

Ασφαλής χρήση Τεχνητής Νοημοσύνης στον εργασιακό χώρο

Στόχοι

Κατανόηση των δυνατοτήτων και ορίων της AI

Οφέλη

Παραγωγικότητα, αυτοματοποίηση, δημιουργικότητα

Κίνδυνοι

Διαρροή δεδομένων, hallucinations, νομικά ζητήματα



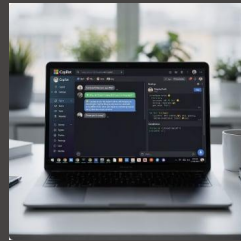
Τι είναι η παραγωγική Τεχνητή Νοημοσύνη;

Η παραγωγική AI (Generative AI) είναι η τεχνολογία που δημιουργεί κείμενο, εικόνες, κώδικα και άλλο περιεχόμενο βάσει φυσικής γλώσσας. Τα μεγάλα γλωσσικά μοντέλα (LLMs) έχουν εκπαιδευτεί σε τεράστιες ποσότητες δεδομένων και μπορούν να ανταποκρίνονται σε σύνθετα ερωτήματα.



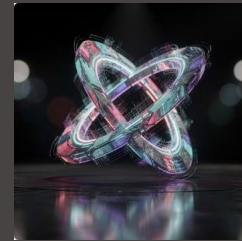
ChatGPT

Ανεπτυγμένο από την OpenAI. Ευρέως χρησιμοποιούμενο για κείμενο, ανάλυση και κώδικα.



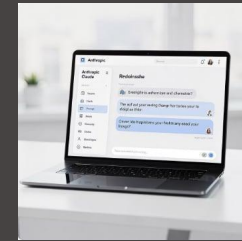
Microsoft Copilot

Ενσωματωμένο στο Microsoft 365. Αυτοματοποιεί εργασίες σε Word, Excel, Teams και Outlook.



Google Gemini

Η AI πλατφόρμα της Google. Ενσωματώνεται στο Google Workspace και τις υπηρεσίες αναζήτησης.



Claude (Anthropic)

Εστιάζει στην ασφάλεια και την ευθυγράμμιση. Ιδανικό για ανάλυση εγγράφων και συνομιλία.

Χρήσεις της AI στις επιχειρήσεις

Η παραγωγική AI μπορεί να επιταχύνει σημαντικά καθημερινές επαγγελματικές εργασίες. Από τη σύνταξη επικοινωνιών μέχρι την ανάλυση δεδομένων, οι εφαρμογές είναι πολυάριθμες — αρκεί να χρησιμοποιούνται με ασφάλεια.

1

Email & επικοινωνία

Σύνταξη, περίληψη και μετάφραση επαγγελματικών μηνυμάτων με συνέπεια ύφους και τόνου.

2

Έγγραφα & αναφορές

Δημιουργία προσχεδίων, δομημένων αναφορών και παρουσιάσεων από ακατέργαστες σημειώσεις.

3

Ανάλυση δεδομένων

Επεξεργασία δεδομένων σε υπολογιστικά φύλλα, εξαγωγή συμπερασμάτων και οπτικοποίηση αποτελεσμάτων.

4

Κώδικας & αυτοματισμός

Συγγραφή, εντοπισμός σφαλμάτων και τεκμηρίωση κώδικα σε δεκάδες γλώσσες προγραμματισμού.



Οφέλη της AI στον εργασιακό χώρο

Η σωστή αξιοποίηση των εργαλείων AI μπορεί να μεταμορφώσει τον τρόπο εργασίας — εξοικονομώντας χρόνο, μειώνοντας επαναλαμβανόμενες εργασίες και απελευθερώνοντας δημιουργικό δυναμικό.



Παραγωγικότητα

Μείωση χρόνου για επαναλαμβανόμενες εργασίες έως και 40%. Ταχύτερη σύνταξη εγγράφων, απαντήσεων και αναφορών.



