ΗΔΙΚΑ
ΗΛΕΚΤΡΟΝΙΚΗ ΔΙΑΚΥΒΕΡΝΗΣΗ ΚΟΙΝΩΝΙΚΗΣ ΑΣΦΑΛΙΣΗΣ Α.Ε.

Όταν το GDPR συνάντησε το ISO 27000 στην ΗΔΙΚΑ

Νικόλας Αναστασόπουλος

για τη δικηγορική εταιρεία

ΝΙΚΟΛΑΣ ΚΑΝΕΛΛΟΠΟΥΛΟΣ, ΧΑΡΑ ΖΕΡΒΑ & ΣΥΝΕΡΓΑΤΕΣ

Υπεύθυνος Προστασίας Δεδομένων

Δικηγόρος Master 2 – CIPP/E

Γεώργιος-Ευάγγελος Βαρελτζής

Υπεύθυνος Ασφάλειας Πληροφοριών

BSc, MSc in Computer Science

CISA, CISM, ISO 27001 Certified Auditor

ΗΔΙΚΑ
ΗΛΕΚΤΡΟΝΙΚΗ ΔΙΑΚΥΒΕΡΝΗΣΗ
ΚΟΙΝΩΝΙΚΗΣ ΑΣΦΑΛΙΣΗΣ Α.Ε.

Γνωριμία με την ΗΔΙΚΑ

Ο ρόλος της ΗΔΙΚΑ

Η Η.ΔΙ.Κ.Α. Α.Ε. είναι ΔΕΚΟ με αποστολή (μεταξύ άλλων):

- Την «***μελέτη, ανάπτυξη, λειτουργία, εκμετάλλευση, διοίκηση, διαχείριση και συντήρηση Συστημάτων Πληροφορικής και Επικοινωνιών***, εξοπλισμού, λογισμικού και υπηρεσιών για την εξυπηρέτηση ***όλων των Φορέων Κοινωνικής Ασφάλισης και των λοιπών φορέων υγείας, πρόνοιας και κοινωνικής πολιτικής***» **(άρθρο 3 παρ. 1 περ. (α) του Ν.3607/2007 – Καταστατικοί σκοποί)**,
- Παρέχοντας «ολοκληρωμένες ***λύσεις υψηλής ποιότητας στον τομέα της πληροφορικής και επικοινωνιών***, οι οποίες θα υποστηρίζουν την ορθή, πλήρη και αποτελεσματική λειτουργία των ***φορέων κοινωνικής ασφάλισης και παροχής υγείας*** σε βάθος χρόνου και την ***εξυπηρέτηση των πολιτών, μέσω της παροχής σύγχρονων ηλεκτρονικών υπηρεσιών και πληροφοριών***» **(Κανονισμός Εσωτερικής Λειτουργίας & Οργάνωσης),**
- Ενώ ταυτόχρονα, έχει επιφορτιστεί με την «διασφάλιση και υποστήριξη της ***διαλειτουργικότητας των Συστημάτων Πληροφορικής και Επικοινωνιών*** (…) φορέων που δραστηριοποιούνται σε θέματα ασφάλισης, υγείας, πρόνοιας και κοινωνικής πολιτικής» **(άρθρο 3 παρ. 1 περ. (δ) του Ν.3607/2007 – Καταστατικοί σκοποί)**

ΗΔΙΚΑ
ΗΛΕΚΤΡΟΝΙΚΗ ΔΙΑΚΥΒΕΡΝΗΣΗ ΚΟΙΝΩΝΙΚΗΣ ΑΣΦΑΛΙΣΗΣ Α.Ε.

Χαρακτηριστικά της ΗΔΙΚΑ

- **Κρατικός μη κερδοσκοπικός** φορέας (ΔΕΚΟ)
- **ΠΔ 81/2019 & Ν.4623/2019** : Μεταφορά της ΗΔΙΚΑ στην εποπτεία του Υπουργείου Ψηφιακής Διακυβέρνησης (τροποποίηση διατάξεων *Ν.3607/2007 με τον οποίο συστάθηκε)*
- Ένα ευέλικτο **κρατικό** «εργαλείο» για την ανάπτυξη και διαχείριση έργων πληροφορικής για τους τομείς της **Κοινωνικής Ασφάλισης,** της **Υγείας και της Πρόνοιας**
- Ο φορέας που είναι εκ του νόμου αρμόδιος να υλοποιεί τα έργα πληροφορικής όλων των ΦΚΑ (ν.3607/2007)

ΗΔΙΚΑ
ΗΛΕΚΤΡΟΝΙΚΗ ΔΙΑΚΥΒΕΡΝΗΣΗ ΚΟΙΝΩΝΙΚΗΣ ΑΣΦΑΛΙΣΗΣ Α.Ε.

Τι προσφέρει η ΗΔΙΚΑ

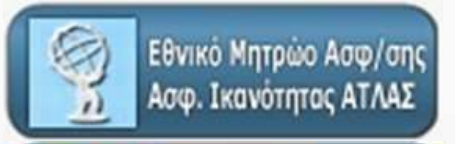
- **Υποστηρίζει τεχνολογικά** τους τομείς της Κοινωνικής Ασφάλισης, της Πρόνοιας και της Υγείας
- **Παρέχει** καινοτόμες ψηφιακές υπηρεσίες *υποστήριξης των Δημόσιων Φορέων*
- **Προσφέρει** σύγχρονες διαδικτυακές υπηρεσίες *προς τους Πολίτες*
- **Διασφαλίζει και υποστηρίζει** τη *διαλειτουργικότητα* των πληροφοριακών συστημάτων
- **Υλοποιεί** *έργα* πληροφορικής Δημόσιων Φορέων με *σύγχρονες τεχνολογίες* και μέσα
- **Αποτελεί** *ψηφιακή πύλη* της χώρας μας προς τον «κόσμο» των *Ευρωπαϊκών Υπηρεσιών Κοινωνικής Ασφάλισης και Υγείας*
- **Διαχειρίζεται και αξιοποιεί** τα ψηφιακά δεδομένα για την άσκηση τεκμηριωμένης πολιτικής

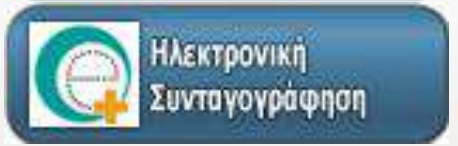
ΗΔΙΚΑ
ΗΛΕΚΤΡΟΝΙΚΗ ΔΙΑΚΥΒΕΡΝΗΣΗ ΚΟΙΝΩΝΙΚΗΣ ΑΣΦΑΛΙΣΗΣ Α.Ε.

