

PREMIA

Properties

**ΠΛΑΙΣΙΟ ΠΡΟΣΤΑΣΙΑΣ
ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ**

Περιεχόμενα

A. ΠΟΛΙΤΙΚΗ.....	2
1. Εισαγωγή	2
2. Αντικείμενο	3
3. Ορισμοί.....	3
4. Νομικό πλαίσιο προστασίας προσωπικών δεδομένων	4
5. Σκοπός επεξεργασίας των προσωπικών δεδομένων.....	5
6. Χρόνος διατήρησης των δεδομένων	5
7. Δικαιώματα αναφορικά με την προστασία προσωπικών δεδομένων	6
8. Δικαίωμα καταγγελίας	7
9. Μέτρα ασφαλείας	7
9.1 Γενικά	7
9.1.1 Μεταφορά Προσωπικών Δεδομένων με ηλεκτρονικό ταχυδρομείο.....	8
9.1.2. Μεταφορά Δεδομένων Μέσω Ψηφιακών Μέσων.....	8
9.1.3. Μεταφορά Δεδομένων Μέσω Δικτύων	8
B. Διαδικασία διαχείρισης παραβίασης δεδομένων προσωπικού χαρακτήρα.....	8
1. Σκοπός και Πεδίο Εφαρμογής Διαδικασίας	9
2. Νομική Βάση	9
3. Ορισμός της Παραβίασης Δεδομένων Προσωπικού Χαρακτήρα	9
4. Υποχρεώσεις του Υπεύθυνου Επεξεργασίας.....	10
5. Υποχρεώσεις του Εκτελούντος την Επεξεργασία	11
6. Αναλυτική Περιγραφή Διαχείρισης Παραβίασης Δεδομένων Προσωπικού Χαρακτήρα	12
Παράρτημα 1: Υπόδειγμα Φόρμας Γνωστοποίησης Παραβίασης Δεδομένων Προσωπικού χαρακτήρα Αναφορά Πιθανής Παραβίασης	16

ΠΛΑΙΣΙΟ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ	Ημερομηνία έναρξης ισχύος: 14/09/2022
Έγκριση: Διοικητικό Συμβούλιο	Επικαιροποίηση 09.12.2025

A. ΠΟΛΙΤΙΚΗ

Σκοπός της Πολιτικής αποτελεί η συνολική ενημέρωση για τους όρους και τις προϋποθέσεις με βάση τις οποίες η PREMIA Α.Ε.Ε.Α.Π. διαχειρίζεται τα Προσωπικά Δεδομένα που λαμβάνει με την παράλληλη λήψη μέτρων για την ασφάλεια των πληροφοριών.

1. Εισαγωγή

Η PREMIA Α.Ε.Ε.Α.Π. (**εφεξής PREMIA**) ενεργεί ως υπεύθυνος επεξεργασίας των δεδομένων προσωπικού χαρακτήρα, των εργαζομένων της, των προμηθευτών της, των υποψηφίων αντισυμβαλλόμενων με την Εταιρεία, των συνεργατών της, ταχυμεταφορέων και επισκεπτών της.

Η PREMIA λαμβάνει σοβαρά υπόψη την προστασία της ιδιωτικότητας των συναλλασσόμενων μαζί της. Για το λόγο αυτό ακολουθείται με αυστηρότητα η ακόλουθη Πολιτική Προστασίας Προσωπικών Δεδομένων, η οποία διασφαλίζει το υψηλό επίπεδο των προσφερόμενων υπηρεσιών και τηρεί απαρέγκλιτα το ισχύον Ευρωπαϊκό και εθνικό νομοθετικό πλαίσιο και ειδικότερα με την αυστηρή τήρηση του υπ' αριθ. 2016/679 Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένων (εφεξής καλούμενος «ΓΚΠΔ») και του υπ' αριθ. Ν. 4624/2019 περί λήψης μέτρων εφαρμογής του ΓΚΠΔ.

Η παρούσα πολιτική αφορά φυσικά πρόσωπα που διενεργούν οιαδήποτε συναλλαγή με την PREMIA εργαζόμενους, συνεργάτες, μισθωτές, πιστωτές, οφειλέτες αυτής υποψηφίους αντισυμβαλλόμενους, ταχυμεταφορείς και επισκέπτες της.

Τα δεδομένα προσωπικού χαρακτήρα των ως άνω φυσικών προσώπων συλλέγονται και διατηρούνται για τον απαιτητήτως αναγκαίο χρόνο, για καθορισμένους, ρητούς και νόμιμους σκοπούς, τυγχάνουν σύννομης και θεμιτής επεξεργασίας με διαφανή τρόπο σύμφωνα πάντα με το ισχύον νομικό πλαίσιο και κατά τρόπο που εγγυάται την ακεραιότητα και την εμπιστευτικότητα αυτών. Τα δεδομένα αυτά είναι κάθε φορά κατάλληλα, συναφή, πρόσφορα και όχι περισσότερα από όσα απαιτούνται εν όψει των ανωτέρω σκοπών, είναι δε ακριβή και επικαιροποιημένα.

2. Αντικείμενο

Με την παρούσα Πολιτική καθορίζονται οι όροι και οι προϋποθέσεις που τηρούνται από την PREMIA, για την προστασία εν γένει της ιδιωτικότητας των εργαζόμενων, συνεργατών, πιστωτών, μισθωτών, οφειλετών, των υποψηφίων αντισυμβαλλόμενων, ταχυμεταφορέων και επισκεπτών της. Σκοπός της παρούσας Πολιτικής είναι η ενημέρωση για τον τρόπο συλλογής, διατήρησης και επεξεργασίας των πληροφοριών.

Η PREMIA διατηρεί το δικαίωμα να τροποποιεί και να αναπροσαρμόζει την παρούσα Πολιτική, όποτε κρίνει αυτό αναγκαίο, ενώ οι εκάστοτε αλλαγές τίθενται σε ισχύ από την επικαιροποίηση και κυκλοφορία της παρούσας καθώς και την ανάρτηση των όσων τροποποιούνται στον ιστότοπο: www.premia.gr.

3. Ορισμοί

«**Δεδομένα προσωπικού χαρακτήρα**» ή «**προσωπικά δεδομένα**» είναι κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο, που μπορεί δηλαδή να συσχετιστεί με ένα φυσικό πρόσωπο. Τα δεδομένα θεωρούνται προσωπικά, αν το πρόσωπο στο οποίο αναφέρονται μπορεί να ταυτοποιηθεί, άμεσα ή έμμεσα (π.χ. μέσω αναφοράς ονόματος, αριθμού ταυτότητας, δεδομένων θέσης, επιγραφμικού (on-line) αναγνωριστικού ταυτότητας ή παραγόντων που χαρακτηριστικά γνωρίσματα της σωματικής, φυσιολογικής, γενετικής, ψυχολογικής, οικονομικής, πολιτιστικής ή κοινωνικής ταυτότητας του εν λόγω φυσικού προσώπου).

