Πρακτική εφαρμογή της προστασίας δεδομένων στα Λογιστικά Γραφεία

Μία σύντομη αναφορά για το πως επηρεάζονται τα λογιστικά γραφεία από την εφαρμογή του Γενικού Κανονισμού για την Προστασία Δεδομένων, ανάλυση περιπτώσεων, προτάσεις εφαρμογής νέων και βελτίωσης υπαρχουσών διαδικασιών

ΣΥΓΓΡΑΦΗ – ΕΠΙΜΕΛΕΙΑ ΚΕΙΜΕΝΟΥ:

Θεόδωρος Κεντιστός-Ράννος

Έκδοση 1.0 / 20181201

Βεβαιωθείτε ότι διαβάζετε την τελευταία έκδοση του ενημερωτικού πατώντας ΕΔΩ

ή στον ιστότοπο της Π.Ο.Φ.Ε.Ε. (www.pofee.gr)

Μπορείτε να υποβάλετε σχόλια, διορθώσεις, προτάσεις βελτίωσης και εμπλουτισμού μέσω φόρμας στο https://goo.gl/forms/KLw8nRvqsgrOktBU2 ή με email στο info@pofee.gr

Περιεχόμενα

Εισαγωγή

Αυτό το έντυπο έχει ως στόχο την ενημέρωση των λογιστικών γραφείων σε πρακτικό και πλαίσιο.

Είναι βασισμένο σε κείμενα από τα προηγούμενα ενημερωτικά της Π.Ο.Φ.Ε.Ε., της Ε.Ε. καθώς και άλλων πηγών. Σκοπός του είναι να γίνει ανάλυση ορισμένων βασικών δραστηριοτήτων των λογιστικών γραφείων, όπως την επεξεργασία των δεδομένων και την προστασία αυτών, και των ενδεχόμενων κινδύνων που σχετίζονται με αυτές.

Σκοπός αυτού του εντύπου δεν είναι η κινδυνολογία, αλλά η ενημέρωση και ο ενδεχόμενος δημιουργικός διάλογος μεταξύ συναδέλφων – και όχι μόνο – με στόχο την εξοικείωση των λογιστικών γραφείων (ελευθέρων επαγγελματιών και υπαλλήλων) με το **τι περιέχει** και **τι απαιτεί** ο Γενικός Κανονισμός Προστασίας Δεδομένων από ένα λογιστικό γραφείο σε ότι αφορά στις διαδικασίες που αφορούν δεδομένα προσωπικού χαρακτήρα των υπαλλήλων και των πελατών καθώς και σε θέματα πιο τεχνικής φύσεως, με στόχο την δημιουργία μιας κουλτούρας προστασίας δεδομένων σε προσωπικό και σε επαγγελματικό επίπεδο.

Ο Γενικός Κανονισμός Προστασίας Δεδομένων και τα Λογιστικά Γραφεία

Ο Γενικός Κανονισμός για την Προστασία Δεδομένων (Κανονισμός (ΕΕ) 2016/679) της Ευρωπαϊκής Ένωσης, επηρεάζει σε μεγάλο βαθμό τις διαδικασίες διαχείρισης δεδομένων προσωπικού χαρακτήρα που επεξεργάζονται τα λογιστικά γραφεία.

Σε αυτό το κείμενο θα επικεντρωθούμε σε δύο βασικά σημεία που απαιτούν ιδιαίτερη προσοχή και τα οποία είναι: η **ασφάλεια (προστασία) των δεδομένων** και ο **λόγος (νομική βάση) της επεξεργασίας** τους.

Τι σημαίνει «επεξεργασία» δεδομένων προσωπικού χαρακτήρα;

Επεξεργασία είναι η εκτέλεση οποιασδήποτε εργασίας ή συνόλου εργασιών σε δεδομένα προσωπικού χαρακτήρα, μεταξύ των οποίων:

- συλλογή, καταχώριση ή διατήρηση δεδομένων
- οργάνωση ή τροποποίηση των δεδομένων
- ανάκτηση, αναζήτηση ή χρήση των δεδομένων
- αποκάλυψη των δεδομένων σε τρίτο μέρος (συμπεριλαμβανομένης της δημοσίευσης)
- διαγραφή ή καταστροφή των δεδομένων.

Ένα λογιστικό γραφείο μπορεί να επεξεργάζεται δεδομένα προσωπικού χαρακτήρα, όπως ενδεικτικά:

- Φορολογούμενων **φυσικών προσώπων**, για τους οποίους μπορεί να:
  - υποβάλλουν φορολογικά έντυπα όπως δηλώσεις Ε1, Ε2, Ε3, Ε9, κ.α.
  - υποβάλλουν ασφαλιστικές δηλώσεις για μη-μισθωτούς στον ΕΦΚΑ
  - εκτυπώνουν ή να αποστέλλουν εκκαθαριστικά δηλώσεων, ΕΝΦΙΑ, κ.α.
- **Υπαλλήλων** του ίδιου του λογιστικού γραφείου ή επιχειρήσεων-πελατών:
  - μισθοδοσία, προσλήψεις, αποχωρήσεις, κλπ διαδικασίες που αφορούν το προσωπικό
  - υποβολή ΑΠΔ στον ΕΦΚΑ, υποβολή ετήσιου πίνακα προσωπικού Ε4
  - υποβολή βεβαιώσεων αποδοχών
  - διατήρηση των στοιχείων αυτών (φυσική ή ηλεκτρονική μορφή) στο λογιστικό γραφείο μέχρι να λήξει αυτή η συμφωνία/υποχρέωση ή για όσο ορίζει ο εκάστοτε νόμος, κλπ.
- Πελατών γενικότερα ή εν δυνάμει πελατών (φυσικών προσώπων) με σκοπό:
  - την αποστολή ενημερωτικών (π.χ. newsletters) μέσω email ή SMS
  - την τηλεφωνική επικοινωνία μετά το πέρας της ανατιθέμενης εργασίας (π.χ. για μελλοντική υποβολή κάποιας δήλωσης)

«Υπεύθυνος Επεξεργασίας» ή «Εκτελών την Επεξεργασία»;

Υπεύθυνος επεξεργασίας: είναι το πρόσωπο ή εταιρία ή ο οργανισμός που αποφασίζει τους «σκοπούς για τους οποίους» και τα «μέσα με τα οποία» γίνεται η επεξεργασία των δεδομένων προσωπικού χαρακτήρα. Ο «σκοπός» της επεξεργασίας των δεδομένων περιλαμβάνει «γιατί» τα δεδομένα προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία και τα «μέσα» της επεξεργασίας περιλαμβάνουν «πώς» τα δεδομένα υποβάλλονται σε επεξεργασία.

Εκτελών την επεξεργασία: ένα πρόσωπο ή μια εταιρία ή ένας οργανισμός που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό ενός υπεύθυνου δεδομένων.

Σε κάθε μία από αυτές τις περιπτώσεις ένα λογιστικό γραφείο επεξεργάζεται δεδομένα προσωπικού χαρακτήρα ως:

- **Εκτελών την επεξεργασία**, στις περιπτώσεις που γίνεται επεξεργασία δεδομένων προσωπικού χαρακτήρα για λογαριασμό άλλου ατόμου ή επιχείρησης. Όπως για παράδειγμα:
    - Επεξεργασία δεδομένων προσωπικού χαρακτήρα πελάτη - ιδιώτη για λογαριασμό του ίδιου του πελάτη (π.χ. φορολογική δήλωση)
    - Επεξεργασία δεδομένων προσωπικού χαρακτήρα εργαζομένων για λογαριασμό ενός πελάτη που έχει επιχείρηση και απασχολεί το προσωπικό αυτό (π.χ. μισθοδοσία, υποβολή ΑΠΔ στον ΕΦΚΑ)
- **Υπεύθυνος επεξεργασίας,** (π.χ. ιδιοκτήτης του λογιστικού γραφείου) στις περιπτώσεις:
    - που γίνεται συλλογή δεδομένων προσωπικού χαρακτήρα των υπαλλήλων του λογιστικού γραφείου για χρήση σε δημόσιους οργανισμούς όπως π.χ. ΣΕΠΕ, ΕΦΚΑ, εφορία, κλπ.
    - που υπάρχει σύστημα βιντεοεπιτήρησης στο λογιστικό γραφείο
    - που το λογιστικό γραφείο διαχειρίζεται κάποια βάση δεδομένων για δική του χρήση για παράδειγμα λίστα πελατών ή εν δυνάμει πελατών ή λίστα παραληπτών για αποστολή ενημερωτικών email (newsletter).

Υπεύθυνος Προστασίας Δεδομένων (DPO) σε ένα λογιστικό γραφείο;

Τα περισσότερα λογιστικά γραφεία δεν απαιτούνται να διορίζουν έναν DPO, αλλά μπορούν να το κάνουν αν το επιθυμούν.

Η υποχρέωση ορισμού DPO, σύμφωνα με τον Γενικό Κανονισμό ισχύει για:

- όλες τις **δημόσιες αρχές και φορείς**
  (ανεξαρτήτως του είδους δεδομένων που επεξεργάζονται)
- για εταιρίες που έχουν ως **βασική δραστηριότητα** τη **τακτική** και **συστηματική παρακολούθηση** φυσικών προσώπων σε **μεγάλη κλίμακα**
- ή την επεξεργασία **ειδικών κατηγοριών** δεδομένων προσωπικού χαρακτήρα σε **μεγάλη κλίμακα**

Ο κανονισμός δεν θέτει κάποια υποχρεωτική απαίτηση για πιστοποίηση του DPO[1], και ένας DPO ενώ μπορεί να επιτελεί «και άλλα καθήκοντα και υποχρεώσεις» μέσα σε μια επιχείρηση, ωστόσο **δεν θα πρέπει αυτά να συνεπάγονται σε σύγκρουση συμφερόντων**, δηλαδή δεν θα πρέπει να έχει και θέση ευθύνης στην επιχείρηση αυτή (για παράδειγμα δεν μπορεί DPO να είναι ο ίδιος ο επιχειρηματίας στην επιχείρηση του)

Η ομάδα εργασίας του άρθρου 29 συνιστά στους υπεύθυνους επεξεργασίας και τους εκτελούντες την επεξεργασία: Να καταγράφουν την εσωτερική ανάλυση που διενεργούν προκειμένου να προσδιορίσουν αν πρέπει ή όχι να διοριστεί DPO, ώστε να μπορούν να αποδείξουν ότι λήφθηκαν δεόντως υπόψη οι σχετικοί

[1] Έγγραφο Γ/ΕΞ/6007 στις 9/8/2017 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

παράγοντες. Η εν λόγω ανάλυση αποτελεί μέρος της απαιτούμενης τεκμηρίωσης δυνάμει της αρχής της λογοδοσίας, μπορεί να ζητηθεί από την εποπτική αρχή και θα πρέπει να επικαιροποιείται όταν κρίνεται απαραίτητο.

Να σημειωθεί ότι ενώ ένα λογιστικό γραφείο μπορεί να μην έχει την υποχρέωση ορισμού ενός DPO, ωστόσο έχει πάντα την υποχρέωση εφαρμογής του κανονισμού και καλό είναι να αναζητεί γενικές συμβουλές ή και πιο εξειδικευμένες από άτομα ή εταιρίες που συνεργάζεται και έχουν αυτή την γνώση.

Για παράδειγμα: Μια εταιρία λογισμικού της οποίας τα προγράμματα χρησιμοποιούνται στα λογιστικά γραφεία, ενδέχεται να έχει προσθέσει κάποιες επιπλέον δυνατότητες στα προγράμματα της έτσι ώστε να είναι «περισσότερο συμβατά» με τον GDPR (π.χ. δυνατότητα πρόσβασης με κωδικό στο πρόγραμμα ή κρυπτογράφησης βάσης δεδομένων ή εξαγωγή αρχείων pdf με κωδικό πρόσβασης ή ανωνυμοποίηση, κλπ). Αυτό για το λογιστικό γραφείο σημαίνει ότι μια τέτοια νέα λειτουργία μπορεί να βελτιώσει την ασφάλεια και την προστασία των δεδομένων που διαχειρίζεται.

Αρχεία δραστηριοτήτων επεξεργασίας

Οι μικρομεσαίες επιχειρήσεις (λιγότερα από 250 άτομα) **είναι υποχρεωμένες** να τηρούν αρχεία επεξεργασίας δεδομένων για τις περιπτώσεις που η επεξεργασία των δεδομένων:

- Είναι **τακτική** (ενδεικτικά: μισθοδοσία προσωπικού)
- Αποτελεί **κίνδυνο** για τα δικαιώματα και τις ελευθερίες των ατόμων
- Αφορά **ευαίσθητα δεδομένα** ή **ποινικό μητρώο**

Αρχεία δραστηριοτήτων επεξεργασίας πρέπει να τηρούν και οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία και να υφίστανται και μεταξύ άλλων σε ηλεκτρονική μορφή και να τίθεται στην διάθεση της εποπτικής αρχής κατόπιν αιτήματος (αρχή της λογοδοσίας). Η κάθε επιχείρηση θα πρέπει να έχει τα δικά της αρχεία ανάλογα με το είδος της επεξεργασίας που κάνει. Για παράδειγμα αν κάποια επιχείρηση έχει και τις δυο ιδιότητες θα πρέπει να διατηρεί και τα δυο αρχεία συμπληρωμένα με τις εκάστοτε δραστηριότητες της.

Παράδειγμα: Αν ένα λογιστικό γραφείο έχει αναλάβει την μισθοδοσία μιας επιχείρησης, τότε η επιχείρηση αυτή διατηρεί για την συγκεκριμένη δραστηριότητα μια εγγραφή στο αρχείο δραστηριοτήτων επεξεργασίας (*αρχείο: υπεύθυνος επεξεργασίας*) δηλώνοντας το λογιστικό γραφείο ως εκτελών την επεξεργασία. Αντίστοιχα το λογιστικό γραφείο δηλώνει στο δικό του αρχείο δραστηριοτήτων επεξεργασίας (*αρχείο: εκτελών την επεξεργασία*) τα στοιχεία της επιχείρησης.