Λειτουργίες που στηρίζει η ΗΔΙΚΑ

Η ΗΔΙΚΑ σήμερα εξυπηρετεί

- >10 εκ. Ασφαλισμένους (ΑΜΚΑ, ΑΤΛΑΣ, ΣΗΣ)
- 2,66 εκ συνταξιούχους για τη μηνιαία πληρωμή 4,49εκ συντάξεων
- 1,85 εκατομμύρια ασφαλισμένους των προ ενοποίησης ΦΚΑ (ΟΓΑ, ΟΑΕΕ, ΤΑΝ, ΕΤΑΠ-ΜΜΕ)
- 50.000 Ιατρούς, 12.000 Φαρμακοποιούς
- 37.000 Μισθοδοτούμενους
- 500.000 Νοσηλευόμενους
- 5.000 υπαλλήλους του ΕΦΚΑ/ΕΤΕΑΕΠ





ΗΔΙΚΑ
ΗΛΕΚΤΡΟΝΙΚΗ ΔΙΑΚΥΒΕΡΝΗΣΗ ΚΟΙΝΩΝΙΚΗΣ ΑΣΦΑΛΙΣΗΣ Α.Ε.

ΗΔΙΚΑ
ΗΛΕΚΤΡΟΝΙΚΗ ΔΙΑΚΥΒΕΡΝΗΣΗ
ΚΟΙΝΩΝΙΚΗΣ ΑΣΦΑΛΙΣΗΣ Α.Ε.

Κανονιστικές απαιτήσεις GDPR και NISD – Στοχεύοντας σε μια ολιστική αντιμετώπιση

Ιστορική αναδρομή

Πριν τον GDPR

Οδηγία* 95/45 (ΕΚ)

28 εθνικοί νόμοι
&
28 διαφορετικές ερμηνείες εφαρμογής *της Οδηγίας 95/46 (ΕΚ) για την προστασία των δεδομένων προσωπικού χαρακτήρα*

Μάιος 2018

Γενικός Κανονισμός 2016/679 (ΕΕ)**

Ένας μοναδικός Κανονισμός *εναρμονισμένος και εφαρμόσιμος σε όλη την Ευρωπαϊκή Επικράτεια ταυτόχρονα*

Οι **Οδηγίες καθορίζουν ορισμένα αποτελέσματα που πρέπει να επιτευχθούν, αλλά κάθε κράτος μέλος είναι ελεύθερο να αποφασίσει πώς να μεταφέρει τις οδηγίες στις εθνικές νομοθεσίες*

***Οι **Κανονισμοί** έχουν δεσμευτική νομική ισχύ σε όλα τα κράτη μέλη και τίθενται σε ισχύ σε καθορισμένη ημερομηνία σε όλα τα κράτη μέλη*

ΗΔΙΚΑ
ΗΛΕΚΤΡΟΝΙΚΗ ΔΙΑΚΥΒΕΡΝΗΣΗ ΚΟΙΝΩΝΙΚΗΣ ΑΣΦΑΛΙΣΗΣ Α.Ε.

Ήδη από τον Ν.2472/1997 …

Άρθρο 10 Απόρρητο και ασφάλεια της επεξεργασίας

2. Για τη διεξαγωγή της επεξεργασίας **ο υπεύθυνος επεξεργασίας οφείλει να επιλέγει πρόσωπα** με αντίστοιχα επαγγελματικά προσόντα **που παρέχουν επαρκείς εγγυήσεις από πλευράς τεχνικών γνώσεων και προσωπικής ακεραιότητας για την τήρηση του απορρήτου**.

3. Ο υπεύθυνος επεξεργασίας οφείλει να λαμβάνει τα ***κατάλληλα οργανωτικά και τεχνικά μέτρα για την ασφάλεια των δεδομένων*** και την προστασία τους από ***τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση*** και κάθε άλλη μορφή αθέμιτης επεξεργασίας. ***Αυτά τα μέτρα πρέπει να εξασφαλίζουν επίπεδο ασφαλείας ανάλογο προς τους κινδύνους*** *που συνεπάγεται η επεξεργασία και η φύση των δεδομένων* που είναι αντικείμενο της επεξεργασίας...

4. Αν η επεξεργασία διεξάγεται για λογαριασμό του υπεύθυνου … ο ενεργών την επεξεργασία την διεξάγει μόνο κατ' εντολή του υπεύθυνου και ότι **οι υποχρεώσεις του παρόντος άρθρου βαρύνουν αναλόγως και αυτόν**.

ΗΔΙΚΑ
ΗΛΕΚΤΡΟΝΙΚΗ ΔΙΑΚΥΒΕΡΝΗΣΗ ΚΟΙΝΩΝΙΚΗΣ ΑΣΦΑΛΙΣΗΣ Α.Ε.

Μερική κατάργηση του Ν.2472/1997 με τον Ν.4624/2019 (άρθρο 84)…

- Με το άρθρο 84 του Ν.4624/2019 καταργήθηκαν οι περισσότερες διατάξεις του Ν.2472/1997 διότι με την θέση σε ισχύ του ΓΚΠΔ, που σαν ευρωπαϊκός κανονισμός έχει υπερνομοθετική ισχύ, ο Ν.2472/1997 κατέστη ανίσχυρος και παρωχημένος.
- Ο Ν.4624/2019 δεν αντικατέστησε άρθρα του Ν.2472/1997 αλλά έθεσε μέτρα εφαρμογής του ΓΚΠΔ στην εσωτερική έννομη τάξη.
- Ο ΓΚΠΔ αντικατέστησε συνολικά το προϊσχύον κανονιστικό πλαίσιο, θέτοντας νέους κοινούς κανόνες εντός ΕΕ/ΕΟΧ με παγκόσμια απήχηση.

Σύγχρονο κανονιστικό πλαίσιο- ΓΚΠΔ

Τμήμα 2 – Ασφάλεια Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

Άρθρο 32 – Ασφάλεια επεξεργασίας

Παράγραφος 1

Γενικό πλαίσιο οφειλόμενων ενεργειών Υπεύθυνου και Εκτελούντος για την ασφάλεια

«Λαμβάνοντας υπόψη τις τελευταίες εξελίξεις, το κόστος εφαρμογής και τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ***ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία εφαρμόζουν ΚΑΤΑΛΛΗΛΑ ΤΕΧΝΙΚΑ και ΟΡΓΑΝΩΤΙΚΑ ΜΕΤΡΑ προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων*****, περιλαμβανομένων, μεταξύ άλλων, κατά περίπτωση:**

α) της ***ψευδωνυμοποίησης*** *και της* ***κρυπτογράφησης*** *δεδομένων προσωπικού χαρακτήρα,*

β) της δυνατότητας ***διασφάλισης του απορρήτου****, της* ***ακεραιότητας****, της* ***διαθεσιμότητας*** *και της* ***αξιοπιστίας των συστημάτων και των υπηρεσιών*** *επεξεργασίας* ***ΣΕ ΣΥΝΕΧΗ ΒΑΣΗ****,*

γ) της δυνατότητας ***αποκατάστασης της διαθεσιμότητας και της πρόσβασης*** *σε δεδομένα προσωπικού χαρακτήρα* ***σε εύθετο χρόνο σε περίπτωση φυσικού ή τεχνικού συμβάντος****,*

δ) διαδικασίας για ***την τακτική δοκιμή, εκτίμηση και αξιολόγηση*** *της αποτελεσματικότητας των τεχνικών και των οργανωτικών μέτρων για τη διασφάλιση της ασφάλειας της επεξεργασίας».*

Σύγχρονο κανονιστικό πλαίσιο- ΓΚΠΔ

Τμήμα 2 – Ασφάλεια Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
Άρθρο 32 – Ασφάλεια επεξεργασίας
Παράγραφοι 2 έως 4

Επιμέρους οφειλόμενες ενέργειες Υπεύθυνου και Εκτελούντος για την ασφάλεια

2. Κατά την εκτίμηση του ενδεδειγμένου επιπέδου ασφάλειας **λαμβάνονται ιδίως υπόψη οι κίνδυνοι που απορρέουν από την επεξεργασία**, ιδίως από τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, άνευ αδείας κοινολόγηση ή προσπέλαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία.