Αυτοματοποίηση

Αυτόματη διεκπεραίωση ρουτίνας: ταξινόμηση email, δημιουργία εκθέσεων, σύνταξη τυποποιημένων εγγράφων.



Δημιουργικότητα

Παραγωγή και ανάπτυξη δημιουργικών ιδεών και συνδυαστικού περιεχομένου για σκοπούς marketing και επικοινωνίας.



Βαθύτερη ανάλυση

Εξαγωγή χρήσιμων πληροφοριών από μεγάλες ποσότητες κειμένου, εγγράφων ή δεδομένων σε δευτερόλεπτα.



Κίνδυνοι χρήσης AI

Παράλληλα με τα οφέλη, η χρήση AI ενέχει σοβαρούς κινδύνους που κάθε επαγγελματίας πρέπει να γνωρίζει. Η άγνοια δεν αποτελεί άλλοθι — η οργάνισμός φέρει ευθύνη για τα δεδομένα που διαχειρίζεται.

Διαρροή δεδομένων

Οι πληροφορίες που εισάγονται σε δημόσιες πλατφόρμες AI ενδέχεται να χρησιμοποιηθούν για εκπαίδευση μοντέλων ή να γίνουν προσβάσιμες σε τρίτους.

Hallucinations

Τα μοντέλα AI παράγουν μερικές φορές πληροφορίες που φαίνονται αληθινές αλλά είναι εντελώς ανακριβείς — χωρίς κανένα προειδοποιητικό σήμα.

Prompt injection

Κακόβουλες οδηγίες κρυμμένες σε έγγραφα ή ιστοσελίδες μπορούν να «ξεγελάσουν» το AI και να προκαλέσουν ανεπιθύμητες ενέργειες.

Δημόσιες υπηρεσίες AI

Οι δημόσιες πλατφόρμες AI — όπως το ChatGPT free tier, το Gemini ή το Claude.ai — προσφέρουν εύκολη πρόσβαση χωρίς κόστος, αλλά συνοδεύονται από σημαντικούς περιορισμούς για επαγγελματική χρήση.

Χαρακτηριστικά

- Δωρεάν ή χαμηλού κόστους πρόσβαση
- Δεν απαιτούν εγκατάσταση
- Άμεση διαθεσιμότητα μέσω browser
- Τακτικές ενημερώσεις μοντέλου

Περιορισμοί & κίνδυνοι

- Τα δεδομένα μπορεί να χρησιμοποιηθούν για εκπαίδευση
- Δεν υπάρχουν εγγυήσεις εμπιστευτικότητας
- Απουσία ελέγχου από τον οργανισμό
- Μη συμμόρφωση με GDPR σε πολλές περιπτώσεις



Ποτέ μην εισάγετε εταιρικά ή προσωπικά δεδομένα σε δημόσιες πλατφόρμες AI.



Enterprise AI: εταιρικές λύσεις

Οι Enterprise εκδόσεις των εργαλείων AI — όπως το Microsoft Copilot for Microsoft 365, το ChatGPT Enterprise ή το Google Workspace AI — παρέχουν ενισχυμένες εγγυήσεις ασφάλειας και συμμόρφωσης που τις καθιστούν κατάλληλες για επαγγελματική χρήση.

Εταιρικές πολιτικές

Τα δεδομένα παραμένουν εντός του εταιρικού tenant και δεν χρησιμοποιούνται για εκπαίδευση μοντέλων.

Έλεγχος πρόσβασης

Ο οργανισμός διαχειρίζεται ποιοι χρήστες έχουν πρόσβαση και σε ποια εργαλεία, μέσω κεντρικής διαχείρισης.

Συμμόρφωση & Audit

Υποστήριξη για GDPR, ISO 27001 και άλλα πρότυπα. Καταγραφή χρήσης και ελεγκσιμότητα.

SLA & Υποστήριξη

Επίπεδα υπηρεσιών, εγγυήσεις διαθεσιμότητας και εταιρική υποστήριξη για κρίσιμα περιβάλλοντα.

