ΔΙΑΔΙΚΑΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΠΕΡΙΣΤΑΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ

ΣΧΕΤΙΚΑ ΜΕ ΤΗΝ ΕΠΕΞΕΡΓΑΣΙΑ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Πειραιάς, Μάρτιος 2021

ΚΑΤΑΣΤΑΣΗ ΑΝΑΘΕΩΡΗΣΕΩΝ

Αριθμός Έκδοσης	Ημερομηνία Έναρξης Ισχύος	Αιτιολογία
		Αρχική Έκδοση

Πίνακας Περιεχομένων

I. ΕΙΣΑΓΩΓΗ – ΣΚΟΠΟΣ

Σκοπός της Διαδικασίας Διαχείρισης Περιστατικών Ασφαλείας σχετικά με την επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα (εφεξής «Διαδικασία») είναι η διασφάλιση της συμμόρφωσης της ανώνυμης εταιρείας με την επωνυμία **«AEGEAN CONTAINER AGENCY S.A. ΝΑΥΤΙΛΙΑΚΟ ΠΡΑΚΤΟΡΕΙΟ ΜΟΝ/ΠΗ Α.Ε.»** και το δ.τ. **«**AEGEAN CONTAINER AGENCY S.A.**»** (εφεξής «Εταιρεία») με τις επιταγές του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (στο εξής «Κανονισμός») αναφορικά με την αποτελεσματική αντιμετώπιση πιθανής Παραβίασης Προσωπικών Δεδομένων, τη γνωστοποίησή της στην εποπτική αρχή και την ενημέρωση των Υποκειμένων σύμφωνα με τα Άρθρα 33 και 34 του Κανονισμού.

Η Εταιρεία, ως Υπεύθυνος Επεξεργασίας, επεξεργάζεται Προσωπικά Δεδομένα Υποκειμένων, εφαρμόζοντας τα κατάλληλα τεχνικά και οργανωτικά μέτρα για τη διασφάλιση της προστασίας τους.

Η Εταιρεία είναι υποχρεωμένη σύμφωνα με τις επιταγές του Κανονισμού να θεσπίσει ένα πλαίσιο προστασίας των Προσωπικών Δεδομένων, συμπεριλαμβανομένων σαφών αρμοδιοτήτων των εργαζομένων. Αυτή η Διαδικασία καθορίζει το πλαίσιο για μια συνεπή και αποτελεσματική προσέγγιση στη διαχείριση περιστατικών παραβίασης δεδομένων και ασφάλειας των πληροφοριών.

II. ΟΡΙΣΜΟΙ – ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ

Περιστατικό Παραβίασης Προσωπικών Δεδομένων ή Περιστατικό: κάθε περιστατικό παραβίασης της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση σε Προσωπικά Δεδομένα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε Επεξεργασία.

Προσωπικά Δεδομένα: κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο και του οποίου η ταυτότητα μπορεί να εξακριβωθεί άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως, κατ' ενδεικτική και όχι περιοριστική απαρίθμηση, ονοματεπώνυμο, τηλέφωνο, ηλεκτρονική διεύθυνση επικοινωνίας, αριθμό ταυτότητας, αριθμό φορολογικού μητρώου (ΑΦΜ).

Ειδικές Κατηγορίες Προσωπικών Δεδομένων («Ευαίσθητα Προσωπικά Δεδομένα»): Δεδομένα προσωπικού χαρακτήρα που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε

συνδικαλιστική οργάνωση, καθώς και γενετικά δεδομένα, βιομετρικά δεδομένα, δεδομένα που αφορούν στην υγεία ή στη σεξουαλική ζωή ή στο γενετήσιο προσανατολισμό του φυσικού προσώπου.

Αρμόδιος για θέματα προστασίας προσωπικών δεδομένων εντός της Εταιρείας: Λειτουργεί ως σημείο επικοινωνίας, τόσο εσωτερικά όσο και εξωτερικά, συνεργάζεται με την εποπτική αρχή και εκτελεί τα καθήκοντά του σύμφωνα με τις εσωτερικές πολιτικές και διαδικασίες της Εταιρείας.

