ΚΑΤΕΥΘΥΝΤΗΡΙΕΣ ΟΔΗΓΙΕΣ ΓΙΑ ΤΗΝ ΕΦΑΡΜΟΓΗ ΤΟΥ ΚΑΝΟΝΙΣΜΟΥ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΑ ΞΕΝΟΔΟΧΕΙΑ ΚΑΙ ΚΑΜΠΙΝΓΚ

H
HOTELS

ΞΕΝΟΔΟΧΕΙΑΚΟ ΕΠΙΜΕΛΗΤΗΡΙΟ ΕΛΛΑΔΟΣ

Η εφαρμογή του ΓΚΠΔ στα ξενοδοχεία

ΜΙΑ ΕΙΣΑΓΩΓΗ ΣΤΟ ΝΕΟ ΔΙΚΑΙΟ

Από την άφιξη μέχρι την αναχώρηση, από την κράτηση έως τη δημιουργία μίας ιστοσελίδας για το ξενοδοχείο, ο ξενοδόχος προβαίνει καθημερινά σε συλλογή και επεξεργασία προσωπικών δεδομένων για τους πελάτες του. Η επεξεργασία αυτή, αναγκαία για την υποστήριξη των υπηρεσιών που παρέχει ένα ξενοδοχείο, υπόκειται ωστόσο σε προϋποθέσεις και όρους που θέτει μεταξύ άλλων η νομοθεσία για την προστασία προσωπικών δεδομένων.

Οι σχετικές υποχρεώσεις δεν είναι ακριβώς νέες. Στην Ελλάδα ήδη από το 1997 ισχύει ο ν. 2472/97 που έθετε τους κανόνες της σύννομης επεξεργασίας προσωπικών δεδομένων. Ονόμος αυτός επέβαλε ουσιαστικές αλλά και διαδικαστικές υποχρεώσεις, όπως η γνωστοποίηση αρχείων, επεξεργασιών και συστημάτων βιντεοεπιτήρησης στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

Στις 25 Μαΐου 2018 τίθεται σε εφαρμογή ο Γενικός Κανονισμός Προστασίας Δεδομένων, ένα νέο ευρωπαϊκό, ενιαίο και συνεκτικό πλαίσιο το οποίο αντικαθιστά τις σχετικές εθνικές νομοθεσίες στα κράτη μέλη της Ευρωπαϊκής Ένωσης.

Λόγω της νομικής φύσης του ο Κανονισμός έχει άμεση εφαρμογή σε όλα τα κράτη μέλη της Ευρωπαϊκής Ένωσης και δεν απαιτείται αλλά και ούτε επιτρέπεται η ενσωμάτωση των ρυθμίσεων στην εθνική νομοθεσία τους. Ωστόσο ο συγκεκριμένος Κανονισμός περιέχει αρκετές «ρήτρες ευελιξίας», αναγνωρίζοντας στα κράτη μέλη την ευχέρεια να εξειδικεύσουν τους κανόνες του, και να προσδιορίζουν τις περιστάσεις ειδικών καταστάσεων επεξεργασίας, μεταξύ άλλων τον ακριβέστερο καθορισμό των προϋποθέσεων υπό τις οποίες η επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι σύννομη. Ο εθνικός νομοθέτης έχει επίσης την ευχέρεια που παρέχει ο Κανονισμός ως προς τη ρύθμιση ειδικών περιπτώσεων επεξεργασίας, όπως η επεξεργασία των δεδομένων στο πλαίσιο της απασχόλησης για να εξειδικεύσει και να συμπληρώσει τις ρυθμίσεις του Κανονισμού .

Όλα τα κράτη μέλη πρέπει να υιοθετήσουν και εθνικούς κανόνες που πλαισιώνουν τον Κανονισμό. Στην Ελλάδα αναμένεται η ψήφιση νόμου για την προστασία δεδομένων προσωπικού χαρακτήρα. το προσχέδιο νόμου είναι δημοσιευμένο στην διεύθυνση http://www.opengov.gr/ministryofjustice/wp-content/uploads/downloads/2018/02/sxedio_nomou_prostasia_pd.pdf. ορίζει

ότι θα καταργηθεί ο Νόμος 2472/1997 και θα τεθούν σε ισχύ διατάξεις που συμπληρώνουν τον Κανονισμό και εξειδικεύουν ορισμένες από τις υποχρεώσεις που θεσπίζει ο Κανονισμός.Ωστόσο προς το παρόν και παρά την θέση σε εφαρμογή του Κανονισμού δεν έχει κατατεθεί στη Βουλή .

Κρίνεται όμως αναγκαίο να επισημανθεί ότι η υποχρέωση ως προς την τήρηση της νομοθεσίας θα περιλαμβάνει και τις διατάξεις του ελληνικού δικαίου που θα συμπληρώσουν και εξειδικεύσουν τον Κανονισμό, ως προς τα σημεία που αυτό επιτρέπεται.

Το νέο δίκαιο απαλλάσσει τους υπευθύνους επεξεργασίας από τις διαδικαστικές, γραφειοκρατικές υποχρεώσεις αλλά επιβάλλει σε αυτούς τη μέριμνα να οργανώνουν με ιδιαίτερη προσοχή και συνέπεια τη συμμόρφωσή τους προς τη νομοθεσία. Μία υποχρέωση στην οποία πρέπει να ανταποκριθούμε όλοι καθώς η παράβαση του νόμου ενδέχεται να μας φέρει αντιμέτωπους με πολύ υψηλά πρόστιμα αλλά και δικαστικές αξιώσεις των προσώπων, τα δικαιώματα των οποίων ενδέχεται να θίγονται από την επεξεργασία των δεδομένων τους.

1. Μερικοί χρήσιμοι ορισμοί

Η γνώση και κατανόηση του νέου δικαίου προυποθέτει τη γνώση και κατανόηση μερικών βασικών εννοιών

Δεδομένα προσωπικού χαρακτήρα ή προσωπικά δεδομένα είναι κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο».

Ο όρος είναι πολύ ευρύς και καλύπτει κάθε πληροφορία ανεξάρτητα από το ποια πλευρά του ατόμου αφορά, την ιδιωτική ή την επαγγελματική διάσταση, τις ιδιότητες, τις γνώσεις του, τα ψυχολογικά χαρακτηριστικά, τις οικονομικές σχέσεις ή στοιχεία της προσωπικής του ιστορίας. Στον όρο "προσωπικά δεδομένα" περιλαμβάνονται και αυτά τα οποία χρησιμοποιούνται συνήθως για τον προσδιορισμό της ταυτότητας του προσώπου (ο αριθμός της διαβατηρίου, ο αριθμός του δελτίου ταυτότητας, ο αριθμός πελάτη και άλλα παρόμοια στοιχεία.)αλλά και νομιμοποιητικά στοιχεία που αποδίδονται σε πρόσωπα ή επιλέγονται από αυτά (κωδικός αναγνώρισης ή πρόσβασης, PIN κ.α.).Προσωπικά δεδομένα είναι και τα δεδομένα εικόνας και ήχου και συνεπώς η λήψη φωτογραφιων και βιντεο αφορά προσωπικά δεδομένα . Ως προσωπικά δεδομένα νοούνται και αυτά που αφορούν την περιουσιακή κατάσταση, για την επαγγελματική και οικονομική δραστηριότητα, την οικογενειακή κατάσταση, τις προσωπικές δραστηριότητες και σχέσεις κ.α. Δεδομένα προσωπικού χαρακτήρα θεωρούνται και οι αξιολογικού χαρακτήρα κρίσεις όπως π.χ. "καλός πελάτης" .

Ειδική κατηγορία δεδομένων αποτελούν τα λεγόμενα ευαίσθητα, στα οποία συμπεριλαμβάνονται η φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, οι θρησκευτικές ή φιλοσοφικές πεποιθήσεις, η συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και η επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, τα δεδομένα που αφορούν την υγεία ή δεδομένα που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό. Ως ειδική κατηγορία νοούνται και τα Δεδομένα προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα

Ο Κανονισμός επιφυλάσσει πιο ενισχυμένη προστασία στα ευαίσθητα δεδομένα.

«**Υποκείμενο των δεδομένων**» : το ταυτοποιήσιμο φυσικό πρόσωπο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου,

Η αναγνώριση ταυτότητας επιτυγχάνεται κανονικά μ ε βάση συγκεκριμένες πληροφορίες που καλούνται «στοιχεία αναγνώρισης», όπως διάφορα εξωτερικά γνωρίσματα της εμφάνισης του εν λόγω προσώπου, όπως το ύψος, το χρώμα των μαλλιών, η ένδυση, κλπ ή κάποια ιδιότητα του προσώπου που δεν μπορεί να γίνει αμέσως αντιληπτή, όπως επάγγελμα, αξίωμα, όνομα κλπ. "η ταυτότητα ενός προσώπου μπορεί να προσδιορισθεί άμεσα από το όνομα ή έμμεσα από έναν αριθμό τηλεφώνου, αριθμό κυκλοφορίας αυτοκινήτου, αριθμό κοινωνικής ασφάλισης, αριθμό διαβατηρίου ή από ένα συνδυασμό κριτηρίων που επιτρέπουν την αναγνώρισή του περιορίζοντας το εύρος της ομάδας στην οποία ανήκει (ηλικία, επάγγελμα, τόπος διαμονής, κλπ.).

Στο πλαίσιο του ξενοδοχείου υποκείμενα των δεδομένων είναι οι πελάτες του αλλά και οι εργαζόμενοι και οι προμηθευτές τους, εφόσον είναι φυσικά πρόσωπα.

«**Επεξεργασία**» κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή.

Στην ουσία δηλ. κάθε ενέργεια που αφορά προσωπικά δεδομένα, είτε γίνεται με ηλεκτρονικά μέσα είτε όχι, συνιστά επεξεργασία προσωπικών δεδομένων.

«**Υπεύθυνος Επεξεργασίας**» το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζει τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

Κρίσιμο είναι δηλ. ποιος φορέας λαμβάνει την απόφαση για μία επεξεργασία και τον τρόπο διεξαγωγής της κι ως εκ τούτου φέρει και την ευθύνη της συμμόρφωσης και υφίσταται τις κυρώσεις και εν γένει τις συνέπειες της μη συμμόρφωσης.