Δημόσια vs Enterprise AI

Η επιλογή μεταξύ δημόσιας και εταιρικής πλατφόρμας AI επηρεάζει άμεσα την ασφάλεια των δεδομένων του οργανισμού σας. Η παρακάτω σύγκριση αναδεικνύει τις βασικές διαφορές.

Δημόσια AI

-  **Απόρρητο:** Δεδομένα ενδέχεται να χρησιμοποιηθούν για εκπαίδευση
-  **GDPR:** Χωρίς εγγυήσεις συμμόρφωσης
-  **Πρόσβαση:** Καμία κεντρική διαχείριση
-  **Κόστος:** Δωρεάν / Χαμηλό κόστος
-  **Υποστήριξη:** Κοινότητα / Βασική
-  **Προσαρμογή:** Περιορισμένη

Enterprise AI

-  **Απόρρητο:** Δεδομένα παραμένουν εντός εταιρικού tenant
-  **GDPR:** GDPR & ISO 27001 συμβατό
-  **Πρόσβαση:** Κεντρική διαχείριση από οργανισμό
-  **Κόστος:** Συνδρομητικό μοντέλο
-  **Υποστήριξη:** SLA & Εταιρική υποστήριξη
-  **Προσαρμογή:** Ενσωματωμένη με εταιρικά εργαλεία

Δεδομένα που ΑΠΑΓΟΡΕΥΕΤΑΙ να εισάγονται σε AI

Ορισμένες κατηγορίες δεδομένων δεν πρέπει ποτέ να εισαχθούν σε εργαλεία AI — ιδίως σε δημόσιες πλατφόρμες. Η παραβίαση αυτού του κανόνα μπορεί να έχει σοβαρές νομικές και επιχειρηματικές συνέπειες.



Κωδικοί & credentials

Κωδικοί πρόσβασης, tokens, API keys, SSH keys και διαπιστευτήρια συστημάτων.



Πελατολόγια

Ονόματα, διευθύνσεις, τηλέφωνα, email και οποιαδήποτε προσωπικά στοιχεία πελατών (PII).



Συμβόλαια & νομικά

Εμπιστευτικά συμβόλαια, νομικές συμφωνίες και έγγραφα με ρήτρες εμπιστευτικότητας (NDA).



Οικονομικά δεδομένα

Μη δημοσιευμένα οικονομικά στοιχεία, προϋπολογισμοί, προβλέψεις και εμπιστευτικά reports.



Δεδομένα που επιτρέπονται

Δεν είναι όλα τα δεδομένα επικίνδυνα. Ορισμένες κατηγορίες μπορούν να χρησιμοποιηθούν με ασφάλεια στα εργαλεία AI, εφόσον έχουν ανωνυμοποιηθεί ή αφορούν ήδη δημόσιες πληροφορίες.

✓ Επιτρεπόμενα

- Ανωνυμοποιημένα κείμενα χωρίς αναγνωριστικά
- Δημόσιες πληροφορίες και ανοιχτά δεδομένα
- Γενικά ερωτήματα χωρίς εταιρικό περιεχόμενο
- Κείμενα εκπαίδευσης και θεωρητικά σενάρια
- Πρότυπα έγγραφα με υποθετικά παραδείγματα

