HADPP ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ & ΙΔΙΩΤΙΚΟΤΗΤΑΣ

Προσωπικά Δεδομένα

στο νέο ρυθμιστικό πλαίσιο στην Ε.Ε.

www.dataprotection.gr

Σπύρος Τάσσης, LLM

Γενικά

- **Το νέο ιδιαίτερα αυστηρό πλαίσιο του Κανονισμού φαίνεται ότι αποτελεί και μία προσπάθεια κανονικοποίησης των οικονομικών/επιχειρηματικών όρων δραστηριοποίησης ιδίως στην ψηφιακή αγορά.**

- **Οι παραβάσεις ασφαλείας των δεδομένων είναι αναμενόμενες.**

- **Το ζητούμενο είναι κάθε υπεύθυνος να ενεργήσει σύμφωνα με τα όσα ορίζει ο Κανονισμός ώστε να ελαχιστοποιηθεί ο κίνδυνος.**

Γενικά

Είναι λοιπόν σημαντικό να ξεκινήσουμε με την παραδοχή ότι υπάρχει κίνδυνος για τα προσωπικά δεδομένα που οφείλεται κυρίως σε δύο παράγοντες:

- **Οργανωτικό (ανεπαρκείς διαδικασίες, μη ασφαλή συστήματα και ελλιπής οργάνωση της επίβλεψης τους, ελλιπείς συμβατικές σχέσεις)**
- **Ανθρώπινο (ελλιπής εκπαίδευση του προσωπικού που τα χειρίζεται, ανεπάρκεια συμβατικών ρητρών). Είναι εκπληκτικό το πόσα περιστατικά ασφαλείας οφείλονται στον ανθρώπινο παράγοντα.**

Υποχρεώσεις Υπευθύνων Επεξεργασίας

Οι υποχρεώσεις είναι διάσπαρτες στον Κανονισμό (κυρίως όμως άρθρα 28-37)

- **Υποχρέωση Λογοδοσίας**
- **Ενημέρωση (awareness)**
- **Προστασία Ανηλίκων**
- **Συγκατάθεση**
- **Καταγραφή (διαδικασίες και συμβάντα)**
- **Εκτίμηση Επιπτώσεων**
- **Ανασχεδιασμός Διαδικασιών και Συστημάτων**
- **Υπεύθυνος Προστασίας Δεδομένων**
- **Πολιτικές Ασφαλείας**
- **Σεβασμός στα δικαιώματα**
- **Συνεργασία με τις Εποπτικές Αρχές**
- **Διαχείριση Παραβάσεων**
- **Ενημέρωση Αρχής και Υποκειμένων (γνωστοποίηση/ανακοίνωση)**
- **Διασυνοριακή Ροή (επάρκεια, δεσμευτικοί εταιρικοί κανόνες κλπ.)**

Υποχρεώσεις Υπευθύνων Επεξεργασίας

που αφορούν και συνεργάτες

- Υποχρέωση Λογοδοσίας
- Ενημέρωση (awareness)
- Προστασία Ανηλίκων
- Συγκατάθεση
- Καταγραφή (διαδικασίες και συμβάντα)
- Εκτίμηση Επιπτώσεων
- Ανασχεδιασμός Διαδικασιών και Συστημάτων
- Υπεύθυνος Προστασίας Δεδομένων
- Πολιτικές Ασφαλείας
- Σεβασμός στα δικαιώματα
- Συνεργασία με τις Εποπτικές Αρχές
- Διαχείριση Παραβάσεων
- Ενημέρωση Αρχής και Υποκειμένων (γνωστοποίηση/ανακοίνωση)
- Διασυνοριακή Ροή (επάρκεια, δεσμευτικοί εταιρικοί κανόνες κλπ.)

