ΤΕΥΧΟΣ 23 | 14 Μαρτίου 2018

ΟΙΚΟΝΟΜΙΑ & ΕΠΙΧΕΙΡΗΣΕΙΣ | SPECIAL REPORT
ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

ΣΕΒ
Σύγχρονες Επιχειρήσεις, Σύγχρονη Ελλάδα

Ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR): ευκαιρίες και προκλήσεις για τις επιχειρήσεις στην εποχή της ψηφιοποίησης

Τα data είναι το "πετρέλαιο" της 4ης βιομηχανικής επανάστασης. Σύμφωνα με εκτιμήσεις, η αξία της αγοράς των προσωπικών δεδομένων υπολογίζεται ότι θα ανέλθει σε σχεδόν €1 τρισ. το 2020, ενώ έως το 2025 εκτιμάται ότι ο όγκος των δεδομένων θα αυξηθεί από 16,1 ZB σε 163 ZB. Αναμενόμενα, καθώς τα ίδια τα δεδομένα και η αγορά που διαμορφώνεται γύρω από αυτά διογκώνονται, αυξάνονται εκθετικά και οι κίνδυνοι παραβίασής τους ακόμη και σε μεγάλες επιχειρήσεις, με εξαιρετικά δυσμενείς επιπτώσεις. Ταυτόχρονα, η διαχείρισή τους με σεβασμό στην προσωπικότητα και την ιδιωτική ζωή του καθενός μας, θα γίνει σταδιακά βασικό κριτήριο αξιολόγησης κάθε επιχείρησης που χειρίζεται προσωπικά δεδομένα, δηλαδή πρακτικά όλων. Επιχειρηματικοί κολοσσοί όπως η Yahoo!, η Uber και η Target, όταν ήρθαν αντιμέτωπες εσωτερικά με σοβαρές υποθέσεις παραβίασης ή διαρροής προσωπικών δεδομένων, δεν έχασαν μόνο δεδομένα αξίας εκατομμυρίων ευρώ, αλλά και μέρος του σημαντικότερου περιουσιακού στοιχείου της επιχείρησης: αυτό της καλής φήμης και της αξιοπιστίας.

Η αλυσίδα τέτοιων φαινομένων, αλλά και η ανάγκη ρύθμισης της αγοράς των προσωπικών δεδομένων, οδήγησαν στην αυστηροποίηση του νομικού πλαισίου πανευρωπαϊκά και στη θέσπιση του νέου Γενικού Κανονισμού GDPR. Με έναρξη εφαρμογής την 25η Μαΐου 2018, ο νέος Κανονισμός, προβλέποντας ένα αρκετά αυστηρό και γραφειοκρατικό πλαίσιο, έρχεται να θωρακίσει την ιδιωτικότητα και να μεταθέσει την ευθύνη της προστασίας στην ίδια την επιχείρηση, προβλέποντας κυρώσεις ύψους έως και 4% του παγκόσμιου τζίρου για όσους αποτύχουν να συμμορφωθούν με τις απαιτήσεις του. Συνεπώς η συμμόρφωση με τις απαιτήσεις του Ευρωπαϊκού Κανονισμού παρουσιάζει ένα δίλημμα για τον επιχειρηματικό κόσμο: θα την αντιμετωπίσουμε ως άλλη μια κανονιστική υποχρέωση - δηλαδή σαν βάρος - ή σαν μια ευκαιρία αλλαγής του επιχειρηματικού μοντέλου και εισαγωγής των ελληνικών επιχειρήσεων στον κόσμο της ψηφιακής οικονομίας;

Παρότι η «συμμόρφωση» φαίνεται να συνεπάγεται υψηλά κόστη και βαριές διαδικασίες, οι ειδικοί του χώρου επιμένουν: Εκείνος που θα μετατρέψει την κουλτούρα σεβασμού και προστασίας των προσωπικών δεδομένων σε πυρήνα της καθημερινής του λειτουργίας, θα αποκτήσει αυτόματα ένα «ανταγωνιστικό πλεονέκτημα». Γιατί θα είναι εκείνος που θα είναι διαρκώς σε θέση να αποδείξει στον καταναλωτή, τον πελάτη, τον εργαζόμενο, όχι μόνο ότι έχει λάβει τα απαραίτητα μέτρα προστασίας των προσωπικών δεδομένων τους, αλλά και ότι είναι διαρκώς σε θέση να τα διατηρεί προστατευμένα.

Με την τεχνολογία πολύτιμο συμπαραστάτη στη διαδικασία συμμόρφωσης, και ακολουθώντας τα 10 + 1 βήματα για έξυπνη συμμόρφωση που ο ΣΕΒ προτείνει, είναι εφικτή η υιοθέτηση λύσεων «κομμένων και ραμμένων» στις ανάγκες και τις ιδιαιτερότητες κάθε οργανισμού, ακόμα και τώρα, λίγες ημέρες μόλις πριν την έναρξη εφαρμογής του.

Το παρόν συντάχθηκε από τον Τομέα Επιχειρηματικού Περιβάλλοντος και Ρυθμιστικών Πολιτικών του ΣΕΒ, αξιοποιώντας στοιχεία που παράχθηκαν στο πλαίσιο του έργου «Μηχανισμός παρακολούθησης των αλλαγών και υποστήριξης των δράσεων ανάπτυξης και προσαρμοστικότητας της βιομηχανίας», το οποίο συγχρηματοδοτείται από την Ελλάδα και την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο) μέσω του ΕΠ «Ανταγωνιστικότητα, Επιχειρηματικότητα και Καινοτομία».

Τομέας Μακροοικονομικής Ανάλυσης και Ευρωπαϊκής Πολιτικής

Μιχάλης Μασουράκης
Chief Economist
E: mmassourakis@sev.org.gr
T: +30 211 500 6104

Μιχάλης Μητσόπουλος
Senior Advisor
E: mmitsopoulos@sev.org.gr
T: +30 211 500 6157

Θανάσης Πρίντσιπας
Associate Advisor
E: printsipas@sev.org.gr
T: +30 211 500 6176

Τι είναι ο νέος Γενικός Κανονισμός για την Προστασία Δεδομένων και τι σημαίνει για τις επιχειρήσεις;

Σε δύο μήνες περίπου, δηλαδή στις 25 Μαΐου 2018, ξεκινάει στην Ευρωπαϊκή Ένωση (ΕΕ) η οριζόντια και καθολική εφαρμογή του **Γενικού Κανονισμού για την Προστασία Δεδομένων** (γνωστού ως General Data Protection Regulation - GDPR)[1]. Η υψηλή τεχνικότητα που απαιτείται για τη διαχείριση του ζητήματος προϋποθέτει τη διαμόρφωση ενός υβριδίου γνώσεων νομικής και πληροφορικής επιστήμης, και σε συνδυασμό με την προοπτική ιδιαιτέρως υψηλών προστίμων σε περίπτωση μη συμμόρφωσης (έως €20 εκ. ή έως το 4% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών, ανάλογα με το ποιο είναι υψηλότερο), προκαλεί στις επιχειρήσεις ανάμεικτα συναισθήματα ανασφάλειας, φόβου, άγνοιας, αλλά ακόμη και αδιαφορίας.

Αυτό αναδείχτηκε τόσο στο **θεματικό εργαστήριο** που πραγματοποιήσαμε για τις προκλήσεις και τις ευκαιρίες συμμόρφωσης στον Κανονισμό στις αρχές Φεβρουαρίου, με διακεκριμένους ομιλητές από την Ελλάδα και το εξωτερικό, όσο και κατά τη διάρκεια μιας περιορισμένης έκτασης έρευνας που πραγματοποιήσαμε σε επιχειρήσεις μέλη μας. Εύλογα αναρωτιέται κανείς, ιδίως με το βεβαρημένο ιστορικό μας στην αργοπορημένη ενσωμάτωση της ευρωπαϊκής νομοθεσίας, πώς θα καταφέρουμε να συμμορφωθούμε επί της ουσίας και στην ώρα μας. Πώς θα μπορέσουν να προσαρμοστούν, ιδίως οι μικρομεσαίες επιχειρήσεις, με τους ήδη περιορισμένους πόρους που διαθέτουν, σε ένα αντικειμενικά βαρύ πλαίσιο υποχρεώσεων (π.χ. κόστος συμβούλων, ηλεκτρονικά συστήματα προστασίας, πρόσληψη Υπευθύνου Προστασίας Δεδομένων-ΥΠΔ). Αλλά και σε ό,τι αφορά τις μεγαλύτερες επιχειρήσεις, ή όσες αντιμετωπίζουν ένα ήδη απαιτητικό κανονιστικό πλαίσιο (π.χ. τράπεζες, εισηγμένες, τηλεπικοινωνίες κ.ά.), πώς αυτές θα μπορέσουν να προσαρμόσουν με ομαλό τρόπο στην επιχειρηματική τους λειτουργία τον Κανονισμό.

Με απλά λόγια, ο Κανονισμός αποτελεί ένα κοινό πλαίσιο ρυθμίσεων για τον τρόπο με τον οποίο συλλέγονται, επεξεργάζονται, φυλάσσονται, διακινούνται, αξιοποιούνται, αλλά και καταστρέφονται, δεδομένα προσωπικού χαρακτήρα των πολιτών της ΕΕ, ανεξαρτήτως του τόπου διαμονής τους, τόσο σε ηλεκτρονική όσο και σε φυσική μορφή. Έχει γενική εφαρμογή, καθώς αφορά τόσο τις επιχειρήσεις του ιδιωτικού τομέα (ανεξαρτήτως μεγέθους και κλάδου δραστηριοποίησης), όσο και τους φορείς του δημοσίου. Ταυτίζεται συνεπώς με πολιτικές και διαδικασίες της επιχείρησης (π.χ. για τις συμβάσεις, τη διεξαγωγή διαγωνισμών, την εξυπηρέτηση πελατών), με υποδομές και συστήματα που χρησιμοποιούνται (π.χ. servers, ηλεκτρονικό ταχυδρομείο, USB sticks, CRM, POS), με πράξεις αυτοδέσμευσης της διοίκησης (π.χ. Κώδικες Δεοντολογίας και συστήματα πιστοποίησης), με το ανθρώπινο δυναμικό (π.χ. διαδικασίες προσλήψεων, συμβάσεις προσωπικού, ομαδικά συμβόλαια ασφάλισης, βιογραφικά σημειώματα και συνεντεύξεις), αλλά κυρίως με την κουλτούρα της επιχείρησης. Δηλαδή αποτελεί έναν εναλλακτικό τρόπο οργάνωσης και λειτουργίας της επιχείρησης που θέτει στο επίκεντρο τη διαφύλαξη των προσωπικών δεδομένων. Ή για να ακριβολογούμε, που θέτει στο επίκεντρο την ικανότητα να αποδείξει η επιχείρηση με τεκμήρια ότι κατά τη λειτουργία της λαμβάνει όλα τα αναγκαία μέτρα για να διαφυλάξει τα προσωπικά δεδομένα.

Στην πράξη, για ένα μάλλον μεγάλο αριθμό επιχειρήσεων ο νέος Κανονισμός αποτελεί άλλη μια υποχρέωση που πρέπει να εκπληρώσουν έως τα μισά του χρόνου, αναθέτοντας σε κάποιο εξωτερικό σύμβουλο τη σύνταξη κάποιας έκθεσης (την οποία θα διατηρούν «ξεχασμένη» σε κάποιο συρτάρι), αγοράζοντας κάποια πρόσθετα πληροφοριακά συστήματα (τα οποία ούτε καν θα αναβαθμίζουν) και αναθέτοντας την ιδιότητα του ΥΠΔ σε ένα στέλεχος που διαθέτει ήδη μερικές ακόμη (π.χ. Υπεύθυνος Κανονιστικής Συμμόρφωσης, Νομικός Σύμβουλος κ.λπ.). Δηλαδή ως μια υποχρέωση στατική, σημειακή και πάντως όχι ως οργανικό κομμάτι της λειτουργίας ή της

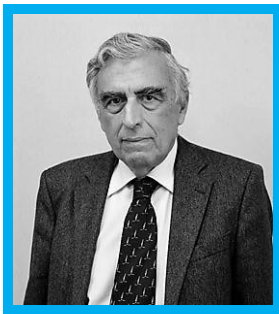
[1] **Δείτε εδώ συγκεντρωμένους τους ορισμούς των βασικότερων εννοιών του Κανονισμού, προς διευκόλυνσή σας.**

κουλτούρας τους.

Για ένα μικρότερο αριθμό επιχειρήσεων ο νέος Κανονισμός αποτελεί μια ευκαιρία να αποκτήσουν ανταγωνιστικό πλεονέκτημα και να ενισχύσουν την αξία τους, επενδύοντας στην ασφάλεια των δεδομένων, πελατών, προμηθευτών και προσωπικού.

Για τον ΣΕΒ, σκοπός δεν πρέπει να είναι η εφαρμογή του Κανονισμού «μόνο στα χαρτιά». Πραγματική στόχευση αυτής της «υποχρεωτικής άσκησης» στην οποία όλοι θα υποβληθούμε, είναι να αλλάξουμε ουσιαστικά την κουλτούρα των επιχειρήσεών μας, διαφυλάττοντας τα προσωπικά δεδομένα που διαχειριζόμαστε. Στις επόμενες ενότητες της παρούσας έκθεσης παρουσιάζουμε τον τρόπο με τον οποίο μπορεί να υπάρξει μια ουσιαστική αλλά και έξυπνη συμμόρφωση, που δεν θα επιβαρύνει με σημαντικό χρηματικό και διοικητικό κόστος την καθημερινή λειτουργία των επιχειρήσεων.

Ο Γενικός Κανονισμός για την Προστασία Δεδομένων αποτελεί ένα κοινό πλαίσιο ρυθμίσεων για τον τρόπο με τον οποίο συλλέγονται, επεξεργάζονται, φυλάσσονται, διακινούνται, αξιοποιούνται, αλλά και καταστρέφονται, δεδομένα προσωπικού χαρακτήρα των πολιτών της ΕΕ, ανεξαρτήτως τόπου διαμονής τους, με άμεση εφαρμογή από την 25η Μαΐου 2018.



Κωνσταντίνος Φ. Μενουδάκος
Πρόεδρος της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

«…Υπάρχει προσδοκία ότι ο Γενικός Κανονισμός θα αποτελέσει λυσιτελές θεσμικό πλαίσιο ώστε να περιοριστούν οι κίνδυνοι που δημιουργούνται για τα προσωπικά δεδομένα στο κοινωνικό, οικονομικό και τεχνολογικό περιβάλλον της σύγχρονης ψηφιακής εποχής. Η αποτελεσματικότητά του εξαρτάται από την ορθή εφαρμογή του. Προς τούτο απαιτείται αντικειμενική ενημέρωση και προετοιμασία των υπευθύνων και εκτελούντων επεξεργασία προσωπικών δεδομένων σύμφωνα με τις πραγματικά υφιστάμενες υποχρεώσεις τους και όχι με βάση υπερβολικές και ανεύθυνες εκτιμήσεις και υποδείξεις…».

