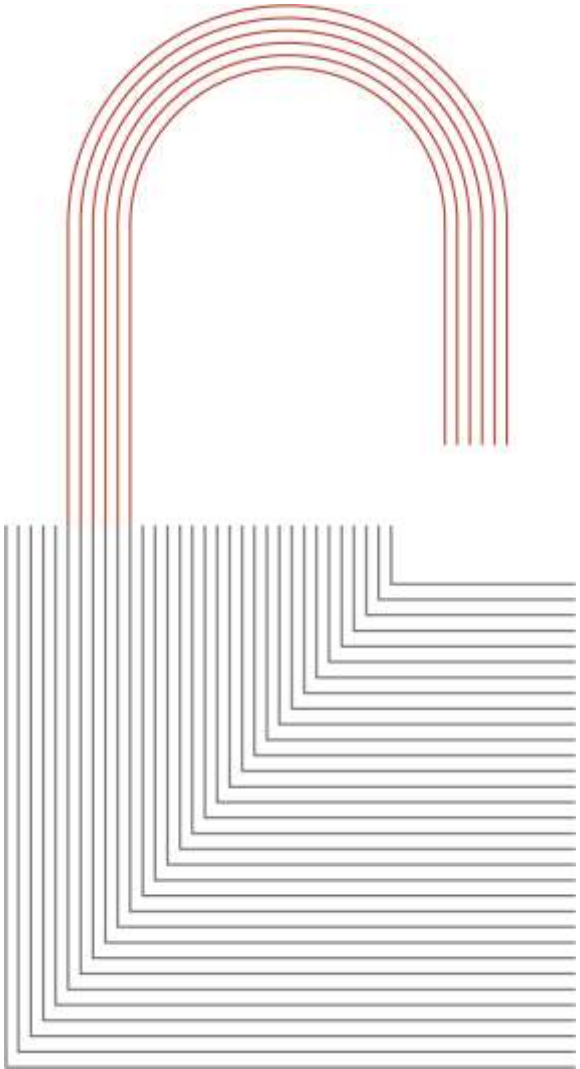
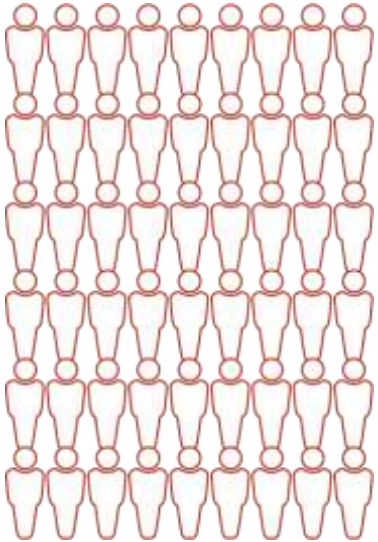
ΖΕΠΟΣ & ΓΙΑΝΝΟΠΟΥΛΟΣ

Ένας χρόνος GDPR:
Οι προκλήσεις για τις επιχειρήσεις, ο ρόλος των εποπτικών αρχών & η αυριανή ημέρα

25.06.2019

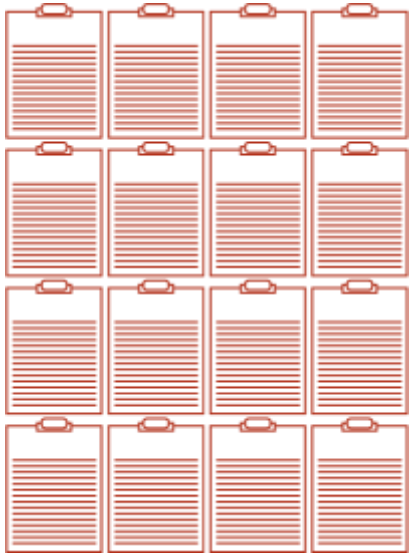


Ένας χρόνος GDPR: που βρισκόμαστε;



