Διαχείριση Παραβίασης Προσωπικών Δεδομένων

Εισηγήτρια: Νόπη Τιντζογλίδου, Δικηγόρος με ειδίκευση σε θέματα προσωπικών δεδομένων

● Δικηγορικό Γραφείο Νόπη Τιντζογλίδου και Συνεργάτες ● Ακαδημίας 25, Αθήνα ● nopi@nopilaw.gr ● 2100080600

ΤΙΝΤΖΟΓΛΙΔΟΥ & ΣΥΝΕΡΓΑΤΕΣ
ΔΙΚΗΓΟΡΙΚΟ ΓΡΑΦΕΙΟ

Ορισμός παραβίασης δεδομένων προσωπικού χαρακτήρα (άρθρο 4 παρ. 12 ΓΚΠΔ):

Παραβίαση προσωπικών δεδομένων είναι η παραβίαση της ασφάλειας που οδηγεί σε τυχαία και παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία.

! ***Η παραβίαση είναι ένα είδος περιστατικού ασφάλειας. Δεν είναι όλα τα περιστατικά ασφάλειας παραβιάσεις προσωπικών δεδομένων.***

! ***Συνέπεια μιας παραβίασης είναι ότι ο Υπεύθυνος Επεξεργασίας δεν είναι σε θέση να διασφαλίσει τη συμμόρφωση με τις αρχές που αφορούν την επεξεργασία δεδομένων προσωπικού χαρακτήρα, οι οποίες περιγράφονται συνοπτικά στο άρθρο 5 του GDPR, ιδίως της ακεραιότητας και της εμπιστευτικότητας.***

Είδη παραβίασης

Η Ομάδα Εργασίας του άρθρου 29 στις Κατευθυντήριες Γραμμές της για την Γνωστοποίηση παραβίασης προσωπικών δεδομένων υπό τον Κανονισμό 679/2016/ΕΕ κατηγοριοποίησε παραβιάσεις λαμβάνοντας υπόψη της τις αρχές ασφάλειας των πληροφοριακών συστημάτων σε:

- "**Παραβίαση εμπιστευτικότητας**" - μη εξουσιοδοτημένη ή τυχαία κοινολόγηση ή πρόσβαση σε προσωπικά δεδομένα.
- "**Παραβίαση ακεραιότητας**" - μη εξουσιοδοτημένη ή τυχαία αλλοίωση των προσωπικών δεδομένων.
- "**Παραβίαση διαθεσιμότητας**" - μη εξουσιοδοτημένη ή τυχαία απώλεια πρόσβασης ή καταστροφή προσωπικών δεδομένων.

Μια παραβίαση θα πρέπει πάντα να θεωρείται ως παραβίαση διαθεσιμότητας σε περίπτωση μόνιμης απώλειας ή καταστροφής προσωπικών δεδομένων.

Παραδείγματα απώλειας διαθεσιμότητας:

- Τα δεδομένα έχουν διαγραφεί είτε κατά λάθος είτε από ένα μη εξουσιοδοτημένο άτομο.
- Το κλειδί αποκρυπτογράφησης κρυπτογραφημένων δεδομένων έχει χαθεί.

Σε περίπτωση που ο Υπεύθυνος Επεξεργασίας δεν μπορεί να επαναφέρει την πρόσβαση στα δεδομένα, για παράδειγμα, από ένα αντίγραφο ασφάλειας, τότε αυτό θεωρείται ως μόνιμη απώλεια διαθεσιμότητας.

Η απώλεια της διαθεσιμότητας μπορεί επίσης να προκύψει όταν έχει επέλθει σημαντική αναστάτωση στην κανονική λειτουργία μιας επιχείρησης, για παράδειγμα, όταν γίνεται μια διακοπή ρεύματος ή μια επίθεση που διακόπτει αναγκαστικά την παροχή υπηρεσιών, καθιστώντας τα προσωπικά δεδομένα μη διαθέσιμα.

Είναι παραβίαση η μη διαθεσιμότητα δεδομένων προσωπικού χαρακτήρα για ένα περιορισμένο χρονικό διάστημα;

- Ένα περιστατικό ασφάλειας που έχει ως αποτέλεσμα τη μη διαθεσιμότητα δεδομένων προσωπικού χαρακτήρα για ένα χρονικό διάστημα είναι ένα είδος παραβίασης, καθώς η έλλειψη πρόσβασης στα δεδομένα μπορεί να έχει σημαντικό αντίκτυπο στα δικαιώματα και τις ελευθερίες των φυσικών προσώπων.

- Όταν, όμως, για παράδειγμα τα προσωπικά δεδομένα δεν είναι διαθέσιμα λόγω της προγραμματισμένης συντήρησης του συστήματος, δεν πρόκειται για «παραβίαση της ασφάλειας» όπως ορίζεται στο άρθρο 4 παράγραφος 12.

- **Παράδειγμα:** Εάν κρίσιμα ιατρικά δεδομένα των ασθενών σε ένα νοσοκομείο δεν είναι διαθέσιμα, ακόμη και προσωρινά, αυτό θα μπορούσε να αποτελέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των ατόμων. Για παράδειγμα, οι εγχειρίσεις μπορεί να ακυρωθούν και οι ζωές να τεθούν σε κίνδυνο.

