ΠΑΝΕΠΙΣΤΗΜΙΟ ΙΩΑΝΝΙΝΩΝ
ΓΡΑΦΕΙΟ ΥΠΕΥΘΥΝΟΥ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

Πολιτική Προστασίας Δεδομένων Προσωπικού Χαρακτήρα Πανεπιστημίου Ιωαννίνων

Έκδοση:	0.2
Ημερομηνία:	**Μάιος 2019(επικαιροποιηση Απρίλιος 2021)**
Σύνταξη:	• **Υπεύθυνη Προστασίας Δεδομένων-Σταυρούλα Σταθαρα** • **Ζητήματα ΑσφαλείαςΔικτύων-Κωνσταντίνος Πλατής, Ιωάννα Κανλίδου, Χρήστος Ντόκος**

Περιεχόμενα

1 Εισαγωγή

1.1 Γενικά

Η εποχή που διανύουμε, με την ευρύτατη και πολυσχιδή χρήση του διαδικτύου, την ανάπτυξη της ψηφιακής οικονομίας, τη χρήση μέσων κοινωνικής δικτύωσης με την ταυτόχρονη διάθεση των δεδομένων σε διεθνές επίπεδο, κατέστησε την ανάγκη προστασίας των δεδομένων προσωπικού χαρακτήρα ως επιτακτική ανάγκη.

Απόρροια αυτής της ανάγκης ήταν η θέσπιση ενός Ευρωπαϊκού νομικού πλαισίου προστασίας των δεδομένων, η οποία οδήγησε στην κατάργηση της Οδηγίας95/46/ΕΚ καιτην θέσπιση του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (Γενικός Κανονισμός για την Προστασία Δεδομένων -ΓΚΠΔ). Ο Κανονισμός τέθηκε σε ισχύ την 25η Μαΐου 2018.

Η προστασία των δεδομένων προσωπικού χαρακτήρα, προϋποθέτει συλλογική προσπάθεια και συνεργασία όλων των μελών της πανεπιστημιακής κοινότητας των φοιτητών, του πάσης φύσεως προσωπικού του Πανεπιστημίου, καθώς και τωντρίτων πουσυναλλάσσονταιμε τις οργανωτικές δομές του Ιδρύματος.

Στην προσπάθεια της διαδικασίας συμμόρφωσης με τα οριζόμενα στον ΓΚΠΔ, συνδράμειο Υπεύθυνος Προστασίας Δεδομένων, σύμφωνα με τον Κανονισμό (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, ο οποίος παρακολουθεί και εποπτεύει τη συμμόρφωση. Ο Κανονισμός εν τέλει βρίσκεται στην κατεύθυνση της προάσπισης του ατόμου και της προσωπικής του αξιοπρέπειας και για αυτό τον σκοπό απαιτείται συλλογική προσπάθεια όλων όσων με οποιαδήποτε σχέση υπηρετούμε ή συναλλασσόμαστε με το Πανεπιστήμιο Ιωαννίνων, το οποίομε την υπερπεντακονταετή λειτουργία του, διαθέτει διεθνές κύρος, συγκαταλέγεται δε στα διεθνώςκαταξιωμέναιδρύματακυρίωςλόγω των ερευνητικών του δραστηριοτήτων.

Η προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα είναι θεμελιώδεςΣυνταγματικά κατοχυρωμένο δικαίωμα που περιγράφεται στο άρθρο 9 του Συντάγματος. Το δικαίωμα,πρέπει να εκτιμάται σε σχέση με τη λειτουργία του στην κοινωνία και να σταθμίζεται με άλλα θεμελιώδη δικαιώματα.

Ο Κανονισμός είναι πράξη γενικής ισχύος, δεσμευτικής ως προς όλα τα μέρη της και ισχύει άμεσα. Τα κράτη μέλη, τα θεσμικά όργανα της Ε.Ε. και οι ιδιώτες πρέπει να συμμορφώνονται πλήρως με αυτόν. Ο Κανονισμός είναι εφαρμοστέος αμέσως μετά την έναρξη ισχύος του και δεν είναι απαραίτητη η μεταφορά του στο εθνικό δίκαιο(αιτιολογική σκέψη αρ. 10) Σκοπός του είναι η διασφάλιση της ενιαίας εφαρμογής του δικαίου της Ένωσης σε όλα τα κράτη μέλη. Υπερισχύει των εθνικών νόμων καιειδικότερα οι διατάξεις του ισχύουνέναντι τουΝ.2472/1997 «Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα» (Α' 84), ο οποίος ενσωμάτωσε στο εθνικό μας δίκαιο την υπό (α) Οδηγία, για ότι δεν προβλέπεται στον προαναφερόμενο νόμο.

Επίκειται η ψήφιση εθνικού νόμουγια την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την

ελεύθερη κυκλοφορία των δεδομένων αυτών, σύμφωνα δε, μετην αιτιολογική σκέψη (10) του Κανονισμού, η επεξεργασία δεδομένων προσωπικού χαρακτήρα που γίνεται προς συμμόρφωση με νομική υποχρέωση, προς εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας, τα κράτη μέλη θα πρέπει να έχουν τη δυνατότητα να διατηρούν ή να θεσπίζουν εθνικές διατάξεις για τον περαιτέρω προσδιορισμό της εφαρμογής των κανόνων του παρόντος κανονισμού. Τέλος η αιτιολογική -10- σκέψη αναφέρει ότι : «ο Κανονισμός παρέχει επίσης περιθώρια χειρισμού στα κράτη μέλη, ώστε να εξειδικεύσουν τους κανόνες του, συμπεριλαμβανομένων αυτών που αφορούν την επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα («ευαίσθητα δεδομένα»). Σε αυτόν τον βαθμό, ο παρών κανονισμός δεν αποκλείει το δίκαιο των κρατών μελών να προσδιορίζει τις περιστάσεις ειδικών καταστάσεων επεξεργασίας, μεταξύ άλλων τον ακριβέστερο καθορισμό των προϋποθέσεων υπό τις οποίες η επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι σύννομη».

1.2 Συνοπτική Περιγραφή του ΓΚΠΔ

1.2.1 ΕΝΝΟΙΑ –ΔΙΑΧΩΡΙΣΜΟΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Ως δεδομένα προσωπικού χαρακτήρα-«απλά», σύμφωνα με το άρθρο 4 του Γενικού Κανονισμού νοείται 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,αριθμό ταυτότητας, 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.

Τα προσωπικά δεδομένα διακρίνονται σε «απλά» και «ειδικών κατηγοριών».

Ο Κανονισμός παρέχει στα δεδομένα «Ειδικών κατηγοριών» του άρθρου 9 διευρυμένη προστασία, απαγορεύοντας καταρχήν στην παράγραφο 1την «Επεξεργασία τους», την οποία στη συνέχεια με την παράγραφο 2, επιτρέπει υπό ρητά αναφερόμενους όρους, ορίζοντας επί λέξει «Η παράγραφος 1 δεν εφαρμόζεται στις ακόλουθες περιπτώσεις» (βλέπε αρξ 9) του συνημμένου Κανονισμού. Επίσης, ορίζει αυστηρότερες προϋποθέσεις για την πρόσβαση σε αυτού του είδους τα δεδομένα και την τήρηση αρχείων που να τα εμπεριέχουν.

Τα δεδομένα προσωπικού χαρακτήρα μπορούν, στο πλαίσιο διαμόρφωσης αποθετηρίων και τήρησης των σχετικών αρχείων, είτε να συνίστανται σε στοιχεία αναγνώρισης είτε να αναφέρονται σε ενδιαφέροντα – συνήθειες, δεδομένα ακαδημαϊκής δραστηριότητας, δεδομένα θέσης, τα οποία να συνδέονται με συγκεκριμένο πρόσωπο.

Δεδομένα «ειδικών κατηγοριών» είναι τα δεδομένα που αφορούν στη φυλετική ή εθνική προέλευση, στα πολιτικά φρονήματα, στις θρησκευτικές ή φιλοσοφικές

πεποιθήσεις, στη συμμετοχή σε συνδικαλιστική οργάνωση, στην επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων, με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένων που αφορούν στην υγεία, ή δεομένων που αφορούν στη σεξουαλική ζωή φυσικού προσώπου, ή τον γενετήσιο προσανατολισμό

Παράδειγμα: Το ονοματεπώνυμο, η διεύθυνση ηλεκτρονικού ταχυδρομείου (email), η διεύθυνση πρωτοκόλλου διαδικτύου (IPaddress), τα στοιχεία θέασης, διαβάσματος αρχείων, τα στοιχεία που αφορούν λήψεις ή παραγγελίες αρχείων ενός ηλεκτρονικού αποθετηρίου αποτελούν προσωπικά δεδομένα.

1.2.2 ΚΑΤΑΛΟΓΟΣ ΟΡΩΝ ΚΑΝΟΝΙΣΜΟΥ (σύμφωνα με το άρθρο 4 ΓΚΠΔ)

- **«Επεξεργασία»** είναι 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.
- **«περιορισμός της επεξεργασίας»** είναι η επισήμανση αποθηκευμένων δεδομένων προσωπικού χαρακτήρα με στόχο τον περιορισμό της επεξεργασίας τους στο μέλλον.
- **«κατάρτιση προφίλ»** είναι η 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.
- **«ψευδωνυμοποίηση»** είναι 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.
- **«σύστημα αρχειοθέτησης»** είναι 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.
- **«υπεύθυνος επεξεργασίας»** είναι 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.

- **«εκτελών την επεξεργασία»** είναι το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπεύθυνου της επεξεργασίας.
- **«αποδέκτης»** είναι 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.
- **«τρίτος»** είναι 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.
- **«συγκατάθεση»** του υποκειμένου των δεδομένων είναι 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.
- **«παραβίαση δεδομένων προσωπικού χαρακτήρα»** είναι 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.
- **«γενετικά δεδομένα»** είναι τα δεδομένα προσωπικού χαρακτήρα που αφορούν τα γενετικά χαρακτηριστικά φυσικού προσώπου που κληρονομήθηκαν ή αποκτήθηκαν, όπως προκύπτουν, ιδίως, από ανάλυση βιολογικού δείγματος του εν λόγω φυσικού προσώπου και τα οποία παρέχουν μοναδικές πληροφορίες σχετικά με την φυσιολογία ή την υγεία του εν λόγω φυσικού προσώπου.
- **«βιομετρικά δεδομένα»** είναι τα δεδομένα προσωπικού χαρακτήρα τα οποία προκύπτουν από ειδική τεχνική επεξεργασία συνδεόμενη με φυσικά, βιολογικά ή συμπεριφορικά χαρακτηριστικά φυσικού προσώπου και τα οποία επιτρέπουν ή επιβεβαιώνουν την αδιαμφισβήτητη ταυτοποίηση του εν λόγω φυσικού προσώπου, όπως εικόνες προσώπου ή δακτυλοσκοπικά δεδομένα.
- **«δεδομένα που αφορούν την υγεία»** είναι τα 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.

Ο Κανονισμός δεν εφαρμόζεται στη συλλογή και επεξεργασία δεδομένων θανόντων ή νομικών προσώπων.

1.2.3 ΣΥΝΟΠΤΙΚΗ ΠΑΡΑΘΕΣΗ ΤΩΝ ΒΑΣΙΚΩΝ ΑΡΘΡΩΝ ΤΟΥ ΓΚΠΔ

Κατωτέρω προχωρούμε στην παράθεση και ανάλυση βασικών άρθρων, εννοιών και υποχρεώσεων, που ορίζονται στον ΓενικόΚανονισμό.

ΑΡΘΡΟ 1: Ορίζει το αντικείμενο και τους στόχους του Κανονισμού. Θέτει τους βασικούς κανόνες εφαρμογής του και συγκεκριμένα:

Α. Προστατεύει τα φυσικά πρόσωπα έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

Β. Θέτει κανόνες που αφορούν την ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα.

Γ. Προστατεύει θεμελιώδη δικαιώματα και ελευθερίες των φυσικών προσώπων και ειδικότερα το δικαίωμά τους στην προστασία των δεδομένων προσωπικού χαρακτήρα.

Δ. Η ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα εντός της Ένωσης δεν περιορίζεται ούτε απαγορεύεται για λόγους που σχετίζονται με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

ΑΡΘΡΟ 2: Προσδιορίζει το ουσιαστικό πεδίο εφαρμογής του Κανονισμού, το οποίο είναι η, εν όλω ή εν μέρει, αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα και η μη αυτοματοποιημένη επεξεργασία των δεδομένων αυτών, τα οποία περιλαμβάνονται ή θα περιληφθούν σε αρχείο.

ΑΡΘΡΟ 3: Ορισμόςτουεδαφικού πεδίου εφαρμογής του Κανονισμού.

ΑΡΘΡΟ 4: Περιλαμβάνει όλους τους ορισμούς για την κατανόηση του κειμένου του Κανονισμού.

ΑΡΘΡΟ 5:Περιλαμβάνει τις θεμελιώδεις αρχές που πρέπει να διέπουν τη συλλογή και επεξεργασία των δεδομένων προσωπικού χαρακτήρα.

Ως Υπεύθυνος Επεξεργασίας και σε εφαρμογή της αρχής της λογοδοσίας, που θεσπίζει στο άρθρο αυτό ο Κανονισμός, το Πανεπιστήμιο Ιωαννίνων οφείλει να αποδεικνύει εγγράφως ότι τηρεί τις ακόλουθες αρχές:

5.1.Αρχή της νομιμότητας, της αντικειμενικότητας και της διαφάνειας.

Σύμφωνα με τον Κανονισμό, υπάρχουνέξι (6) νόμιμες βάσεις επεξεργασίας απλών προσωπικών δεδομένων και δέκα (10) νόμιμες βάσεις επεξεργασίας ειδικών κατηγοριών προσωπικών δεδομένων [ειδικότερα, βλέπετε, παράγραφο 8 του παρόντος κεφαλαίου]. Η επεξεργασία πρέπει να είναι και νόμιμη και θεμιτή. Η επεξεργασία απαιτεί ενημέρωση του υποκειμένου των δεδομένων, η οποία να είναι

πλήρης, συνοπτική, σαφής και κατανοητή, με απλή διατύπωση, διαρκής και εύκολα προσβάσιμη.

5.2.Αρχή του περιορισμού του σκοπού. Η επεξεργασία γίνεται για συγκεκριμένο σκοπό. Εξαιρείται η περαιτέρω επεξεργασία για αρχειοθέτηση προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας καιγια στατιστικούς σκοπούς (τεκμήριο συμβατότητας). Νόμιμη είναι η επεξεργασία για σκοπό συμβατό με τον αρχικό χωρίς να απαιτείται άλλη νομική βάση.

5.3.Αρχή της ελαχιστοποίησης των δεδομένων, που συλλέγονται.

5.4.Αρχή της ακρίβειας των δεδομένων που συλλέγονται. Αν τα δεδομένα δεν είναι ακριβή, πρέπει να επικαιροποιούνται.

5.5.Αρχή του περιορισμού (και εξ αρχής ορισμού) της περιόδου αποθήκευσης. Τα δεδομένα πρέπει να τηρούνται σε μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων τους μόνο για όσο χρονικό διάστημα αυτό είναι αναγκαίο για τον σκοπό της επεξεργασίας. Για μεγαλύτερο χρονικό διάστημα και εφόσον προβλέπεται από τον Κανονισμό ή το δίκαιο, θα πρέπει να επιλέγεται η ψευδωνυμοποίηση και η ανωνυμοποίηση.

Τα ανωνυμοποιημένα δεδομένα δεν θεωρούνται προσωπικά δεδομένα. Δεν θα πρέπει να φυλάσσονται έγγραφα (ιδιωτικά ή δημόσια) με προσωπικά δεδομένα χωρίς λόγο. Κάθε υπηρεσία θα πρέπει να λαμβάνει υπόψη της την κείμενη νομοθεσία, που ορίζει ανά κατηγορία εγγράφων, τον χρόνο τήρησης των δεδομένων. Επίσης, θα πρέπει να λαμβάνεται υπόψη η νομοθεσία σχετικά με την αρμοδιότητα των υπηρεσιών του Γενικού Αρχείου του Κράτους, πριν αποφασισθεί καταστροφή αρχείων.

5.6.Αρχή της ακεραιότητας και της εμπιστευτικότητας. Τα δεδομένα υπόκεινται σε επεξεργασία κατά τρόπο ασφαλή, που εγγυάται την προστασία τους από παράνομη επεξεργασία, απώλεια, διάδοση ή κοινοποίηση, και φθορά. Δεν έχουν πρόσβαση όλοι οι εργαζόμενοι σε όλα τα δεδομένα, αλλά μόνο σε αυτά που τους επιτρέπουν να ασκούν τα καθήκοντά τους. Όλοι οι εργαζόμενοι πρέπει να αυτοπεριορίζονται στον τομέα αυτό. Δεδομένα ειδικών κατηγοριών αποστέλλονται με αυξημένα μέτρα προστασίας (κρυπτογράφηση, ενδείξεις απορρήτου και εμπιστευτικότητας).

ΑΡΘΡΟ 6:Αναφέρει τις έξι (6)νομικές βάσεις (προϋποθέσεις), που καθιστούν την επεξεργασία απλών δεδομένων προσωπικού χαρακτήρα νόμιμη. Από αυτές οι υπό στοιχεία (γ) και (ε) είναι οι προσφορότερες (κατά περίπτωση) για το Πανεπιστήμιο.

Ειδικότερα – νομική βάση για τη σύννομη επεξεργασία δεδομένων συνιστούν:

(α) η συναίνεση,

(β) η ανάγκη εκτέλεσης σύμβασης,

(γ) η ανάγκη συμμόρφωσης σε έννομη υποχρέωση του Πανεπιστημίου,

(δ) η ανάγκη διαφύλαξης ζωτικού συμφέροντος φυσικού προσώπου,

(ε) η ανάγκη εκπλήρωσης καθήκοντος υπέρ του δημοσίου συμφέροντος ή κατά την άσκηση δημόσιας εξουσίας του Πανεπιστημίου και

(στ) η ανάγκη άσκησης των σκοπών των εννόμων συμφερόντων του υπευθύνου επεξεργασίας ή τρίτου.

Η διάταξη της παρ. 4 του ίδιου άρθρου θεσπίζει τις αρχές, που πρέπει να ακολουθηθούν, σε περίπτωση που το Πανεπιστήμιο θέλει να προβεί σε επεξεργασία των δεδομένων, που έχει συλλέξει για σκοπό άλλο από τον αρχικώς ορισθέντα (έννοια της συμβατότητας των σκοπών).

Επισημαίνεται ότι η συναίνεση ως νομική βάση επεξεργασίας δεδομένων, δεν έχει απόλυτη ισχύ στο Δημόσιο Τομέα διότι δεν συνάδει με τη φύση και την αποστολή του Πανεπιστημίουως εκπαιδευτικού Ιδρύματος και ως εκ τούτου συνιστάται η αποφυγή της χρήσης της..

Στα έντυπα ενημέρωσης δεν μπορούν να τεθούν πολλές ή εναλλακτικές νομικές βάσεις. Επιλέγεται μόνο μία, δηλαδή, αυτή που συμφωνεί με τη φύση των δεδομένων (απλά ή ειδικών κατηγοριών) και με τον σκοπό της συλλογής και επεξεργασίας.

Στα έντυπα ενημέρωσης το υποκείμενο των δεδομένων θέτει την υπογραφή του υπό την ένδειξη **«ενημερώθηκα»** ή **«έλαβα γνώση των ανωτέρω»** και όχι «συναινώ».

ΑΡΘΡΟ 7:Νομική βάση της «συγκατάθεσης». Αναφέρονται οι προϋποθέσεις, που πρέπει να πληρούνται, προκειμένου η συναίνεση να είναι έγκυρη ως νομική βάση.
7.2. Νομικές βάσεις σύννομης επεξεργασίας:

(α) η συναίνεση,

(β) η ανάγκη εκτέλεσης υποχρεώσεων και άσκησης δικαιωμάτων του Πανεπιστημίου στους τομείς του εργατικού δικαίου, του δικαίου κοινωνικής ασφάλισης και του δικαίου κοινωνικής προστασίας,

(γ) η ανάγκη διαφύλαξης ζωτικού συμφέροντος φυσικού προσώπου,

(δ) η επεξεργασία στο πλαίσιο δραστηριοτήτων ιδρύματος κλπ με στόχο πολιτικό, φιλοσοφικά κ.α. (υπό τους όρους της διάταξης),

(ε) η προηγούμενη δημοσιοποίηση των δεδομένων από το υποκείμενό τους,

(στ) η άσκηση νομικών αξιώσεων

(ζ) λόγοι ουσιαστικού δημοσίου συμφέροντος ανάλογου προς τον επιδιωκόμενο σκοπό (υπό τους όρους της διάταξης),

(η) η ανάγκη εξυπηρέτησης συγκεκριμένων ιατρικών σκοπών,

(θ) λόγοι δημοσίου συμφέροντος στον τομέας της δημόσιας υγείας (υπό τους όρους της διάταξης) και

(ι) σκοποί αρχειοθέτησης προς το δημόσιο συμφέρον, σκοποί επιστημονικής και ιστορικής έρευνας και σκοποί στατιστικοί (υπό τους όρους της διάταξης).

ΑΡΘΡΟ 9: Έννοια «ειδικών κατηγοριών δεδομένων και όροι που καθιστούν νόμιμη την επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα (παλιότερα αναφέρονταν ως ευαίσθητα προσωπικά δεδομένα). Από αυτές οι υπό στοιχεία (α), (β), (στ) (ζ) και (ι) είναι οι προσφορότερες (κατά περίπτωση).

Ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα:

- Φυλετική ή εθνοτική καταγωγή
- Πολιτικά φρονήματα
- Θρησκευτικές και φιλοσοφικές πεποιθήσεις
- Συμμετοχή σε συνδικαλιστική οργάνωση
- Γενετικά και βιομετρικά δεδομένα (αδιαμφισβήτητη ταυτοποίηση προσώπου)
- Υγεία
- Σεξουαλική ζωή / γενετήσιος προσανατολισμός
- Ειδικές προβλέψεις για τα ποινικά μητρώα.

ΑΡΘΡΑ 12 έως και 23: Περιγραφή των δικαιώματα των υποκειμένων των δεδομένων.

ΑΡΘΡΑ 24-31: Ανάλυση των υποχρεώσεις των υπευθύνων επεξεργασίας και των εκτελούντων την επεξεργασία. Με βάση τον ορισμό του «υπεύθυνου επεξεργασίας» και του «εκτελούντα την επεξεργασία», θα πρέπει να ανατρέχετε στα άρθρα αυτά, προκειμένου να γνωρίζετε – πριν την εκτέλεση της επεξεργασίας – αν το Πανεπιστήμιο δρα ως υπεύθυνος ή εκτελών την επεξεργασία (άρθρο 28) και, αντιστοίχως, τι υποχρεώσεις αναλαμβάνει σε σχέση με την έννομη σχέση που πρόκειται να εκτελέσει.

ΑΡΘΡΟ 24:Περιγράφει την αρχή της λογοδοσίας («ο υπεύθυνος επεξεργασίας εφαρμόζει τα κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τον παρόντα κανονισμό»).

ΑΡΘΡΟ 25: Περιγράφει τις υποχρεώσεις του υπευθύνου επεξεργασίας για τη λήψη μέτρων τόσο κατά τη στιγμή καθορισμού των μέσων επεξεργασίας όσο και κατά τη στιγμή της επεξεργασίας, όπως, ψευδωνυμοποίηση, ελαχιστοποίηση των δεδομένων, εγγυήσεις απορρήτου (προστασία από τον σχεδιασμό και εξ ορισμού).

ΑΡΘΡΟ 30:Υποχρέωση τήρησης αρχείου δραστηριοτήτων εκ μέρους τωντων υπευθύνων επεξεργασίας και των εκτελούντων την επεξεργασία να τηρούν έγγραφη και ηλεκτρονική τεκμηρίωση των πράξεων επεξεργασίας (αρχείο δραστηριοτήτων). Είναι το κύριο εργαλείο απόδειξης τήρησης της αρχής της λογοδοσίας και αντικαθιστά την παλιά διαδικασία κοινοποίησης/γνωστοποίησης επεξεργασίας δεδομένων στην ΑΠΔΠΧ.

ΑΡΘΡΑ 32-36:Ασφάλεια επεξεργασίας,γνωστοποίηση παραβίασης δεδομένων στην εποπτική αρχή και ανακοίνωση παραβίασης δεδομένων στο υποκείμενο των δεδομένων.

ΑΡΘΡΟ 35:Θεσπίζει την διενέργεια εκτίμησης επιπτώσεων (DPIA) εφόσον η επεξεργασία δεδομένων προσωπικού χαρακτήρα που πρόκειται να γίνει, ενδέχεται να ενέχει κινδύνους για τα δικαιώματα των υποκειμένων.

ΑΡΘΡΑ 37-38: Ορισμός Υπευθύνου Προστασίας Δεδομένων (DataProtectionOfficer - DPO) και θέση αυτού στον Οργανισμό. Για την περίπτωση του Πανεπιστημίου Ιωαννίνων ο ορισμός Υπευθύνου Προστασίας Δεδομένων είναι υποχρεωτικός. Η θέση του στην οργάνωση του Πανεπιστημίου και οι αρμοδιότητές του καθορίζονται ειδικώς στα άρθρα 38 και 39. Ειδικότερα, σύμφωνα με το άρθρο 39, προβλέπεται ότι ο Υπεύθυνος Προστασίας Δεδομένων:

«α) ενημερώνει και συμβουλεύει τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία και τους υπαλλήλους που επεξεργάζονται τις υποχρεώσεις τους που απορρέουν από τον παρόντα κανονισμό και από άλλες διατάξεις της Ένωσης ή του κράτους μέλους σχετικά με την προστασία δεδομένων,

β) παρακολουθεί τη συμμόρφωση με τον παρόντα κανονισμό, με άλλες διατάξεις της Ένωσης ή του κράτους μέλους σχετικά με την προστασία δεδομένων και με τις πολιτικές του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία σε σχέση με την προστασία των δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων της ανάθεσης αρμοδιοτήτων, της ευαισθητοποίησης και της κατάρτισης των υπαλλήλων που συμμετέχουν στις πράξεις επεξεργασίας, και των σχετικών ελέγχων,

γ) παρέχει συμβουλές, όταν ζητείται, όσον αφορά την εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων και παρακολουθεί την υλοποίησή της.

δ) συνεργάζεται με την εποπτική αρχή,

ε) ενεργεί ως σημείο επικοινωνίας για την εποπτική αρχή για ζητήματα που σχετίζονται με την επεξεργασία, περιλαμβανομένης της προηγούμενης διαβούλευσης που αναφέρεται στο άρθρο 36, και πραγματοποιεί διαβουλεύσεις, ανάλογα με την περίπτωση, για οποιοδήποτε άλλο θέμα».

ΑΡΘΡΑ 85-91:Ειδικές περιπτώσεις επεξεργασίας.

1.2.4 ΔΙΚΑΙΩΜΑΤΑ ΤΩΝ ΥΠΟΚΕΙΜΕΝΩΝ ΤΩΝ ΔΕΔΟΜΕΝΩΝ

Σημαντική επισήμανση:

Προ της ικανοποίησης αιτήματος κάθε «υποκειμένου δεδομένων», οφείλουμε να ταυτοποιούμε-επαληθεύουμε τα στοιχεία του αιτούντος.

Σε όλα τα αιτήματα «υποκειμένων των δεδομένων» καθώς και «τρίτων», υποχρεούμεθα να απαντήσουμε εγγράφως, στο πλαίσιο των προθεσμιών που ορίζονται από τον Κανονισμό, ήτοι:(άρθρο 12 παρ. 3 και 4: κατά περίπτωση, είτε άμεσα είτε μέσα σε ένα (1) μήνα με δικαίωμα παράτασης, οπότε και υποχρεούμαστε να ενημερώσουμε για τον λόγο για τον οποίο δεν προβήκαμε σε ενέργειεςμέσα σε ένα (1) μήνα.

1. Δικαίωμα ενημέρωσης (άρθρο 12):

1α. Ο Κανονισμός θεσπίζει μία διαφανή πολιτική ενημέρωσης των υποκειμένων δεδομένων, ώστε το κάθε υποκείμενο να μπορεί να ασκεί τα δικαιώματά του αποτελεσματικά.

1β. Κάθε πληροφορία και ανακοίνωση σχετικά με την επεξεργασία προσωπικών δεδομένων πρέπει να είναι εύκολα προσβάσιμη, κατανοητή, με σαφή και απλή γλώσσα, γλώσσα καθημερινή, ανάλογα με το μορφωτικό επίπεδο και την ηλικία του ατόμου. Να αποφεύγεται η υπερπληροφόρηση.

1γ. Οι πληροφορίες να δίνονται γραπτώς ή με ηλεκτρονική μορφή. Όταν οι πληροφορίες δίνονται προφορικώς, πρέπει να αποδεικνύεται εγγράφως η πληροφόρηση.

1δ. Η προθεσμία για παροχή ενημέρωσης είναι ένας μήνας και μπορεί να παραταθεί για δύο μήνες ανάλογα με την πολυπλοκότητα.

1στ. Κάθε αίτηση ενημέρωσης δεν συνεπάγεται και υποχρέωση για ενέργεια. Πρέπει, όμως, να ενημερωθεί το υποκείμενο δεδομένων για τους λόγους που δεν ενήργησε και τη δυνατότητα προσφυγής στην εποπτική αρχή και στα δικαστήρια.

2. Δικαίωμα πρόσβασης (άρθρα 13 -15):

2α. Το υποκείμενο δεδομένων έχει δικαίωμα να ελέγξει τον τρόπο επεξεργασίας των προσωπικών του δεδομένων (νομιμότητα) ώστε να ασκήσει τα υπόλοιπα δικαιώματά του (όπως, το δικαίωμα διόρθωσης, το δικαίωμα εναντίωσης κ.α.)

2β.Το δικαίωμα (και ο λόγος άσκησής του) δεν χρήζει αιτιολόγησης.

2γ. Πρώτα πρέπει να εξετασθεί αν υπάρχουν δεδομένα του υποκειμένου στον φορέα. Συνεπώς, στην αρχική απάντηση πρέπει να διατυπώνετε επιφύλαξη για την κατοχή τέτοιων δεδομένων.

2δ. Σε θετική περίπτωση το υποκείμενο δεδομένων έχει πρόσβαση στις ακόλουθες πληροφορίες (α) σκοπό επεξεργασίας, (β) κατηγορίες δεδομένων, (γ) αποδέκτες, (δ) χρονικό διάστημα διατήρησης, (ε) ύπαρξη δικαιώματος υποβολής αιτήματος για διορθωση, διαγραφή κλπ, (στ) δικαίωμα υποβολής καταγγελίας στην εποπτική αρχή, (ζ) προέλευσή τους.

3. Δικαίωμα διόρθωσης (άρθρο 16):

3α. Το υποκείμενο δεδομένων έχει δικαίωμα να απαιτήσει από τον υπεύθυνο επεξεργασίας τη διόρθωση ανακριβών του δεδομένων, την επικαιροποίηση των δεδομένων του και τη συμπλήρωση ελλιπών δεδομένων.

