



Προστασία προσωπικών δεδομένων στα συστήματα Τεχνητής Νοημοσύνης

Οι προκλήσεις κατά τον έλεγχο συμμόρφωσης
από τις ΑΠΔ – Τελευταίες εξελίξεις

Γεωργία Παναγοπούλου

Μηχανικός Η/Υ και Πληροφορικής, DESS, ITIL

ΕΕΠ Ελέγκτρια Πληροφορικής

Προϊσταμένη Τμήματος Ελέγχων και Ασφάλειας

Μοντέλο Τεχνητής Νοημοσύνης

Εκπαίδευση Μοντέλου

Ένα μοντέλο ΤΝ προκύπτει από μηχανισμούς εκπαίδευσης που εφαρμόζονται σε ένα σύνολο δεδομένων εκπαίδευσης, στο πλαίσιο της Τεχνητής Νοημοσύνης, συμπεριλαμβανομένων της Μηχανικής Μάθησης, της Βαθιάς Μάθησης ή άλλων συναφών τεχνολογιών.

Κύκλος ζωής συστήματος ΤΝ

- Σχεδιασμός και ανάλυση
- Ανάπτυξη
- Λειτουργία
- Συντήρηση
- Απόσυρση

Τα στάδια επιδέχονται επανάληψη, ανάλογα με το επιλεγμένο μοντέλο ανάπτυξης.



Γενικός Κανονισμός Προστασίας Δεδομένων και Τεχνητή Νοημοσύνη

Πτυχές προστασίας δεδομένων σχετίζονται τόσο με την εκπαίδευση όσο και με την ανάπτυξη και τη χρήση μοντέλων τεχνητής νοημοσύνης.

Προσωπικά δεδομένα μπορεί να αποτελούν μέρος του σχετικού συνόλου δεδομένων στα οποία το μοντέλο εκπαιδεύεται, βελτιστοποιείται ή ενημερώνεται.

Ο ΓΚΠΔ είναι τεχνολογικά ουδέτερος, η επεξεργασία που σχετίζεται με την τεχνητή νοημοσύνη.

Ιδιαίτερη/πρωτότυπη/καινοτόμα/σύνθετη Καλύπτεται από τον ΓΚΠΔ κάθε φορά που υποβάλλονται σε επεξεργασία προσωπικά δεδομένα.



Έλεγχος συμμόρφωσης ΤΝ με ΓΚΠΔ

Κριτήρια εφαρμογής

Για να είναι εφαρμόσιμοι οι έλεγχοι για την προστασία προσωπικών δεδομένων, αρκεί το σύστημα ΤΝ να εκτελεί επεξεργασία προσωπικών δεδομένων σε κάποιο στάδιο του κύκλου ζωής του ή η σχετική επεξεργασία προσωπικών δεδομένων να οδηγεί σε δημιουργία προφίλ ή να αυτοματοποιεί αποφάσεις σχετικά με φυσικά πρόσωπα που ενδέχεται να συνεπάγονται νομικές συνέπειες ή να επηρεάσουν σημαντικά τα πρόσωπα αυτά.



Μετασχηματισμός Δεδομένων

Όταν τα δεδομένα εκπαίδευσης περιέχουν προσωπικά δεδομένα, υφίστανται μετασχηματισμό κατά τη διαδικασία μηχανικής μάθησης, μετατρέποντάς τα σε αφηρημένες μαθηματικές αναπαραστάσεις. Αυτή η διαδικασία αφαίρεσης έχει ως αποτέλεσμα την απώλεια συγκεκριμένων χαρακτηριστικών και αναφορών σε συγκεκριμένα άτομα.

Το εάν και πότε μπορεί να θεωρηθεί ότι δεν πραγματοποιείται επεξεργασία ΠΔ σε ένα μοντέλο γίνεται σύμφωνα με τον ορισμό του ανώνυμου δεδομένου.

