Πρακτική εφαρμογή του Ευρωπαϊκού Κανονισμού 679/2016 για την προστασία δεδομένων

Ομιλία

Αγαπητέ Πρόεδρε και μέλη του Διοικητικού Συμβουλίου του Συνδέσμου *(Association of Certified Anti-Money Laundering Specialists)*

Αγαπητά μέλη του Συνδέσμου και λοιποί προσκεκλημένοι,

σας ευχαριστώ για την τιμητική πρόσκληση και την ευκαιρία που μου δίνεται να σας μιλήσω για την πρακτική εφαρμογή του νέου Ευρωπαϊκού Κανονισμού που αφορά στην προστασία των προσωπικών δεδομένων.

Στη σημερινή εποχή, με τη χρήση του διαδικτύου και τις νέες υπηρεσίες που παρέχει, την ανάπτυξη της ψηφιακής οικονομίας και την ευρεία χρήση των μέσων κοινωνικής δικτύωσης, η ανάγκη προστασίας της ιδιωτικής ζωής έχει αναδειχθεί σε ένα ιδιαίτερα σημαντικό ζήτημα.

Μέσα σ' ένα τέτοιο πλαίσιο εύλογα μπορεί να αναρωτηθεί κανείς κατά πόσο υπάρχει σήμερα προστασία των προσωπικών δεδομένων. Αυτές ακριβώς οι συνθήκες, οι οποίες δικαιολογούν την ύπαρξη αβεβαιότητας, εξηγούν ταυτόχρονα την αναγκαιότητα ενός ισχυρού νομικού πλαισίου προστασίας. Λόγω της ιλιγγιώδους τεχνολογικής ανάπτυξης, η υφιστάμενη Οδηγία (95/46/ΕΚ), μετά από περίπου μια εικοσαετία, θεωρείται ξεπερασμένη.

Ο Ευρωπαϊκός Κανονισμός 2016/679 τίθεται σε εφαρμογή για όλα τα κράτη μέλη της Ευρωπαϊκής Ένωσης στις 25.05.2018, διαμορφώνοντας ένα ενιαίο νομικό πλαίσιο, χωρίς την ανάγκη ψήφισης εθνικής νομοθεσίας και καταργώντας την υφιστάμενη νομοθεσία. Ο νέος κανονισμός αυξάνει σημαντικά τις υποχρεώσεις των δημόσιων αρχών και των εταιρειών/οργανισμών και αφορά πρακτικά όλες τις επιχειρήσεις, εντός και εκτός Ευρωπαϊκής Ένωσης, εφόσον τα δεδομένα αφορούν Ευρωπαίους πολίτες.

Σε περίπτωση παράβασης προβλέπονται αυξημένα πρόστιμα, που ανάλογα με το είδος και το μέγεθος της, φτάνουν έως τα 20 εκατομμύρια ευρώ ή το 4% του παγκόσμιου ετήσιου κύκλου εργασιών.

Κάποιοι από τους κανόνες του νέου Κανονισμού, υπάρχουν ήδη στο υφιστάμενο νόμο για την προστασία προσωπικών δεδομένων, όπως για παράδειγμα: νομιμότητα, διαφάνεια, περιορισμός του σκοπού, ασφάλεια των δεδομένων, ακεραιότητα και εμπιστευτικότητα.

Ο νέος Κανονισμός, από τη μία πλευρά, ενισχύει τα δικαιώματα των πολιτών και από την άλλη, επιβάλλει μια σειρά νέων υποχρεώσεων στους υπευθύνους επεξεργασίας.

Οι νέες αυτές υποχρεώσεις απορρέουν από τις βασικές αρχές και κυρίως από την ενισχυμένη αρχή της διαφάνειας στον τρόπο συλλογής, τήρησης και γενικά της επεξεργασίας των δεδομένων και τη νέα αρχή της λογοδοσίας, σύμφωνα με την οποία οι υπεύθυνοι επεξεργασίας **φέρουν την ευθύνη και θα πρέπει να είναι σε θέση να αποδείξουν τη συμμόρφωση τους με όλες τις αρχές** που διέπουν την επεξεργασία προσωπικών δεδομένων.

