ΠΟΛΙΤΙΚΗ ΑΠΟΡΡΗΤΟΥ ΚΑΙ ΑΣΦΑΛΕΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Έκδοση 0.2 – Μάιος 2025

Η παρούσα Πολιτική Απορρήτου και Ασφαλείας ΔΠΧ εφαρμόζεται από το ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ (Εφεξής «το Πανεπιστήμιο»)

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Ι. Εισαγωγή, περιεχόμενο & πεδίο εφαρμογής

Ι.1. Εισαγωγή

Αποτελεί δέσμευση του Πανεπιστημίου Κρήτης, αφενός, η τήρηση του απορρήτου και της ασφάλειας των Δεδομένων Προσωπικού Χαρακτήρα (στο εξής, ΔΠΧ), τα οποία συλλέγονται κατά την άσκηση των δραστηριοτήτων του και, αφετέρου, η συμμόρφωσή του με τους εφαρμοστέους νόμους και κανονισμούς σχετικά με την επεξεργασία ΔΠΧ, συμπεριλαμβανομένων των Δεδομένων Ειδικών Κατηγοριών.

Η πολιτική αυτή στοχεύει να διασφαλίσει ότι η διαχείριση των ΔΠΧ γίνεται σύμφωνα με:

- τον Κανονισμό (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 (L 119)[1] και την εν γένει εφαρμοστέα ευρωπαϊκή νομοθεσία για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας ΔΠΧ και για την ελεύθερη κυκλοφορία των δεδομένων αυτών
- τον εφαρμοστικό νόμο 4624/2019 "Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις"
- κάθε σχετική εθνική νομοθεσία

Το Πανεπιστήμιο, ενεργών ως Υπεύθυνος Επεξεργασίας των ΔΠΧ ή ως εκτελών την επεξεργασία ΔΠΧ διασφαλίζει ότι η πολιτική αυτή θα επικαιροποιείται και θα γνωστοποιείται με κάθε πρόσφορο μέσο τόσο στα μέλη και το προσωπικό του όσο και στους τρίτους συναλλασσόμενους με αυτή.

Ι.2. Περιεχόμενο

Στο πλαίσιο των δραστηριοτήτων του, το Πανεπιστήμιο Κρήτης συλλέγει και επεξεργάζεται ΔΠΧ, σύμφωνα με τους ισχύοντες νόμους και κανονισμούς για την προστασία των ΔΠΧ και την ελεύθερη κυκλοφορία τους. Για το σκοπό αυτό, το Πανεπιστήμιο Κρήτης έχει υιοθετήσει και εφαρμόζει πολιτικές και διαδικασίες για τη σύννομη επεξεργασία των ΔΠΧ,

[1] Γενικός Κανονισμός για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα ή ΓΚΠΔ.

διασφαλίζοντας το απόρρητο και την ασφάλειά τους και την προστασία των δικαιωμάτων των Υποκειμένων των Δεδομένων.

Στην Πολιτική αυτή συνοψίζονται όλες οι διαδικασίες και οι αρχές, που διέπουν τη σύννομη επεξεργασία των ΔΠΧ προς εξασφάλιση της συμμόρφωσης με τους νόμους και τους κανονισμούς για την προστασία των ΔΠΧ εντός του Πανεπιστημίου Κρήτης.

Το περιεχόμενο της παρούσας Πολιτικής περιλαμβάνει τα εξής:

•Τις αρχές, που διέπουν την προστασία των ΔΠΧ, με τις οποίες το Πανεπιστήμιο Κρήτης οφείλει να συμμορφώνεται.

•Τα οργανωτικά και τεχνικά μέτρα ασφαλείας, που θα πρέπει να λάβει το Πανεπιστήμιο Κρήτης.

•Τις Πολιτικές για τη διασφάλιση της συμμόρφωσης προς την ισχύουσα νομοθεσία:

- Πολιτική Διαβίβασης ΔΠΧ
- Πολιτική Διατήρησης ΔΠΧ
- Πολιτική Συγκατάθεσης
- Πολιτική για την προστασία των δικαιωμάτων του Υποκειμένου Δεδομένων
- Πολιτική για την αντιμετώπιση παραβίασης ΔΠΧ

• Παραρτήματα

Ι.3. Πεδίο Εφαρμογής

Η Πολιτική αυτή δεσμεύει και εφαρμόζεται από όλες τις Σχολές, Τμήματα, Τομείς, Υπηρεσίες, Μονάδες και Δομές του Πανεπιστημίου Κρήτης, από το πανεπιστημιακό, διοικητικό, οικονομικό, τεχνικό, βοηθητικό και λοιπό προσωπικό του (ανεξάρτητα από τη συμβατική σχέση που τα συνδέει), καθώς και τους φοιτητές του (προπτυχιακούς, μεταπτυχιακούς, διδακτορικούς, μεταδιδακτορικούς, απόφοιτους). Αφορά κάθε δραστηριότητα στο πλαίσιο της οποίας συλλέγονται, χρησιμοποιούνται, αποθηκεύονται και τυγχάνουν κάθε είδους επεξεργασία τα ΔΠΧ.

Σύμφωνα με τον ορισμό των ΔΠΧ, που παρατίθεται πιο κάτω, τα ΔΠΧ μπορούν να αφορούν στο πιο πάνω προσωπικό του Πανεπιστημίου Κρήτης, τους εργαζόμενούς του, τους ως άνω φοιτητές του, αλλά και, εν γένει, όλα τα φυσικά πρόσωπα, που συνδέονται καθ' οιονδήποτε τρόπο με το Πανεπιστήμιο ως συνεργάτες, προμηθευτές, εργολάβοι και υπεργολάβοι και πελάτες του.

II. Ορισμοί & Αρχές που διέπουν την επεξεργασία ΔΠΧ

II.1. Ορισμοί

Ακολουθούν οι ορισμοί όλων των αναγκαίων όρων της παρούσας Πολιτικής (που αναφέρονται με κεφαλαία γράμματα στις πολιτικές και διαδικασίες) που ακολουθεί το Πανεπιστήμιο Κρήτης.

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

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

3) «**Περιορισμός της Επεξεργασίας**»: η επισήμανση αποθηκευμένων δεδομένων προσωπικού χαρακτήρα με στόχο τον περιορισμό της επεξεργασίας τους στο μέλλον,

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

5) «**Ψευδωνυμοποίηση**»: η επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο ώστε τα δεδομένα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρωματικές πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλιστεί ότι δεν μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο,

6) «**Σύστημα Αρχειοθέτησης**»: κάθε διαρθρωμένο σύνολο δεδομένων προσωπικού χαρακτήρα τα οποία είναι προσβάσιμα με γνώμονα συγκεκριμένα κριτήρια, είτε το σύνολο αυτό είναι συγκεντρωμένο είτε αποκεντρωμένο είτε κατανεμημένο σε λειτουργική ή γεωγραφική βάση,

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

8) «**Εκτελών την Επεξεργασία**»: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας,

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

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

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

12) «**Παραβίαση ΔΠΧ**»: 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,

13) «**Δεδομένα που αφορούν την υγεία**»: δεδομένα προσωπικού χαρακτήρα τα οποία σχετίζονται με τη σωματική ή ψυχική υγεία ενός φυσικού προσώπου, περιλαμβανομένης

της παροχής υπηρεσιών υγειονομικής φροντίδας, και τα οποία αποκαλύπτουν πληροφορίες σχετικά με την κατάσταση της υγείας του,

14) «**Εποπτική Αρχή**»: ανεξάρτητη δημόσια αρχή που συγκροτείται σύμφωνα με το άρθρο 51 του Κανονισμού,

15) «**Κανονισμός**», «**Γενικός Κανονισμός**»: 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 (Γενικός Κανονισμός για την Προστασία Δεδομένων ή ΓΚΠΔ).

II.2. Αρχές που διέπουν την επεξεργασία των ΔΠΧ

Σύμφωνα με το Γενικό Κανονισμό για την Προστασία Δεδομένων, το Πανεπιστήμιο Κρήτης, υπό την ιδιότητα του Υπεύθυνου Επεξεργασίας, αλλά και όταν ενεργεί ως Εκτελών την Επεξεργασία, υποχρεούται να εφαρμόζει αρχές προστασίας των ΔΠΧ καθ' όλη τη διάρκεια επεξεργασίας τους.

1. Τα ΔΠΧ επεξεργάζονται **νόμιμα**, **δίκαια** και με **διαφάνεια** σε σχέση με το Υποκείμενο των Δεδομένων.
2. Τα ΔΠΧ συλλέγονται για **συγκεκριμένους**, **σαφείς** και **νόμιμους** σκοπούς.
3. Τα ΔΠΧ είναι **επαρκή**, **συναφή** και **περιορίζονται** σε όσα είναι απαραίτητα σε σχέση με το σκοπό για τον οποίο υποβάλλονται σε επεξεργασία.
4. Τα ΔΠΧ είναι **ακριβή** και, όπου είναι απαραίτητο, επικαιροποιημένα.
5. Τα ΔΠΧ διατηρούνται σε μορφή που επιτρέπει την ταυτοποίηση των Υποκειμένων των Δεδομένων για χρονικό διάστημα όχι μεγαλύτερο από αυτό που είναι απαραίτητο για τους σκοπούς για τους οποίους επεξεργάζονται τα ΔΠΧ.
6. Τα ΔΠΧ υποβάλλονται σε επεξεργασία με τρόπο που εξασφαλίζει την **κατάλληλη ασφάλειά** τους.

III. Μέτρα Ασφαλείας

Τα μέτρα ασφαλείας, τα οποία οφείλει να λάβει το Πανεπιστήμιο Κρήτης, προκειμένου να διασφαλίσει την ορθή και νόμιμη επεξεργασία των ΔΠΧ, εντάσσονται στις παρακάτω τρεις κύριες κατηγορίες:

III.1. Οργανωτικά μέτρα ασφαλείας

III.1.Α. Υπεύθυνος Ασφαλείας – Υπεύθυνος Προσωπικών Δεδομένων

Το Πανεπιστήμιο Κρήτης έχει ορίσει Υπεύθυνο Ασφαλείας (Security Officer), καθώς και Υπεύθυνο Προστασίας Δεδομένων (Data Protection Officer), οι οποίοι θα είναι επιφορτισμένοι, στο πλαίσιο των καθηκόντων του ο καθένας, με την επίβλεψη και τον έλεγχο της εφαρμογής των πολιτικών και των μέτρων ασφαλείας, που έχει υιοθετήσει το Πανεπιστήμιο για την προστασία των ΔΠΧ.

Ο Υπεύθυνος Προστασίας Προσωπικών Δεδομένων του Πανεπιστημίου είναι υπεύθυνος για θέματα απορρήτου και ασφαλείας των ΔΠΧ και διαδραματίζει βασικό ρόλο στη διατήρηση της συμμόρφωσης του Πανεπιστημίου Κρήτης, όσον αφορά στις υποχρεώσεις προστασίας δεδομένων.

Αυτό περιλαμβάνει ότι ο Υπεύθυνος Προστασίας Δεδομένων:

(i) Είναι το μοναδικό σημείο επαφής για τα θέματα του Υποκειμένου των Δεδομένων, συμπεριλαμβανομένης της άσκησης των δικαιωμάτων του Υποκειμένων των Δεδομένων.

(ii) Παρακολουθεί τη συμμόρφωση με το Γενικό Κανονισμό για την Προστασία Δεδομένων [παροχή συμβουλών για την Εκτίμηση Αντίκτυπου Προστασίας Δεδομένων (DPIA), συντονισμό με σχετικές ομάδες για θέματα απορρήτου και ασφάλειας των ΔΠΧ].

(iii) Ευαισθητοποιεί και εκπαιδεύει το προσωπικό που ασχολείται με τις διαδικασίες επεξεργασίας δεδομένων.

(iv) Ενεργεί ως σημείο επαφής για την Αρχή Προστασίας Δεδομένων.

(v) Συμμετέχει σε συζητήσεις / συναντήσεις εντός του Πανεπιστημίου για θέματα που αφορούν τη διαχείριση / επεξεργασία ΔΠΧ.

(vi) Πραγματοποιεί τακτικές συναντήσεις με έκαστο τμήμα του Πανεπιστημίου για θέματα ασφαλείας ΔΠΧ.

(vii) Προβαίνει στις απαραίτητες γνωστοποιήσεις σε περίπτωση παραβίασης ΔΠΧ.

(viii) Επιλαμβάνεται των καταγγελιών των Υποκειμένων των Δεδομένων.

(ix) Αναφέρεται απευθείας στη Διοίκηση του Πανεπιστημίου.

III.1.Β. Οργάνωση / Διαχείριση προσωπικού

III.1.Β.i. Ρόλοι/εξουσιοδοτήσεις

Το Πανεπιστήμιο Κρήτης έχει δημιουργήσει τους απαραίτητους οργανωτικούς ρόλους για συγκεκριμένες εργασίες εντός εκάστου των τμημάτων του (Οργανόγραμμα) και έχει ορίσει τα καθήκοντα που αντιστοιχούν σε κάθε οργανωτικό ρόλο, συνδέοντάς τον παράλληλα με συγκεκριμένο εργαζόμενο, τον οποίο έχει προηγουμένως ενημερώσει εγγράφως σχετικά με τα καθήκοντα που του αναθέτει. Κάθε εργαζόμενος έχει δικαίωμα πρόσβασης μόνο στα απολύτως απαραίτητα ΔΠΧ, βάσει των αρμοδιοτήτων και καθηκόντων που του έχουν ανατεθεί και υπαγορεύονται από το ρόλο του.

III.1.Β.ii. Αναθεώρηση ρόλων

Εφόσον υφίσταται σχετική ανάγκη (π.χ. μετακίνηση μέλους του προσωπικού ή εργαζόμενου σε έτερο τμήμα του Πανεπιστημίου, αλλαγή καθηκόντων, αποχώρηση κ.λπ.) το Πανεπιστήμιο Κρήτης υποχρεούται να επανεξετάσει ή/και αναθεωρήσει τις εξουσιοδοτήσεις και δικαιώματα πρόσβασης του μέλους ή του εργαζόμενου, τους οποίους οφείλει να ενημερώσει εγγράφως.

III.1.Β.iii. Δέσμευση εμπιστευτικότητας

Το Πανεπιστήμιο Κρήτης οφείλει να επιλέγει πρόσωπα με αντίστοιχα επαγγελματικά προσόντα που παρέχουν επαρκείς εγγυήσεις από πλευράς τεχνικών γνώσεων και προσωπικής ακεραιότητας για την τήρηση του απορρήτου. Με την επιφύλαξη ειδικών διατάξεων της ισχύουσας νομοθεσίας, το Πανεπιστήμιο Κρήτης υποχρεούται να δεσμεύει τα μέλη του προσωπικού του, τους εργαζόμενούς του και τους εν γένει εκτελούντες την επεξεργασία ΔΠΧ για λογαριασμό του με ρήτρες εμπιστευτικότητας και τήρησης του νόμου, οι οποίες θα πρέπει να περιέχονται στις έγγραφες συμβάσεις / συμφωνητικά που θα συνδέουν το Πανεπιστήμιο με αυτούς. Η ισχύς των εν λόγω διατάξεων θα πρέπει να λήγει τουλάχιστον πέντε έτη μετά την καθ' οιονδήποτε τρόπο λύση ή λήξη των ανωτέρω συμβάσεων / συμφωνητικών.

III.1.Β.iv. Αποχώρηση μέλους του προσωπικού ή εργαζομένου

Σε περίπτωση αποχώρησης μέλους του προσωπικού ή εργαζομένου, λόγω λύσης ή λήξης της εργασιακής του σχέσης με το Πανεπιστήμιο Κρήτης, το Πανεπιστήμιο υποχρεούται να λάβει όλα τα απαραίτητα μέτρα για την προστασία της ασφάλειας των ΔΠΧ, που τηρούνταν από το μέλος ή τον εργαζόμενο ή είχαν δικαίωμα πρόσβασης σε αυτά, ενδεικτικά ήτοι:

α) Κατάργηση όλων των λογαριασμών πρόσβασης, των εξουσιοδοτήσεων και των κωδικών-συνθηματικών πρόσβασης.

β) Κατάργηση των λογαριασμών ηλεκτρονικού ταχυδρομείου. Σε περίπτωση αποχώρησης εργαζομένου, θα επιλέγεται από τη Διοίκηση του Πανεπιστημίου έτερος εργαζόμενος, στην

ηλεκτρονική διεύθυνση του οποίου θα ανακατευθύνονται οι ηλεκτρονικές επιστολές, που τυχόν θα λαμβάνει ο αποχωρήσας εργαζόμενος μετά την αποχώρησή του.
γ) Επιστροφή οποιουδήποτε εξοπλισμού έχει παρασχεθεί στο μέλος του προσωπικού ή τον εργαζόμενο και ανήκει στο Πανεπιστήμιο (συμπεριλαμβανομένων υπολογιστών, κλειδιών, ηλεκτρονικών καρτών εισόδου/εξόδου, κ.λπ.).

III.1.Γ. Διαχείριση πληροφοριακών αγαθών

III.1.Γ.i. Διαχείριση φυσικού και ηλεκτρονικού αρχείου

Τα φυσικά αρχεία, που περιέχουν ΔΠΧ (απλά και ειδικών κατηγοριών), θα πρέπει να φυλάσσονται σε ερμάρια ή άλλους χώρους που ασφαλίζουν με κλειδί. Το κλειδί θα τηρείται από μέλος του προσωπικού ή εργαζόμενο, που έχει το καθήκον/αρμοδιότητα, σύμφωνα με το Οργανόγραμμα, ή είναι ειδικά εξουσιοδοτημένος να έχει πρόσβαση στα εν λόγω αρχεία. Αντίγραφο του κλειδιού θα τηρείται μόνο από εξουσιοδοτημένο για τον σκοπό αυτό εργαζόμενο. Για λόγους ασφαλείας θα τηρείται αντίγραφο κάθε φυσικού φακέλου και σε ηλεκτρονική μορφή.

Τα ηλεκτρονικά αρχεία, που περιέχουν ΔΠΧ (απλά και ειδικών κατηγοριών) θα αποθηκεύονται στους διακομιστές (servers) του Πανεπιστημίου Κρήτης και θα έχουν πρόσβαση σε αυτά τα μέλη του προσωπικού και οι εργαζόμενοι, που είναι κατάλληλα εξουσιοδοτημένοι, σύμφωνα με το Οργανόγραμμα του Πανεπιστημίου. Η πρόσβαση στα εν λόγω αρχεία θα γίνεται με τη χρήση κωδικών ασφαλείας (username και password), οι οποίοι θα είναι μοναδικοί για καθέναν από τους παραπάνω.

III.1.Γ.ii. Διαβάθμιση πληροφοριών

Τα δεδομένα πρέπει να διαβαθμίζονται βάσει του είδους (απλά, ειδικών κατηγοριών) και της κρισιμότητάς τους. Η διαχείριση των φυσικών και ηλεκτρονικών αρχείων που περιέχουν προσωπικά δεδομένα, ανεξάρτητα από τη διαβάθμισή τους, θα γίνεται με τον τρόπο που περιγράφεται ανωτέρω.

III.1.Γ.iii. Διακίνηση πληροφοριακών αγαθών

Εξοπλισμός του Πανεπιστημίου Κρήτης (π.χ. ηλεκτρονικός υπολογιστής ή USB) με δεδομένα προσωπικού χαρακτήρα δεν επιτρέπεται να μεταφέρεται εκτός των εγκαταστάσεων του Πανεπιστημίου. Αν τέτοια μεταφορά επιβάλλεται, σύμφωνα με τους σκοπούς και τις δραστηριότητες του Πανεπιστημίου, τότε αυτή θα πρέπει να καταγράφεται (ιδίως, η ημερομηνία και ώρα εξόδου, το πρόσωπο που χρησιμοποιεί τον εξοπλισμό και η επιστροφή του εξοπλισμού) και να τελεί υπό την έγκριση, κατά περίπτωση, είτε του αρμόδιου για τον σκοπό και τη δραστηριότητα του Πανεπιστημίου μέλους του προσωπικού του είτε του Προϊσταμένου της υπηρεσίας είτε του Υπευθύνου Ασφαλείας είτε του νομίμου εκπροσώπου του Πανεπιστημίου.