3β. Ελλιπή είναι τα δεδομένα που οδηγούν σε παραπλάνηση ή παρεξήγηση.

4. Δικαίωμα διαγραφής (λήθης) (άρθρο 17):

Το υποκείμενο δεδομένων έχει το δικαίωμα να ζητήσει από τον υπεύθυνο επεξεργασίας τη διαγραφή των δεδομένων του, όταν συντρέχουν συγκεκριμένοι λόγοι, ήτοι όταν:

(α) τα δεδομένα δεν είναι πλέον αναγκαία για τους σκοπούς της επεξεργασίας,

(β) το υποκείμενο δεδομένων έχει ανακαλέσει τη συναίνεσή του ως νομική βάση επεξεργασίας και δεν υπάρχει άλλη,

(γ) το υποκείμενο δεδομένων αντιτίθεται στην επεξεργασία και δεν υπάρχουν επιτακτικοί λόγοι για αυτή,

(δ) τα δεδομένα έτυχαν επεξεργασίας παράνομα,

(ε) τα δεδομένα πρέπει να διαγραφούν ώστε να τηρηθεί νομική υποχρέωση,

(στ) τα δεδομένα συλλέχθηκαν σε σχέση με την προσφορά υπηρεσιών της κοινωνίας της πληροφορίας

Επισήμανση: Κρίσιμη είναι η διάταξη της παρ. 3 του ίδιου άρθρου, καθώς τα παραπάνω δεν εφαρμόζονται στο βαθμό που επεξεργασία είναι απαραίτητη, μεταξύ άλλων, (α) για την τήρηση νομικής υποχρέωσης που επιβάλλει την επεξεργασία κατά το δίκαιο ή για την εκπλήρωση καθήκοντος υπέρ του δημοσίου συμφέροντος ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας, καθώς και (β) για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς και (γ) για θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων.

Τέλος πρέπει να επισημανθεί ότι στο Δημόσιο Τομέα, το δικαίωμα διαγραφής, δεν είναι απόλυτο ως εκ τούτου δύσκολα εφαρμόζεται.

5. Δικαίωμα περιορισμού της επεξεργασίας (άρθρο 18) όταν:

5α. Το υποκείμενο δεδομένων έχει δικαίωμα να εξασφαλίζει από τον υπεύθυνο επεξεργασίας τον περιορισμό της επεξεργασίας των δεδομένων του σε συγκεκριμένες περιπτώσεις. Ειδικότερα:

5β. Η ακρίβεια των δεδομένων αμφισβητείται από το υποκείμενο για χρονικό διάστημα που επιτρέπει στον υπεύθυνο επεξεργασίας να τα επαληθεύσει,

5γ. η επεξεργασία είναι παράνομη, το υποκείμενο αντιτάσσεται στη διαγραφή και ζητά περιορισμό,

5δ. ο υπεύθυνος επεξεργασίας δεν χρειάζεται πια τα δεδομένα, τα χρειάζεται όμως το υποκείμενο για άσκηση νομικών αξιώσεων,

5ε. το υποκείμενο δεδομένων έχει αντιρρήσεις για την επεξεργασία και εν αναμονή του ελέγχου βασιμότητας των αντιρρήσεών του.

5στ. Ενημέρωση του υποκειμένου των δεδομένων για την άρση του περιορισμού.

6. Δικαίωμα στη φορητότητα των δεδομένων (άρθρο 20) όταν:

6α. Το υποκείμενο δεδομένων έχει δικαίωμα να λάβει ή να ζητήσει τη μεταφορά των δεδομένων του, σε μηχαναγνώσιμη μορφή, από έναν υπεύθυνο επεξεργασίας σε άλλον, υπό συγκεκριμένες προϋποθέσεις.

6β. Αφορά σε δεδομένα που λήφθηκαν με βάση τη νομική βάση της συναίνεσης) ή όταν η επεξεργασία διενεργείται με αυτοματοποιημένα μέσα Άρα, κατά κανόνα, δεν εφαρμόζεται στο Πανεπιστήμιο Ιωαννίνων ενόψει και της παρ. 3 του ίδιου άρθρου.

6γ. Δεν αφορά σε έγχαρτα αρχεία δεδομένων.

6δ. Η μεταφορά γίνεται από υπεύθυνο επεξεργασίας προς υπεύθυνο επεξεργασίας.

6ε.Αφορά μόνο στα προσωπικά δεδομένα και όχι σε εργασία (στοιχεία αξιολόγησης) του φορέα, που συνοδεύει ή αφορά στα δεδομένα.

7. Δικαίωμα εναντίωσης στην επεξεργασία (άρθρο 21):

7α. Το υποκείμενο δεδομένων έχει δικαίωμα να αντιτάσσεται στην επεξεργασία των δεδομένων του, ανά πάσα στιγμή και για λόγους που αφορούν στην ιδιαίτερη κατάστασή του, συμπεριλαμβανομένης και της κατάρτισης «προφίλ».

7β. Ιδιαίτερη κατάσταση είναι οι ειδικές περιστάσεις της ζωής του κάθε ανθρώπου, νομικές, κοινωνικές, οικογενειακές καταστάσεις ανάγκης.

8. Δικαίωμα στην ανθρώπινη παρέμβαση (άρθρο 22):

8α. Το υποκείμενο δεδομένων έχει δικαίωμα να μην υπόκειται σε απόφαση που λαμβάνεται αποκλειστικά με αυτοματοποιημένη επεξεργασία, χωρίς, δηλαδή, να λαμβάνονται υπ' όψη τα προσωπικά χαρακτηριστικά του.

1.2.4.1 ΣΥΝΑΙΝΕΣΗ ΥΠΟΚΕΙΜΕΝΟΥ ΔΙΚΑΙΩΜΑΤΩΝ (άρθρα 4 και 7)

Επισημαίνεται ότι στον Δημόσιο Τομέα η «συγκατάθεση», πρέπει να αποφεύγεται διότι δεν συνάδει με τους σκοπούς του.Στην περίπτωση κατά την οποία απαιτείται «συγκατάθεση», προηγείται αυτής υποχρεωτικά η ενημέρωση του υποκειμένου των δεδομένων.

Στις εξαιρετικές περιπτώσεις, που η επεξεργασία των προσωπικών δεδομένων θα γίνεται επί τη βάσει της συναίνεσης, ισχύουν τα ακόλουθα:

1. Συναίνεση του υποκειμένου των δεδομένων: κάθε ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, ρητή και εν πλήρη 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.

2. Όταν η επεξεργασία βασίζεται σε συναίνεση, ο υπεύθυνος επεξεργασίας πρέπει να είναι σε θέση να αποδείξει ότι το υποκείμενο των δεδομένων συγκατατέθηκε στην επεξεργασία.

3. Εάν η συναίνεση του υποκειμένου των δεδομένων παρέχεται στο πλαίσιο γραπτής δήλωσης, που αφορά και άλλα θέματα, το αίτημα για συναίνεση υποβάλλεται κατά τρόπο διακριτό από τα άλλα θέματα, σε κατανοητή και εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή διατύπωση.

4. Το υποκείμενο των δεδομένων έχει δικαίωμα να ανακαλέσει τη συναίνεσή του ανά πάσα στιγμή. Η ανάκληση της συναίνεσης δεν θίγει τη νομιμότητα της επεξεργασίας που βασίστηκε σε αυτήν προ της ανάκλησής της. Πριν την παροχή της συναίνεσης, το υποκείμενο των δεδομένων ενημερώνεται σχετικά. Η ανάκληση της συναίνεσης είναι εξίσου εύκολη με την παροχή της.

5. Κατά την εκτίμηση κατά πόσο η συναίνεση δίνεται ελεύθερα, λαμβάνεται ιδιαιτέρως υπόψη κατά πόσο, μεταξύ άλλων, για την εκτέλεση σύμβασης, συμπεριλαμβανομένης της παροχής μιας υπηρεσίας, τίθεται ως προϋπόθεση η συναίνεση στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που δεν είναι αναγκαία για την εκτέλεση της εν λόγω σύμβασης.

1.2.4.2 ΕΝΗΜΕΡΩΣΗ ΥΠΟΚΕΙΜΕΝΩΝ ΔΙΚΑΙΩΜΑΤΩΝ (άρθρο 13)

Η συλλογή και η επεξεργασία δεδομένων προσωπικού χαρακτήρα προϋποθέτει την απαραίτητη προηγούμενη ενημέρωση του υποκειμένου τους και υπογραφή του

εντύπου ενημέρωσης, που θα περιλαμβάνει τα στοιχεία, που αναφέρονται κατωτέρω:

1. Την ταυτότητα και τα στοιχεία επικοινωνίας του υπευθύνου επεξεργασίας,
2. Τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων,
3. Τους σκοπούς της επεξεργασίας για τους οποίους προορίζονται τα δεδομένα προσωπικού χαρακτήρα, καθώς και τη νομική βάση για την επεξεργασία,
4. Στην περίπτωση που η επεξεργασία βασίζεται στο άρθρο 6 παράγραφος 1 στοιχείο στ), τα έννομα συμφέροντα που επιδιώκονται από τον υπεύθυνο επεξεργασίας ή από τρίτο, τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων προσωπικού χαρακτήρα, εάν υπάρχουν,
5. κατά περίπτωση, την πρόθεση του υπευθύνου επεξεργασίας να διαβιβάσει δεδομένα προσωπικού χαρακτήρα σε τρίτη χώρα ή διεθνή οργανισμό,
6. Το χρόνο διατήρησης των δεδομένων,
7. Τη δυνατότητα άσκησης δικαιωμάτων,
8. Τυχόν κινδύνους από την επεξεργασία των δεδομένων.

1.2.4.3 ΕΝΗΜΕΡΩΣΗ ΥΠΟΚΕΙΜΕΝΩΝ ΔΙΚΑΙΩΜΑΤΩΝ (άρθρο 14,

Όταν τα δεδομένα προσωπικού χαρακτήρα υποκειμένου δεδομένων, δεν έχουν συλλεγεί από το ίδιο το υποκείμενο, αλλά λαμβάνονται από άλλο φορέα, που τα συνέλεξε σύννομα (άλλως δεν λαμβάνονται), το Πανεπιστήμιο Ιωαννίνωνπαρέχει στο υποκείμενο τις ακόλουθες πληροφορίες:

1. Την ταυτότητα και τα στοιχεία επικοινωνίας του υπευθύνου επεξεργασίας.
2. Τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων.
3. Τους σκοπούς της επεξεργασίας για τους οποίους προορίζονται τα δεδομένα προσωπικού χαρακτήρα, καθώς και τη νομική βάση για την επεξεργασία,
4. Τις σχετικές κατηγορίες προσωπικών δεδομένων,
5. τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων προσωπικού χαρακτήρα, εάν υπάρχουν,
6. κατά περίπτωση, την πρόθεση του υπευθύνου επεξεργασίας να διαβιβάσει δεδομένα προσωπικού χαρακτήρα σε τρίτη χώρα ή διεθνή οργανισμό,
7. Τον χρόνο διατήρησης των δεδομένων,
8. τη δυνατότητα άσκησης δικαιωμάτων,
9. τη δυνατότητα ανάκλησης της συγκατάθεσής του,
10. Το δικαίωμα υποβολής καταγγελίας στην ΑΠΔΠΧ.
11. Την πηγή από την οποία προέρχονται τα δεδομένα,
12. Την ύπαρξη αυτοματοποιημένης λήψης απόφασης,
13. τυχόν κινδύνους από την επεξεργασία των δεδομένων.

1.2.4.4 ΕΞΑΙΡΕΣΕΙΣ ΚΑΙ ΠΕΡΙΟΡΙΣΜΟΙ ΣΤΗΝ ΑΣΚΗΣΗ ΤΩΝ ΔΙΚΑΙΩΜΑΤΩΝ

Πότε παρέχει το Πανεπιστήμιο Ιωαννίνων τις πιο πάνω πληροφορίες:

1. Εντός εύλογης προθεσμίας από την απόκτηση και το αργότερο μέσα σε ένα μήνα,
2. κατά την πρώτη επικοινωνία με το υποκείμενο, όταν τα δεδομένα πρόκειται να χρησιμοποιηθούν για επικοινωνία με το υποκείμενο,

3. κατά την γνωστοποίηση σε άλλο αποδέκτη, όταν τα δεδομένα γνωστοποιούνται πρώτη φορά.

Πότε δεν απαιτείται να τηρηθούν όλα τα παραπάνω:

5. όταν το υποκείμενο έχει όλες τις πληροφορίες,

6. όταν η παροχή των πιο πάνω πληροφοριών είναι αδύνατη ή δυσανάλογα δύσκολη (ιδίως, στην περίπτωση αρχειοθέτησης υπέρ δημοσίου συμφέροντος, έρευνας και στατιστικής). Στην περίπτωση αυτή, πρέπει να ληφθούν μέτρα προστασίας και ασφάλειας,

7. όταν η απόκτηση ή κοινολόγηση προβλέπεται από νομοθεσία, που παρέχει προστασία των εννόμων συμφερόντων του υποκειμένου,

8. όταν συντρέχει εμπιστευτικός χαρακτήρας των δεδομένων λόγω υποχρέωσης τήρησης απορρήτου.

1.2.5 ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΠΡΟΣΤΑΣΙΑΣ ΤΩΝ ΔΕΔΟΜΕΝΩΝ (άρθρα 25 και 32)

1. Το άρθρο 25 περιγράφει τις υποχρεώσεις του υπεύθυνου επεξεργασίας για τήρηση (τεχνικών και οργανωτικών) μέτρων ασφάλειας και προστασίας πριν ακόμα την έναρξη συλλογής και επεξεργασίας των δεδομένων προσωπικού χαρακτήρα (dataprotectionbydesign / dataprotectionbydefault). Ανεξάρτητα αν η επεξεργασία είναι ηλεκτρονική ή έγχαρτη. Ειδικότερα, στο άρθρο προβλέπεται ότι ο υπεύθυνος επεξεργασίας, αφού λάβει υπόψη τις τελευταίες εξελίξεις, το κόστος εφαρμογής και τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων από την επεξεργασία, εφαρμόζει αποτελεσματικά, τόσο κατά τη στιγμή του καθορισμού των μέσων επεξεργασίας όσο και κατά τη στιγμή της επεξεργασίας, κατάλληλα τεχνικά και οργανωτικά μέτρα. Τέτοια μέτρα είναι η ψευδωνυμοποίηση, η ελαχιστοποίηση των δεδομένων, και η ενσωμάτωση εγγυήσεων στην επεξεργασία ώστε να πληρούνται οι απαιτήσεις του Κανονισμού και να προστατεύονται τα δικαιώματα των υποκειμένων των δεδομένων.

2. Στο άρθρο 32 τα μέτρα ασφάλειας και προστασίας ορίζονται ειδικότερα σε:

- ψευδωνυμοποίηση και κρυπτογράφηση των δεδομένων προσωπικού χαρακτήρα,
- 25
- διασφάλιση του απορρήτου, της ακεραιότητας, της διαθεσιμότητας και της αξιοπιστίας των συστημάτων
- δυνατότητα αποκατάστασης της διαθεσιμότητας και της πρόσβασης σε δεδομένα προσωπικού χαρακτήρα σε εύθετο χρόνο σε περίπτωση συμβάντος,
- διασφάλιση διαδικασιών για την τακτική δοκιμή, εκτίμηση και αξιολόγηση της αποτελεσματικότητας των τεχνικών και οργανωτικών μέτρων για τη διασφάλιση της ασφάλειας της επεξεργασίας.
- τήρηση κώδικα δεοντολογίας.

3. Πέρα από τους ορισμούς του συγκεκριμένου άρθρου, στο Πανεπιστήμιο θα πρέπει:

- να εφαρμόζεται η ανωνυμοποίηση, ιδίως στις περιπτώσεις επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς λόγους.
- να προσδιοριστούν εγγράφως, με βάση τα καθηκοντολόγιά και τις αρμοδιότητές τους, ποια πρόσωπα (ονομαστικά) είναι εξουσιοδοτημένα για συγκεκριμένες πράξεις
- να τηρούνται αντίγραφα ασφαλείας αρχείων με δεδομένα προσωπικού χαρακτήρα,
- να μη γίνεται χρήση εξωτερικών αποθηκευτικών μέσων και να μην εξάγονται αρχεία για εργασία στο σπίτι,
- να μην παραμένουν οι χώροι αφύλακτοι και ανοιχτοί, όταν λείπουμε από αυτούς,
- να τηρείται η αρχή «cleandesk» και να μην μπορούν να δουν τρίτοι έγγραφα και αρχεία με δεδομένα προσωπικού χαρακτήρα
- να επικαιροποιούνται τα λογισμικά και, ιδίως, τα λογισμικά για προστασία των υπολογιστών από ιούς.
- να καταστρέφονται – με την τήρηση του νόμου και των διαδικασιών ασφαλείας – όλα τα αρχεία δεδομένων μετά το πέρας του χρόνου τήρησής τους.

Τα πιο πάνω μέτρα πρέπει να υφίστανται και στους ενεργούντες την επεξεργασία για λογαριασμό του Πανεπιστήμιο Ιωαννίνων. Πριν την έναρξη μίας τέτοιας συνεργασίας θα πρέπει να λαμβάνεται σχετική βεβαίωση από τους ενεργούντες την επεξεργασία.

1.2.6 ΑΡΧΕΙΟ ΔΡΑΣΤΗΡΙΟΤΗΤΩΝ ΕΠΕΞΕΡΓΑΣΙΑΣ [ΑΡΘΡΟ 30]

- Το βασικό εργαλείο απόδειξης τήρησης της αρχής της λογοδοσίας
- Ποιες πληροφορίες περιλαμβάνει:

  α) το όνομα και τα στοιχεία επικοινωνίας του υπευθύνου επεξεργασίας, του εκπροσώπου του υπευθύνου επεξεργασίας και του υπευθύνου προστασίας δεδομένων.

  β) τους σκοπούς της επεξεργασίας,

  γ) περιγραφή των κατηγοριών υποκειμένων των δεδομένων και των κατηγοριών δεδομένων προσωπικού χαρακτήρα,

  δ) τις κατηγορίες αποδεκτών στους οποίους πρόκειται να γνωστοποιηθούν ή γνωστοποιήθηκαν τα δεδομένα προσωπικού χαρακτήρα, περιλαμβανομένων των αποδεκτών σε τρίτες χώρες ή διεθνείς οργανισμούς,

  ε) όπου συντρέχει περίπτωση, τις διαβιβάσεις προσωπικού χαρακτήρα σε τρίτη χώρα ή διεθνή οργανισμό

  στ) όπου είναι δυνατό, τις προβλεπόμενες προθεσμίες διαγραφής των διάφορων κατηγοριών δεδομένων,

  ζ) όπου είναι δυνατό, γενική περιγραφή των τεχνικών και οργανωτικών μέτρων ασφάλειας
- Τηρείται και σε γραπτή και σε ηλεκτρονική μορφή αρχείου.

2 Πολιτική Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα

2.1 ΠΛΗΡΟΦΟΡΙΕΣ ΓΙΑ ΤΗΝ ΕΠΕΞΕΡΓΑΣΙΑ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑΤΩΝ ΦΟΙΤΗΤΩΝ ΤΟΥ ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΙΩΑΝΝΙΝΩΝ

Στο παρόν κείμενο ενημερώνουμε τους φοιτητές του Πανεπιστημίου Ιωαννίνων(προπτυχιακούς- μεταπτυχιακούς και υποψηφίους διδάκτορες) για τον τρόπο με τον οποίο συλλέγει και επεξεργάζεται το Πανεπιστήμιο τα προσωπικά τους δεδομένα.

2.1.1 Είδη και τρόποι επεξεργασίας

Πληροφορίες που συλλέγουμεκαι πως τις συλλέγουμε.

Πληροφορίες που μας χορηγεί το υποκείμενο των δεδομένων:

1. Με την εγγραφή σας στο Πανεπιστήμιο Ιωαννίνων, δημιουργούμε ένα αρχείο στο όνομά σας. Σε αυτό το αρχείο προσθέτουμε τις πληροφορίες που μας δίνετε κατά την αίτηση εγγραφής σας.
2. Τηρούμε γενικές πληροφορίες για εσάς, όπως το όνομα, τη διεύθυνση, τα μαθήματα που ολοκληρώσατε και τα προσόντα που αποκτήσατε, καθώς επίσης και βαθμολογίες σχετικά με τις εξετάσεις, τις αξιολογήσεις και τα αποτελέσματα των μαθημάτων. Μπορεί να μας έχετε δώσει πληροφορίες σχετικά με τις "ειδικές κατηγορίες" δεδομένων συμπεριλαμβανομένων αυτών της φυλετικής ή εθνικής καταγωγής σας, των θρησκευτικών πεποιθήσεων σας, της σωματικής ή ψυχικής υγείας σας, ή/ και γενετικά δεδομένα. Πληροφορίες που συλλέγουμε αυτόματα:
3. Αυτόματη συλλογή πληροφοριών σχετικά με εσάς γίνεται κατά την είσοδο σας στα δίκτυα του Πανεπιστημίου, ενσύρματο ή ασύρματο. Χωρίς τις πληροφορίες αυτές, η σύνδεση στο δίκτυο δεν είναι δυνατή. Το Πανεπιστήμιο διατηρεί το δικαίωμα να εξετάζει και να διαχειρίζεται τις πληροφορίες κίνησης σας στο δίκτυο, για σκοπούς προστασίας του δικτύου πληροφορικής.

Πληροφορίες που συλλέγουμε από τρίτους:

1. Τα απαραίτητα προσωπικά σας δεδομένα κατά την εγγραφή σας μεταβιβάζονται σε μας από το Υπουργείο Παιδείας . Μπορούμε επίσης να επικοινωνήσουμε με άλλο οργανισμό ή εκπαιδευτικό ίδρυμα για να επιβεβαιώσουμε τα προσόντα που έχετε αποκτήσει.

Τρόπος επεξεργασίας των δεδομένων προσωπικού χαρακτήρα

1. Συλλέγουμε και επεξεργαζόμαστε ένα ευρύ φάσμα των προσωπικών δεδομένων προκειμένου να σας χορηγήσουμε τις υπηρεσίες μας και να σας υποστηρίξουμε, να διαχειριστούμε αποτελεσματικά τις λειτουργίες μας και να ανταποκριθούμε στις νομικές μας υποχρεώσεις.
2. Χρησιμοποιούμε τις "ειδικές κατηγορίες" των δεδομένων σας για δραστηριότητες όπως: Παροχή ίσων ευκαιριών ή για να προσδιορίζουμε εάν χρειάζεστε υποστήριξη. Πληροφορίες για τυχόν αναπηρίες ή/ και ειδικές απαιτήσεις που έχετε θα χρησιμοποιηθούν για να σας παρέχουμε

1.2.7 11. ΕΠΕΞΕΡΓΑΣΙΑ ΓΙΑ ΣΚΟΠΟΥΣ ΕΠΙΣΤΗΜΟΝΙΚΗΣ ΕΡΕΥΝΑΣ [ΑΡΘΡΟ 89]

- Η επεξεργασία για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς υπόκειται σε κατάλληλες εγγυήσεις ως προς τα δικαιώματα και τις ελευθερίες του υποκειμένου δεδομένων. Οι εγγυήσεις διασφαλίζουν ότι έχουν θεσπιστεί τα τεχνικά και οργανωτικά μέτρα, ιδίως για να διασφαλίζουν την τήρηση της αρχής της ελαχιστοποίησης των δεδομένων.

  Τα μέτρα αυτά μπορούν να περιλαμβάνουν τη χρήση ψευδωνύμων, εφόσον οι σκοποί μπορούν να εκπληρωθούν με τον τρόπο αυτό. Εφόσον οι σκοποί μπορούν να εκπληρωθούν από περαιτέρω επεξεργασία, η οποία δεν επιτρέπει την ταυτοποίηση των υποκειμένων δεδομένων, οι σκοποί εκπληρώνονται κατ' αυτόν τον τρόπο.
- Όταν δεδομένα προσωπικού χαρακτήρα υφίστανται επεξεργασία για σκοπούς έρευνας, το δίκαιο της Ένωσης ή κράτους μέλους μπορεί να προβλέπει παρεκκλίσεις από τα δικαιώματα του υποκειμένου, με την επιφύλαξη των προϋποθέσεων και των εγγυήσεων που αναφέρονται πιο πάνω. Όρος: τα εν λόγω δικαιώματα είναι πιθανό να καταστήσουν αδύνατη ή να παρακωλύσουν σοβαρά την επίτευξη των ειδικών σκοπών και εφόσον οι εν λόγω παρεκκλίσεις είναι απαραίτητες για την εκπλήρωση των εν λόγω σκοπών.
- Η επεξεργασία δεδομένων προσωπικού χαρακτήρα για επιστημονικούς σκοπούς θα πρέπει να συμμορφώνεται επίσης με άλλες σχετικές νομοθεσίες, όπως αυτή για τις κλινικές δοκιμές.
- Πληροφορίες από μητρώα: οι ερευνητές μπορούν να αποκτούν νέες γνώσεις μεγάλης σημασίας (π.χ. για διαδεδομένες παθολογικές καταστάσεις όπως καρδιαγγειακά νοσήματα, καρκίνος, κατάθλιψη). Βάσει των μητρώων, τα αποτελέσματα των ερευνών ενισχύονται, δεδομένου ότι στηρίζονται σε ευρύτερη πληθυσμιακή βάση. Στις κοινωνικές επιστήμες, η έρευνα βάσει μητρώων δίνει στους ερευνητές τη δυνατότητα να αποκτούν ουσιαστικές γνώσεις για τον μακροπρόθεσμο συσχετισμό ορισμένων κοινωνικών καταστάσεων (π.χ. η ανεργία, η εκπαίδευση με άλλες συνθήκες διαβίωσης). Τα αποτελέσματα των ερευνών που αποκτώνται μέσω μητρώων παρέχουν αξιόπιστες και ποιοτικές γνώσεις οι οποίες μπορούν να αποτελέσουν τη βάση για την εκπόνηση και εφαρμογή πολιτικής βασισμένης στη γνώση, να βελτιώσουν την ποιότητα ζωής ορισμένων ανθρώπων και να βελτιώσουν την αποτελεσματικότητα των κοινωνικών υπηρεσιών. Με στόχο τη διευκόλυνση της επιστημονικής έρευνας, τα δεδομένα προσωπικού χαρακτήρα μπορούν να υφίστανται επεξεργασία για σκοπούς επιστημονικής έρευνας, υπό τις κατάλληλες προϋποθέσεις και εγγυήσεις που θεσπίζονται στο ενωσιακό δίκαιο ή στο δίκαιο κράτους μέλους.

τις απαραίτητες διευκολύνσεις για να είστε σε θέση να ανταποκριθείτε στους ακαδημαϊκούς ή/και ερευνητικούς σας στόχους.

3. Υπάρχει η δυνατότητα να μας υποβληθούν πρόσθετες πληροφορίες που ανήκουν στις "ειδικές κατηγορίες", για παράδειγμα ιατρικά στοιχεία ή πληροφορίες σχετικά με τη θρησκεία σας που μπορεί να διαφοροποιούν τον τρόπο παρακολούθησης μαθημάτων.

Τα προσωπικά δεδομένα που μας παρέχονται τα επεξεργαζόμαστε μόνο για τον σκοπό για τον οποίο υποβάλλονται και όταν υπάρχει νόμιμη αιτία.

Οι νομικές βάσεις της επεξεργασίας των προσωπικών δεδομένων είναι οι εξής:

1. Έχει δοθεί συναίνεση από εσάς(μέσω των εντύπων δηλώσεων οι οποίες υποβάλλονται κατά την εγγραφή).
2. Γίνεται στο πλαίσιο εκτέλεσης σύμβασης που έχουμε μαζί σας
3. Επιβάλλεται συμμόρφωση με έννομη υποχρέωση του Πανεπιστημίου
4. Επιβάλλεται διαφύλαξη ζωτικού συμφέροντος σας (ανθρωπιστικοί σκοποί π.χ. επιδημίες, ανταπόκριση σε καταστροφές)
5. Αποτελεί μέρος εκπλήρωσης καθήκοντος για δημόσιο συμφέρον ή άσκηση δημόσιας εξουσίας του Πανεπιστημίου

Η νόμιμη βάση επεξεργασίας των προσωπικών σας δεδομένων παρατίθεται πιο κάτω:

Κατηγορία Προσωπικού Δεδομένου

Πως συλλέγεται

Σκοπός

Νόμιμη βάση επεξεργασίας

Προσωπικά Δεδομένα:

Όνομα, Διεύθυνση, ημερομηνία γέννησης

Αίτηση/ Εγγραφή

Για ταυτοποίηση του φοιτητή και για επικοινωνία

Ειδικές κατηγορίες προσωπικών δεδομένων

1. Θρήσκευμα, Εθνικότητα, Ποινικές διώξεις, Υγεία.

2.Αίτηση/ Εγγραφή

3.Στατιστικούς λόγους /παροχή ίσων ευκαιριών/ παροχή διευκολύνσεων

4.Για την άσκηση του δημόσιου και του έννομου συμφέροντος του Πανεπιστημίου

Με συγκατάθεση των υποκειμένων των δεδομένων

1.Δεδομένα που αφορούν παρουσιολόγια

2.Αξιολογήσεις διδασκόντων-μαθημάτων

3.Για την άσκηση του δημόσιου και του έννομου συμφέροντος του Πανεπιστημίου

4.Για την εξασφάλιση ενός ασφαλούς περιβάλλοντος

5.Για την επίτευξη του έννομου συμφέροντος του Πανεπιστημίου

6.Οπτικοακουστικό Υλικό (Βιντεοσκοπήσεις και φωτογραφήσεις)

7.Κατά την διάρκεια τελετών/ συνεδρίων

8.Για ιστορικούς σκοπούς/ τήρηση αρχείων και για την προώθηση και

9.Για την επίτευξη του έννομου συμφέροντος του Πανεπιστημίου.

Τα δεδομένα προσωπικού χαρακτήρα των φοιτητών

1.Για την προβολή του Πανεπιστημίου

2.Βαθμολογίες και ανατροφοδότηση

3.Γραπτά/ εργασίες.

4.Για τους σκοπούς αξιολόγησης

Δεδομένα που αφορούν την χρήση της Βιβλιοθήκης

1.Μέσω της ηλεκτρονικής σας πρόσβασης ή μέσω του δανεισμού έντυπου υλικού

2.Για την διαχείριση των μαθημάτων και την υποστήριξη των μαθησιακών στόχων του Πανεπιστημίου

Ιατρικά Δεδομένα

1.Μέσω της Υπηρεσίας Σπουδών και Φοιτητικής Μέριμνας και της διαδικασίας παραπομπής για αξιολόγηση

2.Για παροχή και ασφάλειας και υγειονομικής περίθαλψης

Με συγκατάθεση των υποκειμένων των δεδομένων

1.Ποινικά μητρώα και δεδομένα που αφορούν πειθαρχικά παραπτώματα

2.Αίτηση/ Εγγραφή

3. Ως αποτέλεσμα απόφασης δικαστηρίου/ αρμόδιου οργάνου κατόπιν έρευνας

4.Για την άσκηση του δημόσιου συμφέροντος και της έννομης υποχρέωσης του Πανεπιστημίου

Το Πανεπιστήμιο Ιωαννίνων δεσμεύεται ότι θα επεξεργάζεται τα δεδομένα προσωπικού χαρακτήρα που συλλέγει σύννομα και σύμφωνα με τα οριζόμενα στις διατάξεις του Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένων (2016/679), των διατάξεων του Ν. 4624/2019 και κάθε τροποποίησης τους, εφαρμόζοντας ορθές πρακτικές για την προστασία των δεδομένων. Η ασφάλεια στην διατήρηση των προσωπικών πληροφορίων αποτελεί βασική αρχή και τυχόν μεταφορά τους εντός του Πανεπιστημίου σκοπεί στην υποστήριξη της μάθησης, της έρευνας και στην παροχή ποιοτικής τριτοβάθμιας εκπαίδευσης.