Αποφάσεις της ΑΠΔΠΧ για παραβιάσεις προσωπικών δεδομένων

- **Αποφ. 87/2011**: περιστατικό παραβίασης προσωπικών δεδομένων από το **ΕΤΑΑ – Τομέας Υγειονομικών**.
- **Αποφ. 85/ 2015:** περιστατικό διαρροής δεδομένων πιστωτικών καρτών τριών ατόμων τα οποία πραγματοποίησαν, από ξεχωριστές τοποθεσίες (διαφορετικά κράτη) ηλεκτρονική κράτηση στο ξενοδοχείο **Royal Olympic**.
- **Αποφ. 98/ 2013:** Το μεγαλύτερο πρόστιμο που έχει επιβληθεί από την ΑΠΔΠΧ προ GDPR αφορά περιστατικό παραβίασης προσωπικών δεδομένων στη **Γενική Γραμματεία Πληροφοριακών Συστημάτων**. Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα επέβαλε πρόστιμο ύψους 150.000 Ευρώ κρίνοντας ότι η Γενική Γραμματεία Πληροφοριακών Συστημάτων παραβίασε την υποχρέωσή της για λήψη κατάλληλων μέτρων ασφάλειας, γεγονός που οδήγησε σε ιδιαίτερα σοβαρό περιστατικό παραβίασης προσωπικών δεδομένων, δηλαδή σε διαρροή δεδομένων που αφορούν το σύνολο σχεδόν των φορολογουμένων στην Ελλάδα.

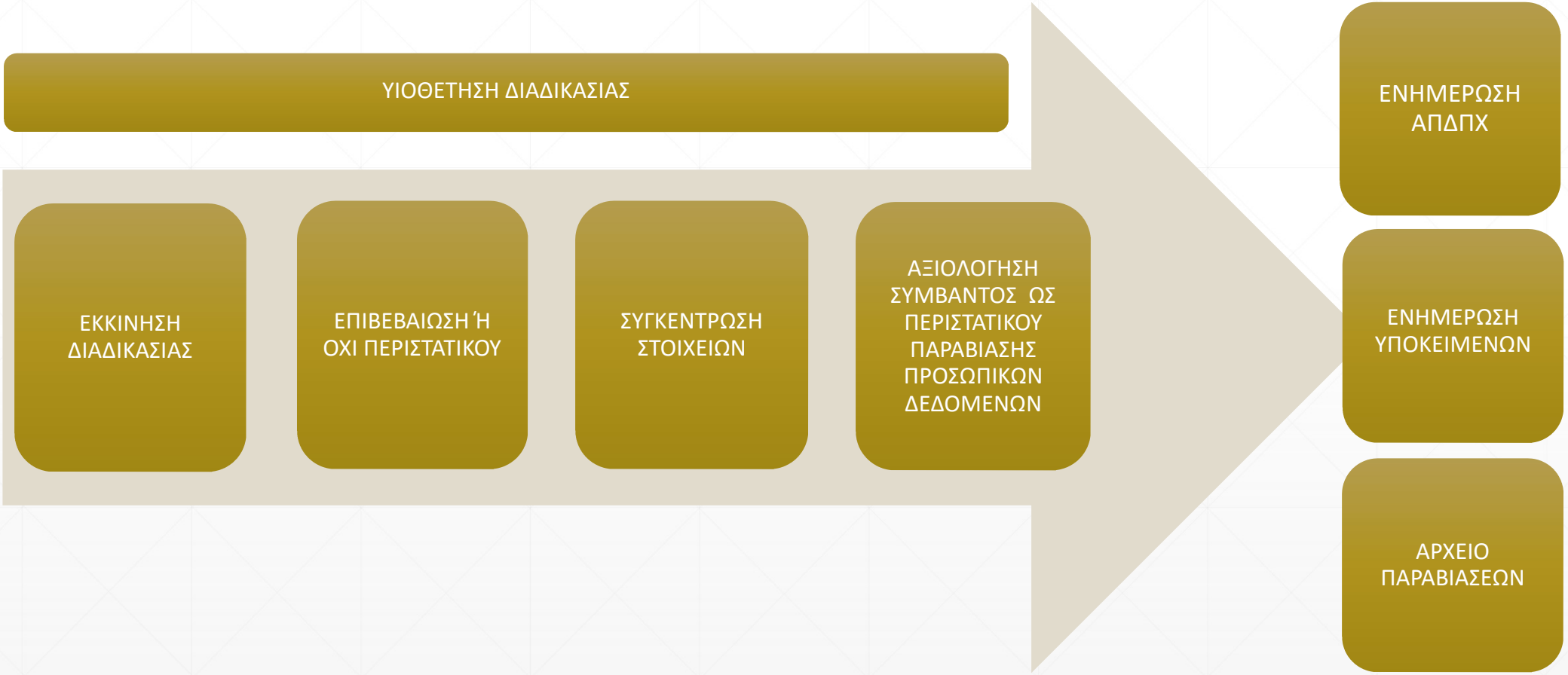
Άρθρο 33- Γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα στην ΑΠΔΠΧ

Άρθρο 34- Ανακοίνωση παραβίασης δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων

Για την υλοποίηση των ανωτέρω υποχρεώσεων είναι χρήσιμο να υπάρχει διαδικασία αντιμετώπισης περιστατικών ασφάλειας και γνωστοποίησης παραβιάσεων, δηλ. διαδικασία που θα ακολουθείται σε περίπτωση περιστατικού ασφάλειας που επηρεάζει προσωπικά δεδομένα, συμπεριλαμβανομένου του τρόπου περιορισμού, διαχείρισης και ανάκτησης του περιστατικού, καθώς και την αξιολόγηση του κινδύνου και τη γνωστοποίηση της παραβίασης.

