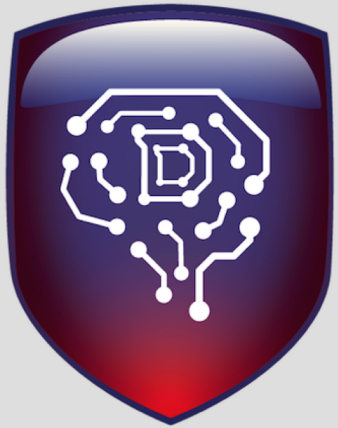
Ημερίδα Προστασίας Δεδομένων

«ΑΣΦΑΛΕΙΑ ΔΕΔΟΜΕΝΩΝ: Η ΕΦΑΡΜΟΓΗ ΤΟΥ ΓΕΝΙΚΟΥ ΚΑΝΟΝΙΣΜΟΥ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ»

"Η συμμόρφωση με τον Γενικό Κανονισμό ως στοιχείο κουλτούρας των Οργανισμών"

Ελπίδα Βαμβακά
Πρόεδρος *Homo Digitalis*
Νομικός Σύμβουλος ομίλου εταιρειών *Enartia*

Λευτέρης Σταυρακάκης
DPO ομίλου εταιρειών *Enartia*



Homo Digitalis

Protect your rights

*“Η **Homo Digitalis** είναι η πρώτη και μοναδική μέχρι στιγμής Μη Κυβερνητική Οργάνωση για την προστασία και προώθηση των ψηφιακών δικαιωμάτων στην Ελλάδα”*


enartia
GROUP OF BRANDS


papaki
HAPPY.PEOPLE.ONLINE


Top.Host
EXTREME SUPPORT


the core


magic press
by Enartia

Παρότι η «συμμόρφωση» φαίνεται να συνεπάγεται υψηλά κόστη και βαριές διαδικασίες,

εκείνος που θα μετατρέψει την κουλτούρα σεβασμού και προστασίας των προσωπικών δεδομένων σε πυρήνα της καθημερινής του λειτουργίας, θα αποκτήσει αυτόματα ένα «ανταγωνιστικό πλεονέκτημα».

Homo Digitalis
Protect your rights

enartia
GROUP OF BRANDS

Θα σταθώ σε 3 διαδικασίες που θεωρώ βοήθησαν τη δική μας εταιρεία να αποκτήσει την κουλτούρα αυτή:

1. Σωστή εκπαίδευση του προσωπικού σε θέματα προστασίας δεδομένων
2. Πλήρες αρχείο δραστηριοτήτων - επικαιροποίηση συμβάσεων/νομικών κειμένων.
3. Υιοθέτηση Διαδικασίας Αντιμετώπισης Περιστατικών Ασφάλειας και Γνωστοποίησης Παραβιάσεων

Homo Digitalis
Protect your rights

enartia
GROUP OF BRANDS

Σωστή εκπαίδευση του προσωπικού

Είναι σημαντικό να μιλάμε την ίδια γλώσσα

Homo Digitalis
Protect your rights

enartia
GROUP OF BRANDS

Πλήρες αρχείο δραστηριοτήτων

1. Σύσταση Ομάδας Εργασίας (privacy champions κάθε τμήματος)
2. Ενημερωτικό Υλικό και Επεξήγηση του τρόπου συμπλήρωσης
3. Οργάνωση Συναντήσεων ατομικές (15-30 λεπτών) κάθε εβδομάδα ή κάθε δύο εβδομάδες
   - ❑ Παρατηρήσεις
   - ❑ Απορίες
   - ❑ Πρόοδος
1. Συνολική συνάντηση όλων των ομάδων μετά από δύο μήνες.
2. Παράδοση για σχόλια στους Προϊσταμένους κάθε τμήματος.
3. Παράδοση στον DPO για τον οριστικό έλεγχο και ενοποίηση.
4. Καθορισμός ημερομηνιών για επικαιροποίηση και έλεγχο 2 φορές ανά έτος.

Μόνοι μπορούμε να κάνουμε τόσα λίγα-μαζί
μπορούμε να κάνουμε τόσα πολλά

Έλεν Κέλερ

Homo Digitalis
Protect your rights

enartia
GROUP OF BRANDS

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	**Αρχείο Δραστηριοτήτων**														
2	**Όνομα Οργανισμού:**														
3	(1) Δραστηριότητα Επεξεργασίας	(2) Κύρια ή Παρεπόμενη	(3) Νομική Βάση	(4) Υπεύθυνος ή Εκτελών την Επεξεργασία ή τυχόν εκπρόσωπός τους		(5) Σκοπός Επεξεργασίας	(6) Κατηγορίες Υποκειμένων Δεδομένων και Κατηγορίες Προσωπικών Δεδομένων		(7) Κατηγορίες Αποδεκτών	(8) Διαβίβαση Δεδομένων σε τρίτη χώρα διεθνή οργανισμό	(9) Προβλεπόμενη Περίοδος Διαγραφής	(10) Τεχνικά και Οργανωτικά Μέτρα Ασφάλειας	(11) Εκτίμηση αντίκτυπου / προηγούμενη διαβούλευση		(12) Ενημέρωση στα Υποκείμενα Δεδομένων
4				(α) Ιδιότητα	(β) Όνομα και Στοιχεία Επικονωνίας		(α) Υποκειμένων Δεδομένων	(β) Προσωπικών Δεδομένων					(α) Εκτίμηση αντίκτυπου	(β) Προηγούμενη διαβούλευση	
5															
6															
7															
8															
9															
10															
11															
12															

http://www.dataprotection.gov.cy/

Homo Digitalis
Protect your rights

enartia
GROUP OF BRANDS

Οδηγός Συμπλήρωσης Αρχείου Δραστηριοτήτων

καταγράφονται σε κάθε πεδίο του Πίνακα.

