Γραφεία ΣΕΒ,
Τετάρτη 7 Φεβρουαρίου 2018

Σύνοψη πρακτικών

(Τα παρακάτω αποτελούν βασικά σημεία των τοποθετήσεων που πραγματοποιήθηκαν κατά τη διάρκεια της εκδήλωσης, στο πλαίσιο του έργου «Παραγωγή προτάσεων βιομηχανικής πολιτικής και ανάπτυξης σύγχρονου περιβάλλοντος για τις επενδύσεις». Δεν αποτελούν επίσημα πρακτικά και συντάχθηκαν από τα στελέχη της Στέγης της Ελληνικής Βιομηχανίας για λογαριασμό του ΣΕΒ.)

Το πλαίσιο

Ο ΣΕΒ, στο πλαίσιο μετάβασης των επιχειρήσεων στην ψηφιακή οικονομία, έχει αναλάβει την εκπόνηση μιας **σειράς εξειδικευμένων εργαστηρίων** που θα βοηθήσουν τις ελληνικές επιχειρήσεις να γίνουν **ψηφιακά ανταγωνιστικές** και να εκμεταλλευτούν τις νέες ευκαιρίες και τις προκλήσεις που δημιουργούνται.

Η θέσπιση του Ευρωπαϊκού Κανονισμού Προστασίας Δεδομένων Προσωπικού Χαρακτήρα εισάγει **νέες απαιτήσεις αναβάθμισης των λειτουργικών δομών και εκσυγχρονισμού των πολιτικών τήρησης και διαχείρισης των δεδομένων** των επιχειρήσεων και έχει προξενήσει το ενδιαφέρον αλλά και την ανησυχία τους για το μέγεθος των προσαρμογών στις οποίες πρέπει να προβούν και τον τρόπο που διαχειρίζονται τα δεδομένα που συγκεντρώνουν.

Αναγνωρίζοντας την ανάγκη για εξειδικευμένη ενημέρωση και υποστήριξη των μελών του στο θέμα αυτό, ο ΣΕΒ διοργάνωσε εργαστήριο με τίτλο **«Ευκαιρίες και προκλήσεις από την εφαρμογή του νέου Κανονισμού για τα Προσωπικά Δεδομένα (GDPR)»** στις εγκαταστάσεις του (Ξενοφώντος 5).

Σκοπός της εκδήλωσης

Σκοπό του εργαστηρίου αποτέλεσε η κατανόηση των ευκαιριών και προκλήσεων που απορρέουν από τον Κανονισμό, η καλύτερη προετοιμασία των επιχειρήσεων για τη συμμόρφωση με τις απαιτήσεις του αλλά και η άρση των ανησυχιών τους μέσα από την παρουσίαση καλών ευρωπαϊκών πρακτικών αλλά και των διαθέσιμων εργαλείων της νομικής επιστήμης, των τεχνολογιών πληροφορικής και της αγοράς.

Τα βασικά ερωτήματα:

Πρέπει να συμμορφωθώ με τον Κανονισμό; Ποια θεωρούνται προσωπικά δεδομένα; Είναι απαραίτητο να προσλάβω Data Protection Officer (DPO); Ποια προσωπικά δεδομένα τηρώ και δεν το ξέρω; Θα προλάβω να συμμορφωθώ; Πόσο θα κοστίσει αυτή η διαδικασία; Πόσο θα αλλάζει τον τρόπο που λειτουργώ ήδη; Τι κάνουν οι επιχειρήσεις στις άλλες ευρωπαϊκές χώρες;

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Βασικά συμπεράσματα:

Στο πλαίσιο των παρουσιάσεων των ομιλητών αλλά και της συζήτησης που αναπτύχθηκε με αφορμή τις απαντήσεις που δόθηκαν σε ερωτήματα του κοινού, ακολουθούν τα βασικότερα σημεία της εκδήλωσης.

Ο **Γενικός Διευθυντής του ΣΕΒ κ. Σκέρτσος**, απευθύνοντας ένα σύντομο χαιρετισμό προς τα μέλη και τους ομιλητές ανέδειξε την υψηλή τεχνικότητα που χαρακτηρίζει τις διατάξεις του νέου Γενικού Κανονισμού GDPR στις οποίες ενσωματώνονται οι αρχές των επιστημών της νομικής και της πληροφορικής.

Παράλληλα, μετέφερε τον φόβο και την ανασφάλεια που κυριαρχούν στην αγορά ως απόρροια των προβλέψεων του Κανονισμού για ιδιαιτέρως υψηλά πρόστιμα, αλλά και τη σύγχυση που έχει προκληθεί από τη λανθασμένη αντίληψη ορισμένων επιχειρήσεων περί παράτασης της εφαρμογής του Κανονισμού.

Τέλος, με αφορμή την πρόσφατη εμπειρία του ίδιου του ΣΕΒ από την πρώτη απόπειρα για συμμόρφωση με τον Κανονισμό, παρέθεσε τα τρία σημαντικότερα βήματα που θα πρέπει να εφαρμόσουν όλες οι επιχειρήσεις προκειμένου να επιτύχουν αυτό που κατά τον ΣΕΒ αποτελεί την «έξυπνη συμμόρφωση»:

Πρώτον, «νοικοκύρεμα» των δεδομένων, ως μια ευκαιρία που δίνει το νέο πλαίσιο για καλύτερη εσωτερική οργάνωση, δεύτερον, μετατροπή της υποχρέωσης συμμόρφωσης σε ανταγωνιστικό πλεονέκτημα και τρίτον, ενσωμάτωση των ψηφιακών τεχνολογιών στην επιχειρηματική λειτουργία.

