Συχνές ερωτήσεις – απαντήσεις για τον ΓΚΠΔ (GDPR ΕΕ 2016/679)

1. **Τι είναι τα «δεδομένα προσωπικού χαρακτήρα»**

«δεδομένα προσωπικού χαρακτήρα» (Αρ 4 ΓΚΠΔ) είναι κάθε πληροφορία που αφορά ταχτοποιημένο 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. **Τι είναι η «επεξεργασία δεδομένων»**

«επεξεργασία» (Αρ 4 ΓΚΠΔ) 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,

3. **Τι είναι ο «εκτελών την επεξεργασία»**

«εκτελών την επεξεργασία» (Αρ 4 ΓΚΠΔ) : το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας,

4. **Τι είναι η «παραβίαση δεδομένων προσωπικού χαρακτήρα»**

«παραβίαση δεδομένων προσωπικού χαρακτήρα» (Αρ 4 ΓΚΠΔ): 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.

Η εταιρεία ή ο οργανισμός σας πρέπει να ειδοποιήσει την εποπτική αρχή χωρίς αδικαιολόγητη καθυστέρηση και το **αργότερο εντός 72 ωρών** αφού αντιληφθεί την παραβίαση. Εάν η εταιρεία ή ο οργανισμός σας είναι ο εκτελών την επεξεργασία, πρέπει να ενημερώνει τον **υπεύθυνο επεξεργασίας δεδομένων** για κάθε παραβίαση δεδομένων.

Εάν η παραβίαση δεδομένων θέτει σε υψηλό κίνδυνο τα φυσικά πρόσωπα που επηρεάζονται, τότε πρέπει επίσης να ενημερωθεί το καθένα εξ αυτών, εκτός εάν έχουν τεθεί σε εφαρμογή αποτελεσματικά τεχνικά και οργανωτικά μέτρα προστασίας ή άλλα μέτρα που διασφαλίζουν ότι ο κίνδυνος δεν είναι πλέον πιθανό να προκύψει.

5. Ποια δεδομένα προσωπικού χαρακτήρα θεωρούνται «ειδικών κατηγοριών δεδομένα προσωπικού χαρακτήρα» («*ευαίσθητα δεδομένα» κατά προγενέστερο ορισμό***);** (ΓΚΠΔ - Άρθρο 4 σημεία 13, 14 και 15, άρθρο 9)

Τα παρακάτω δεδομένα προσωπικού χαρακτήρα θεωρούνται «ευαίσθητα» και υπόκεινται σε συγκεκριμένες προϋποθέσεις επεξεργασίας:

- ✓ δεδομένα προσωπικού χαρακτήρα που αποκαλύπτουν φυλετική ή εθνοτική καταγωγή, πολιτικά φρονήματα, θρησκευτικές ή φιλοσοφικές πεποιθήσεις·
- ✓ συμμετοχή σε συνδικαλιστική οργάνωση·
- ✓ γενετικά δεδομένα, βιομετρικά δεδομένα που υποβάλλονται σε επεξεργασία αποκλειστικά για την ταυτοποίηση ενός ατόμου·
- ✓ δεδομένα σχετικά με την υγεία·
- ✓ δεδομένα σχετικά με τη σεξουαλική ζωή ή τον γενετήσιο προσανατολισμό ενός ατόμου.

6. Πώς πρέπει να διεκπεραιώνονται τα αιτήματα ατόμων που ασκούν τα δικαιώματά τους σχετικά με την προστασία των δεδομένων;

(*Άρθρα 12 και 15 έως 22*)
Φυσικά πρόσωπα μπορούν να επικοινωνήσουν με την εταιρεία ή τον οργανισμό σας με σκοπό την άσκηση των δικαιωμάτων τους σύμφωνα με τον ΓΚΠΔ (δικαιώματα πρόσβασης, διόρθωσης, διαγραφής, φορητότητας κ.λπ.). Όταν τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία **με ηλεκτρονικά μέσα**, η εταιρεία ή ο οργανισμός σας θα πρέπει να παρέχει μέσα για την υποβολή ηλεκτρονικών αιτημάτων. Επιπλέον, πρέπει να απαντά στα αιτήματα που λαμβάνει χωρίς αδικαιολόγητη καθυστέρηση και κατ' αρχή εντός ενός μηνός από τη λήψη του αιτήματος.

Η εταιρεία ή ο οργανισμός σας μπορεί να ζητά περαιτέρω πληροφορίες από τα πρόσωπα που έχουν υποβάλει αίτημα, για να επιβεβαιώσει την ταυτότητά τους.