Υποκείμενο των Προσωπικών Δεδομένων ή Υποκείμενο: Το ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο στο οποίο αφορούν τα Προσωπικά Δεδομένα ή/και τα Ευαίσθητα Προσωπικά Δεδομένα.

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, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλης μορφής διάθεση, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή.

Υπεύθυνος Επεξεργασίας: Για τους σκοπούς της Διαδικασίας, ως Υπεύθυνος Επεξεργασίας νοείται η Εταιρεία που καθορίζει τους σκοπούς και τον τρόπο επεξεργασίας των Προσωπικών Δεδομένων.

Εκτελών την Επεξεργασία: Το φυσικό ή νομικό πρόσωπο, η Δημόσια Αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται Προσωπικά Δεδομένα για λογαριασμό του Υπεύθυνου Επεξεργασίας.

III. ΒΑΣΙΚΕΣ ΚΑΤΗΓΟΡΙΕΣ ΚΑΙ ΠΑΡΑΔΕΙΓΜΑΤΑ ΠΑΡΑΒΙΑΣΗΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Ένα περιστατικό Παραβίασης Προσωπικών Δεδομένων περιλαμβάνει αλλά δεν περιορίζεται στα παρακάτω:

- Απώλεια, κλοπή ή βλάβη εξοπλισμού, ο οποίος χρησιμοποιείται για τη φύλαξη ή την επεξεργασία απλών ή/και ευαίσθητων προσωπικών δεδομένων (π.χ. απώλεια φορητού υπολογιστή, συσκευή USB, συσκευή iPad / tablet ή χαρτί)
- Μη εξουσιοδοτημένη χρήση, πρόσβαση ή τροποποίηση δεδομένων ή πληροφοριακών συστημάτων
- Προσπάθειες (αποτυχημένες ή επιτυχημένες) να αποκτηθεί πρόσβαση σε προσωπικά δεδομένα ή σε πληροφοριακά συστήματα που φυλάσσονται ή επεξεργάζονται προσωπικά δεδομένα

- Μη εξουσιοδοτημένη αποκάλυψη απλών ή/και ευαίσθητων προσωπικών δεδομένων
- Υποκλοπή ιστότοπου
- Κακόβουλη επίθεση στα πληροφοριακά συστήματα, από την οποία προέκυψε ή ενδέχεται να προέκυψε διαρροή ή απώλεια προσωπικών δεδομένων
- Απρόβλεπτες καταστάσεις (π.χ. πυρκαγιά, πλημμύρα), από τις οποίες προέκυψε ή ενδέχεται να προέκυψε διαρροή ή απώλεια προσωπικών δεδομένων.
- Ανθρώπινο λάθος, από το οποίο προκλήθηκε διαρροή ή απώλεια προσωπικών δεδομένων.
- Απώλεια εγγράφου με προσωπικά δεδομένα ή έκθεση του σε μη εξουσιοδοτημένα πρόσωπο.

IV. ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Όλοι οι εργαζόμενοι της Εταιρείας πρέπει να λαμβάνουν γνώση της Διαδικασίας, να την κατανοούν και να συμμορφώνονται με αυτή. Επίσης, υποχρεούνται να αναφέρουν εγκαίρως κάθε Περιστατικό Παραβίασης Προσωπικών Δεδομένων.

Ο αρμόδιος για θέματα προστασίας προσωπικών δεδομένων εντός της Εταιρείας είναι υπεύθυνος για την αξιολόγηση κάθε Περιστατικού Παραβίασης Προσωπικών Δεδομένων καθώς και για τη διερεύνηση του Περιστατικού, διασφαλίζοντας ότι τηρούνται όλα τα βήματα αντιμετώπισης που ορίζονται στη Διαδικασία αυτή.

Ο αρμόδιος για θέματα προστασίας προσωπικών δεδομένων εντός της Εταιρείας αξιολογεί και διερευνά τα Περιστατικά Παραβίασης Προσωπικών Δεδομένων, διατηρεί και ενημερώνει το αρχείο περιστατικών ασφαλείας, προβαίνει στις αναγκαίες κοινοποιήσεις στο πλαίσιο του Κανονισμού και εφαρμόζει όλα τα μέτρα ασφαλείας που κρίνονται απαραίτητα για την ελαχιστοποίηση του κινδύνου παρόμοιων μελλοντικών περιστατικών.

V. ΔΙΑΔΙΚΑΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΠΕΡΙΣΤΑΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ

Στην παρούσα ενότητα περιγράφονται τα επιμέρους βήματα της Διαδικασίας, αναφέροντας τα μέσα, τους ρόλους, τις ροές της πληροφορίας αλλά και τα χρονικά περιθώρια ανταπόκρισης και αντιμετώπισης των Περιστατικών Παραβίασης Προσωπικών Δεδομένων.

1. Αναφορά Περιστατικού Παραβίασης Προσωπικών Δεδομένων

Κάθε εργαζόμενος της Εταιρείας που θα αντιληφθεί Περιστατικό Παραβίασης Προσωπικών Δεδομένων, έχει την ευθύνη για την άμεση αναφορά του Περιστατικού στον αρμόδιο για θέματα προστασίας προσωπικών δεδομένων εντός της Εταιρείας μέσω τηλεφώνου, email ή με κάθε διαθέσιμο τρόπο επικοινωνίας.

Η αναφορά περιλαμβάνει κατά το δυνατόν πλήρεις και ακριβείς λεπτομέρειες του περιστατικού, πότε συνέβη χρονικά (ημερομηνία και ώρα), ποιός είναι αυτός που το αναφέρει, τη φύση των πληροφοριών, τον αριθμό των ατόμων που εμπλέκονται και κάθε άλλο σχετικό στοιχείο {βλέπε VI. Έντυπο Υποβολής Γνωστοποίησης Περιστατικού Παραβίασης Προσωπικών Δεδομένων (εφεξής «Αναφορά»)}.

Η Αναφορά συμπληρώνεται από τον αρμόδιο για θέματα προστασίας προσωπικών δεδομένων εντός της Εταιρείας με τη συνδρομή του προσώπου που αναφέρει το περιστατικό και αξιοποιώντας κάθε διαθέσιμη πληροφορία. Εν συνεχεία, το Περιστατικό καταγράφεται στο Αρχείο Καταγραφής Περιστατικών Ασφαλείας, το οποίο θα ενημερώνει και θα διαχειρίζεται ο αρμόδιος για θέματα προστασίας προσωπικών δεδομένων εντός της Εταιρείας.

Ενθαρρύνεται η αναφορά και των παρ' ολίγον Περιστατικών Παραβίασης Προσωπικών Δεδομένων (δηλαδή συμβάντων τα οποία θα είχαν οδηγήσει σε παραβίαση της ασφάλειας και η οποία δεν έλαβε χώρα λόγω παρέμβασης ή άλλου τυχαίου γεγονότος) για την καλύτερη πρόληψη των κινδύνων που αντιμετωπίζει η Εταιρεία καθώς και για την αποφυγή Περιστατικών Παραβίασης Προσωπικών Δεδομένων. Τα παρ' ολίγον Περιστατικά θα πρέπει να αναφέρονται με την ίδια διαδικασία που ισχύει για τα πραγματικά Περιστατικά Παραβίασης Προσωπικών Δεδομένων, με την ένδειξη όμως ότι πρόκειται για παρ' ολίγον Περιστατικά.

2. Περιορισμός και διερεύνηση περιστατικού

Μόλις ο αρμόδιος για θέματα προστασίας προσωπικών δεδομένων εντός της Εταιρείας ενημερωθεί σχετικά με πιθανό Περιστατικό Παραβίασης Προσωπικών Δεδομένων και συμπληρώσει ή λάβει τη συμπληρωμένη Αναφορά, πρέπει να ακολουθηθούν τα παρακάτω βήματα:

i. **Διερεύνηση και τεκμηρίωση Περιστατικού Παραβίασης Προσωπικών Δεδομένων**: Ανάλογα με τον είδος και τη σοβαρότητα του Περιστατικού Παραβίασης Προσωπικών Δεδομένων, ο αρμόδιος για θέματα προστασίας προσωπικών δεδομένων εντός της Εταιρείας αξιολογεί εάν απαιτείται η

