5 – Νομικά Θέματα

Εθνική Σχολή Δημόσιας Διοίκησης & Αυτοδιοίκησης
Απρίλιος 2021

Ασφάλεια Πληροφοριακών Συστημάτων, Δικτύων και Δεδομένων

Νόμος 4577/2018

- Με το Νόμο 4577/2018 (ΦΕΚ Α’ 199/3-12-2018) ενσωματώθηκε στην ελληνική νομοθεσία η **Οδηγία 2016/1148/ΕΕ (Network and Information Security – NIS)** του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου με την οποία «θεσπίζονται μέτρα για την επίτευξη υψηλού επιπέδου ασφάλειας των συστημάτων δικτύου και πληροφοριών».

Οδηγία NIS

- Η Οδηγία προτείνει ένα ευρύ φάσμα μέτρων για την ενίσχυση του επιπέδου ασφάλειας των συστημάτων δικτύου και πληροφοριών για την εξασφάλιση υπηρεσιών που είναι ζωτικής σημασίας για την οικονομία και την κοινωνία της Ευρωπαϊκής Ένωσης.

Επιθέσεις στον κυβερνοχώρο

- Στόχος της είναι να εξασφαλίσει ότι οι χώρες της Ε.Ε. είναι καλά προετοιμασμένες και έτοιμες να χειριστούν και να αντιμετωπίσουν επιθέσεις στον κυβερνοχώρο μέσω:
  - του διορισμού αρμόδιων αρχών,
  - της δημιουργίας ομάδων απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών Computer Security Incident Response Teams (CSIRT)
  - της υιοθέτησης εθνικών στρατηγικών για την ασφάλεια στον κυβερνοχώρο.

CSIRTs

Οι CSIRT είναι υπεύθυνες μεταξύ άλλων για:

- (α) την παρακολούθηση και την αντιμετώπιση συμβάντων ασφαλείας στον κυβερνοχώρο,
- (β) την παροχή ανάλυσης κινδύνων και συμβάντων και την επίγνωση της κατάστασης,
- (γ) τη συμμετοχή στο δίκτυο CSIRT,
- (δ) τη συνεργασία με τον ιδιωτικό τομέα και
- (ε) την προώθηση της χρήσης τυποποιημένων πρακτικών για τον χειρισμό συμβάντων και κινδύνων και την ταξινόμηση πληροφοριών.

Βασικό Σημείο της Οδηγίας

- Βελτίωση των εθνικών δυνατοτήτων για την ασφάλεια στον κυβερνοχώρο. Οι χώρες της Ε.Ε., μεταξύ αυτών και η Χώρα μας είναι υποχρεωμένες:
  - **να ορίζουν** μία ή περισσότερες εθνικές αρμόδιες αρχές και CSIRT
  - **να προσδιορίζουν** ένα ενιαίο κέντρο επαφής [Εθνική Αρχή Κυβερνοασφάλειας] (σε περίπτωση που υπάρχουν περισσότερες από μία αρμόδιες αρχές)·
  - **να προσδιορίζουν τους παρόχους βασικών υπηρεσιών σε σημαντικούς τομείς**, όπως η ενέργεια, οι μεταφορές, η χρηματοδότηση, οι τράπεζες, η υγεία, η ύδρευση και η ψηφιακή υποδομή, **στους οποίους μια επίθεση στον κυβερνοχώρο θα μπορούσε να διαταράξει μια βασική υπηρεσία**.

Εθνική Αρχή Κυβερνοασφάλειας

- Με το Ν. 4577/2018 ορίσθηκε για την Ελλάδα ως Εθνική Αρχή Κυβερνοασφάλειας **η Διεύθυνση Κυβερνοασφάλειας Υπουργείου Ψηφιακής Διακυβέρνησης**.
- Η Αρχή αυτή, **ως φορέας υψηλού πολιτικού - κυβερνητικού επιπέδου με εξειδικευμένα στελέχη**, παρακολουθεί και υλοποιεί τις δράσεις της Εθνικής Στρατηγικής Κυβερνοασφάλειας.

Εθνική Αρχή Κυβερνοασφάλειας

- Είναι αρμόδια για τον συντονισμό μεταξύ των φορέων που δραστηριοποιούνται στην Ελλάδα στον τομέα της ασφάλειας στον κυβερνοχώρο, τόσο στο δημόσιο *[Διεύθυνση Κυβερνοχώρου (ΕΥΠ) – Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων – Εθνικό CERT, Διεύθυνση Κυβερνοάμυνας (ΓΕΕΘΑ), Αρχή Διασφάλισης Απορρήτου Επικοινωνιών (ΑΔΑΕ), Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), Κέντρο Μελετών Ασφαλείας* όσο και στον ιδιωτικό τομέα.

Εθνική Στρατηγική Κυβερνοασφάλειας

- Η Εθνική Στρατηγική Κυβερνοασφάλειας, που εγκρίθηκε το Μάρτιο του 2018, αποτελεί τον επιτελικό σχεδιασμό της Ελληνικής Πολιτείας για την ασφάλεια στον κυβερνοχώρο.
  - **Στόχος είναι** η δημιουργία ενός ασφαλούς περιβάλλοντος Διαδικτύου, υποδομών και υπηρεσιών, που θα τονώσει την εμπιστοσύνη των πολιτών και θα τους οδηγήσει στην περαιτέρω χρήση νέων ψηφιακών προϊόντων και υπηρεσιών και στην τόνωσης της οικονομικής ανάπτυξης της Χώρας.
  - https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSSGR.pdf/

Τι περιλαμβάνει

- Μεταξύ άλλων, στην Εθνική Στρατηγική Κυβερνοασφάλειας περιλαμβάνονται τα εξής:
  - **πλαίσιο διακυβέρνησης** για την επίτευξη των στόχων και των προτεραιοτήτων της εθνικής στρατηγικής για την ασφάλεια συστημάτων δικτύων και πληροφοριών, συμπεριλαμβανομένων του **ρόλου και των αρμοδιοτήτων** των κυβερνητικών οργάνων και των λοιπών αρμόδιων φορέων,
  - **μέτρα ετοιμότητας, απόκρισης και αποκατάστασης**, συμπεριλαμβανομένης **της συνεργασίας** ανάμεσα στο δημόσιο και ιδιωτικό τομέα,

Τι περιλαμβάνει

- Στην Εθνική Στρατηγική Κυβερνοασφάλειας περιλαμβάνονται τα εξής:
  - αναφορά σε προγράμματα εκπαίδευσης, ευαισθητοποίησης και κατάρτισης σε σχέση με την εθνική στρατηγική ασφάλειας δικτύων και συστημάτων πληροφοριών,
  - αναφορά στα σχέδια έρευνας και ανάπτυξης σχετικά με την εθνική στρατηγική ασφάλειας **συστημάτων δικτύου και πληροφοριών**,
  - σχέδιο εκτίμησης κινδύνου για τον προσδιορισμό κινδύνων,
  - κατάλογος των διαφόρων φορέων που εμπλέκονται στην υλοποίηση της εθνικής στρατηγικής ασφάλειας συστημάτων δικτύου και πληροφοριών.

