Πολιτική Προστασίας Ιδιωτικότητας και Δεδομένων Προσωπικού Χαρακτήρα

Περιεχόμενα

1 ΕΙΣΑΓΩΓΗ 2

3 ΠΟΛΙΤΙΚΗ ΠΡΟΣΤΑΣΙΑΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΚΑΙ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ 3

3.1 Ο Γενικος Κανονισμος Προστασιας Δεδομενων 3
3.2 Ορισμοι 3
3.3 Αρχες Που Διεπουν Την Επεξεργασια Των Δεδομενων Προσωπικου Χαρακτηρα 4
3.4 Ατομικα Δικαιωματα 5
3.5 Συγκαταθεση 6
3.6 Προστασια των δεδομενων ηδη απο το σχεδιασμο 6
3.7 Διαβιβαση Δεδομενων Προσωπικου Χαρακτηρα 7
3.8 Υπευθυνος Προστασιας Δεδομενων 7
3.9 Ειδοποιηση Παραβιασης 7
3.10 Εφαρμογη της Συμμορφωσης προς το ΓΚΠΔ 8

Λίστα Πινάκων

Πινακας 1 - Χρονοδιαγραμματα αιτηματων των υποκειμενων δεδομενων 6

Εισαγωγή

Στις καθημερινές επιχειρηματικές λειτουργίες, η Space Hellas χρησιμοποιεί μία πληθώρα δεδομένων που αφορούν σε ταυτοποιημένα άτομα, συμπεριλαμβανομένων και δεδομένων που αφορούν:

- Τρέχοντες, παλιούς και υποψήφιους υπαλλήλους
- Πελάτες
- Συνεργάτες
- Χρήστες των ιστοσελίδων τους
- Άλλους μετόχους

Ο σκοπός της συγκεκριμένης πολιτικής είναι να περιγράψει τη σχετική νομοθεσία και να παρουσιάσει τα βήματα που ακολουθεί η Space Hellas για να εξασφαλίσει τη συμμόρφωσή της σε αυτή.

Ο έλεγχος αυτός εφαρμόζεται σε όλα τα συστήματα, τους ανθρώπους και τις διαδικασίες της Space Hellas, συμπεριλαμβανομένων και των μελών του διοικητικού συμβουλίου, των διευθυντών, των εργαζομένων, των πελατών, των προμηθευτών, των συνεργατών, των υπεργολάβων και άλλων τρίτων μερών που έχουν πρόσβαση στα συστήματα της Space Hellas.

Οι παρακάτω πολιτικές και διαδικασίες σχετίζονται με αυτό το έγγραφο:

- *Διαδικασία Αξιολόγησης των Επιπτώσεων στην Προστασία των Δεδομένων*
- *Διαδικασία Χαρτογράφησης Δεδομένων Προσωπικού Χαρακτήρα*
- *Διαδικασία Απόκρισης σε Περιστατικά Ασφάλειας Πληροφοριών*
- *Ρόλοι, Υποχρεώσεις σε σχέση με το Γενικό Κανονισμό Προστασίας Δεδομένων*
- *Διατήρηση Αρχείων και Πολιτική Προστασίας*

2 Πολιτική Προστασίας Ιδιωτικότητας και Δεδομένων Προσωπικού Χαρακτήρα

2.1 Ο Γενικός Κανονισμός Προστασίας Δεδομένων

Ο Γενικός Κανονισμός Προστασίας Δεδομένων 679/2016 (ΓΚΠΔ) είναι ένα από τα πιο σημαντικά κομμάτια της νομοθεσίας που επηρεάζει τον τρόπο που η Space Hellas εκτελεί δραστηριότητες σχετικές με την επεξεργασία δεδομένων. Σε περίπτωση που υπάρξει παραβίαση του ΓΚΠΔ, ο οποίος είναι σχεδιασμένος για να προστατεύει τα δεδομένα προσωπικού χαρακτήρα όσων βρίσκονται στην Ευρωπαϊκή Ένωση, είναι πιθανό να επιβληθούν σημαντικά πρόστιμα. Είναι πολιτική της Space Hellas να εξασφαλίσει ότι η συμμόρφωσή με το ΓΚΠΔ και άλλες σχετικές νομοθεσίες είναι ξεκάθαρη και μπορεί να αποδειχτεί ανά πάσα στιγμή.

