ΘΕΜΑΤΟΛΟΓΙΑ ΣΕΜΙΝΑΡΙΟΥ Data Protection Officer (DPO)

1η ημέρα

Εισαγωγή

- Εισαγωγή – Βασικές Ανάγκες & Αιτίες
- Πως φτάσαμε ως εδώ;
- Περί Προστασίας Προσωπικών Δεδομένων (Βασικοί όροι, Λειτουργία, κα)

Κανονιστικές και Νομικές διατάξεις

- Αντικείμενο, βασικοί ορισμοί και έννοιες
- Δεδομένα Προσωπικού Χαρακτήρα
- Κανονισμός και όχι Οδηγία
- Έλεγχοι και πρόστιμα
- Αναγκαιότητα και πεδίο εφαρμογής
- Για ποιο λόγο δημιουργήθηκε;
- Ποιους αφορά;
- Πότε ο νόμος επιτρέπει την επεξεργασία;
- Ποιες οι προϋποθέσεις νόμιμης επεξεργασίας;
- Ποιες οι προϋποθέσεις για συγκατάθεση;
- Πως λαμβάνεται η συγκατάθεση;
- Πλαίσιο ποινικής προστασίας/κυρώσεων σχετικά με την παραβίαση των διατάξεων για την προστασία των προσωπικών δεδομένων
- Τι πρέπει να προσέχουν εργαζόμενοι και υπεύθυνοι επεξεργασίας, πιθανοί κίνδυνοι
- Νομολογιακή αντιμετώπιση μέχρι σήμερα από ποινικής σκοπιάς
- Προϋποθέσεις ισχύουν αν το υποκείμενο των δεδομένων είναι ανήλικος;

2η ημέρα

Ανάλυση και συνοπτική παρουσίαση βασικών άρθρων-σημείων του Κανονισμού

- Έλεγχος Συμμόρφωσης GDPR για Υποκείμενα Δεδομένων
- Μέτρα Συμμόρφωσης που αφορούν τα εξής άρθρα:
- Άρθρο 5- 10 (Αρχές που διέπουν την Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα, Νομιμότητα της Επεξεργασίας, κλπ) Άρθρο 12- Διαφανής Ενημέρωση, Ανακοίνωση και Ρυθμίσεις για την Άσκηση των Δικαιωμάτων του υποκειμένου των Δεδομένων
- Άρθρα 13 και 15-22 (Ενημέρωση, Διόρθωση, Διαγραφή, κλπ.)
- Άρθρο 34- Ανακοίνωση Παραβίασης Δεδομένων Προσωπικού Χαρακτήρα στο υποκείμενο των Δεδομένων
- Άρθρο 88- Επεξεργασία στο Πλαίσιο της Απασχόλησης

Έλεγχος Συμμόρφωσης GDPR για Υπεύθυνους Επεξεργασίας (Controllers)

- Μέτρα συμμόρφωσης που αφορούν τα εξής άρθρα:
- Άρθρο 24- Ευθύνη του Υπευθύνου Επεξεργασίας
- Άρθρο 25- Προστασία των Δεδομένων ήδη από το Σχεδιασμό και εξ' ορισμού
- Άρθρο 26-31 Από κοινού Υπεύθυνοι Επεξεργασίας, Αρχεία Επεξεργασίας, κλπ.
- Άρθρο 32- 34 Ασφάλεια Επεξεργασίας και γνωστοποίηση Παραβίασης Δεδομένων
- Άρθρο 35- Εκτίμηση αντίκτυπου σχετικά με την Προστασία Δεδομένων

- Άρθρο 37- 39 Υπεύθυνος Προστασίας Δεδομένων
- Άρθρο 44- 50 Διαβίβαση Προσωπικών Δεδομένων

Έλεγχος Συμμόρφωσης GDPR για Εκτελούντες την Επεξεργασία (Processors)

- Άρθρο 27- Εκπρόσωποι Υπευθύνων Επεξεργασίας ή Εκτελούντων την Επεξεργασία μη εγκατεστημένων στην Ένωση
- Άρθρο 28- Εκτελών την Επεξεργασία
- Άρθρο 29- Επεξεργασία υπό την εποπτεία του Υπευθύνου Επεξεργασίας ή του Εκτελούντος την Επεξεργασία
- Άρθρο 30- Αρχεία των Δραστηριοτήτων Επεξεργασίας
- Άρθρο 31- Συνεργασία με την Εποπτική
- Αρχή Άρθρο 32- 34 Ασφάλεια Επεξεργασίας και γνωστοποίηση Παραβίασης Δεδομένων
- Άρθρο 37- 39 Υπεύθυνος Προστασίας Δεδομένων
- Άρθρο 44- 50 Διαβίβαση Προσωπικών Δεδομένων