περαιτέρω διερεύνησή του ώστε να τεκμηριωθεί το Περιστατικό. Εφόσον τεκμηριωθεί η παραβίαση, πρέπει να εκτιμηθεί η βαρύτητα και η σοβαρότητα αυτής και ειδικά εάν είναι πιθανό από την παραβίαση να επέλθει υψηλός κίνδυνος για τα δικαιώματα και τις ελευθερίες των Υποκειμένων των Προσωπικών Δεδομένων.

ii. **Περιορισμός Εξέλιξης Περιστατικού:** Ο αρμόδιος για θέματα προστασίας προσωπικών δεδομένων εντός της Εταιρείας προσδιορίζει αν το περιστατικό παραβίασης εξακολουθεί να είναι σε εξέλιξη και, σε καταφατική περίπτωση, συντονίζει άμεσα τη λήψη των απαραίτητων μέτρων τα οποία θα περιορίσουν την εξέλιξη του περιστατικού.

iii. **Περιορισμός του Αντικτύπου του Περιστατικού:** Εάν είναι εφικτό, μέσα σε 24 ώρες από την αποκάλυψη της Παραβίασης, ο αρμόδιος για θέματα προστασίας προσωπικών δεδομένων εντός της Εταιρείας σε συνεργασία με τη Διοίκηση της Εταιρείας αξιολογούν τον αντίκτυπο της παραβίασης στα Υποκείμενα των Προσωπικών Δεδομένων. Πιο συγκεκριμένα, αξιολογούν τις δυσμενείς επιπτώσεις που ενδέχεται να έχουν προκύψει από το Περιστατικό για τα δικαιώματα και τις ελευθερίες των Υποκειμένων. Στην αξιολόγησή των επιπτώσεων λαμβάνουν υπόψη και τα ακόλουθα:

- Τον τύπο των Προσωπικών Δεδομένων που εμπλέκονται
- Εάν είναι Ευαίσθητα Προσωπικά Δεδομένα
- Εάν είναι ενεργά τα μέτρα προστασίας των Προσωπικών Δεδομένων (π.χ. κρυπτογράφηση)
- Εάν έχουν κλαπεί ή χαθεί Προσωπικά Δεδομένα και ποια είναι αυτά
- Εάν τα Προσωπικά Δεδομένα μπορούν να χρησιμοποιηθούν παράνομα
- Ποια είναι τα Υποκείμενα των Προσωπικών Δεδομένων, ποιος ο αριθμός τους και ποιες οι πιθανές επιπτώσεις σε αυτά τα Υποκείμενα
- Περαιτέρω τυχόν συνέπειες του Περιστατικού

Στη συνέχεια, ο αρμόδιος για θέματα προστασίας προσωπικών δεδομένων εντός της Εταιρείας σε συνεργασία με τη Διοίκηση της Εταιρείας σχεδιάζουν και εφαρμόζουν τα απαραίτητα μέτρα για τον περιορισμό του αντικτύπου στα Υποκείμενα και τη διαχείριση του Περιστατικού.

iv. Διερεύνηση Αιτίας Περιστατικού: Ο αρμόδιος για θέματα προστασίας προσωπικών δεδομένων εντός της Εταιρείας πραγματοποιεί τις απαραίτητες ενέργειες προκειμένου να διερευνηθούν τα αίτια που προκάλεσαν το περιστατικό παραβίασης.

