Greek

information and privacy commission new south wales

Ενημερωτικό δελτίο **Νοέμβριος 2023**

Συχνές ερωτήσεις για το σύστημα MNDB

Για ποιον προορίζονται αυτές οι πληροφορίες;	Μέλη του κοινού στην ΝΝΟ που αναζητούν πληροφορίες σχετικά με το σύστημα υποχρεωτικής κοινοποίησης παραβίασης δεδομένων.
Γιατί αυτές οι πληροφορίες είναι σημαντικές γι' αυτούς;	Αυτό το ενημερωτικό δελτίο θα βοηθήσει τα μέλη του κοινού να κατανοήσουν περισσότερα για το Σύστημα και ποια είναι τα δικαιώματά τους όταν συμβεί παραβίαση δεδομένων που αφορά τις προσωπικές τους πληροφορίες.

Τι είναι το Σχέδιο Υποχρεωτικής Δημοσιοποίησης Παραβίασης Δεδομένων;

Το Σχέδιο Υποχρεωτικής Δημοσιοποίησης Παραβίασης Δεδομένων (Σχέδιο MNDB) είναι μια υποχρεωτική απαίτηση δημοσιοποίησης βάσει του νόμου του 1998 περί Προστασίας Προσωπικών Δεδομένων και Προσωπικών Πληροφοριών (Νόμος PPIP) για τους οργανισμούς του δημόσιου τομέα της ΝΝΟ σε περίπτωση " παραβίασης επιλέξιμων δεδομένων".

Πότε ξεκίνησε το Σχέδιο MNDB;

Το Σχέδιο MNDB άρχισε να ισχύει στις 28 Νοεμβρίου 2023.

Σε ποιον εφαρμόζεται το Σχέδιο MNDB;

Το Σχέδιο MNDB εφαρμόζεται σε οργανισμούς του δημόσιου τομέα της ΝΝΟ, υπουργούς, πανεπιστήμια, Δημαρχίες και πολιτειακές επιχειρήσεις που δεν καλύπτονται από τη νομοθεσία της Κοινοπολιτείας για την προστασία προσωπικών δεδομένων.

Τι είναι η Πολιτική για Παραβίαση Δεδομένων;

Η Πολιτική για Παραβίαση Δεδομένων (ή DBP) είναι μια τεκμηριωμένη πολιτική ή σχέδιο που καθορίζει τον τρόπο με τον οποίο ένας οργανισμός θα ανταποκριθεί σε μια παραβίαση δεδομένων. Σύμφωνα με τη νομοθεσία, οι οργανισμοί υποχρεούνται να διαθέτουν DBP. Η DBP πρέπει να καθορίζει τους ρόλους και τις αρμοδιότητες του προσωπικού του οργανισμού σε σχέση με τη διαχείριση μιας παραβίασης, καθώς και τα βήματα που θα ακολουθήσει ο οργανισμός όταν συμβεί μια παραβίαση.

Οι οργανισμοί υποχρεούνται να διασφαλίζουν ότι η DBP τους είναι προσβάσιμη από το κοινό, πράγμα που σημαίνει ότι οι οργανισμοί θα πρέπει να δημοσιεύουν τη DBP τους στον ιστότοπό τους.

Τι είναι μια "παραβίαση επιλέξιμων δεδομένων";

Σύμφωνα με το Σχέδιο MNDB, ο οργανισμός πρέπει να ενημερώνει τα θιγόμενα άτομα και τον Επίτροπο Προστασίας Προσωπικών Δεδομένων όταν συμβεί κάποια παραβίαση επιλέξιμων δεδομένων.