Computer Security Incident Response Team

- Ως «Αρμόδια Ομάδα Απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών (CSIRT)», ορίζεται η Διεύθυνση Κυβερνοάμυνας του Γενικού Επιτελείου Εθνικής Άμυνας (ΓΕΕΘΑ).
  - Η ΔΙ.ΚΥΒ. καλύπτει τομείς όπως η ενέργεια, οι μεταφορές, οι τράπεζες, οι υποδομές χρηματοπιστωτικών αγορών, η υγεία, η προμήθεια και διανομή πόσιμου νερού και η ψηφιακή υποδομή, καθώς και υπηρεσίες όπως οι online αγορές, οι online μηχανές αναζήτησης και οι υπηρεσίες cloud (νεφοϋπολογιστική), και είναι υπεύθυνη για το χειρισμό κινδύνων και συμβάντων βάσει επακριβώς καθορισμένης διαδικασίας.

Επιθέσεις κατά Συστημάτων Πληροφοριών

Νόμος 4411/2016

- Με το Νόμο 4411/2016 (ΦΕΚ 142–Α΄/3-8-2016), η Ελλάδα προέβη στην Κύρωση της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο και του Προσθέτου Πρωτοκόλλου της, σχετικά με την ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσης, που διαπράττονται μέσω Συστημάτων Υπολογιστών, καθώς και στην ενσωμάτωση της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών (και την αντικατάσταση της απόφασης πλαισίου 2005/222/ΔΕΥ του Συμβουλίου).

Αλλαγές στο Ουσιαστικό Ποινικό Δίκαιο

- Πληροφοριακό Σύστημα
  - νοείται **οποιαδήποτε συσκευή ή ομάδα διασυνδεδεμένων** ή σχετικών μεταξύ τους συσκευών, από τις οποίες **μία ή περισσότερες εκτελούν αυτόματη επεξεργασία ψηφιακών δεδομένων**, καθώς **και τα ψηφιακά δεδομένα** που αποθηκεύονται, επεξεργάζονται ή διαβιβάζονται από τη συσκευή με σκοπό τη λειτουργία, τη χρήση, την προστασία και τη συντήρηση των συσκευών αυτών

Αλλαγές στο Ουσιαστικό Ποινικό Δίκαιο

- Ψηφιακά Δεδομένα
  - νοούνται **γεγονότα και πληροφορίες** που μπορούν να επεξεργαστούν από πληροφοριακό σύστημα ή πρόγραμμα που παρέχει τη δυνατότητα στο πληροφοριακό σύστημα να εκτελέσει μια λειτουργία.

Παρακώληση λειτουργίας Πληροφοριακών Συστημάτων – 292Β Π.Κ.

- Η διάταξη αυτή περιλαμβάνει, προστατεύει και τιμωρεί, αναλογικά (ειδικά και αυστηρότερα), τις επιθέσεις κατά κρατικών πληροφοριακών συστημάτων και κρίσιμων υποδομών της Χώρας που χρησιμοποιούνται ευρύτερα από την κοινωνία και το Κράτος.
  - Προβλέπονται αυστηρότερες ποινές όταν η κακόβουλη πράξη προκαλεί σημαντική ζημιά σε πληροφοριακά συστήματα με τη χρήση ειδικών για το σκοπό αυτό εργαλείων ή τελείται οργανωμένα από εγκληματική οργάνωση ή προκαλεί ιδιαίτερα μεγάλη ζημιά ή πλήττει πληροφοριακά συστήματα υποδομής που παρέχουν σημαντικές, ζωτικές υπηρεσίες για την κοινωνία και το Κράτος

292Γ Π.Κ.

- Νομοθετήθηκε για πρώτη φορά στη Χώρα μας <u>το αξιόποινο προπαρασκευαστικών πράξεων για τη διάπραξη των σχετικών με το άρθρο 292Β αδικημάτων, ανεξαρτήτως αν αυτά τελικά διαπράχθηκαν</u>.
  - Δηλαδή ποινικοποιούνται αυτοτελώς προπαρασκευαστικές ενέργειες και συμπεριφορές που στοχεύουν στην τέλεση των εγκλημάτων που περιλαμβάνονται στο άρθρο 292Β, όπως η παραγωγή, η πώληση, η εισαγωγή, η κατοχή ή με οποιονδήποτε τρόπο διευκόλυνση αυτών με τη διανομή προγραμμάτων υπολογιστών ή συσκευών.

370Γ Π.Κ. «Παράνομη πρόσβαση σε πληροφοριακό σύστημα»

- Η διάταξη προβλέπει και τιμωρεί την χωρίς δικαίωμα πρόσβαση σε Πληροφοριακό Σύστημα ή τμήμα αυτού.
- Ο όρος «πρόσβαση» περιλαμβάνει τη «χωρίς εξουσιοδότηση είσοδο» σε ολόκληρο τον ηλεκτρονικό υπολογιστή ή σε μέρος αυτού, (όπως π.χ. σε επιμέρους αρχεία και φακέλους).

370Δ Π.Κ.

- Ποινικοποιείται και τιμωρείται αυτοτελώς η παραβίαση του απορρήτου των επικοινωνιών με τη χρήση τεχνικών μέσων και πληροφοριακών συστημάτων, καθώς και η χρήση από τον ίδιο ή η διαβίβαση των πληροφοριών αυτών σε τρίτα πρόσωπα.
  - Σε περίπτωση που οι πράξεις αυτές έχουν ως αποτέλεσμα την παραβίαση στρατιωτικού ή διπλωματικού απορρήτου ή αφορούν απόρρητο που αναφέρεται στην ασφάλεια του κράτους σε καιρό πολέμου, τιμωρούνται σε βαθμό κακουργήματος.

370Ε Π.Κ.

- Ποινικοποιείται και τιμωρείται αυτοτελώς η εισαγωγή, η διανομή, η κατοχή, ο σχεδιασμός και η με οποιοδήποτε τρόπο διάθεση μηχανογραφικών εφαρμογών και προγραμμάτων λογισμικού, συσκευών ή τεχνικών μέσων, με τα οποία ευνοείται και καθίσταται δυνατή η δόλια πρόσβαση στο σύνολο ή μέρος ενός πληροφοριακού συστήματος, με σκοπό τη διάπραξη εγκλημάτων που περιλαμβάνονται στις διατάξεις των άρθρων 370Β, 370Γ παράγραφοι 2 και 3 και 370Δ του Π.Κ..