3η ημέρα

Οργανωτικές υποχρεώσεις

- **Υπεύθυνος Προστασίας Δεδομένων (Data Protection Officer, DPO)**
  - Προϋποθέσεις ύπαρξης DPO:
  ~ διενέργεια επεξεργασίας από δημόσια αρχή ή φορέα
  ~ τακτική και συστηματική παρακολούθηση σε μεγάλη κλίμακα
  ~ οι βασικές δραστηριότητες του ΥΕ ή του ΕΕ συνιστούν μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα
  – Ποιες είναι οι βασικές δραστηριότητες του DPO;
  – Ευθύνες & Απαιτήσεις
  – Ποια είναι τα απαιτούμενα προσόντα;
  – Ποιος μπορεί να οριστεί ως DPO;
  – Διαχείριση μέσω outsource ή in-house;
  – Πότε και από ποιους πρέπει να υποστηρίζεται;
  – Ανώτατη Διοίκηση
  – Υποστηρικτικές Ομάδες
  – Τι κάνει ο DPO πριν τον Μάιο του 2018 και τι μετά;
- **Υπεύθυνος Επεξεργασίας (Controllers)**
  – Ευθύνες και καθήκοντα
  – Ρόλος
  – Παραδείγματα
- **Εκτελών την Επεξεργασία (Processors)**
  – Ευθύνες και καθήκοντα
  – Ρόλος
  – Παραδείγματα
- **Τι ισχύει για τις ειδικές κατηγορίες Δεδομένων Προσωπικού Χαρακτήρα;**
  – Πληροφόρηση
  – Πότε πρέπει να παρέχεται η πληροφόρηση;
  – Ποια πληροφόρηση πρέπει να παρέχεται;

– Πως παρέχεται η πληροφόρηση;
– Ποιο το κόστος της πληροφόρησης;
– Ποιες οι εξαιρέσεις;
– Από κοινού υπεύθυνοι επεξεργασίας
– Αυτοματοποιημένη λήψη αποφάσεων και κατάρτιση προφίλ

• **Αρχείο Δραστηριοτήτων Επεξεργασίας (Data Flow Mapping)**
– Πότε απαιτείται η τήρηση του αρχείου;
– Τι περιλαμβάνει το αρχείο;
– Ποια είναι η μορφή του αρχείου;
– Τρόποι και συχνότητα τήρησης

• **Μελέτη Εκτίμησης Αντίκτυπου Επικινδυνότητας (Data Protection Impact Assessment, DPIA)**

• **Δικαιώματα Φυσικών Προσώπων**
– Δικαίωμα πρόσβασης
– Δικαίωμα διόρθωσης
– Δικαίωμα διαγραφής
– Δικαίωμα περιορισμού επεξεργασίας
– Δικαίωμα στη φορητότητα
– Δικαίωμα εναντίωσης
– Case studies – Real Case Scenarios
– Δικαίωμα στη φορητότητα
– Δικαίωμα εναντίωσης

• **Εσωτερική Οργάνωση**
– Πολιτικές και Διαδικασίες PIMS
– Ποιες είναι οι νέες πολιτικές και διαδικασίες που απαιτούνται;
– Πως επιτυγχάνεται η άμεση και αποτελεσματική τροποποίησή τους;
– Συμβατικές υποχρεώσεις:
~ Έλεγχος
~ Βελτίωση
~ Επικαιροποίηση
– Σχέσεις με προμηθευτές
– Γνώση και εκπαίδευση προσωπικού
– Μηχανισμοί ικανοποίησης αιτημάτων φυσικών προσώπων
– Επιθεώρηση και συνεχής βελτίωση
– Μηχανισμοί εσωτερικού ελέγχου
– Πότε γίνεται εσωτερική επιθεώρηση
– Πως γίνεται η μέτρηση της απόδοσης-KPIs
– Πως επιτυγχάνεται η συνεχής βελτίωση

4η ημέρα

Τεχνικά Μέτρα – Τεχνικές προδιαγραφές

• **Πότε απαιτείται Μελέτη Εκτίμησης Αντικτύπου Επικινδυνότητας;**

– Ποιος είναι υπεύθυνος για τη διενέργειά της;
– Κάθε πότε πρέπει να διενεργείται;
– Με ποιον τρόπο;
– Τι περιέχει;