"Παραβίαση Επιλέξιμων δεδομένων" συμβαίνει όταν υπάρχει:

- μη εξουσιοδοτημένη πρόσβαση ή μη εξουσιοδοτημένη αποκάλυψη προσωπικών πληροφοριών που τηρούνται από έναν οργανισμό, η οποία είναι πιθανό να οδηγήσει σε **σοβαρή βλάβη** του ατόμου το οποίο αφορούν οι πληροφορίες.
- απώλεια προσωπικών πληροφοριών που τηρούνται από έναν οργανισμό υπό συνθήκες όπου είναι πιθανό να υπάρξει μη εξουσιοδοτημένη πρόσβαση ή αποκάλυψη και η οποία θα μπορούσε να οδηγήσει σε **σοβαρή βλάβη** ενός ατόμου στο οποίο αναφέρονται οι πληροφορίες.

Τι είναι «σοβαρή βλάβη»;

Η σοβαρή βλάβη μπορεί να περιλαμβάνει σωματική, οικονομική ή υλική βλάβη, συναισθηματική ή ψυχολογική βλάβη ή βλάβη της φήμης. Ο αντίκτυπος της βλάβης μπορεί να διαφέρει από άτομο σε άτομο, αλλά μπορεί να περιλαμβάνει:

- οικονομική απώλεια λόγω απάτης
- πιθανό κίνδυνο σωματικής ή ψυχολογικής βλάβης, όπως από έναν βίαιο πρώην σύντροφο
- κλοπή ταυτότητας, η οποία μπορεί να επηρεάσει τα οικονομικά σας ή/και το πιστωτικό σας μητρώο
- σοβαρή βλάβη στη φήμη ενός ατόμου.

Πώς μπορεί να συμβεί παραβίαση δεδομένων;

Σε γενικές γραμμές, μια παραβίαση δεδομένων μπορεί να συμβεί λόγω ανθρώπινου λάθους, αποτυχίας των συστημάτων ή κακόβουλης πράξης ή κυβερνοπαραβίασης.

Ποια είναι παραδείγματα παραβίασης δεδομένων;

Ορισμένα παραδείγματα παραβιάσεων δεδομένων είναι τα εξής:

Ανθρώπινο λάθος:

- Μια επιστολή ή ένα μήνυμα ηλεκτρονικού ταχυδρομείου αποστέλλεται σε λάθος παραλήπτη.

- Η πρόσβαση στο σύστημα χορηγείται εσφαλμένα σε κάποιον χωρίς εξουσιοδότηση ή υπάρχει ανεπαρκής προστασία με κωδικό πρόσβασης.
- Μέσα που περιέχουν Προσωπικές Πληροφορίες χάνονται ή τοποθετούνται λάθος, π.χ. αρχεία, φορητός υπολογιστής, USB, τηλέφωνο.

Βλάβη συστήματος:

- Σφάλμα κωδικοποίησης που επιτρέπει πρόσβαση στο σύστημα χωρίς έλεγχο ταυτότητας ή αυτόματη δημιουργία ειδοποιήσεων.
- Τα συστήματα δεν συντηρούνται μέσω της εφαρμογής γνωστών και υποστηριζόμενων διορθώσεων.

Κακόβουλη ή εγκληματική επίθεση:

- Περιστατικά στον κυβερνοχώρο, π.χ. ransomware, κακόβουλο λογισμικό, hacking, phishing, απόπειρες πρόσβασης με ωμή βία.
- Κοινωνική μηχανική/προσωποποίηση που σημαίνει ακατάλληλη αποκάλυψη προσωπικών πληροφοριών.
- Απειλές εκ των έσω (εργαζόμενοι) που χρησιμοποιούν έγκυρα διαπιστευτήρια για πρόσβαση/αποκάλυψη προσωπικών πληροφοριών εκτός του πεδίου των καθηκόντων ή των δικαιωμάτων τους.

Πρέπει ο οργανισμός να ενημερώσει τον Επίτροπο Προστασίας Προσωπικών Δεδομένων;

Όταν μια παραβίαση δεδομένων αξιολογείται ως παραβίαση επιλέξιμων δεδομένων, οι οργανισμοί πρέπει να ειδοποιήσουν αμέσως τον Επίτροπο Προστασίας Προσωπικών Δεδομένων, χρησιμοποιώντας το έντυπο στον ιστότοπο της IPC.

