ΠΟΛΙΤΙΚΗ ΚΑΙ ΔΙΑΔΙΚΑΣΙΑ ΔΙΑΡΡΟΗΣ ΔΕΔΟΜΕΝΩΝ

OLYMPIC AIR A.E.
Έδρα: Διεθνής Αερολιμένας Αθηνών «Ελ. Βενιζέλος»,
Κτίριο 57, Τ.Κ. 190 19 Σπάτα Αττικής, Τ: 210 3550000,
F: 210 3550431, Α.Φ.Μ.: 998939913, Δ.Ο.Υ.: Φ.Α.Ε. ΑΘΗΝΩΝ,
ΑΡ. Γ.Ε.ΜΗ.: 6705101000

Πίνακας Περιεχομένων

1. Πολιτική

Η Πολιτική διέπεται από την δήλωση απορρήτου της εταιρείας.
Η εταιρεία έχει δεσμευτεί να διαχειρίζεται προσωπικές πληροφορίες σύμφωνα με τον Ευρωπαϊκό Κανονισμό 679/2016.
Το παρόν έγγραφο καθορίζει τις διαδικασίες που πρέπει να ακολουθούνται από το προσωπικό σε περίπτωση που η εταιρεία διαπιστώσει παραβίαση δεδομένων ή υποψιάζεται ότι έχει σημειωθεί παραβίαση δεδομένων.
Η παραβίαση δεδομένων συνεπάγεται απώλεια, μη εξουσιοδοτημένη πρόσβαση ή μη εξουσιοδοτημένη αποκάλυψη προσωπικών πληροφοριών.
Ο ευρωπαϊκός κανονισμός απαιτεί από τους οργανισμούς να κοινοποιούν σε άτομα που ενδέχεται να διατρέχουν κίνδυνο σοβαρής βλάβης από παραβίαση δεδομένων. Η Ελληνική Αρχή Προστασίας Δεδομένων πρέπει επίσης να ενημερώνεται. Ως εκ τούτου, η εταιρεία πρέπει να είναι έτοιμη να ενεργήσει γρήγορα σε περίπτωση παραβίασης των δεδομένων (ή υποψίας παραβίασης) και να καθορίσει κατά πόσο είναι πιθανό να προκαλέσει σοβαρή βλάβη.
Η τήρηση αυτού του Σχεδίου Διαδικασίας και Ανταπόκρισης θα εξασφαλίσει ότι η εταιρεία θα μπορεί να αξιολογεί και να ανταποκρίνεται ταχέως σε παραβιάσεις δεδομένων και να μετριάζει την πιθανή βλάβη του προσώπου που επηρεάζεται.

2. Σκοπός

Σκοπός της πολιτικής αυτής είναι να καθοριστούν οι αρχές και οι κανόνες για την ορθή χρήση των συστημάτων των πληροφοριών και των κρίσιμων τεχνολογιών από όλους τους εργαζομένους, τους τρίτους και τους εργολάβους. Εάν δεν υφίσταται πολιτική χρήσης, το προσωπικό μπορεί να χρησιμοποιεί τα συστήματα και τις κρίσιμες τεχνολογίες κατά παράβαση της πολιτικής της εταιρείας, επιτρέποντας έτσι σε κακόβουλους, να έχουν πρόσβαση σε κρίσιμα συστήματα.

3. Προειδοποίηση

Σε περίπτωση κατά την οποία είναι γνωστό (ή υπάρχει υποψία) παραβίασης δεδομένων, οποιοδήποτε μέλος του προσωπικού που το γνωρίζει πρέπει, εντός 24 ωρών, να ειδοποιήσει σε πρώτη φάση τον Υπεύθυνο Προστασίας Δεδομένων. Οι πληροφορίες που πρέπει να παρέχονται (εάν είναι γνωστές) περιλαμβάνουν:

- Πότε σημειώθηκε η παραβίαση (ώρα και ημερομηνία),
- Περιγραφή της παραβίασης (τύπος προσωπικών πληροφοριών),
- Αιτία της παραβίασης (εάν είναι γνωστή) αλλιώς πώς ανακαλύφθηκε,
- Ποια συστήματα, εάν υπάρχουν, επηρεάζονται,
- Ποιο τμήμα / διεύθυνση ασχολείται,
- Εάν έχουν πραγματοποιηθεί διορθωτικές ενέργειες για την αποκατάσταση ή την αποφυγή πιθανής παραβίασης (ή της υποψίας παραβίασης).

4. Αξιολόγηση και καθορισμός πιθανών επιπτώσεων

Μόλις κοινοποιηθούν οι παραπάνω πληροφορίες, ο ΥΠΔ πρέπει να εξετάσει εάν έχει διαπραχθεί (ή είναι πιθανό να σημειωθεί) παραβίαση δεδομένων προσωπικού

χαρακτήρα και να προβεί σε προκαταρκτική κρίση ως προς τη σοβαρότητά του.
Κριτήρια για τον προσδιορισμό της παράβασης δεδομένων απορρήτου αποτελούν τα παρακάτω:

- Συμπεριλαμβάνονται προσωπικές πληροφορίες;
- Είναι οι προσωπικές πληροφορίες ευαίσθητου χαρακτήρα;
- Υπήρξε μη εξουσιοδοτημένη πρόσβαση σε προσωπικές πληροφορίες ή μη εξουσιοδοτημένη αποκάλυψη προσωπικών πληροφοριών ή απώλεια προσωπικών πληροφοριών σε περιπτώσεις όπου είναι πιθανό να υπάρξει πρόσβαση στις πληροφορίες;

Κριτήρια για τον προσδιορισμό της σοβαρότητας:

- Ο τύπος και η έκταση των εμπλεκόμενων προσωπικών πληροφοριών,
- Εάν έχουν επηρεαστεί πολλά άτομα,
- Εάν οι πληροφορίες προστατεύονται από τυχόν μέτρα ασφαλείας (προστασία με κωδικό πρόσβασης ή κρυπτογράφηση),
- Το άτομο ή τα είδη ατόμων που έχουν τώρα πρόσβαση,
- Εάν υπάρχει (ή θα μπορούσε να υπάρχει) ένας πραγματικός κίνδυνος σοβαρής βλάβης στα άτομα που έχουν προσβληθεί,
- Το κατά πόσον μπορεί να υπάρξει μέριμνα για τα μέσα ενημέρωσης ή για τα ενδιαφερόμενα μέρη ως αποτέλεσμα της παραβίασης ή ύπαρξης ύποπτου παραβίασης.