«**Επεξεργασία προσωπικών δεδομένων**» σημαίνει κάθε πράξη ή σειρά πράξεων σε δεδομένα προσωπικού χαρακτήρα. Είναι οποιαδήποτε ενέργεια, δραστηριότητα ή σύνολο δραστηριοτήτων που εφαρμόζονται στα προσωπικά δεδομένα ή σε σύνολα αυτών, ανεξάρτητα από τη διαδικασία και τα μέσα (αυτοματοποιημένα ή μη) που επιλέγονται, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η αναθεώρηση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, η διασύνδεση, το μπλοκάρισμα (κλείδωμα), η διαγραφή αρχείων, η προβολή και η καταστροφή των προσωπικών δεδομένων.

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

«**Εκτελών την επεξεργασία**» είναι το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται προσωπικά δεδομένα για λογαριασμό του υπευθύνου επεξεργασίας.

«**Ευαίσθητα προσωπικά δεδομένα ή Ειδικές Κατηγορίες Δεδομένων**» είναι δεδομένα που αφορούν:

- i. θρησκευτικές, ιδεολογικές, πολιτικές ή συνδικαλιστικές απόψεις ή δραστηριότητες,
- ii. την υγεία, γενετικές ή βιομετρικές πληροφορίες, τη σεξουαλική ζωή ή τη φυλετική και εθνοτική καταγωγή,
- iii. ποινικές διαδικασίες και κυρώσεις.

«**Κατάρτιση Προφίλ**» είναι οποιαδήποτε μορφή αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα που συνίσταται στη χρήση των δεδομένων αυτών με σκοπό την αξιολόγηση ορισμένων προσωπικών πτυχών ενός φυσικού προσώπου.

«**Υποκείμενο των Δεδομένων**» είναι ένα φυσικό πρόσωπο στο οποίο αφορούν τα προσωπικά δεδομένα.

«**Αρχείο δεδομένων**» είναι κάθε δομημένο σύνολο προσωπικών δεδομένων, το οποίο είναι προσβάσιμο κατά τέτοιο τρόπο ώστε να καθίσταται δυνατό να συνάγεται ποιο είναι το εν λόγω πρόσωπο από τα δεδομένα αυτά (π.χ. οποιοδήποτε εργαλείο του Τμήματος Πληροφορικής που εμπεριέχει προσωπικά δεδομένα).

«**Έντυπο δεδομένων**» είναι κάθε έγγραφο στο οποίο εμπεριέχονται δεδομένα προσωπικού χαρακτήρα.

«**Βάση δεδομένων**» είναι κάθε μορφής ηλεκτρονική ή έγχαρτη βάση εγγράφων ή δεδομένων που περιέχουν δεδομένα προσωπικού χαρακτήρα.

«**Δημόσια προσβάσιμος διακομιστής**» είναι ο υπολογιστής που μέσω αυτού παρέχονται υπηρεσίες υποστήριξης ιστοσελίδων και λογισμικών τα οποία είναι δημόσια προσβάσιμα.

«**Κοινολόγηση**» είναι η πρόσβαση σε προσωπικά δεδομένα, για παράδειγμα επιτρέποντας την πρόσβαση, τη διαβίβαση ή τη δημοσίευση.

«**Η Εκτίμηση Αντικτύπου σχετικά με την Προστασία Δεδομένων**» είναι μια συστηματική διαδικασία προσδιορισμού, αξιολόγησης και τεκμηρίωσης των κινδύνων και των επιπτώσεων των δραστηριοτήτων επεξεργασίας δεδομένων προσωπικού χαρακτήρα στα δικαιώματα των υποκειμένων.

4. Νομικό πλαίσιο προστασίας προσωπικών δεδομένων

Ως «**νομικό πλαίσιο προστασίας προσωπικών δεδομένων**» στο πλαίσιο της παρούσας Πολιτικής νοείται ο υπ' αριθ. 2016/679 Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (ΓΚΠΔ) για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών, ο υπ' αριθ. Ν. 4624/2019, ο οποίος αφορά στην αντικατάσταση του νομοθετικού πλαισίου που ρυθμίζει τη συγκρότηση και λειτουργία της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (εφεξής «**Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα**»), τη λήψη μέτρων εφαρμογής του υπ' αριθ. 2016/679 Γενικού Κανονισμού Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, καθώς και την ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 για την προστασία των φυσικών

προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων. Ακόμη, νοείται κάθε εθνικός νόμος που ισχύει και εφαρμόζεται και αφορά την επεξεργασία και την προστασία των προσωπικών δεδομένων γενικότερα. Διευκρινίζεται, πως σε κάθε περίπτωση ισχύει ο ΓΚΠΔ. Σε οποιαδήποτε διαφοροποίηση μεταξύ ΓΚΠΔ και εθνικής νομοθεσίας, θα υπερισχύουν οι διατάξεις που συνάδουν με την ενωσιακή νομοθεσία και πρακτική.

5. Σκοπός επεξεργασίας των προσωπικών δεδομένων

Σύμφωνα με το ανωτέρω νομικό πλαίσιο, η PREMIA συλλέγει και επεξεργάζεται προσωπικά δεδομένα φυσικών προσώπων για τους κατωτέρω σκοπούς και μόνο στο απολύτως αναγκαίο μέτρο για την αποτελεσματική εξυπηρέτηση των σκοπών αυτών. Τα δεδομένα αυτά είναι κάθε φορά συναφή, πρόσφορα και όχι περισσότερα από όσα απαιτούνται εν όψει των κατωτέρω σκοπών, είναι δε ακριβή και, εφόσον χρειάζεται, υποβάλλονται σε ενημέρωση - επικαιροποίηση. Η PREMIA δύναται, να επεξεργάζεται δεδομένα προσωπικού χαρακτήρα, εφόσον η επεξεργασία είναι απαραίτητη για μία τουλάχιστον από τις ακόλουθες νομικές βάσεις, ήτοι:

- Για την εκτέλεση της σύμβασης μεταξύ της PREMIA και τρίτων (εργαζομένων, προμηθευτών, οφειλετών κλπ.)
- προκειμένου να συμμορφωθεί σε έννομη υποχρέωσή του, ή
- για τους σκοπούς των εννόμων συμφερόντων της, ή
- εφόσον έχει δοθεί στην PREMIA η συγκατάθεση του φυσικού προσώπου στο οποίο αυτά αναφέρονται ή
- για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον.