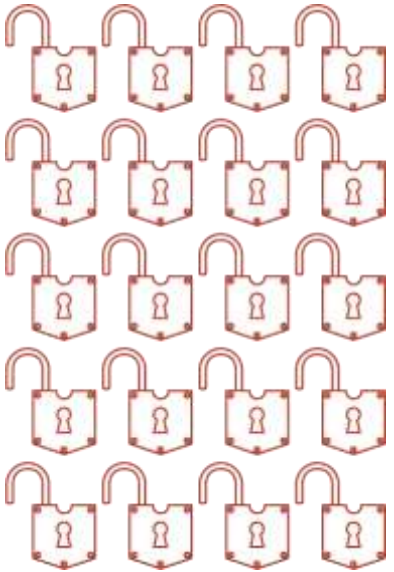
500.000+

διορισμένοι DPOs



144.000+

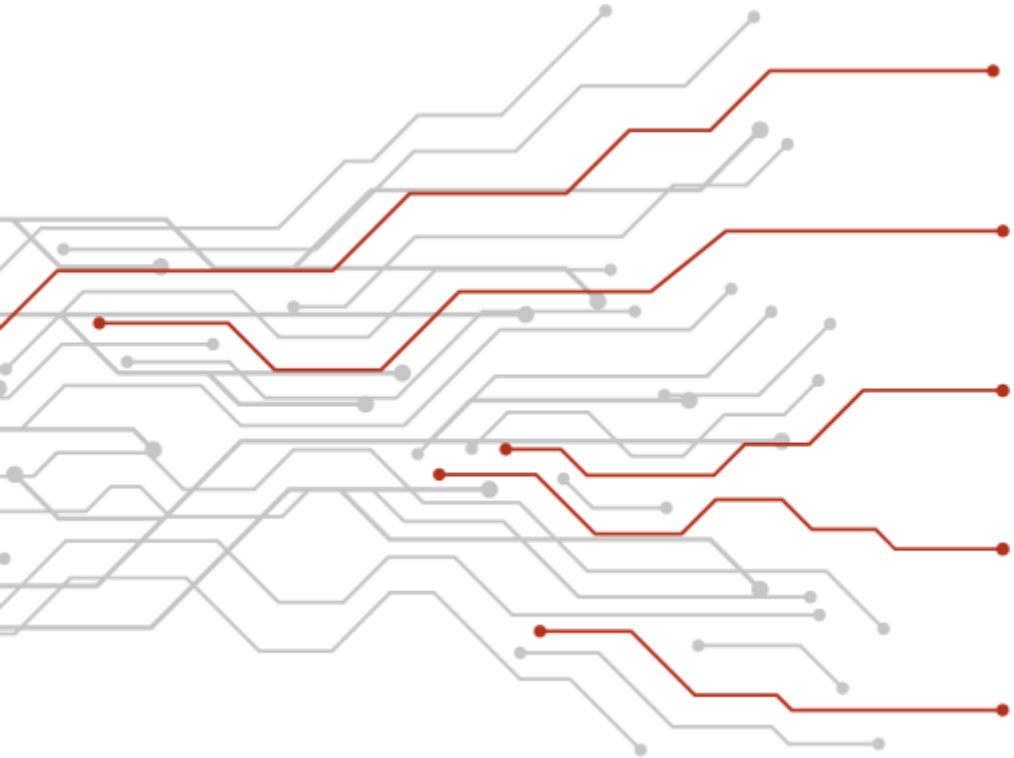
καταγγελίες



89.000+

περιστατικά παραβίασης δεδομένων

Οι μεγαλύτερες προκλήσεις για τις επιχειρήσεις



Έλλειψη κουλτούρας ιδιωτικότητας

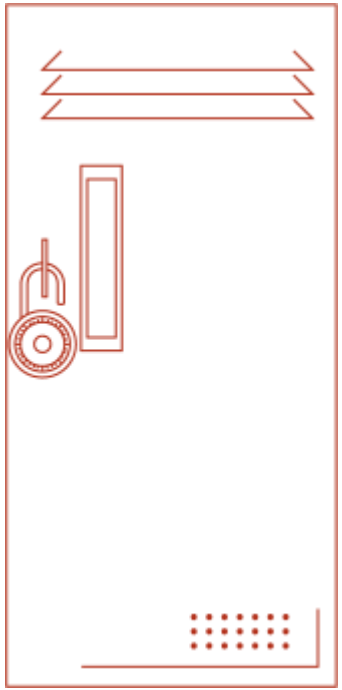
Διαχείριση περιστατικών παραβίασης

Συμβάσεις ανάθεσης επεξεργασίας

Χρόνοι τήρησης των δεδομένων

Ελλιπές νομοθετικό πλαίσιο

Έλλειψη κουλτούρας ιδιωτικότητας



- Αντιμετώπιση του GDPR ως ένα επιπλέον βάρος που συνεπάγεται δυσβάσταχτο κόστος
- Minimum συμμόρφωση με έτοιμα «πακέτα συμμόρφωσης» ή απευθείας εφαρμογή πολιτικών του ομίλου χωρίς τοπική παραμετροποίηση
- Διορισμός DPOs χωρίς ουσιαστικό ρόλο και λόγο στις δραστηριότητες των οργανισμών
- Εσφαλμένη εντύπωση της διοίκησης ότι «*επιτέλους τελειώσαμε με τον GDPR!*»

Διαχείριση περιστατικών παραβίασης

