




Βέροια 10-05-2018

**ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ  
ΝΟΜΟΣ ΗΜΑΘΙΑΣ  
ΔΗΜΟΣ ΒΕΡΟΙΑΣ  
ΔΙΕΥΘΥΝΣΗ ΠΡΟΓΡΑΜΜΑΤΙΣΜΟΥ –  
ΟΡΓΑΝΩΣΗΣ - ΠΛΗΡΟΦΟΡΙΚΗΣ**

Αριθ. Πρωτ. : Δ.Υ.

ΔΙΕΥΘΥΝΣΗ  : Μητροπόλεως 55 ,  
59100 Βέροια

ΠΡΟΣ: **ΤΟ ΔΗΜΟΤΙΚΟ ΣΥΜΒΟΥΛΙΟ**

ΠΛΗΡΟΦΟΡΙΕΣ  : Μ. Γεωργιάδου

ΤΗΛΕΦΩΝΟ  : 2331350586

Fax :

e-mail : m.georgiadou@veria.gr

**ΘΕΜΑ:** «Έγκριση Διαδικασίας Συμμόρφωσης με τον Γενικό Κανονισμό (ΕΕ) 2016/679 περί Προστασίας Προσωπικών Δεδομένων (General Data Protection Regulation (GDPR))».

### **ΕΙΣΗΓΗΤΙΚΟ ΣΗΜΕΙΩΜΑ**

Από τις 25/5/2018 τίθεται σε υποχρεωτική εφαρμογή ο «Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών.»

Επιπλέον και σύμφωνα με το άρθρο 288 της Ενοποιημένης απόδοσης της Συνθήκης για την Ευρωπαϊκή Ένωση και της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης ο Κανονισμός είναι μία νομική πράξη της Ευρωπαϊκής Ένωσης που «έχει γενική ισχύ. Είναι [δε] δεσμευτικός ως προς όλα τα μέρη του και ισχύει άμεσα σε κάθε κράτος μέλος.» Πρακτικά αυτό σημαίνει ότι η ημερομηνία εφαρμογής είναι απολύτως ανελαστική και ο Κανονισμός τίθεται καθολικά σε ισχύ από τις 25/5/2018.

Διαμορφώνεται μ' αυτόν ένα ενιαίο νομικό πλαίσιο, για όλα τα κράτη –μέλη, χωρίς την ανάγκη ψήφισης εθνικής νομοθεσίας που αφορά τις ιδιωτικές και δημόσιες επιχειρήσεις, καθώς και τις κρατικές αρχές που με οποιοδήποτε τρόπο συγκεντρώνουν, επεξεργάζονται και εν γένει διαχειρίζονται δεδομένα προσωπικού χαρακτήρα πελατών, σχετιζόμενων με τους πελάτες τους, εργαζομένων, συνεργατών ή άλλων φυσικών προσώπων. Κάθε προγενέστερη εθνική η ενωσιακή νομοθεσία καταργείται (σχετ. η οδηγία 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) και ο Νόμος 2472/1997 του Ελληνικού κράτους).

Ο Κανονισμός θεσπίζει όρους που αφορούν την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και κανόνες που αφορούν την ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα με αντικειμενικό σκοπό την προστασία των θεμελιωδών δικαιωμάτων και ελευθεριών των φυσικών προσώπων και ειδικότερα το δικαίωμά τους στην προστασία των δεδομένων προσωπικού χαρακτήρα.