3. Η **τήρηση εγκεκριμένου κώδικα δεοντολογίας όπως αναφέρεται στο άρθρο 40 ή εγκεκριμένου μηχανισμού πιστοποίησης όπως αναφέρεται στο άρθρο 42 δύναται να χρησιμοποιηθεί ως στοιχείο για την απόδειξη της συμμόρφωσης με τις απαιτήσεις της παραγράφου 1 του παρόντος άρθρου.**

4. Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία **λαμβάνουν μέτρα ώστε να διασφαλίζεται ότι κάθε φυσικό πρόσωπο που ενεργεί υπό την εποπτεία του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία το οποίο έχει πρόσβαση σε δεδομένα προσωπικού χαρακτήρα τα επεξεργάζεται μόνο κατ' εντολή του υπευθύνου επεξεργασίας**, εκτός εάν υποχρεούται προς τούτο από το δίκαιο της Ένωσης ή του κράτους μέλους.

Σύγχρονο κανονιστικό πλαίσιο- ΓΚΠΔ

Τμήμα 2 – Ασφάλεια Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

Άρθρα 33 – 34

Περαιτέρω οφειλόμενες ενέργειες – Γνωστοποίηση / Ενημέρωση / Ανακοίνωση

- **Άρθρο 33 – Γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα στην εποπτική αρχή**
  - ✓ Ο Υπεύθυνος Επεξεργασίας **γνωστοποιεί ΑΜΕΛΛΗΤΙ και ει δυνατόν εντός 72 ωρών** από την στιγμή που αποκτά γνώστη του περιστατικού παραβίασης την εποπτεύουσα αρχή.
  - ✓ Αντίστοιχα, ο Εκτελών την Επεξεργασία **ενημερώνει ΑΜΕΛΛΗΤΙ** τον Υπεύθυνο Επεξεργασίας
  - ✓ Ελάχιστο περιεχόμενο γνωστοποίησης

- **Άρθρο 34 – Ανακοίνωση παραβίασης δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων**
  - ✓ Όταν η παραβίαση θέτει ή ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ό Υπεύθυνος Επέργασίας οφείλει να ανακοινώσει ΑΜΕΛΛΗΤΙ τα εμπλεκόμενα υποκείμενα.
  - ✓ Περιεχόμενο ανακοίνωσης

ΗΔΙΚΑ
ΗΛΕΚΤΡΟΝΙΚΗ ΔΙΑΚΥΒΕΡΝΗΣΗ ΚΟΙΝΩΝΙΚΗΣ ΑΣΦΑΛΙΣΗΣ Α.Ε.

Σύγχρονο κανονιστικό πλαίσιο- ΓΚΠΔ

Τμήμα 3 – Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων και προηγούμενη διαβούλευση

- **Άρθρο 35 – Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων (DPIA)**: Παρ. 1 – «Όταν ένα είδος επεξεργασίας, ιδίως με χρήση νέων τεχνολογιών και **συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων,** ο υπεύθυνος επεξεργασίας διενεργεί, **πριν από την επεξεργασία**, εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα»
- **Απόφαση 65/2018 ΑΠΔΠΧ (ΦΕΚ Β΄ 1622/2019)** «Κατάλογος με τα είδη των πράξεων επεξεργασίας που υπόκεινται στην απαίτηση για διενέργεια εκτίμησης αντίκτυπου σχετικά με την προστασία δεδομένων σύμφωνα με το άρθρο 35 παρ. 4 του ΓΚΠΔ» : Θέτει τα κριτήρια που καθιστούν υποχρεωτική την ΕΑΠΔ.

Σύγχρονο κανονιστικό πλαίσιο – NISD ΕΕ 2016/1148 & Ν.4577/2018 & Υ.Α.1027 (ΦΕΚ Β' 3739/8-10-2019)

Αφορά τους …

I. **«Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών» (operators of essential services),**

II. **«Παρόχους ψηφιακών υπηρεσιών» (digital service providers)**

δηλαδή κάθε (άρθρο 4 παράγραφος 4 και 6)

I. **δημόσια ή ιδιωτική οντότητα** των **τομέων ενέργειας, μεταφορών, τραπεζών, υποδομών χρηματοπιστωτικών αγορών, υγείας, προμήθειας και διανομής πόσιμου νερού, ψηφιακών υποδομών** (π.χ. Internet eXchange Points, μητρώα ονομάτων χώρου, παρόχους DNS-Domain Name resolution Systems) (παράρτημα ΙΙ οδηγίας) **καθώς επίσης και**

II. **οποιαδήποτε οντότητα** παρέχει υπηρεσίες (παράρτημα ΙΙΙ οδηγίας) **νεφοϋπολογιστικής, επιγραμμικής αγοράς ή επιγραμμική μηχανή αναζήτησης** (cloud, online market, online search engines)

η οποία (άρθρο 5 παράγραφος 2)

- παρέχει **υπηρεσία ουσιώδη για τη διατήρηση κρίσιμων κοινωνικών και/ή οικονομικών δραστηριοτήτων**·
- η **παροχή της υπηρεσίας αυτής στηρίζεται σε συστήματα δικτύου και πληροφοριών** και
- τυχόν **περιστατικό ασφάλειας θα προκαλούσε σοβαρή διατάραξη** της παροχής της εν λόγω υπηρεσίας

Σύγχρονο κανονιστικό πλαίσιο – NISD ΕΕ 2016/1148 & Ν.4577/2018 & Υ.Α.1027 (ΦΕΚ Β' 3739/8-10-2019)

Για τον προσδιορισμό του «περιστατικού ασφάλειας» (κατά NS)...

(άρθρο 4) ***«περιστατικό ασφάλειας / incident»***: κάθε (συμβάν) γεγονός που έχει στη πραγματικότητα μια *δυσμενή επίπτωση* στην *ασφάλεια συστημάτων δικτύου και πληροφοριών*

(άρθρο 4) **«*ασφάλεια συστημάτων δικτύου και πληροφοριών»:*** η ικανότητα συστημάτων δικτύου και πληροφοριών να ***ανθίστανται***, *σε δεδομένο βαθμό αξιοπιστίας, σε ενέργειες που πλήττουν τη* ***διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα ή το απόρρητο των δεδομένων*** που αποθηκεύονται, μεταδίδονται ή υποβάλλονται σε επεξεργασία ή των συναφών υπηρεσιών που προσφέρονται ή είναι προσβάσιμες μέσω των εν λόγω συστημάτων δικτύου και πληροφοριών.