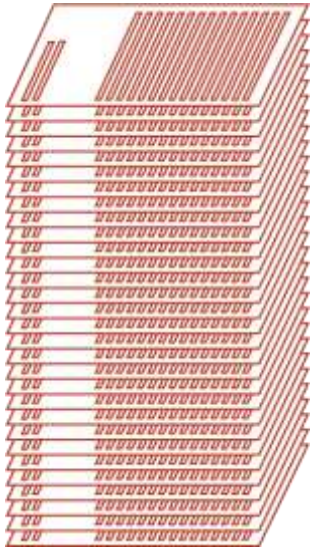
Διαφορετική αντιμετώπιση για το πότε μία παραβίαση πρέπει να γνωστοποιηθεί

Πού τοποθετείται ο πήχης για το πότε η παραβίαση προκαλεί κίνδυνο ή υψηλό κίνδυνο στα φυσικά πρόσωπα;

Βλάβη φήμης, κλονισμός εμπιστοσύνης των καταναλωτών και κίνδυνος για ελέγχους της εποπτικής αρχής

Πώς θα γίνονται λελογισμένα οι γνωστοποιήσεις, ώστε να μετριασθεί η επιβάρυνση των εποπτικών αρχών;

Συμβάσεις ανάθεσης επεξεργασίας



Δυσκολία εντοπισμού των παρόχων που έχουν πρόσβαση σε προσωπικά δεδομένα του οργανισμού

Διαφωνίες στον ρόλο των παρόχων (εκτελούντες, ανεξάρτητοι υπεύθυνοι ή από κοινού υπεύθυνοι;)

Συμβάσεις ανάθεσης επεξεργασίας

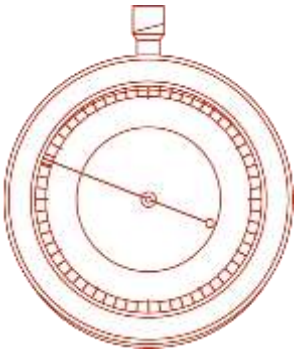
Αντιρρήσεις των παρόχων να αναλάβουν τις minimum υποχρεώσεις που θέτει το άρ. 28 GDPR λόγω άγνοιας του νέου πλαισίου ή ελλειπούς συμμόρφωσης