Θα ειδοποιηθώ εάν επηρεάζομαι από παραβίαση επιλέξιμων δεδομένων;

Εάν ένας οργανισμός αποφασίσει ότι υπήρξε παραβίαση επιλέξιμων δεδομένων σε σχέση με τα προσωπικά σας δεδομένα, πρέπει να σας ενημερώσει το συντομότερο δυνατό για την παραβίαση αυτή. Αυτό σημαίνει ότι ο οργανισμός πρέπει να σας ειδοποιήσει εγγράφως και να σας παράσχει πληροφορίες σχετικά με την παραβίαση επιλέξιμων δεδομένων, συμπεριλαμβανομένων των εξής:

- τα μέτρα που έχει λάβει ή σκοπεύει να λάβει ο οργανισμός για τον έλεγχο ή τον μετριασμό της ζημίας που σας προκλήθηκε
- τα μέτρα που θα πρέπει να λάβετε μετά την παραβίαση επιλέξιμων δεδομένων
- πληροφορίες σχετικά με τον τρόπο με τον οποίο μπορείτε να ζητήσετε εσωτερική επανεξέταση της συμπεριφοράς του οργανισμού ή με τον τρόπο με τον οποίο μπορείτε να υποβάλετε παράπονο για την προστασία των προσωπικών δεδομένων στον Επίτροπο Προστασίας Προσωπικών Δεδομένων.

Πόσο καιρό μετά από μια παραβίαση δεδομένων μπορώ να περιμένω να ενημερωθώ;

Όταν ένας οργανισμός έχει βάσιμες υποψίες ότι μπορεί να έχει σημειωθεί παραβίαση επιλέξιμων δεδομένων, ο οργανισμός πρέπει να λάβει ορισμένα μέτρα:

- Να καταβάλει κάθε εύλογη προσπάθεια για τον περιορισμό της παραβίασης.
- Να εκτιμήσει εντός 30 ημερών εάν υπήρξε μη-εξουσιοδοτημένη πρόσβαση, αποκάλυψη ή απώλεια προσωπικών πληροφοριών που τηρούνται από έναν οργανισμό.
- Να εκτιμήσει εντός 30 ημερών εάν υπάρχει πιθανότητα σοβαρής βλάβης για οποιοδήποτε επηρεαζόμενο άτομο.
- Να καταβάλλει κάθε εύλογη προσπάθεια για τον μετριασμό της βλάβης που προκλήθηκε από την πιθανολογούμενη παραβίαση.

Εάν, μετά την ανάληψη των ανωτέρω βημάτων, ένας οργανισμός αποφασίσει ότι υπήρξε παραβίαση επιλέξιμων δεδομένων σε σχέση με τις προσωπικές σας πληροφορίες, πρέπει να σας ενημερώσει το συντομότερο δυνατό για την παραβίαση αυτή.

Τι γίνεται αν ο οργανισμός δεν έχει πλέον τα στοιχεία μου για να με ειδοποιήσει για παραβίαση δεδομένων;

Οι οργανισμοί διαθέτουν εξουσίες ανταλλαγής πληροφοριών στο πλαίσιο του συστήματος MNDB, ώστε να μπορούν να ζητούν σχετικές προσωπικές πληροφορίες από άλλον οργανισμό του δημόσιου τομέα. Οι πληροφορίες που μπορεί να ζητήσει ένας οργανισμός περιορίζονται στις πληροφορίες που είναι εύλογα αναγκαίες για την επιβεβαίωση του ονόματος και των στοιχείων επικοινωνίας ενός ατόμου που έχει πληγεί από παραβίαση δεδομένων.

Ωστόσο, εάν ο οργανισμός δεν είναι σε θέση να σας ειδοποιήσει άμεσα, πρέπει να δημοσιεύσει ειδοποίηση στον ιστότοπό του και να λάβει εύλογα μέτρα για τη δημοσιοποίηση της ειδοποίησης. Η κοινοποίηση πρέπει να παραμείνει στο μητρώο δημόσιων κοινοποιήσεων του οργανισμού για τουλάχιστον 12 μήνες.

