

Πολιτική Προστασίας Δεδομένων ΠΔΜ

Ελληνικό Κείμενο

Δήλωση Εφαρμογής

Η εφαρμογή του Γενικού Κανονισμού για την Προστασία των Δεδομένων (Γ.Κ.Π.Δ.) αποτελεί προτεραιότητα για το Π.Δ.Μ.

Το Π.Δ.Μ. δέχεται ως προσωπικά δεδομένα : Κάθε πληροφορία που αφορά τα φυσικά πρόσωπα, ως ένα ταυτοποιημένο ή ταυτοποιήσιμο άτομο εν ζωή . Για παράδειγμα σε αυτές τις πληροφορίες περιλαμβάνονται το ονοματεπώνυμο , η διεύθυνση κατοικίας , ο αριθμός ταυτότητας, ο κώδικας διαδικτυακού πρωτοκόλλου (IP), οι πληροφορίες για την υγεία τους και την ασφαλιστική τους ικανότητα , την εργασιακή τους κατάσταση, και άλλα.

Τα δεδομένα ειδικής κατηγορίας, όπως τα δεδομένα που αφορούν την υγεία, τη φυλετική ή εθνοτική καταγωγή , συνδικαλιστική δραστηριότητα και άλλα, λαμβάνουν ειδική προστασία.

Οι κανόνες ισχύουν όταν η συλλογή , η χρήση και η αποθήκευση των δεδομένων των φυσικών προσώπων γίνεται ψηφιακά ή σε έντυπη μορφή μέσω ενός διαρθρωμένου συστήματος αρχειοθέτησης.

Η πολιτική αυτή είναι σύμφωνη με τον Γενικό Κανονισμό Προστασίας Δεδομένων της Ε.Ε. (Γ.Κ.Π.Δ.), καθώς και με γνωμοδοτήσεις / αποφάσεις που εκδόθηκαν από την Ελληνική Αρχή Προστασίας Δεδομένων.

Για οποιαδήποτε διευκρίνιση μπορείτε να επικοινωνήσετε με τον Υπεύθυνο Προσωπικών Δεδομένων του Πανεπιστημίου Δυτικής Μακεδονίας στο dpo@uowm.gr.

Ορισμοί

1. «Δεδομένα Προσωπικού Χαρακτήρα»: κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»): το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου,
2. «Επεξεργασία»: κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η

- συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή,
3. «Περιορισμός της Επεξεργασίας»: η επισήμανση αποθηκευμένων δεδομένων προσωπικού χαρακτήρα με στόχο τον περιορισμό της επεξεργασίας τους στο μέλλον,
 4. «Κατάρτιση Προφίλ»: οποιαδήποτε μορφή αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα που συνίσταται στη χρήση δεδομένων προσωπικού χαρακτήρα για την αξιολόγηση ορισμένων προσωπικών πτυχών ενός φυσικού προσώπου, ιδίως για την ανάλυση ή την πρόβλεψη πτυχών που αφορούν την απόδοση στην εργασία, την οικονομική κατάσταση, την υγεία, τις προσωπικές προτιμήσεις, τα ενδιαφέροντα, την αξιοπιστία, τη συμπεριφορά, τη θέση ή τις μετακινήσεις του εν λόγω φυσικού προσώπου,
 5. «Ψευδωνυμοποίηση»: η επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο ώστε τα δεδομένα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρωματικές πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλιστεί ότι δεν μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο,
 6. «Σύστημα Αρχειοθέτησης»: κάθε διαρθρωμένο σύνολο δεδομένων προσωπικού χαρακτήρα τα οποία είναι προσβάσιμα με γνώμονα συγκεκριμένα κριτήρια, είτε το σύνολο αυτό είναι συγκεντρωμένο είτε αποκεντρωμένο είτε καταναμημένο σε λειτουργική ή γεωγραφική βάση,
 7. «Υπεύθυνος Επεξεργασίας»: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα· όταν οι σκοποί και ο τρόπος της επεξεργασίας αυτής καθορίζονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια για τον διορισμό του μπορούν να προβλέπονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους,
 8. «Εκτελών την Επεξεργασία»: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας,
 9. «Αποδέκτης»: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας, στα οποία κοινολογούνται τα δεδομένα προσωπικού χαρακτήρα, είτε πρόκειται για τρίτον είτε όχι. Ωστόσο, οι δημόσιες αρχές που ενδέχεται να λάβουν δεδομένα προσωπικού χαρακτήρα στο πλαίσιο συγκεκριμένης έρευνας σύμφωνα με το δίκαιο της Ένωσης ή κράτους μέλους δεν θεωρούνται ως αποδέκτες· η επεξεργασία των δεδομένων αυτών από τις εν λόγω δημόσιες αρχές πραγματοποιείται σύμφωνα με τους ισχύοντες κανόνες προστασίας των δεδομένων ανάλογα με τους σκοπούς της επεξεργασίας,
 10. «Τρίτος»: οποιοδήποτε φυσικό ή νομικό πρόσωπο, δημόσια αρχή, υπηρεσία ή φορέας, με εξαίρεση το υποκείμενο των δεδομένων, τον υπεύθυνο επεξεργασίας, τον εκτελούντα την επεξεργασία και τα πρόσωπα τα οποία, υπό την άμεση εποπτεία του υπευθύνου επεξεργασίας ή του εκτελούντος την

επεξεργασία, είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα,

11. «Συγκατάθεση» του υποκειμένου των δεδομένων: κάθε ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει, με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν,
12. «Παραβίαση Δεδομένων Προσωπικού Χαρακτήρα»: η παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία,
13. «Δεδομένα Ειδικών Κατηγοριών»: δεδομένα προσωπικού χαρακτήρα που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και η επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένων που αφορούν την υγεία ή δεδομένων που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό,
14. «Κύρια Εγκατάσταση»: α) ο τόπος της κεντρικής διοίκησης του υπευθύνου β) όταν πρόκειται για εκτελούντα την επεξεργασία η εγκατάσταση του εκτελούντος την επεξεργασία στην οποία εκτελούνται οι κύριες δραστηριότητες επεξεργασίας.
15. «Εποπτική Αρχή»: ανεξάρτητη δημόσια αρχή που συγκροτείται από κράτος μέλος σύμφωνα με το άρθρο 51 του Γ.Κ.Π.Δ

Κατηγορίες Δεδομένων Προσωπικού Χαρακτήρα που συλλέγονται

Το Π.Δ.Μ. στο πλαίσιο των ως άνω δραστηριοτήτων του και της συνήθους λειτουργίας του χάριν του δημοσίου συμφέροντος , δύναται να συλλέγει δεδομένα προσωπικού χαρακτήρα τόσο πολιτών ή συνεργατών του που κάνουν χρήση των υπηρεσιών – εφαρμογών του, όσο και των εργαζομένων του, των φοιτητών καθώς επίσης και των εν γένει συνεργατών του, αλλά και λοιπών φυσικών προσώπων με τα οποία συναλλάσσεται στο πλαίσιο των αρμοδιοτήτων του.