Bras de fer επί των όρων της σύμβασης, που είναι συχνά μη διαπραγματεύσιμοι (“*take it or leave it*”)

Συχνότερα σημεία τριβής μεταξύ υπευθύνων και εκτελούντων:

+ ευθύνη εκτελούντος
+ τεχνικά και οργανωτικά μέτρα
+ διορισμός υπεργολάβων

Χρόνοι τήρησης των δεδομένων



«*Κρατάμε τα πάντα σε περίπτωση που τα χρειαστούμε στο μέλλον!*»

Άσκηση που απαιτεί γνώση ποικίλων διατάξεων από διαφορετικούς κλάδους δικαίου (π.χ. εργατικό, κοινωνικο-ασφαλιστικό, τραπεζικό, φορολογικό κλπ.)

Ελλιπές νομοθετικό πλαίσιο

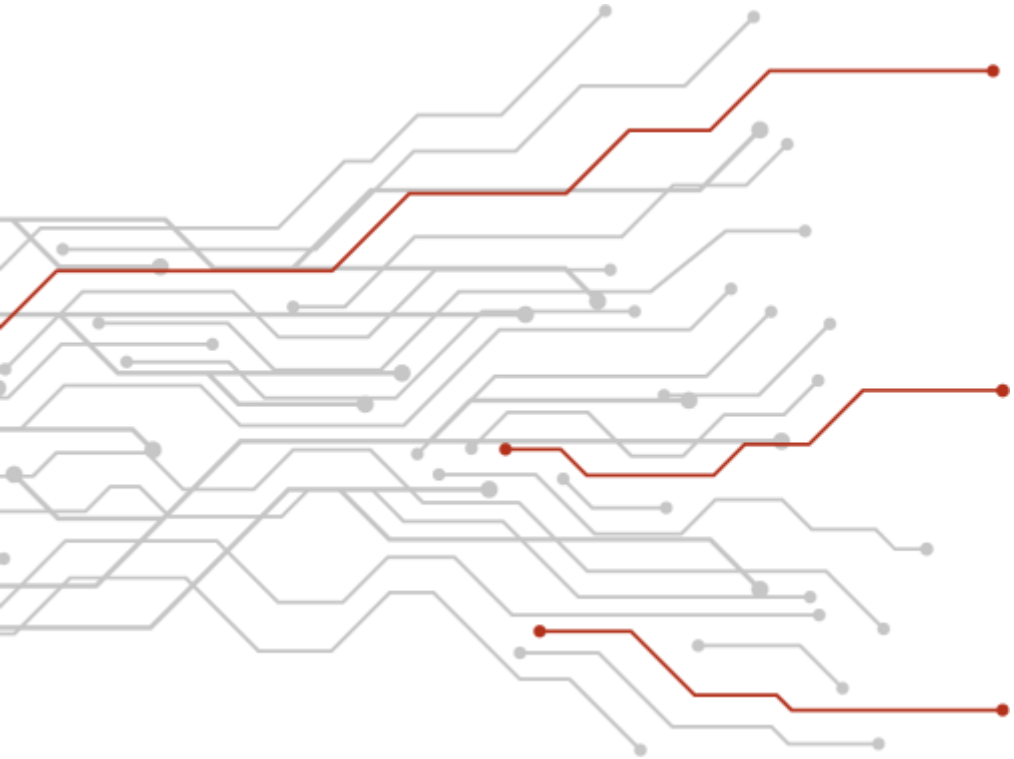
- Η Ελλάδα μία από τις τελευταίες 3 χώρες που δεν έχει ψηφίσει τον εκτελεστικό νόμο του GDPR

- Ανάγκη αναθεώρησης πολιτικών και διαδικασιών μετά την ψήφιση του

- Σημαντικά θέματα που αναμένεται να περιλαμβάνονται στο νόμο:

  + Δεδομένα εργαζομένων
  + Δεδομένα υγείας, γενετικά και βιομετρικά
  + Ποινικές καταδίκες και αδικήματα
  + Περιορισμοί των δικαιωμάτων των υποκειμένων
  + Πρόσθετες περιπτώσεις για προηγούμενη διαβούλευση
  + Ποινικές κυρώσεις

Ο ρόλος των εποπτικών αρχών

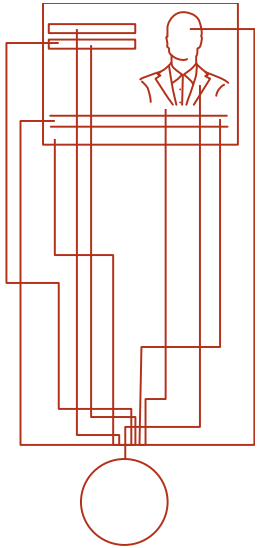


Κατευθυντήριες οδηγίες του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων (EDPB)

Οδηγίες και εργαλεία της Ελληνικής ΑΠΔΠΧ

Οδηγίες και εργαλεία άλλων Ευρωπαϊκών εποπτικών αρχών

Ο ρόλος των εποπτικών αρχών



- Κυρίως καθοδηγητικός τόσο σε Ευρωπαϊκό όσο και σε εθνικό επίπεδο

- Λίγα πρόστιμα παρά τον τεράστιο αριθμό καταγγελιών και γνωστοποιήσεων παραβίασης προσωπικών δεδομένων

Πιθανές αιτίες

- Παροχή σιωπηρής περιόδου χάριτος
- Και οι ίδιες οι αρχές ήταν ανέτοιμες
- Ενασχόληση με παλαιότερες σημαντικές υποθέσεις

Κατευθυντήριες οδηγίες του EDPB

16 guidelines του WP29 εγκρίθηκαν

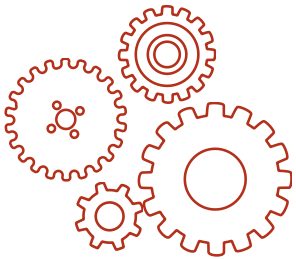
6 νέα guidelines εκδόθηκαν

4 opinions εκδόθηκαν

Σημαντικότερα θέματα:

+ Εδαφική εφαρμογή του GDPR
+ Ενημέρωση και εγκυρότητα συγκατάθεσης
+ Γνωστοποίηση περιστατικών παραβίασης
+ Υπεύθυνοι Προστασίας Δεδομένων
+ Διαβιβάσεις δεδομένων εκτός ΕΕ/ΕΕΑ χωρίς κατάλληλες εγγυήσεις
+ Αυτοματοποιημένη λήψη αποφάσεων και κατάρτιση προφίλ
+ Κατάλογοι πράξεων επεξεργασίας που απαιτούν DPIA
+ Μηχανισμοί πιστοποίησης
+ Συσχετισμός ePrivacy Directive και GDPR

Οδηγίες και εργαλεία της Ελληνικής ΑΠΔΠΧ



- Υποδείγματα αρχείων δραστηριοτήτων επεξεργασίας
- Έντυπο γνωστοποίησης περιστατικών παραβίασης δεδομένων
- Λίστα πράξεων επεξεργασίας για τις οποίες απαιτείται DPIA
- Υποδείγματα καταγγελιών ανάλογα με την φύση της καταγγελίας
- Έντυπο ορισμού DPO ενώπιον της ΑΠΔΠΧ
- Φόρμα για προηγούμενη διαβούλευση με την ΑΠΔΠΧ

Οδηγίες και εργαλεία άλλων Ευρωπαϊκών εποπτικών αρχών

ICO
Ηνωμένο Βασίλειο
https://ico.org.uk/

- The Guide to the GDPR
- Data Protection Self Assessment Toolkit
- Guidelines on Data Protection and Brexit
- Regulatory Sandbox

