LOGISOFT

Γενικός Κανονισμός Προστασίας Δεδομένων (Γ.Κ.Π.Δ.)
Πως οι επιχειρήσεις προστατεύουν τα προσωπικα δεδομένα των Ευρωπαίων πολιτών.

Τι είναι ο ΓΚΠΔ 2016/679 (ΕΕ);

Μετά από τέσσερα χρόνια προετοιμασίας και συζήτησης, το GDPR εγκρίθηκε τελικά από το κοινοβούλιο της ΕΕ στις 14 Απριλίου 2016. Θα τεθεί σε ισχύ 20 ημέρες μετά τη δημοσίευση του στην Επίσημε Εφημερίδα της ΕΕ και θα εφαρμοστεί άμεσα σε όλα τα κράτη μέλη δυο χρόνια μετά την ημερομηνία αυτή. Ημερομηνιά αναγκαστικής εκτέλεσης: 25 Μαίου 2018 - οπότε οιοργανώσεις που δεν συμμορφώνονται με τις διατάξεις αυτές θα υποστούν βαριά πρόστιμα.
Ο γενικός κανονισμός για την προστασία των δεδομένων της ΕΕ (GDPR) αντικαθιστά την οδηγία 95/46/ΕΚ, ο οποίος θα καταργηθεί επίσημα στις 26 Μαιου 2020, για την προστασία των δεδομένων και αποσκοπεί στην εναρμόνιση των νομοθετών περί προστασίας της ιδιωτικής ζωής σε ολόκληρη την Ευρώπη, για την προστασία και την ενδυνάμωση του ιδιωτικού απόρρητου των πολιτών της ΕΕ και για την αναμόρφωση του τρόπου προσέγγισης των οργανισμών στα δεδομένα.

Ποιός πρέπει να εφαρμόσει τον Κανονισμό;

Ο κανονισμός ισχύει για κάθε οργανισμό ο οποίος συλλέγει, επεξεργάζεται και αποθηκεύει δεδομένα προσωπικού χαρακτήρα από πολίτες της ΕΕ ή φυσικό πρόσωπο που διαμένει στην ΕΕ ή ολοκληρώνει συναλλαγές εντός οργανισμών της ΕΕ.

Ποιές είναι οι κατευθηντήριες γραμμές;

Το GDPR αναφέρει ότι οι οργανισμοί πρέπει να υιοθετήσουν τις κατάλληλες πολιτικές και διαδικασίες για την προστασία των προσωπικών δεδομένων που κατέχουν.

Το άρθρο 32 του GDPR ορίζει σαφώς ότι “ο υπεύθυνος της επεξεργασίας και ο επεξεργαστής δεδομένων εφφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα για να εξασφαλλίσουν ένα επίπεδο ασφαλείας κατάλληλο για τον κατά περίπτωση κίνδυνο, μεταξύ άλλων.
το άρθρο 32 απαιτεί επιπλέον να προσδιορίζονται και να μετριάζονται οι κίνδυνοι “από τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση μη εξουσιοδοτημένη αποκάλυψη ή πρόσβαση σε προσωπικά δεδομένα¨.
το αρθρο 32 του GDPR είναι η πρώτη διάταξη που απαιτέι τεχνικά μέτρα για την προστασία των δεδομένων.

Παρόλο που δίνει παραδείγματα μέτρων ασφαλείας και ελέγχων, το άρθρο δεν παρέχει λεπτομείς οδηγίες σχετικά με το τι πρέπει να κάνετε για να το επιτύχετε αυτό.

Πως μπορώ να ξεκινήσω;

Ο κανονισμός Προστασία Προσωπικών Δεδομένων απαιτεί την ύπαρξη και την τεκμιρίωση πολλών ενημερωτικών δελτίων, ελέγχων, διαδικασιών, εντύπων και ενημερώσεων λογισμικού. θα χρειαστείτε μια ομάδα ανρώπων που έχουν αναπτύξει μια επιχειρηματική διαβούλευση που θα καλύπτει την πτυχή των Εσωτερικών διαδικασιών IT / IS, DPIA, Auditing, Editing, Proofing and Mapping και θα συμμορφώνεται με τον νέο κανονισμό.
Θα ήταν καλύτερο να αναζητήσετε μια επαγγελματική συμβουλή σε πρώιμο στάδιο παρά να διακινδυνεύσετε τη φήμη σας και την οποιαδήποτε πιθανή αρνητική επίδραση στους πελάτες σας. εκτός απο τις οικονομικές ζημιές πο μπορεί να προκύψουν στον οργανισμό σας, εχέτε επίσης νομικές ευθύνες για οποιοδήποτε ακατάλληλη χρήση προσωπικών δεδομένων.

