ΣΕΒ

Σύγχρονες Επιχειρήσεις, Σύγχρονη Ελλάδα



ΟΔΗΓΟΣ
AI Act στην πράξη

για τη συμμόρφωση των επιχειρήσεων
με τον Κανονισμό **EU AI Act**
και τον **Ν. 5321/2026**

Νοέμβριος 2026

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΡΟΛΟΓΟΣ 03

ΛΙΓΑ ΛΟΓΙΑ ΓΙΑ ΤΟΝ ΟΔΗΓΟ 04

Α. ΣΥΝΟΠΤΙΚΗ ΠΑΡΟΥΣΙΑΣΗ ΤΟΥ ΚΑΝΟΝΙΣΜΟΥ EU AI ACT 06

1. Τι είναι ο Κανονισμός για την Τεχνητή Νοημοσύνη και ο Ν. 5321/2026; 06
2. Ποιοι είναι οι στόχοι και τα οφέλη του Κανονισμού; 07
3. Τι συνεπάγεται ο Κανονισμός για τις επιχειρήσεις; 08
4. Βασικές έννοιες: σύστημα ΤΝ, κατηγορίες κινδύνου, ρόλοι 08
5. Χρονοδιάγραμμα εφαρμογής 10

Β. ΔΙΑΔΙΚΑΣΙΕΣ & ΒΗΜΑΤΑ ΠΡΟΕΤΟΙΜΑΣΙΑΣ ΜΙΑΣ ΕΠΙΧΕΙΡΗΣΗΣ ΓΙΑ ΣΥΜΜΟΡΦΩΣΗ ΜΕ ΤΟΝ ΚΑΝΟΝΙΣΜΟ 13

ΔΙΑΔΙΚΑΣΙΑ 1: Διακυβέρνηση ΤΝ & Στρατηγικός Σχεδιασμός 14
ΔΙΑΔΙΚΑΣΙΑ 2: Χαρτογράφηση Συστημάτων ΤΝ & Τήρηση Μητρώου 19
ΔΙΑΔΙΚΑΣΙΑ 3: Ταξινόμηση Κινδύνου & Προσδιορισμός Ρόλου 22
ΔΙΑΔΙΚΑΣΙΑ 4: Υλοποίηση Υποχρεώσεων Συμμόρφωσης (ανά ρόλο & κατηγορία κινδύνου) 24
ΔΙΑΔΙΚΑΣΙΑ 5: Εκπαίδευση & AI Literacy 28
ΔΙΑΔΙΚΑΣΙΑ 6: Διαχείριση Προμηθευτών 30
ΔΙΑΔΙΚΑΣΙΑ 7: Παρακολούθηση, Εποπτεία & Διαχείριση Περιστατικών 32

Γ. ΣΗΜΕΙΑ ΠΡΟΣΟΧΗΣ: ΠΟΥ ΔΗΜΙΟΥΡΓΕΙΤΑΙ ΣΥΓΧΥΣΗ ΣΤΗΝ ΠΡΑΞΗ 34

Δ. CHECKLIST ΣΥΜΜΟΡΦΩΣΗΣ ΓΙΑ ΤΗ ΔΙΟΙΚΗΣΗ 39

Ε. ΕΤΟΙΜΟΤΗΤΑ ΑΠΕΝΑΝΤΙ ΣΕ ΕΠΟΠΤΙΚΟ ΕΛΕΓΧΟ 41

1. Τι μπορεί να ζητήσει μια εποπτική αρχή; 41
2. Διαδικασία αντίδρασης σε αίτημα αρχής, καταγγελία ή σοβαρή απόκλιση 42

ΣΤ. ΣΥΧΝΕΣ ΕΡΩΤΗΣΕΙΣ 43

ΠΑΡΑΡΤΗΜΑ Ι: Αναλυτικές υποχρεώσεις για συστήματα υψηλού κινδύνου 45

1. Όταν η επιχείρηση είναι πάροχος 45
2. Όταν η επιχείρηση είναι φορέας εφαρμογής 46
3. Όταν η επιχείρηση είναι εισαγωγέας, διανομέας ή εξουσιοδοτημένος αντιπρόσωπος 46
4. Συγκεντρωτικός πίνακας υποχρεώσεων ανά ρόλο 47

ΠΑΡΑΡΤΗΜΑ ΙΙ: FRIA | Πεδίο εφαρμογής & ελάχιστο περιεχόμενο 48

ΠΑΡΑΡΤΗΜΑ ΙΙΙ: Ενδεικτικά use cases ανά επιχειρησιακή λειτουργία 49

ΠΑΡΑΡΤΗΜΑ IV: AI Agents | Κίνδυνοι & αναλυτική διαδικασία ασφαλούς ενσωμάτωσης 50

ΠΗΓΕΣ 52

ΠΡΟΛΟΓΟΣ

Η Τεχνητή Νοημοσύνη (ΤΝ) περνά με ταχύτητα από τη φάση του πειραματισμού στον πυρήνα της επιχειρηματικής λειτουργίας. Αναδιαμορφώνει τον τρόπο με τον οποίο οι οργανισμοί λαμβάνουν αποφάσεις, σχεδιάζουν προϊόντα και υπηρεσίες, οργανώνουν την εργασία και δημιουργούν αξία. Για την Ελλάδα, η ΤΝ αποτελεί μια σημαντική ευκαιρία να ενισχύσει την παραγωγικότητα, την ανταγωνιστικότητα και την εξωστρέφεια της οικονομίας της.

Η αξιοποίηση αυτής της δυναμικής, όμως, δεν μπορεί να στηριχθεί μόνο στην τεχνολογική δυνατότητα. Προϋποθέτει εμπιστοσύνη, σαφή διακυβέρνηση και υπεύθυνη χρήση. Ο Κανονισμός της Ευρωπαϊκής Ένωσης για την Τεχνητή Νοημοσύνη εισάγει ένα κοινό πλαίσιο κανόνων που επιδιώκει ακριβώς αυτή την ισορροπία. Να προστατεύσει δηλαδή τα θεμελιώδη δικαιώματα και την ασφάλεια, χωρίς να ανακόψει την καινοτομία.

Για τις επιχειρήσεις, η συμμόρφωση δεν είναι μια αποσπασματική άσκηση αλλά ζήτημα εταιρικής διακυβέρνησης και στρατηγικής ετοιμότητας. Απαιτεί από τη Διοίκηση να γνωρίζει ποια συστήματα ΤΝ χρησιμοποιούνται, για ποιον σκοπό, με ποια δεδομένα, ποιοι επηρεάζονται και ποιος λογοδοτεί για τις αποφάσεις και τα αποτελέσματά τους.

Ο παρών Οδηγός δημιουργήθηκε για να μεταφράσει ένα σύνθετο κανονιστικό πλαίσιο σε πρακτικά βήματα. Προσφέρει στις επιχειρήσεις μια σαφή διαδρομή, από τη χαρτογράφηση και την ταξινόμηση των συστημάτων ΤΝ έως την εκπαίδευση των ανθρώπων, τη διαχείριση προμηθευτών, την ανθρώπινη εποπτεία, την τεκμηρίωση και τη συνεχή παρακολούθηση. Στόχος του δεν είναι μόνο η τυπική συμμόρφωση, αλλά η οικοδόμηση της κουλτούρας και των δομών που επιτρέπουν την ασφαλή και ουσιαστική αξιοποίηση της ΤΝ.

Η πρόκληση για κάθε οργανισμό είναι να κινηθεί έγκαιρα και μεθοδικά. Να αντιμετωπίσει τη συμμόρφωση όχι ως τροχοπέδη, αλλά ως προϋπόθεση εμπιστοσύνης και ανταγωνιστικού πλεονεκτήματος. Οι επιχειρήσεις που θα συνδέσουν την καινοτομία με υπευθυνότητα, δεξιότητες και λογοδοσία θα είναι εκείνες που θα μετατρέψουν τις δυνατότητες της ΤΝ σε μετρήσιμη αξία και ουσιαστικό αντίκτυπο.

Εύχομαι ο Οδηγός να αποτελέσει χρήσιμο σημείο αναφοράς για τις διοικήσεις και τα στελέχη των ελληνικών επιχειρήσεων, διευκολύνοντας τη μετάβαση από την κατανόηση του νέου πλαισίου στην οργανωμένη δράση.

Δρ. Κυριάκος Σαμπατακάκης
Πρόεδρος & Διευθύνων Σύμβουλος, Accenture
Συμπροεδρεύων Επιτροπής Τεχνολογίας
& Ψηφιακού Μετασχηματισμού

ΛΙΓΑ ΛΟΓΙΑ ΓΙΑ ΤΟΝ ΟΔΗΓΟ

Ο Κανονισμός (ΕΕ) 2024/1689 για την Τεχνητή Νοημοσύνη – EU AI Act (ο «Κανονισμός») αποτελεί το πρώτο ολοκληρωμένο νομοθετικό πλαίσιο διεθνώς για τη ρύθμιση της ανάπτυξης, διάθεσης στην αγορά και χρήσης συστημάτων Τεχνητής Νοημοσύνης (ΤΝ). Αποσκοπεί στη δημιουργία μιας εναρμονισμένης εσωτερικής αγοράς για την ΤΝ στην ΕΕ, διασφαλίζοντας την αξιόπιστη παραγωγή και χρήση των τεχνολογιών ΤΝ και την προστασία των θεμελιωδών δικαιωμάτων των πολιτών, ενθαρρύνοντας παράλληλα την υιοθέτηση της τεχνολογίας και την καινοτομία.

Ο ΣΕΒ, μέσα από σειρά δράσεων (Συνέδριο με θέμα «AI στην πράξη: Πώς θα εφαρμόσουμε την Τεχνητή Νοημοσύνη στις επιχειρήσεις μας», AI First Enterprise: Πρακτικός Οδηγός Επιχειρησιακού Μετασχηματισμού με Τεχνητή Νοημοσύνη), έχει αναδείξει την κρισιμότητα της αξιοποίησης των τεχνολογιών ΤΝ ως προϋπόθεση για την ενίσχυση της παραγωγικότητας και βέλτιστης λειτουργίας των επιχειρήσεων.

Ωστόσο, η υιοθέτηση της ΤΝ δεν είναι απλώς ζήτημα τεχνολογικής ετοιμότητας. Συνοδεύεται πλέον από ένα συγκεκριμένο πλαίσιο κανονιστικών υποχρεώσεων, το οποίο οι επιχειρήσεις οφείλουν να λάβουν υπόψη ήδη από το στάδιο σχεδιασμού των έργων ΤΝ, και όχι εκ των υστέρων.

Σε αυτό το πλαίσιο, ο Οδηγός του ΣΕΒ φιλοδοξεί να αποτελέσει πρακτικό εργαλείο για τις επιχειρήσεις-μέλη, ώστε η συμμόρφωση με τον Κανονισμό να μην αντιμετωπίζεται ως εμπόδιο στην καινοτομία, αλλά ως αναπόσπαστο κομμάτι μιας υπεύθυνης και βιώσιμης στρατηγικής υιοθέτησης της ΤΝ.

Ο Οδηγός προτείνει **7 κρίσιμες διαδικασίες** που πρέπει να υλοποιήσουν οι επιχειρήσεις που αναπτύσσουν, διαθέτουν στην αγορά ή χρησιμοποιούν συστήματα ΤΝ, προκειμένου να εντοπίσουν τις υποχρεώσεις τους και να εναρμονιστούν με τις απαιτήσεις του Κανονισμού. Για κάθε διαδικασία περιγράφονται ο σκοπός, τα βήματα, οι αρμοδιότητες και, κυρίως, η τεκμηρίωση που πρέπει να τηρείται, καθώς βασικός κανόνας συμμόρφωσης που συνάδει με τον Κανονισμό είναι ότι **«ό,τι δεν τεκμηριώνεται, δεν αποδεικνύεται».**

Ο Οδηγός Συμμόρφωσης με το AI Act αναπτύχθηκε με πρωτοβουλία της **Επιτροπής Τεχνολογίας και Ψηφιακού Μετασχηματισμού του ΣΕΒ** και με τη συνδρομή των:

- **Μελών ΣΕΒ:** Drakopoulos Law Firm, Grant Thornton, Pobuca και Siemens.
- **Ειδικής Γραμματείας Τεχνητής Νοημοσύνης και Διακυβέρνησης Δεδομένων** (που εκπροσωπήθηκε από τη Μαρία Δερεδάκη, ΕΕΠ-νομικό και τον εξωτερικό εμπειρογνώμονα Χρήστο Ζαγγανά, δικηγόρο, εταίρο της Δικηγορικής Εταιρείας Σκόπα-Ζαγγανάς & Συνεργάτες).
- **Ειδικής Εμπειρογνώμονα** Λίλιαν Μήτρου, δικηγόρο, καθηγήτρια στο Πανεπιστήμιο Αιγαίου και Πρόεδρο του Ινστιτούτου για την Ιδιωτικότητα, τα Προσωπικά Δεδομένα και την Τεχνολογία (European Public Law Organisation).

ΜΕΓΑΣ ΧΟΡΗΓΟΣ

Digital Academy

EUROBANK

ΧΟΡΗΓΟΙ

Coca-Cola Τρία Έψιλον
ΜΕΛΟΣ ΤΟΥ ΟΜΙΛΟΥ COCA-COLA HBC

Grant Thornton

TITAN

Α. ΣΥΝΟΠΤΙΚΗ ΠΑΡΟΥΣΙΑΣΗ ΤΟΥ ΚΑΝΟΝΙΣΜΟΥ EU AI ACT



1. Τι είναι ο Κανονισμός για την Τεχνητή Νοημοσύνη και ο Ν. 5321/2026;

Ο Κανονισμός αποτελεί το νομοθετικό πλαίσιο της Ευρωπαϊκής Επιτροπής για τη ρύθμιση της ανάπτυξης, διάθεσης και χρήσης συστημάτων ΤΝ στις χώρες της ΕΕ. **Υιοθετεί μία προσέγγιση με βάση τον κίνδυνο (risk-based approach)**, κατατάσσοντας τα συστήματα ΤΝ σε κατηγορίες ανάλογα με τον βαθμό κινδύνου που ενέχουν για τα θεμελιώδη δικαιώματα και την ασφάλεια των πολιτών: όσο μεγαλύτερος ο κίνδυνος ενός συστήματος, τόσο αυστηρότερες οι απαιτήσεις συμμόρφωσης.
Ο Ν. 5321/2026 (Α΄ 114/20.7.2026) καθορίζει τις αρμόδιες αρχές και τις διαδικασίες εποπτείας και συντονισμού για την εφαρμογή του Κανονισμού στην Ελλάδα.

Συνοπτικά:

- Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) ορίζεται ως βασική αρχή εποπτείας της αγοράς για τις απαγορευμένες πρακτικές, τα συστήματα του Παραρτήματος ΙΙΙ και τα συστήματα του άρθρου 50 του Κανονισμού, και ενιαίο σημείο επαφής[1].
- Οι αρμόδιες τομεακές αρχές εποπτεύουν συστήματα ΤΝ υψηλού κινδύνου που συνδέονται με προϊόντα του Παραρτήματος Ι του Κανονισμού.
- Η Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων (ΕΕΤΤ) ορίζεται ως κοινοποιούσα αρχή[2], ενώ αναλαμβάνει -από κοινού με την ΑΠΔΠΧ- τη λειτουργία του εθνικού ρυθμιστικού δοκιμαστηρίου ΤΝ.

Για τις ελληνικές επιχειρήσεις, το πλαίσιο προβλέπει ελέγχους από τις εποπτικές αρχές, υποχρεώσεις παροχής στοιχείων και δυνατότητα επιβολής κυρώσεων και προστίμων σε περιπτώσεις μη συμμόρφωσης.

[1] Η ΑΠΔΠΧ ελέγχει αν τα συστήματα ΤΝ που διατίθενται ή χρησιμοποιούνται στην αγορά συμμορφώνονται με τις νομικές απαιτήσεις. Ως ενιαίο σημείο επαφής, αποτελεί το βασικό σημείο επικοινωνίας της χώρας με την Ευρωπαϊκή Επιτροπή, το ευρωπαϊκό AI Office και τις αντίστοιχες αρχές άλλων ευρωπαϊκών χωρών.

[2] Η ΕΕΤΤ πιστοποιεί και δηλώνει επίσημα στην Ευρωπαϊκή Επιτροπή ποιοι οργανισμοί στην Ελλάδα μπορούν να πραγματοποιούν αξιολογήσεις συμμόρφωσης για συστήματα ΤΝ υψηλού κινδύνου.

Πεδίο εφαρμογής:

Ο Κανονισμός εφαρμόζεται σε:
- παρόχους που διαθέτουν στην αγορά ή θέτουν σε λειτουργία συστήματα ΤΝ ή διαθέτουν στην αγορά μοντέλα ΤΝ γενικού σκοπού στην Ένωση, ανεξάρτητα από τον τόπο εγκατάστασής τους (εντός ή εκτός ΕΕ),
- φορείς εφαρμογής συστημάτων ΤΝ (χρήστες) με εγκατάσταση εντός της ΕΕ,
- παρόχους και φορείς εφαρμογής εκτός ΕΕ, στο βαθμό που τα παραγόμενα από τα συστήματα ΤΝ στοιχεία εξόδου προορίζονται για χρήση στην ΕΕ,
- εισαγωγείς και διανομείς συστημάτων ΤΝ, κατασκευαστές προϊόντων και εξουσιοδοτημένους αντιπροσώπους παρόχων.

Εξαιρέσεις:

Ο Κανονισμός ΔΕΝ εφαρμόζεται σε:
- συστήματα αποκλειστικά για στρατιωτικούς / αμυντικούς σκοπούς ή σκοπούς εθνικής ασφάλειας,
- συστήματα αμιγώς επιστημονικής έρευνας και ανάπτυξης,
- συστήματα για αποκλειστικά προσωπική, μη επαγγελματική χρήση,
- συστήματα κατά τη φάση της έρευνας και δοκιμής τους, εκτός αν η δοκιμή τους γίνεται σε πραγματικές συνθήκες.
- συστήματα που διατίθενται με άδεια ελεύθερου και ανοιχτού κώδικα (open-source)[3].

2. Ποιοι είναι οι στόχοι και τα οφέλη του Κανονισμού;

- Προώθηση αξιόπιστης και ασφαλούς ΤΝ στην ευρωπαϊκή αγορά και προστασία των θεμελιωδών δικαιωμάτων.
- Δημιουργία ενιαίων κανόνων σε όλα τα κράτη μέλη της ΕΕ και ενίσχυση της εμπιστοσύνης των χρηστών και των πολιτών στις εφαρμογές ΤΝ.
- Ενίσχυση της καινοτομίας και της ανταγωνιστικότητας, με ειδική στήριξη ΜμΕ και νεοφυών επιχειρήσεων (AI Regulatory Sandboxes).

Για τις επιχειρήσεις, η ευθυγράμμιση / συμμόρφωση συνεπάγεται νομική βεβαιότητα και ενιαίο πλαίσιο συμμόρφωσης σε όλη την ΕΕ, ευκολότερη πρόσβαση στην ενιαία αγορά, ενίσχυση της εμπιστοσύνης πελατών και συνεργατών και καλύτερη διαχείριση των κινδύνων που συνδέονται με τη χρήση ΤΝ.