Τεχνολογίες Βελτίωσης της Ιδιωτικότητας (PETs) και TN

- Η εφαρμογή τεχνολογιών βελτίωσης της ιδιωτικότητας (PETs) σε προσωπικά δεδομένα στα συστήματα TN ενέχει ιδιαίτερες προκλήσεις.
- Καμία τεχνική PET δεν πρέπει να θεωρείται ως πανάκεια όσον αφορά τον μετριασμό των σχετικών κινδύνων που απορρέουν από τη διαδικασία του μοντέλου εκπαίδευσης
- Η εφαρμογή PETs μπορεί επίσης να επηρεάσει την συνολική ακρίβεια του μοντέλου.
- Μια προσέγγιση είναι τα συνθετικά δεδομένα: συνθετικά δεδομένα μπορούν να δημιουργηθούν χρησιμοποιώντας αλγόριθμους μηχανικής μάθησης που μαθαίνουν μοτίβα από πραγματικά δεδομένα και στη συνέχεια χρησιμοποιούν αυτά τα μοτίβα για να δημιουργήσουν νέα δεδομένα που είναι στατιστικά παρόμοια, αλλά δεν περιέχουν αναγνωρίσιμες προσωπικές πληροφορίες



Ειδικές ευπάθειες μοντέλων TN

- Οι επιθέσεις αντιστροφής μοντέλου συμβαίνουν όταν ένας εισβολέας αναστρέψει το μοντέλο για να εξάγει πληροφορίες από αυτό.
- Οι επιθέσεις συμπερασμάτων μέλους επιτρέπουν σε κακόβουλους να συμπεράνουν εάν ένα συγκεκριμένο άτομο περιέχεται στα δεδομένα εκπαίδευσης ενός μοντέλου TN.

Επιθέσεις «μαύρου» και «λευκού» κουτιού

- Λευκού κουτιού: ο εισβολέας έχει πλήρη πρόσβαση στο ίδιο το μοντέλο και μπορεί να επιθεωρήσει τον υποκείμενο κώδικα και τις ιδιότητές του (αν και όχι τα δεδομένα εκπαίδευσης).
- Μαύρου κουτιού: ο εισβολέας έχει τη δυνατότητα να ρωτήσει το μοντέλο και να παρατηρήσει τις σχέσεις μεταξύ εισόδων και εξόδων



Έλεγχος συμμόρφωσης από ΑΠΔ

Κριτήρια

Νομιμότητα, αντικειμενικότητα και διαφάνεια, περιορισμός σκοπού, ελαχιστοποίηση δεδομένων, ακρίβεια, περιορισμός αποθήκευσης, ακεραιότητα και εμπιστευτικότητα, λογοδοσία.

Το εύρος και η εμβάθυνση του ελέγχου, ο βαθμός εξαντλητικότητας κατά την ανάλυση των στοιχείων ελέγχου προσαρμόζεται στα χαρακτηριστικά του συστήματος ΤΝ



Αντικείμενα Ελέγχου

- Η ύπαρξη ή η απουσία προσωπικών δεδομένων.
- Η ανάλυση της αποτελεσματικότητας των εφαρμοζόμενων PETs
- Οι νομικές βάσεις επεξεργασίας και ο προσδιορισμός των ρόλων (υπεύθυνος επεξεργασίας - εκτελών την επεξεργασία)
- Η δημιουργία προφίλ ή αυτοματοποιημένων αποφάσεων σχετικά με τα υποκείμενα των δεδομένων.
- Η εκπλήρωση των περιορισμών στις αυτοματοποιημένες αποφάσεις, η εκτίμηση, κατά περίπτωση, της ποιότητας της ανθρώπινης παρέμβασης και των εποπτικών μηχανισμών που υιοθετήθηκαν.
- Η επαλήθευση και η εκτέλεση των δοκιμών σχετικά με την καταλληλότητα των αλγορίθμων που χρησιμοποιούνται για τη δημιουργία προφίλ και την εξαγωγή συμπερασμάτων



