

Εφαρμογή του Κανονισμού (ΕΕ) 679/2016 για την προστασία προσωπικών δεδομένων και της εθνικής νομοθεσίας (Νόμος 125(Ι)/2018)

Μητρόπολη Λεμεσού

Γραφείο Επιτρόπου Προστασίας
Δεδομένων Προσωπικού Χαρακτήρα

5 Μαρτίου 2019

1

Προσωπικά δεδομένα

- **Απλά δεδομένα** – δεδομένα θέσης και επιγραμμικά (on line) αναγνωριστικά στοιχεία ταυτότητας τα οποία παρέχονται από συσκευές, εφαρμογές, εργαλεία και πρωτόκολλα τους και διευκολύνουν τον εντοπισμό του φυσικού προσώπου π.χ. IP address, εντοπισμός θέσης μέσω GPS)
- **Ειδικές κατηγορίες δεδομένων**
 - **γενετικά δεδομένα:** τα χαρακτηριστικά φυσικού προσώπου που κληρονομήθηκαν ή αποκτήθηκαν και τα οποία παρέχουν μοναδικές πληροφορίες για το εν λόγω φυσικό πρόσωπο π.χ. DNA
 - **βιομετρικά δεδομένα:** τα δεδομένα τα οποία προκύπτουν από ειδική τεχνική επεξεργασία, η οποία επιτρέπει ή επιβεβαιώνει την αδιαμφισβήτητη ταυτοποίηση φυσικού προσώπου π.χ. φωτογραφία, δακτυλικά αποτυπώματα, ίριδα, παλάμη, φωνή κτλ)

2

Υπεύθυνος Επεξεργασίας

- Το νομικό πρόσωπο που καθορίζει τους σκοπούς και τον τρόπο επεξεργασίας προσωπικών δεδομένων
- Για σκοπούς εφαρμογής του Κανονισμού:
 - η Μητρόπολη Λεμεσού συνιστά υπεύθυνο επεξεργασίας
 - και
 - έκαστος ναός / εκκλησία ως ξεχωριστή νομική οντότητα συνιστά υπεύθυνο επεξεργασίας

3

Εκτελών την επεξεργασία

- Φυσικό ή νομικό πρόσωπο που επεξεργάζεται προσωπικά δεδομένα για λογαριασμό του υπευθύνου επεξεργασίας

π.χ. εταιρεία (ή φυσικό πρόσωπο) που συνάπτει σύμβαση με τη Μητρόπολη / εκκλησία για παροχή υπηρεσιών πληροφορικής / λογιστικών υπηρεσιών

4

Τήρηση των Αρχών νόμιμης επεξεργασίας

- Αρχή της νομιμότητας, αντικειμενικότητας και διαφάνειας της επεξεργασίας
- Αρχή του περιορισμού του σκοπού
- Αρχή της ελαχιστοποίησης των δεδομένων
- Αρχή του περιορισμού της περιόδου αποθήκευσης
- Αρχή της ακεραιότητας και εμπιστευτικότητας
- Αρχής της Λογοδοσίας

5

Κυριότερες Υποχρεώσεις Μητρόπολης Λεμεσού και εκκλησιών

1. Φέρει το βάρος της απόδειξης όσον αφορά στην παροχή συγκατάθεσης

π.χ. η Μητρόπολη / εκκλησία πρέπει να αποδείξει ότι παρείχε σε τρίτο, μη εξουσιοδοτημένο πρόσωπο, αντίγραφο πιστοποιητικού γάμου με τη συγκατάθεση των επηρεαζόμενων προσώπων

2. Υποχρέωση κατασκευαστών στο στάδιο του σχεδιασμού και εξ' ορισμού

- Π.χ. εταιρεία που θα κατασκευάσει το λογισμικό για λογαριασμό της εκκλησίας
- Π.χ. εκκλησία που θα δημιουργήσει αρχείο έκδοσης πιστοποιητικών

3. Υποχρέωση καθορισμού ευθυνών μέσω συμφωνίας όταν υπάρχουν από κοινού υπεύθυνοι επεξεργασίας