Δείτε ολόκληρο το άρθρο εδώ.

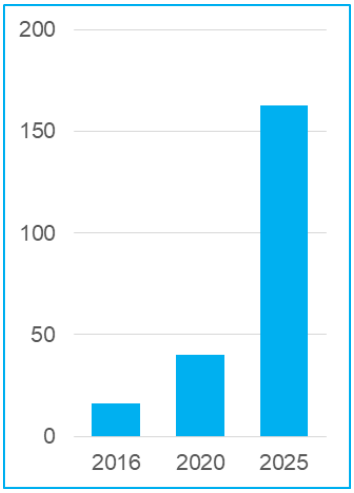
Πόσο αναγκαίος ήταν τελικά ο Κανονισμός και γιατί όλοι πασχίζουν να τον εφαρμόσουν;

Η ανάγκη προστασίας των προσωπικών δεδομένων και το κανονιστικό πλαίσιο που τη διασφαλίζει, δεν είναι κάτι νέο ούτε στην ΕΕ αλλά ούτε και στη χώρα μας. Ήδη από το 1995 ο Ευρωπαίος νομοθέτης εισήγαγε σημαντικές υποχρεώσεις στα κράτη-μέλη (βλ. Οδηγία 95/46/ΕΚ), διασφαλίζοντας αφενός την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, (δηλαδή το σεβασμό στην ιδιωτικότητα) και αφετέρου την εξασφάλιση της ελεύθερης κυκλοφορίας των δεδομένων αυτών, ως μέσο επίτευξης οικονομικής και κοινωνικής προόδου.

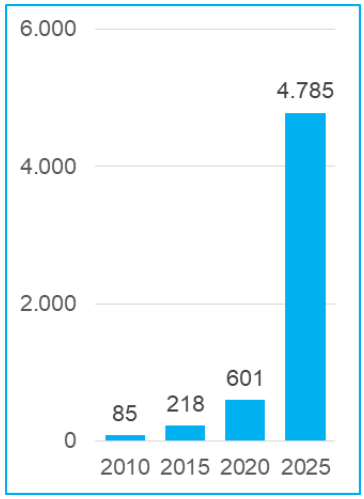
Ωστόσο, **δύο καθοριστικές παράμετροι κατέστησαν αναγκαία τη μεταρρύθμιση του κανονιστικού πλαισίου**, όπως αυτή εκφράστηκε με τον νέο Κανονισμό, καθώς τα μέτρα πολιτικής που ίσχυσαν μέχρι σήμερα εξάντλησαν την όποια αποτελεσματικότητά τους. Η πρώτη, αναμενόμενα, αφορά στις **ραγδαίες τεχνολογικές εξελίξεις** που έλαβαν χώρα, αλλάζοντας τον κόσμο όπως τον ξέραμε και καθιστώντας την Οδηγία παρωχημένη. Η δεύτερη αφορά στην **ασυμμετρία εφαρμογής της Οδηγίας από τα κράτη-μέλη**, αλλά και τελικά στο έλλειμμα προστασίας της ιδιωτικότητας που φάνηκε στην πράξη. Ειδικότερα:

Όταν το 1995 θεσπίστηκε η Οδηγία 95/46/ΕΚ, το διαδίκτυο όχι μόνο δεν ήταν διόλου διαδεδομένο, αλλά πολύ λίγοι ήταν εκείνοι που θα μπορούσαν να προβλέψουν την εξέλιξή του. Μέσα σε λίγα μόλις χρόνια, οι ραγδαίες τεχνολογικές εξελίξεις (διαδίκτυο, κινητή τηλεφωνία, big data κ.ά.) οδήγησαν στην αύξηση της έκτασης και έντασης της συλλογής, ανταλλαγής και επεξεργασίας δεδομένων προσωπικού χαρακτήρα από ιδιωτικές επιχειρήσεις και δημόσιες αρχές με γεωμετρική πρόοδο. Είναι χαρακτηριστικό ότι έως το 2025 εκτιμάται ότι ο όγκος των δεδομένων θα αυξηθεί από 16,1 ZB σε 163 ZB[2], σύμφωνα με μελέτη της εταιρείας επιχειρηματικής πληροφόρησης International Data Corporation (IDC) **(Δ1)**. Τόσο τα προσωπικά, όσο και αλλά πάσης φύσεως δεδομένα, απέκτησαν μια έντονα εμπορική διάσταση, δημιουργώντας μια νέα παγκόσμια αγορά για την εύρυθμη λειτουργία της οποίας απαιτούνταν η ελεύθερη κυκλοφορία τους. Τέλος, μεταβλήθηκε ο τρόπος που τα ίδια τα φυσικά πρόσωπα χειρίζονται τα δεδομένα τους, δημοσιοποιώντας πλέον ολοένα και περισσότερο, αλλά και ευκολότερα, προσωπικές πληροφορίες και κατ' επέκταση καθιστώντας τες διαθέσιμες προς εκμετάλλευση (π.χ. μέσα κοινωνικής δικτύωσης). Στην προαναφερθείσα μελέτη εκτιμάται ότι έως το 2025 ο μέσος άνθρωπος θα έχει αλληλεπίδραση με μία συνδεδεμένη συσκευή σχεδόν 4.800 φορές την ημέρα **(Δ2)**.

Δ1. Όγκος δεδομένων που δημιουργούνται ανά έτος, σε zettabytes
Πηγή: IDC, "Data Age 2025: The Evolution of Data to Life-Critical", Απρίλιος 2017



Δ2. Αλληλεπίδραση με μία συνδεδεμένη συσκευή, σε φορές ανά ημέρα
Πηγή: IDC, "Data Age 2025: The Evolution of Data to Life-Critical", Απρίλιος 2017



[2] 1 ZB = 10^{21} bytes

Οι οικονομικές συνέπειες της ψηφιακής επανάστασης είναι σίγουρα εντυπωσιακές. Σύμφωνα με εκτιμήσεις, **η αξία της αγοράς των προσωπικών δεδομένων υπολογίζεται ότι θα ανέλθει σε σχεδόν €1 τρισ. το 2020**[3]**.**

Όμως, η εξέλιξη της τεχνολογίας δεν δημιούργησε απλά μια νέα εκθετικά αναπτυσσόμενη αγορά προσωπικών δεδομένων, διευκολύνοντας τη συγκέντρωση και την επεξεργασία τους, αλλά ταυτόχρονα διευκόλυνε και την παραβίασή τους. Στον πίνακα **(Δ3)** παρουσιάζονται ενδεικτικά ορισμένα πρόσφατα παραδείγματα περιπτώσεων παραβίασης της ασφάλειας δεδομένων προσωπικού χαρακτήρα, τα οποία αιτιολογούν την αναγκαιότητα ενός νέου πλαισίου προστασίας των προσωπικών δεδομένων, αλλά και του κυβερνοχώρου, που να ανταποκρίνεται στη σύγχρονη πραγματικότητα. Για το λόγο αυτό άλλωστε, παράλληλα με τον Κανονισμό, το Μάιο του 2018 θα ξεκινήσει και η υποχρέωση συμμόρφωσης των κρατών-μελών στην **Οδηγία 1148/2016** σχετικά με τα μέτρα ασφαλείας συστημάτων δικτύου και πληροφοριών (Network and Information Systems - NIS), στο πλαίσιο μιας ολοκληρωμένης ευρωπαϊκής πολιτικής για την κυβερνοασφάλεια.

Η συζήτηση για τον κίνδυνο ανάδυσης μια «ψηφιακής δικτατορίας» μόλις σε μερικές δεκαετίες από σήμερα, η οποία θα αντλεί τη δύναμή της από τον τεράστιο όγκο προσωπικών δεδομένων που θα έχουν κάποιοι λίγοι στα χέρια τους (δείτε **εδώ** την πρόσφατη ομιλία του ιστορικού Yuval Harari), εξηγεί εξίσου την αναγκαιότητα που γέννησε, για κάποιους μάλλον καθυστερημένα[4], το νέο Γενικό Κανονισμό για την Προστασία Δεδομένων. Με άλλα λόγια, **ο Κανονισμός αποτελεί μια χαρακτηριστική περίπτωση εκ των υστέρων ρύθμισης, όπου ο νομοθέτης έρχεται να θεραπεύσει και όχι να προλάβει**, καθώς η τεχνολογία προπορεύεται κατά πολύ του δικαίου, αλλά και ίσως της ηθικής.

Δ3. Παραδείγματα περιπτώσεων παραβίασης της ασφάλειας δεδομένων προσωπικού χαρακτήρα

Περίπτωση Yahoo! Inc.

Προφίλ: Εταιρεία διαδικτυακών υπηρεσιών, με έδρα τις ΗΠΑ
Ημερομηνία συμβάντος: 2013-2014
Ημερομηνία ανακοίνωσης συμβάντος: Σεπτέμβριος 2016 (αρχική) - Οκτώβριος 2017
Περιγραφή συμβάντος: Απώλεια προσωπικών δεδομένων (ονομάτων, ημερομηνιών γέννησης, ηλεκτρονικών διευθύνσεων και κωδικών πρόσβασης) 3 δισ. πελατών.
Εκτίμηση κόστους: $350 εκ. (εκτίμηση για τις απώλειες της αξίας της τιμής της μετοχής της Yahoo! ενόψει της πώλησής της στην Verizon Communications, καθώς εκείνο το διάστημα εξελίσσονταν οι διαπραγματεύσεις)
Άλλα στοιχεία: Η εταιρεία προέβη σε διαδοχικές ανακοινώσεις, το διάστημα από Σεπτέμβριο του 2016 έως τον Οκτώβριο του 2017, σχετικά με τον αριθμό χρηστών των οποίων τα δεδομένα παραβιάστηκαν, αυξάνοντας τον αριθμό από 500 εκ., σε 1 δισ. και τελικά σε 3 δισ. χρήστες. Τα περιστατικά παραβίασης ήταν περισσότερα από ένα, την περίοδο 2013 και 2014.

Περίπτωση Uber Technologies Inc.

Προφίλ: Εταιρεία παροχής υπηρεσιών μετακίνησης, με έδρα τις ΗΠΑ
Ημερομηνία συμβάντος: Οκτώβριος 2016
Ημερομηνία ανακοίνωσης συμβάντος: 22 Νοεμβρίου 2017
Περιγραφή συμβάντος: Κλοπή προσωπικών δεδομένων (ονομάτων, ηλεκτρονικών διευθύνσεων και κινητών τηλεφώνων) 57 εκ. χρηστών και 600 χιλ. οδηγών, λόγω κυβερνοεπίθεσης.
Άλλα στοιχεία: Η εταιρεία, εκτός του ότι προέβη σε ανακοίνωση του συμβάντος με καθυστέρηση σχεδόν ενός έτους, παραδέχτηκε ότι κατέβαλε λύτρα αξίας $100 χιλ. στους χάκερς, προκειμένου να καταστρέψουν τα προσωπικά δεδομένα που απέκτησαν (δίχως βεβαίως να υπάρχει απόδειξη για τις ενέργειες καταστροφής). Το συμβάν προκάλεσε την απόλυση του Διευθυντή Ασφαλείας.

[3] Ευρωπαϊκή Επιτροπή, Fact Sheet "Questions and Answers-General Data Protection Regulation", Ιανουάριος 2018
[4] Ενδεικτικό είναι το γεγονός ότι η Ευρωπαϊκή Επιτροπή επισήμανε την ανάγκη τροποποίησης της Οδηγίας από τον Ιανουάριο του 2012, το Ευρωπαϊκό Κοινοβούλιο υπερψήφισε το σχέδιο Κανονισμού το Μάρτιο του 2014 και η τελική συμφωνία μεταξύ του Κοινοβουλίου, της Επιτροπής και του Συμβουλίου επήλθε το Δεκέμβριο του 2015. Ο Κανονισμός ψηφίστηκε το Μάιο του 2016 και δόθηκε διετής περίοδος προσαρμογής στα κράτη-μέλη έως το Μάιο του 2018.

Περίπτωση Target Stores Inc.

Προφίλ: Εταιρεία λιανικού εμπορίου, με έδρα τις ΗΠΑ
Ημερομηνία συμβάντος: Δεκέμβριος 2013
Περιγραφή συμβάντος: Κλοπή προσωπικών δεδομένων (ονομάτων, ταχυδρομικών διευθύνσεων, ηλεκτρονικών διευθύνσεων και τηλεφώνων) 110 εκ. πελατών, λόγω κυβερνοεπίθεσης.
Εκτίμηση κόστους: $162 εκ.
Άλλα στοιχεία: Εκτιμάται ότι οι χάκερς απέκτησαν πρόσβαση στα μηχανήματα υποδοχής καρτών (POS) των πελατών, μέσω ενός τρίτου προμηθευτή της εταιρείας. Η παραβίαση των δεδομένων εκτιμάται ότι αποκαλύφθηκε με καθυστέρηση ορισμένων εβδομάδων. Προκάλεσε την παραίτηση του Διευθυντή Πληροφοριακών Συστημάτων το Μάρτιο του 2014 και του Διευθύνοντα Συμβούλου δύο μήνες μετά.

Πηγή: https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html και https://www.techworld.com/security/uks-most-infamous-data-breaches-3604586/

Οι τεχνολογικές εξελίξεις μετέβαλαν τον όγκο των δεδομένων και την ευκολία πρόσβασης και επεξεργασίας τους, τον τρόπο επιχειρηματικής λειτουργίας, αλλά και τις συνήθειες των φυσικών προσώπων.