Στη συνέχεια**, ο Πρόεδρος Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα**, προέβη σε ιδιαίτερα κρίσιμες αποσαφηνίσεις αναφορικά με το νομοθετικό και κανονιστικό πλαίσιο, αλλά και σε επεξηγήσεις ως προς τα πρακτικά εφαρμοστικά ζητήματα. Ιδιαίτερα σημαντική ήταν η επισήμανσή του ως προς την πρόθεση της Αρχής να εστιάσει σε ενημερωτικές και εκπαιδευτικές δράσεις με αποδέκτες τις επιχειρήσεις, αλλά και η διαβεβαίωσή του ότι δεν αποτελεί αυτοσκοπό η επιβολή υπέρογκων προστίμων και κυρώσεων, ειδικά κατά την πρώτη περίοδο εφαρμογής του Κανονισμού.

Παράλληλα και ενώ ενημέρωσε για τους περιορισμένους πόρους της Αρχής σε επίπεδο στελεχιακού δυναμικού, δεν παρέλειψε να αναφερθεί στην διακριτική ευχέρεια που διαθέτουν οι ελεγκτές για διαβαθμισμένη εξέταση των υποθέσεων και να αποτραπεί η ευδοκίμηση καταχρηστικών και κακόβουλων καταγγελιών.

Κλείνοντας, υπενθύμισε στους συμμετέχοντες το πνεύμα του Κανονισμού με βάση το οποίο θα πρέπει να κινούνται οι επιχειρήσεις και το οποίο καλεί για διαρκή ικανότητα απόδειξης της προσαρμογής τους στις διατάξεις του καθώς και την πραγματική αλλαγή στη φιλοσοφία απέναντι στην προστασία των προσωπικών δεδομένων.

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Ο **κεντρικός ομιλητής κ. Watkins, UK Country Leader της International Association of Privacy Professionals (IAPP),** επιβεβαίωσε ότι ποτέ δεν είναι υπερβολικά αργά να ξεκινήσει κανείς να συμμορφώνεται με τον Κανονισμό, καθώς ακόμα και για το Ηνωμένο Βασίλειο, ο βαθμός συμμόρφωσης αρκετών επιχειρήσεων δεν είναι ιδιαίτερα υψηλός. Βασικό σημείο της παρουσίασής του αποτέλεσε η αποτύπωση των οικονομικών μεγεθών τα οποία σχετίζονται με την αξία που έχουν τα προσωπικά δεδομένα που τηρούν οι επιχειρήσεις. Στη συνέχεια, τόνισε ότι όπως συμβαίνει και με τα θέματα κυβερνοασφάλειας, έτσι και με την ιδιωτικότητα, δεν νοείται η έννοια της απόλυτης ασφάλειας και προστασίας.

Όπως πολύ παραστατικά εμφάνισε στο πλαίσιο της παρουσίασης παραδειγμάτων επιχειρήσεων που εντοπίστηκαν να παραβιάζουν τη νομοθεσία περί προσωπικών δεδομένων και του οικονομικού αντικτύπου που οι σχετικές παραβάσεις προκάλεσαν, οι τέτοια περιστατικά μπορεί να αποδειχθούν εξαιρετικά επαχθή καθώς μπορεί να επιφέρουν τεράστιο πλήγμα στις επιχειρήσεις που συνακόλουθα θα τους κοστίσει την εμπιστοσύνη και την πίστη των καταναλωτών τους.

Ο κ. Watkins ανέδειξε επίσης τη σημασία επιλογής των κατάλληλων συνεργατών αλλά και την ανάγκη επένδυσης σε αξιόπιστους συμβούλους και ιδίως στον Data Protection Officer.

Συζήτηση - Ερωτήσεις

Απαντώντας σε ερωτήματα του κοινού, τοποθετήθηκε ως προς το ρόλο του DPO αποσαφηνίζοντας τη φύση του ως απόλυτα ανεξάρτητου οργάνου, είτε βρίσκεται εντός είτε εκτός της επιχείρησης, εκτιμώντας ωστόσο ότι είναι πιθανό να αναθεωρηθεί στο μέλλον η παρούσα αντίληψη, λόγω του μεγάλου αριθμού των σχετικών απόψεων.

Ως προς την αυστηρότητα των εποπτικών αρχών κατά το πρώτο διάστημα εφαρμογής του Κανονισμού και δεδομένης της αδυναμίας επίτευξης απόλυτης ασφάλειας, εκτίμησε ότι οι εθνικές αρχές θα φανούν επιεικείς εφόσον διαπιστώσουν ότι η επιχείρηση κατέβαλε τη δέουσα προσπάθεια συμμόρφωσης με τον Κανονισμό.