Αντικείμενα Ελέγχου

- Η ενημέρωση και η αποτελεσματικότητα των μηχανισμών διαφάνειας που έχουν εφαρμοστεί και η επάρκεια των μηχανισμών για άσκηση δικαιωμάτων
- Η εφαρμογή της αρχής της λογοδοσίας και διαχείριση κινδύνου για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων (ΕΑΠΔ)
- Η εκ των προτέρων ανάλυση της αναγκαιότητας επεξεργασίας προσωπικών δεδομένων, από πλευράς ποσότητας και έκτασης, σε διάφορες φάσεις σύμφωνα με κριτήρια ελαχιστοποίησης.
- Η ανάλυση της ακρίβειας, της αξιοπιστίας, της ποιότητας και μεροληψίας των δεδομένων που χρησιμοποιήθηκαν ή συγκεντρώθηκαν για την ανάπτυξη ή τη λειτουργία του συστήματος ΤΝ
- Η καταλληλότητα των μέτρων ασφαλείας για την αποφυγή κινδύνων προστασίας της ιδιωτικής ζωής



Ενδεικτικά σημεία ελέγχου - σκοπός

- ✓ Είναι τεκμηριωμένος ο επιδιωκόμενος σκοπός του συστήματος που βασίζεται σε ΤΝ;
- ✓ Υπάρχει σχέση μεταξύ της χρήσης του συστήματος τεχνητής νοημοσύνης με τον απώτερο σκοπό της επεξεργασίας;
- ✓ Εντοπίζονται οι διαφορετικές δυναμικές, δραστηριότητες ή/και διαδικασίες εντός του οργανισμού στον οποίο ενσωματώνεται το στάδιο του κύκλου ζωής του ελεγχόμενου συστήματος ΤΝ, οριοθετώντας όσο το δυνατόν περισσότερο το πλαίσιο χρήσης;
- ✓ Οι πιθανοί χρήστες του συστήματος που βασίζεται σε τεχνητή νοημοσύνη κατηγοριοποιούνται;
- ✓ Υπάρχουν άλλες πιθανές χρήσεις και δευτερεύοντες χρήστες για το σύστημα ΤΝ; Έχουν τεκμηριωθεί επαρκώς;



Ενδεικτικά σημεία ελέγχου - διαφάνεια

- ✓ Είναι τεκμηριωμένες οι πηγές των δεδομένων;
- ✓ Τα χαρακτηριστικά των δεδομένων που χρησιμοποιούνται για την εκπαίδευση του συστήματος TN προσδιορίζονται, τεκμηριώνονται και αιτιολογούνται δεόντως;
- ✓ Είναι τεκμηριωμένη η επεξήγηση του κώδικα του αλγορίθμου προκειμένου να διευκολυνθεί η αναγνωσιμότητα, η λογική κατανόηση και η εσωτερική του συνέπεια;
- ✓ Οι αποφάσεις που λαμβάνονται από ένα σύστημα TN μπορούν να επεξηγηθούν, βάσει της γενικότερης τεκμηρίωσης που παρέχεται; (επεξηγησιμότητα)
- ✓ Σε περίπτωση λανθασμένης συμπεριφοράς του συστήματος που βασίζεται σε TN που θα μπορούσε να προκαλέσει βλάβη στα υποκείμενα των δεδομένων, έχουν δημιουργηθεί μηχανισμοί για την ελαχιστοποίηση αυτής της ζημίας; παρέχονται κανάλια επικοινωνίας για τη διευκόλυνση της επικοινωνίας μεταξύ όλων των ενδιαφερομένων που εμπλέκονται στη διαδικασία;



Ενδεικτικά σημεία ελέγχου – αναλογικότητα, αναγκαιότητα, ακρίβεια

- ✓ Έχει αξιολογηθεί η χρήση του συστήματος ΤΝ έναντι άλλων πιθανών επιλογών από μια προσέγγιση που εστιάζει στα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων;
- ✓ Εντοπίζονται οι κατηγορίες των υποκειμένων των δεδομένων που επηρεάζονται από την ανάπτυξη του συστήματος ΤΝ και τη χρήση του στο πλαίσιο της προβλεπόμενης επεξεργασίας;
- ✓ Έχει αναλυθεί και αντιμετωπιστεί ο κίνδυνος για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων που εισάγεται με τη χρήση ενός συστήματος που βασίζεται σε τεχνητή νοημοσύνη στην επεξεργασία δεδομένων;
- ✓ Εντοπίζονται οι βραχυπρόθεσμες και μακροπρόθεσμες συνέπειες που μπορεί να έχει η εφαρμογή του συστήματος τεχνητής νοημοσύνης στις κατηγορίες των υποκειμένων των δεδομένων;
- ✓ Υπάρχει τεκμηριωμένη διαδικασία για τη διαχείριση και τη διασφάλιση της σωστής διακυβέρνησης δεδομένων;
- ✓ Υπάρχουν εποπτικοί μηχανισμοί για τις διαδικασίες συλλογής, επεξεργασίας, αποθήκευσης και χρήσης δεδομένων;



