ΔΗΜΟΣ ΚΙΛΚΙΣ

Διαδικασία Γνωστοποίησης Παραβίασης Προσωπικών Δεδομένων

Personal Data Breach Notification Procedure

ΔΗΜΟΣ ΚΙΛΚΙΣ

Διαδικασία Γνωστοποίησης Παραβιάσεων Προσωπικών Δεδομένων

Personal Data Breach Notification Procedure

Ταξινόμηση Εγγράφου:	**Εσωτερικό Έγγραφο**
Έγγραφο Ανάφ.	**GDPR-DOC-18**
Έκδοση:	**1**
Χρονολογημένο:	**29 Νοεμβρίου 2018**
Συντάκτης Εγγράφου:	**Proset I.K.E**

Ιστορικό Αλλαγών

Έκδοση	Ημερομηνία	Σύνοψη αλλαγών

Έγκριση

Όνομα	Θέση	Υπογραφή	Ημερομηνία

Περιεχόμενα

Κατάλογος Πινάκων

1 Εισαγωγή

Αυτή η διαδικασία προορίζεται να χρησιμοποιηθεί όταν συμβεί ένα περιστατικό κάποιου είδους, που έχει ως αποτέλεσμα ή πιστεύεται ότι έχει οδηγήσει σε απώλεια προσωπικών δεδομένων για τα οποία ο οργανισμός είναι υπεύθυνος επεξεργασίας. Αυτό το έγγραφο θα πρέπει να χρησιμοποιείται σε συνδυασμό με τη διαδικασία GDPR-DOC-15 Διαδικασία Αντιμετώπισης Περιστατικών της Ασφάλειας Πληροφοριών που περιγράφει τη συνολική διαδικασία αντίδρασης σε ένα περιστατικό που επηρεάζει την ασφάλεια πληροφοριών του «Δήμου Κιλκίς»

Είναι υποχρέωση από τον GDPR τα περιστατικά που επηρεάζουν δεδομένα προσωπικού χαρακτήρα και ενδέχεται να θέσουν σε κίνδυνο τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων να αναφέρονται χωρίς αδικαιολόγητη καθυστέρηση στην εποπτική αρχή προστασίας δεδομένων, και όπου είναι εφικτό, εντός 72 ωρών από τη στιγμή που της επίγνωσης της παραβίασης. Σε περίπτωση που δεν επιτευχθεί ο στόχος των 72 ωρών, πρέπει να δοθούν λόγοι για την καθυστέρηση.

Όταν ένα περιστατικό επηρεάζει δεδομένα προσωπικού χαρακτήρα, πρέπει να ληφθεί απόφαση σχετικά με την έκταση, το χρονοδιάγραμμα και το περιεχόμενο της επικοινωνίας με τα πρόσωπα στα οποία αναφέρονται τα δεδομένα. Το GDPR απαιτεί ότι η επικοινωνία πρέπει να πραγματοποιείται «χωρίς αδικαιολόγητη καθυστέρηση» εάν η παραβίαση ενδέχεται να οδηγήσει σε «υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων».

Οι ενέργειες που περιγράφονται στο παρόν έγγραφο πρέπει να χρησιμοποιούνται μόνο ως καθοδήγηση όταν πρόκειται να ανταποκριθείτε σε ένα περιστατικό. Η ακριβής φύση ενός συμβάντος και ο αντίκτυπός του δεν μπορούν να προβλεφθούν με κανένα βαθμό βεβαιότητας και έτσι είναι σημαντικό να χρησιμοποιείται ένας καλός βαθμός κοινής λογικής όταν αποφασίζεται τι πρέπει να γίνει. Ωστόσο, τα βήματα που παρατίθενται εδώ, είναι απολύτως χρήσιμα για την εξασφάλιση της εκπλήρωσης των υποχρεώσεών της εταιρείας βάσει του GDPR.