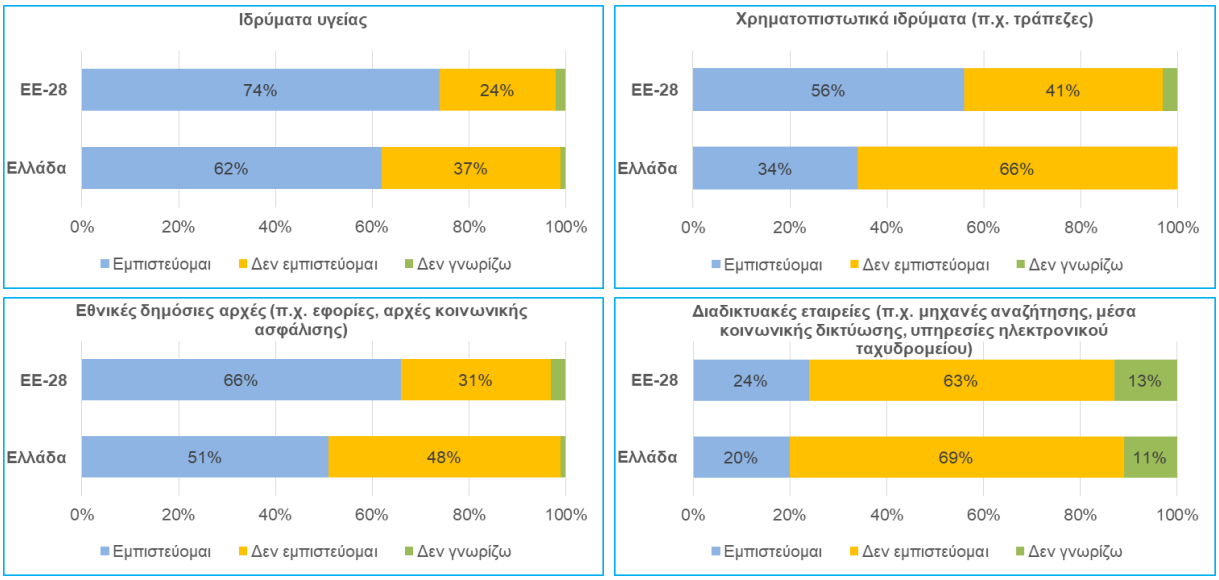
Στα παραπάνω έρχεται να προστεθεί και η αποτυχία της ευρωπαϊκής πολιτικής (μέσω της Οδηγίας) να αποτρέψει τον **κατακερματισμό του τρόπου εφαρμογής των διατάξεων για την προστασία των προσωπικών δεδομένων στην ΕΕ**, προκαλώντας ανασφάλεια δικαίου εξαιτίας της ύπαρξης αποκλίσεων, κατά την εκτέλεση και εφαρμογή της, μεταξύ των κρατών-μελών. Οι εν λόγω διαφορές στο επίπεδο προστασίας των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα, όχι μόνο δεν κατάφεραν να προστατεύσουν ενιαία την ιδιωτικότητα των Ευρωπαίων πολιτών, αλλά θεωρήθηκαν και ως εμπόδιο στην ψηφιακή επανάσταση και ως στρέβλωση του ανταγωνισμού. Περαιτέρω, οι διάσπαρτες διατάξεις και οι διαφορετικές ερμηνείες και πρακτικές καθιέρωσαν μια διαδεδομένη αντίληψη στους πολίτες ότι υπάρχουν σημαντικοί κίνδυνοι για την προστασία των προσωπικών τους δεδομένων.

Στα αποτελέσματα της έρευνας του Ευρωβαρόμετρου σχετικά με την προστασία των προσωπικών δεδομένων[5], αποτυπώνεται εύληπτα ότι υπάρχει ανάγκη οριζόντιας διαχείρισης του ζητήματος και μεγάλο περιθώριο βελτίωσης της εμπιστοσύνης μεταξύ των υποκειμένων και των επεξεργαστών δεδομένων. Ειδικότερα, σύμφωνα με την έρευνα, τόσο στην Ελλάδα όσο και στην ΕΕ-28 συνολικά, 9 στους 10 πολίτες δηλώνουν ότι είναι σημαντικό να έχουν τα ίδια δικαιώματα και την ίδια προστασία των προσωπικών τους στοιχείων ανεξάρτητα από τη χώρα στην οποία είναι εγκατεστημένος ο οργανισμός (επιχείρηση ή δημόσιος φορέας) που προβαίνει στην επεξεργασία τους. Ωστόσο, στην Ελλάδα είναι αισθητά χαμηλότερος ο βαθμός εμπιστοσύνης των πολιτών προς τους οργανισμούς που διαχειρίζονται προσωπικά τους δεδομένα από ότι στην ΕΕ **(Δ4)**. Τέλος, οι Έλληνες πολίτες παρουσιάζουν σημαντική διαφορά συγκριτικά με το μέσο όρο της ΕΕ ως προς τη στάση της κυβέρνησης σχετικά με τη συγκέντρωση προσωπικών δεδομένων, νιώθοντας ότι συνεχώς τους ζητείται να δώσουν όλο και περισσότερα προσωπικά στοιχεία **(Δ5)**. Το γεγονός αυτό αποτυπώνει, σε ένα βαθμό, το «σκεπτικισμό» και την επιφυλακτικότητα που επικρατεί στην Ελλάδα σχετικά με τα προσωπικά δεδομένα, καθώς συχνά η συγκέντρωση προσωπικών στοιχείων από τους φορείς ταυτίζεται με παραβίαση της ιδιωτικότητας (π.χ. τοποθέτηση καμερών ασφαλείας στους δρόμους, δήλωση ΑΜΚΑ για την αγορά εισιτηρίων αθλητικών

[5] Η σχετική έκθεση είναι διαθέσιμη **εδώ**. Σημειώνεται ότι το χρονικό διάστημα διεξαγωγής των συνεντεύξεων ήταν από 28/02 έως 09/03/2015. Το δείγμα για την ΕΕ28 ανήλθε σε 27.980 άτομα και για την Ελλάδα σε 1.004 άτομα.

γεγονότων κ.λπ.) και όχι με ενέργειες που είναι απαραίτητες για την ασφάλεια ή/και τη καθαυτή λειτουργία του εκάστοτε οργανισμού. Επίσης, αποτυπώνει το έλλειμμα εμπιστοσύνης ότι τα προσωπικά στοιχεία που θα συγκεντρωθούν θα αξιοποιηθούν με σεβασμό στο δικαίωμα προστασίας τους.

Δ4. Βαθμός εμπιστοσύνης πολιτών προς επιλεγμένους δημόσιους φορείς και κλάδους επιχειρήσεων σχετικά με την προστασία προσωπικών στοιχείων στην ΕΕ-28.
Πηγή: Ευρωβαρόμετρο, Προστασία προσωπικών δεδομένων, Έρευνα 431, Στοιχεία 2015



Δ5. Αξιολόγηση βαθμού εμπλοκής κυβέρνησης στα προσωπικά στοιχεία.
Πηγή: Ευρωβαρόμετρο, Προστασία προσωπικών δεδομένων, Έρευνα 431, Στοιχεία 2015

Η Οδηγία 95/46/ΕΚ απέτυχε να δημιουργήσει ένα συνεκτικό πλαίσιο προστασίας των προσωπικών δεδομένων, με αρνητικές συνέπειες στον ανταγωνισμό, στην ασφάλεια δικαίου, αλλά και στο αίσθημα ασφάλειας του μέσου πολίτη της ΕΕ.

Καθίσταται συνεπώς απολύτως κατανοητό γιατί ήταν πράγματι αναγκαίο ένα σύγχρονο, ισχυρό και πιο συνεκτικό πλαίσιο προστασίας των προσωπικών δεδομένων στην ΕΕ, καθώς και μια αυστηρότερη προσέγγιση στην εφαρμογή της νομοθεσίας. Στόχος ήταν αφενός να δημιουργηθεί η αναγκαία εμπιστοσύνη που θα επιτρέψει στην ψηφιακή οικονομία να αναπτυχθεί στο σύνολο της εσωτερικής αγοράς και αφετέρου τα φυσικά πρόσωπα να νιώσουν ότι, πρέπει, και έχουν τον έλεγχο των δικών τους δεδομένων προσωπικού χαρακτήρα.

Αυτός που δεν γίνεται κατανοητός είναι ο φορμαλιστικός, γραφειοκρατικός, πολύπλοκος ορισμένες φορές, αλλά και αρκετά κοστοβόρος τρόπος που προβλέπεται για να το πετύχει. Ενδεικτικά, πρόκειται για ένα εκτεταμένο Κανονισμό, 5 φορές μεγαλύτερο από την Οδηγία, με 99 άρθρα, εκ των οποίων τα 28 αφήνουν περιθώριο παρέκκλισης για τα κράτη-μέλη, για τον οποίο προηγήθηκαν έντονες και πολυετείς διαπραγματεύσεις μεταξύ των διαφορετικών ομάδων συμφερόντων[6].

Τάσσης Σπύρος, Δικηγόρος
Πρόεδρος της Ελληνικής Ένωσης για την Προστασία των Προσωπικών Δεδομένων και της Ιδιωτικότητας
https://www.linkedin.com/in/spiros-tassis-4b535820/

«GDPR: Εταιρική αυτορρύθμιση και λογοδοσία»

«…Ο Κανονισμός επιβάλλει την ύπαρξη των κατάλληλων διαδικασιών σε κάθε οργανισμό για την προστασία των δεδομένων και την διασφάλιση των δικαιωμάτων των φυσικών προσώπων καθώς και την απόδειξη της συμμόρφωσης της εταιρείας. Το σύστημα αυτό λέγεται λογοδοσία και θα πρέπει να διέπει κάθε διαδικασία επεξεργασίας προσωπικών δεδομένων, αφού πλέον παύουν οι υποχρεώσεις αδειοδότησης και γνωστοποίησης στην ΑΠΔΠΧ…».

Δείτε ολόκληρο το άρθρο **εδώ**.

Ο νέος Κανονισμός «έρχεται» με την επιδίωξη να ανταπεξέλθει στις προκλήσεις που προαναφέρθηκαν, εισαγάγοντας δύο ουσιώδεις διαφοροποιήσεις. **Πρώτον**, εισάγει την αρχή της λογοδοσίας, καθώς μεταφέρει το βάρος για την απόδειξη της συμμόρφωσης από τον ρυθμιστή / ελεγκτή στον ρυθμιζόμενο / ελεγχόμενο. Πλέον, οι επονομαζόμενοι «Υπεύθυνοι Επεξεργασίας» είναι εκείνοι που πρέπει να είναι σε θέση να αποδείξουν ότι έχουν λάβει όλα τα απαραίτητα μέτρα για την προστασία των προσωπικών δεδομένων, με την εποπτική Αρχή να αναλαμβάνει ρόλο και δράση σε δεύτερο χρόνο, ενώ στο παρελθόν ήταν εκείνη που είχε την πρωτοβουλία για την εποπτεία και τον έλεγχο συμμόρφωσης. **Δεύτερον**, ο Κανονισμός ανανεώνει τα δικαιώματα των υποκειμένων. Δηλαδή, πλέον, οι ιδιοκτήτες των προσωπικών δεδομένων έχουν ενισχυμένα δικαιώματα, γεγονός στο οποίο οι επιχειρήσεις-υπεύθυνοι επεξεργασίας οφείλουν να προσαρμοστούν και συνεπώς να μεταβάλλουν ανάλογα τη λειτουργία και τις αποφάσεις τους.

Ο Κανονισμός, εν μέρει γραφειοκρατικός και πολύπλοκος, επιφέρει δύο ουσιώδεις διαφοροποιήσεις: μεταφέρει το βάρος απόδειξης συμμόρφωσης στις επιχειρήσεις και ενισχύει τα δικαιώματα των υποκειμένων.

[6] Αναφερόμαστε σε αντιδράσεις κυρίως από την πλευρά των ΗΠΑ, με τις επιχειρήσεις που χειρίζονται προσωπικά δεδομένα πολιτών της ΕΕ να είναι επίσης υπόχρεες, όπου η φιλοσοφία του κανονιστικού πλαισίου είναι διαφορετική: λιγότερο ανθρωποκεντρική και περισσότερη κλαδική.

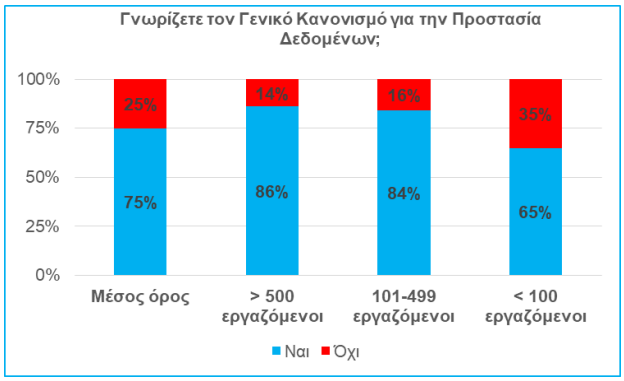
Που βρισκόμαστε σήμερα; Υπάρχει χρόνος για συμμόρφωση και ποιος θα με ελέγξει;

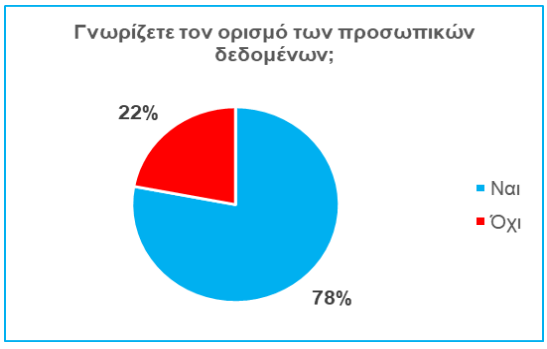
Που βρισκόμαστε όμως σήμερα και πόσο κοντά είναι οι ελληνικές επιχειρήσεις στην κατ' αρχήν εκπλήρωση των προβλέψεων του Κανονισμού;

Τα συμπεράσματα πρόσφατης έρευνας της ICAP[7], δεν είναι ιδιαίτερα αισιόδοξα **(Δ6)**. Ειδικότερα:

- **1 στις 4 επιχειρήσεις** δηλώνει ότι **δεν γνωρίζει τον νέο Κανονισμό**. Το ποσοστό αυτό αυξάνεται σε 35% για τις επιχειρήσεις με λιγότερο από 100 εργαζομένους.
- Μερίδιο **22%** δηλώνει ότι, ακόμα, **δεν γνωρίζει τον ορισμό των προσωπικών δεδομένων**. Ωστόσο, μεταξύ των επιχειρήσεων που δηλώνουν ότι γνωρίζουν τον ορισμό, ενδέχεται να περιλαμβάνονται αρκετές που νομίζουν ότι κατέχουν σχετική γνώση, ενώ στην πραγματικότητα δεν έχουν.
- Σχεδόν 1 στις 4 επιχειρήσεις δηλώνει ότι δεν συμμορφώνεται στον Κανονισμό. Σε συνδυασμό με ποσοστό 57,7% των επιχειρήσεων που δηλώνει ότι συμμορφώνεται μερικώς, διαπιστώνεται ότι απαιτείται άμεση δράση και εντατικοποίηση ενεργειών από την πλειονότητα των επιχειρήσεων.