381Α Π.Κ.

- Περιλαμβάνει διατάξεις που εξειδικεύουν το αντικείμενο της φθοράς των Ψηφιακών Δεδομένων ενός Συστήματος Πληροφοριών και ποινικοποιούν ειδικά την με δόλο και χωρίς δικαίωμα «Φθορά Ηλεκτρονικών Δεδομένων».
  - Αυτοτελής προστασία των Ψηφιακών Δεδομένων, από πράξεις καταστροφής, απόκρυψης ή ανέφικτης χρήσης τους, διαγραφής ή αλλοίωσής τους.

381Β Π.Κ.

- Αφορούν την αγορά, την πώληση, την προμήθεια, την κατοχή και διακίνησης συσκευών και προγραμμάτων υπολογιστών και των συνθηματικών ή κωδικών εισόδου, προκειμένου αυτά να χρησιμοποιηθούν με δόλο για την επίτευξη παράνομης πρόσβασης σε μέρος ή στο σύνολο ενός Πληροφοριακού Συστήματος.

Απόρρητο επικοινωνιών & άρση του σε περιπτώσεις κυβερνοεγκλημάτων

Απόρρητα δεδομένα

- Στις ηλεκτρονικές επικοινωνίες, σύμφωνα με τη νομοθεσία, απόρρητα θεωρούνται:
  - Το περιεχόμενο της επικοινωνίας (περιεχόμενο τηλεφωνικών κλήσεων, ηλεκτρονικού ταχυδρομείου και γενικά οποιασδήποτε επικοινωνίας φωνής, εικόνας, δεδομένων).
  - Η ταυτότητα του καλούντος και του καλουμένου.
  - Η ταυτότητα του αποστολέα και του παραλήπτη ηλεκτρονικού ταχυδρομείου.
  - Τα δεδομένα θέσης της τερματικής συσκευής (γεωγραφικός εντοπισμός).

Υποχρεώσεις παρόχων & συνδρομητών

- Οι πάροχοι ηλεκτρονικών επικοινωνιών είναι υπεύθυνοι να λαμβάνουν όλα τα αναγκαία μέτρα για τη διασφάλιση του απορρήτου των επικοινωνιών τους στο δημόσιο τηλεπικοινωνιακό δίκτυο τους (δίκτυα κορμού και πρόσβασης).
- Οι συνδρομητές και οι χρήστες οφείλουν να μεριμνούν για το απόρρητο της επικοινωνίας στα ιδιωτικά δίκτυα τα οποία περιλαμβάνουν τις διατάξεις μεταγωγής (αν υπάρχουν) όπως και τις καλωδιώσεις στα κτίρια, τα εσωτερικά δίκτυα (LAN) και τις τερματικές συσκευές (σταθερά ενσύρματα και ασύρματα τηλέφωνα, κινητά τηλέφωνα, fax, προσωπικοί υπολογιστές).

Νομοθετικές ρυθμίσεις

- Καταρχήν το απόρρητο των επικοινωνιών προστατεύεται από το άρθρο 19 του Συντάγματος, με το οποίο προβλέφθηκε και η σύσταση της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ).

Νομοθετικές ρυθμίσεις

- Σε νομοθετικό επίπεδο σχετικές με το απόρρητο των επικοινωνιών είναι:
  - οι ρυθμίσεις του Ν. 2225/1994 **για την προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας**,
  - οι διατάξεις του Ν. 3115/2003, με τον οποίο συστάθηκε η ΑΔΑΕ, του Ν. 3471/2006, όπως τροποποιήθηκε και ισχύει, με το οποίο **ρυθμίζονται θέματα προστασίας δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών**, καθώς και
  - οι διατάξεις του Ν. 3674/2008 σχετικά με τη **διασφάλιση του απορρήτου της τηλεφωνικής επικοινωνίας**.

Άρση του απορρήτου των επικοινωνιών

- Η άρση του απορρήτου των επικοινωνιών είναι **μια κατ' εξαίρεση επιτρεπόμενη διαδικασία**, βάσει της οποίας τα στοιχεία της επικοινωνίας, τα οποία είναι καταρχήν απόρρητα, **καθίστανται γνωστά σε συγκεκριμένες Αρχές και για συγκεκριμένους λόγους**.
- Σύμφωνα με τη διάταξη του άρθρου 19 παρ. 1 του Συντάγματος, η άρση αυτή είναι δυνατόν να ισχύσει **για τη δικαστική αρχή** και όχι έναντι της διοίκησης **για λόγους εθνικής ασφάλειας** ή **για τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων**.

Άρση του απορρήτου των επικοινωνιών

- Οι προαναφερθέντες λόγοι εξειδικεύονται με τις διατάξεις του ν. 2225/1994, όπως ισχύει, ο οποίος **περιλαμβάνει και κατάλογο των εγκλημάτων** για τη διακρίβωση των οποίων μπορεί να διαταχθεί με διάταξη του αρμόδιου δικαστικού συμβουλίου η άρση του απορρήτου.
- Τις διαδικασίες, τις τεχνικές και τις οργανωτικές ρυθμίσεις για την άρση του απορρήτου των επικοινωνιών προβλέπουν, εξειδικεύοντας τη διάταξη του άρθρου 19 του Συντάγματος, οι διατάξεις του ν. 2225/1994 και του ΠΔ 47/2005, όπως ισχύουν.

Άρση του απορρήτου των επικοινωνιών

- Ειδικότερα ο ν. 2225/1994, όπως ισχύει, **προβλέπει τους λόγους** για τους οποίους η άρση του απορρήτου επιτρέπεται, **τα όργανα** που μπορούν να τη διατάξουν, **τα χρονικά όρια** εντός των οποίων μπορεί η άρση να πραγματώνεται**, καθώς και τη διαδικασία** που πρέπει να ακολουθείται σε κάθε περίπτωση.
- Το ΠΔ 47/2005, όπως ισχύει, προβλέπει τα είδη αλλά και τα επιμέρους στοιχεία της επικοινωνίας, τα οποία μπορεί να αφορά η άρση του απορρήτου.
  - Προβλέπει επίσης **τα μέσα και τις μεθόδους** πραγμάτωσης της άρσης, καθώς και **τις σχετικές υποχρεώσεις** των παρόχων υπηρεσιών και δικτύων επικοινωνίας.

