

Πού βρίσκεστε;

Με βάση τις απαντήσεις σας, η τρέχουσα κατάσταση συμμόρφωσης με τον GDPR αξιολογείται ως εξής:

ΠΡΟΧΩΡΗΜΕΝΟΣ

Εν συντομία: Διαδικασίες για την συνεχή παρακολούθηση και ενημέρωση των υποχρεώσεων που ενδέχεται να προκύψουν από τις αλλαγές στη νομοθεσία έχουν θεσπιστεί. Οι αλλαγές κοινοποιούνται στο προσωπικό λίγο μετά την έγκρισή τους. Διατηρείται αρχείο που καλύπτει όλες τις περιπτώσεις και χρήσεις προσωπικών πληροφοριών.

Επίπεδο Δεδομένων

βαθμολογία 100%

Τεχνικά μέτρα

βαθμολογία 78.6%

Οργανωτικά μέτρα

βαθμολογία 85.7%

Αναλυτική αξιολόγηση

Ερώτηση 1 από 15

Για ποια ομάδα (ομάδες) ατόμων κατέχετε προσωπικά δεδομένα;

- Πελάτες

Οι προτάσεις μας

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα πρέπει πάντα να είναι σύμφωνη με την ισχύουσα νομοθεσία για την προστασία των δεδομένων. Επί του παρόντος υπάρχουν παρόμοιες νομοθεσίες σε κάθε χώρα της ΕΕ, εξαιτίας της οδηγίας του Ευρωπαϊκού Κοινοβουλίου και τους Συμβουλίου 95/46/EC της 24ης Οκτωβρίου 1995 αναφορικά με την προστασία των φυσικών προσώπων έναντι

της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών. Ο νέος κανονισμός Γενικής Προστασίας Δεδομένων θα εφαρμοστεί άμεσα σε κάθε κράτος μέλος της ΕΕ και θα πρέπει ως εκ τούτου να οδηγήσει στη θέσπιση παρόμοιων κανόνων που ισχύουν σε ολόκληρη την ΕΕ.

Ερώτηση 2 από 15

Επεξεργάζεστε ειδικές κατηγορίες προσωπικών δεδομένων (π.χ. βιομετρικά δεδομένα, δεδομένα υγείας κ.λπ.);

• Όχι

Οι προτάσεις μας

Αυτό θα διευκολύνει την εργασία σας, αλλά σας συνιστούμε να επαληθεύσετε ότι σίγουρα δεν επεξεργάζεστε ειδικές κατηγορίες προσωπικών δεδομένων (π.χ. γενετικά δεδομένα, βιομετρικά δεδομένα με σκοπό τη μοναδική αναγνώριση ενός φυσικού προσώπου, δεδομένα σχετικά με την υγεία κ.λπ.). Εάν διαπιστώσετε ότι το κάνετε, θα χρειαστεί να πραγματοποιήσετε μια αξιολόγηση των επιπτώσεων των εργασιών επεξεργασίας στην προστασία των προσωπικών δεδομένων.

Ερώτηση 3 από 15

Υπό ποια νομική βάση αποθηκεύετε και επεξεργάζεστε προσωπικά δεδομένα;

• Λαμβάνουμε τη συγκατάθεση των υποκειμένων των δεδομένων για τη συλλογή των προσωπικών τους δεδομένων

Οι προτάσεις μας

Πολύ καλά. Σύμφωνα με το GDPR, θα πρέπει να εξετάσετε τον τρόπο με τον οποίο επεξεργάζεστε τα προσωπικά σας δεδομένα και να προσδιορίσετε τη νομική βάση επάνω στην οποία πραγματοποιείτε και τεκμηριώνετε αυτές τις διαδικασίες. Αυτό είναι απαραίτητο επειδή

τα δικαιώματα κάποιων ατόμων θα τροποποιηθούν από το GDPR, ανάλογα με τη νομική βάση που διέπει την επεξεργασία των προσωπικών δεδομένων τους. Για παράδειγμα, τα άτομα θα έχουν πλέον πιο ισχυρό δικαίωμα να διαγράψουν τα δεδομένα τους, όταν χρησιμοποιείτε τη συναίνεση ως νομική βάση για την επεξεργασία τους.