2.2 Ορισμοί

Στο ΓΚΠΔ εμπεριέχονται συνολικά 26 ορισμοί και δεν είναι πρέπον να τους αναπαράγουμε όλους εδώ. Ωστόσο, οι πιο βασικοί ορισμοί σχετικά με τη συγκεκριμένη πολιτική παρατίθενται παρακάτω:

Τα δεδομένα Προσωπικού Χαρακτήρα ορίζονται ως:

κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («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 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.

Ως «επεξεργασία» ορίζεται:

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» σημαίνει*:*

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 επεξεργασίας αυτής 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.

2.3 Αρχές Που Διέπουν Την Επεξεργασία Των Δεδομένων Προσωπικού Χαρακτήρα

Υπάρχουν κάποιες βασικές αρχές στις οποίες στηρίζεται ο ΓΚΠΔ.

Αυτές παρατίθενται παρακάτω:

1. Τα Δεδομένα Προσωπικού Χαρακτήρα πρέπει να :

(α) υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων («νομιμότητα, αντικειμενικότητα και διαφάνεια»),

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

(γ) είναι κατάλληλα, συναφή και περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία («ελαχιστοποίηση των δεδομένων»),

(δ) είναι ακριβή και, όταν είναι αναγκαίο, επικαιροποιούνται· πρέπει να λαμβάνονται όλα τα εύλογα μέτρα για την άμεση διαγραφή ή διόρθωση δεδομένων προσωπικού χαρακτήρα τα οποία είναι ανακριβή, σε σχέση με τους σκοπούς της επεξεργασίας («ακρίβεια»),

(ε) διατηρούνται υπό μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων μόνο για το διάστημα που απαιτείται για τους σκοπούς της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα· τα δεδομένα προσωπικού χαρακτήρα μπορούν να αποθηκεύονται για μεγαλύτερα διαστήματα, εφόσον τα δεδομένα προσωπικού χαρακτήρα θα υποβάλλονται σε επεξεργασία μόνο για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς, σύμφωνα με το άρθρο 89 παράγραφος 1 και εφόσον εφαρμόζονται τα κατάλληλα τεχνικά και οργανωτικά μέτρα που απαιτεί ο παρών κανονισμός για τη διασφάλιση των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων («περιορισμός της περιόδου αποθήκευσης»),

(στ) υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλεια των δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή

φθορά, με τη χρησιμοποίηση 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 Space Hellas πρέπει να διασφαλίσει ότι συμμορφώνεται με όλες αυτές τις αρχές, τόσο στις τρέχουσες επεξεργασίες, όσο και κατά την εισαγωγή νέων μεθόδων επεξεργασίας, όπως νέων πληροφοριακών συστημάτων. Η λειτουργία Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ) σύμφωνα με το διεθνές πρότυπο ISO/IEC 27001 είναι ένα κρίσιμο σημείο αυτής της δέσμευσης.

2.4 Ατομικά Δικαιώματα

Το υποκείμενο των δεδομένων έχει επίσης δικαιώματα, αναφορικά με το ΓΚΠΔ. Σε αυτά περιλαμβάνονται:

1. Το δικαίωμα της πληροφόρησης
2. Το δικαίωμα της πρόσβασης
3. Το δικαίωμα της διόρθωσης
4. Το δικαίωμα της διαγραφής
5. Το δικαίωμα του περιορισμού της επεξεργασίας
6. Το δικαίωμα της φορητότητας των δεδομένων
7. Το δικαίωμα της εναντίωσης
8. Δικαιώματα που σχετίζονται με την αυτοματοποιημένη λήψη αποφάσεων για το άτομο και την κατάρτιση προφίλ.