Κυβερνοέγκλημα, κυβερνοεπιθέσεις και Δίκτυο 24/7

Σημείο Επαφής 24/7

- Τόσο στη Σύμβαση της Βουδαπέστης όσο και στην Οδηγία 2013/40/ΕΕ προβλέπεται το κάθε Κράτος να ορίσει ένα «**Σημείο Επαφής 24/7**», που θα ανταποκρίνεται σε αιτήματα των αντίστοιχων Σημείων Επαφής των άλλων Κρατών για θέματα που αφορούν το κυβερνοέγκλημα και τις κυβερνοεπιθέσεις. Έτσι, έχει δημιουργηθεί ένα «Δίκτυο 24/7», για την άμεση συνεργασία μεταξύ των Κρατών
  - Το κυβερνοέγκλημα δεν περιορίζεται εδαφικά, διαπράττεται ταχύτατα και μπορεί να υπάρξουν θύματα ταυτόχρονα σε πολλά σημεία του κόσμου (π.χ. κακόβουλο λογισμικό που αποστέλλεται με email σε εκατομμύρια παραλήπτες).

Σημείο Επαφής για την Ελλάδα

- Με το έκτο άρθρο του Νόμου 4411/2016, **η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος (ΔΙ.Δ.Η.Ε.) της Ελληνικής Αστυνομίας, ορίσθηκε ως σημείο επαφής που λειτουργεί σε 24ωρη βάση**, επτά ημέρες την εβδομάδα, **παρέχοντας** άμεση συνδρομή σε περιπτώσεις έρευνας και δίωξης αδικημάτων σχετικών με υπολογιστικά συστήματα και δεδομένα, υπό την εποπτεία Εισαγγελέα Εφετών.

Σημείο Επαφής

- Στο πλαίσιο αυτό, η ΔΙ.Δ.Η.Ε. ως αρμόδιο σημείο επαφής παρέχει τεχνικές συμβουλές, προβαίνει σε ενέργειες διατήρησης ψηφιακών δεδομένων σε κατεπείγουσες περιπτώσεις, τη συλλογή των αποδεικτικών στοιχείων, την παροχή νομικής ενημέρωσης και τον εντοπισμό των υπόπτων, επικοινωνώντας για το σκοπό αυτό με οποιοδήποτε σημείο επαφής άλλου Κράτους.

Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια & Πράξη για την κυβερνοασφάλεια

Κανονισμός 2019/881

- Δημοσιεύθηκε στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης ο Κανονισμός 2019/881 σχετικά με τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA) και την Πράξη για την Κυβερνοασφάλεια.
  - Ο συγκεκριμένος Κανονισμός περιλαμβάνει και διατάξεις σχετικά με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της Τεχνολογίας Πληροφοριών και Επικοινωνιών (ΤΠΕ)

Οργανισμός της Ε.Ε. για την Κυβερνοασφάλεια

- Ο ENISA, που έχει έδρα στην Ελλάδα, συμβάλλει στην ασφάλεια των δικτύων και πληροφοριών της ΕΕ από τότε που ιδρύθηκε το 2004. Με τους νέους κανόνες παρέχεται στον ENISA μόνιμη εντολή και αποσαφηνίζεται ο ρόλος του ως οργανισμού της ΕΕ για την κυβερνοασφάλεια.
  - Ανατέθηκαν, πλέον, στον ENISA νέα καθήκοντα για την παροχή στήριξης στα κράτη μέλη, τα θεσμικά όργανα της ΕΕ και άλλους φορείς σε ζητήματα κυβερνοχώρου.
  - Ο ENISA θα προωθήσει την υιοθέτηση του νέου συστήματος πιστοποίησης, ενώ θα οργανώνει τακτικές ασκήσεις ασφάλειας στον κυβερνοχώρο σε επίπεδο ΕΕ καθώς και μια μεγάλης κλίμακας γενική άσκηση ανά διετία.

Οργανισμός της Ε.Ε. για την Κυβερνοασφάλεια

- Στον Κανονισμό προβλέπεται επίσης ένα δίκτυο εθνικών υπαλλήλων-συνδέσμων με σκοπό τη διευκόλυνση της ανταλλαγής πληροφοριών μεταξύ του ENISA και των κρατών μελών.
- Η πρώτη νομοθετική πράξη της ΕΕ στον τομέα της κυβερνοασφάλειας - η οδηγία του 2016 σχετικά με την ασφάλεια δικτύων και πληροφοριών (NIS) - είχε ήδη προσδώσει στον ENISA βασικό ρόλο στη στήριξη της εφαρμογής της οδηγίας.

Κοινή πιστοποίηση της κυβερνοασφάλειας

- Στον Κανονισμό προβλέπεται επίσης η **θέσπιση μηχανισμού για τη δημιουργία ευρωπαϊκών συστημάτων πιστοποίησης** της κυβερνοασφάλειας για ειδικές διαδικασίες, προϊόντα και υπηρεσίες ΤΠΕ.
- Τα πιστοποιητικά που εκδίδονται στο πλαίσιο των συστημάτων θα ισχύουν σε όλες τις χώρες της ΕΕ, ώστε να είναι ευκολότερο για τους χρήστες να αποκτήσουν εμπιστοσύνη στην ασφάλεια των τεχνολογιών αυτών και για τις εταιρείες να διεξαγάγουν τις επιχειρηματικές τους δραστηριότητες πέραν των συνόρων.

Κοινή πιστοποίηση της κυβερνοασφάλειας

- Οι πιθανές χρήσεις για τα εν λόγω πιστοποιητικά ποικίλουν σε μεγάλο βαθμό, από τα συνδεδεμένα παιχνίδια και τις έξυπνες φορητές συσκευές έως τα συστήματα βιομηχανικού αυτοματισμού και ελέγχου και τα έξυπνα ενεργειακά δίκτυα.
- Τα σημερινά συστήματα πιστοποίησης θα βασιστούν σε ό,τι ήδη υπάρχει σε διεθνές, ευρωπαϊκό και εθνικό επίπεδο. Τα συστήματα θα εγκρίνονται από την Επιτροπή και θα εφαρμόζονται και θα επιβλέπονται από τις εθνικές αρχές πιστοποίησης της ασφάλειας στον κυβερνοχώρο.

Γενικός Κανονισμός Προσωπικών Δεδομένων

General Data Protection Regulation

Κανονισμός (ΕΕ) 2016/679

- Από τις 25 Μαΐου 2018 τέθηκε σε ισχύ σε επίπεδο Ευρωπαϊκής Ένωσης ο Κανονισμός για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών.
- Ο Κανονισμός επιτρέπει στους πολίτες της ΕΕ, να ελέγχουν καλύτερα τα προσωπικά τους δεδομένα. Εκσυγχρονίζει επίσης και ενοποιεί τους κανόνες που επιτρέπουν στις επιχειρήσεις να μειώσουν τη γραφειοκρατία και να επωφεληθούν από τη μεγαλύτερη εμπιστοσύνη των καταναλωτών.