Η διαδικασία αυτή βοηθά τον Υπεύθυνο Επεξεργασίας (αλλά και τον Εκτελούντα την Επεξεργασία) να ανταποκριθεί στο σύντομο χρονικό περιθώριο γνωστοποίησης των παραβιάσεων προσωπικών δεδομένων, αλλά και να αποφύγει αναίτια γνωστοποίηση συμβάντων ασφαλείας που δεν συνιστούν παραβιάσεις ή συνιστούν αλλά δεν προκαλούν κίνδυνο για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων.

ΕΝΔΕΙΚΤΙΚΗ ΔΙΑΔΙΚΑΣΙΑ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΠΕΡΙΣΤΑΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ



ΕΚΚΙΝΗΣΗ ΔΙΑΔΙΚΑΣΙΑΣ:

Η Διαδικασία Αντιμετώπισης Περιστατικών Ασφάλειας ενδέχεται να εκκινηθεί:

- από τις διαδικασίες της εταιρίας:
    i. Ελέγχου Εφαρμογής της Πολιτικής Ασφάλειας
    ii. Καταγραφής και Τεκμηρίωσης των Αδυναμιών Συμμόρφωσης
- από Πελάτες - Υποκείμενα των Δεδομένων, οι οποίοι αντιλαμβάνονται πιθανά συμβάντα/περιστατικά ασφάλειας,
- από εργαζομένους της Εταιρείας (π.χ. τον Τεχνικό),
- από Εκτελούντες την Επεξεργασία,
- από την ΑΠΔΠΧ ή άλλες Δημόσιες Αρχές,
- από τον Τύπο.

ΕΠΙΒΕΒΑΙΩΣΗ ή ΟΧΙ ΠΕΡΙΣΤΑΤΙΚΟΥ:

Τα αρμόδια όργανα λαμβάνουν γνώση του συμβάντος → το αξιολογούν προκειμένου να το χαρακτηρίσουν ή όχι ως περιστατικό ασφάλειας.
Με βάση τα αποτελέσματα της αξιολόγησης, αποφασίζουν: α) εάν το συμβάν δύναται να αποτελεί περιστατικό ασφάλειας και β) εάν το συμβάν δεν είναι περιστατικό ασφάλειας.

ΣΥΓΚΕΝΤΡΩΣΗ ΣΤΟΙΧΕΙΩΝ:

Συλλογή:
α) στοιχείων που μπορούν να χρησιμοποιηθούν για την αντιμετώπιση και την αξιολόγηση των επιπτώσεων του περιστατικού,
β) κάθε πληροφορίας που αφορά το συμβάν (ένδειξη, απόδειξη ή στοιχείο), απαραίτητη σε περίπτωση ελέγχου από την Εποπτική Αρχή.

ΑΞΙΟΛΟΓΗΣΗ ΠΕΡΙΣΤΑΤΙΚΟΥ:

Σύμφωνα με τα ευρήματα της συλλογής στοιχείων, ο DPO/ αρμόδια στελέχη της εταιρίας αξιολογούν αν από το περιστατικό προκύπτουν κίνδυνοι για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων και αν απαιτείται να ενημερωθεί η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ).

Σύμφωνα με το άρθρο 33, ο Υπεύθυνος Επεξεργασίας θα πρέπει να γνωστοποιήσει την παραβίαση, εκτός αν η παράβαση είναι απίθανο να οδηγήσει σε κίνδυνο για τα δικαιώματα και τις ελευθερίες των ατόμων.

ΕΝΗΜΕΡΩΣΗ ΑΠΔΠΧ:

Ο Υπεύθυνος Επεξεργασίας ενημερώνει την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) **αμελλητί** μέσα σε χρονικό διάστημα **72 ωρών** από τη στιγμή που αποκτά γνώση του γεγονότος της παραβίασης των προσωπικών δεδομένων, **εκτός αν έχει αξιολογηθεί ότι το περιστατικό δεν αποτελεί κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων**.

Ο Υπεύθυνος Επεξεργασίας είναι υπεύθυνος για την παροχή κατ' ελάχιστο των ακόλουθων πληροφοριών στην ΑΠΔΠΧ:

- Περιγραφή της **φύσης της παραβίασης** και πιθανές επιπτώσεις του περιστατικού
- Κατηγορίες και κατά προσέγγιση αριθμό των **υποκειμένων των δεδομένων** που επηρεάζονται από το περιστατικό
- **Κατηγορίες προσωπικών δεδομένων** και αριθμός επηρεαζόμενων αρχείων που περιέχουν προσωπικά δεδομένα
- Ενδεχόμενες **συνέπειες της παραβίασης**
- **Μέτρα** που έχουν ληφθεί ή που έχουν προταθεί άμεσα να υλοποιηθούν με σκοπό την αντιμετώπιση του περιστατικού παραβίασης ή/ και τον περιορισμό των επιπτώσεών του
- Όνομα και **στοιχεία επικοινωνίας του DPO** ή/ και άλλου προσώπου που μπορεί να παρέχει πληροφορίες.

