Εισαγωγή
Ο Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων (Κανονισμός ΕΕ 2016/679) είναι μια δεσμευτική νομοθετική πράξη μέσω της οποίας το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο της Ευρωπαϊκής Ένωσης και η Ευρωπαϊκή Επιτροπή προτίθενται να ενισχύσουν και να ενοποιήσουν την προστασία των δεδομένων για όλα τα άτομα εντός της Ευρωπαϊκής Ένωσης (ΕΕ). Αφορά επίσης την εξαγωγή δεδομένων προσωπικού χαρακτήρα, εκτός της ΕΕ.

Ο Κανονισμός εγκρίθηκε στις 27 Απριλίου 2016 κι εφαρμόζεται από τις 25 Μαΐου 2018 μετά από μεταβατική περίοδο περίπου δύο ετών σε όλα τα κράτη μέλη κι αντίθετα από μια οδηγία, δεν απαιτεί από τις εθνικές κυβερνήσεις να εγκρίνουν οποιαδήποτε νομοθετική πράξη με συνέπεια να είναι άμεσα δεσμευτικός και εφαρμόσιμος.

Ο Κανονισμός εισάγει ένα νέο σύνολο "δικαιωμάτων" για τους πολίτες της ΕΕ και υποχρεώσεων για τις επιχειρήσεις, σε μια εποχή που η οικονομική αξία των προσωπικών δεδομένων αυξάνεται και ιδιαίτερα στην ψηφιακή οικονομία.

Ο Ξενοδοχειακός Κλάδος & ο Κανονισμός

Η συμβουλευτική εταιρεία EDC μελέτησε 300 ξενοδοχεία στην Αγγλία (Νοέμβριος 2017) και ανέφερε ότι περίπου 60% δεν έχουν αρχίσει προετοιμασία για τον Κανονισμό και ότι 67% θεωρεί τον κλάδο ως την πλέον τρωτή σε παραβιάσεις βιομηχανία.

Όσον αφορά την ασφάλεια των δεδομένων, υπάρχουν λίγοι τομείς που είναι τόσο ευάλωτοι σε απειλές, όσο ο κλάδος των ξενοδοχείων. Το ξενοδοχείο επεξεργάζεται και σε πολλές περιπτώσεις αποθηκεύει μακροπρόθεσμα έναν πολύ μεγάλο όγκο προσωπικών πληροφοριών και οικονομικών συναλλαγών. Λαμβάνει, επίσης, σχετικές πληροφορίες από πολλές πηγές, όπως συστήματα κρατήσεων τρίτων, συστήματα σημείων πώλησης, παραχωρήσεις, ηλεκτρονικά μηνύματα, φαξ, τηλέφωνα και walk-ins. Επιπλέον, τα ξενοδοχεία τείνουν να αποθηκεύουν δεδομένα σε διάφορα σημεία.

Με τον όγκο των επεξεργασμένων δεδομένων προσωπικού χαρακτήρα και πιστωτικών καρτών, σε καθημερινή βάση, ο ξενοδοχειακός κλάδος είναι σήμερα ένας από τους πιο ευάλωτους σε παραβιάσεις (έρευνα για την παραβίαση δεδομένων, Verizon 2016).

Μετά τις 25 Μαΐου 2018, κάθε ξενοδοχείο, ανεξάρτητα από το μέγεθος του, εφόσον επεξεργάζεται προσωπικά δεδομένα κατοίκων της ΕΕ, πρέπει να συμμορφώνεται με τις απαιτήσεις του Κανονισμού.

Καταγραφή & Χρήση δεδομένων προσωπικού χαρακτήρα

Με τον όρο "Δεδομένα Προσωπικού Χαρακτήρα" νοείται οποιαδήποτε πληροφορία που αφορά ένα φυσικό πρόσωπο, είτε σχετίζεται με την ιδιωτική, επαγγελματική ή δημόσια ζωή του, σε ψηφιακή ή σε φυσική μορφή.

Μπορεί να είναι οτιδήποτε από όνομα, διεύθυνση κατοικίας, φωτογραφία, διεύθυνση ηλεκτρονικού ταχυδρομείου, τραπεζικά στοιχεία, αναρτήσεις σε ιστότοπους κοινωνικής δικτύωσης, ιατρικές πληροφορίες, διατροφικές προτιμήσεις ή διεύθυνση IP ενός υπολογιστή.

Σε ένα ξενοδοχείο, τέτοιες προσωπικές πληροφορίες μπορεί να διατίθενται σε όλα σχεδόν τα ξενοδοχειακά τμήματα, όπως για παράδειγμα, πωλήσεις και μάρκετινγκ, κρατήσεις, φαγητό / ποτό, κέντρο αναψυχής ή spa.