Σύγχρονο κανονιστικό πλαίσιο – NISD ΕΕ 2016/1148 & Ν.4577/2018 & Υ.Α.1027 (ΦΕΚ Β' 3739/8-10-2019)

Με βάση τα προβλεπόμενα στο άρθρο 14 (παράγραφος 1-3) και άρθρο 16:

1. *Τα κράτη μέλη εξασφαλίζουν ότι οι φορείς εκμετάλλευσης βασικών υπηρεσιών / πάροχοι ψηφιακών υπηρεσιών λαμβάνουν* ***κατάλληλα και αναλογικά τεχνικά και οργανωτικά μέτρα*** για τη διαχείριση των κινδύνων όσον αφορά την ασφάλεια των συστημάτων δικτύου και πληροφοριών *που χρησιμοποιούν στις δραστηριότητές τους. Λαμβάνοντας υπόψη τις πλέον πρόσφατες τεχνικές δυνατότητες,* ***τα μέτρα αυτά διασφαλίζουν επίπεδο ασφάλειας των συστημάτων δικτύου και πληροφοριών ανάλογο προς τον εκάστοτε κίνδυνο***.

2. *Τα κράτη μέλη εξασφαλίζουν ότι οι φορείς εκμετάλλευσης βασικών υπηρεσιών / πάροχοι ψηφιακών υπηρεσιών* λαμβάνουν κατάλληλα μέτρα για την αποτροπή και την ελαχιστοποίηση του αντίκτυπου συμβάντων που επηρεάζουν την ασφάλεια των συστημάτων δικτύου και πληροφοριών που χρησιμοποιούνται για την παροχή αυτών των βασικών υπηρεσιών, ***με σκοπό τη διασφάλιση της συνέχειάς τους***.

ΗΔΙΚΑ
ΗΛΕΚΤΡΟΝΙΚΗ ΔΙΑΚΥΒΕΡΝΗΣΗ ΚΟΙΝΩΝΙΚΗΣ ΑΣΦΑΛΙΣΗΣ Α.Ε.

Σύγχρονο κανονιστικό πλαίσιο – NISD ΕΕ 2016/1148 & Ν.4577/2018 & Υ.Α.1027 (ΦΕΚ Β’ 3739/8-10-2019)

Με βάση τα προβλεπόμενα στο άρθρο 14 (παράγραφος 1-3) και άρθρο 16:

3. *Τα κράτη μέλη εξασφαλίζουν ότι οι φορείς εκμετάλλευσης βασικών υπηρεσιών / πάροχοι ψηφιακών υπηρεσιών* ***κοινοποιούν χωρίς αδικαιολόγητη καθυστέρηση*** *στην αρμόδια αρχή ή στην CSIRT συμβάντα* ***με σοβαρό αντίκτυπο στη συνέχεια των βασικών υπηρεσιών που παρέχουν****. Οι κοινοποιήσεις περιλαμβάνουν πληροφορίες που επιτρέπουν στην αρμόδια αρχή ή την CSIRT να προσδιορίσει τυχόν* ***διασυνοριακό αντίτυπο του συμβάντος.*** *Η κοινοποίηση δεν συνεπάγεται αυξημένη ευθύνη για τον κοινοποιούντα.*

Χαμένοι στη «μετάφραση» …

Υποχρεώσεις …

- ***« … κατάλληλα και αναλογικά τεχνικά και οργανωτικά μέτρα…»***
- ***« … τα μέτρα αυτά διασφαλίζουν επίπεδο ασφάλειας των συστημάτων ανάλογο προς τον εκάστοτε κίνδυνο …»***
- ***« … κοινοποίηση χωρίς αδικαιολόγητη καθυστέρηση*** *στην αρμόδια αρχή συμβάντων* ***με σοβαρό αντίκτυπο …» και λοιπές ενημερώσεις & ανακοινώσεις***
- ***Παροχή τεκμηρίων συμμόρφωσης*** (το βάρος απόδειξης ανήκει στον Φορέα)
- ***Αρμόδιο όργανο ως σημείο επαφής για συντονισμό ενεργειών και επικοινωνία***

Προσπάθεια «μετάφρασης» …

- ✓ *Σχεδιασμός ενεργειών με στόχο την πρόληψη (ΓΚΠΔ & NISD)*
  … και στη συνέχεια τον εντοπισμό και την αντιμετώπιση
  - ➔ *Η ασφάλεια αφορά τον πλήρη κύκλο ζωής συστημάτων και δεδομένων*
    - ❑ *Ασφάλεια & ιδιωτικότητα εκ σχεδιασμού & εξ' ορισμού (Σχεδιασμός / Υλοποίηση)*
    - ❑ *Παρακολούθηση και προσαρμογή (Λειτουργία)*
    - ❑ *Ασφαλής απόσυρση*
  - ➔ *Η αποτίμηση της αποτελεσματικότητας (επιπέδου ασφάλειας) είναι διαρκής*

- ✓ *Λογοδοσία (ΓΚΠΔ) - αυτοέλεγχος & (αυτό)συμμόρφωση (NISD)*

- ✓ *Προτεραιοποίηση δράσεων με βάση τον κίνδυνο (ΓΚΠΔ & NISD)*

ΗΔΙΚΑ
ΗΛΕΚΤΡΟΝΙΚΗ ΔΙΑΚΥΒΕΡΝΗΣΗ ΚΟΙΝΩΝΙΚΗΣ ΑΣΦΑΛΙΣΗΣ Α.Ε.

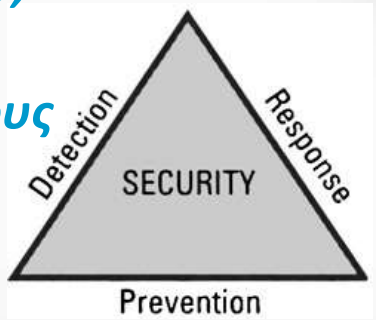
Οι απαιτήσεις αναλυτικότερα … (1/3)

- ✓ ***Αποτύπωση επεξεργασιών, δεδομένων & πόρων***
  - ➔ ***Ποιες είναι οι επεξεργασίες και ποια βήματα περιλαμβάνουν***
  - ➔ ***Ποια είναι τα δεδομένα***
  - ➔ ***Ποιοί είναι οι χρησιμοποιούμενοι πόροι (πληροφοριακά συστήματα, υποδομές, υπηρεσίες τρίτων μερών κλπ)***

- ✓ ***Ικανοποιούνται τα δικαιώματα των υποκειμένων και οι άλλες θεσμικές απαιτήσεις (νομιμότητα & συγκατάθεση, δέουσα ασφάλεια, λογοδοσία κτλ);***
  - ➔ ***Κατάλληλη προσαρμογή διεργασιών***
  - ➔ ***Στάθμιση κινδύνου***

Οι απαιτήσεις αναλυτικότερα … (2/3)

