Πολιτική Απορρήτου και Προστασίας Προσωπικών Δεδομένων

Περιεχόμενα

Λίστα πινάκων

1 Εισαγωγή

Στις καθημερινές επιχειρηματικές της δραστηριότητες, η SenseOne χρησιμοποιεί μια ποικιλία δεδομένων σχετικά με αναγνωρίσιμα άτομα, συμπεριλαμβανομένων δεδομένων σχετικά με:

- Τρέχοντες, πρώην και μελλοντικούς εργαζόμενους
- Πελάτες
- Εταίρους
- Χρήστες των ιστοσελίδων της
- Άλλα ενδιαφερόμενα μέρη

Κατά τη συλλογή και χρήση αυτών των δεδομένων, η εταιρία υπόκειται σε έναν αριθμό νομοθεσιών που ελέγχουν τον τρόπο διεξαγωγής τέτοιων δραστηριοτήτων και τα μέτρα που πρέπει να τεθούν σε εφαρμογή για την προστασία τους.

Σκοπός αυτής της πολιτικής είναι να καθορίσει τη σχετική νομοθεσία και να περιγράψει τα βήματα που λαμβάνει η SenseOne για να διασφαλίσει ότι συμμορφώνεται με αυτήν.

Αυτός ο έλεγχος ισχύει για όλα τα συστήματα, τα άτομα και τις διαδικασίες που αποτελούν τα πληροφοριακά συστήματα του οργανισμού, συμπεριλαμβανομένων των μελών του διοικητικού συμβουλίου, των διευθυντών, των υπαλλήλων, των προμηθευτών και άλλων τρίτων μερών που έχουν πρόσβαση στα συστήματα της SenseOne.

Οι ακόλουθες πολιτικές και διαδικασίες σχετίζονται με το παρόν έγγραφο:

- *Διαδικασία εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων*
- *Διαδικασία Χαρτογράφησης Προσωπικών Δεδομένων*
- *Διαδικασία αντιμετώπισης περιστατικών που αφορούν την ασφάλεια πληροφοριών*
- *Ρόλοι, αρμοδιότητες και αρχές GDPR*
- *Πολιτική Διατήρησης και Προστασίας Αρχείων*

3 Πολιτική Απορρήτου και Προστασίας Προσωπικών Δεδομένων

3.1 Ο γενικός κανονισμός για την προστασία δεδομένων

Ο Γενικός Κανονισμός Προστασίας Δεδομένων 679/2016 (GDPR) είναι μία από τις σημαντικότερες νομοθεσίες που επηρεάζουν τον τρόπο με τον οποίο η SenseOne διεξάγει τις δραστηριότητες επεξεργασίας πληροφοριών. Σημαντικά πρόστιμα επιβάλλονται εάν θεωρηθεί ότι έχει σημειωθεί παραβίαση βάσει του GDPR, ο οποίος έχει σχεδιαστεί για την προστασία των προσωπικών δεδομένων των πολιτών της Ευρωπαϊκής Ένωσης. Είναι πολιτική της SenseOne να διασφαλίζει ότι η συμμόρφωσή μας με τον GDPR και άλλη σχετική νομοθεσία είναι σαφής και αποδείξιμη ανά πάσα στιγμή.

3.2 Ορισμοί

Υπάρχουν συνολικά 26 ορισμοί που αναφέρονται στο GDPR και δεν είναι σκόπιμο να αναπαραχθούν όλοι εδώ. Ωστόσο, οι πιο θεμελιώδεις ορισμοί σε σχέση με αυτήν την πολιτική είναι οι εξής:

Τα προσωπικά δεδομένα ορίζονται ως:

κάθε πληροφορία που αναφέρεται σε φυσικό πρόσωπο του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί («υποκείμενο των δεδομένων»)· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο 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 online αναγνωριστικό ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου·

«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·

«υπεύθυνος επεξεργασίας»:

το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα· όταν οι σκοποί και ο τρόπος της εν λόγω

επεξεργασίας καθορίζονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια για τον διορισμό του μπορούν να προβλέπονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους·

3.3 Αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα

Υπάρχουν ορισμένες θεμελιώδεις αρχές στις οποίες βασίζεται ο GDPR.