Πέραν των όσων αναλυτικά προβλέπονται στον Κανονισμό η παραβίαση των διατάξεων του Κανονισμού ή/και η μη συμμόρφωση προς τις εντολές της Εποπτικής Αρχής (Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα) επισύρει σύμφωνα με το άρθρο 83 του



**ΔΙΕΥΘΥΝΣΗ ΠΡΟΓΡΑΜΜΑΤΙΣΜΟΥ –  
ΟΡΓΑΝΩΣΗΣ - ΠΛΗΡΟΦΟΡΙΚΗΣ**

Μητροπόλεως 55 , 59123 Βέροια

Email: [m.georgiadou@veria.gr](mailto:m.georgiadou@veria.gr)

Έκδοση 2<sup>η</sup>

Σελίδα 1 από 3

Κανονισμού διοικητικά πρόστιμα που δύναται να ανέλθουν ανάλογα με τις περιστάσεις κάθε μεμονωμένης περίπτωσης έως και 20.000.000,00 € (είκοσι εκατομμύρια ευρώ) ή, σε περίπτωση επιχειρήσεων, έως το 4 % του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους, ανάλογα με το ποιο είναι υψηλότερο.

Ο Κανονισμός 2016/679 έχει εφαρμογή σε όλες τις κρατικές αρχές που με οποιοδήποτε τρόπο συγκεντρώνουν, επεξεργάζονται και εν γένει διαχειρίζονται δεδομένα προσωπικού χαρακτήρα πελατών, σχετιζόμενων με τους πολίτες, εργαζομένους, συνεργάτες ή άλλα φυσικά πρόσωπα, είτε έχουν έδρα και δραστηριότητα σε χώρα της Ευρωπαϊκής Ένωσης είτε όχι, εφόσον τα δεδομένα αφορούν Ευρωπαίους πολίτες ή σχετίζονται με οποιοδήποτε είδους υπηρεσίες και αγαθά προς Ευρωπαίους πολίτες.

Σύμφωνα με τον GDPR, θα πρέπει να εφαρμοστεί ένα ευρύ φάσμα μέτρων, προκειμένου να διασφαλιστεί ότι θα μειωθεί ο κίνδυνος υπέρβασης του Κανονισμού και θα επιτρέπεται σε κάθε φορέα να αποδείξει ότι λαμβάνει τη διαχείριση των δεδομένων προσωπικού χαρακτήρα πολύ σοβαρά.

Μεταξύ των αναγκαίων μέτρων λογοδοσίας είναι: αξιολόγηση των επιπτώσεων προσωπικών δεδομένων, έλεγχος, αξιολόγηση της πολιτικής, διατήρηση αρχείων κ.λ.π..

Βασικές προβλέψεις του Γενικού Κανονισμού Προστασίας Δεδομένων είναι περιορισμοί που τίθενται σε ότι αφορά :

- την επεξεργασία των προσωπικών δεδομένων σε όλο τον κύκλο ζωής τους, από τη συλλογή έως και την καταστροφή τους,
- τη δυνατότητα μεταφοράς τους σε άλλες χώρες,
- την προστασία των δικαιωμάτων των φυσικών προσώπων,
- την ασφάλεια (εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα) των προσωπικών δεδομένων και τις ενέργειες γνωστοποίησης που οφείλει να κάνει η επιχείρηση σε περίπτωση παραβίασης.

Οι οργανισμοί που υπόκεινται στην τήρηση του κανονισμού θα πρέπει:

1. να τηρούν τις βασικές αρχές προστασίας των προσωπικών δεδομένων, δηλαδή να τα συλλέγουν για συγκεκριμένο νόμιμο σκοπό και μόνο όσα εξ' αυτών είναι απαραίτητα,
2. να μην τα υποβάλουν σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο με το σκοπό για τον οποίο συλλέχθηκαν, να τα επικαιροποιούν,
3. να τα αποθηκεύουν για το μικρότερο δυνατό χρονικό διάστημα που απαιτείται, να λαμβάνουν - κατά περίπτωση - την ελεύθερη και σαφή συγκατάθεση των φυσικών προσώπων,
4. να τα μεταφέρουν σε χώρες εκτός ΕΕ μόνον υπό συγκεκριμένες προϋποθέσεις, να δίνουν πρόσβαση στα προσωπικά δεδομένα σε συνεργάτες τους μόνον υπό συγκεκριμένες συνθήκες και εφόσον αυτοί αποδεικνύουν τη συμμόρφωσή τους με τον νέο κανονισμό,
5. να αναπτύξουν ηλεκτρονικά εργαλεία για την έγκαιρη και δωρεάν ανταπόκριση σε αιτήματα που θα ανακύπτουν.
6. να γνωστοποιούν κατάλληλα και εγκαίρως στα φυσικά πρόσωπα τα δικαιώματά τους να εξασφαλίζουν την ασφάλεια των προσωπικών δεδομένων σε όλο τον κύκλο ζωής τους,
7. να τηρούν σε αρχείο και να γνωστοποιούν κάθε παραβίαση των δεδομένων εντός 72 ωρών στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και στα φυσικά πρόσωπα με απευθείας ενημέρωση ή δημόσια ανακοίνωση,
8. να αποδεικνύουν ότι τηρούν όλες τις απαιτήσεις του Κανονισμού.