Αν η γνωστοποίηση στην εποπτική αρχή δεν πραγματοποιηθεί εντός 72 ωρών, πρέπει να συνοδεύεται από αιτιολόγηση για την καθυστέρηση σύμφωνα με το άρθρο 33 παράγραφος 1.

Για την ενημέρωση της ΑΠΔΠΧ χρησιμοποιείται η **τυποποιημένη φόρμα γνωστοποίησης** περιστατικού παραβίασης προσωπικών δεδομένων, διαθέσιμη στον ιστότοπο της ΑΠΔΠΧ (www.dpa.gr), η οποία δύναται να αφορά:

α) **Αρχική γνωστοποίηση** (αν πρόκειται για υποβολή κάποιων πρώτων διαθέσιμων στοιχείων, ενώ εκκρεμούν κάποια γιατί ακόμα δεν είναι διαθέσιμα),

β) **Συμπληρωματική γνωστοποίηση** (αν παρέχονται συμπληρωματικά στοιχεία επί προηγούμενης υποβληθείσας ως αρχική),

γ) **Πλήρης γνωστοποίηση** (αν παρέχονται όλες οι πληροφορίες επί του περιστατικού).

Προτείνεται, **για την ασφάλεια της ηλεκτρονικής αποστολής να αποστέλλεται η εν λόγω φόρμα κρυπτογραφημένη**, με τρόπο τέτοιο ώστε να μπορεί να αναγνωσθεί (αποκρυπτογραφηθεί) μόνο από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

Για να διασφαλιστεί αυτό, θα πρέπει να χρησιμοποιηθεί το λογισμικό GnuPG (GPG), το οποίο αποτελεί ελεύθερη διανομή του προτύπου OpenPGP. Θα πρέπει πρώτα να κρυπτογραφήσετε το αρχείο (συμπληρωμένη φόρμα γνωστοποίησης) τοπικά στο υπολογιστικό σας σύστημα, ανεξάρτητα από το πρόγραμμα/υπηρεσία ηλεκτρονικού ταχυδρομείου που χρησιμοποιείτε, και ακολούθως να το επισυνάψετε, ως κρυπτογραφημένο πλέον αρχείο, σε μήνυμα ηλεκτρονικού ταχυδρομείου.

Το δημόσιο GPG κλειδί της Αρχής, με το οποίο θα πρέπει να κρυπτογραφηθεί η συμπληρωθείσα φόρμα γνωστοποίησης πριν επισυναφθεί στο μήνυμα ηλεκτρονικού ταχυδρομείου* που θα αποσταλεί στην Αρχή, είναι διαθέσιμο εδώ (Key ID:445EA68B, Key Fingerprint: AD28 60E4 2CBA CA97 A2AD A5F1 75BD F233 445E A68B). Με τον ίδιο τρόπο μπορεί να κρυπτογραφηθεί και όποιο άλλο τυχόν συνοδευτικό αρχείο της φόρμας.

Η συμπληρωμένη φόρμα αποστέλλεται στην ηλεκτρονική διεύθυνση databreach@dpa.gr

Αποφάσεις

Συχνές ερωτήσεις

Θεματικές ενότητες
Επιλογή Ενότητας

Σημαντικά αρχεία
Επιλογή Ενότητας

ΜΙΚΡΟΙ ΠΟΛΙΤΕΣ

ΑΣΦΑΛΕΙΑ

Γνωστοποίηση περιστατικών παραβίασης στην Αρχή

Για τη γνωστοποίηση περιστατικού παραβίασης στην Αρχή, σε συμμόρφωση με τη σχετική υποχρέωση του **άρ. 33 του Κανονισμού (ΕΕ) 2016/679**, ο υπεύθυνος επεξεργασίας πρέπει να συμπληρώσει ειδική φόρμα και να την υποβάλει στην Αρχή **ηλεκτρονικά***, με αποστολή στην ηλεκτρονική διεύθυνση:

databreach@dpa.gr

**Μόνο σε εξαιρετική περίπτωση μπορεί η φόρμα να υποβληθεί με άλλο τρόπο (π.χ. με φυσική υποβολή) και σε αυτήν την περίπτωση θα πρέπει να τεκμηριώνεται επαρκώς ο λόγος που δεν προτιμήθηκε η ηλεκτρονική υποβολή.*

Προσοχή, αφορά μόνο υποβολή περιστατικών παραβίασης Δ.Π.Χ. από υπευθύνους επεξεργασίας. Για υποβολή καταγγελίας παρακαλούμε δείτε εδώ.
Μηνύματα που λαμβάνονται στην εν λόγω διεύθυνση και δεν αφορούν περιστατικά παραβίασης αγνοούνται.

Διατίθενται **δύο μορφές της φόρμας**: η πρώτη (Φορμα_interactive_v3.xlsm) διαθέτει αυτοματισμούς με σκοπό τη διευκόλυνση της συμπλήρωσής της, και κατά το «άνοιγμά» της, θα πρέπει να ενεργοποιούνται οι μακροεντολές. Η δεύτερη (Φορμα_simple_v2.xls) είναι η απλή μορφή, χωρίς μακροεντολές.