Τέλος, αναφορικά με τον προβληματισμό ως προς την εγκυρότητα των πιστοποιήσεων που προσφέρονται στην αγορά, διευκρίνισε ότι παρότι η πιστοποίηση δεν επιβάλλεται, εντούτοις είναι σημαντική η εκπαίδευση του DPO καθώς αποδεικνύει την επίδειξη της απαιτούμενης επιμέλειας εκ μέρους της επιχείρησης για τήρηση των διατάξεων του Κανονισμού.

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

1ο μέρος

Ο κ. **Neil Patrick, Director of the Centre of Excellence for GRC & Security της SAP,** παρουσίασε την ετοιμότητα της SAP να προσφέρει τεχνολογικά προϊόντα ως λύσεις συμμόρφωσης με το νέο πλαίσιο διευκρινίζοντας ωστόσο ότι η σωστή συμμόρφωση προϋποθέτει την αλλαγή κουλτούρας εντός της επιχείρησης, από το επίπεδο του μεμονωμένου εργαζομένου ως το Διοικητικό Συμβούλιο που φέρει και την ευθύνη για το νομικό πρόσωπο.

Παράλληλα επιβεβαίωσε την ασάφεια του Κανονισμού ως προς τις ενέργειες στις οποίες καλούνται να προβούν οι επιχειρήσεις αλλά και την έλλειψη καλών παραδειγμάτων από περιστατικά εφαρμογής του.

Απαρίθμησε ωστόσο τις βασικές αρχές οποίες θα πρέπει να τηρούνται διαρκώς προκειμένου να αποδεικνύεται η συμμόρφωση με το νέο πλαίσιο:

1. Τήρηση αρχείων

2. Τεκμηρίωση των αποφάσεων διεκπεραίωσης και επεξεργασίας των δεδομένων

3. Εντοπισμός των δεδομένων

4. Εκτίμηση κινδύνου

5. Κατάταξη δεδομένων σε δομημένα και αδόμητα

6. Εντοπισμός παρωχημένων δεδομένων και διαγραφή τους εφόσον δεν είναι απαραίτητα

7. Καταγραφή των προσώπων που έχουν πρόσβαση στα δεδομένα

8. Καταγραφή των τηρούμενων διαδικασιών

9. Διερεύνηση περιπτώσεων μεταφοράς δεδομένων από επιχείρηση σε επιχείρηση και διασυνοριακά εντός της Ευρώπης

10. Καταγραφή περιπτώσεων φορητότητας δεδομένων και ακολουθούμενης διαδικασίας

11. Εκπαίδευση προσωπικού

Σύμφωνα με τον κ. Patrick, η μείωση του κόστους εφαρμογής με τον Κανονισμό περνάει μέσα από τις λύσεις και τα τεχνικά εργαλεία που παρέχει η πληροφορική και τα οποία θα επιτρέψουν την αυτοματοποίηση των διαδικασιών που θα πρέπει να επαναλαμβάνονται.

Και τέλος, κάνοντας συγκεκριμένη αναφορά σε ένα περιστατικό παραβίασης της ασφάλειας των δεδομένων, απέδειξε τη σημασία της αξίας αυτών, καθώς μετά το περιστατικό, χάθηκε το 1/3 της αξίας της επιχείρησης.

Ευρωπαϊκή Ένωση · ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ ΥΠΟΥΡΓΕΙΟ ΟΙΚΟΝΟΜΙΑΣ & ΑΝΑΠΤΥΞΗΣ · ΕΠΑνΕΚ 2014-2020 ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ ΚΑΙΝΟΤΟΜΙΑ · ΕΣΠΑ 2014-2020

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Οι εκπρόσωποι της εταιρείας **Microsoft, κκ. Παπανικολάου, Διευθύντρια Νομικών & Εταιρικών Υποθέσεων, και Αναστόπουλος, Solution Sales Team Manager,** παρουσίασαν τα διαθέσιμα εργαλεία πληροφορικής που είναι σε θέση να διασφαλίσουν την προστασία των δεδομένων ανάλογα με τις ανάγκες και τις προδιαγραφές κάθε επιχειρηματικής μονάδας, με προσιτούς οικονομικούς όρους και να αποτελέσουν μια καλή ευκαιρία αξιοποίησης του ανεκμετάλλευτου πλούτου των δεδομένων που συχνά διαθέτουν οι επιχειρήσεις με εφαρμογές και εργαλεία big data και business analytics. Σύμφωνα με τους ίδιους, η τεχνολογία μπορεί να είναι σύμμαχος για την διασφάλιση τήρησης της ορθής διαδικασίας πρόσβασης στα δεδομένα και έγκαιρου εντοπισμού και εκτίμησης των κινδύνων.

Ειδικότερα, έμφαση έδωσαν στην εμπειρία των τεχνικών συμβούλων ως προς τη διασφάλιση του privacy by design και του privacy by default.