Δ6. Έρευνα για το επίπεδο συμμόρφωσης των επιχειρήσεων με τον Κανονισμό στην Ελλάδα.
Πηγή: ICAP Management Consultants, Φεβρουάριος 2018





Ενδιαφέροντα συμπεράσματα προκύπτουν επίσης, στην - περιορισμένης έκτασης - έρευνα που εκπονήσαμε[8] **(Δ7)**:

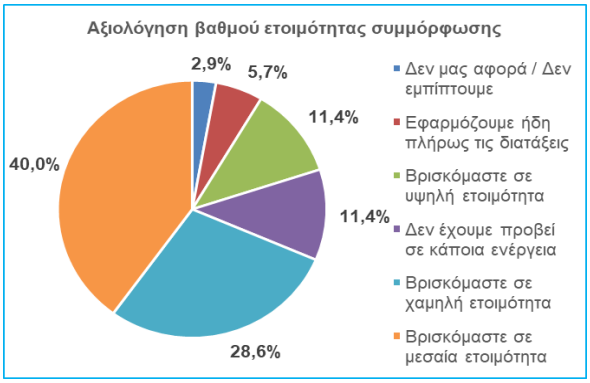
- 8 στις 10 επιχειρήσεις αξιολογούν ως μέτριο ή χαμηλό το βαθμό ετοιμότητας ως προς τη συμμόρφωση με τον Κανονισμό, ή δεν έχουν προβεί ακόμα σε κάποια ενέργεια.

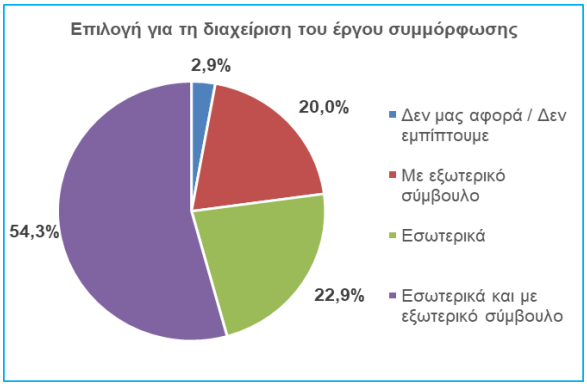
[7] Τα αποτελέσματα της έρευνας, η οποία πραγματοποιήθηκε το Δεκέμβριο 2017, είναι διαθέσιμα **εδώ**. Σημειώνεται ότι το δείγμα ανήλθε σε 210 επιχειρήσεις.

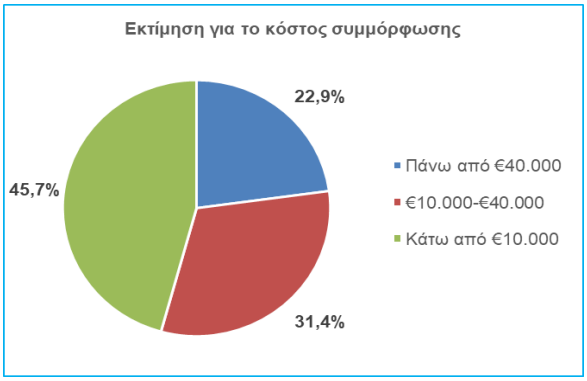
[8] Η έρευνα πραγματοποιήθηκε την περίοδο από 13 έως 23 Φεβρουαρίου 2018, αποκλειστικά σε επιχειρήσεις μέλη του ΣΕΒ και το δείγμα ανέρχεται σε 35 επιχειρήσεις.

- Το 54,3% των επιχειρήσεων δηλώνει ότι διαχειρίζεται το έργο συμμόρφωσης τόσο με ίδιες δυνάμεις, όσο και με τη χρήση εξωτερικού συμβούλου.
- Το κόστος συμμόρφωσης εκτιμάται μικρότερο από €40 χιλ. για το 77,1% του δείγματος. Σημειώνεται ότι όλες οι επιχειρήσεις που δήλωσαν κόστος μεγαλύτερο από €40 χιλ. παρουσιάζουν Κύκλο Εργασιών πάνω από €100 εκ. (συνεπώς, διαφαίνεται μια συσχέτιση μεταξύ μεγέθους επιχείρησης και κόστους συμμόρφωσης).
- 2 στις 3 επιχειρήσεις αντιμετωπίζουν τον Κανονισμό ως ευκαιρία για ανασχεδιασμό των πολιτικών και διαδικασιών τους.

Δ7. Συμμόρφωση επιχειρήσεων στον Κανονισμό και άλλα στοιχεία. Πηγή: Έρευνα ΣΕΒ, Φεβ. 2018



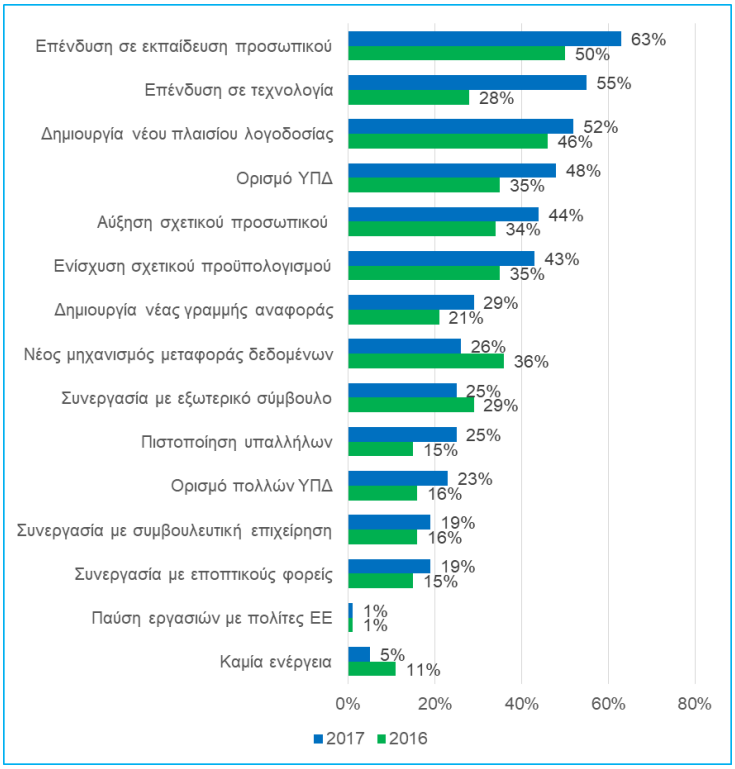




Όσον αφορά στις ενέργειες στις οποίες προβαίνουν οι επιχειρήσεις προκειμένου να πετύχουν τη συμμόρφωση στον Κανονισμό, στη διεθνή έρευνα των International Association of Privacy Professionals (IAPP) και EY, η οποία πραγματοποιήθηκε το 2017, προκύπτει ότι **(Δ8)**:

- Το 63% των επιχειρήσεων επενδύει πλέον σε δράσεις εκπαίδευσης του προσωπικού και το 55% σε τεχνολογικά εργαλεία. Τα αντίστοιχα ποσοστά το 2016 ήταν σημαντικά χαμηλότερα (50% και 28% αντίστοιχα).
- Σημαντικά ποσοστά καταλαμβάνουν και οι δράσεις σχετικές με τη λογοδοσία και τον ορισμό του ΥΠΔ (52% και 48% αντίστοιχα).
- Το ποσοστό των επιχειρήσεων που δεν προβαίνει σε καμία ενέργεια σχετικά με τον Κανονισμό έχει μειωθεί από 11% σε 5%.

Δ8. Ενέργειες στις οποίες προβαίνουν οι επιχειρήσεις για τη συμμόρφωσή τους στον Κανονισμό.
Σημείωση: Δυνατότητα πολλαπλών επιλογών.
Πηγή: IAPP-EY, "Annual Privacy Governance Report", 2017



Ο βαθμός ετοιμότητας των ελληνικών επιχειρήσεων στο νέο Γενικό Κανονισμό για την Προστασία Δεδομένων χαρακτηρίζεται ως μέτριος. Ειδικά οι μικρότερες επιχειρήσεις έχουν πολύ δρόμο να διανύσουν ακόμα.

Τα παραπάνω στοιχεία αναδεικνύουν ότι στην Ελληνική πραγματικότητα υπάρχει αρκετός δρόμος ακόμα για τις επιχειρήσεις, προκειμένου να καταφέρουν να συμμορφωθούν στις διατάξεις του Κανονισμού. Υπό αυτή την έννοια, ο ρόλος της αρμόδιας εποπτικής Αρχής στην Ελλάδα, εν προκειμένω της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), είναι ιδιαίτερα σημαντικός. Πέρα από τις πρωτοβουλίες που έχει ήδη αναλάβει για την ενημέρωση όλων των εμπλεκομένων (υπευθύνων επεξεργασίας και υποκειμένων), αναμένεται, ειδικά στο αρχικό διάστημα μετά την έναρξη εφαρμογής του Κανονισμού, να έχει ενισχυμένο ρόλο λειτουργώντας ως «σύμμαχος» των επιχειρήσεων στη συμμόρφωση.

Ειδικότερα, εκτιμάται ότι μετά και την ψήφιση του εφαρμοστικού Νόμου του Κανονισμού, η ΑΠΔΠΧ θα προχωρήσει σε αρκετές διευκρινίσεις που θα διευκολύνουν την κατανόηση των απαιτήσεων συμμόρφωσης, ενώ σημαντικές θα είναι και οι πρώτες αποφάσεις και γνωμοδοτήσεις που θα εκδώσει[9].

Σημειώνεται ότι η ΑΠΔΠΧ είναι συνταγματικά κατοχυρωμένη ανεξάρτητη Αρχή, η οποία ιδρύθηκε με το Νόμο 2472/1997 που ενσωμάτωνε την Ευρωπαϊκή Οδηγία 95/46/ΕΚ. Στον πίνακα **(Δ9)** αποτυπώνεται συνοπτικά το έργο της Αρχής, η οποία παρά την ελλιπή στελέχωσή της[10], λαμβάνει και καλείται να διαχειριστεί σχεδόν δύο

9 Δείτε **εδώ** το Σχέδιο Νόμου που κατατέθηκε για διαβούλευση έως την 5η Μαρτίου 2018.
10 Στην ετήσια έκθεση του 2016 αναφέρεται ότι υφίστανται 25 οργανικές θέσεις στην ΑΠΔΠΧ, 14 δικηγόρων-ελεγκτών και 11 πληροφορικών-ελεγκτών.

καταγγελίες την ημέρα και περισσότερα από τρία ερωτήματα, ενώ εκδίδει μία απόφαση σχεδόν κάθε δεύτερη ημέρα του έτους.

Δ9. Το έργο της ΑΠΔΠΧ την περίοδο 2008-2016.
Πηγή: Ετήσια έκθεση ΑΠΔΠΧ, 2016

	Προσφυγές / Καταγγελίες	Ερωτήματα	Αποφάσεις	Γνωμοδοτήσεις
2008	670	1.118	69	0
2009	702	1.106	91	4
2010	674	1.261	84	4
2011	812	1.432	168	7
2012	675	1.330	194	5
2013	562	1.421	158	6
2014	659	1.615	202	5
2015	506	1.299	138	7
2016	714	1.465	132	8
Μέσος όρος	**664**	**1.339**	**137**	**5**

10 +1 προτεινόμενα βήματα για την ορθή εφαρμογή του Κανονισμού από τις επιχειρήσεις

Στην ενότητα αυτή παρουσιάζονται οι ενέργειες στις οποίες πρέπει να προβούν οι επιχειρήσεις, προκειμένου να συμμορφωθούν στις απαιτήσεις του Κανονισμού, δηλαδή να είναι σε θέση να αποδείξουν ότι έχουν λάβει όλα τα απαραίτητα μέτρα για την προστασία των προσωπικών δεδομένων που διαχειρίζονται[11].

Είναι σημαντικό να διευκρινιστεί ότι η λίστα των ενεργειών δεν είναι εξαντλητική, ούτε μοναδική (δεν υφίσταται δηλαδή μία λύση για όλους). Όμως, κάθε επιχείρηση, με βάση τις δικές τις ανάγκες, τα χαρακτηριστικά (φύση και όγκος δεδομένων), το μέγεθος, το αντικείμενο των εργασιών και τη στρατηγική της, μπορεί να προσαρμοστεί σε αυτόν τον «οδηγό» και να πετύχει το σκοπό της[12].

Σημειώνεται ότι για τον ΣΕΒ, **τρεις είναι οι βασικές προϋποθέσεις** με οριζόντια ισχύ, **προτού μία επιχείρηση εκκινήσει την προσπάθειά της να ακολουθήσει τα βήματα για την ορθή εφαρμογή του Κανονισμού**, δίχως τις οποίες δεν μπορεί να επιτευχθεί η συμμόρφωση. Πρώτα από όλα, απαιτείται η ευαισθητοποίηση και δέσμευση της ανώτατης διοίκησης, να κατανοήσει δηλαδή την αναγκαιότητα συμμόρφωσης και έμπρακτα να αποφασίσει να δράσει προς αυτήν την κατεύθυνση. Δεύτερον, απαιτείται εξασφάλιση του σχετικού προϋπολογισμού, ο οποίος είναι απαραίτητος για την υλοποίηση του πλάνου συμμόρφωσης. Τρίτον, είναι σημαντικό να ενημερωθεί το σύνολο του προσωπικού για το νέο νομικό πλαίσιο και τις επερχόμενες αλλαγές, διαφορετικά θα προκύψουν προβλήματα στην υλοποίηση.

Ειδικότερα, τα προτεινόμενα βήματα για την ορθή εφαρμογή του Κανονισμού από τις επιχειρήσεις έχουν ως εξής:

Βήμα 1: Σύσταση Ομάδας Εργασίας
Σύσταση Ομάδα Εργασίας, η οποία θα απαρτίζεται από εκπροσώπους Διευθύνσεων που εμπλέκονται περισσότερο με την προστασία των προσωπικών δεδομένων. Ενδεικτικά, αναφέρονται οι Διευθύνσεις Πληροφορικής, Νομικής και Ανθρώπινου Δυναμικού. Στις επιχειρήσεις που τα προσωπικά δεδομένα αποτελούν βασικό αντικείμενο της δραστηριότητας (π.χ. εταιρείες τηλεπικοινωνιών, ασφαλιστικές, τράπεζες), τότε είναι προφανές ότι πρέπει να συμμετέχουν και εκπρόσωποι των επιχειρησιακών Διευθύνσεων. Σε κάθε περίπτωση, η Ομάδα Εργασίας πρέπει να έχει μικρό και ευέλικτο μέγεθος, αλλά και δυνατότητα λήψης αποφάσεων.

[11] Σημειώνεται ότι η λίστα ενεργειών είναι ενδεικτική και αποτελεί ένα «οδηγό κατευθύνσεων» προς τις επιχειρήσεις. Ωστόσο, σε καμία περίπτωση η υιοθέτηση αυτών των βημάτων δεν αποτελεί τεκμήριο πλήρους συμμόρφωσης με τον Κανονισμό. Επιπλέον, μέχρι την ψήφιση του εφαρμοστικού Νόμου, αλλά και την εφαρμογή του Κανονισμού στην πράξη, είναι πιθανό να προκύψουν αλλαγές στα «βήματα συμμόρφωσης» ή νέες συνθήκες στις οποίες θα πρέπει να προσαρμοστούν οι επιχειρήσεις και οι οποίες δεν είναι γνωστές αυτή τη στιγμή.

