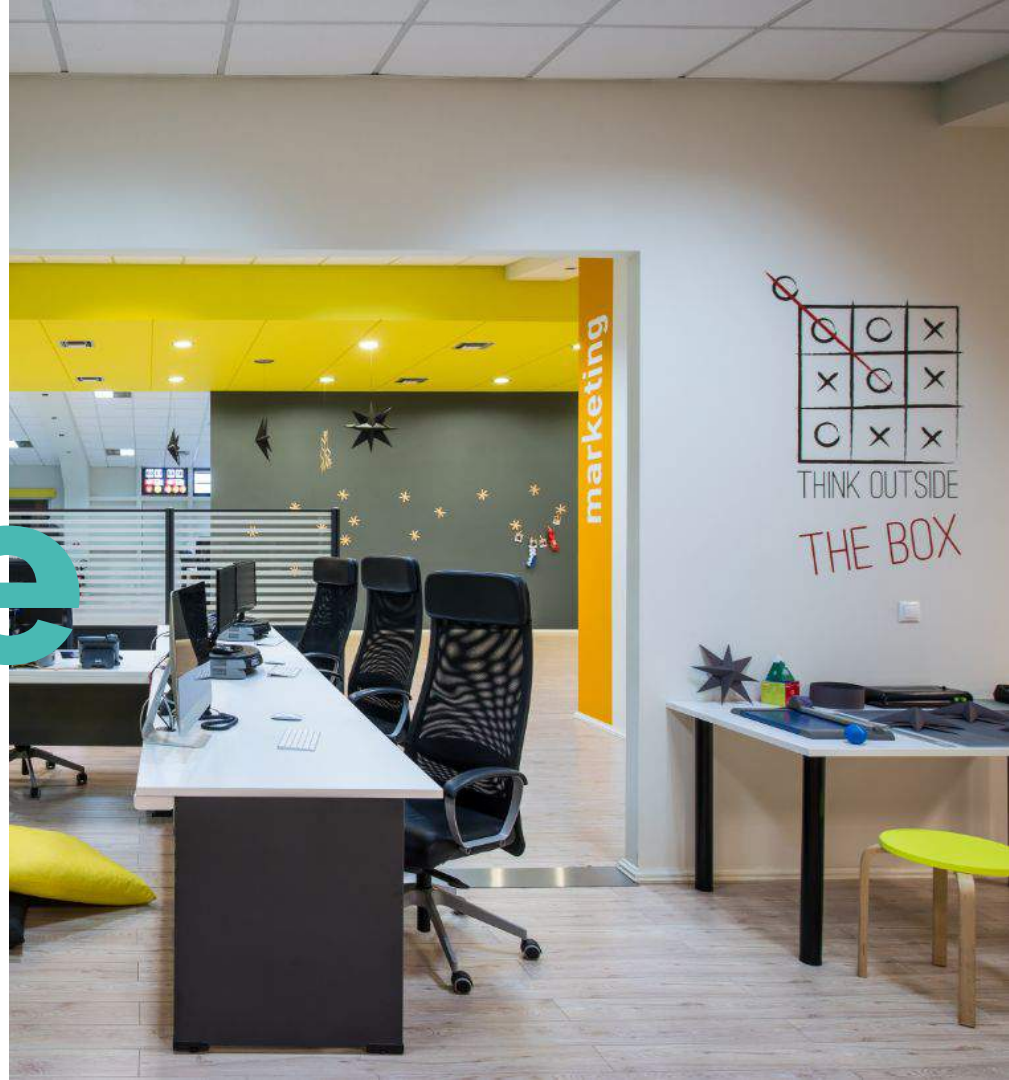
enartia
GROUP OF BRANDS

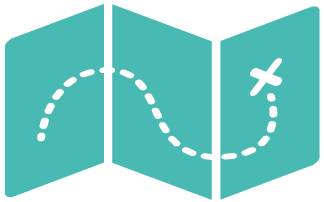
Culture

Building for Privacy and Data Protection



Standards - Frameworks

- BS10012
- ISO27701
- NIST Privacy Framework
- Nymity™ Privacy Management and Accountability Framework (PMAF)