π.χ. σύναψη συμφωνίας μεταξύ Μητρόπολης Λεμεσού και εκκλησιών

6

4. **Επιλογή εκτελούντων την επεξεργασία** που παρέχουν επαρκείς διαβεβαιώσεις για την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων
5. **Τήρηση αρχείων των δραστηριοτήτων επεξεργασίας**
6. **Υποχρέωση τήρησης της ασφάλειας της επεξεργασίας**
 - Ο υπεύθυνος επεξεργασίας αξιολογεί τους κινδύνους της επεξεργασίας και εφαρμόζει μέτρα για τον μετριασμό τους π.χ. μέσω κρυπτογράφησης
 - Γίνεται εκτίμηση του ενδεδειγμένου επιπέδου ασφαλείας, λαμβάνοντας υπόψη τους κινδύνους που απορρέουν από την επεξεργασία (π.χ. από παράνομη καταστροφή, απώλεια, πρόσβαση στον εξυπηρετητή από hackers, κλοπή εγγράφων, διαρροή δεδομένων κ.λ.π.)

7

➤ **Λήψη μέτρων για φυσική ασφάλεια:**

- ❖ Έλεγχος φυσικής πρόσβασης π.χ ηλεκτρονικός εξοπλισμός και απόρρητα έγγραφα σε δωμάτια ασφαλείας με ελεγχόμενη και περιορισμένη πρόσβαση, φάκελοι σε φωριαμούς που κλειδώνουν και μηχανισμοί ελέγχου πρόσβασης
- ❖ Ασφάλεια από φυσικές καταστροφές ή κακόβουλες πράξεις
- ❖ Προστασία φορητών μέσων αποθήκευσης / Κλειδαριές ασφαλείας

8

➤ **Λήψη μέτρων για τεχνική ασφάλεια**

- ❖ Antivirus /ασφάλεια επικοινωνιών και λογισμικού
- ❖ Firewalls
- ❖ Backups (να φυλάσσονται σε ασφαλές μέρος)
- ❖ Επίπεδα πρόσβασης

7. Υποχρέωση γνωστοποίησης παραβιάσεων ασφάλειας
8. Υποχρέωση ανακοίνωσης παραβιάσεων ασφάλειας
9. Διενέργεια Εκτίμησης Αντικτύπου και Προηγούμενη Διαβούλευση: θα πρέπει να εκτιμώνται οι πιθανότητες επέλευσης κινδύνων και οι συνέπειες στα προσωπικά δεδομένα
10. Ορισμός Υπεύθυνου Προστασίας Δεδομένων

9

Δικαιώματα

- Δικαίωμα ενημέρωσης
- Δικαίωμα πρόσβασης
- Δικαίωμα διόρθωσης
- Δικαίωμα διαγραφής «Δικαίωμα στη λήθη»
- Δικαίωμα περιορισμού
- Δικαίωμα στη φορητότητα των δεδομένων
- Δικαίωμα εναντίωσης
- Δικαίωμα αντίρρησης σε αυτοματοποιημένη απόφαση περιλαμβανομένης της κατάρτισης προφίλ

10

Αρμόδια Εποπτική Αρχή

- Ανεξάρτητη, χωρίς εξωτερικές επιρροές, δεν ζητεί ούτε λαμβάνει οδηγίες από κανέναν
- Τα μέλη της διορίζονται με διαφανή διαδικασία και απέχουν από κάθε πράξη ασυμβίβαστη προς τα καθήκοντά τους
- Διαθέτει τους απαραίτητους ανθρώπινους, τεχνικούς και οικονομικούς πόρους και τις αναγκαίες εγκαταστάσεις και υποδομές
- Διαθέτει δικούς της υπαλλήλους
- Υπόκειται σε οικονομικό έλεγχο ο οποίος δεν επηρεάζει την ανεξαρτησία της και διαθέτει δικό της ετήσιο προϋπολογισμό
- Τα μέλη και οι υπάλληλοι δεσμεύονται από το επαγγελματικό απόρρητο κατά τη διάρκεια της θητείας και μετά το πέρας αυτής
- Δια νόμου προβλέπεται η σύσταση της εποπτικής αρχής, τα προσόντα, η διάρκεια θητείας των μελών *(δεν πρέπει να είναι μικρότερη από 4 χρόνια)*