Νέο Σύστημα Κυρώσεων

- Οι εποπτικές αρχές είναι εξουσιοδοτημένες να επιβάλλουν σημαντικά διοικητικά πρόστιμα τόσο στους υπεύθυνους επεξεργασίας δεδομένων όσο και στους εκτελούντες επεξεργασία δεδομένων.
- Τα πρόστιμα μπορούν να επιβληθούν αντί ή, σωρευτικά με επανορθωτικά μέτρα για ένα ευρύ φάσμα παραβάσεων, συμπεριλαμβανομένων των αμιγώς διαδικαστικών παραβάσεων.
- Τα διοικητικά πρόστιμα δεν είναι υποχρεωτικά. Πρέπει να επιβάλλονται κατά περίπτωση και πρέπει να είναι «αποτελεσματικά, αναλογικά και αποτρεπτικά».
- Δύο επίπεδα διοικητικών προστίμων: - Ορισμένες παραβάσεις θα υπόκεινται σε διοικητικά πρόστιμα ύψους μέχρι 10.000.000 ευρώ ή, στην περίπτωση επιχειρήσεων, 2% του συνολικού κύκλου εργασιών, όποιο από τα δύο είναι υψηλότερο. - Άλλοι θα υπόκεινται σε διοικητικά πρόστιμα ύψους έως 20.000.000 ευρώ ή, στην περίπτωση επιχειρήσεων, το 4% του συνολικού κύκλου εργασιών, όποιο από τα δύο είναι υψηλότερο.

Νέο Σύστημα Κυρώσεων

- **Πρόστιμα μέχρι 20.000.000 ή έως το 4% του συνολικού παγκόσμιου κύκλου εργασιών (όποιο είναι υψηλότερο) για παράβαση:**
- **των βασικών αρχών επεξεργασίας, συμπεριλαμβανομένων των όρων για την έγκριση (αρχές επεξεργασίας, νομιμότητα, συγκατάθεση, ευαίσθητα δεδομένα)**
- **στα δικαιώματα των προσώπων στα οποία αναφέρονται τα δεδομένα (άρθρα 12-22)**
- **στις διασυνοριακές ροές (άρθρα 44-49)**
- **στις υποχρεώσεις που απορρέουν από τις νομοθεσίες των κρατών μελών που εγκρίθηκαν στο πλαίσιο του Κεφαλαίου IX (ειδικές περιπτώσεις επεξεργασίας)**
- **μη συμμόρφωση με εντολή που έχει επιβληθεί από την εποπτική αρχή ή μη συμμόρφωσης με την έρευνα της εποπτικής αρχής βάσει του άρθρου 58 παράγραφος 1**

Νέο Σύστημα Κυρώσεων

- **Πρόστιμα μέχρι 10.000.000 ή έως το 2% του παγκόσμιου κύκλου εργασιών (όποιο είναι υψηλότερο) για παράβαση που αφορά:**
- **συγκατάθεσή για την επεξεργασία των δεδομένων παιδιών (άρθρο 8)**
- **την εφαρμογή των καταλλήλων τεχνικών και οργανωτικών μέτρων**
- **την διασφάλιση της προστασίας δεδομένων από το σχεδιασμό και εξ ορισμού και γενικώς η αθέτηση των υποχρεώσεων του άρθρου 25**
- **μη συμμόρφωση προς εντολή ή προς προσωρινό ή οριστικό περιορισμό της επεξεργασίας ή προς αναστολή της κυκλοφορίας δεδομένων που επιβάλλει η εποπτική αρχή**

- **<u>Σε περίπτωση κοινών υπευθύνων (κατά το άρθρο 26) καλό είναι να συμφωνούν μεταξύ τους την συμμόρφωση γιατί ευθύνονται όλοι</u>**

Νέο Σύστημα Κυρώσεων

- ο υπεύθυνος επεξεργασίας ευθύνεται για την επιλογή των εκτελούντων την επεξεργασία σύμφωνα με το άρθρο 28 παρ. 1 και 2. Υπεργολάβοι μόνο με τη συγκατάθεσή (οπότε και κοινή ευθύνη) του υπευθύνου επεξεργασίας.
- η Επιτροπή μπορεί να θεσπίσει τυποποιημένες συμβατικές ρήτρες για τα θέματα που αναφέρονται στις παραγράφους 3 και 4 του παρόντος άρθρου και σύμφωνα με τη διαδικασία εξέτασης που αναφέρεται στο άρθρο 93 παράγραφος 2.
- πλάσμα γνώσης (και ευθύνης) του υπευθύνου επεξεργασίας το άρθρο 29 (ο εκτελών την επεξεργασία επεξεργάζεται τα εν λόγω δεδομένα μόνον κατ' εντολή του υπευθύνου επεξεργασίας)
- υποχρέωση διατήρησης καταγεγραμμένων αρχείων (άρθρο 30)
- υποχρέωση γνωστοποίησης για παραβιάσεις (εντός 72) ωρών από την γνώση
- κάθε υποκείμενο των δεδομένων έχει το δικαίωμα να υποβάλει καταγγελία σε εποπτική αρχή, ιδίως στο κράτος μέλος στο οποίο έχει τη συνήθη διαμονή του ή τον τόπο εργασίας του ή τον τόπο της εικαζόμενης παράβασης (forum shopping)