Η φόρμα υποβάλλεται στην **ελληνική**, ενώ είναι διαθέσιμη και αγγλική έκδοση, η οποία πρέπει να χρησιμοποιείται **όταν το περιστατικό αφορά διασυνοριακή επεξεργασία**.

	Ελληνικά	Αγγλικά
Μορφή με αυτοματισμούς	Φορμα_interactive.xlsm	Φορμα_interactive - english.xlsm
Απλή μορφή	Φορμα_simple.xls	Φορμα_simple – english.xls

Προσοχή: Επιλέξτε μόνο μία από τις δύο μορφές της φόρμας.

Για τη συμπλήρωση κάθε γραμμής της φόρμας υπάρχουν **αναλυτικές οδηγίες** στο τέλος της εκάστοτε γραμμής.

Προτείνεται, για την ασφάλεια της ηλεκτρονικής αποστολής να αποστέλλεται η εν λόγω φόρμα **κρυπτογραφημένη**, με τρόπο τέτοιο ώστε να μπορεί να αναγνωσθεί (αποκρυπτογραφηθεί) μόνο από την Αρχή.

Για να διασφαλιστεί αυτό, θα πρέπει να χρησιμοποιηθεί το λογισμικό GnuPG (GPG), το οποίο αποτελεί ελεύθερη διανομή του προτύπου OpenPGP.

Θα πρέπει πρώτα να κρυπτογραφήσετε το αρχείο (συμπληρωμένη φόρμα γνωστοποίησης) τοπικά στο υπολογιστικό σας σύστημα, ανεξάρτητα από το πρόγραμμα/υπηρεσία ηλεκτρονικού ταχυδρομείου που χρησιμοποιείτε, και ακολούθως να το επισυνάψετε, ως κρυπτογραφημένο πλέον αρχείο, σε μήνυμα ηλεκτρονικού ταχυδρομείου.

Το δημόσιο GPG κλειδί της Αρχής, με το οποίο θα πρέπει να κρυπτογραφηθεί η συμπληρωθείσα φόρμα γνωστοποίησης πριν επισυναφθεί στο μήνυμα ηλεκτρονικού ταχυδρομείου* που θα αποσταλεί στην Αρχή, είναι διαθέσιμο εδώ (Key ID:445EA68B, Key Fingerprint: AD28 60E4 2CBA CA97 A2AD A5F1 75BD F233 445E A68B). Με τον ίδιο τρόπο μπορεί να κρυπτογραφηθεί και όποιο άλλο τυχόν συνοδευτικό αρχείο της φόρμας.

**Προσοχή: Μην κρυπτογραφήσετε συνολικά όλο το μήνυμα ηλεκτρονικού ταχυδρομείου (π.χ. με χρήση κατάλληλου plugin), διότι υπάρχουν διαπιστωμένα ζητήματα ασφάλειας σε αυτήν την προσέγγιση (βλέπε εδώ).*

Για τη γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα, από φορέα παροχής διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, με βάση το άρθρο 12 παρ. 5 του ν. 3471/2006 (οδηγία 2002/58/ΕΚ όπως έχει τροποποιηθεί) και τον Κανονισμό (ΕΕ) 611/2013 παρακαλούμε όπως χρησιμοποιήσετε την ειδική φόρμα που βρίσκεται διαθέσιμη στην ιστοσελίδα της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών. Η φόρμα αυτή συνυποβάλλεται αυτόματα και στην ΑΠΔΠΧ.

Αναζήτηση
Επιλογή κειμένου αναζήτησης
Επιλέξτε ενότητα
Αναζήτηση

ΥΠΗΡΕΣΙΕΣ ΠΡΟΣ ΠΟΛΙΤΕΣ

ΥΠΗΡΕΣΙΕΣ ΠΡΟΣ ΦΟΡΕΙΣ

DPO CORNER

Παράδειγμα, όπου δικαιολογείται καθυστέρηση στην γνωστοποίηση της παραβίασης:

Δικαιολογείται η καθυστέρηση στην γνωστοποίηση της παραβίασης όταν:

- Ο Υπεύθυνος Επεξεργασίας αντιμετωπίζει πολλαπλές, παρόμοιες παραβιάσεις εμπιστευτικότητας σε σύντομο χρονικό διάστημα που επηρεάζουν τον ίδιο μεγάλο αριθμό υποκειμένων των δεδομένων.

- Ο Υπεύθυνος Επεξεργασίας αντιλήφθηκε μια παραβίαση και, ενώ ξεκίνησε την έρευνά του και πριν από την κοινοποίηση, εντόπισε και άλλες παρόμοιες παραβιάσεις, οι οποίες έχουν διαφορετικές αιτίες.

Ανάλογα με τις περιστάσεις, μπορεί να χρειαστεί αρκετός χρόνος για τον Υπεύθυνο Επεξεργασίας ούτως ώστε να προσδιορίσει την έκταση των παραβιάσεων και, αντί να γνωστοποιήσει κάθε παραβίαση ξεχωριστά, ο Υπεύθυνος Επεξεργασίας σχεδιάζει μια σημαντική γνωστοποίηση που αντιπροσωπεύει αρκετές παρόμοιες παραβιάσεις, με πιθανές διαφορετικές αιτίες. Αυτό θα μπορούσε να οδηγήσει σε καθυστέρηση της γνωστοποίησης στην εποπτική αρχή περισσότερο από 72 ώρες από τη στιγμή που ο Υπεύθυνος Επεξεργασίας θα λάβει γνώση αυτών των παραβιάσεων.