Σύμφωνα με τον Κανονισμό, τα προσωπικά δεδομένα, πρέπει να συλλέγονται για σαφείς και νόμιμους σκοπούς και δεν μπορούν να επεξεργαστούν περαιτέρω κατά τρόπο αντίθετο με τους σκοπούς που περιγράφηκαν αρχικά. Για παράδειγμα, λαμβάνοντας μια διεύθυνση ηλεκτρονικού ταχυδρομείου κατά την κράτηση και στη συνέχεια χρησιμοποιώντας τη, χωρίς περαιτέρω συγκατάθεση, για το μάρκετινγκ ηλεκτρονικού ταχυδρομείου σε μεταγενέστερο στάδιο.

Το ξενοδοχείο πρέπει να εξασφαλίσει ότι οι πελάτες γνωρίζουν τις συγκεκριμένες χρήσεις των δεδομένων τους.

Συνεπώς, το ξενοδοχείο πρέπει να αναπτύξει μια στρατηγική για τη λήψη συναίνεσης του πελάτη, με την κατάλληλη μορφή, πριν από την έναρξη ισχύος του Κανονισμού.

Προμηθευτές του ξενοδοχείου

Στο πλαίσιο της συμμόρφωσης με τον Κανονισμό, πρέπει να επανεξεταστούν οι συμβάσεις συνεργασίας του ξενοδοχείου με τους προμηθευτές του που χρησιμοποιούν τα προσωπικά δεδομένα των επισκεπτών, συμπεριλαμβανομένων των εταιρειών παροχής υπηρεσιών εστίασης, των συνεργείων καθαριότητας, των παρόχων υπηρεσιών φυσικής και ηλεκτρονικής ασφάλειας, των online ταξιδιωτικών πρακτορείων, των μεταφορικών εταιρειών, κα.

Το ξενοδοχείο, ως Υπεύθυνος Επεξεργασίας Δεδομένων, πρέπει να δώσει έμφαση στο σχεδιασμό συμβάσεων συνεργασίας με τους παραπάνω, σύμφωνα με τις απαιτήσεις του Κανονισμού. Επίσης, για να διασφαλιστεί ότι τα δεδομένα αυτά δεν θα παραμείνουν περισσότερο από ό,τι είναι απαραίτητο, πρέπει να οριστούν χρονικά όρια από το ξενοδοχείο για διαγραφή ή για περιοδική αναθεώρηση. Επιπρόσθετα, το ξενοδοχείο οφείλει να λαμβάνει κάθε εύλογο μέτρο για να πιστοποιείται ότι τα στοιχεία προσωπικών δεδομένων που είναι ανακριβή, διορθώνονται ή και διαγράφονται.

Τι νέο εισάγει ο Κανονισμός

Σήμερα, οι κανόνες σχετικά με τη συλλογή στοιχείων επισκεπτών (ή δυνητικών επισκεπτών) είναι κάπως ευέλικτοι. Οι ξενοδόχοι μπορούν να αξιοποιούν τη δυνατότητα opt-out και τη σιωπηρή συγκατάθεση για την εγγραφή πελατών σε διάφορα ενημερωτικά δελτία και καμπάνιες ηλεκτρονικού ταχυδρομείου. Τα γενικευμένα αιτήματα συγκατάθεσης και ένας μεγάλος αριθμός λιστών με ονόματα μπορούν να χρησιμοποιηθούν ώστε το ξενοδοχείο να προσεγγίσει πιθανούς επισκέπτες.

Όλα αυτά αλλάζουν στο πλαίσιο του Κανονισμού. Η απαίτηση για σαφή και διαφανή συγκατάθεση του πελάτη σημαίνει ότι το ξενοδοχείο πρέπει να του εξηγήσει:
• τι δεδομένα συλλέγει,
• γιατί συλλέγει αυτά τα δεδομένα
• ποιος τα ζητάει (ποιος είναι ο Υπεύθυνος Επεξεργασίας) και
• ποιος άλλος θα έχει πρόσβαση σε αυτά τα δεδομένα.

Το τελικό αποτέλεσμα είναι τα φυσικά πρόσωπα να γνωρίζουν με σαφήνεια τι πληροφορίες θέλει το ξενοδοχείο και τι σχεδιάζει να κάνει με αυτές.

Ωστόσο, το δύσκολο μέρος για το ξενοδοχείο είναι ότι η συναίνεση που κάποιος τους παρέχει, ισχύει μόνο για το σκοπό που έχει δηλωθεί ρητά.