2 Διαδικασία Γνωστοποίησης Παραβίασης Προσωπικών Δεδομένων

Μόλις αποφασιστεί ότι έχει σημειωθεί παραβίαση προσωπικών δεδομένων, υπάρχουν δύο μέρη που μπορεί να απαιτείται από το GDPR να ενημερωθούν. Αυτά είναι:

1. Η εποπτική αρχή
2. Τα υποκείμενα των δεδομένων που επηρεάζονται από την παραβίαση

Η γνωστοποίηση της παραβίασης δεν είναι ούτε προκαθορισμένη ενέργεια ούτε εκτελείται με προκαθορισμένο τρόπο. Αντιθέτως, εξαρτάται από την εκτίμηση του κινδύνου η παραβίαση αντιπροσωπεύει *«στα δικαιώματα και τις ελευθερίες των φυσικών προσώπων» (άρθρο 33 του GDPR).* Οι ακόλουθες ενότητες περιγράφουν τον τρόπο με τον οποίο πρέπει να ληφθεί αυτή η απόφαση και τι πρέπει να γίνει εάν απαιτείται ειδοποίηση.

2.1 Η Εποπτική Αρχή

Η εποπτική αρχή για τους σκοπούς του GDPR για το «Δήμο Κιλκίς» έχει ως εξής:

Όνομα:	Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
Διεύθυνση:	Κηφισίας 1-3, Τ.Κ. 115 23, Αθήνα
Τηλέφωνο:	210 6475600
Fax:	210 6475628
Email:	contact@dpa.gr
Web:	http://www.dpa.gr/

Πίνακας 1 – Στοιχεία επικοινωνίας με την Εποπτική Αρχή

2.1.1 Αποφασίζοντας αν θα ειδοποιηθεί η Εποπτική Αρχή

Ο Κανονισμός αναφέρει ότι η παραβίαση προσωπικών δεδομένων πρέπει να γνωστοποιείται στην εποπτική αρχή *"εκτός αν η παραβίαση προσωπικών δεδομένων δεν ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων" (GDPR άρθρο 33).* Αυτό απαιτεί ο οργανισμός να εκτιμήσει το επίπεδο κινδύνου πριν αποφασίσει αν θα ειδοποιήσει ή όχι.

Οι παράγοντες που πρέπει να λαμβάνονται υπόψη στο πλαίσιο αυτής της εκτίμησης κινδύνου πρέπει να περιλαμβάνουν:

- Εάν τα προσωπικά δεδομένα ήταν κρυπτογραφημένα
- Εάν ήταν κρυπτογραφημένα, η ισχύς της κρυπτογράφησης που χρησιμοποιήθηκε
- Σε ποιο βαθμό τα δεδομένα ψευδωνυμοποιήθηκαν (δηλ. εάν τα άτομα μπορούν εύλογα να αναγνωριστούν από τα δεδομένα)
- Τα στοιχεία δεδομένων που περιλαμβάνονται πχ. όνομα, διεύθυνση, στοιχεία υγείας κοκ
- Ο όγκος των εμπλεκόμενων δεδομένων
- Ο αριθμός των υποκειμένων των δεδομένων που επηρεάζονται
- Η φύση της παραβίασης, πχ. κλοπή, τυχαία καταστροφή

- Όποιοι άλλοι παράγοντες θεωρούνται σχετικοί

Η ομάδα ΟΑΠ (Ομάδα Αντιμετώπισης Παραβίασης*)* προβαίνει σε εκτίμηση του κινδύνου όπως περιγράφεται στο ***GDPR-DOC-15 Διαδικασία Αντιμετώπισης Περιστατικών της Ασφάλειας Πληροφοριών***

Η μέθοδος εκτίμησης του κινδύνου, η λογική και τα συμπεράσματά του θα πρέπει να τεκμηριώνονται πλήρως και να υπογράφονται από την ανώτατη διοίκηση. Το αποτέλεσμα της εκτίμησης κινδύνου πρέπει να περιλαμβάνει ένα από τα ακόλουθα συμπεράσματα:

1. Η παραβίαση των προσωπικών δεδομένων δεν απαιτεί ειδοποίηση
2. Η παραβίαση των προσωπικών δεδομένων απαιτεί γνωστοποίηση μόνο στην εποπτική αρχή
3. Η παραβίαση των προσωπικών δεδομένων απαιτεί γνωστοποίηση τόσο στην εποπτική αρχή όσο και στα ενδιαφερόμενα πρόσωπα στα οποία αναφέρονται τα δεδομένα

Αυτά τα συμπεράσματα ενδέχεται να υπόκεινται σε αλλαγές που βασίζονται στην ανατροφοδότηση από την εποπτική αρχή και σε άλλες πληροφορίες που ανακαλύπτονται στο πλαίσιο της διεξαγόμενης έρευνας της παραβίασης.