[3] Δεν ισχύει για συστήματα υψηλού κινδύνου ή για συστήματα που εμπίπτουν στα άρθρα 5 ή 50 του Κανονισμού.

3. Τι συνεπάγεται ο Κανονισμός για τις επιχειρήσεις;

Ο Κανονισμός αφορά μεγάλο φάσμα επιχειρήσεων, ανεξάρτητα από τον κλάδο δραστηριότητας.

Ο Κανονισμός μετατρέπει την ΤΝ από τεχνολογικό εργαλείο σε θέμα εταιρικής διακυβέρνησης. Η Διοίκηση πρέπει να γνωρίζει ποια συστήματα ΤΝ χρησιμοποιούνται, για ποιο σκοπό και ποιους κινδύνους ενέχουν.

Οι επιχειρήσεις καλούνται να:

- Χαρτογραφήσουν τα συστήματα ΤΝ που αναπτύσσουν, προμηθεύονται ή χρησιμοποιούν.
- Προσδιορίσουν τον ρόλο τους σύμφωνα με τον Κανονισμό (πάροχος, φορέας εφαρμογής κλπ.).
- Αξιολογήσουν σε ποια κατηγορία κινδύνου εντάσσεται κάθε σύστημα.
- Εφαρμόσουν τις απαιτήσεις συμμόρφωσης που αντιστοιχούν στον συγκεκριμένο ρόλο και επίπεδο κινδύνου.
- Δημιουργήσουν διαδικασίες διακυβέρνησης, τεκμηρίωσης και ελέγχου για τη χρήση ΤΝ.

4. Βασικές έννοιες: σύστημα ΤΝ, κατηγορίες κινδύνου, ρόλοι

Τι είναι «Σύστημα Τεχνητής Νοημοσύνης» κατά τον Κανονισμό;
Ως σύστημα ΤΝ νοείται ένα μηχανικό σύστημα που λειτουργεί με διαφορετικά επίπεδα αυτονομίας, ενδέχεται να παρουσιάζει προσαρμοστικότητα μετά την ανάπτυξή του και, για συγκεκριμένους ή σιωπηρούς στόχους, συνάγει από τα δεδομένα εισόδου πώς να παράγει αποτελέσματα, όπως προβλέψεις, συστάσεις, αποφάσεις ή περιεχόμενο, τα οποία επηρεάζουν φυσικά ή εικονικά περιβάλλοντα.

Δεν έχει σημασία πώς ονομάζεται το εργαλείο. Σημασία έχει τι κάνει.
Αν αξιοποιεί δεδομένα για να παράγει αποτέλεσμα (πρόβλεψη, σύσταση, απόφαση, περιεχόμενο) που επηρεάζει το περιβάλλον γύρω του, εμπίπτει στον Κανονισμό.
Είτε το αποκαλούμε «ΤΝ», «machine learning» είτε απλώς «αναλυτικό εργαλείο», η ονομασία δεν αλλάζει την ουσία.

Αντίθετα, ένα σύστημα που λειτουργεί και παράγει αποτελέσματα εκτελώντας ένα προκαθορισμένο σύστημα κανόνων «αν-τότε», χωρίς να συνάγει κάτι από δεδομένα, δεν συνιστά σύστημα ΤΝ.

Κατηγορίες κινδύνου

Κατηγορία	Τι περιλαμβάνει	Βασική συνέπεια
Απαγορευμένες πρακτικές	Χειραγώγηση/εκμετάλλευση ευαλωτοτήτων (πχ λόγω ηλικίας), social scoring, βιομετρική κατηγοριοποίηση βάσει ευαίσθητων χαρακτηριστικών, μη στοχευμένη συλλογή εικόνων προσώπων, αναγνώριση συναισθημάτων σε εργασία/εκπαίδευση, ορισμένες μορφές προγνωστικής αστυνόμευσης, μη συναινετικές εικόνες ιδιωτικού χαρακτήρα.	Πλήρης απαγόρευση ανάπτυξης, διάθεσης και χρήσης.
Υψηλού κινδύνου	(α) ΤΝ ως προϊόν ή κατασκευαστικό στοιχείο ασφάλειας προϊόντων της νομοθεσίας εναρμόνισης (πχ ιατροτεχνολογικά, οχήματα, ανελκυστήρες κ.ά.) (β) αυτοτελή συστήματα σε ευαίσθητους τομείς (π.χ. βιομετρικά, κρίσιμες υποδομές, εκπαίδευση, απασχόληση, βασικές υπηρεσίες, επιβολή νόμου κ.ά.).	Εκτεταμένες απαιτήσεις συμμόρφωσης και εποπτείας.
Περιορισμένου κινδύνου	Συστήματα που αλληλοεπιδρούν με ανθρώπους ή παράγουν συνθετικό περιεχόμενο (chatbots, εργαλεία δημιουργίας εικόνων, deepfakes).	Υποχρεώσεις διαφάνειας (ενημέρωση ότι πρόκειται για ΤΝ, επισήμανση συνθετικού περιεχομένου).
Ελάχιστου κινδύνου	Εφαρμογές χωρίς ουσιώδεις κινδύνους (π.χ. spam filters).	Καμία ειδική υποχρέωση· εφαρμόζεται το λοιπό δίκαιο (GDPR, κυβερνοασφάλεια κλπ.).

Επισήμανση: Για μεγαλύτερη σαφήνεια ως προς το τι περιλαμβάνει η κάθε κατηγορία μπορείτε να ανατρέξετε στα σχετικά άρθρα του Κανονισμού: Απαγορευμένες πρακτικές: άρθρο 5, Υψηλού κινδύνου: άρθρο 6 (και Παραρτήματα I και III), Περιορισμένου κινδύνου: άρθρο 50.

i

Τα επίπεδα κινδύνου δεν προσδιορίζονται με βάση την τεχνολογική μέθοδο αλλά τις πιθανές επιπτώσεις (βλάβη) στην υγεία, την ασφάλεια, τη δημοκρατία, το κράτος δικαίου και τα θεμελιώδη δικαιώματα.

Ρόλοι επιχείρησης

Ρόλος	
Πάροχος (Provider)	Αναπτύσσει ή αναθέτει την ανάπτυξη συστήματος ΤΝ και το διαθέτει στην αγορά ή το θέτει σε λειτουργία με το δικό του όνομα / σήμα. Φέρει το βαρύτερο κανονιστικό φορτίο.
Φορέας Εφαρμογής (Deployer)	Χρησιμοποιεί σύστημα ΤΝ στο πλαίσιο της επαγγελματικής του δραστηριότητας. Ο συνηθέστερος ρόλος για τις ελληνικές επιχειρήσεις.
Εισαγωγέας / Διανομέας	Εισάγει στην ΕΕ ή καθιστά διαθέσιμο στην αγορά σύστημα τρίτου. Υποχρεώσεις κυρίως ελέγχου τεκμηρίωσης και σήμανσης.
Εξουσιοδοτημένος Αντιπρόσωπος	Εγκατεστημένος στην ΕΕ, ενεργεί για λογαριασμό παρόχου εκτός ΕΕ.
Κατασκευαστής προϊόντος με ενσωματωμένη ΤΝ	Διαθέτει προϊόν (του Παραρτήματος Ι του Κανονισμού) που ενσωματώνει σύστημα ΤΝ ως στοιχείο ασφαλείας και το προϊόν φέρει το όνομά του ή το εμπορικό του σήμα. Θεωρείται υπεύθυνος για τη συμμόρφωση του συστήματος με τον Κανονισμό.

Επισήμανση: Μία επιχείρηση μπορεί να φέρει ταυτόχρονα περισσότερους από έναν ρόλους. Ο ρόλος μπορεί επίσης να μεταβληθεί εκ των υστέρων (βλ. Ενότητα Γ, Σημείο 4).

5. Χρονοδιάγραμμα εφαρμογής

Ο Κανονισμός τέθηκε σε ισχύ την 1.8.2024 και εφαρμόζεται σταδιακά. Με το πακέτο τροποποιήσεων Digital Omnibus (τελική έγκριση από το Συμβούλιο στις 29.6.2026) οι υποχρεώσεις για τα συστήματα υψηλού κινδύνου μετατέθηκαν, χωρίς να αλλάξει η αρχιτεκτονική του Κανονισμού. Οι βασικές ημερομηνίες διαμορφώνονται πλέον ως εξής:

Ημερομηνία	Υποχρέωση
2.2.2025 (σε ισχύ)	Απαγορευμένες πρακτικές ΤΝ (άρθρο 5) και υποχρέωση λήψης μέτρων για την ανάπτυξη γνώσεων και δεξιοτήτων ΤΝ του προσωπικού — AI literacy (άρθρο 4).
2.8.2025 (σε ισχύ)	Υποχρεώσεις παρόχων μοντέλων ΤΝ γενικού σκοπού (GPAI, άρθρα 51–55) και δομές διακυβέρνησης σε επίπεδο ΕΕ.
2.8.2026 (σε ισχύ)	Υποχρεώσεις διαφάνειας του άρθρου 50 (ενημέρωση ότι ο χρήστης αλληλοεπιδρά με ΤΝ, επισήμανση deepfakes κλπ.), δεν μετατέθηκαν από το Digital Omnibus.
2.12.2026	Τεχνική σήμανση συνθετικού περιεχομένου (άρθρο 50 παρ. 2 watermarking) για συστήματα ήδη στην αγορά. Νέα απαγόρευση συστημάτων παραγωγής μη συναινετικού προσωπικού υλικού.
2.12.2027	Πλήρεις υποχρεώσεις για αυτοτελή συστήματα ΤΝ υψηλού κινδύνου (Παράρτημα ΙΙΙ του Κανονισμού).
2.8.2028	Υποχρεώσεις για ΤΝ ενσωματωμένη σε προϊόντα που υπόκεινται σε ενωσιακή νομοθεσία ασφάλειας προϊόντων (Παράρτημα Ι του Κανονισμού).

Η μετάθεση των προθεσμιών για τα συστήματα υψηλού κινδύνου δεν πρέπει να εκληφθεί ως λόγος αναβολής. Τα πιο χρονοβόρα στάδια (απογραφή, ταξινόμηση, διακυβέρνηση, τεκμηρίωση) απαιτούν συνήθως 12–24 μήνες, ενώ ορισμένες υποχρεώσεις ισχύουν ήδη (βλ. παραπάνω πίνακα).

Σημείωση: Ο παρών Οδηγός έχει ενημερωτικό χαρακτήρα και δεν υποκαθιστά εξατομικευμένη νομική ή τεχνική συμβουλή. Οι αναφερόμενες προθεσμίες αποτυπώνουν το κανονιστικό τοπίο κατά τον χρόνο σύνταξης (Οκτώβριος 2026, μετά την έκδοση του Digital Omnibus) και ενδέχεται να εξειδικευθούν περαιτέρω με κατευθυντήριες γραμμές της Ευρωπαϊκής Επιτροπής.

Παραδείγματα πεδίου εφαρμογής & ορισμού συστήματος ΤΝ

Α. Εδαφικό πεδίο εφαρμογής

Παραδείγματα που εμπίπτουν

- Αμερικανικός πάροχος με πελάτες στην ΕΕ: Εταιρεία με έδρα στις ΗΠΑ προσφέρει υπηρεσία Generative AI μέσω διαδικτύου, την οποία χρησιμοποιούν επιχειρήσεις και πολίτες σε Ελλάδα, Γερμανία και Γαλλία. Παρότι ο πάροχος δεν είναι εγκατεστημένος στην ΕΕ, το σύστημα εμπίπτει στο πεδίο εφαρμογής, επειδή χρησιμοποιείται εντός της ΕΕ.
- Σύστημα αξιολόγησης εργαζομένων από τρίτη χώρα: Πολυεθνική με έδρα στη Σιγκαπούρη διαθέτει σε ευρωπαϊκές επιχειρήσεις σύστημα ΤΝ για αξιολόγηση υποψηφίων και εργαζομένων. Αν και η ανάπτυξη και λειτουργία γίνεται εκτός ΕΕ, ο Κανονισμός εφαρμόζεται επειδή τα στοιχεία εξόδου του συστήματος χρησιμοποιούνται στην ΕΕ.

Παράδειγμα που ΔΕΝ εμπίπτει

- Τοπική χρήση εκτός ΕΕ χωρίς σύνδεση με την ΕΕ: Εταιρεία στη Βραζιλία χρησιμοποιεί σύστημα ΤΝ αποκλειστικά για διαχείριση αποθεμάτων στα καταστήματά της στη Βραζιλία, χωρίς προϊόντα/υπηρεσίες στην ΕΕ και χωρίς επιρροή σε πρόσωπα στην ΕΕ. Ο Κανονισμός δεν εφαρμόζεται.

Β. Ορισμός συστήματος ΤΝ

Συστήματα που αποτελούν ΤΝ

- Πρόβλεψη ζήτησης προϊόντων: Αλυσίδα λιανικής χρησιμοποιεί αλγόριθμο μηχανικής μάθησης που αναλύει ιστορικά στοιχεία πωλήσεων και προβλέπει μελλοντική ζήτηση. Πραγματοποιεί συναγωγή αποτελεσμάτων από δεδομένα | εμπίπτει στον Κανονισμό.
- Ανίχνευση απάτης: Ασφαλιστική εταιρεία χρησιμοποιεί ΤΝ για ανίχνευση ύποπτων απαιτήσεων αποζημίωσης. Αναλύει πρότυπα συμπεριφοράς και παράγει προβλέψεις/συστάσεις | εμπίπτει στον Κανονισμό.

Συστήματα που ΔΕΝ αποτελούν ΤΝ

- Λογιστικό φύλλο Excel: Υπολογιστικό φύλλο με προκαθορισμένους μαθηματικούς τύπους για προϋπολογισμούς. Δεν πραγματοποιεί συναγωγή, δεν διαθέτει αυτονομία ή δυνατότητα αυτοεκμάθησης | δεν θεωρείται σύστημα ΤΝ.
- Σύστημα στατικών κανόνων: Πληροφοριακό σύστημα εγκρίνει αυτόματα αγορές βάσει του κανόνα «εάν το ποσό είναι μικρότερο από €500, τότε έγκριση». Λειτουργεί αποκλειστικά με προκαθορισμένους κανόνες | δεν θεωρείται σύστημα ΤΝ.

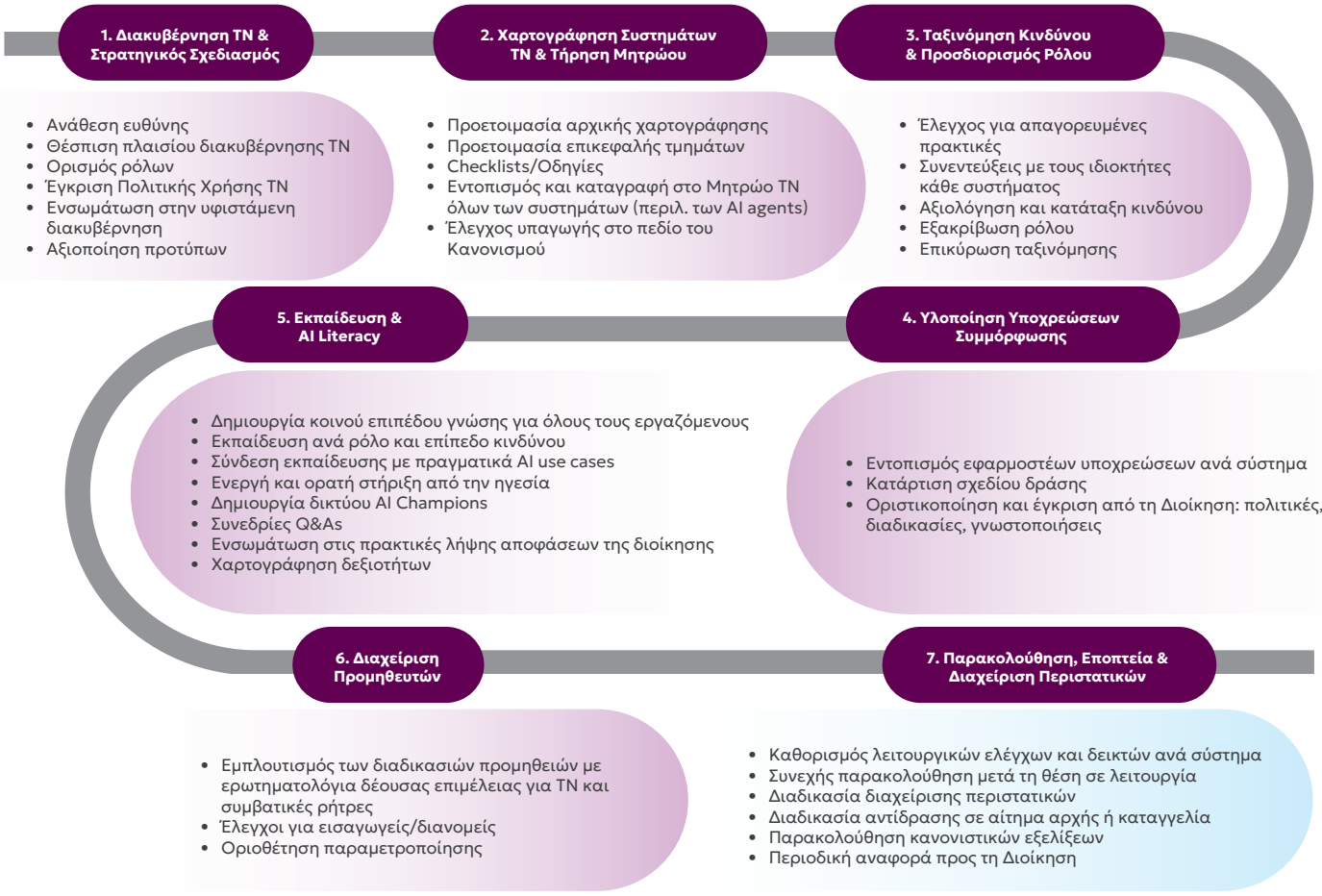
Γ. Μεταβολή κατηγορίας κινδύνου

- Chatbot που χρησιμοποιείται αποκλειστικά για απαντήσεις σε ερωτήσεις πελατών θεωρείται συνήθως περιορισμένου κινδύνου. Εάν το ίδιο εργαλείο χρησιμοποιηθεί για να αξιολογεί υποψήφιους εργαζομένους ή να προτείνει προσλήψεις, ενδέχεται να χαρακτηριστεί υψηλού κινδύνου.

Β. ΔΙΑΔΙΚΑΣΙΕΣ & ΒΗΜΑΤΑ ΠΡΟΕΤΟΙΜΑΣΙΑΣ ΜΙΑΣ ΕΠΙΧΕΙΡΗΣΗΣ ΓΙΑ ΣΥΜΜΟΡΦΩΣΗ ΜΕ ΤΟΝ ΚΑΝΟΝΙΣΜΟ



Η συμμόρφωση με τον Κανονισμό δεν αποτελεί αποκλειστικά νομική άσκηση, αλλά σταδιακή διαδικασία που απαιτεί συντονισμό διοίκησης, νομικών/κανονιστικών λειτουργιών, IT και επιχειρησιακών μονάδων. Στην πράξη, μπορεί να οργανωθεί σε επτά διακριτά στάδια.