Ερώτηση 4 από 15

Αποθηκεύετε μόνο τα προσωπικά δεδομένα που απαιτούνται για την εκπλήρωση του σκοπού για τον οποίο συλλέχθηκαν;

- **Ναι, διατηρούμε μόνο τα σχετικά προσωπικά δεδομένα και τα αποθηκεύουμε μόνο για τον ελάχιστο απαιτούμενο χρόνο.**

Οι προτάσεις μας

Είστε καλά προετοιμασμένοι. Θα πρέπει να συνεχίσετε να δίνετε προσοχή στον τρόπο συμμόρφωσής σας με τις αρχές που ορίζονται στο GDPR σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα (νομιμότητα, δικαιοσύνη, διαφάνεια, σκοπός και περιορισμός της αποθήκευσης, ελαχιστοποίηση δεδομένων, ακρίβεια, ακεραιότητα και εμπιστευτικότητα). Η όλη διαδικασία επεξεργασίας δεδομένων, ξεκινώντας από τη συλλογή δεδομένων προσωπικού χαρακτήρα και τερματίζοντας την καταστροφή τους, διέπεται από το συγκεκριμένο σύνολο βασικών κανόνων.

Ερώτηση 5 από 15

Έχετε οποιαδήποτε τεκμηρίωση σχετικά με τα προσωπικά δεδομένα που συλλέγετε, από ποιες πηγές τα συλλέγετε και με ποιους τα μοιράζεστε;

- **Ναι, διατηρούμε τεκμηρίωση σχετικά με τη συλλογή και κοινή χρήση προσωπικών δεδομένων, η οποία ελέγχεται τακτικά.**

Οι προτάσεις μας

Πολύ καλά. Συνεχίστε να δίνετε προσοχή στις απαιτήσεις του GDPR σχετικά με τα αρχεία των δραστηριοτήτων επεξεργασίας. Η τεκμηρίωση πρέπει να περιλαμβάνει, μεταξύ άλλων, τους σκοπούς της επεξεργασίας, περιγραφή των κατηγοριών προσωπικών δεδομένων ή περιγραφή των χρησιμοποιούμενων τεχνικών και οργανωτικών μέτρων ασφαλείας. Η υποχρέωση καταγραφής των δραστηριοτήτων επεξεργασίας ισχύει τόσο για τους υπεύθυνους πραγματοποίησης ελέγχων όσο και επεξεργασίας.

Ερώτηση 6 από 15

Ποια τεχνικά μέτρα έχετε λάβει για την προστασία των προσωπικών δεδομένων από μη εξουσιοδοτημένη πρόσβαση;

Λογισμικό προστασίας από ιούς που παρέχει προστασία κακόβουλου λογισμικού: **Ναι**

Λογισμικό προστασίας από ιούς που παρέχει προστασία ηλεκτρονικού ταχυδρομείου και προγράμματος περιήγησης στον ιστό: **Ναι**

Το εταιρικό μας δίκτυο προστατεύεται από λογισμικό ασφαλείας: **Ναι**

Τακτικό αντίγραφο ασφαλείας των προσωπικών δεδομένων εφαρμόζεται αυτόματα: **Ναι**

Το εταιρικό μας ασύρματο δίκτυο προστατεύεται με κωδικό πρόσβασης: **Ναι**

Η απομακρυσμένη πρόσβαση στο εταιρικό μας δίκτυο είναι δυνατή μόνο μέσω ενός εικονικού ιδιωτικού δικτύου (VPN): **Δεν εφαρμόζεται**

Οι λογαριασμοί με προνομιακά δικαιώματα δεν χρησιμοποιούνται για καθημερινές εργασίες. Η σύνδεση με χρήστες με προνομιακά δικαιώματα είναι δυνατή μόνο από εξειδικευμένες συσκευές και η πρόσβαση περιορίζεται μόνο σε εξουσιοδοτημένα άτομα: **Εν μέρη**

Η πρόσβαση σε ευαίσθητα/προσωπικά δεδομένα ελέγχεται και περιορίζεται μόνο σε άτομα που χρειάζονται πρόσβαση σε αυτά: **Ναι**

Το λογισμικό πρόληψης διαρροών δεδομένων χρησιμοποιείται για την προστασία ευαίσθητων/προσωπικών δεδομένων: **Ναι**