ΜΕΡΟΣ Β - Συμπλήρωση του Πίνακα

1. Δραστηριότητα Επεξεργασίας

Στη στήλη αυτή γίνεται μια σύντομη περιγραφή της κάθε δραστηριότητας του οργανισμού. Ως πρώτο βήμα, συστήνεται η επίσκεψη σε κάθε τμήμα του οργανισμού και η καταγραφή της κάθε δραστηριότητας που διενεργεί έκαστο. Αν ο οργανισμός έχει οργανόγραμμα, συμβουλευτείτε το. Κάποιες από αυτές τις δραστηριότητες συνεπάγονται επεξεργασία

προσωπικών δεδομένων. Αυτές πρέπει να καταγραφούν στη στήλη αυτή. Αν ένας οργανισμός, έχει τμήμα διεύθυνσης, τμήμα πωλήσεων, τμήμα μάρκετινγκ και τμήμα προσωπικού, συστήνεται όπως η στήλη αυτή χωριστεί σε τέσσερα αντίστοιχα τμήματα και όπως, κάτω από κάθε τμήμα, καταγραφούν οι δραστηριότητές του. Για κάθε δραστηριότητα, πρέπει να γίνει μια σύντομη περιγραφή. Για παράδειγμα, στο τμήμα προσωπικού μπορεί να καταγραφούν δύο δραστηριότητες. «Αρχείο υποψηφίων υπαλλήλων» και «Αρχείο προσωπικού». Για το πρώτο, η περιγραφή μπορεί να διατυπωθεί ως εξής: *Στο αρχείο αυτό τηρούνται τα βιογραφικά σημειώματα υποψήφιων για πρόσληψη* και για το δεύτερο: *Προσωπικοί φάκελοι υπαλλήλων*. Είναι σημαντικό να καταγραφούν όλες οι δραστηριότητες του οργανισμού. Αν το τμήμα μάρκετινγκ διαχειρίζεται την ιστοσελίδα του οργανισμού και συλλέγει στοιχεία πλοήγησης των επισκεπτών της στο διαδίκτυο, μέσω **cookies**, η διαχείριση της ιστοσελίδας θα πρέπει να γραφτεί ως ξεχωριστή δραστηριότητα, με την περιγραφή *παρακολούθηση ιστορικού πλοήγησης επισκεπτών της ιστοσελίδας*. Η χρήση κλειστού κυκλώματος βίντεο-παρακολούθησης πρέπει να καταγράφεται ως ξεχωριστή δραστηριότητα.

2. Κύρια ή Παρεπόμενη

Ο Κανονισμός ξεχωρίζει μεταξύ κύριων/ βασικών και παρεπόμενων δραστηριοτήτων και επιβάλλει κάποιες πρόσθετες υποχρεώσεις για τις πρώτες, όπως για παράδειγμα, τον ορισμό Υπεύθυνου Προστασίας Δεδομένων (**Άρθρο 37(1)(β),(γ)**). Αυτό δεν σημαίνει ότι, τα προσωπικά δεδομένα που τυγχάνουν επεξεργασίας στα πλαίσια παρεπόμενων δραστηριοτήτων είναι λιγότερης σημασίας ή ότι απολαμβάνουν χαμηλότερο επίπεδο προστασίας. Για παράδειγμα, κύρια δραστηριότητα ενός λογιστικού γραφείου είναι η παροχή λογιστικών υπηρεσιών και παρεπόμενη δραστηριότητά του είναι η τήρηση των φακέλων του προσωπικού. Παρόλο που το γραφείο δεσμεύεται από επαγγελματικό απόρρητο να προστατεύει τα προσωπικά δεδομένα του κάθε πελάτη του καθώς και τα δεδομένα των πελατών του κάθε πελάτη, τα δεδομένα υγείας που αναγράφονται στα ιατρικά πιστοποιητικά των υπαλλήλων που λαμβάνουν άδεια ασθενείας τυγχάνουν αυξημένης προστασίας (**Άρθρο 9**), έστω και αν η τήρηση τους συνιστά παρεπόμενη δραστηριότητα. Στη στήλη αυτή, δίπλα από την κάθε δραστηριότητα της πρώτης στήλης, θα πρέπει να γραφτεί αν αυτή είναι κύρια/ βασική ή παρεπόμενη δραστηριότητα. Η άσκηση αυτή βοηθά να εντοπιστούν άλλες υποχρεώσεις που ενδέχεται να βαραίνουν ένα οργανισμό, με βάση τον Κανονισμό.