Ανάλογα με τη μορφή και τον σκοπό επεξεργασίας ανά υπηρεσία , το Π.Δ.Μ. δύναται να συλλέγει και να επεξεργάζεται δεδομένα προσωπικού χαρακτήρα , όπως ενδεικτικά τα ακόλουθα:

ΚΑΤΗΓΟΡΙΕΣ ΥΠΟΚΕΙΜΕΝΩΝ	ΚΑΤΗΓΟΡΙΕΣ ΔΕΔΟΜΕΝΩΝ	
Φοιτητές του Π.Δ.Μ.	Φοιτητές που κατά καιρό έχουν φοιτήσει ή φοιτούν στο Π.Δ.Μ. Τα δπχ που κατέχει το Π.Δ.Μ. μπορεί να περιλαμβάνουν:	

<p>Ωφελούμενοι (εκπαιδευτικών υπηρεσιών)</p>	<ol style="list-style-type: none"> 1. Στοιχεία ταυτότητας και δημογραφικά (λ.χ. ονοματεπώνυμο, πατρώνυμο κ.λπ.), 2. Στοιχεία ασφάλισης (λ.χ. ΑΜΚΑ ή ΑΥΠΙΑ και λοιπά στοιχεία Μητρώου Φορέα Κοινωνικής Ασφάλισης αν απαιτούνται), 3. Στοιχεία επικοινωνίας (λ.χ. ταχυδρομική διεύθυνση , τηλέφωνο, Email κ.λπ.), 4. Δεδομένα υγείας (λ.χ. ιατρικές βεβαιώσεις και γνωματεύσεις, συνταγές ιατροφαρμακευτικής αγωγής κ.λπ.), 5. Οικονομικά στοιχεία (λ.χ. τραπεζικοί λογαριασμοί , εκκαθαριστικά εφορίας κ.λπ.), 6. Στοιχεία οικογενειακής κατάστασης κ.ο.κ. 7. Άλλα στοιχεία 8. Δεδομένα οικογενειακής κατάστασης και δεδομένα τρίτων προσώπων (πχ συγγενείς) 9. Βαθμολογίες και πτυχία 10. Παρουσίες σε μαθήματα 11. Έργα πνευματικής ιδιοκτησίας (πχ εργασίες , διπλωματικές κ.α.) 12. Φωτογραφικό υλικό <p>Δεδομένα ελλήνων και μη ελλήνων πολιτών που είναι ωφελούμενοι ή συναλλάσσονται με Π .Δ.Μ, διότι αρκεί η ιδιότητα του φυσικού προσώπου προκειμένου μια πληροφορία που αναφέρεται σε αυτό να εμπίπτει στα δεδομένα προσωπικού χαρακτήρα, χωρίς να απαιτείται και η ιδιότητα του Έλληνα πολίτη κι επομένως οι διατάξεις προστατεύουν επίσης δεδομένα προσωπικού χαρακτήρα αλλοδαπών όπως μπορεί να είναι οι φοιτητές και μέλη ΔΕΠ σε κινητικότητα μέσω προγραμμάτων ανταλλαγής,</p>
--	---

	<p>πρόσφυγες και μετανάστες που ενδέχεται να παρακολουθούν προγράμματα δια βίου μάθησης και άλλοι.</p>
<p>Προμηθευτές/Ανάδοχοι</p>	<p>Τα δεδομένα προμηθευτών των Π.Δ.Μ. και Ε.Λ.Κ.Ε, εφόσον πρόκειται για φυσικά πρόσωπα ή για τους νόμιμους εκπροσώπους νομικών προσώπων, διότι τα «δεδομένα προσωπικού χαρακτήρα» αφορούν μόνο πληροφορίες που αφορούν φυσικά πρόσωπα και δεν εμπίπτουν σε αυτή την κατηγορία δεδομένα που αφορούν νομικά πρόσωπα όπως είναι οι εταιρείες, τα σωματεία, τα ιδρύματα. Αυτά μπορεί να περιλαμβάνουν:</p> <ol style="list-style-type: none"> 1. Στοιχεία ταυτότητας και δημογραφικά (λ.χ. ονοματεπώνυμο, πατρώνυμο κ.λπ.), 2. Στοιχεία ασφάλισης (λ.χ. ΑΜΚΑ ή ΑΥΠΙΑ και λοιπά στοιχεία Μητρώου Φορέα Κοινωνικής Ασφάλισης αν απαιτούνται), 3. Στοιχεία επικοινωνίας (λ.χ. ταχυδρομική διεύθυνση έδρας, τηλέφωνο, Email κ.λπ.), 4. Αντίγραφο Ποινικού Μητρώου 5. Επαγγελματικά στοιχεία
<p>Δεδομένα άλλων Φυσικών Προσώπων</p>	<p>Τα δεδομένα άλλων φυσικών προσώπων που τυχαίνει να επισκέπτονται υποδομές του Π.Δ.Μ, ή να συνεργάζονται με αυτό ή να ανήκουν σε συνεργαζόμενους φορείς.</p>
<p>Εργαζόμενοι (Ενεργοί Και Μη) / Υποψήφιοι Εργαζόμενοι</p>	<p>Δεδομένα εργαζομένων του Π.Δ.Μ. και Ε.Λ.Κ.Ε., υπό οποιαδήποτε εργασιακή σχέση καθώς και δεδομένα πρώην και υποψήφιων εργαζομένων, τα οποία τηρούνται σε υπηρεσιακούς φακέλους ή και τυχόν άλλων υπηρεσιών για σκοπούς λειτουργίας της εργασιακής σχέσης τους με το νομικό πρόσωπο. Αυτά μπορεί να περιλαμβάνουν:</p> <ol style="list-style-type: none"> 1. Στοιχεία ταυτότητας και δημογραφικά (λ.χ. ονοματεπώνυμο, πατρώνυμο κ.λπ.), 2. Στοιχεία ασφάλισης (λ.χ. ΑΜΚΑ και λοιπά στοιχεία Μητρώου Φορέα Κοινωνικής Ασφάλισης αν απαιτούνται), 3. Στοιχεία επικοινωνίας (λ.χ. ταχυδρομική διεύθυνση ,