Πρέπει να επισημάνουμε ότι υπεύθυνος επεξεργασίας είναι το ξενοδοχείο, όποια κι αν είναι η μορφή της επιχείρησης. Δεν είναι υπεύθυνος υπό την έννοια του νόμου όποιος π.χ. έχει την ευθύνη της λειτουργίας των πληροφοριακών συστημάτων ενός ξενοδοχείου.

"**Εκτελών επεξεργασία**" το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας.

Ο εκτελών επεξεργασία επεξεργάζεται προσωπικά δεδομένα για λογαριασμό και με βάση τις εντολές και οδηγίες του υπευθύνου.

Δεν είναι εκτελούντες οι υπάλληλοι του ξενοδοχείου. Θεωρείται όμως εκτελών το λογιστικό γραφείο, το οποίο τηρεί τα βιβλία του ξενοδοχείου ή η εταιρεία που υποστηρίζει το πρόγραμμα διαχείρισης ή τα πληροφοριακά συστήματα ενός ξενοδοχείου, εφόσον για να εκπληρώσει αυτές τις υπηρεσίες διαβιβάζονται δεδομένα των πελατών, των εργαζομένων ή των προμηθευτών ή αποκτά και πρόσβαση στα αρχεία, στα συστήματα ή στις βάσεις όπου τηρούνται τα δεδομένα αυτά. Εκτελών επεξεργασία μπορεί να είναι και μια εταιρεία ασφάλειας, εάν έχει πρόσβαση και αποθηκεύει τις λήψεις που λαμβάνονται από συστήματα βιντεοεπιτήρησης.

2. Ποιοι υποχρεούνται να εφαρμόσουν τον Κανονισμό

Η υποχρέωση εφαρμογής των ρυθμίσεων του Κανονισμού προκύπτει από το γεγονός ότι ένα ξενοδοχείο είναι εγκατεστημένο σε χώρα της ΕΕ και πιο συγκεκριμένα από το γεγονός ότι η επεξεργασία των δεδομένων γίνεται
στο πλαίσιο των δραστηριοτήτων μιας εγκατάστασης στην ΕΕ, ανεξάρτητα από το κατά πόσο η επεξεργασία πραγματοποιείται εντός της Ένωσης. Αυτό έχει ιδιαίτερη σημασία στην περίπτωση που πρόκειται για αλυσίδες ξενοδοχείων.

Σημασία δεν έχει η έδρα που δηλώνεται αλλά η ουσιαστική και πραγματική άσκηση δραστηριότητας . *Σημασία δεν έχει επίσης ο νομικός τύπος μιας ξενοδοχειακής επιχείρησης, αν πρόκειται δηλ. για μεμονωμένο ξενοδοχείο, θυγατρική, ξενοδοχείο αλυσίδας ή όχι*.
Προστατεύονται τα προσωπικά δεδομένα των προσώπων (πελατών, εργαζομένων, προμηθευτών) χωρίς να έχει σημασία η ιθαγένειά τους ή ο τόπος της μόνιμης διαμονής τους
Η υποχρέωση εφαρμογής του Κανονισμού υπάρχει ανεξάρτητα από εάν τα μέσα που χρησιμοποιούνται για την επεξεργασία είναι ηλεκτρονικά ή όχι.

3. Οι νόμιμες βάσεις της επεξεργασίας προσωπικών δεδομένων

Η επεξεργασία προσωπικών δεδομένων είναι νόμιμη μόνο εφόσον εδράζεται σε μία από τις βάσεις νομιμότητας που προβλέπει ο Κανονισμός.

"Ένα ξενοδοχείο επεξεργάζεται ή πρέπει να επεξεργάζεται δεδομένα επί τη βάσει σχεδόν όλων των προβλεπομένων νομικών βάσεων

Σύμφωνα με τον Κανονισμό επιτρέπεται η επεξεργασία

- **Συγκατάθεση**:όταν το υποκείμενο των δεδομένων, εν προκειμένω ο πελάτης δώσει τη συγκατάθεσή του για να προβεί ο ξενοδόχος στην επεξεργασία των δεδομένων του. Ωστόσο για να θεωρηθεί νόμιμη, έγκυρη και αποδεκτή η συγκατάθεση θα πρέπει να έχει τα χαρακτηριστικά που απαιτεί ο Κανονισμός. Συγκεκριμένα η συγκατάθεση θα πρέπει να είναι ελεύθερη, συγκεκριμένη, αδιαμφισβήτητη και εν πλήρη επιγνώσει (δηλ. ύστερα από ενημέρωση ….)δήλωση,

  Η συγκατάθεση θα πρέπει να παρέχεται με σαφή θετική για παράδειγμα με γραπτή δήλωση, μεταξύ άλλων με ηλεκτρονικά μέσα, ή με προφορική δήλωση. Αυτό θα μπορούσε να περιλαμβάνει τη συμπλήρωση ενός τετραγωνιδίου κατά την επίσκεψη σε διαδικτυακή ιστοσελίδα. Η σιωπή, τα προσυμπληρωμένα τετραγωνίδια ή η αδράνεια δεν θα πρέπει να εκλαμβάνονται ως συγκατάθεση.
  Ο ξενοδόχος ως υπεύθυνος επεξεργασίας θα πρέπει να είναι σε θέση να αποδείξει την ύπαρξη της συγκατάθεσης. Η συγκατάθεση δεν είναι απαραίτητο να είναι έγγραφη αλλά για λόγους σαφήνειας και απόδειξης προτείνεται αυτός ο τύπος (έγγραφο).
  Η παροχή αγαθών και υπηρεσιών δεν επιτρέπεται να εξαρτάται από την παροχή συγκατάθεσης για επεξεργασία δεδομένων, όταν η συγκατάθεση δεν είναι αναγκαία για την παροχή των αγαθών/υπηρεσιών αυτών. Π.*χ. δεν νοείται και δεν επιτρέπεται να εξαρτηθεί η κράτηση ενός δωματίου από τη συγκατάθεση για σκοπούς μάρκετινγκ.*
  Σημαντικό είναι επίσης ότι πρέπει να καθίσταται σαφές στο πρόσωπο που συγκατατέθηκε ότι μπορεί να ανακαλέσει τη συγκατάθεσή του οποτεδήποτε.

- **Σύμβαση** : όταν είναι αναγκαία για την εκπλήρωση των συμβατικών υποχρεώσεων μεταξύ ξενοδοχείου και πελατών ή π.χ. μεταξύ ξενοδοχείου

και ταξιδιωτικών γραφείων/ τουριστικών πρακτόρων.[1] *Π.χ. προφανώς ο ξενοδόχος δικαιούται ήδη επί τη βάσει της σύμβασης να συλλέγει προσωπικά δεδομένα που συνίστανται στις καταναλώσεις του πελάτη.*

-

- **Υποχρέωση από τον νόμο**: όταν στον υπεύθυνο επεξεργασίας επιβάλλεται από διάταξη νόμου, όπως π.χ. η *καταχώριση σε βιβλία πελατών επί τη βάσει αστυνομικών διατάξεων*

-

- **Έννομο συμφέρον του υπευθύνου επεξεργασίας** (ή τρίτου όταν πρόκειται για επεξεργασία που συνίσταται σε διαβίβαση σε αυτόν): Τα έννομα συμφέροντα του ξενοδόχου ως υπευθύνου επεξεργασίας, μπορεί να παρέχουν τη νομική βάση για την επεξεργασία, υπό τον όρο ότι υπερισχύουν των συμφερόντων ή των θεμελιωδών δικαιωμάτων και ελευθεριών του πελάτη (υποκειμένου των δεδομένων), λαμβάνοντας υπόψη τις θεμιτές προσδοκίες του βάσει της σχέσης που έχει με τον υπεύθυνο επεξεργασίας
  Στην περίπτωση αυτή ο ξενοδόχος επιτρέπεται να επεξεργάζεται δεδομένα που δεν είναι υπό στενή έννοια απαραίτητα για να εκτελέσει τη σύμβαση που έχει με τον πελάτη.Μία τέτοια περίπτωση υφίσταται π.χόταν ο ξενοδόχος χρησιμοποιεί συστήματα βιντεοεπιτήρησης για την προστασία αγαθών. Περίπτωση επεξεργασία που μπορεί , υπό προυποθέσεις, να θεωρηθεί ότι διενεργείται χάριν έννομου συμφέροντος είναι και η επεξεργασία δεδομένων προσωπικού χαρακτήρα για σκοπούς άμεσης εμπορικής προώθησης (directmarketing).

[1] Προφανώς η ίδια αυτή βάση συνίσταται και στην περίπτωση της επεξεργασίας προσωπικών δεδομένων των εργαζομένων στο ξενοδοχείο, αναφορικά δηλ. με την επεξεργασία προσωπικών δεδομένων για την εκπλήρωση των υποχρεώσεων και δικαιωμάτων από τη σύμβαση εργαζομένου και εργοδότη.

4. Επεξεργασία ειδικών κατηγοριών δεδομένων (ευαίσθητα δεδομένα).