Οδηγίες και εργαλεία άλλων Ευρωπαϊκών εποπτικών αρχών

CNIL
Γαλλία
https://www.cnil.fr/

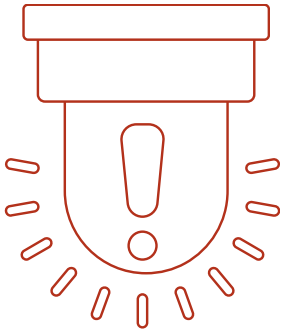
- A Guide to assist data processors with respect to their GDPR obligations
- Open source DPIA tool
- Template data processing agreements
- Paper on the responsible use of the blockchain in the context of personal data
- CNIL's Guidance on requirements for the lawful sharing of personal data with business partners and other third parties

Οδηγίες και εργαλεία άλλων Ευρωπαϊκών εποπτικών αρχών

DPC
Ιρλανδία
https://www.dataprotection.ie/

- Guidance on the GDPR requirements
- Guidance on specific technological issues (Cloud, connected devices and connected toys, CCTV)

Σημαντικότερα διοικητικά πρόστιμα

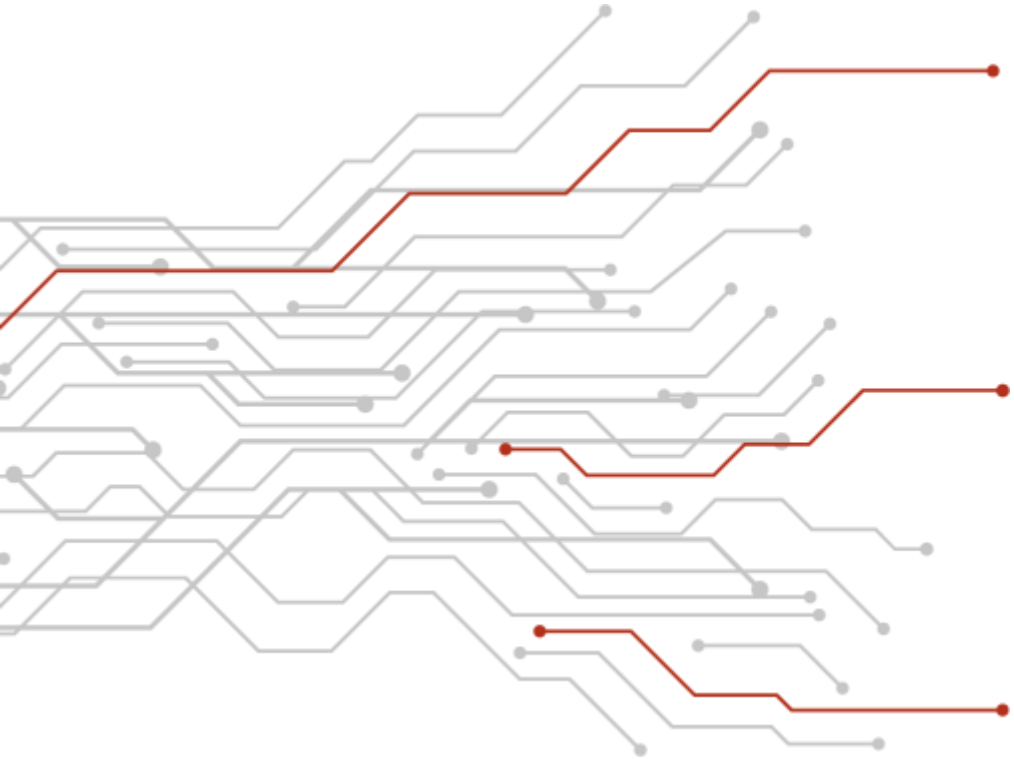


- Πρόστιμα συνολικού ύψους 56 m € από 11 εποπτικές αρχές

- Τα μεγαλύτερα πρόστιμα που έχουν επιβληθεί αφορούν:
  + ελλιπή ενημέρωση των υποκειμένων,
  + έλλειψη κατάλληλων μέτρων ασφαλείας, και
  + τήρηση των δεδομένων για μεγαλύτερο χρονικό διάστημα