6. Χρόνος διατήρησης των δεδομένων

Η PREMIA διατηρεί τα δεδομένα προσωπικού χαρακτήρα των φυσικών προσώπων για όσο χρονικό διάστημα προβλέπεται ανά περίπτωση, από το εκάστοτε ισχύον νομοθετικό και κανονιστικό πλαίσιο και σε κάθε περίπτωση για χρονικό διάστημα είκοσι (20) ετών από την τελευταία ημερολογιακή ημέρα του έτους λήξης της εκάστοτε συναλλακτικής σχέσης με την PREMIA.

Σε περίπτωση δικαστικής αντιδικίας, τα προσωπικά δεδομένα θα τηρούνται μέχρι τη λήξη της εκκρεμοδικίας, ακόμα και σε περίπτωση υπέρβασης του ανώτερου χρονικού διαστήματος των είκοσι (20) ετών.

Η διαγραφή των δεδομένων ξεκινάει τον τελευταίο μήνα πριν την πάροδο του ανωτέρω χρόνου διατήρησής τους. Τα δεδομένα διαγράφονται από τα ηλεκτρονικά αρχεία, ή καταστρέφονται με φυσικό τρόπο, εφόσον το μέσο διατήρησής τους είναι ενσώματο (έντυπο, ηλεκτρονικός φορέας κ.λπ.), με μη αναστρέψιμο τρόπο τηρουμένων των αναγκαίων μέτρων ασφαλείας.

7. Δικαιώματα αναφορικά με την προστασία προσωπικών δεδομένων

Η νομοθεσία για την προστασία των προσωπικών δεδομένων παρέχει τα ακόλουθα δικαιώματα, τα οποία δύναται κατ' αρχήν να ασκηθούν δωρεάν και με βάση όσα προβλέπονται στο νομικό πλαίσιο:

- Δικαίωμα πρόσβασης, ήτοι ενημέρωση για το ποια δεδομένα τα οποία έχει συλλέξει η PREMIA υφίστανται επεξεργασία, την προέλευση των δεδομένων, τους σκοπούς και τη νομική βάση επεξεργασίας αυτών, τους τυχόν αποδέκτες ή τις κατηγορίες αποδεκτών των προσωπικών δεδομένων, ιδίως σε τρίτες χώρες καθώς και το χρόνο διατήρησής τους.
- Δικαίωμα διόρθωσης τυχόν ανακριβών προσωπικών δεδομένων, ώστε να καταστούν ακριβή, υποβάλλοντας στη PREMIA σχετική δήλωση με τα ακριβή προσωπικά δεδομένα.
- Δικαίωμα συμπλήρωσης τυχόν ελλιπών προσωπικών δεδομένων, ώστε να καταστούν πλήρη, υποβάλλοντας στη PREMIA σχετική δήλωση με τα πλήρη προσωπικά δεδομένα.
- Δικαίωμα διαγραφής των προσωπικών δεδομένων στις εξής περιπτώσεις :
 - i. όταν τα προσωπικά δεδομένα δεν είναι πλέον απαραίτητα σε σχέση με τους σκοπούς για τους οποίους συλλέχθηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία,
 - ii. όταν ανακαλείται η συγκατάθεση επί της οποίας βασίσθηκε η επεξεργασία των προσωπικών δεδομένων και δεν υπάρχει άλλη νομική βάση για την επεξεργασία,
 - iii. όταν τα προσωπικά δεδομένα υποβλήθηκαν σε επεξεργασία χωρίς την ύπαρξη της απαραίτητης νομικής βάσης,
 - iv. όταν προβλέπεται από το νόμο η υποχρέωση διαγραφής των προσωπικών δεδομένων,
- Δικαίωμα περιορισμού της επεξεργασίας των προσωπικών δεδομένων, στις εξής περιπτώσεις :
 - i. αμφισβητείται η ακρίβεια των προσωπικών δεδομένων και μέχρι να επαληθεύσει η PREMIA την ακρίβεια τους,
 - ii. όταν συντρέχουν οι προϋποθέσεις διαγραφής της προηγούμενης παραγράφου και αντί της διαγραφής, ζητηθεί ο περιορισμός της επεξεργασίας των προσωπικών δεδομένων,

- Δικαίωμα εναντίωσης-αντίταξης στην επεξεργασία των δεδομένων, εκτός εάν υφίστανται επιτακτικοί και νόμιμοι λόγοι για την επεξεργασία, οι οποίοι υπερισχύουν των συμφερόντων, των δικαιωμάτων και των ελευθεριών του φυσικού προσώπου.
- Δικαίωμα φορητότητας, ήτοι λήψης και διαβίβασης σε άλλον υπεύθυνο επεξεργασίας των προσωπικών δεδομένα των φυσικών προσώπων, τα οποία έχουν παρασχεθεί στη PREMIA σε κατάλληλο μορφότυπο, εφόσον η επεξεργασία των προσωπικών δεδομένων έχει λάβει χώρα κατόπιν συγκατάθεσης ή υπήρξε απαραίτητη για την εκτέλεση σχετικής σύμβασης.
- Δικαίωμα ανάκλησης ανά πάσα στιγμή της συγκατάθεσης (χωρίς αναδρομική ισχύ) που έχει παρασχεθεί στη PREMIA από τα αφορώντα φυσικά πρόσωπα, σε περίπτωση που η επεξεργασία των προσωπικών δεδομένων βασίζεται σε συγκατάθεση.

Τα εν λόγω δικαιώματα, οφειλετών και μη, μπορεί να περιοριστούν λόγω υποχρέωσης εφαρμογής άλλου νόμου, όπως για παράδειγμα στην περίπτωση που υπάρξει αίτηση διαγραφής δεδομένων, ενώ η PREMIA υποχρεούται να τα διατηρήσει βάσει νόμου.

- Οιοδήποτε αίτημα οφειλετών απαντάται, χωρίς καθυστέρηση και σε κάθε περίπτωση εντός μηνός από την παραλαβή του αιτήματος, εκτός εξαιρετικών περιπτώσεων, οπότε η ανωτέρω προθεσμία μπορεί να παραταθεί κατά δυο ακόμη μήνες, εφόσον απαιτείται, λαμβανομένων υπόψη της πολυπλοκότητας του αιτήματος ή και του αριθμού των αιτημάτων. Σε αυτή την περίπτωση η PREMIA θα παρέχει σχετική ενημέρωση για τους λόγους της καθυστέρησης εντός μηνός από την παραλαβή του αιτήματος.

8. Δικαίωμα καταγγελίας

Επίσης, σε περίπτωση που θεωρηθεί από τα φυσικά πρόσωπα ότι προσβάλλονται τα δικαιώματα περί προστασίας των προσωπικών δεδομένων διατηρείται το δικαίωμα υποβολής καταγγελίας στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Λ. Κηφισίας 1-3, Τ.Κ. 115 23, Αθήνα, τηλ.: +30 2106475600, fax.: +30 210 6475628, email: complaints@dpa.gr).