Ο νέος Κανονισμός ενισχύει τις υφιστάμενες αρχές προστασίας των δεδομένων, ως εξής:

Διαφάνεια: Ο υπεύθυνος επεξεργασίας θα πρέπει να αποδεικνύει ότι οι εσωτερικές διαδικασίες του οργανισμού είναι διαφανείς σε σχέση με τα άτομα των οποίων επεξεργάζεται τα προσωπικά δεδομένα τους.

Θα πρέπει να εξηγεί τον τρόπο που τα δεδομένα τυγχάνουν επεξεργασίας, ποια τα δικαιώματα των ατόμων και πως αυτά ασκούνται. Για παράδειγμα, η γλώσσα θα πρέπει να είναι απλή και κατανοητή από τα άτομα στα οποία απευθύνεται.

Περιορισμός του σκοπού: Με κάποιες επιφυλάξεις, η αρχειοθέτηση των δεδομένων προσωπικού χαρακτήρα, τα οποία είναι προς το δημόσιο συμφέρον ή για σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς δεν θεωρείται ασυμβίβαστη με τον αρχικό σκοπό της επεξεργασίας.

Διατήρηση / αποθήκευση: Τα προσωπικά δεδομένα πρέπει να διατηρούνται σε μορφή που να επιτρέπει την αναγνώριση των υποκειμένων των δεδομένων για διάστημα όχι μεγαλύτερο από ότι είναι αναγκαίο για τους σκοπούς για τους οποίους γίνεται η επεξεργασία τους.

Όσον αφορά στο χρονικό διάστημα διατήρησης των προσωπικών δεδομένων των ατόμων, μετά τη λήξη της συμβατικής σχέσης και /ή της διευθέτησης οποιασδήποτε οικονομικής ή άλλης διαφοράς, η θέση του Γραφείου μου είναι ότι, το εν λόγω χρονικό διάστημα **δεν θα πρέπει να υπερβαίνει τα πέντε έτη σχετικά με την παροχή διοικητικών/συμβουλευτικών υπηρεσιών και τα επτά έτη σχετικά με την παροχή λογιστικών/ελεγκτικών υπηρεσιών.**

Όσον αφορά στα δεδομένα πρώην πελατών των τραπεζών, το χρονικό διάστημα δεν θα πρέπει να υπερβαίνει τα 10 έτη. Από το 8^{ο} έτος τα δεδομένα θα πρέπει να αρχειοθετούνται με ειδική διαδικασία και η πρόσβαση σε αυτά θα πρέπει να είναι αυστηρά περιορισμένη, ενώ κάθε εξουσιοδοτημένη πρόσβαση στο ηλεκτρονικό ή έντυπο αρχείο θα πρέπει να αιτιολογείται ειδικά σε μητρώο που θα τηρεί η Τράπεζα και το οποίο θα διαβιβάζεται στο Γραφείο μου ετησίως.

Αναφορικά με τους υποψήφιους πελάτες των οποίων το αίτημα για πιστωτική διευκόλυνση έχει απορριφθεί από την Τράπεζα, θα πρέπει να διαγράφονται το αργότερο εντός 6 μηνών από την κοινοποίηση της σχετικής απόρριψης

Λογοδοσία: Τα άτομα της εταιρείας που διαχειρίζονται και επεξεργάζονται τα προσωπικά δεδομένα, καθίστανται υπεύθυνοι για την απόδειξη της συμμόρφωσης με τις αρχές.

Ο Κανονισμός θέτει νέες υποχρεώσεις στους οργανισμούς οι οποίοι θα πρέπει να εφαρμόσουν ένα ευρύ φάσμα μέτρων, προκειμένου να διασφαλίσουν τη συμμόρφωση τους:

(1) Εφαρμογή κατάλληλων μέτρων και πολιτικών ασφαλείας.

Ο Κανονισμός καθορίζει την κρυπτογράφηση ως μια επιλογή που μπορεί να βοηθήσει να εξασφαλιστεί η συμμόρφωση με κάποιες από τις υποχρεώσεις του. Μάλιστα, το άρθρο 34 προβλέπει ότι, δεν θα χρειαστεί να ανακοινώνεται τυχόν παραβίαση του Κανονισμού, όταν αυτή ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες φυσικών προσώπων, όταν έχουν εφαρμοστεί τα *κατάλληλα τεχνικά και οργανωτικά μέτρα προστασίας και τα μέτρα αυτά εφαρμόστηκαν στα επηρεαζόμενα από την παραβίαση δεδομένα προσωπικού χαρακτήρα, κυρίως μέτρα που καθιστούν μη κατανοητά τα δεδομένα προσωπικού χαρακτήρα σε όσους δεν διαθέτουν άδεια πρόσβασης σε αυτά,* ***όπως είναι η κρυπτογράφηση***.