Ενδεικτικά σημεία ελέγχου – νομική βάση, ελαχιστοποίηση

- ✓ Εντοπίζονται νομικές βάσεις για την επεξεργασία προσωπικών δεδομένων στα διάφορα στάδια του κύκλου ζωής του συστήματος που βασίζεται σε τεχνητή νοημοσύνη;
- ✓ Είναι επαρκώς προσδιορισμένα και τεκμηριωμένα τα κριτήρια για τη διενέργεια προηγούμενης εκκαθάρισης των αρχικών συνόλων δεδομένων και τυχόν άλλων εργασιών που απαιτούνται κατά τη διάρκεια των διαφορετικών επαναλήψεων της εκπαιδευτικής διαδικασίας που βασίζεται σε τεχνητή νοημοσύνη;
- ✓ Τα δεδομένα έχουν προηγουμένως ταξινομηθεί σε κατηγορίες, σε μη προσωπικά και προσωπικά δεδομένα και, για τα τελευταία, προσδιορίζοντας ποια πεδία αποτελούν αναγνωριστικά, οιονεί αναγνωριστικά και ειδικές κατηγορίες δεδομένων;
- ✓ Έχουν καθοριστεί και εφαρμοστεί κριτήρια ελαχιστοποίησης δεδομένων στα διαφορετικά στάδια του συστήματος ΤΝ, χρησιμοποιώντας στρατηγικές όπως η απόκρυψη δεδομένων, διαχωρισμός, αφαίρεση, ανωνυμοποίηση και ψευδωνυμοποίηση που ενδέχεται να ισχύουν για τους σκοπούς βελτίωσης της ιδιωτικότητας των δεδομένων;



Ενδεικτικά σημεία ελέγχου – μεροληψία

- ✓ Έχουν καθοριστεί κατάλληλες διαδικασίες για τον εντοπισμό και την άρση, ή τουλάχιστον τον περιορισμό, τυχόν μεροληψίας στα δεδομένα που χρησιμοποιούνται για την εκπαίδευση του σχετικού μοντέλου;
- ✓ Έχει επαληθευτεί ότι στην εκπαίδευση τα δεδομένα δεν είχαν προηγούμενες προκαταλήψεις;
- ✓ Υπάρχουν μηχανισμοί ανθρώπινης εποπτείας που εφαρμόζονται προκειμένου να ελέγχεται και να διασφαλίζεται ότι τα αποτελέσματα είναι απαλλαγμένα από μεροληψία;
- ✓ Εφαρμόζονται μηχανισμοί που επιτρέπουν στα υποκείμενα των δεδομένων να ζητούν ανθρώπινη παρέμβαση, να παρέχουν ανατροφοδότηση ή να αντικρούουν τα αποτελέσματα που λαμβάνονται μέσω αυτοματοποιημένων αλγορίθμων λήψης αποφάσεων;