Την πλήρη νομική ευθήνη των δεδομένων που διατηρείτε στην εταιρεία σας την έχει ο Υπεύθηνος Επεξεργασίας Δεδομένων(Κεφάλαιο IV, Άρθρο 24, Άρθρο 27, Άρθρο 27)

*“ The controllerand the processor shall implement **appropriate technical and organisational measures** to ensure a level of security appropriate to the risk, including ... **encryption of personal data.**”*

GDPR Article 32, Security of Processing

*In order to be able to demonstrate compliance with this Regulation, the controller should **adopt internal policies and implement measures** which meet in particular the **principles of data protection by design and data protection by default.**”*

GDPR Recital 78: Appropriate technical and organisational measures.

*“Personal data shall be : (a) **processed lawfully, fairly and in a transparent manner** in relation to the data subject, ...”*

GDPR Article 5. Principles relating to the processing of personal data

Αυτό το έγγραφο περιέχει ορισμένες βασικές πληροφορίες σχετικά με το ΓΚΠΔ 2016/ 679. Το εγγραφό αυτό δεν παρέχει πλήρη καθοδήγηση για την εφαρμογή του ΓΚΠΔ 2016/679
Συνιστούμε να αναζητήσετε επαγγελματική συμβουλή πριν εφαρμόσετε το ΓΚΠΔ 2016/679.

Αν δεν συμμορφωθώ με τον Κανονισμό

Η μη συμμόρφωση σημαίνει ότι δεν έχετε εγκατεστημένες τις κατάλληλες διαδικασίες και εργαλεία για την αποφυγή παραβίασης των δεδομένων, δεν έχετε τη συγκατάθεση του φυσικού προσώπου να χρησιμοποιεί τα δεδομένα του/της εντός του οργανισμού σας και δεν έχετε τις κατάλλληλες διαδικασίες και εργαλεία για την κοινοποίηση σε περίπτωση παραβίασης των δεδομένων από τις αρχές.
Ο ΓΚΠΔ έχει ιδιαίτερα υψηλό προφίλ κινδύνου λόγω των σημαντικών προστίμων που μπορούν να προσδεθούν στις παραβιάσεις. Μια παραβίαση τύπου Ι (που συνεπάγεται παραβίαση καθήκοντος φροντίδας των πληροφοριών των πελατών σας και ελαφρά παραβίαση του κανονισμού) μπορεί να φέρει πρόστιμα μέχρι 10 εκατομ. ευρώ ή 2% του ετήσιου κύκλου εργασιών του οργανισμού σας. Οι παραβιάσεις τύπου ΙΙ (σημαντικές παραβιάσεις δεδομένων και αποδεικτικά στοιχεία σημαντικής εταιρικής αμέλειας για την εφαρμογή των προβλεπόμενων ελέγχων του κανονισμού) επιφέρουν μέγιστα πρόστιμα 20 εκατ. ευρώ ή 4% του ετήσιου κύκλλυ εργασιών του οργανισμού σας. Αυτά τα πρόστιμα έχουν για να διασφαλίσουν ότι κάθε πελάτης ή δεδομένα προσωπικού που κατέχει ο οργανισμός σας προστατεύονται επαρκώς και κατηγοριοποιούνται κατάκληηλα για να εξασφλίζεται ότι μπορούν να ενημερωθούν ή να αφαιρεθούν κατάλληλα κατόπιν αιτήματος του ατόμου.
Οποιοσδήποτε πολίτης ή φυσικό πρόσωπο που διαμένει σε χώρα της ΕΕ έχει δικαίωμα να αναζητήσει την νομική και ηθική προστασία των δεδομένων του σε οποιαδήποτε Αρχή Προστασίας Δεδομένων ανεξάρτητα από την χώρα που κατοικεί.
Μια σημαντική λεπτομέρεια είναι ότι ο ΓΚΠΔ είναι "Κανονισμός" και όχι "Οδηγία". Η νομική διαφορά είναι ότι ο "Κανονισμός" είναι άμμεσα εκτελεστέως από τα μέλη της ΕΕ και επιφέρει πρόστιμα.