[12] Σημειώνεται ότι σε αντίστοιχες ενέργειες μπορούν (και πρέπει) να προβούν και οι φορείς του δημοσίου τομέα.

Βήμα 2: Ορισμός Υπεύθυνου Προστασίας Δεδομένων (ΥΠΔ)[13]

Υποχρεωτικό βήμα για όσες επιχειρήσεις προβαίνουν σε μεγάλης κλίμακας επεξεργασία προσωπικών δεδομένων, προαιρετικό για τις υπόλοιπες. Ο ΥΠΔ συμβουλεύει την επιχείρηση για τις υποχρεώσεις που απορρέουν από τον Κανονισμό και παρακολουθεί τις ενέργειες συμμόρφωσης με αυτόν. Συμμετέχει ενεργά σε όλα τα ζητήματα που σχετίζονται με τον Κανονισμό και αποτελεί το πρόσωπο επικοινωνίας τόσο με τα υποκείμενα των δεδομένων όσο και με την εποπτική Αρχή. Ο ΥΠΔ πρέπει να είναι άτομο κατάλληλα καταρτισμένο και προσεκτικά επιλεγμένο ώστε να είναι σε θέση να διεκπεραιώσει τις υποχρεώσεις του.

Βήμα 3: Χαρτογράφηση της ροής των δεδομένων

Η χαρτογράφηση της πορείας των δεδομένων προσωπικού χαρακτήρα που τηρούνται και επεξεργάζονται εντός επιχείρησης (δηλαδή των δεδομένων προσωπικού, πελατών, προμηθευτών και τρίτων προσώπων) αποτελεί μια διαδικασία μέσω της οποίας απαντώνται τα εξής ερωτήματα: τί είδους δεδομένα, για ποιο σκοπό, πόσο συχνά, πώς αποκτώνται, πού υπάρχουν, ποιος έχει πρόσβαση και τα επεξεργάζεται, για πόσο χρόνο διακρατούνται. Προτείνεται η χρήση ερωτηματολογίων και η πραγματοποίηση «συνεντεύξεων» ανά Διεύθυνση προκειμένου να γίνει πλήρης καταγραφή.

Βήμα 4: Εντοπισμός και ανάλυση κινδύνων και ελλείψεων

Αξιοποιώντας την πλήρη γνώση της ροής των προσωπικών δεδομένων (βήμα 3), η επιχείρηση οφείλει να καταγράψει τους πιθανούς κινδύνους και τις ελλείψεις που - ενδεχομένως - εντοπίστηκαν. Ενδεικτικά παραδείγματα σχετικών «κενών» είναι: πολύ μεγάλη περίοδος διατήρησης των δεδομένων άνευ λόγου, διατήρηση των ίδιων δεδομένων σε περισσότερα του ενός σημεία και ανεμπόδιστη πρόσβαση σε δεδομένα από όλα τα στελέχη ενώ δεν χρειάζεται.

Βήμα 5: Εκπόνηση Εκτίμησης Αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑ)[14]

Υποχρεωτικό βήμα για όσες επιχειρήσεις προβαίνουν σε επεξεργασία που ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, προαιρετικό για τις υπόλοιπες. Η εκπόνηση της ΕΑ εξ ορισμού προηγείται της επεξεργασίας των δεδομένων και περιλαμβάνει ανάλυση για τις πιθανότητες επέλευσης κινδύνων και τις συνέπειες στα προσωπικά δεδομένα. Καταλήγει σε κατηγοριοποίηση των δραστηριοτήτων επεξεργασίας σε υψηλού, μεσαίου και χαμηλού κινδύνου και σε επανεξέταση των απαιτούμενων διαδικασιών σε κάθε περίπτωση.

Βήμα 6: Αναθεώρηση πολιτικών και διαδικασιών

Με βάση τα συμπεράσματα των βημάτων 4 και 5, η επιχείρηση προβαίνει σε αναθεώρηση των πολιτικών και των διαδικασιών τήρησης και επεξεργασίας δεδομένων προσωπικού χαρακτήρα[15]. Παραδείγματα αποτελούν: οριστική διαγραφή και καταστροφή δεδομένων με το πέρας Χ ετών, διαμόρφωση κοινού γλωσσάριου ώστε να υπάρχει η σωστή κατανόηση από όλο το προσωπικό, θέσπιση πολιτικής «καθαρού γραφείου», απαγόρευση εξόδου από την επιχείρηση USB sticks και laptops, ανάπτυξη πολιτικής διαβαθμισμένης πρόσβασης, ανάπτυξη πολιτικής για τις διαδρομές των φυσικών αρχείων εντός της επιχείρησης, θέσπιση ορισμένου χρόνου διατήρησης CVs κ.λπ.

---

13 Δείτε επιπλέον στοιχεία στην ενότητα **«Συχνές Ερωτήσεις και Απαντήσεις για τις επιχειρήσεις»** της παρούσας έκθεσης.

14 Δείτε επιπλέον στοιχεία στην ενότητα **«Συχνές Ερωτήσεις και Απαντήσεις για τις επιχειρήσεις»** της παρούσας έκθεσης.

15 Οι πολιτικές και διαδικασίες της επιχείρησης πρέπει, όπου αυτό είναι δυνατόν, να λαμβάνουν υπόψη την αρχή της προστασίας των δεδομένων ήδη από το σχεδιασμό (privacy by default). Δηλαδή, όποτε αυτό είναι δυνατόν, ο Υπεύθυνος Επεξεργασίας να εφαρμόζει κατά τη στιγμή του καθορισμού των μέσων επεξεργασίας αλλά και της ίδιας της επεξεργασίας, κατάλληλα τεχνικά και οργανωτικά μέτρα, σχεδιασμένα για την εφαρμογή των αρχών προστασίας των δεδομένων.

Βήμα 7: Αξιοποίηση των εργαλείων πληροφορικής

Κάθε επιχείρηση ανάλογα με τη φύση των εργασιών της, τα μεγέθη και τις δυνατότητές της, οφείλει να αξιοποιήσει κάποια από τα εργαλεία πληροφορικής που ενισχύουν την ασφάλεια των συστημάτων. Ενδεικτικά παραδείγματα αποτελούν: εργαλεία που με αυτοματοποιημένο τρόπο χαρτογραφούν τα δεδομένα (βήμα 3), εργαλεία που αξιολογούν την αποτελεσματικότητα των πολιτικών και διαδικασιών που έχουν αναπτυχθεί και εργαλεία που βοηθούν στην αποτροπή ή τον εντοπισμό των αποπειρών παραβίασης δεδομένων. Επιπλέον, η κρυπτογράφηση και η ψευδωνυμοποίηση αποτελούν δύο εκ των απλούστερων τεχνικών μέτρων προστασίας.

Βήμα 8: Ανάπτυξη διαδικασιών γνωστοποίησης εποπτικής Αρχής και ανακοίνωσης υποκειμένου

Υποχρεωτικές διαδικασίες για κάθε επιχείρηση. Η πρώτη αφορά στη διαδικασία γνωστοποίησης της παραβίασης δεδομένων προσωπικού χαρακτήρα στην εποπτική Αρχή, εντός μόλις 72 ωρών από τη στιγμή που η επιχείρηση αποκτά γνώση του γεγονότος[16]. Το σύντομο χρονικό διάστημα που προβλέπεται είναι προφανές ότι αυξάνει το βαθμό δυσκολίας. Η δεύτερη αφορά στη διαδικασία άμεσης ανακοίνωσης της παραβίασης δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων, όταν υπάρχει ενδεχόμενο να τεθούν σε υψηλό κίνδυνο τα δικαιώματα και οι ελευθερίες του[17]. Ο επικοινωνιακός χειρισμός σε αυτήν την περίπτωση είναι κρίσιμης σημασίας και μπορεί να κάνει τη διαφορά όσον αφορά στη φήμη της επιχείρησης.

Βήμα 9: Δοκιμαστικοί έλεγχοι συστημάτων και διαδικασιών

Πρόκειται για το τελευταίο χρονικά στάδιο. Αναφέρεται σε δοκιμαστικούς ελέγχους επί των συστημάτων και διαδικασιών που έχει αναπτύξει η επιχείρηση στα προηγούμενα βήματα, προκειμένου να εξασφαλιστεί ότι μετά την 25η Μαΐου 2018 οι ενέργειες συμμόρφωσης θα δουλέψουν αποτελεσματικά στην πράξη. Ενδεχομένως, οδηγήσει σε ανάγκη υλοποίησης διορθωτικών παρεμβάσεων.

Βήμα 10: Διαρκής παρακολούθηση και επικαιροποίηση των διαδικασιών και των συστημάτων

Η συμμόρφωση στον Κανονισμό είναι μια δυναμική «άσκηση» και στο πλαίσιο αυτό οι επιχειρήσεις οφείλουν συνεχώς να επικαιροποιούν τις διαδικασίες τους (ή έστω να εξετάζουν την αναγκαιότητα επικαιροποίησής τους) και να αναβαθμίζουν τα συστήματά τους. Επιβάλλεται συνεχής επαγρύπνηση και διαρκής παρακολούθηση, καθώς οι κίνδυνοι παραβίασης των δεδομένων είναι πιθανοί ανά πάσα στιγμή. Με άλλα λόγια, όπως στο βήμα 9 συστήνονται δοκιμαστικοί έλεγχοι των συστημάτων και διαδικασιών πριν την έναρξη εφαρμογής του Κανονισμού, όμοια προτείνονται αντίστοιχες δοκιμές και μετά την έναρξη εφαρμογής του.

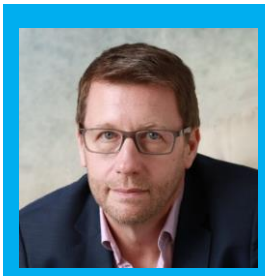
Βήμα 11: Εκπαίδευση προσωπικού

Η επιχείρηση οργανώνει εκπαιδευτικές δράσεις, προς το σύνολο του προσωπικού, προκειμένου να εξασφαλίσει ότι όλοι γνωρίζουν τις πολιτικές και τις διαδικασίες που έχουν αναπτυχθεί για την προστασία των προσωπικών δεδομένων, γιατί είναι σημαντικές για την επιχείρηση, αλλά και τί πρέπει να κάνουν σε περίπτωση που αντιληφθούν απειλή παραβίασης. Οι εν λόγω δράσεις προτείνεται να επαναλαμβάνονται, με βάση τις ανάγκες και τα χαρακτηριστικά κάθε επιχείρησης (π.χ. δραστηριότητα υψηλού κινδύνου, μεγάλη / συχνή αλλαγή προσωπικού, σημαντικές αλλαγές επί των πολιτικών και διαδικασιών κ.λπ.).

---

[16] Κατά το άρθρο 33 του Κανονισμού, η γνωστοποίηση προς την Αρχή πρέπει να περιλαμβάνει, κατ' ελάχιστο: α) τη φύση της παραβίασης, συμπεριλαμβανομένων, όπου είναι δυνατό, των κατηγοριών και του κατά προσέγγιση αριθμού των επηρεαζόμενων υποκειμένων, καθώς και αντίστοιχα των επηρεαζόμενων αρχείων, β) το όνομα και τα στοιχεία επικοινωνίας του ΥΠΔ για περισσότερες πληροφορίες, γ) τις ενδεχόμενες συνέπειες της παραβίασης και δ) τα ληφθέντα, ή έστω τα προτεινόμενα προς λήψη, μέτρα από τον Υπεύθυνο Επεξεργασίας για την αντιμετώπιση της παραβίασης και της άμβλυνσης των ενδεχόμενων δυσμενών συνεπειών.

[17] Στο άρθρο 34 του Κανονισμού προβλέπεται ότι στην ανακοίνωση προς το υποκείμενο πρέπει να περιγράφεται με σαφήνεια η φύση της παραβίασης και να περιέχονται τουλάχιστον οι πληροφορίες και τα μέτρα που προαναφέρθηκαν στην περίπτωση της γνωστοποίησης προς την Αρχή. Ωστόσο, υφίστανται εξαιρέσεις για την υποχρέωση ανακοίνωσης, σε συγκεκριμένες περιπτώσεις (π.χ. ο Υπεύθυνος Επεξεργασίας εφάρμοσε κατάλληλα τεχνικά και οργανωτικά μέτρα προστασίας των δεδομένων, έλαβε μέτρα που διασφαλίζουν ότι δεν είναι πλέον πιθανό να προκύψει υψηλός κίνδυνος κ.ά.).



Neil Patrick
Director of SAP Centre of Excellence for GRC & Security covering EMEA
https://www.linkedin.com/in/neil-patrick/

"GDPR compliance: more than just a checklist"

«…The GDPR requires demonstrating that use of personal data is specific to the purpose it was acquired for, that it can be 'lawfully' processed, and data controllers and processors actively record how they will process and protect personal data. What evidence would you need?...».

Δείτε ολόκληρο το άρθρο **εδώ**.

Προκλήσεις και παγίδες για τις επιχειρήσεις κατά την εφαρμογή του Κανονισμού

Ο Κανονισμός θέτει νέες κανονιστικές απαιτήσεις προς τις επιχειρήσεις, οι οποίες έρχονται να προστεθούν στις ήδη υφιστάμενες για την προστασία των προσωπικών δεδομένων (αλλά και φυσικά σε όλες τις υπόλοιπες απαιτήσεις που προκύπτουν από το λοιπό θεσμικό πλαίσιο κάθε κλάδου). Έχει πολύ μεγαλύτερο πεδίο εφαρμογής από ό,τι η Οδηγία, αφορά πολύ περισσότερες επιχειρήσεις, «καταργεί» τα σύνορα δραστηριοποίησης, προβλέπει πολύ μεγαλύτερες ποινές, στρέφει όλο το βάρος της απόδειξης συμμόρφωσης στις επιχειρήσεις δίνοντας «δευτερεύοντα» ρόλο στις εποπτικές Αρχές και στην κατεύθυνση αυτή θέτει πολύ συγκεκριμένες απαιτήσεις που εξασφαλίζουν τη συμμόρφωση.

Αναλυτικότερα, με τον Κανονισμό προκύπτουν **κόστη που επιβαρύνουν την καθημερινή λειτουργία** των επιχειρήσεων και ο τρόπος που θα επιδιώξουν να τα διαχειριστούν αποτελεί σημαντική πρόκληση:

- Συγκρότηση και μισθοδοσία της Ομάδας Εργασίας ή /και του ΥΠΔ που θα αναλάβει τις ενέργειες συμμόρφωσης στον Κανονισμό,
- Εκπόνηση της εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων, είτε αξιοποιηθούν ίδιες δυνάμεις της επιχείρησης, είτε υπάρξει συνεργασία με εξωτερικό σύμβουλο,
- Ανασχεδιασμό των συστημάτων σχετικά με τον τρόπο εξασφάλισης της συγκατάθεσης των υποκειμένων,
- Ανασχεδιασμό όλων των πληροφοριακών συστημάτων για την ενίσχυση της προστασίας από επιθέσεις παραβίασης ασφάλειας,
- Διαμόρφωση των νέων πολιτικών και διαδικασιών για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και
- Διάδοση και κατανόηση εντός της επιχείρησης των νέων υποχρεώσεων, πολιτικών και διαδικασιών που προκύπτουν.