3. Νομική Βάση

5. Σκοπός της Επεξεργασίας

Στη στήλη αυτή γίνεται μια σύντομη περιγραφή του σκοπού της κάθε επεξεργασίας. Η στήλη αυτή είναι απόλυτα συνυφασμένη με τη στήλη 2 που αφορά στο αν μια επεξεργασία είναι κύρια/ βασική ή παρεπόμενη, τη στήλη 3 που αφορά στη νομική βάση της κάθε επεξεργασίας και με τις στήλες 6(β) και 9 που αφορούν στις κατηγορίες των δεδομένων προσωπικού χαρακτήρα και στην προβλεπόμενη προθεσμία διαγραφής τους, αντίστοιχα. Αν μια δραστηριότητα εξυπηρετεί διάφορους σκοπούς, στη στήλη αυτή θα πρέπει να καταγραφεί έκαστος σκοπός και η περιγραφή του. Για παράδειγμα, μια υπεραγορά έχει, ως παρεπόμενη επεξεργασία σύστημα δωροκάρτας (**loyalty card**) το οποίο χρησιμοποιεί μόνο για σκοπούς παροχής προνομίων ή δώρων στους πελάτες της. Στο σύστημα δεν το καταχωρούνται οι αγορές του κάθε πελάτη. Μια δεύτερη υπεραγορά, διατηρεί παρόμοιο σύστημα, το οποίο όμως χρησιμοποιεί για σκοπούς παροχής προνομίων ή δώρων αλλά και για σκοπούς αποστολής μηνυμάτων **sms** στους πελάτες της για προσφορές. Για το σκοπό αυτό, συλλέγει και τον αριθμό του κινητού τηλεφώνου των πελατών της. Μια τρίτη υπεραγορά έχει διαφορετικό σύστημα το οποίο χρησιμοποιεί για την παροχή προνομίων ή δώρων, την αποστολή διαφημιστικών **sms** αλλά και για την κατάρτιση προφίλ (**Άρθρο 4(4)**) των πελατών τους, με βάση τις καταναλωτικές τους συνήθειες, δηλαδή τι αγοράζουν, πότε το αγοράζουν, προτιμήσεις σε προϊόντα, ποσότητες, τρόπος πληρωμής κλπ, για σκοπούς προγραμματισμού των παραγγελιών της και προσφοράς εξατομικευμένων προσφορών. Και οι τρεις υπεραγορές συλλέγουν τα προσωπικά δεδομένα, με τη συγκατάθεση των πελατών τους. Για τις δύο πρώτες, η δραστηριότητα αυτή μπορεί να θεωρηθεί ως παρεπόμενη αλλά, για την τρίτη, η δραστηριότητα θα πρέπει να θεωρηθεί ως κύρια/ βασική. Στη στήλη αυτή, η κάθε υπεραγορά θα πρέπει να καταγράψει τους σκοπούς που επιδιώκει με το δικό της σύστημα δωροκάρτας. Ο Κανονισμός επιβάλλει σε οργανισμούς όπως ενημερώνουν κατάλληλα τα υποκείμενα των δεδομένων για τους σκοπούς της κάθε επεξεργασίας. Γι' αυτό, η συμπλήρωση της στήλης αυτής θα βοηθήσει και στη συμπλήρωση της τελευταίας στήλης που αφορά στην πληροφόρηση που δίνεται στα υποκείμενα των δεδομένων, για κάθε ξεχωριστή δραστηριότητα. Στο πιο πάνω παράδειγμα, αν οι δύο πρώτες υπεραγορές, αποφασίσουν σε κάποιο στάδιο να εγκαταστήσουν σύστημα δωροκάρτας παρόμοιο με της τρίτης, θα πρέπει να εξετάσουν αν οι καινούργιοι σκοποί που επιδιώκουν είναι συμβατοί με τους αρχικούς (**Άρθρο 5(1)(β)**) και αν η επεξεργασία των προσωπικών δεδομένων των υφιστάμενων πελατών τους

μπορεί να βασιστεί στη συγκατάθεση που αρχικά είχαν δώσει (**Άρθρο 6(4)**). Αν η εκπλήρωση ενός σκοπού βασίζεται στο έννομο συμφέρον που επιδιώκει ο οργανισμός (**Άρθρο 6(1)στ**)), συστήνεται όπως, στο πεδίο αυτό καταγραφτεί το σκεπτικό γιατί το συμφέρον αυτό υπερέχει των συμφερόντων, θεμελιωδών δικαιωμάτων και ελευθεριών των υποκειμένων των δεδομένων. Η συμπλήρωση της στήλης αυτής είναι ιδιαίτερα σημαντική και για δημόσιες Αρχές που προσφέρουν αριθμό υπηρεσιών ή επιδομάτων στη βάση διαφορετικών νομοθεσιών και πρέπει να συλλέγουν, στα έντυπα των αιτήσεων, εκείνα τα δεδομένα που είναι απαραίτητα, με βάση την οικεία νομοθεσία.

6(α),(β). Κατηγορίες υποκειμένων των δεδομένων και κατηγορίες προσωπικών δεδομένων

Στη στήλη 6(α) καταγράφεται η κατηγορία των υποκειμένων των δεδομένων στην οποία αφορά η κάθε επεξεργασία. Κατηγορίες δεδομένων μπορεί να είναι πελάτες, προμηθευτές, συνεργάτες, υπάλληλοι, επισκέπτες της ιστοσελίδας κλπ, ανάλογα με τον τομέα δραστηριότητας του κάθε οργανισμού. Για δημόσιες Αρχές, μια κατηγορία υποκειμένων των δεδομένων μπορεί να είναι τα πρόσωπα που αιτούνται μια συγκεκριμένη υπηρεσία ή επίδομα. Αν μια κατηγορία αφορά παιδιά ή αν σε αυτή περιλαμβάνονται και παιδιά, συστήνεται όπως αυτό καταγραφτεί στη στήλη 6(α), αφού ο Κανονισμός θεσπίζει ειδικές

cy/

Σκονάκι

(3) Legal Basis	(5) Purposes	(6.a) Categories of Data Subjects	(6.b) Categories of Personal Data
Consent	Accounting and auditing	Advisers, consultants and other professional experts	Criminal proceedings, outcomes and sentences
Performance of a contract	Accounts and records	Candidates	Education and training details
Legal obligation	Administration of justice	Complainants, correspondents and enquirers	Employment details
Protection of vital interest	Administration of membership records	Customers and clients	Family, lifestyle and social circumstances
Public interest	Advertising marketing and public relations for others	Members or supporters	Financial details