Ενδεικτικά σημεία ελέγχου – ασφάλεια

- ✓ Έχει διενεργηθεί ανάλυση επικινδυνότητας σχετικά με τους κινδύνους για τα δικαιώματα και τις ελευθερίες των προσώπων; Έχουν χρησιμοποιηθεί τα αποτελέσματα για τον προσδιορισμό των απαιτήσεων ασφάλειας και απορρήτου του συστήματος που βασίζεται σε ΤΝ στο πλαίσιο της επεξεργασίας;
- ✓ Έχουν ληφθεί υπόψη τα πρότυπα και οι βέλτιστες πρακτικές για την ασφαλή διαμόρφωση και ανάπτυξη του σχετικού συστήματος ΤΝ;
- ✓ Εφαρμόζονται μέτρα που για την εγγύηση της εμπιστευτικότητας μέσω της ανωνυμοποίησης ή ψευδωνυμοποίησης δεδομένων και της ακεραιότητας για την προστασία από τυχαία ή εκούσια χειραγώγηση;
- ✓ Έχουν εφαρμοστεί διαδικασίες για την ορθή παρακολούθηση της λειτουργίας του μοντέλου και τον έγκαιρο εντοπισμό τυχόν πιθανής διαρροής δεδομένων, μη εξουσιοδοτημένης πρόσβασης ή άλλες παραβιάσεις ασφαλείας;
- ✓ Έχει εξεταστεί εάν το μοντέλο είναι ευάλωτο σε επιθέσεις αντιστροφής μοντέλου ή επιθέσεις συμπερασμάτων μέλους και έχουν εφαρμοστεί τεχνικές αποφυγής;
- ✓ Έχουν εφαρμοστεί μέτρα για την αποφυγή επιθέσεων μαύρου κουτιού;



ΕΣΠΔ και Τεχνητή Νοημοσύνη

Η πρόσφατη Γνωμοδότηση 28/2024 του ΕΣΠΔ

Η Ιρλανδική Αρχή υπέβαλε αίτημα στο ΕΣΠΔ για γνωμοδότηση σύμφωνα με το άρθρο 64 παράγραφος 2 του ΓΚΠΔ.

❖ **Ανωνυμία:** Για να είναι ένα μοντέλο ανώνυμο, θα πρέπει να είναι πολύ απίθανο:

1. να ταυτοποιεί άμεσα ή έμμεσα πρόσωπα των οποίων τα δεδομένα χρησιμοποιήθηκαν για τη δημιουργία του μοντέλου και
2. να εξάγει τέτοια δεδομένα προσωπικού χαρακτήρα από το μοντέλο μέσω ερωτημάτων. Η γνωμοδότηση παρέχει μη περιοριστικό και μη εξαντλητικό κατάλογο μεθόδων για την απόδειξη της ανωνυμίας.

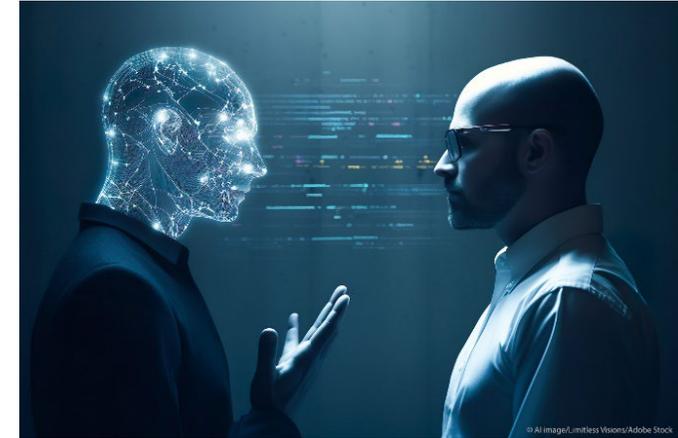
❖ **Έννομο συμφέρον:** Η εξέταση τριών σταδίων (εντοπισμός έννομου συμφέροντος, διασφάλιση της αναγκαιότητας της επεξεργασίας και διεξαγωγή άσκησης εξισορρόπησης για να επιβεβαιωθεί ότι το έννομο συμφέρον του υπεύθυνου επεξεργασίας υπερισχύει των συμφερόντων των υποκειμένων των δεδομένων ή των θεμελιωδών δικαιωμάτων και ελευθεριών) συμβάλλει στην αξιολόγηση της χρήσης του έννομου συμφέροντος ως νομικής βάσης. Η γνωμοδότηση περιλαμβάνει επίσης μια σειρά κριτηρίων που βοηθούν τις ΑΠΔ να αξιολογήσουν εάν τα άτομα μπορούν εύλογα να αναμένουν ορισμένες χρήσεις των προσωπικών τους δεδομένων.

❖ Τέλος, όταν έχει ήδη αναπτυχθεί ένα μοντέλο ΤΝ με **δεδομένα προσωπικού χαρακτήρα που υποβλήθηκαν σε παράνομη επεξεργασία**, αυτό θα μπορούσε να έχει αντίκτυπο στη νομιμότητα της χρήσης του, εκτός εάν το μοντέλο έχει δεόντως ανωνυμοποιηθεί.