III.1.Δ. Εκτελούντες την επεξεργασία

III.1.Δ.i. Καταγραφή

Το Πανεπιστήμιο Κρήτης οφείλει να τηρεί κατάλογο όλων των εκτελούντων την επεξεργασία, που χειρίζονται προσωπικά δεδομένα για λογαριασμό του εντός ή εκτός των εγκαταστάσεων του.

III.1.Δ.ii. Έγγραφη ανάθεση

Στην περίπτωση που το Πανεπιστήμιο Κρήτης αναθέτει την επεξεργασία δεδομένων σε εκτελούντα, κατά την έννοια των σχετικών διατάξεων του Κανονισμού, η σχετική ανάθεση γίνεται υποχρεωτικά εγγράφως και προβλέπει ότι ο εκτελών την επεξεργασία τη διεξάγει μόνο κατ' εντολή του Πανεπιστημίου και ότι οι λοιπές υποχρεώσεις του άρθρου 28 του Κανονισμού βαρύνουν τον εκτελούντα.

Οι έγγραφες αναθέσεις - συμβάσεις πρέπει να περιέχουν κατ' ελάχιστο περιγραφή των προσωπικών δεδομένων, που θα τύχουν επεξεργασίας, τον σκοπό, τον τόπο και τον τρόπο/διαδικασία της επεξεργασίας, τα επίπεδα των υπηρεσιών που πρέπει να επιτυγχάνει ο εκτελών την επεξεργασία (σε επίπεδο ασφαλείας και ποιότητας δεδομένων), καθώς και τις υποχρεώσεις του εκτελούντος την επεξεργασία, όπως αναφέρονται στο άρθρο 28 του Κανονισμού.

III.1.Δ.iii. Μέτρα ασφαλείας που αφορούν τους εκτελούντες

Ο εκτελών την επεξεργασία οφείλει να λαμβάνει τα κατάλληλα οργανωτικά και τεχνικά μέτρα για την ασφαλή τήρηση και επεξεργασία των ΔΠΧ, σύμφωνα με την παρούσα Πολιτική του Πανεπιστημίου Κρήτης. Το Πανεπιστήμιο οφείλει να διασφαλίσει ότι ο εκτελών την επεξεργασία τηρεί τους όρους των Πολιτικών, που έχει υιοθετήσει το Πανεπιστήμιο για την προστασία των προσωπικών δεδομένων στο μέτρο που αυτές τον αφορούν.

Δικαιώματα πρόσβασης σε μέλη του προσωπικού του εκτελούντος στα συστήματα του Πανεπιστημίου εκχωρούνται μόνο όταν αυτό είναι απαραίτητο για την υλοποίηση των συμβατικών τους υποχρεώσεων. Πρέπει να ανατίθενται οι ελάχιστες απαιτούμενες εξουσιοδοτήσεις, οι οποίες με τη σειρά τους θα πρέπει να καταργούνται με τη λήξη της συμβατικής υποχρέωσης.

III.1.Δ.iv. Τόπος επεξεργασίας

Για τη συντήρηση/αναβάθμιση του εξοπλισμού, που φέρει ΔΠΧ θα πρέπει πάντοτε να εξετάζεται το ενδεχόμενο, εφόσον είναι εφικτό και πρόσφορο, αυτή να πραγματοποιείται εντός των χώρων του Πανεπιστημίου Κρήτης. Όταν η επεξεργασία γίνεται εκτός των εγκαταστάσεων του Πανεπιστημίου, το Πανεπιστήμιο Κρήτης πρέπει να ζητά και ο εκτελών την επεξεργασία να παρέχει έγγραφη βεβαίωση ότι ο τελευταίος εξασφαλίζει και παρέχει επίπεδο ασφαλείας τουλάχιστον ανάλογο με αυτό που ορίζεται στην παρούσα Πολιτική.

III.1.Δ.v. Δέσμευση εμπιστευτικότητας του προσωπικού του εκτελούντος

Οι εργαζόμενοι του εκτελούντος την επεξεργασία, που επεξεργάζονται, κατά το χρονικό διάστημα της σύμβασης, ΔΠΧ για λογαριασμό του Πανεπιστημίου Κρήτης πρέπει να δεσμεύονται εγγράφως με κατάλληλη δήλωση εμπιστευτικότητας, τουλάχιστον ισοδύναμης με αυτή που περιέχεται στις συμβάσεις / συμφωνητικά του προσωπικού και των εργαζομένων του Πανεπιστημίου.

III.1.Ε. Καταστροφή δεδομένων και αποθηκευτικών μέσων

Με την επιφύλαξη των διατάξεων για την εκκαθάριση αρχείων ν.π.δ.δ. και τη νομοθεσία για τα Γενικά Αρχεία του Κράτους, πριν από την καταστροφή εντύπων ή ηλεκτρονικών αρχείων που περιέχουν προσωπικά δεδομένα θα πρέπει να λαμβάνονται τα κατάλληλα μέτρα ώστε να διασφαλίζεται η πλήρης και μόνιμη διαγραφή των δεδομένων αυτών, ώστε να αποκλειστεί η περαιτέρω μη νόμιμη και αθέμιτη επεξεργασία τους, όπως είναι η κάθε μορφή διάθεσης σε τρίτους. Ειδικότερα, θα πρέπει να ακολουθούνται κατ' ελάχιστον όσα προβλέπονται στην Οδηγία 1/2005 της Αρχής Προστασίας Δεδομένων για την ασφαλή καταστροφή των προσωπικών δεδομένων μετά το πέρας της περιόδου που απαιτείται για την πραγματοποίηση του σκοπού της επεξεργασίας. Ως ασφαλής τρόπος καταστροφής των δεδομένων θεωρείται κάθε σύνολο διαδικασιών και μέτρων που μετά από την ολοκλήρωση της εφαρμογής τους δεν είναι δυνατό να αναγνωρισθούν τα υποκείμενα των δεδομένων, ενώ παράλληλα η καταστροφή είναι μη αναστρέψιμη, δηλαδή δεν είναι δυνατή η ανάκτηση των δεδομένων μετά την καταστροφή με τεχνικά ή άλλα μέσα.

Ο Υπεύθυνος Προστασίας Δεδομένων υποχρεούται να εφαρμόζει τους κατάλληλους μηχανισμούς ελέγχου της ορθής τήρησης της διαδικασίας καταστροφής που εφαρμόζει το Πανεπιστήμιο Κρήτης. Ο έλεγχος θα ανατίθεται σε εξουσιοδοτημένους για τον σκοπό αυτό εργαζόμενους του Πανεπιστημίου.

Αν η καταστροφή των δεδομένων εκτελείται για λογαριασμό του Πανεπιστημίου από πρόσωπο μη εξαρτώμενο από αυτό (εκτελούντα την επεξεργασία), το Πανεπιστήμιο οφείλει να πραγματοποιεί τη σχετική ανάθεση μόνον εγγράφως. Στη σύμβαση της ανάθεσης θα πρέπει να ορίζονται τα μέτρα που θα εφαρμόσει ο εκτελών την επεξεργασία για την ασφαλή μεταφορά των δεδομένων στον τόπο καταστροφής, ο τόπος καταστροφής, οι τυχόν ενδιάμεσοι τόποι αποθήκευσης των δεδομένων, ο τρόπος καταστροφής, καθώς επίσης και ο μέγιστος επιτρεπόμενος χρόνος από την στιγμή της παράδοσης των δεδομένων από το Πανεπιστήμιο στον εκτελούντα την επεξεργασία μέχρι την οριστική καταστροφή τους. Επίσης, στη σύμβαση της ανάθεσης πρέπει να αναφέρονται και τυχόν πρόσθετες υποδείξεις του Πανεπιστημίου σχετικά με τεχνικά και οργανωτικά μέτρα καταστροφής, καθώς επίσης και τα ακριβή στοιχεία τυχόν τρίτων

(υπεργολάβων) που πρόκειται να πραγματοποιήσουν μέρος ή το σύνολο της καταστροφής των δεδομένων για λογαριασμό του εκτελούντος την επεξεργασία. Επίσης, πρέπει να διασφαλίζεται ότι το Πανεπιστήμιο έχει την εξουσία διάθεσης και ελέγχου των δεδομένων μέχρι την οριστική καταστροφή τους. Ως εκ τούτου, ο εκτελών την επεξεργασία πρέπει να διατηρεί ξεχωριστά τα προς καταστροφή δεδομένα του Πανεπιστημίου με την οποία συνάπτει σχετική σύμβαση. Ο εκτελών την επεξεργασία πρέπει να είναι σε θέση να εφαρμόσει τα κατάλληλα τεχνικά και οργανωτικά μέσα για την ασφαλή καταστροφή των δεδομένων, και να έχει προβλέψει αντίστοιχη διαδικασία καταστροφής και ελέγχου καταστροφής με αυτή του Πανεπιστημίου. Τα φυσικά πρόσωπα – υπάλληλοι του εκτελούντος την επεξεργασία που θα πραγματοποιήσουν την καταστροφή πρέπει να υποχρεώνονται ειδικώς στο απόρρητο της επεξεργασίας.

Με την επιφύλαξη των διατάξεων για την εκκαθάριση αρχείων ν.π.δ.δ. και τη νομοθεσία για τα Γενικά Αρχεία του Κράτους, **το Πανεπιστήμιο Κρήτης δύναται να εφαρμόζει ενδεικτικά τα ακόλουθα μέτρα καταστροφής δεδομένων:**

α) τεμαχισμός των εγγράφων σε λωρίδες με χρήση ειδικών μηχανημάτων τεμαχισμού εγγράφων εντός των εγκαταστάσεων και από εξουσιοδοτημένους εργαζόμενους του Πανεπιστημίου,

β) πολτοποίηση/ανακύκλωση των εγγράφων,

γ) αποτέφρωση του υλικού υποστρώματος των δεδομένων.

Μετά την καταστροφή των δεδομένων θα πρέπει να συντάσσεται Πρωτόκολλο Καταστροφής Δεδομένων, στο οποίο θα περιέχονται τουλάχιστον τα παρακάτω στοιχεία:

α) ημερομηνία καταστροφής των δεδομένων,

β) περιγραφή των δεδομένων που καταστράφηκαν,

γ) μέθοδος καταστροφής,

δ) ονοματεπώνυμο αρμόδιου εργαζόμενου του Πανεπιστημίου που είναι υπεύθυνος για την καταστροφή,

ε) εκτελών την καταστροφή (στην περίπτωση που η καταστροφή ανατίθεται σε εκτελούντα την επεξεργασία).

Για την ασφαλή καταστροφή δεδομένων σε ηλεκτρονική μορφή δεν επαρκεί η απλή διαγραφή τους (π.χ. με την εντολή «DELETE»), καθώς κατά τον τρόπο αυτό διαγράφεται μόνο η αναφορά στα δεδομένα, ενώ τα ίδια τα δεδομένα ενδέχεται να είναι ανακτήσιμα με χρήση ειδικών προγραμμάτων λογισμικού.

Ο ενδεικνυόμενος τρόπος για την ασφαλή καταστροφή των δεδομένων που είναι αποθηκευμένα σε επανεγγράψιμα μέσα (π.χ. σκληροί δίσκοι, δισκέττες, επανεγγράψιμα DVD και CD) είναι η αλλοίωση των δεδομένων μέσω της αντικατάστασης τους με τυχαίους χαρακτήρες (overwrite). Η αλλοίωση μπορεί να γίνει με τη χρήση ειδικών προγραμμάτων (fileerasers, fileshredders, filepulveritizers). Στην περίπτωση της καθημερινής

καταστροφής δεδομένων, ένας εναλλακτικός τρόπος καταστροφής είναι η μορφοποίηση του υλικού υποστρώματος (format).

Στην περίπτωση της προγραμματισμένης καταστροφής του συνόλου των δεδομένων, ένας εναλλακτικός τρόπος καταστροφής (για ιδιαίτερα κρίσιμα δεδομένα) είναι και η φυσική καταστροφή του ίδιου του υλικού υποστρώματος (π.χ. με θρυμματισμό, κονιορτοποίηση, αποτέφρωση, με την επιφύλαξη ειδικών διατάξεων σχετικά με τη διαχείριση ειδικών αποβλήτων / προστασία του περιβάλλοντος).

Η καταστροφή των δεδομένων περιλαμβάνει και την καταστροφή όλων των αντιγράφων ασφαλείας (back up) που τηρεί το Πανεπιστήμιο, εφόσον αυτό είναι πρακτικά και τεχνικά εφικτό.

Η προγραμματισμένη καταστροφή των δεδομένων πρέπει να συνοδεύεται από Πρωτόκολλο Καταστροφής Δεδομένων, σύμφωνα με τα ανωτέρω.

III.1.Στ. Εκπαίδευση προσωπικού και εργαζομένων

Η εκπαίδευση των μελών του προσωπικού και των εργαζομένων του Πανεπιστημίου Κρήτης σε θέματα προστασίας ΔΠΧ, καθώς και σε ειδικές σχετικές με ασφάλεια λειτουργίες του πληροφοριακού συστήματος (π.χ. χρήση μη προβλέψιμων κωδικών πρόσβασης και συνθηματικών, τρόπο εντοπισμού και αναφοράς των περιστατικών παραβίασης της ασφαλείας, σωστή χρήση των e-mail και των αποσπώμενων μέσων αποθήκευσης, διαδικασία καταστροφής προσωπικών δεδομένων) είναι ιδιαιτέρως σημαντική για την ορθή εφαρμογή των οργανωτικών και τεχνικών μέτρων ασφαλείας.

Η εκπαίδευση κατά την πρόσληψη πρέπει να περιλαμβάνει κατ' ελάχιστο την κοινοποίηση στους εργαζόμενους των Πολιτικών, που έχει υιοθετήσει το Πανεπιστήμιο, καθώς επίσης και των διαδικασιών διαχείρισης περιστατικών παραβίασης δεδομένων. Στον εσωτερικό αποθετήριο εγγράφων είναι αναρτημένες οι εν λόγω πολιτικές. Η εκπαίδευση θα συνεχίζεται και μετά την πρόσληψη, είτε σε σημαντικές αλλαγές των διαδικασιών ασφαλείας είτε κατά την εμφάνιση σημαντικών θεμάτων ασφαλείας. Η εκπαίδευση θα γίνεται από τον Υπεύθυνο Προστασίας Δεδομένων.

III.1.Ζ. Έλεγχος

Ο Υπεύθυνος Ασφαλείας σε συνεργασία με τον Υπεύθυνο Προστασίας Δεδομένων οφείλουν να διενεργούν άπαξ ανά ημερολογιακό έτος δειγματοληπτικό έλεγχο συμμόρφωσης του Πανεπιστημίου Κρήτης, του προσωπικού και των εργαζομένων του στις πολιτικές που έχει υιοθετήσει το Πανεπιστήμιο για την προστασία των ΔΠΧ με απώτερο στόχο την επισκόπηση της ορθής εφαρμογής τους και την αποτίμηση της αποτελεσματικότητας των μέτρων ασφαλείας, που έχει υιοθετήσει το Πανεπιστήμιο. Τυχόν ευρήματα του ανωτέρω ελέγχου θα πρέπει να καταγράφονται και να υποβάλλονται

εγγράφως στις Πρυτανικές Αρχές του Πανεπιστημίου μαζί με τις έγγραφες εισηγήσεις αυτών που διενήργησαν τον έλεγχο για τα προσήκοντα διορθωτικά μέτρα που θα πρέπει να λάβει το Πανεπιστήμιο.

III.1.Η. Εκτίμηση Αντικτύπου Προστασίας Δεδομένων

Για κάθε μορφή επεξεργασίας ΔΠΧ, ιδίως με χρήση νέων τεχνολογιών και συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, το Πανεπιστήμιο Κρήτης διενεργεί, πριν από την επεξεργασία, εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία ΔΠΧ, στα δικαιώματα και τις ελευθερίες των Υποκειμένων των Δεδομένων.

Η εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων απαιτείται ιδίως στην περίπτωση:

α) συστηματικής και εκτενούς αξιολόγησης προσωπικών πτυχών σχετικά με φυσικά πρόσωπα, η οποία βασίζεται σε αυτοματοποιημένη επεξεργασία, περιλαμβανομένης της κατάρτισης προφίλ, και στην οποία βασίζονται αποφάσεις, που παράγουν έννομα αποτελέσματα σχετικά με το φυσικό πρόσωπο ή ομοίως επηρεάζουν σημαντικά το φυσικό πρόσωπο,

β) μεγάλης κλίμακας επεξεργασία ευαίσθητων ΔΠΧ ή ΔΠΧ που αφορούν ποινικές καταδίκες και αδικήματα ή

γ) συστηματικής παρακολούθησης δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα

III.1.Θ. Επισκόπηση – Αναθεώρηση - Αξιολόγηση του επιπέδου αποτελεσματικότητας

Η παρούσα Πολιτική και οι διαδικασίες, που προβλέπονται σε αυτή υποβάλλονται σε τακτικές αναθεωρήσεις προκειμένου να διασφαλιστεί ότι εφαρμόζονται σωστά και σε πλήρη ευθυγράμμιση με την εκάστοτε ισχύουσα νομοθεσία. Ενδεικτικά, δύνανται να τροποποιούνται στις περιπτώσεις που συμβαίνουν σημαντικές αλλαγές σε κάποιο τουλάχιστον από τα εξής: α) στην οργανωτική δομή του Πανεπιστημίου, β) στα πληροφοριακά συστήματα, γ) στις απαιτήσεις ασφαλείας, δ) στις τεχνολογικές εξελίξεις, ε) στο είδος ή/και στην επεξεργασία των προσωπικών δεδομένων. Η παρούσα Πολιτική και οι διαδικασίες, που προβλέπονται σε αυτή μπορούν, επίσης, να μεταβάλλονται κατόπιν διενέργειας εσωτερικού ή εξωτερικού ελέγχου, ο οποίος καταδεικνύει μη επαρκή ή/και μη αποτελεσματικά μέτρα ως προς την ασφάλεια, ή κατόπιν περιστατικού παραβίασης της ασφάλειας.

Ο Υπεύθυνος Ασφαλείας σε συνεργασία με τον Υπεύθυνο Προστασίας Δεδομένων είναι αρμόδιοι να προβαίνουν στις απαραίτητες επικαιροποιήσεις/αναθεωρήσεις της

παρούσας Πολιτικής και των διαδικασιών που περιέχονται σε αυτή, οι οποίες θα τίθενται σε ισχύ μετά την έγγραφη έγκρισή τους από τη διοίκηση του Πανεπιστημίου.

Το Πανεπιστήμιο θα πρέπει να διενεργεί ετήσια αξιολόγηση του επιπέδου αποτελεσματικότητας για να διαπιστωθεί εάν οι εφαρμοζόμενες πολιτικές και διαδικασίες εξασφαλίζουν το κατάλληλο επίπεδο προστασίας, που απαιτεί ο Κανονισμός.

Αυτή η αξιολόγηση του επιπέδου αποτελεσματικότητας θα συντονίζεται από το Πανεπιστήμιο, με την υποστήριξη των υπευθύνων των τμημάτων του Πανεπιστημίου και του Υπεύθυνου Προστασίας Προσωπικών Δεδομένων.