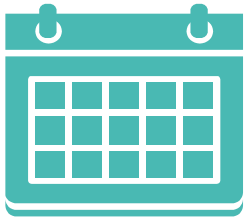
enartia
GROUP OF BRANDS

Δομή διακυβέρνησης

- Ανάθεση ευθύνης για την προστασία δεδομένων σε ένα άτομο.
- Ορισμός Υπευθύνου Προστασίας Δεδομένων (DPO) σε ανεξάρτητο ρόλο εποπτείας.
- Διατήρηση των ρόλων και αρμοδιοτήτων των ατόμων που είναι υπεύθυνα για την επεξεργασία δεδομένων προσωπικού χαρακτήρα (π.χ. περιγραφές θέσεων εργασίας)
- Διεξαγωγή τακτικής επικοινωνίας μεταξύ του Υπευθύνου Επεξεργασίας, ΥΠΔ, και άλλων υπεύθυνων για την προστασία προσωπικών δεδομένων

Αρχείο Δραστηριοτήτων

- Διατήρηση καταλόγου των δεδομένων προσωπικού χαρακτήρα (ποια προσωπικά δεδομένα διατηρούνται και πού βρίσκονται)
- Διατήρηση αρχείων του μηχανισμού μεταφοράς για διασυνοριακές ροές δεδομένων (π.χ. τυποποιημένες συμβατικές ρήτρες, δεσμευτικοί εταιρικοί κανόνες, εγκρίσεις από ρυθμιστικές αρχές)



Πολιτική προστασίας δεδομένων

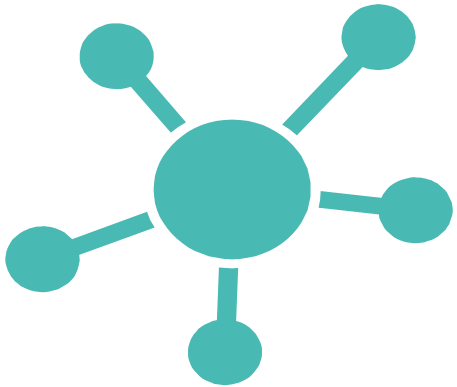
- Αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα
  (νομιμότητα, αντικειμενικότητα και διαφάνεια, περιορισμός του σκοπού, ελαχιστοποίηση, κλπ.)
- Διακυβέρνηση και λογοδοσία
- Διαχείριση παραβιάσεων και γνωστοποιήσεις
- Δικαιώματα των υποκειμένων των δεδομένων
- Προστασία δεδομένων από το σχεδιασμό και εξ ορισμού
- Εκτίμηση Αντικτύπου Προσωπικών Δεδομένων (ΕΑΠΔ)
- Εκτελούντες την Επεξεργασία

enartia
GROUP OF BRANDS

Ενσωμάτωση στις λειτουργίες του οργανισμού

Διατήρηση πολιτικών / διαδικασιών συλλογής και χρήσης προσωπικών δεδομένων σχετικά με:

- Κοινωνικα δίκτυα
- Ερευνητικές πρακτικές
- Παιδιά και ανήλικους
- Διαγραφή των προσωπικών δεδομένων
- Προκηρύξεις - Συμβάσεις
- Έγκυρη συναίνεση



Πρόγραμμα Εκπαίδευσης και Ευαισθητοποίησης

- Ετήσια εκπαίδευση για **όλους**
- Case studies με χρήση δημοφιλών εφαρμογών/υπηρεσιών
- Εξειδικευμένη εκπαίδευση για προϊσταμένους, marketing, HR, προγραμματιστές
- Συνεχής υπενθύμιση μέσω δραστηριοτήτων και ενεργειών
- Παραδείγματα (καλά και άσχημα) από άλλους οργανισμούς
- Data Protection Coordinators / Privacy Champions

enartia
GROUP OF BRANDS

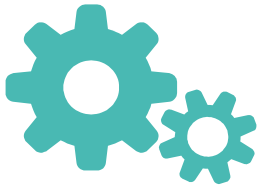
Διαχείριση κινδύνου ασφάλειας πληροφοριών