	<p>τηλέφωνο, Email κ.λπ.),</p> <p>4. Δεδομένα υγείας (λ.χ. ιατρικές βεβαιώσεις και γνωματεύσεις, στοιχεία αιμοδοσίας κ.λπ.),</p> <p>5. Οικονομικά στοιχεία (λ.χ. τραπεζικοί λογαριασμοί , εκκαθαριστικά εφορίας , δήλωση περιουσιακής κατάστασης κ.λπ.),</p> <p>6. Περιουσιακά στοιχεία (λ.χ. δήλωση περιουσιακής κατάστασης)</p> <p>7. Στοιχεία οικογενειακής κατάστασης (λ.χ. βεβαιώσεις και πιστοποιητικά, αριθμός και στοιχεία τέκνων κ.ο.κ.)</p>
--	---

Πίνακας 1. Οι κατηγορίες Υποκειμένων και των δεδομένων τους

Σκοποί και Νόμιμες Βάσεις Επεξεργασίας

Το Π.Δ.Μ. και ο Ε.Λ.Κ.Ε., στο πλαίσιο των σχετικών με την ηλεκτρονική διακυβέρνηση δραστηριοτήτων του και της λειτουργίας τους χάριν δημοσίου συμφέροντος , δύναται να συλλέγει και επεξεργάζεται δεδομένα προσωπικού χαρακτήρα πολιτών και των άλλων φυσικών προσώπων τα οποία αναφέρθηκαν στην ανωτέρα παράγραφο και που κάνουν χρήση των παρεχόμενων εκπαίδευσης , εργαζομένων του, και εν γένει συνεργατών της. Επί της αρχής , το Π .Δ.Μ. και ο Ε .Λ.Κ.Ε. ενδέχεται να συλλέγει και επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για τους κάτωθι σκοπούς με τις αντίστοιχες νόμιμες βάσεις επεξεργασίας:

ΣΚΟΠΟΣ ΕΠΕΞΕΡΓΑΣΙΑΣ	ΝΟΜΙΜΕΣ ΒΑΣΕΙΣ
<p>Λειτουργία του Π.Δ.Μ. και του Ε.Λ.Κ.Ε. σε όλους τους τομείς αρμοδιοτήτων τους , καθώς και η μελέτη, εκμετάλλευση, διοίκηση, διαχείριση Συστημάτων Πληροφορικής και Επικοινωνιών , εξοπλισμού, λογισμικού και υπηρεσιών αντίστοιχα.</p>	<p>1. Συμμόρφωση με έννομη υποχρέωση [αρθ. 6 §1 περ. γ) Γ.Κ.Π.Δ.] ή/και</p> <p>2. Εκτέλεση σύμβασης [αρθ. 6 §1 περ. β) Γ.Κ.Π.Δ.], όπου υφίσταται ή/και</p> <p>3. Εκτέλεση καθήκοντος προς το δημόσιο συμφέρον [αρθ. 6 §1 περ.</p>

	ε) Γ.Κ.Π.Δ.]
Την εξυπηρέτηση σε υπηρεσίες τριτοβάθμιας εκπαίδευσης (και δια βίου)	<ol style="list-style-type: none"> 1. Συμμόρφωση με έννομη υποχρέωση [αρθ. 6 §1 περ. γ) Γ.Κ.Π.Δ.] ή/και 2. Εκτέλεση καθήκοντος προς το δημόσιο συμφέρον [αρθ. 6 §1 περ. ε) Γ.Κ.Π.Δ.]
Τη συνεργασία και διασύνδεση με αντίστοιχους φορείς της Ευρωπαϊκής Ένωσης	Συμμόρφωση με έννομη υποχρέωση [αρθ. 6 §1 περ. γ) Γ.Κ.Π.Δ.]
Τη διασφάλιση της διαλειτουργικότητας των Συστημάτων Πληροφορικής και Επικοινωνιών	<ol style="list-style-type: none"> 1. Συμμόρφωση με έννομη υποχρέωση [αρθ. 6 §1 περ. γ) Γ.Κ.Π.Δ.] ή/και 2. Εκτέλεση σύμβασης [αρθ. 6 §1 περ. β) Γ.Κ.Π.Δ.], όπου υφίσταται ή/και 3. Εκτέλεση καθήκοντος προς το δημόσιο συμφέρον [αρθ. 6 §1 περ. ε) Γ.Κ.Π.Δ.]
Την παροχή συμβουλών προς φοιτητές και άλλα φυσικά πρόσωπα	<ol style="list-style-type: none"> 1. Συμμόρφωση με έννομη υποχρέωση [αρθ. 6 §1 περ. γ) Γ.Κ.Π.Δ.] 2. Εκτέλεση σύμβασης [αρθ. 6 §1 περ. β) Γ.Κ.Π.Δ.], όπου υφίσταται ή/και 3. Εκτέλεση καθήκοντος προς το δημόσιο συμφέρον [αρθ. 6 §1 περ. ε) Γ.Κ.Π.Δ.]
Τη παροχή προς κάθε υπηρεσία του Κράτους και της Ευρωπαϊκής Ένωσης στατιστικών και άλλου τύπου πληροφοριών και αξιολογήσεων στο πλαίσιο συμμετοχής σε ευρωπαϊκά προγράμματα	<ol style="list-style-type: none"> 1. Συμμόρφωση με έννομη υποχρέωση [αρθ. 6 §1 περ. γ) Γ.Κ.Π.Δ.] ή/και 2. Εκτέλεση σύμβασης [αρθ. 6