3. Κοινοποίηση στην Αρχή Προστασίας Προσωπικών Δεδομένων

Όταν απαιτείται να γνωστοποιηθεί το Περιστατικό στην εποπτική αρχή, ο Κανονισμός απαιτεί ότι αυτό θα γίνεται χωρίς αδικαιολόγητη καθυστέρηση και, όπου αυτό είναι εφικτό, το αργότερο 72 ώρες αφότου το Περιστατικό αναφερθεί ή γίνει αντιληπτό, σύμφωνα με τα Άρθρα 33 και 34 του Κανονισμού, εκτός και αν αξιολογηθεί ότι δεν υπάρχει κίνδυνος για τα δικαιώματα και τις ελευθερίες του Υποκειμένου. Σε περίπτωση που ο αρμόδιος για θέματα προστασίας προσωπικών δεδομένων εντός της Εταιρείας αξιολογήσει το Περιστατικό και διαπιστώσει ότι δεν υπάρχει κίνδυνος για τα Προσωπικά Δεδομένα των Υποκειμένων, το Περιστατικό δεν απαιτείται να κοινοποιηθεί στην εποπτική αρχή. Η κοινοποίηση είναι υποχρεωτική εφόσον επιβεβαιωθεί ότι υπήρξε Περιστατικό, από το οποίο πιθανολογείται ότι επέρχεται ή πρόκειται να επέλθει κίνδυνος για τα δικαιώματα και τις ελευθερίες των Υποκειμένων. Πρόσθετες πληροφορίες μπορούν να παρέχονται στην εποπτική αρχή σταδιακά, υπό την προϋπόθεση ότι αυτό θα γίνει χωρίς περαιτέρω αδικαιολόγητη καθυστέρηση. Εάν η αρχική κοινοποίηση δε γίνει εντός 72 ωρών, είναι απαραίτητο να ενημερωθεί η εποπτική αρχή για τους λόγους της καθυστέρησης στην αναφορά του Περιστατικού.

Η κοινοποίηση προς την εποπτική αρχή πρέπει να περιλαμβάνει τα ακόλουθα στοιχεία (σε κάθε περίπτωση συμπληρώνεται σχετικό έντυπο που τυχόν διαθέτει προς χρήση η εποπτική αρχή):

- Περιγράφει τη φύση του Περιστατικού Παραβίασης Προσωπικών Δεδομένων συμπεριλαμβανομένων, όπου είναι δυνατόν, των κατηγοριών και του αριθμού των Υποκειμένων που επηρεάζονται από το Περιστατικό καθώς και τις κατηγορίες και τα αρχεία Προσωπικών Δεδομένων που παραβιάστηκαν
- Κοινοποιεί το όνομα και τα στοιχεία επικοινωνίας του αρμόδιου για θέματα προστασίας προσωπικών δεδομένων εντός της Εταιρείας
- Να υπάρχει περιγραφή των πιθανών συνεπειών από το Περιστατικό Παραβίασης Προσωπικών Δεδομένων
- Να υπάρχει περιγραφή για τα μέτρα που έχουν ληφθεί ή πρόκειται να ληφθούν από τον αρμόδιο για θέματα προστασίας προσωπικών δεδομένων εντός της Εταιρείας για την αντιμετώπιση του Περιστατικού

Όταν δεν είναι δυνατή η ταυτόχρονη παροχή των πληροφοριών, οι σχετικές πληροφορίες μπορούν να παρέχονται σταδιακά χωρίς περαιτέρω αδικαιολόγητη καθυστέρηση.

4. Κοινοποίηση Περιστατικού Παραβίασης Προσωπικών Δεδομένων στα Υποκείμενα

Όταν το Περιστατικό Παραβίασης Προσωπικών Δεδομένων είναι πιθανό να οδηγήσει σε υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των Υποκειμένων, ο αρμόδιος για θέματα προστασίας προσωπικών δεδομένων εντός της Εταιρείας κοινοποιεί, χωρίς

αδικαιολόγητη καθυστέρηση το Περιστατικό στα Υποκείμενα στα οποία αφορούν τα Προσωπικά Δεδομένα που παραβιάστηκαν.

Η γνωστοποίηση προς το Υποκείμενο πρέπει να είναι σαφής ως προς τη φύση του Περιστατικού Παραβίασης των Προσωπικών Δεδομένων και να περιλαμβάνει πληροφορίες σχετικά με τα μέτρα που έχουν ληφθεί για την αντιμετώπισή του.