Σχήμα 1: Διάγραμμα ροής διαδικασιών συμμόρφωσης

ΔΙΑΔΙΚΑΣΙΑ **No1**

Διακυβέρνηση ΤΝ & Στρατηγικός Σχεδιασμός



ΣΚΟΠΟΣ

Η αναγωγή της υπεύθυνης χρήσης ΤΝ σε συστηματικό μέρος της εταιρικής διακυβέρνησης, υπό την εποπτεία της Διοίκησης, με σαφείς ρόλους, πολιτικές και μηχανισμούς λογοδοσίας.

Χωρίς μηχανισμό που να εντοπίζει / προσδιορίζει, κατηγοριοποιεί και καταγράφει διαρκώς ποια συστήματα ΤΝ χρησιμοποιούνται, με ποιον ρόλο, σε ποια κατηγορία κινδύνου, με ποιες δικλίδες και με ποιον υπεύθυνο, η συμμόρφωση δεν είναι ούτε εφικτή ούτε αποδείξιμη.

ΒΗΜΑΤΑ

1. **Ανάθεση ευθύνης** έγκρισης, εποπτείας και λογοδοσίας στο ανώτατο όργανο Διοίκησης (ΔΣ ή Γενική Διεύθυνση).

2. **Θέσπιση πλαισίου διακυβέρνησης ΤΝ** με βάση το μοντέλο των «τριών γραμμών άμυνας»: η πρώτη γραμμή κατέχει και λειτουργεί τα συστήματα, η δεύτερη θέτει το πλαίσιο και εποπτεύει τη συμμόρφωση, η τρίτη (εσωτερικός ή εξωτερικός έλεγχος) παρέχει ανεξάρτητη διασφάλιση.

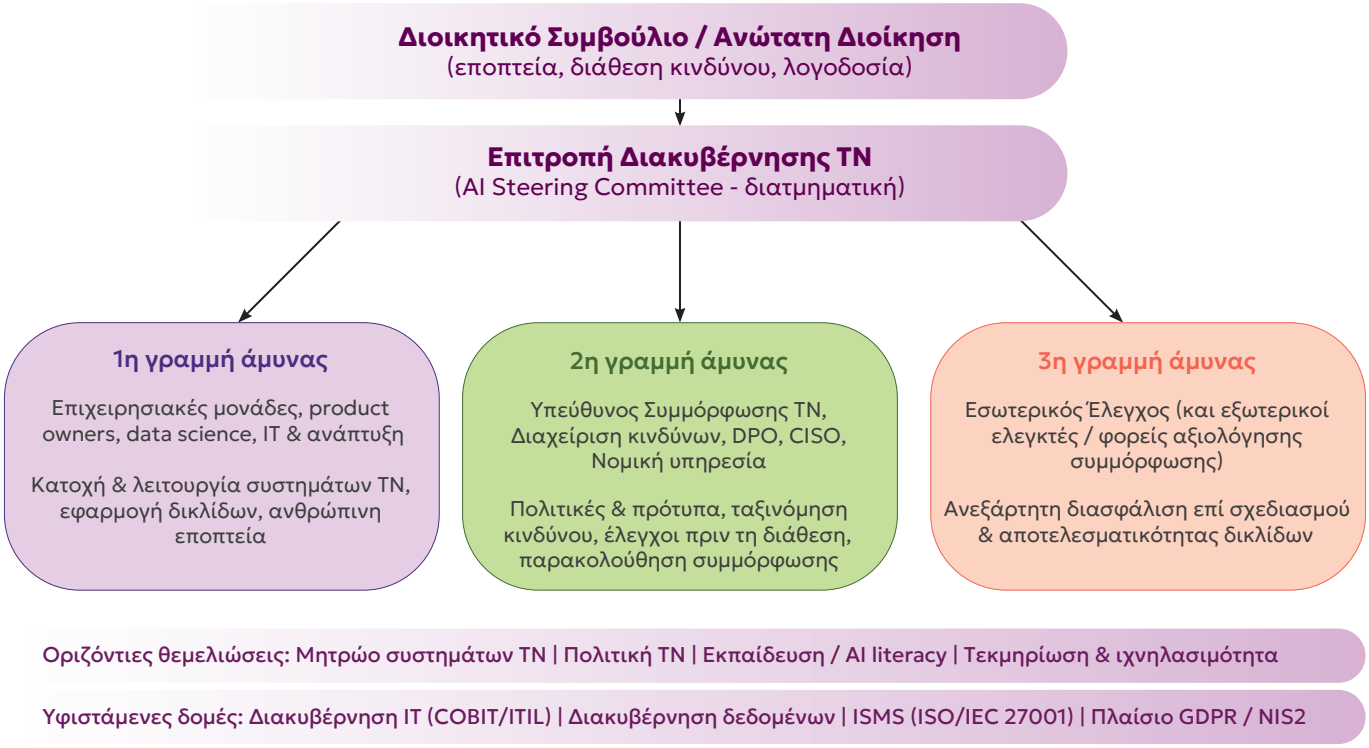
3. **Ορισμός ρόλων:** Επιτροπή Διακυβέρνησης ΤΝ (AI Steering Committee, διατμηματική), ιδιοκτήτες συστημάτων (Υπεύθυνος Συμμόρφωσης ΤΝ - AI Officer, Τεχνικός Υπεύθυνος - CISO, κοκ), Εσωτερικός Έλεγχος. Σε μικρότερους οργανισμούς ρόλοι μπορούν να συγχωνεύονται, με τεκμηρίωση της διαχείρισης συγκρούσεων καθηκόντων.

4. **Έγκριση Πολιτικής Χρήσης ΤΝ από τη Διοίκηση:** Επιτρεπόμενες/μη επιτρεπόμενες χρήσεις, κανόνες δεδομένων, ανθρώπινη εποπτεία, εγκρίσεις, αναφορές. Ρητή κάλυψη της χρήσης εργαλείων παραγωγικής ΤΝ (GenAI) από εργαζομένους, όπου συχνά εντοπίζεται «σκιώδης ΤΝ» (shadow AI).

5. **Ενσωμάτωση στην υφιστάμενη διακυβέρνηση:** Όχι νέο «σιλό». Κοινό ή διασυνδεδεμένο μητρώο, διασταυρούμενη συμμετοχή σε επιτροπές, ενιαία πύλη αιτημάτων, συντονισμός με GDPR, NIS2 και DORA ώστε μία δικλίδα να καλύπτει πολλαπλές κανονιστικές απαιτήσεις.

6. **Αξιοποίηση προτύπων:** ISO/IEC 42001:2023 (πιστοποιήσιμο σύστημα διαχείρισης ΤΝ), ISO/IEC 23894:2023 (διαχείριση κινδύνου), ISO/IEC 42005:2025 (εκτιμήσεις επιπτώσεων), NIST AI RMF.

Η πιστοποίηση ISO/IEC 42001 αποδεικνύει οργανωτική ωριμότητα, δεν συνιστά όμως τεκμήριο νομικής συμμόρφωσης. Το τεκμήριο θα το παρέχουν τα εναρμονισμένα ευρωπαϊκά πρότυπα της CEN-CENELEC (JTC 21), όταν δημοσιευθούν στην Επίσημη Εφημερίδα της ΕΕ (άρθρο 40).



Σχήμα 2: Ενδεικτικό οργανωτικό μοντέλο διακυβέρνησης ΤΝ με προσαρμογή του μοντέλου των «τριών γραμμών άμυνας»

Οι υποχρεώσεις συμμόρφωσης που προβλέπονται από τον Κανονισμό βαρύνουν την επιχείρηση, είτε αυτή είναι πάροχος είτε χρήστης.
Ο Κανονισμός ΔΕΝ θεσπίζει αυτοτελή προσωπική ευθύνη των μελών του ΔΣ για την εκπλήρωση των υποχρεώσεων αυτών[4].

ΡΟΛΟΙ - ΑΡΜΟΔΙΟΤΗΤΕΣ - ΕΥΘΥΝΗ

Ρόλος /Όργανο	Ενδεικτικές αρμοδιότητες στο πλαίσιο του Κανονισμού	Ευθύνη / Λογοδοσία
Διοικητικό Συμβούλιο / Ανώτατη Διοίκηση	• Έγκριση στρατηγικής και πολιτικής ΤΝ • Καθορισμός διάθεσης ανάληψης κινδύνου • Διασφάλιση πόρων	• Τελική λογοδοσία για την οργάνωση και συντονισμό του πλαισίου διακυβέρνησης ΤΝ • Διασφάλιση ότι η επιχείρηση διαθέτει κατάλληλους μηχανισμούς συμμόρφωσης
Επιτροπή Διακυβέρνησης ΤΝ (AI Steering Committee)	• Λήψη ή εισήγηση στρατηγικών αποφάσεων για τη χρήση ΤΝ • Αξιολόγηση νέων χρήσεων ΤΝ • Επικύρωση ταξινόμησης κινδύνου • Εποπτεία μητρώου ΤΝ και σχεδίων αποκατάστασης	• Συλλογική λογοδοσία (στο ΔΣ) για την ορθή εφαρμογή του πλαισίου διακυβέρνησης • Τεκμηρίωση, επάρκεια και ορθότητα των αποφάσεων και εγκρίσεων που λαμβάνει ή εισηγείται
DPO	• Διενέργεια DPIA / συσχέτιση με FRIA (όπου απαιτείται) • Παροχή συμβουλών για τη νόμιμη επεξεργασία προσωπικών δεδομένων • Υποστήριξη στην άσκηση δικαιωμάτων των υποκειμένων	• Παροχή συμβουλών • Παρακολούθηση συμμόρφωσης με το πλαίσιο προστασίας δεδομένων
Ιδιοκτήτες συστημάτων[5]:		
Επιχειρησιακός Υπεύθυνος (Business Owner)	• Καθημερινή επιχειρησιακή διαχείριση του συστήματος • Χρήση σύμφωνα με τις οδηγίες του παρόχου και τις εσωτερικές πολιτικές • Διασφάλιση ανθρώπινης εποπτείας. • Έλεγχος ποιότητας δεδομένων εισόδου • Εκπαίδευση χρηστών • Αναφορά περιστατικών	• Νόμιμη, ασφαλής και εγκεκριμένη χρήση του συστήματος στον επιχειρησιακό τομέα ευθύνης του • Έγκαιρη αναφορά αποκλίσεων, κινδύνων και μη εξουσιοδοτημένων χρήσεων • Τήρηση των εσωτερικών πολιτικών και διαδικασιών της επιχείρησης

[4]Ο Κανονισμός δεν επηρεάζει τις γενικές υποχρεώσεις επιμέλειας, πίστης και ορθής διοίκησης που απορρέουν από το εφαρμοστέο εταιρικό δίκαιο και εξακολουθούν να ισχύουν για τα μέλη της Διοίκησης.

[5]Στέλεχος ή οργανωτική μονάδα που έχει την ευθύνη για τον επιχειρησιακό σκοπό, τη χρήση, την ορθή λειτουργία, την απόδοση και τη συμμόρφωση ενός πληροφοριακού συστήματος, ανεξάρτητα από το ποιος παρέχει την τεχνική του υποστήριξη.

Τεχνικός Υπεύθυνος (Technical Owner: CISO / IT Manager)	• Τεχνική λειτουργία και υποστήριξη του συστήματος • Καθορισμός και εφαρμογή μέτρων κυβερνοασφάλειας • Αντιμετώπιση ειδικών κινδύνων ΤΝ (data poisoning, model evasion, prompt injection) • Ενσωμάτωση συστημάτων ΤΝ στο ISMS	• Επάρκεια των μέτρων κυβερνοασφάλειας και την παρακολούθηση των σχετικών κινδύνων • Έγκαιρη ενημέρωση της Διοίκησης για κρίσιμες αδυναμίες ή περιστατικά
Υπεύθυνος Συμμόρφωσης (Compliance Owner: AI Officer)	• Καθημερινός συντονισμός του προγράμματος συμμόρφωσης • Παρακολούθηση κανονιστικών εξελίξεων • Εφαρμογή μεθοδολογίας ταξινόμησης κινδύνου • Διατήρηση απαιτούμενης τεκμηρίωσης • Τήρηση μητρώου ΤΝ • Σημείο επαφής με τις αρχές	• Ορθή εκτέλεση των δράσεων συμμόρφωσης σε καθημερινή βάση • Έγκαιρη ενημέρωση της Διοίκησης για κινδύνους, παραβάσεις ή ελλείψεις
Εσωτερικός Έλεγχος	• Διενέργεια τακτικών ελέγχων βάσει εγκεκριμένου ελεγκτικού προγράμματος • Αξιολόγηση επάρκειας και αποτελεσματικότητας δικλίδων ελέγχου • Υποβολή ευρημάτων και συστάσεων βελτίωσης προς τη Διοίκηση	• Αντικειμενικότητα και ανεξαρτησία των ελεγκτικών εργασιών

i

Πρακτικός κανόνας: κάθε σύστημα ΤΝ πρέπει να έχει τρεις «ιδιοκτήτες»: έναν επιχειρησιακό υπεύθυνο που ξέρει γιατί χρησιμοποιείται, έναν τεχνικό υπεύθυνο που ξέρει πώς λειτουργεί και έναν υπεύθυνο συμμόρφωσης που ξέρει ποιο κανονιστικό πλαίσιο εφαρμόζεται κατά περίπτωση.

ΕΡΓΑΛΕΙΑ & ΤΕΚΜΗΡΙΩΣΗ

Τεκμήριο / εργαλείο	Περιγραφή
Πολιτική Χρήσης ΤΝ / GenAI	Εσωτερικές πολιτικές, εγκρίσεις, οδηγίες χρήσης, SOPs. Επιτρεπόμενες και μη επιτρεπόμενες χρήσεις, κανόνες δεδομένων, εγκρίσεις, ανθρώπινος έλεγχος.
Κανονισμός ρόλων & αρμοδιοτήτων (RACI)	Τεκμηριώνει ποιος αποφασίζει, ποιος εκτελεί, ποιος ελέγχει, ανά στάδιο του κύκλου ζωής ΤΝ, και ορίζει τις διαδικασίες ανθρώπινης εποπτείας.
Πρακτικά εγκρίσεων Διοίκησης	Αποφάσεις έγκρισης πολιτικής, διάθεσης πόρων και αποδοχής κινδύνου.
GRC (Governance, Risk & Compliance) πλατφόρμα	Τεκμηρίωση της διακυβέρνησης και των ελέγχων.

ΧΡΟΝΟΣ ΕΚΤΕΛΕΣΗΣ

- Άμεσα: έγκριση βασικής Πολιτικής Χρήσης ΤΝ και ορισμός υπευθύνων.
- 3–6 μήνες: πλήρης λειτουργία πλαισίου διακυβέρνησης, το αργότερο πριν από τον πρώτο εσωτερικό έλεγχο ή αυτοαξιολόγηση.

ΔΙΑΔΙΚΑΣΙΑ No2

Χαρτογράφηση Συστημάτων ΤΝ & Τήρηση Μητρώου



ΣΚΟΠΟΣ

Η διαμόρφωση πλήρους εικόνας των συστημάτων ΤΝ που χρησιμοποιεί ή αναπτύσσει η επιχείρηση και η τήρηση ενιαίου μητρώου (AI inventory), το οποίο αποτελεί τη βάση κάθε επόμενης ενέργειας συμμόρφωσης.

ΒΗΜΑΤΑ

1. **Προετοιμασία αρχικής χαρτογράφησης** με καθορισμό μεθοδολογίας, χρονοδιαγράμματος και εμπλεκομένων για την καταγραφή όλων των συστημάτων ΤΝ που χρησιμοποιούνται ή αναπτύσσονται.
2. **Προετοιμασία των επικεφαλής τμημάτων** με ενημέρωσή τους για το ρόλο τους στη διαδικασία, καθώς η χαρτογράφηση δεν μπορεί να γίνει αποκλειστικά κεντρικά. Απαιτεί τη συμβολή κάθε λειτουργίας που χρησιμοποιεί εργαλεία ΤΝ (Marketing, HR, Πωλήσεις, IT, Customer Service κλπ.).
3. **Κατάρτιση checklist και οδηγιών:** δημιουργία ενός τυποποιημένου ερωτηματολογίου / checklist που θα διανεμηθεί στα τμήματα, ώστε η συλλογή πληροφορίας να είναι συστηματική και συγκρίσιμη μεταξύ λειτουργιών.
4. **Εντοπισμός και καταγραφή στο Μητρώο ΤΝ όλων των συστημάτων** σε χρήση ή υπό ανάπτυξη/προμήθεια, από εργαλεία παραγωγικότητας (Copilot, chatbots) έως σύνθετα συστήματα (αξιολόγηση πιστοληπτικής ικανότητας, recruitment, predictive maintenance) και αυτόνομους AI agents.

Ειδικά για κάθε AI agent:

- **Καταγραφή στο Μητρώο ΤΝ βασικών στοιχείων:** όνομα, σκοπός, υπεύθυνοι, πλατφόρμα, συστήματα με τα οποία διασυνδέεται, δεδομένα που επεξεργάζεται, διαδικασίες που επηρεάζει.
- **Ορισμός επιτρεπόμενου σκοπού, απαγορευμένων χρήσεων και επιπέδου αυτονομίας του agent** (κλίμακα L0–L4), με ανθρώπινη έγκριση για κρίσιμες ή μη αναστρέψιμες ενέργειες (αποστολή δεσμευτικού περιεχομένου, διαγραφή δεδομένων, πληρωμές, εργασιακές αποφάσεις).
- **Τεχνική ταυτότητα agent με αρχή ελάχιστου προνομίου,** σαφής δήλωση ταυτότητας ΤΝ προς τρίτους, πιλοτική λειτουργία σε ελεγχόμενο δοκιμαστικό περιβάλλον της επιχείρησης (technical sandbox), πλήρες logging/audit trail, kill switch και διαδικασία rollback.

Αναλυτική διαδικασία 11 βημάτων, κίνδυνοι και παραδείγματα: Παράρτημα IV.

5.Έλεγχος υπαγωγής: για κάθε σύστημα εξετάζεται αν εμπίπτει στον ορισμό «σύστημα ΤΝ» του Κανονισμού.

Οι AI agents πρέπει να αντιμετωπίζονται ως ψηφιακοί ρόλοι / συνεργάτες με σαφή ιδιοκτήτη, δικαιώματα, καθήκοντα, περιορισμούς και μηχανισμούς ελέγχου, προσέγγιση που επιτρέπει την ασφαλή χρήση τους και την επίβλεψη της ορθής λειτουργίας τους, χωρίς να εμποδίζει την καινοτομία.

ΕΥΘΥΝΗ

- **Υπεύθυνος Συμμόρφωσης:** Συντονισμός εργασιών διαδικασίας.
- **Επιχειρησιακοί Υπεύθυνοι:** Καταγραφή όλων των συστημάτων ΤΝ που χρησιμοποιούνται και/ή αναπτύσσονται. Επίβλεψη ορθής παραγωγικής λειτουργίας κάθε συστήματος και AI agent.
- **Τεχνικοί Υπεύθυνοι:** Διαχείριση τεχνικών ταυτοτήτων και δικαιωμάτων των AI agents. Ευθύνη ασφαλούς διασύνδεσης με λοιπά εταιρικά συστήματα.
- **Επιτροπή Διακυβέρνησης ΤΝ:** Έγκριση Μητρώου ΤΝ.