- Η ΑΠΔΠΧ δεν έχει επιβάλει ακόμα πρόστιμα με βάση τον GDPR

Ένας χρόνος GDPR: κοιτάζοντας την αυριανή ημέρα



Παροχή σημαντικών κατευθυντήριων οδηγιών από το EBPD

Εντατικότερες έρευνες και μεγαλύτερα πρόστιμα από τις εποπτικές αρχές

Σημαντικές νομοθετικές εξελίξεις

Παροχή σημαντικών κατευθυντήριων οδηγιών από το EDPB

Εντατικότερες έρευνες & μεγαλύτερα πρόστιμα από τις εποπτικές αρχές

- Η τάση αυτή έχει διαφανεί ήδη από τα πρώτα σημαντικά πρόστιμα και υπονοήθηκε από την Πρόεδρο του EDPB, η οποία ανέφερε χαρακτηριστικά «a tiger without teeth is not respected».

- Η Ιρλανδική Αρχή ερευνά 52 υποθέσεις, εκ των οποίων 18 αφορούν μεγάλες εταιρείες τεχνολογίας, και οι πρώτες αποφάσεις αναμένονται εντός του καλοκαιριού.

- Θέματα τα οποία θα απασχολήσουν τις εποπτικές αρχές το επόμενο έτος:
  - + Παραβιάσεις στα δικαιώματα των υποκειμένων
  - + Σχέσεις υπευθύνου / εκτελούντος
  - + Στοχευμένες διαφημίσεις
  - + Προσωπικά δεδομένα παιδιών
  - + AI και big data
  - + Μέθοδοι επιτήρησης και facial recognition technology

Σημαντικές νομοθετικές εξελίξεις

Ψήφιση του Ελληνικού εκτελεστικού νόμου για τον GDPR

Ψήφιση του ePrivacy Regulation

Υιοθέτηση νέων standard contractual clauses για διαβιβάσεις εκτός ΕΕ

Ψήφιση και θέση σε εφαρμογή νέων νόμων για τα προσωπικά δεδομένα διεθνώς (CCPA, LGPD κλπ)

Τί απαιτεί η συμμόρφωση με τον GDPR;

- Διαμόρφωση κουλτούρας ιδιωτικότητας εντός του οργανισμού
- Πραγματοποίηση τακτικών compliance audits και εκπαιδεύσεων των εργαζομένων
- Κατανόηση ότι η συμμόρφωση είναι μία συνεχής και διά βίου άσκηση
- Παροχή ουσιαστικών αρμοδιοτήτων στους DPOs και/ή χρήση εξειδικευμένων συμβούλων που θα συνδράμουν ουσιαστικά και πρακτικά τον οργανισμό
- Ανάγκη παρακολούθησης εξελίξεων σε παγκόσμιο επίπεδο και υιοθέτηση διεθνών προτύπων συμμόρφωσης
- Συνειδητοποίηση ότι τα προσωπικά δεδομένα αποτελούν βασικό περιουσιακό στοιχείο και η προστασία τους ωφελεί την ίδια την επιχείρηση και εμπεδώνει την εμπιστοσύνη των πελατών, συνεργατών και εργαζομένων

ΖΕΠΟΣ & ΓΙΑΝΝΟΠΟΥΛΟΣ

Ευχαριστώ

Μαίρη Δεληγιάννη
Senior Associate

t_ +30 210 6967000 | e_ m.deligianni@zeya.com

www.zeya.com

280 Kifissias Ave. | 152 32 Halandri | Athens, Greece
T_ (+30) 210 69 67 000 | F_(+30) 210 69 94 640
info@zeya.com