Επίσης υπάρχει δικαίωμα προσφυγής στις αρμόδιες δικαστικές αρχές για την προστασία των προσωπικών δεδομένων.

9. Μέτρα ασφαλείας

9.1 Γενικά

Η PREMIA έχει λάβει τα κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται η εφαρμογή της νομοθεσίας και το κατάλληλο επίπεδο ασφάλειας των προσωπικών δεδομένων. Επιπλέον, έχει εκπαιδεύσει προσηκόντως το προσωπικό της (και δεσμεύει όλους τους

συνεργάτες της, οι οποίοι ενεργούν για λογαριασμό της ως Εκτελούντες την Επεξεργασία με συμβάσεις που διέπονται από τα εχέγγυα και τις διασφαλίσεις του νομικού πλαισίου προστασίας προσωπικών δεδομένων.

9.1.1 Μεταφορά Προσωπικών Δεδομένων με ηλεκτρονικό ταχυδρομείο

Η μεταφορά μέσω ηλεκτρονικού ταχυδρομείου είναι ο πιο συνήθης τρόπος για μεταφορά δεδομένων. Η εταιρεία χρησιμοποιεί Microsoft Exchange Online και η επικοινωνία των email πραγματοποιείται με ασφαλή τρόπο (TLS).

9.1.2. Μεταφορά Δεδομένων Μέσω Ψηφιακών Μέσων

Η κρυπτογράφηση είναι υποχρεωτική και κατά τη μεταφορά με χρήση ψηφιακών μέσων (USB stick, CD , DVD, κ.α.).

Η κρυπτογράφηση των δεδομένων για τη μεταφορά τους με χρήση USB επιτυγχάνεται με τη χρήση της εφαρμογής BitLocker, η οποία περιλαμβάνεται στο χρησιμοποιούμενο λειτουργικό σύστημα των υπολογιστών (desktop / laptop), για όσους εργαζομένους είναι εξουσιοδοτημένοι και έχουν πρόσβαση στη USB θύρα.

9.1.3. Μεταφορά Δεδομένων Μέσω Δικτύων

Κατά τη μεταφορά δεδομένων μέσω δικτύων (π.χ. ανταλλαγή αρχείων με υπεύθυνους επεξεργασίας και εκτελούντες την επεξεργασία) είναι υποχρεωτική η χρήση πρωτόκολλων επικοινωνίας που παρέχουν κρυπτογράφηση (χρήση FTP over TLS 1.2).

B. Διαδικασία διαχείρισης παραβίασης δεδομένων προσωπικού χαρακτήρα

Το νομικό πλαίσιο προστασίας προσωπικών δεδομένων, λαμβάνοντας υπόψη την ασφάλεια των δεδομένων προσωπικού χαρακτήρα, ορίζει αυστηρότερες απαιτήσεις γνωστοποίησης παραβίασης δεδομένων προσωπικού χαρακτήρα σε ολόκληρη την Ευρώπη. Σύμφωνα με αυτό, όλες οι οντότητες υποχρεούνται να αναφέρουν ορισμένες παραβιάσεις δεδομένων προσωπικού χαρακτήρα στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και σε ορισμένες περιπτώσεις στα υποκείμενα των δεδομένων που επεξεργάζεται.

Η PREMIA, η οποία ενεργεί ως υπεύθυνος επεξεργασίας των δεδομένων προσωπικού χαρακτήρα των εργαζομένων της, των προμηθευτών της, των μισθωτών της, των συνεργατών της, των ταχυμεταφορέων και επισκεπτών, έχει υιοθετήσει αυτή την διαδικασία για να ανταποκριθεί στις προαναφερθείσες ρυθμιστικές και νομικές υποχρεώσεις.

1. Σκοπός και Πεδίο Εφαρμογής Διαδικασίας

Η PREMIA δεσμεύεται να διασφαλίζει τη δίκαιη, διαφανή και νόμιμη επεξεργασία των δεδομένων προσωπικού χαρακτήρα των εργαζομένων της, των προμηθευτών της, των μισθωτών της, των συνεργατών της, των ταχυμεταφορέων και επισκεπτών της. Η διαδικασία αυτή θεσπίζει οργανωτικά και τεχνικά μέτρα για να διασφαλίσει ότι οι υποχρεώσεις γνωστοποίησης παραβίασης δεδομένων προσωπικού χαρακτήρα αντιμετωπίζονται με συνοχή και ει δυνατόν, σε εύθετο χρόνο.

Η διαδικασία αυτή ισχύει για όλους τους εργαζόμενους, αντιπροσώπους, εργολάβους και εν γένει προμηθευτές, συμπεριλαμβανομένων των εκτελούντων την επεξεργασία και λοιπών αποδεκτών, και δημιουργεί ένα ελάχιστο πλαίσιο για την προστασία δεδομένων προσωπικού χαρακτήρα.

Το προσωπικό της PREMIA πρέπει να λαμβάνει όλα τα κατάλληλα μέτρα για να διασφαλίζει ότι η επεξεργασία των δεδομένων προσωπικού χαρακτήρα, συμμορφώνεται με την παρούσα διαδικασία. Το προσωπικό της PREMIA καλείται περαιτέρω, να υποβάλλει τυχόν ερωτήματα σχετικά με την παρούσα διαδικασία, καθώς και την εν γένει νομιμότητα της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα, χρησιμοποιώντας τα ακόλουθα στοιχεία επικοινωνίας:

2. Νομική Βάση

Η διαδικασία αυτή είναι σύμφωνη με το νομικό πλαίσιο προστασίας προσωπικών δεδομένων για την προστασία του ατόμου από την επεξεργασία των προσωπικών του δεδομένων, όπως τροποποιείται και ισχύει, καθώς και κάθε άλλη εφαρμοστέα νομοθεσία / γνωμοδότηση / απόφαση που εκδίδει η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα ή οποιαδήποτε σχετική νομοθεσία που αφορά τον κλάδο.

3. Ορισμός της Παραβίασης Δεδομένων Προσωπικού Χαρακτήρα

Το άρθρο 4 (12) του ΓΚΠΔ ορίζει την «Παραβίαση Δεδομένων Προσωπικού Χαρακτήρα» ως:

«η παραβίαση της ασφάλειας 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 προαναφερθείσα παραβίαση μπορεί να περιλαμβάνει ηλεκτρονικά ή έντυπα αρχεία.

Σενάρια

Απώλεια Δεδομένων

- Μια βάση δεδομένων που περιέχει δεδομένα προσωπικού χαρακτήρα καταστράφηκε ακούσια λόγω ανθρωπίνου σφάλματος ενός διαχειριστή συστήματος. Υπάρχει ένα

πλήρες και ενημερωμένο αντίγραφο ασφαλείας της βάσης δεδομένων, βάσει του οποίου η βάση δεδομένων μπορεί να αποκατασταθεί άμεσα. Σε αυτή την περίπτωση δεν έχει σημειωθεί Παραβίαση Δεδομένων Προσωπικού Χαρακτήρα, αφού τα δεδομένα είναι ανακτήσιμα.