Αυτά είναι τα εξής:

1. Τα δεδομένα προσωπικού χαρακτήρα:

α) υποβάλλονται σε σύννομη, θεμιτή και διαφανή επεξεργασία σε σχέση με το πρόσωπο στο οποίο αναφέρονται τα δεδομένα («νομιμότητα, αντικειμενικότητα και διαφάνεια»)·

β) συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασυμβίβαστο με τους σκοπούς αυτούς· η περαιτέρω επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς δεν θεωρείται, σύμφωνα με το άρθρο 89 παράγραφος 1, ασυμβίβαστη με τους αρχικούς σκοπούς («περιορισμός του σκοπού»)·

γ) είναι κατάλληλα, συναφή και περιορίζονται σε ό,τι είναι αναγκαίο σε σχέση με τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία («ελαχιστοποίηση των δεδομένων»)·

δ) είναι ακριβή και, εφόσον απαιτείται, επικαιροποιούνται· πρέπει να λαμβάνεται κάθε εύλογο μέτρο ώστε τα δεδομένα προσωπικού χαρακτήρα που είναι ανακριβή, σε σχέση με τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία, να διαγράφονται ή να διορθώνονται χωρίς καθυστέρηση («ακρίβεια»)·

ε) διατηρούνται υπό μορφή που επιτρέπει την εξακρίβωση της ταυτότητας των προσώπων στα οποία αναφέρονται τα δεδομένα για χρονικό διάστημα που δεν υπερβαίνει το αναγκαίο για την επίτευξη των σκοπών για τους οποίους τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία· τα δεδομένα προσωπικού χαρακτήρα μπορούν να αποθηκεύονται για μεγαλύτερο χρονικό διάστημα, εφόσον τα δεδομένα προσωπικού χαρακτήρα θα υποβληθούν σε επεξεργασία αποκλειστικά για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον και την επιστημονική ή ιστορική έρευνα σκοπούς ή στατιστικούς σκοπούς σύμφωνα με το άρθρο 89 παράγραφος 1, με την επιφύλαξη της εφαρμογής των κατάλληλων τεχνικών και οργανωτικών μέτρων που απαιτούνται από τον παρόντα κανονισμό για τη διασφάλιση των δικαιωμάτων και

των ελευθεριών του υποκειμένου των δεδομένων («περιορισμός της περιόδου αποθήκευσης»)·

στ) υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλεια των δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένης της προστασίας από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά, με τη χρήση κατάλληλων τεχνικών ή οργανωτικών μέτρων («ακεραιότητα και εμπιστευτικότητα»).

2. Ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και είναι σε θέση να αποδείξει τη συμμόρφωση με την παράγραφο 1 («λογοδοσία»).

Η SenseOne πρέπει να διασφαλίσει ότι συμμορφώνεται με όλες αυτές τις αρχές τόσο κατά την επεξεργασία που πραγματοποιεί επί του παρόντος όσο και ως μέρος της εισαγωγής νέων μεθόδων επεξεργασίας, όπως τα νέα συστήματα πληροφορικής. Η λειτουργία ενός συστήματος διαχείρισης ασφάλειας πληροφοριών (ISMS) που συμμορφώνεται με το διεθνές πρότυπο ISO / IEC 27001 αποτελεί βασικό μέρος αυτής της δέσμευσης.

3.4 Δικαιώματα του ατόμου

Το υποκείμενο των δεδομένων έχει επίσης δικαιώματα βάσει του GDPR. Αυτά αποτελούνται από:

1. Το δικαίωμα ενημέρωσης
2. Το δικαίωμα πρόσβασης
3. Το δικαίωμα διόρθωσης
4. Το δικαίωμα διαγραφής
5. Το δικαίωμα περιορισμού της επεξεργασίας
6. Το δικαίωμα στη φορητότητα των δεδομένων
7. Το δικαίωμα εναντίωσης
8. Δικαιώματα σε σχέση με την αυτοματοποιημένη λήψη αποφάσεων και την κατάρτιση προφίλ.

Κάθε ένα από αυτά τα δικαιώματα υποστηρίζεται από κατάλληλες διαδικασίες εντός της SenseOne που επιτρέπουν την ανάληψη της απαιτούμενης ενέργειας εντός των χρονικών ορίων που ορίζονται στον ΓΚΠΔ.

Αυτά τα χρονοδιαγράμματα παρουσιάζονται στον πίνακα 1.

Αίτημα υποκειμένου δεδομένων	**Χρονική κλίμακα**
Το δικαίωμα ενημέρωσης	Όταν συλλέγονται δεδομένα (εάν παρέχονται από το υποκείμενο των δεδομένων) ή εντός ενός μηνός (εάν δεν

	παρέχονται από το υποκείμενο των δεδομένων)
Το δικαίωμα πρόσβασης	Ένας μήνας
Το δικαίωμα διόρθωσης	Ένας μήνας
Το δικαίωμα διαγραφής	Χωρίς αδικαιολόγητη καθυστέρηση
Το δικαίωμα περιορισμού της επεξεργασίας	Χωρίς αδικαιολόγητη καθυστέρηση
Το δικαίωμα στη φορητότητα των δεδομένων	Ένας μήνας
Το δικαίωμα εναντίωσης	Με την παραλαβή της ένστασης
Δικαιώματα σε σχέση με την αυτοματοποιημένη λήψη αποφάσεων και την κατάρτιση προφίλ.	Δεν προσδιορίζεται