Υποδείγματα αρχείου δραστηριοτήτων καθώς και επιπλέον πληροφορίες, μπορείτε να βρείτε στην σελίδα της ΑΠΔΠΧ: http://www.dpa.gr/portal/page?_pageid=33,211400&_dad=portal&_schema=PORTAL

Υποδείγματα αρχείου δραστηριοτήτων (αρχεία excel)	
Υπεύθυνος επεξεργασίας	Εκτελών την επεξεργασία

Σημείωση: Τα αρχεία περιέχουν μια καρτέλα (επεξήγηση) με όλες τις απαραίτητες πληροφορίες συμπλήρωσης

Σύμφωνα με την θέση της ομάδας εργασίας του άρθρου 29 για το άρθρο 30 παρ.5 του GDPR:

(Για παράδειγμα) Μια μικρή επιχείρηση είναι πιθανό να επεξεργάζεται τακτικά, δεδομένα σχετικά με τους εργαζομένους της. Ως εκ τούτου, η εν λόγω επεξεργασία **δεν μπορεί να θεωρηθεί «περιστασιακή» και πρέπει επομένως να συμπεριληφθεί στο αρχείο δραστηριοτήτων επεξεργασίας.**

Η ομάδα εργασίας του άρθρου 29, θεωρεί ότι μια δραστηριότητα επεξεργασίας μπορεί να θεωρηθεί ως «περιστασιακή» μόνον εάν δεν πραγματοποιείται τακτικά, και εμφανίζεται εκτός της τακτικής πορείας της επιχείρησης ή της δραστηριότητας του υπευθύνου της επεξεργασίας ή του εκτελών την επεξεργασία.[2]

[2] Διαβάσετε εδώ τις κατευθυντήριες γραμμές της ομάδας εργασίας του άρθρου 29 για το άρθρο 49 του κανονισμού 2016/679 (WP262)

Το προφίλ του κινδύνου σε γενικές γραμμές

Το προφίλ κινδύνου των δεδομένων προσωπικού χαρακτήρα που επεξεργάζεται η κάθε επιχείρηση θα πρέπει να προσδιορίζεται σύμφωνα με τις διαδικασίες επεξεργασίας δεδομένων προσωπικού χαρακτήρα που διενεργούνται, την πολυπλοκότητα και την κλίμακα της επεξεργασίας δεδομένων, την ευαισθησία των δεδομένων που υποβάλλονται σε επεξεργασία και την προστασία που απαιτείται για την επεξεργασία των δεδομένων αυτών. Για παράδειγμα, όταν μια δραστηριότητα επεξεργασίας δεδομένων είναι ιδιαίτερα περίπλοκη, ή όπου γίνεται σε μεγάλη κλίμακα ή αφορά ευαίσθητα δεδομένα (δηλ. μια διαδικτυακή, υγειονομική, οικονομική ή ασφαλιστική εταιρία), αυτό εμπεριέχει υψηλότερο κίνδυνο από τα συνήθη δεδομένα προσωπικού χαρακτήρα που αφορούν αποκλειστικά στα στοιχεία του λογαριασμού ενός υπαλλήλου ή ενός πελάτη.

Όταν εξετάζετε το προφίλ κινδύνου των δεδομένων προσωπικού χαρακτήρα που επεξεργάζεται η επιχείρηση σας, είναι χρήσιμο να εξετάσετε τις απτές βλάβες που μπορεί να προκληθούν στα άτομα και για τις οποίες η επιχείρηση σας πρέπει να λάβει μέτρα προστασίας. Αυτά αναφέρονται λεπτομερώς στην αιτιολογική σκέψη 75 του GDPR και περιλαμβάνουν επεξεργασία που θα μπορούσε να οδηγήσει σε: διακρίσεις, κλοπή ταυτότητας ή απάτη, οικονομική ζημία, ζημία στη φήμη, απώλεια του εμπιστευτικού χαρακτήρα των δεδομένων προσωπικού χαρακτήρα που προστατεύονται από το επαγγελματικό απόρρητο, μη εξουσιοδοτημένη αντιστροφή του ψευδωνύμου, ή οποιοδήποτε άλλο σημαντικό οικονομικό ή κοινωνικό μειονέκτημα.

Αναλυτικότερα στο κεφάλαιο «Προστασία Δεδομένων».

Προστασία δεδομένων

Την προστασία των δεδομένων (είτε είναι προσωπικού χαρακτήρα είτε όχι), είναι κάτι το οποίο τα τελευταία χρόνια τα λογιστικά γραφεία έχουν αφιερώσει αρκετό χρόνο για να βελτιώσουν διαδικαστικά και να εντάξουν στην κουλτούρα τους.

Όμως, σύμφωνα με τον GDPR θα πρέπει να δοθεί ιδιαίτερη έμφαση σε κάποιες πτυχές της προστασίας των δεδομένων, και συγκεκριμένα στα δεδομένα προσωπικού χαρακτήρα των φυσικών προσώπων.

Καλό είναι ο κάθε ένας μας να αφιερώσει χρόνο να κατανοήσει την έννοια της αυτό-προστασίας έτσι ώστε να είναι σε καλύτερη θέση να αντιληφθεί τους τρόπους με τους οποίους μπορεί να βελτιώσει την προστασία σε προσωπικό επίπεδο και να φέρει αυτή την εμπειρία και στην εργασία του.

Τα δεδομένα προσωπικού χαρακτήρα που περνάνε μέσα από ένα λογιστικό γραφείο μπορεί να διαφέρουν σε τρόπο συλλογής και επεξεργασίας από τα δεδομένα που π.χ. μπορεί να συλλέγει ένα νοσοκομείο που επεξεργάζεται κατά κύριο λόγο ευαίσθητα δεδομένα ασθενών ή μια εταιρία που κάνει επεξεργασία δεδομένων για κατάρτιση προφίλ καταναλωτών σε μεγάλη κλίμακα, όμως ένα λογιστικό γραφείο σε αρκετές περιπτώσεις διατηρεί για την εκτέλεση των εργασιών του, δεδομένα (προσωπικού χαρακτήρα και μη) είτε σε φυσική μορφή είτε ψηφιακή τα οποία ενέχουν εξίσου υψηλό κίνδυνο.

Ενδεικτικά, μια κατηγοριοποίηση της επικινδυνότητας των δεδομένων που ενδέχεται να επεξεργάζεται ένα λογιστικό γραφείο είναι:

- Δεδομένα **χαμηλής-μέτριας** επικινδυνότητας

π.χ. **ονοματεπώνυμα, διευθύνσεις, τηλέφωνα, email, φωτογραφίες ατόμου, κ.α.**

Στοιχεία αυτής της κατηγορίας μπορεί κάποιος εύκολα να τα βρει ίσως και μέσω μιας αναζήτησης στο internet σε μέσα κοινωνικής δικτύωσης, σε τηλεφωνικούς καταλόγους, κλπ.

- Δεδομένα **μέτριας-υψηλής** επικινδυνότητας

π.χ. **εισοδήματα, περιουσιακά στοιχεία, κ.α.**

Τα στοιχεία αυτά μπορούν να οδηγήσουν σε διακρίσεις, ζημιά στην φήμη, στοχοποίηση για εγκληματικές ενέργειες.

- Δεδομένα **υψηλής** επικινδυνότητας

π.χ. **αριθμός ΑΦΜ, εκκαθαριστικό (έντυπο), αριθμός ΑΜΙΚΑ - ΑΜΚΑ, αριθμό ή και φωτοτυπία ταυτότητας ή διπλώματος οδήγησης κ.α.**

Τα στοιχεία αυτά μπορεί να οδηγήσουν σε κλοπή ταυτότητας ή απάτη, δημιουργώντας ακόμα και οικονομική ή και κοινωνική ζημιά.

- Δεδομένα **πολύ υψηλής** επικινδυνότητας

π.χ. **όνομα χρήστη και κωδικός πρόσβασης σε υπηρεσίες Taxisnet, ΕΦΚΑ, τραπεζικούς λογαριασμούς, κ.α.**

*Τα στοιχεία αυτά δίνουν άμεση πρόσβαση σε δεδομένα προσωπικού χαρακτήρα και μπορούν να προκαλέσουν ακόμα και **άμεση οικονομική** ή και κοινωνική ζημιά.*

👉 Σημείωση: Μια παραβίαση δεδομένων επέρχεται όταν σημειώνεται συμβάν ασφαλείας σε σχέση με τα δεδομένα για τα οποία ευθύνεστε, με αποτέλεσμα:

- την **παραβίαση** του **απορρήτου**
  Ενδεικτικά: να τα διαβάσει ή φωτογραφήσει ή επεξεργαστεί κάποιο μη εξουσιοδοτημένο άτομο

- την **παραβίαση** της **διαθεσιμότητας**
  Ενδεικτικά: να χαθούν από το αρχείο του λογιστικού γραφείου λόγω κλοπής ή να καταστραφούν

- την **παραβίαση** της **ακεραιότητας**
  Ενδεικτικά: εσκεμμένη αλλαγή στοιχείων ενός εγγράφου ή π.χ. μερική καταστροφή ενός πρωτότυπου εντύπου

Προστασία δεδομένων σε έντυπη μορφή

Ένα λογιστικό γραφείο λαμβάνει αρκετά έγγραφα σε έντυπη μορφή, όπως συμβάσεις υπαλλήλων, συμβόλαια πελατών κλπ. Κύριο μέλημα σε όλες αυτές τις περιπτώσεις είναι η προστασία τους από οποιαδήποτε παραβίαση και αυτό μπορεί να επιτευχθεί έως έναν βαθμό με τους εξής τρόπους:

Ανάλυση: Πρόσβαση στον χώρο, έγγραφα σε κοινή θέα, διατήρηση & καταστροφή εγγράφων

Θέμα	Ανάλυση - Κίνδυνοι - Ενέργειες
Πρόσβαση στον χώρο Έγγραφα σε κοινή θέα Αποθήκευση φυσικών εγγράφων	ℹ Τα λογιστικά γραφεία είναι ανοιχτά προς το κοινό και οι πελάτες μπορούν εύκολα να εισέρχονται και ίσως και να κινούνται εύκολα μέσα σε αυτά. Διάφορα έγγραφα μπορεί να είναι σε ένα γραφείο την ώρα που ο Λογιστής-Φοροτεχνικός έχει κάποιον πελάτη στον συγκεκριμένο χώρο ή όταν κάποιος τρίτος έχει πρόβαση στον συγκεκριμένο χώρο (π.χ. τεχνικός υπολογιστών ή συνεργείο καθαρισμού, κλπ). ⚠ Ένα έγγραφο (ακόμα και αν δεν περιέχει δεδομένα προσωπικού χαρακτήρα) το οποίο βρίσκεται σε κοινή θέα ενέχει το κίνδυνο αρχικά κάποιος να το διαβάσει, ή σε λιγότερο πίθανα - και ίσως σε σχετικά απίθανα σενάρια - να το φωτογραφήσει, να το κλέψει ή να το αλλοιώσει έστω και κατά λάθος (π.χ. να ρίξει καφέ πάνω του καταστρέφοντας το μερικώς ή ολικώς). **Ο κίνδυνος εδώ είναι ανάλογος του είδους των δεδομένων προσωπικού χαρακτήρα που περιλαμβάνονται.** Περιορίστε και ελέγχετε τον χώρο στον οποίο μπορεί να κινηθεί το κοινό σας. Για παράδειγμα, μπορεί να γίνει βάζοντας μερικές καρέκλες στην είσοδο και ζητώντας από το κοινό να κάτσει και να περιμένει ή τοποθετήστε «εμπόδια» όπως γραφεία ή φυτά για να αποτρέψετε κινήσεις σε μέρη που δεν πρέπει να έχει πρόσβαση το κοινό. Μεριμνήστε για την αποθήκευση των εγγράφων σε σημεία εκτός κοινής θέας και πρόσβασης (συρτάρια, ντουλάπια, ή άλλος χώρος που η πρόσβαση είναι περιορισμένη). Αν π.χ. τα ντουλάπια δεν έχουν πόρτες καλό είναι να **μην είναι ευδιάκριτο κάποιο αναγνωριστικό** (π.χ. ετικέτα) στην περίπτωση που στον χώρο έχει πρόσβαση το κοινό ή κάποιος τρίτος. Ιδανικά τα μέρη αποθήκευσης που έχουν αρχεία με υψηλό κίνδυνο δεδομένα θα πρέπει να κλειδώνουν και πρόσβαση να έχουν μόνο εξουσιοδοτημένα άτομα.

ΔΙΑΤΗΡΗΣΗ ΕΓΓΡΑΦΩΝ Έγγραφα που δεν είναι απαραίτητα για την συγκεκριμένη φάση επεξεργασίας ή που έχει ολοκληρωθεί η επεξεργασία τους	Το λογιστικό γραφείο μπορεί να έχει στην κατοχή του έγγραφα που δεν είναι απαραίτητα για την συγκεκριμένη φάση επεξεργασίας ή που έχει ολοκληρωθεί η επεξεργασία τους και δεν έχουν επιστραφεί στον πελάτη ή τα διατηρεί βάσει της συνεχιζόμενης συνεργασίας μεταξύ των δυο μερών. (Όπως παραπάνω) Τα φυσικά αυτά έγγραφα μπορεί να περιέχουν δεδομένα προσωπικού χαρακτήρα, τα οποία μπορεί κάποιος να τα δει / φωτογραφήσει / κλέψει ή αλλοιώσει. **Ο κίνδυνος είναι ανάλογος των δεδομένων προσωπικού χαρακτήρα που περιλαμβάνονται.** Επιστροφή εγγράφων στον πελάτη (ιδιώτης ή επιχείρηση) Καλό είναι να μην διατηρείτε έγγραφα που δεν είναι απαραίτητα για να εκτελέσετε την εργασία που σας έχουν αναθέσει και πέραν την ολοκλήρωση αυτής (*περιορισμός της περιόδου αποθήκευσης*) και να μην δέχεστε δεδομένα πέρα αυτών που είναι απαραίτητα για την ολοκλήρωση της εργασίας σας (*ελαχιστοποίηση των δεδομένων*). Σε περίπτωση που κάποια έγγραφα **πρέπει** να διατηρηθούν από τον ιδιώτη ή επιχείρηση – πελάτη, ενημερώστε τους για το **διάστημα** για το οποίο θα πρέπει με δική τους ευθύνη να διατηρηθούν βάσει σχετικής νομοθεσίας και επιστρέψτε τα. Αν χρειαστεί να διατηρήσετε τα πρωτότυπα ή αντίγραφα έγγραφα στο λογιστικό σας γραφείο θα πρέπει αυτό να γίνει κατ' εντολή του πελάτη (και ως απόρροια της συνεχιζόμενης συνεργασίας) και να έχετε προβλέψει επιπλέον μέτρα ασφαλείας/προστασίας βάσει της επικινδυνότητας τους.
ΚΑΤΑΣΤΡΟΦΗ ΕΓΓΡΑΦΩΝ	Διάφορα έγγραφα που καταλήγουν στα απορρήματα ενδέχεται να περιέχουν από ονοματεπώνυμο ή διεύθυνση του υποκειμένου των δεδομένων μέχρι και κωδικούς πρόσβασης. Η επικινδυνότητα είναι ανάλογη των δεδομένων που περιέχονται και της ευκολίας ανάκτησης των πληροφοριών από τα έγγραφα αυτά. Θα πρέπει να θεωρείται αυτονόητο ότι φυσικά έγγραφα από χαρτιά μέχρι χαρτάκια post-it που περιέχουν κωδικούς πρόσβασης ή άλλα αντίστοιχα δεδομένα υψηλής επικινδυνότητας **πρέπει να καταστρέφονται ολοσχερώς**. **Δώστε προσοχή στην διαδικασία καταστροφής των εγγράφων** ή σκίζοντας τις σελίδες σε μικρά κομμάτια με το χέρι ή καλύτερα χρησιμοποιώντας καταστροφείς εγγράφων ιδανικά τύπο κοπής cross cut (τρίμμα) και όχι λωρίδες, έτσι ώστε να είναι όσο το δυνατόν δυσκολότερη η ανάκτηση πληροφοριών από αυτά.