(7) Categories of Recipients	Logical Controls	Physical Controls	Organisational Controls
Business associates and other professional advisers	Anonymisation	Avoiding Sources of Risk	Integrating PDP in projects
Central government	Archiving	Backups	Managing PDP violations
Credit reference agencies	Encryption	Clamping down on malicious software	Managing Privacy Risk
Current, past or prospective employers of the data subject	Logical Access Control	Hardware Security	Organisation
Data processors	Minimisation	Maintenance	Personnel Management
Data subjects themselves	Paper Document Security	Managing workstations	Policy
Debt collection and tracing agencies	Partitioning	Monitoring Network Activity	Relations with Third-Parties
Education, training establishments and examining bodies	Traceability/Logging	Network Security	Supervision
Employees and agents of the data controller		Operating Security	Training
Financial organisations and advisers		Physical Access Control	
Healthcare, social and welfare advisers or practitioners		Processing Contracts	
Local government		Protecting against non-human sources of risk	
Ombudsmen and regulatory authorities		Website security	
Other companies in the same group as the data controller			
Persons making an enquiry or complaint			
Police forces			
Political organisations			
Private investigators			
Relatives, guardians or other persons associated with the data subject			
Religious organisations			
Suppliers, providers of goods or services			
Survey and research organisations			
The media			
Trade, employer associations and professional bodies			
Trustees of personal data			
Voluntary and charitable organisations			

Homo Digitalis
Protect your rights

enartia
GROUP OF BRANDS

Έλεγχος στα απαιτούμενα νομικά κείμενα.Ενδεικτικά:

- Χαρτογράφηση δεδομένων της επιχείρησης - Αρχείο Δραστηριοτήτων
- Έκθεση ελλείψεων *(Gap Analysis)*
- Πολιτική Προστασίας Προσωπικών Δεδομένων και Πολιτική Χρήσης Cookies ιστοσελίδας
- Αιτήσεις άσκησης των δικαιωμάτων των υποκειμένων των δεδομένων (πρόσβασης, διόρθωσης, διαγραφής, περιορισμού, εναντίωσης ή ανάκλησης συγκατάθεσης και φορητότητας)
- Κείμενα ενημέρωσης ή/και λήψης συγκατάθεσης σχετικά με την επεξεργασία προσωπικών δεδομένων
- Κείμενο ενημέρωσης και λήψης συγκατάθεσης για λήψη και χρήση φωτογραφιών/βίντεο
- Newsletter ▪ Disclaimer προσωπικών δεδομένων για emails
- Συμβάσεις/παραρτήματα συμβάσεων/τροποποίηση συμβάσεων μεταξύ

  α) Υπευθύνων Επεξεργασίας και Εκτελούντων την Επεξεργασία,

  β) Από Κοινού Υπευθύνων Επεξεργασίας

  γ) Συμβάσεις ανάληψης καθηκόντων Υπευθύνου Προστασίας Προσωπικών Δεδομένων (DPO)

  δ) Συμβάσεις/παραρτήματα συμβάσεων/τροποποίηση συμβάσεων εργαζομένων, (περιλαμβάνεται όλη η αναγκαία σύμφωνα με τον GDPR ενημέρωση για την επεξεργασία των προσωπικών τους δεδομένων και να δεσμεύονται με τήρηση εμπιστευτικότητας και πολιτικής «καθαρού γραφείου»)

  ε) Συμβάσεις Εμπιστευτικότητας

- Αρχείο Καταγραφής Παραβιάσεων
- Πρωτόκολλο Καταστροφής
- Πινακίδα για βιντεοεπιτήρηση χώρου και βασικές αρχές για τη νόμιμη χρήση συστήματος βιντεοεπιτήρησης
- Privacy by design σε νέα προϊόντα και υπηρεσίες

Homo Digitalis
Protect your rights

enartia
GROUP OF BRANDS

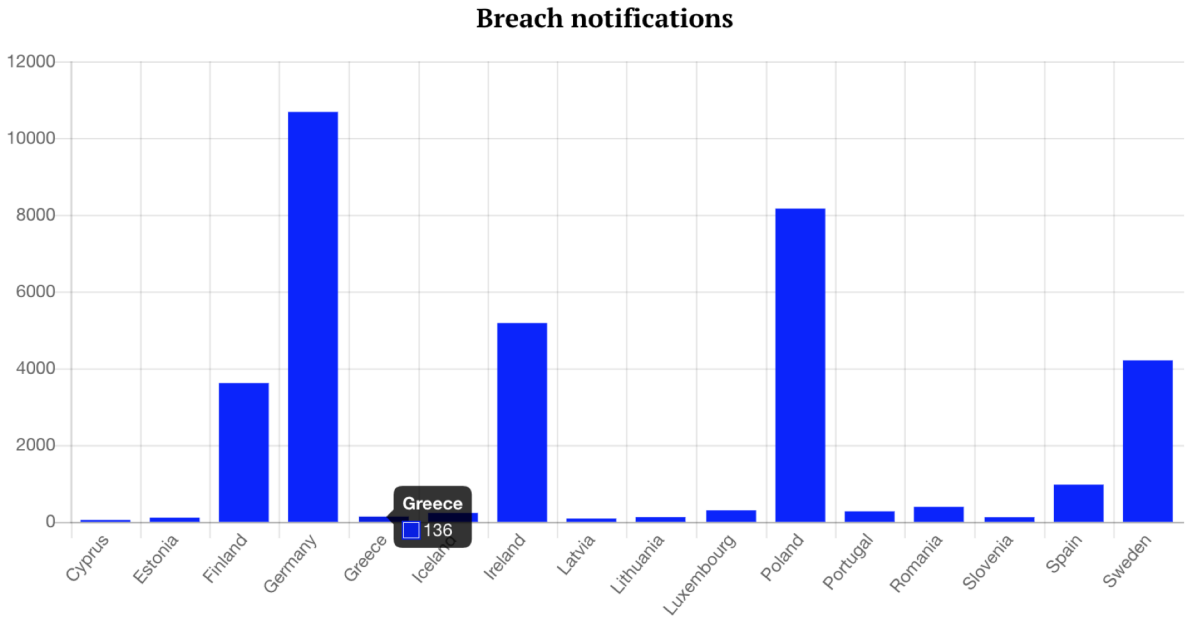
Βασικές συμβουλές για τη σύμβαση μεταξύ Υπευθύνου Επεξεργασίας και Εκτελούντα την Επεξεργασία