Σήμερα, το ξενοδοχείο μπορούσε να αντλήσει τη διεύθυνση ηλεκτρονικού ταχυδρομείου μια φορά και στη συνέχεια να την επαναχρησιμοποιεί σε καμπάνιες και ενημερωτικά δελτία. Ωστόσο, με τη θέσπιση του Κανονισμού, αυτή η "αοριστία" πρέπει να περιοριστεί. Εάν έχετε καταγράψει την ηλεκτρονική διεύθυνση για την αποστολή ενημερωτικού δελτίου, τότε θα πρέπει να ζητήσετε ξανά ρητή συγκατάθεση για μια άλλη προωθητική καμπάνια, ιδιαίτερα μάλιστα όταν πρόκειται για μη συναφή σκοπό.

Τι αλλάζει στο μάρκετινγκ

Συχνά το ξενοδοχείο βασίζεται σε online προωθητικές ενέργειες, ως μια μορφή μάρκετινγκ, όποτε ο Κανονισμός μπορεί να έχει σημαντικό αντίκτυπο στη στρατηγική μάρκετινγκ. Ο Κανονισμός αναφέρει ότι οι πελάτες θα πρέπει να έχουν δυνατότητα Opt-in, σε αντίθεση με το σημερινό ευρέως χρησιμοποιούμενο σύστημα opt-out.

Η πρόκληση, από την προοπτική του ψηφιακού μάρκετινγκ, είναι ότι τα ξενοδοχεία πρέπει να είναι απολύτως διαφανή με τον πελάτη, αλλά αυτό μπορεί να οδηγήσει σε μια

‘’βαριά’’ και λιγότερο φιλική ιστοσελίδα, όπου τα πολλά Opt-in πιθανώς θα κουράσουν τον πελάτη.

Το ξενοδοχείο πρέπει να είναι σε θέση να αποδείξει ότι έχει τη συγκατάθεση των πελατών του για την περαιτέρω χρήση των δεδομένων τους για σκοπούς μάρκετινγκ και πρέπει επίσης να έχει καθορίσει ποια δεδομένα επιθυμούν να χρησιμοποιηθούν. Αν αγοραστεί κατάλογος πιθανών πελατών, τότε το ξενοδοχείο πρέπει να έχει λάβει τεκμηρίωση που αποδεικνύει ότι υπήρξε συγκατάθεση χρήσης των δεδομένων από αυτούς τους πελάτες.

Τι πρέπει να γίνει;

Για να διασφαλιστεί η συμμόρφωση με τον Κανονισμό, το ξενοδοχείο θα πρέπει να σχεδιάσει ορισμένες φαινομενικά προφανείς αλλά μάλλον προσεκτικά σχεδιασμένες ενέργειες για τη διασφάλιση των δεδομένων προσωπικού χαρακτήρα των πελατών του και την αποφυγή επιπτώσεων που θα μπορούσαν να προκύψουν από την έλλειψη συμμόρφωσης, οπότε το ξενοδοχείο πρέπει:

• Να καθορίσει τις βασικές του αρχές όσον αφορά τα δεδομένα πελατών (και των εργαζομένων), και να αναγνωρίσει ότι τα δεδομένα ανήκουν στον επισκέπτη και όχι στο ξενοδοχείο.
• Να περιγράψει τον τρόπο συλλογής και διαχείρισης δεδομένων (informationflow / datamapping).
• Να θεσπίσει κώδικα δεοντολογίας ή πολιτικής απορρήτου για το ξενοδοχείο και το προσωπικό του.
• Να ορίσει τρόπο ‘’αυτό-ελέγχου’’ του ως προς τη συμμόρφωση με τον Κανονισμό (reporting / monitoring).
• Να τεκμηριώσει γιατί χρειάζεται να επεξεργαστεί τα προσωπικά δεδομένα και πόσο καιρό σκοπεύει να τα διατηρήσει.
• Να διατηρεί δομημένα αρχεία για να αποδείξει ότι προστατεύει τα δεδομένα.
• Να επιτρέπει στους πελάτες την πρόσβαση, τροποποίηση ή τη διαγραφή πληροφοριών.
• Να γνωρίζει τη θέση των δεδομένων που κατέχει. Αυτά τα δεδομένα μπορούν να βρεθούν σε πολλά σημεία (από την ρεσεψιόν και το εστιατόριο μέχρι το σπα και το θυρωρείο) σε υπολογιστές, σε προσωπικά τηλέφωνα, σε φακέλους, σε παλιά αρχεία αρχειοθέτησης ηλεκτρονικού ταχυδρομείου ακόμη και σε post-it που απομένουν στη ρεσεψιόν ή στο backoffice. Μόλις ληφθούν υπόψη τα παραπάνω, θα πρέπει να ληφθούν αποφάσεις σχετικά με τον τρόπο διαχείρισης. Οι ενέργειες μπορούν να περιλαμβάνουν τη διαγραφή, την επεξεργασία, την κρυπτογράφηση, την καταστροφή ή την αποθήκευση (σε μια ασφαλή τοποθεσία, όπου είναι εύκολη η πρόσβαση από το προσωπικό, αλλά με ελεγχόμενη πρόσβαση).
• Το προσωπικό του ξενοδοχείου πρέπει να γνωρίζει πώς να συλλέγει, να αποκτά πρόσβαση, να χρησιμοποιεί και να αποκαλύπτει προσωπικές πληροφορίες καθώς και τον τρόπο περιορισμού της πρόσβασης στα δεδομένα κατόχων καρτών. Οι εργαζόμενοι πρέπει επίσης να ενημερώνονται σχετικά με τον τρόπο δημιουργίας ισχυρών κωδικών πρόσβασης και να γνωρίζουν πώς να διαθέτουν σωστά τα έγγραφα που περιέχουν προσωπικά δεδομένα. Τα παραπάνω διασφαλίζονται με εκπαίδευση (από ευαισθητοποίηση μέχρι επιμόρφωση).
• Να αναρτήσει την πολιτική του για την ασφάλεια των προσωπικών δεδομένων και, πιθανώς να καθορίσει τον Υπεύθυνο για την Προστασία των Δεδομένων.
• Να μεριμνήσει για την τοποθέτηση και συντήρηση ασφαλών συστημάτων για την αποφυγή παραβιάσεων δεδομένων και επένδυση σε τεχνολογίες φυσικής και ηλεκτρονικής ασφάλειας.