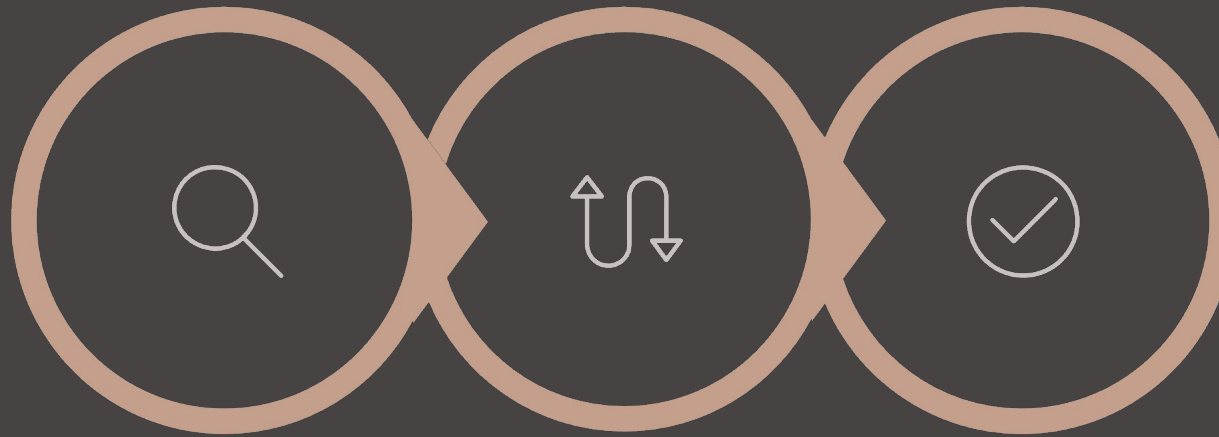
🔍 Σημείωση

Ακόμα και φαινομενικά αθώα δεδομένα μπορούν να γίνουν ευαίσθητα όταν συνδυαστούν. Ένας συνδυασμός τμήματος, ρόλου και ημερομηνίας μπορεί να οδηγήσει στην ταυτοποίηση ατόμου.

Εφαρμόστε την αρχή της **ελαχιστοποίησης δεδομένων**: δώστε μόνο ό,τι είναι απολύτως απαραίτητο για την εκτέλεση της εργασίας.

Ανωνυμοποίηση δεδομένων

Η ανωνυμοποίηση είναι η διαδικασία αφαίρεσης ή αντικατάστασης στοιχείων που μπορούν να ταυτοποιήσουν ένα άτομο, πριν από την εισαγωγή του κειμένου σε AI εργαλεία.



Εντοπισμός

Αντικατάσταση

Επαλήθευση

Παράδειγμα: Αντί για «Ο πελάτης Γεώργιος Παπαδόπουλος, ΑΦΜ 123456789», χρησιμοποιήστε «Ο πελάτης [CUSTOMER_A], αριθμός [TAX_ID]». Η ανωνυμοποίηση δεν πρέπει να συγχέεται με την ψευδωνυμοποίηση — η τελευταία εξακολουθεί να επιτρέπει ταυτοποίηση υπό συνθήκες.

AI και GDPR

Ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) εφαρμόζεται πλήρως στη χρήση AI εργαλείων. Η εισαγωγή προσωπικών δεδομένων σε μη εγκεκριμένες πλατφόρμες μπορεί να συνιστά παραβίαση του Κανονισμού.

Ελαχιστοποίηση δεδομένων (Art. 5)

Συλλέγετε και επεξεργάζεστε μόνο τα δεδομένα που είναι απολύτως απαραίτητα για τον συγκεκριμένο σκοπό. Μην εισάγετε επιπλέον πληροφορίες «για κάθε ενδεχόμενο».

Σκοπός επεξεργασίας (Art. 6)

Η επεξεργασία προσωπικών δεδομένων μέσω AI πρέπει να έχει συγκεκριμένη νόμιμη βάση. Η διαβίβαση σε τρίτους (ακόμα και μέσω AI) χωρίς συγκατάθεση ή σύμβαση είναι παράνομη.

Μεταφορά δεδομένων εκτός ΕΕ

Πολλές δημόσιες AI πλατφόρμες επεξεργάζονται δεδομένα σε servers εκτός ΕΕ. Αυτό απαιτεί πρόσθετες εγγυήσεις (SCCs, adequacy decisions) για να είναι νόμιμο.