2.1.2 Τρόπος γνωστοποίησης στην Εποπτική Αρχή

Σε περίπτωση που αποφασιστεί η γνωστοποίηση στην εποπτική αρχή, ο GDPR απαιτεί να γίνει αυτό *"χωρίς αδικαιολόγητη καθυστέρηση και, αν είναι δυνατό, εντός 72 ωρών από τη στιγμή επίγνωσης της παραβίασης" (GDPR άρθρο 33).* Εάν υπάρχουν βάσιμοι λόγοι για τους οποίους δεν έχει δοθεί η κοινοποίηση εντός του απαιτούμενου χρονικού πλαισίου, οι λόγοι αυτοί πρέπει να περιλαμβάνονται στο πλαίσιο της κοινοποίησης.

Η γνωστοποίηση πρέπει να παρέχεται μέσω κατάλληλων ασφαλών μέσων στον φορέα που αναφέρεται στον Πίνακα 1, χρησιμοποιώντας ως πρότυπο τη *Φόρμα GDPR-FORM-5 Γνωστοποίησης της Παραβίασης Προσωπικών Δεδομένων*.

Στο πλαίσιο της γνωστοποίησης πρέπει να παρέχονται οι ακόλουθες πληροφορίες:

1 Η φύση της παραβίασης των προσωπικών δεδομένων, συμπεριλαμβανομένων, όπου είναι δυνατόν:

   i. των κατηγοριών και του κατά προσέγγιση αριθμού των επηρεαζόμενων υποκειμένων των δεδομένων

   ii. των κατηγοριών και του κατά προσέγγιση αριθμού των επηρεαζόμενων αρχείων δεδομένων προσωπικού χαρακτήρα,

2 Το όνομα και τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων ή άλλου σημείου επικοινωνίας από το οποίο μπορούν να ληφθούν περισσότερες πληροφορίες

3 Μια περιγραφή των ενδεχόμενων συνεπειών της παραβίασης των δεδομένων προσωπικού χαρακτήρα

4 Τα ληφθέντα ή τα προτεινόμενα προς λήψη μέτρα από τον υπεύθυνο επεξεργασίας για την αντιμετώπιση της παραβίασης των δεδομένων προσωπικού χαρακτήρα, καθώς και, όπου ενδείκνυται, μέτρα για την άμβλυνση ενδεχόμενων δυσμενών συνεπειών της

5 Εάν η γνωστοποίηση δεν γίνει εντός των 72 ωρών, οι λόγοι για τους οποίους δεν υποβλήθηκε νωρίτερα

Απαιτείται γραπτή επιβεβαίωση από την εποπτική αρχή ότι έχει παραληφθεί η γνωστοποίηση παραβίασης προσωπικών δεδομένων, συμπεριλαμβανομένων της ημερομηνίας και της ώρας κατά την οποία ελήφθη η γνωστοποίηση. Όπου είναι απαραίτητο, το GDPR επιτρέπει την παροχή των πληροφοριών σταδιακά (σε φάσεις) χωρίς περαιτέρω αδικαιολόγητη καθυστέρηση.

Η τεκμηρίωση της παραβίασης των προσωπικών δεδομένων, συμπεριλαμβανομένων των επιπτώσεών της και των διορθωτικών ενεργειών που θα αναληφθούν, θα παραχθεί ως μέρος της ***GDPR-DOC-15 Διαδικασίας Αντιμετώπισης Περιστατικών της Ασφάλειας Πληροφοριών*** .