Τι ρυθμίζει

- Ο Κανονισμός ρυθμίζει την επεξεργασία από άτομο, εταιρεία ή οργανισμό των δεδομένων προσωπικού χαρακτήρα που αφορούν άτομα στην ΕΕ. Δεν υπάγεται σε αυτόν η επεξεργασία δεδομένων προσωπικού χαρακτήρα αποθανόντων προσώπων ή νομικών προσώπων.
  - Οι κανόνες δεν εφαρμόζονται σε δεδομένα που υποβάλλονται σε επεξεργασία από ένα άτομο για αυστηρά προσωπικούς λόγους ή για δραστηριότητες που διενεργούνται κατ' οίκον, υπό την προϋπόθεση ότι δεν συνδέονται με κάποια επαγγελματική ή εμπορική δραστηριότητα.

Δεδομένα προσωπικού χαρακτήρα

- Τα δεδομένα προσωπικού χαρακτήρα είναι πληροφορίες που αφορούν ένα ταυτοποιημένο ή ταυτοποιήσιμο εν ζωή άτομο. Διαφορετικές πληροφορίες οι οποίες, εάν συγκεντρωθούν όλες μαζί, μπορούν να οδηγήσουν στην ταυτοποίηση ενός συγκεκριμένου ατόμου, αποτελούν επίσης δεδομένα προσωπικού χαρακτήρα.

Δεδομένα προσωπικού χαρακτήρα

- Ο ΓΚΠΔ προστατεύει τα δεδομένα προσωπικού χαρακτήρα **ανεξάρτητα από την τεχνολογία που χρησιμοποιείται για την επεξεργασία τους**. Είναι τεχνολογικά ουδέτερος και εφαρμόζεται τόσο στην αυτοματοποιημένη όσο και στη χειροκίνητη επεξεργασία.
  - Επίσης, δεν έχει σημασία ο τρόπος που αποθηκεύονται τα δεδομένα – σε σύστημα τεχνολογίας πληροφοριών, μέσω βιντεοεπιτήρησης ή σε έντυπη μορφή. Σε όλες τις περιπτώσεις τα δεδομένα προσωπικού χαρακτήρα υπόκεινται στις απαιτήσεις προστασίας που προβλέπει ο ΓΚΠΔ.

Παραδείγματα ΔΠΧ

- όνομα και επώνυμο
- διεύθυνση κατοικίας
- ηλεκτρονική διεύθυνση, π.χ. όνομα.επώνυμο@εταιρεία.com
- αναγνωριστικός αριθμός κάρτας
- δεδομένα τοποθεσίας (π.χ. η λειτουργία δεδομένων τοποθεσίας σε κινητό τηλέφωνο)
- διεύθυνση διαδικτυακού πρωτοκόλλου (IP)
- αναγνωριστικό cookie

Επεξεργασία ΔΠΧ

- Ο όρος «**επεξεργασία**» καλύπτει ευρύ φάσμα πράξεων που πραγματοποιούνται σε δεδομένα προσωπικού χαρακτήρα, είτε με χειροκίνητα είτε με αυτοματοποιημένα μέσα. Περιλαμβάνει τη συλλογή, καταχώριση, οργάνωση, διάρθρωση, αποθήκευση, προσαρμογή ή μεταβολή, ανάκτηση, αναζήτηση πληροφοριών, χρήση, κοινολόγηση με διαβίβαση, διάδοση ή κάθε άλλη μορφή διάθεσης, συσχέτιση ή συνδυασμό, περιορισμό, διαγραφή ή καταστροφή δεδομένων προσωπικού χαρακτήρα.

Αυτοματοποιημένη και μη επεξεργασία

- Ο Κανονισμός εφαρμόζεται στην εξ ολοκλήρου ή μερική επεξεργασία δεδομένων προσωπικού χαρακτήρα με αυτοματοποιημένα μέσα καθώς και στη μη αυτοματοποιημένη επεξεργασία, εάν αποτελεί μέρος διαρθρωμένου συστήματος αρχειοθέτησης.

Παραδείγματα επεξεργασίας

- διαχείριση προσωπικού και μισθοδοσία
- προσπέλαση/αναζήτηση πληροφοριών σε βάση δεδομένων επαφών που περιλαμβάνει δεδομένα προσωπικού χαρακτήρα
- αποστολή διαφημιστικών ηλεκτρονικών μηνυμάτων
- δημοσίευση/ανάρτηση φωτογραφίας ενός ατόμου σε ιστότοπο
- αποθήκευση διευθύνσεων IP ή διευθύνσεων MAC
- μαγνητοσκόπηση (τηλεόραση κλειστού κυκλώματος)

Υπεύθυνος Προστασίας Δεδομένων

- Ο Γενικός Κανονισμός για την Προστασία Δεδομένων εισάγει για πρώτη φορά αναλυτικές διατάξεις για τον ρόλο, τις παρεχόμενες εγγυήσεις και τα καθήκοντα του Υπευθύνου Προστασίας Δεδομένων (άρθρα 37-40), ο οποίος βρίσκεται πλέον στο επίκεντρο του νέου νομικού πλαισίου.
- Ειδικότερα, ορίζεται ότι υπό συγκεκριμένες προϋποθέσεις, **ορισμένοι υπεύθυνοι αλλά και εκτελούντες την επεξεργασία υποχρεούνται πλέον να ορίζουν υπεύθυνο προστασίας δεδομένων**.

Υπεύθυνος Προστασίας Δεδομένων

- Ο Υπεύθυνος Προστασίας Δεδομένων (DPO) διευκολύνει τη συμμόρφωση του υπευθύνου επεξεργασίας και του εκτελούντος την επεξεργασία με τις διατάξεις του ΓΚΠΔ και μεσολαβεί μεταξύ των διαφόρων ενδιαφερομένων (π.χ. εποπτικές αρχές, υποκείμενα των δεδομένων). Ο ρόλος του είναι συμβουλευτικός (όχι αποφασιστικός) και δεν φέρει προσωπική ευθύνη για τη μη συμμόρφωση με τον Κανονισμό.
  - Υπεύθυνος να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τον ΓΚΠΔ είναι ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία.

Υπεύθυνος Προστασίας Δεδομένων

- Προβλέπονται συγκεκριμένα καθήκοντα του DPO και αντίστοιχες υποχρεώσεις του εργοδότη του. Παράβαση των σχετικών με τον DPO διατάξεων επιφέρει κυρώσεις
  - Τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων πρέπει να δημοσιοποιούνται προκειμένου να διασφαλίζεται η απρόσκοπτη επικοινωνία με τα υποκείμενα των δεδομένων.
  - Προβλέπεται υποχρέωση για τον υπεύθυνο και εκτελούντα την επεξεργασία να ανακοινώνουν στην εποπτική αρχή στοιχεία που αφορούν στον ορισμό του υπευθύνου προστασίας δεδομένων.