- ✓ ***Επιλογή και εφαρμογή αντισταθμιστικών μέτρων*** (Υ.Α. 1027 *κατάλληλα, αναλογικά, αξιόπιστα, συγκεκριμένα, περιεκτικά, αποτελεσματικά και αποδοτικά*)
  - ➔ ***Σε επίπεδο τεχνικό αλλά και οργανωτικό (καθορισμός ρόλων, αρμοδιοτήτων, δομών)…***
  - ➔ ***Παρακολουθείται η εφαρμογή και η αποτελεσματικότητά τους***
  - ➔ ***Συλλέγονται σχετικά τεκμήρια***
    - ➔ ***Λογοδοσία***
    - ➔ ***Αξιολόγηση***



- ✓ ***Κοινοποίηση*** *συμβάντων* ***χωρίς αδικαιολόγητη καθυστέρηση*** *στην αρμόδια αρχή* ***= Ανάπτυξη ικανοτήτων***
  - ➔ ***Παρακολούθησης καταγραφών ΚΑΙ***
  - ➔ ***Έγκαιρου εντοπισμού ΚΑΙ***
  - ➔ ***Αντιμετώπισης και αναφοράς***

Οι απαιτήσεις αναλυτικότερα … (3/3)

✓ ***Κεντρικό σημείο συντονισμού και επικοινωνίας***

Το αρμόδιο εποπτεύον όργανο ασκεί τις αρμοδιότητές του:

➔ ***Εσωτερικά*** (προς τον οργανισμό)

➔ ***Εξωτερικά*** (προς τις Αρμόδιες Αρχές και το λειτουργικό περιβάλλον του οργανισμού)

✓ ***Ωφέλειες συνεκτικού σχεδιασμού δράσεων***

➔ ***Εξοικονόμηση (ανθρώπινων) πόρων και προσπάθειας***

➔ ***Αποτελεσματική αντιμετώπιση***

➔ ***«Ξεκάθαρες» αρμοδιότητες***

ΗΔΙΚΑ
ΗΛΕΚΤΡΟΝΙΚΗ ΔΙΑΚΥΒΕΡΝΗΣΗ ΚΟΙΝΩΝΙΚΗΣ ΑΣΦΑΛΙΣΗΣ Α.Ε.

Από τη «μετάφραση» στην πράξη

… του Ελληνικού Δημόσιου Τομέα …

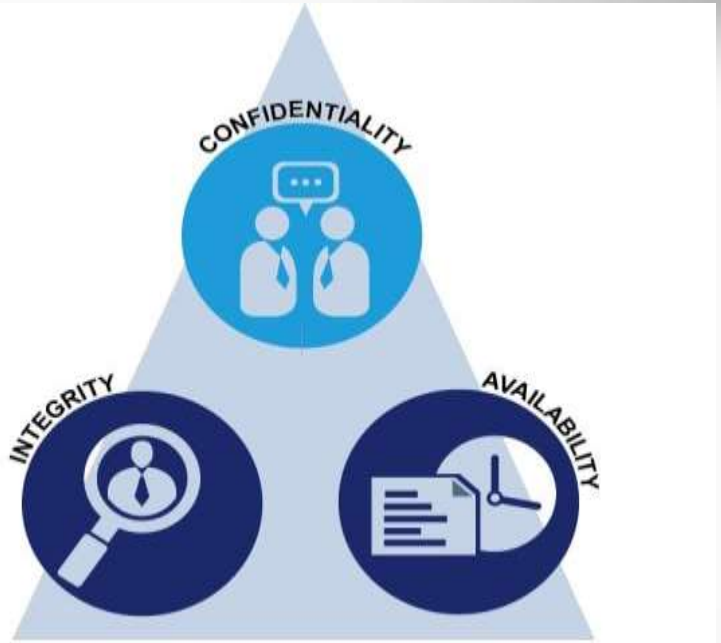
- Διαθεσιμότητα ανθρώπινων και υλικών πόρων;

- Εμπειρογνωσία; Με ποια κριτήρια;

- Δεξιότητες & «χαρακτηριστικά»;

- Συμμετοχή στον «πλήρη» κύκλο ζωής;

ΗΔΙΚΑ
ΗΛΕΚΤΡΟΝΙΚΗ ΔΙΑΚΥΒΕΡΝΗΣΗ ΚΟΙΝΩΝΙΚΗΣ ΑΣΦΑΛΙΣΗΣ Α.Ε.



Ασφάλεια Πληροφοριών ⟺ **Εταιρική Διακυβέρνηση**

Διαχείριση Ασφάλειας Πληροφοριών

ISO 27001:2013

- **Πρότυπο Διαχείρισης Ασφάλειας (Information Security Management)**
- **Προσανατολισμένο στην επιλογή** κατάλληλων μέτρων (ελέγχων) για τη διαχείριση του «ρίσκου» (risk-based)
- **Εστιάζει στην πρόληψη** και λιγότερο στη λήψη διορθωτικών ενεργειών
- Καθορίζει και **οριοθετεί ρόλους και αρμοδιότητες** για την ασφάλεια πληροφοριών
- «Κληρονομεί - χρησιμοποιεί» τον μηχανισμό διαχείρισης και διαρκούς βελτίωσης **P**lan-**D**o-**C**heck-**A**ct


INTERNATIONAL STANDARD

ISO/IEC 27001

Second edition
2013-10-01

Information technology — Security techniques — Information security management systems — Requirements

Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences

Reference number
ISO/IEC 27001:2013(E)

© ISO/IEC 2013

Πώς λειτουργεί ένα ΣΔΑΠ;

Περιοχές που αποδίδεται έμφαση

14 θεματικές περιοχές διαχείρισης, 35 στόχοι, 114 μέτρα (ISO 27002:2013)

5. Security Policy
5.1 Information Security Policy
6. Organization of Information Security
6.1 Internal Organization
6.2 Mobile devices and teleworking
7. Human resource security
7.1 Prior to employment
7.2 During employment
7.3 Termination and change of employment
8. Asset Management
8.1 Responsibility for assets
8.2 Information classification
8.3 Media handling
9. Access Control
9.1 Business requirements of access control
9.2 User access management
9.3 User responsibilities
9.4 System and application access control
10. Cryptography
10.1 Cryptographic controls
11. Physical and environmental security
11.1 Secure areas
11.2 Equipment
12. Operations Security
12.1 Operational procedures and responsibilities
12.2 Protection from malware
12.3 Backup
12.4 Logging and monitoring
12.5 Control of operational software
12.6 Technical vulnerability management
12.7 Information systems audit considerations
13. Communications security
13.1 Network security management
13.2 Information transfer
14. System acquisition, development and maintenance
14.1 Security requirements of information systems
14.2 Security in development and support processes
14.3 Test data
15. Supplier relationships
15.1 Information security in supplier relationships
15.2 Supplier service delivery management
16. Information security incident management
16.1 Management of information security incidents and improvements
17. Information security aspects of business continuity management
17.1 Information security continuity
17.2 Redundancies
18. Compliance
18.1 Compliance with legal and contractual requirements
18.2 Information security reviews