• **Υποκείμενο των Δεδομένων**

• **Υπεύθυνος Επεξεργασίας**
– από κοινού Υπεύθυνοι
– Εκτελών την Επεξεργασία
– η αυξημένη ευθύνη του processor

• **Αρχείο καταγραφής δραστηριοτήτων**

• **Τι σημαίνει Privacy by design και Privacy by default;**

• **Μεταφορά προσωπικών δεδομένων**
– Διαβίβαση Δεδομένων Προσωπικού Χαρακτήρα
– Πότε επιτρέπεται η Διαβίβαση;
– Διαβίβαση εκτός ΕΕ
– Πως διαχειριζόμαστε τα Δεδομένα Προσωπικού Χαρακτήρα για τους εργαζόμενους:
~ Διαδικασία πρόσληψης
~ Κατά την εργασία
~ Μετά την αποχώρηση

• **IT Department & GDPR**
– Διαχείριση δεδομένων (καταγραφή, ανάκτηση, mapping, ταξινόμηση)
– Data masking or data obfuscation
– Κρυπτογράφηση δεδομένων
– Security Information and Event Management (SIEM)
– Monitoring/ IDS/ IPS
– Κρυπτογράφηση και διαχείριση δεδομένων που διακινούνται μέσω Email
– Διαχείριση κινητών και άλλων συναφών συσκευών
– Διαχείριση του Personally Identifiable Information (PII) owner rights
– Data deletion and data portability

5η ημέρα

Ασφάλεια Πληροφοριών GDPR

• **Φυσική Ασφάλεια εγκαταστάσεων και πληροφοριών σε σχέση με τις υποχρεώσεις του Γενικού Κανονισμού**
– Διαχείριση φυσικού αρχείου δεδομένων προσωπικού χαρακτήρα
– Μέτρα ασφάλειας σε περιπτώσεις φυσικού συμβάντος
• **Ασφάλεια Πληροφοριών/Δεδομένων (IT SECURITY) – Βασικές Αρχές**
• **Θέματα Cyber Safety/Security και Ασφάλειας Δεδομένων**

• Συμμόρφωση με Πρότυπα και Βέλτιστες Πρακτικές Ασφάλειας (ISO 27001, 27002 κτλ) – Πολιτικές Ασφάλειας Πληροφοριών

– Γενικά – ISO 27001

~ Οδηγίες για τον καθορισμό προδιαγραφών για:

-> το Σχεδιασμό -> την Υλοποίηση -> τη Λειτουργία -> την Παρακολούθηση

– τον Έλεγχο και Συντήρηση ενός τεκμηριωμένου Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ) σε ένα οργανωσιακό πλαίσιο

• Αντιμετώπιση και Διαχείριση περιστατικών παραβίασης προσωπικών δεδομένων (data breaches)

– Πότε απαιτείται γνωστοποίηση για συμβάν παραβίασης;

– Ποιος είναι ο υπεύθυνος για τη γνωστοποίηση;

– Τι πρέπει να περιλαμβάνει η γνωστοποίηση;

– Τεκμηρίωση συμβάντων – συνέπειες και μέτρα

– Ανακοίνωση παραβίασης δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων

– Πότε απαιτείται ανακοίνωση;

– Ποιος είναι ο υπεύθυνος για την ανακοίνωση;

– Σχέδιο για την Αντιμετώπιση Περιστατικών παραβίασης δεδομένων προσωπικού χαρακτήρα (Incident Reponse Plan)

• Μελέτες περίπτωσης (Case Studies) και υποθετικές περιπτώσεις παραβίασης Προσωπικών Δεδομένων (προσομοίωση συμβάντων – περιστατικών)

• Τεχνικά και οργανωτικά μέτρα (controls) για τον μετριασμό κινδύνων από τη διαχείριση των προσωπικών δεδομένων και την πρόληψη περιστατικών παραβιάσεων προσωπικών δεδομένων

• Προετοιμασία για τις εξετάσεις

Εκπαιδευτές

Ενδεικτικά Αναφέρονται

ΚΟΥΡΟΥΠΗΣ ΚΩΝΣΤΑΝΤΙΝΟΣ:

Λέκτορας Τμήματος Νομικής, Σχολής Νομικής και Διοίκησης Επιχειρήσεων του Πανεπιστημίου FREDERICK στην Κύπρο, Ακαδημαϊκά Υπεύθυνος του Μοντέλου Προσομοίωσης Οργανισμού Ηνωμένων Εθνών, υπό τον τίτλο FREDMUN (Frederick Model United Nations). Εκπαιδευτής και αξιολογητής στο ευρωπαϊκό πρόγραμμα «*Σχολείο-Πρεσβευτής του Ευρωπαϊκού Κοινοβουλίου*», υπό την αιγίδα του Γραφείου Ενημέρωσης του Ευρωπαϊκού Κοινοβουλίου στην Κύπρο σε συνεργασία με το Υπουργείο Παιδείας και Πολιτισμού της Κυπριακής Δημοκρατίας.