Εάν η εταιρεία ή ο οργανισμός σας απορρίψει το αίτημα, πρέπει να ενημερώσει το άτομο σχετικά με τους λόγους για τους οποίους το έκανε και σχετικά με το δικαίωμα του ατόμου να υποβάλει καταγγελία ενώπιον της αρχής προστασίας δεδομένων και να επιδιώξει έννομη προστασία.

Η επεξεργασία αιτημάτων φυσικών προσώπων θα πρέπει να γίνεται δωρεάν. Όταν τα αιτήματα είναι προδήλως αβάσιμα ή υπερβολικά, ιδίως λόγω του επαναλαμβανόμενου χαρακτήρα τους, μπορείτε να χρεώσετε εύλογο τέλος ή να αρνηθείτε να δώσετε συνέχεια.

7. Ποιοι οργανισμοί πρέπει να ορίζουν ΥΠΔ - DPO;
Ο ορισμός DPO είναι υποχρεωτικός όταν:

- Η επεξεργασία διενεργείται από **δημόσια αρχή** ή δημόσιο φορέα (συμπεριλαμβανομένων και φυσικών ή νομικών προσώπων δημοσίου ή ιδιωτικού δικαίου που ασκούν δημόσια εξουσία). Εξαιρούνται τα δικαστήρια όταν ενεργούν υπό τη δικαιοδοτική τους αρμοδιότητα.
- Απαιτείται τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε μεγάλη κλίμακα (π.χ. ασφαλιστικές ή τραπεζικές υπηρεσίες, υπηρεσίες τηλεφωνίας ή διαδικτύου, παροχή υπηρεσιών ασφαλείας, όλες οι μορφές παρακολούθησης και διαμόρφωσης «προφίλ» στο διαδίκτυο, όπως για σκοπούς συμπεριφορικής διαφήμισης).

- Διενεργείται μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων (π.χ. στο πλαίσιο παροχής υπηρεσιών υγείας από νοσοκομεία) ή δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα.

Για τον προσδιορισμό της μεγάλης κλίμακας επεξεργασίας πρέπει να λαμβάνονται υπόψη: α) ο αριθμός των εμπλεκομένων υποκειμένων, είτε ως συγκεκριμένος αριθμός είτε ως ποσοστό επί του πληθυσμού, β) ο όγκος και το εύρος των δεδομένων, γ) η διάρκεια ή ο μόνιμος χαρακτήρας της επεξεργασίας, δ) η γεωγραφική έκταση της επεξεργασίας. Παραδείγματα που **δεν** συνιστούν επεξεργασία μεγάλης κλίμακας είναι, μεταξύ άλλων, η επεξεργασία δεδομένων ασθενών από ιδιώτη ιατρό και η επεξεργασία δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα από ιδιώτη δικηγόρο.

8. **Είμαι ιδιοκτήτης εργαστηρίου παροχής υπηρεσιών υγείας και δεν έχω υποχρέωση ορισμού ΥΠΔ – DPO. Οφείλω να συμμορφωθώ με τις απαιτήσεις του ΓΚΠΔ**

- Η απάντηση είναι **ΝΑΙ.**
- Ακόμα και εάν κάποιος υπεύθυνος επεξεργασίας ΔΕΝ έχει νομική υποχρέωση ορισμού ΥΠΔ, έχει υποχρέωση **συμμόρφωσης** με τις συνολικές απαιτήσεις του ΓΚΠΔ

9. **Μπορώ να δίνω αποτελέσματα ιατρικών εξετάσεων σε τρίτους;**
   Η απάντηση αρχικά είναι **ΟΧΙ**. Τα αποτελέσματα εξετάσεων αποτελούν δεδομένα προσωπικού χαρακτήρα (ειδικής κατηγορίας), επομένως πρέπει να διασφαλίσετε ότι δεν τα παρέχετε σε τρίτους που δεν είναι εξουσιοδοτημένοι. Μπορείτε να παρέχετε τα αποτελέσματα μόνο με τη συγκατάθεση του ασθενούς, π.χ. κατά την εξέταση να συμπληρωθεί έντυπο, στο οποίο θα περιέχει τη συγκατάθεση του ασθενούς για παραλαβή των εξετάσεων (ή κάποιας εκτίμησης του εργοθεραπευτή) και τα πλήρη στοιχεία του ατόμου (Όνομα – Επίθετο, Αρ. Δελτίου Ταυτότητας) το οποίο θα παραλάβει τις εξετάσεις.
   Όταν πρόκειται για ανήλικο (παιδί), δικαίωμα πρόσβασης στα ιατρικά δεδομένα του παιδιού (εξετάσεων εκτιμήσεων κ.λ.π.), έχουν αποκλειστικά και μόνο οι γονείς που ασκούν τη γονική μέριμνα. Ακόμα και εάν ένας από τους 2 γονείς (περιπτώσεις διάστασης ή διαζυγίου) ασκεί την «επιμέλεια», δικαίωμα πρόσβασης έχουν και οι 2 γονείς (μητέρα-πατέρας) ως ασκούντες από κοινού τη γονική μέριμνα