11

Εξουσίες Επιτρόπου

- Εισάγονται αυξημένες εξουσίες
 - Εγκρίνει πιστοποιητικά και κριτήρια πιστοποίησης
 - Προβαίνει σε επανεξέταση των πιστοποιήσεων
 - Παρέχει διαπίστευση σε φορείς πιστοποίησης
 - Εκδίδει γνώμες για σχέδια κωδίκων δεοντολογίας και τα εγκρίνει
 - Εγκρίνει δεσμευτικούς εταιρικούς κανόνες
 - Εγκρίνει τυποποιημένες ρήτρες
- Επιβάλλει αυξημένα διοικητικά πρόστιμα

12

Διοικητικές κυρώσεις

- Εντολή στον υπεύθυνο επεξεργασίας/εκτελούντα να παράσχουν οποιαδήποτε πληροφορία
- Διεξαγωγή έρευνας με τη μορφή ελέγχου
- Ειδοποίηση στον υπεύθυνο επεξεργασίας/εκτελούντα για εικαζόμενη παράβαση
- Πρόσβαση Επιτρόπου σε οποιαδήποτε δεδομένα διατηρεί ο υπεύθυνος επεξεργασίας/εκτελών για εκτέλεση των καθηκόντων της
- Πρόσβαση Επιτρόπου στις εγκαταστάσεις του υπεύθυνου επεξεργασίας/εκτελούντα (περιλαμβανομένων κάθε εξοπλισμού και μέσου επεξεργασίας)

13

- Απευθύνει προειδοποιήσεις στον υπεύθυνο επεξεργασίας /εκτελούντα
- Απευθύνει επιπλήξεις στον υπεύθυνο επεξεργασίας /εκτελούντα
- Δίνει εντολή στον υπεύθυνο επεξεργασίας /εκτελούντα για συμμόρφωση στα αιτήματα των υποκειμένων των δεδομένων για άσκηση των δικαιωμάτων τους
- Δίνει εντολή στον υπεύθυνο επεξεργασίας /εκτελούντα να καθιστούν τις πράξεις επεξεργασίας σύμφωνες με τον Κανονισμό
- Δίνει εντολή στον υπεύθυνο επεξεργασίας να ανακοινώνει την παραβίαση προσωπικών δεδομένων στο υποκείμενο των δεδομένων

14

- Να επιβάλλει προσωρινό ή οριστικό περιορισμό, περιλαμβανομένης και της απαγόρευσης της επεξεργασίας
- Δίνει εντολή διόρθωσης ή διαγραφής των δεδομένων
- Αποσύρει την πιστοποίηση ή διατάζει τον οργανισμό πιστοποίησης να αποσύρει ένα πιστοποιητικό που είχε εκδοθεί
- Δίνει εντολή για αναστολή της κυκλοφορίας δεδομένων σε αποδέκτη σε τρίτη χώρα ή σε διεθνή οργανισμό
- **Διοικητικό πρόστιμο**

15

Διοικητικά πρόστιμα

- **Αυστηρότατα πρόστιμα, με ανώτατο όριο: €10.000.000 ή 2% του παγκόσμιου κύκλου εργασιών** για παραβιάσεις που αφορούν, μεταξύ άλλων:
 - ❖ στις υποχρεώσεις σχετικά με την συγκατάθεση ανηλίκων
 - ❖ στις υποχρεώσεις του υπεύθυνου επεξεργασίας σχετικά με την εκτέλεση καθηκόντων του ΥΠΔ
 - ❖ στην προστασία των προσωπικών δεδομένων από τον σχεδιασμό και εξ ορισμού
- **Το ανώτατο όριο είναι €20.000.000 ή 4% του παγκόσμιου κύκλου εργασιών** για παραβιάσεις των υποχρεώσεων που σχετίζονται, μεταξύ άλλων:
 - ❖ με τις βασικές αρχές επεξεργασίας
 - ❖ τα δικαιώματα των φυσικών προσώπων
 - ❖ την μη παροχή πρόσβασης στην ΑΠΔΠΧ, προκειμένου να είναι σε θέση να ασκήσει τις εποπτικές της αρμοδιότητες,

16

Ποινικά αδικήματα δυνάμει του Νόμου 125(Ι)/2018

➤ Ποινή φυλάκισης που δεν υπερβαίνει τα 3 έτη ή χρηματική ποινή που δεν υπερβαίνει τις €30.000 ή και οι δύο αυτές ποινές