- Έντυπα που περιέχουν δεδομένα προσωπικού χαρακτήρα έχουν κλαπεί. Αυτό θα ήταν μια Παραβίαση Δεδομένων Προσωπικού Χαρακτήρα λόγω της απώλειας και της άνευ άδειας κοινολόγησης των δεδομένων προσωπικού χαρακτήρα.

Παράνομη επεξεργασία

- Ένα αρχείο δεδομένων που περιέχει δεδομένα προσωπικού χαρακτήρα έχει μεταφορτωθεί (εκ προθέσεως ή κατά λάθος) σε ένα δημόσια προσβάσιμο διακομιστή. Αυτό θα ήταν μια Παραβίαση Δεδομένων Προσωπικού Χαρακτήρα λόγω μη εξουσιοδοτημένου χειρισμού των δεδομένων προσωπικού χαρακτήρα.
- Ένας υπάλληλος έχει παράσχει σε έναν τρίτο, το όνομα χρήστη και τον κωδικό του/της, τα οποία δίνουν στον μη εξουσιοδοτημένο τρίτο πρόσβαση σε όλα τα δεδομένα οφειλετών της εκκαθάρισης. Αυτό θα ήταν μια Παραβίαση Δεδομένων Προσωπικού Χαρακτήρα λόγω της μη εξουσιοδοτημένης πρόσβασης και χρήσης των δεδομένων προσωπικού χαρακτήρα.

Άνευ άδειας κοινολόγηση

- Ένας υπάλληλος απέστειλε τυχαία μέσω ηλεκτρονικού ταχυδρομείου μη κρυπτογραφημένα δεδομένα προσωπικού χαρακτήρα σε λάθος οφειλέτη. Αυτό θα ήταν μια Παραβίαση Δεδομένων Προσωπικού Χαρακτήρα λόγω της ακούσιας κοινολόγησης των δεδομένων προσωπικού χαρακτήρα σε τρίτο.
- Τα έγγραφα δύο διαφορετικών μερών έχουν συμπεριληφθεί κατά λάθος σε ένα πακέτο κοινολογώντας έτσι τα δεδομένα προσωπικού χαρακτήρα του καθενός σε ένα μη εξουσιοδοτημένο πρόσωπο. Αυτό θα ήταν μια Παραβίαση Δεδομένων Προσωπικού Χαρακτήρα λόγω της ακούσιας κοινολόγησης των δεδομένων προσωπικού χαρακτήρα σε έναν τρίτο.

4. Υποχρεώσεις του Υπεύθυνου Επεξεργασίας

Σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα, η PREMIA πρέπει, να γνωστοποιεί αμελλητί την παραβίαση των δεδομένων προσωπικού χαρακτήρα στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Συγκεκριμένα, η PREMIA έχει την υποχρέωση:

- να αναφέρει την παραβίαση των δεδομένων προσωπικού χαρακτήρα σύμφωνα με το Άρθρο 33 του ΓΚΠΔ,
- να λάβει τα απαραίτητα οργανωτικά και τεχνικά μέτρα για να περιορίσει την παραβίαση δεδομένων προσωπικού χαρακτήρα,

- να αξιολογήσει την έκταση και τον αντίκτυπο της παραβίασης δεδομένων προσωπικού χαρακτήρα,
- να τεκμηριώσει και καταγράψει την παραβίαση δεδομένων προσωπικού χαρακτήρα,
- να εξετάσει το ενδεχόμενο γνωστοποίησης στα υποκείμενα που επηρεάζονται,
- όταν χρειάζεται να γνωστοποιήσει σε λοιπά μέρη, ήτοι εκτός της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και
- να αποτρέψει μελλοντικές παραβιάσεις δεδομένων προσωπικού χαρακτήρα.

5. Υποχρεώσεις του Εκτελούντος την Επεξεργασία

5.1. Ο εκτελών την επεξεργασία επεξεργάζεται τα προσωπικά δεδομένα αποκλειστικά για τους σκοπούς που ορίζονται στη σύμβαση του με την PREMIA (υπεύθυνος επεξεργασίας), δυνάμει της οποίας ανατίθεται στον εκτελούντα την επεξεργασία από την PREMIA η εκτέλεση δραστηριοτήτων επεξεργασίας προσωπικών δεδομένων (εφεξής «**Σύμβαση**») σύμφωνα με τις ρητές και καταγεγραμμένες οδηγίες της PREMIA, εκτός εάν ο εκτελών την επεξεργασία υποχρεούται να επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για πρόσθετους σκοπούς σύμφωνα με το νομοθετικό πλαίσιο. Σε τέτοιες περιπτώσεις, ο εκτελών την επεξεργασία, θα πρέπει να ειδοποιήσει αμελλητί και προσηκόντως την PREMIA πριν από οποιαδήποτε περαιτέρω επεξεργασία, εκτός αν υπάρχει ρητή απαγόρευση να το πράξει βάσει του νομοθετικού πλαισίου. Σε οποιαδήποτε άλλη περίπτωση κατά την οποία ο εκτελών την επεξεργασία αποκλίνει από τις οδηγίες της PREMIA και προσδιορίζει τους σκοπούς και τα μέσα επεξεργασίας, ο εκτελών την επεξεργασία αποκτά την ιδιότητα του υπευθύνου επεξεργασίας και φέρει ο ίδιος πλήρη και αποκλειστική ευθύνη έναντι των υποκειμένων των δεδομένων και των αρμόδιων αρχών.

5.2. Ο εκτελών την επεξεργασία υποχρεούται να ενημερώνει ανά πάσα στιγμή και προσηκόντως την PREMIA για έννομες υποχρεώσεις που υπέχει και που καθιστούν παράνομη ή πρακτικά αδύνατη τη συμμόρφωση με τις οδηγίες της PREMIA.

5.3. Ο εκτελών την επεξεργασία έχει την υποχρέωση να ενημερώνει αμελλητί και προσηκόντως τον υπεύθυνο επεξεργασίας (την PREMIA) για κάθε περιστατικό παραβίασης προσωπικών δεδομένων που ανήκουν στον υπεύθυνο επεξεργασίας και που υποπίπτει στην αντίληψή του. Η ενημέρωση θα λαμβάνει χώρα άμεσα, χωρίς αδικαιολόγητη καθυστέρηση, και σε κάθε περίπτωση εντός είκοσι τεσσάρων (24) ωρών το αργότερο από τον χρόνο κατά τον οποίο αποδεδειγμένα έγινε γνωστό για πρώτη φορά το περιστατικό παραβίασης. Οι ακριβείς απαιτήσεις αυτής της ενημέρωσης θα προσδιορίζονται στη Σύμβαση μεταξύ του υπευθύνου επεξεργασίας (την PREMIA) και του εκτελούντος την επεξεργασία.