ΕΡΓΑΛΕΙΑ & ΤΕΚΜΗΡΙΩΣΗ

Τεκμήριο / εργαλείο	Περιγραφή
Μητρώο συστημάτων ΤΝ (AI inventory)	Ανά εγγραφή: σκοπός, ρόλος επιχείρησης, κατηγορία κινδύνου, δεδομένα, προμηθευτής, ιδιοκτήτης, δικλίδες. Καταγραφή κάθε agent με επίπεδο αυτονομίας, εγκρίσεις και περιορισμούς. Επικαιροποιείται σε κάθε ουσιώδη μεταβολή[6].
Ερωτηματολόγιο χαρτογράφησης	Τυποποιημένη φόρμα συλλογής στοιχείων ανά τμήμα, ώστε η πληροφορία να είναι συστηματική και συγκρίσιμη.
Τεκμηρίωση ελέγχου ορισμού	Αιτιολόγηση, ανά σύστημα, της κρίσης περί υπαγωγής ή μη στον ορισμό «σύστημα ΤΝ».
Audit trail ενεργειών agent	Εντολές, tool calls, εγκρίσεις, εκτελεσθείσες ενέργειες, αποτυχίες, έκδοση μοντέλου.

ΧΡΟΝΟΣ ΕΚΤΕΛΕΣΗΣ

- Άμεσα: έναρξη χαρτογράφησης· ολοκλήρωση πρώτης πλήρους απογραφής εντός 2–4 μηνών.
- Διαρκώς: κάθε νέο εργαλείο περνά από την ίδια διαδικασία πριν την παραγωγική χρήση.
- Πριν από την παραγωγική χρήση κάθε agent: καταγραφή, ορισμός αυτονομίας, sandbox δοκιμές. Περιοδική επανεξέταση σε κάθε αλλαγή μοντέλου, εργαλείων, δεδομένων ή σκοπού.

[6]Κάθε αλλαγή η οποία ενδέχεται να μεταβάλει τις υποχρεώσεις συμμόρφωσης βάσει του Κανονισμού.
Πχ. εισαγωγή νέου συστήματος ΤΝ ή απόσυρση υφισταμένου, αλλαγή σκοπού χρήσης, ενσωμάτωση νέων λειτουργιών ΤΝ, χρήση νέων κατηγοριών δεδομένων, ένταξη του συστήματος σε διαδικασία που ενδέχεται να εμπίπτει σε χρήση υψηλού κινδύνου.

ΔΙΑΔΙΚΑΣΙΑ **No3**

Ταξινόμηση Κινδύνου & Προσδιορισμός Ρόλου



ΣΚΟΠΟΣ

Η αξιολόγηση και κατάταξη κάθε συστήματος ΤΝ στην κατάλληλη κατηγορία κινδύνου και ο προσδιορισμός του ρόλου της επιχείρησης ως προς αυτό, ώστε να καθοριστούν οι εφαρμοστέες υποχρεώσεις.

ΒΗΜΑΤΑ

1. **Έλεγχος για απαγορευμένες πρακτικές.** Πριν από κάθε ανάπτυξη, προμήθεια ή εμπορική αξιοποίηση ενός συστήματος ΤΝ, προηγείται **νομικός έλεγχος** ως προς το ότι η σκοπούμενη χρήση του συστήματος δεν είναι, εξαρχής, απαγορευμένη.
2. **Συνεντεύξεις με τους ιδιοκτήτες κάθε συστήματος:**
   - Επιχειρησιακός Υπεύθυνος: σκοπός χρήσης και επιχειρησιακός αντίκτυπος.
   - Τεχνικός Υπεύθυνος: τεχνική αρχιτεκτονική, λειτουργία, δεδομένα.
   - Υπεύθυνος Συμμόρφωσης: εφαρμοστέο κανονιστικό πλαίσιο, υποχρεώσεις συμμόρφωσης.

   Συμπληρωματικά Q&A για συστήματα στα όρια μεταξύ κατηγοριών.
3. **Αξιολόγηση και κατάταξη κινδύνου:** εφαρμογή των κριτηρίων του Κανονισμού ώστε κάθε σύστημα να λάβει τελική ταξινόμηση. Πρέπει να υπάρχει **εσωτερικός μηχανισμός ταξινόμησης, ελέγχου και τεκμηρίωσης** των συστημάτων χρήσης ΤΝ εντός της κάθε επιχείρησης που να απαντά στα εξής βασικά ερωτήματα:
   - Πρόκειται πράγματι για σύστημα ΤΝ;
   - Ποια είναι η λειτουργία του συστήματος και για ποιους σκοπούς το χρησιμοποιεί η επιχείρηση;
   - Ποιος είναι ο ρόλος της επιχείρησης ως προς το συγκεκριμένο σύστημα;
   - Σε ποια κατηγορία κινδύνου εμπίπτει το σύστημα;
4. **Εξακρίβωση του ρόλου** που έχει η επιχείρηση σε σχέση με αυτό (πάροχος, φορέας εφαρμογής κλπ.) και αξιολόγηση κατά πόσον η χρήση, τροποποίηση ή περαιτέρω ανάπτυξη του συστήματος μπορεί να μεταβάλει τον ρόλο αυτό και να οδηγήσει σε πρόσθετες υποχρεώσεις συμμόρφωσης.
5. **Επικύρωση της ταξινόμησης** από τη δεύτερη γραμμή άμυνας (Compliance/Νομική Υπηρεσία) και καταχώριση στο μητρώο, με την αιτιολόγηση της απόφασης.

Η ύπαρξη ανθρώπου «στο τέλος» δεν αρκεί από μόνη της. Χρειάζεται πραγματική δυνατότητα κατανόησης, αμφισβήτησης, παράκαμψης ή διακοπής της λειτουργίας του συστήματος, ειδικά σε use cases που επηρεάζουν φυσικά πρόσωπα ή κρίσιμες λειτουργίες.

ΕΥΘΥΝΗ

- **Υπεύθυνος Συμμόρφωσης:** Συντονισμός και ευθύνη ταξινόμησης κινδύνου, σε στενή συνεργασία με τους Επιχειρησιακούς και Τεχνικούς Υπεύθυνους.
- **Νομική Υπηρεσία:** Έλεγχος απαγορευμένων πρακτικών με τη συνδρομή του DPO, όπου απαιτείται.
- **Επιτροπή Διακυβέρνησης ΤΝ:** Έγκριση κατάταξης κινδύνου.

ΕΡΓΑΛΕΙΑ & ΤΕΚΜΗΡΙΩΣΗ

Τεκμήριο / εργαλείο	Περιγραφή
AI inventory	Πλήρης κατάλογος εργαλείων και εφαρμογών ΤΝ.
Τυποποιημένη φόρμα αξιολόγησης	Κοινά κριτήρια για κάθε νέα χρήση ΤΝ, με συμμετοχή τεχνικών, κανονιστικών και επιχειρησιακών τμημάτων.
Τεκμηρίωση κατάταξης κινδύνου	Αποτελέσματα της αξιολόγησης και κατηγοριοποίησης του επιπέδου κινδύνου του αντίστοιχου συστήματος βάσει των κατηγοριών κινδύνου του Κανονισμού και αιτιολόγηση απόφασης ανά σύστημα.
Χαρτογράφηση ρόλων ανά σύστημα	Καταγραφή ρόλου (πάροχος, φορέας εφαρμογής κλπ.) και της συλλογιστικής προσδιορισμού του.

ΧΡΟΝΟΣ ΕΚΤΕΛΕΣΗΣ

- Μετά την ολοκλήρωση της πρώτης χαρτογράφησης (Διαδικασία Νο2) και πριν από κάθε νέα προμήθεια, ανάπτυξη ή ουσιώδη αλλαγή.
- Επανεξέταση: σε κάθε νέα έκδοση, αλλαγή προμηθευτή, νέα λειτουργία ή αλλαγή σκοπού χρήσης.

ΔΙΑΔΙΚΑΣΙΑ **No4**

Υλοποίηση Υποχρεώσεων Συμμόρφωσης (ανά ρόλο & κατηγορία κινδύνου)



ΣΚΟΠΟΣ

Ο προσδιορισμός και η υλοποίηση των συγκεκριμένων υποχρεώσεων που ενεργοποιούνται για κάθε σύστημα, με βάση την ταξινόμηση κινδύνου και τον ρόλο της επιχείρησης.

ΒΗΜΑΤΑ

1. **Εντοπισμός των εφαρμοστέων υποχρεώσεων ανά σύστημα:** για κάθε σύστημα προσδιορίζεται με ακρίβεια ποιες υποχρεώσεις ισχύουν (π.χ. τεχνική τεκμηρίωση και σύστημα διαχείρισης κινδύνου για συστήματα υψηλού κινδύνου, υποχρεώσεις διαφάνειας για συστήματα περιορισμένου κινδύνου).
2. **Κατάρτιση σχεδίου δράσης (action plan):** προτεραιοποίηση ενεργειών με βάση τον κίνδυνο, τους διαθέσιμους πόρους και τις προθεσμίες που θέτει ο Κανονισμός, με σαφή ανάθεση ευθυνών ανά τμήμα.
3. **Για συστήματα υψηλού κινδύνου όπου η επιχείρηση είναι πάροχος:** σύστημα διαχείρισης κινδύνου σε όλον τον κύκλο ζωής του συστήματος, διακυβέρνηση και ποιότητα δεδομένων, τεχνικός φάκελος, τήρηση αρχείων καταγραφής (logs) για τουλάχιστον έξι (6) μήνες, σχεδιασμός ανθρώπινης εποπτείας, διασφάλιση επαρκούς ακρίβειας, ανθεκτικότητας και κυβερνοασφάλειας, αξιολόγηση συμμόρφωσης, δήλωση συμμόρφωσης ΕΕ, σήμανση CE, καταχώριση στη βάση δεδομένων της ΕΕ και σύστημα παρακολούθησης της λειτουργίας μετά τη διάθεση στην αγορά.
4. **Για συστήματα υψηλού κινδύνου όπου η επιχείρηση είναι φορέας εφαρμογής:** χρήση σύμφωνα με τις οδηγίες του παρόχου, μέτρα ανθρώπινης εποπτείας από καταρτισμένα πρόσωπα, ενημέρωση εργαζομένων/επηρεαζόμενων προσώπων για χρήση ΤΝ και παροχή εξηγήσεων για αποφάσεις που τους αφορούν, παρακολούθηση λειτουργίας και αναφορά σοβαρών περιστατικών, τήρηση logs για τουλάχιστον 6 μήνες και, όπου απαιτείται, Εκτίμηση Αντικτύπου στα Θεμελιώδη Δικαιώματα (FRIA) πριν από την πρώτη χρήση.
5. **Για συστήματα περιορισμένου κινδύνου με υποχρεώσεις διαφάνειας:** ενημέρωση προσώπων που αλληλοεπιδρούν με ΤΝ, τεχνική επισήμανση deepfakes/συνθετικού περιεχομένου, ενημέρωση προσώπων που εκτίθενται σε αναγνώριση συναισθημάτων ή βιομετρική κατηγοριοποίηση (βλ. άρθρο 50). Οι ενημερώσεις παρέχονται σε εμφανές σημείο, χωρίς να «κρύβονται» σε εκτενείς όρους χρήσης.

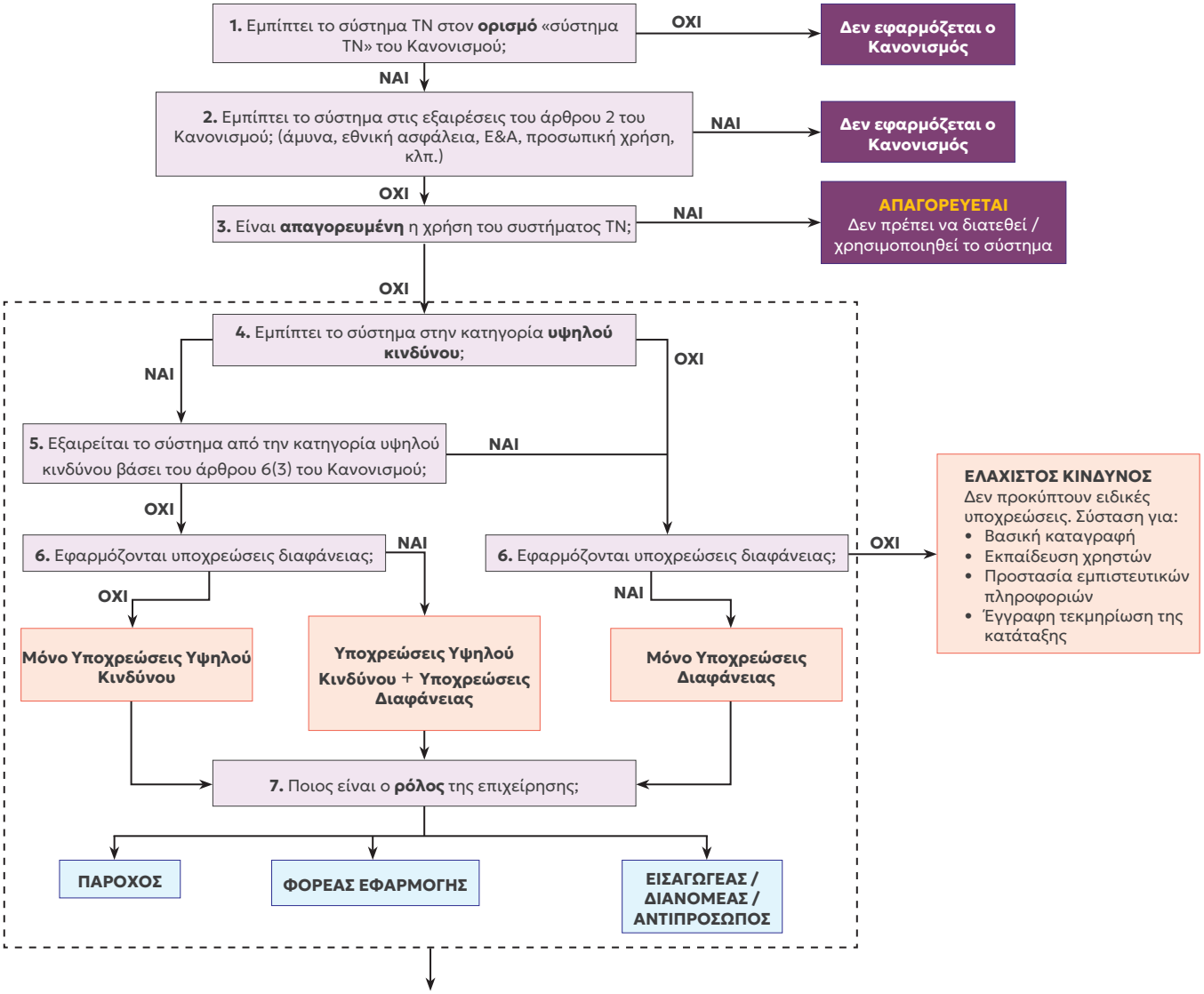
6. **Για συστήματα ελάχιστου κινδύνου:** συστάσεις για βασική καταγραφή, εκπαίδευση χρηστών, προστασία εμπιστευτικών πληροφοριών και έγγραφη τεκμηρίωση των λόγων κατάταξης.
7. **Οριστικοποίηση, έγκριση από τη Διοίκηση** και θέση σε ισχύ πολιτικών, διαδικασιών και γνωστοποιήσεων (notices) προς εργαζομένους, πελάτες ή το κοινό.

ΕΥΘΥΝΗ

- **Υπεύθυνος Συμμόρφωσης:** Προσδιορισμός εφαρμοστέων υποχρεώσεων σε συνεργασία με Επιχειρησιακούς και Τεχνικούς Υπεύθυνους.
- **Νομική Υπηρεσία:** Έλεγχος εφαρμοστέων υποχρεώσεων με τη συνδρομή του DPO, όπου απαιτείται.
- **Επιτροπή Διακυβέρνησης ΤΝ:** Έγκριση εφαρμοστέων υποχρεώσεων ανά μεμονωμένο σύστημα ΤΝ.
- **Διοικητικό Συμβούλιο:** Φέρει την τελική, συλλογική λογοδοσία για την επάρκεια του σχεδίου συμμόρφωσης (βλ. Διαδικασία 1 ως προς το ζήτημα των ευθυνών).

i

Ο ρόλος του Διοικητικού Συμβουλίου είναι εποπτικός, όχι εκτελεστικός:
- έχει ήδη εγκρίνει τη στρατηγική/πολιτική ΤΝ, καθώς και το πόσο κίνδυνο είναι διατεθειμένη να αναλάβει η επιχείρηση,
- λαμβάνει περιοδική ενημέρωση για συστήματα υψηλού κινδύνου, σχέδια δράσης και τυχόν αποκλίσεις συμμόρφωσης και
- φέρει την τελική, συλλογική λογοδοσία για την επάρκεια του πλαισίου διακυβέρνησης ΤΝ.



Εντοπισμός εφαρμοστέων υποχρεώσεων

	Υψηλός κίνδυνος	Περιορισμένος κίνδυνος
Πάροχος	• Σύστημα διαχείρισης κινδύνου • Διακυβέρνηση και ποιότητα δεδομένων • Τεχνικός φάκελος • Τήρηση αρχείων καταγραφής • Σχεδιασμός ανθρώπινης εποπτείας • Διασφάλιση επαρκούς ακρίβειας, ανθεκτικότητας και κυβερνοασφάλειας • Αξιολόγηση συμμόρφωσης • Δήλωση συμμόρφωσης ΕΕ • Σήμανση CE • Καταχώριση στη βάση δεδομένων της ΕΕ • Σύστημα παρακολούθησης της λειτουργίας μετά τη διάθεση στην αγορά	• Ενημέρωση χρηστών ότι αλληλοεπιδρούν με ΤΝ • Τεχνική επισήμανση συνθετικού περιεχομένου και deepfakes

Σχήμα 3: Δέντρο αποφάσεων για τον προσδιορισμό των εφαρμοστέων υποχρεώσεων.

Φορέας εφαρμογής	• Χρήση σύμφωνα με τις οδηγίες του παρόχου • Διασφάλιση ανθρώπινης εποπτείας από εκπαιδευμένο προσωπικό • Ενημέρωση εργαζομένων και επηρεαζόμενων προσώπων για χρήση ΤΝ / εξήγηση για τις αποφάσεις που τους αφορούν • Παρακολούθηση λειτουργίας και αναφορά προβλημάτων • Τήρηση αρχείων καταγραφής • FRIA όπου απαιτείται	• Ενημέρωση προσώπων που εκτίθενται σε αναγνώριση συναισθημάτων ή βιομετρική κατηγοριοποίηση • Γνωστοποίηση ότι το περιεχόμενο αποτελεί deepfake • Γνωστοποίηση χρήσης περιεχομένου παραγόμενου από ΤΝ σε δημοσιευμένο κείμενο σε θέματα δημόσιου συμφέροντος
Εισαγωγέας / Διανομέας / Αντιπρόσωπος	• Επιβεβαίωση ότι ο πάροχος έχει αναπτύξει τεχνική τεκμηρίωση και είναι διαθέσιμη • Δήλωση συμμόρφωσης ΕΕ • Σήμανση CE • Οδηγίες χρήσης	

ΕΡΓΑΛΕΙΑ & ΤΕΚΜΗΡΙΩΣΗ

Τεκμήριο / εργαλείο	Περιγραφή
Σχέδιο δράσης συμμόρφωσης	Ενέργειες, υπεύθυνοι, προθεσμίες, προτεραιοποίηση βάσει κινδύνου.
Τεχνικός φάκελος (πάροχοι)	Σκοπός, σχεδιασμός, σύνολα δεδομένων, αρχιτεκτονική, δείκτες, αποτελέσματα δοκιμών, μέτρα εποπτείας.
FRIA / DPIA	Όπου απαιτείται, το Fundamental Rights Impact Assessment συμπληρώνει το Data Protection Impact Assessment.
Σχέδιο ανθρώπινης εποπτείας	Ποιος εποπτεύει, με ποιες αρμοδιότητες και δικαίωμα παρέμβασης, πώς εκπαιδεύτηκε.
Γνωστοποιήσεις διαφάνειας	Κείμενα ενημέρωσης χρηστών, εργαζομένων και επηρεαζόμενων προσώπων.
Αρχεία καταγραφής (logs)	Αυτόματη καταγραφή γεγονότων, για παρόχους και φορείς εφαρμογής συστημάτων υψηλού κινδύνου, τήρηση τουλάχιστον 6 μηνών.

ΧΡΟΝΟΣ ΕΚΤΕΛΕΣΗΣ

- Άμεσα: υποχρεώσεις ήδη σε ισχύ (απαγορευμένες πρακτικές και AI literacy από 2.2.2025, διαφάνεια άρθρου 50 από 2.8.2026).
- Έως 2.12.2027 / 2.8.2028: πλήρης συμμόρφωση για συστήματα υψηλού κινδύνου (Παράρτημα III / Παράρτημα I του Κανονισμού αντίστοιχα), με έγκαιρη έναρξη λόγω του απαιτούμενου χρόνου προετοιμασίας 12–24 μηνών.

ΔΙΑΔΙΚΑΣΙΑ **No5**

Εκπαίδευση & AI Literacy



ΣΚΟΠΟΣ

Λήψη οργανωτικών και εκπαιδευτικών μέτρων για την υποστήριξη της ανάπτυξης γνώσεων και δεξιοτήτων ΤΝ (άρθρο 4 του Κανονισμού), ώστε όσοι επιλέγουν, προμηθεύονται, σχεδιάζουν, επιβλέπουν ή χρησιμοποιούν συστήματα ΤΝ να κατανοούν τις δυνατότητες, τους περιορισμούς και τους κινδύνους τους.

ΒΗΜΑΤΑ

1. **Δημιουργία κοινού επιπέδου γνώσης για όλους τους εργαζόμενους που χρησιμοποιούν ή επηρεάζονται από ΤΝ:** βασικές έννοιες (σύστημα ΤΝ, GenAI, hallucination, bias, prompt, προσωπικά δεδομένα, ανθρώπινη εποπτεία), με σύντομα e-learning modules και πρακτικά παραδείγματα.
2. **Εκπαίδευση ανά ρόλο και επίπεδο κινδύνου:** διαφορετικό περιεχόμενο για Διοίκηση, business owners, τελικούς χρήστες, τεχνικές ομάδες, Legal/Compliance/DPO, HR, Procurement.
3. **Σύνδεση της εκπαίδευσης με τα πραγματικά AI use cases** της επιχείρησης και τον κίνδυνο κάθε χρήσης, όχι γενικόλογα σεμινάρια.
4. **Ενεργή και ορατή στήριξη από την ηγεσία:** σαφές μήνυμα «χρησιμοποιήστε παραγωγικά την ΤΝ με κανόνες, έλεγχο και λογοδοσία», σύνδεση της υιοθέτησης με επιχειρησιακούς στόχους, επιβράβευση της υπεύθυνης χρήσης και της έγκαιρης αναφοράς προβλημάτων.
5. **Δημιουργία δικτύου AI Champions[7] ανά βασική λειτουργία:** σημεία αναφοράς για ασφαλή χρήση, συλλογή ερωτήσεων, διάδοση καλών πρακτικών και έγκαιρη αναγνώριση νέων ή ανεπίσημων χρήσεων.
6. **Συνεδρίες ερωτήσεων-απαντήσεων (Q&As):** Παρέχουν τη δυνατότητα υποβολής ερωτημάτων και διευκρίνισης γκρίζων ζωνών, ενισχύοντας την ουσιαστική κατανόηση των νέων κανόνων πέρα από την τυπική ενημέρωση.

[7]Οι AI Champions είναι εργαζόμενοι από διαφορετικά τμήματα που λειτουργούν ως πρεσβευτές της ΤΝ μέσα στην ομάδα τους. Δεν είναι απαραίτητα τεχνικοί – είναι ενθουσιώδεις, ικανοί και αξιόπιστοι στο τμήμα τους.

7. **Ενσωμάτωση στις πρακτικές λήψης αποφάσεων της διοίκησης:** στις συναντήσεις διοίκησης και στις εγκρίσεις νέων συστημάτων τίθενται συστηματικά τα ερωτήματα: ποιο πρόβλημα λύνει το use case, ποιοι επηρεάζονται, ποια δεδομένα χρησιμοποιούνται, ποιος ελέγχει το αποτέλεσμα, ποια τεκμήρια υπάρχουν.
8. **Χαρτογράφηση δεξιοτήτων σε τρία επίπεδα** (βασικό, προχωρημένο επιχειρησιακό, εξειδικευμένο) και απόφαση για το ποιες δεξιότητες αναπτύσσονται εσωτερικά, τι καλύπτεται με προσλήψεις και τι μέσω συνεργατών.

ΕΥΘΥΝΗ

- **Διοίκηση:** έγκριση πολιτικής και πόρων, δημιουργία και διατήρηση κουλτούρας υπεύθυνης, ασφαλούς και σύμφωνης με τους κανόνες χρήσης της ΤΝ σε όλο τον οργανισμό.
- **Υπεύθυνος Ανθρώπινου Δυναμικού (HR):** σχεδιασμός, υλοποίηση και συντονισμός των δράσεων του εκπαιδευτικού πλάνου, τήρηση αρχείων και reporting.
- **Επιτροπή Διακυβέρνησης ΤΝ:** παρακολούθηση & αξιολόγηση δράσεων.
- **Επιχειρησιακοί υπεύθυνοι:** εκπαίδευση χρηστών στις λειτουργίες των συστημάτων.
- **AI Champions:** ενημέρωση συναδέλφων, υποστήριξη πρώτης γραμμής, συλλογή feedback, εντοπισμός use cases.

ΕΡΓΑΛΕΙΑ & ΤΕΚΜΗΡΙΩΣΗ

Τεκμήριο / εργαλείο	Περιγραφή
AI Literacy Plan	Πλάνο εκπαίδευσης ανά ρόλο: συχνότητα, περιεχόμενο, υπεύθυνοι, παρακολούθηση.
Role-Based Training Matrix	Αντιστοίχιση κάθε ομάδας χρηστών με τις απαιτούμενες γνώσεις.
Αρχεία εκπαίδευσης	Συμμετοχές, ολοκληρώσεις, αξιολογήσεις, επικαιροποιήσεις, αποδεικτικά για ελέγχους.
Οδηγίες ασφαλούς χρήσης GenAI	Πρακτικοί κανόνες για prompts, εμπιστευτικά δεδομένα, έλεγχο αποτελεσμάτων.

ΧΡΟΝΟΣ ΕΚΤΕΛΕΣΗΣ

- Άμεσα (υποχρέωση ήδη σε ισχύ από 2.2.2025): βασική ενημέρωση όλων για επιτρεπόμενες/μη επιτρεπόμενες χρήσεις.
- Πριν από κάθε νέα παραγωγική χρήση: εκπαίδευση των χρηστών του συστήματος.
- Κατά το onboarding: βασικό AI literacy για νέους εργαζομένους.
- Περιοδικά (τουλάχιστον ετησίως) και ad hoc μετά από νέο εργαλείο, περιστατικό ή αλλαγή κανονιστικού πλαισίου.

ΔΙΑΔΙΚΑΣΙΑ **Νο6**

Διαχείριση Προμηθευτών



ΣΚΟΠΟΣ

Η ενσωμάτωση των απαιτήσεων του Κανονισμού στις διαδικασίες προμήθειας και στη χρήση συστημάτων τρίτων.

ΒΗΜΑΤΑ

1. **Εμπλουτισμός των διαδικασιών προμηθειών με ερωτηματολόγια δέουσας επιμέλειας για ΤΝ και συμβατικές ρήτρες:** παροχή πληροφοριών και τεκμηρίωσης, συνεργασία σε περιστατικά και εποπτικούς ελέγχους, μη χρήση εταιρικών δεδομένων για εκπαίδευση μοντέλων χωρίς συμφωνία.
2. **Έλεγχοι για εισαγωγείς/διανομείς:** επιβεβαίωση ότι ο πάροχος έχει αναπτύξει και διαθέτει τεχνική τεκμηρίωση, οδηγίες χρήσης, δηλώσεις συμμόρφωσης και σήμανση, πριν τη διάθεση στην αγορά.
3. **Οριοθέτηση παραμετροποίησης:** εσωτερικές οδηγίες για το τι επιτρέπεται να αλλάξει στη χρήση ή τη λειτουργία ενός συστήματος τρίτου και ποια αλλαγή απαιτεί εκ νέου αξιολόγηση, καθώς ουσιώδης τροποποίηση του συστήματος ή η διάθεση του σε χρήστες υπό την επωνυμία ή/και τα εμπορικά σήματα της επιχείρησης ενδέχεται να καταστήσει την επιχείρηση πάροχο (άρθρο 25 Κανονισμού, βλ. Ενότητα Γ, Σημείο 4).

ΕΥΘΥΝΗ

- **Υπεύθυνος Προμηθειών:** ενσωμάτωση απαιτήσεων διακυβέρνησης, ασφάλειας, διαφάνειας και διαχείρισης κινδύνων ΤΝ σε αξιολογήσεις προμηθευτών και συμβάσεις.
- **Επιχειρησιακός Υπεύθυνος:** καθορισμός του σκοπού χρήσης και των λειτουργικών/επιχειρησιακών απαιτήσεων του νέου συστήματος ή AI agent, συμμετοχή στην αξιολόγηση της καταλληλότητας του προμηθευτή.
- **Υπεύθυνος Συμμόρφωσης:** Έγκριση -πριν την ολοκλήρωση της προμήθειας- ότι η λύση καλύπτει την επιχειρησιακή ανάγκη εντός των εγκεκριμένων ορίων κινδύνου.
- **Τεχνικός Υπεύθυνος:** έλεγχος πληρότητας του τεχνικού φακέλου και των μέτρων ασφαλείας του παρόχου, καθορισμός των τεχνικών ορίων παραμετροποίησης και ασφαλής τεχνική ένταξη του συστήματος πριν τη θέση σε παραγωγική χρήση.
- **Νομική Υπηρεσία:** ρήτρες σύμβασης και έλεγχος ρόλου (πάροχος / φορέας εφαρμογής / εισαγωγέας-διανομέας).
- **Επιτροπή Διακυβέρνησης ΤΝ:** τελική έγκριση

Είναι σημαντικό οι υπεύθυνοι να μην περιορίζονται στην εμπορική περιγραφή του προμηθευτή. Η πραγματική νομική αξιολόγηση εξαρτάται από τον τρόπο λειτουργίας του συστήματος και, κυρίως, τον τρόπο χρήσης του από την ίδια την επιχείρηση.

Παράδειγμα: Ένα εργαλείο αξιολόγησης βιογραφικών για προσλήψεις εξετάζεται προσεκτικά, καθώς τα συστήματα ΤΝ στην απασχόληση θεωρούνται συνήθως υψηλού κινδύνου βάσει του Παραρτήματος ΙΙΙ και υπόκεινται σε αυξημένες υποχρεώσεις τεκμηρίωσης και εποπτείας.

ΕΡΓΑΛΕΙΑ & ΤΕΚΜΗΡΙΩΣΗ

Τεκμήριο / εργαλείο	Περιγραφή
Vendor AI Questionnaire	Ερωτηματολόγιο προς προμηθευτές: δεδομένα εκπαίδευσης, logs, ανθρώπινη εποπτεία, δικαιώματα audit, υποστήριξη σε περιστατικά.
Συμβατικές ρήτρες ΤΝ	Αποδεικτικά ελέγχου δέουσας επιμέλειας για προμηθευτές και όροι συμβάσεων για προμηθευτές ΤΝ. Τεκμηρίωση και ενημέρωση για ουσιώδεις αλλαγές, συνεργασία με αρχές, όροι χρήσης δεδομένων.

ΧΡΟΝΟΣ ΕΚΤΕΛΕΣΗΣ

- Άμεσα: ενσωμάτωση ερωτηματολογίων και ρητρών σε κάθε νέα προμήθεια.

ΔΙΑΔΙΚΑΣΙΑ No7

Παρακολούθηση, Εποπτεία & Διαχείριση Περιστατικών



ΣΚΟΠΟΣ

Η διατήρηση της συμμόρφωσης σε βάθος χρόνου, η ετοιμότητα απέναντι σε ελέγχους και καταγγελίες και η έγκαιρη διαχείριση περιστατικών ΤΝ[8] και σοβαρών αποκλίσεων[9].

ΒΗΜΑΤΑ

1. **Καθορισμός λειτουργικών ελέγχων ανά σύστημα:** ακρίβεια, ποσοστά σφαλμάτων ανά ομάδες πληθυσμού, ποσοστό "μετατόπισης" της απόδοσης του μοντέλου ΤΝ με την πάροδο του χρόνου, αριθμός αναφορών, αποκλίσεις από οδηγίες χρήσης.
2. **Συνεχής παρακολούθηση μετά τη θέση σε λειτουργία**, με δείκτες που ενεργοποιούν επανεξέταση. Προτεινόμενοι δείκτες:
   - συστηματικά λανθασμένα στοιχεία εξόδου,
   - αυξημένος αριθμός αναφορών,
   - δυσμενείς επιπτώσεις σε συγκεκριμένες κατηγορίες προσώπων,
   - διαπιστωμένες αποκλίσεις από τις οδηγίες χρήσης,
   - νέα δεδομένα για τους περιορισμούς του συστήματος.
3. **Διαδικασία διαχείρισης περιστατικών:** ένα περιστατικό ΤΝ ή σοβαρή απόκλιση δεν αντιμετωπίζεται μόνο ως τεχνικό πρόβλημα / σφάλμα, αλλά ως πιθανό συμβάν με νομικές απαιτήσεις και συνέπειες.
   - Για συστήματα υψηλού κινδύνου:
     - Πάροχος: υποβάλλει αναφορά σοβαρού περιστατικού στην αρμόδια αρχή εποπτείας (εντός 15, 10 ή 2 ημερών, ανάλογα με τη σοβαρότητα του περιστατικού). Ακολούθως, προβαίνει σε εκτίμηση κινδύνου του περιστατικού και λήψη διορθωτικών μέτρων.
     - Φορέας εφαρμογής: ενημερώνει χωρίς καθυστέρηση πάροχο/διανομέα και την αρχή εποπτείας και αναστέλλει τη χρήση όταν διαπιστώνει σοβαρό κίνδυνο.
   - Για συστήματα περιορισμένου και ελάχιστου κινδύνου: Δεν προβλέπεται στον Κανονισμό υποχρέωση αναφοράς περιστατικών. Συστήνεται η εσωτερική καταγραφή και αξιολόγηση του περιστατικού, με σκοπό τη λήψη διορθωτικών μέτρων.

[8]Περιστατικό ΤΝ: κάθε γεγονός ή δυσλειτουργία κατά τη λειτουργία συστήματος ΤΝ που μπορεί να οδηγήσει σε ανεπιθύμητο αποτέλεσμα, παραβίαση απαιτήσεων συμμόρφωσης ή πρόκληση βλάβης σε φυσικά πρόσωπα, οργανισμούς ή περιουσιακά στοιχεία.

[9]Σοβαρή απόκλιση: σημαντική και μη προβλεπόμενη απόκλιση της συμπεριφοράς ή των επιδόσεων του συστήματος από τις τεχνικές προδιαγραφές, τον προβλεπόμενο σκοπό, τις οδηγίες χρήσης ή τις απαιτήσεις συμμόρφωσης, η οποία μπορεί να οδηγήσει σε σοβαρό περιστατικό ή σε μη συμμόρφωση με τον Κανονισμό.

4. **Διαδικασία αντίδρασης σε αίτημα αρχής ή καταγγελία:** καταγραφή αιτήματος, ταυτοποίηση συστήματος και ρόλου, ενεργοποίηση ομάδας απόκρισης, διατήρηση αποδεικτικών (logs, εκδόσεις, approvals), αξιολόγηση για το αν η χρήση πρέπει να περιοριστεί ή να ανασταλεί, συγκρότηση φακέλου τεκμηρίωσης, εγκεκριμένη απάντηση, lessons learned (αναλυτικός πίνακας βημάτων: Ενότητα Ε).
5. **Παρακολούθηση κανονιστικών και τεχνικών εξελίξεων:** επικαιροποίηση του εσωτερικού πλαισίου καθώς εκδίδονται κατευθυντήριες γραμμές, εναρμονισμένα πρότυπα, ερμηνευτικές οδηγίες, και εντοπίζονται νέες ευπάθειες ή αδυναμίες των χρησιμοποιούμενων συστημάτων/μοντέλων.
6. **Περιοδική αναφορά προς τη Διοίκηση:** αριθμός και είδος συστημάτων, κατηγορίες κινδύνου, ανοιχτά ευρήματα, διορθωτικές ενέργειες.

ΕΥΘΥΝΗ

- **Υπεύθυνος Συμμόρφωσης:** συντονισμός εποπτείας, επαφή με αρχές.
- **Επιχειρησιακός Υπεύθυνος:** παρακολούθηση λειτουργίας, αναφορά αποκλίσεων.
- **Τεχνικός Υπεύθυνος:** logs, monitoring, ασφάλεια.
- **Νομική Υπηρεσία:** αξιολόγηση υποχρεώσεων αναφοράς, εγκρίσεις απαντήσεων.
- **Εσωτερικός Έλεγχος:** περιοδικοί ανεξάρτητοι έλεγχοι.

ΕΡΓΑΛΕΙΑ & ΤΕΚΜΗΡΙΩΣΗ

Τεκμήριο / εργαλείο	Περιγραφή
Monitoring dashboard / δείκτες	Μετρήσιμοι δείκτες λειτουργίας ανά σύστημα και όρια ενεργοποίησης επανεξέτασης.
Μητρώο περιστατικών & αναφορών	Αρχεία καταγραφής περιστατικών, αναφορές συμβάντων, διορθωτικές ενέργειες, στοιχεία παρακολούθησης μετά τη θέση σε λειτουργία, όπου απαιτούνται, αναφορές σε αρχές.
Φάκελος ετοιμότητας ελέγχου	Οργανωμένα ανά υποχρέωση τα στοιχεία που μπορεί να ζητήσει εποπτική αρχή (βλ. Ενότητα Ε).
Εκθέσεις προς τη Διοίκηση	Περιοδικό reporting με ευρήματα, κενά και επόμενα βήματα.

ΧΡΟΝΟΣ ΕΚΤΕΛΕΣΗΣ

- Σε συνεχή βάση, από τη θέση κάθε συστήματος σε λειτουργία.
- Άμεση ενεργοποίηση σε κάθε περιστατικό, καταγγελία ή αίτημα αρχής.
- Περιοδική αναφορά προς τη Διοίκηση τουλάχιστον ανά τρίμηνο.

Γ.
ΣΗΜΕΙΑ ΠΡΟΣΟΧΗΣ: ΠΟΥ ΔΗΜΙΟΥΡΓΕΙΤΑΙ ΣΥΓΧΥΣΗ ΣΤΗΝ ΠΡΑΞΗ



Η ενότητα αυτή δεν επαναλαμβάνει συστάσεις συμμόρφωσης. Καταγράφει τα σημεία του ίδιου του Κανονισμού των οποίων η ερμηνεία απαιτεί περαιτέρω εξειδίκευση, είτε επειδή οι σχετικές νομοθετικές προβλέψεις δεν μπορούν να εφαρμοστούν με οριζόντιο τρόπο σε όλες τις περιπτώσεις, είτε επειδή εκκρεμούν κατευθυντήριες γραμμές και εναρμονισμένα πρότυπα. Στα σημεία αυτά είναι πιθανές αποκλίνουσες ερμηνείες μεταξύ επιχειρήσεων, προμηθευτών και εποπτικών αρχών, αντιδικίες στην αλυσίδα αξίας και, ενδεχομένως, δικαστικές διαμάχες. Για κάθε σημείο αποτυπώνεται τι ορίζει ο νόμος, τι παραμένει αδιευκρίνιστο και πού μπορεί να οδηγήσει η ασάφεια.

1. Ορισμός «συστήματος ΤΝ» (άρθρο 3 παρ. 1): τα όρια της «συναγωγής»

Τι ορίζει ο νόμος: Κρίσιμο στοιχείο του ορισμού είναι η ικανότητα του συστήματος να «συνάγει» από τα δεδομένα εισόδου πώς να παράγει αποτελέσματα, σε αντιδιαστολή με την εκτέλεση προκαθορισμένων κανόνων.
Τι παραμένει αδιευκρίνιστο: Οι Κατευθυντήριες Γραμμές της Επιτροπής για τον ορισμό είναι ενδεικτικές και μη δεσμευτικές, και αφήνουν γκρίζα ζώνη για κάποιες κατηγορίες συστημάτων στα όρια της εφαρμογής. Σε κάποιες περιπτώσεις δεν υπάρχει απόλυτα αντικειμενική κρίση για το πού ακριβώς σταματά ο «απλός» αλγόριθμος και αρχίζει το «σύστημα ΤΝ».
Πού μπορεί να οδηγήσει: Η έλλειψη επαρκών αντικειμενικών κριτηρίων και πληροφορίας για την ερμηνεία αυτών των οριακών περιπτώσεων μπορεί να οδηγήσει κάποια επιχείρηση στο να μην αναγνωρίσει σωστά το αν κάποιο σύστημά της αποτελεί ή όχι, από νομική σκοπιά, σύστημα ΤΝ. Όμως, ο χαρακτηρισμός είναι το σημείο εκκίνησης κάθε υποχρέωσης, συνεπώς, τυχόν εσφαλμένη κρίση «εκτός πεδίου» συμπαρασύρει το σύνολο της συμμόρφωσης.

2. Απαγορευμένες πρακτικές (άρθρο 5): αόριστες έννοιες με τα βαρύτερα πρόστιμα

Τι ορίζει ο νόμος: Απαγορεύονται, μεταξύ άλλων, συστήματα που χρησιμοποιούν «παραπλανητικές ή υποσυνείδητες τεχνικές» για να επηρεάσουν «ουσιωδώς» τη συμπεριφορά, που «εκμεταλλεύονται ευαλωτότητες» προσώπων, καθώς και η «αναγνώριση συναισθημάτων» στον χώρο εργασίας.
Τι παραμένει αδιευκρίνιστο: Πότε η εξατομικευμένη διαφήμιση ή ο σχεδιασμός διεπαφής (nudging, dark patterns) γίνεται «ουσιώδης στρέβλωση συμπεριφοράς»; Η αλληλοεπικάλυψη με έννοιες άλλων κλάδων δικαίου, όπως ο DSA και το δίκαιο καταναλωτή, αναμένεται να διευκρινίσει σε μεγάλο βαθμό το σημείο αυτό, ωστόσο η αναλογική εφαρμογή της σχετικής νομολογίας σε αυτόν τον Κανονισμό δεν είναι 100% αυτονόητη. Αντίστοιχα ασαφές παραμένει το πού σταματά ένα εργαλείο ασφάλειας εργαζομένων (π.χ. ανίχνευση κόπωσης οδηγών) και πού αρχίζει η απαγορευμένη «αναγνώριση συναισθημάτων στην εργασία». Οι κατευθυντήριες γραμμές της Επιτροπής για το άρθρο 5 απαντούν μερικώς και δεν δεσμεύουν τα δικαστήρια.
Πού μπορεί να οδηγήσει: Από όλα τα σημεία ασάφειας αυτής της ενότητας, αυτό είναι το πιο επικίνδυνο για την επιχείρηση: λάθος ερμηνεία εδώ δεν οδηγεί απλώς σε διορθωτικά μέτρα, αλλά κατευθείαν στα ανώτατα πρόστιμα του Κανονισμού (έως €35 εκ. ή 7% του παγκόσμιου κύκλου εργασιών).

3. Το «φίλτρο εξαίρεσης» του άρθρου 6 παρ. 3: αόριστα κριτήρια και εκκρεμείς κατευθυντήριες γραμμές

Τι ορίζει ο νόμος: Σύστημα του Παραρτήματος ΙΙΙ μπορεί κατ' εξαίρεση να μη χαρακτηριστεί υψηλού κινδύνου εάν δεν ενέχει «σημαντικό κίνδυνο», ιδίως όταν εκτελεί «στενή διαδικαστική εργασία», βελτιώνει το αποτέλεσμα ήδη ολοκληρωμένης ανθρώπινης δραστηριότητας, εντοπίζει αποκλίσεις χωρίς να αντικαθιστά την ανθρώπινη αξιολόγηση ή εκτελεί «προπαρασκευαστική εργασία». Σύστημα που πραγματοποιεί profiling φυσικών προσώπων δεν μπορεί ποτέ να υπαχθεί στην εξαίρεση.
Τι παραμένει αδιευκρίνιστο: Οι έννοιες «στενή διαδικαστική εργασία», «ουσιώδης επιρροή» στην απόφαση και «προπαρασκευαστική εργασία» δεν ορίζονται. Πότε π.χ. η προ-ταξινόμηση βιογραφικών είναι «προπαρασκευαστική» και πότε επηρεάζει ουσιωδώς την τελική κρίση; Οι κατευθυντήριες γραμμές της Επιτροπής για την ταξινόμηση (άρθρο 6 παρ. 5) δεν έχουν οριστικοποιηθεί, παρότι η προβλεπόμενη προθεσμία (2.2.2026) έχει παρέλθει, με αποτέλεσμα οι επιχειρήσεις να ταξινομούν σήμερα χωρίς επίσημα παραδείγματα εφαρμογής. Παρά ταύτα, το σχέδιο των σχετικών κατευθυντηρίων, το οποίο έχει ήδη δημοσιευθεί (19.5.2026) και αναμένεται η οριστική έκδοσή του, αναφέρεται εκτενώς στο συγκεκριμένο ζήτημα και την ορθή ερμηνεία του.
Πού μπορεί να οδηγήσει: Το φίλτρο είναι ένα από τα βασικά πιθανά σημεία σύγκρουσης μεταξύ επιχειρήσεων και εποπτικών αρχών: ο πάροχος που το επικαλείται τεκμηριώνει και καταχωρίζει την εκτίμησή του, την οποία η αρχή μπορεί εκ των υστέρων να ανατρέψει, με αναδρομική ενεργοποίηση του συνόλου των υποχρεώσεων υψηλού κινδύνου. Έως την οριστικοποίηση των κατευθυντήριων γραμμών, συνιστάται συντηρητική ερμηνεία.

4. Άρθρο 25: πότε ο φορέας εφαρμογής καθίσταται πάροχος | χωρίς σαφές κατώφλι

Τι ορίζει ο νόμος: Τρίτος (συνήθως φορέας εφαρμογής) αναλαμβάνει τις υποχρεώσεις παρόχου όταν διαθέτει σύστημα υψηλού κινδύνου με το δικό του όνομα/σήμα, όταν επιφέρει «ουσιαστική τροποποίηση» σε σύστημα υψηλού κινδύνου ή όταν τροποποιεί τον επιδιωκόμενο σκοπό συστήματος ώστε αυτό να καθίσταται υψηλού κινδύνου.
Τι παραμένει αδιευκρίνιστο: Ο νόμος δεν θέτει συγκεκριμένο και αντικειμενικό ποσοτικό ή ποιοτικό κατώφλι: πού τελειώνει η επιτρεπτή παραμετροποίηση και πού αρχίζει η «ουσιαστική τροποποίηση»; Ενδεικτικά, όταν μια επιχείρηση κάνει fine-tuning ενός μοντέλου γενικού σκοπού ή το ενσωματώνει σε workflow μέσω system prompts για συγκεκριμένη λειτουργία, αυτό συνιστά κατά κανόνα τροποποίηση του επιδιωκόμενου σκοπού. Το αδιευκρίνιστο σημείο είναι σε ποιο βαθμό απλούστερη παραμετροποίηση (π.χ. RAG, prompting χωρίς fine-tuning) περνά το ίδιο κατώφλι. Για παράδειγμα μια επιχείρηση που συνδέει ένα γενικού σκοπού chatbot με τα δικά της δεδομένα πελατών μέσω RAG ώστε να προτείνει κατά προτεραιότητα ποιοι θα εξυπηρετηθούν πρώτοι, χωρίς να αλλάξει καθόλου το ίδιο το μοντέλο. Επιπλέον, ο «επιδιωκόμενος σκοπός» ορίζεται μονομερώς από τον αρχικό πάροχο μέσα από οδηγίες χρήσης και εμπορικό υλικό, κείμενα που συχνά είναι γενικόλογα ή σκοπίμως ευρεία, καθιστώντας δυσδιάκριτο πότε μια χρήση «εκφεύγει» από αυτόν.
Πού μπορεί να οδηγήσει: Πρόκειται για το σημείο με τον μεγαλύτερο κίνδυνο αντιδικιών στην αλυσίδα αξίας: σε περίπτωση ζημίας ή ελέγχου, πάροχος και φορέας εφαρμογής έχουν αντίθετα συμφέροντα ως προς το ποιος «κατέστη πάροχος» και μαζί του, ποιος φέρει τεχνικό φάκελο, σήμανση CE και ευθύνη. Η αβεβαιότητα αυτή μεταφέρεται ήδη στις συμβάσεις (ρήτρες κατανομής ευθύνης, εγγυήσεις σκοπού χρήσης) και είναι πιθανό να κριθεί δικαστικά πριν εκδοθεί σχετική καθοδήγηση.

5. «Ουσιαστική» ανθρώπινη εποπτεία (άρθρα 14 και 26): πότε το σύστημα «υποβοηθά» και πότε «αποφασίζει»

Τι ορίζει ο νόμος: Τα συστήματα υψηλού κινδύνου σχεδιάζονται ώστε να μπορούν να εποπτεύονται αποτελεσματικά από φυσικά πρόσωπα, τα οποία πρέπει να διαθέτουν τις γνώσεις και να είναι σε θέση να κατανοούν, να αμφισβητούν, να παρακάμπτουν ή να διακόπτουν τη λειτουργία τους. Ο φορέας εφαρμογής αναθέτει την εποπτεία σε πρόσωπα με επαρκή κατάρτιση και εξουσία.
Τι παραμένει αδιευκρίνιστο: Αν ο άνθρωπος εγκρίνει το 98% των εισηγήσεων του συστήματος χωρίς πραγματικό έλεγχο (automation bias), ασκείται εποπτεία; Αντίστοιχα ασαφής είναι η διάκριση μεταξύ συστήματος που «υποβοηθά» τη λήψη απόφασης και συστήματος που ουσιαστικά την καθορίζει, διάκριση κρίσιμη τόσο για την ταξινόμηση (βλ. Σημείο 3) όσο και για τη σχέση με το άρθρο 22 GDPR περί αυτοματοποιημένων ατομικών αποφάσεων.
Πού μπορεί να οδηγήσει: Σε καταγγελίες επηρεαζόμενων προσώπων (π.χ. απόρριψη υποψηφίου ή δανείου), το κατά πόσον η ανθρώπινη εμπλοκή ήταν πραγματική ή προσχηματική θα αποτελέσει κεντρικό αποδεικτικό ζήτημα, με αντικρουόμενη νομολογιακή ερμηνεία πιθανή μεταξύ κρατών μελών, όπως συνέβη και με το άρθρο 22 GDPR.

6. FRIA (άρθρο 27): ασαφές υποκειμενικό πεδίο και αδιευκρίνιστη σχέση με τη DPIA

Τι ορίζει ο νόμος: Υποχρέωση εκτίμησης αντικτύπου στα θεμελιώδη δικαιώματα φέρουν, μεταξύ άλλων, φορείς εφαρμογής που είναι «οργανισμοί δημόσιου δικαίου ή ιδιωτικές οντότητες που παρέχουν δημόσιες υπηρεσίες», καθώς και φορείς που αξιολογούν πιστοληπτική ικανότητα ή τιμολογούν ασφαλίσεις ζωής/υγείας.
Τι παραμένει αδιευκρίνιστο: Η έννοια «ιδιωτική οντότητα που παρέχει δημόσιες υπηρεσίες» δεν ορίζεται: καταλαμβάνει κάθε ανάδοχο δημόσιας σύμβασης; Ιδιωτικά σχολεία, κλινικές, παρόχους κοινής ωφέλειας; Επιπλέον, ο νόμος ορίζει ότι όπου υποχρέωση καλύπτεται ήδη από τη DPIA, η FRIA τη «συμπληρώνει» χωρίς να διευκρινίζει ποια στοιχεία θεωρούνται καλυμμένα και ποια απαιτούν αυτοτελή ανάλυση. Η έκδοση συναφών κατευθυντηρίων γραμμών ή/και προτύπων διενέργειας FRIA θα παρείχε αυξημένη ασφάλεια δικαίου στις επιχειρήσεις.
Πού μπορεί να οδηγήσει: Επιχειρήσεις στα όρια του πεδίου (ανάδοχοι, παραχωρησιούχοι, ιδιωτικοί πάροχοι κοινωνικών υπηρεσιών) δεν μπορούν σήμερα να γνωρίζουν με βεβαιότητα αν υπέχουν την υποχρέωση, και θα πρέπει να τεκμηριώσουν νομικά την επιλεχθείσα προσέγγισή τους. Η παράλειψη FRIA όπου τελικά κριθεί απαιτητή συνιστά αυτοτελή παράβαση, ενώ αντίστροφα η άσκοπη διενέργειά της δημιουργεί κόστος και αποδεικτικό υλικό χωρίς νομική ανάγκη.

7. Κενό εναρμονισμένων προτύπων (άρθρο 40): συμμόρφωση χωρίς μέτρο σύγκρισης

Τι ορίζει ο νόμος: Η συμμόρφωση με εναρμονισμένα ευρωπαϊκά πρότυπα δημοσιευμένα στην Επίσημη Εφημερίδα δημιουργεί τεκμήριο συμμόρφωσης με τις αντίστοιχες απαιτήσεις για τα συστήματα υψηλού κινδύνου.
Τι παραμένει αδιευκρίνιστο: Τα πρότυπα της CEN-CENELEC (JTC 21) καθυστερούν και αναμένονται προς το τέλος του 2026 ή αργότερα. Έως τη δημοσίευσή τους, οι ουσιαστικές απαιτήσεις (ακρίβεια, στιβαρότητα, ποιότητα δεδομένων, ανθρώπινη εποπτεία) διατυπώνονται στον νόμο ως γενικές ρήτρες χωρίς μετρήσιμο σημείο αναφοράς: Τι επίπεδο ακρίβειας είναι «κατάλληλο»; Πόσο αντιπροσωπευτικό είναι «επαρκώς» ένα σύνολο δεδομένων; Η πιστοποίηση ISO/IEC 42001 δεν παρέχει το νόμιμο τεκμήριο.
Πού μπορεί να οδηγήσει: Στο μεταβατικό διάστημα, η κρίση περί συμμόρφωσης επαφίεται στην εκτίμηση κάθε αρχής και, σε περίπτωση αμφισβήτησης, των δικαστηρίων, με πιθανές αποκλίσεις μεταξύ κρατών μελών. Επιπλέον, εάν τα πρότυπα δημοσιευθούν λίγο πριν από τις προθεσμίες του 2027–2028, οι επιχειρήσεις θα κληθούν να προσαρμοστούν σε αυτά με ελάχιστο χρόνο, ενδεχομένως αναθεωρώντας ήδη υλοποιημένες λύσεις.

8. Επικαλύψεις με GDPR και κατακερματισμένη εποπτεία: ποιος κανόνας και ποια αρχή υπερισχύει

Τι ορίζει ο νόμος: Ο Κανονισμός εφαρμόζεται παράλληλα με τον GDPR και εποπτεύεται εθνικά από περισσότερες αρχές: στην Ελλάδα, την ΑΠΔΠΧ ως αρχή εποπτείας της αγοράς, και τις τομεακές αρχές για ΤΝ ενσωματωμένη σε προϊόντα του Παραρτήματος Ι.
Τι παραμένει αδιευκρίνιστο: Η οριοθέτηση μεταξύ των δύο καθεστώτων δεν είναι πλήρης: η ίδια πράξη (π.χ. αυτοματοποιημένη απόρριψη υποψηφίου) μπορεί να ελεγχθεί ως ζήτημα άρθρου 22 GDPR, ως ζήτημα υποχρεώσεων υψηλού κινδύνου του Κανονισμού, ή και ως τα δύο, με διαφορετικές προϋποθέσεις, εξαιρέσεις και κυρώσεις. Ασαφής παραμένει και η πρακτική οριοθέτηση αρμοδιοτήτων όταν ένα σύστημα εμπίπτει ταυτόχρονα σε τομεακή εποπτεία και στην εποπτεία της ΑΠΔΠΧ, καθώς και ο βαθμός συντονισμού των εθνικών αρχών μεταξύ κρατών μελών πριν λειτουργήσουν πλήρως οι ενωσιακοί μηχανισμοί.
Πού μπορεί να οδηγήσει: Κίνδυνος παράλληλων ή διαδοχικών διαδικασιών για την ίδια πράξη, δυνατότητα επιλογής της ευνοϊκότερης νομικής βάσης από καταγγέλλοντες (forum shopping) και αποκλίνουσα εφαρμογή μεταξύ κρατών μελών κατά τα πρώτα έτη, έως ότου διαμορφωθεί ενιαία πρακτική και νομολογία.

Δ.
CHECKLIST ΣΥΜΜΟΡΦΩΣΗΣ ΓΙΑ ΤΗ ΔΙΟΙΚΗΣΗ



Οργανωτική ετοιμότητα
☐ Υπάρχει υπεύθυνος για τη Διακυβέρνηση της ΤΝ;
☐ Υπάρχει εγκεκριμένη πολιτική χρήσης ΤΝ / GenAI;
☐ Έχει οριστεί υπεύθυνος για κάθε σύστημα ΤΝ και AI agent;
☐ Υπάρχουν μηχανισμοί εσωτερικού / εξωτερικού ελέγχου;

Χαρτογράφηση
☐ Υπάρχει κεντρικό Μητρώο όλων των συστημάτων ΤΝ της επιχείρησης;
☐ Έχουμε καταγράψει όλα τα συστήματα ΤΝ που χρησιμοποιούμε στο μητρώο ΤΝ;
☐ Έχουμε επιβεβαιώσει αν κάθε σύστημα εμπίπτει στον ορισμό του «συστήματος ΤΝ»;
☐ Έχουμε περιγράψει το σκοπό και το πλαίσιο χρήσης κάθε συστήματος;
☐ Έχουμε εντοπίσει ποια είναι κρίσιμα για επιχειρησιακές αποφάσεις;

Ταξινόμηση & Ενέργειες Συμμόρφωσης
☐ Έχουμε ελέγξει αν κάποιο σύστημα εμπίπτει στις απαγορευμένες πρακτικές;
☐ Έχουμε προσδιορίσει την κατηγορία κινδύνου και τυχόν υποχρεώσεις διαφάνειας όλων των συστημάτων μας;
☐ Έχουμε προσδιορίσει τον ρόλο μας για κάθε σύστημα;
☐ Έχουμε υλοποιήσει τις ενέργειες συμμόρφωσης που αντιστοιχούν στην ταξινόμηση;

Εκπαίδευση
☐ Έχει εκπαιδευτεί η Διοίκηση;
☐ Έχουν εκπαιδευτεί οι χρήστες ανάλογα με τον ρόλο και τον κίνδυνο;
☐ Τεκμηριώνονται τα μέτρα AI literacy που εφαρμόζονται;
☐ Ανασκοπούνται τα μέτρα AI literacy τουλάχιστον ετήσια ή μετά από σημαντικές αλλαγές;

Ανθρώπινη Εποπτεία & Διαφάνεια
☐ Υπάρχει διαδικασία ανθρώπινης εποπτείας για κρίσιμες ενέργειες;
☐ Υπάρχει δυνατότητα override, διακοπής ή rollback;
☐ Έχουμε εκπαιδεύσει τους approvers ώστε να μην βασιζόμαστε μηχανικά στο output;
☐ Είναι σαφές πότε ο χρήστης αλληλοεπιδρά με ΤΝ;
☐ Υπάρχει κατάλληλη σήμανση σε email, chat, voice ή περιεχόμενο;
☐ Υπάρχει διαδικασία μεταφοράς σε άνθρωπο όταν χρειάζεται;

Διαχείριση Προμηθευτών & AI agents

☐ Έχουμε καταγράψει όλους τους προμηθευτές;
☐ Έχουμε καταγράψει όλους τους AI agents που χρησιμοποιούμε στο μητρώο ΤΝ;
☐ Υπάρχει διαδικασία αξιολόγησης προμηθευτών;
☐ Υπάρχει διαδικασία έγκρισης νέων εργαλείων;
☐ Έχουμε ορίσει τα δεδομένα που επιτρέπεται να χρησιμοποιεί κάθε agent;
☐ Έχουμε εφαρμόσει least privilege και χωριστή ταυτότητα agent;
☐ Έχουμε κάνει έλεγχο στα προσωπικά ή εμπιστευτικά δεδομένα;

Έλεγχος και παρακολούθηση

☐ Υπάρχουν μηχανισμοί καταγραφής, όπως logs και audit trails;
☐ Υπάρχει διαδικασία παραπόνων, αιτημάτων αρχών και αναφοράς περιστατικών;
☐ Υπάρχουν δείκτες απόκλισης και alerts;
☐ Έχουμε ορίσει περιοδικό έλεγχο;
☐ Επανεξετάζουμε κάθε σύστημα ΤΝ ή agent μετά από σημαντική αλλαγή;
☐ Υπάρχει διαδικασία παύσης ή απόσυρσης συστήματος ΤΝ ή agent;

Ε. ΕΤΟΙΜΟΤΗΤΑ ΑΠΕΝΑΝΤΙ ΣΕ ΕΠΟΠΤΙΚΟ ΕΛΕΓΧΟ



1. Τι μπορεί να ζητήσει μια εποπτική αρχή

Κατηγορία πληροφορίας	Ενδεικτικά στοιχεία που πρέπει να είναι διαθέσιμα
Μητρώο συστημάτων ΤΝ	Κατάλογος συστημάτων, σκοπός χρήσης, επιχειρησιακός υπεύθυνος, προμηθευτής, κατηγορία κινδύνου, ρόλος επιχείρησης.
Κατάταξη κινδύνου	Τεκμηρίωση ελέγχου απαγορευμένων πρακτικών, αξιολόγηση υπαγωγής, αιτιολόγηση απόφασης.
Τεχνική & λειτουργική τεκμηρίωση	Οδηγίες χρήσης, πληροφορίες παρόχου, τεχνικός φάκελος όπου απαιτείται, περιορισμοί, επιδόσεις, διαδικασίες αλλαγών.
Ανθρώπινη εποπτεία	Ποιος εποπτεύει, με ποιες αρμοδιότητες και δικαίωμα παρέμβασης, πώς εκπαιδεύτηκε, πότε ενεργοποιείται.
Αρχεία καταγραφής & monitoring	Logs, αναφορές απόκλισης, αξιολογήσεις ακρίβειας, έλεγχοι μεροληψίας, δείκτες, διορθωτικές ενέργειες.
Διαφάνεια & ενημέρωση	Ενημερώσεις και εξηγήσεις προς χρήστες, εργαζομένους ή επηρεαζόμενα πρόσωπα.
Αξιολογήσεις Συμμόρφωσης	Πιστοποιητικά αξιολόγησης της συμμόρφωσης, αναφορές εσωτερικής διαδικασίας αξιολόγησης συμμόρφωσης (όπου προβλέπεται), σχετικές πιστοποιήσεις βάσει προτύπων, δήλωση συμμόρφωσης ΕΕ, αποδεικτικά σήμανσης CE.
Δεδομένα & δικαιώματα	DPIA, FRIA όπου απαιτείται, περιγραφή δεδομένων εισόδου, έλεγχος καταλληλότητας.
Προμηθευτές	Due diligence, συμβατικές ρήτρες, δηλώσεις συμμόρφωσης, SLAs, διαδικασία ενημέρωσης για σοβαρά περιστατικά.
AI literacy	Πλάνο εκπαίδευσης ανά ρόλο, παρουσιολόγια, αξιολογήσεις, υλικό, επικαιροποιήσεις.

Παράδειγμα:
Υποψήφιος εργαζόμενος καταγγέλλει ότι απορρίφθηκε λόγω εργαλείου ΤΝ που αξιολογεί βιογραφικά. Η επιχείρηση πρέπει να μπορεί να δείξει: γιατί χρησιμοποιείται το εργαλείο, ποιος είναι ο ρόλος της, αν έχει ταξινομηθεί ως υψηλού κινδύνου, πώς ασκείται ανθρώπινη εποπτεία, τι ενημέρωση δόθηκε στους υποψηφίους και ποια τεκμήρια υπάρχουν ως προς τη συμμόρφωση του συστήματος με τις έννομες απαιτήσεις που αντιστοιχούν στην κατηγορία κινδύνου του.

2. Διαδικασία αντίδρασης σε αίτημα αρχής, καταγγελία ή σοβαρή απόκλιση

Βήμα	Τι κάνει η επιχείρηση
1. Καταγραφή αιτήματος	Ημερομηνία λήψης, αρχή/πρόσωπο, σύστημα ΤΝ που αφορά, προθεσμία απάντησης.
2. Ταυτοποίηση συστήματος & ρόλου	Εντοπισμός use case στο μητρώο και επιβεβαίωση ρόλου (πάροχος, φορέας εφαρμογής κλπ.).
3. Ενεργοποίηση ομάδας απόκρισης	Legal/Compliance, IT/Data, DPO, business owner, Procurement και προμηθευτής όπου χρειάζεται.
4. Διατήρηση αποδεικτικών	Παγώνουν/εξασφαλίζονται logs, εκδόσεις μοντέλου, οδηγίες χρήσης, datasets, approvals, εκπαιδευτικά αρχεία.
5. Αρχική αξιολόγηση κινδύνου	Εξετάζεται αν η χρήση θα περιοριστεί, ανασταλεί ή συνεχιστεί υπό πρόσθετη εποπτεία.
6. Συλλογή φακέλου τεκμηρίωσης	Εσωτερικός φάκελος / data room, ταξινομημένος ανά υποχρέωση συμμόρφωσης.
7. Απάντηση & διορθωτικές ενέργειες	Η απάντηση εγκρίνεται πριν αποσταλεί. Για κάθε κενό: υπεύθυνος, χρονοδιάγραμμα, τεκμηρίωση.
8. Lessons learned	Επικαιροποίηση μητρώου, κατάταξης, πολιτικής, εκπαιδευτικού υλικού και συμβάσεων προμηθευτών.

i

Για συστήματα υψηλού κινδύνου, η διαδικασία λαμβάνει υπόψη και την υποχρέωση αναφοράς σοβαρών περιστατικών: ο πάροχος ενημερώνει την αρμόδια αρχή όταν διαπιστώνεται ή πιθανολογείται αιτιώδης συνάφεια μεταξύ συστήματος και περιστατικού, εντός των προβλεπόμενων προθεσμιών ανάλογα με τη βαρύτητα.

ΣΤ.
ΣΥΧΝΕΣ ΕΡΩΤΗΣΕΙΣ



Ε: Χρησιμοποιούμε μόνο ChatGPT/Copilot για γραφειακές εργασίες. Μας αφορά ο Κανονισμός;

Α: Ναι, τουλάχιστον ως προς το AI literacy (άρθρο 4, ήδη σε ισχύ), την πολιτική χρήσης και τον έλεγχο ότι καμία χρήση δεν εμπίπτει σε απαγορευμένη πρακτική. Οι χρήσεις γενικής παραγωγικότητας είναι συνήθως ελάχιστου/περιορισμένου κινδύνου, αλλά πρέπει να καταγράφονται και να επανελέγχονται όταν επεκτείνονται.

Ε: Ο προμηθευτής μάς διαβεβαιώνει ότι το εργαλείο του «είναι συμμορφωμένο». Αρκεί;

Α: Όχι. Ο φορέας εφαρμογής φέρει δικές του υποχρεώσεις (χρήση σύμφωνα με οδηγίες, εποπτεία, διαφάνεια, παρακολούθηση) και οφείλει να τεκμηριώνει τη δική του αξιολόγηση. Η δήλωση και συμμόρφωση του προμηθευτή είναι αναγκαίο στοιχείο αρχικού ελέγχου, όχι υποκατάστατο.

Ε: Πότε γινόμαστε «πάροχος» χωρίς να το καταλάβουμε;

Α: Όταν διαθέτουμε σύστημα υψηλού κινδύνου με δικό μας σήμα ή υπό την επωνυμία μας, όταν το τροποποιούμε ουσιωδώς ή όταν το χρησιμοποιούμε για σκοπό διαφορετικό από τον επιδιωκόμενο του αρχικού παρόχου.

Ε: Το σύστημά μας κάνει προτάσεις, ο άνθρωπος αποφασίζει. Είμαστε εκτός υψηλού κινδύνου;

Α: Όχι απαραίτητα. Η ύπαρξη ανθρώπου «στο τέλος» δεν αρκεί. Κρίσιμο είναι αν ο άνθρωπος έχει πραγματική δυνατότητα κατανόησης, αμφισβήτησης και παράκαμψης. Συστήματα που επηρεάζουν ουσιωδώς αποφάσεις για φυσικά πρόσωπα (π.χ. προσλήψεις) παραμένουν κατά κανόνα υψηλού κινδύνου. Μάλιστα, η εισαγωγή μέτρων ανθρώπινης εποπτείας είναι μία από τις βασικές υποχρεώσεις ως προς τα συστήματα ΤΝ υψηλού κινδύνου.

Ε: Πρέπει να κάνουμε FRIA;

Α: Μόνο αν είστε φορέας εφαρμογής συστήματος υψηλού κινδύνου του Παραρτήματος III και είτε παρέχετε δημόσιες υπηρεσίες συνδεόμενες με καθήκοντα δημόσιου συμφέροντος, είτε αξιολογείτε πιστοληπτική ικανότητα φυσικών προσώπων, είτε τιμολογείτε ασφαλίσεις ζωής/υγείας (βλ. Παράρτημα ΙΙ).

Ε: Η πιστοποίηση ISO/IEC 42001 μάς καλύπτει νομικά;

Α: Αποδεικνύει οργανωτική ωριμότητα και διευκολύνει σημαντικά, αλλά τεκμήριο νομικής συμμόρφωσης θα παρέχουν μόνο τα εναρμονισμένα ευρωπαϊκά πρότυπα όταν δημοσιευθούν (βλ. Ενότητα Γ, Σημείο 7).

Ε: Οι προθεσμίες μετατέθηκαν στο 2027–2028. Μπορούμε να περιμένουμε;

Α: Όχι: ορισμένες υποχρεώσεις ισχύουν ήδη, ενώ η προετοιμασία για τα συστήματα υψηλού κινδύνου απαιτεί 12–24 μήνες (βλ. Ενότητα Α, Χρονοδιάγραμμα εφαρμογής).

Ε: Ποια αρχή μάς εποπτεύει στην Ελλάδα;

Α: Κατά κανόνα η ΑΠΔΠΧ, ως αρχή εποπτείας της αγοράς και ενιαίο σημείο επαφής. Για ΤΝ ενσωματωμένη σε προϊόντα του Παραρτήματος Ι, οι αντίστοιχες τομεακές αρχές· κοινοποιούσα αρχή είναι η ΕΕΤΤ.

ΠΑΡΑΡΤΗΜΑ Ι.
Αναλυτικές υποχρεώσεις για συστήματα υψηλού κινδύνου

1. Όταν η επιχείρηση είναι πάροχος

Ο πάροχος φέρει το βαρύτερο κανονιστικό φορτίο. Αναλυτικά:

- **Σύστημα διαχείρισης κινδύνου:** συνεχής διεργασία αναγνώρισης, αξιολόγησης, μετριασμού και επανεξέτασης κινδύνων σε όλη τη διάρκεια ζωής, με σαφή μεθοδολογία: ποιοι κίνδυνοι εξετάζονται, ποια τα κριτήρια/όρια αποδοχής, ποια τα μέτρα μετριασμού, ποιος εγκρίνει, πότε επανεκτιμάται. Καλύπτει και κινδύνους ειδικούς της ΤΝ: δυσμενείς διακρίσεις, μεροληψία, παραβίαση ιδιωτικότητας, αναξιόπιστες προβλέψεις.
- **Διακυβέρνηση και ποιότητα δεδομένων:** τεκμηρίωση πηγής, διαδικασίας και κριτηρίων επιλογής των συνόλων δεδομένων εκπαίδευσης/δοκιμών/επικύρωσης, των παραδοχών και περιορισμών, ελέγχου αντιπροσωπευτικότητας/ακρίβειας/καταλληλότητας και ελέγχου μεροληψίας. Αξιολόγηση επίδοσης σε διαφορετικά περιβάλλοντα ή ομάδες χρηστών, όπου απαιτείται.
- **Τεχνική τεκμηρίωση:** τεχνικός φάκελος που καλύπτει σκοπό, διαδικασία σχεδιασμού/ανάπτυξης, σύνολα δεδομένων, αρχιτεκτονική, δείκτες μέτρησης, αποτελέσματα δοκιμών, μέτρα ανθρώπινης εποπτείας. Βασικός μηχανισμός λογοδοσίας — όχι «engineering paperwork».
- **Αρχεία καταγραφής (logs) και ιχνηλασιμότητα:** τεχνική δυνατότητα αυτόματης καταγραφής γεγονότων καθ' όλη τη διάρκεια ζωής, για διερεύνηση περιστατικών, εποπτεία και βελτίωση.
- **Ανθρώπινη εποπτεία:** ενσωμάτωση τεχνικών χαρακτηριστικών ώστε οι φορείς εφαρμογής να ασκούν ουσιαστική εποπτεία· αποτύπωση μέτρων στα εγχειρίδια χρήσης, δείκτες αξιοπιστίας, εκπαιδευτικό υλικό.
- **Αξιολόγηση συμμόρφωσης:** διενέργεια διαδικασίας αξιολόγησης, έκδοση δήλωσης συμμόρφωσης ΕΕ, σήμανση CE και καταχώριση στη βάση δεδομένων της ΕΕ, όπου προβλέπεται.
- **Παρακολούθηση μετά τη διάθεση:** παρακολούθηση συμμόρφωσης και ορθής λειτουργίας μετά τη διάθεση στην αγορά, λήψη διορθωτικών μέτρων σε προβλήματα ή σοβαρά περιστατικά.

Για παρόχους συστημάτων υψηλού κινδύνου απαιτείται τυπικό σύστημα διαχείρισης ποιότητας (άρθρο 17 του Κανονισμού), με σημαντική επικάλυψη με το ISO/IEC 42001:2023.

2. Όταν η επιχείρηση είναι φορέας εφαρμογής

- **Χρήση σύμφωνα με τις οδηγίες:** χρήση για τον σκοπό για τον οποίο το σύστημα σχεδιάστηκε και αξιολογήθηκε. Ουσιώδης αλλαγή χρήσης ή λειτουργίας μπορεί να μεταβάλει την ταξινόμηση κινδύνου ή/και να καταστήσει την επιχείρηση πάροχο — απαιτούνται εσωτερικές οδηγίες για το τι επιτρέπεται και ποια αλλαγή απαιτεί εκ νέου αξιολόγηση.
- **Ανθρώπινη εποπτεία:** ανάθεση σε εξουσιοδοτημένα, καταρτισμένα πρόσωπα που κατανοούν δυνατότητες και περιορισμούς, εντοπίζουν ανωμαλίες, είναι εκπαιδευμένα στον κίνδυνο automation bias και μπορούν να αγνοούν, να παρακάμπτουν ή να αντιστρέφουν αποτελέσματα όταν το κρίνουν απαραίτητο.
- **Διαφάνεια στην εργασία:** πριν τη χρήση συστήματος υψηλού κινδύνου στον χώρο εργασίας, ενημέρωση εκπροσώπων εργαζομένων και επηρεαζόμενων εργαζομένων για τη λειτουργία του (π.χ. συστήματα αξιολόγησης ή κατανομής καθηκόντων).
- **Διαφάνεια σε αποφάσεις για φυσικά πρόσωπα:** όταν σύστημα του Παραρτήματος ΙΙΙ χρησιμοποιείται για λήψη ή υποβοήθηση αποφάσεων που αφορούν φυσικό πρόσωπο, ενημέρωση των επηρεαζόμενων προσώπων (π.χ. υποψήφιοι εργαζόμενοι σε αυτόματη αξιολόγηση βιογραφικών, αιτούντες πιστωτικών προϊόντων). Επίσης: διαδικασία διαχείρισης αιτημάτων εξήγησης σχετικά με τον ρόλο του συστήματος ΤΝ στη λήψη της απόφασης που αφορά φυσικό πρόσωπο.
- **Παρακολούθηση και αναφορά:** παρακολούθηση λειτουργίας· όταν διαπιστώνεται σοβαρός κίνδυνος για ζωή, υγεία, θεμελιώδη δικαιώματα, περιουσία, κρίσιμες υποδομές ή περιβάλλον, ενημέρωση χωρίς αδικαιολόγητη καθυστέρηση του παρόχου/διανομέα και της αρμόδιας αρχής και αναστολή της χρήσης.
- **Τήρηση logs:** τουλάχιστον έξι μήνες (άρθρο 26 του Κανονισμού).
- **FRIA:** όπου απαιτείται (βλ. Παράρτημα ΙΙ του Κανονισμού).