Υπάρχει κάποια πιστοποιήση ή ISO που να με καλύπτει;

Παρόλο που τα πρότυπα ISO είναι πιστοποιημένη διαδικασία και αναφέρεται πολλές φορές στο ΓΚΠΔ, βοηθά μόνο σε ένα βαθμό στο πλαίσιο μιας πλήρους συμμόρφωσης με το ΓΚΠΔ. Αυτή τη στιγμή δεν υπάρχει πρότυπο ISO ή οποιοδήποτε άλλο είδος πιστοποιητικού που θα εφαρμόζεται και θα ισχύει σε όλα τα κράτη μέλη της ΕΕ. Στο άρθρο 42 του Κανονισμού ενθαρύνεται η θέσπιση μηχανισμών πιστοποιήσης, σφραγίδων και σημάτων προστασίας δεδομένων με σκοπό την απόδειξη συμμόρφωσης με τον Κανονισμό. Ο συνεργάτης της LogiSoft, Βασίλης Αθανασίου, κατέχει το πιστοποιητικό DPO Executive που έγινε πιστοποιήση επαγγελματικών προσόντων με βάση το ISO 17024 το οποίο διασφαλίζει ότι τα προσόντα των επαγγελματιών της αξιολογούνται αντικειμενικά και αξιόπιστα με καθορισμένες απαιτήσεις και κριτήρια. Η LogiSoft μπορεί να βοηθήσει τον οργανισμό σας να επιτύχει μαι διαδικασία προστασίας δεδομένων που να συμμορφώνεται με τον κανονισμό με τις βέλτιστες διεθνείς διαδικασίες πιστοποιήσης.

Πως μπορώ να εφαρμόσω των ΓΚΠΔ;

- Ενημερώστε τους ανθρώπους στον οργανισμό σας για τις νέες απαιτήσεις του νόμου.
- Θα πρέπει να τεκμηριώσετε ποια προσωπικά δεδομένα διατηρείτε, από πού προήλθε και με ποιον τα μοιράζεστε. Μπορεί να χρειαστεί να οργανώσετε έναν έλεγχο πληροφοριών.
- Θα πρέπει να ελέγξετε τις τρέχουσες ειδοποιήσεις απορρήτου και να βάλετε ένα σχέδιο για αλλαγές.
- Θα πρέπει να ελέγξετε τις διαδικασίες σας για να βεβαιωθείτε ότι καλύπτουν όλα τα δικαιώματα, συμπεριβελμένου του τρόπου με τον οποίο θα διαγράψετε προσωπικά δεδομένα ή θα παράσχετε δεδομένα ηλεκτρονικά και σε μορφή που χρησιμποιείται συνήθως.
- Θα πρέπει να προσδιορίσετε τη νόμιμη βάση για τη δραστηριότητα επεξεργασίας σας στο ΓΚΠΔ, να την τεκμηριώσετε και να ενημερώσετε την ειδοποιήση σας περί απόρρητου.
- Οι όροι για τη συναίνεση έχουν ενισχυθεί και οι εταιρείες δεν θα μπορούν πλεόν να χρησιμοποιούν μακρούς δυσανάγνωστους όρους νόμιμους, κάθως η αίτηση συγκατάθεσης πρέπει να παρέχεται με κατανοητή και εύκολα προσβάσιμη μορφή, με σκοπό την επεξεργασία δεδομένων που επισυνάπτεται με αυτή τη συναίνεση.
- Πρέπει να βεβαιωθείτε ότι έχετε εφαρμόσει τις καταλληλες διαδικασίες για να εντοπίσετε, να αναφέρετε και να δειρευνήσετε μια παραβίαση προσωπικών δεδομένων.
- Θα πρέπει να εξοικειωθείτε τώρα με τον κώδικα πρακτικής σχετικά με τις αξιολογήσεις των επιπτώσεων στην ιδιωτίκη ζωή,
- Θα πρέπει να ορίσετε κάποιον να αναλάβει την ευθύνη για τη συμμόρφωση με την προστασία των δεδομένων και να αξιολογηθεί πού θα διαδρματιστεί αυτός ο ρόλος στο πλαίσιο της δομής και της διακυβέρνησης του. Εάν ο οργανισμός σας δραστηριοποιείται σε περισσότερα από ένα κράτη μέλη της ΕΕ (δηλ. διεξάγετε διασυνοριακή επεξεργασία), θα πρέπει να καθορίσετε σε ποιά χώρα θα είναι η εποπτική αρχή προστασίας δεδομένων σας.