- Διατήρηση τεχνικών μέτρων ασφάλειας
  (π.χ. ανίχνευση εισβολών, τείχη προστασίας, παρακολούθηση)
- Μέτρα κρυπτογράφησης των προσωπικών δεδομένων κατά τη μεταφορά και αποθήκευση
- Διαδικασίες για τον περιορισμό της πρόσβασης σε προσωπικά δεδομένα
  (π.χ. πρόσβαση βάσει ρόλου, διαχωρισμός καθηκόντων)
- Τακτικοί έλεγχοι της στάσης ασφαλείας δεδομένων
  (ασκήσεις παρείσδυσης, αυτοματοποιημένη αναγνώριση ευπαθειών, επιθεωρήσεις)

enartia
GROUP OF BRANDS

Διαχείριση κινδύνου τρίτων

- Διατηρήστε τις απαιτήσεις προστασίας δεδομένων για τρίτους (π.χ. πελάτες, προμηθευτές, εκτελούντες την επεξεργασία, συνεργάτες)
- Διατηρήστε διαδικασίες για την εκτέλεση συμβάσεων ή συμφωνιών με όλους τους εκτελούντες
- Αρθρο 28 GDPR - και πως εφαρμόζεται
- Διεξαγωγή της δέουσας επιμέλειας (due diligence) σχετικά με την προστασία των δεδομένων και τη στάση ασφαλείας των τρίτων



enartia
GROUP OF BRANDS

Διατήρηση ειδοποιήσεων

- Ποιοί είμαστε
- Τι προσωπικά δεδομένα συλλέγουμε και γιατί
- Για πόσο καιρό διατηρούμε τα δεδομένα
- Περιεχόμενο από άλλα websites
- Cookies, Analytics, Διαφήμιση και Marketing
- Ασφάλεια δεδομένων
- Επικοινωνία με DPO
- Δικαιώματα των χρηστών

enartia
GROUP OF BRANDS

Απάντηση σε αιτήματα και καταγγελίες

- Διαδικασίες για απάντηση σε αιτήματα ενημέρωσης, πρόσβασης, διόρθωσης, φορητότητας, διαγραφής, εναντίωσης κλπ.
- Εκπαίδευση όλου του οργανισμού στην αναγνώριση των αιτημάτων
- Δοκιμές/τεστ ετοιμότητας

Παρακολούθηση νέων επιχειρησιακών πρακτικών

- Ενσωμάτωση της Προστασίας Προσωπικών Δεδομένων από το σχεδιασμό σε ανάπτυξη συστημάτων και προϊόντων
- Διατήρηση οδηγιών και πρότυπα για ΕΑΠΔ (DPIA)
- Συμμετοχή εξωτερικών ενδιαφερομένων (π.χ. ατόμων, ΜΚΟ) στο πλαίσιο της διαδικασίας ΕΑΠΔ
- Αναφέρετε την ανάλυση ΕΑΠΔ και τα αποτελέσματα στις ρυθμιστικές αρχές (όπου απαιτείται) και τους εξωτερικούς ενδιαφερόμενους (εάν χρειάζεται)

enartia
GROUP OF BRANDS

Πρόγραμμα διαχείρισης παραβιάσεων

- Σχέδιο απόκρισης περιστατικού παραβίασης δεδομένων
- Ειδοποίηση παραβίασης (στα ενδιαφερόμενα άτομα) και υποβολή αναφοράς (σε ρυθμιστικές αρχές, πιστωτικές υπηρεσίες, αστυνομικές αρχές)
- Διατηρήστε ένα αρχείο καταγραφής για να εντοπίσετε περιστατικά / παραβιάσεις απορρήτου δεδομένων