III.2. Τεχνικά μέτρα ασφαλείας

III.2.A. Έλεγχος πρόσβασης

III.2.A.i. Διαχείριση λογαριασμών χρηστών

Το Πανεπιστήμιο Κρήτης έχει υιοθετήσει συγκεκριμένες διαδικασίες για τη διαχείριση των λογαριασμών των χρηστών, οι οποίες περιλαμβάνουν διαδικασίες για την προσθήκη, μεταβολή ιδιοτήτων και διαγραφή λογαριασμού. Αποδίδεται δε διαφορετικός λογαριασμός πρόσβασης σε κάθε χρήστη. Ειδικότερα, με την πρόσληψη κάθε εργαζομένου και ανάλογα με τη θέση του στο οργανόγραμμα του Πανεπιστημίου γίνεται η καταχώρηση των στοιχείων του στο “active directory” του Πανεπιστημίου με συγκεκριμένα δικαιώματα πρόσβασης και συγκεκριμένα “username” και “password”.

III.2.A.ii. Μηχανισμοί ελέγχου πρόσβασης

Το Πανεπιστήμιο Κρήτης έχει αναπτύξει μηχανισμούς που δεν επιτρέπουν προσβάσεις σε πόρους/εφαρμογές/αρχεία από μη εξουσιοδοτημένους χρήστες και εξασφαλίζουν την εγγυημένα ορθή ταυτοποίηση και αυθεντικοποίηση των χρηστών, ενώ ταυτοχρόνως γίνεται σε τεχνικό επίπεδο συγκεκριμένη εκχώρηση δικαιωμάτων / εξουσιοδοτήσεων σε κάθε χρήστη. Ειδικότερα, το Πανεπιστήμιο έχει δύο διαφορετικά επίπεδα τείχους προστασίας (Firewall). Το πρώτο επίπεδο διασφαλίζει τους κανόνες για τη σωστή λειτουργία του δικτύου του Πανεπιστημίου, ενώ παράλληλα προστατεύει το Πανεπιστήμιο από απειλές εκτός αυτού. Το δεύτερο επίπεδο είναι ένα τείχος προστασίας των ηλεκτρονικών αλληλογραφιών από κακόβουλες αλληλογραφίες, που προέρχονται είτε από εξωτερικούς παράγοντες είτε από εσωτερικούς, που μπορεί να έχουν προσβληθεί από κάποιον ιό.

III.2.A.iii. Διαχείριση συνθηματικών

Το Πανεπιστήμιο Κρήτης έχει υιοθετήσει συγκεκριμένη πολιτική διαχείρισης των συνθηματικών των χρηστών, η οποία να περιλαμβάνει τουλάχιστον κανόνες αποδοχής για το ελάχιστο μήκος (τουλάχιστον 8 χαρακτήρες) και επιτρεπτούς χαρακτήρες των συνθηματικών (πολυπλοκότητα συνθηματικού), την ιστορικότητα του συνθηματικού και τη συχνότητα αλλαγής του.

Όλα τα συνθηματικά / κωδικοί πρόσβασης των χρηστών θα πρέπει να πληρούν ή να υπερβαίνουν τις ακόλουθες κατευθυντήριες γραμμές:

Ως αποδεκτοί κωδικοί πρόσβασης θεωρούνται αυτοί που διαθέτουν τα ακόλουθα χαρακτηριστικά:

- Περιέχουν τουλάχιστον 8 αλφαριθμητικούς χαρακτήρες
- Περιέχουν πεζά και κεφαλαία γράμματα
- Περιέχουν τουλάχιστον έναν αριθμό (για παράδειγμα 0-9).
- Περιέχουν τουλάχιστον έναν ειδικό χαρακτήρα (για παράδειγμα, $% ^ & * () _ + | ~ - = \ '{} []: "?" <>, /!;)

Ως μη αποδεκτοί κωδικοί πρόσβασης, θεωρούνται αυτοί που διαθέτουν τα ακόλουθα χαρακτηριστικά:

- Περιέχουν λιγότερους από 8 χαρακτήρες.
- Μπορούν να βρεθούν σε ένα λεξικό, συμπεριλαμβανομένων των ξένων γλωσσών, ή υπάρχουν σε γλώσσα αργκό, διαλέκτου, ή φρασεολογία.
- Περιέχουν προσωπικές πληροφορίες, όπως ημερομηνίες γέννησης, διευθύνσεις, αριθμούς τηλεφώνων ή τα ονόματα των μελών της οικογένειας, κατοικίδιων ζώων, φίλων και φανταστικών χαρακτήρων / ηρώων.
- Περιέχουν πληροφορίες που σχετίζονται με την εργασία, όπως ονόματα κτιρίου, τις εντολές του συστήματος, ιστοσελίδες, εταιρείες εξοπλισμού ή λογισμικού.
- Περιέχουν επαναλαμβανόμενα μοτίβα όπως aaabbb, qwerty, zyxwvuts ή 123.321.
- Περιέχουν συνηθισμένες λέξεις γραμμένες ανάποδα ή συνοδεύονται πριν ή μετά τη λέξη από έναν αριθμό (για παράδειγμα, terces, secret1 ή 1secret).

Οι κωδικοί πρόσβασης δε θα πρέπει να είναι κάπου καταγεγραμμένοι (σε φυσικό ή ηλεκτρονικό αρχείο, συσκευή κινητού τηλεφώνου, tablet ή οπουδήποτε αλλού), ούτε να γνωστοποιούνται σε τρίτους εντός ή εκτός του Πανεπιστημίου ή να κοινοποιούνται μέσω ηλεκτρονικού ταχυδρομείου, τηλεφώνου ή άλλου μέσου. Αντιθέτως, θα πρέπει να θεωρούνται από τους χρήστες τους ως ευαίσθητη εμπιστευτική πληροφορία. Για το λόγο αυτό θα πρέπει να επιλέγονται κωδικοί πρόσβασης που μπορεί εύκολα να τους αποστηθίσει / θυμηθεί ο χρήστης. Ένας τρόπος για να επιτευχθεί αυτό είναι να επιλέξει ο χρήστης έναν κωδικό πρόσβασης που βασίζεται π.χ. σε έναν τίτλο τραγουδιού, επιβεβαίωση ή άλλες φράσεις.

Για παράδειγμα, η φράση "ThisMayBeOneWayToRemember" θα μπορούσε εύκολα να απομνημονευθεί ως κωδικός πρόσβασης “TmB1w2R!” ή μια άλλη παραλλαγή.

(**ΠΡΟΣΟΧΗ:** Τα ανωτέρω παραδείγματα δεν πρέπει να χρησιμοποιηθούν ως κωδικοί πρόσβασης).

Εάν οι κωδικοί πρόσβασης διατηρούνται ηλεκτρονικά στο πλαίσιο της διαδικασίας ταυτοποίησης-αυθεντικοποίησης των χρηστών, τότε πρέπει να είναι σε μη αναγνώσιμη μορφή, από την οποία δεν πρέπει να είναι εφικτή η ανάκτηση της αρχικής τους μορφής. Επίσης, οι χρήστες υποχρεούνται να αλλάζουν οι ίδιοι το (προκαθορισμένο) συνθηματικό που τους παρέχεται εξαρχής, καθώς επίσης και να αλλάζουν το συνθηματικό τους ανά τακτά χρονικά διαστήματα (οπωσδήποτε εντός διαστήματος μικρότερου του τετραμήνου).

Εφόσον αυτό είναι εφικτό, κάθε χρήστης θα πρέπει να διαθέτει διαφορετικό κωδικό για κάθε εφαρμογή του Πανεπιστημίου, για την πρόσβαση στην οποία απαιτείται η χρήση κωδικού.

III.2.A.iv. Μη επιτυχημένες προσπάθειες πρόσβασης

Σε περίπτωση που οιοσδήποτε χρήστης εισάγει τρεις συνεχόμενες φορές λανθασμένο κωδικό πρόσβασης, το Πανεπιστήμιο Κρήτης δύναται να επανεξετάσει την εξουσιοδότησή του για να έχει δικαίωμα πρόσβασης στο εν λόγω αρχείο.

III.2.A.v. Αδρανοποιημένος υπολογιστής

Προς αποφυγή περιπτώσεων όπου θα δύναται κάποιος να έχει εύκολα πρόσβαση οποιουδήποτε τύπου σε ΔΠΧ, λόγω ενός ανοιχτού υπολογιστή, ο οποίος μένει χωρίς επίβλεψη (έστω και για λίγα λεπτά), το Πανεπιστήμιο Κρήτης έχει προβλέψει τη δυνατότητα αυτόματης αποσύνδεσης του υπολογιστή (μετά από τρία λεπτά αδράνειας) ή/και ενεργοποίηση της προφύλαξης οθόνης (screensaver) του υπολογιστή – για την απενεργοποίηση της οποίας θα απαιτείται χρήση κωδικού πρόσβασης.

III.2.Β. Αντίγραφα ασφαλείας

Το Πανεπιστήμιο Κρήτης λαμβάνει αντίγραφα ασφαλείας (backup) εκ των πρωτότυπων δεδομένων των υπολογιστών (εγγράφων, φωτογραφιών, βίντεο κ.λπ.) του προσωπικού και των εργαζομένων του. Τα αντίγραφα ασφαλείας λαμβάνονται σε καθημερινή βάση και αφού επισημανθεί η ημεροχρονολογία λήψης τους αποθηκεύονται εβδομαδιαίως σε χώρο φύλαξης εκτός της έδρας του Πανεπιστημίου, ο οποίος κλειδώνει και το κλειδί φυλάσσεται από το νόμιμο εκπρόσωπο του Πανεπιστημίου. Κάθε μήνα πραγματοποιείται από τον Υπεύθυνο Ασφαλείας έλεγχος της ακεραιότητας/αξιοπιστίας των αντιγράφων που έχουν ληφθεί, προκειμένου να διασφαλιστεί η ορθή ανάκτηση των δεδομένων από τα αντίγραφα ασφαλείας σε περίπτωση εκτάκτων περιστατικών ασφαλείας και απώλειας ή καταστροφής δεδομένων για άλλη αιτία (π.χ. αστοχία υλικού).

III.2.Γ. Διαμόρφωση υπολογιστών

III.2.Γ.i. Προστασία από κακόβουλο λογισμικό

Το Πανεπιστήμιο Κρήτης διαθέτει προστασία από κακόβουλο λογισμικό σε όλους τους υπολογιστές [τόσο τους προσωπικούς υπολογιστές του προσωπικού και των

εργαζομένων όσο και τους διακομιστές (servers)) που τηρούν ή επεξεργάζονται ΔΠΧ, χρησιμοποιώντας αντιβιοτικά προγράμματα (antivirus), καθώς και προγράμματα τειχών ασφαλείας (firewall)]. Το προσωπικό και οι εργαζόμενοι ενημερώνονται σε τακτά χρονικά διαστήματα για τη σωστή χρήση των υπολογιστών και του διαδικτύου, αλλά και πως να αντιδρούν σε περίπτωση προσβολής του υπολογιστή τους από κακόβουλο λογισμικό. Τόσο το antivirus όσο και το firewall διαθέτουν ανά πάσα στιγμή τις πλέον πρόσφατες ενημερώσεις. Επιπλέον, στο λειτουργικό σύστημα των υπολογιστών (εφόσον είναι συνδεδεμένοι στο Διαδίκτυο) εγκαθίστανται ανά τακτά διαστήματα ενημερώσεις ασφαλείας.

Σε περίπτωση δυσλειτουργίας των αντιβιοτικών προγραμμάτων ή των τειχών ασφαλείας εμφανίζονται προειδοποιητικά μηνύματα στην οθόνη του υπολογιστή. Τέτοια μηνύματα πρέπει να αναφέρονται άμεσα στον Υπεύθυνο Ασφαλείας.

Αρχεία επισυναπτόμενα σε ηλεκτρονικές επιστολές (e-mails), των οποίων ο αποστολέας δεν είναι γνωστός ή αρχεία αγνώστου τύπου, δεν θα πρέπει να ανοίγονται. Στην περίπτωση αυτή θα πρέπει να ενημερώνεται **άμεσα** ο Υπεύθυνος Ασφαλείας.

Αν υπάρχει έστω και υποψία ότι ο υπολογιστής έχει προσβληθεί από κακόβουλο λογισμικό θα πρέπει να απενεργοποιείται αμέσως και να ενημερώνεται ο Υπεύθυνος Ασφαλείας.

III.2.Γ.ii. Ρυθμίσεις υπολογιστών

Απαγορεύονται ενέργειες απλών χρηστών στους υπολογιστές, οι οποίες επηρεάζουν τη συνολική τους διαμόρφωση (π.χ. απενεργοποίηση αντιβιοτικών προγραμμάτων, εγκατάσταση νέων προγραμμάτων ή αλλαγή ρυθμίσεων υπαρχόντων, κ.λπ.). Ο Υπεύθυνος Ασφαλείας διενεργεί περιοδικούς ελέγχους του εγκατεστημένου λογισμικού των υπολογιστών του Πανεπιστημίου Κρήτης για τον τυχόν εντοπισμό προγραμμάτων που έχουν εγκατασταθεί εκτός των εγκεκριμένων. Σε περίπτωση που απαιτείται η εγκατάσταση συγκεκριμένου λογισμικού, για την εκτέλεση κάποιας εργασίας, ο ενδιαφερόμενος χρήστης θα πρέπει να υποβάλει εγγράφως σχετικό αίτημα προς τον Υπεύθυνο Ασφαλείας, στο οποίο θα αναφέρει το λογισμικό, που ενδιαφέρεται να εγκαταστήσει στον υπολογιστή του, και να αιτιολογεί επαρκώς τους λόγους που καθιστούν αναγκαία την εγκατάστασή του. Εφόσον το αίτημα γίνει δεκτό, το λογισμικό θα πρέπει να εγκατασταθεί στον υπολογιστή είτε από τον Υπεύθυνο Ασφαλείας, είτε παρουσία του Υπεύθυνου Ασφαλείας.

III.2.Γ.iii. Υπολογιστές-διακομιστές

Σε περίπτωση που κάποιος υπολογιστής χρησιμοποιείται σαν κεντρικός διακομιστής (server) για άλλους υπολογιστές, τότε δεν θα χρησιμοποιείται ως σταθμός εργασίας από κάποιον χρήστη.

III.2.Γ.iv. Υπολογιστές με πρόσβαση στο Διαδίκτυο

Δεν επιτρέπεται να αποθηκεύονται ΔΠΧ σε υπολογιστές που έχουν σύνδεση με το διαδίκτυο (εκτός αν κάτι τέτοιο είναι απολύτως απαραίτητο στο πλαίσιο του ρόλου/αρμοδιοτήτων που έχουν ανατεθεί στο χρήστη του υπολογιστή).

III.2.Δ. Αρχεία καταγραφής ενεργειών χρηστών και συμβάντων ασφαλείας

III.2.Δ.i. Τήρηση και έλεγχος αρχείων καταγραφής

Στα κρίσιμα συστήματα, τηρούνται αρχεία καταγραφής όλων των ενεργειών (logfiles) των χρηστών, συμπεριλαμβανομένων και των ενεργειών των διαχειριστών των συστημάτων, καθώς και των συμβάντων ασφαλείας. Τα εν λόγω αρχεία θα προστατεύονται με κωδικό πρόσβασης που θα γνωρίζει μόνο ο Υπεύθυνος Ασφαλείας.

Στα αρχεία αυτά δύναται να έχουν πρόσβαση ο Υπεύθυνος Ασφαλείας, οι διαχειριστές συστημάτων και όποιοι άλλοι εργαζόμενοι είναι επιφορτισμένοι με αρμοδιότητες διαχείρισης περιστατικών ασφαλείας κατόπιν έγγραφης εξουσιοδότησης.

Η πρόσβαση στα αρχεία καταγραφής καταγράφεται και τα σχετικά αρχεία καταγραφής τηρούνται από τον Υπεύθυνο Ασφαλείας.

III.2.Δ.ii. Ειδικές ενέργειες που πρέπει να καταγράφονται

Στα αρχεία καταγραφής ενεργειών τηρούνται οπωσδήποτε, κατ' ελάχιστο, τα εξής: το αναγνωριστικό του χρήστη που αιτήθηκε την προσπέλαση δεδομένων προσωπικού χαρακτήρα, η ημερομηνία και ώρα του σχετικού αιτήματος, το σύστημα μέσω του οποίου αιτήθηκε την πρόσβαση (υπολογιστής, πρόγραμμα λογισμικού, κ.λπ.), καθώς και αν τελικά προσπέλασε τα αρχεία που αιτήθηκε. Επίσης, πρέπει να καταγράφονται και τα αιτήματα εκτύπωσης αρχείων με ΔΠΧ, καθώς και οι αλλαγές σε κρίσιμα αρχεία του συστήματος ή στα δικαιώματα των χρηστών. Επίσης, τηρούνται στοιχεία που αφορούν τις προσπάθειες μη εξουσιοδοτημένης πρόσβασης και τις αλλαγές στην παραμετροποίηση εφαρμογών και συστημάτων, τον προκαθορισμό κρίσιμων γεγονότων (events), η καταγραφή των οποίων θα επιβλέπεται άμεσα από τον Υπεύθυνο Ασφαλείας και τους διαχειριστές των συστημάτων και γενικότερα κάθε ενέργεια η οποία μπορεί να υποδηλώνει διενέργεια επίθεσης, όπως προσπάθειες καταγραφής των προσφερόμενων υπηρεσιών του συστήματος (portscanning).

III.2.Δ.iii. Διαγραφή αρχείων καταγραφής

Δεν παρέχεται η δυνατότητα διαγραφής των αρχείων καταγραφής του συστήματος από ένα μόνο άτομο. Τέτοια διαγραφή θα πρέπει να γίνεται με την παρουσία δύο τουλάχιστον ατόμων, ήτοι του Υπεύθυνου Ασφαλείας και του Υπεύθυνου Μηχανογράφησης.

III.2.Ε. Ασφάλεια επικοινωνιών

III.2.Ε.i. Έλεγχος δικτυακών συσκευών

Ο Υπεύθυνος Ασφαλείας είναι επιφορτισμένος με τον έλεγχο των συνδεόμενων στο δίκτυο συσκευών (ως προς την πρόσβαση σε αυτές, αλλά και τη χρήση τους).

III.2.Ε.ii. Απομακρυσμένη πρόσβαση

Η απομακρυσμένη πρόσβαση σε συστήματα (π.χ. από εταιρείες συντήρησης ή από εργαζόμενους) πραγματοποιείται μέσω ασφαλών καναλιών με δυνατή ταυτοποίηση / αυθεντικοποίηση και κρυπτογράφηση. Επισημαίνεται ότι οι τεχνολογίες απομακρυσμένης πρόσβασης (π.χ. RemoteDesktop, Ammy, ασύρματη σύνδεση, κ.λπ.) επιτρέπονται μόνο σε εξουσιοδοτημένα πρόσωπα για τα οποία είναι απόλυτα απαραίτητες στο πλαίσιο των αρμοδιοτήτων τους. Η απομακρυσμένη πρόσβαση γίνεται υπό την εποπτεία και έλεγχο του Υπευθύνου Ασφαλείας και καταγράφεται.

III.2.Ε.iii. Κανάλι επικοινωνίας

Η επικοινωνία μεταξύ υπολογιστών/κόμβων γίνεται μέσω επαρκώς ασφαλούς καναλιού επικοινωνίας (π.χ. με χρήση κρυπτογράφησης ή/και ιδιωτικών γραμμών ελεγχόμενης φυσικής πρόσβασης).

III.2.Ε.iv. Πρωτόκολλα δικτύου

Απαγορεύεται η χρήση ευπαθών ως προς την ασφάλεια πρωτοκόλλων όπως FTP, telnet (όπου δεν γίνεται κρυπτογράφηση) και, όταν υπηρεσίες τέτοιων πρωτοκόλλων είναι αναγκαίες, γίνεται χρήση των αντίστοιχων ασφαλών (όπως, για παράδειγμα, SFTP, SSH).