Για την κ. Παπανικολάου, τα τέσσερα βήματα βοηθούν στην συμμόρφωση:

1. Καταγραφή των δεδομένων που τηρούνται από την επιχείρηση είναι τα εξής

2. Αναθεώρηση του τρόπου και των πολιτικών διαχείρισης

3. Ενίσχυση ασφάλειας των συστημάτων

4. Εύρεση τρόπων τεκμηρίωσης προς το υποκείμενο των δεδομένων αλλά και της ΑΠΔΠΧ περί της ορθότητας του τρόπου διαχείρισης των δεδομένων και περί τήρησης της δέουσας επιμέλειας

Ο κ. Αναστόπουλος παρουσίασε με συνοπτικό τρόπο την ποικιλία των εργαλείων που διατίθενται για κάθε στάδιο συμμόρφωσης με τον Κανονισμό, από τον εντοπισμό, την καταγραφή και την κατηγοριοποίηση των δεδομένων έως την παρακολούθηση του κύκλου ζωής τους, τη λήψη των προληπτικών και κατασταλτικών μέτρων και την σύνταξη και αποστολή αναφοράς σε περίπτωση παραβίασης.

Ο κ. Γιώργος Γιαννόπουλος, Επίκουρος Καθηγητής στη Νομική Σχολή του Πανεπιστημίου Αθηνών και Διευθυντής του Εργαστηρίου Νομικής Πληροφορικής της Νομικής Σχολής, απομόνωσε τις απαντήσεις στα κυριότερα ερωτήματα των επιχειρήσεων διευκρινίζοντας ότι:

1. Υπεύθυνος για την επεξεργασία είναι πάντα η επιχείρηση η οποία φέρει την, αντικειμενική κατά τον κ. Γιαννόπουλο, ευθύνη αφενός μεν να λάβει όλα τα κατάλληλα τεχνικά και οργανωτικά μέτρα και να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τον Κανονισμό και αφετέρου να επανορθώσει τη ζημία από την παράνομη επεξεργασία. Δεν αρκεί επομένως να αποδείξει ότι δεν έφταιγε, αλλά οφείλει ανά πάσα στιγμή να αποδεικνύει ότι κινήθηκε εντός των ορίων του Κανονισμού. Ευθύνη ωστόσο φέρει και ο εκτελών, για λογαριασμό της επιχείρησης, την επεξεργασία

2. Εισάγονται αλλαγές στις εσωτερικές διαδικασίες των επιχειρήσεων, οι οποίες αφορούν α) στην ενημέρωση του υποκειμένου σχετικά με τις ενέργειες στις οποίες πρόκειται να προβεί

Ευρωπαϊκή Ένωση
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ ΥΠΟΥΡΓΕΙΟ ΟΙΚΟΝΟΜΙΑΣ & ΑΝΑΠΤΥΞΗΣ ΕΙΔΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΕΠΑ & ΤΣ
ΕΠΑνΕΚ 2014-2020 ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ ΚΑΙΝΟΤΟΜΙΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

η επιχείρηση για την αποστολή των δεδομένων του, εντός ενός μηνός από το χρονικό σημείο που τα αναζήτησε, β) στη δυνατότητα τεχνικής υποστήριξης της φορητότητας των δεδομένων σε ηλεκτρονική μορφή, ανά πάσα στιγμή το ζητήσει το υποκείμενο των δεδομένων, γ) στην ικανότητα γνωστοποίησης των παραβιάσεων εντός 72 ωρών τόσο προς την ΑΠΔΠΧ όσο και προς το υποκείμενο των δεδομένων στην περίπτωση που υπάρχει παραβίαση των δικαιωμάτων και των ελευθεριών αυτών και δ) στην υποχρέωση για τήρηση ειδικών αρχείων στην περίπτωση επιχειρήσεων που απασχολούν πάνω από 250 εργαζόμενους ή επεξεργάζονται ειδικές κατηγορίες δεδομένων

3. Σε επίπεδο συστημάτων εισάγονται δυο έννοιες από τον χώρο της πληροφορικής, α) η έννοια του data protection by design, δηλαδή του σχεδιασμού των συστημάτων κατά τέτοιο τρόπο ώστε να είναι συμβατά με τον Κανονισμό και β) η έννοια του data protection by default δηλαδή η υποχρέωση υιοθέτησης συστημάτων που εξ ορισμού έχουν τις κατάλληλες ιδιότητες για επεξεργασία μόνο των ελάχιστων δεδομένων σύμφωνα με τις προϋποθέσεις του Κανονισμού

4. Ο διορισμός υπεύθυνου Προστασίας Προσωπικών Δεδομένων (Data Protection Officer) εξαρτάται από τον όγκο και το είδος των δεδομένων που τηρούνται, όπως για παράδειγμα η τακτική ή συστηματική παρακολούθηση δεδομένων σε μεγάλη κλίμακα, η λειτουργία συστημάτων γεωεντοπισμού, η μεγάλης κλίμακας επεξεργασία των ειδικών κατηγοριών, όπως φυλετική και εθνική καταγωγή, πολιτικές πεποιθήσεις κ.ά.

Καθώς η παράλειψη διορισμού DPO από τις επιχειρήσεις που φέρουν την υποχρέωση αυτή από τον Κανονισμό, επισύρει ξεχωριστό πρόστιμο, φαίνεται, σύμφωνα και με τα όσα ανέφερε ο κ. Watkins, ότι όσες διόρισαν DPO παρότι δεν όφειλαν, θα αντιμετωπιστούν με επιείκεια από την εποπτεύουσα αρχή.