Ανάλυση: Αποστολή αρχείων πελατών σε έντυπη μορφή

Αποστολή αρχείων πελατών σε έντυπη μορφή **ή** **παραλαβή των αρχείων αυτών**	Δεν είναι σπάνιο για έναν πελάτη να ζητήσει από το λογιστικό γραφείο να τυπώσει ένα εκκαθαριστικό ή μια βεβαίωση ή μια ταυτότητα οφειλής και να τα στείλει ταχυδρομικώς ή να έρθει να τα παραλάβει ο πελάτης ή κάποιος τρίτος εκ μέρους του πελάτη από το λογιστικό γραφείο. Ο κίνδυνος είναι ανάλογος των δεδομένων προσωπικού χαρακτήρα που περιλαμβάνονται στα εν λόγω έγγραφα που δίνονται ή αποστέλλονται. Καλό είναι η αποστολή τέτοιων εγγράφων να γίνεται κυρίως κατόπιν εντολής του πελάτη και με τρόπο που θα εξασφαλίζει ότι θα τα παραλάβει ή ο ίδιος ή ένα άτομο το οποίο έχει επιλέξει αυτός. Το ίδιο και στην περίπτωση της παραλαβής από το λογιστικό γραφείο, όπου θα πρέπει το λογιστικό γραφείο ή να τα δώσει μόνο στον τον πελάτη ή κατ' εντολή του πελάτη σε κάποιο τρίτο άτομο. Εφ' όσον είναι εφικτό, προτιμητέο είναι στην περίπτωση που παραλαβμάνει τα έγγραφα κάποιος τρίτος να υπάρχει κάπου το αίτημα του ίδιου του πελάτη το οποίο αποδικνύει την εντολή αυτή, όπως για παράδειγμα ένα γραπτό μήνυμα (sms ή email) ή ακόμα και μια εξουσιοδότηση **και να ελέγχεται η ταυτότητα του παραλήπτη.** Ένα επιπλέον βήμα θα ήταν η ύπαρξη κάποιου είδους πρωτοκόλλου για την παράδοση τέτοιων εγγράφων σε τρίτους στο οποίο να αναφέρεται η εντολή του υποκειμένου των δεδομένων, το όνομα και η υπογραφή του παραλήπτη, και ίσως και το περιεχόμενο των εγγράφων. *Παρόμοια είναι και η αποστολή ψηφιακών ή ψηφιοποιημένων εγγράφων με ηλεκτρονικά μέσα η οποία αναλύεται παρακάτω.*

Γενικά, θα πρέπει να σκεφτείτε την προστασία των εγγράφων που έχετε σε φυσική μορφή

<u>Από άτομα:</u>

- που μπορεί να βρίσκονται στον χώρο σας με δική σας άδεια (υπάλληλοι)
- τρίτους που μπορεί να βρίσκονται στον χώρο σας (π.χ. κοινό ή συνεργείο καθαρισμού κλπ.)
- που μπορεί να παραβιάσουν την πρόσβαση

<u>και από ενέργειες όπως:</u>

- Καταστροφές (π.χ. πλημμύρα, φωτιά, κλπ.)
- Κλοπές ή εκούσιες καταστροφές (είτε την ώρα που το λογιστικό γραφείο είναι ανοιχτό είτε όταν είναι κλειστό)

και πάντα σε συσχετισμό με τον βαθμό επικινδυνότητας τους να λαμβάνετε περισσότερα/ασφαλέστερα μέτρα προστασίας τους.

Προστασία δεδομένων σε ψηφιακή μορφή

Με την εξέλιξη της τεχνολογίας, τα έγγραφα σε έντυπη μορφή σιγά σιγά εξαλείφονται, όμως η παραβίαση των ψηφιακών αρχείων είναι ακόμα πιο επικίνδυνη και ως προς την ομαλή ροή της επεξεργασίας καθώς και την προστασία των δεδομένων προσωπικού χαρακτήρα που βρίσκονται σε αυτά, πόσο μάλλον όταν μια ψηφιακή κλοπή είναι δυσκολότερο να εντοπιστεί χωρίς ειδικό λογισμικό, λόγω του ότι μπορεί να αντιγραφεί το αρχείο χωρίς να επηρεαστεί το πρωτότυπο του λογιστικού γραφείου. Ακόμα υπάρχει περίπτωση να καταστραφούν ή να καταστούν μη προσπελάσιμα αρχεία από κάποιο ελάττωμα στον σκληρό δίσκο του υπολογιστή ή προσβολή από ιό ή κάποιο άλλο κακόβουλο πρόγραμμα.

Χρειάζεται, αν δεν υφίσταται ήδη, **η δημιουργία μιας κουλτούρας προστασίας δεδομένων** έτσι ώστε μαζί με την εξοικείωση των υπαλλήλων / χρηστών των υπολογιστών του γραφείου με τους υπολογιστές και τα διάφορα προγράμματα που χρησιμοποιούν καθημερινά να είναι σε θέση να αναγνωρίσουν πιθανούς κινδύνους που μπορούν να προκύψουν από την χρήση του κάθε προγράμματος (π.χ. περιήγησης internet, λογιστικής διαχείρισης) ή της κάθε διαδικασίας (π.χ. μη εξουσιοδοτημένη πρόσβαση στους υπολογιστές ή τα αρχεία σε κάποιο αντίγραφο ασφαλείας) και ακόμα και να προτείνουν διορθώσεις ή και νέες διαδικασίες που θα προσφέρουν καλύτερα επίπεδα ασφάλειας.

Ανάλυση: Πρόσβαση στους υπολογιστές (τοπικά και απομακρυσμένα) και το τοπικό δίκτυο

Θέμα	Ανάλυση - Κίνδυνοι - Ενέργειες
Πρόσβαση στους υπολογιστές που βρίσκονται στο γραφείο	Τα λογιστικά γραφεία είναι συνήθως ανοιχτά προς το κοινό και μέσα μπορεί να εισέρχεται οποιοσδήποτε κάνει μια συναλλαγή με κάποιο από τα άτομα του λογιστικού γραφείου. Στην οθόνη του υπολογιστή μπορεί να βρίσκονται ανοιχτά διάφορα παράθυρα που μπορεί να περιέχουν δεδομένα προσωπικού χαρακτήρα. Ενδεικτικά αν δεν υπάρχει επίβλεψη του υπολογιστή, ένα μη εξουσιοδοτημένο άτομο μπορεί να διαβάσει αυτό που φαίνεται στην οθόνη εκείνη την στιγμή ή και σε πιο απίθανα και ακραία σενάρια να έχει πρόσβαση στα ανοιχτά παράθυρα, εφαρμογές, και αρχεία και να προβεί ακόμα και σε ανάγνωση, κλοπή, τροποποίηση ή και καταστροφή των αρχείων αυτών που μπορεί να περιέχουν ή όχι δεδομένα προσωπικού χαρακτήρα. Ο κίνδυνος είναι ανάλογος των δεδομένων προσωπικού χαρακτήρα στα οποία μπορεί να υπάρξει πρόσβαση. **Η πρόσβαση στον κάθε υπολογιστή του γραφείου θα πρέπει να γίνεται μόνο με την χρήση προσωπικού κωδικού χρήστη.** Επίσης, όταν κάποιος σηκώνεται από την θέση του θα πρέπει να «κλειδώνει» τον χρήστη. Για κάποιον που χρησιμοποιεί τον υπολογιστή και δεν βρίσκεται εκεί, κλειδώνοντας τον υπολογιστή εξασφαλίζεται ότι δεν φαίνεται στην οθόνη κάτι πέρα από την εικόνα κλειδώματος και λειτουργεί ως ένα στοιχειώδες μέτρο προστασίας για κάποιον που δεν έχει τον κωδικό πρόσβασης. Το κλείδωμα του χρήστη του υπολογιστή μπορεί να γίνει άμεσα και πολύ απλά πατώντας τον συνδυασμό πλήκτρων **Windows + L** στο πληκτρολόγιο. Η οθόνη δεν θα δείχνει τα ανοιχτά προγράμματα και μετά απλά με την εισαγωγή του κωδικού μπορεί ο χρήστης να συνεχίσει την δουλειά του από εκεί που ήταν.

Remote Control / Desktop Sharing Απομακρυσμένη σύνδεση, πρόσβαση, υποστήριξη / διαμοιρασμός επιφάνειας εργασίας	Απομακρυσμένη σύνδεση στον υπολογιστή είναι συνήθως το πρώτο βήμα για άμεση υποστήριξη του συγκεκριμένου συστήματος από τεχνικούς χρησιμοποιώντας προγράμματα όπως το TeamViewer, AnyDesk, Ammyy Admin, κ.α. Επίσης αρκετοί επαγγελματίες/εργαζόμενοι χρησιμοποιούν την απομακρυσμένη σύνδεση για να συνδεθούν από κάποιον διαφορετικό χώρο και υπολογιστή στον υπολογιστή της εργασίας, όπου συνήθως έχουν και όλα τα αρχεία που χρειάζονται. **Τέτοια προγράμματα δίνουν εξ αποστάσεως την ίδια σχεδόν πρόσβαση που θα είχε ο απομακρυσμένος χρήστης αν βρισκόταν μπροστά σον υπολογιστή που συνδέεται.** Αυτό σημαίνει ότι μπορεί να έχει πρόσβαση σε όποιο αρχείο βρίσκεται στον υπολογιστή καθώς και στους άλλους υπολογιστές, εκτυπωτές, σέρβερς, μέσα αποθήκευσης που βρίσκονται στο δικτύου του υπολογιστή και επίσης: μπορεί να διαβάσει, τροποποιήσει, αντιγράψει, διαγράψει αρχεία και να έχει πρόσβαση σε όλα τα προγράμματα του υπολογιστή όπου ειδικά σε αρκετές περιπτώσεις (π.χ. προγράμματα λογιστικής διαχείρισης ή διαχείρισης ανθρώπινου δυναμικού ή πλοήγησης στο internet ή email) ενδέχεται να μην έχουν κωδικό πρόσβασης τα ίδια και περιέχουν και δεδομένα προσωπικού χαρακτήρα. **Είναι σημαντικό να τονιστεί και να κατανοηθεί ότι μια τέτοια μη εξουσιοδοτημένη πρόσβαση θα ήταν ΕΞΑΙΡΕΤΙΚΑ ΕΠΙΚΙΝΔΥΝΗ και ΑΠΑΙΤΕΙΤΑΙ να υπάρχουν μέτρα ασφαλείας όταν χρησιμοποιούνται τέτοια προγράμματα.** Αρχικά και εφ'όσον δεν απαιτείται να είναι μόνιμα σε αναμονή, μπορείτε να μην επιτρέψετε στα προγράμματα να ξεκινάνε από μόνα τους κατά την εκκίνηση του υπολογιστή και να φροντίζετε **να μην** παραμένουν ανοιχτά αν δεν είναι απαραίτητη η λειτουργία τους. Να γνωρίζετε ότι συνήθως **ο κωδικός πρόσβασης που δημιουργείται αυτόματα από κάποια προγράμματα ΕΝΔΕΧΕΤΑΙ ΝΑ ΜΗΝ ΑΝΑΝΕΩΝΕΤΑΙ μετά την λήξη της κάθε συνεδρίας**, παρά μόνο μετά από επανεκκίνηση του συστήματος. Αυτό σημαίνει ότι αν κάποιος έχει συνδεθεί στον υπολογιστή και μετά ο υπολογιστής μείνει ανοιχτός, ανεπιτήρητος και με ένα τέτοιο πρόγραμμα ανοιχτό, μπορεί ΜΕ ΤΟΝ ΙΔΙΟ ΚΩΔΙΚΟ να συνδεθεί ξανά. Αν είναι υποχρεωτικό για την εργασία σας να χρησιμοποιείτε τέτοια προγράμματα μπορείτε να περιορίσετε την δυνατότητα πρόσβασης στον υπολογιστή να γίνεται μόνο από συγκεκριμένους χρήστες (whitelist) μέσω των ρυθμίσεων της κάθε εφαρμογής, έτσι ακόμα και αν κάποιος έχει τον κωδικό αν δεν είναι στην λίστα των εγκεκριμένων χρηστών δεν μπορεί να συνδεθεί. Αν χρειαστεί να συνδεθεί τρίτος χρήστης μπορείτε να απενεργοποιήσετε την λειτουργία αυτή προσωρινά.

Πρόσβαση στο δίκτυο της επιχείρησης (Wi-Fi ή ενσύρματα)	Όλο και περισσότερος κόσμος χρησιμοποιεί πλέον smartphone και άλλες έξυπνες φορητές συσκευές και για ένα μέγαλο εύρος λειτουργιών τους απαιτείται σύνδεση στο internet, όπου συνήθως γίνεται μέσω ασύρματων δικτύων (Wi-Fi) για ευκολία και εξοικονόμηση χρημάτων των χρηστών. Ενώ τα Wi-Fi είναι συνήθως κλειδωμένα με κωδικό πρόσβασης, από την άλλη, η ενσύρματη σύνδεση (με καλώδιο δικτύου) δεν απαιτεί κανένα κωδικό! Όποιος συνδέεται στο δίκτυο σας είτε μέσω Wi-Fi είτε μέσω καλωδίου δικτύου ενδέχεται να έχει πρόσβαση στις υπόλοιπες συνδεδεμένες συσκευές, όπως τους υπολογιστές του γραφείου, τους εκτυπωτές, κλπ. Είναι ένας παράγοντας που σε ένα ακραίο σενάριο (π.χ. ο υπολογιστής που συνδέθηκε να έχει κάποιον ιό ή άλλο κακόβουλο λογισμικό) ίσως μπορεί να προκαλέσει ζημιά στους άλλους υπολογιστές ή ακόμα και να διαβάσει δεδομένα που περνάνε από το δίκτυο. Αποφεύγετε να αφήνετε να συνδέονται ενσύρματα ή ασύρματα στο δίκτυο σας συσκευές που δεν έχουν λόγο να συνδεθούν. Επίσης αποφύγετε να δίνετε τον κωδικό του Wi-Fi σας στο κοινό. Αν θέλετε να παρέχετε την δυνατότητα ασύρματης σύνδεσης στο internet για να έχετε την μέγιστη δυνατή προφύλαξη, χρησιμοποιήστε ένα ασύρματο router που να έχει την **λειτουργία guest mode** όπου μπορείτε να δημιουργήσετε ένα ξεχωριστό ασύρματο δίκτυο με άλλο όνομα και κωδικό το οποίο δίνει πρόσβαση μόνο προς το internet και όχι στις υπόλοιπες συσκευές του δικτύου. Τέτοια συσκευή δεν είναι απαραίτητο να είναι DSL modem αλλά μόνο WiFi router (και κατ'επέξταση είναι φθηνότερο) και μπορεί να λειτουργήσει συμπληρωματικά με το modem/router που ήδη μπορεί να έχετε μέσω του παρόχου τηλεπικοινωνιακών υπηρεσιών σας.
Εξωτερικά μέσα αποθήκευσης (μνήμη USB – στικάκια, εξωτερικοί δίσκοι, κλπ) προσωπικής χρήσης υπαλλήλων ή τρίτων στον υπολογιστή του γραφείου	Αν και η χρήση εξωτερικών μέσων αποθήκευσης φθίνει για τις απλές διαβιβάσεις δεδομένων και έναντι αυτής χρησιμοποιείται κατά κύριο λόγο η αποστολή μέσω email, ενδέχεται κάποιος πελάτης ή και υπάλληλος να χρησιμοποιήσει κάποιο εξωτερικό μέσο αποθήκευσης, όπως μνήμη USB (στικάκι), έναν εξωτερικό σκληρό δίσκο, μια κάρτα μνήμης, κλπ. για την μεταφορά αρχείων προσωπικών ή της επιχείρισης ή κάποιου πελάτη της επιχείρισης, για επαγγελματική ή και για προσωπική χρήση. Η χρήση εξωτερικών μέσων αποθήκευσης τα οποία χρησιμοποιούνται και για προσωπική χρήση ενέχουν μεγαλύτερο κίνδυνο προσβολής των υπολογιστών του γραφείου από ιούς, πόσο μάλλον όταν δεν επιβλέπεται η χρήση τους σε υπολογιστές εκτός του λογιστικού γραφείου. Ένας επιπλέον μεγάλος κίνδυνος είναι αν ένα τέτοιο μέσο που χρησιμοποιείται και για επαγγελματική χρήση χαθεί ή κλαπεί. Ο κίνδυνος είναι ανάλογος των δεδομένων που περιέχονται μέσα στην συσκευή αυτή και σε μερικές περιπτώσεις, ακόμα και αυτών που έχουν διαγραφεί. Προτιμήστε για μεταφορές εντός του επαγγελματικού χώρου να χρησιμοποιείτε το τοπικό δίκτυο και όχι ενδιάμεσα μέσα αποθήκευσης. Μπορείτε να ορίσετε στους **υπολογιστές κοινόχρηστους φάκελους με κωδικό πρόσβασης** έτσι ώστε ακόμα και κάποιος να έχει πρόσβαση στο τοπικό δίκτυο να μην μπορεί να συνδεθεί. *Για θέματα backup με χρήση εξωτερικών μέσων αποθήκευσης, αποστολής αρχείων με email, δείτε παρακάτω*