2.2 Υποκείμενα των Δεδομένων

2.2.1 Αποφασίζοντας εάν θα ειδοποιηθούν τα υποκείμενα των δεδομένων

Ο Κανονισμός προβλέπει ότι η παραβίαση προσωπικών δεδομένων πρέπει να γνωστοποιηθεί στο υποκείμενο των δεδομένων *"όταν η παραβίαση των προσωπικών δεδομένων είναι πιθανό να οδηγήσει σε υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων" (άρθρο 34 του GDPR).*

Η εκτίμηση κινδύνου που αναφέρθηκε προηγουμένως σε αυτή τη διαδικασία (τμήμα 2.1.1) θα έχει καθορίσει κατά πόσον ο κίνδυνος για τα δικαιώματα και τις ελευθερίες των προσώπων στα οποία αναφέρονται τα δεδομένα κρίνεται επαρκώς υψηλός ώστε να δικαιολογείται η γνωστοποίηση.

Ωστόσο, αν έχουν ληφθεί μεταγενέστερα μέτρα για τον μετριασμό του υψηλού κινδύνου για τα υποκείμενα των δεδομένων, έτσι ώστε να μην είναι πλέον πιθανό να συμβεί, τότε η ενημέρωση των υποκειμένων των δεδομένων δεν απαιτείται από το GDPR.

Η γνωστοποίηση στα επηρεαζόμενα υποκείμενα των δεδομένων δεν είναι επίσης υποχρεωτική από το GDPR εάν *«προϋποθέτει δυσανάλογες προσπάθειες» (άρθρο 34 του GDPR).* Ωστόσο, σε αυτή την περίπτωση θα πρέπει να γίνει αντ' αυτής μια μορφή δημόσιας ενημέρωσης εφόσον αιτιολογημένα κριθεί ότι απαιτείται.

Τα ανωτέρω μπορεί να διαφοροποιηθούν ανάλογα με την ανατροφοδότηση από την εποπτική αρχή και άλλες πληροφορίες που θα συλλεχθούν κατά την έρευνα της παραβίασης.

2.2.2 Τρόπος ειδοποίησης των υποκειμένων των δεδομένων

Μόλις αποφασιστεί ότι η παραβίαση δικαιολογεί την ανακοίνωση στα επηρεαζόμενα υποκείμενα των δεδομένων, το GDPR απαιτεί αυτό να γίνει χωρίς αδικαιολόγητη καθυστέρηση.

Η ανακοίνωση στα επηρεαζόμενα υποκείμενα των δεδομένων θα πρέπει να *«περιγράφει με σαφήνεια τη φύση της παραβίασης των προσωπικών δεδομένων» (άρθρο 34 του GDPR)* και πρέπει επίσης να καλύπτει:

1 Το όνομα και τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων ή άλλου σημείου επικοινωνίας από το οποίο μπορούν να ληφθούν περισσότερες πληροφορίες

2 Μια περιγραφή των ενδεχόμενων συνεπειών της παραβίασης των δεδομένων προσωπικού χαρακτήρα

3 Τα ληφθέντα ή τα προτεινόμενα προς λήψη μέτρα από τον υπεύθυνο επεξεργασίας για την αντιμετώπιση της παραβίασης των δεδομένων προσωπικού χαρακτήρα, καθώς και, όπου ενδείκνυται, μέτρα για την άμβλυνση ενδεχόμενων δυσμενών συνεπειών της

Πέραν των σημείων που απαιτούνται από το GDPR, μπορεί να είναι σκόπιμο να παρέχονται συμβουλές στα υποκείμενα των δεδομένων σχετικά με τις ενέργειες που ενδέχεται να λάβουν για να μειώσουν τους κινδύνους που συνδέονται με την παραβίαση των προσωπικών δεδομένων.

Στις περισσότερες περιπτώσεις, θα ήταν σκόπιμο να ειδοποιηθούν τα επηρεαζόμενα υποκείμενα των δεδομένων μέσω επιστολής ή ηλεκτρονικού ταχυδρομείου ή και των δύο, προκειμένου να εξασφαλιστεί ότι το μήνυμα έχει ληφθεί και ότι έχουν την ευκαιρία να λάβουν τα απαιτούμενα μέτρα.