5.4. Ο εκτελών την επεξεργασία δεν προσλαμβάνει άλλον εκτελούντα την επεξεργασία χωρίς προηγούμενη ειδική ή γενική γραπτή άδεια και συναίνεση της PREMIA.

5.5. Ο εκτελών την επεξεργασία διασφαλίζει ότι το προσωπικό του ή/και τα πρόσωπα που είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα έχουν αναλάβει δέσμευση τήρησης εμπιστευτικότητας ή τελούν υπό τη δέουσα κανονιστική υποχρέωση τήρησης εμπιστευτικότητας.

5.6. Ο εκτελών την επεξεργασία θέτει στη διάθεση της PREMIA όλες τις απαραίτητες πληροφορίες και τα σχετικά έγγραφα προκειμένου το τελευταίο να είναι σε θέση να αποδείξει ότι συμμορφώνεται με τις υποχρεώσεις που επιβάλλονται από το νομικό πλαίσιο προστασίας προσωπικών δεδομένων σχετικά με την ανάθεση εκτέλεσης δραστηριοτήτων επεξεργασίας προσωπικών δεδομένων στον εκτελούντα την επεξεργασία και επιτρέπει και διευκολύνει τους ελέγχους, περιλαμβανομένων των επιθεωρήσεων, που δύναται να διενεργούνται από την PREMIA.

5.7. Η PREMIA έχει δικαίωμα κατά τη διακριτική της ευχέρεια να ζητήσει από τον εκτελούντα την επεξεργασία τη διαγραφή ή την επιστροφή των δεδομένων προσωπικού χαρακτήρα που του ανήκουν, μετά τη λύση της Σύμβασης με οποιοδήποτε τρόπο. Μετά την τυχόν επιστροφή των δεδομένων προσωπικού χαρακτήρα στην PREMIA, ο εκτελών την επεξεργασία διαγράφει το σύνολο των προσωπικών δεδομένων από τα συστήματά του, εκτός αν επιβάλλονται άλλες υποχρεώσεις από διατάξεις του εθνικού ή/και ευρωπαϊκού δικαίου.

5.8. Οι περαιτέρω κάθε φορά υποχρεώσεις του εκτελούντος την επεξεργασία θα προσδιορίζονται στη Σύμβαση μεταξύ της PREMIA, ως υπεύθυνου επεξεργασίας και του εκτελούντος την επεξεργασία, στην οποία θα καθορίζεται και το αντικείμενο και η διάρκεια της επεξεργασίας, η φύση και ο σκοπός της επεξεργασίας, το είδος των δεδομένων προσωπικού χαρακτήρα και οι κατηγορίες των υποκειμένων των δεδομένων και οι υποχρεώσεις και τα δικαιώματα της PREMIA.

6. Αναλυτική Περιγραφή Διαχείρισης Παραβίασης Δεδομένων Προσωπικού Χαρακτήρα

Οι παρακάτω ενότητες περιγράφουν λεπτομερώς τα βήματα της διαδικασίας διαχείρισης παραβίασης δεδομένων προσωπικού χαρακτήρα.

6.1 ΑΝΑΓΝΩΡΙΣΗ & ΑΡΧΙΚΗ ΔΙΑΒΟΥΛΕΥΣΗ (ΒΗΜΑ 1)

Η επιτυχής αντιμετώπιση πιθανών περιστατικών εξαρτάται από την έγκαιρη ανίχνευση και γνωστοποίηση των γεγονότων. Για το σκοπό αυτό, θα πρέπει να δημιουργηθεί ένα σημείο επικοινωνίας το οποίο θα λειτουργεί ως κεντρικό κανάλι αναφοράς για όλα τα περιστατικά παραβίασης δεδομένων προσωπικού χαρακτήρα, το οποίο θα παρέχει έναν μηχανισμό αναφοράς περιστατικών 24 ώρες την ημέρα, 7 μέρες την εβδομάδα.

Είναι υψίστης σημασίας όλοι οι εργαζόμενοι, οι συνεργάτες, οι εξωτερικοί συνεργάτες, οι εκπρόσωποι, οι εκτελούντες την επεξεργασία δεδομένων προσωπικού χαρακτήρα να κατανοούν σαφώς τι συνιστά ένα περιστατικό και σε ποιους πρέπει να αναφέρεται. Μόλις ένα άτομο αντιληφθεί ότι ένα περιστατικό έχει λάβει ή λαμβάνει χώρα, θα πρέπει να αναφέρει αμέσως και χωρίς καθυστέρηση το συμβάν στην Διοίκηση της Εταιρείας.

Μετά τη λήψη γνωστοποίησης περί παραβίασης δεδομένων προσωπικού χαρακτήρα, η Διοίκηση της Εταιρείας, πρέπει να επικοινωνήσει με το άτομο που εκκίνησε την αναφορά και να προβεί σε αρχική εκτίμηση για το κατά πόσον συνέβη ή ενδέχεται να συμβαίνει κάποιο περιστατικό. Σε καταφατική περίπτωση, η Διοίκηση θα πρέπει:

- Να συγκεντρώσει πληροφορίες σχετικά με τη φύση και την έκταση του συμβάντος,
- Να καθορίσει σε αρχικό επίπεδο αν υπάρχει κάποια εύλογη πιθανότητα τα δεδομένα να έχουν κοινολογηθεί χωρίς αδείας ή εξ' αιτίας μη ορθής χρήσης,
- Να προσδιορίσει και να προσπαθήσει να ανακτήσει τα απολεσθέντα δεδομένα, να περιορίσει τον αντίκτυπο και εάν είναι δυνατόν να αποτρέψει περαιτέρω ζημιές,
- Εφόσον η διαβάθμιση της παραβίασης κριθεί από την Νομική Υπηρεσία σημαντική, να ειδοποιήσει άμεσα τη Διοίκηση,
- Εάν απαιτείται, να ζητήσει τη συνδρομή εμπειρογνομόνων.

Οι εν λόγω ενέργειες πρέπει να ολοκληρωθούν εντός 24 ωρών από τη γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα.

6.2 ΔΙΕΡΕΥΝΗΣΗ & ΑΞΙΟΛΟΓΗΣΗ (ΒΗΜΑ 2)

Βάσει του αποτελέσματος του Βήματος 1, ενδέχεται να απαιτείται περαιτέρω ανάλυση και έρευνα από την Διοίκηση της Εταιρείας, ή/και εξωτερικούς εμπειρογνώμονες, προκειμένου να ληφθούν πληροφορίες και αποδεικτικά στοιχεία σχετικά με το περιστατικό και να εκτιμηθεί το επίπεδο κινδύνου και αντίκτυπου.