ΙΩΑΝΝΗΣ Α. ΣΑΡΑΚΗΝΟΣ:

Δικηγόρος LL.M. (London School of Economics), με ειδίκευση στο χρηματοπιστωτικό, εμπορικό και δημόσιο δίκαιο. Νομικός σύμβουλος διεθνών εταιρειών και ΝΠΔΔ ΟΤΑ. Επικεφαλής Νομικός Σύμβουλος Δήμος Data, ειδικός σε θέματα ΝΠΔΔ, Σχολικών Επιτροπών και Προσωπικών Δεδομένων. Εκτεταμένη εμπειρία σε πολύπλοκα ζητήματα επεξεργασίας Προσωπικών Δεδομένων, υποβολής απαιτούμενων γνωστοποιήσεων στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και στην διασυνοριακή διαβίβαση Προσωπικών Δεδομένων εντός και εκτός ΕΕ. Ένας εκ των συνεργατών-συντακτών του ετήσιου ένθετου για το "Επιχειρείν στην Ελλάδα" για λογαριασμό της Παγκόσμιας Τράπεζας.

ΣΤΕΦΑΝΟΣ Ι.ΑΝΔΡΙΑΚΟΠΟΥΛΟΣ:

Δικηγόρος παρ' Αρείω Πάγω - Νομικός Σύμβουλος με εξειδίκευση στο Δίκαιο του Διαδικτύου, το Ηλεκτρονικό Εμπόριο, την Προστασία Προσωπικών Δεδομένων και το Ηλεκτρονικό Έγκλημα.

ΖΑΦΕΙΡΟΠΟΥΛΟΣ Γ.ΑΝΔΡΕΑΣ

Εμπειρογνώμονας – Πληροφορικός, εξειδικευμένος σε θέματα Ασφάλειας Προσώπων και Κρίσιμων Υποδομών, καθώς και σε θέματα σχετικά με την Ψηφιακή Ασφάλεια, την Ιδιωτικότητα και τη Προστασία Προσωπικών Δεδομένων στις Νέες Τεχνολογίες. Διαθέτει εργασιακή εμπειρία άνω των 15 ετών στη φυσική Ασφάλεια Προσώπων και Εγκαταστάσεων και στην Ασφάλεια Τεχνολογιών Πληροφορικής και Επικοινωνιών (Information and Communication Technologies – ICT Security). Πτυχιούχος Πληροφορικής του Πανεπιστημίου Πειραιώς, Πτυχιούχος Λογιστικής του Α.Τ.Ε.Ι. Πειραιά και υποψήφιος κάτοχος Μεταπτυχιακού Διπλώματος του Εθνικού & Καποδιστριακού Πανεπιστημίου Αθηνών, με Ειδίκευση: «Διοίκηση & Οικονομική των Τηλεπικοινωνιακών Δικτύων».

ΓΕΩΡΓΙΟΣ ΓΕΡΜΑΝΟΣ

Αξιωματικός της Ε.Α. με επαγγελματική εμπειρία πλέον των 10 ετών στην πρόληψη και στην αντιμετώπιση κυβερνοεγκλήματων, στην προστασία προσωπικών δεδομένων στο Διαδίκτυο και στην Ασφάλεια Τεχνολογιών Πληροφοριών και Επικοινωνιών (ICT Security). Πτυχιούχος Πληροφορικής του Πανεπιστημίου Πειραιώς, κάτοχος μεταπτυχιακών στις «Τεχνολογίες & Διοίκηση Πληροφοριακών και Επικοινωνιακών Συστημάτων» (Πανεπιστήμιο Αιγαίου) καθώς και στις «Διεθνείς & Ευρωπαϊκές Σπουδές» (Πάντειο Πανεπιστήμιο). Αναπλ. Καθηγητής στην Σχολή Αξιωματικών της Ε.Α. και επισκέπτης καθηγητής στο Διεθνές Πανεπιστήμιο Ελλάδος, στο πρόγραμμα μεταπτυχιακών σπουδών «MSc in Communications & Cybersecurity».