Διαδικασίες παρακολούθησης, ανίχνευσης, ανάλυσης και αναφοράς περιστατικών ασφάλειας εφαρμόζονται και κοινοποιούνται στην επιχείρηση: **Ναι**

Οι προτάσεις μας

Πολύ καλά. Οι απαντήσεις σας δείχνουν ότι δίνετε την δέουσα προσοχή στην ανάπτυξη τεχνικών μέτρων. Σύμφωνα με το GDPR, πρέπει, λαμβάνοντας υπόψη τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τη διαφορετική πιθανότητα και σοβαρότητα των κινδύνων για τα δικαιώματα και τις ελευθερίες φυσικών προσώπων, να εφαρμόσετε κατάλληλα τεχνικά και οργανωτικά μέτρα για να διασφαλίσετε και να είστε σε θέση να αποδείξετε ότι η επεξεργασία πραγματοποιείται σύμφωνα με τον κανονισμό. Τα μέτρα αυτά επανεξετάζονται και ενημερώνονται, όπου χρειάζεται. Η λίστα των μέτρων που προτείνουμε εδώ αποτελεί ένα παράδειγμα μέτρων που είναι στη διάθεσή σας. Όλα τα μέτρα πρέπει να επιλέγονται προσεκτικά κατά περίπτωση.

Ερώτηση 7 από 15

Η κρυπτογράφηση είναι ένα πολύ σημαντικό μέτρο ασφάλειας. Ποια από τις ακόλουθες λειτουργίες κρυπτογράφησης χρησιμοποιείτε για την προστασία προσωπικών δεδομένων;

Κρυπτογράφηση Ευαίσθητων/Προσωπικών αρχείων δεδομένων: **Ναι**

Πλήρης κρυπτογράφηση δίσκων υπολογιστή/laptop: **Ναι**

Κρυπτογράφηση ηλεκτρονικής επικοινωνίας: **Ναι**

Κρυπτογράφηση Αφαιρούμενων Δίσκων: **Ναι**

Κρυπτογράφηση φακέλου δικτύου/Cloud: **Ναι**

Οι προτάσεις μας

Οι απαντήσεις σας υποδεικνύουν ότι έχετε δώσει μεγάλη προσοχή στην προστασία δεδομένων μέσω κρυπτογράφησης. Ο GDPR ορίζει την κρυπτογράφηση ως ένα από τα τεχνικά μέτρα που μπορούν να συμβάλουν στην εξασφάλιση της συμμόρφωσης με ορισμένες από τις υποχρεώσεις του. Πρέπει να είστε πάντα σίγουροι ότι η κρυπτογράφηση χρησιμοποιείται τόσο για δεδομένα που μετακινούνται (που μεταδίδονται μέσω δικτύου) όσο και για αυτά που βρίσκονται σε κατάσταση ηρεμίας (αποθηκευμένα σε διάφορα μέσα).

Ερώτηση 8 από 15

Έχετε τεχνικά και οργανωτικά μέτρα για να διασφαλίσετε ότι τα υποκείμενα των δεδομένων έχουν τα ακόλουθα δικαιώματα;

Για να αποκτήσουν πρόσβαση στα επεξεργασμένα προσωπικά τους δεδομένα: **Ναι**

Προκειμένου να αποκατασταθεί η ανακρίβειες των προσωπικών τους δεδομένων: **Ναι**

Για να διαγραφούν τα προσωπικά τους δεδομένα - το δικαίωμα στη λήθη: **Ναι**

Για να αποτρέψουν τις άμεσες προωθητικές ενέργειες: **Ναι**

Για να αποτρέψουν την αυτοματοποιημένη λήψη αποφάσεων και τη δημιουργία προφίλ: **Ναι**

Φορητότητα δεδομένων: **Όχι**

Οι προτάσεις μας

Πολύ καλά: οι απαντήσεις σας δείχνουν ότι δίνετε την δέουσα προσοχή στα ατομικά δικαιώματα των υποκειμένων των δεδομένων.