Τα κόστη αυτά είναι αναμενόμενο ότι προκαλούν - το λιγότερο - προβληματισμό όσον αφορά στον τρόπο που μπορεί να κερδηθεί το στοίχημα της συμμόρφωσης με τον Κανονισμό, ειδικά τη στιγμή που η ελληνική επιχειρηματικότητα, και κυρίως οι μικρομεσαίες επιχειρήσεις, αντιμετωπίζει δύσκολες οικονομικές συνθήκες, παρά τα - διστακτικά - σημάδια ανάκαμψης.

Τα κόστη που προκύπτουν από τις απαιτήσεις του Κανονισμού εύλογα προκαλούν προβληματισμό για τον τρόπο που μπορεί να κερδηθεί το στοίχημα της συμμόρφωσης.

Επιπροσθέτως, αποτελεί πρόκληση για τις επιχειρήσεις η **επιλογή των κατάλληλων στελεχών ή / και συνεργατών** που θα τους βοηθήσουν στην ικανοποίηση των απαιτήσεων του Κανονισμού, καθώς ήδη «ανοίγεται» μια νέα αγορά παροχής συμβουλευτικών και εκπαιδευτικών υπηρεσιών, αλλά και στελεχών ΥΠΔ, η οποία προφανώς δεν μπορεί να είναι όλη υψηλού επιπέδου. Απαιτείται επομένως, ιδιαίτερη προσοχή στον τρόπο και τα κριτήρια επιλογής, αλλά και προσεκτική αξιολόγηση των προσφερόμενων υπηρεσιών κάθε συνεργάτη. Η αξιοπιστία και η αποτελεσματικότητα πρέπει να αποτελούν τη βάση επιλογής, με τις επιχειρήσεις να εστιάζουν σε επιλογές που ταιριάζουν στα δικά τους χαρακτηριστικά, ανάγκες, πληροφοριακά συστήματα κ.λπ. Κατά τη γνώμη μας, οι επιχειρήσεις μπορούν να θέσουν σε δεύτερο επίπεδο το καθαρά οικονομικό κόστος, καθώς αυτό που είναι σημαντικό είναι ότι μέσα από τη διαδικασία συμμόρφωσης στον Κανονισμό φιλοδοξείται να προκύψουν οφέλη που θα αναμορφώσουν συνολικά το επιχειρηματικό μοντέλο και την επιχειρηματική κουλτούρα.

Giles Watkins
International Association of Privacy Professionals (IAPP) UK Country Leader
https://www.linkedin.com/in/giles-watkins-37ab3b2/

"GDPR – Friend not Foe"

«…Despite the challenges, leading organisations see the change in legislation as an opportunity to create competitive advantage. They believe that good data protection practices create trust, leading to further data sharing, deeper insight and an opportunity to deliver their customers more relevant products and services, more efficiently, which can only be good for business…».

Δείτε ολόκληρο το άρθρο **εδώ**.

Σημαντική «παγίδα» για τις επιχειρήσεις αποτελεί επίσης, το γεγονός λανθασμένα **να έχουν την πεποίθηση ότι δεν εμπίπτουν στον Κανονισμό** και ως εκ τούτου να θεωρούν ότι δεν χρειάζεται να προβούν σε καμία δράση συμμόρφωσης. Η αντίληψη αυτή είναι ιδιαίτερα επικίνδυνη καθώς μπορεί να φέρει τις επιχειρήσεις αντιμέτωπες με υψηλά πρόστιμα και ισχυρό πλήγμα στη φήμη τους και για το λόγο αυτό καλούμε για την ιδιαίτερη προσοχή τους. Ενδεικτικά, οι επιχειρήσεις μπορεί να μην έχουν αντιληφθεί ότι κατέχουν και επεξεργάζονται προσωπικά δεδομένα, ή να μην κατανοούν πώς αυτά ορίζονται, ή να νομίζουν ότι μόνο οι μεγάλες επιχειρήσεις πρέπει να λάβουν μέτρα κ.ο.κ.

Τέλος, η πεποίθηση ορισμένων επιχειρήσεων ότι **δεν απειλούνται από περιστατικά παραβίασης των συστημάτων τους** πρόκειται περί πλάνης. Πρέπει να γίνει απόλυτα κατανοητό ότι κανένας οργανισμός (επιχείρηση ή δημόσιος φορέας) δεν έχει συστήματα 100% ασφαλή έναντι περιστατικών παραβίασης δεδομένων, για αυτό άλλωστε χρειάζεται επαγρύπνηση και διαρκής παρακολούθηση.

Άγγελος Κούρος
Legal Counsel, ΑΛΦΑ ΒΗΤΑ ΒΑΣΙΛΟΠΟΥΛΟΣ ΑΕ
https://www.linkedin.com/in/kouros-aggelos-68491a59/

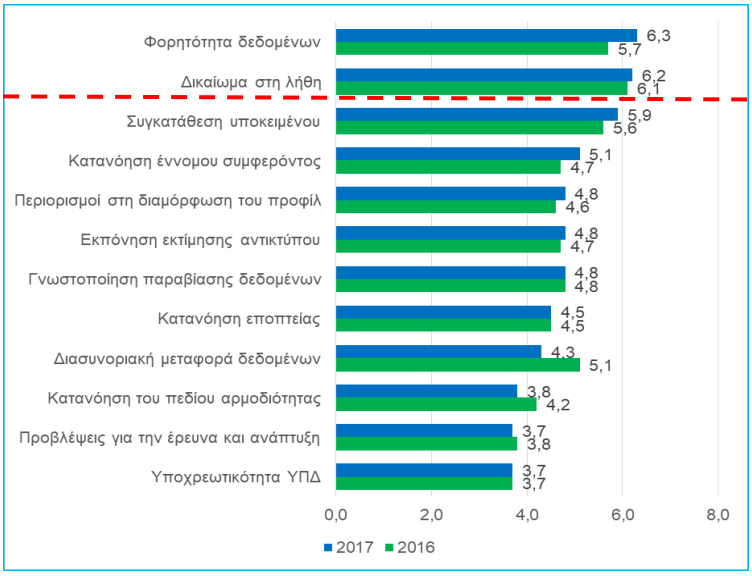
«Νέες προοπτικές εσωτερικής οργάνωσης και προστιθέμενες αξίες για την επιχείρηση»

«…Κάθε επιχείρηση, που διαχειρίζεται προσωπικά δεδομένα πελατών και υπαλλήλων, θα πρέπει να έχει ως γνώμονα ότι η εμπιστοσύνη τους για την ορθή διαχείριση των δεδομένων τους είναι ιδιαίτερα σημαντική. Για το λόγο αυτό πρέπει να υιοθετήσει διαδικασίες ελέγχου και προστασίας των δεδομένων, τις οποίες θα πρέπει να μεταλαμπαδεύσει τόσο στους υπαλλήλους όσο και σε τρίτους συνεργάτες, που άμεσα ή έμμεσα έχουν πρόσβαση στα δεδομένα αυτά…».

Δείτε ολόκληρο το άρθρο **εδώ**.

Πλέον των όσων ήδη προαναφέρθηκαν, οι επιχειρήσεις έρχονται αντιμέτωπες και με ορισμένες υψηλής «τεχνικότητας» διατάξεις, που χρήζουν ιδιαίτερης προσοχής. Σύμφωνα με τη διεθνή έρευνα των IAPP και EY, αυτές αποτελούν **α) η φορητότητα των δεδομένων** (με αξιοσημείωτη διαφορά από το προηγούμενο έτος, γεγονός που σημαίνει ότι όσο πλησιάζει η έναρξη εφαρμογής του Κανονισμού, γίνεται αντιληπτή η δυσκολία σχετικά με την ικανοποίηση της συγκεκριμένης πρόβλεψης) και **β) το δικαίωμα στη λήθη (Δ10)**.

Δ10. Σημεία συμμόρφωσης στον Κανονισμό που δυσκολεύουν τις επιχειρήσεις, 2016-2017.
Σημείωση: Κλίμακα 0 έως 10 (0: Κανένας βαθμός δυσκολίας, 10: Πάρα πολύ υψηλός βαθμός δυσκολίας), Δυνατότητα πολλαπλών επιλογών.
Πηγή: IAPP-EY, "Annual Privacy Governance Report", 2017



Ειδικότερα, για τα ως άνω σημεία, σημειώνουμε τα εξής:

Φορητότητα δεδομένων

Στο άρθρο 20 του Κανονισμού προβλέπεται ότι το υποκείμενο έχει το δικαίωμα **να λαμβάνει** τα δεδομένα προσωπικού χαρακτήρα που το αφορούν από τον Υπεύθυνο Επεξεργασία στον οποίο τα έχει παράσχει, σε δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα μορφότυπο. Περαιτέρω, έχει το δικαίωμα **να διαβιβάζει** τα εν λόγω δεδομένα σε άλλον Υπεύθυνο Επεξεργασίας, όταν η επεξεργασία: α) βασίζεται σε συγκατάθεση και β) διενεργείται με αυτοματοποιημένα μέσα. Σε αυτές τις περιπτώσεις, έχει το δικαίωμα να ζητά την **απευθείας** διαβίβαση των δεδομένων του από έναν Υπεύθυνο Επεξεργασίας σε άλλον, σε περίπτωση που αυτό είναι τεχνικά εφικτό (π.χ. αλλαγή παρόχου κινητής/σταθερής τηλεφωνίας).

Δικαίωμα διαγραφής (εναλλακτικά, Δικαίωμα στη λήθη)

Στο άρθρο 17 του Κανονισμού προβλέπεται ότι ο Υπεύθυνος Επεξεργασίας υποχρεούται να διαγράψει τα δεδομένα προσωπικού χαρακτήρα, **χωρίς αδικαιολόγητη καθυστέρηση**, σε περίπτωση που το υποκείμενο των δεδομένων υποβάλλει σχετικό αίτημα, με την προϋπόθεση ότι ισχύει έστω μία από τις ακόλουθες συνθήκες[18]: α) τα δεδομένα να μην είναι πλέον απαραίτητα για τους σκοπούς για τους οποίους συλλέχθηκαν ή υποβλήθηκαν σε επεξεργασία, β) το υποκείμενο να ανακαλέσει τη συγκατάθεσή του, γ) το υποκείμενο να αντιτίθεται στην επεξεργασία και δ) τα δεδομένα υποβλήθηκαν σε επεξεργασία παράνομα. Ιδιαίτερη προσοχή χρειάζεται από τις επιχειρήσεις στην περίπτωση που έχουν δημοσιοποιήσει τα εν λόγω δεδομένα. Ο Κανονισμός προβλέπει ότι οφείλουν να τα διαγράψουν, λαμβάνοντας υπόψη τη διαθέσιμη τεχνολογία και αναλαμβάνοντας το κόστος εφαρμογής της ενέργειας. Είναι προφανές ότι οι προκλήσεις για τους Υπευθύνους Επεξεργασίας είναι πολύ υψηλές, καθώς θα πρέπει να εξασφαλίζουν την πλήρη διαγραφή των δεδομένων ενδεικτικά από τις μηχανές αναζήτησης, αρχεία εφημερίδων κ.λπ.

Δρ. Αλέξανδρος Βαρβέρης
Αν. Διευθυντής Εργαστηρίου Νομικής Πληροφορικής του ΕΚΠΑ
https://www.linkedin.com/in/alexandros-varveris-357bb036/

«Υπεύθυνος Προστασίας Δεδομένων: ο άνθρωπος-κλειδί για τη συμμόρφωση και την προστασία. Ένα υβρίδιο γνώσης και εμπειρίας νομικής και πληροφορικής»

«..Πρέπει συνεπώς να διαθέτει βαθιά γνώση τόσο της νομοθεσίας, των προσωπικών δεδομένων όσο και των πρακτικών για την προστασία τους, ιδίως στη σημερινή ψηφιακή εποχή. Γι' αυτό και άλλωστε αποτελεί ένα υβρίδιο γνώσης και εμπειρίας νομικής και πληροφορικής. Έχει κρίσιμο ρόλο στη διαμόρφωση νοοτροπίας-κουλτούρας ως προς την προστασία των δεδομένων σε έναν οργανισμό και συμβάλλει στην εφαρμογή του Κανονισμού...».

Δείτε ολόκληρο το άρθρο **εδώ**.

Πρόταση ΣΕΒ: «έξυπνη» συμμόρφωση

Στον ΣΕΒ πιστεύουμε ότι ο Κανονισμός παρουσιάζει σημαντικές ευκαιρίες, που αν αξιοποιηθούν, μπορούν να συμβάλουν στην ουσιαστική βελτίωση του τρόπου λειτουργίας του επιχειρηματικού μοντέλου, με αποτέλεσμα όχι απλά την τυπική συμμόρφωση, αλλά την επίτευξη θετικού προσήμου μέσα από την εν λόγω διαδικασία. Αυτό μπορεί να επιτευχθεί εάν οι επιχειρήσεις, αντί για ένα ακόμα «στείρο» νομικό κείμενο υποχρεώσεων, εκλάβουν τον Κανονισμό ως υποχρεωτική «άσκηση» χάρη στην οποία θα αλλάξουν την επιχειρηματική κουλτούρα προς όφελός τους, δίχως να επιβαρυνθούν με σημαντικό χρηματικό και διοικητικό κόστος. Αυτό στον ΣΕΒ θέλουμε να αποκαλούμε **«έξυπνη συμμόρφωση», βασισμένη σε τρεις αρχές που αναδεικνύουν εύληπτα και τα οφέλη που προκύπτουν από τον Κανονισμό**.