Υπεύθυνος & εκτελών επεξεργασία

- «**υπεύθυνος επεξεργασίας**»: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα
- «**εκτελών την επεξεργασία**»: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας,

Ασφάλεια επεξεργασίας

- Οι υποχρεώσεις του υπευθύνου επεξεργασίας σχετικά με την ασφάλεια της επεξεργασίας προσδιορίζονται ρητά στο άρθρο 32 ΓΚΠΔ, ενώ η γενικότερη ευθύνη του για τον προσδιορισμό των κατάλληλων τεχνικών και οργανωτικών μέτρων προκειμένου να διασφαλίζει και να μπορεί να αποδεικνύει τη νομιμότητα μιας επεξεργασίας πηγάζει και από το άρθρο 24 ΓΚΠΔ.
- Επίσης, στον ΓΚΠΔ **για πρώτη φορά προσδιορίζεται ρητά αυτοτελής υποχρέωση και των εκτελούντων την επεξεργασία για λήψη μέτρων ασφάλειας**.

Ασφάλεια επεξεργασίας

- Παραδοσιακά, ο όρος **ασφάλεια πληροφορίας / δεδομένων** (information / data security), χρησιμοποιείται για να περιγράψει τη μεθοδολογία, καθώς και τις μεθόδους και τεχνικές που ακολουθούνται προκειμένου να επιτευχθούν οι εξής στόχοι:
  - Εμπιστευτικότητα (confidentiality): Τα δεδομένα δεν πρέπει να αποκαλύπτονται σε μη εξουσιοδοτημένα άτομα.
  - Ακεραιότητα (integrity): Τα δεδομένα πρέπει να είναι ακριβή, ακέραια και γνήσια – όχι εσφαλμένα, αλλοιωμένα ή μη ενημερωμένα.
  - Διαθεσιμότητα (availability): Τα δεδομένα πρέπει να είναι στη διάθεση των χρηστών όποτε απαιτείται η χρήση τους.
- Πλήγμα σε οποιοδήποτε από τα ανωτέρω –από τυχαία ή εσκεμμένη ενέργεια– συνιστά, γενικά, περιστατικό ασφάλειας.

Τεχνικά & οργανωτικά μέτρα ασφάλειας

- Στον ΓΚΠΔ προτείνονται τα ακόλουθα «ενδεδειγμένα» τεχνικά και οργανωτικά μέτρα ασφάλειας:
  - Ψευδωνυμοποίηση και Κρυπτογράφηση.
  - Διασφάλιση Απορρήτου, Ακεραιότητας, Διαθεσιμότητας και Αξιοπιστίας.
  - Αποκατάσταση Διαθεσιμότητας και της πρόσβασης σε περίπτωση συμβάντος.
  - Δοκιμή, εκτίμηση και διαρκής αξιολόγηση της αποτελεσματικότητας των μέτρων.
  - Χρήση εγκεκριμένου κώδικα δεοντολογίας ή μηχανισμού πιστοποίησης για την απόδειξη της συμμόρφωσης.
  - Διαδικασίες χειρισμού περιστατικών παραβίασης.

Γνωστοποίηση περιστατικών παραβίασης δεδομένων

- Σύμφωνα με το άρ. 33 του Κανονισμού, **οι υπεύθυνοι επεξεργασίας**, σε περίπτωση που συμβεί περιστατικό παραβίασης προσωπικών δεδομένων από το οποίο ενδέχεται να προκληθεί κίνδυνος στα δικαιώματα και τις ελευθερίες των προσώπων τα οποία αφορά το περιστατικό, **οφείλουν να γνωστοποιήσουν το εν λόγω περιστατικό στην εθνική Αρχή που είναι αρμόδια για την προστασία των δεδομένων προσωπικού χαρακτήρα** [(στην Ελλάδα η Αρχή αυτή είναι η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ)].

Γνωστοποίηση

- **Η γνωστοποίηση αυτή πρέπει να γίνεται αμελλητί** και, αν είναι δυνατό, **εντός 72 ωρών** από τη στιγμή που ο υπεύθυνος επεξεργασίας ενημερωθεί για το περιστατικό.
- **Η γνωστοποίηση πρέπει να περιέχει σύνολο σχετικών πληροφοριών** (φύση/έκταση του περιστατικού, κατηγορίες προσώπων που επλήγησαν, αιτία και συνέπειες αυτού, ενέργειες που έγιναν προς αντιμετώπισή του, κ.ά.).

Ανακοίνωση στα υποκείμενα

- Περαιτέρω, σύμφωνα με το άρ. 34 του Κανονισμού, **όταν η παραβίαση ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων τα οποία αφορά το περιστατικό, τότε ο υπεύθυνος επεξεργασίας οφείλει να ανακοινώνει αμελλητί την παραβίαση και στα πρόσωπα αυτά**. Αυτή η ανακοίνωση είναι ανεξάρτητη της προαναφερθείσας γνωστοποίησης στην Αρχή (η οποία γνωστοποίηση στην Αρχή υποβάλλεται ακόμα και αν ο σχετικός κίνδυνος δεν κρίνεται ως υψηλός).

Ανακοίνωση στα υποκείμενα

- Η ανακοίνωση στα φυσικά πρόσωπα θα πρέπει να γίνει με τον πλέον πρόσφορο και αποτελεσματικό τρόπο, με τη μορφή προσωποποιημένης πληροφόρησης και όχι μέσω κάποιας γενικού χαρακτήρα ανακοίνωσης, στο βαθμό που αυτό είναι εφικτό.
- Σημειώνεται ότι η Αρχή δύναται σε κάθε περίπτωση να δώσει εντολή στον υπεύθυνο επεξεργασίας να ενημερώσει τα φυσικά πρόσωπα για το περιστατικό (άρ. 58 παρ. 2 ε' Κανονισμού).

Μελέτη Περίπτωσης

- Στο Γενικό Κανονισμό Προστασίας Δεδομένων (2016/679/ΕΕ) περιγράφονται **οι υποχρεώσεις του Υπεύθυνου Επεξεργασίας**.
  - Τεκμηριώστε πως η πολιτική ασφάλειας συμβάλει στην καλύτερη συμμόρφωση του φορέα με τον Κανονισμό.
- Στο Νόμο 3979/2011 (ΦΕΚ 138 Α/16-6-2011), "Για την ηλεκτρονική διακυβέρνηση και λοιπές διατάξεις", αναζητήστε τα άρθρα που αναφέρονται στα θέματα της ασφάλειας και τεκμηριώστε ποιες είναι οι υποχρεώσεις των φορέων του δημοσίου.