Παραδείγματα επαγγελματιών προς συμμόρφωση

Σας παραθέτουμε μερικά **παραδείγματα** επαγγελματιών που οφείλουν να συμμορφωθούν

- ✓ **Ιατρός – Επαγγέλματα Υγείας (π.χ. εργοθεραπευτής),** οι οποίοι μάλιστα επεξεργάζονται ευαίσθητα προσωπικά δεδομένα (ειδικής κατηγορίας)
- ✓ **ΝΠΔΔ** – σύλλογος (Υποχρεωτικά και διορισμός ΥΠΔ - DPO)
- ✓ **Παιδικός σταθμός** που συλλέγει μάλιστα δεδομένα προσωπικού χαρακτήρα ανηλίκου (π.χ. ηλικίες 2-5 ετών). Η εταιρεία (παιδικός σταθμός) μπορεί να επεξεργαστεί δεδομένα προσωπικού χαρακτήρα ενός παιδιού βάσει συγκατάθεσης (*Άρθρα 8 και 12 ΓΚΠΔ*) εφόσον έχει λάβει τη ρητή συγκατάθεση του γονιού ή κηδεμόνα τους μέχρι μια συγκεκριμένη ηλικία. Το όριο ηλικίας για τη λήψη γονικής συγκατάθεσης ποικίλλει από τα 13 έως τα 16 έτη, ανάλογα με την ηλικία

που καθορίζεται εν προκειμένω σε κάθε κράτος μέλος της ΕΕ. Στη συγκεκριμένη περίπτωση πρέπει να διασφαλίζεται ότι οποιαδήποτε πληροφορία και επικοινωνία που απευθύνεται σε ένα παιδί είναι εύκολα προσβάσιμη και σε σαφή και απλή γλώσσα η οποία είναι ευνόητη για ένα παιδί.

- ✓ **Web Site** – eshop το οποίο συλλέγει δεδομένα προσωπικού χαρακτήρα και πιθανώς να καταρτίζει προφίλ των μελών (π.χ. μέσω cookies). Ακόμη και εάν η συλλογή είναι απαραίτητη προς την εκπλήρωση των συμβατικών υποχρεώσεων προς τον αγοραστή (*σχέση πωλητή αγοραστή*), ο ιστότοπος οφείλει να ενημερώσει το μέλος – επισκέπτη (ή αγοραστή) για τη δικαιώματα του και να του παράσχει τις εγγυήσεις για την ασφάλεια και το απόρρητο των δεδομένων που τον αφορούν
- ✓ **Κατάστημα λιανικής πώλησης** το οποίο μάλιστα συλλέγει πληροφορίες από το πελατολόγιο με σκοπό μελλοντικές προωθητικές ενέργειες
- ✓ **Γυμναστήριο,** το οποίο συλλέγει δεδομένα προσωπικού χαρακτήρα των μελών του και πιθανότατα επεξεργάζεται και «ευαίσθητα» δεδομένα με σκοπό δημιουργίας «σωματικού» προφίλ για δημιουργία προγράμματος εκγύμνασης
- ✓ **Παιδότοπος,** ο οποίος εκτός των απαραίτητων πληροφοριών που συλλέγει για τα ανήλικα (όνομα επίθετο κ.λ.π.) πιθανότατα να προβαίνει σε τακτική και συστηματική παρακολούθηση των «υποκείμενων» (π.χ. με σταθερή παρακολούθηση μέσω κάμερας ή/και WebCam)
- ✓ **Φροντιστήριο μέσης εκπαίδευσης – ξένων γλωσσών ,** το οποίο συλλέγει δεδομένα προσωπικού χαρακτήρα ανήλικων μαθητών, πιθανότατα δε και για ηλικίες<15-16.

Για οποιαδήποτε απορία που αφορά αποκλειστικά σε θέματα προστασίας δεδομένων προσωπικού χαρακτήρα, παρακαλούμε να στείλετε email στην διεύθυνση: privacy@pse.org.gr

Τα ερωτήματα θα συγκεντρωθούν, έτσι ώστε να απαντηθούν αρχικά με τη μορφή ερωτήσεων – απαντήσεων.