(2) Διενέργεια εκτίμησης επιπτώσεων των σχεδιαζόμενων πράξεων (impact assessment), για επεξεργασίες που παρουσιάζουν υψηλό κίνδυνο και σχετίζονται με αξιολόγηση προσωπικών πτυχών, αφορούν σε δεδομένα μεγάλης κλίμακας ή σε παρακολούθηση δημοσίου χώρου. Το impact assessment έχει ως στόχο τον εντοπισμό και την ελαχιστοποίηση των κινδύνων μη συμμόρφωσης.

(3) Τήρηση αρχείου δραστηριοτήτων επεξεργασίας: ο οργανισμός θα διατηρεί πλέον λεπτομερή εσωτερικά αρχεία αναφορικά με τις δραστηριότητες προστασίας δεδομένων.

(4) Ορισμός Υπευθύνου Προστασίας Δεδομένων: ο ΥΠΔ θα είναι υπεύθυνος για την παρακολούθηση της συμμόρφωσης με τον Κανονισμό, θα ενημερώνει για τις υποχρεώσεις, θα παράσχει συμβουλές σχετικά με το πότε και πώς θα πρέπει να διενεργηθεί εκτίμηση των επιπτώσεων της σχεδιαζόμενης πράξης και θα αποτελεί το άτομο στο οποίο θα απευθύνεται το Γραφείο μου.

(5) Εφαρμογή της αρχής «Privacy by Design»: θα οφείλει ο Οργανισμός να δημιουργεί δομή, τεχνολογία και διαδικασίες που θα ανταποκρίνονται στις απαιτήσεις του Κανονισμού. Αυτό σημαίνει ότι, ο αρχικός σχεδιασμός κάθε υπηρεσίας ή προϊόντος θα πρέπει να δημιουργεί φιλικές συνθήκες για την προστασία των δεδομένων. Αυτή η προσέγγιση, ενώ προηγουμένως αποτελούσε βέλτιστη πρακτική, πλέον είναι ρητή απαίτηση.

(6) Εφαρμογή της αρχής «Privacy by Default»: θα οφείλει ο Οργανισμός να εφαρμόζει κατάλληλα μέτρα που να διασφαλίζουν ότι, εξ ορισμού, υφίστανται επεξεργασία μόνο τα δεδομένα που είναι απαραίτητα για το σκοπό της επεξεργασίας.

(7) Εκπόνηση και τήρηση Κωδίκων Δεοντολογίας καθώς και εξασφάλιση πιστοποιήσεων, σφραγίδων και σημάτων προστασίας δεδομένων *(εθελοντικά)*.

(8) Προετοιμασία για την πιθανότητα παραβίασης της ασφάλειας των δεδομένων π.χ. παράνομη καταστροφή, απώλεια, αλλοίωση, μη εξουσιοδοτημένη αποκάλυψη ή πρόσβαση σε προσωπικά δεδομένα που διαβιβάζονται, αποθηκεύονται ή επεξεργάζονται με οποιονδήποτε τρόπο.

Οι οργανισμοί θα πρέπει να θέσουν σαφείς πολιτικές και διαδικασίες, έτσι ώστε να διασφαλιστεί ότι θα μπορούν να αντιδράσουν και να γνωστοποιήσουν κάθε παραβίαση δεδομένων, εντός 72 ωρών από τη στιγμή που αποκτούν γνώση του γεγονότος. Επομένως, ενθαρρύνονται να υιοθετούν διαδικασίες γνωστοποίησης ενδεχόμενων παραβάσεων στο Γραφείο μου.

(9) Σε περίπτωση που διεξάγει Οργανισμός διασυνοριακή επεξεργασία, εντός της ΕΕ, πρέπει να ορίσει το κράτος μέλος της κύριας εγκατάστασης, του οποίου η εποπτεύουσα αρχή θα είναι αρμόδια ως επικεφαλής αρχή, για την εποπτεία της νομιμότητας της επεξεργασίας εντός της Ε.Ε.