	<p>§1 περ. β) Γ.Κ.Π.Δ.], όπου υφίσταται ή/και</p> <p>3. – Εκτέλεση καθήκοντος προς το δημόσιο συμφέρον [αρθ. 6 §1 περ. ε) Γ.Κ.Π.Δ.]</p>
<p>Τη μελέτη , ανάπτυξη, λειτουργία, εκμετάλλευση, διαχείριση και συντήρηση Συστημάτων Πληροφορικής και Επικοινωνιών Π.Δ.Μ</p>	<p>1. Συμμόρφωση με έννομη υποχρέωση [αρθ. 6 §1 περ. γ) Γ.Κ.Π.Δ.] ή/και</p> <p>2. Εκτέλεση σύμβασης [αρθ. 6 §1 περ. β) Γ.Κ.Π.Δ.], όπου υφίσταται ή/και</p> <p>1. Εκτέλεση καθήκοντος προς το δημόσιο συμφέρον [αρθ. 6 §1 περ. ε) Γ.Κ.Π.Δ.]</p>
<p>Τη συλλογή , επεξεργασία, διασταύρωση και διαβίβαση στοιχείων της Φορολογικής Ασφαλιστικής και Εργασιακής Διοίκησης αποκλειστικώς για την υποστήριξη και λειτουργία του πλαισίου των αρμοδιοτήτων του</p>	<p>1. Συμμόρφωση με έννομη υποχρέωση [αρθ. 6 §1 περ. γ) Γ.Κ.Π.Δ.] ή/και</p> <p>2. Εκτέλεση καθήκοντος προς το δημόσιο συμφέρον [αρθ. 6 §1 περ. ε) Γ.Κ.Π.Δ.]</p>
<p>Τη συλλογή και επεξεργασία δεδομένων εικόνας με χρήση κλειστού κυκλώματος καμερών (CCTV), καθώς επίσης τη συλλογή και επεξεργασία δεδομένων ταυτοποίησης (λ.χ. αστυνομικό δελτίο ταυτότητας), για λόγους ασφάλειας</p>	<p>Εξυπηρέτηση έννομων συμφερόντων [αρθ. 6 §1 περ. στ) Γ.Κ.Π.Δ.] ή/και</p>
<p>Τη συλλογή και επεξεργασία των αναγκαίων δεδομένων εργαζομένων ή /και υποψήφιων εργαζομένων και συνεργατών για την δέουσα εξυπηρέτηση υφιστάμενων εργασιακών σχέσεων ή σχέσεων συνεργασίας ή την εξέταση ενδεχόμενης μελλοντικής συνεργασίας</p>	<p>1. Συμμόρφωση με έννομη υποχρέωση [αρθ. 6 §1 περ. γ) Γ.Κ.Π.Δ.] ή/και</p> <p>2. Εξυπηρέτηση έννομων συμφερόντων [αρθ. 6 §1 περ. στ) Γ.Κ.Π.Δ.]</p>
<p>Τη συλλογή και επεξεργασία των αναγκαίων δεδομένων ανήλικων τέκνων για την διασταύρωση δυνητικής παροχής ή την παροχή κοινωνικών</p>	<p>1. Συμμόρφωση με έννομη υποχρέωση [αρθ. 6 §1 περ. γ) Γ.Κ.Π.Δ.] ή/και</p>

ωφελημάτων προς τους φοιτητές.	2. Εκτέλεση σύμβασης [αρθ. 6 §1 περ. β) Γ.Κ.Π.Δ.]
Για κάθε άλλη μορφή επεξεργασίας, το Π.Δ.Μ. και ο Ε .Λ.Κ.Ε. ζητά ειδική γραπτή , ελεύθερη και κατόπιν προγενέστερης ενημέρωσης συγκατάθεση των υποκειμένων πριν την έναρξη της επεξεργασίας, εφόσον απαιτείται.	

Πίνακας 2. Οι κύριοι σκοποί και νόμιμες βάσεις επεξεργασίας

Η αναφορά σε περισσότερες της μίας νόμιμων βάσεων επεξεργασίας, δεν έχει την έννοια ότι το Π.Δ.Μ. προβαίνει σε αλλαγή αυτών (lawful basis swapping) υποσκάπτοντας τα δικαιώματα των υποκειμένων των δεδομένων, αλλά ότι υφίστανται περιπτώσεις που είναι εφαρμοστέες περισσότερες από μία νόμιμες βάσεις επεξεργασίας.

Περαιτέρω και καθότι το Π.Δ.Μ. εντάσσεται στους φορείς Δημόσιας Διοίκησης (σύμφωνα με το αρ.14 του ν.4270/2014 αλλά και το Μητρώο Υπηρεσιών και Φορέων της Ελληνικής Διοίκησης), συνεφαρμόζεται μετά το πέρας μιας επεξεργασίας η περαιτέρω επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς, η οποία δεν θεωρείται ασύμβατη με τους αρχικούς σκοπούς σύμφωνα με το άρθρο 5 παρ.1 περιπτ. β' και αρ. 89 παράγραφος 1 του Γ.Κ.Π.Δ..

Τέλος το Π.Δ.Μ. δε χρησιμοποιεί ως κύρια βάση επεξεργασίας τη συγκατάθεση των υποκειμένων των δεδομένων (είτε πρόκειται για απλά δεδομένα είτε για ειδικών κατηγοριών), αναγνωρίζοντας την εγγενή ανισομέρεια που υπάρχει στη σχέση του με τα κάθε φορά υποκείμενα των δεδομένων και σύμφωνα άλλωστε με τις συστάσεις της Ομάδας Εργασίας του Αρ.29 (πλέον Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων). Πλην όμως και κατ' εξαίρεση, για ελάχιστες περιπτώσεις όπου παρέχεται μια επιπλέον υπηρεσία στα υποκείμενα (πέραν δηλαδή των νόμιμων προβλεπόμενων), χρησιμοποιείται περιορισμένα η συγκατάθεση ως νόμιμη βάση επεξεργασίας και μόνο τότε.

