**Δομή Εκπαιδευτικού προγράμματος DPO 7**

Πρώτο Μέρος Εκπαίδευσης (Βασικές έννοιες)

Ενότητα 1:

Εισαγωγή στις βασικές έννοιες του Γενικού Κανονισμού Προστασίας Δεδομένων: Βασικές Αρχές και ορισμοί της νομοθεσίας, νομιμότητα της επεξεργασίας και η ερμηνεία τους σύμφωνα με αποφάσεις εθνικών και Ευρωπαϊκών Ανεξάρτητων Αρχών και Δικαστηρίων. Συνοπτική παρουσίαση του Ευρωπαϊκού και του νέου εθνικού νομικού πλαισίου.

Ενότητα 2:

Συνοπτική παρουσίαση των ρόλων και των καθηκόντων του Υπεύθυνου Επεξεργασίας (Data Controller), του από Κοινού Υπεύθυνου Επεξεργασίας, του Εκτελούντος την επεξεργασία (Για την κατανόηση των ρόλων και καθηκόντων θα χρησιμοποιηθούν παραδείγματα και ερμηνευτικά κείμενα). Στην ενότητα περιλαμβάνεται επίσης ειδική αναφορά στην τεχνική του ελέγχου των συμβατικών κειμένων που ρυθμίζουν τις υποχρεώσεις των μερών.

Ενότητα 3:

Ο Υπεύθυνος Προστασίας Δεδομένων (DPO) και οι υποχρεώσεις του. Ενημέρωση του Υπεύθυνου επεξεργασίας ή του εκτελούντα την επεξεργασία, η παρακολούθηση της συμμόρφωσης και εφαρμογής της νομοθεσίας σχετικά με την προστασία δεδομένων, η ενημέρωση των υπαλλήλων και η πραγματοποίηση ελέγχων, παρακολούθηση υλοποίησης, και η επικοινωνία και συνεργασία με εποπτικές αρχές, η πραγματοποίηση διαβούλευσης (πρακτικές ασκήσεις μέσω ειδικά διαμορφωμένων σεναρίων προσομοίωσης).

Ενότητα 4:

Η διενέργεια μελέτης εκτίμησης αντικτύπου (Μεθοδολογία CNIL, ENISA και πρακτικά υποδείγματα) και κινδύνων που συνδέονται με δραστηριότητες επεξεργασίας- Η διασυνοριακή μεταβίβαση δεδομένων (Γενικές αρχές για διαβιβάσεις- Δεσμευτικοί εταιρικοί κανόνες- Παρεκκλίσεις για ειδικές καταστάσεις).

Ενότητα 5:

Προστασία δεδομένων στις ηλεκτρονικές επικοινωνίες. Η οδηγία 2002/58 και η ενσωμάτωσή της στο Ν. 3471/2006. Η νέα Πρόταση Κανονισμού.

Ενότητα 6:

Βιντεοεπιτήρηση. Υποχρεώσεις υπευθύνων επεξεργασίας. Υποδείγματα ενημέρωσης δύο επιπέδων. Δικαιώματα υποκειμένων των δεδομένων. Δημόσιοι και ιδιωτικοί χώροι.

Ενότητα 7:

Αντιμετώπιση και Διαχείριση περιστατικών παραβίασης προσωπικών δεδομένων (Data breaches).Γνωστοποίηση παραβίασης στην ΑΠΔΧ και ανακοίνωση παραβίασης στο υποκείμενο. Σχέδιο/Διαδικασία  για την αντιμετώπιση κ διαχείριση περιστατικών παραβίασης προσωπικών δεδομένων (Incident Response Plan). Μελέτες περίπτωσης (case studies) και υποθετικές παραβιάσεις προσωπικών δεδομένων-προσομοίωση συμβάντων και περιστατικών ( με  ενεργητική συμμετοχή εκπαιδευομένων/ συμμετεχόντων).

Ενότητα 8:

Ασφάλεια Πληροφοριών και Δεδομένων προσωπικού χαρακτήρα (IT Security). Βασικές Αρχές – Θέματα Cyber Security and Safety.  Αξιολόγηση κινδύνων ασφάλειας πληροφοριών (risk assessment- Μεθοδολογίες κ εργαλεία).

Ενότητα 9:

Φυσική Ασφάλεια εγκαταστάσεων και δεδομένων σε σχέση με τον ΓΚΠΔ. Κίνδυνοι, Αξιολόγηση και εκτίμηση κινδύνων, μέτρα φυσικής ασφάλειας, Πολιτική  φυσικής και περιβαλλοντικής ασφάλειας. Χρήσης συστημάτων ασφάλειας (κάμερες / cctv) και συμμόρφωση με ΓΚΠΔ.

Ενότητα 10:

Τεχνικά και οργανωτικά μέτρα ασφάλειας επεξεργασίας προσωπικών δεδομένων. Σχέδιο Ασφάλειας του Συστήματος Επεξεργασίας Προσωπικών Δεδομένων. Πολιτικές ασφάλειας πληροφοριακών συστημάτων. Επίδειξη τεχνικών και μεθοδολογιών κρυπτογράφησης και ψευδωνυμοποίησης στην πράξη με ενεργητική συμμετοχή εκπαιδευομένων και πρακτική άσκηση Συμμόρφωση  με Βέλτιστες Πρακτικές και Διεθνή πρότυπα ασφάλειας πληροφοριών ( ISO 27001, ISO 27002, CobIT), NIST/SP 800-53).