Ειδική διαδικασία Γνωστοποίησης παραβίασης δεδομένων προσωπικού χαρακτήρα για τους φορείς παροχής διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών

Στην περίπτωση αυτή θα πρέπει να **χρησιμοποιείται ειδική φόρμα που βρίσκεται διαθέσιμη στην ιστοσελίδα της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών**.

Σύμφωνα με το ειδικό καθεστώς που ορίζεται στο άρθρο **12 παρ. 5 του ν. 3471/2006** και τον **Κανονισμό (ΕΕ) 611/2013** σχετικά με τα εφαρμοστέα μέτρα για την κοινοποίηση παραβιάσεων προσωπικών δεδομένων βάσει της οδηγίας 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες

Η φόρμα αυτή συνυποβάλλεται αυτόματα και στην ΑΠΔΠΧ.

www.adae.gr/online-ypiresies/koinopoiisi-parabiasis-prosopikon-dedomenon/

90%

Run Adobe Flash

| Σύνδεσμοι | Επικοινωνία

Αναζήτηση: Αναζήτηση

Η ΑΔΑΕ | ΝΟΜΟΘΕΤΙΚΟ ΠΛΑΙΣΙΟ | ΕΚΘΕΣΕΙΣ ΠΕΠΡΑΓΜΕΝΩΝ | ONLINE ΥΠΗΡΕΣΙΕΣ | ΕΝΗΜΕΡΩΣΗ

Βρίσκεστε εδώ: Αρχική σελίδα / ONLINE ΥΠΗΡΕΣΙΕΣ / Κοινοποίηση παραβίασης προσωπικών δεδομένων>

Δείτε στην κατηγορία:

- Κοινοποίηση παραβίασης προσωπικών δεδομένων
- Καταγγελία
- Ερώτημα
- Ερωτήσεις για Πολίτες
- Ερωτήσεις για Παρόχους

Φόρμα κοινοποίησης περιστατικού παραβίασης προσωπικών δεδομένων από παρόχους ηλεκτρονικών επικοινωνιών

Συμπληρώνοντας αυτή τη φόρμα μας ενημερώνετε για ένα περιστατικό παραβίασης προσωπικών δεδομένων.

Συμπληρώστε τη φόρμα...

Τα πεδία με * είναι υποχρεωτικά.

Γενικά στοιχεία περιστατικού παραβίασης προσωπικών δεδομένων- Τμήμα Ι

1. Ονομασία του παρόχου *

2. Ταυτότητα και στοιχεία επικοινωνίας του υπεύθυνου προστασίας δεδομένων ή άλλου αρμόδιου επικοινωνίας από τον οποίο μπορούν να ληφθούν περισσότερες πληροφορίες.

Όνομα: *

ΤΣΙΝΤΖΟΓΛΙΔΟΥ & ΣΥΝΕΡΓΑΤΕΣ
ΔΙΚΗΓΟΡΙΚΟ ΓΡΑΦΕΙΟ

ΕΝΗΜΕΡΩΣΗ ΥΠΟΚΕΙΜΕΝΩΝ ΤΩΝ ΔΕΔΟΜΕΝΩΝ:

Ο υπεύθυνος επεξεργασίας ανακοινώνει αμελλητί την παραβίαση των δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων, όταν η παραβίαση δεδομένων προσωπικού χαρακτήρα ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων.

Η ανακοίνωση στο υποκείμενο των δεδομένων **δεν απαιτείται**, εάν πληρείται οποιαδήποτε από τις ακόλουθες προϋποθέσεις:

1) ο υπεύθυνος επεξεργασίας **εφάρμοσε κατάλληλα τεχνικά και οργανωτικά μέτρα προστασίας**, και τα μέτρα αυτά εφαρμόστηκαν στα επηρεαζόμενα από την παραβίαση δεδομένα προσωπικού χαρακτήρα, **κυρίως μέτρα που καθιστούν μη κατανοητά τα δεδομένα προσωπικού χαρακτήρα σε όσους δεν διαθέτουν άδεια πρόσβασης σε αυτά, όπως η κρυπτογράφηση**,

2) ο υπεύθυνος επεξεργασίας έλαβε στη συνέχεια **μέτρα που διασφαλίζουν ότι δεν είναι πλέον πιθανό να προκύψει υψηλός κίνδυνος για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων**,

3) **η ανακοίνωση προϋποθέτει δυσανάλογες προσπάθειες**. Στην περίπτωση αυτή, γίνεται αντ' αυτής δημόσια ανακοίνωση ή υπάρχει παρόμοιο μέτρο με το οποίο τα υποκείμενα των δεδομένων ενημερώνονται με εξίσου αποτελεσματικό τρόπο.

Οι ανακοινώσεις αυτές θα πρέπει να πραγματοποιούνται το συντομότερο δυνατό, σε στενή συνεργασία με την εποπτική αρχή, τηρώντας την καθοδήγηση που παρέχεται από αυτήν ή άλλες σχετικές αρχές επιβολής του νόμου.