3. Όταν η επιχείρηση είναι εισαγωγέας, διανομέας ή εξουσιοδοτημένος αντιπρόσωπος

Πιο περιορισμένες υποχρεώσεις, με στόχο να αποτρέπεται η διάθεση στην αγορά συστημάτων με προφανείς ενδείξεις μη συμμόρφωσης ή χωρίς τα απαιτούμενα στοιχεία. Ενσωματώνονται κυρίως στις διαδικασίες προμήθειας, ένταξης προμηθευτών, συμμόρφωσης προϊόντος και διαχείρισης συμβάσεων: έλεγχοι τεκμηρίωσης, οδηγιών χρήσης, δηλώσεων συμμόρφωσης, σήμανσης, και διαδικασίες συνεργασίας με τις αρχές.

4. Συγκεντρωτικός πίνακας υποχρεώσεων ανά ρόλο

Υποχρέωση	Πάροχος	Φορέας Εφαρμογής	Εισαγωγέας	Διανομέας
Έλεγχος απαγορευμένων πρακτικών & ταξινόμηση	✓	✓	✓	✓
Εκπαίδευση προσωπικού (AI literacy)	✓	✓	✓	✓
Υποχρεώσεις διαφάνειας	✓	✓	—	—
Σύστημα διαχείρισης κινδύνων	✓	Σε ειδικές περιπτώσεις	—	—
Διακυβέρνηση δεδομένων	✓	Σε περιορισμένο βαθμό	—	—
Τεχνική τεκμηρίωση	✓	—	Επιβεβαίωση διαθεσιμότητας	Επιβεβαίωση διαθεσιμότητας
Logging	✓	✓	—	—
Ανθρώπινη εποπτεία	✓	✓	—	—
FRIA	—	Σε ειδικές περιπτώσεις	—	—
Παρακολούθηση μετά τη διάθεση	✓	Υποχρεώσεις αναφοράς περιστατικών	—	—

ΠΑΡΑΡΤΗΜΑ ΙΙ.

FRIA | Πεδίο εφαρμογής & ελάχιστο περιεχόμενο

Ποιους αφορά

Η υποχρέωση διενέργειας FRIA αφορά μόνο:

- φορείς εφαρμογής συστημάτων υψηλού κινδύνου του Παραρτήματος ΙΙΙ (πλην κρίσιμων υποδομών), εφόσον παρέχουν δημόσιες υπηρεσίες συνδεόμενες με καθήκοντα δημόσιου συμφέροντος (εκπαίδευση, υγειονομική περίθαλψη, κοινωνικές υπηρεσίες, στέγαση). Παράδειγμα: ανάδοχος δημόσιου οργανισμού που αξιολογεί με δικό του σύστημα ΤΝ την επιλεξιμότητα πολιτών για επίδομα.
- φορείς εφαρμογής συστημάτων υψηλού κινδύνου για αξιολόγηση/βαθμολόγηση πιστοληπτικής ικανότητας φυσικών προσώπων (πλην εντοπισμού οικονομικής απάτης) ή για εκτίμηση κινδύνων και τιμολόγηση σε ασφαλίσεις ζωής και υγείας. Παραδείγματα: τράπεζες και ασφαλιστικές εταιρείες.

Η FRIA πραγματοποιείται πριν από την πρώτη χρήση και επικαιροποιείται όταν αλλάζει ουσιωδώς το σύστημα ή το περιβάλλον χρήσης. Εξετάζει ευρύτερους κινδύνους: ανθρώπινη αξιοπρέπεια, ισότητα, ιδιωτικότητα, ελευθερία έκφρασης, πρόσβαση σε υπηρεσίες.

Ελάχιστο περιεχόμενο

- Περιγραφή των διαδικασιών του φορέα εφαρμογής στις οποίες θα χρησιμοποιείται το σύστημα, σύμφωνα με τον επιδιωκόμενο σκοπό του.
- Χρονικό διάστημα και συχνότητα σκοπούμενης χρήσης.
- Κατηγορίες φυσικών προσώπων και ομάδων που ενδέχεται να επηρεαστούν στο συγκεκριμένο πλαίσιο χρήσης.
- Συγκεκριμένοι κίνδυνοι βλάβης για τις κατηγορίες αυτές, λαμβανομένων υπόψη των πληροφοριών του παρόχου.
- Μέτρα ανθρώπινης εποπτείας που εφαρμόζει ο φορέας εφαρμογής.
- Μέτρα σε περίπτωση επέλευσης των κινδύνων, συμπεριλαμβανομένων ρυθμίσεων εσωτερικής διακυβέρνησης και μηχανισμών υποβολής καταγγελιών.

i

Η FRIA παρουσιάζει κοινά στοιχεία με τη DPIA χωρίς να ταυτίζονται. Εάν κάποια υποχρέωση εκπληρώνεται ήδη μέσω της DPIA, η FRIA τη συμπληρώνει. Μεθοδολογικό στήριγμα: ISO/IEC 42005:2025.

ΠΑΡΑΡΤΗΜΑ ΙΙΙ.

Ενδεικτικά use cases ανά επιχειρησιακή λειτουργία

Ο πίνακας λειτουργεί ως πρακτικός οδηγός για τα πρώτα σημεία προσοχής ανά λειτουργία.

Λειτουργία	Ενδεικτικά use cases	Σημεία ελέγχου
Γενική παραγωγικότητα	Σύνοψη εγγράφων, σύνταξη email, παρουσιάσεις, αναζήτηση σε εσωτερική γνώση.	Συνήθως ελάχιστος/περιορισμένος κίνδυνος εφόσον δεν λαμβάνονται αποφάσεις για φυσικά πρόσωπα. Κανόνες για εμπιστευτικά δεδομένα, ανθρώπινος έλεγχος.
Marketing & πωλήσεις	Δημιουργία περιεχομένου, εξατομίκευση, προτάσεις επόμενης ενέργειας.	Έλεγχος για παραπλανητικό περιεχόμενο, πνευματική ιδιοκτησία, profiling, διαφάνεια προς πελάτες/κοινό.
Εξυπηρέτηση πελατών	Chatbot/voicebot, δημιουργία tickets, ενημέρωση CRM.	Ενημέρωση ότι ο χρήστης αλληλοεπιδρά με ΤΝ, escalation σε άνθρωπο, έλεγχος απαντήσεων σε ευαίσθητα ζητήματα.
Ανθρώπινο Δυναμικό	Ανάλυση βιογραφικών, κατάταξη υποψηφίων, αξιολόγηση εργαζομένων, κατανομή καθηκόντων.	Πιθανή υπαγωγή σε υψηλό κίνδυνο. Προσοχή σε διακρίσεις, ανθρώπινη απόφαση, ενημέρωση εργαζομένων/υποψηφίων, απαγόρευση αναγνώρισης συναισθημάτων στην εργασία.
Οικονομική διεύθυνση	Πρόβλεψη cash flow, αναγνώριση τιμολογίων, ανίχνευση απάτης, πιστοληπτική αξιολόγηση.	Back-office αυτοματοποίηση: χαμηλότερος κίνδυνος. Πιστοληπτική αξιολόγηση φυσικών προσώπων: πιθανώς υψηλός κίνδυνος + FRIA.
Νομική & συμμόρφωση	Ανάλυση συμβάσεων, περιλήψεις, compliance Q&A.	Ανθρώπινος νομικός έλεγχος πριν τη χρήση του output, προστασία απορρήτου, τεκμηρίωση πηγών.
IT & ανάπτυξη	Coding agents, tests, ανάλυση logs, scripts.	Έλεγχος πρόσβασης σε repositories/παραγωγή, code review, sandbox, secrets scanning, approval πριν από merge/deploy.
Προμήθειες	Αναζήτηση προμηθευτών, σύγκριση προσφορών, RFP.	Ανθρώπινη έγκριση για οικονομικές δεσμεύσεις, διαφάνεια, κανόνες σύγκρουσης συμφερόντων.
Λειτουργίες / παραγωγή	Predictive maintenance, πρόβλεψη ζήτησης, βελτιστοποίηση, βάρδιες.	Έλεγχος αν επηρεάζεται κρίσιμη υποδομή, ασφάλεια προϊόντος ή εργασιακές αποφάσεις· σύνδεση με IT/OT security.
Διοίκηση & BI	Dashboards με προβλέψεις, ανάλυση αγοράς, σύνοψη reports.	Καταγραφή ότι το output είναι υποστηρικτικό· οι σημαντικές αποφάσεις παραμένουν στη Διοίκηση με ανεξάρτητα στοιχεία.

ΠΑΡΑΡΤΗΜΑ IV.

AI agents | Κίνδυνοι & αναλυτική διαδικασία ασφαλούς ενσωμάτωσης

Τι είναι στην πράξη

Ο Κανονισμός δεν χρησιμοποιεί ως διακριτή κατηγορία τον όρο «AI agent», όμως ένας agent εμπίπτει στον ορισμό του συστήματος ΤΝ. Στην πράξη, agent είναι σύστημα που επιδιώκει στόχο μέσα από βήματα: σχεδιάζει ενέργειες, χρησιμοποιεί εργαλεία, καλεί APIs, ενημερώνει συστήματα, στέλνει email, δημιουργεί κώδικα, ανοίγει tickets ή αλληλοεπιδρά με άλλους agents. Περιλαμβάνονται personal productivity και coding agents, καθώς και αυτόνομοι «digital coworkers» με δική τους ταυτότητα στην επιχείρηση.

Κίνδυνοι που εμφανίζονται εντονότερα

- Εκτελούν ενέργειες και όχι μόνο απαντήσεις — ένα σφάλμα μπορεί να αλλάξει δεδομένα, να αποστείλει μήνυμα, να δημιουργήσει δέσμευση.
- Συνδέονται με πολλά συστήματα (email, CRM, ERP, ticketing, repositories, APIs), αυξάνοντας τον κίνδυνο υπερβολικών δικαιωμάτων πρόσβασης.
- Μπορεί να επηρεαστούν από prompt injection ή κακόβουλες οδηγίες σε ιστοσελίδες, έγγραφα, emails ή tickets που διαβάζουν.
- Μπορεί να δημιουργήσουν σύγχυση ταυτότητας — ο αποδέκτης πρέπει να γνωρίζει αν επικοινωνεί με άνθρωπο ή σύστημα ΤΝ.
- Σε machine-to-machine περιβάλλοντα ανταλλάσσουν εντολές/δεδομένα χωρίς ανθρώπινη παρέμβαση σε κάθε βήμα.
- Η εποπτεία δυσχεραίνεται όταν οι ενέργειες είναι πολλές, γρήγορες, κατανεμημένες και δύσκολα αναστρέψιμες.

Αναλυτική διαδικασία (11 βήματα)

1. Καταγραφή του agent στο μητρώο ΤΝ: όνομα, ιδιοκτήτης, σκοπός, προμηθευτής/ομάδα, μοντέλο/πλατφόρμα, συνδεδεμένα συστήματα, δεδομένα, επηρεαζόμενες διαδικασίες.
2. Ορισμός επιτρεπόμενου σκοπού και απαγορευμένων χρήσεων (π.χ. agent πωλήσεων συντάσσει προσχέδια και ενημερώνει CRM μετά από έγκριση, αλλά δεν αποστέλλει δεσμευτική προσφορά χωρίς ανθρώπινη έγκριση).
3. Καθορισμός επιπέδου αυτονομίας με κλιμακωτό μοντέλο: L0 ενημερωτική απάντηση, L1 προτεινόμενη ενέργεια, L2 εκτέλεση μόνο μετά από ανθρώπινη έγκριση, L3 αυτόνομη εκτέλεση εντός προκαθορισμένων ορίων, L4 ευρεία αυτονομία. Για κρίσιμες ή μη αναστρέψιμες ενέργειες αποφεύγονται υψηλά επίπεδα χωρίς ειδική αξιολόγηση.
4. Περιορισμός πρόσβασης: δική του τεχνική ταυτότητα και δικαιώματα με αρχή ελάχιστου προνομίου — όχι προσωπικός λογαριασμός εργαζομένου, όχι πρόσβαση σε περισσότερα δεδομένα από όσα απαιτεί ο εγκεκριμένος σκοπός.
5. Ανθρώπινη έγκριση για κρίσιμες ενέργειες: εξωτερικό email με δεσμευτικό περιεχόμενο, διαγραφή δεδομένων, αλλαγή οικονομικών στοιχείων, εκτέλεση κώδικα σε παραγωγή, πληρωμή, παραγγελία, απόρριψη αιτήματος, εργασιακή απόφαση.
6. Διαφάνεια και σαφής ταυτότητα: όταν επικοινωνεί με φυσικά πρόσωπα, ιδίως εκτός οργανισμού, πρέπει να είναι σαφές ότι πρόκειται για σύστημα ΤΝ (π.χ. ονομασία «AI Assistant»).
7. Πιλοτική λειτουργία σε sandbox: περιορισμένα δεδομένα, χωρίς δικαιώματα μη αναστρέψιμων ενεργειών, σενάρια δοκιμών για σφάλματα, κακόβουλες οδηγίες, αστοχίες, υπερβάσεις ορίων.
8. Logging και audit trail: εντολές, δεδομένα εισόδου όπου επιτρέπεται, outputs, tool calls, εγκρίσεις, εκτελεσθείσες ενέργειες, αποτυχίες, warnings, έκδοση μοντέλου/agent, χρήστης/σύστημα ενεργοποίησης.
9. Παρακολούθηση και ειδοποιήσεις: αριθμός ενεργειών, ποσοστό ανθρώπινων διορθώσεων, απορρίψεις από approvers, απόπειρες πρόσβασης σε μη επιτρεπτά δεδομένα, κόστος χρήσης, ασυνήθιστη συμπεριφορά, αναφορές χρηστών.
10. Kill switch, rollback και διαδικασία περιστατικού: άμεση απενεργοποίηση, ανάκληση δικαιωμάτων, διακοπή πρόσβασης σε εργαλεία, επαναφορά δεδομένων όπου είναι εφικτό, διερεύνηση περιστατικού ΤΝ.
11. Περιοδική επανεξέταση: σε αλλαγή μοντέλου, προμηθευτή, επιπέδου αυτονομίας, εργαλείων, δεδομένων, σκοπού ή ομάδας χρηστών, και μετά από σοβαρή απόκλιση ή παράπονο.

Παραδείγματα

- Digital coworker εξυπηρέτησης πελατών: AI Customer Support Assistant απαντά μέσω chat/email. Ο πελάτης ενημερώνεται ότι αλληλοεπιδρά με ΤΝ, υπάρχει δυνατότητα μεταφοράς σε άνθρωπο, και απαγορεύεται στον agent να αποδέχεται παράπονα, αποζημιώσεις ή συμβατικές τροποποιήσεις χωρίς ανθρώπινη έγκριση.

- Machine-to-machine procurement agent: Agent λαμβάνει αίτημα αγοράς, ζητά προσφορές από συστήματα προμηθευτών και προτείνει παραγγελία. Ορίζονται όρια αξίας, λίστα εγκεκριμένων προμηθευτών, κανόνες σύγκρισης, διπλή έγκριση για δέσμευση και πλήρες audit trail.

ΠΗΓΕΣ

ΣΕΒ
Ειδική Γραμματεία Τεχνητής Νοημοσύνης & Διακυβέρνησης Δεδομένων
Υπουργείο Ψηφιακής Διακυβέρνησης και Τεχνητής Νοημοσύνης
Ευρωπαϊκή Επιτροπή
International Organization for Standardization
National Institute of Standards and Technology

Κανονισμός (ΕΕ) 2024/1689 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Ιουνίου 2024, για τη θέσπιση εναρμονισμένων κανόνων σχετικά με την τεχνητή νοημοσύνη και την τροποποίηση των κανονισμών (ΕΚ) αριθ. 300/2008, (ΕΕ) αριθ. 167/2013, (ΕΕ) αριθ. 168/2013, (ΕΕ) 2018/858, (ΕΕ) 2018/1139 και (ΕΕ) 2019/2144 και των οδηγιών 2014/90/ΕΕ, (ΕΕ) 2016/797 και (ΕΕ) 2020/1828 (κανονισμός για την τεχνητή νοημοσύνη)

Κανονισμός (ΕΕ) 2026/1744 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 8ης Ιουλίου 2026, για την τροποποίηση των κανονισμών (ΕΕ) 2024/1689, (ΕΕ) 2018/1139 και (ΕΕ) 2023/1230 όσον αφορά την απλούστευση της εφαρμογής εναρμονισμένων κανόνων σχετικά με την τεχνητή νοημοσύνη (ψηφιακό Omnibus για την ΤΝ)

Κατευθυντήριες γραμμές της Επιτροπής σχετικά με τον ορισμό του συστήματος τεχνητής νοημοσύνης που καθορίζεται στον κανονισμό (ΕΕ) 2024/1689 (κανονισμός για την τεχνητή νοημοσύνη)

Κατευθυντήριες γραμμές σχετικά με τις απαγορευμένες πρακτικές τεχνητής νοημοσύνης που καθορίζονται με τον κανονισμό (ΕΕ) 2024/1689 (κανονισμός για την ΤΝ)

Κατευθυντήριες γραμμές σχετικά με τις υποχρεώσεις διαφάνειας για τους παρόχους και τους φορείς εφαρμογής ορισμένων συστημάτων ΤΝ

Κατευθυντήριες γραμμές για τους παρόχους και τους φορείς εφαρμογής συστημάτων ΤΝ υψηλού κινδύνου

Κατευθυντήριες γραμμές της Επιτροπής σχετικά με το πεδίο εφαρμογής των υποχρεώσεων για παρόχους μοντέλων ΤΝ γενικού σκοπού που θεσπίζονται με τον κανονισμό (ΕΕ) 2024/1689 (κανονισμός για την ΤΝ)

Ν. 5321/2026 Μέτρα εφαρμογής του Κανονισμού(ΕΕ) 2024/1689 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 13ης Ιουνίου 2024 (Κανονισμός για την τεχνητή νοημοσύνη) Τροποποίηση του ν. 4961/2022 (Α΄146) και άλλες διατάξεις

ΣΕΒ

Σύγχρονες Επιχειρήσεις, Σύγχρονη Ελλάδα

ΣΕΒ σύνδεσμος επιχειρήσεων και βιομηχανιών

Τομέας Τεχνολογίας & Ψηφιακού Μετασχηματισμού

www.sev.org.gr
E. info@sev.org.gr
T. 211 5006 000

SEVfacts
ΣΕΒ σύνδεσμος επιχειρήσεων και βιομηχανιών
SEV_Fed
SEVFed