III.2.Ε.v. Περιμετρική ασφάλεια

Ο Υπεύθυνος Ασφαλείας θα πρέπει να ελέγχει τις δικτυακές συνδέσεις του εσωτερικού δικτύου του Πανεπιστημίου από και προς το διαδίκτυο ή άλλα εξωτερικά, μη έμπιστα, δίκτυα όπως μέσω του σημείου ελέγχου της περιμέτρου (firewall). Οι συνδέσεις που ενεργοποιούνται μέσω του firewall και οι υπηρεσίες που εξυπηρετούν πρέπει να εγκρίνονται από τον Υπεύθυνο Ασφαλείας, ο οποίος τηρεί επικαιροποιημένο κατάλογο με τις εγκεκριμένες συνδέσεις από και προς το δίκτυο του Πανεπιστημίου και τις υπηρεσίες που εξυπηρετούν.

III.2.Στ. Ασφάλεια λογισμικού

III.2.Στ.i. Σχεδιασμός εφαρμογών

Ο σχεδιασμός των εφαρμογών, που χρησιμοποιούνται για την επεξεργασία ΔΠΧ πραγματοποιείται λαμβάνοντας υπόψη τις βασικές αρχές της προστασίας δεδομένων προσωπικού χαρακτήρα και της ιδιωτικότητας (privacy by design). Ως εκ τούτου, οι εφαρμογές πρέπει να ακολουθούν την αρχή της ελαχιστοποίησης των δεδομένων, καθώς και της ποιότητας των δεδομένων και να περιλαμβάνουν τη δυνατότητα της διαγραφής

δεδομένων μετά το χρονικό διάστημα που απαιτείται για την πραγματοποίηση του σκοπού της επεξεργασίας. Επίσης, πρέπει να επιτρέπουν την υλοποίηση όλων των απαιτούμενων τεχνικών μηχανισμών ασφαλείας για την προστασία των δεδομένων από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας.

III.2.Στ.ii. Ασφαλής ανάπτυξη εφαρμογών

Σε περίπτωση ανάπτυξης εφαρμογών είτε εσωτερικά από το Πανεπιστήμιο Κρήτης είτε από εξωτερικό συνεργάτη θα πρέπει να προβλέπεται διαδικασία ασφαλούς υλοποίησης λογισμικού, ώστε να εντοπισθούν τυχόν ευπάθειες αυτού ως προς την ασφάλεια, προτού αυτό μεταβεί σε λειτουργική φάση. Στις περιπτώσεις που η ανάπτυξη των εφαρμογών γίνεται από εξωτερικό συνεργάτη, θα πρέπει να υπάρχουν προδιαγραφές ασφαλείας της εφαρμογής στο έγγραφο περιγραφής απαιτήσεων λογισμικού, το οποίο θα εμπεριέχεται στη σύμβαση με τον εκάστοτε εξωτερικό συνεργάτη.

III.2.Στ.iii. Προστασία αρχείων λειτουργικών συστημάτων

Τα λειτουργικά αρχεία των συστημάτων (system files), τα δεδομένα ελέγχου συστημάτων (system test data), καθώς και ο πηγαίος κώδικας (sourcecode) των προγραμμάτων λογισμικού πρέπει να ελέγχονται και να προστατεύονται από μη εξουσιοδοτημένη πρόσβαση ή τροποποίηση.

III.2.Ζ. Διαχείριση αλλαγών

III.2.Ζ.i. Πολιτική διαχείρισης αλλαγών

Ο Υπεύθυνος Ασφαλείας θα πρέπει, στο πλαίσιο της πολιτικής διαχείρισης όλων των αλλαγών που πραγματοποιούνται στα πληροφοριακά συστήματα, να καταγράφει τα αιτήματα αλλαγής, να καθορίζει τα άτομα που έχουν δικαίωμα έγκρισης των αλλαγών, καθώς και τα κριτήρια αποδοχής της αλλαγής και το χρονοδιάγραμμα υλοποίησης της. Καμία αλλαγή δεν θα γίνεται αποδεκτή αν δεν επιβάλλεται για την προσήκουσα εκτέλεση των εργασιών του χρήστη, που αιτείται την αλλαγή.

III.2.Ζ.ii. Περιβάλλον δοκιμών

Πριν από τη θέση σε λειτουργία των ενημερώσεων λογισμικού θα πρέπει να γίνεται δοκιμή αυτών τόσο σε επίπεδο επιμέρους εφαρμογών όσο και σε επίπεδο λειτουργικού συστήματος σε δοκιμαστικό περιβάλλον.

Η ανάπτυξη λογισμικού γίνεται σε δοκιμαστικό περιβάλλον, το οποίο είναι απομονωμένο από το παραγωγικό σύστημα και επικαιροποιημένο. Κατά την ανάπτυξη ή αναβάθμιση λογισμικού και τη δοκιμή του χρησιμοποιούνται δοκιμαστικά και όχι πραγματικά δεδομένα ή δεδομένα του παραγωγικού συστήματος, εκτός εάν κάτι τέτοιο είναι απολύτως απαραίτητο και δεν υπάρχει εναλλακτική λύση. Αν είναι αναγκαίο μπορούν να χρησιμοποιηθούν πραγματικά δεδομένα σε ανωνυμοποιημένη μορφή ή διαφορετικά πρέπει να περιορίζονται στα απολύτως απαραίτητα για τους σκοπούς του ελέγχου.

III.3. Μέτρα φυσικής ασφαλείας

III.3.1. Έλεγχος φυσικής πρόσβασης

III.3.1.i. Φυσική πρόσβαση σε εγκαταστάσεις και computer room

Στο χώρο όπου βρίσκεται ο φυσικός εξοπλισμός (συμπεριλαμβανομένης τηλεπικοινωνιακής και δικτυακής καλωδίωσης) που υποστηρίζει τα πληροφοριακά συστήματα και την επεξεργασία ΔΠΧ, επιτρέπεται η πρόσβαση μόνο σε εξουσιοδοτημένο προσωπικό με τη χρήση κωδικού ασφαλείας. Η πρόσβαση στο συγκεκριμένο φυσικό χώρο καταγράφεται.

III.3.1.ii. Τήρηση καταλόγου

Ο Υπεύθυνος Ασφαλείας διατηρεί επικαιροποιημένο κατάλογο με τα δικαιώματα φυσικής πρόσβασης των μελών του προσωπικού και των εργαζομένων του Πανεπιστημίου Κρήτης, καθώς και με τους εργαζόμενους που διαθέτουν κωδικούς, κάρτες εισόδου και κλειδιά για πρόσβαση σε κρίσιμους, ως προς την ασφάλεια, χώρους. Οι κατάλογοι αυτοί υπόκεινται σε τακτική αναθεώρηση.

III.3.2. Περιβαλλοντική ασφάλεια - Προστασία από φυσικές καταστροφές

Το Πανεπιστήμιο Κρήτης υποχρεούται να λαμβάνει όλα εκείνα τα απαραίτητα μέτρα για την προστασία των κτιρίων, των κρίσιμων χώρων, του computer room, των γραφείων των εργαζομένων, του εξοπλισμού πληροφορικής και του χώρου τήρησης φυσικού αρχείου από ζημιές που μπορούν να προκληθούν από φυσικές καταστροφές ή κακόβουλες ενέργειες, όπως πλημμύρα, υπερθέρμανση, πυρκαγιά, σεισμό, έκρηξη, διαρροή νερού, διακοπή ρεύματος, διάρρηξη/κλοπή, βανδαλισμό, κ.λπ. Ενδεικτικά μέτρα που έχουν ληφθεί προς αυτή την κατεύθυνση είναι τα εξής: συναγερμός, πόρτες και παράθυρα ασφαλείας, πυροπροστασία, απομάκρυνση εξοπλισμού από υδροσωληνώσεις και πηγές σκόνης, ανιχνευτές υγρασίας και πλημμύρας, αδιάλειπτη παροχή ρεύματος μέσω σταθεροποιητών/γεννητριών, κ.λπ.

III.3.3. Έκθεση εγγράφων

III.3.3.i. Τοποθέτηση φακέλων

Οι φάκελοι που περιέχουν ΔΠΧ (φυσικό αρχείο) πρέπει να είναι τοποθετημένοι σε φωριαμούς που κλειδώνουν και να μην εκτίθενται σε κοινή θέα.

III.3.3.ii. Μεταφορά φακέλων

Η μεταφορά των φυσικών φακέλων σε διαφορετικά γραφεία ή οργανωτικές μονάδες του Πανεπιστημίου πρέπει να καταγράφεται, από το μέλος του προσωπικού ή τον εργαζόμενο που είναι υπεύθυνος για την τήρηση των εν λόγω φακέλων.

III.3.3.iii. Πολιτική «καθαρού Γραφείου» (Clean desk policy)

Έγγραφα και φορητά μέσα αποθήκευσης, που περιέχουν δεδομένα προσωπικού χαρακτήρα ή εμπιστευτικές πληροφορίες δεν θα πρέπει να αφήνονται εκτεθειμένα πάνω σε γραφεία, χωρίς επίβλεψη.

Τα μέλη του προσωπικού και οι εργαζόμενοι θα πρέπει να φροντίζουν ώστε όλα τα δεδομένα προσωπικού χαρακτήρα και οι εμπιστευτικές πληροφορίες (σε έντυπη ή ηλεκτρονική μορφή) να είναι ασφαλή στο χώρο εργασίας τους στο τέλος του ωραρίου εργασίας τους και όταν απουσιάζουν από τη θέση εργασίας τους.

Ο υπολογιστής θα πρέπει να κλειδώνει (screensaver), όταν ο χρήστης απουσιάζει από τη θέση εργασίας του και να απενεργοποιείται κατά το πέρας του ωραρίου εργασίας.

Συρτάρια και φωριαμοί που περιέχουν δεδομένα προσωπικού χαρακτήρα και εμπιστευτικές πληροφορίες, θα πρέπει να παραμένουν κλειστά και κλειδωμένα όταν δεν επιβλέπονται.

Κλειδιά που χρησιμοποιούνται για την πρόσβαση σε χώρους, όπου φυλάσσονται δεδομένα προσωπικού χαρακτήρα και εμπιστευτικές πληροφορίες, δεν θα πρέπει να αφήνονται εκτεθειμένα πάνω σε γραφεία.

Στο τέλος του ωραρίου εργασίας οι φορητοί υπολογιστές θα πρέπει να κλειδώνονται σε συρτάρι ή φωριαμό.

Οι κωδικοί πρόσβασης δεν θα πρέπει να γράφονται σε αυτοκόλλητα σημειώματα επικολλημένα στον υπολογιστή ή να αφήνονται εκτεθειμένοι στο γραφείο του χρήστη.

Εκτυπώσεις που περιέχουν δεδομένα προσωπικού χαρακτήρα και εμπιστευτικές πληροφορίες θα πρέπει να αναλαμβάνονται αμέσως από τον εκτυπωτή.

Έγγραφα προς καταστροφή που περιέχουν δεδομένα προσωπικού χαρακτήρα και εμπιστευτικές πληροφορίες, θα πρέπει να τεμαχίζονται σε λωρίδες σε μηχανή τεμαχισμού (shredder).

Δεδομένα προσωπικού χαρακτήρα και εμπιστευτικές πληροφορίες που γράφονται σε λευκοπίνακα (πίνακα μαρκαδόρου) θα πρέπει να διαγράφονται αμέσως μετά τη χρήση τους.

Φορητοί υπολογιστές και tablets θα πρέπει να φυλάσσονται σε χώρους που κλειδώνουν ακόμη και όταν απομακρύνονται από το χώρο εργασίας (π.χ. οικία χρήστη).

Φορητά μέσα μαζικής αποθήκευσης, όπως CDROM, DVD ή USB θα πρέπει να φυλάσσονται σε χώρο που κλειδώνει.

Θα πρέπει να αναλαμβάνονται αμέσως τα έγγραφα από τα φωτοτυπικά, εκτυπωτικά και τηλεομοιοτυπικά μηχανήματα, προκειμένου να διασφαλιστεί ότι τα έγγραφα που περιέχουν δεδομένα προσωπικού χαρακτήρα / εμπιστευτικές πληροφορίες δεν αφήνονται εκτεθειμένα ή δεν αναλαμβάνονται από μη εξουσιοδοτημένα για τη χρήση τους πρόσωπα.

IV. Πολιτικές για τη διασφάλιση της συμμόρφωσης προς την ισχύουσα νομοθεσία

Το Πανεπιστήμιο Κρήτης έχει υιοθετήσει μία σειρά πολιτικών και διαδικασιών για να διασφαλίσει τη συμμόρφωσή του προς την εκάστοτε ισχύουσα νομοθεσία για την προστασία των δεδομένων προσωπικού χαρακτήρα.

Ειδικότερα, το Πανεπιστήμιο **έχει υιοθετήσει πολιτικές που αφορούν:**

Α. τη διαβίβαση των δεδομένων προσωπικού χαρακτήρα

Β. τη διατήρηση των δεδομένων προσωπικού χαρακτήρα

Γ. τα δικαιώματα των Υποκειμένων των Δεδομένων

Δ. την παραβίαση των δεδομένων προσωπικού χαρακτήρα

Ε. τη Συγκατάθεση των Υποκειμένων των Δεδομένων, όπου αυτή απαιτείται

IV Α. Πολιτική Διαβίβασης ΔΠΧ

Για τις ανάγκες των δραστηριοτήτων του, το Πανεπιστήμιο Κρήτης ενδέχεται να απαιτηθεί να διαβιβάσει δεδομένα προσωπικού χαρακτήρα σε τρίτους εκτός Ευρωπαϊκής Ένωσης (Ε.Ε.). Στην περίπτωση αυτή οφείλει να εξασφαλίσει ένα επαρκές επίπεδο προστασίας των δεδομένων προσωπικού χαρακτήρα, που θα αποτελέσουν αντικείμενο διαβίβασης, ακολουθώντας τους κάτωθι κανόνες.

Προαπαιτούμενα για τις διαβιβάσεις

Το Πανεπιστήμιο Κρήτης οφείλει να συμβουλεύεται τον Υπεύθυνο Προστασίας Δεδομένων, ο οποίος θα ελέγχει συγκεκριμένα στοιχεία πριν από οποιαδήποτε διαβίβαση εκτός ΕΕ, όπως αναφέρεται κατωτέρω:

- Τις κατηγορίες των ΔΠΧ που αφορά η διαβίβαση,
- Τη φύση της Επεξεργασίας,
- Τη νομική βάση της διαβίβασης,
- Να καθορίσει αν είναι αναγκαία μία Εκτίμηση Αντίκτυπου Προστασίας Δεδομένων (DPIA).

Για όλες τις διαβιβάσεις, ο Υπεύθυνος Προστασίας Δεδομένων οφείλει:

- Να παρέχει μία αιτιολογημένη γνώμη και να καθορίζει τα αναγκαία απαιτούμενα για να ολοκληρωθεί η διαβίβαση.
- Να συγκεντρώσει όλες τις διαθέσιμες πληροφορίες σχετικά με τον αποδέκτη των ΔΠΧ.

Διαβίβαση σε χώρες εκτός ΕΕ οι οποίες δεν παρέχουν επαρκές επίπεδο προστασίας

Ι. Χρήση Τυποποιημένων Ρητρών της ΕΕ που προτείνονται από την Ευρωπαϊκή Επιτροπή

Η Ευρωπαϊκή Επιτροπή έχει εκδώσει διάφορες σειρές τυποποιημένων συμβατικών ρητρών για τη διαβίβαση Δεδομένων Προσωπικού Χαρακτήρα σε Εκτελούντα την Επεξεργασία που έχει την έδρα του εκτός ΕΕ (*https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32010D0087&from=EL*) (“Τυποποιημένες Ρήτρες της ΕΕ”). Αυτές οι ρήτρες παρέχουν επαρκείς εγγυήσεις σχετικά με την προστασία του απορρήτου και τα θεμελιώδη δικαιώματα και ελευθερίες του Υποκειμένου των Δεδομένων και σχετικά με την άσκηση των αντίστοιχων δικαιωμάτων.

Όταν διαβιβάζονται ΔΠΧ σε τρίτο, που δεν παρέχει επαρκές επίπεδο προστασίας, το Πανεπιστήμιο Κρήτης:

- θα υπογράφει συγκεκριμένο συμφωνητικό με τον τρίτο ώστε να καθοριστούν οι όροι και το νομικό πλαίσιο της διαβίβασης.
- οι Τυποποιημένες Ρήτρες της ΕΕ θα επισυνάπτονται ως παράρτημα στο εν λόγω συμφωνητικό ώστε να διασφαλίζεται η παροχή ενός επαρκούς επιπέδου προστασίας των ΔΠΧ.

II. Χρήση κώδικα δεοντολογίας και εγκεκριμένης πιστοποίησης

Είναι δυνατό να επιτραπούν διαβιβάσεις εκτός ΕΕ, αν ο τρίτος συμφωνήσει να εφαρμόσει εγγυήσεις που περιλαμβάνονται σε συγκεκριμένο κώδικα δεοντολογίας ή πιστοποίηση για την προστασία ΔΠΧ.

Διαβίβαση σε χώρες εκτός ΕΕ οι οποίες παρέχουν επαρκές επίπεδο προστασίας

- Η Ευρωπαϊκή Επιτροπή έχει καταρτίσει έναν κατάλογο, ο οποίος βασίζεται σε συγκεκριμένα κριτήρια, **τρίτων χωρών οι οποίες εγγυώνται επαρκές επίπεδο προστασίας** (Ανδόρα, Αργεντινή, Καναδάς, Νήσοι Φερόες, Guernsey, Ισραήλ, Νήσος Μαν, Ιαπωνία, Jersey, Νέα Ζηλανδία, Ελβετία, Ουρουγουάη και, για συγκεκριμένες περιπτώσεις, ΗΠΑ).
- **Όταν διαβιβάζονται ΔΠΧ σε αυτές τις χώρες δεν απαιτείται ειδική εξουσιοδότηση.**

Παρεκκλίσεις σε ειδικές περιπτώσεις

Ελλείψει απόφασης επάρκειας ή επαρκών εγγυήσεων από τον τρίτο, η διαβίβαση δεν μπορεί να λάβει χώρα εκτός ΕΕ.

Παρόλα αυτά, σε συγκεκριμένες περιπτώσεις, η διαβίβαση ΔΠΧ εκτός ΕΕ μπορεί να επιτραπεί μόνο αν ισχύουν οι ακόλουθες προϋποθέσεις:

- Το Υποκείμενο των Δεδομένων έχει συναινέσει ρητά στη διαβίβαση: αφού έχει ενημερωθεί για τους πιθανούς κινδύνους μίας τέτοιας διαβίβασης για το ίδιο, λόγω της απουσίας απόφασης επάρκειας και κατάλληλων εγγυήσεων.
- Η διαβίβαση είναι απαραίτητη για την εκτέλεση σύμβασης μεταξύ του Υποκειμένου των Δεδομένων και του Υπεύθυνου Επεξεργασίας ή την εφαρμογή προσυμβατικών μέτρων που λαμβάνονται κατόπιν αιτήματος του Υποκειμένου.
- Η διαβίβαση είναι απαραίτητη για θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων.
- Η διαβίβαση είναι απαραίτητη για την προστασία ζωτικών συμφερόντων του Υποκειμένου των Δεδομένων ή άλλων προσώπων, όταν το Υποκείμενο των Δεδομένων είναι σε φυσική ή νομική αδυναμία να δώσει συγκατάθεση.