Πνευματική ιδιοκτησία & AI

Η χρήση AI δεν αναστέλλει τους νόμους περί πνευματικής ιδιοκτησίας και εμπιστευτικότητας. Ό,τι εισάγετε ή λαμβάνετε από ένα AI εργαλείο υπόκειται στις ίδιες νομικές υποχρεώσεις με οποιοδήποτε άλλο έγγραφο.

Copyright

Μην εισάγετε κείμενα τρίτων που προστατεύονται από πνευματικά δικαιώματα. Οι εξόδοι του AI ενδέχεται να μην είναι πρωτότυπα έργα και να μην προστατεύονται αυτόματα.

Source code

Μην εισάγετε ιδιόκτητο κώδικα ή κώδικα με εταιρική άδεια. Ο κώδικας που παράγει το AI μπορεί να έχει ζητήματα άδειας χρήσης.

NDA & εμπιστευτικότητα

Αν έχετε υπογράψει συμφωνία εμπιστευτικότητας, η διαβίβαση πληροφοριών σε AI ενδέχεται να αποτελεί παραβίαση — ανεξάρτητα από την πλατφόρμα.

 Ελέγξτε πάντα την πολιτική χρήσης της πλατφόρμας AI σχετικά με τα δικαιώματα στο περιεχόμενο που εισάγετε.

Ασφαλή prompts: παραδείγματα σωστής χρήσης

Ένα καλά διατυπωμένο prompt μπορεί να επιτύχει εξαιρετικά αποτελέσματα χωρίς να θέτει σε κίνδυνο ευαίσθητες πληροφορίες. Ο κανόνας είναι απλός: **γενικεύστε, ανωνυμοποιήστε, περιγράψτε τον στόχο.**

1

Ανωνυμοποιημένη σύνοψη email

Κάνε μία περίληψη του παρακάτω email αφαιρώντας ονόματα: [κείμενο χωρίς ονόματα]»

✓ Χωρίς πραγματικά ονόματα ή διευθύνσεις

2

Γενικό ερώτημα κώδικα

«Πώς μπορώ να διαβάσω ένα JSON αρχείο σε Python;»

✓ Χωρίς εταιρικό κώδικα ή credentials

3

Θεωρητικό σενάριο

«Βοήθησέ με να γράψω μια πολιτική GDPR για μια υποθετική εταιρεία B2B SaaS»

✓ Δεν αποκαλύπτει πραγματικά δεδομένα

Prompts προς αποφυγή

Ορισμένοι τρόποι χρήσης της AI δημιουργούν σοβαρούς κινδύνους — ακόμα και όταν ο χρήστης δεν το αντιλαμβάνεται. Παρακάτω παρουσιάζονται χαρακτηριστικά παραδείγματα λανθασμένης χρήσης.

✗ Κωδικοί στο prompt

«Μπορείς να διορθώσεις αυτό το script;
API_KEY=sk-abc123...»
Ποτέ μην εισάγετε πραγματικά credentials
στο prompt.

✗ Πελατολόγιο για ανάλυση

«Ανάλυσε αυτή τη λίστα: Παπαδόπουλος
Γ. 6971234567, Νικολάου Μ.
6982345678...»
Απαγορεύεται η εισαγωγή πραγματικών
στοιχείων επικοινωνίας.

✗ Εμπιστευτικό συμβόλαιο

Κάνε μία περίληψη αυτού του συμβόλαιου:
[full text of confidential NDA]»
Συμβόλαια με ρήτρες εμπιστευτικότητας δεν
επιτρέπεται να διαβιβάζονται σε τρίτες
υπηρεσίες.

AI και email: ασφαλής πρακτική

Η χρήση AI για περίληψη, μετάφραση ή απάντηση email είναι ιδιαίτερα διαδεδομένη — αλλά συχνά γίνεται χωρίς τις απαραίτητες προφυλάξεις. Ακολουθήστε αυτά τα βήματα πριν «επικολλήσετε» οποιοδήποτε email σε AI πλατφόρμα.