Τέλος, εξήγησε με τη σειρά του ότι η πιστοποίηση, παρότι δεν προβλέπεται από τον Κανονισμό ως επίσημη και υποχρεωτική διαδικασία, εντούτοις μπορεί να βοηθήσει στην καλύτερη ενημέρωση και προετοιμασία των επιχειρήσεων καθώς και στην απόδειξη προς την εποπτεύουσα Αρχή, ότι επέδειξαν την απαιτούμενη επιμέλεια συμμόρφωσης με το νέο πλαίσιο.

Ο κ. **Τάσσης, Πρόεδρος της Ελληνικής Ένωσης για την Προστασία των Προσωπικών Δεδομένων και την Ιδιωτικότητα** παρουσίασε τη σημασία που έχει η διενέργεια της έκθεσης εκτίμησης αντικτύπου (Data Protection Impact Assessment- DPIA) καθώς μπορεί, εφόσον δεν γίνει τυπικά και επικαιροποιείται τακτικά, να αποτελέσει ένα ευέλικτο εργαλείο ανάλυσης κινδύνων για τις επιχειρήσεις, βοηθώντας τις επιχειρήσεις να κατανοήσουν και να μετριάσουν τους κινδύνους από τους οποίους απειλούνται όχι μόνο κατά την τήρηση των προσωπικών δεδομένων αλλά και ως μέρος της γενικότερης πολιτικής ασφαλείας που έτσι κι αλλιώς θα έπρεπε να ακολουθούν.

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Μεγάλη βαρύτητα έδωσε στην γνώση που θα πρέπει να έχουν όλοι οι εργαζόμενοι σε μια επιχείρηση, ως προς το είδος των δεδομένων που τηρούνται και τις σχετικές διαδικασίες καθώς η συγκεκριμένη πληροφορία είναι η πρώτη που θα ζητηθεί από την εποπτεύουσα αρχή σε περίπτωση ελέγχου.

Διευκρίνισε ότι η εκτίμηση αντικτύπου ανταποκρίνεται στην αρχή της λογοδοσίας που εισάγει ο Κανονισμός και είναι υποχρεωτική για τις επιχειρήσεις που εκτελούν συστηματική και εκτενή αξιολόγηση προσωπικών πτυχών, μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών (ευαίσθητων) δεδομένων καθώς και συστηματική παρακολούθηση δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα δηλαδή κάμερες σε δημόσιους χώρους.

Προσδιόρισε την έννοια του «κινδύνου» για κάθε κατηγορία δεδομένων, ως την υπόθεση εργασίας που περιγράφει ένα συμβάν και τις επιπτώσεις του και την εκτίμηση με όρους σοβαρότητας και πιθανότητας επέλευσης ενώ, ως διαχείριση κινδύνου προσδιόρισε τις συντονισμένες δραστηριότητες για την καθοδήγηση και τον έλεγχο ενός Οργανισμού ως προς τον κίνδυνο.

Ιδιαίτερα ως προς τα προσωπικά δεδομένα, η ανάλυση κινδύνου θα πρέπει να περιέχει τις πιθανές απειλές για το πρόσωπο, για το υποκείμενο των προσωπικών δεδομένων, για το φυσικό πρόσωπο και την κατηγοριοποίηση των προσωπικών δεδομένων αναλόγως με την κρισιμότητά τους.

Ο βαθμός κινδύνου των δεδομένων και η απαίτηση για εκπόνηση DPIA αποτελεί συνάρτηση της κατηγοριοποίησης της επεξεργασίας σε α) υψηλού κινδύνου, όπου χρειάζεται οπωσδήποτε DPIA και για την οποία ο Κανονισμός και η ομάδα του άρθρου 29 προτείνει διαβούλευση και με την Αρχή, αλλά και με τις ομάδες των υποκειμένων καθώς και γνωστοποιήσεις του άρθρου 33 προς την Αρχή, β) απλού κινδύνου, όπου απαιτείται η εκπόνηση DPIA καθώς και κάποιες γενικές γνωστοποιήσεις στον τύπο ή στο site της εταιρείας και γ) χαμηλού κινδύνου, όπου η εκπόνηση DPIA είναι προαιρετική χωρίς υποχρέωση γνωστοποιήσεων.

Παρόλα αυτά, ανεξαρτήτως του είδους της επεξεργασίας, ο κ. Τάσσης εκτιμά ότι η εκπόνηση DPIA είναι καλό να πραγματοποιηθεί σε κάθε περίπτωση καθώς βοηθά στην διαμόρφωση και καταγραφή συγκεκριμένης πολιτικής της επιχείρησης ως προς την αντιμετώπιση συμβάντων παραβίασης της προστασίας των προσωπικών δεδομένων αλλά και συμβάντων υποβολής κακόβουλων καταγγελιών και αθέμιτου ανταγωνισμού.