IV Β. Πολιτική Διατήρησης ΔΠΧ

Τα δεδομένα προσωπικού χαρακτήρα πρέπει να υφίστανται την κατάλληλη διαχείριση και επεξεργασία καθ' όλη τη διάρκεια του κύκλου ζωής τους, από τη συλλογή μέχρι την καταστροφή τους. Ο προγραμματισμός της καταστροφής των ΔΠΧ αποτελεί ταυτόχρονα κανονιστική απαίτηση για την προστασία των ΔΠΧ και αναπόσπαστο μέρος της σύννομης επεξεργασίας τους. Η παρούσα Πολιτική καθορίζει τις αρχές διατήρησης και καταστροφής των ΔΠΧ που επεξεργάζεται το Πανεπιστήμιο Κρήτης, προκειμένου αυτή να συμμορφώνεται με τον Κανονισμό και την εφαρμοστέα νομοθεσία περί προστασίας ΔΠΧ.

I. Σκοπός

Μία βασική υποχρέωση, η τήρηση της οποίας θα πρέπει να διασφαλίζεται κατά την επεξεργασία των ΔΠΧ προκειμένου αυτή να είναι σύννομη, είναι η διατήρηση των ΔΠΧ για χρονικό διάστημα όχι περισσότερο από όσο είναι απαραίτητο για τους λόγους για τους οποίους υφίσταται η επεξεργασία. Πέραν από αυτή την απαίτηση, νομικές και συμβατικές απαιτήσεις θα καθορίζουν την ελάχιστη περίοδο διατήρησης των ΔΠΧ πριν καταστραφούν και τις συνθήκες υπό τις οποίες αυτά θα καταστραφούν, όταν λήξει η ελάχιστη περίοδος διατήρησης.

Η παρούσα Πολιτική εφαρμόζεται για κάθε επεξεργασία ΔΠΧ στην οποία προβαίνει το Πανεπιστήμιο ως Υπεύθυνος Επεξεργασίας ή ως Εκτελών την Επεξεργασία.

II. Απαιτήσεις διατήρησης και διαγραφής

Χρόνος Χρήσης

Τα ΔΠΧ είναι ακόμα απαραίτητα για τους σκοπούς της Επεξεργασίας.

Χρόνος αποκλεισμού

Τα ΔΠΧ δεν είναι πλέον απαραίτητα για τους σκοπούς της επεξεργασίας, παρόλα αυτά θα μπορούσε ακόμα να υφίσταται ανάγκη διατήρησής τους για ορισμένο διάστημα (όπως, για την εκπλήρωση νομικών, κανονιστικών ή λογιστικών σκοπών). Κατά τη διάρκεια αυτής της φάσης τα ΔΠΧ:

- Δεν μπορούν να καταστραφούν,
- Πρέπει να είναι διαθέσιμα μόνο σε ένα περιορισμένο αριθμό ανθρώπων (συνήθως μόνο σε εκείνους που είναι υπεύθυνοι να εκπληρώσουν αυτούς τους νομικούς, κανονιστικούς ή λογιστικούς σκοπούς).

Χρόνος καταστροφής

Τα ΔΠΧ δεν είναι πλέον απαραίτητα ούτε για τους σκοπούς επεξεργασίας ούτε για νομικές ή κανονιστικές ανάγκες. Συνεπώς, τα ΔΠΧ θα πρέπει να καταστραφούν (διαγραφούν ή ανωνυμοποιηθούν) σύμφωνα με τη νομοθεσία.

III. Αρχές διατήρησης και διαγραφής

Αποτελεί κατευθυντήρια αρχή ότι όταν τα ΔΠΧ δεν είναι πλέον απαραίτητα και μπορούν (ή πρέπει) να καταστραφούν, η διαγραφή τους καθίσταται απαραίτητη.

Η συμμόρφωση με αυτήν την πολιτική θα διασφαλίσει ότι τα αρχεία τηρούνται όσο είναι απαραίτητο και ότι παρωχημένα αρχεία καταστρέφονται με συστηματικό, ελεγχόμενο, ανιχνεύσιμο και ασφαλή τρόπο. Για να εφαρμοστεί ένας τέτοιος μηχανισμός διαγραφής, πρέπει να ληφθούν υπόψη τα κάτωθι:

Ελάχιστο Διάστημα Διατήρησης

Για πόσο διάστημα πρέπει να διατηρηθούν τα ΔΠΧ πριν καταστραφούν. Το ελάχιστο διάστημα διατήρησης αποτρέπει την καταστροφή των ΔΠΧ για ένα χρονικό διάστημα. Συνήθως είναι το μεγαλύτερο χρονικό διάστημα μεταξύ:

- Το ελάχιστο χρονικό διάστημα διατήρησης που απαιτείται από νομικούς, κανονιστικούς ή λογιστικούς σκοπούς και
- Το ελάχιστο χρονικό διάστημα διατήρησης που απαιτείται από το Πανεπιστήμιο για τους σκοπούς επεξεργασίας.

Μέγιστο Διάστημα Διατήρησης

Για πόσο διάστημα τα ΔΠΧ επιτρέπεται να διατηρηθούν πριν καταστραφούν. Αυτό το ανώτατο όριο προσδιορίζεται κυρίως από:

- Απαιτήσεις προστασίας ΔΠΧ (όπως ο Γενικός Κανονισμός για την Προστασία Δεδομένων), που επιβάλουν τα δεδομένα να μην τηρούνται για χρονικό διάστημα μεγαλύτερο από όσο είναι

	απαραίτητο για τους σκοπούς για τους οποίους επεξεργάζονται, • Συστάσεις από αρχές προστασίας δεδομένων, • Συμφωνία με το υποκείμενο των δεδομένων.
Συμβάν ενεργοποίησης	Αποτελεί το σημείο εκκίνησης για να ξεκινήσει η περίοδος διατήρησης των δεδομένων (π.χ. ημερομηνία της τελευταίας χρήσης των ΔΠΧ, ημερομηνία λήξης/λύσης συμβάσεων, χρόνος παραγραφής απαιτήσεων κ.λπ.).

IV. Παράγοντες που επηρεάζουν τις περιόδους διατήρησης

- **Νομικές υποχρεώσεις**
    - ΓΚΠΔ,
    - Ασφαλιστική νομοθεσία,
    - Φορολογική νομοθεσία,
    - Νομοθεσία που διέπει το Πανεπιστήμιο και τη λειτουργία του.

- **Απαιτήσεις Αρχής Προστασίας ΔΠΧ**

- **Συμβατικές υποχρεώσεις**

V. Εσωτερικές απαιτήσεις

ΔΠΧ εργαζομένων του Πανεπιστημίου: Θα διατηρούνται καθ' όλη τη διάρκεια της σχέσης εργασίας με το Πανεπιστήμιο και για είκοσι (20) έτη μετά τη λύση ή λήξη της, εκτός αν εκκρεμεί δικαστική διαμάχη του υποκειμένου των ΔΠΧ με το Πανεπιστήμιο, οπότε θα διατηρούνται μέχρι την έκδοση αμετάκλητης δικαστικής απόφασης. Από το χρόνο λύσης ή λήξης της εργασιακής σχέσης με τον εργαζόμενο και μέχρι τη συμπλήρωση είκοσι (20) ετών, τα ΔΠΧ θα τηρούνται ψευδωνυμοποιημένα.

Τα ΔΠΧ των υποψηφίων εργαζομένων θα διαγράφονται αμέσως μετά την απόρριψη της υποψηφιότητάς τους.

ΔΠΧ πελατών & προμηθευτών: Θα διατηρούνται για όσο χρόνο είναι απαραίτητος για την ολοκλήρωση του σκοπού επεξεργασίας και μέχρι τη συμπλήρωση 20ετίας. Από το

χρόνο ολοκλήρωσης του σκοπού επεξεργασίας των ΔΠΧ και μέχρι τη συμπλήρωση 20ετίας τα ΔΠΧ θα διατηρούνται ψευδωνυμοποιημένα.

VI. Εφαρμογή μηχανισμών διαγραφής

Μηχανισμοί καταστροφής (χειροκίνητοι ή αυτοματοποιημένοι) πρέπει να εφαρμόζονται για να επιτρέπουν την καταστροφή (συμπεριλαμβανομένης της ανωνυμοποίησης) των διαφόρων ομάδων ΔΠΧ, σύμφωνα με τα προβλεπόμενα στην παράγραφο **III.1.Ε. Καταστροφή δεδομένων και αποθηκευτικών μέσων** της παρούσας.

Οι απαιτήσεις της παρούσας Πολιτικής θα πρέπει να ληφθούν υπόψη κατά τη διάρκεια της φάσης σχεδιασμού νέων συστημάτων/διαδικασιών, στο πλαίσιο των οποίων θα διενεργείται επεξεργασία ΔΠΧ, έτσι ώστε να καταστεί δυνατή η αυτοματοποιημένη διαγραφή (ανωνυμοποίηση) των ΔΠΧ.

Όταν πρόκειται να πραγματοποιηθεί επεξεργασία των ΔΠΧ για λογαριασμό του Πανεπιστημίου από εκτελούντες την επεξεργασία, θα πρέπει αυτή να χρησιμοποιήσει μόνο εκτελούντες την επεξεργασία που εγγυώνται ότι θα πληρούν τις απαιτήσεις της παρούσας Πολιτικής και θα εξασφαλίζουν τεκμηρίωση της επιλογής επεξεργασίας, ως μέρος των αρχών της λογοδοσίας και του απορρήτου από το σχεδιασμό.

VII. Αναθεώρηση της πολιτικής και του προγράμματος διατήρησης ΔΠΧ σε τακτική βάση

Ως αποτέλεσμα των αλλαγών στους κανονισμούς, τη νομολογία, τις συστάσεις από την Αρχή Προστασίας ΔΠΧ ή την εξέλιξη των επιχειρηματικών αναγκών, αυτή η Πολιτική θα πρέπει να αναθεωρείται σε τακτική βάση.

VIII. Σύνταξη αναφοράς σχετικά με τη συμμόρφωση με την παρούσα πολιτική σε ετήσια βάση

Το Πανεπιστήμιο θα διεξάγει ετήσιο έλεγχο για να διαπιστώσει τα κενά της παρούσας Πολιτικής, καθώς και το επίπεδο συμμόρφωσης και ωριμότητας αυτής.

IV Γ. Πολιτική Συγκατάθεσης

I. Πεδίο εφαρμογής

Όταν κάποια από τις δραστηριότητες του Πανεπιστημίου Κρήτης συνεπάγεται την επεξεργασία ΔΠΧ και το Πανεπιστήμιο ενεργεί ως Υπεύθυνος Επεξεργασίας δεδομένων, πρέπει πάντοτε να εξετάζει πρώτα την κατάλληλη νόμιμη βάση για την προβλεπόμενη επεξεργασία.

Κατάλληλη νομική βάση για τις δραστηριότητες του Πανεπιστημίου, που αφορούν στη συνταγματική αποστολή του, είναι, κατ' αρχήν, η νόμιμη βάση του άρθρου 6 παράγραφος 1 περίπτωση (ε) του ΓΚΠΔ, που αφορά στα απλά ΔΠΧ. Σε θέματα εργασιακών σχέσεων και συμβάσεων εφαρμόζεται η περίπτωση (β) της πιο πάνω παραγράφου 1 του ίδιου άρθρου.

Όσον αφορά στα ΔΠΧ ειδικών κατηγοριών θα πρέπει να συμβουλεύεστε το άρθρο 9 του ΓΚΠΔ. Προκρίνονται οι βάσεις της παρ. 2 περ. (β) [για θέματα εργατικού δικαίου και κοινωνικής ασφάλισης], (ζ) [για θέματα δημοσίου συμφέροντος] και (ι) [για θέματα έρευνας και στατιστικούς σκοπούς].

Η συγκατάθεση επιλέγεται ως νόμιμη βάση επεξεργασίας, **μόνο** όταν δεν υπάρχει άλλη νόμιμη βάση για την Επεξεργασία των ΔΠΧ του Υποκειμένου των Δεδομένων. Το Υποκείμενο των Δεδομένων μπορεί να κληθεί να συναινέσει στην Επεξεργασία των Δεδομένων του, προκειμένου να είναι νόμιμη η Επεξεργασία.

II. Ορισμός της Συγκατάθεσης

Όπως ορίζεται στον Κανονισμό (άρθρο 4 παρ. 11), η συγκατάθεση πρέπει να είναι:

Ορισμός σύμφωνα με τον Κανονισμό (άρθρο 4 παρ. 11)	**Επεξήγηση[2]**
"ελεύθερη"	Αυτό σημαίνει να παρέχεται στο υποκείμενο των δεδομένων πραγματική συνεχής επιλογή και έλεγχος του τρόπου χρήσης των δεδομένων τους. *-Εάν η συγκατάθεση αποτελεί μη διαπραγματεύσιμο μέρος των όρων και προϋποθέσεων για τη συνεργασία - συναλλαγή με το Πανεπιστήμιο, θεωρείται ότι δεν δόθηκε ελεύθερα.* *- η συγκατάθεση δεν θα θεωρείται ελεύθερη εάν το Υποκείμενο των δεδομένων δεν είναι σε θέση να αρνηθεί ή να αποσύρει τη συναίνεσή του χωρίς βλάβη.*

[2]Επεξήγηση από τις «Κατευθυντήριες γραμμές για τη Συναίνεση» σύμφωνα με τον Κανονισμό 2016/679 που υιοθετήθηκε στις 28 Νοεμβρίου 2017.

“συγκεκριμένη ”	Η συγκατάθεση πρέπει να δίνεται ειδικά σε σχέση με έναν ή περισσότερους ειδικούς σκοπούς της Επεξεργασίας. *Εάν ο υπεύθυνος επεξεργασίας επεξεργάζεται δεδομένα βάσει συγκατάθεσης και επιθυμεί να επεξεργαστεί τα δεδομένα για έναν καινούργιο σκοπό, ο υπεύθυνος επεξεργασίας πρέπει να ζητήσει νέα συγκατάθεση από το Υποκείμενο των δεδομένων για το νέο σκοπό της Επεξεργασίας. Η αρχική συγκατάθεση δεν θα νομιμοποιήσει ποτέ περαιτέρω ή νέους σκοπούς επεξεργασίας.*
“ρητή”	Το αίτημα για συγκατάθεση πρέπει να αναφέρει σαφώς την ταυτότητα του Υπεύθυνου Επεξεργασίας, το είδος των ΔΠΧ που θα τύχουν επεξεργασίας, την ύπαρξη του δικαιώματος ανάκλησης της συγκατάθεσης και το σκοπό της Επεξεργασίας. *Η παροχή πληροφοριών στα Υποκείμενα των δεδομένων πριν από τη συναίνεσή τους είναι απαραίτητη προκειμένου να μπορέσουν να λάβουν τεκμηριωμένες αποφάσεις, να κατανοήσουν σε τι συμφωνούν και για παράδειγμα να ασκήσουν το δικαίωμά τους να αποσύρουν τη συγκατάθεσή τους.*
“εν πλήρει επιγνώσει”	Το αίτημα συγκατάθεσης πρέπει να είναι εμφανές, να διαχωρίζεται από άλλους όρους και προϋποθέσεις, να είναι σύντομο, σε σαφή γλώσσα και να κατανοείται εύκολα. *Η συγκατάθεση μπορεί να ληφθεί μέσω γραπτής ή (καταγεγραμμένης) προφορικής δήλωσης, συμπεριλαμβανομένων ηλεκτρονικών μέσων.*
“[που δίνεται] με δήλωση ή με σαφή θετική ενέργεια [του Υποκειμένου των Δεδομένων]”	Η συγκατάθεση πρέπει να είναι προφανής και να απαιτεί θετική ενέργεια επιλογής. *Η συγκατάθεση μπορεί να επιτευχθεί μέσω καταγεγραμμένης προφορικής δήλωσης, αν και πρέπει να γίνει μνεία των πληροφοριών που είναι διαθέσιμες στο Υποκείμενο των δεδομένων πριν από την ένδειξη της συγκατάθεσης.*
“[το Υποκείμενο των Δεδομένων] εκδηλώνει ότι συμφωνεί να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν]”	Σε ορισμένες περιπτώσεις όπου εγκυμονούνται σοβαροί κίνδυνοι προστασίας δεδομένων, η ρητή συγκατάθεση πρέπει να επιβεβαιώνεται ρητά με λόγια και όχι με οποιαδήποτε άλλη θετική ενέργεια με αποτελεσματική και ρητή διάρκεια. *Ένας προφανής τρόπος προκειμένου να εξασφαλιστεί ότι η συναίνεση είναι σαφής θα ήταν να επιβεβαιωθεί ρητά η συγκατάθεσή σε γραπτή δήλωση.*

Δεδομένου ότι η συγκατάθεση του Υποκειμένου των Δεδομένων μπορεί να ανακληθεί χωρίς προειδοποίηση και ανά πάσα στιγμή, η συγκατάθεση δεν πρέπει να αποτελεί προϋπόθεση για τη λήψη μιας υπηρεσίας εκ μέρους του Υποκειμένου των Δεδομένων, εκτός εάν είναι η μόνη νόμιμη βάση για την επεξεργασία των Δεδομένων Προσωπικού Χαρακτήρα.

Η συγκατάθεση ενδέχεται να απαιτείται, εάν η προτεινόμενη Επεξεργασία Δεδομένων περιλαμβάνει συλλογή Ειδικών Κατηγοριών Δεδομένων, αυτοματοποιημένη λήψη αποφάσεων, επεξεργασία δεδομένων ανηλίκων ή μεταφορά δεδομένων εκτός ΕΕ/ΕΟΧ.

Όπου είναι αναγκαίο να λαμβάνεται η συγκατάθεση του Υποκειμένου των Δεδομένων:

- **Το Πανεπιστήμιο Κρήτης ενεργώντας ως Υπεύθυνος Επεξεργασίας δεδομένων, πρέπει να συλλέγει και να τηρεί αποδείξεις** σχετικά με τη συγκατάθεση του Υποκειμένου των Δεδομένων.
- **Το Πανεπιστήμιο** Κρήτης **ενεργώντας ως Εκτελών την επεξεργασία ή Υπο-Εκτελών πρέπει να διασφαλίζει και να τηρεί όσο το δυνατόν περισσότερα αποδεικτικά στοιχεία** ότι η Συγκατάθεση των υποκειμένων των δεδομένων έχει συλλεχθεί.

Η λεκτική διατύπωση της συγκατάθεσης πρέπει να αντικατοπτρίζει την κατηγορία Επεξεργασίας και των Δεδομένων Προσωπικού Χαρακτήρα που αφορά και να αποδεικνύει τη θετική συγκατάθεση του Υποκειμένου των Δεδομένων.

III. Χρονική διάρκεια συγκατάθεσης

Δεν προβλέπεται στον Κανονισμό συγκεκριμένο χρονικό διάστημα που θα διαρκέσει η Συγκατάθεση.

Ο χρόνος διαρκείας της συγκατάθεσης θα εξαρτηθεί από το περιεχόμενο, το πεδίο της αρχικής συγκατάθεσης και τις προσδοκίες του Υποκειμένου των Δεδομένων.

Εάν οι εργασίες επεξεργασίας αλλάξουν ή εξελιχθούν σημαντικά, τότε η αρχική συγκατάθεση δεν ισχύει πλέον. Εάν συμβαίνει αυτό, τότε πρέπει να ληφθεί νέα συγκατάθεση.

Η συγκατάθεση πρέπει να ανανεώνεται σε κατάλληλα χρονικά διαστήματα. Η παροχή όλων των πληροφοριών βοηθά να εξασφαλιστεί ότι το Υποκείμενο των Δεδομένων παραμένει καλά ενημερωμένο σχετικά με τον τρόπο με τον οποίο χρησιμοποιούνται τα δεδομένα του και τον τρόπο άσκησης των δικαιωμάτων του.

IV. Διαδικασία για τη διαχείριση της συγκατάθεσης του Υποκειμένου των Δεδομένων

Ταυτοποίηση του Υπεύθυνου Επεξεργασίας Δεδομένων

Το πρώτο βήμα για την έναρξη μιας Επεξεργασίας είναι η ταυτοποίηση του Υπεύθυνου Επεξεργασίας Δεδομένων.

Επαλήθευση των Πληροφοριών που παρέχονται στο Υποκείμενο των Δεδομένων πριν ζητηθεί η Συγκατάθεση

Παροχή των απαραίτητων πληροφοριών στο Υποκείμενο των Δεδομένων ως ακολούθως για τη λήψη της Συγκατάθεσης του:

- **Όνομα του Υπευθύνου Επεξεργασίας,**

- **Κατάλογος των ΔΠΧ που συλλέγονται** και στόχευση σε αυτά που είναι Δεδομένα Ειδικών Κατηγοριών, σύμφωνα με τον Κανονισμό,
- **Αναφορά της ύπαρξης ή πρόβλεψης οποιασδήποτε Διαβίβασης**: προσδιορισμός της χώρας του κάθε εμπλεκόμενου Υπό-Εκτελούντος την επεξεργασία και αν αφορά μέρος ή σύνολο της επεξεργασίας και των σχετικών ΔΠΧ,
- **Αναφορά στις περιόδους διατήρησης** (την περίοδο αρχειοθέτησης και διαγραφής),
- **Αναφορά στην εμπιστευτικότητα:** να διασφαλιστεί και να διατηρηθεί η ακεραιότητα και η εμπιστευτικότητα των ΔΠΧ κάθε Υποκείμενου των Δεδομένων κατά τη διάρκεια όλης της Επεξεργασίας,
- **Επεξήγηση των δικαιωμάτων του σχετικά με την επεξεργασία** (πρόσβαση, τροποποίηση, αντίθεση, ανάκληση, φορητότητα, καταγγελία κ.λπ.).

Λήψη της Συγκατάθεσης του Υποκειμένου των Δεδομένων

Η Συγκατάθεση του Υποκειμένου των Δεδομένων πρέπει να λαμβάνεται πριν από την Επεξεργασία των Προσωπικών Δεδομένων του για το σκοπό για τον οποίο απαιτείται η συγκατάθεση.

Το Πανεπιστήμιο Κρήτης πρέπει να τηρεί τα αποδεικτικά στοιχεία ότι έχει λάβει τη Συγκατάθεση του Υποκειμένου των Δεδομένων (ή ότι η Επεξεργασία αποτελεί εξαίρεση) και για τη νομιμότητά της.

Στο Παράρτημα ΙΙ της παρούσας επισυνάπτεται υπόδειγμα εντύπου ενημέρωσης και συγκατάθεσης του Υποκειμένου των Δεδομένων.

Βήματα που πρέπει να ακολουθηθούν κατά το τέλος της Επεξεργασίας

Το Πανεπιστήμιο Κρήτης οφείλει να φροντίσει ότι μετά το τέλος της Περιόδου Διατήρησης ή Επεξεργασίας δεν δίνεται περαιτέρω πρόσβαση στα ΔΠΧ. Η Μονάδα Ψηφιακής Διακυβέρνησης θα κληθεί να αποκλείσει όλα τα δικαιώματα πρόσβασης στα σχετικά ΔΠΧ και τα Δεδομένα θα ανωνυμοποιηθούν ή θα διαγραφούν σύμφωνα με τη σχετική Πολιτική Διατήρησης και τις πληροφορίες που παρέχονται στο Υποκείμενο των Δεδομένων.

Το τελικό βήμα της λήξης της διαδικασίας επεξεργασίας είναι η ενημέρωση του Υποκειμένου των Δεδομένων για την καταστροφή ή την ανωνυμοποίηση των Δεδομένων Προσωπικού Χαρακτήρα του.

IV Δ. Πολιτική για την προστασία των δικαιωμάτων του Υποκειμένου

I. Εισαγωγή

Η διαχείριση των αιτημάτων των Υποκειμένων των Δεδομένων είναι μία από τις κύριες προτεραιότητες για τη διασφάλιση της πλήρους συμμόρφωσης με τους νόμους και τους κανονισμούς σχετικά με την προστασία των ΔΠΧ.

Για το σκοπό αυτό, το Πανεπιστήμιο υιοθετεί την παρούσα πολιτική για να διαχειρίζεται τα αιτήματα των Υποκειμένων των Δεδομένων.

Η παρούσα πολιτική εφαρμόζεται:

- Για τη διαχείριση αιτημάτων του Υποκειμένου των Δεδομένων, όταν το Πανεπιστήμιο ενεργεί ως Υπεύθυνος Επεξεργασίας Δεδομένων,
- Για τη διαχείριση αιτημάτων του Υποκειμένου των Δεδομένων για επεξεργασία, όταν το Πανεπιστήμιο ενεργεί ως Εκτελών την Επεξεργασία Δεδομένων,
- Για τη διαχείριση της άσκησης του δικαιώματος αποζημίωσης του Υποκειμένου των Δεδομένων.

II. Περιγραφή των αρχών των δικαιωμάτων του Υποκειμένου των Δεδομένων

α. Δικαίωμα πρόσβασης του Υποκειμένου των Δεδομένων

Το Υποκείμενο των Δεδομένων θα έχει το δικαίωμα να λαμβάνει από τον Υπεύθυνο Επεξεργασίας Δεδομένων επιβεβαίωση για το εάν τα ΔΠΧ του υφίστανται επεξεργασία ή όχι, και σε περίπτωση που αυτό συμβαίνει, θα του παρέχεται πρόσβαση στα ΔΠΧ καθώς και στις ακόλουθες πληροφορίες, ακόμα και αν αυτές οι πληροφορίες έχουν ήδη παρασχεθεί στο Υποκείμενο των Δεδομένων (όπως στο έντυπο Συγκατάθεσης, Ενημέρωσης ή μέσω συμβατικών όρων):

- Ο **σκοπός** της επεξεργασίας,
- Οι **κατηγορίες των Δεδομένων Προσωπικού Χαρακτήρα** που αφορά η επεξεργασία,
- Οι **Αποδέκτες** ή οι κατηγορίες Αποδεκτών στους οποίους έχουν διαβιβαστεί, ή θα διαβιβαστούν τα ΔΠΧ, ιδιαίτερα παραλήπτες σε τρίτες χώρες ή διεθνείς οργανισμούς,
- Το **χρονικό διάστημα διατήρησης** για το οποίο θα αποθηκευτούν τα ΔΠΧ ή, αν αυτό δεν είναι δυνατό, τα κριτήρια που θα χρησιμοποιηθούν για να καθοριστεί αυτό το διάστημα,
- Την ύπαρξη του **δικαιώματος άσκησης δικαιώματος στον Υπεύθυνο Επεξεργασίας**,
- Την ύπαρξη του **δικαιώματος υποβολής καταγγελίας** σε εποπτική αρχή,
- Όταν τα Δεδομένα Προσωπικού Χαρακτήρα δεν έχουν συλλεγεί από το Υποκείμενο των Δεδομένων, **κάθε διαθέσιμη πληροφορία σχετικά με την προέλευσή τους,**

- Την ύπαρξη **αυτοματοποιημένης λήψης αποφάσεων**, συμπεριλαμβανομένης της κατάρτισης προφίλ και, τουλάχιστον στις περιπτώσεις αυτές, σημαντικές πληροφορίες σχετικά με τη λογική που ακολουθείται, καθώς και τη σημασία και τις προβλεπόμενες συνέπειες της εν λόγω επεξεργασίας για το Υποκείμενο των Δεδομένων,
- Ο Υπεύθυνος Επεξεργασίας Δεδομένων παρέχει **αντίγραφο των Δεδομένων Προσωπικού Χαρακτήρα που υφίστανται την επεξεργασία**. Για επιπλέον αντίγραφα που ενδέχεται να ζητηθούν από το Υποκείμενο των Δεδομένων, ο Υπεύθυνος Επεξεργασίας Δεδομένων μπορεί να επιβάλει την καταβολή εύλογου τέλους για διοικητικά έξοδα. Ο Υπεύθυνος Επεξεργασίας μπορεί να αρνηθεί εγγράφως την ικανοποίηση αιτήματος άσκησης δικαιώματος, αν αυτό ασκείται καταχρηστικά.
- Εάν το Υποκείμενο των Δεδομένων υποβάλει το αίτημα με ηλεκτρονικά μέσα και εκτός αν το Υποκείμενο των Δεδομένων ζητήσει κάτι διαφορετικό, η ενημέρωση παρέχεται σε ηλεκτρονική μορφή που χρησιμοποιείται συνήθως.

β. Δικαίωμα στην διόρθωση

Το Υποκείμενο των Δικαιωμάτων θα έχει το **δικαίωμα να υποβάλει αίτηση στον Υπεύθυνο Επεξεργασίας Δεδομένων χωρίς αδικαιολόγητη καθυστέρηση για τη διόρθωση ανακριβών ΔΠΧ** που το αφορούν, με την οποία ο Υπεύθυνος Επεξεργασίας Δεδομένων πρέπει να συμμορφωθεί, λαμβάνοντας υπ' όψιν τους σκοπούς της επεξεργασίας. Το Υποκείμενο των Δεδομένων έχει το δικαίωμα να απαιτήσει τη συμπλήρωση ελλιπών ΔΠΧ, μεταξύ άλλων μέσω υποβολής συμπληρωματικής δήλωσης.

Ο Υπεύθυνος Επεξεργασίας Δεδομένων θα ανακοινώνει κάθε διόρθωση ΔΠΧ σε κάθε Αποδέκτη στον οποίο διαβιβάστηκαν τα ΔΠΧ, εκτός αν αυτό αποδεικνύεται ανέφικτο, ή αν συνεπάγεται δυσανάλογη προσπάθεια, όσον αφορά στα έξοδα και στο κατά πόσο είναι τεχνικά εφικτό. Ο Υπεύθυνος Επεξεργασίας Δεδομένων ενημερώνει το Υποκείμενο των Δεδομένων σχετικά με τους εν λόγω Αποδέκτες, εφόσον αυτό ζητηθεί από το Υποκείμενο των Δεδομένων.

γ. Δικαίωμα διαγραφής (δικαίωμα στη λήθη)

Ο Υπεύθυνος Επεξεργασίας Δεδομένων θα διαγράφει ΔΠΧ χωρίς αδικαιολόγητη καθυστέρηση αν το ζητήσει το Υποκείμενο των Δεδομένων και εάν ισχύει ένας από τους ακόλουθους λόγους:

(i) Τα ΔΠΧ δεν είναι πλέον απαραίτητα σε σχέση με τους σκοπούς για τους οποίους συλλέχθηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία,

(ii) Το Υποκείμενο των Δεδομένων ανακαλεί τη συγκατάθεση επί της οποίας βασίζεται η επεξεργασία και δεν υπάρχει άλλη νομική βάση για την επεξεργασία,

(iii) Δεν υπάρχουν επιτακτικοί και νόμιμοι λόγοι για την επεξεργασία,

(iv) Τα ΔΠΧ υποβλήθηκαν σε επεξεργασία παράνομα,

(v) Τα ΔΠΧ πρέπει να διαγραφούν ώστε να τηρηθεί νομική υποχρέωση βάσει του ενωσιακού δικαίου ή του δικαίου κράτους μέλους, στην οποία υπόκειται ο Υπεύθυνος Επεξεργασίας Δεδομένων, και / ή

(vi) Τα ΔΠΧ έχουν συλλεχθεί σε σχέση με την προσφορά υπηρεσιών της κοινωνίας πληροφοριών απευθείας από ένα παιδί.

Όταν τα ΔΠΧ υπόκεινται σε επεξεργασία, συμπεριλαμβανομένης κατάρτισης προφίλ, για σκοπούς άμεσης εμπορικής προώθησης, το Υποκείμενο των Δεδομένων έχει το δικαίωμα να αντιταχθεί οποιαδήποτε στιγμή στην επεξεργασία των ΔΠΧ που το αφορούν.

Περιορισμός του δικαιώματος διαγραφής:

Το δικαίωμα διαγραφής του Υποκειμένου των Δεδομένων δεν θα εφαρμόζεται και δεν υποχρεούται το Πανεπιστήμιο να ικανοποιήσει το αίτημα, όταν η επεξεργασία είναι απαραίτητη:

- Για την άσκηση του δικαιώματος της ελευθερίας της έκφρασης ή
- Για συμμόρφωση με νομική υποχρέωση στην οποία υπόκειται ο Υπεύθυνος Επεξεργασίας Δεδομένων ή για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον,
- Για λόγους δημοσίου συμφέροντος στον τομέα της δημόσιας υγείας,
- Για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων.

δ. Δικαίωμα περιορισμού της επεξεργασίας

Το Υποκείμενο των Δεδομένων δικαιούται να εξασφαλίζει από τον Υπεύθυνο Επεξεργασίας Δεδομένων τον περιορισμό (αναστολή) της επεξεργασίας, όταν ισχύει ένα από τα ακόλουθα:

- η ακρίβεια των ΔΠΧ αμφισβητείται από το Υποκείμενο των Δεδομένων για χρονικό διάστημα που επιτρέπει στον Υπεύθυνο Επεξεργασίας Δεδομένων να επαληθεύσει την ακρίβεια των ΔΠΧ,
- η επεξεργασία είναι παράνομη και το Υποκείμενο των Δεδομένων αντιτάσσεται στη διαγραφή των ΔΠΧ και ζητεί, αντ' αυτής, τον περιορισμό της χρήσης τους,
- ο Υπεύθυνος Επεξεργασίας Δεδομένων δεν χρειάζεται πλέον τα ΔΠΧ για τους σκοπούς της επεξεργασίας, αλλά τα δεδομένα αυτά απαιτούνται από το υποκείμενο των δεδομένων για τη θεμελίωση, άσκηση ή την υποστήριξη νομικών αξιώσεων,
- το Υποκείμενο των Δεδομένων έχει αντιρρήσεις για την επεξεργασία εν αναμονή της επαλήθευσης του κατά πόσον οι νόμιμοι λόγοι του Υπεύθυνου Επεξεργασίας Δεδομένων υπερισχύουν έναντι των λόγων του Υποκειμένου των Δεδομένων.

Όταν η επεξεργασία έχει περιοριστεί, τα εν λόγω ΔΠΧ, εκτός της αποθήκευσης και της ανωνυμοποίησης, υφίστανται επεξεργασία μόνο με την συγκατάθεση του Υποκειμένου των Δεδομένων ή για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων ή για την προστασία των δικαιωμάτων άλλου φυσικού ή νομικού προσώπου ή για λόγους σημαντικού δημοσίου συμφέροντος της Ένωσης ή κράτους μέλους και για κανέναν άλλο λόγο κατά τη διάρκεια του περιορισμού.

Το Υποκείμενο των Δεδομένων το οποίο έχει εξασφαλίσει τον περιορισμό της επεξεργασίας ενημερώνεται από τον Υπεύθυνο Επεξεργασίας Δεδομένων πριν από την άρση του περιορισμού της επεξεργασίας.

ε. Δικαίωμα στη φορητότητα των δεδομένων

Το Υποκείμενο των Δεδομένων έχει το δικαίωμα να λαμβάνει τα ΔΠΧ που το αφορούν και τα οποία έχει παράσχει στον Υπεύθυνο Επεξεργασίας, σε δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα μορφότυπο, καθώς και το δικαίωμα να διαβιβάζει τα εν λόγω δεδομένα σε άλλον Υπεύθυνο Επεξεργασίας χωρίς αντίρρηση από τον Υπεύθυνο Επεξεργασίας στον οποίο παρασχέθηκαν τα δεδομένα προσωπικού χαρακτήρα.

Κατά την άσκηση του δικαιώματος στη φορητότητα δεδομένων, το Υποκείμενο των Δεδομένων έχει το δικαίωμα να ζητά την απευθείας διαβίβαση των ΔΠΧ από έναν Υπεύθυνο Επεξεργασίας σε άλλο, σε περίπτωση που αυτό είναι τεχνικά εφικτό.

Το δικαίωμα στη φορητότητα των δεδομένων ασκείται με την επιφύλαξη του δικαιώματος στη διαγραφή. Το εν λόγω δικαίωμα δεν ισχύει για την επεξεργασία που είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον Υπεύθυνο Επεξεργασίας.

Το δικαίωμα στη φορητότητα δεν επηρεάζει δυσμενώς τα δικαιώματα και τις ελευθερίες άλλων.

στ. Δικαίωμα εναντίωσης

Το Υποκείμενο των Δεδομένων δικαιούται να αντιτάσσεται, ανά πάσα στιγμή και για λόγους που σχετίζονται με την ιδιαίτερη κατάστασή του, στην επεξεργασία ΔΠΧ που το αφορούν.

Ο Υπεύθυνος Επεξεργασίας δεν υποβάλει πλέον τα ΔΠΧ σε επεξεργασία, εκτός αν ο Υπεύθυνος Επεξεργασίας μπορεί να καταδείξει ότι:

- Η Επεξεργασία γίνεται για λόγους δημοσίου συμφέροντος, ή
- Υφίστανται επιτακτικοί και νόμιμοι λόγοι για την επεξεργασία οι οποίο υπερισχύουν των συμφερόντων, των δικαιωμάτων και των ελευθεριών του Υποκειμένου των Δεδομένων ή για την θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων.

Εάν τα ΔΠΧ υποβάλλονται σε επεξεργασία για σκοπούς απευθείας εμπορικής προώθησης, το Υποκείμενο των Δεδομένων δικαιούται να αντιταχθεί ανά πάσα στιγμή στην επεξεργασία ΔΠΧ που το αφορούν για την εν λόγω εμπορική προώθηση, περιλαμβανομένης της κατάρτισης προφίλ, εάν σχετίζεται με αυτήν την απευθείας εμπορική προώθηση.

Όταν τα Υποκείμενα των Δεδομένων αντιτίθενται στην επεξεργασία ΔΠΧ για σκοπούς απευθείας εμπορικής προώθησης, τα ΔΠΧ δεν θα υποβάλλονται πλέον σε επεξεργασία για τους σκοπούς αυτούς.

Το Υποκείμενο των Δεδομένων έχει το δικαίωμα να μην υπόκειται σε απόφαση που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης διαδικασίας συμπεριλαμβανομένης της κατάρτισης προφίλ, η οποία παράγει έννομα αποτελέσματα που το αφορούν ή το επηρεάζει σημαντικά με παρόμοιο τρόπο.

Αυτό το δικαίωμα στην εναντίωση δεν εφαρμόζεται όταν η απόφαση:

- Είναι αναγκαία για τη σύναψη ή την εκτέλεση σύμβασης μεταξύ του Υποκειμένου των Δεδομένων και του Υπεύθυνου Επεξεργασίας,
- Επιτρέπεται από σχετικό νόμο που προβλέπει τα κατάλληλα μέτρα για την προστασία των δικαιωμάτων του Υποκειμένου των Δεδομένων ή,
- Βασίζεται στη ρητή συγκατάθεση του Υποκειμένου των Δεδομένων.

III. Περιγραφή της διαχείρισης των αιτημάτων του Υποκειμένου των Δεδομένων από το Πανεπιστήμιο

Διαχείριση των αιτημάτων του Υποκειμένου των Δεδομένων όταν το Πανεπιστήμιο ενεργεί ως Υπεύθυνος Επεξεργασίας

Παραλαβή του αιτήματος του Υποκειμένου των Δεδομένων από τον Υπεύθυνο Προστασίας Δεδομένων

Το αίτημα μπορεί:

- Να παραληφθεί με διάφορα μέσα (τηλεφωνικά, μέσω ηλεκτρονικού ταχυδρομείου, ταχυδρομικά κ.λ.π.). Παρόλα αυτά, όταν το αίτημα υποβάλλεται προφορικά, θα πρέπει εν συνεχεία το Υποκείμενο των Δεδομένων να συμπληρώσει το έντυπο, που υπάρχει στον σχετικό ιστότοπο του Πανεπιστημίου Κρήτης https://www.uoc.gr/prostasia-dedomenvn/ https://www.uoc.gr/gdpr-προστασία-δεδομένων-προσωπικού-χαρα/

- Να διαβιβαστεί από τον εκτελούντα την Επεξεργασία για λογαριασμό του Πανεπιστημίου για την εν λόγω επεξεργασία και να παραληφθεί από τον Υπεύθυνο Προστασίας Δεδομένων του Πανεπιστημίου.