(10) Οργανισμός που διαβιβάζει προσωπικά δεδομένα σε τρίτη χώρα οφείλει να λάβει την Άδεια μου, εάν επιλέξει ως νομική βάση για τη διαβίβαση συμβατικές ρήτρες που θα ετοιμάσει και θα εγκριθούν από το Γραφείο μου. Εάν από τη διαβίβαση επηρεάζονται και πολίτες κρατών μελών, οι συμβατικές ρήτρες θα εγκριθούν στα πλαίσια του μηχανισμού συνεκτικότητας.

Επιπλέον, ο Κανονισμός ενισχύει τα δικαιώματα των πολιτών.

Μπορεί να χρειαστεί να **αναθεωρηθεί ο τρόπος με τον οποίο λαμβάνεται η συγκατάθεση των ατόμων.** Η συγκατάθεση πρέπει με την ίδια ευκολία να δίδεται και να ανακαλείται. Επιπλέον, η συγκατάθεση θα πρέπει να προέρχεται από μια θετική ένδειξη συμφωνίας για τα δεδομένα που υποβάλλονται σε επεξεργασία και δεν μπορεί να συναχθεί από τη σιωπή ή την αδράνεια του ατόμου.

Ο Κανονισμός **ενισχύει το επίπεδο προστασίας των παιδιών,** αφού πλέον οι γονείς πρέπει να συγκατατίθενται για τη συμμετοχή των παιδιών τους σε υπηρεσίες του διαδικτύου.

Θα πρέπει να επικαιροποιηθούν/ διαμορφωθούν ανάλογα οι διαδικασίες για ικανοποίηση των δικαιωμάτων των ατόμων, που αφορούν:

Στο δικαίωμα πρόσβασης, με βάση το οποίο, το άτομο έχει δικαίωμα να λαμβάνει από τον υπεύθυνο επεξεργασίας επιβεβαίωση για το κατά πόσον ή όχι τα προσωπικά του δεδομένα υφίστανται επεξεργασία και, εάν κάτι τέτοιο συμβαίνει, έχει το δικαίωμα να λάβει (και σε αντίγραφα) αρκετές πληροφορίες, όπως π.χ. το σκοπό της επεξεργασίας, τις κατηγορίες προσωπικών δεδομένων κ.λ.π.

Δεν χρεώνεται το άτομο για τη συμμόρφωση με το αίτημα του και θα πρέπει σε ένα μήνα ο Οργανισμός να συμμορφωθεί.

Στο δικαίωμα εναντίωσης (αντίρρησης), το οποίο μπορεί να ασκηθεί από το άτομο με σκοπό να περιοριστούν συγκεκριμένες επεξεργασίες και να μην υποβληθούν προσωπικά του δεδομένα σε επεξεργασία για σκοπούς απευθείας (άμεσης) εμπορικής προώθησης. Μόλις ένα άτομο αρνηθεί, τα στοιχεία του δεν θα πρέπει να υποβάλλονται σε επεξεργασία για περαιτέρω απευθείας εμπορική προώθηση.

Στο δικαίωμα στη λήθη (διαγραφή των δεδομένων), με το οποίο το άτομο μπορεί να ζητήσει από μηχανές αναζήτησης να αφαιρέσουν συγκεκριμένα αποτελέσματα που το αφορούν, αν δεν υφίσταται νόμιμη βάση για τη διατήρηση τους (εφόσον δεν θίγεται το δικαίωμα ενημερώσεως της κοινής γνώμης) (υπόθεση GOOGLE SPAIN).

Γι' αυτό, θα πρέπει να εξεταστεί πώς πραγματοποιείται η επεξεργασία των δεδομένων και να προσδιοριστεί η νομική βάση με την οποία πραγματοποιείται η εν λόγω επεξεργασία, αφού οι πολίτες θα έχουν ισχυρότερο δικαίωμα σε ότι αφορά στη διαγραφή των δεδομένων τους στις περιπτώσεις που χρησιμοποιείται η συγκατάθεση ως νομική βάση για την επεξεργασία.