Τέλος, απαρίθμησε τα στάδια που πρέπει να ακολουθήσουν οι επιχειρήσεις στο πλαίσιο της εκπόνησης της DPIA ως εξής:

• Αναγνώριση της ανάγκης για εκπόνηση DPIA σύμφωνα με τα κριτήρια του Κανονισμού αλλά και τις ιδιαιτερότητες κάθε εταιρείας και, σε κάθε περίπτωση εκπόνησή της πριν από την επεξεργασία από τον υπεύθυνος επεξεργασίας σε συνεργασία με τον DPO αλλά και τον εκτελούντα την επεξεργασία

Ευρωπαϊκή Ένωση
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ ΥΠΟΥΡΓΕΙΟ ΟΙΚΟΝΟΜΙΑΣ & ΑΝΑΠΤΥΞΗΣ
ΕΠΑνΕΚ 2014-2020 ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ ΚΑΙΝΟΤΟΜΙΑ
ΕΣΠΑ 2014-2020
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

• Σχηματοποίηση της ροής των data flows

• Καταγραφή του εύρους των απειλών που είναι δυνατό να εμφανιστούν

• Προσδιορισμός και αξιολόγηση της πιθανότητας κινδύνου για κάθε κατηγορία δεδομένων

• Τμηματοποίηση και επικαιροποίηση της DPIA μετά από κάθε αλλαγή

• Εφαρμογή της DPIA τόσο στο πλαίσιο του Κανονισμού όσο και στο πλαίσιο της γενικότερης πολιτικής της επιχείρησης

• Δημοσίευσή της μετά από απαλοιφή των επιχειρηματικών και τεχνολογικών μυστικών, όπως και των ιδιαιτεροτήτων πάνω στις οποίες στηρίχθηκε η εκπόνησή της

Αναφορικά με τη μεθοδολογία, εξήγησε ότι παρότι αυτή δεν είναι συγκεκριμένη, η γαλλική εποπτική αρχή έχει δημοσιεύσει σχετικά μια μεθοδολογία και ένα εργαλείο στο site της.

Στη συνέχεια, το πρώτο μέρος του εργαστηρίου ολοκληρώθηκε με τις απαντήσεις των ομιλητών σε ερωτήσεις του κοινού.

Συζήτηση - Ερωτήσεις

Ειδικότερα, ο κ. Γιαννόπουλος αποσαφήνισε ότι έννοια της επεξεργασίας «μεγάλης κλίμακας» δεν συνδέεται με τον αριθμό των εργαζομένων που απασχολεί ο υπεύθυνος επεξεργασίας αλλά με το είδος των δεδομένων που επεξεργάζεται.

Ο κ. Τάσσης αναφέρθηκε στον υπό έκδοση εφαρμοστικό του Κανονισμού νόμο, εκτιμώντας ότι δεν θα συμπεριλάβει διατάξεις της νέας Οδηγίας e- privacy αναφορικά με θέματα όπως το spam mail και τους τρόπους παροχής σχετικής συγκατάθεσης καθώς και τις επιθετικές πωλήσεις και στις προωθήσεις προϊόντων.

Ως προς την υποχρεωτικότητα εκπόνησης έκθεσης εκτίμησης αντικτύπου, επανέλαβε την αξία που έχει η δυνατότητα τεκμηρίωσης της όποιας επιλογής της επιχείρησης αλλά και καθησύχασε το κοινό εξηγώντας ότι η DPIA δεν απαιτεί ιδιαίτερο κόστος και πόρους, αλλά αποδεικνύει την καλή γνώση που οφείλει να έχει ο υπεύθυνος επεξεργασίας των δεδομένων που τηρεί και του κινδύνου απώλειάς τους.

Στο ίδιο θέμα, ανέδειξε την ελευθερία που έχει ο κάθε υπεύθυνος επεξεργασία κατά την επιλογή της μεθοδολογίας εκπόνησης DPIA και τις πιθανές διαφοροποιήσεις ως προς τον απαιτούμενο χρόνο ολοκλήρωσής της καθώς και τα ερωτηματικά που παραμένουν έως την έκδοση του εφαρμοστικού νόμου σχετικά με τον τρόπο ορισμού DPO στους δημόσιους οργανισμούς και φορείς.

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Περαιτέρω, αναλύοντας τα επιτρεπόμενα όρια της συναίνεσης που καλείται να δώσει προς την επιχείρηση το υποκείμενο των δεδομένων, ανέδειξε το στοιχείο της αναλογικότητας εντός των αρχών της οποίας οφείλει να κινείται η συγκεκριμένη διαδικασία.

Τέλος, με αφορμή την αναφορά που έκανε στις υπό ενσωμάτωση νέες Οδηγίες ePrivacy και NES και τις υποχρεώσεις που θα επιβάλουν σε συγκεκριμένες οντότητες, τόνισε την κρισιμότητα που η διενέργεια μιας DPIA τη δεδομένη χρονική στιγμή μπορεί να έχει για την προετοιμασία των επιχειρήσεων για το ευρύτερο νέο θεσμικό πλαίσιο.

2ο μέρος

Ο κ. Νίκος Μαρουλιανάκης, Head of Infrastructure & Enterprise Data της Interamerican ξεκίνησε την παρουσίασή του τονίζοντας τη σημασία του awareness και της εκπαίδευσης του προσωπικού ούτως ώστε να αποφευχθούν φαινόμενα απώλειας ή κλοπής δεδομένων. Στο πλαίσιο αυτό, στην Interamerican έχουν οργανώσει τις ακόλουθες ενέργειες: Ανέβασμα videos, κουίζ, ζωντανές παρουσιάσεις, εκκαθάριση των επιφανειών εργασίας (clean desk assessment) και οργάνωση αποθηκευτικών χώρων, καταγραφή του ιστορικού των δεδομένων (data lineage) και τήρηση αρχείου επεξεργασίας προσωπικών δεδομένων (personal data processing registry) με ιδιαίτερη επισήμανση των προσωπικών και ευαίσθητων δεδομένων καθώς και των δεδομένων με αξία για την εταιρεία.