Αρμόδιοι φορείς & Αρχές

Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας

- Με το Π.Δ. 178/2014 προβλέφθηκε η ίδρυση και η διάρθρωση της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος (ΔΙ.Δ.Η.Ε.) με έδρα την Αθήνα και η ίδρυση και διάρθρωση Υποδιεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος με έδρα τη Θεσσαλονίκη.
- Η αποστολή της ΔΙΔΗΕ συμπεριλαμβάνει την πρόληψη, την έρευνα και την καταστολή εγκλημάτων που διαπράττονται μέσω του διαδικτύου ή άλλων μέσων ηλεκτρονικής επικοινωνίας. Στην εσωτερική της δομή αποτελείται από πέντε τμήματα.

Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας

- Τμήμα Διοικητικής Υποστήριξης και Διαχείρισης Πληροφοριών,
- Τμήμα Καινοτόμων Δράσεων και Στρατηγικής,
- Τμήμα Ασφάλειας Ηλεκτρονικών και Τηλεφωνικών Επικοινωνιών και Προστασίας λογισμικού και Πνευματικών Δικαιωμάτων,
- Τμήμα Διαδικτυακής Προστασίας Ανηλίκων και Ψηφιακής Διερεύνησης και
- Τμήμα Ειδικών Υποθέσεων και Δίωξης Διαδικτυακών Οικονομικών Εγκλημάτων.

Εθνική Υπηρεσία Πληροφοριών – Διεύθυνση Κυβερνοχώρου

- Είναι αρμόδια:
  - για τεχνικής φύσεως θέματα ασφάλειας πληροφοριών (INFOSEC) και ειδικότερα για την ασφάλεια των εθνικών επικοινωνιών, των συστημάτων τεχνολογίας πληροφοριών καθώς και για την αξιολόγηση και πιστοποίηση των διαβαθμισμένων συσκευών και συστημάτων ασφάλειας επικοινωνιών και πληροφορικής
  - για τον έλεγχο και την αξιολόγηση ασφάλειας συστημάτων καθώς και για τη συλλογή, εξόρυξη (data mining) και εκμετάλλευση δεδομένων

Εθνική Υπηρεσία Πληροφοριών – Διεύθυνση Κυβερνοχώρου

- Είναι αρμόδια:
  - για τη συλλογή, την επεξεργασία δεδομένων και την ενημέρωση των αρμόδιων φορέων καθώς και για την, κατά περίπτωση, στατική και ενεργητική αντιμετώπιση των ηλεκτρονικών επιθέσεων κατά των κρίσιμων υποδομών της χώρας και ειδικότερα κατά των δικτύων επικοινωνιών, εγκαταστάσεων αποθήκευσης πληροφοριών και συστημάτων πληροφορικής.

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

- Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα έχει ως αποστολή της την εποπτεία της εφαρμογής του Γενικού Κανονισμού Προστασίας Δεδομένων, του νόμου 4624/2019, του νόμου 3471/2006 και άλλων ρυθμίσεων που αφορούν την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, καθώς και την ενάσκηση των αρμοδιοτήτων που της ανατίθενται κάθε φορά.

Αρμοδιότητες

- Παρακολουθεί και επιβάλλει την εφαρμογή του ΓΚΠΔ.
- Προωθεί την ευαισθητοποίηση του κοινού στα ζητήματα προστασίας προσωπικών δεδομένων και των υπευθύνων και εκτελούντων επεξεργασίας σχετικά με τις υποχρεώσεις τους δυνάμει του ΓΚΠΔ. Ειδική προσοχή αποδίδεται σε δραστηριότητες που απευθύνονται ειδικά σε παιδιά.
- Συμβουλεύει το εθνικό κοινοβούλιο, την κυβέρνηση και άλλα όργανα και οργανισμούς για νομοθετικά και διοικητικά μέτρα που σχετίζονται με την προστασία των προσωπικών δεδομένων.

Αρμοδιότητες

- Παρέχει κατόπιν αιτήματος πληροφορίες στα υποκείμενα των δεδομένων σχετικά με την άσκηση των δικαιωμάτων τους.
- Χειρίζεται τις υποβληθείσες για παράβαση διατάξεων του ΓΚΠΔ καταγγελίες.
- Διενεργεί έρευνες σχετικά με την εφαρμογή του ΓΚΠΔ.
- Συνεργάζεται με άλλες εποπτικές αρχές μέσω ανταλλαγής πληροφοριών και να παρέχει αμοιβαία συνδρομή σε αυτές με σκοπό τη διασφάλιση της συνεκτικότητας εφαρμογής του ΓΚΠΔ.

Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών

- Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ) είναι μια από τις συνταγματικά καθιερωμένες Ανεξάρτητες Αρχές με διοικητική αυτοτέλεια, η οποία συστάθηκε ως ειδικός εποπτεύων φορέας για να προστατεύει το απόρρητο της επικοινωνίας.
- Η Αρχή συστάθηκε με το Ν.3115/2003 κατ' εφαρμογή της συνταγματικής επιταγής του άρθρου 19 παρ. 2 του Συντάγματος. Με τον παραπάνω νόμο ρυθμίζονται τα θέματα της συγκρότησης, των αρμοδιοτήτων και της λειτουργίας της ΑΔΑΕ, ενώ με το ΠΔ 40/2005 ρυθμίζεται η εσωτερική της διάρθρωση.

Αρμοδιότητες

- Διενεργεί, αυτεπαγγέλτως ή κατόπιν καταγγελίας τακτικούς και έκτακτους ελέγχους σε εγκαταστάσεις, τεχνικό εξοπλισμό, αρχεία, τράπεζες δεδομένων και έγγραφα της ΕΥΠ, άλλων δημοσίων υπηρεσιών, οργανισμών, επιχειρήσεων του ευρύτερου δημοσίου τομέα, καθώς και ιδιωτικών επιχειρήσεων που ασχολούνται με ταχυδρομικές, τηλεπικοινωνιακές ή άλλες υπηρεσίες σχετικές με την ανταπόκριση και την επικοινωνία.

Αρμοδιότητες

- Λαμβάνει πληροφορίες σχετικές με την αποστολή της από τις προαναφερθείσες υπηρεσίες, οργανισμούς και επιχειρήσεις, καθώς και από τους εποπτεύοντες Υπουργούς.
- Καλεί σε ακρόαση τις παραπάνω υπηρεσίες, οργανισμούς, νομικά πρόσωπα και επιχειρήσεις και κάθε άλλο πρόσωπο, που κρίνει ότι μπορεί να συμβάλει στην εκπλήρωση της αποστολής της.