Η επεξεργασία των ευαίσθητων δεδομένων (βλ. ορισμό παραπάνω) καταρχήν απαγορεύεται. Επιτρέπεται μόνο κατ' εξαίρεση και υπό ειδικές προυποθέσεις.
Αναφορικά με τη σχέση ξενοδοχείου-πελάτη ως βάση της κατ' εξαίρεση επεξεργασίας προσφέρονται κατ' ουσίαν οι ακόλουθες

- ✓ Το υποκείμενο των δεδομένων (ο πελάτης) έχει παράσχει τη ρητή συγκατάθεση (βλ παραπάνω)
- ✓ η επεξεργασία αφορά δεδομένα προσωπικού χαρακτήρα τα οποία έχουν προδήλως δημοσιοποιηθεί από το υποκείμενο των δεδομένων[*π.χ. δεδομένα γνωστά για έναν «διάσημο πελάτη» όταν ο ίδιος έχει δημοσιοποιήσει σε ευρύ κοινό π.χ. συνέντευξη ευαίσθητα προσωπικά δεδομένα αλλά αμφισβητείται η έκταση εφαρμογής αυτής της ρύθμισης στα ψηφιακά κοινωνικά δίκτυα καθώς εξαρτάται από το είδος του δικτύου, του λογαριασμού, τον αριθμό των φίλων*]
- ✓ η επεξεργασία είναι απαραίτητη για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων – *πρόκειται για την επεξεργασία προσωπικών δεδομένων εάν ένα ξενοδοχείο έχει νομικές αξιώσεις κατά ενός πελάτη ή πρέπει να αποκρούσει τις νομικές αξιώσεις αυτού*

Αναφορικά με τη σχέση ξενοδοχείου – εργαζομενου ως βάση της κατ' εξαίρεση επεξεργασίας προσφέρονται κατ' ουσίαν οι ακόλουθες

- η επεξεργασία είναι απαραίτητη για την εκτέλεση των υποχρεώσεων και την άσκηση συγκεκριμένων δικαιωμάτων του υπευθύνου επεξεργασίας ή του υποκειμένου των δεδομένων στον τομέα του εργατικού δικαίου και του δικαίου κοινωνικής ασφάλισης και κοινωνικής προστασίας, εφόσον επιτρέπεται από το δίκαιο της Ένωσης ή κράτους μέλους ή από συλλογική συμφωνία σύμφωνα με το εθνικό δίκαιο
- η επεξεργασία είναι απαραίτητη για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων ή όταν τα δικαστήρια ενεργούν υπό τη δικαιοδοτική τους ιδιότητα,
- η επεξεργασία επιβάλλεται από ρητή διάταξη ενωσιακού ή εθνικού νόμου, που – στη δεύτερη περίπτωση – θα πρέπει να κρίνεται σύμφωνος με τον Κανονισμό.
- η επεξεργασία είναι απαραίτητη για σκοπούς προληπτικής ή επαγγελματικής ιατρικής, εκτίμησης της ικανότητας προς εργασία του εργαζομένου, ιατρικής διάγνωσης, παροχής υγειονομικής ή κοινωνικής περίθαλψης ή θεραπείας ή διαχείρισης υγειονομικών και κοινωνικών συστημάτων και υπηρεσιών βάσει του ενωσιακού δικαίου ή του δικαίου της χώρας

5. Βασικές αρχές επεξεργασίας

Τα δεδομένα πρέπει υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων. *Ο ξενοδόχος π.χ. δεν θα πρέπει να καταφεύγει σε παραπλανητικές μεθόδους για να συλλέξει προσωπικά δεδομένα των πελατών του***(«νομιμότητα, αντικειμενικότητα και διαφάνεια»**).

Ο υπεύθυνος επεξεργασίας οφείλει να συλλέγει τα προσωπικά δεδομένα για καθορισμένους ρητούς και νόμιμους σκοπούς και δεν πρέπει να τα επεξεργάζεται περαιτέρω κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς(**αρχή του σκοπού**). Η συμβατότητα της περαιτέρω χρήσης είναι ποικιλη και κρίνεται κατά περίπτωση. *Κριτήριο για να κρίνει ένας ξενοδόχος αν η περαιτέρω επεξεργασία είναι συμβατή ή όχι είναι το πραγματικό πλαίσιο αλλά και οι συνέπειες που μπορεί να έχει για το πρόσωπο του πελάτη η παρέκταση των σκοπών της επεξεργασίας, η δευτερεύουσα, περαιτέρω χρήση των προσωπικών δεδομένων του ή το να διαβιβάζεται η πληροφορία σε τρίτους για διαφορετικούς σκοπούς.*
Ιδιαίτερα σημαντικό στοιχείο είναι ο σκοπός που αναφέρεται στον πελάτη-υποκείμενο των δεδομένων: εάν π.χ. *δεν έχει προβλεφθεί στους όρους και δεν ενημερωθεί ο πελάτης ότι τα δεδομένα που προκύπτουν από τη χρήση loyalty cards ενδέχεται να χρησιμοποιηθούν και για την «κατάρτιση προφίλ» και για συνακόλουθες διαφημιστικές, προωθητικές ενέργειες, τότε η χρήση αυτή θα μπορούσε να θεωρηθεί ίσως και ασύμβατη με τον αρχικό σκοπό επεξεργασίας.*

Ο Κανονισμός απαιτεί να «είναι [τα προσωπικά δεδομένα] κατάλληλα, συναφή και [να] περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία» (**αρχή της αναλογικότητας/ αρχή της ελαχιστοποίησης**).

Ήδη, κατά τη συλλογή των προσωπικών δεδομένων ο ξενοδόχος θα πρέπει να εξετάζει, εάν, ποια και πόσα δεδομένα χρειάζεται πραγματικά για τους πελάτες του και για την προσφορά των κάθε φορά συγκεκριμένων υπηρεσιών σε αυτούς. *Τα ελάχιστα δεδομένα που δικαιούται σε κάθε περίπτωση να συλλέγει και να καταγράφει ένα ξενοδοχείο (ονοματεπώνυμο, διεύθυνση, ιθαγένεια, ημερομηνίες άφιξης και αναχώρησης) προσδιορίζονται τόσο από τους όρους σύμβασης όσο και από τον νόμο (βιβλία πελατών). Εάν απαιτείται π.χ. να γνωρίζει κανείς αρκετές πληροφορίες ακόμη και για την υγεία ή την προσωπική ζωή ενός πελάτη για να του εξασφαλίσει ασφαλή και ευχάριστη διαμονή θα πρέπει να το θεμελιώσει στη συγκατάθεση του πελάτη αλλά και σε αυτήν την περίπτωση θα πρέπει να περιορίζεται στα απολύτως απαραίτητα στοιχεία. Το ίδιο ισχύει και ως προς τη χρήση προσωπικών δεδομένων για σκοπούς marketing*.

Συνεπής προς τη βασική συνιστώσα του συστήματος είναι η απαγόρευση αξιοποίησης πληροφοριών που προκύπτουν μεν από τα υπάρχοντα στοιχεία αλλά υπερβαίνουν τον συγκεκριμένο σκοπό της επεξεργασίας. *Ο αυτοπεριορισμός, σε εκπλήρωση και της νομικής υποχρέωσης εξασφαλίζει την προστασία της διακριτικότητας και της ιδιωτικότητας που πρέπει να απολαμβάνει κανείς σε ένα ξενοδοχείο, ανεξάρτητα από το μέγεθός και την κατηγορία του.*

Στις υποχρεώσεις του ξενοδόχου ως υπευθύνου επεξεργασίας είναι να φροντίζει ώστε τα προσωπικά δεδομένα να είναι ακριβή, να αποδίδουν δηλ. την πραγματικότητα, και, όταν είναι αναγκαίο, να επικαιροποιούνται (**αρχή της «ακρίβειας»**). Η ακρίβεια και η επικαιροποίηση είναι ιδιαίτερης σημασίας καθώς είναι προς το συμφέρον όλων να υπάρχει βεβαιότητα για την ορθότητα μίας πληροφορίας

Ο Κανονισμός περιλαμβάνει και την αρχή του «**περιορισμού της περιόδου αποθήκευσης»** προσδιορίζοντας ως νόμιμο χρονικό όριο διατήρησης των προσωπικών δεδομένων το διάστημα που απαιτείται για την επίτευξη των σκοπών της επεξεργασίας. Κατ' εφαρμογή και της αρχής της ελαχιστοποίησης θα πρέπει να «διασφαλίζεται ότι το διάστημα αποθήκευσης των δεδομένων προσωπικού χαρακτήρα να περιορίζεται στο ελάχιστο δυνατό». Είναι, σε κάθε περίπτωση, ο σκοπός της επεξεργασίας που προσδιορίζει το μέτρο αυτό και ενδέχεται για τα ίδια δεδομένα να προβλέπονται στον νόμο ή να απαιτούνται διαφορετικές ημερομηνίες. *Έτσι π.χ. εάν ένας πελάτης καταβάλλει το ποσό που αντιστοιχεί στις καταναλώσεις του δεν απαιτείται πλέον να τηρείται η πληροφορία αυτή. Θα πρέπει ωστόσο για λόγους φορολογικού ελέγχου να τηρηθεί το σχετικό παραστατικό.*

Ο Κανονισμός εντάσσει τη λογοδοσία στις αρχές που διέπουν την επεξεργασία των προσωπικών δεδομένων αλλά κυρίως προσδίδει σε αυτή τη λειτουργία ενός μηχανισμού εγγύησης της τήρησής τους: σύμφωνα με το άρθρο 5 παρ. 2, ο υπεύθυνος επεξεργασίας, εν προκειμένω ο ξενοδόχος φέρει την ευθύνη και είναι σε θέση να αποδείξει τη συμμόρφωση με τις αρχές της προστασίας προσωπικών δεδομένων **(αρχή της λογοδοσίας) .** Η εισαγωγή της αρχής αυτής συνδέθηκε με τον περιορισμό των διοικητικών διατυπώσεων (γνωστοποιήσεις), ερμηνευόμενη μάλιστα και ως αντιστάθμισμα της κατάργησης αυτών.

6. Η χρήση προσωπικών δεδομένων για σκοπούς διαφήμισης

Η υιοθέτηση πρακτικών άμεσης διαφήμισης από ξενοδοχεία (ανεξαρτήτως κατηγορίας και μεγέθους) γίνεται όλο και περισσότερο συνήθης και συνίσταται στην επικοινωνία με πελάτες ή και δυνητικούς πελάτες μέσω της αποστολής διαφημιστικών μηνυμάτων, newsletter, προωθητικών ενεργειών κλπ.