Με τη συλλογή των απαιτούμενων στοιχείων, η Διοίκηση της Εταιρείας πρέπει να καλεί όλα τα βασικά ενδιαφερόμενα μέρη να συμμετάσχουν στις διαβουλεύσεις για τη διαχείριση της κρίσης. Η διαβούλευση αυτή πρέπει να οδηγήσει στην εκπόνηση και εφαρμογή σχεδίου αντιμετώπισης που θα θέτει προτεραιότητες, με βάση το χρονοδιάγραμμα, τον κίνδυνο και τον αντίκτυπο, συμπεριλαμβανομένων τυχόν ενεργειών για τον περιορισμό του συμβάντος.

Η διερεύνηση και η αξιολόγηση πρέπει να πραγματοποιηθούν εντός 24 ωρών από την ολοκλήρωση του Βήματος 1 και το αργότερο εντός 48 ωρών από την γνωστοποίηση παραβίασης των δεδομένων προσωπικού χαρακτήρα.

6.3 ΓΝΩΣΤΟΠΟΙΗΣΗ & ΑΠΟΚΑΤΑΣΤΑΣΗ (ΒΗΜΑ 3)

Η Διοίκηση της Εταιρείας αποφασίζει συντρέχει κάποια υποχρέωση γνωστοποίησης, δηλαδή εάν:

1. Η PREMIA πρέπει, να ενημερώσει την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα για τυχόν παραβίαση δεδομένων προσωπικού χαρακτήρα, η οποία ενδέχεται να θέσει σε κίνδυνο τα δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων.
2. Η PREMIA πρέπει να ενημερώσει επίσης το(τα) πρόσωπο(-α) που επηρεάζονται όταν η παραβίαση δεδομένων προσωπικού χαρακτήρα ενδέχεται να οδηγήσει σε «υψηλό κίνδυνο» για τα δικαιώματα και τις ελευθερίες του ατόμου(-ων).

Γνωστοποίηση στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ)

Εάν πρέπει να πραγματοποιηθεί γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, αυτή θα πρέπει να πραγματοποιηθεί εντός 72 ωρών από τη στιγμή που η PREMIA έλαβε γνώση του γεγονότος και θα πρέπει να περιλαμβάνει τις ακόλουθες πληροφορίες:

- Περιγραφή της φύσης της παραβίασης δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων, όπου είναι δυνατό, των κατηγοριών και του κατά προσέγγιση αριθμού των επηρεαζόμενων υποκειμένων δεδομένων, καθώς και των κατηγοριών και του κατά προσέγγιση αριθμού των επηρεαζόμενων αρχείων δεδομένων προσωπικού χαρακτήρα,
- Περιγραφή των ενδεχόμενων συνεπειών της παραβίασης των δεδομένων προσωπικού χαρακτήρα,
- Περιγραφή των ληφθέντων ή των προτεινόμενων προς λήψη μέτρων από την PREMIA, για την αντιμετώπιση της παραβίασης των δεδομένων προσωπικού χαρακτήρα, καθώς και, όπου ενδείκνυται, τη λήψη μέτρων για την άμβλυνση τυχόν δυσμενών συνεπειών, και
- Αιτιολόγηση για την καθυστέρηση κοινοποίησης, αν η κοινοποίηση πραγματοποιηθεί μετά τις 72 ώρες.

Σε περίπτωση που δεν είναι δυνατόν να παρασχεθούν όλες οι πληροφορίες ταυτόχρονα, μπορούν να παρέχονται σταδιακά χωρίς περαιτέρω αδικαιολόγητη καθυστέρηση.

Γνωστοποίηση στα επηρεαζόμενα υποκείμενα

Γνωστοποιήσεις στα επηρεαζόμενα υποκείμενα πρέπει να περιλαμβάνουν τις ακόλουθες πληροφορίες, ανάλογα με την περίπτωση:

- Ημερομηνία παραβίασης.
- Περιγραφή της παραβίασης (και του εύρους της).
- Περιγραφή των πληροφοριών που διέρρευσαν.
- Κίνδυνος (-οι) για το υποκείμενο που προκύπτει από την παραβίαση.
- Μέτρα που λήφθηκαν για τον περιορισμό της παραβίασης και των δυσμενών συνεπειών από αυτήν.

- Προγραμματισμένα επόμενα βήματα και μακροπρόθεσμοι σχεδιασμοί για την πρόληψη μελλοντικών παραβιάσεων.
- Βήματα που μπορεί να ακολουθήσει το υποκείμενο για να περιορίσει περαιτέρω δυσμενείς συνέπειες ή βήματα που έχει ακολουθήσει η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα για να συνδράμει το υποκείμενο στον περιορισμό αυτό.

Σημειώνεται ότι η επικοινωνία με το επηρεαζόμενο άτομο δεν θα πρέπει να θεωρείται απαραίτητη, εάν πληρούται οποιαδήποτε από τις ακόλουθες προϋποθέσεις:

- (α) Η PREMIA έχει εφαρμόσει τα κατάλληλα τεχνικά και οργανωτικά μέτρα προστασίας και τα μέτρα αυτά εφαρμόστηκαν στα δεδομένα προσωπικού χαρακτήρα που επηρεάστηκαν από την παραβίαση των δεδομένων προσωπικού χαρακτήρα, ιδίως εκείνα που καθιστούν τα δεδομένα ακατάλληλα σε οποιοδήποτε άτομο δεν είναι εξουσιοδοτημένο να έχει πρόσβαση, όπως η κρυπτογράφηση.
- (β) Η γνωστοποίηση συνεπάγεται δυσανάλογη προσπάθεια. Σε αυτή την περίπτωση, πρέπει αντί γνωστοποίησης να γίνει μια δημόσια ανακοίνωση ή να ληφθεί παρόμοιο μέτρο με το οποίο τα υποκείμενα των δεδομένων να ενημερώνονται με εξίσου αποτελεσματικό τρόπο.

6.4 ΑΞΙΟΛΟΓΗΣΗ ΣΥΜΒΑΝΤΩΝ ΣΕ ΥΣΤΕΡΟ ΧΡΟΝΟ (ΒΗΜΑ 4)

Η Διοίκηση της Εταιρείας πρέπει να αναλύσει τη γενεσιουργό αιτία του περιστατικού, προκειμένου να προσδιορίσει εάν το περιστατικό είναι αποτέλεσμα κοινών, συχνά επαναλαμβανόμενων ενεργειών. Σε καταφατική περίπτωση, θα πρέπει να συμπεριλάβει στις μελλοντικές επικοινωνίες του μέτρα ευαισθητοποίησης ως προς την πρόληψη και τις σχετικές διορθωτικές ενέργειες και να ενσωματώσει τις βέλτιστες πρακτικές στο πλαίσιο της συνεχούς βελτίωσης. Η Διοίκηση της Εταιρείας θα πρέπει να εξετάσει επίσης εάν υπάρχει ανάγκη αλλαγής, τροποποίησης ή προσθήκης κάποιας πολιτικής, κατευθυντήριων γραμμών ή διαδικασιών για να συμβάλλει στην μείωση του κινδύνου παρόμοιων περιστατικών στο μέλλον.