Στο δικαίωμα στη φορητότητα, το οποίο είναι ένα νέο δικαίωμα που εισάγεται στον Κανονισμό και κατ επέκταση του δικαιώματος στην απαίτηση για παροχή προσωπικών δεδομένων σε μια ευρέως χρησιμοποιούμενη ηλεκτρονική μορφή (format). Συγκεκριμένα, απαιτείται από τον οργανισμό να παρέχει τις σχετικές πληροφορίες σε μια δομημένη, κοινή και αναγνώσιμη από μηχανή μορφή.

π.χ. πελάτης τράπεζας μπορεί να ζητήσει να λάβει όλες τις πληροφορίες που ο ίδιος παρείχε στην εν λόγω τράπεζα και/ή να ζητήσει, με τεχνολογικά μέσα, τη μεταφορά τους σε άλλη τράπεζα.

Στο **δικαίωμα εναντίωσης που θα μπορούν να ασκήσουν οι πολίτες στην αυτοματοποιημένη λήψη αποφάσεων που τους αφορούν και στη δημιουργία του προφίλ τους**: Για παράδειγμα, αν μια επενδυτική εταιρεία κρίνει βάσει αυτοματοποιημένων υπολογισμών ότι δεν πρέπει να παρέχει μια υπηρεσία σε κάποιο πρόσωπο, πρέπει η τελική αξιολόγηση να υπόκειται σε ανθρώπινη παρέμβαση.

Είναι σχεδόν βέβαιο ότι, αρκετοί τουλάχιστον οργανισμοί, θα αντιμετωπίσουν αρκετές δυσκολίες όπως:

1. Η ακριβής γνώση για το ποια δεδομένα συλλέγονται και τυγχάνουν επεξεργασίας σε κάθε φάση των δραστηριοτήτων τους, ποιοι εμπλέκονται και με ποια εργαλεία και διαδικασίες γίνεται η επεξεργασία.

2. Ο καθορισμός και διαχωρισμός των αναγκών, ώστε να διασφαλίζεται ότι λαμβάνονται οι απαιτούμενες συγκαταθέσεις από τα άτομα και ότι δεν συλλέγονται υπερβολικά δεδομένα.

3. Ο συστηματικός έλεγχος για συμμόρφωση με τις απαιτήσεις του Κανονισμού, σε κάθε στάδιο επεξεργασίας των δεδομένων.

4. Ο εντοπισμός και η αξιολόγηση των κινδύνων (ποιοι είναι, από πού προέρχονται, το είδος της βλάβης π.χ είναι οικονομική ζημιά ή θίγονται τα δικαιώματα των ατόμων;). Το είδος της βλάβης που ενδεχομένως να οδηγήσει σε παραβίαση των προσωπικών δεδομένων, θα υπόκειται σε ψηλές διοικητικές κυρώσεις και επιπτώσεις στη φήμη του οργανισμού.

5. Η λήψη αποτελεσματικών μέτρων με σκοπό να περιοριστεί ή ακόμα και να αποφευχθεί ο κίνδυνος παραβίασης του Κανονισμού, χωρίς να θίγονται οι προτεραιότητες του οργανισμού.

6. Οι τρόποι αντιμετώπισης των παραβάσεων ώστε να διαμορφωθεί στρατηγική και να καταρτιστεί πλάνο και προϋπολογισμός για συμμόρφωση.

Εν κατακλείδι, πιστεύω ότι, ο νέος Κανονισμός θα ενδυναμώσει τα δικαιώματα των πολιτών και θα τους παρέχει καλύτερο έλεγχο των δεδομένων τους, διασφαλίζοντας ότι, η ιδιωτική τους ζωή θα εξακολουθήσει να προστατεύεται στη ψηφιακή εποχή.

Παρ' όλες τις δυσκολίες που συναντούμε και τις αδυναμίες στη στελέχωση και λειτουργία του Γραφείου μου, συνεχίζουμε τις προσπάθειές μας τόσο για ευαισθητοποίηση των πολιτών όσο για ακόμα πιο αποτελεσματική ενημέρωση των υπεύθυνων επεξεργασίας και υιοθέτηση από μέρους τους πολιτικών και πρακτικών που στοχεύουν στην πλήρη συμμόρφωση τους με το νέο Κανονισμό για την προστασία των προσωπικών δεδομένων.

Σας ευχαριστώ για την προσοχή σας.

Ειρήνη Λοϊζίδου Νικολαΐδου
Επίτροπος Προστασίας Δεδομένων
Προσωπικού Χαρακτήρα

13.09.2017