Ενότητα 11:

Επιχειρησιακή συνέχεια και πλάνο ανάκαμψης συστημάτων, πληροφοριών και δεδομένων  μετά από καταστροφή (Business continuity plan and disaster recovery plan). Βέλτιστες πρακτικές στη Διαχείριση επιχειρησιακής συνέχειας  σύμφωνα και με το Διεθνές Πρότυπο ISO 22301.

Ενότητα 12:

Κυρώσεις (Πειθαρχικές Κυρώσεις και Πρόστιμα).

Δεύτερο Μέρος Εκπαίδευσης (Ειδικό)

Κατεύθυνση: Ειδικά ζητήματα κανονιστικής συμμόρφωσης

Ενότητα 1:

Η Οδηγία 2016/680/ΕΕ («Αστυνομική οδηγία») και η ενσωμάτωση της στο εθνικό δίκαιο με Ν. 4624/2019: Πεδίο εφαρμογής, Βασικές αρχές. Υποχρεώσεις διωκτικών και δικαστικών αρχών. Διαφορές με τον  ΓΚΠΔ.

Ενότητα 2:

Βασικές αρχές και υποχρεώσεις του Δημοσίου Τομέα στο πλαίσιο του Γενικού Κανονισμού Προστασίας Δεδομένων (Κανονισμός (ΕΕ) 2016/679)-Ειδικότερη εφαρμογή των αρχών του Κανονισμού (ΕΕ) 2016/679 στο Δημόσιο Τομέα. Ορισμοί και καθορισμός των ρόλων που θέτει ο Κανονισμός στο Δημόσιο Τομέα: Πότε το Δημόσιο είναι Υπεύθυνος Επεξεργασίας, Εκτελών ή Από Κοινού Υπεύθυνος Επεξεργασίας;

Οι βασικές  Αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα στο Δημόσιο Τομέα και η νομική βάση των επεξεργασιών που πραγματοποιούνται από το Δημόσιο. Ο διορισμός ΥΠΔ στο Δημόσιο και οι υποχρεώσεις του.

Ενότητα 3:

Ειδικότερες εκφάνσεις των δικαιωμάτων των υποκειμένων των δεδομένων στο Δημόσιο.  Η διαχείριση αιτημάτων πρόσβασης σε στοιχεία τρίτων και η εφαρμογή των ειδικών κανόνων του Διοικητικού  Δικαίου.  Τα δικαιώματα των υποκείμενων των δεδομένων (διοικούμενοι, εργαζόμενοι, προμηθευτές) στο Δημόσιο και οι υποχρεώσεις του τελευταίου. Η διαμόρφωση ενημερωτικών εντύπων και Πολιτικών που διασφαλίζουν την προστασία των δεδομένων προσωπικού χαρακτήρα.

Ενότητα 4:

Η κοινοποίηση των δεδομένων προσωπικού χαρακτήρα σε τρίτους. Το Πρόγραμμα Δι@υγεια και η εφαρμογή του Κανονισμού ΕΕ 2016/679. Η δημοσίευση των δεδομένων προσωπικού χαρακτήρα στις δημοσιευτέες Διοικητικές πράξεις. Η ανάρτηση δεδομένων προσωπικού χαρακτήρα στις ιστοσελίδες των Δημοσίων Φορέων

Ενότητα 5:

Η διαχείριση ειδικών κατηγοριών δεδομένων υγείας στον Δημόσιο (Νοσοκομεία- Κοινωνικές Υπηρεσίες Περιφερειών- Φορείς κοινωνικής Ασφάλισης) και στον Ιδιωτικό Τομέα (Ασφαλιστικές Εταιρείες, Ιδιωτικά Νοσοκομεία, Διαγνωστικά Κέντρα) Η διαχείριση ειδικών κατηγοριών δεδομένων- Νομιμότητα της επεξεργασίας- Συγκατάθεση και δικαιώματα του υποκειμένου- Υποχρεώσεις Υπεύθυνου Επεξεργασίας, Υπεύθυνου προστασίας δεδομένων, Εκτελούντων την επεξεργασία (πρακτικές ασκήσεις σεναρίων προσομοίωσης από μελέτες περιπτώσεων)

Ενότητα 6:

Ειδικές επεξεργασίες δεδομένων σε Χρηματοπιστωτικά ιδρύματα – (Διαδικασία AML, Τειρεσίας)- Συγκατάθεση και δικαιώματα του υποκειμένου- Πρόσβαση σε έγγραφα και διαχείριση καταγγελιών- Υποχρεώσεις Υπεύθυνου Επεξεργασίας, Υπεύθυνου προστασίας δεδομένων, Εκτελούντων την επεξεργασία(πρακτικές ασκήσεις σεναρίων προσομοίωσης από μελέτες περιπτώσεων)

Ενότητα 7:

Η εφαρμογή του Κανονισμού σε πολύ μικρές, μικρές και μεσαίες επιχειρήσεις. Η υιοθέτηση πολιτικών συμμόρφωσης με τον Κανονισμό (Πρακτικά υποδείγματα)

Ενότητα 8:

Η εφαρμογή του Κανονισμού στους φορείς του δημοσίου τομέα (Πρακτικά υποδείγματα)