Η δυνατότητα των υποκειμένων των δεδομένων να ασκούν τα δικαιώματά τους είναι ζωτικής σημασίας για την επεξεργασία των προσωπικών δεδομένων. Εάν δεν προβείτε στις προβλεπόμενες ενέργειες μετά από αίτηση του υποκειμένου των δεδομένων, θα

πρέπει να το ενημερώσετε αμέσως για τους λόγους μη ανάληψης δράσης, καθώς και για το ότι μπορεί να καταθέσει καταγγελία σε εποπτική αρχή, επιζητώντας ένδικα μέσα.

Ερώτηση 9 από 15

Είναι οι βασικοί σας συνεργάτες και οι υπεύθυνοι λήψης αποφάσεων ενήμεροι για τις αλλαγές στους κανόνες που επιφέρει ο GDPR;

- **Ναι, γνωρίζουμε πολύ καλά τις επικείμενες αλλαγές**

Οι προτάσεις μας

Πολύ καλά. Θα πρέπει να προσδιορίσετε όλες τις απαιτήσεις του GDPR και να τις εφαρμόζετε προκειμένου να διασφαλίσετε ότι παραμένετε συμβατοί. Ο GDPR απαιτεί την προσοχή της διοίκησης σε επίπεδο C όχι μόνο λόγω του καταλόγου υποχρεώσεων του, αλλά και λόγω των εξαιρετικά υψηλών προστίμων που μπορεί να επιβληθούν σε εκείνους που δεν συμμορφώνονται με αυτόν.

Ερώτηση 10 από 15

Το προσωπικό σας που είναι επιφορτισμένο με την επεξεργασία δεδομένων προσωπικού χαρακτήρα λαμβάνει εκπαίδευση σε ότι αφορά τις υποχρεώσεις και τα δικαιώματα που σχετίζονται με την προστασία των προσωπικών δεδομένων;

- **Ναι**

Οι προτάσεις μας

Πολύ καλά. Ο GDPR απαιτεί κατάρτιση του προσωπικού που εμπλέκεται σε εργασίες επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Βεβαιωθείτε ότι η εκπαίδευσή σας περιλαμβάνει όλες τις πτυχές της επεξεργασίας των προσωπικών δεδομένων (όπως η συλλογή, η καταγραφή, η διαμόρφωση, η αποθήκευση, η

τροποποίηση, η ανάκτηση, η αποκάλυψη μέσω μετάδοσης, η διάδοση, ο συνδυασμός, η διαγραφή, η καταστροφή κλ.π.), καθώς και ότι τα ανάλογα τμήματα των αρχείων σας σχετικά με τις δραστηριότητες επεξεργασίας είναι προσβάσιμα στο σχετικό προσωπικό.

Ερώτηση 11 από 15

Είναι ενημερωμένοι όσοι είναι επιφορτισμένοι με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα για τις επερχόμενες αλλαγές που θα επιφέρει ο GDPR; Έχουν σχέδιο συμμόρφωσης;

- **Δεν ισχύει επειδή δεν έχει προσληφθεί σχετικό προσωπικό επεξεργασίας προσωπικών δεδομένων.**

Οι προτάσεις μας

Η επεξεργασία προσωπικών δεδομένων σε έναν οργανισμό μπορεί να είναι πολύ περίπλοκη διαδικασία και στις περισσότερες περιπτώσεις περιλαμβάνει την ανταλλαγή δεδομένων με όσους έχουν επιφορτιστεί με τη διαδικασία αυτή (όταν δηλαδή τα δεδομένα μεταφέρονται σε τρίτους). Ελέγξτε τις δραστηριότητες επεξεργασίας των προσωπικών δεδομένων και βεβαιωθείτε ότι δεν έχετε προσλάβει άτομα ειδικά για την επεξεργασία των δεδομένων. Λάβετε υπόψη ότι τα άτομα αυτά έχουν τώρα άμεσες υποχρεώσεις βάσει του GDPR. Εάν παραβιάζουν τις υποχρεώσεις τους, μπορούν να επιβληθούν πρόστιμα και να φέρουν από κοινού ευθύνη με τον υπεύθυνο της επεξεργασίας για οποιαδήποτε ζημία στο υποκείμενο των δεδομένων, εκτός εάν μπορούν να αποδείξουν ότι δεν ήταν υπεύθυνοι για το περιστατικό.