- Τα άτομα που επεξεργάζονται τα δεδομένα υπογράφουν σύμβαση εχεμύθειας και εμπιστευτικότητας.

Ο Εκτελών την Επεξεργασία:

- λαμβάνει τα κατάλληλα οργανωτικά και τεχνικά μέτρα για να εξασφαλίσει την ασφάλεια της επεξεργασίας.
- ενεργεί μόνο με γραπτή εντολή του Υπευθύνου Επεξεργασίας.
- οφείλει να βοηθά τον Υπεύθυνο Επεξεργασίας στα αιτήματα πρόσβασης των υποκειμένων στα δεδομένα τους επιτρέποντας τους να ασκούν τα δικαιώματά τους βάσει του Κανονισμού.
- οφείλει να επικουρεί τον Υπεύθυνο Επεξεργασίας στην εκπλήρωση των υποχρεώσεών του Κανονισμού σε σχέση με την ασφάλεια της επεξεργασίας, την γνωστοποίηση των παραβιάσεων των προσωπικών δεδομένων και την Εκτίμηση Αντικτύπου σχετικά με την προστασία δεδομένων.
- δεν μπορεί να προσλάβει άλλον εκτελούντα την επεξεργασία χωρίς προηγούμενη ειδική ή γενικά άδεια του υπεύθυνου επεξεργασίας.
- πρόβλεψη δυνατότητας ελέγχου του

25 May 2018 – 15 May 2019



https://www.gdprtoday.org/

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

- 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.

«καταστροφή»δεδομένων προσωπικού χαρακτήρα:
πρόκειται για την περίπτωση όπου τα δεδομένα παύουν πλέον να υπάρχουν ή παύουν πλέον να υπάρχουν σε μορφή την οποία μπορεί να χρησιμοποιήσει ο υπεύθυνος επεξεργασίας.

«απώλεια» δεδομένων προσωπικού χαρακτήρα:
πρέπει να ερμηνεύεται ως μια περίπτωση όπου τα δεδομένα μπορεί να εξακολουθούν να υπάρχουν, αλλά ο υπεύθυνος επεξεργασίας έχει χάσει τον έλεγχό τους ή την πρόσβαση σ' αυτά ή δεν τα έχει πλέον στην κατοχή του.

μη εξουσιοδοτημένη ή παράνομη επεξεργασία:
μπορεί να περιλαμβάνει την αποκάλυψη δεδομένων προσωπικού χαρακτήρα σε (ή την πρόσβαση από) αποδέκτες που δεν είναι εξουσιοδοτημένοι να λαμβάνουν τα δεδομένα (ή να έχουν πρόσβαση σ' αυτά) ή οποιαδήποτε άλλη μορφή επεξεργασίας που παραβιάζει τον ΓΚΠΔ.

Είδη παραβίασης

Η Ομάδα Εργασίας του άρθρου 29 (νυν Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων) στις Κατευθυντήριες Γραμμές της κατηγοριοποίησε παραβιάσεις τις 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.

Υιοθέτηση Διαδικασίας Αντιμετώπισης Περιστατικών Ασφάλειας και Γνωστοποίησης Παραβιάσεων

Άρθρο 33: Γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα στην ΑΠΔΠΧ

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

- για να ανταποκριθείτε στις υποχρεώσεις των άρθρων 33 και 34, αλλά
- για να αποφύγετε αναίτια γνωστοποίηση συμβάντων που δεν συνιστούν παραβιάσεις δεδομένων προσωπικού χαρακτήρα ή συνιστούν αλλά δεν προκαλούν κίνδυνο για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων

→ **πρέπει να υιοθετήσετε διαδικασία αντιμετώπισης περιστατικών ασφάλειας και γνωστοποίησης παραβιάσεων**

- αρμοδιότητα
- τρόπος αναφοράς συμβάντων
- διοίκηση της εταιρίας, ενημέρωση εμπλεκομένων, ΑΠΔΠΧ,
- τρόπος και μέτρα περιορισμού των επιπτώσεων του περιστατικού παραβίασης.

Homo Digitalis
Protect your rights

enartia
GROUP OF BRANDS

Ενδεικτικά στάδια διαδικασίας αντιμετώπισης περαστατικού ασφαλείας

ΥΙΟΘΕΤΗΣΗ ΔΙΑΔΙΚΑΣΙΑΣ

01 Εκκίνηση διαδικασίας

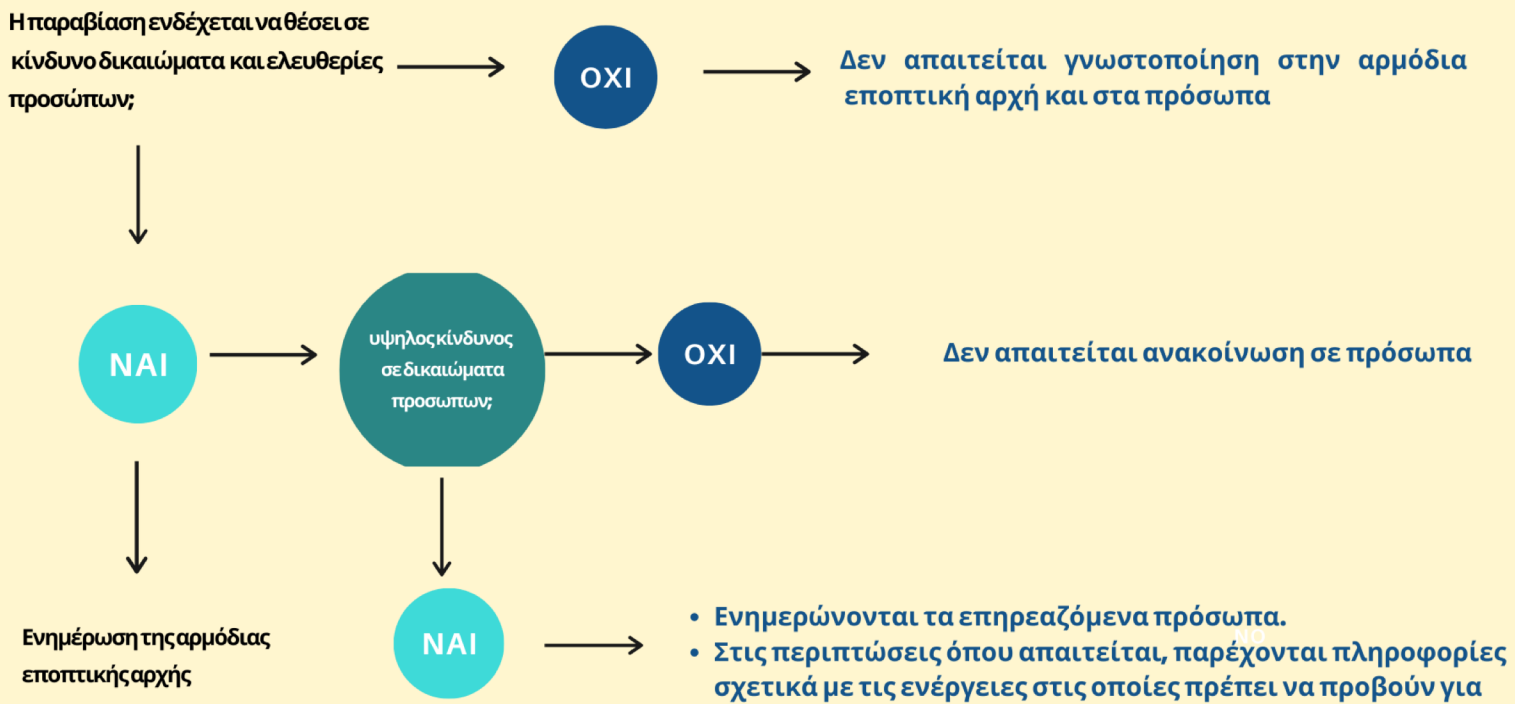
02 Επιβεβαίωση ή όχι του περιστατικού

03 Συγκέντρωση στοιχείων

04 Αξιολόγηση αν πρόκειται για παραβίαση προσωπικών δεδομένων ή όχι

Homo Digitalis
Protect your rights

enartia
GROUP OF BRANDS

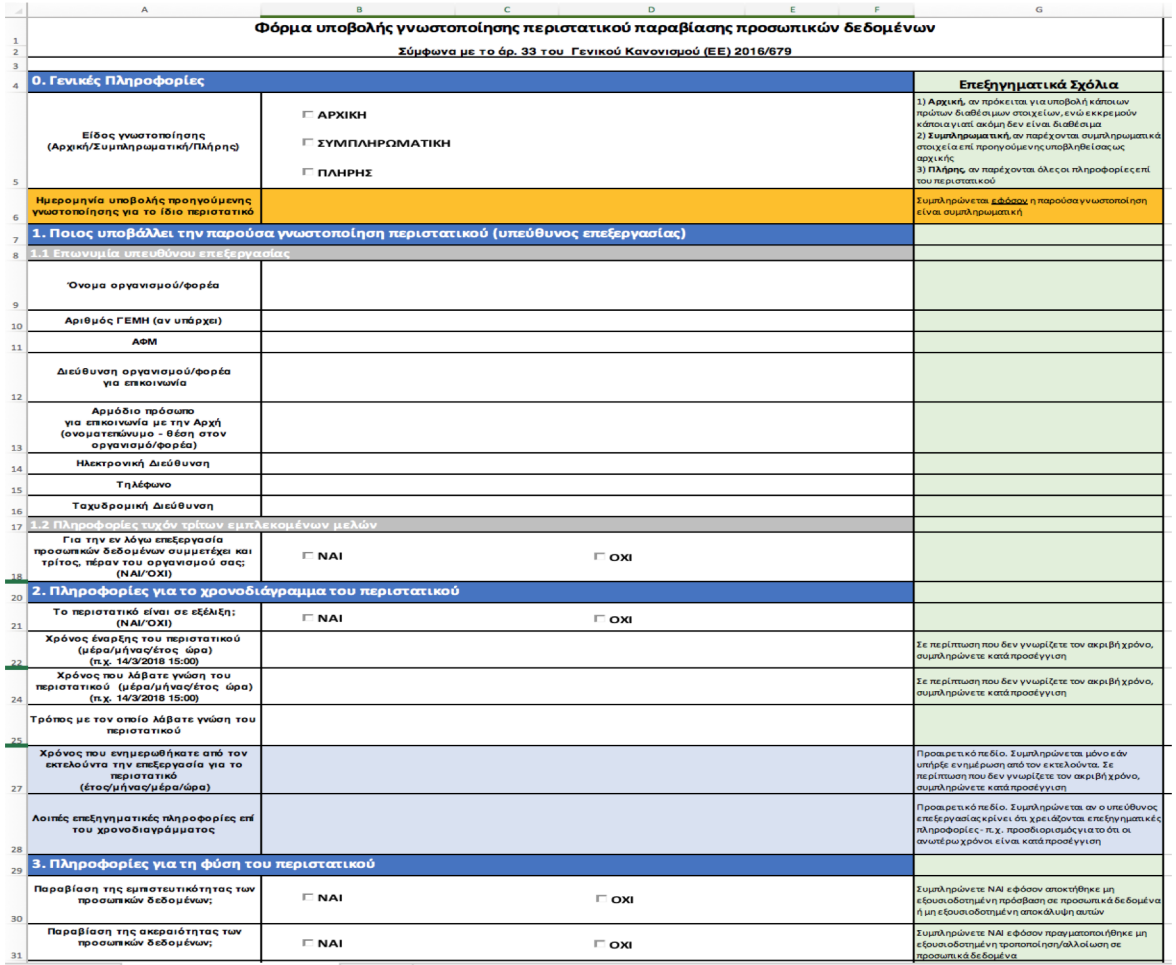


Homo Digitalis
Protect your rights

enartia
GROUP OF BRANDS

Πως γίνεται η γνωστοποίηση στην ΑΠΔΠΧ?

- αμελλητί και, αν είναι δυνατό, **εντός 72 ωρών από τη στιγμή που αποκτά γνώση**
- Όταν η γνωστοποίηση στην εποπτική αρχή δεν πραγματοποιείται εντός 72 ωρών, συνοδεύεται από αιτιολόγηση για την καθυστέρηση.



Φόρμα υποβολής γνωστοποίησης περιστατικού παραβίασης προσωπικών δεδομένων

Σύμφωνα με το άρ. 33 του Γενικού Κανονισμού (ΕΕ) 2016/679

0. Γενικές Πληροφορίες		Επεξηγηματικά Σχόλια
Είδος γνωστοποίησης (Αρχική/Συμπληρωματική/Πλήρης)	☐ ΑΡΧΙΚΗ ☐ ΣΥΜΠΛΗΡΩΜΑΤΙΚΗ ☐ ΠΛΗΡΗΣ	1) **Αρχική**, αν πρόκειται για υποβολή κάποιων πρώτων διαθέσιμων στοιχείων, ενώ εκρεμούν κάποια γιατί ακόμη δεν είναι διαθέσιμα 2) **Συμπληρωματική**, αν παρέχονται συμπληρωματικά στοιχεία επί προηγούμενης υποβληθείσας ως αρχικής 3) **Πλήρης**, αν παρέχονται όλες οι πληροφορίες επί του περιστατικού
Ημερομηνία υποβολής προηγούμενης γνωστοποίησης για το ίδιο περιστατικό		Συμπληρώνεται εφόσον η παρούσα γνωστοποίηση είναι συμπληρωματική
1. Ποιος υποβάλλει την παρούσα γνωστοποίηση περιστατικού (υπεύθυνος επεξεργασίας)		
1.1 Επωνυμία υπευθύνου επεξεργασίας		
Όνομα οργανισμού/φορέα		
Αριθμός ΓΕΜΗ (αν υπάρχει)		
ΑΦΜ		
Διεύθυνση οργανισμού/φορέα για επικοινωνία		
Αρμόδιο πρόσωπο για επικοινωνία με την Αρχή (ονοματεπώνυμο - θέση στον οργανισμό/φορέα)		
Ηλεκτρονική Διεύθυνση		
Τηλέφωνο		
Ταχυδρομική Διεύθυνση		
1.2 Πληροφορίες τυχόν τρίτων εμπλεκομένων μελών		
Για την εν λόγω επεξεργασία προσωπικών δεδομένων συμμετέχει και τρίτος, πέραν του οργανισμού σας; (ΝΑΙ/ΟΧΙ)	☐ ΝΑΙ ☐ ΟΧΙ	
2. Πληροφορίες για το χρονοδιάγραμμα του περιστατικού		
Το περιστατικό είναι σε εξέλιξη; (ΝΑΙ/ΟΧΙ)	☐ ΝΑΙ ☐ ΟΧΙ	
Χρόνος έναρξης του περιστατικού (μέρα/μήνας/έτος ώρα) (π.χ. 14/3/2018 15:00)		Σε περίπτωση που δεν γνωρίζετε τον ακριβή χρόνο, συμπληρώνετε κατά προσέγγιση
Χρόνος που λάβατε γνώση του περιστατικού (μέρα/μήνας/έτος ώρα) (π.χ. 14/3/2018 15:00)		Σε περίπτωση που δεν γνωρίζετε τον ακριβή χρόνο, συμπληρώνετε κατά προσέγγιση
Τρόπος με τον οποίο λάβατε γνώση του περιστατικού		
Χρόνος που ενημερωθήκατε από τον εκτελούντα την επεξεργασία για το περιστατικό (έτος/μήνας/μέρα/ώρα)		Προαιρετικό πεδίο. Συμπληρώνεται μόνο εάν υπήρξε ενημέρωση από τον εκτελούντα. Σε περίπτωση που δεν γνωρίζετε τον ακριβή χρόνο, συμπληρώνετε κατά προσέγγιση
Λοιπές επεξηγηματικές πληροφορίες επί του χρονοδιαγράμματος		Προαιρετικό πεδίο. Συμπληρώνεται αν ο υπεύθυνος επεξεργασίας κρίνει ότι χρειάζονται επεξηγηματικές πληροφορίες - π.χ. προσδιορισμός για το ότι οι ανωτέρω χρόνοι είναι κατά προσέγγιση
3. Πληροφορίες για τη φύση του περιστατικού		
Παραβίαση της εμπιστευτικότητας των προσωπικών δεδομένων;	☐ ΝΑΙ ☐ ΟΧΙ	Συμπληρώνετε ΝΑΙ εφόσον αποκτήθηκε μη εξουσιοδοτημένη πρόσβαση σε προσωπικά δεδομένα ή μη εξουσιοδοτημένη αποκάλυψη αυτών
Παραβίαση της ακεραιότητας των προσωπικών δεδομένων;	☐ ΝΑΙ ☐ ΟΧΙ	Συμπληρώνετε ΝΑΙ εφόσον πραγματοποιήθηκε μη εξουσιοδοτημένη τροποποίηση/αλλοίωση σε προσωπικά δεδομένα