Κάθε ένα από τα δικαιώματα των φυσικών προσώπων υποστηρίζεται από κατάλληλες διαδικασίες της Space Hellas. Οι διαδικασίες αυτές εξασφαλίζουν ότι λαμβάνουν χώρα οι απαραίτητες ενέργειες στο πλαίσιο των χρονοδιαγραμμάτων που υποδηλώνονται στο ΓΚΠΔ.

Αυτά τα χρονοδιαγράμματα παρουσιάζονται στον Πίνακα 1.

Αίτημα του Υποκειμένου των Δεδομένων	**Χρονοδιάγραμμα**
Το δικαίωμα της πληροφόρησης	Τη στιγμή που συλλέγονται τα δεδομένα (εφόσον συλλέγονται από το υποκείμενο των δεδομένων) ή μέσα σε ένα μήνα (εφόσον δε συλλέγονται από το υποκείμενο των δεδομένων)
Το δικαίωμα της πρόσβασης	Ένας μήνας
Το δικαίωμα της διόρθωσης	Ένας μήνας
Το δικαίωμα της διαγραφής	Χωρίς αναίτια καθυστέρηση
Το δικαίωμα του περιορισμού της επεξεργασίας	Χωρίς αναίτια καθυστέρηση

Το δικαίωμα της φορητότητας των δεδομένων	Ένας μήνας
Το δικαίωμα της εναντίωσης	Τη στιγμή λήψης μίας ένστασης
Δικαιώματα που σχετίζονται με την αυτοματοποιημένη λήψη αποφάσεων και την κατάρτιση προφίλ.	Δε διευκρινίζεται

Πίνακας 1 - Χρονοδιαγράμματα αιτημάτων των υποκειμένων δεδομένων

2.5 Συγκατάθεση

Εκτός και αν είναι απαραίτητο για λόγους που επιτρέπονται από το ΓΚΠΔ, πρέπει να ληφθεί σαφής συγκατάθεση από το υποκείμενο των δεδομένων για τη συλλογή και την επεξεργασία των δεδομένων του. Σε περίπτωση που πρόκειται για παιδιά κάτω των 16 ετών, πρέπει να λαμβάνεται συγκατάθεση του γονέα / κηδεμόνα. Τα υποκείμενα των δεδομένων πρέπει να ενημερώνονται για τα δικαιώματά τους –σε σχέση με τα προσωπικά δεδομένα τους- όπως για παράδειγμα το δικαίωμα της συγκατάθεσης, τη χρονική στιγμή που λαμβάνεται η συγκατάθεσή τους. Οι πληροφορίες που αφορούν τα δικαιώματα των υποκειμένων πρέπει να είναι εύκολα προσβάσιμα, χωρίς χρέωση, και γραμμένα με σαφή τρόπο.

Εάν η συλλογή των προσωπικών δεδομένων δε γίνεται απευθείας από το υποκείμενο των δεδομένων, τότε αυτές οι πληροφορίες πρέπει να δίνονται σε ένα λογικό χρονικό διάστημα μετά την απόκτηση των δεδομένων και σίγουρα όχι αργότερα από το διάστημα ενός μήνα.

2.6 Προστασία των δεδομένων ήδη από το σχεδιασμό

Η Space Hellas έχει υιοθετήσει την αρχή της προστασίας των δεδομένων ήδη από το σχεδιασμό και θα εξασφαλίσει ότι ο ορισμός και ο σχεδιασμός όλων των καινούριων ή των σημαντικά τροποποιημένων συστημάτων που συλλέγουν ή επεξεργάζονται δεδομένα προσωπικού χαρακτήρα θα λάβουν τη δέουσα προσοχή σε ζητήματα ασφάλειας πληροφοριών και προστασίας προσωπικών δεδομένων, συμπεριλαμβανομένης και της διενέργειας μίας ή περισσότερων αξιολογήσεων των επιπτώσεων στην προστασία των δεδομένων (Μελέτες Αντικτύπου – DPIAs).

Η αξιολόγηση των επιπτώσεων στην προστασία των δεδομένων περιλαμβάνει:

- Τον τρόπο με τον οποίο τα δεδομένα προσωπικού χαρακτήρα τίθενται σε επεξεργασία και για ποιους σκοπούς
- Αξιολόγηση του κατά πόσο η προτεινόμενη επεξεργασία των δεδομένων προσωπικού χαρακτήρα είναι ταυτόχρονα απαραίτητα και ανάλογη του σκοπού (ή των σκοπών)
- Αξιολόγηση των κινδύνων στους οποίους εκτίθενται τα άτομα, λόγω της επεξεργασίας των προσωπικών τους δεδομένων

- Την επιλογή των μέτρων, οι οποίοι είναι απαραίτητοι για την αντιμετώπιση των κινδύνων που εντοπίστηκαν και αποδεικνύουν συμμόρφωση με τη νομοθεσία.

Η χρήση τεχνικών όπως η ελαχιστοποίηση των δεδομένων και η ψευδονυμοποίηση πρέπει να ληφθεί υπόψιν, σε περιπτώσεις που είναι κατάλληλη και δυνατή η εφαρμογή τους.

2.7 Διαβίβαση Δεδομένων Προσωπικού Χαρακτήρα

Η διαβίβαση δεδομένων προσωπικού χαρακτήρα εκτός της Ευρωπαϊκής Ένωσης πρέπει να εξετάζεται προσεκτικά και πριν η διαβίβαση λάβει χώρα, προκειμένου να εξασφαλιστεί ότι γίνεται σύμφωνα με το πλαίσιο που έχει οριστεί από το ΓΚΠΔ. Αυτό εξαρτάται εν μέρει από την κρίση της Ευρωπαϊκής Επιτροπής, καθώς και από την επάρκεια της ασφάλειας που εφαρμόζεται σχετικά με τα δεδομένα προσωπικού χαρακτήρα στη χώρα που θα δεχτεί τα δεδομένα, και μπορεί να μεταβληθεί σε βάθος χρόνου.

Οι διεθνείς μεταφορές δεδομένων εντός ομίλων πρέπει να υποβάλλονται σε νομικά δεσμευτικές συμφωνίες αναφερόμενες ως Δεσμευτικοί Εταιρικοί Κανόνες (Corporate Binding Rules) που παρέχουν δικαιώματα στα υποκείμενα των δεδομένων.

2.8 Υπεύθυνος Προστασίας Δεδομένων

Στα πλαίσια του ΓΚΠΔ απαιτείται η ανάδειξη Υπεύθυνου Προστασίας Δεδομένων (ΥΠΔ), σε περίπτωση που ο οργανισμός είναι δημόσια αρχή, εκτελεί επεξεργασίες μεγάλης κλίμακας ή επεξεργάζεται ιδιαίτερα ευαίσθητες κατηγορίες δεδομένων σε μεγάλη κλίμακα. Ο ΥΠΔ πρέπει να κατέχει το κατάλληλο επίπεδο γνώσεων και μπορεί να προέρχεται είτε από τον ίδιο τον οργανισμό είτε να είναι εξωτερικός συνεργάτης.

Με βάση αυτά τα κριτήρια, θεωρούμε ότι είναι απαραίτητος ο ορισμός Υπευθύνου Προστασίας Δεδομένων στη Space Hellas.