Προσωπικά Δεδομένα και Κανονισμός ΤΝ

- ❖ Τα συστήματα τεχνητής νοημοσύνης, στο συντριπτικά μεγαλύτερο ποσοστό τους, περιλαμβάνουν επεξεργασία δεδομένων προσωπικού χαρακτήρα και εξ' αυτού υφίσταται ισχυρή συνάφεια μεταξύ των ρυθμίσεων για τα συστήματα τεχνητής νοημοσύνης και των ρυθμίσεων για την προστασία δεδομένων.
- ❖ Για τη σχέση μεταξύ Κανονισμού ΤΝ και προστασίας προσωπικών δεδομένων - εκκρεμούν σχετικές Κατευθυντήριες Γραμμές από το ΕΣΠΔ
- ❖ Δήλωση ΕΣΠΔ 3/2024 σχετικά με τον ρόλο των αρχών προστασίας δεδομένων στο πλαίσιο του κανονισμού για την τεχνητή νοημοσύνη: Οι Αρχές Προστασίας Δεδομένων να ορίζονται ως αρχές εποπτείας της αγοράς για συστήματα τεχνητής νοημοσύνης υψηλού κινδύνου



Ελληνική Αρχή: Προσωπικά Δεδομένα και ΤΝ

Η Αρχή πρότεινε και το ΕΣΠΔ ανέλαβε την χρηματοδότηση για δύο έργα

1. Ανάπτυξη προγράμματος σπουδών για την εκπαίδευση επαγγελματιών κυβερνοασφάλειας, και εμπλεκόμενων στην παραγωγή και ανάπτυξη συστημάτων τεχνητής νοημοσύνης, στην Ελλάδα, σχετικά με την τεχνητή νοημοσύνη και την προστασία προσωπικών δεδομένων
2. Ανάπτυξη προγράμματος σπουδών για την εκπαίδευση υπευθύνων προστασίας δεδομένων και επαγγελματιών σχετικών με προστασία δεδομένων, στην Ελλάδα, σχετικά με την τεχνητή νοημοσύνη και την προστασία προσωπικών δεδομένων.
Το υλικό αναπτύχθηκε σε συνεργασία με ειδικούς εξωτερικούς εμπειρογνώμονες του ΕΣΠΔ, και η Αρχή σχεδιάζει την αξιοποίηση των παραδοτέων μέσα στο 2025.

Η Αρχή έχει ξεκινήσει την υλοποίηση Έργου χρηματοδοτούμενου από την ΕΕ που περιλαμβάνει καθοδήγηση και εργαλεία για τη διευκόλυνση των ΜΜΕ στην αξιολόγηση των κινδύνων προστασίας δεδομένων και ιδιωτικού απορρήτου, συμπεριλαμβανομένων ειδικά των κινδύνων από τη χρήση συστημάτων ΤΝ, καθώς και ευαισθητοποίηση των υποκειμένων των δεδομένων σχετικά με τους κινδύνους προστασίας δεδομένων, συμπεριλαμβανομένων ειδικά των κινδύνων από τη χρήση συστημάτων ΤΝ.



Διακυβέρνηση - Κανονισμός ΤΝ – Ο ρόλος Αρχής

- ❖ Η εφαρμογή του Κανονισμού ΤΝ απαιτεί έναν ικανό και έμπειρο ρυθμιστή, λόγω της πολυπλοκότητάς της. Η ΑΠΔ λόγω της εμπειρίας εφαρμογής του επίσης πολύπλοκου ΓΚΠΔ **διαθέτει σχετική εμπειρία και γνώση.**
- ❖ Η ΑΠΔ, λόγω της **πλήρους ανεξαρτησίας** της, μπορεί να παρέχει αποτελεσματική ανεξάρτητη εποπτεία των συστημάτων ΤΝ.
- ❖ Ο ορισμός της ΑΠΔ ως αρμόδιας αρχής εποπτείας της αγοράς για την ΤΝ θα ωφελούσε τα ενδιαφερόμενα μέρη να έχουν ένα **ενιαίο σημείο επαφής** για όλες τις επεξεργασίες προσωπικών δεδομένων που εμπίπτουν στο πεδίο εφαρμογής του Κανονισμού
- ❖ Θα πρέπει να υπάρχει **συνεργασία** με τις εποπτικές αρχές που διαθέτουν εμπειρογνωμοσύνη και αρμοδιότητες στον συγκεκριμένο τομέα ανάπτυξης του συστήματος τεχνητής νοημοσύνης.