Παράλληλα δημιουργήθηκε κοινό γλωσσάρι δεδομένων ώστε να υπάρχει η σωστή κατανόηση από όλους, δημιουργήθηκε διαδικασία ελέγχου κίνησης δεδομένων (data traffic control) ώστε για οποιοδήποτε εξερχόμενο να ακολουθείται συγκεκριμένη διαδικασία και ολοκληρώθηκε η καταστροφή των παλαιών φακέλων, κάτι το οποίο διήρκησε πολύ περισσότερο από όσο εκτιμήθηκε αρχικά. Τέλος, εξαιρετικά βασικό κομμάτι της διαδικασίας αποτέλεσε ο εντοπισμός των περιττών δεδομένων (waste) αλλά και των αδόμητων δεδομένων (unstructured) καθώς όπως αποδείχθηκε, ο όγκος τους είναι μεγαλύτερος από τον εκτιμώμενο και απαιτείται διαρκής παρακολούθηση και εκκαθάρισή τους.

Κλείνοντας, συνέστησε τη διενέργεια Data Protection Impact Assessment ακόμη κι αν δεν είναι υποχρεωτική βάσει των διατάξεων του Κανονισμού, καθώς θα βοηθήσει και στη διάγνωση της ψηφιακής ετοιμότητας της επιχείρησης (digital benchmark) και την αναβάθμισή της ως προς το στοιχείο αυτό.

Ο κ. Άγγελος Κούρος, Corporate Lawyer της ΑΒ Βασιλόπουλος, εξήγησε ότι στην επιχείρηση, η κουλτούρα σεβασμού των προσωπικών δεδομένων προϋπήρχε του νέου Κανονισμού και συνεπώς, είχε δει πολύ νωρίς το νέο πλαίσιο ως «ευκαιρία». Στη συνέχεια, μίλησε για τις ενέργειες στις οποίες προέβη ο Όμιλος προκειμένου να εναρμονίσει τις πολιτικές και τις διαδικασίες του στα νέα δεδομένα, λαμβάνοντας υπόψη ότι τα φυσικά πρόσωπα των οποίων τα δεδομένα τηρούνται από την επιχείρηση ήταν τεσσάρων ειδών, προμηθευτές, πελάτες, υπάλληλοι και τρίτα πρόσωπα. Στη βάση αυτή, έγιναν τα ακόλουθα βήματα: 1) συστάθηκε ομάδα εργασίας σε κάθε επιχείρηση του Ομίλου, η οποία εξασφάλισε τη δέσμευση των

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

ιεραρχικά ανώτερων στελεχών για διάθεση των απαιτούμενων πόρων για τους σκοπούς του έργου και 2) προέβη σε ενημέρωση όλων των τμημάτων που διαχειρίζονται προσωπικά δεδομένα. Στη συνέχεια 3) δημιουργήθηκαν ερωτηματολόγια για την καταγραφή των δεδομένων αυτών, 4) συντάχθηκαν record keepings για αναλυτικό προσδιορισμό των τηρούμενων διαδικασιών και των αρμοδίων προσώπων, όπως του processor και του controller, των εμπλεκόμενων συστημάτων, τυχόν retention periods κ.ά., 5) καταγράφηκαν τα κενά (gaps), εκ των οποίων το βασικότερο είναι η περίοδος διατήρησης των δεδομένων (retention period), 6) ενημερώθηκαν σχετικά τα στελέχη και 7) οργανώθηκαν οι επόμενες κινήσεις ως εξής:

Αλλαγή της ενημέρωσης των υποκειμένων των σχημάτων loyalty, ανάληψη δράσεων εκπαίδευσης και ενημέρωσης, μείωση του χρόνου διατήρησης των βιογραφικών, αλλαγές των όρων των συμβάσεων, υιοθέτηση νέων πολιτικών, εκπόνηση DPIA, αξιολόγηση της συμμόρφωσης των προμηθευτών με τον νέο Κανονισμό.

Ακόμα, τόνισε τη σημασία της εκπαίδευσης, της ορθής επιλογής του DPO, της ανάθεσης διακριτών ρόλων και ανάλογης διαβάθμισης στην πρόσβαση στα δεδομένα αλλά και της ιδιαίτερης προσοχής που πρέπει να δοθεί στα φυσικά αρχεία και τις διαδρομές που ακολουθούν αυτά εντός της επιχείρησης. Και τέλος, προσδιόρισε την προστιθέμενη αξία του κανονισμού σε δύο επίπεδα, πρώτον την δημιουργία αισθήματος εμπιστοσύνης στον πελάτη και εξασφάλιση της πιστότητάς του και δεύτερον, την δημιουργία ευκαιριών για οργανωτικές αλλαγές στην επιχείρηση και αναβάθμιση των συστημάτων.