❏ Εάν χρησιμοποιείτε το Microsoft Copilot μέσα στο Outlook του οργανισμού σας (Enterprise έκδοση), τα δεδομένα παραμένουν εντός του εταιρικού tenant και δεν απαιτείται ανωνυμοποίηση.

AI και Excel: κίνδυνοι με δεδομένα

Τα υπολογιστικά φύλλα συχνά περιέχουν συνδυασμούς ευαίσθητων πληροφοριών — οικονομικά στοιχεία, προσωπικά δεδομένα, εμπιστευτικές μετρήσεις. Η εισαγωγή τέτοιων δεδομένων σε AI απαιτεί ιδιαίτερη προσοχή.

Τι να αποφύγετε

- Αντιγραφή στηλών με ονόματα πελατών ή εργαζομένων
- Εισαγωγή μισθοδοτικών καταστάσεων ή ΑΦΜ
- Μη δημοσιευμένα οικονομικά αποτελέσματα
- Κωδικοί προϊόντων με εμπιστευτική τιμολόγηση

Ασφαλής χρήση

- Χρησιμοποιήστε ανώνυμα δείγματα δεδομένων (π.χ. Column A, Column B)
- Περιγράψτε τη δομή του αρχείου χωρίς πραγματικές τιμές
- Ζητήστε τύπους ή μακροεντολές με υποθετικά παραδείγματα
- Χρησιμοποιείτε Copilot εντός Microsoft 365 για πραγματικά δεδομένα

AI και προγραμματισμός

Τα εργαλεία AI είναι εξαιρετικοί βοηθοί για developers — αλλά ο κώδικας συχνά κρύβει ευαίσθητα δεδομένα που δεν πρέπει να φύγουν εκτός οργανισμού.



Secrets & tokens

Ποτέ μην εισάγετε API keys, OAuth tokens, database passwords ή οποιαδήποτε hardcoded credentials. Αντικαταστήστε με `YOUR_API_KEY` πριν το paste.



Ιδιωτικά repositories

Μην αντιγράφετε κώδικα από ιδιωτικά repositories που περιέχουν εταιρική λογική ή ιδιόκτητους αλγόριθμους. Χρησιμοποιήστε ψευδώνυμες δομές.



Εσωτερική αρχιτεκτονική

Αποφύγετε την κοινοποίηση διαγραμμάτων ή περιγραφών εσωτερικής αρχιτεκτονικής συστημάτων που θα μπορούσαν να χρησιμοποιηθούν από κακόβουλους.

AI και εικόνες: κρυφοί κίνδυνοι

Πέρα από το κείμενο, οι εικόνες και τα αρχεία που ανεβάζουμε στα AI εργαλεία μπορεί να περιέχουν ευαίσθητες πληροφορίες που δεν είναι άμεσα ορατές.

1

Metadata εικόνων

Τα EXIF δεδομένα φωτογραφιών μπορεί να περιέχουν GPS τοποθεσία, ημερομηνία, μοντέλο συσκευής και ονόματα αρχείων. Αφαιρέστε metadata πριν την ανάρτηση.

2

Πρόσωπα & βιομετρικά

Η ανάρτηση φωτογραφιών με αναγνωρίσιμα πρόσωπα εγείρει σοβαρά ζητήματα GDPR. Τα βιομετρικά δεδομένα ανήκουν στις «ειδικές κατηγορίες» του Κανονισμού.

3

Screenshots συστημάτων

Screenshots από εσωτερικά συστήματα, ERP, CRM ή emails αποκαλύπτουν πληροφορίες για αρχιτεκτονική, διαδικασίες και εμπιστευτικά δεδομένα.

Hallucinations: όταν το AI «εφευρίσκει»

Τα μεγάλα γλωσσικά μοντέλα δεν «ξέρουν» με την ανθρώπινη έννοια — παράγουν κείμενο που στατιστικά «ακούγεται σωστό», ακόμα και αν δεν είναι. Αυτό το φαινόμενο ονομάζεται **hallucination** και αποτελεί έναν από τους σημαντικότερους κινδύνους.