Όταν απευθύνεται κανείς σε προηγούμενους πελάτες θα μπορούσε υπό προϋποθέσεις να γίνει επίκληση του εννόμου συμφέροντος του ξενοδόχου (ως υπευθύνου επεξεργασίας) να αποστείλει ενημέρωση για συναφείς υπηρεσίες έστω και χωρίς συγκατάθεση (βλ. και παραπάνω). Η ερμηνεία αυτή θεμελιώνεται στη σκέψη 47 του Προοιμίου του Κανονισμού σύμφωνα με την οποία, τέτοιο έννομο συμφέρον θα μπορούσε λόγου χάρη να υπάρχει όταν υφίσταται σχετική και κατάλληλη σχέση μεταξύ του υποκειμένου των δεδομένων και του υπευθύνου επεξεργασίας, όπως αν το υποκείμενο των δεδομένων είναι πελάτης του υπευθύνου επεξεργασίας … ..Εν πάση περιπτώσει η ύπαρξη έννομου συμφέροντος θα χρειαζόταν προσεκτική αξιολόγηση, μεταξύ άλλων ως προς το κατά πόσον το υποκείμενο των δεδομένων, κατά τη χρονική στιγμή και στο πλαίσιο της συλλογής των δεδομένων προσωπικού χαρακτήρα, μπορεί εύλογα να αναμένει ότι για τον σκοπό αυτό μπορεί να πραγματοποιηθεί επεξεργασία.

Παρά το γεγονός ότι η ίδια σκέψη αναγνωρίζει ότι «η επεξεργασία δεδομένων προσωπικού χαρακτήρα για σκοπούς άμεσης εμπορικής προώθησης μπορεί να θεωρηθεί ότι διενεργείται χάριν έννομου συμφέροντος» κρίνεται σκόπιμο και από άποψη ασφάλειας προτιμότερο να επιδιώκεται εφεξής η θεμελίωση της χρήσης των στοιχείων επικοινωνίας για σκοπούς άμεσης διαφήμισης στη συγκατάθεση των πελατών,

- *είτε με αποστολή μηνυμάτων για επιβεβαίωση της βούλησής τους να εξακολουθούν να λαμβάνουν ενημερώσεις*
- *είτε με υπογραφή σχετικού εντύπου κατά προτίμηση κατά την άφιξη*.

Οι ίδιες παρατηρήσεις ισχύουν αναφορικά με τη χρήση των δεδομένων που προκύπτουν από την εγγραφή και χρήση loyaltycards που χρησιμοποιούνται συνήθως από μεγαλύτερα ξενοδοχεία ή αλυσίδες ξενοδοχείων. Για τον λόγο αυτό αλλά και προκειμένου να είναι σαφής ο σκοπός της επεξεργασίας προσωπικών δεδομένων που προκύπτουν από/ για την έκδοση loyalty card προτείνεται η επανεξέταση των διατυπώσεων συγκατάθεσης αλλά και των όρων που περιλαμβάνονται στα loyalty programs προκειμένου να διαπιστωθούν ασυνέπειες και κενά σε σχέση με τα προβλεπόμενα στον Κανονισμό.

7. Η χρήση συστημάτων βιντεοεπιτήρησης στα ξενοδοχεία

Ηχρήση συστημάτων βιντεοεπιτήρησης επεκτείνεται όλο και περισσότερο. Η χρήση τέτοιων συστημάτων, η οποία καταλήγει και σε καταγραφή προσωπικών δεδομένων (εικόνας) υπόκειται στις προυποθέσεις που ορίζει ο Κανονισμός και πρέπει να πραγματοποιείται με βάση τις αρχές επεξεργασίας που αυτός υιοθετεί.

Ο Κανονισμός δεν περιέχει ειδικές ρυθμίσεις για τη λεγόμενη βιντεοεπιτήρηση αλλά καθώς πρόκειται για συλλογή και επεξεργασία προσωπικών δεδομένων εικόνας (ή και ήχου) εφαρμόζονται οι γενικοί κανόνες.

Εν γένει, γίνεται αποδεκτή η χρήση τέτοιων συστημάτων για σκοπούς προστασίας προσώπων και αγαθών αλλά θα πρέπει να λαμβάνεται υπόψη κυρίως η αρχή της αναλογικότητας – ελαχιστοποίησης.

Η Αρχή Προστασίας Προσωπικών Δεδομένων είχε - υπό το καθεστώς της εφαρμογής του ν. 2472/97 – εκδώσει την Οδηγία 1/2011 Χρήση συστημάτωνβιντεοεπιτήρησης για την προστασία προσώπων και αγαθών , στην οποία περιλαμβάνεται ειδικό άρθρο για τη λειτουργεία συστημάτων βιντεοεπιτήρησης σε ξενοδοχεία. [2] Αν και α) δεν είναι σαφής η ισχύς της Οδηγίας αυτής μετά την 25ηΜαίου 2018 και β) στο προσχέδιο εθνικού νόμου περιλαμβάνεται ειδικό άρθροκρίνεται σκόπιμη η αναφορά στην ως άνω Οδηγία της ΑΠΔΠΧ γιατί δηλώνει την προσέγγισή της στο όλο θέμα και συνεπώς θα πρέπει να ληφθεί υπόψη στο πλαίσιο της συμμόρφωσης.

[2] *Άρθρο 17 Ξενοδοχεία*

1. Η λειτουργία συστημάτωνβιντεοεπιτήρησης σε ξενοδοχειακές μονάδες υπό οποιαδήποτε μορφή (ξενοδοχεία, πανσιόν, ενοικιαζόμεναδωμάτια κλπ.) πρέπει να περιορίζεται αποκλειστικά σε χώρους που αποσκοπούν στον έλεγχο εισερχομένων/εξερχομένων (όπως π.χ. η κεντρική είσοδος, ο χώρος υποδοχής, οι είσοδοι/έξοδοι των ανελκυστήρων και των κλιμακοστασίων)καθώς και στους χώρους φύλαξης χρημάτων (π.χ. ταμεία) και στις ηλεκτρομηχανολογικές εγκαταστάσεις.

2. Δεν επιτρέπεται η τοποθέτηση καμερών στους χώρους εστίασης και στους διαδρόμους που οδηγούν στα δωμάτια του ξενοδοχείου και σε χώρους όπου ενδέχεται να παρακολουθούνται οι πελάτες ή/και επισκέπτες του ξενοδοχείου. Τέτοιοι χώροι είναι ιδίως οι είσοδοι των κατ' ιδίαν δωματίων, οι τουαλέτες και οι χώροι όπου πραγματοποιούνται δραστηριότητες αναψυχής (όπως πισίνες, γυμναστήρια, χώροι άθλησης, αποδυτήρια κλπ.)

8. Τα δικαιώματα των προσώπων

Ο Κανονισμός ενισχύει τα δικαιώματα των προσώπων που προβλεπόταν στο προισχύσαν δίκαιο και εισάγει και νέα. Καταρχήν προσδιορίζει ένα πλαίσιο γενικών αρχών και διαδικαστικών όρων που επιβάλλεται να τηρεί ο υπεύθυνος επεξεργασία προκειμένου να καταστήσει εφικτή και αποτελεσματική την άσκηση των δικαιωμάτων. Οι σχετικές ρυθμίσεις (άρθρο 12) αναφέρονται σε μία γενική υποχρέωση ενημέρωσης και παροχής πληροφοριών[3] που είναι αναγκαίες για την άσκηση των δικαιωμάτων (άρθρα 13-22), την υποχρέωση της διευκόλυνσης της άσκησής τους, την υποχρέωση ενημέρωσης για την πορεία του αιτήματος και την ανταπόκριση του υπεύθυνου επεξεργασίας αλλά και τα δικαιώματα του υποκειμένου, εφόσον ο υπεύθυνος επεξεργασίας δεν ανταποκριθεί στο αίτημα (υποβολή καταγγελίας στην ανεξάρτητη αρχή, δικαστική προσφυγή κλπ.).

Ο Κανονισμός εισάγει ως κανόνα την άσκηση των δικαιωμάτων ατελώς, προβλέποντας ωστόσο σε περίπτωση προφανώς αβασίμων ή υπερβολικών αιτημάτων την ευχέρεια του υπεύθυνου επεξεργασίας είτε να ζητήσει την καταβολή ευλόγου τέλους είτε να μην ασχοληθεί με το αίτημα.

Δικαίωμα πρόσβασηςΟ Κανονισμός προβλέπει το δικαίωμα ενός προσώπου να ζητά επιβεβαίωση για το κατά πόσον ή όχι τα προσωπικά δεδομένα έχουν αποτελέσει αντικείμενο επεξεργασίας και, εάν συμβαίνει τούτο, την πρόσβαση στα δεδομένα προσωπικού χαρακτήρα και σε πληροφορίες που αφορούν τους σκοπούς επεξεργασίας, τις κατηγορίες δεδομένων, τους αποδέκτες κ.α. Ρητά προβλέπεται μάλιστα η υποχρέωση παροχής αντιγράφου, η οποία δεν αναγνωριζόταν υπό το προισχύσαν νομοθετικό καθεστώς. *Κατά την ικανοποίηση αυτού του δικαιώματος ένα ξενοδοχείο θα πρέπει να λάβει υπόψη του ότι ένα τέτοιο δικαίωμα μπορεί να ασκείται κυρίως εξ' αποστάσεως και να τεθούν ζητήματα ως προς την ταυτοποίηση του αιτούντος και τον τρόπο ανταπόκρισης στο αίτημα με ασφάλεια.* Το δικαίωμα πρόσβασης συνοδεύεται από σειρά άλλων δικαιωμάτων

Το **δικαίωμα διόρθωσης** και επικαιροποίησης ανακριβών προσωπικών δεδομένων αλλά και τη συμπλήρωση ελλιπών προσωπικών δεδομένων.

[3]Ο ΓΚΠΔ αναφέρεται και στον τρόπο παροχής των πληροφοριών: «…..σε συνοπτική, διαφανή, κατανοητή και εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή διατύπωση, ιδίως όταν πρόκειται για πληροφορία απευθυνόμενη ειδικά σε παιδιά. Οι πληροφορίες μπορούν να παρέχονται γραπτώς ή με άλλα μέσα, μεταξύ άλλων, εφόσον ενδείκνυται, ηλεκτρονικώς..» (άρθρο 12 παρ. 1). Οι πληροφορίες μπορούν επίσης να παρέχονται «σε συνδυασμό με τυποποιημένα εικονίδια προκειμένου να δίνεται με ευδιάκριτο, κατανοητό και ευανάγνωστο τρόπο μια ουσιαστική επισκόπηση της σκοπούμενης επεξεργασίας.