2.9 Ειδοποίηση Παραβίασης

Είναι πολιτική της Space Hellas να ενημερώνει όλους όσους απαιτείται, σε περίπτωση παραβίασης που αφορά προσωπικά δεδομένα, με δίκαιο και ανάλογο τρόπο. Σε ευθυγράμμιση με το ΓΚΠΔ, όταν γίνεται γνωστό ότι έλαβε χώρα μία παραβίαση η οποία είναι πιθανό να έχει ως αποτέλεσμα τη διακύβευση των δικαιωμάτων και των ελευθεριών των ατόμων, θα ενημερωθεί η Αρχή Προστασία Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) εντός 72 ωρών. Αυτό θα γίνει σύμφωνα με τη Διαδικασία Διαχείρισης Περιστατικών Ασφάλειας Πληροφοριών της Space Hellas.

Υπό το ΓΚΠΔ, η αντίστοιχη ΑΠΔΠΧ έχει την εξουσιοδότηση να επιβάλει ένα εύρος προστίμων έως το 4 τις εκατό του ετήσιου παγκόσμιας κύκλου εργασιών ή τα είκοσι εκατομμύρια ευρώ, όποιο από τα δύο είναι μεγαλύτερο, για παραβίαση του Κανονισμού.

2.10 Εφαρμογή της Συμμόρφωσης προς το ΓΚΠΔ

Οι παρακάτω ενέργειες έχουν γίνει για να εξασφαλιστεί ότι η Space Hellas συμμορφώνεται σε κάθε περίπτωση με την αρχή της λογοδοσίας του ΓΚΠΔ:

- Η νόμιμη βάση της επεξεργασίας δεδομένων προσωπικού χαρακτήρα είναι ξεκάθαρη και αδιαμφισβήτητη.
- Ορίζεται Υπεύθυνος Προστασίας Δεδομένων με αρμοδιότητα την προστασία των δεδομένων εντός του οργανισμού.
- Όλο το προσωπικό που εμπλέκεται στη διαχείριση των προσωπικών δεδομένων αντιλαμβάνεται τις ευθύνες του, ώστε να ακολουθεί τις βέλτιστες πρακτικές προστασίας δεδομένων.
- Όλο το προσωπικό έχει εκπαιδευτεί στην προστασία των δεδομένων.
- Τηρούνται οι υποχρεώσεις σχετικά με τη συγκατάθεση.
- Υπάρχουν διαθέσιμες οδοί, μέσω των οποίων τα υποκείμενα δεδομένων που επιθυμούν να ασκήσουν τα δικαιώματα τους σχετικά με τα προσωπικά τους δεδομένα έχουν αυτή τη δυνατότητα.
- Διεξάγονται τακτικά ανασκοπήσεις των διαδικασιών που αφορούν προσωπικά δεδομένα.
- Η προστασία των δεδομένων ήδη από το σχεδιασμό υιοθετείται για όλα τα νέα συστήματα και διαδικασίες ή σε σημαντικές αλλαγές των υπαρχόντων.
- Στο έγγραφο όπου περιγράφονται οι ενέργειες που λαμβάνουν χώρα σε μία επεξεργασία καταγράφεται:
    - Το όνομα του οργανισμού και οι σχετικές λεπτομέρειες
    - Οι σκοποί της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα
    - Οι κατηγορίες των ατόμων και των δεδομένων προσωπικού χαρακτήρα που είναι υπό επεξεργασία
    - Οι κατηγορίες των παραληπτών των προσωπικών δεδομένων
    - Οι συμφωνίες και οι μηχανισμοί με βάση τους οποίους γίνονται οι μεταφορές των προσωπικών δεδομένων σε χώρες εκτός της Ευρωπαϊκής Ένωσης, συμπεριλαμβανομένων και λεπτομερειών για τα μέτρα που ελήφθησαν
    - Χρόνος διατήρησης των προσωπικών δεδομένων
    - Τα κατάλληλα τεχνικά και οργανωτικά μέτρα που έχουν υλοποιηθεί.

Αυτές οι ενέργειες θα επιθεωρούνται σε τακτική βάση, ως κομμάτι της διαδικασίας επιθεώρησης διαχείρισης του Προγράμματος Προστασίας Προσωπικών Δεδομένων.