικασία για τη Διαχείριση Αιτημάτων Φυσικών Προσώπων**

Το Πανεπιστήμιο Πειραιώς διαθέτει στον ιστότοπο του φόρμα την οποία μπορεί να χρησιμοποιήσει το Υποκείμενο των Δεδομένων ώστε να υποβάλει αίτημα που εμπίπτει στα δικαιώματά του.

### **A6.9. Ρόλοι και αρμοδιότητες για τα δικαιώματα των Υποκειμένων των Δεδομένων**

Ο Υπεύθυνος Προστασίας Δεδομένων διαχειρίζεται τα αιτήματα των Υποκειμένων των Δεδομένων. Το Πανεπιστήμιο Πειραιώς 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).

## **A.7. Διαβίβαση Δεδομένων Προσωπικού Χαρακτήρα σε τρίτες χώρες**

Το Πανεπιστήμιο Πειραιώς 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.

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

## **A.8. Διαχείριση Τρίτων – Εκτελούντων Επεξεργασία Προσωπικών Δεδομένων**

Εφόσον το Πανεπιστήμιο Πειραιώς 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.

## **A.9. Προστασία δεδομένων κατά τη διαβίβαση ή κοινοποίηση**

Το Πανεπιστήμιο Πειραιώς υποστηρίζει διαδικασία με 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 εμπλεκόμενων ακολουθεί τους κανόνες που ορίζει το Πανεπιστήμιο Πειραιώς.

## **A.10. Ενσωμάτωση Προδιαγραφών Προστασίας Δεδομένων από το Σχεδιασμό και Εξ' Ορισμού**

### **A10.1. Προδιαγραφές Προστασίας Δεδομένων κατά το Σχεδιασμό Συστημάτων και εξ' Ορισμού**

Το Πανεπιστήμιο Πειραιώς 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 συμβουλευεται τον Υπεύθυνο Προστασίας Δεδομένων και επιλέγει μέθοδο ανάπτυξης συστημάτων που επιτρέπει την αναγνώριση και μοντελοποίηση των προδιαγραφών προστασίας δεδομένων, κατά την ανάλυση των συνολικών προδιαγραφών κάθε νέου συστήματος και πριν την υλοποίηση του συστήματος αυτού. 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.

## **A10.2. Διαδικασίες για την Προμήθεια Συστημάτων**

Το Πανεπιστήμιο Πειραιώς μεριμνά κατά την προμήθεια νέων συστημάτων για την αναγνώριση και διασφάλιση προδιαγραφών προστασίας δεδομένων προσωπικού χαρακτήρα. Ο Υπεύθυνος Ανάπτυξης Πληροφοριακών Συστημάτων συμβουλευτεί τον Υπεύθυνο Προστασίας Δεδομένων και διασφαλίζει ότι κάθε προκήρυξη προμήθειας νέου πληροφοριακού συστήματος περιλαμβάνει στις υποχρεώσεις του αναδόχου υλοποίησης την αναγνώριση και μοντελοποίηση προδιαγραφών 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 προσφέρουν.

## **A.11. Αντιμετώπιση Περιστατικών Παραβίασης Δεδομένων Προσωπικού Χαρακτήρα**

Το Πανεπιστήμιο Πειραιώς 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 υπονόμηση 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 επιτευχθεί, 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.

### **A11.1. Γνωστοποίηση στην Εποπτική Αρχή**

Όταν συμβεί/εντοπιστεί πιθανή παραβίαση δεδομένων, και εφόσον υπάρχει κίνδυνος για φυσικά πρόσωπα, Το Πανεπιστήμιο Πειραιώς 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 (Πανεπιστήμιο Πειραιώς) 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 κάθε έναν από αυτούς.