Πρόκειται για δικαίωμα σύστοιχο της αρχής της ακρίβειας των προσωπικών δεδομένων

Το **δικαίωμα διαγραφής**, εφόσον τα δεδομένα δεν είναι πλέον απαραίτητα ή το υποκείμενο των δεδομένων (ο πελάτης) έχει ανακαλέσει τη συγκατάθεσή του ή έχει εναντιωθεί στην επεξεργασία, έχουν υποβληθεί παράνομα σε επεξεργασία ή η διαγραφή τους προβλέπεται από τον νόμο.

Το **δικαίωμα εναντίωσης** σημαίνει ότι ένα πρόσωπο, ένας πελάτης π.χ. δικαιούται να αντιτάσσεται, ανά πάσα στιγμή και για λόγους που σχετίζονται με την ιδιαίτερη κατάστασή του, στην επεξεργασία των προσωπικών δεδομένων του, η οποία βασίζεται σε λόγους που αφορούν μεταξύ άλλων, την ικανοποίηση εννόμου συμφέροντος του υπευθύνου επεξεργασία. *Εν προκειμένω, ο ξενοδόχος ως υπεύθυνος επεξεργασίας φέρει το βάρος να αποδείξει ότι υπάρχουν επιτακτικοί, νόμιμοι λόγοι για την επεξεργασία που υπερισχύουν των συμφερόντων, των δικαιωμάτων και των ελευθεριών του προσώπου που εναντιώθηκε και συνεπώς θα συνεχίζουν τηνεπεξεργασία. Ένα πρόσωπο δικαιούται να αντιταχθεί στην εν λόγω επεξεργασία, συμπεριλαμβανομένης της κατάρτισης προφίλ στον βαθμό που αυτή συνδέεται με την εν λόγω απευθείας εμπορική προώθηση, είτε πρόκειται για αρχική είτε για περαιτέρω επεξεργασία, ανά πάσα στιγμή και χωρίς χρέωση και εν προκειμένω ο ξενοδόχος ως υπεύθυνος επεξεργασίας θα πρέπει να συμμορφωθεί σε κάθε περίπτωση*.

Το δικαίωμα περιορισμού της επεξεργασίας, δηλ. η επισήμανση αποθηκευμένων δεδομένων προσωπικού χαρακτήρα με στόχο τον περιορισμό της επεξεργασίας τους στο μέλλον, αντιστοιχεί σε ένα δικαίωμα μερικής ή προσωρινής εναντίωσης αλλά ταυτόχρονα έχει χαρακτηριστικά «ασφαλιστικών μέτρων», καθώς το υποκείμενο των δεδομένων μπορεί να παρεμβαίνει αναστέλλοντας την επεξεργασία των δεδομένων του, εάν εκκρεμεί η επαλήθευση της ακρίβειας αυτών ή και της ίδιας της νομιμότητας της επεξεργασίας.

Το δικαίωμα στη φορητότητα των δεδομένων που συνίσταται στο δικαίωμα του προσώπου να λαμβάνει δεδομένα που έχει παράσχει σε υπεύθυνο επεξεργασίας και το δικαίωμα να διαβιβάζει τα δεδομένα του σε άλλον υπεύθυνο επεξεργασίας, χωρίς να εμποδίζεται σε αυτό από τον υπεύθυνο επεξεργασίας στον οποίο παρασχέθηκαν. Μπορεί δηλ. να αιτηθεί τη διαβίβαση προσωπικών δεδομένων σε άλλον Υπεύθυνο Επεξεργασίας σε δομημένη, ευρέως χρησιμοποιούμενη και μηχανικά αναγνώσιμη μορφή. Το δικαίωμα περιορίζεται στις περιπτώσεις που η επεξεργασία θεμελιώνεται στη συγκατάθεση του προσώπου ή σε μία συμβατική σχέση με αυτό.

Το Δικαίωμα εναντίωσης στην αυτοματοποιημένη λήψη αποφάσεων, συμπεριλαμβανόμενης της κατάρτισης προφίλ. Ένα πρόσωπο έχει δικαίωμα να διατυπώσει αντιρρήσεις και να μην υπόκειται σε μία απόφαση, όταν αυτή απόφαση βασίζεται αποκλειστικά σε αυτοματοποιημένη επεξεργασία, συμπεριλαμβανομένης της κατάρτισης προφίλ, και η απόφαση αυτή παράγει έννομα αποτελέσματα ή επηρεάζει σημαντικά το υποκείμενο των δεδομένων. Ο Κανονισμός αποδέχεται πάντως, υπό την αίρεση εγγυήσεων («κατάλληλων μέτρων») και την αυτοματοποιημένη λήψη ατομικής απόφασης, συμπεριλαμβανομένης της κατάρτισης προφίλ, και αναφορικά με τις ειδικές κατηγορίες δεδομένων (ευαίσθητα), εάν η επεξεργασία θεμελιώνεται στη ρητή συγκατάθεσητου προσώπου. Ο Κανονισμός προβλέπει το δικαίωμα να ζητείται η ανθρώπινη παρέμβαση στην επεξεργασία δεδομένων προσωπικού χαρακτήρα. *Το δικαίωμα αυτό ενδέχεται να απασχολήσει ένα ξενοδοχείο συνήθως σε σχέση με την κατάρτιση προφίλ ενός πελάτη, ιδίως στο πλαίσιο της χρήσης προγραμμάτων loyalty.*

9. Νέες υποχρεώσεις του υπευθύνου επεξεργασίας

Στο πλαίσιο της συμμόρφωσης οι υπεύθυνοι επεξεργασίας έχουν μία γενική υποχρέωση να «επιδείξουν αποτελέσματα», να επιδείξουν και να αποδείξουν συμμόρφωση, αλλά διατηρούν μία ελευθερία ως προς τον προσδιορισμό των ειδικότερων μέσων.

Τα μέτρα οργάνωσης κι επίδειξης της συμμόρφωσης συμπεριλαμβάνουν: α) την εκτίμηση αντικτύπου (της επεξεργασίας) στην προστασία δεδομένων (άρθρα 35), β) την προηγούμενη διαβούλευση (άρθρο 36) και τη συνεργασία με την ανεξάρτητη αρχή, γ) την υιοθέτηση κωδίκων δεοντολογίας και μηχανισμών πιστοποίησης (άρθρα 40-43), δ) τον ορισμό υπεύθυνου προστασίας δεδομένων (άρθρα 37-39), ε) την τήρηση αρχείων επεξεργασίας (άρθρο 30), Η συμμόρφωση προς αυτές τις υποχρεώσεις θα πρέπει να επιδιώκεται και να διασφαλίζεται με την υιοθέτηση διαφανών εσωτερικών πολιτικών προστασίας δεδομένων, την εφαρμογή και τη διαρκή επανεξέτασή τους.
Σημαντική σημείωση : οι νέες αυτές απαιτήσεις δεν είναι υποχρεωτικές για όλους. Η υπαγωγή σε διάφορες υποχρεώσεις να εξαρτάται από το είδος της επεξεργασίας και την κλίμακα του κινδύνου για τα δικαιώματα.

Εκτίμηση επιπτώσεων/αντικτύπου στην προστασία προσωπικών δεδομένων

Η εκτίμηση επιπτώσεων/αντικτύπου της επεξεργασίας στην προστασία προσωπικών δεδομένων εισήχθη ως υποκατάστατο κι αντίβαρο της κατάργησης των γενικών υποχρεώσεων γνωστοποίησης της επεξεργασίας στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Ο Κανονισμός επιτάσσει την εκτίμηση αντικτύπου, εφόσον ο υπεύθυνος επεξεργασίας κρίνει ότι συντρέχει «υψηλός κίνδυνος» για τα δικαιώματα των προσώπων και ιδίως για την προστασία των δεδομένων τους, κίνδυνος που προκύπτει αναφορικά με «ένα είδος επεξεργασίας, ιδίως με χρήση νέων τεχνολογιών».Τέτοια περίπτωση θα μπορούσε να είναι π.χ. η εγκατάσταση αισθητήρων (sensors) στα δωμάτια (smartrooms-hotels) από τη χρήση των οποίων ωστόσο θα μπορούσαν να συναχθούν συμπεράσματα για τις συνήθειες των ενοίκων.

Η διενέργεια εκτίμησης αντικτύπου απαιτείται ιδίως όταν πρόκειται για α) συστηματική και εκτενή αξιολόγηση προσωπικών πτυχών (profiling), β) μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων (ευαίσθητα) ή δεδομένων που αφορούν ποινικές καταδίκες, αδικήματα και μέτρα ασφαλείας, γ) συστηματική παρακολούθηση δημοσίως προσβάσιμων χώρων σε μεγάλη κλίμακα.
Αν υπάρχει υψηλός κίνδυνος πρέπει να το αξιολογεί ο υπεύθυνος επεξεργασίας, εν προκειμένω ο ξενοδόχος, αλλά η Αρχή Προστασίας Δεδομένων Προσωπικού

Χαρακτήρα μπορεί να αξιολογεί και να αναθεωρεί την εκτίμηση που έχει κάνει ο υπεύθυνος επεξεργασίας και να ζητήσει πρόσθετες εγγυήσεις και μέτρα, αν φρονεί ότι ο υπεύθυνος επεξεργασίας «δεν έχει προσδιορίσει ή μετριάσει επαρκώς τον κίνδυνο».

Το ελάχιστο περιεχόμενο» μιας εκτίμησης αντικτύπου, που πρέπει να διενεργείται πριν από μία επεξεργασία (εν γένει κι όχι κάθε μεμονωμένη πράξη επεξεργασίας) είναι α) η συστηματική περιγραφή των προβλεπόμενων πράξεων επεξεργασίας και των σκοπών της επεξεργασίας, β) η εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας σε συνάρτηση με τους σκοπούς που επιδιώκονται , γ) η εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων δ) τα προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων, περιλαμβανομένων των εγγυήσεων, των μέτρων και μηχανισμών ασφάλειας.