Ερώτηση 12 από 15

Διαθέτετε μια γενική περιγραφή των τεχνικών και οργανωτικών μέτρων ασφαλείας ως μέρος των αρχείων σας σχετικά με τις δραστηριότητες επεξεργασίας;

- **Ναι, έχουμε τέτοια τεκμηρίωση η οποία ενημερώνεται τακτικά.**

Οι προτάσεις μας

Πολύ καλά. Ο GDPR απαιτεί να διαθέτετε μια γενική περιγραφή των υιοθετημένων τεχνικών και οργανωτικών μέτρων ασφαλείας ως μέρος των "Καταγραφών δραστηριοτήτων επεξεργασίας".

Ερώτηση 13 από 15

Έχετε διεργασίες και διαδικασίες σε περίπτωση παραβίασης των δεδομένων (συμπεριλαμβανομένης της ενημέρωσης της τοπικής αρχής DPA);

- **Ναι.**

Ερώτηση 14 από 15

Εφαρμόζετε αρχές "προστασίας της ιδιωτικής ζωής από το στάδιο του σχεδιασμού" σε οποιαδήποτε νέα διαδικασία ή προϊόν που αναπτύσσετε;

- **Ναι, η "προστασία της ιδιωτικής ζωής από το σχεδιασμό" εφαρμόζεται πλήρως στον οργανισμό μας.**

Οι προτάσεις μας

Πολύ καλά. Ο GDPR απαιτεί από εσάς να υιοθετήσετε εσωτερικές πολιτικές και να εφαρμόσετε μέτρα τα οποία πληρούν, ειδικότερα, τις αρχές της προστασίας δεδομένων τόσο στη φάση του σχεδιασμού όσο και από προεπιλογή. Τα μέτρα αυτά θα μπορούσαν να συνίστανται, μεταξύ άλλων, στην ελαχιστοποίηση της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, στην υιοθέτηση ψευδωνύμου για τα προσωπικά δεδομένα το συντομότερο δυνατόν ή στην παροχή δυνατότητας στο υποκείμενο των δεδομένων να παρακολουθεί την

επεξεργασία των δεδομένων που τον αφορούν. Βεβαιωθείτε ότι έχετε λάβει υπόψη όλες τις πτυχές των κανόνων αυτών.

Ερώτηση 15 από 15

Έχετε κάποιο πλάνο για το πως να συμμορφωθείτε με τον GDPR;

- **Είμαστε ενήμεροι για τη σπουδαιότητα του GDPR, αλλά δεν έχουμε ακόμα χρόνο να προετοιμάσουμε ένα σχέδιο συμμόρφωσης.**

Οι προτάσεις μας

Ο GDPR απαιτεί από οργανισμούς όλων των μεγεθών να υιοθετήσουν ένα νέο σύνολο διαδικασιών και πολιτικών που στοχεύουν στο να παρέχουν στα άτομα των οποίων τα προσωπικά δεδομένα υφίστανται οποιασδήποτε μορφής επεξεργασία, μεγαλύτερο έλεγχο στα δεδομένα και τις εγγραφές που τους αφορούν. Πολλές από αυτές τις πολιτικές, θα περιλαμβάνουν τη σύνταξη νέων διαδικασιών και εγχειριδίων, την επανεκπαίδευση του προσωπικού και την αναβάθμιση των συστημάτων ώστε να εξυπηρετούνται αυτές οι νέες διαδικασίες. Άλλα βήματα περιλαμβάνουν πρακτικά μέτρα, όπως η χρήση κρυπτογράφησης σε όποιες περιπτώσεις τα προσωπικά δεδομένα εκτίθενται σε κίνδυνο. Ο νέος Κανονισμός θα ισχύσει από τις 25 Μαΐου 2018. Τώρα είναι η στιγμή να προσδιορίσετε επακριβώς όλες οι απαιτήσεις του GDPR και να ξεκινήσετε άμεσα ενέργειες για να συμμορφωθείτε πλήρως με αυτές.

Πιστοποιήθηκε από την ESET spol. s r.o. τη Παρασκευή 13 Απριλίου 2018 για λογαριασμό της Αφοί Λεπτοκαρίδη ΟΕ και του ιστότοπου www.polisafety.gr