Η γνωστοποίηση προς το Υποκείμενο δεν είναι αναγκαία αν πληρείται μία από τις ακόλουθες περιπτώσεις:

- Η Εταιρεία έχει εφαρμόσει τα κατάλληλα μέτρα τεχνικής και οργανωτικής προστασίας των Προσωπικών Δεδομένων στα οποία αφορά η παραβίαση και ιδίως τα μέτρα εκείνα που καθιστούν τα Προσωπικά Δεδομένα μη προσβάσιμα ή μη κατανοητά από άτομα που δεν έχουν την κατάλληλη εξουσιοδότηση π.χ. Κρυπτογράφηση
- Η Εταιρεία έλαβε μεταγενέστερα μέτρα που εξασφαλίζουν ότι δεν συντρέχει κίνδυνος για τα δικαιώματα και τις ελευθερίες του Υποκειμένου.

5. Αξιολόγηση

Μόλις ολοκληρωθούν τα παραπάνω βήματα, ο αρμόδιος για θέματα προστασίας προσωπικών δεδομένων εντός της Εταιρείας οφείλει να:

1. Διερευνήσει τα αίτια της παραβίασης, με στόχο να προσδιορίσει το ενδεχόμενο βελτιωτικών ενεργειών ή/και αλλαγών σε πολιτικές και διαδικασίες προκειμένου να μειωθεί η πιθανότητα επανάληψης μιας τέτοιας παραβίασης.
2. Αξιολογήσει την αποτελεσματικότητα της αντίδρασης της Εταιρείας στο Περιστατικό Παραβίασης των Προσωπικών Δεδομένων και μελετήσει πιθανές βελτιώσεις στις διαδικασίες της Εταιρείας ώστε να διασφαλιστεί η σωστή αντιμετώπιση ανάλογων περιστατικών στο μέλλον.

VI. Έντυπο Υποβολής Γνωστοποίησης Περιστατικού Παραβίασης Προσωπικού Δεδομένων

Ενότητα 1: Ειδοποίηση Περιστατικού Παραβίασης Προσωπικών Δεδομένων	**Να συμπληρωθεί από το πρόσωπο που αναφέρει το Περιστατικό**
Ημερομηνία που έγινε αντιληπτό το Περιστατικό:	
Ημερομηνία που συνέβη Περιστατικού:	
Τοποθεσία όπου σημειώθηκε το Περιστατικό:	
Ονοματεπώνυμο του προσώπου που αναφέρει το Περιστατικό:	
Στοιχεία επικοινωνίας του προσώπου που αναφέρει το Περιστατικό (ηλεκτρονική διεύθυνση, τηλέφωνο):	
Σύντομη περιγραφή του Περιστατικού και λεπτομέρειες των Προσωπικών Δεδομένων που επηρεάστηκαν:	
Αριθμός Υποκειμένων που επηρεάζονται, εάν γνωρίζετε:	
Υπάρχουν Προσωπικά Δεδομένα που να βρίσκονται σε κίνδυνο; Εάν ναι, παρακαλώ δώστε πληροφορίες:	
Σύντομη περιγραφή κάθε ενέργειας που έγινε από τη στιγμή της ανακάλυψης:	
Για τον αρμόδιο για θέματα προστασίας προσωπικών δεδομένων εντός της Εταιρείας:	
Ελήφθη από:	
Ημερομηνία Παραλαβής:	
Προωθήθηκε στον/στην:	
Ημερομηνία Προώθησης:	