Υπάρχουν λόγοι για τους οποίους ένας οργανισμός μπορεί να μην με ειδοποιήσει;

Ναι. Υπάρχουν ορισμένες εξαιρέσεις από την υποχρέωση των οργανισμών να ειδοποιούν τα θιγόμενα άτομα για παραβίαση δεδομένων. Για παράδειγμα, εάν ένας οργανισμός ενεργήσει γρήγορα για μετριασμό μιας παραβίασης δεδομένων και λόγω αυτής της ενέργειας η παραβίαση δεδομένων δεν είναι πιθανό να οδηγήσει σε σοβαρή βλάβη, δεν υπάρχει απαίτηση να ειδοποιηθούν τα θιγόμενα άτομα.

Θα μου παράσχει ο οργανισμός οποιαδήποτε βοήθεια μετά την κοινοποίηση;

Το είδος της βοήθειας ή της υποστήριξης που μπορεί να παράσχει ένας οργανισμός μετά την κοινοποίηση εξαρτάται από τις συγκεκριμένες περιστάσεις της παραβίασης δεδομένων. Τα παραδείγματα μπορεί να περιλαμβάνουν:

- βοήθεια για την αντικατάσταση των εγγράφων ταυτότητας ή των διαπιστευτηρίων που έχουν εκδοθεί από το κράτος - όπως η άδεια οδήγησης
- συμβουλές σχετικά με την προστασία των προσωπικών σας δεδομένων
- παροχή συνδέσμων προς πρόσθετες υπηρεσίες υποστήριξης και συμβουλευτικής.

Τι πρέπει να κάνω αν λάβω ειδοποίηση;

Υπάρχουν πρακτικά μέτρα που μπορείτε να λάβετε για να προστατεύσετε τις προσωπικές σας πληροφορίες και να μειώσετε τον κίνδυνο να υποστείτε ζημία από μια παραβίαση δεδομένων. Τα είδη των ενεργειών που μπορείτε να λάβετε εξαρτώνται από τις συνθήκες της παραβίασης δεδομένων και τον τύπο των σχετικών πληροφοριών. Η ειδοποίηση που λαμβάνετε θα πρέπει να σας συστήνει ενέργειες που μπορείτε να λάβετε ως απάντηση στον τύπο της παραβίασης που προσδιορίζεται στην ειδοποίηση.

Εάν θέλετε περισσότερες πληροφορίες σχετικά με την παραβίαση δεδομένων ή τον τρόπο προστασίας των προσωπικών σας δεδομένων, θα πρέπει να επικοινωνήσετε με τον οργανισμό που σας έστειλε την ειδοποίηση.

Πού μπορώ να βρω περισσότερες πληροφορίες;

Η Επιτροπή ΝΝΟ για Πληροφορίες και Προσωπικά Δεδομένα (IPC) διαθέτει περαιτέρω πληροφορίες και πρόσθετα μέσα στον διαδικτυακό τόπο της. Εναλλακτικά, μπορείτε να επικοινωνήσετε με την IPC χρησιμοποιώντας τα παρακάτω στοιχεία επικοινωνίας.

Για περισσότερες πληροφορίες

Επικοινωνήστε με την Επιτροπή ΝΝΟ για Πληροφορίες και Προσωπικά Δεδομένα (IPC):

Δωρεάν κλήση: 1800 472 679

Ηλεκτρονικό ταχυδρομείο: ipcinfo@ipc.nsw.gov.au

Δικτυακός τόπος: www.ipc.nsw.gov.au

ΣΗΜΕΙΩΣΗ: *Οι πληροφορίες στο παρόν δελτίο πρέπει να χρησιμοποιούνται μόνο ως οδηγός. Θα πρέπει να ζητείται νομική συμβουλή σε σχέση με τις εκάστοτε περιστάσεις.*