Διαβίβαση του αιτήματος από τον Υπεύθυνο Προστασίας Δεδομένων στον προϊστάμενο της τμήματος του Πανεπιστημίου που αφορά το αίτημα

Το αργότερο εντός 3 ημερών, ο Υπεύθυνος Προστασίας Δεδομένων θα πρέπει να διαβιβάσει το αίτημα στον προϊστάμενο της Υπηρεσίας του Πανεπιστημίου, οι εργαζόμενοι του οποίου προέβησαν στην επεξεργασία, που αποτελεί αντικείμενο του αιτήματος.

Ταυτοποίηση του Υποκειμένου των Δεδομένων από το τμήμα του Πανεπιστημίου που προέβη στην επεξεργασία

Η ταυτοποίηση του Υποκειμένου των Δεδομένων είναι απαραίτητη για την άσκηση των δικαιωμάτων του Υποκειμένου των Δεδομένων (ευθύνη της Υπηρεσίας που ενεργεί ως Υπεύθυνος Επεξεργασίας Δεδομένων). Η Υπηρεσία του Πανεπιστημίου, που προέβη στην επεξεργασία των δεδομένων, μπορεί να δεχτεί ως απόδειξη της ταυτότητας τα ακόλουθα έγγραφα:

- Διαβατήριο σε ισχύ,
- Δίπλωμα οδήγησης με φωτογραφία σε ισχύ,
- Αστυνομική ταυτότητα και/ή άλλα έγκυρα έγγραφα ταυτοποίησης όπως άδεια διαμονής.

Αν το αίτημα υποβληθεί για λογαριασμό του Υποκειμένου των Δεδομένων, η Υπηρεσία του Πανεπιστημίου που προέβη στην επεξεργασία των δεδομένων θα πρέπει να βεβαιωθεί ότι ο αιτών έχει επαρκή εξουσιοδότηση από το Υποκείμενο των Δεδομένων.

Αν η πιο πάνω Υπηρεσία έχει εύλογες αμφιβολίες σχετικά με την ταυτότητα του Υποκειμένου των Δεδομένων, μπορεί να ζητήσει την παροχή πρόσθετων πληροφοριών για την επιβεβαίωση της ταυτότητάς του.

Αρχείο καταγραφής των αιτημάτων (Παράρτημα ΙΙΙ)

Τήρηση αρχείου των αιτημάτων, ώστε να παρακολουθείται η εξέλιξη της υπόθεσης.
Ο Υπεύθυνος Επεξεργασίας φέρει το βάρος απόδειξης αυτής της παρακολούθησης της εξέλιξης, ώστε να μπορεί να αποδείξει τη συμμόρφωση με τον Κανονισμό.

Ειδοποίηση του Υποκειμένου των Δεδομένων από τον Υπεύθυνο Προστασίας Δεδομένων

Ο Υπεύθυνος Προστασίας Δεδομένων θα ειδοποιεί το Υποκείμενο των Δεδομένων για την παραλαβή του αιτήματος.

Είναι το αίτημα βάσιμο/υπερβολικό/αβάσιμο;

Βάσιμο: για παράδειγμα, αν η διεύθυνση του Υποκειμένου των Δεδομένων είναι εσφαλμένη και το Υποκείμενο των Δεδομένων αιτείται την τροποποίηση της διεύθυνσης, το αίτημα θεωρείται βάσιμο.

Αβάσιμο: για παράδειγμα, η διαγραφή δεν μπορεί να πραγματοποιηθεί επειδή τα Δεδομένα Προσωπικού Χαρακτήρα είναι ακόμα απαραίτητα για την εκτέλεση υφιστάμενης σύμβασης μεταξύ του Υποκειμένου των Δεδομένων και του Πανεπιστημίου.

Αν το Πανεπιστήμιο έχει οποιαδήποτε αμφιβολία σχετικά με το εάν το αίτημα είναι βάσιμο ή όχι, τότε θα πρέπει να συμβουλευτεί τον Υπεύθυνο Προστασίας Δεδομένων.

Υπερβολικό: Εάν το αίτημα είναι υπερβολικό και έχει επαναλαμβανόμενο χαρακτήρα, ο Υπεύθυνος Επεξεργασίας Δεδομένων δύναται να χρεώσει το Υποκείμενο των Δεδομένων για την ικανοποίηση του αιτήματός του ή να αρνηθεί αιτιολογημένα το αίτημα ως προφανώς καταχρηστικό.

Εάν το αίτημα δεν μπορεί να ικανοποιηθεί, επειδή θεωρείται αβάσιμο ή υπερβολικό, ο Υπεύθυνος Επεξεργασίας Δεδομένων οφείλει να τεκμηριώσει αυτήν την απόφαση. Ο Υπεύθυνος Επεξεργασίας Δεδομένων μπορεί να ζητήσει την υποστήριξη του Υπεύθυνου Προστασίας Δεδομένων για την τεκμηρίωση.

Πριν την ικανοποίηση του αιτήματος του Υποκειμένου των Δεδομένων, ο Υπεύθυνος Επεξεργασίας Δεδομένων οφείλει να ελέγξει αν το αίτημα εμπίπτει στις εξαιρέσεις, που προβλέπονται στον Κανονισμό, για την ενάσκηση δικαιώματος.

Ειδοποίηση του Υποκειμένου των Δεδομένων από τον Υπεύθυνο Προστασίας Δεδομένων

Ο Υπεύθυνος Προστασίας Δεδομένων ενημερώνει το Υποκείμενο των Δεδομένων σχετικά με το θέμα του αιτήματός του εντός μηνός από τη λήψη του. Το χρονικό διάστημα του ενός μήνα μπορεί να παραταθεί για δύο ακόμα μήνες στην περίπτωση περίπλοκου αιτήματος.

Επικαιροποίηση και κλείσιμο φακέλου από τον Υπεύθυνο Επεξεργασίας

Σύμφωνα με την αρχή της λογοδοσίας, όλα τα αιτήματα θα τεκμηριώνονται και θα καταγράφονται σε ένα ειδικό μητρώο, που θα τηρεί το Πανεπιστήμιο. Ο Υπεύθυνος Προστασίας Δεδομένων είναι υπεύθυνος για να εξασφαλίσει ότι το αρχείο των αιτημάτων τηρείται σωστά από το Πανεπιστήμιο.

Διαχείριση των αιτημάτων του Υποκειμένου των Δεδομένων όταν το Πανεπιστήμιο ενεργεί ως Εκτελών την Επεξεργασία

Παραλαβή του αιτήματος από το Υποκείμενο των Δεδομένων

Το αίτημα του Υποκειμένου των Δεδομένων παραλαμβάνεται πάντα από τον Υπεύθυνο Επεξεργασίας. Αυτό σημαίνει ότι τα στοιχεία επικοινωνίας που δίνονται στο Υποκείμενο των Δεδομένων θα είναι αυτά του Υπεύθυνου Επεξεργασίας.

Ειδοποίηση του Υποκειμένου των Δεδομένων για την παραλαβή του αιτήματος

Μόλις ο Υπεύθυνος Επεξεργασίας παραλαμβάνει το αίτημα, ειδοποιεί το Υποκείμενο των Δεδομένων για την παραλαβή. Από την ειδοποίηση αυτή, ο Υπεύθυνος Επεξεργασίας έχει ένα μήνα να επεξεργαστεί το αίτημα του Υποκειμένου των Δεδομένων.

Επαλήθευση της ταυτότητας και της νομικής βάσης του αιτήματος από τον Υπεύθυνο Επεξεργασίας

Ο Υπεύθυνος Επεξεργασίας οφείλει να επαληθεύσει την ταυτότητα του Υποκειμένου των Δεδομένων και τη νομική βάση του αιτήματος.

Διαβίβαση το Πανεπιστήμιο, που ενεργεί ως Εκτελών την Επεξεργασία, για την επεξεργασία του αιτήματος.

Μόλις ο Υπεύθυνος Επεξεργασίας επαληθεύσει το αίτημα, αυτό θα διαβιβάζεται στο Πανεπιστήμιο, ο οποίος ενεργεί ως Εκτελών την Επεξεργασία. Ο Υπεύθυνος Επεξεργασίας θα αναλαμβάνει να διαβιβάζει **εγκαίρως** το αίτημα και όλα τα απαραίτητα έγγραφα (ειδικές οδηγίες αν χρειάζονται) στον Υπεύθυνο Προστασίας Δεδομένων του Πανεπιστημίου, για την ικανοποίηση του αιτήματος από το Πανεπιστήμιο.

Καταγραφή του αιτήματος

Καταγραφή του αιτήματος από το Πανεπιστήμιο ώστε να μπορεί να παρακολουθηθεί η εξέλιξη της υπόθεσης. Το Πανεπιστήμιο, ως Εκτελών την Επεξεργασία, θα τηρεί αποδείξεις αυτής της παρακολούθησης, ώστε να μπορεί να αποδείξει τη συμμόρφωσή του με τον Κανονισμό και ότι έχει ακολουθήσει τις οδηγίες του Υπεύθυνου Επεξεργασίας.

Ειδοποίηση για την ικανοποίηση στον Υπεύθυνο Επεξεργασίας

Μόλις ικανοποιηθεί το αίτημα, το Πανεπιστήμιο ενημερώνει τον Υπεύθυνο Επεξεργασίας για την ικανοποίηση.

Ενημέρωση και κλείσιμο φακέλου

Μόλις ενημερωθεί ο Υπεύθυνος Επεξεργασίας για την ικανοποίηση του αιτήματος, η υπόθεση θεωρείται από το Πανεπιστήμιο ως περατωθείσα.

- **Ειδοποίηση του Υποκειμένου των Δεδομένων**

Ο Υπεύθυνος Επεξεργασίας πληροφορεί το Υποκείμενο των Δεδομένων για το αίτημά του εντός μηνός από τη λήψη του αιτήματος. Ο Υπεύθυνος Επεξεργασίας ευθύνεται για την τήρηση αυτής της προθεσμίας.

IV. Το δικαίωμα του Υποκειμένου των Δεδομένων σε αποζημίωση

Σύμφωνα με το άρθρο 82 του Κανονισμού, στην περίπτωση υλικής ή μη υλικής ζημίας ως αποτέλεσμα παραβίασης, το Υποκείμενο των Δεδομένων δικαιούται αποζημίωση από τον Υπεύθυνο Επεξεργασίας για τη ζημία που υπέστη.

IV Ε. Πολιτική για την αντιμετώπιση Παραβίασης ΔΠΧ

Η διαχείριση μίας παραβίασης Δεδομένων Προσωπικού Χαρακτήρα (ΔΠΧ) αποτελεί μία από τις κύριες προτεραιότητες για να διασφαλιστεί η πλήρης συμμόρφωση με τους νόμους και κανονισμούς σχετικά με την προστασία ΔΠΧ. Για το σκοπό αυτό, το Πανεπιστήμιο έχει υιοθετήσει την παρούσα πολιτική, στοχεύοντας να διασφαλίσει ότι παραβιάσεις ΔΠΧ, εάν υπάρξουν, θα τύχουν σωστής διαχείρισης εντός του Πανεπιστημίου, με τους όρους και στο χρονοδιάγραμμα που απαιτείται από τον Γενικό Κανονισμό για την Προστασία Δεδομένων.

I. Σκοπός

Η παρούσα Πολιτική εφαρμόζεται όποτε προκύπτει ένα συμβάν, το οποίο πληροί όλες τις προϋποθέσεις ώστε στη συνέχεια να θεωρηθεί ως Παραβίαση ΔΠΧ. Ειδικότερα, η παρούσα πολιτική:

- Περιγράφει τα διάφορα βήματα που πρέπει να ακολουθηθούν για να διαχειριστούν οι παραβιάσεις ΔΠΧ, να αναφερθούν εντός του Πανεπιστημίου και εκτός, αν αυτό απαιτείται,
- Παρέχει συστάσεις για γνωστοποιήσεις, όταν απαιτείται, στην Αρχή Προστασίας Δεδομένων, στα Υποκείμενα των Δεδομένων και στους Υπεύθυνους Επεξεργασίας (όταν το Πανεπιστήμιο είναι Εκτελών την Επεξεργασία).
- Παρέχει υποδείγματα γνωστοποίησης Παραβίασης Δεδομένων Προσωπικού Χαρακτήρα στην Αρχή Προστασίας Δεδομένων και στο Υποκείμενο Δεδομένων που επηρεάζεται.

II. Πότε ένα συμβάν θεωρείται παραβίαση Δεδομένων Προσωπικού Χαρακτήρα

Ως παραβίαση ΔΠΧ θεωρείται κάθε παραβίαση της ασφάλειας που οδηγεί στην τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, άνευ αδείας κοινολόγηση ή πρόσβαση σε ΔΠΧ που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία[3].

Οι παραβιάσεις μπορούν να χωριστούν στις ακόλουθες κατηγορίες:

- Παραβίαση εμπιστευτικότητας: όταν υπάρχει άνευ αδείας ή τυχαία κοινολόγηση ή πρόσβαση σε ΔΠΧ,
- Παραβίαση διαθεσιμότητας: όταν υπάρχει τυχαία ή άνευ αδείας απώλεια της πρόσβασης σε ή καταστροφή ΔΠΧ,
- Παραβίαση ακεραιότητας: όταν υπάρχει άνευ αδείας ή τυχαία μεταβολή ΔΠΧ.

Ανάλογα με τις περιστάσεις, μία παραβίαση μπορεί επίσης να αποτελείται από συνδυασμό αυτών των κατηγοριών.

III. Διαχείριση παραβίασης ΔΠΧ

Ανίχνευση μίας παραβίασης ΔΠΧ

Η ανίχνευση μίας παραβίασης ΔΠΧ μπορεί να γίνει είτε από το προσωπικό του Πανεπιστημίου είτε από τον Υπεύθυνο Προστασίας Δεδομένων του Πανεπιστημίου είτε από τον εκτελούντα την επεξεργασία είτε από το ίδιο το Υποκείμενο των Δεδομένων.

Επείγουσα ειδοποίηση και συγκρότηση ομάδας αντιμετώπισης του περιστατικού

Όταν έχει γίνει αντιληπτή η παραβίαση ΔΠΧ, θα πρέπει να ειδοποιηθεί επειγόντως για να λάβει τα κατάλληλα μέτρα για την έρευνα και αντιμετώπιση της παραβίασης ο Υπεύθυνος Προστασίας Δεδομένων.

Σε συνέχεια της επείγουσας ειδοποίησης, πρέπει να συγκροτηθεί μία ομάδα για την αντιμετώπιση του περιστατικού. Αυτή η ομάδα θα αποτελείται τουλάχιστον από:

- τον Υπεύθυνο Προστασίας Δεδομένων,
- τον Υπεύθυνο Ασφαλείας Πληροφοριών,
- το Νομικό Σύμβουλο του Πανεπιστημίου,
- τον επικεφαλής της Υπηρεσίας, όπου έλαβε χώρα η παραβίαση.

[3] Άρθρο 4 (12) του Γενικού Κανονισμού για την Προστασία Δεδομένων

Η ομάδα θα ηγείται της παρακολούθησης του περιστατικού και θα λαμβάνει κατάλληλα μέτρα για να αντιμετωπιστεί το συμβάν. Κατ' αρχάς θα πρέπει να διενεργηθούν έρευνες με σκοπό να εξακριβωθούν:

- οι αιτίες της Παραβίασης ΔΠΧ (διαρροή δεδομένων, κυβερνοεπίθεση, αμέλεια υπαλλήλου κ.λπ.),
- τα άτομα που μπορεί να προκάλεσαν την παραβίαση (υπάλληλος, συνεργάτης, προμηθευτής κ.λπ.),
- τις πιθανές συνέπειες και τους κινδύνους για τα δικαιώματα και τις ελευθερίες του Υποκειμένου των Δεδομένων, προκειμένου να διαπιστωθεί αν απαιτείται γνωστοποίηση στην Αρχή Προστασίας Δεδομένων.

Στοιχεία που πρέπει να ληφθούν υπ' όψιν, όταν γίνεται εκτίμηση κινδύνου:

- ***Το είδος της παραβίασης***: το είδος της παραβίασης μπορεί να επηρεάζει το επίπεδο του κινδύνου στον οποίο εκτίθεται το Υποκείμενο των Δεδομένων. Για παράδειγμα, κοινολόγηση ΔΠΧ σε μη εξουσιοδοτημένους τρίτους δεν θα έχει τον ίδιο αντίκτυπο με την απώλεια πρόσβασης σε ΔΠΧ.
- ***Η φύση, ευαισθησία και ο όγκος των ΔΠΧ:*** ένας συνδυασμός ΔΠΧ είναι πιο ευαίσθητος από ένα μοναδικό ΔΠΧ. Επιπρόσθετα, ο κίνδυνος βλάβης για το Υποκείμενο των Δεδομένων μπορεί να είναι υψηλότερος, εάν η παραβίαση αφορά Ευαίσθητα Δεδομένα.
- ***Ευκολία ταυτοποίησης του Υποκειμένου των Δεδομένων:*** η εκτίμηση πρέπει να λαμβάνει υπ' όψιν πόσο εύκολο θα είναι για κάποιον που έχει πρόσβαση σε παραβιασμένα ΔΠΧ να ταυτοποιήσει το Υποκείμενο των Δεδομένων, ή να συνδέσει τα ΔΠΧ με άλλες πληροφορίες, ώστε να ταυτοποιήσει το Υποκείμενο των Δεδομένων.
- ***Βαρύτητα των συνεπειών στο Υποκείμενο των Δεδομένων:*** η βαρύτητα των συνεπειών καθορίζεται από δύο κριτήρια, την πιθανή ζημία του Υποκειμένου των Δεδομένων και την μονιμότητα των συνεπειών για αυτό. Για παράδειγμα, η βαρύτητα των συνεπειών δεν είναι η ίδια στην περίπτωση ηθικής βλάβης, ζημίας στη φήμη ή κλοπής ταυτότητας.
- ***Ειδικά χαρακτηριστικά του Υποκειμένου των Δεδομένων:*** το επίπεδο του αντίκτυπου στα Υποκείμενα των Δεδομένων εξαρτάται επίσης από την κατηγορία του Υποκειμένου των Δεδομένων. Οι συνέπειες μπορεί να είναι πιο σημαντικές αν τα παραβιασμένα ΔΠΧ ανήκουν σε ένα παιδί ή σε άλλο ευάλωτο Υποκείμενο Δεδομένων.
- ***Ο αριθμός των Υποκειμένων των Δεδομένων που επηρεάζονται:*** όσο μεγαλύτερος είναι ο αριθμός των Υποκειμένων των Δεδομένων που επηρεάζονται, τόσο μεγαλύτερος είναι ο αντίκτυπος που μπορεί να έχει μία παραβίαση.

Αριθμός Υποκειμένων των Δεδομένων που αφορά η παραβίαση και γνωστοποίηση

Εφόσον κριθεί απαραίτητο λόγω της βαρύτητας της παραβίασης, *ο* ***Υπεύθυνος Προστασίας Δεδομένων οφείλει να ενημερώσει το νόμιμο εκπρόσωπο του Πανεπιστημίου.*** Αυτή η γνωστοποίηση πρέπει να γίνει εντός 48 ωρών από την ανακάλυψη της παραβίασης.