Ανάλυση: Ασφάλεια στο internet (phishing, ασφαλής σύνδεση, κωδικοί, ιστορικό, προσωπική χρήση)

Θέμα	Ανάλυση - Κίνδυνοι - Ενέργειες
Γνώση βασικής αυτο-προστασίας στην πλοήγηση στο internet. **PHISHING** («ηλεκτρονικό ψάρεμα») **ΑΣΦΑΛΗΣ ΣΥΝΔΕΣΗ** (κρυπτογραφημένη σύνδεση σε σελίδες) **ΚΩΔΙΚΟΙ ΠΡΟΣΒΑΣΗΣ** & κωδικοί πρόσθετης ασφάλειας ή κωδικοί μίας χρήσης ή έλεγχος ταυτότητας δύο παραγόντων (two-factor authentication)	Δεν είναι όλα τα email που έρχονται ασφαλή, είτε περιέχουν επισυναπτόμενα αρχεία είτε όχι. Ούτε τα προγράμματα που τα λαμβάνουν μπορούν πάντα με σιγουριά να διαχωρίσουν αν είναι ασφαλή ή όχι. Μπορεί το επισυναπτόμενο αρχείο να φαίνεται αθώο αλλά να περιέχει ιό ή το email που ήρθε από την τράπεζα ή από την εταιρία που μου παρέχει email για να μπω να αλλάξω κωδικό να φαίνεται αυθεντικό αλλά ο σύνδεσμος να οδηγεί σε τελείως διαφορετική σελίδα που είναι ακριβές αντίγραφο της κανονικής. Η αποστολή email «ηλεκτρονικού ψαρέματος» (phishing) είναι κάτι που συμβαίνει συχνά και απαιτεί ιδιαίτερη προσοχή γιατί οι **κίνδυνοι που περιλαμβάνονται είναι υψηλοί**, από την κλοπή ενός κωδικού λογαριασμού email ή τράπεζας ή διαδικτυακού χώρου αποθήκευσης/backup, υπάρχει περίπτωση πέρα την άμεσης οικονομικής ζημιάς να γίνει και υποκλοπή αρχείων που μπορεί να περιλαμβάνουν δεδομένων προσωπικού χαρακτήρα δικών σας ή υπαλλήλων σας ή πελατών σας με επιπλέον κίνδυνο την κλοπή ταυτότητας ή την απάτη κάποιου άλλου ατόμου με τα στοιχεία αυτά. Να έχετε υπόψη σας ότι η μορφή μιας σελίδα στο internet μπορεί να αντιγραφεί σχετικά εύκολα και η ψεύτικη που έχει στόχο να «ψαρέψει» τα στοιχεία σας να φαίνεται ακριβώς όπως η πραγματική που θα σας προτρέπει να βάλετε το όνομα χρήση και τον κωδικό πρόσβασής σας και η μόνη διαφορά να είναι η διεύθυνση της. Δεν είναι απαραίτητο κάποιος να μας «ψαρέψει» μόνο μέσω email. Το ίδιο μπορεί να γίνει με την αποστολή ενός συνδέσμου μέσω SMS ή/και υπηρεσιών ηλεκτρονικών μηνυμάτων, όπως skype, messenger, viber, whatsapp, telegram, κλπ που ο αποστολέας μπορεί να είναι ένα γνωστό μας πρόσωπο του οποίου ο λογαριασμός μπορεί να έχει παραβιαστεί. Κάτι βασικό που μπορείτε να κάνετε για να αποφύγετε κάτι τέτοιο είναι να δείτε στην γραμμή διεύθυνσης αν η διεύθυνση είναι η σωστή. Αρκετά προγράμματα πλοήγησης internet και antivirus ενδέχεται να μπορούν να σας προστατέψουν όταν επισκέπτεστε τέτοιες σελίδες βγάζοντας ένα προειδοποιητικό μήνυμα, αλλά αυτό δεν ισχύει πάντα. Ωστόσο το καλύτερο είναι όταν θέλετε να πλοηγηθείτε σε μια ιστοσελίδα που πρόκειται να συνδεθείτε (π.χ. τράπεζας ή taxisnet ή email ή σελίδα κοινωνικής δικτύωσης) να αποφύγετε να χρησιμοποιείτε συνδέσμους που έχετε λάβει με email ή με κάποιο μήνυμα ή χρησιμοποιώντας μια μηχανή αναζήτησης και **να προτιμάτε να γράφετε την διεύθυνση της σελίδας μόνοι σας και να σιγουρευτείτε ότι η σύνδεση σας είναι ασφαλής (κρυπτογραφημένη)**, βλέποντας στην γραμμή διεύθυνσης το λουκέτο (συνήθως πράσινο για ασφαλή σύνδεση ή κόκκινο για μη ασφαλή), την ένδειξη ασφαλές (κυρίως στον chrome) και s (secure) στο https:// πριν την διεύθυνση, όπως ενδεικτικά στον chrome:  Σε ότι αφορά την διαδικασία πρόσβασης, οι περισσότερες υπηρεσίες (email, τράπεζες, μέσα κοινωνικής δικτύωσης, κλπ) **υποστηρίζουν την δυνατότητα σύνδεσης με έλεγχος ταυτότητας δύο παραγόντων (two-factor authentication)**. Αυτό απαιτεί την χρήση του κωδικού πρόσβασης μαζί με έναν τυχαίο κωδικό που μπορεί να προέρχεται από μια συσκευή ή εφαρμογή (συνήθως κινητού) δημιουργίας κωδικών μιας χρήσης ή την αποστολή ενός SMS ή email. Σε αυτή την περίπτωση ακόμα και αν κλαπεί ο κωδικός σας, θα μπορείτε να προστατευτείτε έως έναν βαθμό από αυτό το επιπλέον βήμα προστασίας.

Διατήρηση δεδομένων από την χρήση προγραμμάτων πλοήγησης internet (browsers). **Ιστορικό πλοήγησης** **Κωδικοί πρόσβασης** **Δεδομένα φόρμας αυτόματης συμπλήρωσης**	Κάθε πρόγραμμα πλοήγησης αν δεν ρυθμιστεί διαφορετικά, μπορεί να διατηρεί δεδομένα περιήγησης όπως: ιστορικό περιήγησης, ιστορικό λήψεων, cookies, κωδικούς πρόσβασης, δεδομένα φόρμας αυτόματης συμπλήρωσης, κλπ. Τα παραπάνω δεδομένα μπορεί να περιέχουν κωδικούς λογαριασμών του χρήστη/υπάλληλου ή πελατών ή/και άλλα δεδομένα προσωπικού χαρακτήρα και η αποθήκευση ή διατήρηση των κωδικών/δεδομένων αυτών μπορεί να προκαλέσει σημαντικό κίνδυνο σε περίπτωση διαρροής *(κάτι το οποίο είναι σχετικά εύκολο για κάποιο άτομο που μπορεί να έχει πρόσβαση στον υπολογιστή, απλά βλέποντας το ιστορικό του προγράμματος περιήγησης ή και τους αποθηκευμένους κωδικούς).* Για λόγους προστασίας δεδομένων προσωπικού χαρακτήρα και του προσωπικού απόρρητου των υπαλλήλων που χρησιμοποιούν τους υπολογιστές καθώς και των πελατών καλό είναι **να μην διατηρείται ιστορικό πλοήγησης στα προγράμματα πλοήγησης internet, ούτε δεδομένα φόρμας αυτόματης συμπλήρωσης** και να προβείτε σε διαγραφή των ήδη αποθηκευμένων στοιχείων. Σε ότι αφορά τους κωδικούς πρόσβασης θα πρέπει ιδανικά να απενεργοποιηθεί πλήρως η επιλογή της αποθήκευσης των κωδικών πρόσβασης και να διαγραφούν όλοι οι κωδικοί πρόσβασης που έχουν αποθηκευτεί ήδη για λόγους ασφάλειας και προστασίας. Ενδεικτικά, μπορείτε να βρείτε τις σχετικές διαδικασίες για τον Firefox και τον Chrome: • **Διαχείριση αποθηκευμένων κωδικών πρόσβασης**: Firefox και Chrome • **Διαχείριση ιστορικού περιήγησης**: Firefox και Chrome • **Απόρρητη ή Ιδιωτική περιήγηση** (δηλαδή περιήγηση χωρίς να διατηρούνται τα δεδομένα αυτής, φόρμες, κωδικοί, cookies, ενεργές συνδέσεις, κλπ) Firefox (Ctrl + P) και Chrome (Ctrl + N)
Χρήση του υπολογιστή για προσωπική πλοήγηση στο internet	Οι υπολογιστές του γραφείου ενδέχεται να χρησιμοποιούνται και για προσωπική πλοήγηση, όπως π.χ. πλοήγηση σε ενημερωτικές ιστοσελίδες ή για σύνδεση σε προσωπικό ηλεκτρονικό ταχυδρομείο (email) ή σε μέσα κοινωνικής δικτύωσης, κλπ. Η εκτενής χρήση του υπολογιστή του γραφείου για προσωπική πλοήγηση ενδέχεται να αυξήσει τον κίνδυνο προσβολής του υπολογιστή από ιό ή κάποιο άλλο κακόβουλο πρόγραμμα και κατ' επέκταση και των υπολογιστών που βρίσκονται στο ίδιο δίκτυο (δηλαδή των υπόλοιπων υπολογιστών του γραφείου), ειδικά αν η πλοήγηση οδηγεί έστω (και κατά λάθος ή μέσω phishing) σε επικίνδυνες ιστοσελίδες. Αρχικά θα πρέπει να ορίσετε το τι πρέπει ή τι δεν πρέπει να κάνει κάποιος που έχει πρόσβαση στους υπολογιστές αυτούς σε σχέση με προσωπική πλοήγηση. Ιδανικά η χρήση του υπολογιστή εργασίας για προσωπική πλοήγηση θα πρέπει να αποφεύγεται όσο είναι δυνατόν και εναλλακτικά να χρησιμοποιούνται άλλα μέσα όπως το προσωπικό κινητό το οποίο θα συνδέεται σε απομονωμένο δίκτυο για επισκέπτες (όπου είναι εφικτό, *για περισσότερες πληροφορίες δείτε το τμήμα που αναφέρεται στη πρόσβαση στο δίκτυο της επιχείρησης*). Αν αυτό δεν μπορεί να αποφευχθεί τότε θα πρέπει να ορίσετε κάποια μέτρα ασφαλείας και προστασίας. Ίσως με χρήση firewall για να επιτρέπεται πρόσβαση μόνο σε συγκεκριμένους ιστότοπους, χρήση ανώνυμης περιήγησης έτσι ώστε να διαγράφονται αυτόματα από το ιστορικό όποια δεδομένα πλοήγησης, να μην γίνεται λήψη προσωπικών ή άλλων αρχείων που δεν έχουν σχέση με την εργασία, κλπ.)

Ανάλυση: Λειτουργικό σύστημα, ενημερώσεις & πειρατικό λογισμικό

Θέμα	Ανάλυση - Κίνδυνοι - Ενέργειες
Οι υπολογιστές χρησιμοποιούν **Windows XP** ή και παλαιότερο λειτουργικό σύστημα	Δυστυχώς τα Windows XP και άλλα παλαιότερα λειτουργικά συστήματα έχουν σταματήσει να υποστηρίζονται από την Microsoft και από τις περισσότερες εταιρίες που φτιάχνουν προγράμματα για υπολογιστές. Λόγω της παλαιότητας τους δεν είναι πλήρως συμβατά με τις νεότερες μεθόδους ασφάλειας και κρυπτογράφησης συνδέσεων μέσω internet και λόγω του ότι δεν λαμβάνουν ενημερώσεις ασφαλείας είναι αρκετά πιο επιρρεπή σε προσβολή από ιούς, κακόβουλες ενέργειες και άλλα κενά ασφαλείας. Η μόνη λύση είναι να αναβαθμίζονται όπου είναι εφικτό οι υπολογιστές σε νεότερες εκδόσεις των Windows **και ιδανικά στην τελευταία** (Windows 10), διότι ακόμα και παλαιότερες εκδόσεις (όπως για παράδειγμα τα Windows Vista, 7 και 8 θα σταματήσουν να υποστηρίζονται στο προσεχές μέλλον)
Το λειτουργικό σύστημα στον υπολογιστή εμφανίζει το μήνυμα ότι «δεν έχει γίνει η ενεργοποίηση» του ή ενδέχεται το λογισμικό ή κάποια προγράμματα που χρησιμοποιώ να είναι «**πειρατικά**» ή «**σπασμένα**» ΕΝΗΜΕΡΩΣΕΙΣ ΛΟΓΙΣΜΙΚΟΥ / ΠΡΟΓΡΑΜΜΑΤΩΝ	Το να μην έχει γίνει ενεργοποίηση των windows μπορεί να μην επιβαρύνει αρνητικά την λειτουργία τους, ωστόσο ενδέχεται να μην είναι δυνατή η χρήση του υπολογιστή μετά την λήξη της δοκιμαστικής περιόδου. **«Πειρατικό» λογισμικό ή «σπασμένα» προγράμματα μπορεί έχουν αρνητικές επιπτώσεις σε θέματα ομαλής, ασφαλούς και νόμιμης λειτουργίας.** Μην χρησιμοποιείτε «σπασμένα» λογισμικά και προγράμματα, γιατί υπάρχει πιθανότητα κατά την διαδικασία του «σπασίματος» να προστέθηκε κακόβουλος κώδικας ή να δημιουργήθηκε μια «πίσω πόρτα» (backdoor) και να έχει ως αποτέλεσμα την ευκολότερη προσβολή του υπολογιστή σας από ιό ή κάποιο άλλο κακόβουλο πρόγραμμα ή άλλες απειλές που μπορεί να μην μπορούν να εμποδιστούν ακόμα και από λογισμικό προστασίας οι οποίες μπορούν να προσβάλουν και τους υπόλοιπους υπολογιστές που βρίσκονται στο ίδιο δίκτυο. Χρησιμοποιώντας αυθεντικά και όχι «σπασμένα» λογισμικά και προγράμματα, στις περισσότερες περιπτώσεις έχετε πρόσβαση στις τελευταίες ενημερώσεις που μπορεί να περιέχουν ενημερώσεις ασφαλείας που είναι πολύ χρήσιμες για την ενίσχυση της ασφάλειας του υπολογιστή. Αν θεωρείτε ότι κάτι μπορεί να είναι ακριβό ή δεν θέλετε να πληρώσετε ακριβά για κάτι, **ενδέχεται να** υπάρχει δωρεάν ή/και ανοιχτής πηγής (open-source) λογισμικό για εμπορική χρήση που μπορεί να προσεγγίζει σε λειτουργία το λογισμικό. π.χ. στην περίπτωση του office, υπάρχει το OpenOffice και το LibreOffice που προσεγγίζουν σε λειτουργία το Office της Microsoft. **ΠΡΟΣΟΧΗ** Σε κάθε περίπτωση καλό είναι να έχετε μια σχετική εξοικείωση ή σχετική υποστήριξη πριν προβείτε σε οποιαδήποτε αντικατάσταση προγράμματος ή λογισμικού για λόγους ευκολίας/άνεσης χρήσης και συμβατότητας με άλλα προγράμματα και συσκευές που έχετε.

Ανάλυση: Κρυπτογράφηση αρχείων

Σε γενικές γραμμές η κρυπτογράφηση στα δεδομένα μπορεί να γίνει στα εξής βασικά επίπεδα:

- Σε επίπεδο (μεμονωμένου) **αρχείου**

  Η κρυπτογράφηση σε αυτό το επίπεδο είναι πιο εύκολη διότι για μεμονωμένα αρχεία μπορεί να γίνει και μέσω των προγραμμάτων επεξεργασίας που ήδη χρησιμοποιούνται (π.χ. σε αρχεία Word/Excel/Access με χρήση κωδικού πρόσβασης).

  Σε αυτή τη περίπτωση αρχεία αυτά αποκρυπτογραφούνται μόνο κατά την προσπέλαση τους (με την χρήση του κατάλληλου κωδικού) και με το κλείσιμο της εφαρμογής, σε όποιο φυσικό μέσο αποθήκευσης βρίσκονται ή αντιγράφονται ή μεταφέρονται τα αρχεία αυτά παραμένουν κρυπτογραφημένα.

Προσοχή:

Η αναφορά εδώ γίνεται σε **μεμονωμένα** αρχεία, κυρίως έγγραφα, βιβλία εργασίας, παρουσιάσεις, κλπ, όπως για παράδειγμα: αρχεία PDF, Word, Excel, Access, PowerPoint.

Αν τα αρχεία που θέλετε να κρυπτογραφήσετε δεν μπορούν να λειτουργήσουν αυτόνομα, δηλαδή αν είναι μέρος κάποιας βάσης δεδομένων ή απαιτούνται πολλαπλά αρχεία για να λειτουργήσει σωστά μια εφαρμογή, τότε η κρυπτογράφηση σε επίπεδο μεμονωμένου αρχείου εμποδίζει την σωστή λειτουργία της βάσης ή της εφαρμογής και για τον λόγο αυτό πρέπει να γίνει κρυπτογράφηση όλης της βάσης δεδομένων ή όλων των εμπλεκόμενων αρχείων μαζί (π.χ. σε ένα συμπιεσμένο αρχείο).

- Σε επίπεδο **μέσου αποθήκευσης**

  Αναφερόμενοι στο «φυσικό» μέσο στο οποίο είναι αποθηκευμένο το κάθε αρχείο, το οποίο μπορεί να είναι: ο δίσκος ενός υπολογιστή, ένα στικάκι, ένας εξωτερικός δίσκος ή ένας δίσκος ενός κέντρου δεδομένων που προσφέρει χώρο αποθήκευσης στο νέφος, κ.α.

  Σε αυτή τη περίπτωση χρησιμοποιείται ένα πρόγραμμα ή μια συσκευή για να κρυπτογραφηθεί μέρος ή όλο το περιεχόμενο του μέσου αυτού έτσι ώστε να καλύπτονται όλα τα αρχεία μεταξύ των οποίων και τα αρχεία που περιέχουν τα δεδομένα που επιθυμούμε να προστατεύσουμε.

  Για παράδειγμα, για την πρόσβαση σε έναν κρυπτογραφημένο δίσκο υπολογιστή, ο υπολογιστής κάνει αυτόματα την αποκρυπτογράφηση και την επανακρυπτογράφηση κάθε μέρους όπου απαιτείται για την ανάγνωση, αντιγραφή, τροποποίηση, διαγραφή, κλπ. των αρχείων/δεδομένων, έτσι ώστε ο χρήστης ή και οποιοσδήποτε έχει πρόσβαση να μπορεί να εργαστεί στον υπολογιστή όπως ακριβώς αν τα δεδομένα δεν ήταν κρυπτογραφημένα.

  Ωστόσο, η μεταφορά των αρχείων αυτών εκτός του συγκεκριμένου υπολογιστή συνήθως γίνεται χωρίς κρυπτογράφηση. Για παράδειγμα αν στείλει κάποιος ένα συνημμένο αρχείο από τον συγκεκριμένο υπολογιστή με email, το αρχείο αυτό δεν θα είναι κρυπτογραφημένο. Ακόμα αν κάποιος κρατάει αντίγραφα ασφαλείας των δεδομένων του υπολογιστή χρησιμοποιώντας μια υπηρεσία νέφους, παρ' όλο που ο δίσκος του μπορεί να είναι κρυπτογραφημένος, στο νέφος να μην είναι. Το ίδιο ισχύει όταν γίνεται εξαγωγή των δεδομένων από μια βάση δεδομένων, όπου εκτός και αν έχει προβλεφθεί κάποια κρυπτογράφηση, τα αρχεία αυτά θα είναι

  Εξαίρεση είναι αν τα αρχεία είναι κρυπτογραφημένα τα ίδια πριν την μεταφορά τους, όπου θα παραμείνουν κρυπτογραφημένα ακόμα και αν το μέσο αποθήκευσης του προορισμού δεν είναι κρυπτογραφημένο.

Σε κάθε περίπτωση καλό είναι να γνωρίζετε:

- Τι μέτρα ασφάλειας δεδομένων χρησιμοποιείτε (αντίγραφα ασφαλείας, κρυπτογράφηση, κωδικοί πρόσβασης, κλπ.)
- Πρέπει να φροντίζετε για τον περιορισμό πρόσβασης ή και την κρυπτογράφηση των δεδομένων ανάλογα και με την επικινδυνότητα που έχουν προς τα υποκείμενα τους.
- Έχει ιδιαίτερη σημασία το πόσο δυνατός είναι ο κωδικός και ο αλγόριθμος της κρυπτογράφησης για το αν μπορούν αυτά τα αρχεία να αποκρυπτογραφηθούν και από κάποιον τρίτο.

Ανάλυση: Αντίγραφα ασφαλείας και αποθηκευτικός χώρος στο νέφος

Θέμα	Ανάλυση - Κίνδυνοι - Ενέργειες
Αντίγραφα ασφαλείας από τους υπολογιστές με **στικάκι ή εξωτερικό σκληρό δίσκο εντός ή και εκτός γραφείου.** ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΑΡΧΕΙΩΝ	Το να παίρνει κάποιος τακτικά αντίγραφα ασφαλείας από τους υπολογιστές είναι μια κίνηση που από την μια πλευρά είναι σωστή και βοηθάει στην διατήρηση των αρχείων σε περίπτωση καταστροφής (π.χ. αν χαλάσει ο σκληρός δίσκος και χαθούν τα δεδομένα ή σε περίπτωση προσβολής από ιό του υπολογιστή που αλλοιώνει τα αρχεία) ή από φυσικές καταστροφές που μπορεί να προκληθούν στο γραφείο και στου υπολογιστές (π.χ. κεραυνοί, πυρκαγιά, πλημμύρα) ή ακόμα και από κλοπή του υπολογιστή. Από την άλλη όμως δημιουργεί ένα ακόμα «τρωτό σημείο» γιατί τα δεδομένα (ακόμα και αν είναι αντίγραφα ασφαλείας) είναι συσσωρευμένα σε μια φορητή συσκευή που μπορεί εύκολα να καταστραφεί (αν χρησιμοποιείται λανθασμένα ως βάση αντί για **αντίγραφο** ασφαλείας) ή να ξεχαστεί κάπου ή και να κλαπεί. Ο κίνδυνος απώλειας/κλοπής ίσως να είναι χαμηλός αλλά αν συμβεί κάτι τέτοιο **και ειδικά αν τα δεδομένα δεν είναι κρυπτογραφημένα** μπορεί να έχει **πολύ υψηλό κίνδυνο** (αν π.χ. περιέχει βάσεις με στοιχεία πελατών ή και κωδικούς υπηρεσιών πελατών). **Το μόνο που μπορείτε να κάνετε είναι να φροντίσετε η φορητή συσκευή σας να κρυπτογραφείται.** Στην περίπτωση αυτή αν κλαπεί το στικάκι ή ο εξωτερικός δίσκος, θα είναι πρακτικά αδύνατο να μπορεί κάποιος να διαβάσει το περιεχόμενο του και με αυτόν τον τρόπο μειώνεται σημαντικά η πιθανότητα κινδύνου από μια τέτοια απώλεια. Ενδεικτικά για το θέμα της κρυπτογράφησης υπάρχουν επί πληρωμή αλλά και δωρεάν προγράμματα κρυπτογράφησης τόσο για τον υπολογιστή σας εξ' ολοκλήρου όσο και για εξωτερικές συσκευές αποθήκευσης. Υπάρχουν ακόμα έτοιμες λύσεις στο εμπόριο οι οποίες συνδυάζονται με έναν φορητό δίσκο, και χρησιμοποιούν κρυπτογράφηση σε επίπεδο συσκευής (hardware) και όχι λογισμικού (software). Αυτές οι συσκευές είναι θήκες για εξωτερικό δίσκο που μπορεί να έχουν ένα αριθμητικό πληκτρολόγιο για την εισαγωγή του κωδικού ή και αναγνώστη δακτυλικού αποτυπώματος. Ορισμένοι δίσκοι υποστηρίζουν κρυπτογράφηση σε επίπεδο συσκευής ή μπορούν να κρυπτογραφήσουν δεδομένα μέσω των Windows (bitlocker – συνήθως **δεν** εμπεριέχεται στις βασικές εκδόσεις των Windows [3]) χωρίς να χρειαστείτε να αγοράσετε ή να κάνετε εγκατάσταση κάτι επιπρόσθετο. ΠΡΟΣΟΧΗ: καλό είναι όταν προβαίνετε σε μια λύση κρυπτογράφησης για τα κύρια δεδομένα σας να έχετε γνώση της διαδικασίας, και έναν τρόπο αναστροφής της. Αν δεν έχετε καλή γνώση της διαδικασίας, συμβουλευτείτε έναν τεχνικό υπολογιστών ή κάποιο άτομο με αντίστοιχες γνώσεις. Αν δεν υπάρχει τρόπος πρόσβασης των κρυπτογραφημένων αρχείων ή αναστροφή της κρυπτογράφησης τότε τα αρχεία είναι ουσιαστικά «χαμένα». ΣΗΜΑΝΤΙΚΟ: Η κρυπτογράφηση ή γενικά η χρήση κωδικών πρόσβασης, δεν έχουν καμία αποτελεσματικότητα όταν τον κωδικό τον γνωρίζουν αρκετά άτομα ή αναγράφεται δίπλα στον υπολογιστή ή την συσκευή που τον δέχεται. Ένας μοναδικός κωδικός με όσο το δυνατόν περισσότερα και τυχαία στοιχεία μέσα (σε ειδικές περιπτώσεις ακόμα και πάνω από 20 χαρακτήρες με αριθμούς, κεφαλαία γράμματα και σύμβολα) βοηθάει στην καλύτερη ασφάλεια.

[3] *Συγκεκριμένα στα Windows 10 το σύστημα κρυπτογράφησης bitlocker παρέχεται στις εκδόσεις Pro, Enterprise και Education. Κάντε δεξί κλικ στον «υπολογιστή» ή «ο υπολογιστής μου» ή «αυτός ο υπολογιστής» και πατήστε ιδιότητες. Σε αυτό το παράθυρο μπορείτε να δείτε την έκδοση των windows που τρέχετε. (περισσότερες πληροφορίες για bitlocker – Αγγλικά)*

Διαδικτυακά αντίγραφα ασφαλείας ή αποθηκευτικός χώρος στο νέφος (online backup / cloud storage)	Η δυνατότητα δημιουργίας / διατήρησης αντιγράφου ασφαλείας των σημαντικών αρχείων του υπολογιστή στο νέφος είναι από την μία πλευρά εξαιρετικά χρήσιμη και βολική αλλά από την άλλη ελλοχεύει κινδύνους αν δεν χρησιμοποιείται σωστά. Ένας αποθηκευτικός χώρος στο νέφος (cloud storage) ή ένα διαδικτυακό αντίγραφο ασφαλείας (online backup) είναι όσο ασφαλές όσο ο κωδικός ή τα άλλα μέτρα ασφαλείας που το συνοδεύουν[4]. Χρησιμοποιώντας τέτοιες υπηρεσίες, μη εξουσιοδοτημένη πρόσβαση μπορεί να λόγω παραβίασης των μέτρων ασφαλείας (π.χ. κωδικό) του χρήστη (λογιστικού γραφείου) αλλά μπορεί να είναι αποτέλεσμα παραβίασης των μέτρων ασφαλείας της εταιρίας που φιλοξενεί τα δεδομένα σας. Πρέπει η εταιρία που φιλοξενεί τα δεδομένα σας να σας εξασφαλίζει ότι λαμβάνει επαρκή μέτρα για την ασφάλεια των δεδομένων σας από μη εξουσιοδοτημένη πρόσβαση. Πρέπει επίσης να να έχετε κατ' ελάχιστον έναν ισχυρό κωδικό πρόσβασης και επιπλέον μέτρα ασφάλειας (έλεγχο ταυτότητας δύο παραγόντων, κρυπτογράφηση, κλπ.) που μπορεί να σας προσφέρει η εταιρία φιλοξενίας δεδομένων. ΠΡΟΣΟΧΗ: Αρκετές υπηρεσίες μπορεί να προσφέρουν κοινή χρήση των αρχείων στο νέφος με άλλους χρήστες. Πρέπει να είστε προσεχτικοί με την χρήση μιας τέτοιας λειτουργίας, ποιο άτομο έχει πρόσβαση και να είστε σε θέση να αποσύρετε την πρόσβαση από το άτομο αυτό αν χρειαστεί. Ένα επιπλέον μέτρο ασφάλειας είναι η κρυπτογράφηση (ή χρήση κωδικών) των βάσεων δεδομένων σας ή και των πιο ευαίσθητων αρχείων από τον υπολογιστή σας έτσι ώστε να είναι κρυπτογραφημένα πριν γίνουν μέρος του αντιγράφου ασφαλείας σας στο νέφος.

Αναφερόμενοι στους υπολογιστές που βρίσκονται εντός του λογιστικού γραφείου, φροντίστε:

- Για την πρόσβαση στους υπολογιστές μόνο από εσάς ή τους υπαλλήλους σας με κωδικό πρόσβασης στον υπολογιστή.
- Αποφύγετε την χρήση του υπολογιστή για προσωπική πλοήγηση, ειδικά σε άγνωστους ιστότοπους για τον λόγο του ότι μπορεί μια τέτοια χρήση να οδηγήσει (αν δεν γίνεται με προσοχή) σε προσβολή από ιούς ή άλλου είδους απειλές.
- Για λόγους προστασίας καλό είναι να διατηρείται αντίγραφα ασφαλείας των δεδομένων και των βάσεων δεδομένων. Ωστόσο, αν βρίσκονται σε συσκευές οι οποίες μπορούν εύκολα να χαθούν ή κλαπούν (εξωτερικοί δίσκοι ή στικάκια), οι συσκευές αυτές ΠΡΕΠΕΙ να είναι κρυπτογραφημένες.

[4] *Αναφορά σε κρυπτογράφηση μεμονωμένων αρχείων και έλεγχο ταυτότητας δύο παραγόντων (two-factor authentication)*

Ανάλυση: Αποστολή αρχείων μέσω internet

Αποστολή αρχείων με δεδομένα προσωπικού χαρακτήρα μέσω internet	Αρκετοί πελάτες μπορούν να ζητήσουν να γίνει αποστολή ενός εγγράφου στους ίδιους ή σε κάποιο συνεργαζόμενο (με αυτούς) άτομο το οποίο μπορεί να περιέχει δεδομένα προσωπικού χαρακτήρα. Ο κίνδυνος από την αποστολή ενός αρχείου το οποίο περιέχει δεδομένα προσωπικού χαρακτήρα δεν προκύπτει απαραίτητα άμεσα από την ίδια την αποστολή, αλλά από τον κίνδυνο παραβίασης ενός από τους λογαριασμούς πρόσβασης, την κατά λάθος αποστολή σε διαφορετικό λογαριασμό, την πρόσβαση στον λογαριασμό ενός μη εξουσιοδοτημένου ατόμου (π.χ. κοινόχρηστος υπολογιστής) και γενικά καλό είναι να προβλέπονται επιπλέον μέτρα ασφάλειας κυρίως και λόγω έλλειψης ελέγχου μετά την αποστολή. Αν πρέπει να στείλετε ηλεκτρονικά ένα τέτοιο αρχείο, ενημερώστε το υποκείμενο των δεδομένων αυτών για τους ενδεχόμενους κινδύνους που μπορεί να προκύψουν από την πλευρά του παραλήπτη, και εφ' όσον είναι δυνατόν, βάλτε κωδικό ή κρυπτογραφήστε το αρχείο και στείλτε τον κωδικό με κάποιον διαφορετικό τρόπο (π.χ. με SMS ή τηλεφωνικά). Υπάρχουν επί πληρωμή αλλά και δωρεάν προγράμματα κρυπτογράφησης (με χρήση κωδικού) αρχείων PDF ή και συμπιεσμένων αρχείων (zip, 7z, κ.α.). Τα προγράμματα του Microsoft Office (Word, Excel, Access, κλπ) παρέχουν τα ίδια την δυνατότητα κωδικού / κρυπτογράφησης των αντίστοιχων αρχείων. *(δείτε σχετικά με την κρυπτογράφηση)* ΠΡΟΣΟΧΗ: καλό είναι να είστε σε θέση να αποδείξετε την εντολή του πελάτη για μια αποστολή δεδομένων σε τρίτον, ζητώντας να σας στείλει μήνυμα ή email κλπ (από έναν λογαριασμό του που ήδη γνωρίζετε) στο οποίο να περιγράφει τι ζητάει από εσάς και μετά να προβείτε στην αποστολή ή να το στείλετε στον ίδιο τον πελάτη / υποκείμενο των δεδομένων και ο ίδιος να το προωθήσει.

Αποστολή email

Η αποστολή email πρέπει να αφορά μόνο θέματα που έχουν να κάνουν με την συμβατική υποχρέωση μεταξύ του λογιστικού γραφείου και του πελάτη εκτός και αν υπάρχει συγκατάθεση για κάτι παραπάνω (π.χ. για ένα ενημερωτικό newsletter).

Δεν απαιτείται να ζητάτε συγκατάθεση για την χρήση του email ή του τηλεφώνου ενός πελάτη όταν πρόκειται να το χρησιμοποιήσουμε για να ικανοποιήσετε μια δουλειά που μας έχει αναθέσει.

Για παράδειγμα στην περίπτωση που χρειάζεται να στείλουμε σε έναν πελάτη το εκκαθαριστικό της εφορίας του ή κάτι το οποίο συμπεριλαμβάνεται μέσα σε αυτά που έχει ζητήσει να κάνουμε ή κάτι το οποίο μπορεί να έχει το λογιστικό γραφείο και να έχει δικαίωμα διότι είναι δεδομένο προσωπικού χαρακτήρα του πελάτη. Καλό είναι πάντα να γίνεται η αποστολή με τρόπο που θα διασφαλίζεται η ασφάλεια των δεδομένων που διαβιβάζονται και **πάντα σε συσχετισμό με τον βαθμό επικινδυνότητας τους να λαμβάνετε περισσότερα/ασφαλέστερα μέτρα προστασίας τους.**

⚠ Προσοχή:

- Δεν πρέπει να στέλνετε ενημερωτικό, διαφημιστικό, ή αντίστοιχο email, SMS, ηλεκτρονικό μήνυμα (viber, messenger, skype, whatsapp, telegram, κλπ) σε κάποιο φυσικό πρόσωπο, χωρίς να έχετε λάβει σχετική συγκατάθεση.
- Προσέξτε όταν στέλνετε μαζικά email που χρησιμοποιείτε το πεδίο «ΠΡΟΣ» ή «ΚΟΙΝΟΠΟΙΗΣΗ», διότι φαίνονται τα email όλων στην συγκεκριμένη λίστα χρησιμοποιήστε εναλλακτικά για όλους τους παραλήπτες την κρυφή κοινοποίηση. *(Δεν ισχύει στην περίπτωση που θέλετε να στείλετε ένα email όπου θα υπάρχει μια εμφανή κοινοποίηση των στοιχείων των παραληπτών π.χ. με σκοπό την εκκίνηση διαλόγου με όλους τους συμμετέχοντες και οι απαντήσεις του καθενός να απευθύνονται σε όλους τους παραλήπτες)*
- Αποφεύγετε να στέλνετε email με δεδομένα προσωπικού χαρακτήρα σε τρίτους. Βέβαια να γνωρίζετε ότι εφ' όσον έχετε πάρει την εντολή του ατόμου που αφορούν τα δεδομένα μπορείτε να το κάνετε, ωστόσο θα πρέπει με κάποιον τρόπο να είστε σίγουροι για την κίνηση αυτή. Οι προφορικές εντολές είναι αποδεκτές, ωστόσο γραπτές π.χ. με email εντολές είναι καλύτερες και μπορεί να βοηθήσουν στο να αποφευχθεί ένα λάθος να γραφτεί λάθος μια διεύθυνση email με ευθύνη του λογιστικού γραφείου.
- Κρυπτογράφηση αρχείων των email είναι μια καλή πάγια πρακτική για να αποφευχθεί κάποια λάθος πρόσβαση. Η διαδικασία αυτή μπορεί να γίνει πολύ εύκολα και με διάφορους τρόπους ακόμα και με δωρεάν λογισμικό.

👉 Αξίζει να σημειωθεί ότι υπηρεσίες αποθήκευσης στο νέφος (cloud storage) υποστηρίζουν διαμοιρασμό με σύνδεσμο (link) στον οποίο μπορείτε να προσθέσετε και κωδικό πρόσβασης ή χρήστες πρόσβασης. Τα αρχεία αυτά θα είναι διαθέσιμα μέσω του δικού σας χρήστη, στον δικό σας λογαριασμό αποθήκευσης[5] και ανά πάσα στιγμή μπορείτε να αλλάξετε τα δικαιώματα πρόσβασης στο αρχείο αυτό ή και να τα διαγράψετε μετά το πέρας της χρήσης τους. Αυτό αναφέρεται ως εναλλακτική στην αποστολή αρχείων με email ή μέσω ηλεκτρονικών μηνυμάτων κλπ. που είναι δύσκολη έως απίθανος ο έλεγχος και η διαγραφή μετά την αποστολή.

Ενδεικτικά αυτή τη στιγμή:

- *Το Onedrive υποστηρίζει αποστολή συνδέσμων με ημερομηνία λήξης πρόσβασης και κωδικό πρόσβασης.*
- *Το Google Drive υποστηρίζει πρόσβαση με σύνδεσμο, χωρίς την δυνατότητα κωδικού, με περιορισμένη πρόσβαση (μόνο προβολή, όχι εκτύπωση ή αποθήκευση).*
- *Onedrive, το Google Drive και το Dropbox υποστηρίζουν πρόσβαση με χρήση στοιχείων συγκεκριμένου χρήστη και με δικαιώματα ή μόνο προβολής ή και σχολιασμού ή και τροποποίησης.*

[5] Η εταίρα που παρέχει αυτές τις υπηρεσίες θεωρείται Εκτελών την Επεξεργασία για λογαριασμό του χρήστη (Υπεύθυνος Επεξεργασίας). ΠΡΟΣΟΧΗ αν ο φυσικός χώρος αποθήκευσης (server) της εταιρίας που προσφέρει υπηρεσίες cloud storage βρίσκεται εκτός της Ε.Ε. Αρκετές μεγάλες εταιρίες προσφέρουν από προεπιλογή αποθήκευση σε servers /data centers εντός της Ε.Ε.

Παραβίαση δεδομένων

Παραβίαση δεδομένων επέρχεται όταν σημειώνεται συμβάν ασφαλείας σε σχέση με τα δεδομένα για τα οποία ευθύνεται η εταιρεία ή ο οργανισμός σας, το οποίο έχει ως αποτέλεσμα την παραβίαση του απορρήτου, της διαθεσιμότητας ή της ακεραιότητας. Εάν αυτό συμβεί, και είναι πιθανό η παραβίαση να θέτει σε κίνδυνο τα δικαιώματα και τις ελευθερίες φυσικού προσώπου, η εταιρεία ή ο οργανισμός σας πρέπει να **ειδοποιήσει την εποπτική αρχή χωρίς αδικαιολόγητη καθυστέρηση και το αργότερο εντός 72 ωρών αφού αντιληφθεί την παραβίαση**. Εάν η εταιρεία ή ο οργανισμός σας είναι ο εκτελών την επεξεργασία, πρέπει να ενημερώνει τον υπεύθυνο επεξεργασίας δεδομένων για κάθε παραβίαση δεδομένων.

Εάν η παραβίαση δεδομένων θέτει σε **υψηλό κίνδυνο τα φυσικά πρόσωπα που επηρεάζονται**, τότε πρέπει επίσης να ενημερωθεί το καθένα εξ αυτών, εκτός εάν έχουν τεθεί σε εφαρμογή αποτελεσματικά τεχνικά και οργανωτικά μέτρα προστασίας ή άλλα μέτρα που διασφαλίζουν ότι ο κίνδυνος δεν είναι πλέον πιθανό να προκύψει.

Είναι ζωτικής σημασίας να εφαρμόζετε τα κατάλληλα τεχνικά και οργανωτικά μέτρα για την αποφυγή ενδεχόμενων παραβιάσεων δεδομένων.

👉 **Σε γενικές γραμμές είναι δύσκολο έως απίθανο να αντιληφθεί κάποιος μια κλοπή ή αλλοίωση δεδομένων (ειδικά ψηφιακών) αν δεν παρατηρηθεί η διαδικασία αυτή ή το αποτέλεσμα αυτής.** Σε κάθε περίπτωση, οι σωστά υπολογισμένοι κίνδυνοι σε συνδυασμό με την κατάλληλη πρόληψη είναι η καλύτερη πρόληψη.

Γενικά Παραδείγματα

Ο οργανισμός πρέπει να ειδοποιήσει την Αρχή Προστασίας Δεδομένων και τα φυσικά πρόσωπα: *Τα δεδομένα των εργαζομένων μιας κλωστοϋφαντουργίας γνωστοποιήθηκαν. Τα δεδομένα συμπεριλάμβαναν τις προσωπικές διευθύνσεις, τη σύνθεση της οικογένειας, τον μηνιαίο μισθό και τις ιατρικές αξιώσεις κάθε εργαζομένου. Σε αυτήν την περίπτωση, η κλωστοϋφαντουργία πρέπει να ενημερώσει την εποπτική αρχή σχετικά με την παραβίαση. Καθώς δε τα δεδομένα προσωπικού χαρακτήρα περιλαμβάνουν ευαίσθητα δεδομένα, όπως δεδομένα υγείας, η εταιρεία πρέπει επίσης να ειδοποιήσει τους εργαζομένους.*

Ένας υπάλληλος νοσοκομείου αποφασίζει να αντιγράψει στοιχεία ασθενών σε CD και τα δημοσιεύει στο διαδίκτυο. Το νοσοκομείο το ανακαλύπτει μερικές μέρες αργότερα. Από τη στιγμή που λαμβάνει γνώση το νοσοκομείο, πρέπει σε 72 ώρες να ενημερώσει την εποπτική αρχή και επιπλέον, καθώς τα προσωπικά στοιχεία περιέχουν ευαίσθητες πληροφορίες, για παράδειγμα εάν ο/η ασθενής πάσχει από καρκίνο, είναι έγκυος κ.λπ., πρέπει να ενημερώσει και τους ασθενείς. Στην περίπτωση αυτή, είναι αμφίβολο εάν το νοσοκομείο είχε εφαρμόσει κατάλληλα τεχνικά και οργανωτικά μέτρα προστασίας . Εάν είχε πράγματι εφαρμόσει κατάλληλα μέτρα προστασίας (π.χ. κρυπτογράφηση των δεδομένων), δεν θα ήταν πιθανό να προκύψει ουσιώδης κίνδυνος και το νοσοκομείο θα μπορούσε να είχε απαλλαγεί από την υποχρέωση να ειδοποιήσει τους ασθενείς.

Η εταιρεία πρέπει να ειδοποιήσει τους πελάτες και αυτοί έπειτα μπορεί να πρέπει να ειδοποιήσουν την Αρχή Προστασίας Δεδομένων και τα φυσικά πρόσωπα: *Σε μια υπηρεσία νέφους σημειώνεται απώλεια αρκετών σκληρών δίσκων που περιέχουν δεδομένα προσωπικού χαρακτήρα τα οποία ανήκουν σε αρκετούς πελάτες της. Η εταιρεία πρέπει να ειδοποιήσει τους εν λόγω πελάτες αμέσως μόλις αντιληφθεί την παραβίαση. Οι πελάτες της πρέπει να ειδοποιήσουν την Αρχή Προστασίας Δεδομένων και τα φυσικά πρόσωπα ανάλογα με τα δεδομένα που είχαν υποβληθεί σε επεξεργασία από τον εκτελούντα την επεξεργασία.*

Νομική βάση επεξεργασίας

Πότε μπορούν να υποβάλλονται σε επεξεργασία δεδομένα προσωπικού χαρακτήρα;

Η επεξεργασία των δεδομένων προσωπικού χαρακτήρα γίνεται μόνο στις ακόλουθες περιπτώσεις:

- με τη **συγκατάθεση** των οικείων ατόμων
- εάν υπάρχει **συμβατική υποχρέωση** (σύμβαση ανάμεσα στην εταιρεία ή τον οργανισμό σας και έναν πελάτη)
- για την εκπλήρωση **νομικής υποχρέωσης** (σύμφωνα με τη νομοθεσία της ΕΕ ή την εθνική νομοθεσία)
- όταν η επεξεργασία είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το **δημόσιο συμφέρον** (σύμφωνα με τη νομοθεσία της ΕΕ ή την εθνική νομοθεσία)
- για την προστασία των **ζωτικών συμφερόντων** ενός ατόμου
- προς χάριν των **έννομων συμφερόντων** του οργανισμού σας, αλλά μόνο αφού ελέγξετε ότι τα θεμελιώδη δικαιώματα και οι ελευθερίες του ατόμου του οποίου δεδομένα επεξεργάζεστε δεν επηρεάζονται σοβαρά. Εάν τα δικαιώματα του ατόμου υπερισχύουν των συμφερόντων σας, τότε δεν επιτρέπεται επεξεργασία με βάση έννομο συμφέρον. Η αξιολόγηση σχετικά με το εάν τα έννομα συμφέροντα της εταιρείας ή του οργανισμού σας για επεξεργασία υπερισχύουν των συμφερόντων των οικείων ατόμων εξαρτάται από τις ιδιαίτερες περιστάσεις κάθε περίπτωσης.

Γενικά Παραδείγματα

Συγκατάθεση: *Η εταιρεία ή ο οργανισμός σας προσφέρει μια μουσική εφαρμογή και ζητάτε τη συγκατάθεση των πολιτών για να επεξεργαστείτε τις μουσικές τους προτιμήσεις έτσι ώστε να τους προτείνετε ειδικά επιλεγμένα τραγούδια και πιθανές συναυλίες.*

Συμβατική υποχρέωση: *Η εταιρεία ή ο οργανισμός σας πουλά αγαθά στο διαδίκτυο. Μπορεί να επεξεργάζεται δεδομένα που είναι απαραίτητα για ορισμένες ενέργειες κατόπιν αιτήματος του ατόμου πριν από τη σύναψη της σύμβασης και για την εκτέλεση της σύμβασης. Έτσι μπορείτε να επεξεργαστείτε το ονοματεπώνυμο, τη διεύθυνση παράδοσης, τον αριθμό πιστωτικής κάρτας (εάν η πληρωμή γίνεται με κάρτα) κ.λπ.*

Νομική υποχρέωση: *Είστε ο ιδιοκτήτης μιας εταιρείας που απασχολεί εργαζομένους. Για τη λήψη κάλυψης κοινωνικής ασφάλισης, η νομοθεσία σάς υποχρεώνει να παρέχετε δεδομένα προσωπικού χαρακτήρα (π.χ. εβδομαδιαίο εισόδημα των εργαζομένων σας) στη σχετική αρχή.*

Δημόσιο συμφέρον: *Παράδειγμα: μια επαγγελματική ένωση, π.χ. ένας δικηγορικός σύλλογος ή μια ένωση επαγγελματιών υγείας, μπορεί, σύμφωνα με δημόσια εξουσία που της έχει ανατεθεί, να κινήσει πειθαρχικές διαδικασίες εναντίον κάποιων εκ των μελών της.*

Ζωτικά συμφέροντα ενός ατόμου: *Ένα νοσοκομείο περιθάλπει έναν ασθενή μετά από ένα σοβαρό τροχαίο ατύχημα το νοσοκομείο δεν χρειάζεται τη συγκατάθεσή του για να ψάξει την ταυτότητά του έτσι ώστε να ελέγξει εάν το εν λόγω άτομο συμπεριλαμβάνεται στη βάση δεδομένων του νοσοκομείου για να βρει το ιατρικό ιστορικό του ή να επικοινωνήσει με τους συγγενείς του.*

Τα έννομα συμφέροντα του οργανισμού σας: *Η εταιρεία ή ο οργανισμός σας διασφαλίζει την ασφάλεια του δικτύου που χρησιμοποιεί μέσω της παρακολούθησης της χρήσης των συσκευών τεχνολογίας πληροφοριών των εργαζομένων. Μπορεί να επεξεργάζεται νομίμως δεδομένα προσωπικού χαρακτήρα για αυτόν τον σκοπό μόνο εάν επιλέξει τη λιγότερο επεμβατική μέθοδο όσον αφορά τα δικαιώματα προστασίας της ιδιωτικής ζωής και των δεδομένων των εργαζομένων σας, για παράδειγμα, περιορίζοντας την πρόσβαση σε ορισμένους ιστότοπους. (Σημειωτέον ότι αυτό δεν μπορεί να γίνει σε κράτη μέλη της ΕΕ όπου η εθνική νομοθεσία ορίζει αυστηρότερους κανόνες για την επεξεργασία στο πλαίσιο της απασχόλησης).*

Μπορούν να χρησιμοποιηθούν δεδομένα για άλλον σκοπό;

👉 Στην περίπτωση που ένα λογιστικό γραφείο κάνει την επεξεργασία των δεδομένων για λογαριασμό τρίτου (δηλαδή το λογιστικό γραφείο είναι «εκτελών την επεξεργασία») **θα πρέπει η επεξεργασία που κάνει να γίνεται ΜΟΝΟ στα πλαίσια της εντολής ή της συμφωνίας που υπάρχει με τον εκάστοτε υπεύθυνο επεξεργασίας.**

Οι υπεύθυνοι επεξεργασίας μπορούν να χρησιμοποιήσουν δεδομένα για άλλο σκοπό, αλλά μόνο σε μερικές περιπτώσεις.

Εάν έχει γίνει η συλλογή των δεδομένων με βάση **έννομο συμφέρον**, **σύμβαση** ή **ζωτικά συμφέροντα,** μπορούν να χρησιμοποιηθούν για άλλον σκοπό αλλά μόνο αφού ελεγχτεί ότι **ο νέος σκοπός είναι συμβατός με τον αρχικό σκοπό**.

Στο πλαίσιο αυτό, πρέπει να λαμβάνονται υπόψη τα εξής:

- η σύνδεση μεταξύ του αρχικού και του νέου/μελλοντικού σκοπού
- το πλαίσιο στο οποίο συλλέχθηκαν τα δεδομένα (ποια είναι η σχέση μεταξύ της εταιρείας ή του οργανισμού σας και του φυσικού προσώπου;)
- το είδος και η φύση των δεδομένων (είναι ευαίσθητα;)
- οι ενδεχόμενες συνέπειες της επιδιωκόμενης περαιτέρω επεξεργασίας (πώς θα επηρεάσει το άτομο;)
- η ύπαρξη κατάλληλων εγγυήσεων (όπως η κρυπτογράφηση ή η ψευδωνυμοποίηση).

Εάν τα δεδομένα αυτά χρησιμοποιηθούν για στατιστικούς σκοπούς ή για επιστημονική έρευνα, δεν απαιτείται έλεγχος συμβατότητας.

⚠ ΠΡΟΣΟΧΗ!!

Εάν έχετε συλλέξει τα δεδομένα βάσει **συγκατάθεσης ή σύμφωνα με συμβατική ή νομική υποχρέωση**, δεν είναι δυνατή περαιτέρω επεξεργασία πέραν των σκοπών που καλύπτονται από την αρχική συγκατάθεση ή τις διατάξεις της νομοθεσίας. Τυχόν περαιτέρω επεξεργασία απαιτεί τη λήψη νέας συγκατάθεσης ή νέα νομική βάση.

Σημείωση:

Σε αρκετές περιπτώσεις, συγκατάθεση ή συμβατική ή νομική υποχρέωση παρέχεται από την πλευρά του εντολέα – πελάτη (δηλαδή του υπεύθυνου επεξεργασίας π.χ. επιχείρησης-πελάτη ή ιδιώτη-φορολογούμενου) γιατί το λογιστικό γραφείο έχει τον ρόλο του εκτελών την επεξεργασία σε θέματα όπως: μισθοδοσία υπαλλήλων άλλων επιχειρήσεων που είναι πελάτες του γραφείου ή για την υποβολή δηλώσεων ενός φυσικού προσώπου – πελάτη. Για θέματα όπως μισθοδοσία των ιδίων υπαλλήλων του λογιστικού γραφείου ή αποστολής ενημερωτικών newsletter στο κοινό ή χρήσης καμερών βιντεοπαρακολούθησης, το λογιστικό γραφείο έχει τον ρόλο υπεύθυνου επεξεργασίας και βαρύνεται με την απόδειξη της όποιας συγκατάθεσης ή άλλης βάσης νομικής επεξεργασίας που απαιτείται για την εκάστοτε επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Παραδείγματα από την πλευρά υπεύθυνου επεξεργασίας:

Η περαιτέρω επεξεργασία είναι δυνατή:

Μια τράπεζα έχει σύμβαση με έναν πελάτη για να του παρέχει τραπεζικό λογαριασμό και προσωπικό δάνειο. Στο τέλος του πρώτου έτους η τράπεζα χρησιμοποιεί τα δεδομένα προσωπικού χαρακτήρα του πελάτη για να ελέγξει εάν είναι επιλέξιμος για καλύτερο είδος δανείου και πρόγραμμα αποταμίευσης. Ενημερώνει σχετικά τον πελάτη. Η τράπεζα μπορεί να επεξεργαστεί τα δεδομένα του πελάτη ξανά καθώς οι νέοι σκοποί είναι συμβατοί με τους αρχικούς.

Η περαιτέρω επεξεργασία δεν είναι δυνατή:

Η ίδια τράπεζα επιθυμεί να κοινοποιήσει τα δεδομένα του πελάτη σε ασφαλιστικές εταιρείες, με βάση την ίδια σύμβαση για τραπεζικό λογαριασμό και προσωπικό δάνειο. Αυτή η επεξεργασία δεν επιτρέπεται χωρίς τη ρητή συγκατάθεση του πελάτη, καθώς ο σκοπός δεν είναι συμβατός με τον αρχικό σκοπό επεξεργασίας των δεδομένων.

Παράδειγμα: Πελάτες – Ιδιώτες (φυσικά πρόσωπά)

Είναι σημαντικό να τονιστεί ότι στις περιπτώσεις που το λογιστικό γραφείο αναλαμβάνει να κάνει μια δουλειά για λογαριασμό ενός πελάτη, **έχει τον ρόλο του «εκτελών την επεξεργασία» για λογαριασμό του πελάτη**, κάτι για το οποίο δεν απαιτείται συγκατάθεση, αλλά μόνο κάτι που να αποδεικνύει την σχέση τους.

Ο πελάτης σε αυτή τη περίπτωση δίνει «εντολή» επεξεργασίας των δεδομένων του από το λογιστικό γραφείο, το οποίο επεξεργάζεται τα δεδομένα προσωπικού χαρακτήρα του πελάτη – ιδιώτη, ως μέρος της εκάστοτε **συμβατικής υποχρέωσης** (π.χ. υποβολής φορολογικής δήλωσης). **Αξίζει να σημειωθεί ότι σε περίπτωση κοινής δήλωσης θα πρέπει η «εντολή» επεξεργασίας δεδομένων να δίνεται από κοινού από τους εμπλεκόμενους φορολογούμενους.**

Περίπτωση	Λόγος επεξεργασίας	Ανάλυση - Ενέργειες
Ο πελάτης ζητάει από το λογιστικό γραφείο να κάνει την φορολογική του δήλωση	**Συμβατική υποχρέωση** (συμφωνία μεταξύ πελάτη και λογιστικού γραφείου για υποβολή φορολογικής δήλωσης)	Ο λογιστής θα πρέπει αν χρειαστεί να έχει ένα μέσο απόδειξης της σχέσης του με τον πελάτη που να αποδεικνύει τον λόγο επεξεργασίας των δεδομένων προσωπικού χαρακτήρα του πελάτη. Συμφωνίες ή εντολές δεν είναι απαραίτητο να είναι γραπτές, μπορεί να είναι και προφορικές, ωστόσο στην περίπτωση που χρειαστεί να αποδειχτεί, μια γραπτή συμφωνία ή εντολή έχει μεγαλύτερο βάρος και αποδεικνύεται ευκολότερα. Ενδεικτικά: ζητείται το γνήσιο της υπογραφής για την υποβολή φορολογικών δηλώσεων για λογαριασμό του πελάτη (ΠΟΛ1088/2015).
Ο πελάτης είναι παντρεμένος και η δήλωση φορολογίας έχει και τα στοιχεία του/της συζύγου.	**Συμβατική υποχρέωση** (συμφωνία μεταξύ πελάτη και συζύγου από την μια πλευρά και του λογιστικού γραφείου από την άλλη για την υποβολή φορολογικής δήλωσης)	Στην περίπτωση αυτή, ο/η πελάτης και ο/η σύζυγος αυτού/αυτής είναι **από κοινού** υπεύθυνοι επεξεργασίας και **από κοινού** πρέπει να δώσουν την εντολή της επεξεργασίας των δεδομένων τους από το λογιστικό γραφείο. Αν δεν είναι εφικτό αυτό, θα πρέπει να διευκρινιστεί στον πελάτη ότι για να προχωρήσει το λογιστικό γραφείο στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα θα πρέπει ο πελάτης να έχει ενημερώσει και να έχει λάβει την σύμφωνη γνώμη του ή της συζύγου.
Η φορολογική δήλωση του πελάτη περιλαμβάνει στοιχεία τρίτων (π.χ. ενός ενοικιαστή ή φιλοξενούμενων ατόμων, κλπ.)	**Συμβατική υποχρέωση** (πελάτης με λογιστικό γραφείο) **Νομική υποχρέωση** (υποχρέωση ακριβούς υποβολής δήλωσης)	Στην περίπτωση που σε μία δήλωση απαιτείται η συμπλήρωση στοιχείων τρίτου (π.χ. του ΑΦΜ ενός ενοικιαστή στην περίπτωση ενοικίασης), δεν απαιτείται συγκατάθεση από το υποκείμενο των δεδομένων διότι υποχρεούται νομικά ο φορολογούμενος να δηλώσει τα στοιχεία αυτά και ο «λογιστής-φοροτεχνικός οφείλει να μεταφέρει ορθά τα δεδομένα των στοιχείων και βιβλίων στις δηλώσεις των φορολογούμενων» (Αρ. 38 Ν.2873/2000).

👉 Η σχέση ενός λογιστικού γραφείου και ενός πελάτη φυσικού προσώπου συνήθως δεν περιορίζεται στην υποβολή μόνο μιας φορολογικής δήλωσης ή μιας τροποποίησης Ε9 ή μιας αίτησης για επίδομα, αλλά συνήθως είναι διαρκής, όπου ο πελάτης ανά πάσα στιγμή μπορεί να ζητήσει την υποβολή μίας άλλης δήλωσης/αίτησης ή ακόμα και την εκτύπωση (ή την αποστολή) ενός εκκαθαριστικού ή μιας ταυτότητας οφειλής ή μιας βεβαίωσης, κλπ.

✋ **Αν πρέπει να διατηρηθούν δεδομένα προσωπικού χαρακτήρα ή/και οι κωδικοί από το λογιστικό γραφείο θα πρέπει να έχει συμφωνηθεί (προφορικώς ή προτιμότερα γραπτώς) η συνεχιζόμενη παροχή υπηρεσιών προς τον πελάτη μέχρι την διακοπή της συνεργασίας αυτής.**

Τα δεδομένα αυτά θα μπορούν να χρησιμοποιούνται για τον σκοπό παροχής των εκάστοτε συμφωνημένων υπηρεσιών και μόνο. Για παράδειγμα: δεν θα πρέπει το λογιστικό γραφείο να χρησιμοποιήσει τα στοιχεία του πελάτη για άλλον σκοπό (π.χ. αποστολή ενημερωτικών email προσφορών) χωρίς σχετική ρητή συγκατάθεση του πελάτη. Αν όμως το επιθυμεί μπορεί να ζητήσει την συγκατάθεση του πελάτη για τον συγκεκριμένο λόγο.

⚠ ΠΡΟΣΟΧΗ: **Με την λήξη της συνεργασίας θα πρέπει** να διαγραφούν, καταστραφούν ή να επιστραφούν (βάσει υποχρεώσεων για διατήρηση των εκάστοτε νόμων) όσα αρχεία διατηρεί το λογιστικό γραφείο και αφορούν το φυσικό πρόσωπο ή περιέχουν δεδομένα προσωπικού χαρακτήρα του πελάτη-ιδιώτη

Εξαιρούνται περιπτώσεις που η λήξη συνεργασίας δεν αφορά π.χ. και την αποστολή ενημερωτικών email (δεδομένου ότι υπάρχει σχετική συγκατάθεση για αυτόν τον σκοπό) όπου εκεί μπορούν να διατηρηθούν μόνο τα απαραίτητα στοιχεία για την αποστολή των ενημερωτικών αυτών.

Παράδειγμα: Πελάτες – Επιχειρήσεις (νομικά πρόσωπα)

Στο ζήτημα της επεξεργασίας δεδομένων προσωπικού χαρακτήρα φυσικών προσώπων σε ότι αφορά την συνεργασία ενός λογιστικού γραφείο με μια επιχείρηση-πελάτη, αναφέρεται κατά κύριο λόγο στην «γραφειοκρατία» της διαχείρισης ανθρώπινου δυναμικού (υπαλλήλων) της επιχείρησης πελάτη, δηλαδή τις διαδικασίες της: πρόσληψης, αποχώρησης, μισθοδοσίας, αδειών, πινάκων, κλπ.

Περίπτωση	Λόγος επεξεργασίας	Ανάλυση - Ενέργειες
Η επιχείρηση Χ είναι πελάτης του λογιστικού γραφείου και ζητάει από το λογιστικό γραφείο να αναλάβει την μισθοδοσία του προσωπικού της επιχείρησης Χ και όλες τις ενέργειες γύρω από αυτό.	**Συμβατική υποχρέωση** (μεταξύ λογιστικού γραφείου και επιχείρησης Χ) ***Νομική υποχρέωση*** *(μεταξύ επιχείρησης Χ και του κράτους)*	Ουσιαστικά αναφερόμαστε σε διαδικασίες μεταξύ της επιχείρησης Χ και φορέων του δημοσίου όπως: ΣΕΠΕ – Εργάνη, ΟΑΕΔ, ΕΦΚΑ και Εφορίας. Για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα εκ μέρους του υπεύθυνου επεξεργασίας (*στην περίπτωση αυτή: της επιχείρησης Χ*) θα πρέπει να υπάρχει **σύμβαση ή κάποια άλλη νομική πράξη** με το λογιστικό γραφείο.

⚠ ΠΡΟΣΟΧΗ: Ο τρόπος απόδειξης της σχέσης ενός λογιστικού γραφείου και μιας επιχείρησης-πελάτη σύμφωνα με τον GDPR είναι μια σύμβαση ή κάποιο άλλο νομικό έγγραφο το οποίο μεταξύ άλλων θα αναγράφει και τον σκοπό της ανάθεσης της επεξεργασίας των δεδομένων αυτών και άλλα στοιχεία, συμπληρωματικά με την όποια σύμβαση υπάρχει αυτή τη στιγμή μεταξύ των δυο μερών.

Τα όρια της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα για λογαριασμό της επιχείρησης-πελάτη του λογιστικού γραφείο ορίζεται στη σύμβαση (ή άλλο νομικό έγγραφο) και ο εκτελών την επεξεργασία (λογιστικό γραφείο) **δεν** πρέπει να κάνει τίποτα άλλο επιπλέον από αυτά που ορίζονται στην σύμβαση αυτή, εκτός και αν υπάρξει μια νέα σύμβαση που ορίζει διαφορετικά.

👉 <u>Ενδεικτικά: Στην νομική πράξη (ή άλλο νομικό έγγραφο) θα πρέπει να συμπεριλαμβάνονται οι εξής πρόνοιες:</u>

- Θα πρέπει να καταγράφεται ο σκοπός της επεξεργασίας (μισθοδοσία), και η επεξεργασία θα πρέπει να γίνεται **μόνο βάσει των καταγεγραμμένων εντολών** της επιχείρησης-πελάτη. (*Σημείωση: Το λογιστικό γραφείο μπορεί να συμβουλεύει, <u>αλλά όχι να αποφασίζει</u> στο τι δεδομένα θα συλλέγονται ή στο τι θα γίνονται με αυτά.)*
- Να διασφαλίζεται ότι τα εξουσιοδοτημένα άτομα (εννοώντας τους υπάλληλους του λογιστικού γραφείου) έχουν αναλάβει δέσμευση **τήρησης εμπιστευτικότητας** ή τελούν υπό τη δέουσα κανονιστική υποχρέωση τήρησης εμπιστευτικότητας.
- Το λογιστικό γραφείο θα πρέπει να προσφέρει ένα (**ελάχιστο) επίπεδο ασφάλειας** που καθορίζεται από τον υπεύθυνο επεξεργασίας (επιχείρηση-πελάτη).
- Το λογιστικό γραφείο (ως εκτελών την επεξεργασία) συμβάλλει στην διασφάλιση της συμμόρφωσης με τον GDPR. **Αυτό σημαίνει ότι το λογιστικό γραφείο δεν ακολουθεί τυφλά τις εντολές του υπεύθυνου επεξεργασίας.** *π.χ. οφείλει να βλέπει ότι τα δεδομένα τα οποία λαμβάνει το λογιστικό γραφείο (και η επιχείρηση πελάτης ως υπεύθυνος επεξεργασίας) είναι συμβατά με το αντικείμενο της επεξεργασίας που του έχει οριστεί και ότι υπάρχει η σχετική νομική βάση της επεξεργασίας τους.*

✋ Στην περίπτωση του προσωπικού του λογιστικού γραφείου, τότε το λογιστικό γραφείο - ως εργοδότης - είναι ο υπεύθυνος επεξεργασίας των στοιχείων των υπαλλήλων του. Σε αυτή τη περίπτωση το λογιστικό γραφείο έχει νομική υποχρέωση για την χρήση μόνο των στοιχείων που είναι απαραίτητα και μόνο για τις υποχρεώσεις που ορίζονται από τη νομοθεσία.

Σύστημα βιντεοεπιτήρησης

Η λειτουργία συστήματος βιντεοεπιτήρησης σε ένα λογιστικό γραφείο, καθιστά τον ιδιοκτήτη του λογιστικού γραφείου «υπεύθυνο επεξεργασίας» και οφείλει να συμμορφώνεται με τις όποιες διατάξεις, οδηγίες και κανονισμούς προβλέπονται για το θέμα αυτό.

Ενημερωθείτε για τα συστήματα βιντεοεπιτήρησης στη σχετική θεματική ενότητα της ιστοσελίδας της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ):

http://www.dpa.gr/portal/page?_pageid=33,124762&_dad=portal&_schema=PORTAL

Η υποχρέωση γνωστοποίησης ή λήψης άδειας από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) έχει καταργηθεί, ωστόσο όπως αναφέρεται και στην σελίδα της: «Ενδεχομένως, όμως, λόγω της επεξεργασίας που θα κάνετε μέσω του συστήματος βιντεοεπιτήρησης, να έχετε, εκ του Κανονισμού (ΕΕ) 2016/679, κάποιες πρόσθετες υποχρεώσεις (βλ. οδηγό συμμόρφωσης εδώ - και ιδίως για την υποχρέωση τήρησης αρχείων δραστηριοτήτων εδώ).»

Σε γενικές γραμμές:

- Η εγκατάσταση ενός συστήματος βιντεοεπιτήρησης πρέπει να έχει ως σκοπό την προστασία προσώπων και αγαθών στον χώρο τον οποίο έχει εγκατασταθεί.
- **ΔΕΝ επιτρέπεται η χρήση συστημάτων βιντεοεπιτήρησης για σκοπούς παρακολούθησης εργαζομένων για έλεγχο/αξιολόγηση ή για σκοπούς εκπαίδευσης τους.**
- «Κατά κανόνα, δεν επιτρέπεται η τοποθέτηση καμερών σε δημόσιο χώρο από ιδιώτη για τον σκοπό της προστασίας προσώπων και αγαθών (μια τέτοια τοποθέτηση μπορεί να επιτραπεί σε εξαιρετικές μόνο περιπτώσεις και υπό συγκεκριμένες προϋποθέσεις – βλ. άρθρο 6 της οδηγίας 1/2011).»
- Θα πρέπει να υπάρχει εμφανή και ξεκάθαρη **ενημερωτική σήμανση** ότι ο χώρος καταγράφεται από σύστημα βιντεοεπιτήρησης.
- Θα πρέπει να εξασφαλίσετε ότι τα αρχεία καταγραφής τους είναι **ασφαλή** και **προσβάσιμα μόνο από εσάς** ή κάποιον που έχετε ορίσει εσείς.
- Τα δεδομένα να είναι στην διάθεση των υποκειμένων των δεδομένων *(εφ' όσον ζητηθούν) όπως προβλέπεται από τον GDPR.*
- ***«Τα δεδομένα πρέπει να τηρούνται για το μικρότερο δυνατό χρόνο**. Σε κάθε περίπτωση δεν επιτρέπεται να τηρούνται για διάστημα μεγαλύτερο των 15 ημερών, εκτός από εξαιρέσεις. Ειδικά για πολυκατοικίες, πρέπει να τηρούνται το πολύ μέχρι 48 ώρες, ενώ για σχολικά συγκροτήματα κ.λπ. μέχρι την επόμενη εργάσιμη ημέρα. Οι τράπεζες και τα χρηματοπιστωτικά ιδρύματα μπορούν να τα τηρούν μέχρι 45 ημέρες. Ο χρόνος τήρησης μπορεί να παραταθεί εφόσον υπάρξει κάποιο συμβάν και το υλικό μπορεί να χρησιμοποιηθεί ως αποδεικτικό στοιχείο, (βλ. άρθρο 8 της οδηγίας 1/2011 για αναλυτικότερη περιγραφή, καθώς και το αντίστοιχο άρθρο του Ειδικού Μέρους της οδηγίας ανάλογα με την κατηγορία του υπευθύνου επεξεργασίας)».*[6]

[6] http://www.dpa.gr/portal/page?_pageid=33,124846&_dad=portal&_schema=PORTAL#14

Περισσότερες πληροφορίες και πηγές

Σας ενθαρρύνουμε να μελετήσετε τις πηγές που αναφέρονται για την καλύτερη ενημέρωση σας καθώς και τον ίδιο τον Γενικό Κανονισμό για την Προστασία Δεδομένων στον ιστότοπο της Ευρωπαϊκής Ένωσης.

Μπορείτε επίσης να δείτε τα προηγούμενα ενημερωτικά έντυπα της Π.Ο.Φ.Ε.Ε. σχετικά με τον GDPR:
Οδηγός επιχειρήσεων για τον νέο Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR)
Λίστα Ελέγχου Ετοιμότητας για τον νέο Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR)

Μάθετε περισσότερα στην σελίδα της Ευρωπαϊκής Επιτροπής σχετικά με την μεταρρύθμιση των κανόνων προστασίας δεδομένων της ΕΕ στον σύνδεσμο:
https://ec.europa.eu/info/law/law-topic/data-protection/reform_el

Ακολουθήστε τον διαδραστικό οδηγό ενημέρωσης της Ευρωπαϊκής Επιτροπής στον σύνδεσμο: http://ec.europa.eu/justice/smedataprotect/index_el.htm

Μάθετε περισσότερα στην ιστοσελίδα του Επιτρόπου Προστασίας Δεδομένων της Ιρλανδίας: www.dataprotection.ie (Αγγλικά)

Ακολουθήστε τον διαδραστικό οδηγό ενημέρωσης στον παρακάτω σύνδεσμο:
http://gdprandyou.ie (Αγγλικά)

Το παρόν έντυπο έχει σκοπό την ενημέρωση και δεν στοχεύει να αντικαταστήσει μια εξειδικευμένη επαγγελματική μελέτη. *Οι παράγοντες του εντύπου δεν φέρουν καμία ευθύνη από τυχόν ζημιές προκληθούν από την χρήση του παρόντος ενημερωτικού.*

συγγραφή και επιμέλεια περιεχομένου για την Π.Ο.Φ.Ε.Ε.
Θεόδωρος Κεντιστός - Ράννος

Πανελλήνια Ομοσπονδία Φοροτεχνικών Ελευθέρων Επαγγελματιών (Π.Ο.Φ.Ε.Ε.)
Διεύθυνση: Ιουλιανού 42-46, Αθήνα, ΤΚ 104 34 | τηλ.: 210.82.53.445 | φαξ: 210.82.53.446
site: www.pofee.gr | email$_{(1)}$: info@pofee.gr | email$_{(2)}$: pofee@otenet.gr