Ενότητα 2: Αξιολόγηση Σοβαρότητας Περιστατικού	**Να συμπληρωθεί από τον αρμόδιο για θέματα προστασίας προσωπικών δεδομένων εντός της Εταιρείας**
Πληροφορίες για τα Πληροφοριακά Συστήματα, τον εξοπλισμό, τις συσκευές, αρχεία τα οποία επηρεάζονται από το Περιστατικό:	
Λεπτομέρειες των Προσωπικών Δεδομένων που επηρεάστηκαν:	
Ποια είναι η φύση των Προσωπικών Δεδομένων που χάθηκαν;	
Πόσα Προσωπικά Δεδομένα χάθηκαν; Εάν έχει χαθεί/κλαπεί φορητός υπολογιστής: πότε είχε γίνει το τελευταίο back up στα κεντρικά πληροφοριακά συστήματα της Εταιρείας;	
Οι πληροφορίες είναι μοναδικές; Η απώλεια τους θα έχει αρνητικές συνέπειες στη λειτουργία, στη χρηματοοικονομική και νομική ευθύνη για την Εταιρεία ή για τρίτους;	
Ποιος είναι ο αριθμός των Υποκειμένων που έχουν επηρεαστεί;	
Τα Προσωπικά Δεδομένα δεσμεύονται από κάποια συμβατική ρύθμιση ασφάλειας;	
Ποιος είναι ο τύπος των δεδομένων; Παρακαλώ περιγράψτε λεπτομερώς τους τύπους των πληροφοριών που εμπίπτουν στις παρακάτω κατηγορίες:	
Προσωπικά δεδομένα Υψηλού Κινδύνου • Ευαίσθητα Προσωπικά Δεδομένα i. Φυλετική ή εθνοτική καταγωγή; ii. Πολιτικές απόψεις ή θρησκευτικές ή φιλοσοφικές πιστεύω; iii. Συμμετοχή σε συνδικαλιστική οργάνωση; iv. Σωματική ή ψυχική υγεία ή κατάσταση ή σεξουαλική ζωή; v. Διάπραξη ή υποτιθέμενη διάπραξη οποιουδήποτε αδικήματος, ή	

vi. Αγωγές για διάπραξη ή υποτιθέμενη διάπραξη αδικήματος από το πρόσωπο στο οποίο αναφέρονται τα προσωπικά δεδομένα;	
• Πληροφορίες που θα μπορούσαν να χρησιμοποιηθούν για την τέλεση απάτης όπως τραπεζικός λογαριασμός φυσικού προσώπου και άλλες οικονομικές πληροφορίες, εθνικά αναγνωριστικά στοιχεία, όπως ο Αριθμός Μητρώου Κοινωνικής Ασφάλισης, αντίγραφα διαβατηρίων και θεωρήσεις εισόδων (visa)	
• Προσωπικά Δεδομένα που αφορούν σε ενήλικες που ανήκουν σε ευαίσθητες κοινωνικές ομάδες ή σε παιδιά;	
• Εκτενή στοιχεία (προφίλ) των Υποκειμένων, συμπεριλαμβανομένων δεδομένων αξιολόγησης εργασίας, μισθού ή προσωπικής ζωής που θα μπορούσαν να προκαλέσουν δυσμενείς επιπτώσεις στα Υποκείμενα εάν αποκαλυφθούν;	
• Πληροφορίες που αν αποκαλυφθούν θα μπορούσαν να θέσουν σε κίνδυνο την ασφάλεια των Υποκειμένων;	

Ενότητα 3: Μέτρα αντιμετώπισης	**Να συμπληρωθεί από τον αρμόδιο για θέματα προστασίας προσωπικών δεδομένων εντός της Εταιρείας**
Αριθμός Περιστατικού:	
Παραλαβή Αναφοράς από:	
Ημερομηνία Παραλαβής:	
Ενέργειες που πραγματοποιήθηκαν από τους υπεύθυνους:	

Αναφέρθηκε το περιστατικό στην Αστυνομία;	ΝΑΙ/ΟΧΙ Εάν ΝΑΙ, ημερομηνία αναφοράς:
Παρακολούθηση των ενεργειών που απαιτούνται:	
Ημερομηνία αναφοράς στον αρμόδιο για θέματα προστασίας προσωπικών δεδομένων εντός της Εταιρείας:	
Αναφορά σε άλλους ενδιαφερόμενους εντός της Εταιρείας (λεπτομέρειες, ημερομηνίες):	
Ενημέρωση των Υποκειμένων:	ΝΑΙ/ΟΧΙ εάν ΝΑΙ, ημερομηνία ενημέρωσης: Λεπτομέρειες:
Γνωστοποίηση στην εποπτική αρχή	ΝΑΙ/ΟΧΙ εάν ΝΑΙ, ημερομηνία Γνωστοποίησης: Λεπτομέρειες: