filterit · οδηγός

GDPR checklist για εργαλεία AI στο ελληνικό γραφείο

12 σημεία με τα άρθρα δίπλα, υπόδειγμα πολιτικής χρήσης AI, τι να μασκάρετε.

> **Για ποιον:** λογιστικά και δικηγορικά γραφεία, ασφαλιστικά πρακτορεία, μικρές και μεσαίες επιχειρήσεις που ήδη χρησιμοποιούν ChatGPT, Claude, Gemini ή Copilot στη δουλειά τους, ή σκοπεύουν να το κάνουν. **Τι είναι:** ένας πρακτικός κατάλογος 12 σημείων, με τα άρθρα του GDPR δίπλα σε κάθε ένα. **Τι δεν είναι:** νομική συμβουλή. Για το δικό σας γραφείο μιλήστε με τον DPO ή τον νομικό σας σύμβουλο.

1. Γιατί το θέμα είναι δικό σας, όχι «του IT»

Κάθε φορά που κάποιος στο γραφείο κάνει επικόλληση ένα email πελάτη, μια βεβαίωση αποδοχών, μια αγωγή ή έναν ισολογισμό σε ένα εργαλείο AI, το γραφείο **διαβιβάζει προσωπικά δεδομένα σε τρίτο**. Δεν έχει σημασία ότι το έκανε «για να διορθώσει το κείμενο». Για τον GDPR είναι επεξεργασία (άρθρο 4 παρ. 2), γίνεται από εσάς ως υπεύθυνο επεξεργασίας, και ο πάροχος του AI είναι είτε εκτελών την επεξεργασία είτε αυτοτελής υπεύθυνος, ανάλογα με τους όρους της υπηρεσίας που χρησιμοποιείτε.

Τρία πράγματα κάνουν τη διαφορά ανάμεσα σε μια σωστή χρήση και σε μια παραβίαση:

- **Ποια έκδοση** χρησιμοποιείτε. Οι δωρεάν και καταναλωτικές εκδόσεις των εργαλείων μπορεί να χρησιμοποιούν τις συνομιλίες για εκπαίδευση των μοντέλων, εκτός αν το απενεργοποιήσετε ρητά. Οι επιχειρησιακές εκδόσεις και τα API κατά κανόνα όχι. Ελέγξτε τους τρέχοντες όρους, αλλάζουν.
- **Πού** βρίσκεται ο πάροχος και οι διακομιστές του. Οι περισσότεροι μεγάλοι πάροχοι είναι εκτός ΕΕ. Η διαβίβαση επιτρέπεται μόνο με κάποιο από τα εργαλεία του Κεφαλαίου V (απόφαση επάρκειας, τυποποιημένες συμβατικές ρήτρες).
- **Τι** στέλνετε. Αν το κείμενο δεν περιέχει προσωπικά δεδομένα, τα περισσότερα από τα παραπάνω παύουν να ισχύουν. Εδώ μπαίνει η ψευδωνυμοποίηση.

2. Τι είναι «προσωπικό δεδομένο» στα δικά σας έγγραφα

Στην πράξη, τα ελληνικά επαγγελματικά έγγραφα είναι γεμάτα αναγνωριστικά που ένα ξένο εργαλείο δεν καταλαβαίνει καν ως ευαίσθητα:

Τι	Παράδειγμα	Γιατί μετρά
ΑΦΜ	9 ψηφία, με ψηφίο ελέγχου	Μοναδικό αναγνωριστικό φυσικού προσώπου, άρθρο 4 παρ. 1
ΑΜΚΑ	11 ψηφία, ξεκινά από ημερομηνία γέννησης	Αναγνωριστικό κοινωνικής ασφάλισης· συνδέεται με δεδομένα υγείας
ΑΔΤ / διαβατήριο	π.χ. ΑΚ 123456	Ταυτοποίηση
IBAN	GR + 25 χαρακτήρες	Οικονομικά δεδομένα

Τι	Παράδειγμα	Γιατί μετρά
Ονοματεπώνυμα, διευθύνσεις, τηλέφωνα, email		Άμεση ταυτοποίηση
Δεδομένα υγείας, ποινικές καταδίκες, συνδικαλιστική ιδιότητα	ιατρικές βεβαιώσεις, ποινικά μητρώα	Ειδικές κατηγορίες, άρθρο 9 και άρθρο 10. Απαγορεύεται η επεξεργασία χωρίς ειδική βάση
Ημερομηνίες γέννησης, αριθμοί υποθέσεων, πινακίδες		Έμμεση ταυτοποίηση σε συνδυασμό

Σημείωση για την ελληνική γλώσσα: τα ονόματα κλίνονται. «Ο Παπαδόπουλος», «του Παπαδόπουλου», «τον Παπαδόπουλο» είναι το ίδιο πρόσωπο. Ένα εργαλείο που αναγνωρίζει μόνο τον ονομαστικό τύπο αφήνει τα υπόλοιπα στο κείμενο.

3. Ψευδωνυμοποίηση και ανωνυμοποίηση: η διαφορά που μετρά νομικά

- **Ψευδωνυμοποίηση** (άρθρο 4 παρ. 5): τα δεδομένα δεν μπορούν πλέον να αποδοθούν σε συγκεκριμένο πρόσωπο χωρίς πρόσθετες πληροφορίες, οι οποίες φυλάσσονται χωριστά. Τα δεδομένα **παραμένουν προσωπικά**, αλλά ο GDPR την αναγνωρίζει ρητά ως μέτρο ασφάλειας (άρθρο 32 παρ. 1 στοιχείο α) και ως μέτρο προστασίας από τον σχεδιασμό (άρθρο 25).
- **Ανωνυμοποίηση** (αιτιολογική σκέψη 26): το πρόσωπο δεν μπορεί να ταυτοποιηθεί με κανένα εύλογο μέσο. Τότε ο GDPR δεν εφαρμόζεται.

Όταν αντικαθιστάτε το «Γεώργιος Παπαδόπουλος, ΑΦΜ 123456783» με «[NAME_1], ΑΦΜ [AFM_1]» και κρατάτε την αντιστοιχία στο δικό σας σύστημα, κάνετε **ψευδωνυμοποίηση**. Αυτό που φεύγει προς το AI δεν μπορεί να αποδοθεί σε πρόσωπο από τον πάροχο. Αυτό είναι το ζητούμενο: ο πάροχος δεν χρειάζεται να μάθει ποιος είναι ο πελάτης σας για να σας βοηθήσει με το κείμενο.

Μην το ονομάζετε «ανωνυμοποίηση» στα έγγραφά σας αν κρατάτε τον πίνακα αντιστοίχισης. Είναι ψευδωνυμοποίηση, και είναι αρκετή.

4. Ο κατάλογος των 12 σημείων

Τσεκάρετε ό,τι ισχύει ήδη. Ό,τι μένει κενό είναι το πλάνο σας.

- ☐ **1. Ξέρουμε ποιος χρησιμοποιεί τι.** Καταγράψτε ποια εργαλεία AI χρησιμοποιεί το γραφείο, με ποιους λογαριασμούς (προσωπικούς ή εταιρικούς), σε ποια έκδοση. Οι προσωπικοί δωρεάν λογαριασμοί είναι το συνηθέστερο κενό. *(άρθρο 30, αρχείο δραστηριοτήτων)*
- ☐ **2. Έχουμε αποφασίσει τη νομική βάση.** Για τον πελάτη σας, συνήθως η εκτέλεση σύμβασης ή το έννομο συμφέρον. Για τους τρίτους που εμφανίζονται στα έγγραφα (αντίδικοι, εργαζόμενοι πελάτη), το έννομο συμφέρον με στάθμιση. Γράψτε το. *(άρθρο 6)*
- ☐ **3. Οι ειδικές κατηγορίες μένουν έξω από το AI εκτός αν έχουμε ρητή βάση.** Δεδομένα υγείας, ποινικών καταδικών, θρησκείας. Αν το έγγραφο τα περιέχει, μασκάρονται πριν φύγει, ή δεν φεύγει. *(άρθρα 9, 10)*
- ☐ **4. Έχουμε σύμβαση επεξεργασίας με τον πάροχο.** Οι επιχειρησιακές εκδόσεις των μεγάλων παρόχων προσφέρουν Data Processing Addendum. Οι δωρεάν όχι. Χωρίς σύμβαση, ο πάροχος δεν είναι εκτελών τον οποίο ελέγχετε. *(άρθρο 28 παρ. 3)*

- ☐ **5. Ξέρουμε πού πηγαίνουν τα δεδομένα.** Πάροχος εκτός ΕΕ σημαίνει διαβίβαση. Χρειάζεστε απόφαση επάρκειας ή τυποποιημένες ρήτρες, και το αναγράφετε στην ενημέρωση προς τα υποκείμενα. *(Κεφάλαιο V, άρθρα 44–49· άρθρο 13 παρ. 1 στοιχείο στ)*
- ☐ **6. Ψευδωνυμοποιούμε πριν την αποστολή, ως προεπιλογή.** Όχι «όταν το θυμηθούμε». Το εργαλείο πρέπει να το κάνει αυτόματα στο σημείο που φεύγει το κείμενο: στο πεδίο του chat, στο έγγραφο, στο email. *(άρθρα 25, 32 παρ. 1 στοιχείο α)*
- ☐ **7. Ο πίνακας αντιστοίχισης φυλάσσεται χωριστά και κρυπτογραφημένος.** Η ψευδωνυμοποίηση αξίζει μόνο αν το κλειδί δεν ταξιδεύει μαζί με το κείμενο. Ποιος έχει πρόσβαση, για πόσο, πώς διαγράφεται. *(άρθρο 4 παρ. 5, άρθρο 32)*
- ☐ **8. Ελαχιστοποιούμε.** Στέλνουμε την παράγραφο, όχι όλο τον φάκελο. Το AI δεν χρειάζεται τα 40 σελίδες συνημμένα για να ξαναγράψει ένα email. *(άρθρο 5 παρ. 1 στοιχείο γ)*
- ☐ **9. Έχουμε γραπτή πολιτική χρήσης AI, μιας σελίδας.** Τι επιτρέπεται, τι όχι, με ποια εργαλεία, ποιος εγκρίνει εξαιρέσεις. Υπόδειγμα στην ενότητα 6. *(άρθρο 24, ευθύνη του υπευθύνου)*
- ☐ **10. Οι άνθρωποι έχουν εκπαιδευτεί.** Μισή ώρα αρκεί: τι είναι προσωπικό δεδομένο, τι σημαίνει επικόλληση σε δωρεάν εργαλείο, πώς δουλεύει η ψευδωνυμοποίηση. Από τις 2 Φεβρουαρίου 2025 ο κανονισμός για την τεχνητή νοημοσύνη απαιτεί «γραμματισμό» για όσους χειρίζονται συστήματα AI. *(Κανονισμός (ΕΕ) 2024/1689, άρθρο 4)*
- ☐ **11. Ξέρουμε τι κάνουμε σε περιστατικό.** Κάποιος έστειλε ολόκληρο πελατολόγιο σε δωρεάν chatbot. Είναι παραβίαση; Πιθανότατα ναι. Έχετε 72 ώρες για την Αρχή αν υπάρχει κίνδυνος για τα πρόσωπα. Χρειάζεστε αρχείο καταγραφής για να ξέρετε τι έφυγε. *(άρθρα 33, 34)*
- ☐ **12. Έχουμε εξετάσει αν χρειάζεται εκτίμηση αντικτύπου.** Συστηματική χρήση AI πάνω σε ειδικές κατηγορίες ή σε μεγάλη κλίμακα, ή νέα τεχνολογία με υψηλό κίνδυνο: DPIA. Για ένα γραφείο που ξαναγράφει email με ψευδωνυμοποιημένο κείμενο, συνήθως όχι, αλλά η απόφαση πρέπει να είναι γραπτή. *(άρθρο 35)*

5. Πώς το λύνει το filterit, και τι δεν λύνει

Το filterit κάθεται ανάμεσα στο γραφείο και στο εργαλείο AI. Εντοπίζει τα ελληνικά και αγγλικά προσωπικά δεδομένα, τα αντικαθιστά με σταθερά placeholders, στέλνει το ψευδωνυμοποιημένο κείμενο, και επαναφέρει τις πραγματικές τιμές στην απάντηση.

Ανάγκη	Τι κάνει το filterit	Σημείο του καταλόγου
Ένα έγγραφο πριν από copy-paste	**Anonymizer**: επικόλληση ή ανέβασμα (Word, PDF, σκαναρισμένα με OCR), προεπισκόπηση των ευρημάτων, εξαγωγή σε Word/PDF, επαναφορά αργότερα	6, 8
Συνομιλία με AI με επαναφορά	**Chat** μέσα στην εφαρμογή: ό,τι γράφετε μασκάρεται, η απάντηση επιστρέφει με τα πραγματικά ονόματα	6, 7
ChatGPT / Claude / Gemini στον browser	**Επέκταση browser** (Chrome, Edge, χειροκίνητη εγκατάσταση) που μασκάρει πριν πατήσετε Enter, ή **desktop agent** στα Windows (πλάνα Team και Enterprise) που καλύπτει και τις εφαρμογές	6, 9
Word	**Πρόσθετο Word**: ψευδωνυμοποίηση επιλογής ή εγγράφου, επαναφορά στο ίδιο μηχάνημα	6