Συμβατικές Σχέσεις

- Σχέση υπεύθυνου <-> εκτελούντος
- Σχέση υπεύθυνου <-> βοηθού εκπλήρωσης
- Σχέση από κοινού υπεύθυνων επεξεργασίας
- Σχέση εργασίας εξαρτημένης ή ανεξάρτητης

Συμβατικές Σχέσεις

- **Σχέση από κοινού υπεύθυνων επεξεργασίας**

- **Άρθρο 26**

1. **Σε περίπτωση που δύο ή περισσότεροι υπεύθυνοι επεξεργασίας καθορίζουν από κοινού τους σκοπούς και τα μέσα της επεξεργασίας, αποτελούν από κοινού υπευθύνους επεξεργασίας. Αυτοί καθορίζουν με διαφανή τρόπο τις αντίστοιχες ευθύνες τους για συμμόρφωση προς τις υποχρεώσεις που απορρέουν από τον παρόντα κανονισμό, ιδίως όσον αφορά την άσκηση των δικαιωμάτων του υποκειμένου των δεδομένων και τα αντίστοιχα καθήκοντά τους.**
2. **Η συμφωνία που αναφέρεται στην παράγραφο 1 αντανακλά δεόντως τους αντίστοιχους ρόλους και σχέσεις των από κοινού υπευθύνων επεξεργασίας έναντι των υποκειμένων των δεδομένων. Η ουσία της συμφωνίας τίθεται στη διάθεση του υποκειμένου των δεδομένων.**
3. **Ανεξάρτητα από τους όρους της συμφωνίας που αναφέρεται στην παράγραφο 1, το υποκείμενο των δεδομένων μπορεί να ασκήσει τα δικαιώματά του δυνάμει του παρόντος κανονισμού έναντι και κατά καθενός από τους υπευθύνους επεξεργασίας.**

Συμβατικές Σχέσεις

- **Σχέση υπεύθυνου <-> εκτελούντος**

- **Άρθρο 28**

1. **Όταν η επεξεργασία πρόκειται να διενεργηθεί για λογαριασμό υπευθύνου επεξεργασίας, ο υπεύθυνος επεξεργασίας χρησιμοποιεί μόνο εκτελούντες την επεξεργασία που παρέχουν επαρκείς διαβεβαιώσεις για την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων, κατά τρόπο ώστε η επεξεργασία να πληροί τις απαιτήσεις του παρόντος κανονισμού και να διασφαλίζεται η προστασία των δικαιωμάτων του υποκειμένου των δεδομένων.**
2. **Ο εκτελών την επεξεργασία δεν προσλαμβάνει άλλον εκτελούντα την επεξεργασία χωρίς προηγούμενη ειδική ή γενική γραπτή άδεια του υπευθύνου επεξεργασίας.**
3. **Η επεξεργασία από τον εκτελούντα την επεξεργασία διέπεται από σύμβαση.**
4. **Ο εκτελών επεξεργάζεται τα δεδομένα προσωπικού χαρακτήρα μόνο βάσει καταγεγραμμένων εντολών του υπευθύνου.**

Συμβατικές Σχέσεις

- **Σχέση υπεύθυνου <-> βοηθού εκπλήρωσης**

Σχέση όπως αυτή με τον εκτελούντα την επεξεργασία, χωρίς εντολή συλλογής και επεξεργασίας προσωπικών δεδομένων με αναγκαία όμως ή πιθανά ενδεχόμενη την πρόσβαση σε αυτά λόγω του έργου του (π.χ. Συντήρηση προγράμματος μισθοδοσίας).

Συμβατικές Σχέσεις

- **Σχέση εργασίας εξαρτημένης ή ανεξάρτητης**

- **Είναι απαραίτητο να υπάρχει καταγεγραμμένη η ανάγκη για τήρηση των πολιτικών και διαδικασιών προστασίας προσωπικών δεδομένων**

- **Διαφανείς αρμοδιότητες και δομή σε περίπτωση συμβάντος ασφαλείας.**

- **Διαρκής ενημέρωση και επιμόρφωση**

Ευχαριστώ

Σπύρος Τάσσης
Privacy and TMT
www.tassis.com

HADPP ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ & ΙΔΙΩΤΙΚΟΤΗΤΑΣ

www.dataprotection.gr