Διαχείριση ανεπιθύμητων επικοινωνιών

Οι Υπηρεσίες του Πανεπιστημίου Ιωαννίνων έχουν τη δυνατότητα να επικοινωνούν με τα υποκείμενα των δεδομένων στο πλαίσιο της παροχής των υπηρεσιών του ή για τυχόν υποστήριξη, η για σκοπούς συμμετοχής σε έρευνες.

Η επεξεργασία των δεδομένων για τους προαναφερόμενους σκοπούς, εκτελείται υπό την προϋπόθεση της συγκατάθεσης των υποκειμένων των δεδομένων.

Διαβίβαση σε «τρίτους»

Η διαβίβαση των προσωπικών δεδομένων γίνεται με συγκεκριμένους οργανισμούς για συγκεκριμένους σκοπούς.

Τα δεδομένα προσωπικού χαρακτήρα διαβιβάζονταισε Ν.Π.Δ.Δ. και Οργανισμούς στις περιπτώσεις εκτέλεσης νομικής ή κανονιστικής υποχρέωσης του Ιδρύματος.

6. Αντίγραφα πτυχίων

Οι φοιτητές κατά τη διάρκεια των σπουδών τους στο Πανεπιστήμιο σε εξαιρετικές και μόνο περιπτώσεις συλλέγουν ή επεξεργάζονται προσωπικά δεδομένα, παρα ταυτα αν συντρέχει επιτακτικός λόγος (όπως ανάθεση εργασίας/μελέτης ή στα πλαίσια μιας ερευνητικής δραστηριότητας) που καθιστά την επεξεργασία προσωπικών δεδομένων απαραίτητη αυτό θα γίνεται κατόπιν έγκρισης από τον υπεύθυνο ακαδημαϊκό. Σε αυτή την περίπτωση θα πρέπει υποχρεωτικά να ενημερώνεται ο Υπεύθυνος Προστασίας Δεδομένων του Π.Ι. στα στοιχεία που αναφέρονται κατωτέρω.

Δικαιώματα

Ο Γενικός Κανονισμός Προστασίας Δεδομένων, αναγνωρίζει στα υποκείμενα προσωπικών δεδομένων ορισμένα δικαιώματα. Ο κανονισμός αποσκοπεί στην ενδυνάμωση θεμελιωδών δικαιωμάτων και ελευθεριών των φυσικών προσώπων, ιδίως την προστασία των προσωπικών δεδομένων και της ελεύθερης κυκλοφορίας τους. Για την ενάσκηση οποιουδήποτε δικαιώματος, επικοινωνήστε μαζί μας χρησιμοποιώντας τις λεπτομέρειες στην 4η ενότητα του παρόντος του εγγράφου.

2.1.3 Δικαιώματα υποκειμένων των δεδομένων

1.Δικαίωμα ενημέρωσης: Δικαιούστε να ενημερώνεστε σχετικά με την επεξεργασία των προσωπικών σας δεδομένων, τους λόγους που συλλέγονται, επεξεργάζονται και από ποιον, και με ποιους μοιραζόμαστε τα προσωπικά σας δεδομένα. Δικαιούστε επίσης να λαμβάνετε αντίγραφα εγγράφων που σας αφορούν.

2. Δικαίωμα πρόσβασης στα δεδομένα: Δικαιούστε να ζητήσετε και να λάβετε υποβάλλοντας αίτημα για το σκοπό αυτό.

3. Δικαίωμα διόρθωσης: Δικαιούστε να προβείτε σε διόρθωση ανακριβειών ή λανθασμένων πληροφοριών καθώς και σε συμπλήρωση ελλιπών δεδομένων που αφορούν το άτομό σας.

4. Δικαίωμα στη διαγραφή (λήθη): Δικαιούστε όταν δεν επιθυμείτε πλέον την επεξεργασία και διατήρηση προσωπικών σας δεδομένων, να ζητήσετε τη διαγραφή τους, υπό την προϋπόθεση ότι τα δεδομένα δεν τηρούνται για κάποιο συγκεκριμένο νόμιμο και δηλωμένο σκοπό.

5. Δικαίωμα περιορισμού της επεξεργασίας: Δικαιούστε να ζητήσετε από τον υπεύθυνο της επεξεργασίας τον περιορισμό της επεξεργασίας όταν η ακρίβεια των δεδομένων αμφισβητείται ή είναι παράνομη ή ο υπεύθυνος επεξεργασίας δεν χρειάζεται πλέον τα δεδομένα προσωπικού χαρακτήρα για τους σκοπούς της επεξεργασίας, ή όταν ο υπεύθυνος επεξεργασίας πρόκειται να προβεί στην διαγραφή τους και εσείς έχετε λόγους να μην το επιθυμείτε.

6. Δικαίωμα στη φορητότητα δεδομένων: Δικαιούστε να λαμβάνετε δεδομένα για περαιτέρω ιδιωτική χρήση καθώς και να διαβιβάζετε δεδομένα προσωπικού χαρακτήρα από έναν υπεύθυνο επεξεργασίας σε άλλον. Μπορείτε να ζητήσετε από τον υπεύθυνο επεξεργασίας να λαμβάνετε τα δεδομένα σας σε κοινώς αναγνωρίσιμο μορφότυπο, καθώς επίσης και την απευθείας διαβίβαση των δεδομένων σε άλλον υπεύθυνο επεξεργασίας, εφόσον αυτό είναι τεχνικά δυνατό.

Με οργανισμούς και εταιρίες στο πλαίσιο και για τους σκοπούς πρακτικής άσκησης όπου αυτή αποτελεί προϋπόθεση για την ένταξη των φοιτητών στην αγορά εργασίας.

Άλλοι τρόποι με τους οποίους ενδέχεται να μοιραζόμαστε τα προσωπικά σας δεδομένα:

Μεταφέρουμε τα προσωπικά σας στοιχεία εάν είμαστε υποχρεωμένοι να τα αποκαλύψουμε ή να τα μοιραστούμε για να συμμορφωθούμε με οποιαδήποτε νομική υποχρέωση, να εντοπίσουμε ή να αναφέρουμε ένα ποινικώς διωκόμενο αδίκημα πάντοτε υπό τους όρους και τις προυποθέσεις που ορίζονται στις σχετικές διατάξεις, να επιβάλουμε ή να εφαρμόσουμε τους όρους των συμβάσεων μας ή να προστατεύσουμε τα δικαιώματα, την ιδιοκτησία ή την ασφάλεια των επισκεπτών και των φοιτητών μας. Ωστόσο, πάντα θα προσπαθήσουμε να διασφαλίσουμε ότι τα δικαιώματά σας για την προστασία της ιδιωτικής ζωής θα εξακολουθήσουν να προστατεύονται.

Διαβίβαση δεδομένων εκτός της Ευρωπαϊκής Ένωσης

Γενικά, οι πληροφορίες που μας παρέχετε αποθηκεύονται στους ασφαλείς διακομιστές μας ή σε εφαρμογές που βασίζονται σε συστήματα που βρίσκονται εντός της Ευρωπαϊκής Ένωσης.

1. Πληροφορίες δύναται να διαβιβαστούν εκτός της Ευρωπαϊκής Ένωσης σε περίπτωση που φοιτητής μεταβεί στο εξωτερικό συμμετέχοντας σε προγράμματα ανταλλαγής/ κινητικότητας φοιτητών ή σε δυνητικούς εργοδότες για σκοπούς ένταξης στην αγορά εργασίας.

2. Στην περίπτωση κατά την οποία δεδομένα μεταβιβαστούν εκτός της Ευρωπαϊκής Ένωσης λαμβάνονται όλα τα κατάλληλα μέτρα ασφαλείας όπως αναγράφονται στα άρθρα 45-46 του Κανονισμού 2016/679 για την προστασία των δικαιωμάτων της ιδιωτικότητας, σε συνάρτηση με την πολιτική που ακολουθεί το πανεπιστήμιο Ιωαννίνων. Η διασφάλιση θα γίνει μέσω της επιβολής συμβατικών υποχρεώσεων στον αποδέκτη των προσωπικών σας στοιχείων.

2.1.2 Χρονικό διάστημα διατήρησης των δεδομένων

Το χρονικό διάστημα φύλαξης και αποθήκευσης των δεδομένων προσωπικού χαρακτήρακα θορίζεται από ένα σύνολο παραγόντων, όπως ο σκοπός μας για τη χρήση των πληροφοριών και οι νομικές υποχρεώσεις του Ιδρύματος.

Χρονοδιάγραμμα διατήρησηςαρχείων δεδομένων προσωπικού χαρακτήρα

Περίοδος διατήρησης των αρχείων δεδομένων

1.Αιτήσεις εγγραφής : τουλάχιστον για όσο διάστημα διαρκεί η φοίτηση

2.Αιτήσεις Στέγασης:για όσο διάστημα είναι ενεργός φοιτητής

3.Αιτήσεις Υποτροφιών:8 χρόνια μετά τη λήξη της υποτροφίας.

για έλεγχο από το Υπ. Οικονομικών ή Υπ. Παιδείας και για έκδοση βεβαίωσης μετά από αίτημα του υπότροφου.

4.Δικαίωμα σίτισης: Για όσο διάστημα είναι ενεργός ο φοιτητής

5. Βαθμολογίες Μαθημάτων

7. Δικαίωμα εναντίωσης: Δικαιούστε να αντιτάσσεστε, ανά πάσα στιγμή για λόγους που σχετίζονται με την ιδιαίτερη κατάστασή σας, στην επεξεργασία δεδομένων προσωπικού χαρακτήρα. Επιπλέον, όταν τα προσωπικά δεδομένα σας υφίστανται επεξεργασία για σκοπούς της απευθείας εμπορικής προώθησης (συμπεριλαμβανομένης της κατάρτισης προφίλ), έχετε δικαίωμα να εναντιωθείτε στην επεξεργασία αυτή.

8.Δικαίωμα στην εναντίωση στη λήψη αποφάσεων με αυτοματοποιημένα μέσα: Δικαιούστε να εναντιωθείτε σε αποφάσεις που βασίζονται σε αυτοματοποιημένη επεξεργασία των δεδομένων προσωπικού χαρακτήρα. Μπορείτε να ζητήσετε όπως οι αποφάσεις να γίνονται από φυσικά πρόσωπα και όχι μόνο από υπολογιστές.

Εάν έχετε οποιεσδήποτε αμφιβολίες για τον τρόπο με τον οποίο θα επεξεργαστούμε τα προσωπικά σας δεδομένα, μπορείτε να απευθύνεστε είτε στον Υπεύθυνο Προστασίας Προσωπικών Δεδομένων του Πανεπιστημίου Ιωαννίνων.

2.2 ΥΠΟΔΕΙΓΜΑΤΑ ΕΝΤΥΠΩΝ

2.2.1 Υπόδειγμα Εντύπου Ενημέρωσης για τη συλλογή και επεξεργασία προσωπικών δεδομένων

Οδηγίες:

1. Το κείμενο ενημέρωσης θα πρέπει να χρησιμοποιείται από τις υπηρεσίες του Πανεπιστημίου Ιωαννίνων, όταν συλλέγονται δεδομένα προσωπικού χαρακτήρα για την εκτέλεση της αποστολής του και την άσκηση των καθηκόντων του προσωπικού του. Σε περίπτωση που λαμβάνονται δεδομένα προσωπικού χαρακτήρα από τρίτους φορείς (π.χ. το Υπουργείο Παιδείας) θα πρέπει να διαμορφωθεί το έντυπο σύμφωνα με το άρθρο 14 του Κανονισμού καθώς και τον Ν.4624/2019. Στην περίπτωση αυτή, αρμόδιος υπάλληλος προβαίνει σε πλήρη ενημέρωση κατά την πρώτη επαφή με το υποκείμενο δεδομένων (φοιτητή κλπ). Η ενημέρωση δεν μπορεί να περιλαμβάνεται σε υποσημείωση εγγράφων του Πανεπιστημίου Ιωαννίνων. Λόγω του όγκου των πληροφοριών και της αρχής της λογοδοσίας πρέπει να διαμορφωθεί ξεχωριστό έντυπο στο τέλος του οποίου το υποκείμενο δεδομένων θα υπογράφει ότι ενημερώθηκε (όχι ότι συμφωνεί ή συναινεί).

2. Η ενημέρωση θα πρέπει να αφορά και αντίστοιχα, το έντυπο ενημέρωσης να περιλαμβάνει τις ακόλουθες πληροφορίες:

- αναφορά ότι Υπεύθυνος Επεξεργασίας είναι το Πανεπιστήμιο Ιωαννίνων και τα στοιχεία επικοινωνίας με αυτό (εννοείται με το φυσικό πρόσωπο που έχει την αρμοδιότητα),
- τα στοιχεία επικοινωνίας του Υπεύθυνου Προστασίας Δεδομένων (email dpo@uoi.gr
- με ακρίβεια τους σκοπούς της ενέργειας του Πανεπιστημίου και ότι τα στοιχεία συλλέγονται μόνο για τον συγκεκριμένο σκοπό και δεν θα χρησιμοποιηθούν για άλλο σκοπό,
- τη νομική βάση της επεξεργασίας,
- με ακρίβεια τα δεδομένα που συλλέγονται (απλά ή ειδικής κατηγορίας ή και τα δύο) και ότι τα δεδομένα αυτά είναι απολύτως αναγκαία για τους σκοπούςτης επεξεργασίας. Επισημαίνεται ότι θα πρέπει να ζητούνται μόνο εκείνα τα δεδομένα

που είναι αναγκαία για τον συγκεκριμένο σκοπό (όχι περισσότερα, λόγω εφαρμογής της αρχής της ελαχιστοποίησης).

- τους αποδέκτες των δεδομένων προσωπικού χαρακτήρα (αν υπάρχουν)
- αν υπάρχει περίπτωση να διαβιβαστούν τα δεδομένα προσωπικού χαρακτήρα σε τρίτη χώρα ή διεθνή οργανισμό, θα πρέπει να αναφέρεται και αυτό
- ότι η διατήρηση των προσωπικών του δεδομένων θα διαρκεί συγκεκριμένο χρονικό διάστημα (να οριστεί με ακρίβεια, αν είναι δυνατόν, άλλως να γίνεται πιο γενική αναφορά, όπως, «καθ' όλο το χρονικό διάστημα φοίτησης και ακολούθως για τις ανάγκες αρχειοθέτησης του Πανεπιστημίου με τη λήψη κατάλληλων μέτρων προστασίας και ασφάλειας»),
- ότι το υποκείμενο δεδομένων έχει το δικαίωμα να ασκήσει τα ακόλουθα δικαιώματα: πρόσβασης, διόρθωσης ή διαγραφής, περιορισμού της επεξεργασίας, αντίταξης και φορητότητας των δεδομένων του και ότι για την άσκησή τους μπορεί να απευθυνθεί στο Πανεπιστήμιο Ιωαννίνων (συγκεκριμένη διεύθυνση ή email),
- ότι το υποκείμενο δεδομένων έχει δικαίωμα αναφοράς στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ)
- αν υπάρχουν κίνδυνοι από τη συλλογή των πιο πάνω δεδομένων πρέπει να αναφερθούν.

2.2.2 Υπόδειγμα Ι

«Το Πανεπιστήμιο Ιωαννίνων 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 (ν) ή (ε) και για τα προσωπικά δεδομένα ειδικών κατηγοριών (ευαίσθητα) 9 παρ. 2 (ζ) του Γενικού Κανονισμού 2016/679 και του Ν. 4624/2019). Τα προσωπικά σας δεδομένα θα παραμείνουν στη διάθεση του Πανεπιστημίου Ιωαννίνων 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 Ιωαννίνων 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 Ιωαννίνων στη διεύθυνση _____ (να τεθούν τα στοιχεία του υπεύθυνου ή της γραμματείας της Σχολής ή του Τμήματος). Το Πανεπιστήμιο Ιωαννίνων έχει ορίσει Υπεύθυνο Προσωπικών Δεδομένων με τον οποίο μπορείτε να επικοινωνήσετε στη διεύθυνση ηλεκτρονικής αλληλογραφίας dpo@uoi.gr

2.2.3 Υπόδειγμα ενημέρωσης για φωτογράφιση / βιντεοσκόπηση σε εξέλιξη

Σας ενημερώνουμε ότι πραγματοποιείται φωτογράφιση και βιντεοσκόπηση του χώρου του συνεδρίου, των συνέδρων και όλων των συμμετεχόντων σε αυτό για τους σκοπούς του συνεδρίου ..... της Σχολής ..... του Πανεπιστημίου Ιωαννίνων. Η φωτογράφιση και η βιντεοσκόπηση γίνονται για σκοπούς εκπαιδευτικούς, ερευνητικούς και αρχειακούς. Οι φωτογραφίες και τα βίντεο θα αναρτηθούν στο διαδίκτυο, στην ιστοσελίδα του Πανεπιστημίου Ιωαννίνων καθώς και ....

Αν δεν επιθυμείτε τη λήψη φωτογραφίας σας ή τη βιντεοσκόπησή σας, σας παρακαλούμε ενημερώστε την / τον ....., τηλ.....

Για περισσότερες πληροφορίες σχετικά με τη διαδικασία φωτογράφισης και βιντεοσκόπησης και την χρήση αυτών, σας παρακαλούμε επικοινωνήστε με τον συντονιστή της συνεδρίας κ. ....., τηλ. .....

Για περισσότερες πληροφορίες σχετικά με την πολιτική του Πανεπιστημίου Ιωαννίνων αναφορικά με την προστασία των προσωπικών σας δεδομένων, μπορείτε να επικοινωνήσετε με την Υπεύθυνη Προστασίας Δεδομένων dpo@uoi.gr»

Προσοχή: την ημέρα της κάθε συνεδρίας θα πρέπει:

Α. στην είσοδο να υπάρχει πινακίδα (ευκρινής και σε μέρος που να τη βλέπουν όλοι όσοι προσέρχονται και συμμετέχουν), στην οποία να αναγράφεται το πιο πάνω κείμενο.

Β. στην είσοδο να υπάρχει πινακίδα με τα κατάλληλα σύμβολα – εικόνες (μία κάμερα, μία φωτογραφική μηχανή, ένα μικρόφωνο).

2.2.4 Υπόδειγμα ενημέρωσης πριν τη φωτογράφηση ή τη βιντεοσκόπηση

«Σε εφαρμογή του Γενικού Κανονισμού 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27 Απριλίου 2016 και του Ν. 4624/2019«για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών, το Πανεπιστήμιο Ιωαννίνων σας ενημερώνει ότι οι συνεδρίες του .... Σεμιναρίου – Συνέδριου του Τμήματος ....., που θα πραγματοποιηθούν την .... (ημερομηνία) και ώρα ...., στην αίθουσα ..... της Πανεπιστημιούπολης ..... θα βιντεοσκοπηθούν και θα μεταδοθούν μέσω διαδικτύου ενώ θα ληφθούν και φωτογραφίες των συμμετεχόντων και παρευρισκόμενων.

Το βίντεο και οι φωτογραφίες, σε ψηφιακή ή τυπωμένη μορφή, χωριστά ή ως μέρος εντύπων, θα χρησιμοποιηθούν για τις ανάγκες του συνεδρίου και για την προβολή του, και θα δημοσιευθούν, αποσταλούν και αναρτηθούν στην ιστοσελίδα του Πανεπιστημίου Ιωαννίνων, σε εκδόσεις του Πανεπιστημίου Ιωαννίνων, σε μέσα μαζικής Ενημέρωσης, στον τοπικό και αθηναϊκό Τύπο, [να αναφερθούν όλοι οι πιθανοί τρόποι χρήσης] με σκοπό την ενημέρωση της πανεπιστημιακής και επιστημονικής κοινότητας, των συνέδρων, των συμμετεχόντων μέσω διαδικτύου και του κοινού για το συγκεκριμένο συνέδριο και τα αποτελέσματα του, καθώς και για ερευνητικούς και εκπαιδευτικούς σκοπούς [να αναφερθούν και άλλοι πιθανοί λήπτες της πληροφορίας]. Οι φωτογραφίες ή οι βιντεοσκοπήσεις θα παραμείνουν στο αρχείο του Πανεπιστημίουμόνιμα ως κομμάτι της πανεπιστημιακής δραστηριότητας.

Έχετε δικαίωμα πρόσβασης στα πιο πάνω προσωπικά σας δεδομένα, καθώς και το δικαίωμα να ζητήσετε διόρθωση ή και διαγραφή των προσωπικών σας δεδομένων

εφόσον αυτά δεν είναι πλέον αναγκαία για τον σκοπό που συλλέχθηκαν. Μπορείτε να καταθέσετε προσφυγή σχετικά με την προστασία των προσωπικών σας δεδομένων στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα complaints@dpa.gr. Επίσης, μπορείτε να επικοινωνήσετε με τον Υπεύθυνο Προστασίας Δεδομένων του Πανεπιστημίου Ιωαννίνων στο dpo@uoi.gr.

Όποιος συμμετέχει και παρευρεθεί στις πιο πάνω συνεδρίες δηλώνει ότι γνωρίζει την πιο πάνω συλλογή και επεξεργασία των προσωπικών του δεδομένων και συναινεί.

Εάν δεν επιθυμείτε τη βιντεοσκόπησή σας ή τη λήψη φωτογραφιών σας καθώς και την χρήση αυτών με τον πιο πάνω τρόπο, σας παρακαλώ επικοινωνήστε με τον κ. _____ στο τηλέφωνο _____».

Προσοχή: την ημέρα του συνεδρίου

- να τυπώσετε το κείμενο της ενημέρωσης (αφαιρώντας την τελευταία παράγραφο) και με επιπλέον κείμενο «Δεν επιθυμώ να ληφθούν φωτογραφίες μου ή να εμφανίζομαι στη βιντεοσκόπηση της συνεδρίας» ώστε να υπογράφουν όσοι δεν επιθυμούν να φωτογραφηθούν και
- να δημιουργήσετε ένα μέρος στην αίθουσα που θα κάθονται όσοι δεν θέλουν να βιντεοσκοπηθούν και να φωτογραφηθούν.

3 Πολιτική Ασφάλειας Προσωπικών Δεδομένων

3.1 Περιγραφή Πληροφοριακών Συστημάτων

Η Διεύθυνση Μηχανοργάνωσης και Δικτύων διαχειρίζεται ένα πλήθος πληροφοριακών συστημάτων και εφαρμογών λογισμικού παρέχοντας μηχανογραφική υποστήριξη στο σύνολο της Πανεπιστημιακής Κοινότητας. Τα κεντρικά πληροφοριακά συστήματα που υπεισέρχονται σε επεξεργασία προσωπικών δεδομένων και φιλοξενούνται στη Διεύθυνση Μηχανοργάνωσης και Δικτύων είναι τα εξής:

Σύστημα Φοιτητολογίου: διαχειρίζεται ηλεκτρονικά τις διαδικασίες φοίτησης στα Τμήματα του Πανεπιστημίου διατηρώντας ηλεκτρονικό μητρώο φοιτητών με προσωπικά στοιχεία (στοιχεία ταυτότητας, επικοινωνίας, εγγραφής κ.τ.λ.), στοιχεία φοίτησης (δηλώσεις μαθημάτων, βαθμολογίες, υποτροφίες, πιστοποιητικά, μεταβολές π.χ. αναστολή φοίτησης, διαγραφή, ορκωμοσία κ.τ.λ.), καθώς και μητρώο διδασκόντων με προσωπικά στοιχεία για τους διδάσκοντες (στοιχεία ταυτότητας, στοιχεία επικοινωνίας, βαθμίδα, κ.α.) και στοιχεία διδασκαλίας (ανάθεση μαθημάτων, ανάρτηση βαθμολογιών κ.α.).

Σύστημα Διαχείρισης Προσωπικού: διαχειρίζεται ηλεκτρονικά τα προσωπικά στοιχεία των υπαλλήλων όλων των κατηγοριών του Πανεπιστημίου Ιωαννίνων (μόνιμοι, Αορίστου Χρόνου, Ορισμένου Χρόνου, μέλη ΔΕΠ, ΕΔΙΠ, ΕΤΕΠ), όπως στοιχεία ταυτότητας, υπηρεσιακά στοιχεία, στοιχεία επικοινωνίας, τυπικά προσόντα, πειθαρχικά, ιατρικά στοιχεία κ.α., τις υπηρεσιακές μεταβολές των υπαλλήλων, τις αξιολογήσεις, τις άδειες, τη δημιουργία αναφορών και απογραφικών δελτίων προς αποστολή σε άλλους φορείς.

Σύστημα Ηλεκτρονικού Πρωτοκόλλου: διαχειρίζεται ηλεκτρονικά τα εισερχόμενα και εξερχόμενα έγγραφα όλων των διοικητικών υπηρεσιών του Πανεπιστημίου και υποστηρίζει την ηλεκτρονική διακίνηση των εγγράφων στους αποδέκτες (υπηρεσίες/ υπάλληλοι) καθώς και την ηλεκτρονική αρχειοθέτησή τους σε ψηφιακό αρχείο.

Σύστημα Μισθοδοσίας: διαχειρίζεται ηλεκτρονικά τα μισθολογικά δεδομένα των υπαλλήλων του Πανεπιστημίου Ιωαννίνων, τις εξελίξεις, τις προηγούμενες και νέες μισθοδοσίες, τα αναδρομικά,τη δημιουργία αναφορών και αρχείων προς αποστολή στην ενιαία αρχή πληρωμών.

Σύστημα Οικονομικής Διαχείρισης: διαχειρίζεται ηλεκτρονικά όλες τις οικονομικές υποθέσεις του Πανεπιστημίου Ιωαννίνων (χρηματικά εντάλματα πληρωμής, γραμμάτια είσπραξης, προμήθειες κ.τ.λ.), το κύκλωμα λογιστικής, τους προϋπολογισμούς και απολογισμούς του Ιδρύματος κ.α.

3.2 Ασφάλεια Πληροφοριακών Συστημάτων Αποθήκευσης Προσωπικών Δεδομένων

Στη συνέχεια περιγράφονται συνοπτικά τα τεχνικά μέτρα, τα οποία προβλέπει η πολιτική ασφάλειας των πληροφοριακών συστημάτων, που ακολουθεί το Πανεπιστήμιο Ιωαννίνων.

Το Πανεπιστήμιο Ιωαννίνων για να εξασφαλίσει τη σωστή λειτουργία της Ιστοσελίδας του χρησιμοποιεί ψηφιακό πιστοποιητικό SSL/TLS για να

εξασφαλίσει στους επισκέπτες του ότι μπορούν να πλοηγούνται με ασφάλεια, καθώς τα δεδομένα τους μεταδίδονται κρυπτογραφημένα.

Το πρωτόκολλο SSL (SecureSocketsLayer) αναπτύχθηκε και σχεδιάστηκε για να παρέχει ασφάλεια κατά τη μετάδοση ευαίσθητων δεδομένων στο διαδίκτυο. Πρόκειται για ψηφιακό πιστοποιητικό που εγκαθίσταται σε εξυπηρετητή ιστοχώρων (webserver) ώστε να ενεργοποιείται το πρωτόκολλο "https", το οποίο διασφαλίζει ασφαλή και κρυπτογραφημένη επικοινωνία για τους επισκέπτες των ιστοχώρων.

Το SSL χρησιμοποιεί μεθόδους κρυπτογράφησης των δεδομένων που ανταλλάσσονται μεταξύ δυο συσκευών (συνηθέστερα Ηλεκτρονικών Υπολογιστών) εγκαθιδρύοντας μια ασφαλή σύνδεση μεταξύ τους μέσω του διαδικτύου. Το πρωτόκολλο αυτό χρησιμοποιεί το TCP/IP για τη μεταφορά των δεδομένων και είναι ανεξάρτητο από την εφαρμογή που χρησιμοποιεί ο τελικός χρήστης.
Για τον λόγο αυτό μπορεί να παρέχει υπηρεσίες ασφαλούς μετάδοσης πληροφοριών σε πρωτόκολλα ανώτερου επιπέδου όπως για παράδειγμα το HTTP.

3.2.1 Ασφάλεια στο φυσικό επίπεδο

Το Πανεπιστήμιο Ιωαννίνων διαθέτει ειδικούς χώρους (Datacenters), μέσα στους οποίους φιλοξενούνται υπολογιστές, διακομιστές και συστήματα δικτύωσης τα οποία χρησιμοποιούνται για την αποθήκευση και επεξεργασία των δεδομένων των παραπάνω πληροφοριακών συστημάτων.

Οι χώροι εγκατάστασης του πληροφορικού εξοπλισμού βρίσκονται σε απομονωμένο χώρο, με ελεγχόμενη πρόσβαση, διαθέτουν πόρτα ασφαλείας, κλιματισμό, πυρασφάλεια. Πρόσβαση στους χώρους εξοπλισμού έχουν μόνο οι υπάλληλοι της Διεύθυνσης Μηχανοργάνωσης και Δικτύων.

3.2.2 Ταυτοποίηση – Αυθεντικοποίηση

Η πρόσβαση των χρηστών στα πληροφοριακά συστήματα γίνεται μέσω μηχανισμών ταυτοποίησης και αυθεντικοποίησης με τη χρήση συνθηματικών (username-password). Τα συνθηματικά πιστοποιούν την ταυτότητα του εκάστοτε χρήστη και για το λόγο αυτό είναι μυστικά και αυστηρά προσωπικά. Η διαχείριση των λογαριασμών (δημιουργία συνθηματκών, κ.τ.λ.) σε ορισμένα συστήματα πραγματοποιείται από τους διαχειριστές των συστημάτωνκαι κοινοποιούνται στους ενδιαφερόμενους με τη σύσταση να αλλαχθούν κατά την πρώτη σύνδεση με την εκάστοτε εφαρμογή ώστε να διασφαλίζεται η μυστικότητα.

Σε κάθε χρήστη συστήματος ή εφαρμογής εκχωρείται διαφορετικό όνομα λογαριασμού - συνθηματικού και γενικά αποφεύγεται η απόδοση κοινόχρηστων κωδικών πρόσβασης σε ομάδες χρηστών.

Επιπλέον το Πανεπιστήμιο Ιωαννίνων σε συνεργασία με το GUnet ολοκλήρωσε προσφάτως τις υπηρεσίες καταλόγου για το σύνολο της Ακαδημαϊκής Κοινότητας. Με τις υπηρεσίες αυτές κάθε μέλος του Πανεπιστημίου Ιωαννίνων (φοιτητής, Ακαδημαϊκό ή Διοικητικό Προσωπικό), έχει ένα και μόνο κωδικό (username – password) για πρόσβαση σε ψηφιακές υπηρεσίες (e-mail, ακαδημαϊκή ταυτότητα, σύστημα φοιτητολογίου). Το Σύστημα Ενιαίας Πρόσβασης (SingleSign on – SSO) έχει

τεθεί σε λειτουργία και εξασφαλίζει πρόσβαση στα συστήματα του Πανεπιστημίου Ιωαννίνων, σε όλες τις συνεργαζόμενες διαδικτυακές υπηρεσίες και εφαρμογές με μόνο μία διαδικασία ταυτοποίησης. Η ενεργοποίηση και διαχείριση του κωδικού πρόσβασης γίνεται πλέον από τον κάθε χρήστη ξεχωριστά. Η πολιτική διαχείρισης συνθηματικών μέσω του συστήματος SSO περιλαμβάνει έλεγχο της πολυπλοκότητας, της ιστορικότητας, της συχνότητας αλλαγής του συνθηματικού, καθώς και κλείδωμα λογαριασμού έπειτα από προκαθορισμένο αριθμό διαδοχικών αποτυχημένων προσπαθειών πρόσβασης. Με τον τρόπο αυτό ελαχιστοποιείται η πιθανότητα υποκλοπής διαπιστευτηρίων χρηστών, καθώς αυτά εισάγονται κεντρικά στην υπηρεσία πιστοποίησης χρηστών του Ιδρύματος. Ακόμα και αν η ασφάλεια σε κάποια από τις συνεργαζόμενες διαδικτυακές υπηρεσίες παραβιαστεί από τρίτους, τα διαπιστευτήρια των χρηστών παραμένουν ασφαλή, αφού οι εφαρμογές ποτέ δεν έχουν πρόσβαση σε αυτά.

3.2.3 ΔιαχείρισηΧρηστών

Το Πανεπιστήμιο Ιωαννίνων ακολουθεί συγκεκριμένη πολιτική διαχείρισης των χρηστών των πληροφοριακών συστημάτων, η οποία περιλαμβάνει:

α) διαδικασία για εισαγωγή νέου χρήστη ή για μεταβολή των δικαιωμάτων των χρηστών στα πληροφοριακά συστήματα (π.χ. κατά τη μετακίνηση υπαλλήλου σε άλλη υπηρεσία),

β) διαδικασία για τη διαγραφή μη ενεργού χρήστη (π.χ. σε περίπτωση αποχώρησης υπαλλήλου),

γ) κατηγοριοποίηση των χρηστών σε ομάδες ανάλογα με τα δικαιώματα πρόσβασης που αυτοί έχουν στους πόρους των συστημάτων.

Η πολιτική καλύπτει τόσο τους υπαλλήλους του φορέα, όσο και εξωτερικούς συνεργάτες (π.χ. υπαλλήλους εκτελούντων την επεξεργασία που έχουν πρόσβαση στα πληροφοριακά συστήματα).

Οι διαχειριστές των πληροφοριακών συστημάτων διασφαλίζουν ότι οι χρήστες έχουν πρόσβαση αποκλειστικά στις εφαρμογές και στα δεδομένα τα οποία απαιτούνται για την εκτέλεση της εργασίας τους και όχι σε παραπάνω (π.χ. ο υπάλληλος που χειρίζεται το πρωτόκολλο μιας Γραμματείας Τμήματος έχει πρόσβαση μόνο στα έγγραφα της Οργανικής Μονάδας του).

3.2.4 Αρχεία Καταγραφής

Τα αρχεία καταγραφής των περισσότερων πληροφοριακών συστημάτων διαθέτουν πλήρες ιστορικό κάθε ενέργειας εγγραφής, διόρθωσης και διαγραφής δεδομένων (ποιός/πότε/τι). Τα αρχεία καταγραφής επιβλέπονται ανά τακτά διαστήματα από τον αρμόδιο διαχειριστή συστήματος για τυχόν ανίχνευση και αναγνώριση αθέμιτων ενεργειών.

Επιπλέον πραγματοποιείται καταγραφή επιτυχημένων και αποτυχημένων προσπαθειών σύνδεσης των χρηστών τόσο σε επίπεδο λειτουργικού συστήματος όσο και σε επίπεδο εφαρμογών καθώς και στις επιμέρους βάσεις δεδομένων των εφαρμογών (συμπεριλαμβανομένων και των ενεργειών των διαχειριστών των συστημάτων).

Η πρόσβαση στα αρχεία καταγραφής επίσης καταγράφεται.

3.2.5 Αντίγραφα Ασφαλείας

Η διαδικασία λήψης αντιγράφων ασφαλείας από τα Πληροφοριακά Συστήματα πραγματοποιείται μέσω προγραμματισμένων εργασιών οι οποίες τρέχουν αυτόματα κάθε μέρα σε προκαθορισμένη ώρα. Τααντίγραφα ασφαλείας περιλαμβάνουνπλήρες αντίγραφο των βάσεων δεδομένων και των δεδομένων συστήματος και αποθηκεύονται σε ένα δικτυακό σύστημα αποθήκευσης (NetworkStorageSystem). Έχουν ληφθεί απαραίτητα μέτρα για τηνασφαλή αποθήκευσή τους, καθώς και μέτρα για τον έλεγχο της ορθής εξαγωγής τους (δηλ. περιοδικός έλεγχος ακεραιότητας/αξιοπιστίας των αντιγράφων που λαμβάνονται), έτσι ώστε να είναι δυνατή η αξιοποίησή τους σε περίπτωση που παραστεί ανάγκη.

3.2.6 Προστασία από κακόβουλα λογισμικά

Στους εξυπηρετητές (servers) που φιλοξενούν τα πληροφοριακά συστήματα υπάρχουν εγκατεστημένα κατάλληλα αντι-ιικά προγράμματα (antivirus), τα οποία είναι συνεχώςενημερωμένα. Επίσης αποφεύγεται η εξαγωγή δεδομένων με τη χρήση αποσπώμενων μέσων (π.χ. USB, CD/DVD) από τους συγκεκριμένους υπολογιστές.

3.3 Ασφάλεια Δικτύου και Επικοινωνιών

3.3.1 Εσωτερικό Δίκτυο

Το εσωτερικό δίκτυο έχει κατατμηθεί σε πλήθος εικονικών τοπικών δικτύων (εκτεταμένη χρήση VLANs) που επιτρέπει τον διαχωρισμό της εσωτερικής κίνησης δικτύου ώστε να μπορούν να εφαρμοστούν πολιτικές ασφάλειας ανά εσωτερικό δίκτυο και να περιορίζεται η απειλή από μολυσμένους ή προβληματικούς σταθμούς εργασίας.

Οι εξυπηρετητές και τα πληροφοριακά συστήματα ανήκουν σε αφιερωμένα LANστα οποία η πρόσβαση περιορίζεται ανάλογα με τις εφαρμογές και υπηρεσίες που παρέχονται από κάθε σύστημα.

3.3.1.1 Ενσύρματη επικοινωνία

Η πρόσβαση στο ενσύρματο δίκτυο (Ethernet) γίνεται μέσω εξοπλισμού (accessswitches) ο οποίος είναι διαχειρίσιμος σε επίπεδο θύρας δικτύου ώστε να είναι δυνατός ο εντοπισμός και η απομόνωση προβληματικών υπολογιστών. Επιπλέον εφαρμόζονται τεχνικές ασφάλειας για περιορισμό spoofingσε επίπεδο Ethernet.

3.3.1.2 Ασύρματη πρόσβαση

Η πρόσβαση χρηστών στο δίκτυο μέσω WiFiεπιτρέπει την χρήση πρωτοκόλλων ασφάλειας και κρυπτογράφησης (WPA2 Enterprise και χρήση EAP-TLS/TTLS).

3.3.1.3 Πληροφορικά συστήματα και εξυπηρετητές

Το Πανεπιστήμιο Ιωαννίνων λαμβάνει τα κατάλληλα μέτρα ώστε να διασφαλίζεται η ασφάλεια των δεδομένων που ανταλλάσσονται μεταξύ των χρηστών και των πληροφοριακών συστημάτων. Για τις εφαρμογές τύπου client-server που

περιλαμβάνουν ευαίσθητα προσωπικά δεδομένα (π.χ. Σύστημα Διαχείρισης Προσωπικού) υπάρχει περιορισμένη πρόσβαση με βάση συγκεκριμένες διευθύνσεις δικτύου των χρηστών (IPaddresses).

Για τις Web-based εφαρμογές η επικοινωνία γίνεται μέσω επαρκώς ασφαλούς καναλιού επικοινωνίας με χρήση πρωτοκόλλου SSL, το οποίο χρησιμοποιεί μεθόδους κρυπτογράφησης των δεδομένων.

3.3.2 Σύνδεση με το Internet

Οι πολιτικές ασφάλειας που εφαρμόζονται στην σύνδεση του Πανεπιστημίου Ιωαννίνων με Internetμέσω της διασύνδεσης με το Εθνικό Δίκτυο Έρευνας και Τεχνολογίας (ΕΔΕΤ) περιλαμβάνουν τα παρακάτω.

3.3.2.1 Γενική πολιτική ασφάλειας

Για την προστασία από επιθέσεις τύπου spoofingεφαρμόζονται από το ΕΔΕΤ, που αποτελεί τον πάροχοInternet, σχετικές πολιτικές δρομολόγησης που υλοποιούν τεχνικές προστασίας πληροφορίας δρομολόγησης (στα πλαίσια του MANRS).

Επιπλέον εφαρμόζονται από το Πανεπιστήμιο Ιωαννίνων τεχνικές filteringγια προστασία από spoofing (Bogonprefixesfilteringβάσει του RFC6890).

3.3.2.2 Προστασία από επιθέσεις –κακόβουλα λογισμικά

Για προστασία από επιθέσεις εφαρμόζονται από το Πανεπιστήμιο Ιωαννίνων τεχνικές filtering που απαγορεύουν συνδέσεις σε γνωστά portsπου χρησιμοποιούνται από κακόβουλα λογισμικά (ιοί, worms, κ.α.). Επιπλέον περιορίζεται η πρόσβαση σε portsγια προστασία από emailspam.

Σε περιπτώσεις ανίχνευσης επιθέσεων υπάρχει η δυνατότητα χρήσης της υπηρεσίας Firewallτου ΕΔΕΤ.

3.3.2.3 Πρόσβαση σε εξυπηρετητές

Δικαίωμα απομακρυσμένης διαχειριστικής πρόσβασης στους εξυπηρετητές των πληροφοριακών συστημάτων έχουν μόνο εξουσιοδοτημένοι υπάλληλοι της Διεύθυνσης Μηχανοργάνωσης και Δικτύων και συγκεκριμένα άτομα από εκτελούντες την επεξεργασία (π.χ. εξωτερικός συνεργάτης από εταιρεία υποστήριξης λογισμικού).

Στις περιπτώσεις που απαιτείται απομακρυσμένη σύνδεση σε κάποιο εξυπηρετητή από εξωτερικό συνεργάτη, αυτή γίνεται με χρήση ειδικού κωδικού χρήστη υπό την εποπτεία και τον έλεγχο της Διεύθυνσης Μηχανοργάνωσης και Δικτύων ώστε να καταγράφεται επαρκώς.

Η παρούσα πολιτική προστασίας προσωπικών δεδομένων ενδέχεται να αλλάξει όποτε αυτό απαιτείται και πάντοτε ακολουθώντας το εθνικό και Ευρωπαϊκό δίκαιο. Για το λόγο αυτό, καλείστε ανά τακτά χρονικά διαστήματα να επισκέπτεστε την παρούσα σελίδα προς ενημέρωση σας.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΙΩΑΝΝΙΝΩΝ

ΥΠΕΥΘΥΝΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ: ΣΤΑΥΡΟΥΛΑ ΣΤΑΘΑΡΑ, ΝΟΜΙΚΟΣ, Ε.Τ.Ε.Π. ΤΜΗΜΑΤΟΣ ΜΕΥ.Π.Ι. στοιχεία επικοινωνίας(dpo@uoi.gr, τηλ: 26510-07321).

ΟΜΑΔΑ ΥΠΟΣΤΗΡΙΞΗΣ GDPR:

1. **ΚΩΝΣΤΑΝΤΙΝΟΣ ΠΛΑΤΗΣ,ΠΡΟΙΣΤΑΜΕΝΟΣ Δ/ΝΣΗΣ ΜΗΧΑΝΟΡΓΑΝΩΣΗΣ ΚΑΙ ΔΙΚΤΥΩΝ, ΥΠΕΥΘΥΝΟΣ ΑΣΦΑΛΕΙΑΣ ΜΗΧΑΝΟΡΓΑΝΩΣΗΣ ΚΑΙ ΔΙΚΤΥΩΝ Π.Ι.**
2. **ΑΛΕΞΑΝΔΡΑ ΒΑΝΤΖΙΟΥ, ΝΟΜΙΚΟΣ, ΔΙΟΙΚΗΤΙΚΗ ΥΠΑΛΛΗΛΟΣ-ΠΡΟΙΣΤΑΜΕΝΗ ΤΜΗΜΑΤΟΣ ΕΚΔΗΛΩΣΕΩΝ Π.Ι.**
3. **ΑΛΕΞΑΝΔΡΟΣ ΣΕΡΒΕΤΑΣ, ΠΡΟΙΣΤΑΜΕΝΟΣ ΕΛΚΕ.**
4. **ΙΩΑΝΝΑ ΚΑΝΛΙΔΟΥ, ΔΙΟΙΚΗΤΙΚΗ ΥΠΑΛΛΗΛΟΣ, ΔΝ/ΣΗΣ ΜΗΧΑΝΟΡΓΑΝΩΣΗΣ ΚΑΙ ΔΙΚΤΥΩΝ Π.Ι**
5. **ΧΡΗΣΤΟΣ ΝΤΟΚΟΣ Ε.Τ.Ε.Π. ΔΝ/ΣΗ ΜΗΧΑΝΟΡΓΑΝΩΣΗΣ ΚΑΙ ΔΙΚΤΥΩΝ Π.Ι**
6. **ΙΩΑΝΝΗΣ ΣΙΝΤΟΣ, ΔΙΟΙΚΗΤΙΚΟΣ ΥΠΑΛΛΗΛΟΣ Δ/ΝΣΗΣ ΜΗΧΑΝΩΡΓΑΝΩΣΗΣ ΚΑΙ ΔΙΚΤΥΩΝ.**
7. **ΧΡΗΣΤΟΣ ΒΛΕΤΣΑΣ, ΔΙΟΙΚΗΤΙΚΟΣ ΥΠΑΛΛΗΛΟΣ.**

ΣΧΕΔΙΟ ΑΣΦΑΛΕΙΑΣ ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΙΩΑΝΝΙΝΩΝ

Το Σχέδιο Ασφάλειας (SecurityPlan) είναι το έγγραφο στο οποίο περιγράφονται τα οργανωτικά και τεχνικά μέτρα, καθώς και τα μέτρα φυσικής ασφάλειας που εφαρμόζονται ή/και πρόκειται να εφαρμοστούν με ακρίβεια για την προστασία των πληροφοριών και των προσωπικών δεδομένων, ευαίσθητων και μη, που τηρούνται από το Πανεπιστήμιο καθώς και οι απαραίτητες ενέργειες για την υλοποίησή τους.

.1
Το Σχέδιο Ασφάλειας αποτελείται από την περιγραφή του συστήματος επεξεργασίας προσωπικών δεδομένων του Πανεπιστημίου, τα οργανωτικά, τα τεχνικά μέτρα ασφάλειας, τα μέτρα φυσικής ασφάλειας που εφαρμόζονται, μέτρα ανάκαμψης από καταστροφές και το πλάνο υλοποίησης και εφαρμογής των μέτρων ασφάλειας.

I) Περιγραφή του συστήματος επεξεργασίας προσωπικών δεδομένων

Σύντομη περιγραφή της τεχνολογικής υποδομής και των πληροφοριακών συστημάτων που υποστηρίζουν την επεξεργασία των προσωπικών δεδομένων συμπεριλαμβάνεται στο Παράρτημα .

II) Μέτρα Ασφάλειας

Περιγράφονται τα μέτρα ασφάλειας που εφαρμόζονται από το Πανεπιστήμιοο και εντάσσονται στις παρακάτω τρεις κύριες κατηγορίες:

Α. Οργανωτικά Μέτρα Ασφάλειας
1. Υπεύθυνος Ασφάλειας
2. Οργάνωση / Διαχείριση προσωπικού
3. Διαχείριση πληροφοριακών αγαθών
4. Καταστροφή δεδομένων και αποθηκευτικών μέσων
5. Διαχείριση περιστατικών παραβίασης προσωπικών δεδομένων
6. Εκπαίδευση προσωπικού
7. Έλεγχος

Β. Τεχνικά Μέτρα Ασφάλειας
1. Έλεγχος πρόσβασης
2. Αντίγραφα ασφάλειας
3. Διαμόρφωση υπολογιστών
4. Αρχεία καταγραφής ενεργειών χρηστών και συμβάντων ασφάλειας
5. Ασφάλεια επικοινωνιών
6. Αρχεία σε αποσπώμενα μέσα αποθήκευσης και στο δίκτυο
7. Ασφάλεια λογισμικού
8. Διαχείριση αλλαγών

Γ.Μέτρα Φυσικής Ασφάλειας
1. Έλεγχος φυσικής πρόσβασης
2. Περιβαλλοντική ασφάλεια
3. Έκθεση εγγράφων
4. Προστασία φορητών μέσων αποθήκευσης

Δ. Βασικά μέτρα ανάκαμψης από καταστροφές

Αναλυτικότερα τα μέτρα ασφάλειας κατά κατηγορία:

Α. ΟΡΓΑΝΩΤΙΚΑ ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ

1. Υπεύθυνος Ασφάλειας

Α)Ορισμός Υπεύθυνου Ασφάλειας
προβλέπεται ορισμός διακριτής θέσης υπεύθυνου ασφάλειας (ή, ενδεχομένως, αντίστοιχης ομάδας ατόμων) εντός του Πανεπιστημίου με αρχικές αρμοδιότητες την επίβλεψη και τον έλεγχο της εφαρμογής του σχεδίου ασφάλειας και των μέτρων ασφάλειας πληροφοριών.

2. Οργάνωση/Διαχείριση προσωπικού

Α)Ρόλοι/εξουσιοδοτήσεις
Οι εργαζόμενοι πρέπει να έχουν δικαίωμα πρόσβασης μόνο στα απολύτως απαραίτητα δεδομένα προσωπικού χαρακτήρα, βάσει των αρμοδιοτήτων και καθηκόντων που τους έχουν ανατεθεί (ρόλοι), να ενημερώνονται αρμοδίως για τις ευθύνες και τις υποχρεώσεις τους σε σχέση με την ασφάλεια πληροφοριών και δεδομένων, ώστε να ελαχιστοποιείται ο κίνδυνος από ανθρώπινα σφάλματα κατά τη διάρκεια της κανονικής τους εργασίας.

Β) Αναθεώρηση ρόλων
Οι εξουσιοδοτήσεις και τα δικαιώματα πρόσβασης σε προσωπικά δεδομένα και πληροφορίες επανεξετάζονται από τον διοικητικά υπεύθυνο σε κάθε εργασιακή αλλαγή εργαζομένου: τοποθέτηση, μετακίνηση, αλλαγή καθηκόντων, αποχώρηση κλπ

Επιπρόσθετα, οι εργαζόμενοι πρέπει να ενημερώνονται για τις υποχρεώσεις τους σε σχέση με την τήρηση των όρων εμπιστευτικότητας και εχεμύθειας, όταν αλλάζουν θέση εργασίας ή και κατά την λύση της συνεργασίας τους με το Πανεπιστήμιο.

Γ)Δέσμευση εμπιστευτικότητας
Είναι απαραίτητη η λήψη ειδικών μέτρων ως προς την εμπιστευτικότητα για τη δέσμευση του προσωπικού που επεξεργάζεται προσωπικά δεδομένα, ιδίως όταν το εν λόγω προσωπικό δεν δεσμεύεται ήδη για το απόρρητο.

Συγκεκριμένα στις συμβάσεις και στα συμφωνητικά με συνεργάτες/προμηθευτές πρέπει να συμπεριλαμβάνονται όροι εμπιστευτικότητας και μη αποκάλυψης ευαίσθητων πληροφοριών, όροι προστασίας της ιδιωτικότητας των φυσικών προσώπων και όροι για ασφάλεια των πληροφοριών.

Δ)Αποχώρηση υπαλλήλου
Κατά την αποχώρηση μέλους του προσωπικού ακολουθείται διαδικασία προστασίας των πληροφοριών και των προσωπικών δεδομένων με ευθύνη του διοικητικά υπευθύνου και την λήψη συγκεκριμένων μέτρων:

1. Απενεργοποίηση/κατάργηση των λογαριασμών πρόσβασης και των εξουσιοδοτήσεων σε πληροφοριακά συστήματα, εφαρμογές και υπολογιστές.
2. Κατάργηση των λογαριασμών ηλεκτρονικού ταχυδρομείου και μη ανάθεσή τους σε άλλον (μη επαναχρησιμοποίηση τους).
3. Επιστροφή οποιουδήποτε εξοπλισμού έχει παρασχεθεί συμπεριλαμβανομένων υπολογιστών, περιφερειακών, κλειδιών, ηλεκτρονικών καρτών εισόδου/εξόδου, κ.λπ.

3. Διαχείριση πληροφοριακών αγαθών

Α)Καταγραφή
Σε ενιαίο μητρώο των πληροφοριακών και δικτυακών υποδομών, των συστημάτων του λογισμικού καθώς και των κατηγοριών αρχείων και δεδομένων που χρησιμοποιούνται και τηρούνται, καταγράφεται το σύνολο των κεντρικών πληροφοριακών πόρων του Πανεπιστημίου που σχετίζονται με την ασφάλεια πληροφοριών και την ασφάλεια προσωπικών δεδομένων.

Συγκεκριμένα, κάθε υπηρεσιακή οργανική μονάδα που διαθέτει και λειτουργεί υποδομή πληροφορικής και δικτύων με ευθύνη του διοικητικά υπεύθυνου της μονάδας και σε συνεργασία με τον υπεύθυνο ασφάλειας φροντίζει ώστε να καταγραφούν:

- Υπολογιστικός εξοπλισμός (εξυπηρετητές, σταθμοί εργασίας, συστήματα δίσκων)
- Δικτυακός εξοπλισμός
- Συσκευές δικτυακής ασφάλειας
- Φορητές συσκευές
- Λειτουργικά συστήματα, ενδιάμεσο λογισμικό, βάσεις δεδομένων
- Εφαρμογές λογισμικού και πληροφοριακά συστήματα
- Δεδομένα / πληροφορίες (βάσεις δεδομένων, έντυπα ή ηλεκτρονικά έγγραφα, δεδομένα σε οπτικά ή μαγνητικά μέσα, κ.λπ..)
- Εγκαταστάσεις (γραφεία, DataRoom, κ.λπ..)
- Βοηθητικά δίκτυα / υποστηρικτικά συστήματα (ηλεκτρικό ρεύμα, τηλεπικοινωνίες, κλιματισμός)
- Φυσικό αρχείο (εκτυπώσεις, πρωτότυπα έγγραφα)

Στη συνέχεια για κάθε πληροφοριακό πόρο καταγράφεται ο υπεύθυνος (ιδιοκτήτης) που σε συνεργασία με τον Υπεύθυνο Ασφάλειας, καθορίζουν τα μέτρα που είναι απαραίτητα για την προστασία του πόρου (εξοπλισμός, λογισμικό ή πληροφορία).

Κατά την καταγραφή των πόρων ιδιαίτερη προσοχή δίνεται, ανάλογα με το είδος του πόρου (σύστημα, εφαρμογή, αρχείο, κλπ) , στις ορισμένες κατηγορίες χρηστών και τα δικαιώματα πρόσβασης και εκτέλεσης ενεργειών που αποδίδονται σε αυτές. Καταγράφεται επίσης η αντιστοίχιση των ορισμένων στο σύστημα εργαζομένων με την πρόσβαση και τις ενέργειες που μπορούν να εκτελέσουν, είτε αυτή πραγματοποιείται από προσωπικό λογαριασμό πρόσβασης είτε από κοινό ή προκαθορισμένο λογαριασμό. Επίσης καταγράφεται η διαδικασία διαχείρισης χρηστών, στην οποία περιγράφεται κάθε περίπτωση προσθήκης, αλλαγής ή διαγραφής χρηστών και η απονομή και η μεταβολή των δικαιωμάτων ή επιπέδων πρόσβασης.

Β)Διαχείριση φυσικού αρχείου
Σε κάθε υπηρεσιακή μονάδα πρέπει να εφαρμόζονται συγκεκριμένες διαδικασίες για την ορθή οργάνωση/αρχειοθέτηση/ταξινόμηση του φυσικού αρχείου (δηλ. του αρχείου με τους φυσικούς φακέλους).

Γ)Διαβάθμιση πληροφοριών
Για τις πληροφορίες και τα προσωπικά δεδομένα (ηλεκτρονικά αρχεία, έγγραφα) που διατηρούν και επεξεργάζονται οι υπηρεσιακές μονάδες πρέπει να οριστεί κατάλληλο σχήμα διαβάθμισης. Οι υπεύθυνοι των πόρων χαρακτηρίζουν τις πληροφορίες (δεδομένα) με ευθύνη του διοικητικά υπεύθυνου βάσει του είδους και της κρισιμότητάς τους και σύμφωνα με το ενδεικτικό σχήμα διαβάθμισης.

- Δημόσιας Χρήσης
- Εσωτερικά Αδιαβάθμητα
- Εμπιστευτικά

Για κάθε κατηγορία διαβάθμισης ως προς την Ασφάλεια Πληροφοριών, θα πρέπει να οριστεί αναλυτικά ο τρόπος χειρισμού των πόρων (διαδικασία) από την υπηρεσιακή μονάδα (εκτός εάν προβλέπεται κεντρικά) και σε σχέση με το αντίστοιχο πληροφοριακό σύστημα (εάν χρησιμοποιείται), ώστε να διαφυλάσσεται η εμπιστευτικότητα των πληροφοριών που περιέχουν και να ελαχιστοποιείται η πιθανότητα διαρροής.

Δ)Διακίνηση πληροφοριακών αγαθών
Κάθε υπηρεσιακή μονάδα με ευθύνη του διοικητικά υπεύθυνου θα τηρεί:

- λίστα του μηχανογραφικού εξοπλισμού (προσωπικός υπολογιστής, φορητός, εκτυπωτής, εξωτερικός δίσκος, usbdisk, κλπ) που παραχωρείται στους εργαζομένους της. Επιπλέον οι εργαζόμενοι θα υπογράφουν σε σχετική φόρμα κατά την παραλαβή αλλά και κατά την παράδοση (επιστροφή) του αντίστοιχου εξοπλισμού.
- λίστα με τις κεντρικές εφαρμογές άλλων δημοσίων φορέων που έχει πρόσβαση και τους λογαριασμούς των εργαζομένων που συνδέονται σε αυτές. Επίσης στην ίδια λίστα συμπεριλαμβάνει τις υπηρεσίες cloudή τις άλλες υπηρεσίες τρίτων που χρησιμοποιεί για τις ανάγκες της υπηρεσίας.

Σε περίπτωση που εξοπλισμός (π.χ. υπολογιστής ή USB) με προσωπικά δεδομένα μεταφέρεται εκτός των εγκαταστάσεων του Πανεπιστημίου, η ενέργεια αυτή πρέπει να καταγράφεται (ημερομηνία και ώρα εξόδου, πρόσωπο που χρησιμοποιεί τον εξοπλισμό, επιστροφή του εξοπλισμού).

Στα ψηφιακά μέσα αποθήκευσης πρέπει να τοποθετείται σήμανση, η οποία θα υποδηλώνει το επίπεδο της διαβάθμισης της πληροφορίας που εμπεριέχεται.

Σε περιπτώσεις που μεταφέρονται διαβαθμισμένες πληροφορίες πρέπει να χρησιμοποιούνται συγκεκριμένοι μεταφορείς για την αποστολή εντύπων και ψηφιακών μέσων αποθήκευσης εκτός του Πανεπιστημίου.

Ιδιαίτερη προσοχή πρέπει να δοθεί από το προσωπικό στις παρακάτω περιπτώσεις διακίνησης ευαίσθητων πληροφοριών και προσωπικών δεδομένων:

- Τα έντυπα και τα μέσα αποθήκευσης με κρίσιμα προσωπικά δεδομένα, διακινούνται από και προς το Πανεπιστήμιο, με ειδικών προδιαγραφών φακέλους και πακέτα και καταγράφονται σε ειδικό πρωτόκολλο καταγραφής εισερχομένων/εξερχομένων.
- Τα έντυπα και τα μέσα αποθήκευσης με προσωπικά δεδομένα που διακινούνται εντός του Πανεπιστημίου, από γραφείο σε γραφείο ή μεταξύ οργανωτικών μονάδων επίσης καταγράφονται.
- Για την αποστολή ευαίσθητων πληροφοριών μέσω fax, πρέπει να γίνεται επιβεβαίωση ότι ο παραλήπτης βρίσκεται δίπλα στο fax, πριν την αποστολή τους.
- Κατά την εκτύπωση ευαίσθητων πληροφοριών σε κοινόχρηστους εκτυπωτές, όταν δεν μπορεί να αποφευχθεί, ο εργαζόμενος πρέπει να βρίσκεται δίπλα στον εκτυπωτή αμέσως μετά την αποστολή του αρχείου
- Η ηλεκτρονική αποστολή αρχείων με ευαίσθητα δεδομένα, θα πρέπει να πραγματοποιείται με χρήση ασφαλών μεθόδων, δηλαδή με χρήση κρυπτογραφημένου συνημμένου και αποστολή του κλειδιού κρυπτογράφησης (password) μέσω διαφορετικού καναλιού (τηλεφωνικά ή μέσω SMS).

4. Καταστροφή δεδομένων και αποθηκευτικών μέσων

Α) Διαδικασίες καταστροφής δεδομένων
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. Ειδικότερα, θα πρέπει να ακολουθούνται κατ' ελάχιστον όσα προβλέπονται στην Οδηγία 1/2005 της Αρχής για την ασφαλή καταστροφή των προσωπικών δεδομένων μετά το πέρας της περιόδου που απαιτείται για την πραγματοποίηση του σκοπού της επεξεργασίας.

Στην περίπτωση προσωπικών δεδομένων που παράγονται ή/και χρησιμοποιούνται καθημερινά σε έντυπη μορφή στο πλαίσιο των εργασιών και τα οποία, μετά από την διεκπεραίωση της συγκεκριμένης εργασίας, είναι πλέον άχρηστα (π.χ. αντίγραφα, προχειρες εκθέσεις, σημειώσεις των υπαλλήλων, κ.α.) καταστρέφονται συστηματικά με χρήση καταστροφέων εγγράφων (shredders).

Σε περίπτωση απόσυρσης ή επαναχρησιμοποίησης πληροφοριακού εξοπλισμού (προσωπικοί υπολογιστές, δίσκοι, φορητά μέσα αποθήκευσης), επειδή η διαγραφή αρχείων ή και το format δίσκων δεν είναι επαρκή, θα πρέπει να πραγματοποιείται μόνιμη διαγραφή δεδομένων/αρχείων μέσω προχωρημένων τεχνικών (wipe, securewipe, lowlevelformat) που θα εφαρμόζονται από εξειδικευμένο προσωπικό.

5. Διαχείριση περιστατικών παραβίασης προσωπικών δεδομένων

Α) Αναφορά Συμβάντων και Ευπαθειών Ασφάλειας
Τα μέλη της Ακαδημαϊκής Κοινότητας του Πανεπιστημίου γενικά και ειδικότερα το προσωπικό είναι υποχρεωμένο να αναφέρει οποιαδήποτε συμβάν και ευπάθεια αναγνωρίσει ή του αναφερθεί σε σχέση με την ασφάλεια πληροφοριών, όπως τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας. Η γνωστοποίηση θα γίνεται το συντομότερο δυνατόν στον Υπεύθυνο Ασφάλειας για την αξιολόγηση του συμβάντος και την πιθανή ενεργοποίηση των κατάλληλων διαδικασιών διαχείρισης περιστατικού ασφάλειας και την έγκαιρη εκτέλεση των προβλεπόμενων ενεργειών.

Β) Διαχείριση περιστατικών ασφάλειας
Ο Υπεύθυνος Ασφάλειας ενημερώνει τον ΥΠΔ και εφόσον το γνωστοποιημένο συμβάν αφορά προσωπικά δεδομένα τότε το αξιολογούν από κοινού. Σε περίπτωση που το συμβάν αφορά παραβίαση προσωπικών δεδομένων ο ΥΠΔ ακολουθεί την διαδικασία Διαχείρισης Παραβιάσεων Προσωπικών Δεδομένων (Δ 04).

Ο Υπεύθυνος Ασφάλειας εφαρμόζει τη διαδικασία Διαχείρισης Περιστατικών Ασφάλειας, η οποία ενεργοποιείται αμελλητί σε κάθε περίπτωση που αξιολογηθεί θετικά η αναφορά συμβάντος ασφάλειας και προβλέπει τις ακόλουθες ενέργειες:

- τον καθορισμό των ρόλων των εργαζομένων που θα συμμετάσχουν στην αντιμετώπιση του περιστατικού ασφάλειας (παραλείπεται στην περίπτωση ορισμού Ομάδας Αντιμετώπισης Περιστατικών Ασφάλειας),
- την καταγραφή στοιχείων για κάθε περιστατικό ασφάλειας,
- τη διερεύνηση των αιτιών και τον προσδιορισμό των τεχνικών ή/και οργανωτικών αδυναμιών στις οποίες ενδεχομένως οφείλεται το περιστατικό ασφάλειας,
- την υλοποίηση των ενεργειών αποκατάστασης με συγκεκριμένο χρονοδιάγραμμα ,
- την ενημέρωση των αρμοδίων διοικητικών οργάνων,
- τη διατήρηση των πληροφοριών (έγγραφα ή/και αρχεία) που σχετίζονται με το περιστατικό ασφάλειας, ώστε να τεκμηριώνεται η εκτέλεση των αντίστοιχων προβλεπόμενων ενεργειών .

Ο Υπεύθυνος Ασφάλειας δημιουργεί και συντηρεί μια λίστα (ηλεκτρονική ή μη, ανά τμήμα ή συνολικά) που να περιλαμβάνει τις αρχές, τους οργανισμούς, τους εργαζόμενους, τους συνεργάτες τους ερευνητές που μπορεί να συμμετάσχουν (εμπλακούν) στην αντιμετώπιση ενός Περιστατικού Ασφάλειας Πληροφοριών.

Κάθε συμβάν καταγράφεται σε αρχείο, που περιλαμβάνει τη χρονική στιγμή που έλαβε χώρα, το πρόσωπο που το ανέφερε, σε ποιον το ανέφερε, εκτίμηση των συνεπειών και της κρισιμότητας

του περιστατικού, διαδικασίες ανάκαμψης/διόρθωσης που ακολουθήθηκαν, καθώς και ενδεχόμενη διαδικασία ενημέρωσης των θιγομένων ατόμων ανάλογα με την έκταση του περιστατικού.

Προβλέπεται διαδικασία ανασκόπησης της διαχείρισης του περιστατικού ασφάλειας μετά το πέρας των ενεργειών αντιμετώπισής του. Στο σημείο αυτό θα γίνεται αξιολόγηση των μεθόδων αντιμετώπισης καθώς και αναφορά των μέτρων που ελήφθησαν για την αποτροπή μελλοντικών συμβάντων.

6. Εκπαίδευση προσωπικού

Α)Βασική εκπαίδευση
Το Πανεπιστήμιο πρέπει να διοργανώνει εκπαιδευτικά σεμινάρια μία τουλάχιστον φορά κατά έτος σε χώρο της Πανεπιστημιούπολης, με σκοπό την ορθή εφαρμογή των προβλεπόμενων οργανωτικών και τεχνικών μέτρων ασφάλειας. Η εκπαίδευση θα καλύπτει θέματα προστασίας προσωπικών δεδομένων, καθώς και θέματα ασφάλειας όπως π.χ. χρήση ισχυρών κωδικών πρόσβασης και συνθηματικών, τρόπο εντοπισμού και αναφοράς των περιστατικών παραβίασης της ασφάλειας, σωστή χρήση των e-mail και των αποσπώμενων μέσων αποθήκευσης, socialengineering, phishing, vishing, ασφαλής χρήση εφαρμογών και ιστοτόπων, λογισμικά ασφάλειας, κλπ.

Η περιγραφή των βασικών διαδικασιών και των τεχνικών μέτρων ασφάλειας που πρέπει να γνωρίζουν τα μέλη του προσωπικού αναρτώνται σε κατάλληλο διαμορφωμένο δικτυακό τόπο (webportal).

Β)Εξειδικευμένη εκπαίδευση
Πρέπει να παρέχονται οι απαραίτητοι πόροι για την εξειδικευμένη εκπαίδευση του προσωπικού που έχει αναλάβει τη διαχείριση της ασφάλειας και την διαρκή ενημέρωσή του σχετικά με τις τεχνολογικές εξελίξεις στο χώρο της ασφάλειας πληροφοριών.

Γ) Ενημερώσεις σε θέματα ασφάλειας

Πρέπει να πραγματοποιούνται συχνά και συστηματικά ενημερώσεις ασφάλειας του προσωπικού από ενημερωμένες και έγκυρες πηγές για την ασφάλεια πληροφοριών, ώστε κάθε εργαζόμενος να είναι σε θέση να προστατέψει τόσο το ίδρυμα όσο και τα προσωπικά δεδομένα που αυτό διαχειρίζεται, ιδιαίτερα από τυχόν νέους κινδύνους που εμφανίζονται στο διαδίκτυο.

7. Έλεγχος

Α) Διαδικασία ελέγχων
Ο Υπεύθυνος Ασφάλειας εφαρμόζει τουλάχιστον ετησίως διαδικασία εσωτερικού ελέγχου τήρησης των μέτρων ασφάλειας και της αποτελεσματικότητά τους στην προστασία των πληροφοριακών συστημάτων, των υπηρεσιών τηλεματικής και δικτύων, σύμφωνα με τα ακόλουθα στάδια:
α) προετοιμασία του ελέγχου (καθορισμός πληροφοριακών πόρων/επιμέρους πολιτικών που θα ελεγχθούν, χρονοδιάγραμμα, κλπ),
β) διεξαγωγή του ελέγχου,
γ) αποτελέσματα του ελέγχου (τυχόν ευρήματα, προτεινόμενες ενέργειες κλπ).

Τα αποτελέσματα των ελέγχων διαβιβάζονται ως πόρισμα στα αρμόδια διοικητικά όργανα και ο Υπεύθυνος Ασφάλειας τα αξιοποιεί προβαίνοντας στον προγραμματισμό των αναγκαίων τροποποιήσεων και προσθηκών στα μέτρα ασφάλειας καθώς και στο σχέδιο ασφάλειας.

Υποχρεωτικά ο εσωτερικός έλεγχος της τήρησης των μέτρων ασφάλειας και της αποτελεσματικότητά τους

θα γίνεται στις κρίσιμες πληροφοριακές και δικτυακές υποδομές από κατάλληλα εξουσιοδοτημένο προσωπικό και κατά ελάχιστον θα συμπεριλαμβάνει ελέγχους:
•Ανίχνευσης Ευπαθειών (VulnerabilityScans)
•Δοκιμών Παρείσδυσης (PenetrationTesting)

Β. ΤΕΧΝΙΚΑ ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ

1. Έλεγχος πρόσβασης

Α) Διαχείριση λογαριασμών χρηστών
Τα πληροφοριακά συστήματα και οι εφαρμογές πρέπει να διαθέτουν διαδικασίες για τη διαχείριση των λογαριασμών των χρηστών, οι οποίες πρέπει να περιλαμβάνουν κατ' ελάχιστο την προσθήκη, τη μεταβολή ιδιοτήτων και τη διαγραφή λογαριασμού.

Η σύνδεση με την κεντρική υπηρεσία ταυτοποίησης και εξουσιοδότησης χρηστών, όπου αυτό είναι εφικτό σε οργανωτικό και τεχνικό επίπεδο, είναι επιβεβλημένη για λόγους εξοικονόμησης πόρων (σε προγραμματισμό και διαχείριση), βέλτιστης αξιοπιστίας και γενικευμένης χρήσης ενός κεντρικού λογαριασμού χρήστη.

Β) Μηχανισμοί ελέγχου πρόσβασης
Τα πληροφοριακά συστήματα και οι εφαρμογές θα πρέπει να διαθέτουν μηχανισμούς που να απαγορεύουν την πρόσβαση σε πόρους/υποσυστήματα/αρχεία από μη εξουσιοδοτημένους χρήστες: ουσιαστικά, πρέπει να διαθέτουν κατάλληλα μέτρα που να εξασφαλίζουν την εγγυημένα ορθή ταυτοποίηση και αυθεντικοποίηση των χρηστών ενώ ταυτοχρόνως πρέπει να γίνεται σε τεχνικό επίπεδο συγκεκριμένη εκχώρηση δικαιωμάτων/εξουσιοδοτήσεων σε κάθε χρήστη.

Πρέπει να πραγματοποιείται από τους υπεύθυνους των πληροφοριακών συστημάτων περιοδικός έλεγχος (τουλάχιστον ετησίως) των δικαιωμάτων πρόσβασης και να λαμβάνονται τα απαραίτητα διορθωτικά μέτρα στις περιπτώσεις ύπαρξης λογαριασμών χρήστη με δικαιώματα που δεν αντιστοιχούν στο υφιστάμενο ρόλο του εργαζομένου.

Γ) Διαχείριση συνθηματικών
Η πολιτική διαχείρισης των συνθηματικών των χρηστών, περιλαμβάνει κανόνες αποδοχής για το ελάχιστο μήκος και τους επιτρεπτούς χαρακτήρες των συνθηματικών (πολυπλοκότητα συνθηματικού), την ιστορικότητα του συνθηματικού και τη συχνότητα αλλαγής του. Συγκεκριμένα τα συνθηματικά των χρηστών θα πρέπει:

1. Να έχουν μήκος τουλάχιστον 8 χαρακτήρων.
2. Να περιέχουν χαρακτήρες που να ανήκουν σε τουλάχιστον 3 από τις 4 ακόλουθες ομάδες:
    - Μικρά γράμματα.
    - Κεφαλαία γράμματα.
    - Αριθμοί.
    - Ειδικοί χαρακτήρες.
3. Να αλλάζουν οπωσδήποτε εντός διαστήματος μικρότερου του ενός έτους
4. Να μη συμπίπτουν με τα τελευταία 3 συνθηματικά χρήστη.

Οι χρήστες πρέπει να αλλάζουν οι ίδιοι το (προκαθορισμένο) συνθηματικό που τους ανατίθεται εξαρχής, καθώς επίσης να αλλάζουν όπως έχει αναφερθεί το συνθηματικό τους ανά τακτά χρονικά διαστήματα.

Η παραπάνω πολιτική σε σχέση με τα συνθηματικά των χρηστών (passwordpolicy) θα πρέπει να επιβληθεί μέσω του κεντρικού συστήματος διαχείρισης χρηστών και σε σύνδεση με τους επιμέρους μηχανισμούς ταυτοποίησης των χρηστών στις εφαρμογές και τα συστήματα (π.χ. LDAP, AD). Όπου αυτό δεν είναι εφικτό στο σύνολό του ή σε μέρος του, είναι οι χρήστες

αποκλειστικά υπεύθυνοι να συμμορφώνονται με τις βέλτιστες πρακτικές που επιβάλλει η πολιτική συνθηματικών.

Η ίδια πολιτική συνθηματικών πρέπει να ακολουθείται στους κωδικούς πρόσβασης διαχειριστών και χρηστών στους προσωπικούς υπολογιστές (σταθερούς, φορητούς), tablets και στις άλλες συσκευές.

Επίσης σε σχέση με τις πρακτικές που ακολουθούνται στη διαχείριση και χρήση των συνθηματικών από τους χρήστες **απαγορεύεται:**

1. οι προσωπικοί κωδικοί πρόσβασης χρηστών να γνωστοποιούνται σε άλλους χρήστες. Η συγκεκριμένη πρακτική ενέχει υψηλό κίνδυνο διαρροής των κωδικών και εμφάνισης περιστατικών μη εξουσιοδοτημένης πρόσβασης σε συστήματα, εφαρμογές και πληροφορίες, καθώς επίσης περιορίζει την αξιοπιστία του ελέγχου για το ποιος χρήστης έχει πρόσβαση σε ποιο πληροφοριακό πόρο.
2. οι κωδικοί πρόσβασης να συμπίπτουν με κωδικούς που χρησιμοποιούν οι εργαζόμενοι εκτός Πανεπιστημίου
3. να καταγράφονται οι κωδικοί πρόσβασης σε έντυπα μέσα
4. να αποθηκεύονται οι κωδικοί πρόσβασης σε ηλεκτρονική μορφή χωρίς να κρυπτογραφούνται. Για την ασφαλή αποθήκευση κωδικών πρόσβαση μπορεί να χρησιμοποιούν το λογισμικό Keepass.

Για τα συστήματα ή τις εφαρμογές όπου δεν μπορεί να εφαρμοστεί ένα passwordpolicy, οι χρήστες είναι υπεύθυνοι να συμμορφώνονται με τις βέλτιστες πρακτικές.

Δ) Μη επιτυχημένες προσπάθειες πρόσβασης
Πρέπει να καταγράφονται οι επιτυχημένες και οι αποτυχημένες προσπάθειες σύνδεσης των χρηστών σε όλα τα πληροφοριακά συστήματα. Η καταγραφή αυτή μπορεί να αξιοποιηθεί σε προληπτικούς ελέγχους ασφάλειας για προσπάθειες μη εξουσιοδοτημένης πρόσβασης και στη διερεύνηση περιστατικών ασφάλειας.

Ε) Αδρανοποιημένος υπολογιστής
Προς αποφυγή με εξουσιοδοτημένης πρόσβασης σε προσωπικά δεδομένα, με χρήση ανοιχτού υπολογιστή, ο οποίος μένει χωρίς επίβλεψη (έστω και για λίγα λεπτά) πρέπει ενεργοποιούνται: αυτόματη προφύλαξη της οθόνης (screensaver) του υπολογιστή (μετά από χρονικό διάστημα αδράνειας που προσδιορίζεται στα 10') – για την απενεργοποίηση της οποίας θα απαιτείται χρήση συνθηματικού ή και αυτόματη διαδικασία αποσύνδεσης του χρήστη (μετά από χρονικό διάστημα αδράνειας που προσδιορίζεται στα 60').

2. Αντίγραφα Ασφάλειας

Α) Λήψη και τήρηση αντιγράφων ασφάλειας
Πολιτική για τη λήψη και διαχείριση των αντιγράφων ασφάλειας πρέπει να εφαρμοσθεί σε όλους τους κεντρικούς κρίσιμους πόρους δηλαδή τα πληροφοριακά συστήματα, εφαρμογές, βάσεις δεδομένων, συστήματα, αρχεία, δεδομένα αρχείων χρηστών, αρχεία καταγραφής (logfiles).

Το αρμόδιο προσωπικό για την διαχείριση και προστασία του εκάστοτε κρίσιμου πληροφοριακού πόρου συντάσσει συγκεκριμένη πολιτική αντιγράφων ασφάλειας συμπεριλαμβάνοντας

- τους κατάλληλους μηχανισμούς (τεχνολογίες, λογισμικό και αποθηκευτικά μέσα),

- τη συχνότητα της δημιουργίας/λήψης των αντιγράφων ασφάλειας (ανά τακτά διαστήματα, σε ημερήσια ή εβδομαδιαία βάση, ανάλογα με το μέγεθος και το είδος των δεδομένων, καθώς και με το πότε αυτά μεταβάλλονται),
- τη κατάλληλη επισήμανση αυτών,
- την ασφαλή αποθήκευσή τους,
- την ορθή ανάκτηση των δεδομένων από τα αντίγραφα ασφάλειας,
- τον περιοδικό έλεγχο ακεραιότητας/αξιοπιστίας των αντιγράφων που λαμβάνονται

Πολιτική λήψης αντιγράφων ασφάλειας εφαρμόζεται και στους σταθμούς εργασίας του προσωπικού που επεξεργάζεται προσωπικά δεδομένα, και στην περίπτωση που τα αντίγραφα αποθηκεύονται σε φορητά μέσα, ακόμη και εντός του χώρου εργασίας, τότε αυτά υποχρεωτικά κρυπτογραφούνται για την προστασία τους από μη εξουσιοδοτημένη πρόσβαση.

Η πολιτική διαβιβάζεται υποχρεωτικά στον Υπεύθυνο Ασφάλειας για τον σχετικό έλεγχο.

Σε περίπτωση λήψης αντιγράφων σε φορητά μέσα (εξωτερικοί δίσκοι, κλπ) επισημαίνονται επί αυτών η ημερομηνία λήψης των δεδομένων, το εύρος των λαμβανόμενων δεδομένων, το είδος του αντιγράφου (incremental, full), η περιοδικότητα λήψης του κάθε αντιγράφου (ημερήσιο, εβδομαδιαίο, μηνιαίο, ετήσιο), ο αριθμός των συνολικών αντιγράφων, καθώς και τόπος/τρόπος αποθήκευσης για παραδειγμα χρηματοκιβώτιο.

Β) Τόπος τήρησης
Επιλεγμένα αντίγραφα ασφάλειας πρέπει να διατηρούνται σε διαφορετικό χώρο/φυσική τοποθεσία από το χώρο των πρωτογενών δεδομένων, δηλαδή να φυλάσσονται σε άλλο ασφαλή χώρο εντός του Πανεπιστημίου και να λαμβάνονται μέτρα για την ασφαλή μεταφορά τους. Η φύλαξη αντιγράφων ασφάλειας εκτός των κύριων κτιριακών εγκαταστάσεων του Πανεπιστημίου θα διευκολυνθεί με την δημιουργία και λειτουργία Κέντρου Δεδομένων σε εναλλακτικό χώρο (DR Datacenter), που επιπλέον θα εξασφαλίσει την επιχειρησιακή συνέχεια σε περιπτώσεις καταστροφικών γεγονότων στο (π.χ. πυρκαγιά, πλημμύρα κ.λπ.)..

3. Διαμόρφωση υπολογιστών

Α) Ενιαίο σχήμα διαχείρισης και εφαρμογή της πολιτικής ασφάλειας
Εφαρμόζεται ενιαία πολιτική ασφάλειας στους προσωπικούς υπολογιστές του προσωπικού στο σύνολο των υποδικτύων των διοικητικών υπηρεσιών μέσω υποδομής ActiveDirectory. Κάθε υπολογιστής είναι ενταγμένος στο σύστημα ενιαίας διαχείρισης χρηστών (AD), προκειμένου να εφαρμόζονται καθολικά, σε επίπεδο χρήστη, ομάδας, τμήματος ή διεύθυνσης, οι ρυθμίσεις ασφάλειας πληροφοριών, η επιτρεπτή χρήση προγραμμάτων, η χρήση υπολογιστικών και δικτυακών πόρων (π.χ. εκτυπωτές, δικτυακή δίσκοι, backup).

Η υποδομή AD αξιοποιεί το σύστημα πλήρους διαχείρισης του κύκλου ζωής των προσωπικών λογαριασμών μέσω της σύνδεσής του με το κεντρικό LDAP.

Β) Προστασία από κακόβουλο λογισμικό
Πρέπει να υπάρχει προστασία από κακόβουλο λογισμικό όλων των υπολογιστών, τόσο των προσωπικών υπολογιστών του προσωπικού όσο και των εξυπηρετητών. Αυτό επιτυγχάνεται (πέραν της σωστής χρήσης αυτών από το προσωπικό) με αντιικά προγράμματα (antivirus), καθώς και με χρήση προγραμμάτων τειχών ασφάλειας (firewall). Σε κάθε προσωπικό υπολογιστή με ευθύνη του αρμόδιου προσωπικού υποχρεωτικά εγκαθίσταται και λειτουργεί antivirus και firewall, τα οποία πρέπει να διαθέτουν ανά πάσα στιγμή τις πλέον πρόσφατες ενημερώσεις. Επιπλέον, στο λειτουργικό σύστημα των υπολογιστών (εφόσον είναι συνδεδεμένοι στο Διαδίκτυο) πρέπει να εγκαθίστανται σε τακτά χρονικά διαστήματα οι ενημερώσεις ασφάλειας.

Στους υπολογιστές που τηρούν ή επεξεργάζονται ευαίσθητες πληροφορίες ή προσωπικά δεδομένα πρέπει να λειτουργεί λογισμικό πλήρους προστασίας τελικού σημείου (Endpoint

Protection) του οποίου η λειτουργία καθορίζεται αυτόματα από κεντρική πολιτική προστασίας, για να περιοριστεί η πιθανότητα λάθους στην χρήση του και να εξαλειφθεί ο κίνδυνος μόλυνσής τους με κακόβουλο λογισμικό. Το προσωπικό (οι χρήστες) θα ενημερωθεί και θα εκπαιδευτεί στο λογισμικό Endpoint Protection και στους ελέγχους που πρέπει να εκτελεί όταν λαμβάνει αρχεία που προέρχονται από εξωτερικά δίκτυα ή φορητά μέσα αποθήκευσης.

Στους υπολογιστές που τηρούν ή επεξεργάζονται προσωπικά δεδομένα και κυρίως δεδομένα ειδικών κατηγοριών λειτουργεί λογισμικό ελέγχου, εντοπισμού και παρεμπόδισης μη εξουσιοδοτημένων/λανθασμένων ενεργειών διακίνησης/μεταφοράς πληροφοριών εκτός του Πανεπιστημίου (DLP – DataLossPrevention) του οποίου η λειτουργία καθορίζεται αυτόματα από κεντρική πολιτική προστασίας.

Γ) Ρυθμίσεις υπολογιστών
Στους υπολογιστές του προσωπικού που λειτουργούν ανεξάρτητα επιτρέπεται η σύνδεση με διαχειριστικούς λογαριασμούς μόνο στο αρμόδιο προσωπικό διαχείρισης. Οι εργαζόμενοι συνδέονται μόνο με δικαιώματα απλού χρήστη και χωρίς δυνατότητες ενεργειών που μπορεί να επηρεάσουν την συνολική λειτουργία και διαμόρφωση π.χ. απενεργοποίηση αντιικών προγραμμάτων, εγκατάσταση νέων προγραμμάτων ή αλλαγή ρυθμίσεων υπαρχόντων, κ.λπ.. Στους υπολογιστές αυτούς πρέπει να γίνεται από το αρμόδιο προσωπικό περιοδικός έλεγχος του εγκατεστημένου λογισμικού για τον τυχόν εντοπισμό προγραμμάτων που έχουν εγκατασταθεί με βάση εγκεκριμένες διαδικασίες.

Επίσης πρέπει να ληφθεί υπόψη ότι η χρήση λογαριασμών με κλιμακούμενα δικαιώματα (όχι πλήρους διαχείρισης) στους ανεξάρτητους υπολογιστές βελτιώνει το επίπεδο ασφάλειας, ειδικά στις περιπτώσεις που συγκεκριμένες εφαρμογές έχουν σαν προϋπόθεση για την λειτουργία τους επαυξημένα δικαιώματα χρήστη.

Δ) Σύνδεση αποσπώμενων μέσων
Οι ηλεκτρονικοί υπολογιστές που χρησιμοποιούνται από τους τελικούς χρήστες δεν πρέπει να διαθέτουν δυνατότητα εξαγωγής δεδομένων σε αποσπώμενα μέσα (π.χ. USB, CD/DVD), εκτός αν υπάρχει σχετική έγκριση από την υπηρεσία.

Ε)Υπολογιστές με πρόσβαση στο Διαδίκτυο

Δεν πρέπει να αποθηκεύονται προσωπικά δεδομένα ειδικών κατηγοριών 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).

4. Αρχεία καταγραφής (logfiles)

Α)Τήρηση και έλεγχος αρχείων καταγραφής
Στα κρίσιμα συστήματα τηρούνται από το αρμόδιο προσωπικό (διαχειριστές) και ελέγχονται σε τακτά χρονικά διαστήματα, τα αρχεία καταγραφής των ενεργειών (logfiles) των χρηστών, συμπεριλαμβανομένων και των ενεργειών των διαχειριστών των συστημάτων, καθώς και των συμβάντων που σχετίζονται με την ασφάλεια.
Πρόσβαση στα αρχεία αυτά, εκτός από τους διαχειριστές συστημάτων, δύναται να έχουν ο Υπεύθυνος Ασφάλειας, και όποια άλλα μέλη του προσωπικού είναι επιφορτισμένα με αρμοδιότητες διαχείρισης περιστατικών ασφάλειας κατόπιν κατάλληλης εξουσιοδότησης.

Β) Ειδικές ενέργειες που πρέπει να καταγράφονται
Στα αρχεία καταγραφής ενεργειών (logfiles) των πληροφοριακών συστημάτων και των υπηρεσιών διαδικτύου τηρούνται οπωσδήποτε, κατ' ελάχιστο, τα εξής: το αναγνωριστικό του χρήστη που αιτήθηκε την σύνδεση/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

συνδέθηκε/προσπέλασε την πληροφορία που αιτήθηκε. Επίσης, πρέπει να καταγράφονται στοιχεία που αφορούν τις προσπάθειες μη εξουσιοδοτημένης πρόσβασης και γενικότερα κάθε ενέργεια η οποία μπορεί να υποδηλώνει διενέργεια επίθεσης.

Στα αρχεία καταγραφής κεντρικών συσκευών που συνδέουν το δίκτυο με τα εξωτερικά δίκτυα ή με εσωτερικές ζώνες ασφάλειας δύναται να τηρούνται, για περίοδο ενός έτους, αποκλειστικά: η ημερομηνία και η ώρα της κάθε σύνδεσης/αποσύνδεσης, η διάρκειά της, η διεύθυνση δικτύου (προέλευσης-προορισμού) και το είδος (πρωτόκολλο-πόρτες TCP/IP) της επικοινωνίας. Τα αρχεία αυτά τηρούνται σε κρυπτογραφημένο κατάλογο του οποίου το κλειδί αποκρυπτογράφησης είναι αποκλειστικά γνωστό στον Υπεύθυνο Ασφάλειας και σε σύστημα που έχει διαχειριστικά δικαιώματα συγκεκριμένος εργαζόμενος. Για το έλεγχο των αρχείων απαιτείται ταυτόχρονη πρόσβαση των παραπάνω δύο, σε σύστημα και αρχεία, και με υποχρεωτική τη παρουσία του διοικητικά υπεύθυνου του αρμόδιου για την λειτουργία του δικτύου τμήματος.

Γ) Διαγραφή αρχείων καταγραφής
Τα αρχεία καταγραφής ενσωματώνονται στην πολιτική λήψης αντιγράφων ασφάλειας και δεν διαγράφονται χωρίς κατάλληλη έγκριση και πριν την πάροδο χρονικού διαστήματος δύο τουλάχιστον ετών, το οποίο καθορίζεται επακριβώς από τον υπεύθυνο του συστήματος σε συνεργασία με τον Υπεύθυνο Ασφάλειας.

5. Ασφάλεια επικοινωνιών

Α) Ασφάλεια Δικτύων

Το δίκτυο του Πανεπιστημίου διαχωρίζεται από τα εξωτερικά δίκτυα και λόγω τους μεγέθους του έχει κατατμηθεί σε υποδίκτυα ή/και ζώνες ασφάλειας με στόχο την αποτελεσματική προστασία των πληροφοριακών πόρων. Διαθέτει μηχανισμούς και συστήματα ασφάλειας (ενδεικτικά αναφέρονται: αναχώματα ασφάλειας (firewall), συστήματα ανίχνευσης και αποτροπής εισβολών (IPS), λίστες ελέγχου πρόσβασης (ACL), ιδεατά ιδιωτικά δίκτυα), των οποίων η λειτουργία και η τεχνική διαμόρφωση λαμβάνει υπόψη τις διεθνείς, ευρέως αποδεκτές πρακτικές και πρότυπα. Το αρμόδιο προσωπικό σε συνεννόηση με τον Υπεύθυνο Ασφάλειας παραμετροποιεί και διαμορφώνει τους προαναφερόμενους μηχανισμούς και συστήματα για την άμεση εφαρμογή των απαραίτητων μέτρων και την αποτελεσματική προστασία του δικτύου, των προσωπικών δεδομένων και πληροφοριών.

Β) Απομακρυσμένη πρόσβαση

Η απομακρυσμένη πρόσβαση σε κρίσιμα συστήματα και εφαρμογές επιτρέπεται μόνο μέσω ασφαλών καναλιών με ταυτοποίηση/αυθεντικοποίηση και κρυπτογράφηση (όπως VPN). Η σύνδεση με προγράμματα πρόσβασης όπως RemoteDesktop, VNC, κ.λπ. επιτρέπονται μόνο σε εξουσιοδοτημένο προσωπικό και πάνω από το προβλεπόμενο για την περίπτωση VPN. Για την περαιτέρω μείωση του κινδύνου διαρροής δεδομένων ή μη εξουσιοδοτημένης πρόσβασης, προτείνεται η χρήση 2FA (TwoFactorAuthentication) κατά την σύνδεση μέσω VPN.

Γ) Πρωτόκολλα δικτύου

Είναι υποχρεωτική η χρήση ασφαλών πρωτοκόλλων επικοινωνίας στο δίκτυο, όπως HTTPS, SFTP, SSH, SMTPS, IMAPS. Τα πληροφοριακά συστήματα και οι εφαρμογές με διεπαφή παγκόσμιου ιστού πρέπει να λειτουργούν αποκλειστικά μέσω ασφαλούς (κρυπτογραφημένου) καναλιού (SSL/HTTPS), καθώς επίσης και οι ιστοσελίδες που περιλαμβάνουν φόρμες υποβολής προσωπικών δεδομένων.

Επίσης η μετάδοση των κωδικών πρόσβασης πάνω από το δίκτυο από εφαρμογές, στη φάση της σύνδεσης των χρηστών τους, πρέπει να γίνεται με κρυπτογράφηση, όπου είναι δυνατόν.

Δ) Ζώνες ασφάλειας

Τα συστήματα που υποστηρίζουν και λειτουργούν υπηρεσίες ευρέως προσβάσιμες από το διαδίκτυο τοποθετούνται σε συγκεκριμένες ζώνες ασφάλειας για την καλύτερη προστασία των πληροφοριών και των προσωπικών δεδομένων με την αξιοποίηση μηχανισμών και συστημάτων δικτυακής ασφάλειας.
Σε κάθε περίπτωση καταγράφεται η αρχιτεκτονική που έχει υλοποιηθεί, οι πληροφοριακοί πόροι που έχουν τοποθετηθεί στη ζώνη κι η πολιτική ασφάλειας που εφαρμόζεται στους σχετικούς μηχανισμούς και τα συστήματα που χρησιμοποιούνται.

Ε) Πρόσβαση χρηστών σε υπηρεσίες και εφαρμογές διαδικτύου τρίτων
Η πρόσβαση σε συγκεκριμένες υπηρεσίες και εφαρμογές του διαδικτύου (internet) τρίτων παρόχων από υποδίκτυα υπολογιστών των κεντρικών διοικητικών υπηρεσιών μπορεί να περιοριστεί ή και να απαγορευτεί μέσω των μηχανισμών και συστημάτων ασφάλειας, εάν θέτει αποδεδειγμένα σε κίνδυνο προσωπικά δεδομένα και ευαίσθητες πληροφορίες.

ΣΤ) Αρχεία καταγραφής (logs)
Οι κρίσιμες δικτυακές και υπολογιστικές υποδομές (εξοπλισμός, σχετικό λογισμικό) είναι υποχρεωτικό να συνδέονται με ασφάλεια και να ενημερώνουν κεντρικό σύστημα συλλογής και καταγραφής συμβάντων, όπου αυτό είναι τεχνικά εφικτό. Έτσι επιτυγχάνεται ο βέλτιστος κεντρικός έλεγχος των συμβάντων και η ολοκληρωμένη αξιολόγησή τους σε σχέση με την ασφάλεια των δικτυακών και πληροφοριακών πόρων.

6. Αρχεία σε αποσπώμενα μέσα αποθήκευσης και στο δίκτυο

Α) Χρήση κρυπτογράφησης

Η προστασία της εμπιστευτικότητας, της ακεραιότητας και της αυθεντικότητας των πληροφοριών και των προσωπικών δεδομένων βελτιώνεται σε μεγάλο βαθμό με την χρήση κρυπτογραφικών τεχνικών και προγραμμάτων.

Στους προσωπικούς υπολογιστές του προσωπικού πρέπει να λειτουργεί λογισμικό κρυπτογράφησης, το οποίο θα χρησιμοποιείται υποχρεωτικά για την προστασία αρχείων με ευαίσθητες πληροφορίες και προσωπικά δεδομένα, ειδικά στις παρακάτω περιπτώσεις:
1) αποθήκευση αρχείων σε φορητά μέσα (π.χ. USB δίσκους κ.ο.κ.), αφού για αυτές τις περιπτώσεις ο κίνδυνος διαρροής δεδομένων αυξάνεται.
2) αποθήκευση αρχείων στο cloud ή σε ιστότοπους που προσφέρουν υπηρεσίες αποθήκευσης
3) αποθήκευση αρχείων σε κοινόχρηστους φακέλους

Σε περιπτώσεις ύπαρξης αναγκών πρόσβασης από περισσότερους από ένα εργαζόμενο σε κρυπτογραφημένα αρχεία ή folder, εγκαθίσταται στους υπολογιστές των χρηστών κατάλληλο λογισμικό κρυπτογράφησης με αυτά τα ειδικά χαρακτηριστικά.

Στους υπολογιστές που γίνεται επεξεργασία προσωπικών δεδομένων ειδικών κατηγοριών εγκαθίσταται υποχρεωτικά, από εξειδικευμένο προσωπικό, λογισμικό κρυπτογράφησης (EndpointEncryption) του οποίου η λειτουργία καθορίζεται από κεντρική πολιτική προστασίας και εκπαιδεύεται σε αυτό ο χρήστης.

Επίσης η χρήση κρυπτογραφικών προγραμμάτων προτείνεται στις περιπτώσεις:
- στην ηλεκτρονική αποθήκευση κωδικών πρόσβασης
- στην αποστολή συνημμένων αρχείων που περιέχουν ευαίσθητες πληροφορίες (π.χ. προσωπικά δεδομένα) μέσω e-mail
- στους σκληρούς δίσκους των φορητών υπολογιστών ώστε να ελαχιστοποιείται ο κίνδυνος διαρροής πληροφοριών ή μη εξουσιοδοτημένης πρόσβασης σε περίπτωση κλοπής ή απώλειας της συσκευής.

Β) Αρχεία σε δίκτυα

Τα αρχεία με κρίσιμες πληροφορίες και προσωπικά δεδομένα προτείνεται να αποθηκεύονται από τον χρήστη του υπολογιστή σε κεντρικό σύστημα δικτυακών δίσκων, κατάλληλα διαμορφωμένο ως προς την ασφάλεια και τα δικαιώματα πρόσβασης σε επίπεδο δίσκου, καταλόγων και αρχείων. Στο ίδιο σύστημα (σε άλλους όμως δικτυακούς δίσκους) προτείνεται να αποθηκεύονται τα κοινά αρχεία ή τα αρχεία που ανταλλάσσονται μεταξύ του προσωπικού του ίδιου τμήματος ή της ίδιας διεύθυνσης.

Η χρήση εφαρμογών διαδικτύου αποθήκευσης και ανταλλαγής αρχείων (cloudstorage) για υπηρεσιακούς σκοπούς, όπως dropbox, Gdirve,Onedrive, WeTransferκλπ απαγορεύεται εκτός εάν υπάρχει σχετική σύμβαση/συμφωνία του Πανεπιστημίου με τον πάροχο της υπηρεσίας.

7. Ασφάλεια λογισμικού

Α) Σχεδιασμός εφαρμογών

Ο σχεδιασμός των εφαρμογών που χρησιμοποιούνται στην επεξεργασία προσωπικών δεδομένων πρέπει να πραγματοποιείται λαμβάνοντας υπόψη τις βασικές αρχές της προστασίας προσωπικών δεδομένων και της ιδιωτικότητας (privacybydesign). Ως εκ τούτου, οι εφαρμογές πρέπει να ακολουθούν την αρχή της ελαχιστοποίησης των δεδομένων (dataminimization), 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 ασφάλειας για την προστασία των δεδομένων από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας.

Β) Ασφαλής ανάπτυξη εφαρμογών

Σε περίπτωση ανάπτυξης εφαρμογών, είτε εσωτερικά στον οργανισμό είτε από εξωτερικό συνεργάτη, θα πρέπει να προβλέπεται μεθοδολογία ασφαλούς ανάπτυξης λογισμικού, ώστε να αποφευχθούν τυχόν ευπάθειες αυτού ως προς την ασφάλεια προτού αυτό υλοποιηθεί.
Η εσωτερική ανάπτυξη εφαρμογών γίνεται αποκλειστικά σε κατάλληλα διαμορφωμένο, ανεξάρτητο, συνεργατικό προγραμματιστικό περιβάλλον και με βάση συγκεκριμένη μεθοδολογία ανάπτυξης κώδικα.

Στις περιπτώσεις όπου η ανάπτυξη των εφαρμογών γίνεται από εξωτερικό συνεργάτη, θα πρέπει να υπάρχουν προδιαγραφές ασφάλειας της εφαρμογής στο έγγραφο περιγραφής απαιτήσεων λογισμικού, το οποίο θα εμπεριέχεται στη σύμβαση με τον εκάστοτε ανάδοχο.

Γ) Αναβάθμιση λογισμικού

Το εμπορικό λογισμικό και το λογισμικό ΕΛ/ΛΑΚ των κεντρικών υπολογιστικών και δικτυακών υποδομών πρέπει να ενημερώνεται συχνά με τις νέες εκδόσεις ασφάλειας μέσω των προβλεπόμενων διαδικασιών αναβάθμισης. Ως εκ τούτου θα πρέπει να διασφαλίζεται η συνέχεια της άδειας χρήσης του εμπορικού λογισμικού μέσω έγκαιρης σύναψης συμβάσεων συντήρησης για τη παροχή των νέων εκδόσεων, ενημερώσεων και τεχνικής υποστήριξης. Σε περίπτωση που υπάρχει ενημέρωση ότι σταματά η υποστήριξη συγκεκριμένου λογισμικού τότε προγραμματίζεται από το αρμόδιο τμήμα η άμεση αντικατάστασή του με νέα έκδοση του ίδιου λογισμικού (majorupgrade, θεωρείται νέο/άλλο λογισμικό) ή με αντίστοιχο λογισμικό.

8. Διαχείριση αλλαγών

Α) Πολιτική διαχείρισης αλλαγών

Ο υπεύθυνος κάθε πληροφοριακού συστήματος έχει την ευθύνη της διαχείρισης των αλλαγών (ChangeManagement) σε αυτό και οφείλει να μεριμνά κατ' ελάχιστον για:

- την καταγραφή των αιτημάτων αλλαγής.
- τον καθορισμό των ρόλων που έχουν δικαίωμα έγκρισης των αλλαγών
- τον καθορισμό των κριτηρίων αποδοχής της αλλαγής

- το χρονοδιάγραμμα υλοποίησης

Προτείνεται σε όλα τα πληροφοριακά συστήματα και τις εφαρμογές με ευθύνη του υπεύθυνου να ακολουθείται συγκεκριμένη διαδικασία διαχείρισης αλλαγών σύμφωνα με τα παρακάτω βήματα:

1. Ενέργειες που απαιτούνται για την υλοποίηση της αλλαγής
2. Αξιολόγηση των πιθανών επιπτώσεων στη λειτουργικότητα και στην ασφάλεια πληροφοριών.
3. Πλάνο επαναφοράς σε προηγούμενη κατάσταση σε περίπτωση αποτυχίας υλοποίησης της αλλαγής.
4. Ενέργειες δοκιμών.
5. Αποτελέσματα δοκιμών.
6. Έγκριση αλλαγών.

Β) Περιβάλλον δοκιμών
Οι δοκιμές του λογισμικού, τόσο σε επίπεδο επιμέρους εφαρμογών όσο και σε επίπεδο λειτουργιών διεξάγονται αποκλειστικά σε δοκιμαστικό περιβάλλον. Επίσης συμπεριλαμβάνουν μεθοδολογία επαλήθευσης της ασφάλειας των εφαρμογών και ελτισκόπηση του κώδικα, όπου αυτό είναι τεχνικά εφικτό.

Το λογισμικό ελέγχεται σε επικαιροποιημένο μη παραγωγικό σύστημα και 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.

Γ) Συντήρηση λογισμικού συστήματος / ενδιάμεσου λογισμικού / εφαρμογών
Η ενημέρωση, αναβάθμιση και συντήρηση του λογισμικού των κεντρικών υπολογιστικών και δικτυακών συστημάτων και των παρεχόμενων υπηρεσιών τηλεματικής γίνεται από εξειδικευμένο προσωπικό πληροφορικής, χωρίς να διακόπτεται η λειτουργία τους, όπου αυτό είναι τεχνικά εφικτό ή σε ώρες χαμηλής χρήσης/κίνησης.

Γ. ΜΕΤΡΑ ΦΥΣΙΚΗΣ ΑΣΦΑΛΕΙΑΣ

1. Έλεγχος φυσικής πρόσβασης

Α) Φυσική πρόσβαση σε εγκαταστάσεις και computerroom
Στους χώρους που βρίσκεται κεντρικός υπολογιστικός και δικτυακός εξοπλισμός (συμπεριλαμβανομένης της δικτυακής καλωδίωσης) εφαρμόζονται κατάλληλα μέτρα ελέγχου φυσικής πρόσβασης, έτσι ώστε να επιτρέπεται η πρόσβαση μόνο σε κατάλληλα εξουσιοδοτημένο προσωπικό, για παράδειγμα χώροι που βρίσκεται περιφερειακός δικτυακός ενεργητικός και παθητικός εξοπλισμός πρέπει να είναι μόνιμα κλειδωμένοι.

Στις περιπτώσεις των Κέντρων Δεδομένων (Datacenters) και των Κέντρων Δικτύων (Networkcenters), λόγω της φύσης του εξοπλισμού, των δεδομένων και των υπαρχόντων κινδύνων, είναι απαραίτητο να ελέγχεται και να καταγράφεται κάθε πρόσβαση στους συγκεκριμένους χώρους.

Β) Τήρηση καταλόγου
Διατηρείται με ευθύνη του διοικητικά και τεχνικά υπεύθυνου επικαιροποιημένος κατάλογος με τα δικαιώματα φυσικής πρόσβασης του προσωπικού καθώς και με το προσωπικό που διαθέτει κωδικούς, κάρτες εισόδου και κλειδιά για πρόσβαση σε χώρους που λειτουργεί ο κεντρικός υπολογιστικός και δικτυακός εξοπλισμός και οι κτιριακοί κατανεμητές δικτύου. Οι κατάλογοι αυτοί υπόκεινται σε τακτική αναθεώρηση.

2. Περιβαλλοντική ασφάλεια

Α) Προστασία από φυσικές καταστροφές
Πρέπει να λαμβάνονται τα κατάλληλα μέτρα για την προστασία των κτιρίων, των κρίσιμων χώρων, των computerrooms, των γραφείων του προσωπικού, 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, σεισμός, έκρηξη, διαρροή νερού, διακοπή ρεύματος, διάρρηξη/κλοπή, βανδαλισμός, κ.λπ.

Ενδεικτικά μέτρα που πρέπει να τηρούνται προς αυτή την κατεύθυνση είναι τα εξής: συναγερμός, πόρτες και παράθυρα ασφάλειας, πυροπροστασία, απομάκρυνση εξοπλισμού από υδροσωληνώσεις και πηγές σκόνης, ανιχνευτές υγρασίας και πλημμύρας, αδιάλειπτη παροχή ρεύματος μέσω σταθεροποιητών/γεννητριών, κ.λπ.

3. Έκθεση εγγράφων

Α)Τοποθέτηση φακέλων
Οι φάκελοι που περιέχουν προσωπικά δεδομένα (φυσικό αρχείο) πρέπει να είναι τοποθετημένοι σε φοριαμούς που να μπορεί να κλειδώνουν και να μην εκτίθενται σε κοινή θέα.

Β) Μεταφοράφακέλων
Θα πρέπει να καταγράφεται η μεταφορά των φυσικών φακέλων σε διαφορετικά γραφεία ή σε άλλες υπηρεσιακές μονάδες.

Γ)Cleandeskpolicy
Δεν θα πρέπει να αφήνονται εκτεθειμένα, χωρίς επίβλεψη, έγγραφα και φορητά μέσα αποθήκευσης πάνω σε γραφεία.

Δ)Συσκευές αναπαραγωγής εγγράφων
Λοιπές συσκευές που δύναται να χρησιμοποιηθούν για υποκλοπή ή για την έκθεση προσωπικών δεδομένων σε κοινή θέα, όπως φωτοαντιγραφικά, συσκευές fax, εκτυπωτές, κ.λπ. θα πρέπει να προστατεύονται κατάλληλα.

4. Προστασία φορητών μέσων αποθήκευσης

Α)Ασφάλεια φορητών μέσων
Πρέπει να λαμβάνονται τα κατάλληλα μέτρα για τη φυσική ασφάλεια και προστασία των φορητών αποθηκευτικών μέσων - όπως να φυλάσσονται σε ασφαλή σημεία όταν δεν είναι σε χρήση και να είναι πάντα υπό επίβλεψη κατά τη διάρκεια της χρήσης τους.

Δ. ΜΕΤΡΑ ΑΝΑΚΑΜΨΗΣ ΑΠΟ ΚΑΤΑΣΤΡΟΦΕΣ

Για την προστασία των προσωπικών δεδομένων σε περίπτωση κάποιου έκτακτου περιστατικού, όπως φυσικές καταστροφές (π.χ. σεισμός, πυρκαγιά, πλημμύρα) ή μεγάλης εμβέλειας περιστατικά ασφάλειας (π.χ. καταστροφή από ιομορφικό λογισμικό) είναι απαραίτητη η λειτουργία κατάλληλα διαμορφωμένου κεντρικού υπολογιστικού και δικτυακού εξοπλισμού σε εναλλακτική εγκατάσταση (χώρο). Σε αυτό το χώρο θα γίνει ανάκαμψη και αποκατάσταση των κρίσιμων πληροφοριακών συστημάτων του Πανεπιστημίου σε περιπτώσεις έκτακτης ανάγκης.

Για την ταχύτερη δυνατή αντιμετώπιση των έκτακτων περιστάσεων στους χώρους λειτουργίας της κρίσιμης υπολογιστικής και δικτυακής υποδομής (π.χ. σεισμός, πυρκαγιά, πλημμύρα, κλοπή), είναι απαραίτητα:

1. να υπάρχουν συσκευές ή μέθοδοι που ελέγχουν τη θερμοκρασία, την πίεση, την υγρασία και άλλους περιβαλλοντικούς παράγοντες. Παραδείγματα είναι τα κλιματιστικά, οι ελεγκτές υγρασίας και οι ιονιστές της ατμόσφαιρας.
2. η τοποθέτηση συναγερμών, οι οποίοι χρησιμοποιούνται τόσο για την ανίχνευση (επικείμενης) ζημιάς λόγω των φαινομένων αυτών, αλλά και για την ανίχνευση εισβολών στα συστήματα.

3. η τοποθέτηση πυροσβεστήρων, ειδικών αφρών, ειδικών χρηματοκιβωτίων για την αποθήκευση σπουδαίων εγγράφων, αντιγράφων ασφάλειας και άλλων σημαντικών αντικειμένων, και εγκαταστάσεις αποθήκευσης νερού, οι οποίες να έχουν και δυνατότητες άντλησης.
4. η χρήση ups και ειδικών γεννητριών, για την αδιάλειπτη παροχή ηλεκτρικής ενέργειας στον εξοπλισμού.

III. Πλάνο υλοποίησης των μέτρων ασφάλειας

Περιγράφονται τα μέτρα ασφάλειας τα οποία πρέπει άμεσα να εφαρμόσουν οι αρμόδιες υπηρεσιακές μονάδες του Πανεπιστημίου σε σχέση με τα κενά ασφάλειας που έχουν εντοπιστεί για καθεμία από τις κατηγορίες μέτρων ασφάλειας που αναφέρονται παραπάνω. Επίσης συμπεριλαμβάνεται το χρονοδιάγραμμα υλοποίησης των νέων αυτών μέτρων ασφάλειας που πρέπει να εφαρμοστούν. Μετά την υλοποίηση και εφαρμογή τους, το σχέδιο ασφάλειας επικαιροποιείται.

Α1) Ορισμός Υπεύθυνου Ασφάλειας

Τα καθήκοντα του Υπεύθυνου Ασφάλειας σε σχέση με την παρακολούθηση της υλοποίησης των μέτρων ασφάλειας από τις υπηρεσιακές μονάδες του Πανεπιστημίου και μέχρι τον ορισμό Υπεύθυνου Ασφάλειας από το Πανεπιστήμιο αναλαμβάνει επιτροπή η οποία ενημερώνει Πρύτανη σε τακτική βάση. Στην επιτροπή συμμετέχουν οι Προϊστάμενοι των Γενικών Διευθύνσεων, οι Προϊστάμενοι των Αυτοτελών Διευθύνσεων, οι Προϊστάμενοι των αυτοτελών Τμημάτων Πληροφορικής και ο Υπεύθυνος Προστασίας Προσωπικών Δεδομένων.

Α2) Οργάνωση/Διαχείριση προσωπικού

Οι υπεύθυνοι των υπηρεσιακών μονάδων φροντίζουν ώστε στις συμβάσεις τους με συνεργάτες/προμηθευτές να συμπεριληφθούν σαν παράρτημα, όπου είναι εφικτό, όροι εμπιστευτικότητας και μη αποκάλυψης ευαίσθητων πληροφοριών, όροι προστασίας της ιδιωτικότητας των φυσικών προσώπων και όροι για ασφάλεια των πληροφοριών. [Διάρκεια 2 μήνες, Υλοποίηση έως 31.08.2019].

Α3) Διαχείριση πληροφοριακών αγαθών

Δημιουργείται το μητρώο των πληροφοριακών και επικοινωνιακών υποδομών, των συστημάτων του λογισμικού καθώς και των κατηγοριών αρχείων και δεδομένων των κεντρικών οργανικών μονάδων με ευθύνη του Υπεύθυνου Ασφάλειας και σε συνεργασία με τον διοικητικό υπεύθυνο κάθε υπηρεσιακής μονάδας που διαθέτει και λειτουργεί υποδομή πληροφορικής και δικτύων. [Με ευθύνη του διοικητικά υπεύθυνου της κάθε υπηρεσιακής μονάδας καθορίζονται και καταγράφονται οι διαδικασίες για την ορθή οργάνωση/αρχειοθέτηση/ταξινόμηση του φυσικού αρχείου.
Προσδιορίζεται από το αρμόδιο τμήμα: λίστα μεταφορέων για την αποστολή εντύπων και μέσων αποθήκευσης με διαβαθμισμένες πληροφορίες (προσωπικά δεδομένα ειδικού σκοπού)και οι ειδικών προδιαγραφών φάκελοι και πακέτα.

Σε κάθε τμήμα που διακινεί προσωπικά δεδομένα δημιουργούνται δύο λίστες καταγραφής (πρωτόκολλα) που ενημερώνονται με ευθύνη του διοικητικά υπεύθυνου, μία για τα δεδομένα ειδικού σκοπού και μία για τις υπόλοιπες πληροφορίες. [Άμεσα]

Στους υπολογιστές του προσωπικού θα πρέπει να εγκατασταθεί κατάλληλο πρόγραμμα κρυπτογράφησης αρχείων (Για τον σκοπό αυτό, θα μπορούσαν να χρησιμοποιηθούν τα προγράμματα WinZip, 7zip (για τα Windows) ή iZip, keka (MacOS). Στην περίπτωση των εγγράφων MS-Office, Open-office ή Libre-Office μπορεί να χρησιμοποιηθεί η build-in λειτουργικότητα κρυπτογράφησης που παρέχεται (στην λειτουργία SaveAs και κλειδώματος με κωδικό).

Α4) Εκτελούντες την επεξεργασία

Οι διοικητικά υπεύθυνοι των υπηρεσιακών μονάδων πρέπει να ενημερώσουν τον ΥΠΔ διαβιβάζοντας λίστα με τους εκτελούντες την επεξεργασία προσωπικών δεδομένων με τους οποίους συνεργάζονται στα πλαίσια σύμβασης.

Α7) Εκπαίδευση προσωπικού

Διοργανώνεται άμεσα εκπαίδευση, που πρέπει να παρακολουθήσει το σύνολο του προσωπικού και στην συνέχεια οι νέο-προσλαβανόμενοι, που θα καλύπτει κατ' ελάχιστο την εκπαίδευση των χρηστών σε θέματα ασφάλειας, για την οποία πρέπει κατά το δυνατόν να διασφαλισθεί ότι είναι πλήρως κατανοητές από όλους.
Ο Υπεύθυνος Ασφάλειας αναλαμβάνει την υποχρέωση να ενημερώνει την πανεπιστημιακή κοινότητα μέσω λίστας ηλεκτρονικού ταχυδρομείου για σημαντικά θέματα ασφάλειας και κινδύνους που εμφανίζονται στο διαδίκτυο. [Άμεσα]

Β1) Έλεγχος πρόσβασης

Οι υπεύθυνοι των πληροφοριακών συστημάτων και εφαρμογών πρέπει . :

- να ελέγξουν το συστήματα διαχείρισης χρηστών που χρησιμοποιούν και να αξιολογήσουν τεχνικά και οργανωτικά την σύνδεση με την κεντρική υπηρεσία ταυτοποίησης και εξουσιοδότησης χρηστών (shibboleth).
- να ερευνήσουν την αξιοπιστία του συστήματος εξουσιοδοτήσεων χρηστών που χρησιμοποιούν και να ανακαθορίσουν τα δικαιώματα πρόσβασης των λογαριασμών σε προγράμματα όπου απαιτείται
- να ενσωματώσουν όπου είναι τεχνικά εφικτό την πολιτική διαχείρισης συνθηματικών
- να φροντίσουν για την καταγραφή των επιτυχημένων και οι αποτυχημένων προσπαθειών σύνδεσης των χρηστών

Οι υπεύθυνοι των προσωπικών υπολογιστών που επεξεργάζονται προσωπικά δεδομένα πρέπει να φροντίσουν ώστε να ενεργοποιείται ο screensaverμε passwordμετά από 10' αδράνειας

Β2) Αντίγραφα Ασφάλειας

Οι υπεύθυνοι των κεντρικών κρίσιμων πληροφοριακών και δικτυακών πόρων (πληροφοριακά συστήματα, εφαρμογές, βάσεις δεδομένων, υπολογιστικά και δικτυακά συστήματα, αρχεία, δεδομένα αρχείων χρηστών, αρχεία καταγραφής- logfiles) συντάσσουν και εφαρμόζουν συγκεκριμένη πολιτική λήψης αντιγράφων ασφάλειας η οποία διαβιβάζεται στον Υπεύθυνο Ασφάλειας για έλεγχο και περαιτέρω ενέργειες. **Β3) Διαμόρφωση προσωπικών υπολογιστών**

Πρέπει να δημιουργηθεί με ευθύνη των αρμόδιων τμημάτων υποδομή activedirectory,με σύνδεση στον κεντρικό Ldap, στην οποία θα ενταχθούν σταδιακά οι προσωπικοί υπολογιστές του προσωπικού των διοικητικών μονάδων.
Το υπεύθυνο προσωπικό πληροφορικής σε κάθε τμήμα **ελέγχει** εάν στους υπολογιστές της ευθύνης του

- λειτουργεί antiviruskαι firewall, εάν αυτά είναι ενημερωμένα και εάν εγκαθίστανται τακτικά οι ενημερώσεις ασφάλειας (windowsupdate)
- οι χρήστες συνδέονται με απλούς λογαριασμούς και όχι με διαχειριστικούς
- είναι εγκατεστημένο το προβλεπόμενο λογισμικό/εφαρμογές

Με ευθύνη των αρμόδιων τμημάτωνεγκαθίσταται στους υπολογιστές που τηρούν ή επεξεργάζονται ευαίσθητες πληροφορίες ή προσωπικά δεδομένα λογισμικό προστασίας τελικού σημείου (Endpoint Protection) και αυτό παραμετροποιείται κεντρικά για την αποτελεσματική λειτουργία του.

Με ευθύνη των αρμόδιων τμημάτων εγκαθίσταται στους υπολογιστές που τηρούν ή επεξεργάζονται προσωπικά δεδομένα και κυρίως δεδομένα ειδικών κατηγοριών λογισμικό ελέγχου, εντοπισμού και παρεμπόδισης μη εξουσιοδοτημένων/λανθασμένων ενεργειών διακίνησης/μεταφοράς πληροφοριών (DLP) και αυτό παραμετροποιείται κεντρικά για την αποτελεσματική λειτουργία του.

Β5) Ασφάλεια επικοινωνιών

Με βάση την πραγματοποιηθείσα Αξιολόγηση Επικινδυνότητας και σε πρώτη προτεραιότητα όλες οι κρίσιμες κεντρικές υποδομές σε επίπεδο εξυπηρετητών και προσωπικών υπολογιστών πρέπει να τεθούν σε συγκεκριμένες ζώνες ασφάλειας και να προστατευθούν από τις ήδη υπάρχουσες συσκευές ολοκληρωμένης προστασίας απειλών (UTM). Επιπλέον οι σταθμοί εργασίας των διοικητικών υπηρεσιών να συνδεθούν στο διαδίκτυο μέσω μηχανισμού NAT (NetworkAddressTranslation) και όχι μέσω PublicIpaddress

Θα πρέπει να γίνει εγκατάσταση ή αναβάθμιση υπηρεσίας VPN υψηλής απόδοσης και να διερευνηθεί η χρήση μηχανισμού 2FA (TwoFactorAuthentication). Θα πρέπει να εξεταστεί η αναγκαιότητα ευρείας πρόσβασης από τους υπολογιστές των διοικητικών υπηρεσιών σε υπηρεσίες κοινωνικής δικτύωσης και αποθήκευσης/διαμοιρασμού αρχείων λαμβάνοντας υπόψη τον υψηλό κίνδυνο διαρροής σε προσωπικά δεδομένα. Συγκεκριμένα προτείνεται να τροποποιηθεί η πολιτική σε πλήρη απαγόρευση της πρόσβασης στις εν λόγω υπηρεσίες από τμήματα που επεξεργάζονται προσωπικά δεδομένα (ειδικών κατηγοριών) ή ευαίσθητες πληροφορίες και αυτή να επιτρέπεται μετά από αίτημα της αρμόδιας υπηρεσιακής μονάδας προς τον Υπεύθυνο Ασφάλειας.

Με ευθύνη του αρμόδιου τμήματος θα πρέπει να επιλεχθεί και να εγκατασταθεί κεντρικά το κατάλληλο λογισμικό συλλογής και καταγραφής συμβάντων (όπως, KiwiSyslog Server, Splunk, κλπ), Επίσης προτείνεται η επιλογή και η αξιοποίηση σύγχρονου λογισμικού ενιαίας συσχέτισης συμβάντων ασφάλειας και διαχείριση κινδύνων (SIEM

Β6) Αρχεία σε αποσπώμενα μέσα αποθήκευσης και στο δίκτυο

Το υπεύθυνο προσωπικό πληροφορικής σε κάθε τμήμαπου υποστηρίζει τεχνικά **ελέγχει** εάν :

- στους υπολογιστές λειτουργεί λογισμικό κρυπτογράφησης όπως 7zip (για τα Windows) και φροντίζει για την εγκατάστασή του. [Διάρκεια 1 μήνας, Υλοποίηση έως 31.07.2019]
- εργαζόμενοι έχουν ανάγκη κοινής χρήσης αρχείων ή καταλόγων (folders) με ευαίσθητες πληροφορίες και εγκαθιστά λογισμικό κρυπτογράφησης στους υπολογιστές τους με αυτά τα ειδικά τεχνικά χαρακτηριστικά.

Με ευθύνη των αρμόδιων τμημάτων εγκαθίσταται στους υπολογιστές που τηρούν ή επεξεργάζονται προσωπικά δεδομένα και κυρίως δεδομένα ειδικών κατηγοριών λογισμικό κρυπτογράφησης (EndpointEncryption) του οποίου η λειτουργία καθορίζεται από κεντρική πολιτική προστασίας και εκπαιδεύεται σε αυτό ο χρήστης.

Με ευθύνη των αρμόδιων τμημάτων πρέπει να εγκατασταθεί και παραμετροποιηθεί κεντρικό σύστημα δικτυακών δίσκων (NAS) το οποίο θα παρέχει υπηρεσίες δικτυακών πόρων αποθήκευσης (προσωπικούς και κοινόχρηστους δικτυακούς δίσκους) στους χρήστες των διοικητικών υπηρεσιών. Το σύστημα NAS θα συνδεθεί στην υπό ανάπτυξη υποδομή activedirectory μαζί με τους προσωπικούς υπολογιστές του διοικητικού προσωπικού.

Β7) Ασφάλεια λογισμικού

Τα πληροφοριακά συστήματα και οι εφαρμογές, θα πρέπει με ευθύνη των υπευθύνων και σε συνεργασία με το Υπεύθυνο Ασφάλειας, να ελεγχθούν ως προς τους μηχανισμούς προστασίας των πληροφοριών και προσωπικών δεδομένων που διαθέτουν και στην περίπτωση μη ικανοποιητικής υλοποίησης πρέπει να καθοριστούν και προγραμματισθούν οι απαραίτητες ενέργειες αύξησης του επιπέδου της παρεχόμενης ασφάλειας.

Οι υπηρεσιακές μονάδες που αναλαμβάνουν την εσωτερική ανάπτυξη εφαρμογών θα πρέπει να μεριμνήσουν για την δημιουργία και συντήρηση περιβάλλοντος προγραμματισμού και να ακολουθούν συγκεκριμένη μεθοδολογία προγραμματισμού υποστηριζόμενη από τα κατάλληλα εργαλεία. [Διάρκεια 3 μήνες,

Θα πρέπει να προγραμματιστούν άμεσα από το αρμόδιο προσωπικό οι διαδικασίες αναβάθμισης υπολογιστών και εξυπηρετητών των οποίο το λογισμικό δεν υποστηρίζεται ήδη ή θα σταματήσει να υποστηρίζεται εντός του 2020. Συγκεκριμένα θα πρέπει να αναβαθμιστούν οι

προσωπικοί υπολογιστές με windows 7 και οι εξυπηρετητές με Centos 5 και 6, Windows 2008, SQL Server 2008.

Γ1) Έλεγχος φυσικής πρόσβασης

Καταγράφεται το προσωπικό που έχει πρόσβαση σε χώρους που λειτουργεί κεντρικός υπολογιστικός και δικτυακός εξοπλισμός, καθώς επίσης και τα μέτρα που λαμβάνονται για την προστασία των εν' λόγω χώρων και διαβιβάζονται από τον διοικητικά υπεύθυνο στον υπεύθυνο ασφάλειας.
Οι διοικητικά υπεύθυνοι ελέγχουν τους χώρους που διατηρούν ηλεκτρονικά και φυσικά αρχεία με προσωπικά δεδομένα και σε συνεργασία με τον Υπεύθυνο Ασφάλειας εισηγούνται μέτρα προς την αρμόδια υπηρεσία σχετικά με συστήματα/φωριαμούς αρχειοθέτησης και προστασίας φακέλων, συναγερμός, πόρτες και παράθυρα ασφάλειας, πυροπροστασία, απομάκρυνση εξοπλισμού από υδροσωληνώσεις και πηγές σκόνης, ανιχνευτές υγρασίας και πλημμύρας, αδιάλειπτη παροχή ρεύματος μέσω σταθεροποιητών/γεννητριών, κ.λπ

]Δ) <u>ΜΕΤΡΑ ΑΝΑΚΑΜΨΗΣ ΑΠΟ ΚΑΤΑΣΤΡΟΦΕΣ</u>

Το προσωπικό των αρμόδιων τμημάτων με χρήση του διαθέσιμου υπολογιστικού και δικτυακού εξοπλισμού σε συνδυασμό με το κατάλληλο λογισμικό πρέπει να ξεκινήσει η διαμόρφωση εναλλακτικού χώρου (hotsite) που σε περίπτωση έκτακτης ανάγκης θα λειτουργήσουν, έστω προσωρινά, τα κρίσιμα πληροφοριακά συστήματα και υπηρεσίες του Πανεπιστημίου.

Σε πρώτη φάση θα γίνει η επιλογή του κατάλληλου χώρου, η διαμόρφωσή του, και στην συνέχεια θα μεταφερθεί σε αυτόν ο διαθέσιμος εξοπλισμός κατάλληλα διαμορφωμένος σε επίπεδο υλικού και λογισμικού. Σε περίπτωση ελλείψεων πρέπει να προγραμματισθούν άμεσα οι απαραίτητες ενέργειες.

Πολιτική Προστασίας Προσωπικών Δεδομένων των Εργαζομένων

Σύνταξη: Υπεύθυνος Προστασίας Δεδομένων (DPO)

Έγκριση: Πρύτανης

Το Πανεπιστήμιο και σύμφωνα με τα οριζόμενα στον Γενικό Κανονισμό (ΕΕ) 2016/679 και τις διατάξεις του Ν. 4624/2019 και στο πλαίσιο της προστασίας των δεδομένων προσωπικού χαρακτήρα των εργαζομένων (Διδακτικό και Εκπαιδευτικό εν γένει Προσωπικό και Υπάλληλοι) και της σύννομης και ορθής επεξεργασίας τους. Στο πλαίσιο αυτό, το Πανεπιστήμιο επεξεργάζεται τα εν λόγω προσωπικά δεδομένα για τους εξής σκοπούς:

- Κατάρτιση Πράξης πρόσληψης και Σύμβασης διδασκόντων
  - Εισαγωγή στοιχείων σύμβασης και οικονομικών στοιχείων στο Υπουργείο Εργασίας, Κοινωνικής Ασφάλισης και Πρόνοιας
  - Ανάρτηση συμβάσεων στο "Διαύγεια"
  - Επαλήθευση γνησιότητας εγγράφων
- Διαχείριση υπεύθυνων δηλώσεων και βεβαιώσεων πολυθεσίας μελών ΔΕΠ
  - Αποστολή συγκεντρωτικών στοιχείων πρόσθετων αμοιβών στο Ελεγκτικό Συνέδριο
- Προσλήψεις διδασκόντων με το Π.Δ. 407/80 (αξιολόγηση υποψηφίων)
- Έκδοση βεβαιώσεων προϋπηρεσίας διδασκόντων
- Διαχείριση διακοπής/ λήξης σύμβασης διδακτικού προσωπικού
  - Έκδοση βεβαίωσης εργοδότη, βεβαίωσης απόλυσης
- Χορήγηση αναρρωτικών αδειών
- Διαχείριση εργαζομένων
- Διαχείριση συνταξιοδότησης εργαζομένου και Δελτίου Ατομικής και Υπηρεσιακής Κατάστασης
- Διαχείριση προσωπικού που μισθοδοτείται από το Ελληνικό Δημόσιο
- ***Αξιολόγηση υπαλλήλων του Πανεπιστημίου***
- Διαχείριση πληρωμών/Διαχείριση μισθοδοσίας (τακτικής και έκτακτης)
- ***Διαδικασία Αξιολόγησης μελών Δ.Ε.Π***
- Διαχείριση ιδρυματικού αποθετηρίου
- Διαχείριση κινητικότητας φοιτητών και προσωπικού (ERASMUS)
- Ενημέρωση και προβολή των δράσεων του Πανεπιστημίου
- Εκπόνηση ερευνητικού προγράμματος

Τα προσωπικά δεδομένα που συλλέγονται για τους ως άνω σκοπούς, όπως αυτοί αποτυπώνονται και στο Αρχείο Δραστηριοτήτων Επεξεργασίας που τηρεί και που συλλέγονται και τυγχάνουν επεξεργασίας. **Οι εν** λόγω

επεξεργασίες βασίζονται είτε στη νομιμοποιητική βάση της εκτέλεσης σύμβασης, είτε στη συμμόρφωση με έννομη υποχρέωση.

Τα εν λόγω προσωπικά δεδομένα δεν υποβάλλονται σε περαιτέρω επεξεργασία πέραν των ως άνω ορισμένων σκοπών, ενώ είναι κατάλληλα, συναφή και περιορίζονται στα ελάχιστα απαραίτητα για τους σκοπούς επεξεργασίας. Υπόκεινται σε νόμιμη επεξεργασία σύμφωνα με τα δικαιώματα των φυσικών προσώπων, είναι ακριβή και επικαιροποιούνται, όταν απαιτείται και ειδικά πριν τη λήψη κρίσιμων αποφάσεων για τα φυσικά πρόσωπα,

- δεν τηρούνται για χρονικό διάστημα μεγαλύτερο από αυτό που απαιτείται για το σκοπό της επεξεργασίας ή/ και για τη συμμόρφωση του Πανεπιστημίου με νομικές και κανονιστικές υποχρεώσεις,
- διατηρούνται ασφαλή από μη εξουσιοδοτημένη πρόσβαση, απώλεια ή καταστροφή,
- **διαβιβάζονται σε τρίτους μόνο υπό την προϋπόθεση ότι εξασφαλίζεται επαρκές επίπεδο προστασίας αυτών, και πάντοτε υπό την προϋπόθεση ότι η αρμόδια για την διαβίβαση Δ/νση ή Υπηρεσία , διαθέτει την έγγραφη συναίνεση του Υπευθύνου Προστασίας Δεδομένων, ή και στην περίπτωση κατά την οποία τούτο δεν καθίσταται δυνατόν θα πρέπει ο Υ.Π.Δ να έχει ενημερωθεί προηγουμένως για τον σκοπό και τους λόγους της επεξεργασίας ή της διαβίβασης.**

Η Διευθύνσεις του Πανεπιστημίου καθώς και όλα τα αρμόδια Τμήματα, σε συνεργασία με τον Υπεύθυνο Προστασίας Δεδομένων μεριμνούν για την υπογραφή Συμβάσεων Εμπιστευτικότητας (NDA) με τους εργαζόμενους, σε όποιες περιπτώσεις απαιτείται, ή την περίληψη στις συμβάσεις όρων που σχετίζονται με την προστασία των προσωπικών δεδομένων. Οι όροι αυτοί περιλαμβάνουν:

- **Περιγραφή των σκοπών επεξεργασίας με ξεκάθαρο τρόπο για την εκτέλεση της σύμβασης**
- **Καθορισμός των υπευθυνοτήτων και των ορίων ευθύνης των δύο μερών**
- **Περιγραφή του τρόπου και του είδους των προσωπικών δεδομένων που διαχειρίζονται**
- **Περιγραφή των τρόπων κοινοποίησης περιστατικών ασφάλειας**

Οι Διευθύνσεις και όλα τα Τμήματα του Πανεπιστημίου, τηρούν τα άκρως απαραίτητα δεδομένα μετά την αποχώρηση ενός εργαζομένου, φοιτητή η συναλλασσόμενου για τους σκοπούς που έχει ενημερώσει τον εργαζόμενο.

Το Πανεπιστήμιο δεσμεύεται για την αδιάλειπτη παρακολούθηση και τήρηση του κανονιστικού και νομοθετικού πλαισίου και για τη συνεχή εφαρμογή και βελτίωση της αποτελεσματικότητας των Πολιτικών και Διαδικασιών που υιοθετούνται για την προστασία των προσωπικών δεδομένων.

Ο Πρύτανης

Καθηγητής Τριαντάφυλλος Α.Δ. Αλμπάνης

Προστασία προσωπικών δεδομένων σε πρακτικές διοικητικών διαδικασιών, υγείας και ασφάλειας

Σύνταξη: **Υπεύθυνος Προστασίας Δεδομένων**

Έγκριση: **Πρυτανικό- Συμβούλιο Σύγκλητος**

Σκοπός

Η οδηγία περιγράφει και ενημερώνει συνοπτικά τους εργαζόμενους (διοικητικό και εκπαιδευτικό προσωπικό) για τον τρόπο με τον οποίο πρέπει να χειρίζονται τα προσωπικά δεδομένα, συμπεριλαμβανομένων και δεδομένων ειδικών κατηγοριών (κυρίως δεδομένων υγείας), τα οποία επεξεργάζονται.

Οι εργαζόμενοι του Πανεπιστημίου λαμβάνουν υπόψιν τις παρακάτω οδηγίες για την προστασία των προσωπικών δεδομένων σε πρακτικές υγείας και ασφάλειας:

Σύμφωνα με τα οριζόμενα στο άρθρο 39 ΓΚΠΔ , στα άρθρα 7 και 8 Ν.4624/2019 αλλά και σύμφωνα με τις σχετικές οδηγίες και Αποφάσεις της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), και σε ότι αφορά σε <u>όλα ανεξαιρέτως τα αιτήματα τρίτων</u> που λαμβάνουν οι φορείς του Δημοσίου Τομέα, για χορήγηση δημοσίων εγγράφων του αρθ. 5 (Κωδ. Διοικ. Δ), είτε πρόκειται για «απλά» δεδομένα, είτε για ειδικές κατηγορίες, αρμόδιος να αποφανθεί επί του εννόμου συμφέροντος του αιτούντος, είναι ο Υ.Π.Δ του φορέα.

- οι υπάλληλοι που τηρούν ιατρικό ιστορικό είτε εργαζομένων, είτε φοιτητών, κλπ του Πανεπιστημίου θα πρέπει να ενημερώνονται για την υποχρέωση εχεμύθειας που απορρέει από τον Υπαλληλικό Κώδικα και ενδεχομένως από Κώδικα Δεοντολογίας βάσει του επαγγέλματός τους (π.χ. Κοινωνικοί Λειτουργοί). Σε περιπτώσεις τρίτων θα πρέπει να ακολουθείται η "Πολιτική Συνεργατών Πανεπιστημίου".

- η επεξεργασία προσωπικών δεδομένων ειδικής κατηγορίας από το Πανεπιστήμιο στηρίζεται είτε στην νομιμοποιητική βάση σχετικά με σκοπούς προληπτικής ή επαγγελματικής ιατρικής, εκτίμησης της ικανότητας προς εργασία του εργαζομένου, ιατρικής διάγνωσης, παροχής υγειονομικής ή κοινωνικής περίθαλψης ή θεραπείας ή διαχείρισης υγειονομικών και κοινωνικών συστημάτων και υπηρεσιών βάσει δικαίου ή δυνάμει σύμβασης με επαγγελματία του τομέα της υγείας με υποχρέωση επαγγελματικού απορρήτου, είτε στην εκτέλεση υποχρεώσεων ή άσκησης δικαιωμάτων του Υπεύθυνου Επεξεργασίας ή του φυσικού προσώπου, στο πλαίσιο του εργατικού δικαίου και του δικαίου κοινωνικής ασφάλισης και κοινωνικής προστασίας είτε για σκοπούς δημοσίου συμφέροντος.

- κατά τη διαβίβαση δεδομένων ειδικής κατηγορίας σε άλλες Διευθύνσεις/ Τμήματα του Πανεπιστημίου, ο αρμόδιος υπάλληλος φροντίζει για την τήρηση της αρχής της ελαχιστοποίησης, διαβιβάζοντας στην άλλη Υπηρεσιακή Μονάδα μόνο τα απολύτως απαραίτητα δεδομένα που απαιτούνται για την εκτέλεση της εργασίας του.

- δεν αναρτώνται στη Διαύγεια πράξεις οι οποίες εμπεριέχουν δεδομένα υγείας, σύμφωνα με τις υποδείξεις του ν. 3861/2010. Ακόμη, στις περιπτώσεις που γίνεται ανάρτηση σχετικών πράξεων, το Πανεπιστήμιο λαμβάνει κατάλληλα μέτρα προστασίας, όπως είναι η χρήση των αρχικών των ονοματεπωνύμων, για την προστασία των προσωπικών δεδομένων.
- δεν χορηγούνται έγγραφα που εμπεριέχουν προσωπικά δεδομένα σε τρίτους (π.χ. συγγενείς φυσικών προσώπων) χωρίς την επίδειξη έγγραφης εξουσιοδότησης επικυρωμένης από ΚΕΠ.
  Στοιχεία δεδομένων προσωπικού χαρακτήρα , είτε αφορούν στο υποκείμενο των δεδομένων, είτε σε τρίτο, χορηγούνται αποκλειστικά και μόνο κατόπιν εγγράφου αιτήματος και εφόσον στοιχειοθετείται το έννομα συμφέρον του αιτούντος. Σε περίπτωση αμφισβητήσεως του εννόμου συμφέροντος , το αίτημα διαβιβάζεται στην Υπεύθυνη Προστασίας Δεδομένων του Πανεπιστημίου.
- παρέχεται στα φυσικά πρόσωπα μέσω όλων των εντύπων συλλογής προσωπικών δεδομένων η απαραίτητη πληροφόρηση για την επεξεργασία των προσωπικών τους δεδομένων .
- λαμβάνονται τα κατάλληλα μέτρα προστασίας των προσωπικών δεδομένων που βρίσκονται σε ηλεκτρονική και έντυπη μορφή.
- Το Πανεπιστήμιο συλλέγει για διάφορες δράσεις μόνο τα ελάχιστα και τα απολύτως απαραίτητα στοιχεία δεδομένων προσωπικού χαρακτήρα των φυσικών προσώπων, όπως αυτά ορίζονται τόσο στον Κανονισμό (ΕΕ) 2016/679, όσο και στον Ν. 4624/2019.

Πολιτική Συνεργατών Πανεπιστημίου

Σύνταξη: Υπεύθυνος Προστασίας Δεδομένων (DPO)

Έγκριση: Πρυτανικό Συμβούλιο

Η παρούσα πολιτική περιγράφει τη δέσμευση του Πανεπιστημίου ως προς τη διαχείριση των συνεργατών του, έτσι ώστε να διασφαλίζεται το μέγιστο επίπεδο προστασίας των προσωπικών δεδομένων, στα οποία οι συνεργάτες έχουν πρόσβαση στο πλαίσιο της συμβατικής τους σχέσης με το Πανεπιστήμιο. Παρακάτω περιγράφονται οι απαιτήσεις του Πανεπιστημίου από τους συνεργάτες του αναφορικά με την προστασία των προσωπικών δεδομένων, οι όροι για τη δέουσα επιμέλεια των προσωπικών δεδομένων, ειδικοί όροι για παρόχους υπηρεσιών cloud και άρθρα για την αντιμετώπιση περιπτώσεων μη συμμόρφωσης με τους όρους.

Α. Απαιτήσεις από τους συνεργάτες για την Προστασία των Προσωπικών Δεδομένων κατά την εκτέλεση συμβάσεων ή συμφωνιών

Το Πανεπιστήμιο Ιωαννίνων και σύμφωνα με τα οριζόμενα στον Γενικό Κανονισμό (ΕΕ) 2016/679 και στο πλαίσιο της προστασίας των δεδομένων προσωπικού χαρακτήρα των φυσικών προσώπων, αποδέκτες των οποίων γίνονται σε ορισμένες περιπτώσεις συνεργάτες/ προμηθευτές του Π.Ι, τους δεσμεύει για την τήρηση των απαιτούμενων όρων προστασίας προσωπικών δεδομένων, εφαρμόζοντας τα εξής:

Ο Δ/ντης και οι Προϊστάμενοι των υπηρεσιακών μονάδων του Πανεπιστημίου ή η Διεύθυνση Οικονομικών Υπηρεσιών - Τμήμα Προμηθειών που διαχειρίζονται τα θέματα νέων συνεργασιών με προμηθευτές πληροφορούν τον Υπεύθυνο Προστασίας Δεδομένων (DPO) πριν τη συνεργασία με τρίτο μέρος που περιλαμβάνει επεξεργασία προσωπικών δεδομένων

Οι περιπτώσεις συνεργασίας με τρίτο μέρος κυρίως αφορούν:

- δεδομένα προσωπικού χαρακτήρα φυσικών προσώπων για τα οποία το τρίτο μέρος αποτελεί Υπεύθυνο Επεξεργασίας ή Εκτελών την Επεξεργασία των δεδομένων και των σκοπών της επεξεργασίας αυτών,
- αναγνώρισης ανάγκης λήψης τρίτου μέρους για διενέργεια συγκεκριμένης δραστηριότητας από το αρμόδιο τμήμα,
- διενέργεια επεξεργασίας από κοινού με τρίτο μέρος σε δεδομένα προσωπικού χαρακτήρα φυσικών προσώπων για τα οποία το Πανεπιστήμιο αποφασίζει από κοινού με το τρίτο μέρος,
- αλλαγή νομοθεσίας
- ανανέωση σύμβασης ή τροποποίηση σύμβασης.

Στην περίπτωση που κριθεί ότι το τρίτο μέρος θα αποτελέσει συνεργάτη του Πανεπιστημίου ακολουθούνται συνδυαστικά η παρούσα πολιτική με τη συνήθη διαδικασία διαχείρισης συμβάσεων του Πανεπιστημίου.

- Ο Υπεύθυνος Προστασίας Δεδομένων (DPO) σε συνεργασία με τους Επικεφαλής αρμόδιων Διευθύνσεων/Τμημάτων του Πανεπιστημίου ή/ και τη Διεύθυνση Οικονομικών Υπηρεσιών - Τμήμα Προμηθειών συντάσσουν για κάθε νέα σύμβαση ή συμφωνία με συνεργάτη/ προμηθευτή του Πανεπιστημίου τους όρους για τον προσδιορισμό των θεμάτων της επεξεργασίας, όπως και αποτυπώνονται ακολούθως.

- Για την σύνταξη της σύμβασης ή συμφωνίας ελέγχεται πάντα ο ρόλος του τρίτου μέρους ως προς την επεξεργασία.
- Για τις ισχύουσες συμβάσεις ή συμφωνίες, το Πανεπιστήμιο καταρτίζει παράρτημα όρων επεξεργασίας προσωπικών δεδομένων, το οποίο δίδεται στα συμβαλλόμενα τρίτα μέρη προς υπογραφή.
- **Ο Υπεύθυνος Προστασίας Δεδομένων (DPO) επικαιροποιεί τους όρους των συμβάσεων ή συμφωνιών όταν κρίνεται απαραίτητο.**

Β. Όροι για τη δέουσα επιμέλεια σχετικά με την Προστασία Προσωπικών Δεδομένων για τους προμηθευτές ως εκτελούντες την επεξεργασία

Οι όροι που θα πρέπει να περιλαμβάνονται, όλοι ή μερικοί ανάλογα την περίπτωση, σε κάθε σύμβαση ή συμφωνία με τον εκτελούντα την επεξεργασία είναι οι ακόλουθοι:

- Ο καθορισμός των ρόλων του Πανεπιστημίου και του τρίτου μέρους (Υπεύθυνος Επεξεργασίας, Εκτελών την Επεξεργασία, Υπο-εκτελών την Επεξεργασία), των κατηγοριών επεξεργασίας που θα διενεργούνται από το τρίτο μέρος και τα φυσικά πρόσωπα και τα προσωπικά τους δεδομένα.
- **Η επεξεργασία των προσωπικών δεδομένων γίνεται μόνο βάσει οδηγιών και κατευθύνσεων του Πανεπιστημίου και μόνο για τους σκοπούς που αυτό έχει ορίσει.**
- **Λίστα των τεχνικών και οργανωτικών μέτρων που λαμβάνει το εκάστοτε τρίτο μέρος (εκτελών την επεξεργασία) για τη διασφάλιση της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των δεδομένων.**
- Όροι εχεμύθειας/ τήρησης εμπιστευτικότητας, με τους οποίους δεσμεύονται και οι υπάλληλοι του τρίτου μέρους (εκτελών την επεξεργασία) που επεξεργάζονται προσωπικά δεδομένα.
- **Το τρίτο μέρος που επεξεργάζεται δεδομένα για λογαριασμό του Πανεπιστημίου (εκτελών την επεξεργασία) δεν επιτρέπεται να αναθέσει μέρος ή συνολικά τις κατηγορίες επεξεργασίας σε τρίτο, χωρίς προηγούμενη γραπτή άδεια από το Πανεπιστήμιο.**
- ***Τα προσωπικά δεδομένα που έχει ο εκτελών την επεξεργασία στην κατοχή του, θα πρέπει να διαγράφονται ή να παραδίδονται στο Πανεπιστήμιο κατά τη λήξη της συνεργασίας μαζί του.***
- ***Σε περίπτωση συμβάντος παραβίασης προσωπικών δεδομένων το οποίο γίνεται αντιληπτό από τον εκτελούντα την επεξεργασία, θα πρέπει να ενημερώνει άμεσα το Πανεπιστήμιο με λεπτομέρειες για τη φύση του περιστατικού, πιθανές αιτίες, όγκο δεδομένων και φυσικών προσώπων που επηρεάζονται, μέτρα που ελήφθησαν ή θα ληφθούν κ.λπ. Πιο συγκεκριμένα, καθορίζεται ο τρόπος ενημέρωσης για τη γνωστοποίηση και το χρονικό διάστημα εντός του οποίου είναι απαραίτητο να ενημερώνεται το Πανεπιστήμιο.***
- Το τρίτο μέρος (εκτελών την επεξεργασία) θέτει στη διάθεση του Πανεπιστημίου κάθε πληροφορία προς απόδειξη της συμμόρφωσης της με τον Ευρωπαϊκό Κανονισμό GDPR. Παράλληλα, επιτρέπει και διευκολύνει τους ελέγχους από το Πανεπιστήμιο ή άλλον ελεγκτή εντεταλμένο από το Πανεπιστήμιο.
- Το τρίτο μέρος (εκτελών την επεξεργασία) επικουρεί το Πανεπιστήμιο με τα κατάλληλα τεχνικά και οργανωτικά μέτρα για την εκπλήρωση της υποχρέωσής του να απαντά σε αιτήματα άσκησης δικαιωμάτων του υποκειμένου των δεδομένων.

- Στις περιπτώσεις που διενεργείται διαβίβαση σε Τρίτη χώρα στο πλαίσιο της συνεργασίας, τις κατάλληλες εγγυήσεις για τη διαβίβαση δεδομένων σε Τρίτη χώρα που έχουν επιλεγεί από τα άρθρα 44 έως 49 του ΓΚΠΔ.

Γ. Όροι για τη δέουσα επιμέλεια σχετικά με την Προστασία Προσωπικών Δεδομένων για τους συνεργάτες που είναι από κοινού Υπεύθυνοι Επεξεργασίας με το Πανεπιστήμιο.

Οι όροι που θα πρέπει να περιλαμβάνει κατ' ελάχιστον στο κείμενο της σύμβασης/ συμφωνίας ή του παραρτήματος είναι οι ακόλουθοι (όλοι ή μερικοί ανάλογα την περίπτωση):

- Αναφορά σε όλες τις επεξεργασίες που θα διενεργηθούν στο πλαίσιο της σύμβασης και των δεδομένων που αφορούν και προϋποθέσεις για καταγραφή/ τεκμηρίωση αλλαγών σε αυτά.
- Καθορισμός του ρόλου επεξεργασίας των Από κοινού Υπευθύνων Επεξεργασία και τα όρια των ευθυνών κάθε συμβαλλόμενου μέρους (συμπεριλαμβανομένων ευθυνών για την πληροφόρηση, συγκατάθεση και άσκηση αιτημάτων των φυσικών προσώπων). Στο σημείο αυτό σημειώνεται κι ο τρόπος πληροφόρησης των φυσικών προσώπων των ρόλων αυτών και ευθυνών που διέπουν τη σύμβαση.
- Καθορισμός της νομιμοποιητικής βάσης για τη νόμιμη επεξεργασία των δεδομένων προσωπικού χαρακτήρα, για κάθε σκοπό επεξεργασίας.
- Το σημείο επικοινωνίας που θα τίθεται στη διάθεση των φυσικών προσώπων για επικοινωνία σχετικά με την επεξεργασία. (DPO)
- Όρος για την άμεση ενημέρωση των δύο μερών σε περίπτωση περιστατικού παραβίασης δεδομένων προσωπικού χαρακτήρα, σύμφωνα με τους μηχανισμούς που θα αποφασίσουν από κοινού για την ενημέρωση. Οι μηχανισμοί αυτοί μπορεί να αναφέρονται περιληπτικά σε Παράρτημα της σύμβασης/ συμφωνίας.
- Όρος που προβλέπει ότι τα μέρη δεν αναθέτουν μέρος ή το σύνολο των σε τρίτο, χωρίς προηγούμενη ειδική ή γενική γραπτή άδεια του άλλου μέρους.
- Όροι όπου θα καθορίζουν τους χρόνους ή/ και τα κριτήρια διατήρησης και διαγραφής των δεδομένων από τα συστήματα των δύο μερών. Θα πρέπει να είναι σαφές ότι η διαγραφή αφορά το σύνολο των δεδομένων, για κάθε μορφή (έγχαρτη και ηλεκτρονική) και για κάθε τοποθεσία (παραγωγικές βάσεις δεδομένων, περιβάλλον ελέγχων δοκιμών, αποθηκευτικά συστήματα (storage), αντίγραφα ασφαλείας κ.λπ.).
- Όρος για τον προσδιορισμό της αυτοματοποιημένης επεξεργασίας, σε περίπτωση που διενεργείται στο πλαίσιο της σύμβασης, και πιθανών αποφάσεων που λαμβάνονται βάσει αυτής, συμπεριλαμβανομένης της δημιουργίας προφίλ του φυσικού προσώπου, και των σχετικών απαιτήσεων που προέρχονται από τη Νομοθεσία σχετική με την προστασία προσωπικών δεδομένων.
- Όρος για τη λήψη τεχνικών και οργανωτικών μέτρων από τα μέρη για τη διασφάλιση της προστασίας των δεδομένων προσωπικού χαρακτήρα.
- Τα στοιχεία επικοινωνίας των Υπεύθυνων Προστασίας Δεδομένων και από τα δύο μέρη.

Οι όροι που θα πρέπει να περιλαμβάνει κατ' ελάχιστον στο κείμενο της σύμβασης/ συμφωνίας ή του παραρτήματος με αποδέκτες δεδομένων είναι οι ακόλουθοι:

- Τα στοιχεία επικοινωνίας των Υπεύθυνων Προστασίας Δεδομένων και από τα δύο μέρη.

Δ. Ειδικοί όροι για τους παρόχους cloud

Για τη συμμόρφωση με τα κριτήρια ή άλλες απαιτήσεις Ασφάλειας Πληροφοριών μέσω των οποίων προστατεύονται τα προσωπικά δεδομένα των φυσικών προσώπων, το Πανεπιστήμιο πρέπει να ορίσει τα εξής:

- Εφαρμογή πιστοποιημένου Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών ISO 27001:2013 από την πλευρά του παρόχου που να καλύπτει τις σχετικές με το αντικείμενο των υπηρεσιών δραστηριότητες. Σε κάθε περίπτωση θα πρέπει να καλύπτονται θέματα διαχείρισης των περιστατικών ασφάλειας (Information securityincidentmanagement).
- Υλοποίηση και εφαρμογή του ISO 27017:2015 – cloudsecurity
- Να διαθέτει υποδομές για την επεξεργασία των δεδομένων εντός Ευρωπαϊκής Ένωσης
- Η Σύμβαση με τον πάροχο να περιέχει κατάλληλους όρους εχεμύθειας, τεχνικών και οργανωτικών μέτρων για την προστασία των προσωπικών δεδομένων
- Χρήση από τον πάροχο όρων εμπιστευτικότητας/ εχεμύθειας στις συμβάσεις εργασίας με το προσωπικό του ή υπογραφή ξεχωριστού Non-disclosureagreement (NDA)
- Παροχή κρυπτογραφημένων καναλιών επικοινωνίας (https, vpn) για την μεταφορά ευαίσθητων πληροφοριών από και προς την υπηρεσία
- Ύπαρξη τεχνικών μέτρων για την προστασία των ευαίσθητων πληροφοριών και προσωπικών δεδομένων όταν βρίσκονται αποθηκευμένα στις cloud υποδομές του παρόχου (για παράδειγμα η παροχή δυνατοτήτων κρυπτογράφησης της αποθηκευμένης πληροφορίας, ο έλεγχος δικαιωμάτων και προσβάσεων, η δυνατότητα δημιουργίας και ασφαλούς αποθήκευσης καταγραφών (auditlogs) κ.α.)
- Το προσωπικό του παρόχου έχει λάβει εκπαιδεύσεις σχετικά με την προστασία προσωπικών δεδομένων, όπως και σε τεχνολογίες και πρακτικές ασφάλειας πληροφοριών.
- Εφαρμόζονται ειδικότερες τεχνικές απαιτήσεις όπως η ενσωμάτωση ελέγχων ασφάλειας στον κύκλο ζωής των παρεχόμενων cloud υπηρεσιών (vulnerabilityassessments, penetrationtesting κ.λπ.)
- Εξασφάλιση της διαθεσιμότητας των προσωπικών δεδομένων σε περίπτωση καταστροφικού συμβάντος η διακοπή υπηρεσίας στις υποδομές του παρόχου.
- Ύπαρξη κατάλληλων προδιαγραφών επιπέδων υπηρεσιών και ανάκαμψης από καταστροφή.