Κάθε ξενοδοχείο, σε μικρότερο ή μεγαλύτερο βαθμό, επηρεάζεται από τον Κανονισμό, ανεξάρτητα από το μέγεθος ή την τοποθεσία.

Το ξενοδοχείο που θα κινηθεί, σήμερα, για τη συμμόρφωσή του θα επιβιώνει και αύριο στο νέο ψηφιακό κόσμο.

Τα ανωτέρω θα μπορούσαν να περιγραφούν σε 5 βήματα ως μια συνοπτική προσέγγιση στο πλαίσιο συμμόρφωσης με τον Κανονισμό:

Χαρτογράφηση δεδομένων -Datamapping

Το ξενοδοχείο θα χρειαστεί να σχεδιάσει μια διαδικασία χαρτογράφησης των δεδομένων προσωπικού χαρακτήρα, για να καταλάβει τι δεδομένα συλλέγονται, πού φυλάσσονται, και πώς χρησιμοποιούνται, πριν ξεκινήσει τη διαδικασία για την προστασία των δεδομένων.

Αξιολόγηση της ασφάλειας – IT

Μετά τη χαρτογράφηση των δεδομένων προσωπικού χαρακτήρα, το ξενοδοχείο πρέπει να ελέγξει και να τεκμηριώσει πόσο ασφαλή είναι τα δεδομένα (σε ψηφιακή και έντυπη μορφή) και να εντοπίσει τυχόν αδυναμίες.

Σχεδιασμός Πολιτικών

Το ξενοδοχείο θα πρέπει να αναθεωρήσει τις τρέχουσες πολιτικές (όπως η πολιτική απορρήτου / privacypolicy τους, η πολιτική πρόσβασης στα δεδομένα / subjectaccessrequest, η πολιτική διατήρησης / retentionpolicy, κλπ) στο πλαίσιο της συμμόρφωσης του με τον Κανονισμό.

Εφαρμογή νέων πολιτικών – διαδικασιών

Εκκίνηση της επίπονης εργασίας ‘’ξεκαθάρισμα σημερινών αρχείων δεδομένων’’ με τη διαγραφή των δεδομένων και αρχείων που δεν χρειάζονται και την επικύρωση των δεδομένων & αρχείων που απαιτούνται.

Εκκίνηση της διαδικασίας για επικοινωνία με τους πελάτες ώστε να ενημερωθούν για τη νέα πολιτική και να επιβεβαιωθούν τα προσωπικά δεδομένα τους και η χρήση τους (σκοπός διεργασίας).

Καταγραφή όλων των τυποποιημένων διαδικασιών λειτουργίας (SOP) και επένδυση στην ευαισθητοποίηση / κατάρτιση όλων των εργαζομένων, για να διασφαλιστεί ότι θα έχουν πλήρη γνώση των νέων διαδικασιών και των επιπτώσεων από την εφαρμογή του Κανονισμού.

Συμμόρφωση reporting&monitoring

Το ξενοδοχείο πρέπει να παρακολουθεί την υλοποίηση, να παρέχει επανεκπαίδευση όταν απαιτείται, να διασφαλίζει τη δημιουργία μιας κουλτούρας για την προστασία της ιδιωτικότητας και την ασφάλεια των δεδομένων, από ενδεχόμενες παραβιάσεις.