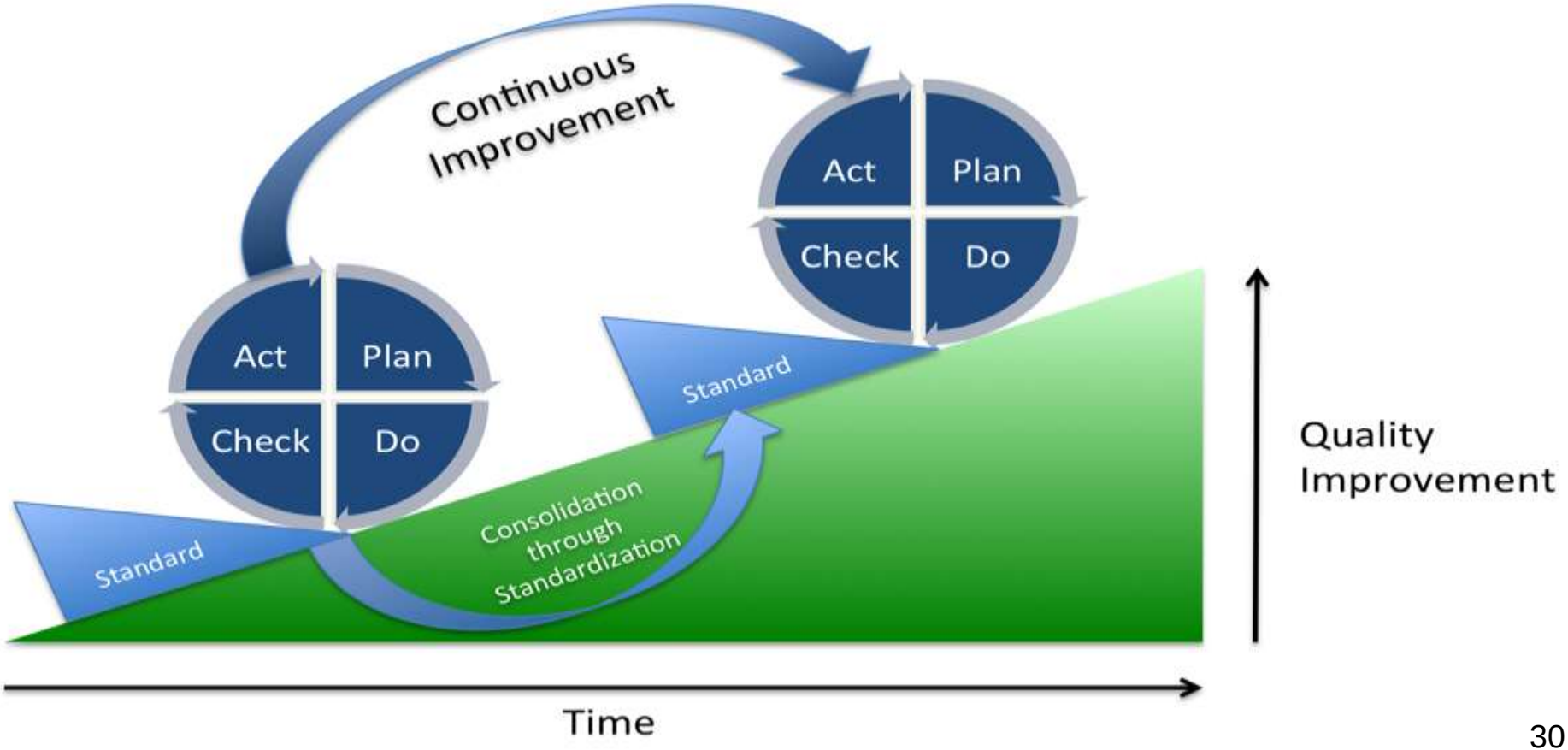
Πολιτικές

Διαδικασίες

Οδηγίες

ΗΔΙΚΑ
ΗΛΕΚΤΡΟΝΙΚΗ ΔΙΑΚΥΒΕΡΝΗΣΗ ΚΟΙΝΩΝΙΚΗΣ ΑΣΦΑΛΙΣΗΣ Α.Ε.

Η φιλοσοφία «διαρκούς βελτίωσης»



Πώς το ISO/IEC *2700x* συμβάλλει … (1)

Επίτευξη επιπέδου ασφάλειας ανάλογου προς τον εκάστοτε κίνδυνο

- ✓ **Το πρότυπο είναι προσανατολισμένο στη διαχείριση κινδύνου !**
- ✓ **Οι απαιτήσεις του επιβάλλουν:**
  - Εκπόνηση μελέτης αποτίμησης κινδύνου ως προς την ασφάλεια στοχεύοντας στην ***προτεραιοποιημένη*** αντιμετώπιση κινδύνων § 6.1.2 & § 6.1.3 (risk assessment & treatment).
  - Μεθοδολογικά η μελέτη αποτίμησης κινδύνου ασφάλειας καλύπτεται από πρότυπα όπως ***ενδεικτικά*** το ISO/IEC 27005 *(information security risk management)* και το NIST SP 800-30 *(risk management guide for information technology systems)*
  - Τα προσωπικά δεδομένα πρέπει να αποτελούν αναπόσπαστο μέρος της μελέτης αυτής και για τον λόγο αυτό έχουν αναπτυχθεί μεθοδολογίες τόσο σε επίπεδο προτύπων π.χ. ISO/IEC 29134 *(Guidelines for privacy impact assessments)* όσο και σε επίπεδο οδηγιών ευρωπαϊκών αρχών (π.χ. CNIL, ICO)

Πώς το ISO/IEC *2700x* συμβάλλει … (2)

Ανάπτυξη ικανοτήτων εντοπισμού, αντιμετώπισης και αναφοράς περιστατικών ασφάλειας και διαρροής δεδομένων

- ✓ **Οι απαιτήσεις του προτύπου επιβάλλουν:**
  - Εφαρμογή συνεκτικής πολιτικής και υλοποίηση μηχανισμών αποτελεσματικής διαχείρισης περιστατικών ασφάλειας (§ A.16) που καλύπτει μεταξύ άλλων υποχρεώσεις
    - Αναφοράς
    - Συλλογής και διαχείρισης ευρημάτων (evidence)
  - Μεθοδολογικά η διαδικασία διαχείρισης και αντιμετώπισης καλύπτεται από πρότυπα όπως ***ενδεικτικά*** το NIST SP 800-61 *(Computer Security Incident Handling Guide)*, ENISA Good Practice Guide for Incident Management κ.α.
  - Τα περιστατικά διαρροής προσωπικών δεδομένων αποτελούν αναπόσπαστο μέρος της διαχείρισης περιστατικών, σύμφωνα ***και*** με τους χρονικούς και λοιπούς περιορισμούς (το πρότυπο δεν προσδιορίζει)

ΗΔΙΚΑ
ΗΛΕΚΤΡΟΝΙΚΗ ΔΙΑΚΥΒΕΡΝΗΣΗ ΚΟΙΝΩΝΙΚΗΣ ΑΣΦΑΛΙΣΗΣ Α.Ε.