Παρακολούθηση εξωτερικών κριτηρίων

- Αρχές Προστασίας άλλων χωρών, όχι μόνο της Ε.Ε.
- Νομοθεσία / νομολογία
- Καλές πρακτικές
- Κώδικες δεοντολογίας
- CJEU
- EDPS
- EDPB

Σχετικά με Ηθική - Ερωτήσεις - Αυτοαξιολόγηση

1. Η εφαρμογή σας είναι σχεδιασμένη για να σεβαστεί την αυτονομία και ψηφιακή αξιοπρέπεια των υποκειμένων;

2. Οι καταναλωτές αντιλαμβάνονται ένα πραγματικό πλεονέκτημα, ή δημιουργείται ασυμμετρία δύναμης;

3. Οι πρακτικές σας είναι διάφανες και υπάρχει λογοδοσία, με τη δυνατότητα να αντιστραφεί ή ακούσια ζημιά;

4. Έχετε σχεδιάσει τις τεχνολογίες σας για να αποφύγετε τις ακούσιες προκαταλήψεις και τις απρόβλεπτες χρήσεις;

5. Ποιοι μηχανισμοί είναι τοποθετημένοι ώστε να αποτρέψουν και να ανιχνεύσουν τους αντιπάλους (και κακόβουλους συνεργάτες) με πρόσβαση σε δεδομένα και στην επιρροή αλγορίθμων;

enartia
GROUP OF BRANDS

Με απλά λόγια:

1. Μην προκαλέσετε έκπληξη - Do Not Surprise
2. Αναλάβετε την Ευθύνη των Αποτελεσμάτων - Own the Outcomes
3. Αναρωτηθείτε, αν αυτή η επεξεργασία αφορούσε εσάς, ή τους αγαπημένους σας;

enartia
GROUP OF BRANDS

Quiz

1. A friend gave you a USB stick with the final season of Game of Thrones.
   What do you do?

   a. Grab a bag of popcorn and binge watch it, Dracaris!

   b. Scan the USB stick using your antivirus before opening any file, then watch it.

   c. Throw the USB stick in the sea, winter is coming.

   d. Explain that you are not allowed to use USB sticks because they are evil.

Quiz

1. Which of these cases would require valid consent?

   a. A controller wants to monitor data subjects for public safety.

   b. A controller wants to profile data subjects for the improvement of services.

   c. A processor wants to profile data subjects without the controllers permission.

   d. The controller and processor want to profile data subjects separately.

Privacy needs you!

Be a Champion

enartia
GROUP OF BRANDS

Ελαφρύ διάβασμα για καλοκαιρινά απογεύματα...

EU Personal Data Protection in Policy and Practice - Custers, Sears, Dechesne, Georgieva, Tani, Van der Hof

Privacy on the Ground: Driving Corporate Behavior in the United States and Europe - Bamberger, Kenneth A.

Ethical Data and Information Management. Concepts, tools and methods - O'Keefe, O' Brien

The Foundations of EU Data Protection Law - Lynskey

Surveillance, Privacy and Trans-Atlantic Relations - Cole, Fabbrini and Schulhofer

Consent in European Data Protection Law - Eleni Kosta

Handling and Exchanging Electronic Evidence Across Europe - Biasiotti, Mifsud Bonnici, Cannataci, Turchi

Blockchain and the Law - De Filippi, Wright

Οτιδήποτε από το EDPB & EDPS

Οδηγοί - Παραδείγματα - Εργαλεία

DPA Cyprus: Οδηγός Συμπλήρωσης Αρχείου Δραστηριοτήτων v3.pdf

DPA Cyprus: Αρχείο Δραστηριοτήτων.xlsx

DPA Norway: Software development with Data Protection by Design and by Default

DPA UK: Lawful basis interactive guidance tool

DPA UK: DPIA Template

EDPS: Website Evidence Collector

Thanks!

Λευτέρης
Σταυρακάκης

dpo@enartia.com