Η πρώτη αρχή αφορά στο «νοικοκύρεμα» των (προσωπικών) δεδομένων. Μέχρι σήμερα οι επιχειρήσεις, κατά συνήθη πρακτική, επιδίδονται σε ένα «κυνήγι όγκου» δεδομένων, γεγονός που συνεπάγεται σημαντικό κόστος συγκέντρωσης, καταχώρισης, ψηφιοποίησης, φύλαξης, επεξεργασίας, ανάλυσης κ.λπ. Ο Κανονισμός «αναγκάζει» τις επιχειρήσεις να επανεξετάσουν τα δεδομένα τους, αλλά και τις δομές, τις εσωτερικές λειτουργίες και τις διαδικασίες τους σε σχέση με αυτά. Δηλαδή τις καλεί να επανεξετάσουν ποια δεδομένα διατηρούν, πώς

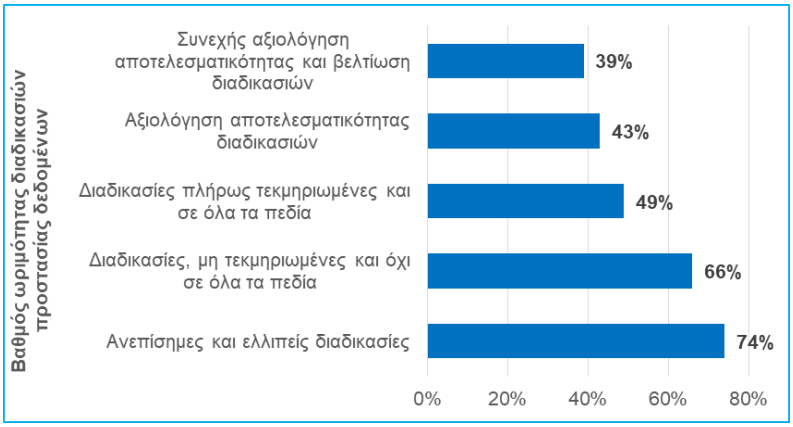
[18] Ο Κανονισμός προβλέπει και ορισμένες άλλες περιπτώσεις οι οποίες για λόγους συντόμευσης δεν αναφέρονται. Δείτε αναλυτικά το άρθρο 17 **εδώ**.

τα συλλέγουν, για ποιο σκοπό, για πόση διάρκεια, ποιος έχει πρόσβαση σε αυτά και πώς φυλάσσονται[19].

Μέσα από αυτή τη διαδικασία είναι βέβαιο ότι θα προκύψουν χρήσιμα συμπεράσματα σχετικά με το αν τα δεδομένα αξιοποιούνται επαρκώς από την επιχείρηση, ή μήπως πολύτιμες πληροφορίες μένουν ανεκμετάλλευτες χάνοντας επιχειρηματικές ευκαιρίες (π.χ. πληροφορίες σχετικές με το προφίλ των πελατών). Παράλληλα, θα αναδειχθούν οι κίνδυνοι που αφορούν τις συνθήκες ασφάλειας των δεδομένων (π.χ. το σύνολο του προσωπικού έχει πρόσβαση σε ευαίσθητα δεδομένα δίχως αυτό να είναι απαραίτητο για την εργασία του, ή παλαιά προσωπικά δεδομένα φυλάσσονται ακόμα, δίχως πραγματικό πλέον λόγο και μάλιστα σε χώρους με ανεμπόδιστη πρόσβαση). Ως εκ τούτου, θα αναδειχθούν τα αναγκαία μέτρα προφύλαξης που πρέπει να υιοθετηθούν και τα οποία προστατεύουν τις επιχειρήσεις από νομικούς και οικονομικούς κινδύνους, όπως η επιβολή προστίμων από την εποπτική Αρχή. Τέλος, είναι προφανές ότι όσο μικρότερος είναι ο όγκος των δεδομένων που διατηρούνται, τόσο μειώνεται το κόστος όπως αυτό εκφράζεται σε εργατοώρες, υλικοτεχνικό εξοπλισμό και έπιπλα, χώρο γραφείων, σε χρόνο και χώρο για backup κ.λπ. Επομένως, τα οφέλη της ελαχιστοποίησης των προσωπικών δεδομένων είναι πολλαπλά.

Στον πίνακα **(Δ11)** αποτυπώνεται η θετική συσχέτιση που υπάρχει μεταξύ: α) του βαθμού ωριμότητας των επιχειρήσεων όσον αφορά στις διαδικασίες τους για την προστασία των δεδομένων (υπό μία έννοια, του βαθμού συμμόρφωσης δηλαδή με τον Κανονισμό) και β) της οικονομικής ζημίας από την παραβίαση της ασφάλειας δεδομένων. Ειδικότερα, σύμφωνα με διεθνή μελέτη της Cisco, το 74% των επιχειρήσεων που είχαν υιοθετήσει ανεπίσημες και ελλιπείς διαδικασίες προστασίας δεδομένων αντιμετώπισαν απώλειες μεγαλύτερες από $500 χιλ. εξαιτίας παραβιάσεων των δεδομένων τους κατά το προηγούμενο έτος. Για τις επιχειρήσεις που είχαν βελτιστοποιήσει αυτές τις διαδικασίες, το ποσοστό ήταν 39%.

Δ11. Ποσοστό επιχειρήσεων, με απώλειες από παραβίαση ασφάλειας δεδομένων μεγαλύτερες από $500 χιλ. το προηγούμενο έτος, ανά βαθμό ωριμότητας ως προς την προστασία των δεδομένων.
Πηγή: CISCO, "Privacy Maturity Benchmark Study", 2018



Ο Κανονισμός καλεί τις επιχειρήσεις να επανεξετάσουν ποια δεδομένα διατηρούν, πώς τα συλλέγουν, για ποιο σκοπό, για πόση διάρκεια, ποιος έχει πρόσβαση σε αυτά και πώς φυλάσσονται.

[19] Σημειώνεται ότι αυτή η διαδικασία χαρτογράφησης δεν είναι απαραίτητο να αφορά μόνο τα προσωπικά δεδομένα, αλλά ανάλογα με τα χαρακτηριστικά της επιχείρησης, να επεκταθεί και σε άλλες (ή και όλες τις) κατηγορίες δεδομένων, με πολλαπλασιαστικά οφέλη.

Η δεύτερη αρχή αφορά στη μετατροπή της υποχρέωσης συμμόρφωσης σε ανταγωνιστικό πλεονέκτημα. Όταν ακόμη οι αναζητήσεις μας στο διαδίκτυο αποκαλύπτουν τις προσωπικές ή επαγγελματικές προτιμήσεις μας και το κινητό μας «εκπέμπει» τα προσωπικά μας δεδομένα, είναι εύλογο ότι ο τρόπος προστασίας τους γρήγορα θα αποτελέσει κριτήριο για τις επιλογές που θα κάνουν οι πελάτες, οι προμηθευτές και οι ίδιοι οι εργαζόμενοι. Είναι δε χαρακτηριστικό ότι έχει ήδη ξεκινήσει διεθνώς μια πολύ ζωντανή και ενδιαφέρουσα συζήτηση γύρω από την προστασία των προσωπικών δεδομένων και την ανάγκη αυτορρύθμισης των επιχειρήσεων, ώστε να αποφευχθούν δυστοπικά σενάρια μιας επερχόμενης «ψηφιακής δικτατορίας».

Γιώργος Γιαννόπουλος
Επίκουρος Καθηγητής στη Νομική Σχολή του Εθνικού και Καποδιστριακού Πανεπιστημίου Αθηνών, Διευθυντής του Εργαστηρίου Νομικής Πληροφορικής
https://www.linkedin.com/in/georgios-yannopoulos-34865511/

«Η συμμόρφωση με τον ΓΚΠΔ απαιτεί πρωτίστως αλλαγή νοοτροπίας»

«…Αυτό το νέο ήθος προστασίας των προσωπικών δεδομένων αναμένεται να οδηγήσει στην υπευθυνότητα και εντέλει στην εμπιστοσύνη του κοινού:
«…εμπιστεύομαι τα δεδομένα μου στον εργοδότη, το σχολείο, το κοινωνικό δίκτυο, τον μηχανισμό έρευνας, τον οργανισμό, την εταιρία διότι αποδεδειγμένα διαθέτουν «κουλτούρα» προστασίας δεδομένων…».

Δείτε ολόκληρο το άρθρο **εδώ**.

Υπό αυτήν την έννοια, η προστασία των προσωπικών δεδομένων σχετίζεται άμεσα με την εμπιστοσύνη πελατών, προμηθευτών και εργαζομένων και κατ' επέκταση με τη φήμη της επιχείρησης. Αυτό που είναι σημαντικό για κάθε επιχείρηση είναι να μπορεί να αποδείξει (σε όλες τις προαναφερθείσες κατηγορίες ενδιαφερομένων) ότι προστατεύει τα προσωπικά τους δεδομένα από τις τέσσερις βασικές περιπτώσεις παραβίασής τους: α) την εισβολή, δηλαδή το να εισέρχεται μια επιχείρηση στον προσωπικό χώρο κάποιου υποκειμένου, να επικοινωνεί μαζί του και να του υποδεικνύει τί να κάνει, β) τη συγκέντρωση δεδομένων σε βαθμό που να εισπράττει το υποκείμενο ότι παρακολουθείται σε μεγαλύτερη έκταση από αυτή που θα έπρεπε, γ) την επεξεργασία δεδομένων με τρόπο που να εισπράττει το υποκείμενο ότι μια επιχείρηση κατέχει πολλά προσωπικά του δεδομένα και προβαίνει σε επεξεργασία αυτών και δ) την αποκάλυψη των δεδομένων του από την επιχείρηση με τρόπο που το υποκείμενο δεν είναι σύμφωνο.

Συνεπώς, η επιχείρηση που θα κάνει το σεβασμό της προσωπικότητας και της ιδιωτικότητας στοιχείο της κουλτούρας της και θα το εντάξει στην επιχειρηματική της στρατηγική θα αποκτήσει σαφές ανταγωνιστικό πλεονέκτημα έναντι των υπολοίπων.

Η υποχρέωση συμμόρφωσης στον Κανονισμό μπορεί να μετατραπεί σε ανταγωνιστικό πλεονέκτημα για την επιχείρηση που θα κάνει στοιχείο της κουλτούρας της το σεβασμό της προσωπικότητας και της ιδιωτικότητας.

Τέλος, η τρίτη αρχή αφορά στην επένδυση σε λύσεις που προσφέρει η τεχνολογία και, μέσω αυτής της διαδικασίας, στην είσοδο στην εποχή της ψηφιακής οικονομίας. Είναι γεγονός ότι η ενσωμάτωση των ψηφιακών τεχνολογιών στην επιχειρηματική λειτουργία αποτελεί πλέον μονόδρομο για την επιβίωση και ανάπτυξη των επιχειρήσεων. Υπό αυτήν την έννοια, ο Κανονισμός μπορεί να αποτελέσει πύλη εισόδου στη ψηφιακή κοσμογονία (ενδεικτικά, business analytics, big data), καθώς οι τεχνολογίες πληροφορικής και επικοινωνιών παρέχουν όχι μόνο εργαλεία συμμόρφωσης χαμηλού κόστους (π.χ. cloud computing, firewalls, κρυπτογράφηση, ψευδωνυμοποίηση κ.ά.), αλλά και λύσεις που τελικά θα αναβαθμίσουν το ίδιο το επιχειρηματικό μοντέλο.

Αντιγόνη Παπανικολάου
Διευθύντρια Νομικών & Εταιρικών Υποθέσεων Microsoft Ελλάδας, Κύπρου & Μάλτας
https://www.linkedin.com/in/antigoni-papanikolaou-9925462/

«Οι ευκαιρίες του Γενικού Κανονισμού και ο ρόλος της τεχνολογίας»

«…Επιπλέον, το θέμα της από κοινού ευθύνης θα οδηγήσει τους οργανισμούς να επιλέγουν πιο προσεχτικά προμηθευτές και συνεργάτες που θα διαχειρίζονται για λογαριασμό τους τα δεδομένα τους ενώ η εμπιστοσύνη θα παίξει σημαντικό ρόλο στην επιλογή αυτήν…»

Δείτε ολόκληρο το άρθρο **εδώ**.

Με άλλα λόγια, όπως αναφέρθηκε στην αρχή της παρούσας έκθεσης, οι τεχνολογικές εξελίξεις ήταν αυτές που σε μεγάλο βαθμό προκάλεσαν την ανάγκη μετάβασης από την Οδηγία στον Κανονισμό για την προστασία των προσωπικών δεδομένων, αλλά ταυτόχρονα είναι εκείνες που προσφέρουν και τις λύσεις συμμόρφωσης σε αυτόν. Μέσω αυτής της διαδικασίας, οι επιχειρήσεις καλούνται να εξοικειωθούν, προβληματιστούν, ερευνήσουν, ανασχεδιάσουν τις δομές και τις λειτουργίες τους με βάση τα εργαλεία που προσφέρει η τεχνολογία συνολικά, όχι μόνο για τις ανάγκες συμμόρφωσης στο νέο κανονιστικό πλαίσιο. Εξάλλου, η ενσωμάτωση των ψηφιακών τεχνολογιών στην επιχειρηματική στρατηγική αποτελεί πλέον προαπαιτούμενο για την επιβίωση και ανάπτυξη των επιχειρήσεων[20].

Η αξιοποίηση των διαθέσιμων εργαλείων συμμόρφωσης που προσφέρει η τεχνολογία για τη συμμόρφωση στον Κανονισμό έχει τη δυναμική να εξελιχθεί σε πύλη εισόδου στην ψηφιακή κοσμογονία για τις επιχειρήσεις.

Ειδικά για τις μικρές και μεσαίες επιχειρήσεις, παραθέτουμε ορισμένες χρήσιμες συμβουλές στην προσπάθειά τους να προσαρμοστούν στον Κανονισμό **(Δ12)**, ώστε να διευκολυνθούν στην «αγωνία» τους να συμμορφωθούν και να αποφύγουν τα υψηλά πρόστιμα που σε περίπτωση επιβολής θα ήταν για αυτές παράγοντας επιβίωσης.

[20] Δείτε **εδώ** το Special Report για το στρατηγικό σχέδιο του ΣΕΒ για μια ψηφιακά ανεπτυγμένη Ελλάδα.

Δ12. Χρήσιμες συμβουλές για τις μικρές και μεσαίες επιχειρήσεις για την συμμόρφωση στον Κανονισμό

1. Προσαρμογή των βημάτων συμμόρφωσης
Κάθε επιχείρηση οφείλει να προσαρμόσει τα βήματα και τις έξυπνες αρχές συμμόρφωσης, με βάση τις δικές της ανάγκες, τα χαρακτηριστικά (φύση και όγκος δεδομένων), το μέγεθος, το αντικείμενο των εργασιών και τη στρατηγική της.

2. Προσοχή, μικρό μέγεθος επιχείρησης, μεγάλη επεξεργασία
Ιδιαίτερη προσοχή απαιτείται, στην περίπτωση που οι επιχειρήσεις είναι μικρού μεγέθους (βάσει κύκλου εργασιών ή /και προσωπικού), ωστόσο προβαίνουν σε εκτενή επεξεργασία προσωπικών δεδομένων, κυρίως λόγω της δραστηριότητάς τους (π.χ. μια εταιρεία παροχής υπηρεσιών φύλαξης, ή μια εταιρεία παροχής υπηρεσιών “cloud”). Με άλλα λόγια, η έμφαση που πρέπει να δοθεί από τον κάθε επιχειρηματία που εξετάζει κατά πόσο επηρεάζεται από τις απαιτήσεις του Κανονισμού είναι στο βαθμό επεξεργασίας των προσωπικών δεδομένων που κατέχει.