5. Έκδοση οδηγιών από τον ΥΠΔ

Μετά την παραλαβή της ανακοίνωσης από το αρμόδιο μέλος του ΥΠΔ, ο τελευταίος θα λάβει προκαταρκτική άποψη ως προς την παραβίαση.
Ο ΥΠΔ αναθέτει τη διαχείριση της παραβίασης των δεδομένων και ο αρμόδιος Υπεύθυνος πρέπει να:

- Βεβαιωθεί ότι λαμβάνονται άμεσα διορθωτικά μέτρα, εάν αυτό δεν έχει ήδη συμβεί (διορθωτικές ενέργειες μπορεί να περιλαμβάνουν: ανάκτηση ή ανάκτηση των προσωπικών πληροφοριών, διακοπή μη εξουσιοδοτημένης πρόσβασης, διακοπή ή απομόνωση του επηρεαζόμενου συστήματος),
- Να υποβάλλει μια αναφορά στον ΥΠΔ εντός 24 ωρών από τη λήψη των οδηγιών. Η αναφορά πρέπει να περιλαμβάνει τα εξής:
  - Περιγραφή της παραβίασης ή της ύποπτης παραβίασης,
  - Δράσεις που ελήφθησαν,
  - Αποτελέσματα δράσης,
  - Διαδικασίες που έχουν εφαρμοστεί για να αποφευχθεί η επανάληψη της κατάστασης,
  - Σύσταση ότι δεν απαιτείται περαιτέρω δράση.

Ο ΥΠΔ θα υπογράψει ότι δεν απαιτείται περαιτέρω ενέργεια.

6. Ρόλος της ομάδας προσωπικών δεδομένων

Δεν υπάρχει ενιαία μέθοδος απάντησης στην παραβίαση δεδομένων και κάθε περιστατικό πρέπει να εξετάζεται κατά περίπτωση, αξιολογώντας τις περιστάσεις και τους

συναφείς κινδύνους για την ενημέρωση σχετικά με την κατάλληλη πορεία δράσης. Τα ακόλουθα βήματα μπορούν να αναληφθούν από την ομάδα προστασίας προσωπικών δεδομένων:

- Αξιολόγηση των κινδύνων που σχετίζονται με την παραβίαση, συμπεριλαμβανομένης της συγκέντρωσης και τεκμηρίωσης όλων των διαθέσιμων αποδεικτικών στοιχείων της παραβίασης.
- Κλήση εμπειρογνώμονα ή συμβουλή από το σχετικό προσωπικό υπό τις συγκεκριμένες συνθήκες.
- Ενεργοποίηση ανεξάρτητης υπηρεσίας ασφαλείας στον κυβερνοχώρο εάν είναι απαραίτητο.
- Αξιολόγηση πιθανότητας σοβαρής βλάβης.
- Κοινοποίηση στην αρμόδια αρχή μέσω του ΥΠΔ.
- Εξέταση ανάπτυξης στρατηγικής επικοινωνίας ή μέσων μαζικής ενημέρωσης, συμπεριλαμβανομένου του χρονοδιαγράμματος, του περιεχομένου και της μεθόδου των ανακοινώσεων προς το προσωπικό ή τα μέσα ενημέρωσης.
- Η ομάδα προστασίας προσωπικών δεδομένων πρέπει να πραγματοποιήσει την αξιολόγησή της εντός 48 ωρών από τη σύγκλησή της.
- Ο ΥΠΔ θα παρέχει περιοδικές ενημερώσεις προς το Διευθύνοντα Σύμβουλο όπου κρίνεται σκόπιμο.

7. Γνωστοποίηση

Εάν η Αρχή πρέπει να ενημερωθεί, ο ΥΠΔ πρέπει να συντάξει μια προκαθορισμένη δήλωση και να παράσχει αντίγραφο εντός 72 ωρών (αφού λάβει γνώση της παραβίασης). Εάν είναι εφικτό, η εταιρεία πρέπει επίσης να ειδοποιήσει κάθε άτομο με το οποίο σχετίζονται οι σχετικές προσωπικές πληροφορίες.
Όπου δεν είναι εφικτό, η εταιρεία πρέπει να λάβει εύλογα μέτρα για να δημοσιοποιήσει τη δήλωση (συμπεριλαμβανομένης της δημοσίευσης στον ιστότοπο).

8. Επικαιροποίηση της πολιτικής

Η πολίτική επικαιροποιείται κάθε πέντε έτη, εκτός και αν είναι απαραίτητο νωρίτερα.

9. Στοιχεία επικοινωνίας

Η επικοινωνία για τα ζητήματα προσωπικών δεδομένων περιλαμβανομένων παραπόνων περί διαρροής απορρήτου, μπορεί να πραγματοποιείται στα παρακάτω στοιχεία:
dpo@aegeanair.com
privacy@aegeanair.com
T: +30 210 6261651
Δ: Βιλτανιώτη 31, Κηφισιά 14564, Αθήνα, Ελλάδα