# ΔΙΑΔΙΚΑΣΙΑ ΧΕΙΡΙΣΜΟΥ ΠΑΡΑΒΙΑΣΗΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

**Ιδιοκτήτης: Υπεύθυνη Προστασίας Δεδομένων**

**Εγκρίθηκε από: Διευθυντή Οικονομικών και Διοίκησης**

**Διευθυντή Πανεπιστημιούπολης**

**Ημερομηνία ελέγχου: Μάϊος 2020**

**Ιούνιος 2020**

# Περιεχόμενα

## 1. Πλαίσιο Εφαρμογής

Αυτή η διαδικασία ισχύει για όλο το Πανεπιστήμιο και για όλες τις πληροφορίες του Πανεπιστημίου, ανεξαρτήτως μορφής.

Ισχύει για όλο το προσωπικό, τους φοιτητές, τους επισκέπτες του Πανεπιστημίου και τους εξωτερικούς συνεργάτες του Πανεπιστημίου.

Οι ευθύνες των Υπεύθυνων Επεξεργασίας των δεδομένων που ενεργούν εκ μέρος του Πανεπιστημίου όσον αφορά τα περιστατικά/συμβάντα / περιστατικά περιγράφονται στο παρών κείμενο.

## 2. Ευθύνες

### 2.1 Χρήστες Πληροφοριών

Είναι ευθύνη όλων των χρηστών πληροφοριών να αναφέρουν γνήσια, πιθανά, ύποπτα περιστατικά παραβίασης Προστασίας Δεδομένων και να βοηθήσουν στις έρευνες ως απαιτείται, ειδικά εάν θα πρέπει να ληφθεί άμεση δράση για αποφυγή περαιτέρω ζημιάς.

### 2.2 Προϊστάμενοι Τμημάτων και Διευθυντές Τμημάτων

Οι προϊστάμενοι τμημάτων καθώς και οι Διευθυντές Τμημάτων θα πρέπει να διασφαλίζουν ότι οι υφιστάμενοι τους ακολουθούν την παρούσα διαδικασία και ότι θα προσφέρουν βοήθεια σε περίπτωση επακόλουθης έρευνας.

### 2.3 Προσωπικό Διαχείρισης Συμβάντων

Το προσωπικό του πανεπιστημίου το οποίο έχει συγκεκριμένες ευθύνες για τη λήψη αναφορών για περιστατικά/συμβάντα παραβίασης προστασίας προσωπικών δεδομένων, και για την έναρξη των ερευνών είναι:

α. Η Υπεύθυνη Προστασίας Δεδομένων (ΥΠΔ)

β. Ο Chief Information Officer (CIO)

γ. Ο Διευθυντής Πανεπιστημιούπολης

Οι αναφορές περιστατικών μπορεί να ληφθούν και να χειρισθούν περαιτέρω από το IT support και το IT management και staff.

### 2.4 Η Υπεύθυνη Προστασίας Δεδομένων (ΥΠΔ)

Η υπεύθυνη προστασίας δεδομένων είναι αποκλειστικά υπεύθυνη για να αποφασίσει εάν θα στείλει αναφορά στο Γραφείο Επιτρόπου Δεδομένων Προσωπικού Χαρακτήρα, εάν θα πρέπει να ενημερωθούν και άλλα μέρη, και για την κοινοποίηση των σχετικών πληροφοριών, όπως απαιτείται.

Η ΥΠΔ θα διατηρεί αρχείο με όλα τα περιστατικά/συμβάντα παραβίασης προστασίας προσωπικών δεδομένων ανεξάρτητα από το εάν το συμβάν θα αναφερθεί στο γραφείο της Επιτρόπου ως παραβίαση προσωπικών δεδομένων.

## 3. Διαχείριση Παραβιάσεων/ Ενημέρωση Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

**3.1** Τα περιστατικά/συμβάντα παραβίασης προστασίας προσωπικών δεδομένων πρέπει να αναφέρονται αμέσως και να κοινοποιούνται ακολουθώντας τις οδηγίες αναφοράς που αναφέρονται σε αυτήν τη διαδικασία:

● Τα περιστατικά πρέπει να αναφέρονται μέσω τηλεφώνου ή αφήνοντας ένα φωνητικό μήνυμα στο Γραφείο Υπεύθυνης Προστασίας Δεδομένων στο τηλέφωνο +357 26843346 ή στέλνοντας email στο dpo.nup@nup.ac.cy

Η ΥΠΔ θα παρακολουθεί αυτόν τον λογαριασμό και θα μεριμνά ώστε να ληφθούν τα κατάλληλα μέτρα μόλις ληφθεί μια αναφορά.

● Η έκθεση θα πρέπει να περιλαμβάνει πλήρεις και ακριβείς λεπτομέρειες του συμβάντος, συμπεριλαμβανομένων και πληροφοριών για το ποιος προβαίνει στη αναφορά και τι είδους προσωπικά δεδομένα αφορά. Ως μέρος της διαδικασίας το «Έντυπο Γνωστοποίησης Περιστατικών Παραβίασης Προσωπικών Δεδομένων» πρέπει να συμπληρωθεί (βλ. http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/page2g_gr/page2g_gr?opendocument).

● Μόλις αναφερθεί ένα περιστατικό/ συμβάν παραβίασης προστασίας δεδομένων, θα γίνει μια αρχική αξιολόγηση από την ΥΠΔ και/ή τον CIO και/ή τον Διευθυντή Πανεπιστημιούπολης και/ή τα αρμόδια στελέχη του Πανεπιστημίου για να διαπιστωθεί η αλήθεια της αναφοράς και η σοβαρότητα του συμβάντος. Αυτό στη συνέχεια θα καθορίσει την απόφαση σχετικά με το ποιος θα είναι ο άμεσα εμπλεκόμενος διαχειριστής του συμβάντος (βλ. Παράρτημα Α).

● Σύμφωνα με τα ευρήματα της συλλογής στοιχείων, η ΥΠΔ και/ή ο CIO και/ή ο Διευθυντής Πανεπιστημιούπολης και/ή τα αρμόδια στελέχη του Πανεπιστημίου αξιολογούν αν από το περιστατικό προκύπτουν κίνδυνοι για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων και αν απαιτείται να ενημερωθεί η Επίτροπος Προστασίας Δεδομένων

Προσωπικού Χαρακτήρα. Σύμφωνα με το άρθρο 33, ο Υπεύθυνος Επεξεργασίας θα πρέπει να γνωστοποιήσει την παραβίαση, εκτός αν η παράβαση είναι απίθανο να οδηγήσει σε κίνδυνο για τα δικαιώματα και τις ελευθερίες των ατόμων.

● Ο Υπεύθυνος Επεξεργασίας ενημερώνει την Επίτροπο Προστασίας Δεδομένων Προσωπικού Χαρακτήρα αμελλητί μέσα σε χρονικό διάστημα 72 ωρών από τη στιγμή που αποκτά γνώση του γεγονότος της παραβίασης των προσωπικών δεδομένων, εκτός αν έχει αξιολογηθεί ότι το περιστατικό δεν αποτελεί κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Ο Υπεύθυνος Επεξεργασίας είναι υπεύθυνος για την παροχή κατ' ελάχιστο των ακόλουθων πληροφοριών στην Επίτροπο:

▪ Περιγραφή της φύσης της παραβίασης και πιθανές επιπτώσεις του περιστατικού

▪ Κατηγορίες και κατά προσέγγιση αριθμό των υποκειμένων των δεδομένων που επηρεάζονται από το περιστατικό

▪ Κατηγορίες προσωπικών δεδομένων και αριθμός επηρεαζόμενων αρχείων που περιέχουν προσωπικά δεδομένα

▪ Ενδεχόμενες συνέπειες της παραβίασης

▪ Μέτρα που έχουν ληφθεί ή που έχουν προταθεί άμεσα να υλοποιηθούν με σκοπό την αντιμετώπιση του περιστατικού παραβίασης ή/ και τον περιορισμό των επιπτώσεών του

▪ Όνομα και στοιχεία επικοινωνίας της ΥΠΔ ή/ και άλλου προσώπου που μπορεί να παρέχει πληροφορίες.

Αν η γνωστοποίηση στην εποπτική αρχή δεν πραγματοποιηθεί εντός 72 ωρών, πρέπει να συνοδεύεται από αιτιολόγηση για την καθυστέρηση σύμφωνα με το άρθρο 33 παράγραφος 1 ΓΚΠΔ.

**3.2** Εάν το περιστατικό/ συμβάν παραβίασης προστασίας δεδομένων έχει στοιχεία ασφαλείας IT - για παράδειγμα, λογαριασμός χρήστη διακυβεύτηκε ως μέρος μιας καμπάνιας ηλεκτρονικού ψαρέματος (phishing) - το Γραφείο Εξυπηρέτησης του Πανεπιστημίου πρέπει επίσης να ειδοποιηθεί, δηλώνοντας σαφώς ότι αυτό σχετίζεται με ένα περιστατικό προστασίας δεδομένων.

**3.3** Η διαχείριση παραβιάσεων έχει τέσσερα κρίσιμα στοιχεία

● **Περιορισμός και ανάκτηση**

Ο στόχος είναι να περιοριστεί όσο το δυνατόν περισσότερο η ζημιά.

● **Αξιολόγηση των συνεχιζόμενων κινδύνων**

Η αξιολόγηση θα συμβάλει στην καθοδήγηση των αποφάσεων σχετικά με τις διορθωτικές ενέργειες που πρέπει να ληφθούν καθώς και εάν και ποιος θα πρέπει να ειδοποιηθεί.

● **Ειδοποίηση των κατάλληλων ατόμων / οργανισμών**

Αυτό θα μπορούσε να γίνει μόνο μετά από μια αξιολόγηση και μόνο από διορισμένο προσωπικό.

●**Εκτίμηση**

Θα εξεταστεί ο τρόπος που αντιμετωπίστηκε το συμβάν, από τον εμπλεκόμενο διαχειριστή και αν μπορούν να ληφθούν μέτρα για μελλοντική αποφυγή του ιδίου τύπου συμβάντος.

Οι δράσεις και τα σημεία προς εξέταση θα αναγράφονται στη «Λίστα Ελέγχου Περιστατικών». Επίσης ο εμπλεκόμενος διαχειριστής θα συμπληρώνει το «Αρχείο Καταγραφής Περιστατικών Παραβίασης» με το χρονοδιάγραμμα της διαχείρισης των συμβάντων.

**3.4** Οι προϊστάμενοι τμημάτων καθώς και οι Διευθυντές Τμημάτων θα πρέπει να συνεργάζονται με τα εμπλεκόμενα άτομα, την ΥΠΔ, τον CIO και τον Διευθυντή Πανεπιστημιούπολης, για να διερευνήσουν και να εξετάσουν οποιοδήποτε αναφερόμενο συμβάν το οποίο εμπίπτει στο δικό τους τομέα ευθύνης.

**3.5** Σε περίπτωση κατά την οποία επηρεάστηκαν προσωπικά δεδομένα τρίτου μέρους, το Τμήμα το οποίο διατηρεί τα συγκεκριμένα δεδομένα θα πρέπει άμεσα να ειδοποιήσει και να συμβουλευτεί την ΥΠΔ.

## 4. Επισκόπηση Συμβάντων

**4.1** Το γραφείο της ΥΠΔ θα εξετάζει τακτικά τα περιστατικά, συμπεριλαμβανόμενης της διαδικασίας η οποία τηρήθηκε για την αντιμετώπιση τους, καθώς και την διαδικασία για την αντιμετώπιση πιθανών επαναλαμβανόμενων περιστατικών αλλά και την αντιμετώπιση τυχόν νέων κινδύνων οι οποίοι επισημάνθηκαν κατά την διάρκεια της έρευνας.

**4.2** Η διαδικασία ελέγχου θα επιτρέψει τον εντοπισμό των απαραίτητων αλλαγών στην Διαδικασία Παραβίασης Προσωπικών Δεδομένων, αλλαγές και/ή προσαρμογές στις υπάρχουσες πολιτικές ή την ανάγκη για καθορισμό νέων πολιτικών.

## 5. Παράρτημα

**ΠΑΡΑΡΤΗΜΑ Α-** Ταξινόμηση Προσωπικών Δεδομένων

Όλα τα αναφερόμενα περιστατικά πρέπει να περιλαμβάνουν τη σχετική ταξινόμηση δεδομένων, έτσι ώστε οι σχετικοί κίνδυνοι μπορούν να εκτιμηθούν με ακρίβεια:

● **Δημόσια δεδομένα**

Πληροφορίες που προορίζονται είτε για δημόσια χρήση ή που μπορούν να δημοσιοποιηθούν χωρίς αρνητικές επιπτώσεις στο Πανεπιστήμιο.

● **Εσωτερικά δεδομένα**

Πληροφορίες που σχετίζονται με τις καθημερινές δραστηριότητες του Πανεπιστημίου.

Προορίζεται κυρίως για χρήση από το προσωπικό και τους φοιτητές, αν και ορισμένα δεδομένα ενδέχεται να είναι χρήσιμα και σε τρίτους που συνεργάζονται με το Πανεπιστήμιο.

● **Εμπιστευτικά δεδομένα**

Πληροφορίες που σχετίζονται με τον πιο ευαίσθητο χαρακτήρα των διαδικασιών και διαδικασιών του Πανεπιστημίου.

Η πρόσβαση σε αυτού του είδους τις πληροφορίες πρέπει να παρέχεται μόνο σε εκείνους τους ανθρώπους που χρειάζεται για να εκπληρώσουν το ρόλο τους στο Πανεπιστήμιο.

● **Ιδιαιτέρως εμπιστευτικά δεδομένα ή προσωπικά δεδομένα**

Πληροφορίες που, θα προκαλούσαν σημαντική ζημιά στην επιχείρηση του Πανεπιστημίου στις δραστηριότητες ή φήμη του. Πρόσβαση σε αυτού του είδους τις πληροφορίες θα πρέπει να είναι πολύ περιορισμένη στο προσωπικό που έχει την ανάγκη και το δικαίωμα πρόσβασης σε αυτά.

……