Ανάγκη	Τι κάνει το filterit	Σημείο του καταλόγου
Email	**Βοηθός email** (Gmail, Outlook): το νήμα ψευδωνυμοποιείται πριν πάει στο AI, το προσχέδιο επιστρέφει πλήρες για έλεγχο	6, 8
Απόδειξη για τον DPO	**Audit trail** ανά συνομιλία: τι μασκαρίστηκε, πότε, από ποιον· **evidence pack** για οργανισμούς	1, 11
Πίνακας αντιστοίχισης	Κρυπτογραφημένος (AES-256-GCM) σε υποδομή ΕΕ (Γερμανία), ανά λογαριασμό, αυτόματη διαγραφή μετά από 30 ημέρες	7
Πού πάει το ψευδωνυμοποιημένο κείμενο	Στον πάροχο LLM που κατονομάζεται στον κατάλογο υποεπεξεργαστών (σήμερα Anthropic, εκτός ΕΕ), πάντα καλυμμένο. Περιορισμός σε παρόχους ΕΕ: σε ανάπτυξη	5

Τι δεν λύνει. Καμία ανίχνευση δεν είναι τέλεια. Το filterit δημοσιεύει τους αριθμούς ακρίβειάς του ανά επίπεδο ανίχνευσης στη σελίδα /accuracy και τους ελέγχει με κάθε έκδοση· διαβάστε τους πριν αποφασίσετε. Η επαναφορά τιμών γίνεται μόνο εκεί όπου φυλάσσεται ο πίνακας αντιστοίχισης. Και το ίδιο το μοντέλο AI μπορεί να «μαντέψει» ή να επινοήσει πρόσωπα. Αυτό δεν είναι διαρροή, αλλά είναι λόγος να ελέγχετε πάντα το αποτέλεσμα πριν το στείλετε.

6. Υπόδειγμα πολιτικής χρήσης AI (μία σελίδα)

Προσαρμόστε τα σημεία σε αγκύλες.

> **Πολιτική χρήσης εργαλείων τεχνητής νοημοσύνης: [Επωνυμία γραφείου]**
>
> 1. Επιτρέπεται η χρήση εργαλείων AI για [σύνταξη, μετάφραση, περίληψη, έλεγχο κειμένου] μόνο μέσω [εγκεκριμένα εργαλεία / λογαριασμοί].
>
> 2. Κανένα προσωπικό δεδομένο πελάτη ή τρίτου δεν αποστέλλεται σε εργαλείο AI χωρίς προηγούμενη ψευδωνυμοποίηση μέσω [εργαλείο]. Απαγορεύεται η χρήση προσωπικών/δωρεάν λογαριασμών για εργασία του γραφείου.
>
> 3. Δεδομένα υγείας, ποινικών καταδικών και λοιπών ειδικών κατηγοριών δεν αποστέλλονται σε εργαλείο AI, ακόμη και ψευδωνυμοποιημένα, χωρίς έγκριση από [υπεύθυνο].
>
> 4. Κάθε αποτέλεσμα εργαλείου AI ελέγχεται από άνθρωπο πριν χρησιμοποιηθεί ή αποσταλεί.
>
> 5. Οι χρήστες ενημερώνουν αμέσως τον [υπεύθυνο] αν υποψιάζονται ότι στάλθηκαν προσωπικά δεδομένα χωρίς ψευδωνυμοποίηση.
>
> 6. Η πολιτική επανεξετάζεται κάθε [12] μήνες και σε κάθε αλλαγή όρων των παρόχων.
>
> Ημερομηνία: [ ] · Υπεύθυνος: [ ] · Υπογραφή: [ ]

7. Σε 30 λεπτά, σήμερα

1. Ρωτήστε στο γραφείο: «Ποιος χρησιμοποιεί ChatGPT ή αντίστοιχο, και με ποιον λογαριασμό;» Γράψτε τις απαντήσεις (σημείο 1).
2. Απενεργοποιήστε την εκπαίδευση στις συνομιλίες σε όσους λογαριασμούς το επιτρέπουν, ή περάστε σε επιχειρησιακή έκδοση (σημείο 4).
3. Βάλτε ένα εργαλείο ψευδωνυμοποίησης στη ροή (στον browser ή στο Word), ώστε η προεπιλογή να είναι «μασκαρισμένο» (σημείο 6).
4. Μοιράστε την πολιτική της ενότητας 6 και ζητήστε υπογραφή (σημείο 9).

5 Κρατήστε αυτόν τον κατάλογο στον φάκελο του GDPR. Είναι η απόδειξη ότι το εξετάσατε (άρθρο 5 παρ. 2, λογοδοσία).

Το παρόν είναι γενική ενημέρωση και όχι νομική συμβουλή. Οι αναφορές στα άρθρα αφορούν τον Κανονισμό (ΕΕ) 2016/679 (GDPR), τον ν. 4624/2019 και τον Κανονισμό (ΕΕ) 2024/1689 (AI Act). Ελέγξτε τους τρέχοντες όρους κάθε παρόχου AI· αλλάζουν συχνά. Έκδοση Σεπτεμβρίου 2026 · filterit.ai