Δικαιώματα Φυσικών Προσώπων

Το Π.Δ.Μ. αναγνωρίζει τα δικαιώματα των φυσικών προσώπων αναφορικά με την προστασία των προσωπικών δεδομένων τους. Έτσι τα φυσικά πρόσωπα έχουν το δικαίωμα να:

1. Ενημερώνονται σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα.
2. Αποκτούν πρόσβαση στα δεδομένα προσωπικού χαρακτήρα που τα αφορούν.
3. Ζητούν τη διόρθωση εσφαλμένων, ανακριβών ή ελλιπών δεδομένων προσωπικού χαρακτήρα.
4. Υποβάλλουν αίτημα για τη διαγραφή δεδομένων προσωπικού χαρακτήρα όταν δεν είναι πλέον απαραίτητα ή εάν η επεξεργασία είναι παράνομη. Εφόσον εφαρμόζεται ως νόμιμη βάση επεξεργασίας το αρ.6 παρ.1 περιπτ. ε' Γ.Κ.Π.Δ. (επεξεργασία για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας και το αρ.9 παρ.2 περιπτ. β', ζ, ι) στις περισσότερες επεξεργασίες του Π.Δ.Μ., το δικαίωμα διαγραφής είναι περιορισμένο και θα κριθεί κατά περίπτωση υπό αυστηρές προϋποθέσεις. Άλλωστε σύμφωνα με το αρ.4 της Αιτιολογικής Έκθεσης Γ.Κ.Π.Δ. το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα δεν είναι απόλυτο δικαίωμα· πρέπει να εκτιμάται σε σχέση με τη λειτουργία του στην κοινωνία και να σταθμίζεται με άλλα θεμελιώδη δικαιώματα, σύμφωνα με την αρχή της αναλογικότητας.
5. Εναντιώνονται στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα για λόγους που σχετίζονται με την ιδιαίτερη κατάστασή τους, υπό την επιφύλαξη του αρ.21 παρ.6 Γ.Κ.Π.Δ..
6. Υποβάλλουν αίτημα για περιορισμό της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα σε συγκεκριμένες περιπτώσεις.
7. Εκφράζουν την άποψη τους και να προσβάλλουν την απόφαση.
8. Να υποβάλουν καταγγελία στην Α.Π.Δ.Π.Χ

Τα εν λόγω δικαιώματα ισχύουν σε ολόκληρη την περιοχή εφαρμογής του Γ.Κ.Π.Δ., ανεξάρτητα από το πού γίνεται η επεξεργασία των δεδομένων και πού έχει έδρα το Π.Δ.Μ.

Αρχές επεξεργασίας

Το Π.Δ.Μ. αποδέχεται τις βασικές Αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Τα δεδομένα προσωπικού χαρακτήρα (άρθρο 5):

1. Υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων («νομιμότητα, αντικειμενικότητα και διαφάνεια»).
2. Συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς· η περαιτέρω επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς δεν θεωρείται ασύμβατη με τους αρχικούς σκοπούς σύμφωνα με το άρθρο 89 παράγραφος 1 («περιορισμός του σκοπού»).
3. Είναι κατάλληλα, συναφή και περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία («ελαχιστοποίηση των δεδομένων»).
4. Είναι ακριβή και, όταν είναι αναγκαίο, επικαιροποιούνται· πρέπει να λαμβάνονται όλα τα εύλογα μέτρα για την άμεση διαγραφή ή διόρθωση δεδομένων προσωπικού χαρακτήρα τα οποία είναι ανακριβή, σε σχέση με τους σκοπούς της επεξεργασίας («ακρίβεια»).

5. Διατηρούνται υπό μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων μόνο για το διάστημα που απαιτείται για τους σκοπούς της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα: τα δεδομένα προσωπικού χαρακτήρα μπορούν να αποθηκεύονται για μεγαλύτερα διαστήματα, εφόσον τα δεδομένα προσωπικού χαρακτήρα θα υποβάλλονται σε επεξεργασία μόνο για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς, σύμφωνα με το άρθρο 89 παράγραφος 1 και εφόσον εφαρμόζονται τα κατάλληλα τεχνικά και οργανωτικά μέτρα που απαιτεί ο παρών κανονισμός για τη διασφάλιση των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων («περιορισμός της περιόδου αποθήκευσης»).
6. Υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλεια των δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά, με τη χρησιμοποίηση κατάλληλων τεχνικών ή οργανωτικών μέτρων («ακεραιότητα και εμπιστευτικότητα»).

Το Π.Δ.Μ. τηρεί αρχείο των δραστηριοτήτων επεξεργασίας για τις οποίες είναι υπεύθυνο. Το εν λόγω αρχείο περιλαμβάνει όλες τις ακόλουθες πληροφορίες:

1. το όνομα και τα στοιχεία επικοινωνίας του υπεύθυνου επεξεργασίας και, κατά περίπτωση, του από κοινού υπευθύνου επεξεργασίας, του εκπροσώπου του υπευθύνου επεξεργασίας και του υπευθύνου προστασίας δεδομένων,
2. τους σκοπούς της επεξεργασίας,
3. περιγραφή των κατηγοριών υποκειμένων των δεδομένων και των κατηγοριών δεδομένων προσωπικού χαρακτήρα,
4. τις κατηγορίες αποδεκτών στους οποίους πρόκειται να γνωστοποιηθούν ή γνωστοποιήθηκαν τα δεδομένα προσωπικού χαρακτήρα, περιλαμβανομένων των αποδεκτών σε τρίτες χώρες ή διεθνείς Οργανισμούς,
5. όπου συντρέχει περίπτωση, τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα σε τρίτη χώρα ή διεθνή οργανισμό, συμπεριλαμβανομένων του προσδιορισμού της εν λόγω τρίτης χώρας ή του διεθνούς Οργανισμού και, σε περίπτωση διαβιβάσεων που αναφέρονται στο άρθρο 49 παράγραφος 1 δεύτερο εδάφιο, της τεκμηρίωσης των κατάλληλων εγγυήσεων,
6. όπου είναι δυνατό, τις προβλεπόμενες προθεσμίες διαγραφής των διαφόρων κατηγοριών δεδομένων,
7. όπου είναι δυνατό, γενική περιγραφή των τεχνικών και οργανωτικών μέτρων ασφάλειας που αναφέρονται στο άρθρο 32 παράγραφος 1.

Προστασία δεδομένων προσωπικού χαρακτήρα

Λαμβάνοντας υπόψη 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, το Π.Δ.Μ. εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τον Κανονισμό.

Κατά την εκτίμηση του ενδεδειγμένου επιπέδου ασφάλειας από το Π.Δ.Μ. λαμβάνονται ιδίως υπόψη οι κίνδυνοι που απορρέουν από την επεξεργασία, ιδίως από τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, άνευ αδείας κοινολόγηση ή προσπέλαση

δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία.

Σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα (άρθρο 33), το Π.Δ.Μ. ως υπεύθυνος επεξεργασίας θα γνωστοποιεί αμελλητί και, αν είναι δυνατό, εντός 72 ωρών από τη στιγμή που αποκτά γνώση του γεγονότος την παραβίαση των δεδομένων προσωπικού χαρακτήρα στην εποπτική αρχή που είναι αρμόδια σύμφωνα με το άρθρο 55, εκτός εάν η παραβίαση δεδομένων προσωπικού χαρακτήρα δεν ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Όταν η γνωστοποίηση στην εποπτική αρχή δεν πραγματοποιείται εντός 72 ωρών, θα συνοδεύεται από αιτιολόγηση για την καθυστέρηση.

Κατάρτιση προσωπικού

Το Π.Δ.Μ. αποδέχεται ότι η προστασία των δεδομένων προσωπικού χαρακτήρα προϋποθέτει την ευαισθητοποίηση του ανθρώπινου δυναμικού του σχετικά με την προστασία των προσωπικών δεδομένων. Στην κατεύθυνση αυτή, αποδέχεται την υιοθέτηση και εφαρμογή των εξής:

1. Προσανατολισμό της δέουσας εκπαίδευσης με εκμετάλλευση των Πρακτικών της Ορθής Πληροφόρησης (Fair Information Practices-FIP), που συμπυκνώνουν ένα σύνολο προτύπων που διέπουν τη συλλογή και χρήση των προσωπικών δεδομένων και την αντιμετώπιση θεμάτων ιδιωτικότητας και ακρίβειας. Το ανθρώπινο δυναμικό δεν δύναται να γίνει ειδήμονας στο πεδίο της προστασίας του απορρήτου από την μία μέρα στην άλλη, ωστόσο η εξοικείωσή του με τις διεθνείς απαιτήσεις της προστασίας της ιδιωτικότητας είναι εφικτή και αναγκαία. Οι εργαζόμενοι που έχουν ρόλους καθοριστικούς στο πεδίο της προστασίας της ιδιωτικής ζωής πρέπει να αποκτήσουν ειδικότερη γνώση. Όσον αφορά, όμως, το μεγαλύτερο μέρος του εργατικού δυναμικού, μια συνολική γνώση των γενικών αρχών της προστασίας του απορρήτου είναι απαραίτητη.
2. Το Π.Δ.Μ. επιδιώκει την εκ μέρους του ανθρώπινου δυναμικού του συνειδητοποίηση βασικών εννοιών προστασίας δεδομένων προσωπικού χαρακτήρα. Κάτι τέτοιο, σε καμία περίπτωση, δεν σημαίνει ότι η κατάρτιση του προσωπικού του αποβαίνει υπερβολικά θεωρητική ή αφηρημένη. Αντιθέτως, γίνεται πρακτική. Ο πυρήνας της εκπαίδευσης επικεντρώνεται σε τρία απλά αλλά ουσιώδη ζητήματα:
3. Κίνητρο: Γιατί πρέπει να νοιάζονται οι εργαζόμενοι για την προστασία της ιδιωτικότητας.
4. Ορισμός: Τι είναι τα προσωπικά δεδομένα.
5. Ευθύνη: Τι πρέπει να γνωρίζουν οι εργαζόμενοι για τον τρόπο με τον οποίο λογοδοτεί το Π.Δ.Μ. για την ιδιωτικότητα.

Επικοινωνία Φυσικών Προσώπων

Τα ανωτέρω δικαιώματα καθώς και κάθε δικαίωμα σχετικά με τα προσωπικά δεδομένα, ασκούνται κατόπιν γραπτής αίτησης που κατατίθεται σε οποιοδήποτε σημείο που είναι

προσβάσιμο από το κοινό, ή μέσω ηλεκτρονικής επικοινωνίας αποστέλλοντας μήνυμα στο dro@uowm.gr και εξετάζεται και από τον Υπεύθυνο Προστασίας για τα Προσωπικά Δεδομένα, όπως αυτός ορίζεται από το Π.Δ.Μ.

Τροποποίηση

Η παρούσα πολιτική ενδέχεται να χρειαστεί τροποποίηση σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα. Σε περίπτωση που η τροποποίηση των υπόψη όρων είναι τέτοιας φύσης και έκτασης, ώστε να μην καλύπτεται από τους ανωτέρω όρους επεξεργασίας δεδομένων, το Π.Δ.Μ. οφείλει να κάνει δημόσια την νέα έκδοση της πολιτικής.

Αγγλικό Κείμενο

Application Statement

The implementation of the General Data Protection Regulation (GDPR) is a priority for U.o.W.M.

U.o.W.M. accepts as personal data: Any information relating to an identified or identifiable natural person alive. For example, this information includes name, home address, ID number, Internet Protocol (IP) code, information about their health and insurance capacity, employment status, and more.

Special categories data, such as health, racial or ethnic origin, trade union activity, etc., receive special protection.

The rules apply when collecting, using, and storing personal data is done digitally or in hard copy through a structured filing system.

This policy is in line with the EU General Data Protection Regulation. (GDPR), and opinions/decisions issued by the Hellenic Data Protection Authority.

For any clarification you can contact U.o.W.M.'s Data Protection Officer Macedonia at dpo@uowm.gr.

Terms and Definitions

1. 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person,
2. 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction,
3. 'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future,
4. 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements,
5. 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational

measures to ensure that the personal data are not attributed to an identified or identifiable natural person,

6. 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised, or dispersed on a functional or geographical basis,
7. 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law,
8. 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller,
9. 'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing,
10. 'third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data,
11. 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her,
12. 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed,
13. 'special categories data' means personal data disclosing racial or ethnic origin, political views, religious or philosophical beliefs, or trade union affiliation, as well as the processing of genetic, biometric data for the data relating to health or data relating to the natural sexual life or sexual orientation of a person,
14. 'main establishment' means a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union. b) as regards a processor with establishments in more than one Member State, the place of its central administration in the Union.
15. 'supervisory authority' means an independent public authority which is established by a Member State pursuant to Article 51.

Categories of Personal Data Collected

U.o.W.M. in the context of the above activities and its regular operation in the public interest, it may collect personal data of both its citizens or associates who use its services

- applications, as well as its employees, students as well as, generates his associates, but also other natural persons with whom he deals within the framework of his responsibilities.