Πώς το ISO/IEC *2700x* συμβάλλει … (3)

Διαχείριση εμπλεκομένων τρίτων μερών

- ✓ **Οι απαιτήσεις του προτύπου επιβάλλουν:**
  - Την αποτύπωση της εμπλοκής τρίτων μερών στις διαδικασίες επεξεργασίας καθώς και τον καθορισμό της πολιτικής ελέγχου και διαχείρισής τους (§ 8)
  - Αναλυτικότερα (§ A.15) προβλέπεται η ενσωμάτωση συμβατικών δεσμεύσεων καθώς και μηχανισμών παρακολούθησης αναφορικά με την
    - προστασίας πληροφοριών και πόρων
    - τήρησης επιπέδου παρεχόμενων υπηρεσιών
  - Τα σχετικά με την προστασία των προσωπικών δεδομένων θέματα αποτελούν αναπόσπαστο μέρος σχετικών συμβάσεων, όπως και το δικαίωμα ελέγχου της εφαρμογής (right to audit) τους.

Πώς το ISO/IEC *2700x* συμβάλλει … (4)

Καταγραφή επεξεργασιών (αρχείο δραστηριοτήτων επεξεργασίας) και πόρων

- ✓ **Οι απαιτήσεις του προτύπου επιβάλλουν :**
  - Την αναλυτική καταγραφή και κατηγοριοποίηση αγαθών και πόρων (αποτύπωση περιβάλλοντος) στοχεύοντας στην αποτίμηση της αξίας τους για τον οργανισμό (§ 8 και (§ A.8)
  - Την συνακόλουθη εκτίμηση κινδύνου για τη λήψη κατάλληλων και αναλογικών ως προς τον κίνδυνο μέτρων προστασίας τους (§ 6.1 και § 6.2)
  - Η παραπάνω διαδικασία συνδέεται άμεσα με την ικανοποίηση της απαίτησης δημιουργίας αρχείου δραστηριοτήτων επεξεργασίας

Πώς το ISO/IEC *2700x* συμβάλλει … (5)

Με ανάλογο τρόπο διαπιστώνει κανείς ότι αντιμετωπίζονται πολλά σχετικά θέματα:

- ✓ Ελέγχου πρόσβασης (§ A.9)
- ✓ Φυσικής και περιβαλλοντικής ασφάλειας (§ A.11)
- ✓ Ασφάλειας λειτουργιών (§ A.12)
- ✓ Ασφαλούς ανάπτυξης και συντήρησης πληροφοριακών συστημάτων (§ A.14, A.12.5)
- ✓ Επιχειρησιακής συνέχεια (§ A.17, A.12.3)
- ✓ Εκπαίδευση και ευαισθητοποίηση προσωπικού (§ A.7.2)
- ✓ …

Συμπερασματικά, το ISO *27001* συμβάλλει πολλαπλά στην ικανοποίηση των κανονιστικών απαιτήσεων !

Πώς προσεγγίζουμε το θέμα στην ΗΔΙΚΑ (1)

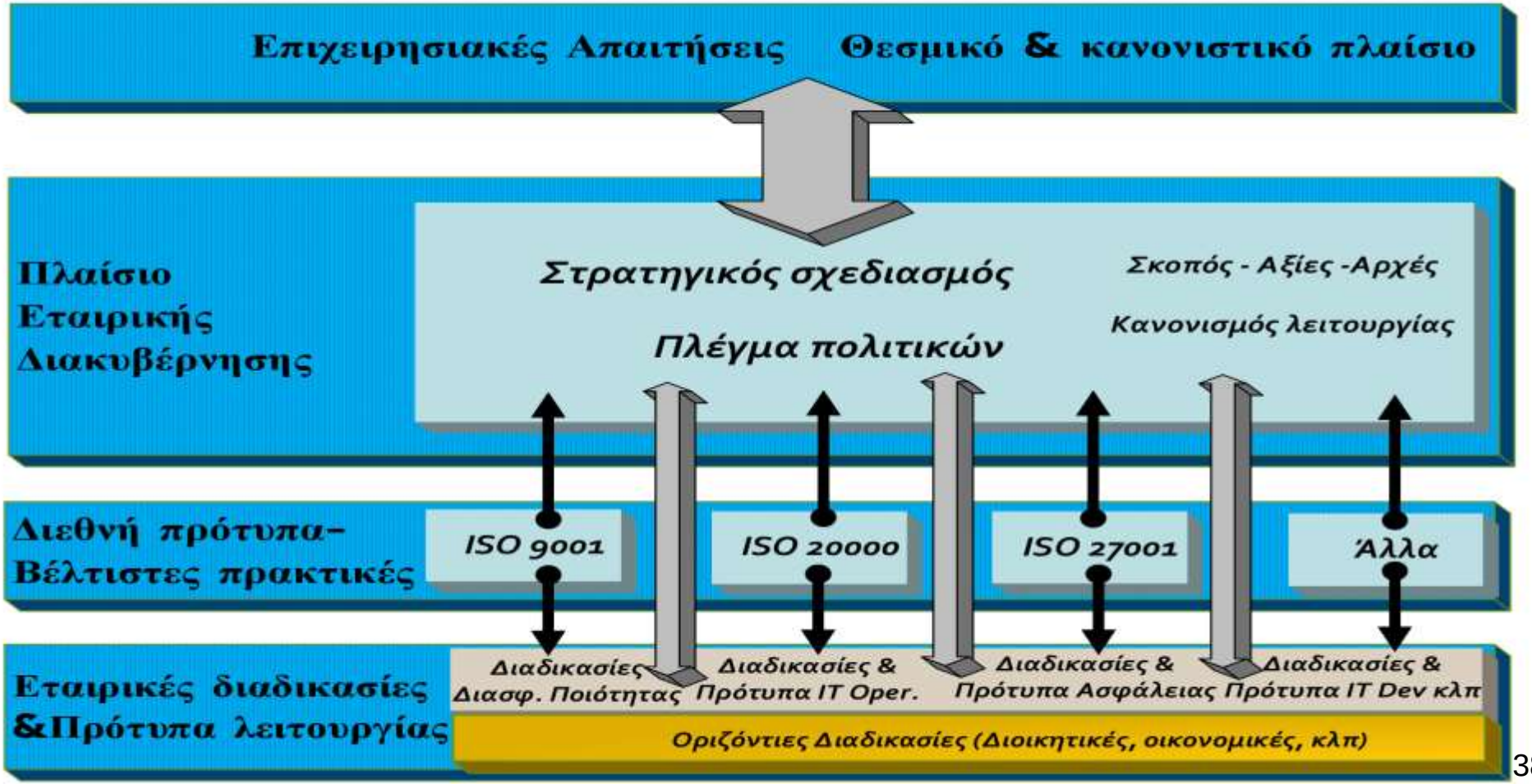
- ✓ ***Βελτίωση πλαισίου ασφάλειας πληροφοριών που προϋπήρχε***
  - Αποτύπωση, υιοθέτηση & εφαρμογή επικαιροποιημένων πολιτικών και διαδικασιών
  - Απόδοση ρόλων & αρμοδιοτήτων
  - «ΚΩΔΙΚΑΣ ΔΕΟΝΤΟΛΟΓΙΑΣ» εξουσιοδοτημένων χρηστών Πληροφοριακών Συστημάτων της ΗΔΙΚΑ ΑΕ.
  - Επιλογή συμβατών Εξωτερικών Συνεργατών και συμβατική δέσμευση αυτών για την προστασία των δεδομένων (Συμβάσεις Επεξεργασίας Δεδομένων) με δυνατότητα ελέγχου του Εκτελούντα από τον Υπεύθυνο.
  - ΣΥΜΒΑΣΕΙΣ ΕΡΓΩΝ: Ενσωμάτωση και επικαιροποίηση δεσμευτικών όρων περί Εμπιστευτικότητας και Εχεμύθειας των Αναδόχων.
- ✓ ***Θεσμοθέτηση και στελέχωση Γραφείων***
  - Προστασίας Δεδομένων (DPO)
  - Ασφάλειας Πληροφοριών
- ✓ ***Ανάλυση επιχειρησιακού περιβάλλοντος & κινδύνων***