Δ. Θέματα τεκμηρίωσης και αξιολόγησης προμηθευτών

Κατά την επιλογή του συνεργάτη το Πανεπιστήμιο μπορεί να ζητήσει τεκμήρια για την απόδειξη συμμόρφωσης του συνεργάτη με το εθνικό και ευρωπαϊκό νομοθετικό πλαίσιο. Ενδεικτικά, αναφέρονται:

- Ύπαρξη ορισμένου Υπεύθυνου Προστασίας Δεδομένων (ΥΠΔ)
- Ύπαρξη ορισμένου Υπεύθυνου Ασφάλειας Πληροφοριών
- Ύπαρξη Πολιτικής Προστασίας Προσωπικών Δεδομένων
- Ύπαρξη Πολιτικής Ασφάλειας Πληροφοριών
- Ύπαρξη Πολιτικής Επιχειρησιακής Συνέχειας
- Διαδικασία εκπαίδευσης/ ευαισθητοποίηση προσωπικού για θέματα προστασίας προσωπικών δεδομένων

- Τήρηση Αρχείου Δραστηριοτήτων Επεξεργασίας
- Διαδικασία διενέργειας Μελέτη Εκτίμησης Αντικτύπου (DPIA) για επεξεργασίες δεδομένων προσωπικού χαρακτήρα που σχετίζονται με τις υπηρεσίες που παρέχει
- Διαδικασία για την ικανοποίηση των δικαιωμάτων (πρόσβαση, διαγραφή, τροποποίηση κ.λπ.) των φυσικών προσώπων τα οποία προωθούνται από το Πανεπιστήμιο
- Ύπαρξη όρων εμπιστευτικότητας με τους οποίους δεσμεύεται το προσωπικό του
- Διαδικασία για τη γνωστοποίηση περιστατικών παραβίασης προσωπικών δεδομένων
- Τήρηση - Επικαιροποίηση Συστήματος Διαχείρισης Προσωπικών Δεδομένων
- Τήρηση -Επικαιροποίηση Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών και σχετική πιστοποίησή του
- Τήρηση -Επικαιροποίηση Συστήματος Διαχείρισης Επιχειρησιακής Συνέχειας και σχετική πιστοποίησή του
- Τήρηση -Επικαιροποίηση Σχεδίου Ανάκαμψης από Καταστροφή (DisasterRecoveryPlan) και Χώρου Ανάκαμψης από Καταστροφή (DisasterRecoverySite)
- Ύπαρξη διαβιβάσεων εκτός της Ε.Ε. και των εγκεκριμένων χωρών (όπως αυτές αναφέρονται στην ιστοσελίδα της Ευρωπαϊκής Επιτροπής), στο πλαίσιο των παρεχόμενων υπηρεσιών
- Συμμόρφωση με κλαδικό κώδικα δεοντολογίας για την τήρηση του ΓΚΠΔ
- ***Τήρηση της αρχής εξ' ορισμού πρόσβαση σε δεδομένα προσωπικού χαρακτήρα αποκλειστικά από το αρμόδιο προσωπικό.***

Με την ολοκλήρωση της υπογραφής της σύμβασης, οι επικεφαλής των αρμόδιων διευθύνσεων/τμημάτων σε συνεργασία με τον Υπεύθυνο Προστασίας Δεδομένων (ΥΠΔ) ενημερώνουν αντίστοιχα το έντυπο «Αρχείο Δραστηριοτήτων Επεξεργασίας» με τα στοιχεία του τρίτου μέρους στην αντίστοιχη δραστηριότητα επεξεργασίας.

Επιπλέον, στην περίπτωση που το τρίτο μέρος αποτελεί Εκτελούντα ή Υπο-Εκτελούντα την Επεξεργασία για λογαριασμό του Πανεπιστημίου με την ολοκλήρωση της υπογραφής της σύμβασης, η Διεύθυνση Οικονομικής Διαχείρισης – Τμήμα Προμηθειών ενημερώνει το έντυπο «Μητρώο Εκτελούντων την Επεξεργασία» με τα απαραίτητα στοιχεία της σύμβασης και σε συνεργασία με τους Επικεφαλής των Διευθύνσεων/Τμημάτων έχει την ευθύνη να το κρατά επικαιροποιημένο μετά από αλλαγές (εισαγωγές, διαγραφές τρίτων μερών κ.λπ.). Το Μητρώο είναι διαθέσιμο σε όλους όσους έχουν αρμοδιότητα διαχείρισης συνεργατών, προμηθευτών κ.λπ. ή για κάποιο άλλο λόγο θα πρέπει να λάβουν γνώση.

Περιοδικά (τουλάχιστον μια φορά το έτος ή σε σημαντικές αλλαγές), η Διεύθυνση Οικονομικής Διαχείρισης – Τμήμα Προμηθειών σε συνεργασία με τον Υπεύθυνο Προστασίας Δεδομένων (ΥΠΔ), προβαίνουν σε ανασκόπηση των όρων των συμβάσεων με τα τρίτα μέρη, ώστε να περιλαμβάνονται όλοι οι απαραίτητοι όροι.

Σε περίπτωση που το τρίτο μέρος αποτελεί Εκτελούντα ή Υπο-εκτελούντα την Επεξεργασία το Πανεπιστήμιο μπορεί να προβεί και στην επαναξιολόγησή του με την αναζήτηση τεκμηρίων για την ικανοποίηση των συμβατικών απαιτήσεων.

Επιπρόσθετα, το Πανεπιστήμιο έχει τη δυνατότητα να ζητήσει και να διενεργήσει επιθεώρηση για την εφαρμογή τεχνικών και οργανωτικών μέτρων για την προστασία των προσωπικών δεδομένων του

Πανεπιστημίου ή τόσο από τους κύριους προμηθευτές, όσο και από τους υπό-προμηθευτές και υπεργολάβους τους.

Στόχος της περιοδικής ανασκόπησης των συνεργασιών είναι να διασφαλιστεί τουλάχιστον, σε συμβατικό επίπεδο, η λήψη τεχνικών και οργανωτικών μέτρων προστασίας των δεδομένων προσωπικού χαρακτήρα από τα τρίτα μέρη του Πανεπιστημίου.

Αντίστοιχη περιοδική ανασκόπηση διενεργείται από το Τμήμα Προμηθειών του ΕΛΚΕ για τις συμβάσεις που διαχειρίζεται.

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΠΑΝΕΠΙΣΤΗΜΙΟ ΙΩΑΝΝΙΝΩΝ

Διαχείριση Αρχείου Δραστηριοτήτων Επεξεργασίας

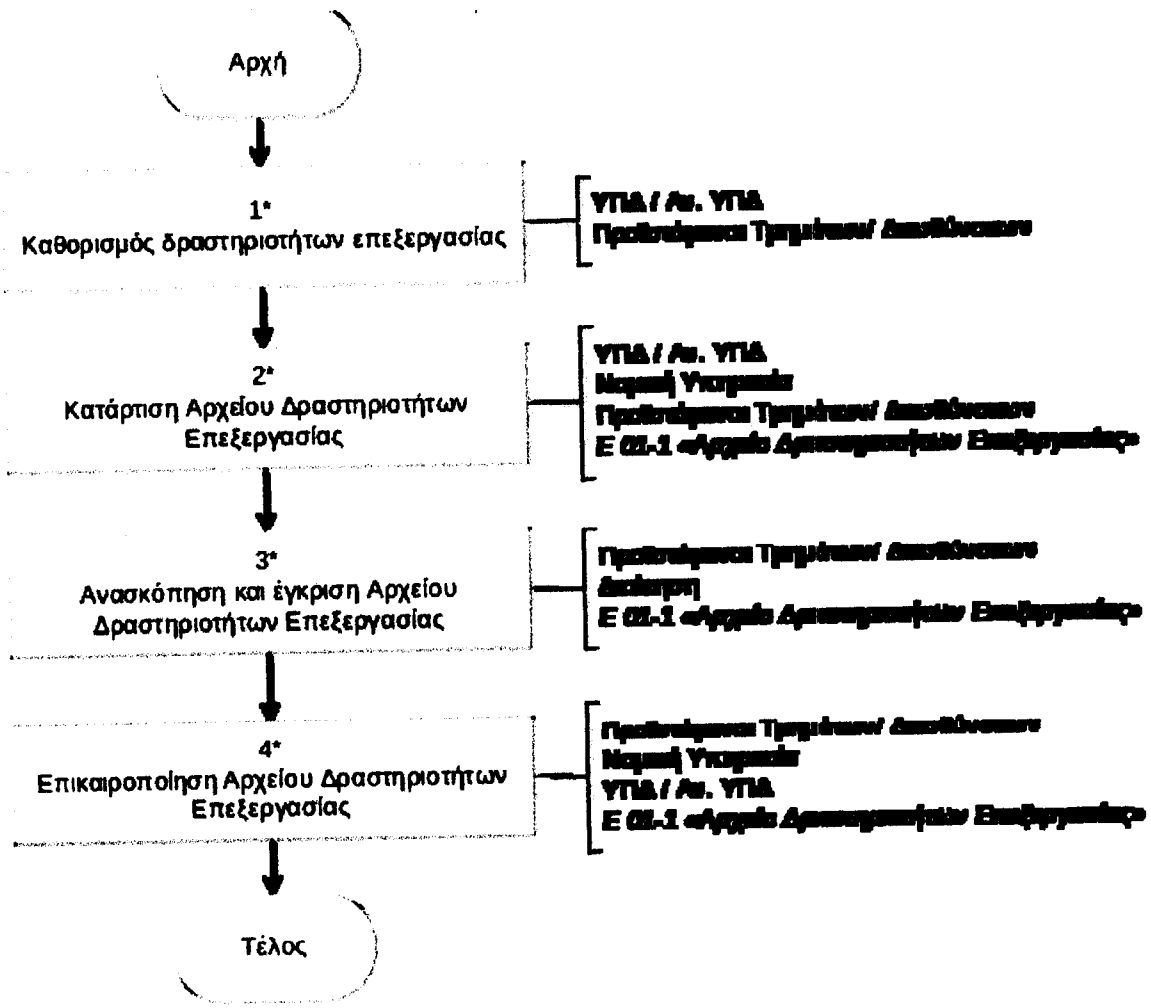
Σύνταξη: Υπεύθυνος Προστασίας Δεδομένων (ΥΠΔ)

Έγκριση:

Σκοπός

Η διαδικασία προσδιορίζει τον τρόπο με τον οποίο γίνεται ο καθορισμός των δραστηριοτήτων του Πανεπιστημίου που περιλαμβάνουν επεξεργασία δεδομένων προσωπικού χαρακτήρα, η κατάρτιση του σχετικού αρχείου δραστηριοτήτων επεξεργασίας και η τακτική και συστηματική επικαιροποίηση του.

Μέθοδος



Ανάλυση

Φάση 1: Ο Υπεύθυνος Προστασίας Δεδομένων του Πανεπιστημίου, σε συνεργασία με τους Προϊσταμένους των Τμημάτων/ Διευθύνσεων, αναγνωρίζει και καταγράφει το σύνολο των δραστηριοτήτων του Πανεπιστημίου που περιλαμβάνουν επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Φάση 2: Με ευθύνη του Υπεύθυνου Προστασίας Δεδομένων καταρτίζεται το έντυπο Ε 01-1 «Αρχείο Δραστηριοτήτων Επεξεργασίας», το οποίο τηρείται σε ηλεκτρονική μορφή και περιλαμβάνει τις διεργασίες στις οποίες γίνεται επεξεργασία δεδομένων προσωπικού χαρακτήρα και στο οποίο καθορίζεται ο σκοπός επεξεργασίας. Για κάθε δραστηριότητα περιγράφονται:

- Υπεύθυνη για την επεξεργασία οργανωτική μονάδα
- Σκοπός της επεξεργασίας
- Κατηγορίες δεδομένων προσωπικού χαρακτήρα.
- Κατηγορίες φυσικών προσώπων που αφορούν τα δεδομένα
- Νομιμοποιητική Βάση επεξεργασίας
- Τρόπος απόδειξης της συγκατάθεσης, σε περίπτωση που αποτελεί νομιμοποιητική βάση για την επεξεργασία
- Ρόλος του Πανεπιστημίου στην επεξεργασία (Υπεύθυνος Επεξεργασίας, Από Κοινού Υπεύθυνος)
- Πηγές λήψης των δεδομένων
- Αποδέκτες των δεδομένων (οργανωτικές μονάδες εντός του Πανεπιστημίου, τρίτα μέρη, από κοινού υπεύθυνοι επεξεργασίας, εκτελούντες την επεξεργασία, προμηθευτές)
- Κύρια συστήματα/ εφαρμογές καθώς και αποθηκευτικά μέσα που χρησιμοποιούνται για την επεξεργασία και την αποθήκευση των δεδομένων
- Διαβιβάσεις δεδομένων εκτός Ευρωπαϊκού Οικονομικού Χώρου (ΕΟΧ)
- Νομική βάση και κατάλληλες εγγυήσεις που λαμβάνονται σε περίπτωση διαβιβάσεων δεδομένων σε χώρες εκτός ΕΟΧ
- Χρόνος τήρησης ή κριτήρια που καθορίζουν την παύση της τήρησης των δεδομένων προσωπικού χαρακτήρα (π.χ. λήξη συνεργασίας με προμηθευτή του Πανεπιστημίου). Για τον καθορισμό του χρόνου τήρησης ακολουθείται η οδηγία Ο 01-1 «Καθορισμός χρόνων τήρησης προσωπικών δεδομένων».
- Γενική περιγραφή των λαμβανόμενων τεχνικών και οργανωτικών μέτρων.

Για κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα οι Προϊστάμενοι των Τμημάτων/ Διευθύνσεων και ο Υπεύθυνος Προστασίας Δεδομένων, συνεργάζονται για την ανάλυση και επιλογή μίας από τις ακόλουθες νομιμοποιητικές βάσεις επεξεργασίας:

- Η ρητή συγκατάθεση του φυσικού προσώπου για το συγκεκριμένο σκοπό ή τους συγκεκριμένους σκοπούς της επεξεργασίας
- Η υλοποίηση σύμβασης στην οποία το φυσικό πρόσωπο αποτελεί συμβαλλόμενο μέρος (ή πρόκειται να αποτελέσει) – με την έννοια της παροχής υπηρεσιών προς το φυσικό πρόσωπο, ακόμη και χωρίς να υπάρχει γραπτή σύμβαση
- Η συμμόρφωση με νομική ή κανονιστική απαίτηση, στην οποία υπόκειται το Πανεπιστήμιο
- Η προστασία των ζωτικών συμφερόντων του φυσικού προσώπου
- Η υλοποίηση εργασιών στο πλαίσιο του δημοσίου συμφέροντος ή κατ' εντολή κρατικής ή άλλης εποπτικής αρχής
- Το έννομο συμφέρον του Πανεπιστημίου ή τρίτου μέρους, εφόσον δεν αντίκειται στο συμφέρον ή στα θεμελιώδη δικαιώματα και τις ελευθερίες του φυσικού προσώπου.

Στην περίπτωση επεξεργασίας ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα, εκτός της ανωτέρω νομιμοποιητικής βάσης, θα πρέπει επιπρόσθετα να επιλέγεται και να αναλύεται τουλάχιστον μια από τις κάτωθι:

- ***Η ρητή συγκατάθεση του φυσικού προσώπου για την επεξεργασία της ειδικής κατηγορίας***
- Η ικανοποίηση εργασιακών δικαιωμάτων ή υποχρεώσεων
- Η προστασία των ζωτικών συμφερόντων του φυσικού προσώπου
- Η εκούσια δημοσίευσή τους από το φυσικό πρόσωπο
- Η άσκηση ή υπεράσπιση νομικών αξιώσεων
- Η προάσπιση του δημόσιου συμφέροντος, της δημόσιας υγείας ή της επαγγελματικής εχεμύθειας
- Η αξιολόγηση της εργασιακής ικανότητας του φυσικού προσώπου
- Η παροχή υπηρεσιών υγείας και κοινωνικής αλληλεγγύης (π.χ. ασφαλιστικό/ συνταξιοδοτικό πρόγραμμα)

Ειδικότερα για τον καθορισμό του ρόλου του Πανεπιστημίου στην κάθε επεξεργασία ακολουθείται η Οδηγία Ο 01-2 «Καθορισμός ρόλου στην Επεξεργασία Προσωπικών Δεδομένων».

Φάση 3: Ο Υπεύθυνος Προστασίας Δεδομένων υποβάλλει το Αρχείο Δραστηριοτήτων Επεξεργασίας στους Προϊσταμένους των Τμημάτων/Διευθύνσεων του Πανεπιστημίου προς έλεγχο. Μετά την ανασκόπηση και την ενσωμάτωση ενδεχόμενων σχολίων και αλλαγών, το αρχείο εγκρίνεται από τη Σύγκλητο ή άλλο αρμόδιο διοικητικό όργανο του Πανεπιστημίου (Πρύτανης, Πρυτανικό).

Φάση 4: ***Οι Προϊστάμενοι των Τμημάτων/ Διευθύνσεων του Πανεπιστημίου φέρουν την ευθύνη για την ενημέρωση του Υπεύθυνου Προστασίας Δεδομένων για οποιαδήποτε αλλαγή επηρεάζει τα περιεχόμενα του Αρχείου Δραστηριοτήτων Επεξεργασίας, όπως***:

- Προσθήκη/ αφαίρεση/ μεταβολή δραστηριοτήτων στις οποίες πραγματοποιείται επεξεργασία δεδομένων προσωπικού χαρακτήρα
- Τροποποίηση των συστημάτων/ εφαρμογών/ αποθηκευτικών μέσων που χρησιμοποιούνται για την επεξεργασία και την αποθήκευση των δεδομένων
- Διαφοροποίηση στη διαβίβαση των δεδομένων εντός του Πανεπιστημίου και εκτός του Πανεπιστημίου (εντός και εκτός ΕΟΧ)
- Μεταβολή των κατηγοριών δεδομένων που τυγχάνουν επεξεργασίας ή/ και των κατηγοριών φυσικών προσώπων
- Αλλαγή του σκοπού επεξεργασίας ή της νομιμοποιητικής βάσης επεξεργασίας
- Αλλαγή στο νομοθετικό και κανονιστικό πλαίσιο, η οποία επηρεάζει το χρόνο τήρησης, τα λαμβανόμενα τεχνικά και οργανωτικά μέτρα ή τα είδη της επεξεργασίας.

Με μέριμνα του Υπεύθυνου Προστασίας Δεδομένων το έντυπο Ε 01-1 «Αρχείο Δραστηριοτήτων Επεξεργασίας» επικαιροποιείται κατάλληλα και υποβάλλεται προς ανασκόπηση από τους Προϊσταμένους των Τμημάτων/ Διευθύνσεων και τελική έγκριση από τη Σύγκλητο ή άλλο αρμόδιο διοικητικό όργανο του Πανεπιστημίου (Πρύτανης, Πρυτανικό). **Οι προηγούμενες εκδόσεις του Αρχείου Δραστηριοτήτων Επεξεργασίας διατηρούνται στο fileserver με μέριμνα του Υπεύθυνου Προστασίας Δεδομένων του Πανεπιστημίου, με κατάλληλη σήμανση της έκδοσης.**

Σε ετήσια βάση, υπό το συντονισμό του Υπεύθυνου Προστασίας Δεδομένων, προγραμματίζεται συνάντηση ανασκόπησης του Αρχείου Δραστηριοτήτων Επεξεργασίας, με τους διοικητικά υπεύθυνους των υπηρεσιακών μονάδων. προκειμένου να διασφαλιστεί ότι το αρχείο παραμένει έγκυρο και πλήρως επικαιροποιημένο.

Σχετικά Έγγραφα

Ο 01-1 «Καθορισμός χρόνου τήρησης προσωπικών δεδομένων»

Ο 01-2 «Καθορισμός ρόλου στην Επεξεργασία Προσωπικών Δεδομένων»

Αρχεία

τίτλος			χρόνος τήρησης	υπεύθυνος τήρησης
Ε 01-1 Αρχείο Δραστηριοτήτων Επεξεργασίας		✓	Επ' άπειρον	Υπεύθυνος Προστασίας Δεδομένων
Ε 01-2 Μητρώο χρόνων τήρησης και καταστροφής προσωπικών δεδομένων		✓	Επ' άπειρον	Υπεύθυνος Προστασίας Δεδομένων

ΔΗΛΩΣΗ ΕΝΗΜΕΡΩΣΗΣ ΕΠΕΞΕΡΓΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Προς
Την Γραμματεία
του Τμήματος .....
του Πανεπιστημίου Ιωαννίνων

Επώνυμο: .....

Όνομα: .....

Όν. Πατέρα: .....

Ημ/νία γέννησης: .....

Α.Δ.Τ.: .....

Κινητό: .....

Τόπος κατοικίας: .....

.....

Email: .....

Με την παρούσα δηλώνω ότι έχω ενημερωθεί ότι το Πανεπιστήμιο Ιωαννίνων συλλέγει και επεξεργάζεται τα δεδομένα προσωπικού χαρακτήρα τα οποία έχω υποβάλλει στο πλαίσιο της εγγραφής μου ,αποκλειστικά για τους σκοπούς της υλοποίησης της εγγραφής και της φοίτησής μου στο:

☐ Προπτυχιακό Πρόγραμμα Σπουδών

☐ Μεταπτυχιακό Πρόγραμμα Σπουδών:

☐ ΠΜΣ .....

☐ Πρόγραμμα Διδακτορικών Σπουδών

☐ Μεταδιδακτορική Έρευνα

ΚΑΝΟΝΙΣΜΟΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Η συλλογή και η επεξεργασία των δεδομένων σας γίνεται βάσει των διατάξεων των άρθρων 22,23,24,25,26, 27 και 30 Ν.4624/19 κατά περίπτωση, καθώς και των άρθρων 6 παρ. 1 περίπτωση (γ),(ε) και για τα προσωπικά δεδομένα ειδικών κατηγοριών 9 παρ. 2 (ζ) του Γενικού Κανονισμού(ΕΕ) 2016/679. Τα προσωπικά σας δεδομένα θα παραμείνουν στη διάθεση του Πανεπιστημίου Ιωαννίνων καθόλο το χρονικό διάστημα φοίτησης σας σε αυτό και στη συνέχεια θα διαγραφούν, εφόσον πληρούνται τα οριζόμενα στην παρ. 1 άρθρου 34 Ν.4624/2019.

Για το χρονικό διάστημα που τα προσωπικά σας δεδομένα θα παραμένουν στη διάθεση του Πανεπιστημίου Ιωαννίνων έχετε τη δυνατότητα να ασκήσετε τα δικαιώματα πρόσβασης, διόρθωσης, επικαιροποίησης, περιορισμού της επεξεργασίας, αντίταξης και φορητότητας σύμφωνα με τους όρους του Γενικού Κανονισμού Προστασίας Δεδομένων Προσωπικού Χαρακτήρα 2016/679 (Ε.Ε.) και τα οριζόμενα στα άρθρα 34 και 35 Ν. 4624/2019.

- Υπεύθυνος Επικοινωνίας για τα προσωπικά δεδομένα του Τμήματος ..... είναι ο/η κ. .....τηλ. 26510 0.....
- Υπεύθυνη Προσωπικών Δεδομένων Πανεπιστημίου Ιωαννίνων η κα. Σταυρούλα Σταθαρά, τηλ.: 26510-07321.

Ιωάννινα, ... 20.....

Ο / Η Αιτ.....

(υπογραφή)

ΔΗΛΩΣΗ ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑΣ

(ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2016/679, Ν.4624/2019)

Εχοντας υπόψη ότι το Πανεπιστήμιο Ιωαννίνων, στο πλαίσιο της άσκησης της ανατεθειμένης σε αυτό δημόσιας εξουσίας σύμφωνα με τα οριζόμενα στο άρθρο 6 παρ.1ε του ΓΚΠΔ και για τους σκοπούς αυτούς συλλέγει και επεξεργάζεται δεδομένα φυσικών προσώπων και φέρει την ιδιότητα του *Υπευθύνου Επεξεργασίας Προσωπικών Δεδομένων* σύμφωνα με τη νομοθεσία (Γενικός Κανονισμός Προστασίας Δεδομένων 2016/679/ΕΕ και Ν.4624/2019), καθώς τηρεί αρχεία και προβαίνει σε επεξεργασία[1] δεδομένων προσωπικού χαρακτήρα (*προσωπικών δεδομένων*)[2], καθορίζοντας το σκοπό και ορίζοντας τα μέσα της επεξεργασίας αυτών.

Αναλαμβάνω την υποχρέωση να αντιμετωπίζω ως εμπιστευτικές τις πληροφορίες που αφορούν φυσικά πρόσωπα (φοιτητές, εργαζομένους, προμηθευτές, συναλλασσομένους κάθε κατηγορίας με το Ιδρυμα) τις οποίες γνωρίζω ή/και στις οποίες αποκτώ πρόσβαση στο πλαίσιο της άσκησης των καθηκόντων που μου έχουν ανατεθεί ή και επ' ευκαιρία αυτών.

Αναλαμβάνω την υποχρέωση να προστατεύω και να διαφυλάττω τον απόρρητο χαρακτήρα των προσωπικών δεδομένων που τηρεί και επεξεργάζεται ο «υπεύθυνος επεξεργασίας» , ή οι προστηθέντες του ως «εκτελούντες επεξεργασία» σύμφωνα με τις εντολές και οδηγίες του.

Αναλαμβάνω την υποχρέωση να χρησιμοποιώ ή εν γένει να επεξεργάζομαι τα προσωπικά δεδομένα μόνο σύμφωνα με τις εντολές και υποδείξεις του «υπευθύνου επεξεργασίας» και του «ΥΠΔ, ή των προστηθέντων του και μόνο για τον σκοπό για τον οποίο γίνεται η εκάστοτε επεξεργασία. Δεν επιτρέπεται να προβαίνω σε κοινοποίηση, διαβίβαση ή καθ' οιονδήποτε άλλον τρόπο αποκάλυψη προσωπικών δεδομένων σε τρίτους, παρά μόνον εφόσον αυτό καθίσταται απολύτως απαραίτητο στο πλαίσιο της εκπλήρωσης των

---

[1] Ως *επεξεργασία προσωπικών δεδομένων* νοείται κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων σε προσωπικά δεδομένα ή σε σύνολα προσωπικών δεδομένων, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση, κάθε άλλης μορφής διάθεση, ο συσχετισμός ή συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή προσωπικών δεδομένων, είτε αυτά ευρίσκονται σε ηλεκτρονική μορφή (ηλεκτρονικό αρχείο) είτε σε έντυπη μορφή (φυσικό αρχείο).

[2] Ως δεδομένο προσωπικού χαρακτήρα ή *προσωπικό δεδομένο* νοείται κάθε πληροφορία που αφορά φυσικά πρόσωπα, η ταυτότητα των οποίων προσδιορίζεται ή μπορεί να προσδιορισθεί άμεσα ή έμμεσα, όπως για παράδειγμα το όνομα, ο αριθμός ταυτότητας ή διαβατηρίου, η διεύθυνση κατοικίας, η διεύθυνση ηλεκτρονικού ταχυδρομείου, τα επιγραμμικά αναγνωριστικά ταυτότητας (πχ.cookies, ip address), ή χαρακτηριστικά που προσδιορίζουν τη φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου, περιλαμβανομένης και της εικόνας ενός φυσικού προσώπου (φωτογραφικό υλικό, βίντεο).

ανατεθειμένων σε αυτόν καθηκόντων, η κατόπιν σχετικών οδηγιών του «υπευθύνου προστασίας δεδομένων»(σύμφωνα με τα οριζόμενα στο άρθ. 8 Ν.4624/2019) ή εφόσον απαιτείται από διάταξη νόμου.

Ως «*τρίτος*» νοείται κάθε φυσικό ή νομικό πρόσωπο, όπως –ενδεικτικά και όχι περιοριστικά- το κάθε είδους προσωπικό του ΝΠΔΙ, καθώς και οι κάθε είδους συναλλασσόμενοι με αυτό. Υποχρεούμαι να συμμορφώνομαι και να ακολουθώ τις εντολές, υποδείξεις και οδηγίες που έχω λάβει ειδικά από τον «υπεύθυνο επεξεργασίας και τον υπεύθυνο προστασίας δεδομένων» ή γνωρίζω λόγω της φύσης της εργασίας ή των καθηκόντων μου αναφορικά με τα μέτρα φυσικής, οργανωτικής και τεχνικής ασφάλειας για την προστασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των προσωπικών δεδομένων.

Υποχρεούμαι να ανακοινώνω στον «υπεύθυνο προστασίας δεδομένων (ΥΠΔ) του Π.Ι.» κ. Σταυρούλα Σταθαρά (τηλ: 26510-07321) οποιαδήποτε παραβίαση των κανόνων και οδηγιών επεξεργασίας προσωπικών δεδομένων ή παραβίαση της ασφάλειας αυτών[3] υποπέσει στην αντίληψή μου.

Ιωάννινα **Ο Δηλών/ουσα**

[3] Οπως η παραβίαση της ασφάλειας του φυσικού ή/και του ηλεκτρονικού αρχείου αλλά και κάθε παραβίαση, η οποία συνεπάγεται ή μπορεί να οδηγήσει σε τυχαία ή παράνομη καταστροφή , απώλεια, μεταβολή, άνευ αδείας κοινολόγηση ή πρόσβαση στα αρχεία προσωπικών δεδομένων.

.....

Μετά από αυτό, επειδή δεν υπάρχει άλλο θέμα λύεται η Συνεδρία και υπογράφεται το παρόν.

Ο ΠΡΥΤΑΝΗΣ ΤΑ ΜΕΛΗ

Ιωάννινα, 25 Μαΐου 2021
Για την ακρίβεια του αποσπάσματος
Ο
ΠΡΥΤΑΝΗΣ

Τριανταφυλλος Α.Χ. Αλιμπάνης

Αποδέκτες για ενέργεια:
-Υπηρεσία Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
Αποδέκτες για ενημέρωση:
-Γραμματείας Πρυτανείας
-Αντιπρυτάνεις
-Δ/νση Μηχανοργάνωσης & Δικτύων
-Ομάδα Υποστήριξης GDPR