Συνεπώς η εκτίμηση αντικτύπου δεν απαιτείται πάντα αλλά πρέπει να κρίνεται κατά περίπτωση και οπωσδήποτε να τεκμηριώνεται στην ύπαρξη κινδύνου για τα πρόσωπα και δεν συναρτάται απαραίτητα με το μέγεθος ή την κατηγοριοποίηση μίας μονάδας. Μεγάλες ξενοδοχειακές μονάδες ή αλυσίδες που προβαίνουν π.χ. σε profiling των πελατών ιδίως μέσω της χρήσης των loyaltyprograms/ cardsθα πρέπει να κάνουν προεκτίμηση αν πρέπει να προβούν σε εκτίμηση αντικτύπου. Το ίδιο ισχύει και για την περίπτωση μονάδων που – ενδεχομένως ανεξάρτητα με το μέγεθός τους – συνδυάζουν τη λειτουργία τους με επεξεργασία ειδικών κατηγοριών δεδομένων (ευαίσθητα), όπως π.χ. ιαματικός τουρισμός.

Ο Υπεύθυνος Προστασίας Δεδομένων – DataProtectionOfficer (DPO)

Ο Γενικός Κανονισμός για την Προστασία Δεδομένων εισάγει για πρώτη φορά αναλυτικές διατάξεις για τον ρόλο, τις παρεχόμενες εγγυήσεις και τα καθήκοντα του Υπευθύνου Προστασίας Δεδομένων, ο οποίος βρίσκεται πλέον στο επίκεντρο του νέου νομικού πλαισίου.

Το θέμα του Υπευθύνου Προστασίας Δεδομένων έγινε κεντρικό θέμα συζήτησης σε τέτοιο βαθμό που να θεωρείται συνώνυμο του Κανονισμού ή το μείζον ζήτημα αυτού. Θα πρέπει να διευκρινιστεί εξαρχής
α) ο ορισμός Υπευθύνου Προστασίας Δεδομένων είναι υποχρεωτικός στις περιπτώσεις που ορίζει ο Κανονισμός και όχι γενικά
β) με τον ορισμό Υπευθύνου Προστασίας Δεδομένων δεν σημαίνει ότι υπάρχει και εξ ορισμού συμμόρφωση με τον Κανονισμό ή ότι εκεί εξαντλείται η συμμόρφωση

Υποχρέωση να οριστεί Υπεύθυνος Προστασίας Δεδομένων υπάρχει

- Όταν η επεξεργασία διενεργείται από Δημόσια αρχή ή φορέα,
- Όταν οι βασικές ("core") δραστηριότητες του υπευθύνου επεξεργασίας συνιστούν ή απαιτούν τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε μεγάλη κλίμακα ή μεγάλης κλίμακας επεξεργασίας ειδικών κατηγοριών (ευαίσθητων) δεδομένων

Ο υπεύθυνος Προστασίας Δεδομένων

Αποτελεί «δίαυλο» (σημείο επικοινωνίας) μεταξύ της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα για ζητήματα επεξεργασίας δεδομένων, προηγούμενης διαβούλευσης με την Αρχή, άλλες διαβουλεύσεις ή λήψη συμβουλών.

● Παρέχει συμβουλές, γνωμοδοτήσεις και ενημέρωση σχετικά με την συμμόρφωση προς τον Κανονισμό και την τήρηση της νομοθεσίας για τα προσωπικά δεδομένα αλλά και τις πολιτικές του οργανισμού (ανάθεση αρμοδιοτήτων, ευαισθητοποίηση, επιμόρφωση-κατάρτιση υπαλλήλων, έλεγχοι)

●Παρακολουθεί την συμμόρφωση με τον Κανονισμό και την εθνική νομοθεσία

●Παρέχει συμβουλές αναφορικά με την διενέργεια εκτίμησης αντικτύπου (PIA) και λαμβάνει υπόψη του τον κίνδυνο επεξεργασίας.

Όπως σημειώνει Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα σημειώνει, «ο Υπεύθυνος Προστασίας Δεδομένων **(**DPO) διευκολύνει τη συμμόρφωση του υπευθύνου επεξεργασίας και του εκτελούντος την επεξεργασία με τις διατάξεις του ΓΚΠΔ και μεσολαβεί μεταξύ των διαφόρων ενδιαφερομένων (π.χ. εποπτικές αρχές, υποκείμενα των δεδομένων). Ο ρόλος του είναι συμβουλευτικός και όχι αποφασιστικός. Ο Υπεύθυνος Προστασίας Δεδομένων δεν φέρει προσωπική ευθύνη για τη μη συμμόρφωση με τον Κανονισμό. Υπεύθυνος να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τον ΓΚΠΔ είναι ο **υπεύθυνος επεξεργασίας** ή ο **εκτελών την επεξεργασία**.»

Κάθε ξενοδοχειακή μονάδα θα πρέπει να εξετάσει εάν εμπίπτει στις περιπτώσεις για τις οποίες ο Κανονισμός προβλέπει υποχρεωτικά τον ορισμό υπευθύνου. Στη μεγάλη πλειοψηφία των περιπτώσεων μία ξενοδοχειακή μονάδα δεν χρειάζεται να ορίσει. Ωστόσο μπορεί να θεωρηθεί ως καλή πρακτική καθώς μπορεί να υποστηρίξει τη συμμόρφωση ιδίως σε αυτήν την πρώτη περίοδο προσαρμογής στη νέα νομοθεσία.

Ο Υπεύθυνος Προστασίας Δεδομένων μπορεί να είναι είτε εργαζόμενος της επιχείρησης (σύμβαση εργασίας), είτε να παρέχει ανεξάρτητες υπηρεσίες ως εξωτερικός συνεργάτης. Σε περίπτωση που παρέχει ανεξάρτητες υπηρεσίες σε περισσότερες από μια επιχειρήσεις θα πρέπει αφενός να διαθέτει τον αναγκαίο χρόνο για την παροχή των υπηρεσιών σε όλες τις επιχειρήσεις και αφετέρου να αποφεύγει τυχόν σύγκρουση συμφερόντων, όταν παρέχει υπηρεσίες σε ανταγωνιστικές επιχειρήσεις.

Ένας όμιλος μπορεί να ορίσει κοινό υπεύθυνο. Ένας ξενοδοχειακός όμιλος μπορεί να ορίσει ένα μόνο υπεύθυνο προστασίας δεδομένων, με μοναδική προϋπόθεση ότι κάθε εγκατάσταση έχει εύκολη πρόσβαση στον υπεύθυνο προστασίας δεδομένων, ότι θα μπορεί δηλ. να λειτουργήσει ως σημείο επαφής για την Αρχή Προστασίας Δεδομένων και τα υποκείμενα των δεδομένων (πελάτες, προμηθευτές, εργαζόμενοι) και να παρέχει συμβουλευτικές και υποστηρικτικές υπηρεσίες.

Ο Υπεύθυνος Προστασίας Δεδομένων πρέπει να επιλέγεται βάσει της γνώσεών του στον τομέα του δικαίου και των πρακτικών περί προστασίας δεδομένων, καθώς και βάση της ικανότητας να εκπληρώνει τα καθήκοντα που περιγράφει ο Κανονισμός και του έχουν ανατεθεί. Σύμφωνα με ανακοίνωση της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα ο Κανονισμός δεν θέτει κάποια υποχρεωτική απαίτηση για πιστοποίηση του Υπευθύνου Προστασίας Δεδομένων, ούτε καν ενθαρρύνει σχετική πιστοποίηση σε προαιρετική βάση. Συνεπώς δεν απαιτείται να είναι «πιστοποιημένος» ένας «DPO». Πρέπει όμως να αποδεικνύει τυχόν εκπαίδευση, γνώσεις και εμπειρία.

Σύμφωνα και με τη Σύσταση των αρχών ελέγχου τα στοιχεία επικοινωνίας του Υπευθύνου Προστασίας Δεδομένων πρέπει να δημοσιοποιούνται. Επιπλέον, προβλέπεται υποχρέωση για τον υπεύθυνο και εκτελούντα την επεξεργασία να ανακοινώνουν στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα στοιχεία που αφορούν στον ορισμό του υπευθύνου προστασίας δεδομένων. Στο πλαίσιο αυτό η Αρχή έχει αναρτήσει στην ιστοσελίδα της **ειδικό έντυπο**, το οποίο καλούνται να συμπληρώνουν οι υπεύθυνοι και εκτελούντες την επεξεργασία προκειμένου να ανακοινώσουν στην Αρχή τον ορισμό του υπευθύνου προστασίας σύμφωνα με την προαναφερθείσα υποχρέωσή τους.

Το έντυπο πρέπει να αποσταλεί ηλεκτρονικά στη διεύθυνση

dpo-announcement@dpa.gr

Όπως επισημαίνει η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα στην ανακοίνωση της 25 Μαίου 2018, η υποχρέωση ανακοίνωσης ορισμού DPO ικανοποιείται ΜΟΝΟ με την υποβολή του συγκεκριμένου εντύπου. Οποιαδήποτε

προηγούμενη (πριν την 25η Μαΐου 2018) δήλωση στοιχείων υπευθύνου προστασίας δεδομένων που έχει υποβληθεί στην Αρχή δεν λαμβάνεται υπόψη.

Αρχεία Επεξεργασίας

Μία επιπλέον υποχρέωση του Υπεύθυνου Επεξεργασίας είναι η τήρηση αρχείου στο οποίο καταγράφονται οι δραστηριότητες επεξεργασίας για τις οποίες είναι υπεύθυνος. Το αρχείο πρέπει να περιλαμβάνει:

Όνομα και στοιχεία επικοινωνίας υπεύθυνου επεξεργασίας, εκπροσώπου και Υπευθύνου Προστασίας Δεδομένων, εάν έχει οριστεί

Σκοπούς επεξεργασίας

Κατηγορίες υποκειμένων δεδομένων (π.χ. πελάτες, προμηθευτές, εργαζόμενοι)

Κατηγορίες αποδεκτών στους οποίους γνωστοποιούνται τα δεδομένα

Διαβιβάσεις σε τρίτες χώρες ή διεθνείς οργανισμούς

Προβλεπόμενες προθεσμίες διαγραφής

Τεχνικά και οργανωτικά μέτρα ασφάλειας

Προβλέπεται παρέκκλιση από αυτήν την υποχρέωση για επιχειρήσεις ή οργανισμούς που απασχολούν λιγότερα από 250 άτομα.

Ωστόσο, η παρέκκλιση που προβλέπεται δεν είναι απόλυτη καθώς όταν συντρέχουν οι παρακάτω περιπτώσεις δεν εφαρμόζεται η εξαίρεση

- Επεξεργασία που ενδέχεται να έχει ως αποτέλεσμα κίνδυνο για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων.
- Επεξεργασία που δεν είναι περιστασιακή.
- Επεξεργασία που περιλαμβάνει ειδικές κατηγορίες δεδομένων ή προσωπικά δεδομένα που αφορούν σε ποινικές καταδίκες και αδικήματα.

Συνεπώς, όταν από ένα ξενοδοχείο π.χ.που εστιάζει σε ιαματικό ή θρησκευτικό τουρισμό γίνεται επεξεργασία δεδομένων υγείας ή θρησκευτικών πεποιθήσεων, που εμπίπτουν στην κατηγορία των ειδικών κατηγοριών δεδομένων, δεν ισχύει η παρέκκλιση, επιβάλλεται δηλ. η τήρηση αρχείου επεξεργασίας, ακόμη και εάν ο υπεύθυνος επεξεργασίας απασχολεί λιγότερα από 250 άτομα.

10. Λήψη μέτρων ασφαλείας δεδομένων και οι υποχρεώσεις ανακοίνωσης παραβιάσεων

Ο πολλαπλασιασμός των επιθέσεων με στόχους πληροφοριακά συστήματα αλλά και - είτε αυτοτελώς, είτε ως «παράπλευρη απώλεια» - προσωπικά δεδομένα που σημειώνεται τα τελευταία χρόνια ανέδειξε το ζήτημα και το αίτημα της ασφάλειας των δεδομένων.
Η ασφάλεια των δεδομένων (και αντίστοιχα του πληροφοριακού συστήματος) είναι σύνθετη έννοια: προϋποθέτει - και ταυτόχρονα συνίσταται σε - ένα οργανωμένο πλαίσιο από έννοιες, αντιλήψεις, αρχές, πολιτικές, διαδικασίες, τεχνικές και μέτρα που απαιτούνται για να προστατευτούν τα στοιχεία ενός πληροφοριακού συστήματος. *Η ασφάλεια των δεδομένων δεν απειλείται μόνο από τον χάκερ αλλά και από την αμελή αντιμετώπιση των δεδομένων από έναν ξενοδόχοι που επιτρέπει π.χ. σε έναν πελάτη να δει ή και πάρει τα δεδομένα άλλου πελάτη, τον αμελή ή κακόβουλο εργαζομένο που ανακοινώνει σε τρίτα πρόσωπα όσα μαθαίνει σε ένα ξενοδοχείο για τους πελάτες.*

Ειδικότερα ο υπεύθυνος επεξεργασίας όφειλε να εξασφαλίζει επίπεδο ασφάλειας ανάλογο προς τους κινδύνους που συνεπάγονται η επεξεργασία και η φύση των δεδομένων. Είναι προφανές ότι ευαίσθητα δεδομένα, στοιχεία πιστωτικών καρτών, οικονομικά στοιχεία πρέπει να προστατεύονται με ενισχυμένο τρόπο. Τα μέτρα πρέπει να είναι τέτοια ώστε να προστατεύονται τα δεδομένα από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας.

"Ένα βασικό μέτρο είναι η υπόδειξη προς τους εργαζόμενους σε ένα ξενοδοχείο ότι όχι μόνο οφείλουν να τηρούν εχεμύθεια για ό,τι πληροφορούνται στο πλαίσιο της εκτέλεσης της εργασίας τους ή επ' ευκαιρία αυτής αλλά ότι η τήρηση εχεμύθειας είναι νομική υποχρέωση και η παραβίασή της σημαίνει ευθύνη και για το ξενοδοχείο και για τον εργαζόμενο. Η λήψη τέτοιων μέτρων που μπορεί να ξεκινούν από το κλείδωμα ενός φοριαμού όπου φυλάσσονται τα αρχεία (ή τον ορισμό κωδικών για την πρόσβαση στο ηλεκτρονικό αρχείο) και να φτάνουν ως την κρυπτογράφηση των δεδομένων είναι νομική υποχρέωση του ξενοδόχου ως υπευθύνου επεξεργασίας και η παραβίασή της συνεπάγεται κυρώσεις, όπως πρόστιμα ή και αστική ευθύνη (για αποζημίωση του πελάτη τα δεδομένα του οποίου π.χ. διέρρευσαν λόγω ελλιπών μέτρων ασφαλείας του ξενοδοχείου.

Στις υποχρεώσεις που σχετίζονται με την ασφάλεια προστίθεται η υποχρέωση του υπευθύνου επεξεργασίας να γνωστοποιεί την παραβίαση (ασφάλειας) προσωπικών δεδομένων στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Ο Κανονισμός ορίζει ως παραβίαση της ασφάλειας (αυτή) που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας

κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία. Η γνωστοποίηση στην Αρχή πρέπει να αμελλητί, δηλ. χωρίς υπαίτια καθυστέρηση και θέτοντας ως ενδεικτικό ορόσημο τις 72 ώρες από τη στιγμή που ο υπεύθυνος επεξεργασίας αποκτά γνώση του γεγονότος. Γνωστοποίηση στην εποπτική αρχή δεν απαιτείται, «εάν η παραβίαση δεδομένων προσωπικού χαρακτήρα δεν ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων». Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα επισημαίνει ότι ακόμα και αν το περιστατικό δεν μπορεί να προκαλέσει κίνδυνο για τα φυσικά πρόσωπα που αφορά, ο υπεύθυνος επεξεργασίας οφείλει σε κάθε περίπτωση να τηρεί δικό του εσωτερικό σχετικό αρχείο.

Στις 25 Μαίου 2018 η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα ανήρτησε στον ιστότοπό της (www.dpa.gr) πληροφορίες και οδηγίες για τη γνωστοποίηση περιστατικών παραβίασης ασφάλειας. Σημειώνει ότι η γνωστοποίηση πρέπει να περιέχει σύνολο σχετικών πληροφοριών (φύση/έκταση του περιστατικού, κατηγορίες προσώπων που επλήγησαν, αιτία και συνέπειες αυτού, ενέργειες που έγιναν προς αντιμετώπισή του, κ.ά.)[4]. Στον ίδιο ιστότοπο δίνεται η δυνατότητα ηλεκτρονικής υποβολής της γνωστοποίησης.

Ο Κανονισμός απαιτεί αντίστοιχη ανακοίνωση της παραβίασης δεδομένων στα πρόσωπα, τα οποία θίγονται από την παραβίαση δεδομένων . Η υποχρέωση υπάρχει σε περίπτωση ύπαρξης «υψηλού κινδύνου» για τα δικαιώματα και τις ελευθερίες των προσώπων, των οποίων παραβιάζονται τα δεδομένα. Οι πληροφορίες που πρέπει να ανακοινωθούν, με εξαίρεση αυτές που αφορούν τη φύση της παραβίασης και τους κατά προσέγγιση αριθμούς των παραβιασθέντων αρχείων και των θιγομένων προσώπων, ταυτίζονται με αυτές που γνωστοποιούνται στην Αρχή. Ο βασικός σκοπός της ανακοίνωσης είναι η παροχή ειδικής ενημέρωσης αναφορικά με τα μέτρα που πρέπει να λάβουν τα υποκείμενα των δεδομένων προκειμένου να αυτοπροστατευτούν (π.χ. σύσταση για αλλαγή κωδικών).

Η παράλειψη της γνωστοποίησης μιας παραβίασης στην Αρχή ή/και της ανακοίνωσης στα υποκείμενα των δεδομένων συνιστά παράβαση του Κανονισμού που ενεργοποιεί τη δυνατότητα της Αρχής να επιβάλλει

[4] Ακόμα και αν οι σχετικές αυτές πληροφορίες δεν είναι όλες διαθέσιμες κατά την υποβολή της γνωστοποίησης, αυτή θα πρέπει να υποβληθεί ως αρχική και να ακολουθήσει στο μέλλον, χωρίς αδικαιολόγητη καθυστέρηση, επικαιροποίησή της (με υποβολή συμπληρωματικής γνωστοποίησης

διορθωτικά μέτρα (π.χ. να υποχρεώσει να γίνει ανακοίνωση στα υποκείμενα) και ταυτόχρονα να επιβάλει πρόστιμα. Επίσης αν υπάρξει τέτοια παράλειψη και υπάρξει βλάβη των προσώπων επειδή δεν είχαν την ευκαιρία να λάβουν μέτρα για να προστατευτούν μπορεί να θέσει ζήτημα ευθύνης για αποζημίωση.

11. Οι σχέσεις με τους εκτελούντες επεξεργασία

Είναι ενδεχόμενο η επεξεργασία προσωπικών δεδομένων ή μέρος αυτής να διεξάγεται από τρίτα νομικά ή φυσικά πρόσωπα. Η επεξεργασία αυτή μπορεί να προκύπτει ως προυπόθεση ή αποτέλεσμα στο πλαισιο της άσκησης μίας δραστηριότητας, η οποία έχει ανατεθεί σε αυτά τα πρόσωπα. Αυτά τα πρόσωπα στα οποία δεν συμπεριλαμβάνονται οι εργαζόμενοι του υπευθύνου επεξεργασίας χαρακτηρίζονται ως εκτελούντες επεξεργασία.

Στο πλαίσιο μίας ξενοδοχειακής επιχείρησης κατηγορίες εκτελούντων επεξεργασία είναι π.χ. εταιρίες που αναλαμβάνουν την υποστήριξη λογιστηρίου ή τη μισθοδοσία προσωπικού, εργασίες ψηφιακής υποστήριξη, υπηρεσίες μάρκετινγκ, καθαριότητα, εστίαση, υπηρεσίες ασφαλείας (security), αλλά και αισθητικοί, φυσικοθεραπευτές, παιδαγωγοί, κομμωτές που παρέχουν υπηρεσίες για λογαριασμό ενός ξενοδοχείου. Οι εταιρίες/επιχειρήσεις αυτές ως εκτελούντες δεσμεύονται από τις νομοθετικές ρυθμίσεις αλλά και τις εντολές και οδηγίες που τους δίνει/ απευθύνει ο υπεύθυνος επεξεργασίας, εν προκειμένω ο ξενοδόχος. Θα πρέπει ωστόσο να εξετάζεται σε κάθε περίπτωση αν πρόκειται για σχέση υπευθύνου επεξεργασίας – εκτελούντα επεξεργασία γιατί μπορεί να μην πρόκειται για εκτελούντα αλλά για τρίτο στον οποίο διαβιβάζονται δεδομένα πελατών με τη συγκατάθεση των τελευταίων για μία δραστηριότητα στην οποία δεν εμπλέκεται ο υπεύθυνος.

Ακριβώς επειδή ο υπεύθυνος επεξεργασίας φέρει ευθύνη και για τις πράξεις ή παραλείψεις του εκτελούντος ο Κανονισμός προβλέπει αρκετά αναλυτικά τις υποχρεώσεις του εκτελούντος. Αυτές είναι μεταξύ άλλων

- η υποχρέωση τήρησης των καταγεγραμμένων εντολών του υπευθύνου επεξεργασίας, μεταξύ άλλων όσον αφορά τη διαβίβαση δεδομένων προσωπικού χαρακτήρα
- η διασφάλιση ότι τα πρόσωπα που είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα έχουν αναλάβει δέσμευση τήρησης εμπιστευτικότητας
- η πρόσληψη άλλου εκτελούντα την επεξεργασία μόνο με προηγούμενη ειδική ή γενική γραπτή άδεια του υπευθύνου επεξεργασίας
- η τήρηση και διαβεβαίωση για την τήρηση των οργανωτικών και τεχνικών μέτρων ασφαλείας
- ηπαροχή συνδρομής στον υπεύθυνο σε σχέση με την γνωστοποίηση παραβιάσεων (ασφάλειας) προσωπικών δεδομένων στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και στην ανακοίνωση στα υποκείμενα των δεδομένων
- η υποχρέωση του εκτελούντος επεξεργασία να παρέχει βοήθεια στον υπεύθυνο ως προς την ανταπόκριση στην άσκηση των δικαιωμάτων των υποκειμένων

- η υποχρέωση του Εκτελούντος επεξεργασία να διαγράφει ή επιστρέφει (κατ' επιλογή του υπευθύνου επεξεργασίας) όλα τα δεδομένα προσωπικού χαρακτήρα στον Υπεύθυνο επεξεργασίας μετά το πέρας της παροχής υπηρεσιών επεξεργασίας και διαγράφει τα υφιστάμενα αντίγραφα
- η τήρηση αρχείου όλων των κατηγοριών δραστηριοτήτων επεξεργασίας που διεξάγονται εκ μέρους του υπευθύνου επεξεργασίας

Επειδή η μη συμμόρφωση των εκτελούντων με τον νόμο και τις οδηγίες του υπευθύνου ενδέχεται να εκθέσει τον τελευταίο σε ευθύνες θα πρέπει να υπάρχει έλεγχος ως προς τη συμμόρφωση του εκάστοτε εκτελούντος με τον Κανονισμό αλλά και έγγραφη και δεσμευτική συμφωνία μαζί του που θα περιλαμβάνει και θα εξειδικεύει τα παραπάνω.

12. Κυρώσεις και ευθύνες

Ο Κανονισμός εισάγει διοικητικές κυρώσεις και αστική ευθύνη σε περίπτωση παραβίασης των κανόνων του.

Τα διοικητικά πρόστιμα συνιστούν το ισχυρότερο κυρωτικό εργαλείο του Κανονισμού. Οι ρυθμίσεις του άρθρου 83 επιβάλλουν δεσμευτικά τόσο το ύψος των προστίμων όσο και το πεδίο των παραβάσεων για τις οποίες αυτά επιβάλλονται. Προσδιορίζονται επακριβώς οι ρυθμίσεις η παράβαση των οποίων επισύρει διοικητικά πρόστιμα α) έως δέκα εκατομμύρια ευρώ ή, σε περίπτωση επιχειρήσεων, έως το 2 % του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους[5] και β) πρόστιμα έως είκοσι εκατομμύρια ευρώ ή, σε περίπτωση επιχειρήσεων, έως το 4 % του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους[6].

Σε αμφότερες τις περιπτώσεις, ο Κανονισμός προβλέπει ότι επιβάλλεται το κάθε φορά υψηλότερο ποσό.

Αν και η ευχέρεια που αναγνωρίζεται στις ανεξάρτητες αρχές, στην περίπτωση της Ελλάδας στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα είναι καταρχήν ευρεία ως προς το ύψος του προστίμου που θα επιβάλλουν σε κάθε περίπτωση, αυτή πρέπει να ασκείται αφενός υπό τους όρους της αρχής της αναλογικότητας και αφετέρου επί τη βάσει των συγκεκριμένων κριτηρίων που παραθέτει ο Κανονισμός.

Κρίσιμα στοιχεία η φύση, η βαρύτητα και η διάρκεια της παράβασης, λαμβανομένων υπόψη της φύσης, της έκτασης ή του σκοπού της επεξεργασίας, του αριθμού των θιγομένων προσώπων και του βαθμού ζημίας των υποκειμένων των δεδομένων που έθιξε η παράβαση και τον βαθμό ζημίας που υπέστησαν καθώς επίσης και η κατηγορία των δεδομένων που επηρεάζονται από την παράβαση. Σημαντικοί παράγοντες για τον προσδιορισμό του ύψους του προστίμου αφορούν την ύπαρξη δόλου ή αμέλειας, τον βαθμό ευθύνης

---

[5] Σύμφωνα με το άρθρο 83 παρ. 4 αυτό αφορά παραβίαση α)των υποχρεώσεων του υπευθύνου επεξεργασίας και του εκτελούντος την επεξεργασία σύμφωνα με τα άρθρα 8, 11, 25 έως 39 και 42 και 43, β) των υποχρεώσεων του φορέα πιστοποίησης σύμφωνα με τα άρθρα 42 και 43 καθώς και γ) των υποχρεώσεων του φορέα παρακολούθησης σύμφωνα με το άρθρο 41 παράγραφος 4.

[6] Σύμφωνα με το άρθρο 83 παρ. 5 αυτό αφορά παραβίαση α) των βασικών αρχών για την επεξεργασία, περιλαμβανομένων των όρων που ισχύουν για την έγκριση, σύμφωνα με τα άρθρα 5, 6, 7 και 9, β) των δικαιωμάτων των υποκειμένων των δεδομένων σύμφωνα με τα άρθρα 12 έως 22, γ) των ρυθμίσεων αναφορικά με τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε αποδέκτη σε τρίτη χώρα ή σε διεθνή οργανισμό σύμφωνα με τα άρθρα 44 έως 49, δ) οποιωνδήποτε υποχρεώσεων σύμφωνα με το δίκαιο του κράτους μέλους οι οποίες θεσπίζονται δυνάμει του κεφαλαίου IX του Κανονισμού.

του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία αναφορικά με τη λήψη τεχνικών και οργανωτικών μέτρων ασφαλείας, τις προσπάθειες και ενέργειες που έγιναν για τον μετριασμό των επιπτώσεων της παράβασης, η ύπαρξη προηγούμενων παραβάσεων αλλά και ο βαθμός συνεργασίας με την Αρχή καθώς και η συμμόρφωση με τα μέτρα που αυτή υπέδειξε. Σε συνάρτηση με την αρχή της λογοδοσίας, ο Κανονισμός εντάσσει στα κριτήρια την τήρηση εγκεκριμένων κωδίκων δεοντολογίας ή εγκεκριμένων μηχανισμών πιστοποίησης.

Ο υπεύθυνος επεξεργασίας έχει και αστική ευθύνη, δηλ. υποχρέωση αποζημίωσης σε περίπτωση που ένα πρόσωπο υπέστη υλική ή μη υλική ζημία ως αποτέλεσμα παραβίασης του κανόνων του Κανονισμού. Ένα πρόσωπο που θεωρεί ότι η επεξεργασία των προσωπικών δεδομένων του παραβιάζει τον Κανονισμό να στραφεί απευθείας κατά του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία.

Σημειώνεται ότι στο προσχέδιο νόμου για την συμπλήρωση των κανονων του Κανονισμού προβλέπονται και ποινικές ευθύνες.

Σύντομος (αυτό) έλεγχος συμμόρφωσης

Τί κάνουμε; Μερικά βασικά βήματα

Ενέργειες συμμόρφωσης

Ενημέρωση/ συνειδητοποίηση των απαιτήσεων και των αλλαγών που απαιτούνται τόσο από τον φορέα της επιχείρησης όσο και από τους εργαζομένους σε αυτή

Εντοπισμός - Χαρτογράφηση δραστηριοτήτων και διαδικασιών που αφορούν προσωπικά δεδομένα : εντοπίστε την προέλευση των δεδομένων, τη νομική βάση στην οποία μπορείτε να θεμελιώσετε τη νόμιμη επεξεργασία τους, το είδος των δεδομένων και τις κατηγορίες προσώπων που αφορούν, τυχόν διαβιβάσεις προσωπικών δεδομένων εκτός Ελλάδας (με διάκριση εάν πρόκειται για χώρες εντός ή εκτός Ευρωπαικής Ένωσης)

Νομικός έλεγχος των συμβάσεων, εντύπων κ.α.: Αναθεώρηση συμβάσεων/εντύπων/ όρων. Έμφαση πρέπει να δοθεί στα έντυπα ενημέρωσης αλλά και στα έντυπα συγκατάθεσης . Προσεκτικά πρέπει επίσης να εξεταστούν οι συμβάσεις με εκτελούντες επεξεργασία ώστε να προστεθούν οι όροι ως προς τις ευθύνες τους

Έλεγχος της ασφάλειας πληροφοριακών συστημάτων/ δικτύων/ δεδομένων - Το ζήτημα αυτό έχει τεχνική, οργανωτική και νομική διάσταση. Έμφαση πρέπει να δοθεί στη δέσμευση των εργαζομένων στην επιχείρηση με ρήτρες εχεμύθειας.

EU General Data
Protection Regulation
25 May 2018

H
HOTELS

ΞΕΝΟΔΟΧΕΙΑΚΟ ΕΠΙΜΕΛΗΤΗΡΙΟ ΕΛΛΑΔΟΣ