Η ανάγκη να μετριαστεί άμεσος κίνδυνος ζημίας θα απαιτούσε την άμεση ανακοίνωση στα υποκείμενα των δεδομένων, ενώ η αναγκαιότητα εφαρμογής κατάλληλων μέτρων κατά συνεχών ή παρόμοιων παραβιάσεων δεδομένων προσωπικού χαρακτήρα μπορεί να δικαιολογεί περισσότερο χρόνο για την ανακοίνωση (αιτιολογική σκέψη Κανονισμού 86).

ΑΡΧΕΙΟ ΚΑΤΑΓΡΑΦΗΣ ΠΕΡΙΣΤΑΤΙΚΩΝ ΠΑΡΑΒΙΑΣΗΣ:

Ανεξαρτήτως του αν η παραβίαση πρέπει να γνωστοποιηθεί στην εποπτική αρχή, ο Υπεύθυνος Επεξεργασίας πρέπει να τηρεί **αρχεία για όλες τις παραβιάσεις**, όπως επεξηγεί το άρθρο 33 παράγραφος 5:

"Ο υπεύθυνος επεξεργασίας τεκμηριώνει κάθε παραβίαση δεδομένων προσωπικού χαρακτήρα, που συνίσταται

- στα **πραγματικά περιστατικά** που αφορούν την παραβίαση δεδομένων προσωπικού χαρακτήρα,
- **τις συνέπειες** και
- τα **ληφθέντα διορθωτικά μέτρα**.

Η εν λόγω τεκμηρίωση επιτρέπει στην εποπτική αρχή να επαληθεύει τη συμμόρφωση προς το παρόν άρθρο. "

Η ΟΕ29 (πλέον Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων) συνιστά στον Υπεύθυνο Επεξεργασίας **να τεκμηριώνει τη συλλογιστική του για τις αποφάσεις που ελήφθησαν σχετικά με την παραβίαση**.

Ειδικότερα και σύμφωνα με την αρχή της λογοδοσίας:

α) Εάν δεν έχει γνωστοποιηθεί μια παραβίαση, πρέπει να τεκμηριώνεται η αιτιολόγηση της απόφασης αυτής. Αυτό πρέπει να περιλαμβάνει **τους λόγους για τους οποίους ο Υπεύθυνος Επεξεργασίας θεωρεί ότι η παραβίαση είναι απίθανο να οδηγήσει σε κίνδυνο για τα δικαιώματα και τις ελευθερίες των ατόμων**. Εναλλακτικά, εάν ο Υπεύθυνος της Επεξεργασίας θεωρήσει ότι πληρούται οιοσδήποτε από τους όρους του άρθρου 34 παράγραφος 3, τότε θα πρέπει να είναι σε θέση να παράσχει τα κατάλληλα αποδεικτικά στοιχεία ότι αυτό συμβαίνει.

β) **Όταν ο Υπεύθυνος Επεξεργασίας γνωστοποιεί μια παραβίαση στην εποπτική αρχή, αλλά η γνωστοποίηση γίνεται με καθυστέρηση, ο Υπεύθυνος Επεξεργασίας πρέπει να είναι σε θέση να αιτιολογήσει την καθυστέρηση αυτή**. Η σχετική τεκμηρίωση θα μπορούσε να βοηθήσει να αποδειχθεί ότι η καθυστέρηση στην υποβολή εκθέσεων είναι δικαιολογημένη και όχι υπέρμετρη.

Αυτό συνδέεται με την αρχή της λογοδοσίας του GDPR, που περιλαμβάνεται στο άρθρο 5 παράγραφος 2.

Ο GDPR δεν καθορίζει την περίοδο διατήρησης των αρχείων καταγραφής. Όταν τα αρχεία αυτά περιέχουν δεδομένα προσωπικού χαρακτήρα, ο Υπεύθυνος Επεξεργασίας πρέπει να καθορίσει την κατάλληλη περίοδο διατήρησης.

ΠΑΡΑΔΕΙΓΜΑΤΑ ΠΑΡΑΒΙΑΣΕΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΟΜΕΝΩΝ ΚΑΙ ΣΕ ΠΟΙΟΝ ΠΡΕΠΕΙ ΝΑ ΓΝΩΣΤΟΠΟΙΗΘΟΥΝ:

ΠΑΡΑΔΕΙΓΜΑ	ΠΡΕΠΕΙ ΝΑ ΓΝΩΣΤΟΠΟΙΗΣΩ ΣΤΗΝ ΕΠΟΠΤΙΚΗ ΑΡΧΗ;	ΠΡΕΠΕΙ ΝΑ ΠΡΟΒΩ ΣΕ ΑΝΑΚΟΙΝΩΣΗ ΣΤΟ ΥΠΟΚΕΙΜΕΝΟ ΤΩΝ ΔΕΔΟΜΕΝΩΝ;	ΣΗΜΕΙΩΣΕΙΣ/ΣΥΣΤΑΣΕΙΣ
I. Υπεύθυνος Επεξεργασίας αποθήκευσε ένα αντίγραφο ασφάλειας αρχείου που περιέχει προσωπικά δεδομένα σε κρυπτογραφημένο σε USB. Το USB κλάπηκε σε μια διάρρηξη.	Όχι.	Όχι.	Εφόσον τα δεδομένα είναι κρυπτογραφημένα, δηλαδή δεν είναι δυνατό να γίνουν προσβάσιμα σε τρίτους και συνάμα δεν επηρεάστηκε η διαθεσιμότητά τους, αφού επρόκειτο για αντίγραφο και υφίσταται η αρχική λίστα που τα περιέχει δεν συνιστά παραβίαση που πρέπει να γνωστοποιηθεί/ ανακοινωθεί, αλλά αρκεί η καταγραφή της στο αρχείο παραβιάσεων.
II. Συνέβη ολιγόλεπτη διακοπή ρεύματος σε τηλεφωνικό κέντρο Υπεύθυνου Επεξεργασίας με αποτέλεσμα οι πελάτες να μην μπορούν να τηλεφωνήσουν στον Υπεύθυνο Επεξεργασίας και να έχουν πρόσβαση στα αρχεία τους.	Όχι.	Όχι.	Δεν πρόκειται για παραβίαση που πρέπει να γνωστοποιηθεί/ ανακοινωθεί, αλλά αρκεί η καταγραφή της στο αρχείο παραβιάσεων. του άρθρου 33 (5).
III. Διεγράφη ένα αρχείο στοιχείων επικοινωνίας με τους αποφοίτους σε πανεπιστήμιο. Τα στοιχεία ανακτήθηκαν από ένα αντίγραφο ασφάλειας.	Όχι.	Όχι, καθώς είναι απίθανο να οδηγήσει σε υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των ατόμων αυτών.	

ΠΑΡΑΔΕΙΓΜΑ	ΠΡΕΠΕΙ ΝΑ ΓΝΩΣΤΟΠΟΙΗΣΩ ΣΤΗΝ ΕΠΟΠΤΙΚΗ ΑΡΧΗ;	ΠΡΕΠΕΙ ΝΑ ΠΡΟΒΩ ΣΕ ΑΝΑΚΟΙΝΩΣΗ ΣΤΟ ΥΠΟΚΕΙΜΕΝΟ ΤΩΝ ΔΕΔΟΜΕΝΩΝ;	ΣΗΜΕΙΩΣΕΙΣ/ΣΥΣΤΑΣΕΙΣ
IV. Κρυπτογραφήθηκαν όλα τα δεδομένα που διατηρούσε ένας Υπεύθυνος Επεξεργασίας λόγω επίθεσης ransomware. Δεν υπάρχουν διαθέσιμα αντίγραφα ασφάλειας και τα δεδομένα δεν μπορούν να αποκατασταθούν.	Ναι, θα πρέπει να γίνει γνωστοποίηση στην Εποπτική Αρχή, εφόσον υφίσταται απώλεια διαθεσιμότητας των δεδομένων.	Θα πρέπει να εξεταστεί η φύση των προσωπικών δεδομένων που επηρεάστηκαν και το πιθανό αποτέλεσμα της απώλεια διαθεσιμότητας των δεδομένων για να αποφασιστεί αν θα πρέπει να γίνει ανακοίνωση στα υποκείμενα των δεδομένων.	Εάν υπήρχε διαθέσιμο αντίγραφο ασφάλειας των δεδομένων και τα δεδομένα μπορούσαν να ανακτηθούν σε σύντομο χρόνο, δεν θα απαιτούνταν γνωστοποίηση στην Εποπτική Αρχή ούτε στα υποκείμενα των δεδομένων.
V. Μια εταιρεία φιλοξενίας ιστοσελίδων που λειτουργεί ως Εκτελών την Επεξεργασία διαπιστώνει συστημικό σφάλμα στη διαδικασία ταυτοποίησης του χρήστη κατά την είσοδο στο λογαριασμό χρήστη. Συνέπεια του σφάλματος είναι ότι κάθε χρήστης μπορεί να έχει πρόσβαση στα στοιχεία του λογαριασμού κάθε άλλου χρήστη.	Η εταιρεία φιλοξενίας ιστοσελίδων, ως Εκτελών την Επεξεργασία, πρέπει να το γνωστοποιήσει στους στους Υπεύθυνους Επεξεργασίας χωρίς αδικαιολόγητη καθυστέρηση. Ο Υπεύθυνος Επεξεργασίας τότε πρέπει να γνωστοποιήσει στην εποπτική αρχή.	Εάν δεν υπάρχει υψηλός κίνδυνος για τα άτομα δεν χρειάζεται να τους ανακοινωθεί.	Σε περιπτώσεις όπως λογαριασμού χρήστη e-banking ο κίνδυνος είναι υψηλός και θα πρέπει να ανακοινωθεί και στα υποκείμενα των δεδομένων.
VI. Εξαιτίας μιας κυβερνοεπίθεσης, δεν είναι διαθέσιμα τα ιατρικά αρχεία ενός νοσοκομείου για περίπου 30 ώρες.	Ναι, το νοσοκομείο έχει υποχρέωση να προβεί σε γνωστοποίηση, λόγω υψηλού κινδύνου για την υγεία των ασθενών και τη προστασία της ιδιωτικής ζωής.	Ναι, πρέπει να γίνει ανακοίνωση στα θιγόμενα άτομα.	

Ευχαριστώ για την προσοχή σας!

Νόπη Τιντζογλίδου

ΤΙΝΤΖΟΓΛΙΔΟΥ
& ΣΥΝΕΡΓΑΤΕΣ
ΔΙΚΗΓΟΡΙΚΟ ΓΡΑΦΕΙΟ