ΕΚΤ
ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΤΕΚΜΗΡΙΩΣΗΣ
NATIONAL DOCUMENTATION CENTRE

Υπηρεσίες SaaS
Διάχυση, Οργάνωση, Ανάδειξη, Διαφύλαξη Ψηφιακού Περιεχομένου

SaaS

Οδηγός προστασίας προσωπικών δεδομένων

ΝΟΜΙΚΕΣ ΕΚΔΟΣΕΙΣ

Εθνικό Κέντρο Τεκμηρίωσης | ΕΙΕ

δ. Βασιλέως Κωνσταντίνου 48, 11635 Αθήνα | **τ.:** 210 7273900
| **f:** 210 7246824 **|** **e:** ekt@ekt.gr | **www.ekt.gr**

Οδηγός προστασίας προσωπικών δεδομένων

Ο παρών οδηγός, με τη μορφή συχνών ερωτήσεων, δίνει μια γενική εικόνα των βασικών εννοιών και διαδικασιών γύρω από τα προσωπικά δεδομένα με σκοπό την επιτυχή αντιμετώπιση τυχόν ζητημάτων προστασίας τους.

Τα δεδομένα προσωπικού χαρακτήρα προστατεύονται κατά κύριο λόγο σύμφωνα με τον νόμο 2472/1997 ο οποίος είναι διαθέσιμος σε ηλεκτρονική μορφή στον σύνδεσμο http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/LAW/NOMOTHESIA%20PROSOPIKA%20DEDOMENA/FILES/2472_97_JUNE2013.PDF

Αρμόδια αρχή για την εποπτεία της εφαρμογής του είναι μια ανεξάρτητη δημόσια αρχή, η Αρχή Προστασίας Προσωπικών Δεδομένων (ΑΠΔΠΧ).

Σε Ευρωπαϊκό επίπεδο, η βασική Οδηγία σε εφαρμογή στην παρούσα φάση είναι η Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:el:HTML).

Στις 14 Απριλίου 2016, εγκρίθηκε από το Ευρωπαϊκό Κοινοβούλιο ο Γενικός Κανονισμός για τα Προσωπικά δεδομένα General Data Protection Regulation, ο οποίος διατίθεται σε ηλεκτρονική μορφή στον σύνδεσμο http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

Ο Κανονισμός θα τεθεί σε ισχύ δύο χρόνια μετά την ημερομηνία δημοσίευσης του στην Επίσημη Εφημερίδα της ΕΕ αντικαθιστώντας την Οδηγία 95/46/ΕΚ.

1) Τι είναι προσωπικά δεδομένα και τι ευαίσθητα προσωπικά δεδομένα ;

«Δεδομένο προσωπικού χαρακτήρα» μπορεί να συνιστά κάθε πληροφορία που αναφέρεται σε ένα ορισμένο πρόσωπο (το υποκείμενο των δεδομένων). Τα προσωπικά δεδομένα διακρίνονται σε απλά και ευαίσθητα. Ο νομοθέτης παρέχει στα ευαίσθητα προσωπικά δεδομένα διευρυμένη προστασία, ορίζοντας αυστηρότερες προϋποθέσεις για την πρόσβαση σε αυτά και την τήρηση αρχείων που να τα εμπεριέχουν.

Τα δεδομένα προσωπικού χαρακτήρα μπορούν, στα πλαίσια διαμόρφωσης αποθετηρίων και τήρησης των σχετικών αρχείων, είτε να συνίστανται σε στοιχεία αναγνώρισης είτε να αναφέρονται σε ενδιαφέροντα - συνήθειες/ δεδομένα ακαδημαϊκής δραστηριότητας/ δεδομένα θέσης κλπ τα οποία να συνδέονται με συγκεκριμένο πρόσωπο.

Ευαίσθητα προσωπικά δεδομένα είναι τα δεδομένα που αφορούν στη φυλετική ή εθνική προέλευση, στα πολιτικά φρονήματα, στις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, στη συμμετοχή σε συνδικαλιστική οργάνωση, στην υγεία, στην κοινωνική πρόνοια και στην ερωτική ζωή, στα σχετικά με ποινικές διώξεις ή καταδίκες, καθώς και στη συμμετοχή σε συναφείς με τα ανωτέρω ενώσεις προσώπων.