Αρμοδιότητες

- Προβαίνει σε κατάσχεση των μέσων παραβίασης του απορρήτου που υποπίπτουν στην αντίληψή της κατά την ενάσκηση του έργου της και ορίζεται μεσεγγυούχος αυτών μέχρι να αποφανθούν τα αρμόδια δικαστήρια. Προβαίνει επίσης στην καταστροφή πληροφοριών ή στοιχείων ή δεδομένων, τα οποία αποκτήθηκαν με παράνομη παραβίαση του απορρήτου των επικοινωνιών.
- Εξετάζει καταγγελίες σχετικά με την προστασία των δικαιωμάτων των αιτούντων, όταν θίγονται από τον τρόπο και τη διαδικασία άρσης του απορρήτου.

Αρμοδιότητες

- Συνεργάζεται με άλλες αρχές της χώρας, με αντίστοιχες αρχές άλλων κρατών, καθώς και με ευρωπαϊκούς και διεθνείς οργανισμούς, για θέματα της αρμοδιότητάς της.
- Γνωμοδοτεί και απευθύνει συστάσεις και υποδείξεις για τη λήψη μέτρων διασφάλισης του απορρήτου των επικοινωνιών, καθώς και τη διαδικασία άρσης του.
- Εκδίδει κανονιστικές πράξεις που δημοσιεύονται στην Εφημερίδα της Κυβερνήσεως με τις οποίες ρυθμίζεται κάθε διαδικασία και λεπτομέρεια σε σχέση με τις ανωτέρω αρμοδιότητές της καθώς και με την εν γένει διασφάλιση του απορρήτου των επικοινωνιών.

Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων

- Η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ) είναι Ανεξάρτητη Διοικητική Αρχή. Αποτελεί τον Εθνικό Ρυθμιστή που ρυθμίζει, εποπτεύει και ελέγχει:
- (α) την αγορά ηλεκτρονικών επικοινωνιών, στην οποία δραστηριοποιούνται οι εταιρίες σταθερής και κινητής τηλεφωνίας, ασύρματων επικοινωνιών και διαδικτύου και
- (β) την ταχυδρομική αγορά, στην οποία δραστηριοποιούνται οι εταιρίες παροχής ταχυδρομικών υπηρεσιών και υπηρεσιών ταχυμεταφοράς.

Αρμοδιότητες

- Ρυθμίζει τα θέματα που αφορούν τον α) καθορισμό σχετικών αγορών, προϊόντων ή υπηρεσιών ηλεκτρονικών επικοινωνιών στην Ελληνική Επικράτεια, β) τον ορισμό και τις υποχρεώσεις Παρόχων με Σημαντική Ισχύ στις ανωτέρω σχετικές αγορές σύμφωνα με την εθνική και κοινοτική νομοθεσία.
- Εποπτεύει και ελέγχει τους παρόχους δικτύων ή/και υπηρεσιών ηλεκτρονικών επικοινωνιών, επιβάλλει τις σχετικές κυρώσεις, τηρεί και διαχειρίζεται το Μητρώο Παρόχων Δικτύων και Υπηρεσιών Ηλεκτρονικών Επικοινωνιών.

Αρμοδιότητες

- Εκδίδει Κώδικες Δεοντολογίας για την παροχή δικτύων και υπηρεσιών των ηλεκτρονικών επικοινωνιών.
- Μεριμνά για την τήρηση της νομοθεσίας περί ηλεκτρονικών επικοινωνιών και επιβάλει σχετικές κυρώσεις.
- Ρυθμίζει τα θέματα ονομάτων χώρου στο Διαδίκτυο με κατάληξη ".gr" και είναι αρμόδια για θέματα ονομάτων χώρου με κατάληξη ".eu".
- Ρυθμίζει θέματα προστασίας του καταναλωτή στον τομέα των ηλεκτρονικών επικοινωνιών και στον τομέα παροχής ταχυδρομικών υπηρεσιών.

Ονόματα χώρου “.gr”

- Ένα όνομα χώρου (domain name) είναι μία λέξη που επιλέγουμε προκειμένου να μπορούμε με εύκολο τρόπο να συνδεθούμε με έναν υπολογιστή στο διαδίκτυο. Η λέξη αυτή πάντα προσδιορίζεται περαιτέρω από μία κατάληξη που χαρακτηρίζει κατά κάποιο τρόπο την "περιοχή" του δικτύου στην οποία ανήκει. Έτσι, για παράδειγμα για τον χώρο ονομάτων με κατάληξη .gr, ένα domain name θα έχει τη μορφή onoma.gr και επισκεπτόμαστε τις ιστοσελίδες που του αντιστοιχούν γράφοντας σε κάποιο πρόγραμμα πλοήγησης (browser) μια διεύθυνση της μορφής http://www.onoma.gr.

Ονόματα χώρου “.gr”

- Η βάση δεδομένων που περιλαμβάνει το σύνολο των καταχωρηθέντων ονομάτων χώρου με κατάληξη .gr και .ελ και των ονομάτων χώρου με κατάληξη .gr ή .ελ που τυχόν αποτελούν αντικείμενο δηλώσεων καταχώρησης, με τα στοιχεία τα οποία αντιστοιχούν σε κάθε ένα από αυτά, όπως κατά καιρούς τα στοιχεία αυτά καθορίζονται από την ΕΕΤΤ με Απόφασή της.
- Το Μητρώο ανήκει στην ΕΕΤΤ, η οποία είναι υπεύθυνη για τη σωστή και σύμφωνη με την κείμενη νομοθεσία χρήση του.

Ονόματα χώρου “.gr”

- Για να εκχωρηθεί ένα όνομα χώρου με κατάληξη .gr ή .ελ θα πρέπει κάποιος να καταθέσει σχετική δήλωση σε κάποιον καταχωρητή. Στην ιστοσελίδα της ΕΕΤΤ, έχει αναρτηθεί Κανονισμός Διαχείρισης και Εκχώρησης Ονομάτων Χώρου με κατάληξη .gr ή .ελ, ο οποίος έχει συνταχθεί από την ΕΕΤΤ και καθορίζει τις προϋποθέσεις και τη διαδικασία για κάθε νέα εκχώρηση.

Ονόματα χώρου ".gr"

- Πέραν της εκχώρησης ονομάτων χώρου με κατάληξη .gr και .ελ (ονόματα 2ου επιπέδου), εκχώρηση ονομάτων χώρου μπορεί να γίνει και στα ακόλουθα subdomains του .gr (ονόματα 3ου επιπέδου):
  - com.gr για όσους ασκούν εμπορική δραστηριότητα
  - edu.gr για εκπαιδευτικούς οργανισμούς
  - net.gr για παρόχους υπηρεσιών διαδικτύου (Internet Service Providers - ISPs) και παρόχους
  - org.gr για μη κερδοσκοπικούς οργανισμούς
  - gov.gr αποκλειστικά για κυβερνητικούς οργανισμούς

Ευχαριστώ για την προσοχή σας

Ερωτήσεις