Γιατί συμβαίνουν;

- Το μοντέλο προβλέπει την επόμενη λέξη, όχι την αλήθεια
- Δεν έχει πρόσβαση σε πραγματικό χρόνο (συνήθως)
- Προσπαθεί πάντα να δώσει μια απάντηση
- Τα training data μπορεί να περιέχουν λάθη

Πώς εντοπίζονται;

- Ελέγξτε τυχόν αναφορές σε πηγές — ζητήστε από το AI να τις παραθέσει
- Επαληθεύστε αριθμούς, ημερομηνίες και ονόματα
- Αναζητήστε ασυνέπειες μέσα στο κείμενο
- Χρησιμοποιήστε το AI ως πρώτο βήμα, όχι ως τελική πηγή

Επαλήθευση απαντήσεων AI

Κανένα αποτέλεσμα AI δεν πρέπει να χρησιμοποιείται χωρίς ανθρώπινο έλεγχο — ιδιαίτερα σε επαγγελματικά ή νομικά ευαίσθητα πλαίσια. Η επαλήθευση δεν είναι επιλογή, είναι υποχρέωση.



AI παράγει

Άνθρωπος
ελέγχει

Εγκρίνεις ή
διορθώνεις

Διασταύρωση πηγών

Για κρίσιμες πληροφορίες, επαληθεύστε πάντα σε επίσημες, αξιόπιστες πηγές (νομοθεσία, επίσημα sites, επιστημονικές δημοσιεύσεις).

Ανθρώπινη κρίση

Ο τελικός ελεγκτής είναι πάντα ο άνθρωπος. Η χρήση AI δεν απαλλάσσει τον εργαζόμενο από την επαγγελματική ευθύνη για τα αποτελέσματα της εργασίας του.



Πραγματικά περιστατικά διαρροών μέσω AI

Τα περιστατικά κατάχρησης AI εργαλείων δεν είναι θεωρητικά. Έχουν ήδη καταγραφεί σημαντικές παραβιάσεις από γνωστές εταιρείες παγκοσμίως.

Samsung (2023)

Μηχανικοί της Samsung ανέβασαν εμπιστευτικό πηγαίο κώδικα και εσωτερικές συσκέψεις στο ChatGPT για βοήθεια. Η εταιρεία απαγόρευσε αμέσως τη χρήση AI χωρίς έγκριση.

Νομικά γραφεία (2023)

Δικηγόροι στις ΗΠΑ υπέβαλαν νομικά υπομνήματα με «ψεύτικες» υποθέσεις που είχε «εφεύρει» το ChatGPT — και τιμωρήθηκαν από το δικαστήριο.

Διδάγματα

Κάθε περιστατικό υπογραμμίζει το ίδιο μάθημα: η έλλειψη πολιτικής χρήσης AI σε επίπεδο οργανισμού οδηγεί αναπόφευκτα σε παραβιάσεις. Ο ανθρώπινος έλεγχος είναι αδιαπραγμάτευτος.

Checklist: 20 βασικές οδηγίες ασφαλούς χρήσης AI

Χρησιμοποιήστε αυτή τη λίστα ως καθημερινό οδηγό πριν από κάθε χρήση εργαλείων AI στον εργασιακό σας χώρο.