- Πρόσωπο που δεν τηρεί αρχείο δραστηριοτήτων
- Πρόσωπο που δεν συνεργάζεται με την Επίτροπο
- Πρόσωπο που δεν γνωστοποιεί στην Επίτροπο παραβίαση προσωπικών δεδομένων
- Πρόσωπο που αποτελεί μέρος του εκτελούντα την επεξεργασία ο οποίος δεν ενημερώνει αμελλητί τον υπεύθυνο επεξεργασίας για παραβίαση δεδομένων προσωπικού χαρακτήρα
- Πρόσωπο που δεν ανακοινώνει παραβίαση προσωπικών δεδομένων στο υποκείμενο των δεδομένων

17

- Πρόσωπο που δεν διενεργεί εκτίμηση αντικτύπου
- Πρόσωπο που επεμβαίνει σε σύστημα αρχειοθέτησης προσωπικών δεδομένων ή λαμβάνει γνώση των δεδομένων αυτών ή τα αφαιρεί, αλλοιώνει, βλάπτει, καταστρέφει, επεξεργάζεται, εκμεταλλεύεται με οποιονδήποτε τρόπο, μεταδίδει, ανακοινώνει, τα καθιστά προσιτά σε μη δικαιούμενα πρόσωπα ή επιτρέπει στα πρόσωπα αυτά να λάβουν γνώση των εν λόγω δεδομένων, για σκοπούς επικερδείς ή μη
- Πρόσωπο που εμποδίζει ή παρακωλύει την άσκηση των εξουσιών της Επιτρόπου

18

➤ Ποινή φυλάκισης που δεν υπερβαίνει τα 3 έτη ή χρηματική ποινή που δεν υπερβαίνει τις €30.000 ή και οι δύο αυτές ποινές

Ή όταν το αδίκημα προσβάλλει τα συμφέροντα της Δημοκρατίας ή προκαλεί κίνδυνο για την απρόσκοπτη λειτουργία της Κυβέρνησης ή απειλεί την εθνική ασφάλεια:

➤ Ποινή φυλάκισης που δεν υπερβαίνει τα 5 έτη ή σε χρηματική ποινή που δεν υπερβαίνει τις €50.000 ή και στις δύο αυτές ποινές

- Πρόσωπο που εμποδίζει τον υπεύθυνο προστασίας δεδομένων στην εκτέλεση των καθηκόντων του
- Φορέας πιστοποίησης που χορηγεί ή δεν ανακαλεί πιστοποίηση, βάσει του άρθρου 42 του Κανονισμού,
- Πρόσωπο που διαβιβάζει προσωπικά σε τρίτη χώρα / διεθνή οργανισμό κατά παράβαση του Κανονισμού
- Πρόσωπο που διαβιβάζει προσωπικά δεδομένα σε τρίτη χώρα / διεθνή οργανισμό κατά παράβαση των περιορισμών που επέβαλε η Επίτροπος βάσει των άρθρων 17 ή 18 του Νόμου 125(Ι)/2018

19

➤ Ποινή φυλάκισης που δεν υπερβαίνει το 1 έτος ή χρηματική ποινή που δεν υπερβαίνει τις €10.000 ή και οι δύο αυτές ποινές

- Πρόσωπο που δεν συμμορφώνεται με τις διατάξεις του Κανονισμού και του Νόμου 125(Ι)/2018
- Πρόσωπο που προβαίνει σε συνδυασμό συστημάτων αρχειοθέτησης μεγάλης κλίμακας κατά παράβαση των διατάξεων του άρθρου 10 του Νόμου 125(Ι)/2018

ΣΗΜ.: εάν ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία είναι επιχείρηση ή όμιλος επιχειρήσεων, **νομική ευθύνη φέρει το πρόσωπο που ορίζεται ως το ανώτατο εκτελεστικό όργανο ή σώμα της επιχείρησης ή ομίλου επιχειρήσεων**

20

**Γραφείο Επιτρόπου Προστασίας Δεδομένων
Προσωπικού Χαρακτήρα**

Ιάσονος 1, 1082 Λευκωσία
Τ.Θ. 23378, 1682 Λευκωσία

Τηλ: 22818456, Φαξ: 22304565
E-mail: commissioner@dataprotection.gov.cy

www.dataprotection.gov.cy