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.

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

ΑΡΧΕΙΟ ΚΑΤΑΓΡΑΦΗΣ ΠΕΡΙΣΤΑΤΙΚΩΝ ΠΑΡΑΒΙΑΣΗ

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.

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 σύμφωνα με την αρχή της λογοδοσίας.

Η σωρευτική τέλεση πολλών διαφορετικών παραβάσεων σε οποιαδήποτε μεμονωμένη περίπτωση **σημαίνει ότι η εποπτική αρχή δύναται να επιβάλει τα διοικητικά πρόστιμα σε επίπεδο αποτελεσματικό, αναλογικό και αποτρεπτικό εντός του ορίου της βαρύτερης παράβασης.»** Σ' αυτή την περίπτωση, η εποπτική αρχή θα έχει επίσης τη δυνατότητα να επιβάλλει κυρώσεις για μη ***γνωστοποίηση ή ανακοίνωση της παραβίασης (άρθρα 33 και 34), αφενός, και για απουσία (επαρκών) μέτρων ασφάλειας (άρθρο 32),*** αφετέρου, δεδομένου ότι πρόκειται για δύο ξεχωριστές παραβιάσεις.

Παράδειγμα	ΑΠΔΠΧ	ΥΔ	Σχόλια
Ιατρικά αρχεία σε ένα νοσοκομείο δεν είναι διαθέσιμα για χρονικό διάστημα 30 ωρών λόγω κυβερνοεπίθεσης.	**Ναι**	**Ναι**	Το νοσοκομείο υποχρεούται να προβεί σε γνωστοποίηση, καθώς ενδέχεται να προκύψει υψηλός κίνδυνος για την ευημερία και την προστασία της ιδιωτικής ζωής των ασθενών. Για παράδειγμα, οι εγχειρίσεις μπορεί να ακυρωθούν και οι ζωές να τεθούν σε κίνδυνο.
Δεδομένα προσωπικού χαρακτήρα μεγάλου αριθμού σπουδαστών εστάλησαν εκ παραδρομής σε εσφαλμένο κατάλογο ηλεκτρονικών διευθύνσεων με περισσότερους από 1000 αποδέκτες.	**Ναι**	**Ναι**	το συμβάν αναφέρεται στα πρόσωπα ανάλογα με την έκταση και το είδος των δεδομένων προσωπικού χαρακτήρα που επηρεάζονται και τη σοβαρότητα των ενδεχόμενων συνεπειών.
Απώλεια Κλοπή Laptop/HY/ κινητού τηλεφώνου με προσωπικά δεδομένα	**Ναι**	**Ναι**	Εφόσον τα δεδομένα έχουν κρυπτογραφηθεί με αλγόριθμο προηγμένης τεχνολογίας, υπάρχουν αντίγραφα ασφαλείας των δεδομένων, το μοναδικό κλειδί δεν έχει τεθεί σε κίνδυνο και είναι δυνατή η επαναφορά των δεδομένων εγκαίρως, αυτό ενδέχεται να μην συνιστά παραβίαση που πρέπει να αναφερθεί. Ωστόσο, εάν τεθεί σε κίνδυνο σε μεταγενέστερο στάδιο, απαιτείται γνωστοποίηση.
Σύντομη διακοπή ρεύματος διάρκειας στο τηλεφωνικό κέντρο υπευθύνου επεξεργασίας	**Όχι**	**Όχι**	Δεν πρόκειται για παραβίαση που πρέπει να γνωστοποιηθεί, ωστόσο δεν παύει να είναι ένα συμβάν που πρέπει να καταγραφεί σύμφωνα με το άρθρο 33 παράγραφος 5.
Διαγραφή αρχείου στοιχείων επικοινωνίας με τους αποφοίτους σε πανεπιστήμιο. Τα στοιχεία ανακτήθηκαν από ένα αντίγραφο ασφάλειας.	**Όχι**	**Όχι**	είναι απίθανο να οδηγήσει σε υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των ατόμων αυτών.

Richard Clarke

> If you spend more on coffee than on IT security, you will be hacked. What's more, you deserve to be hacked.

Thanks!

Elpida Vamvaka