Οι οργανισμοί που υπόκεινται στην τήρηση του κανονισμού έχουν να αντιμετωπίσουν στα πλαίσια του νέου κανονισμού τα ακόλουθα προβλήματα:



1. Ακριβής γνώση για το ποια δεδομένα συλλέγουν και επεξεργάζονται σε κάθε φάση των δραστηριοτήτων τους, ποιοι εμπλέκονται και με ποια εργαλεία και με ποιες διαδικασίες γίνεται η επεξεργασία αυτή,
2. Ακριβής καθορισμός και διαχωρισμός των επιχειρησιακών αναγκών, ώστε να διασφαλίζονται όλες οι απαιτούμενες συγκαταθέσεις του υποκειμένου και να μη γίνεται πλεονάζουσα επεξεργασία,
3. Συστηματικός έλεγχος για την κάλυψη των απαιτήσεων του κανονισμού σε κάθε στάδιο επεξεργασίας των δεδομένων,
4. Αξιολόγηση των κινδύνων που ενδέχεται να οδηγήσουν σε παραβίαση των προσωπικών δεδομένων, με αποτέλεσμα βαρύτερες οικονομικές κυρώσεις και επιπτώσεις στην φήμη.

Στα πλαίσια λοιπόν εφαρμογής του νέου κανονισμού θα πρέπει ο φορέας/οργανισμός να προχωρήσει στην:

- A. Αποτύπωση υπάρχουσας κατάστασης
- B. Διεξαγωγή Αξιολόγησης – αποτίμησης της ασφάλειας του πληροφοριακού συστήματος
- C. Σύνταξη έκθεσης – Κατάρτιση σχεδίου συμμόρφωσης
- D. Στάδιο εφαρμογής- Υλοποίηση προτεινομένων μέτρων- Επίτευξη συμμόρφωσης
- E. Επαναξιολόγηση
- F. Υπηρεσίες Υπευθύνου Προστασίας Δεδομένων

Κατόπιν αυτών εισηγούμαστε:

- Τη λήψη απόφασης από το Δ.Σ. για την έγκριση συμμόρφωσης του Δήμου στα πλαίσια του νέου ενιαίου νομικού πλαισίου, που αφορά στην εφαρμογή του νέου Ευρωπαϊκού Κανονισμού Ε/Ε 2016/679 (General Data Protection Regulation, GDPR).

Ο ΔΗΜΑΡΧΟΣ

ΚΩΝ/ΝΟΣ ΒΟΡΓΙΑΖΙΔΗΣ



ΔΙΕΥΘΥΝΣΗ ΠΡΟΓΡΑΜΜΑΤΙΣΜΟΥ –  
ΟΡΓΑΝΩΣΗΣ - ΠΛΗΡΟΦΟΡΙΚΗΣ

Μητροπόλεως 55 , 59123 Βέροια  
Email: [m.georgiadou@veria.gr](mailto:m.georgiadou@veria.gr)

Έκδοση 2<sup>η</sup>  
Σελίδα 3 από 3