Πίνακας 1 - Χρονοδιαγράμματα για τα αιτήματα των υποκειμένων των δεδομένων

3.5 Συγκατάθεση

Εκτός εάν είναι απαραίτητο για λόγο που επιτρέπεται από το GDPR, πρέπει να ληφθεί ρητή συγκατάθεση από το υποκείμενο των δεδομένων για τη συλλογή και επεξεργασία των δεδομένων του. Σε περίπτωση παιδιών ηλικίας κάτω των 16 ετών, πρέπει να λαμβάνεται γονική συναίνεση. Διαφανείς πληροφορίες σχετικά με τη χρήση των προσωπικών τους δεδομένων πρέπει να παρέχονται στα υποκείμενα των δεδομένων κατά τη στιγμή της λήψης της συγκατάθεσης και να εξηγούνται τα δικαιώματά τους όσον αφορά τα δεδομένα τους, όπως το δικαίωμα ανάκλησης της συγκατάθεσης. Οι πληροφορίες αυτές πρέπει να παρέχονται σε προσιτή μορφή, γραμμένη σε σαφή γλώσσα και δωρεάν.

Εάν τα προσωπικά δεδομένα δεν λαμβάνονται απευθείας από το υποκείμενο των δεδομένων, τότε οι πληροφορίες αυτές πρέπει να παρέχονται εντός εύλογου χρονικού διαστήματος μετά τη λήψη των δεδομένων και οπωσδήποτε εντός ενός μηνός.

3.6 Προστασία προσωπικών δεδομένων από το σχεδιασμό

Η SenseOne έχει υιοθετήσει την αρχή της προστασίας της ιδιωτικής ζωής ήδη από το σχεδιασμό και θα διασφαλίσει ότι ο ορισμός και ο σχεδιασμός όλων των νέων ή σημαντικά τροποποιημένων συστημάτων που συλλέγουν ή επεξεργάζονται προσωπικά δεδομένα θα υπόκεινται στη δέουσα εξέταση των ζητημάτων απορρήτου, συμπεριλαμβανομένης της ολοκλήρωσης μίας ή περισσότερων εκτιμήσεων αντικτύπου σχετικά με την προστασία δεδομένων.

Η εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων θα περιλαμβάνει:

- Εξέταση του τρόπου επεξεργασίας των προσωπικών δεδομένων και για ποιους σκοπούς

- Αξιολόγηση του κατά πόσον η προτεινόμενη επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι αναγκαία και αναλογική προς τον/τους σκοπό/-ούς
- Αξιολόγηση των κινδύνων για τα φυσικά πρόσωπα κατά την επεξεργασία των δεδομένων προσωπικού χαρακτήρα
- Ποιοι έλεγχοι είναι απαραίτητοι για την αντιμετώπιση των εντοπισθέντων κινδύνων και την απόδειξη της συμμόρφωσης με τη νομοθεσία

Θα πρέπει να εξετάζεται το ενδεχόμενο χρήσης τεχνικών όπως η ελαχιστοποίηση των δεδομένων και η ψευδωνυμοποίηση, όπου πρέπει και είναι εφικτό.

3.7 Διαβίβαση Προσωπικών Δεδομένων

Οι μεταφορές προσωπικών δεδομένων εκτός της Ευρωπαϊκής Ένωσης πρέπει να εξετάζονται προσεκτικά πριν από τη μεταφορά για να διασφαλιστεί ότι εμπίπτουν στα όρια που επιβάλλονται από το GDPR. Αυτό εξαρτάται εν μέρει από την κρίση της Ευρωπαϊκής Επιτροπής όσον αφορά την επάρκεια των διασφαλίσεων για τα δεδομένα προσωπικού χαρακτήρα που ισχύουν στη χώρα υποδοχής και αυτό μπορεί να αλλάξει με την πάροδο του χρόνου.

Οι ενδοομιλικές διεθνείς διαβιβάσεις δεδομένων πρέπει να υπόκεινται σε νομικά δεσμευτικές συμφωνίες που αναφέρονται ως δεσμευτικοί εταιρικοί κανόνες (BCR), οι οποίοι παρέχουν εκτελεστά δικαιώματα στα υποκείμενα των δεδομένων.