Θέσπιση μέτρων περιορισμού

Σε συνέχεια της εκτίμησης της παραβίασης, πρέπει να ληφθούν μέτρα περιορισμού για να αντιμετωπιστεί η παραβίαση ΔΠΧ.

Ανάλυση κινδύνων

Χαμηλός κίνδυνος – Τήρηση αρχείου και κλείσιμο

Εάν ο κίνδυνος είναι χαμηλός, η υπόθεση μπορεί να κλείσει, μόλις περιοριστεί η παραβίαση. Επιπρόσθετα, ο Υπεύθυνος Προστασίας Δεδομένων οφείλει να καταγράψει κάθε παραβίαση ΔΠΧ, ανεξάρτητα από το εάν η παραβίαση έχει γνωστοποιηθεί στην Αρχή Προστασίας Δεδομένων ή όχι, σε ένα εσωτερικό μητρώο παραβιάσεων, το οποίο τηρείται από τον ίδιο.

Υψηλός κίνδυνος - Γνωστοποίηση

Εάν ο κίνδυνος είναι ακόμα υψηλός για τα δικαιώματα και ελευθερίες του Υποκειμένου, ο Υπεύθυνος Προστασίας Δεδομένων του Πανεπιστημίου οφείλει να γνωστοποιήσει την παραβίαση των ΔΠΧ στην Αρχή Προστασίας Δεδομένων και, εάν είναι απαραίτητο, στα Υποκείμενα των Δεδομένων τα οποία αφορά.

Η γνωστοποίηση στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα πρέπει να γίνει όχι αργότερα από 72 ώρες από τη στιγμή που θα γίνει αντιληπτή η Παραβίαση των ΔΠΧ. Στο Παράρτημα IV της παρούσας αναφέρεται η σύνδεση link με την αναγκαία Φόρμα Γνωστοποίησης Περιστατικών Παραβίασης προς την Αρχή, που πρέπει να ακολουθηθεί

Όταν απαιτείται από το Πανεπιστήμιο να γνωστοποιήσει κάποια παραβίαση ΔΠΧ στην Αρχή Προστασίας Δεδομένων, το άρθρο 33 του Γενικού Κανονισμού για την Προστασία Δεδομένων αναφέρει ότι υπάρχει ελάχιστο περιεχόμενο πληροφοριών που πρέπει να γνωστοποιηθούν, ήτοι:

- **Περιγραφή της φύσης** της παραβίασης των ΔΠΧ, συμπεριλαμβανομένων, όπου είναι δυνατό, των κατηγοριών (για παράδειγμα παιδιά και άλλες ευαίσθητες ομάδες, υπάλληλοι, πελάτες κ.λπ.) και του **κατά προσέγγιση αριθμού** των επηρεαζόμενων

Υποκειμένων των Δεδομένων καθώς και των κατηγοριών και του κατά προσέγγιση αριθμού των επηρεαζόμενων αρχείων ΔΠΧ (για παράδειγμα δεδομένα υγείας, οικονομικά στοιχεία, αριθμός διαβατηρίου κ.λπ.),

- Το **όνομα και τα στοιχεία επικοινωνίας του Υπεύθυνου Προστασίας Δεδομένων του Πανεπιστημίου**,
- Περιγραφή των **ενδεχόμενων συνεπειών της παραβίασης των ΔΠΧ,**
- Περιγραφή των **μέτρων που έχουν ληφθεί ή προταθεί προς λήψη από το Πανεπιστήμιο** για την αντιμετώπιση της παραβίασης ΔΠΧ, καθώς και, όπου ενδείκνυται, μέτρα για τον περιορισμό ενδεχόμενων δυσμενών συνεπειών.

Επιπρόσθετα, σε κάποιες συγκεκριμένες περιπτώσεις σύνθετης παραβίασης, το Πανεπιστήμιο είναι δυνατόν να μην μπορεί να παρέχει όλες τις πληροφορίες σχετικά με την παραβίαση μέσα στο χρονοδιάγραμμα που απαιτείται από τον Γενικό Κανονισμό για την Προστασία Δεδομένων. Αυτό δεν θα πρέπει να σταθεί εμπόδιο στην έγκαιρη γνωστοποίηση της παραβίασης. Σε τέτοιες περιπτώσεις, θα πρέπει να ενημερώνει την Αρχή ότι θα παρέχει περαιτέρω λεπτομέρειες, όταν θα έχουν διενεργηθεί εις βάθος έρευνες.

Τήρηση αρχείου Παραβίασης ΔΠΧ

Σύμφωνα με την αρχή της ευθύνης, η παραβίαση θα καταγράφεται σε αρχείο παραβιάσεων, το οποίο θα τηρεί ο Υπεύθυνος Προστασίας Δεδομένων. Στο Παράρτημα V της παρούσας επισυνάπτεται σχέδιο Αρχείου Παραβιάσεων.

Έλεγχος

Μετά την παραβίαση, πρέπει να διεξαχθεί έλεγχος για να βεβαιωθεί ότι η παραβίαση περιορίστηκε σωστά και ότι έχουν ληφθεί συγκεκριμένα μέτρα ώστε να αποφευχθεί άλλη παραβίαση ΔΠΧ.

Καθυστερημένες γνωστοποιήσεις

Σε περίπτωση καθυστερημένης γνωστοποίησης στην Αρχή Προστασίας Δεδομένων, θα πρέπει αυτή να συνοδεύεται από τους λόγους της καθυστέρησης. Αυτή η περίπτωση μπορεί να συμβεί όταν ο Υπεύθυνος Επεξεργασίας έχει να διαχειριστεί πολλαπλές και παρόμοιες παραβιάσεις ασφαλείας σε ένα μικρό χρονικό διάστημα, οι οποίες επηρεάζουν μεγάλο αριθμό Υποκειμένων Δεδομένων.

Περιπτώσεις όπου δεν απαιτείται γνωστοποίηση

Δεν απαιτείται γνωστοποίηση στην Αρχή Προστασίας Δεδομένων **αν η παραβίαση είναι απίθανο να οδηγήσει σε κίνδυνο για τα δικαιώματα και τις ελευθερίες των Υποκειμένων των Δεδομένων.** Για παράδειγμα, αν μια παραβίαση εμπιστευτικότητας αφορά ΔΠΧ, τα οποία είναι ήδη διαθέσιμα δημόσια, θεωρείται ότι η παραβίαση δεν αποτελεί πιθανό κίνδυνο στο Υποκείμενο των Δεδομένων. Επιπρόσθετα, στην περίπτωση απώλειας ΔΠΧ, αν τα ΔΠΧ ήταν κρυπτογραφημένα με ασφάλεια και είχαν καταστεί βασικά ακατάληπτα σε μη εξουσιοδοτημένα άτομα, μπορούμε να θεωρήσουμε ότι ο αντίκτυπος στα Υποκείμενα των Δεδομένων θα είναι χαμηλός.

Γνωστοποίηση στα Υποκείμενα των Δεδομένων

Όταν ο ενδεχόμενος κίνδυνος για τα δικαιώματα και τις ελευθερίες των Υποκειμένων των Δεδομένων είναι υψηλός, το Πανεπιστήμιο, ενεργώντας ως Υπεύθυνος Επεξεργασίας, θα γνωστοποιεί την παραβίαση στα Υποκείμενα των Δεδομένων.

Η παραβίαση θα γνωστοποιείται ευθέως στα επηρεαζόμενα Υποκείμενα των Δεδομένων, εκτός αν αυτό θα συνεπαγόταν δυσανάλογη προσπάθεια. Σε αυτή την περίπτωση μπορεί να γίνει δημόσια ανακοίνωση. Συνίσταται η αποστολή προσωπικών μηνυμάτων στα Υποκείμενα των Δεδομένων (e-mail, sms κ.λπ.) και όχι η αποστολή μαζί με άλλες πληροφορίες (ενημερωτικό δελτίο κ.λπ.). Αυτές οι επικοινωνίες θα αποστέλλονται στα Υποκείμενα των Δεδομένων σε συνεργασία με την Αρχή Προστασίας Δεδομένων, η οποία μπορεί να παρέχει συμβουλές σχετικά με την πληροφόρηση των Υποκειμένων των Δεδομένων και σχετικά με το κατάλληλο μέσο γνωστοποίησης.

Το Πανεπιστήμιο οφείλει να ενημερώνει το Υποκείμενο των Δεδομένων για την Παραβίαση των ΔΠΧ, χωρίς υπαίτια καθυστέρηση. Εάν ο κίνδυνος για τις ελευθερίες και τα δικαιώματα του Υποκειμένου των Δεδομένων είναι ξεκάθαρα υψηλός, η γνωστοποίηση μπορεί να γίνει πριν τη γνωστοποίηση στην Αρχή Προστασίας Δεδομένων. Η ενημέρωση θα πρέπει να περιγράφει τη φύση της Παραβίασης των ΔΠΧ, καθώς και συστάσεις για τον περιορισμό ενδεχόμενων δυσμενών συνεπειών για το επηρεαζόμενο Υποκείμενο των Δεδομένων.

Περιπτώσεις όπου η γνωστοποίηση δεν απαιτείται

- Το Πανεπιστήμιο έχει εφαρμόσει τα κατάλληλα τεχνικά και οργανωτικά μέτρα για την προστασία ΔΠΧ πριν την παραβίαση, ώστε τα ΔΠΧ να μην είναι κατανοητά από όσους δεν έχουν άδεια πρόσβασης,
- Το Πανεπιστήμιο έχει λάβει μέτρα για να διασφαλίσει ότι οι υψηλοί κίνδυνοι για τα Υποκείμενα των Δεδομένων δεν είναι πλέον πιθανό να πραγματοποιηθούν.

- Η επικοινωνία με τα Υποκείμενα των Δεδομένων θα συνεπαγόταν δυσανάλογη προσπάθεια, αν τα στοιχεία επικοινωνίας τους έχουν χαθεί ως αποτέλεσμα της παραβίασης ή αν δεν ήταν γνωστά εξαρχής.

Γνωστοποίηση στον Υπεύθυνο Επεξεργασίας

- Όταν το Πανεπιστήμιο ενεργεί ως Εκτελών την Επεξεργασία, εάν μία παραβίαση ΔΠΧ υποπέσει στην αντίληψή της, απαιτείται να το γνωστοποιήσει στον Υπεύθυνο Επεξεργασίας αμελλητί.
- Το χρονοδιάγραμμα και οι όροι της επικοινωνίας προς τον Υπεύθυνο Επεξεργασίας θα καθορίζονται στη σύμβαση μεταξύ των μερών.

Ως Εκτελών την Επεξεργασία, το Πανεπιστήμιο δεν απαιτείται να εκτιμήσει πρώτα την πιθανότητα κινδύνου που απορρέει από μία παραβίαση, προτού ειδοποιήσει τον Υπεύθυνο Επεξεργασίας. Είναι ευθύνη του Υπεύθυνου Επεξεργασίας να καθορίσει εάν απαιτείται η γνωστοποίηση στην Αρχή Προστασίας Δεδομένων.

Γνωστοποίηση από τους Εκτελούντες την Επεξεργασία

Όταν το Πανεπιστήμιο εκτελεί μία συμφωνία με ένα τρίτο μέρος ως Εκτελών την Επεξεργασία, σύμφωνα με τον Γενικό Κανονισμό για την Προστασία Δεδομένων, ο Εκτελών την Επεξεργασία οφείλει να ενημερώσει για την Παραβίαση των ΔΠΧ αμελλητί, μόλις αντιληφθεί παραβίαση ΔΠΧ.

Παρόλα αυτά, προκειμένου να μπορέσει το Πανεπιστήμιο να γνωστοποιήσει την παραβίαση στην Αρχή Προστασίας Δεδομένων εντός 72 ωρών, το Πανεπιστήμιο απαιτεί από τους Εκτελούντες την Επεξεργασία να δεσμεύονται ότι θα γνωστοποιήσουν την παραβίαση στο Πανεπιστήμιο εντός 24 ωρών.

ΠΑΡΑΡΤΗΜΑ Ι

ΥΠΟΔΕΙΓΜΑ ΕΝΤΥΠΟΥ ΕΝΗΜΕΡΩΣΗΣ και ΣΥΓΚΑΤΑΘΕΣΗΣ για τη συλλογή και επεξεργασία ΔΠΧ από το Πανεπιστήμιο Κρήτης

Το Πανεπιστήμιο Κρήτης σας ενημερώνει ότι συλλέγει και επεξεργάζεται τα προσωπικά δεδομένα που δηλώσατε πιο πάνω (*απλά, ειδικών κατηγοριών, και τα δύο*) για την υλοποίηση ..... και μόνο (*ή με σκοπό να …..ή στο πλαίσιο των ακόλουθων σκοπών: .....*). Η συλλογή και η επεξεργασία των δεδομένων σας γίνεται με βάση ……..(*θα αναφερθεί το περιεχόμενο της διάταξης του Κανονισμού που αρμόζει π.χ. άρθρα 6 παρ. 1 περίπτωση (α) και για τα προσωπικά δεδομένα ειδικών κατηγοριών (ευαίσθητα) 9 παρ. 2 (α) του Γενικού Κανονισμού 2016/679*). Μπορείτε να αρνηθείτε τη συγκατάθεση ή να την ανακαλέσετε ανά πάσα στιγμή με τον ακόλουθο τρόπο: ……Τα προσωπικά σας δεδομένα θα παραμείνουν στη διάθεση του Πανεπιστημίου Κρήτης για χρονικό διάστημα _____ μηνών/ετών και ακολούθως θα διαγραφούν. Κατά το πιο πάνω χρονικό διάστημα αποδέκτες των προσωπικών σας δεδομένων θα είναι ……(*αν υπάρχουν*). Επίσης, θα διαβιβασθούν στην …… (*χώρα ή διεθνή οργανισμό αν υπάρχει αυτή η πρόβλεψη*) . Για το χρονικό διάστημα που τα προσωπικά σας δεδομένα θα παραμένουν στη διάθεση του Πανεπιστημίου Κρήτης έχετε τη δυνατότητα να ασκήσετε το δικαίωμα πρόσβασης, διόρθωσης, επικαιροποίησης, περιορισμού της επεξεργασίας, αντίταξης και φορητότητας σύμφωνα με τους όρους του Γενικού Κανονισμού Προστασίας Δεδομένων Προσωπικού Χαρακτήρα 2016/679 (Ε.Ε.). Επίσης, έχετε δικαίωμα αναφοράς στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα στη διεύθυνση www.dpa.gr. Μπορείτε να επικοινωνήσετε με το Πανεπιστήμιο Κρήτης στη διεύθυνση _____ (*να τεθούν τα στοιχεία του υπεύθυνου ή της γραμματείας της Σχολής ή του Τμήματος*).

Το Πανεπιστήμιο Κρήτης έχει ορίσει Υπεύθυνο Προσωπικών Δεδομένων με τον οποίο μπορείτε να επικοινωνήσετε στη διεύθυνση ηλεκτρονικής αλληλογραφίας dpo@uoc.gr.

Έχω ενημερωθεί και συγκατατίθεμαι
στην πιο πάνω συλλογή και επεξεργασία των δεδομένων μου
Τόπος, ημερομηνία
Ονοματεπώνυμο
Υπογραφή

ΠΑΡΑΡΤΗΜΑ ΙΙ

ΥΠΟΔΕΙΓΜΑ ΕΝΤΥΠΟΥ ΕΝΗΜΕΡΩΣΗΣ για τη συλλογή και επεξεργασία ΔΠΧ

(σύμφωνα με τον Οδηγό Συμμόρφωσης του Πανεπιστημίου Κρήτης)

https://www.uoc.gr/files/items/7/7133/guidance_for_compliance_with_gdpr.pdf

Το Πανεπιστήμιο Κρήτης σας ενημερώνει ότι συλλέγει και επεξεργάζεται τα προσωπικά δεδομένα που δηλώσατε πιο πάνω (*απλά, ειδικών κατηγοριών, και τα δύο*) για την υλοποίηση ..... και μόνο (*ή με σκοπό να .....ή στο πλαίσιο των ακόλουθων σκοπών: .....*). Η συλλογή και η επεξεργασία των δεδομένων σας γίνεται με βάση .....(*θα αναφερθεί το περιεχόμενο της διάταξης του Κανονισμού που αρμόζει π.χ. άρθρα 6 παρ. 1 περίπτωση (γ) ή (ε) και για τα προσωπικά δεδομένα ειδικών κατηγοριών (ευαίσθητα) 9 παρ. 2 (ζ) του Γενικού Κανονισμού 2016/679*). Τα προσωπικά σας δεδομένα θα παραμείνουν στη διάθεση του Πανεπιστημίου Κρήτης για χρονικό διάστημα _____ μηνών και ακολούθως θα διαγραφούν. Κατά το πιο πάνω χρονικό διάστημα αποδέκτες των προσωπικών σας δεδομένων θα είναι .....(*αν υπάρχουν*). Επίσης, θα διαβιβασθούν στην ..... (*χώρα ή διεθνή οργανισμό αν υπάρχει αυτή η πρόβλεψη*) . Για το χρονικό διάστημα που τα προσωπικά σας δεδομένα θα παραμένουν στη διάθεση του Πανεπιστημίου Κρήτης έχετε τη δυνατότητα να ασκήσετε το δικαίωμα πρόσβασης, διόρθωσης, επικαιροποίησης, περιορισμού της επεξεργασίας, αντίταξης και φορητότητας σύμφωνα με τους όρους του Γενικού Κανονισμού Προστασίας Δεδομένων Προσωπικού Χαρακτήρα 2016/679 (Ε.Ε.). Επίσης, έχετε δικαίωμα αναφοράς στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα στη διεύθυνση www.dpa.gr. Μπορείτε να επικοινωνήσετε με το Πανεπιστήμιο Κρήτης στη διεύθυνση _____ (*να τεθούν τα στοιχεία του υπεύθυνου ή της γραμματείας της Σχολής ή του Τμήματος*).

Το Πανεπιστήμιο Κρήτης έχει ορίσει Υπεύθυνο Προσωπικών Δεδομένων με τον οποίο μπορείτε να επικοινωνήσετε στη διεύθυνση ηλεκτρονικής αλληλογραφίας dpo@uoc.gr.

Έχω ενημερωθεί
για την πιο πάνω συλλογή και επεξεργασία των δεδομένων μου
Τόπος, ημερομηνία
Ονοματεπώνυμο
Υπογραφή

ΠΑΡΑΡΤΗΜΑ ΙΙΙ

ΥΠΟΔΕΙΓΜΑ – ΑΡΧΕΙΟ ΑΙΤΗΜΑΤΩΝ ΤΩΝ ΥΠΟΚΕΙΜΕΝΩΝ ΤΩΝ ΔΕΔΟΜΕΝΩΝ

Από Υποκείμενο δεδομένων:

……..

Ημερομηνία υποβολής αιτήματος: ……..

Αίτημα:

Πορεία αιτήματος:……

ΠΑΡΑΡΤΗΜΑ IV

ΥΠΟΔΕΙΓΜΑ – ΓΝΩΣΤΟΠΟΙΗΣΗΣ ΠΑΡΑΒΙΑΣΗΣ ΔΠΧ ΣΤΗΝ ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

Θα πρέπει να υποβάλλετε στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα σύμφωνα με τη Φόρμα που υπάρχει στην ιστοσελίδα

https://www.dpa.gr/el/syndesi/foreis/gnostopoiisi_peristatikou_paraviasis

ΠΑΡΑΡΤΗΜΑ V

ΥΠΟΔΕΙΓΜΑ – ΑΡΧΕΙΟ ΠΑΡΑΒΙΑΣΕΩΝ ΔΠΧ