Είστε έτοιμοι για τον ΓΚΠΔ;

Μετά απο τέσσερα χρόνια προετοιμασίας και συζήτησης, το Ευρωπαικό Συμβούλιο για την προστασία των δεδομένων έγκρινε τον κανονισμό στις 14 Απριλίου 2016. Ημερομηνία εφαρμογής: 25 Μαιου 2018. Ο γενικός κανονισμός προστασίας δεδομένων της ΕΕ αντικαθιστά την οδηγία 95/46/ΕΚ για την προστασία των δεδομένων με σκοπό να εναρμονιστούν οι νόμοι περί απορρήτου δεδομένων σε ολόκληρη την Ευρώπη, να προστατευτούν και να ενισχυθεί η ιδιωτικότητα των δεδομένων των πολιτών της ΕΕ και να αναμορφωθεί ο τρόπος με τον οποίο οι οργανισμοί σε ολόκληρη την περιοχή προσεγγίζουν την ιδιωτική ζωή των δεδομένων.

Η LogiSoft συνεργάζεται με εταιρικούς και ιδιωτικούς πελάτες για την παροχή προσιτών και στρατηγικών λύσεων σε ένα συνεχώς εξελισσόμενο περιβάλλον. Συνδυάζουμε τα πλεονεκτήματα των τελευταίων εργαλείων επιχειρηματικής κλάσης, του έμπειρου προσωπικού και των υπηρεσιών ενός ολοκληρωμένου δικτύου μηχανικών και συμβούλων για να έχετε στην εταιρεία σας μια λύση που διασφαλίζει την εταιρική υποδομή σας. Οι Σύμβουλοι μας έχουν δαιπιστευθεί από την TUV Austria με το πιστοποιητικό 'DPO Executive" σύμφωνα με το πρότυπο ISO 17024 και μπορούμε να επαληθεύσουμε ότι η εταιρεία σας θα μπορέσει να ακολουθήσει μια σωστή και ολοκληρομένη διαδικασία για την εφαρμογή του ΓΚΠΔ 2016/679 αύμφωνα με το ISO 17065

ΣΧΕΔΙΟ	Σχεδιασμός δραστηριοτήτων που θα διεξαχθούν σε κάθε σχετικό τομέα: διοικητικές, επιχειρηματικές μονάδες, ΤΠΕ, επεξεργασία δεδομένων και άλλα. Εκτελέστε GAP ανάλυση για αξιολόγηση.
ΕΝΕΡΓΕΙΑ	Επικοινωνία και Κατάρτηση σε εργαζομένους σχετικά με τα βασικά στοιχεία της ανάλυσης που πραγματοποιήθηκε Παραγωγή των απαιτούμενων εγγράφων: Εγχειρίδιο προστασίας ιδιωτικού απ΄΄ορρητου, Μητρώο δραστηριοτήτων επεξεργασίας, Απορρήτου αξιολόγησης αντικτύπου για τα διάφορα είδη θεραπείας, τυχόν νέες πληροφορίες, αλλαγές στη σύμβαση κ.ά. - Εφαρμογή των νέων απαιτήσεων στο πλαίσιο των επιχειρηματικών διαδικασιών, με ιδιαίτερη έμφαση σε εκείνες που επηρεάζουν τις δραστηριότητες των Επιχειρήσιακών Μονάδων, των Πληροφοριακών Συστημάτων.
ΕΛΕΓΧΟΣ	Ανάλυση όλων των επιχειρηματικών διαδικασιών για την εξασφάλιση της δέουσας τεκμηρίωσης των αρχών της Προστασίας Προσωπικών Δεδομένων, καθώς και των υποχρεώσεων που προβλέπονται για τα δικαιώματα, της ασφάλειας, της παραβίασης, της διαγραφής, και της φορητότητας των δεδομένων.
ΠΡΑΞΗ	Ανασκόπηση όλων των διαδικασιών, λογισμικού, συστημάτων και εργαλείων αποθήκευσης σύμφωνα με τις εκροές που πορκύποτυν από τθς δραστηριότητες ανάλυσης που πραγματοποιήθηκαν.