3.8 Υπεύθυνος Προστασίας Δεδομένων

Ένας καθορισμένος ρόλος του Υπεύθυνου Προστασίας Δεδομένων (DPO) απαιτείται βάσει του GDPR εάν ένας οργανισμός είναι δημόσια αρχή, εάν εκτελεί παρακολούθηση μεγάλης κλίμακας ή εάν επεξεργάζεται ιδιαίτερα ευαίσθητους τύπους δεδομένων σε μεγάλη κλίμακα. Ο ΥΠΔ απαιτείται να διαθέτει κατάλληλο επίπεδο γνώσεων και μπορεί είτε να είναι εσωτερικός πόρος είτε να ανατίθεται σε κατάλληλο πάροχο υπηρεσιών.

Με βάση αυτά τα κριτήρια, η SenseOne δεν απαιτείται να διαθέτει ορισμένο Υπεύθυνο Προστασίας Δεδομένων.

3.9 Ειδοποίηση παραβίασης

Αποτελεί πολιτική της SenseOne να είναι δίκαιη και αναλογική κατά την εξέταση των ενεργειών που πρέπει να αναληφθούν για την ενημέρωση των επηρεαζόμενων μερών σχετικά με παραβιάσεις προσωπικών δεδομένων. Σύμφωνα με τον ΓΚΠΔ, όταν είναι γνωστό ότι έχει σημειωθεί παραβίαση η οποία είναι πιθανό να οδηγήσει σε κίνδυνο για τα δικαιώματα και τις ελευθερίες των ατόμων, η αρμόδια Αρχή Προστασίας Δεδομένων (ΑΠΔ) θα ενημερώνεται εντός 72 ωρών. Η διαχείρισή τους θα γίνεται σύμφωνα με *τη Διαδικασία Αντιμετώπισης Περιστατικών Ασφάλειας Πληροφοριών*, η οποία καθορίζει τη συνολική διαδικασία χειρισμού περιστατικών ασφάλειας πληροφοριών.

Σύμφωνα με τον GDPR, η αρμόδια DPA έχει την εξουσία να επιβάλλει μια σειρά προστίμων έως και τέσσερα τοις εκατό του ετήσιου παγκόσμιου κύκλου εργασιών ή είκοσι εκατομμυρίων ευρώ, όποιο είναι υψηλότερο, για παραβάσεις των κανονισμών.

3.10 Αντιμετώπιση της συμμόρφωσης με τον ΓΚΠΔ

Οι ακόλουθες ενέργειες αναλαμβάνονται για να διασφαλιστεί ότι η SenseOne συμμορφώνεται ανά πάσα στιγμή με την αρχή λογοδοσίας του GDPR:

- Η νομική βάση για την επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι σαφής και αδιαμφισβήτητη
- Ένας υπεύθυνος προστασίας δεδομένων διορίζεται με ειδική ευθύνη για την προστασία δεδομένων στον οργανισμό
- Όλο το προσωπικό που εμπλέκεται στη διαχείριση προσωπικών δεδομένων κατανοεί τις ευθύνες του για την τήρηση ορθών πρακτικών προστασίας δεδομένων
- Έχει παρασχεθεί εκπαίδευση σε όλο το προσωπικό στον τομέα της προστασίας δεδομένων
- Ακολουθούνται οι κανόνες σχετικά με τη συγκατάθεση
- Οι διαδρομές είναι διαθέσιμες στα υποκείμενα των δεδομένων που επιθυμούν να ασκήσουν τα δικαιώματά τους σχετικά με τα προσωπικά δεδομένα και τα ερωτήματα αυτά αντιμετωπίζονται αποτελεσματικά
- Διεξάγονται τακτικές αναθεωρήσεις των διαδικασιών που αφορούν δεδομένα προσωπικού χαρακτήρα
- Η προστασία της ιδιωτικής ζωής από το σχεδιασμό υιοθετείται για όλα τα νέα ή τροποποιημένα συστήματα και διαδικασίες
- Καταγράφεται η ακόλουθη τεκμηρίωση των δραστηριοτήτων επεξεργασίας:
    - Επωνυμία οργανισμού και σχετικές λεπτομέρειες
    - Σκοποί της επεξεργασίας προσωπικών δεδομένων
    - Κατηγορίες φυσικών προσώπων και δεδομένα προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία
    - Κατηγορίες αποδεκτών προσωπικών δεδομένων
    - Συμφωνίες και μηχανισμοί για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες, συμπεριλαμβανομένων λεπτομερειών σχετικά με τους ισχύοντες ελέγχους
    - Χρονοδιαγράμματα διατήρησης προσωπικών δεδομένων
    - Σχετικοί τεχνικοί και οργανωτικοί έλεγχοι που εφαρμόζονται

Αυτές οι ενέργειες θα επανεξετάζονται σε τακτική βάση ως μέρος της διαδικασίας αναθεώρησης της διαχείρισης του Προγράμματος Προστασίας Προσωπικών Δεδομένων.