Depending on the form and purpose of processing per service, U.o.W.M. may collect and process personal data, such as the following:

CATEGORIES OF DATA SUBJECTS	CATEGORIES OF DATA	
Students of U.o.W.M.	<p>Students who for some time have studied or are studying at U.o.W.M. Personal data held by the U.o.W.M. may include:</p> <ol style="list-style-type: none"> 1. Identity and demographics (e.g., name, patronymic, etc.), 2. Insurance details (e.g., AMKA or AYPIA and other details of the Social Security Institution Register if required), 3. Contact details (e.g., postal address, telephone, Email, etc.), 4. Health data (e.g., medical certificates and opinions, prescriptions for medical treatment, etc.), 5. Financial data (e.g., bank accounts, tax returns, etc.), 6. Elements of marital status and so on. 7. Other information 8. Third party data (e.g. relatives) 9. Scores and degrees 10. Attendance at classes 11. Intellectual property projects (e.g., works, diplomas, etc.) 12. Photographic material 	
Beneficiaries (educational services)	<p>Data of Greek and foreign citizens who are beneficiaries or trade with U.o.W.M., because the status of a natural person is sufficient for information that refers to it to fall into personal data, without requiring the status of a Greek citizen and therefore the provisions also protect the personal data of foreigners such as students and faculty members in mobility through exchange programs, refugees and migrants who may attend lifelong learning programs and others.</p>	
Suppliers / Contractors	<p>The data of U.o.W.M.and ELKE's suppliers, in the case of natural persons or legal representatives of legal persons, because "personal data" refers only to information relating to natural persons and does not fall into this category of data relating to legal persons such as companies, unions, institutions. These may include:</p> <ol style="list-style-type: none"> 1. Identity and demographics (e.g., name, patronymic, etc.), 2. Insurance details (e.g., AMKA or AYPIA and other 	

	<p>information of the Social Security Institution Register if required),</p> <ol style="list-style-type: none"> 3. Contact details (e.g., postal address, telephone, Email, etc.), 4. Copies of Criminal Records 1. 5. Professional details
Data of other natural persons	The data of other natural persons who happen to visit U.o.W.M.'s infrastructure or belong to collaborating bodies.
Employees (Active or Not) / Candidate Employees	<p>Data of U.o.W.M. and ELKE employees, under any employment relationship, and data of former and prospective employees, which are kept in official files or any other services to operate their employment relationship with the legal entity. These may include:</p> <ol style="list-style-type: none"> 1. Identity and demographics (e.g., name, patronymic, etc.), 2. Insurance details (e.g., AMKA and other Social Security Authority details if required), 3. Contact details (e.g., postal address, telephone, Email, etc.), 4. Health data (e.g., medical certificates and opinions, blood donation data, etc.), 5. Financial data (e.g., bank accounts, tax returns, statement of assets, etc.), 6. Assets (e.g., statement of assets) 7. Marital status details (e.g., certificates and certificates, number and details of children, etc.)

Table 1. The categories of Data Subjects and their data

Purposes and Legal Basis of Processing

U.o.W.M. and ELKE, in the context of its activities related to e-government and their operation for the public interest, may collect and process personal data of citizens and other natural persons referred to in the above paragraph and making use of the training provided, its employees, and its affiliates in general. In principle U.o.W.M. and ELKE may collect and process personal data for the following purposes with the corresponding legal processing bases:

PURPOSE OF PROCESSING	LEGAL BASIS
U.o.W.M. and ELKE's operation in all their areas of responsibility as well as the study, operation, administration, management of Information and Communication Systems, equipment, software and services, respectively.	<ol style="list-style-type: none"> 1. Processing is necessary for compliance with a legal obligation [Art. 6 §1 case. c) GDPR] and/or 2. Processing is necessary for the performance of a

	<p>contract [Art. 6 §1 case. b) GDPR] where it exists and / or</p> <p>3. Processing is necessary for the performance of a task carried out in the public interest [Art. 6 §1 case e) GDPR]</p>
Service in higher and lifelong educational services	<p>1. Processing is necessary for compliance with a legal obligation [Art. 6 §1 case. c) GDPR] and/or</p> <p>2. Processing is necessary for the performance of a task carried out in the public interest [Art. 6 §1 case e) GDPR]</p>
Cooperation and interconnection with relevant bodies of the European Union	<p>Processing is necessary for compliance with a legal obligation [Art. 6 §1 case. c) GDPR]</p>
Ensuring the interoperability of Information and Communication Systems	<p>1. Processing is necessary for compliance with a legal obligation [Art. 6 §1 case. c) GDPR] and/or</p> <p>2. Processing is necessary for the performance of a contract [Art. 6 §1 case. b) GDPR] where it exists and / or</p> <p>3. Processing is necessary for the performance of a task carried out in the public interest [Art. 6 §1 case e) GDPR]</p>
Providing advice to students and other individuals	<p>1. Processing is necessary for compliance with a legal obligation [Art. 6 §1 case. c) GDPR] and/or</p> <p>2. Processing is necessary</p>

	<p>for the performance of a contract [Art. 6 §1 case. b) GDPR] where it exists and / or 3. Processing is necessary for the performance of a task carried out in the public interest [Art. 6 §1 case e) GDPR]</p>
<p>The provision to each State and European Union service of statistics and other information and evaluations in the context of participation in European programs</p>	<p>1. Processing is necessary for compliance with a legal obligation [Art. 6 §1 case. c) GDPR] and/or</p> <p>2. Processing is necessary for the performance of a contract [Art. 6 §1 case. b) GDPR] where it exists and / or 3. Processing is necessary for the performance of a task carried out in the public interest [Art. 6 §1 case e) GDPR]</p>
<p>The study, development, operation, exploitation, management, and maintenance of U.o.W.M.'s Information and Communication Systems</p>	<p>1. Processing is necessary for compliance with a legal obligation [Art. 6 §1 case. c) GDPR] and/or</p> <p>2. Processing is necessary for the performance of a contract [Art. 6 §1 case. b) GDPR] where it exists and / or 3. Processing is necessary for the performance of a task carried out in the public interest [Art. 6 §1 case e) GDPR]</p>
<p>The collection, processing, cross-referencing, and transmission of data of the Tax, Insurance, and Labor Administration exclusively for the support and operation of the framework of their responsibilities</p>	<p>1. Processing is necessary for compliance with a legal obligation [Art. 6 §1 case. c) GDPR] and/or</p> <p>2. Processing is necessary for</p>