Παράδειγμα: Το ονοματεπώνυμο, η διεύθυνση ηλεκτρονικού ταχυδρομείου (email), η διεύθυνση πρωτοκόλλου διαδικτύου (IP address), τα στοιχεία θέασης/διαβάσματος αρχείων, τα στοιχεία που αφορούν λήψεις/ παραγγελίες αρχείων ενός ηλεκτρονικού

αποθετηρίου αποτελούν προσωπικά δεδομένα. Η πληροφορία περί συμμετοχής ενός συγγραφέα σε συνδικαλιστική οργάνωση συνιστά ευαίσθητο προσωπικό του δεδομένο.

2) Σε τι αναφερόμαστε όταν μιλάμε για "επεξεργασία προσωπικών δεδομένων";

Στην έννοια της επεξεργασίας προσωπικών δεδομένων περιλαμβάνεται οποιαδήποτε από τις παρακάτω μεμονωμένες ενέργειες ή και συνδυασμός τους:

α) Η συλλογή τους
β) Η εξαγωγή/καταχώριση/ οργάνωση τους
γ) Η διατήρηση/ αποθήκευση τους
δ) Η τροποποίηση/ χρήση/ διαβίβαση τους
ε) Η κάθε μορφής διάθεση/ συσχέτιση τους ή
στ) Η διαγραφή/ καταστροφή τους

Από οποιαδήποτε από τις παραπάνω ενέργειες προκύπτουν υποχρεώσεις για την εξασφάλιση της νομιμότητας της επεξεργασίας τους. Από τη δε παράλειψη τήρησης αυτών προκύπτει σωρεία κυρώσεων τόσο διοικητικών όσο και ποινικών.

Παράδειγμα: Η συμπλήρωση φόρμας υποβολής ερωτήματος από τον χρήστη μιας ιστοσελίδας στην οποία συμπεριλαμβάνεται το ονοματεπώνυμο και το e-mail του, συνεπάγεται ότι ο λήπτης του ερωτήματος/διαχειριστής θα συλλέξει τα προσωπικά δεδομένα του χρήστη και αυτή του η ενέργεια συνιστά "επεξεργασία".

3) Πότε η επεξεργασία των προσωπικών δεδομένων είναι «νόμιμη»;

Προκειμένου πληροφορίες που συνιστούν προσωπικά δεδομένα να μπορούν να υπόκεινται σε επεξεργασία, πρέπει να συντρέχουν σωρευτικά οι παρακάτω προϋποθέσεις (αρχές):

α) Συλλογή με θεμιτό και νόμιμο τρόπο για καθορισμένους, σαφείς και νόμιμους σκοπούς

Παράδειγμα: Συλλογή, εκ μέρους τρίτου, ηλεκτρονικών διευθύνσεων χωρίς τη συγκατάθεση των δικαιούχων με σκοπό το spamming ή την προώθηση διαφημιστικού υλικού είναι παράνομη (Μον Πρ. Αθ 2110/2002).

β) Θεμιτή και νόμιμη επεξεργασία ενόψει των προκαθορισμένων σκοπών επεξεργασίας

Παράδειγμα: Η τήρηση μητρώου από το Υπουργείο Πολιτισμού κατόχων ανιχνευτών μετάλλων με προσωπικά τους στοιχεία με σκοπό τον έλεγχο της χρήσης των συσκευών αυτών στον ελληνικό χώρο όπου γίνεται ευρείας έκτασης αρχαιοκαπηλία είναι νόμιμη (ΑΠ. 21/2005 ΑΠΔΠΧ).

γ) Δεδομένα συναφή, πρόσφορα, και όχι περισσότερα από όσα κάθε φορά απαιτείται εν όψει των σκοπών της επεξεργασίας

Παράδειγμα: Η συμπλήρωση "ΑΤΟΜΙΚΟΥ - ΑΠΟΓΡΑΦΙΚΟΥ ΔΕΛΤΙΟΥ" από μέλη της ΕΣΗΕΑ για τον έλεγχο και την εκκαθάριση του μητρώου μελών κρίνεται παράνομη κατά το μέρος που ζητούνται στοιχεία σχετικά με το ύψος των αποδοχών του μέλους και με το εάν επιδοτήθηκε από το ταμείο ανεργίας (41/2005ΑΠΔΠΧ).

δ) Δεδομένα ακριβή και ενημερωμένα εφόσον υπόκεινται σε αλλαγές

Παράδειγμα: Εάν μια εταιρεία εμπορίας πληροφοριών (νόμιμη) ενημερώσει μια αντιπροσωπεία αυτοκινήτων ότι ο υποψήφιος επι- πιστώσει αγοραστής αυτοκινήτου έχει στο όνομά του εκκρεμή οφειλή προς άλλη εταιρεία ενώ ο αγοραστής έχει ξοφλήσει την οφειλή του, φέρει ευθύνη, καθώς τα δυσμενή για το υποκείμενο προσωπικά δεδομένα που διαβιβάσθηκαν δεν ήταν ακριβή και ενημερωμένα μέχρι το χρόνο της διαβίβασης (Μον. Πρ. Θεσσαλονίκης 2950/2002).

ε) Διατήρηση των δεδομένων σε μορφή που να επιτρέπει τον προσδιορισμό της ταυτότητας των υποκειμένων τους μόνο κατά τη διάρκεια της περιόδου που απαιτείται για την περάτωση του σκοπού επεξεργασίας για τον οποίο τα αρχεία που περιλαμβάνουν προσωπικά δεδομένα έχουν δημιουργηθεί.

- Η διάρκεια της επεξεργασίας των προσωπικών δεδομένων προσδιορίζεται στην αίτηση γνωστοποίησης που υποβάλλεται στην ΑΠΔΠΧ (αναλυτικότερα βλ. Παράγραφο 5).
- Η παράλειψη λήψης των κατάλληλων μέτρων για την καταστροφή των αρχείων που περιλαμβάνουν προσωπικά δεδομένα μέσα σε εύλογο χρόνο από την περάτωση του σκοπού επεξεργασίας θεωρείται παράνομη.
- Παράδειγμα: προσωπικά δεδομένα που παράγονται ή/και χρησιμοποιούνται καθημερινά στο πλαίσιο των εργασιών του υπεύθυνου επεξεργασίας και τα οποία, μετά από την διεκπεραίωση της συγκεκριμένης εργασίας, είναι πλέον άχρηστα όπως πρόχειρες εκθέσεις, σημειώσεις των υπαλλήλων, πληροφοριακό υλικό, κ.α. σε έντυπη ή/και ηλεκτρονική μορφή πρέπει να καταστρέφονται καθημερινά άλλως γίνεται προγραμματισμένη καταστροφή μέρους ή του συνόλου των δεδομένων αφού έχουν επιτελέσει τον σκοπό για τον οποίο συλλέχθηκαν (Οδηγία 1/2005 ΑΠΔΠΧ).

4) Ποιος είναι ο υπεύθυνος επεξεργασίας και ποιος ο εκτελών την επεξεργασία? Γιατί μας ενδιαφέρει ο καθορισμός τους;

Ο προσδιορισμός της ιδιότητας του προσώπου που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα ως υπευθύνου επεξεργασίας ή εκτελούντα την επεξεργασία, είναι απαραίτητος για τον καθορισμό των υποχρεώσεών του. Η υποχρέωση συμμόρφωσης με τις αρχές νόμιμης επεξεργασίας και η υποχρέωση τήρησης των διαδικασιών γνωστοποίησης στην ΑΠΔΠΧ (αναλυτικότερα βλ. παράγραφο 5) βαρύνουν πρωτίστως τον υπεύθυνο επεξεργασίας και όχι τον εκτελούντα την επεξεργασία.

“Υπεύθυνος επεξεργασίας” είναι οποιοσδήποτε καθορίζει τον σκοπό και τον τρόπο επεξεργασίας των δεδομένων προσωπικού χαρακτήρα, όπως φυσικό ή νομικό πρόσωπο, δημόσια αρχή ή υπηρεσία ή οποιοσδήποτε άλλος οργανισμός.

“Εκτελών την επεξεργασία” είναι οποιοσδήποτε επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό υπεύθυνου επεξεργασίας, όπως φυσικό ή νομικό πρόσωπο, δημόσια αρχή ή υπηρεσία ή οποιοσδήποτε άλλος οργανισμός.

5) Υποχρεώσεις που απορρέουν από την τήρηση αρχείου προσωπικών δεδομένων

i. **Γνωστοποίηση τήρησης αρχείου προς την Αρχή Προστασίας Προσωπικών Δεδομένων (“ΑΠΔΠΧ”):** Κάθε υπεύθυνος επεξεργασίας προσωπικών δεδομένων υποχρεούται να γνωστοποιήσει στην Αρχή τη σύσταση και λειτουργία αρχείου ή την έναρξη της επεξεργασίας. Σε περίπτωση τήρησης αρχείου που περιλαμβάνει ευαίσθητα προσωπικά δεδομένα, η γνωστοποίηση επέχει θέση αιτήσεως για χορήγησης άδειας επεξεργασίας ευαίσθητων δεδομένων. Στην αίτηση/ άδεια προσδιορίζεται και ο σκοπός της επεξεργασίας.