Πώς προσεγγίζουμε το θέμα στην ΗΔΙΚΑ (2)

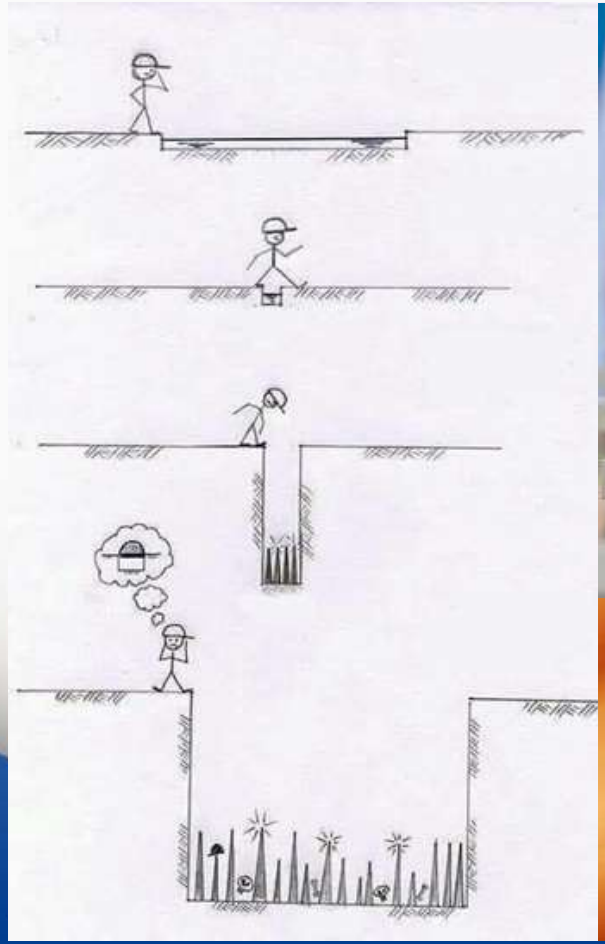
- ✓ ***Αναφορικά με τη συμμόρφωση σε σχέση με τις απαιτήσεις του ΓΚΠΔ***
  - Μητρώο επεξεργασιών (49 ως υπεύθυνος, 68 ως εκτελών)
  - Διενεργήθηκαν συνολικά 28 Εκθέσεις Εκτίμησης Αντικτύπου (DPIAs)
- ✓ ***Εκπόνηση σχεδίων δράσης για την άρση των αποκλίσεων (gap analysis)***
- ✓ ***Ενημέρωση, ευαισθητοποίηση & εκπαίδευση εργαζομένων***
- ✓ ***Διασφάλιση επιχειρησιακής συνέχειας***
- ✓ ***Μηχανισμοί αξιολόγησης δράσεων και λήψης μέτρων βελτίωσης ➔ Πιστοποίηση του οργανισμού κατά ISO 27001***

ΗΔΙΚΑ
ΗΛΕΚΤΡΟΝΙΚΗ ΔΙΑΚΥΒΕΡΝΗΣΗ ΚΟΙΝΩΝΙΚΗΣ ΑΣΦΑΛΙΣΗΣ Α.Ε.

Πώς προσεγγίζουμε το θέμα στην ΗΔΙΚΑ (3)



Συμπεράσματα και προβληματισμοί



"We all have dreams. But in order to make dreams come into reality, it takes an awful lot of determination, dedication, self-discipline, and effort."

–Jesse Owens

ΗΔΙΚΑ
ΗΛΕΚΤΡΟΝΙΚΗ ΔΙΑΚΥΒΕΡΝΗΣΗ ΚΟΙΝΩΝΙΚΗΣ ΑΣΦΑΛΙΣΗΣ Α.Ε.

Συμπεράσματα και προβληματισμοί

- ***GDPR - NISD & ISO 27001***:
  - ✓ Ο ΓΚΠΔ αποτελεί ένα ενιαίο σύνολο κανόνων δικαίου με δεσμευτικό χαρακτήρα, η παραβίαση των οποίων επιφέρει ποινές και πρόστιμα
  - ✓ Το ISO 27001 συνιστά έναν οδηγό βέλτιστων πρακτικών, χωρίς δεσμευτική ισχύ και άμεσες νομικές κυρώσεις.
  - ✓ Κοινός σκοπός και των δυο είναι η ασφάλεια και η προστασία των δεδομένων.
  - ✓ **Ο (Ευρωπαίος και Εθνικός) νομοθέτης**, εμπνεόμενος από την δομή και τη λειτουργία του ISO, **μετέτρεψε βέλτιστες πρακτικές σε κανόνες δικαίου**.
- ***DPO & CISO***: βίοι παράλληλοι & συμπληρωματικοί
  - ? Μπορούν / είναι σκόπιμο να **«ταυτίζονται» ή αντιθέτως πρέπει να είναι διακριτοί;**
  - ? Ποια είναι τα «χαρακτηριστικά» των «ρόλων»;
  - ? Που (πρέπει) να εντάσσονται στο «ιεραρχικό» & οργανωτικό σχήμα;
- **Η πρακτική εφαρμογή απαιτεί**
  - **γνώση** *του κανονιστικού πλαισίου* αλλά και *των αναγκών του οργανισμού* **καθώς και εμπειρία**
  - υποστήριξη και συμμετοχή εκ μέρους της Διοίκησης
  - διασφάλιση απαιτούμενων ανθρώπινων πόρων & υλικοτεχνικής υποδομής
- **Σε θεσμικό επίπεδο χρειάζονται προσπάθειες**
  - περαιτέρω υποστήριξη σε ζητήματα ερμηνείας και εφαρμογής
  - βελτίωσης των δομών και μηχανισμών αντιμετώπισης περιστατικών παραβιάσεων

ΗΔΙΚΑ
ΗΛΕΚΤΡΟΝΙΚΗ ΔΙΑΚΥΒΕΡΝΗΣΗ
ΚΟΙΝΩΝΙΚΗΣ ΑΣΦΑΛΙΣΗΣ Α.Ε.

Ευχαριστούμε για τη προσοχή σας !