	the performance of a task carried out in the public interest [Art. 6 §1 case e) GDPR]
The collection and processing of video data using CCTV, as well as the collection and processing of identification data (e.g., police ID), for security reasons	Processing is necessary for the purposes of the legitimate interests [Art. 6 §1 case f) GDPR]
The collection and processing of the necessary data of employees and / or prospective employees and associates for the proper service of existing employment or cooperation relationships or the consideration of possible future cooperation	1. Processing is necessary for compliance with a legal obligation [Art. 6 §1 case. c) GDPR] and/or 2. Processing is necessary for the purposes of the legitimate interests [Art. 6 §1 case f) GDPR]
The collection and processing of the necessary data of minor children for the intersection of potential benefit or providing social services to students.	1. Processing is necessary for compliance with a legal obligation [Art. 6 §1 case. c) GDPR] and/or 2. Processing is necessary for the performance of a contract [Art. 6 §1 case. b) GDPR]
For any other form of processing, U.o.W.M.and ELKE requests special written, free, and after prior informed consent of the subjects before the start of the processing, if required.	

Table 2. The main purposes and legal bases of processing

The reference to more than one legal basis of processing does not mean that the U.o.W.M. changes them (lawful basis swapping), undermining data subjects' rights. Still, there are cases where more than one legal processing base is applicable.

Furthermore, since U.o.W.M. is part of the Public Administration bodies (according to no. 14 of law 4270/2014 but also the Register of Services and Bodies of the Greek Administration), further process is applied after the end of elaboration to archive in the public interest or for scientific or historical research or statistical purposes, which is not considered incompatible with the original purposes according to Art. 5 paragraph 1, case b) and Art. 89 paragraph 1 of GDPR.

Finally, the P.D.M. does not use the consent of the data subjects (whether it is simple data or special categories) as the main processing base, recognizing the inherent inequality that exists about the data subjects at any time and under the recommendations of its Working Group No. 29 (now European Data Protection Council). However, and exceptionally, for a few cases where additional service is provided to the subjects (beyond the legal ones), the consent is used to a limited extent as a legal basis for processing and only then.

Rights of Data Subjects

U.o.W.M. recognizes individuals' rights concerning the protection of their personal data.

Thus, natural persons have the right to:

1. Be informed about the processing of their personal data.
2. Gain access to the personal data concerning them.
3. Request the correction of incorrect, inaccurate, or incomplete personal data.
4. Request the deletion of personal data when it is no longer necessary or if the processing is illegal. If applied as a legal basis for processing Art.6 par.1 case. e) GDPR (processing for the fulfilment of a duty performed in the public interest or during the exercise of public power and the Art.9 par.2 case b), g), j) in most of the processes of U.o.W.M., the right of deletion is limited and will be evaluated on a case-by-case basis under strict conditions. According to Art. 4 of the Explanatory Memorandum of the GDPR, the right to personal data protection is not absolute; it must be valued concerning its functioning in society and weighed against other fundamental rights under the principle of proportionality.
5. Oppose personal data processing for reasons related to their unique situation, subject to Art.21 par.6 of GDPR.
6. Apply for a restriction on personal data processing in specific cases.
7. Express their opinion and challenge the decision.
8. Submit a complaint to the Hellenic Data Protection Authority.

These rights are valid in the entire application of the GDPR, regardless of where the data processing occurs and where U.o.W.M.is based.

Processing principles

U.o.W.M. accepts the basic principles governing the processing of personal data.

According to article 5 of GDPR, personal data shall be:

1. processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency'),
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation'),
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'),
4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy'),

5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation'),
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

U.o.W.M. keeps a record of the processing activities for which it is responsible. That record contains all of the following information:

1. the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer,
2. the purposes of the processing,
3. a description of the categories of data subjects and of the categories of personal data,
4. the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations,
5. where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards,
6. where possible, the envisaged time limits for erasure of the different categories of data,
7. where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

Protection of Personal Data

Taking into account the nature, the scope, the context, and the purposes of the processing, as well as the risks of the different probability of occurrence and seriousness for the rights and freedoms of natural persons, U.o.W.M. apply appropriate technical and organizational measures to ensure and be able to prove that the processing is carried out under the Regulation.

During the assessment of the appropriate security level by U.o.W.M., account shall be taken in particular of the risks arising from the processing, particularly from an accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to personal data transmitted, stored, or otherwise processed.

In case of a personal data breach (article 33), U.o.W.M. as the controller shall notify without delay and, if possible, within 72 hours of becoming aware of the breach of personal data to the supervisory authority responsible under Article 55, unless a breach of personal data does not endanger the rights and freedoms of individuals. When the notification to the supervisory authority is not made within 72 hours, it will be accompanied by a justification for the delay.

Staff Training

U.o.W.M. accepts that the protection of personal data presupposes the awareness of its human resources regarding personal data protection. In this regard, agrees with the adoption and implementation of the following:

1. Orientation of appropriate training by exploiting Fair Information Practices (FIP), which condense a set of standards governing the collection and use of personal data and addressing issues of privacy and accuracy. Human resources cannot become experts in the field of privacy protection overnight, however, their familiarity with the international requirements of privacy protection is possible and necessary. Employees who have crucial roles in privacy need to acquire more specific knowledge. For most of the workforce, however, a thorough understanding of privacy's general principles is essential.
2. U.o.W.M. seeks to raise awareness of fundamental concepts of personal data protection on its human resources. This in no way means that its staff's training is too theoretical or abstract. Instead, it becomes a practice. The core of education focuses on three simple but essential issues:
 - a. Motivation: Why should employees care about privacy?
 - b. Definition: What is personal data?
 - c. Responsibility: What should employees know about how U.o.W.M. is accountable for privacy?

Communication of Natural Persons

The above rights, as well as any rights related to personal data, are exercised upon a written request submitted to any point that is accessible to the public or via electronic communication by sending a message to dpo@uowm.gr and is also examined by the Data Protection Officer, as defined by U.o.W.M.

Modification

This policy may need to be amended concerning the processing of personal data. In case the modification of the terms in question is of such nature and extent that the above data processing terms do not cover it, U.o.W.M. must make public the new version of the policy.