Διακυβέρνηση - Κανονισμός ΤΝ – Ο ρόλος Αρχής

Σχετικά με την ανάπτυξη και χρήση της ΤΝ οι Έλληνες πολίτες χρειάζονται διασφαλίσεις για ζητήματα όπως

- εξηγήσεις για το πώς λειτουργούν οι εφαρμογές Τεχνητής Νοημοσύνης (41.7%),
- διασφάλιση προστασίας των προσωπικών δεδομένων (40.9%),
- αυστηρή νομοθεσία που περιορίζει τη χρήση της Τεχνητής Νοημοσύνης (39.8%),
- ανεξάρτητος φορέας που θα επιβλέπει την ασφάλεια της Τεχνητής Νοημοσύνης (33.7%),
- δυνατότητα προσφυγής σε άνθρωπο για την επανεξέταση των αποφάσεων Τεχνητής Νοημοσύνης (31.3%).

Έρευνα Eteron <https://eteron.org/research/ereyna-eteron-apo-tin-techniti-sti-syllogiki-noimosyni/>

Ενώ η ανάθεση νέων καθηκόντων και εξουσιών όσον αφορά την εποπτεία συστημάτων τεχνητής νοημοσύνης διευκολύνεται από τις νομικές και τεχνικές δεξιότητες που υπάρχουν ήδη στις ΑΠΔ, το ίδιο **συνεπάγεται την ανάγκη για επαρκείς πρόσθετους ανθρώπινους και οικονομικούς πόρους**



Ευχαριστώ πολύ για την προσοχή σας !

ΑΠΔ, ΕΣΠΔ, ΕΕΠΔ και ΤΝ

- <https://www.aepd.es/sites/default/files/2020-07/adecuacion-rgpd-ia-en.pdf>
- <https://autoriteitpersoonsgegevens.nl/uploads/2024-01/AI%20%26%20Algorithmic%20Risks%20Report%20Netherlands%20-%20winter%202023%202024.pdf>
- <https://ico.org.uk/media/2617219/guidance-on-the-ai-auditing-framework-draft-for-consultation.pdf>
- https://www.edpb.europa.eu/our-work-tools/our-documents/support-pool-experts-projects/ai-auditing_en
- <https://www.cnil.fr/en/self-assessment-guide-artificial-intelligence-ai-systems>
- https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Informationen/240715_Diskussionspapier_HmbBfDI_KI_Modelle.pdf
- https://www.edps.europa.eu/data-protection/our-work/publications/guidelines/2024-06-03-first-edps-orientations-euis-using-generative-ai_en
- https://www.edps.europa.eu/system/files/2024-06/EDPS-2024-09-Generative-AI-guidelines_EN.pdf
- https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Informationen/20231113_Checklist_LLM_Chatbots_EN.pdf
- https://www.edpb.europa.eu/system/files/2024-05/edpb_20240523_report_chatgpt_taskforce_en.pdf
- <https://www.cnil.fr/fr/webform/questionnaire-sur-lapplication-du-rgpd-aux-modeles-dia-questionnaire-application-gdpr-ai-models>
- https://www.edps.europa.eu/data-protection/our-work/publications/techdispatch/2023-11-16-techdispatch-22023-explainable-artificial-intelligence_en
- https://www.edpb.europa.eu/news/news/2024/edpb-opinion-ai-models-gdpr-principles-support-responsible-ai_el
- https://www.edpb.europa.eu/our-work-tools/our-documents/statements/statement-32024-data-protection-authorities-role-artificial_en

19^η Ημέρα Προστασίας Δεδομένων

Τρίτη 28/1/2025

«Ειδικά ζητήματα προστασίας δεδομένων και νέα νομοθετήματα»