ii. **Γνωστοποίηση τροποποίησης/κατάργησης:** Σε περίπτωση επέλευσης αλλαγής σε οποιεσδήποτε από τις πληροφορίες που γνωστοποιούνται στην ΑΠΔΠΧ σχετικά με το αρχείο (π.χ. διεύθυνση τήρησης αρχείου) υποβάλλεται γνωστοποίηση της τροποποίησης. Το ίδιο καλό είναι να συμβαίνει και σε περίπτωση κατάργησης του αρχείου (αλλά δεν συνιστά εκ του νόμου επιβαλλόμενη υποχρέωση).

iii. **Σεβασμός των δικαιωμάτων ενημέρωσης/ πρόσβασης και αντίρρησης** των χρηστών του εκάστοτε αποθετηρίου ή οποιουδήποτε τρίτου του οποίου τα προσωπικά δεδομένα περιλαμβάνονται στο αποθετήριο.

α) Δικαίωμα ενημέρωσης: Κατά τος στάδιο της συλλογής των προσωπικών δεδομένων, ο υπεύθυνος επεξεργασίας οφείλει να ενημερώσει το υποκείμενο για: την ταυτότητά του, τον σκοπό επεξεργασίας, τους αποδέκτες των δεδομένων, την ύπαρξη των δικαιωμάτων του (πρόσβασης και αντίρρησης). Για τον λόγο αυτό υπάρχει η πολιτική προστασίας προσωπικών δεδομένων και οι σχετικές αναφορές στους Όρους χρήσης κάθε αποθετηρίου.

β) Δικαίωμα πρόσβασης: Το υποκείμενο των προσωπικών δεδομένων έχει δικαίωμα να ζητεί και να λαμβάνει από τον υπεύθυνο επεξεργασίας, χωρίς καθυστέρηση και κατά τρόπο εύληπτο και σαφή πληροφορίες σχετικές με τα προσωπικά του δεδομένα που υπόκεινται σε επεξεργασία. Προς τούτο, το ΕΚΤ, εφόσον ενεργεί ως υπεύθυνος επεξεργασίας, έχει υποχρέωση να απαντήσει τόσο για τα δεδομένα και την προέλευσή τους όσο και για τους σκοπούς επεξεργασίας/ αποδέκτες/ την εξέλιξη της επεξεργασίας/ την κοινοποίηση σε τρίτους κ.α.

γ) Δικαίωμα αντίρρησης: Τέλος, το υποκείμενο έχει το δικαίωμα, οποτεδήποτε, να ζητήσει τη διόρθωση, διαγραφή, τροποποίηση ή να εκφράσει οποιαδήποτε άλλη αντίρρηση στην επεξεργασία των προσωπικών του δεδομένων. Ο υπεύθυνος επεξεργασίας έχει την υποχρέωση να απαντήσει εγγράφως επί των αντιρρήσεων μέσα σε αποκλειστική προθεσμία δεκαπέντε (15) ημερών.

iv. **Επεξεργασία μόνο για τους σκοπούς που έχουν γνωστοποιηθεί** στην ΑΠΔΠΧ και διατήρηση των δεδομένων μόνο για την χρονική διάρκεια που απαιτείται για τους σκοπούς αυτούς.

v. **Λήψη των κατάλληλων οργανωτικών και τεχνικών μέτρων για την ασφάλεια των δεδομένων** και την προστασία τους από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας.

ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΤΕΚΜΗΡΙΩΣΗΣ
NATIONAL DOCUMENTATION CENTRE

Υπηρεσίες SaaS
Διάχυση, Οργάνωση, Ανάδειξη, Διαφύλαξη Ψηφιακού Περιεχομένου

saas.ekt.gr

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Ταμείο Περιφερειακής Ανάπτυξης

ψηφιακήελλάδα
Όλα είναι δυνατά
Επιχειρησιακό Πρόγραμμα "Ψηφιακή Σύγκλιση"

ΕΣΠΑ 2007-2013

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Παιδείας Έρευνας & Θρησκευμάτων

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Οι Υπηρεσίες SaaS του ΕΚΤ αναπτύχθηκαν στο πλαίσιο της Πράξης "Πλατφόρμα Παροχής Υπηρεσιών Κατάθεσης, Διαχείρισης και Διάθεσης Ανοικτών Δεδομένων και Ψηφιακού Περιεχομένου", η οποία εντάσσεται στο Επιχειρησιακό Πρόγραμμα "Ψηφιακή Σύγκλιση" (ΕΣΠΑ), με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης - Ευρωπαϊκό Ταμείο Περιφερειακής Ανάπτυξης.