### **A11.2. Διαδικασίες που επιτρέπουν την έγκαιρη γνωστοποίηση**

Το Πανεπιστήμιο Πειραιώς υποστηρίζει διαδικασία που περιγράφει τον τρόπο επικοινωνίας του με την εποπτική Αρχή, και τις πληροφορίες που θα τους κοινοποιήσει. Το Πανεπιστήμιο Πειραιώς 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 Υπεύθυνου Προστασίας Δεδομένων.
- Τις ενδεχόμενες συνέπειες που μπορεί να επιφέρει η παραβίαση.
- Τα ληφθέντα ή προτεινόμενα προς λήψη μέτρα για την αντιμετώπιση της παραβίασης.

### **A11.3. Ανακοίνωση σε Υποκείμενα των Δεδομένων**

Το Πανεπιστήμιο Πειραιώς 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 Πειραιώς υποστηρίζει διαδικασία που περιγράφει 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.

Η διαδικασία περιλαμβάνει παροχή πληροφοριών μέσω εντύπων, ηλεκτρονικά, ή και προφορικά – εφόσον έχει επιβεβαιωθεί η ταυτότητα του Υποκειμένου των Δεδομένων.

### **A11.4. Διαδικασία για τη Διαχείριση Αστοχιών**

Με χρήση κατάλληλων τεχνολογιών, Το Πανεπιστήμιο Πειραιώς 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 Πειραιώς υποστηρίζει κατάλληλη διαδικασία ώστε να μπορεί να αιτιολογήσει/τεκμηριώσει τους μηχανισμούς ασφάλειας που έχει εφαρμόσει.

### **A11.5. Διαδικασία για τη Διαχείριση Καταγγελιών**

Το Πανεπιστήμιο Πειραιώς υποστηρίζει 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.

## **A11.6. Ρόλοι και αρμοδιότητες για τη διαχείριση περιστατικών παραβίασης**

Το Πανεπιστήμιο Πειραιώς έχει δημιουργήσει εσωτερική ομάδα αντιμετώπισης παραβιάσεων η οποία είναι υπεύθυνη για τον περιορισμό, την αντιμετώπιση και την ανάκτηση λειτουργίας του φορέα.

Οι ρόλοι και οι υπευθυνότητες των συμμετεχόντων πρέπει να είναι ξεκάθαροι/ες. Ο Υπεύθυνος Προστασίας Δεδομένων προτείνεται να είναι ο επικεφαλής διοίκησης της ομάδας.

Η ομάδα οφείλει να καταγράψει τα αποδεικτικά στοιχεία ενός περιστατικού.

## **A.12. Εκπαίδευση και Ενημερότητα του Προσωπικού**

Το Πανεπιστήμιο Πειραιώς 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 (εγχειρίδια, εργαλεία) για την ορθή και ασφαλή χρήση των πληροφοριακών συστημάτων που διαχειρίζονται προσωπικά δεδομένα. Το Πανεπιστήμιο Πειραιώς παρέχει, επίσης, σε περιοδική βάση εκπαίδευση στο εξειδικευμένο προσωπικό (όπως το προσωπικό πληροφορικής) 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.

### **A12.1. Ενημερότητα Προσωπικού**

Το Πανεπιστήμιο Πειραιώς μεριμνά ώστε το προσωπικό του 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.

### **A12.2. Εκπαίδευση Εξειδικευμένου Προσωπικού**

Το Πανεπιστήμιο Πειραιώς διασφαλίζει ότι το προσωπικό του διαθέτει τις γνώσεις και τις δεξιότητες για την εφαρμογή της Πολιτικής Ιδιωτικότητας και Προστασίας Δεδομένων. Προς αυτή τη κατεύθυνση αξιολογεί τακτικά (τουλάχιστον ετησίως) τις σχετικές γνώσεις και δεξιότητες.

## **A.13. Παρακολούθηση και Μέτρηση Απόδοσης**

Το Πανεπιστήμιο Πειραιώς διαθέτει πλάνο παρακολούθησης και αξιολόγησης της αποτελεσματικότητας της Πολιτικής Προστασίας Δεδομένων. Το πλάνο 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