Τεκμηρίωση και καταχώρηση παραβίασης δεδομένων προσωπικού χαρακτήρα

Μετά την ολοκλήρωση της προαναφερόμενης διαδικασίας, η Διοίκηση της Εταιρείας θα πρέπει να καταγράψει κάθε περιστατικό σε αντίστοιχο εσωτερικό μητρώο καταγραφής περιστατικών. Το μητρώο πρέπει να περιλαμβάνει πληροφορίες σχετικά με την παραβίαση των δεδομένων προσωπικού χαρακτήρα, τα αποτελέσματά της και τα επανορθωτικά μέτρα που ελήφθησαν, συμπεριλαμβανομένων, μεταξύ άλλων:

- Ημερομηνία και χρόνος έναρξης/λήξης της παραβίασης,
- Πότε η PREMIA έλαβε γνώση της παραβίασης,
- Περιγραφή των γεγονότων της παραβίασης,
- Τύπος δεδομένων προσωπικού χαρακτήρα που επηρεάζονται,

- Αριθμός ατόμων που επηρεάζονται,
- Τυχόν υπό- εκτελούντες την επεξεργασία (sub-processors) που εμπλέκονται,
- Πιθανές συνέπειες για τα υποκείμενα που επηρεάζονται,
- Ενέργειες που ελήφθησαν ως απάντηση στο περιστατικό, ώστε να μειωθούν οι δυσμενείς συνέπειες και η πιθανότητα παρόμοιας επανεμφάνισης.

Παράρτημα 1: Υπόδειγμα Φόρμας Γνωστοποίησης Παραβίασης Δεδομένων Προσωπικού χαρακτήρα Αναφορά Πιθανής Παραβίασης

• Ονοματεπώνυμο αναφέροντος _____ • Πηγή(π.χ. πελάτης, ανώνυμο, αρχές) _____		• E-mail & τηλέφωνο αναφέροντος _____ • Ημερομηνία / Ώρα _____			
Σοβαρότητα Περιστατικού • Κατηγορία 1 ☐ • Κατηγορία 2 ☐ • Κατηγορία 3 ☐ • Κατηγορία 4 ☐					
Αναφορά • Πότε έγινε γνωστό _____ • Που _____ • Πως _____					
Συνοπτική Αναφορά • Πλήθος Δεδομένων _____ • Από που κλάπηκαν _____ • Γιατί είναι σε ρίσκο _____ • Τα δεδομένα είναι κρυπτογραφημένα; _____					
Τύπος ρίσκου Δεδομένων <table border="0"> <tr> <td> • Ονόματα ☐ • Κωδικοί / Passwords ☐ • Credit / Debit cards ☐ • Τραπεζικοί Λογαριασμοί ☐ • Email διευθύνσεις ☐ • Κείμενο σε e-mails ☐ • Τηλέφωνα ☐ • Διευθύνσεις ☐ • Στοιχεία προσωπικού ☐ </td> <td> • ΑΜΚΑ ☐ • Ασφαλιστήρια Συμβόλαια, ☐ • Ιατρικά Στοιχεία ☐ • Αρ. Ταυτότητας ή Αρ. Διαβατηρίου ☐ • Αρ. Διπλώματος Οδήγησης ☐ • Σχέδια, οικονομικές πληροφορίες, αρχεία ☐ • Άλλα ευαίσθητα προσωπικά δεδομένα ☐ • Άλλες ευαίσθητες πληροφορίες ☐ • Συμβατικά Κείμενα, Δικόγραφα, Εξώδικα Αξιόγραφα, κτλ. ☐ </td> </tr> </table>				• Ονόματα ☐ • Κωδικοί / Passwords ☐ • Credit / Debit cards ☐ • Τραπεζικοί Λογαριασμοί ☐ • Email διευθύνσεις ☐ • Κείμενο σε e-mails ☐ • Τηλέφωνα ☐ • Διευθύνσεις ☐ • Στοιχεία προσωπικού ☐	• ΑΜΚΑ ☐ • Ασφαλιστήρια Συμβόλαια, ☐ • Ιατρικά Στοιχεία ☐ • Αρ. Ταυτότητας ή Αρ. Διαβατηρίου ☐ • Αρ. Διπλώματος Οδήγησης ☐ • Σχέδια, οικονομικές πληροφορίες, αρχεία ☐ • Άλλα ευαίσθητα προσωπικά δεδομένα ☐ • Άλλες ευαίσθητες πληροφορίες ☐ • Συμβατικά Κείμενα, Δικόγραφα, Εξώδικα Αξιόγραφα, κτλ. ☐
• Ονόματα ☐ • Κωδικοί / Passwords ☐ • Credit / Debit cards ☐ • Τραπεζικοί Λογαριασμοί ☐ • Email διευθύνσεις ☐ • Κείμενο σε e-mails ☐ • Τηλέφωνα ☐ • Διευθύνσεις ☐ • Στοιχεία προσωπικού ☐	• ΑΜΚΑ ☐ • Ασφαλιστήρια Συμβόλαια, ☐ • Ιατρικά Στοιχεία ☐ • Αρ. Ταυτότητας ή Αρ. Διαβατηρίου ☐ • Αρ. Διπλώματος Οδήγησης ☐ • Σχέδια, οικονομικές πληροφορίες, αρχεία ☐ • Άλλα ευαίσθητα προσωπικά δεδομένα ☐ • Άλλες ευαίσθητες πληροφορίες ☐ • Συμβατικά Κείμενα, Δικόγραφα, Εξώδικα Αξιόγραφα, κτλ. ☐				

Τύπος Περιστατικού			
• Παραβίαση Δικτύου ή Servers	☐	• Απώλεια, κλοπή, παραβίαση Software	☐
• Απώλεια ή κλοπή ή παραβίαση υπολογιστών ή μέσων αποθήκευσης δεδομένων	☐	• Hacking σε συστήματα	☐
		• Μη εξουσιοδοτημένη πρόσβαση σε sites που περιέχουν ευαίσθητες πληροφορίες	☐
		Άλλο	☐
ΠΕΡΙΓΡΑΦΗ ΠΕΡΙΣΤΑΤΙΚΟΥ:			