- ☐ Χρησιμοποιώ εγκεκριμένη εταιρική πλατφόρμα AI
- ☐ Δεν εισάγω κωδικούς ή API keys
- ☐ Δεν εισάγω πελατολόγια ή PII
- ☐ Ανωνυμοποιώ πριν εισάγω κείμενα
- ☐ Δεν ανεβάζω εμπιστευτικά συμβόλαια
- ☐ Δεν εισάγω μη δημοσιευμένα οικονομικά
- ☐ Δεν χρησιμοποιώ δημόσιο AI για εταιρικά θέματα
- ☐ Επαληθεύω όλες τις απαντήσεις του AI
- ☐ Δεν αναθέτω τελικές αποφάσεις στο AI
- ☐ Αφαιρώ metadata από εικόνες πριν την ανάρτηση
- ☐ Δεν εισάγω screenshots εσωτερικών συστημάτων
- ☐ Δεν εισάγω ιδιωτικό κώδικα εταιρείας
- ☐ Ελέγχω την πολιτική χρήσης της πλατφόρμας
- ☐ Ενημερώνω το IT για νέα εργαλεία AI που χρησιμοποιώ
- ☐ Δεν παρακάμπτω εταιρικές πολιτικές ασφάλειας
- ☐ Χρησιμοποιώ AI ως βοηθό, όχι ως αυθεντία
- ☐ Διατηρώ ανθρώπινο έλεγχο στο τελικό αποτέλεσμα
- ☐ Γνωρίζω τη διαδικασία αναφοράς περιστατικού
- ☐ Παρακολουθώ ενημερώσεις πολιτικής AI οργανισμού
- ☐ Συμμορφώνομαι με GDPR σε κάθε χρήση AI

Quiz: σωστή ή λανθασμένη χρήση;

Ελέγξτε τις γνώσεις σας! Για κάθε σενάριο αποφασίστε αν η χρήση AI είναι **αποδεκτή**  ή **προβληματική**  — και γιατί.

Σενάριο Α

«Ζητώ από το ChatGPT free να μου γράψει ένα πρότυπο email για αίτηση άδειας, χωρίς να αναφέρω ονόματα ή εταιρεία.»

 **Αποδεκτό** — Δεν περιλαμβάνει ευαίσθητα δεδομένα.

Σενάριο Β

«Ανεβάζω το συμβόλαιο με έναν προμηθευτή στο Gemini για να πάρω περίληψη — είναι πιο γρήγορο.»

 **Προβληματικό** — Εμπιστευτικά έγγραφα δεν εισάγονται σε δημόσια AI.

Σενάριο Γ

«Χρησιμοποιώ το Copilot μέσα στο Outlook του οργανισμού μου (M365) για να παραλάβω ένα εσωτερικό email.»

 **Αποδεκτό** — Enterprise πλατφόρμα εντός εταιρικού tenant.

Σενάριο Δ

«Επικολλώ λίστα πελατών με ΑΦΜ στο Claude για να βρω διπλοεγγραφές.»

 **Προβληματικό** — Παραβίαση GDPR και εταιρικής πολιτικής.

A vertical image on the left side of the slide showing a city skyline at sunset. The sun is low on the horizon, casting a warm orange glow over the skyscrapers and the street below. The buildings are silhouetted against the bright sky, and the street is filled with cars and lights.

Συμπεράσματα: ΑΙ με ασφάλεια και συμμόρφωση

Η Τεχνητή Νοημοσύνη είναι ένα ισχυρό εργαλείο που αλλάζει τον τρόπο εργασίας. Η ασφαλής χρήση της δεν είναι εμπόδιο στην παραγωγικότητα — είναι η βάση για να την αξιοποιήσουμε υπεύθυνα και αποτελεσματικά.



Προστατέψτε τα δεδομένα

Ανωνυμοποιήστε πριν εισάγετε. Χρησιμοποιήστε εγκεκριμένες εταιρικές πλατφόρμες. Μην εισάγετε εμπιστευτικές πληροφορίες.



Επαληθεύετε πάντα

Κανένα αποτέλεσμα ΑΙ δεν είναι αλάνθαστο. Ο ανθρώπινος έλεγχος παραμένει αδιαπραγμάτευτος σε κάθε επαγγελματικό πλαίσιο.



Συμμορφωθείτε

Ακολουθήστε το GDPR, τις εταιρικές πολιτικές και τους κανόνες πνευματικής ιδιοκτησίας. Η άγνοια δεν αποτελεί νομική υπεράσπιση.



Για ερωτήσεις ή αναφορά περιστατικών, επικοινωνήστε με την ομάδα IT Security του οργανισμού σας.