Κατά το κλείσιμο της εκδήλωσης, **η συντονίστρια κ. Σπυριδάκη Μαρίνα, Διευθύντρια του Τομέα Επιχειρηματικού Περιβάλλοντος και Ρυθμιστικών Πολιτικών του ΣΕΒ** συνόψισε τα βασικότερα σημεία που αναδείχθηκαν από τις παρουσιάσεις όλων των ομιλητών, ως εξής:

Η εφαρμογή του Κανονισμού αποτελεί κυρίως ευκαιρία, παρόλο που οι δυσκολίες είναι υπαρκτές. Υπάρχει ανάγκη για συνεχή ενημέρωση, αφενός γιατί τα πραγματικά ερωτήματα προκύπτουν μόνο όταν ξεκινήσει κανείς να τον εφαρμόζει στην πράξη και αφετέρου γιατί η πολιτική στόχευση του κανονισμού δεν έχει γίνει ακόμη κτήμα μας.

Πρώτο αναγκαίο βήμα και προϋπόθεση μιας επιτυχημένης συμμόρφωσης είναι η γνώση σχετικά με τα δεδομένα που τηρούνται στην επιχείρηση, των προσώπων που τα τηρούν, τη συχνότητα και το λόγο τήρησής τους αλλά και η εκκαθάριση όσων η τήρηση των οποίων δεν είναι απαραίτητη ή τα οποία δεν αξιοποιούνται όπως θα μπορούσαν, είτε σε έντυπη είτε σε ηλεκτρονική μορφή.

Στη συνέχεια, η κ. Σπυριδάκη παρουσίασε μια λίστα με «χρήσιμες συμβουλές προς ναυτιλλομένους» κατά την εφαρμογή των διατάξεων του Κανονισμού στην οποία περιέλαβε τα ακόλουθα:

1. Τη σημασία της δέσμευσης της διοίκησης στη σταδιακή αλλαγή της κουλτούρας, θέτοντας την προστασία των προσωπικών δεδομένων σε μια από τις βασικές εταιρικές αξίες

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

2. Την εμπλοκή όλων των οργανικών μονάδων της επιχείρησης και την εκπαίδευση όσο των δυνατόν περισσότερων στελεχών μαζί με την ενεργό συμμετοχή από την πρώτη στιγμή του προσώπου εκείνου που θα οριστεί ως Data Protection Officer

3. Την αναγνώριση και καταγραφή των τηρούμενων προσωπικών δεδομένων, με στόχο να κρατάμε μόνο τα απαραίτητα και μόνο για το απολύτως αναγκαίο χρονικό διάστημα

4. Την ανάπτυξη πολιτικών και διαδικασιών που δεν επιβαρύνουν και παρεμποδίζουν την συνήθη επιχειρηματική λειτουργία αλλά αντίθετα τη διαφυλάττουν

5. Την επένδυση σε κατάλληλους συνεργάτες και εργαλεία πληροφορικής

6. Και τέλος την επικοινωνία με την ΑΠΔΠΧ

Κλείνοντας, ενημέρωσε ότι, για την υποστήριξη και παρακολούθηση της εφαρμογής του κανονισμού αλλά και τη διατήρηση της ροής της πληροφόρησης και τη δημιουργία μιας κοινότητας γνώσης και εμπειρίας γύρω από τις νέες προκλήσεις, ο ΣΕΒ πρόκειται να δημιουργήσει μόνιμη ομάδα εργασίας. Για το λόγο αυτό, προέτρεψε τους εκπροσώπους των μελών να δηλώσουν συμμετοχή συμπληρώνοντας την κατάλληλη φόρμα εκδήλωσης ενδιαφέροντος.

Ο ΣΕΒ πρόκειται να εκδώσει άμεσα ειδική θεματική μελέτη, στην οποία θα αναπτύσσει τα κυριότερα ζητήματα εφαρμογής του Κανονισμού, καταγράφοντας την πορεία υλοποίησής του, την ευρωπαϊκή εμπειρία και τις καλές πρακτικές και τις ευκαιρίες που αναδεικνύονται από τη σωστή εφαρμογή του νέου πλαισίου.

Φωτογραφικό υλικό

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΟΙΚΟΝΟΜΙΑΣ & ΑΝΑΠΤΥΞΗΣ
ΕΙΔΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΕΠΙΑ & ΤΣ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΕΠΑνΕΚ
ΕΠΑνΕΚ 2014-2020
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ
ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ
ΚΑΙΝΟΤΟΜΙΑ
ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης


What I'm Hearing
Anger
ΣΕΒ
Ν. ΑΝΑΣΤΟΠΟΥΛΟΣ
ΣΠ. ΤΑΣΣΗΣ
Μ. ΣΠΥΡΙΔΑΚΗ
N. PATRICK


Discover
Example solutions
ΣΕΒ
ΣΠ. ΤΑΣΣΗΣ
N. PATRICK

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΟΙΚΟΝΟΜΙΑΣ & ΑΝΑΠΤΥΞΗΣ
ΕΙΔΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΕΠΙΑ & ΤΣ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΕΠΑνΕΚ
ΕΠΑνΕΚ 2014-2020
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ
ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ
ΚΑΙΝΟΤΟΜΙΑ
ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης


INTERAMERICAN
GDPR: Is it just another regulation or a great opportunity for operational excellence?
ΣΕΒ


ΣΕΒ