3. Αποφυγή υπερβολών σε πολιτικές και διαδικασίες
Σκοπός είναι η επίτευξη της συμμόρφωσης δίχως να επιβαρυνθούν περισσότερο με περιττά βάρη και πολύπλοκες ή ανεφάρμοστες διαδικασίες οι μικρομεσαίες επιχειρήσεις, οι οποίες διαθέτουν περιορισμένους πόρους.
Κάθε επιχείρηση πρέπει να υιοθετήσει εκείνα τα μέτρα προστασίας προσωπικών δεδομένων που τις ταιριάζουν και που σκοπεύει έμπρακτα να εφαρμόσει (όχι δηλαδή απλά για τους τύπους), κάποια εκ των οποίων δε είναι ανέξοδα (π.χ. οριστική διαγραφή δεδομένων που δεν χρησιμοποιούνται κ.λπ.).

Μαρουλιανάκης Νίκος,
Head of Infrastructure & Enterprise Data, Interamerican
https://www.linkedin.com/in/nikolaos-maroulianakis-b4b059127/

«GDPR: δείτε την ευκαιρία για επιχειρησιακή αριστεία»

«…Ο Κανονισμός μπορεί και πρέπει να γίνει αφορμή για αλλαγές που θα αποδώσουν επιχειρησιακή αριστεία. Δηλαδή θα ενδυναμώσουν τη σχέση με τους πελάτες, θα δημιουργήσουν ανταγωνιστικό πλεονέκτημα και τελικά θα βελτιώσουν την επιχειρησιακή καθημερινότητα…».

Δείτε ολόκληρο το άρθρο **εδώ**.

Το γλωσσάρι του Κανονισμού

Δ14. Οι 10 βασικότερες έννοιες του Κανονισμού (με βάση το άρθρο 4 του Κανονισμού)	
Προσωπικά Δεδομένα ή Δεδομένα Προσωπικού Χαρακτήρα	Κάθε πληροφορία που αφορά ταυτοποιημένο, ή ταυτοποιήσιμο, φυσικό πρόσωπο («υποκείμενο των δεδομένων»). Παραδείγματα αποτελούν: όνομα, επώνυμο, αριθμός ταυτότητας, ΑΜΚΑ, ΑΦΜ, τηλέφωνο, ταχυδρομική και ηλεκτρονική διεύθυνση, διεύθυνση πρωτοκόλλου διαδικτύου (IP address), γεωχωρικά δεδομένα (GPS), δηλαδή στοιχεία που μπορούν να ταυτοποιήσουν ένα φυσικό πρόσωπο.
Υποκείμενο των Δεδομένων	Πρόκειται για το φυσικό πρόσωπο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας.
Επεξεργασία δεδομένων	Κάθε πράξη που πραγματοποιείται επί των προσωπικών δεδομένων, όπως συλλογή, καταχώριση, οργάνωση, αποθήκευση, μεταβολή, ανάκτηση, αναζήτηση πληροφοριών, χρήση, διαγραφή, καταστροφή κ.λπ.
Υπεύθυνος Επεξεργασίας Δεδομένων	Το φυσικό, ή νομικό, πρόσωπο, ή δημόσια αρχή / υπηρεσία, που καθορίζει τους σκοπούς και τον τρόπο της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα.
Εκτελών την Επεξεργασία	Το φυσικό, ή νομικό, πρόσωπο, ή δημόσια αρχή / υπηρεσία, που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του Υπευθύνου Επεξεργασίας. Παραδείγματα Εκτελούντων την Επεξεργασία αποτελούν οι επιχειρήσεις ενημέρωσης οφειλετών και παροχής υπηρεσιών “cloud”.
Υπεύθυνος Προστασίας Δεδομένων	Ορίζεται από τον Υπεύθυνο Επεξεργασίας και τον Εκτελούντα την Επεξεργασία και συμμετέχει, δεόντως και εγκαίρως, σε όλα τα ζητήματα τα οποία σχετίζονται με την προστασία δεδομένων προσωπικού χαρακτήρα. Αποτελεί το πρόσωπο επικοινωνίας τόσο με τα υποκείμενα των δεδομένων όσο και με την εποπτική Αρχή.
Εκτίμηση Αντικτύπου σχετικά με την προστασία δεδομένων	Όταν ένα είδος επεξεργασίας δεδομένων, 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 οφείλει να διενεργήσει, πριν από την επεξεργασία, εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία προσωπικών δεδομένων.
Συγκατάθεση Υποκειμένου	Κάθε ένδειξη βούλησης (ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει), με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν.
Παραβίαση Δεδομένων Προσωπικού Χαρακτήρα	Παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας αποκάλυψη ή πρόσβαση δεδομένων προσωπικού χαρακτήρα, τα οποία διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία.
Εποπτική Αρχή Προστασίας Δεδομένων	Πρόκειται για την ανεξάρτητη δημόσια Αρχή, καθ’ ύλην αρμόδια για την εποπτεία εφαρμογής του Κανονισμού. Επικεφαλής ορίζεται η Αρχή του κράτους-μέλους όπου βρίσκεται η «κύρια εγκατάσταση»[21] του Υπευθύνου Επεξεργασίας. Ο Κανονισμός ενθαρρύνει την επικοινωνία και συνεργασία μεταξύ των διάφορων Αρχών («μηχανισμός μιας στάσης»), ώστε να διασφαλίζεται ομοιογένεια στην αντιμετώπιση υποθέσεων διευρωπαϊκού ενδιαφέροντος και ασφάλεια δικαίου.

[21] Ο τόπος όπου λαμβάνονται οι αποφάσεις για τους σκοπούς και τα μέσα της επεξεργασίας των προσωπικών δεδομένων.

Συχνές Ερωτήσεις και Απαντήσεις για τις επιχειρήσεις

Δ13. Συχνές Ερωτήσεις και Απαντήσεις για τις επιχειρήσεις (Υπευθύνους Επεξεργασίας και Εκτελούντες την Επεξεργασία) για τη συμμόρφωση στον Κανονισμό[22]

Πότε τα προσωπικά δεδομένα που κατέχει η επιχείρησή μου δεν εμπίπτουν στο πεδίο εφαρμογής του Κανονισμού;
Προσωπικά δεδομένα που έχουν κρυπτογραφηθεί ή ψευδωνυμοποιηθεί κ.λπ., αλλά μπορούν να χρησιμοποιηθούν για την επαναναγνώριση ενός φυσικού προσώπου παραμένουν προσωπικά δεδομένα που εμπίπτουν στο πεδίο εφαρμογής του Κανονισμού.
Αντίθετα, τα προσωπικά δεδομένα που έχουν καταστεί ανώνυμα με τέτοιο τρόπο ώστε πλέον το φυσικό πρόσωπο να μην αναγνωρίζεται, δεν θεωρούνται πλέον δεδομένα προσωπικού χαρακτήρα.
Σημειώνεται ότι το κρίσιμο στοιχείο είναι η ανωνυμοποίηση να είναι μη αναστρέψιμη. Μόνο τότε τα δεδομένα είναι πραγματικά ανώνυμα και δεν εμπίπτουν στο πεδίο εφαρμογής του Κανονισμού.

Πρέπει η επιχείρησή μου να ορίσει Υπεύθυνο Προστασίας Δεδομένων (ΥΠΔ);
Ο ορισμός ΥΠΔ είναι υποχρεωτικός, όταν οι βασικές δραστηριότητες των Υπευθύνων Επεξεργασίας ή των Εκτελούντων την Επεξεργασία συνιστούν πράξεις επεξεργασίας οι οποίες, λόγω της φύσης, του πεδίου εφαρμογής ή/και των σκοπών τους, απαιτούν τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε **μεγάλη κλίμακα**[23] (άρθρο 37).
Επομένως, η λέξη-κλειδί είναι η επεξεργασία «μεγάλης κλίμακας» και εύλογα προκύπτουν ερωτήματα στις επιχειρήσεις για το πώς αυτή ορίζεται. Το ζήτημα αυτό θα πρέπει να φανεί στην πράξη πώς θα εφαρμοστεί και πώς θα το χειριστεί η εποπτική Αρχή, μετά την ψήφιση του εφαρμοστικού Νόμου. Για παράδειγμα, μπορεί να προβεί σε δημοσίευση συγκεκριμένων κριτηρίων για τον καθορισμό της έννοιας «μεγάλης κλίμακας» (π.χ. βάσει κλάδων, μεγέθους επιχειρήσεων, όγκου δεδομένων κ.λπ.).
Σε κάθε περίπτωση, αυτό που συστήνεται στις επιχειρήσεις που επεξεργάζονται προσωπικά δεδομένα και αμφιταλαντεύονται σχετικά, είναι να προβούν σε ορισμό ΥΠΔ, καθώς θα ωφεληθούν πολλαπλά μέσα από το ρόλο και τη δράση που θα αναλάβει ο ΥΠΔ, όπως έχει περιγραφεί προηγούμενα στην παρούσα έκθεση.

Ποιο είναι το κατάλληλο άτομο να οριστεί ως ΥΠΔ;
Ο Κανονισμός ορίζει ότι ο ΥΠΔ πρέπει να είναι ένα άτομο με υψηλά επαγγελματικά προσόντα και τεχνογνωσία στον τομέα του δικαίου και των πρακτικών περί προστασίας δεδομένων, ώστε να είναι ικανό να εκπληρώσει τα καθήκοντά του. Επομένως, πρέπει να επιλεγεί με αυτά τα κριτήρια, λαμβάνοντας περαιτέρω υπόψη τις ακόλουθες προϋποθέσεις: α) Αποφυγή καταστάσεων σύγκρουσης συμφερόντων: ο ΥΠΔ μπορεί να επιτελεί και άλλα καθήκοντα και υποχρεώσεις, αλλά θα πρέπει να εξασφαλίζεται ότι αυτά δεν συνεπάγονται σύγκρουση συμφερόντων (άρθρο 38 παρ. 6), επομένως προτείνεται να είναι διακριτό πρόσωπο από π.χ. το Νομικό Σύμβουλο ή τον Διευθυντή Πληροφορικής και β) Ανεξαρτησία: ο ΥΠΔ λογοδοτεί απευθείας στο ανώτατο διοικητικό επίπεδο της επιχείρησης (άρθρο 38 παρ. 3). Περαιτέρω, διευκρινίζεται ότι η επιχείρηση μπορεί να προβεί σε εξωτερική ανάθεση για την ιδιότητα του ΥΠΔ (άρθρο 37 παρ. 6). Τέλος, σε περίπτωση ομίλου επιχειρήσεων, ακόμα και με διασυνοριακή δραστηριότητα, μπορεί να οριστεί ένας μόνο ΥΠΔ, ο οποίος μάλιστα μπορεί να είναι εγκατεστημένος σε οποιαδήποτε χώρα, ακόμα και εκτός ΕΕ (άρθρο 37 παρ. 2). Στην περίπτωση αυτή, προτείνεται για τη βέλτιστη επικοινωνία και συνεργασία με την εκάστοτε συναρμόδια τοπική Αρχή, αλλά και για την εξυπηρέτηση των υποκειμένων των δεδομένων, ο ορισμός και τοπικά αρμόδιου ΥΠΔ.

Ο ΥΠΔ φέρει ευθύνη έναντι του υποκειμένου ή / και την Αρχής;
Όχι, την ευθύνη έχει ο Υπεύθυνος και ο Εκτελών την Επεξεργασία. Ο ΥΠΔ ευθύνεται μόνο ως προς την πλημμελή εκτέλεση των υποχρεώσεών του (δηλαδή την ποιότητα των υπηρεσιών του) προς τον Υπεύθυνο Επεξεργασίας που

[22] Οι απαντήσεις διαμορφώθηκαν κατά την εκτίμηση των συγγραφέων της παρούσας έκθεσης. Σε καμία περίπτωση δεν δεσμεύουν τον ΣΕΒ και η υιοθέτησή τους δεν αποτελεί τεκμήριο πλήρους συμμόρφωσης με τον Κανονισμό.

[23] Σημειώνεται ότι το άρθρο 37 προβλέπει επίσης υποχρεωτικότητα ορισμού ΥΠΔ σε μια τρίτη περίπτωση που αφορά αποκλειστικά στο δημόσιο τομέα, με ρητή αναφορά στην περίπτωση όταν η επεξεργασία διενεργείται από δημόσια αρχή ή φορέα (εκτός από τα δικαστήρια που ενεργούν στο πλαίσιο της δικαιοδοτικής τους αρμοδιότητας).

τον έχει προσλάβει. Σημειώνεται ότι ισχύουν για τον ΥΠΔ οι γενικές διατάξεις αστικής και ποινικής ευθύνης, απλά δεν υπάρχει προσωπική δίωξη κατά αυτού.

Ο ΥΠΔ πρέπει να πιστοποιηθεί;
Ο Κανονισμός δεν έχει καμία αναφορά σε πιστοποίηση του ΥΠΔ. Επομένως, ούτε είναι υποχρεωτικό να πιστοποιηθεί ο ΥΠΔ, ούτε υπάρχει σχετική πιστοποίηση. Οποιαδήποτε παρακολούθηση εκπαιδευτικών προγραμμάτων και σεμιναρίων είναι φυσικά θεμιτή.

Πρέπει η επιχείρησή μου να εκπονήσει σε Εκτίμηση Αντικτύπου (ΕΑ) σχετικά με την προστασία δεδομένων και ποια είναι τα οφέλη;
Όταν ένα είδος επεξεργασίας ενδέχεται να επιφέρει **υψηλό κίνδυνο** για τα δικαιώματα των φυσικών προσώπων, τότε ο Υπεύθυνος Επεξεργασίας διενεργεί, **πριν** από την επεξεργασία, εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα (άρθρο 35).
Επομένως, η φράση-κλειδί για την υποχρεωτικότητα εκπόνησης ΕΑ είναι «ενδέχεται να επιφέρει υψηλό κίνδυνο».
Σχετικά, στο άρθρο 57 του Κανονισμού προβλέπεται ότι η εποπτική Αρχή καταρτίζει και διατηρεί κατάλογο σε σχέση με την απαίτηση για διενέργεια ΕΑ. Επομένως, αναμένεται μετά την ψήφιση του εφαρμοστικού Νόμου η ΑΠΔΧΠ να προβεί σε σχετικές ενέργειες που θα συμβάλλουν στην αποσαφήνιση της υποχρεωτικότητας.
Έως τότε, εύλογα προκύπτει το ερώτημα στις επιχειρήσεις σχετικά με το αν πρέπει να εκπονήσουν ΕΑ, καθώς αυτή θα πρέπει να έχει ολοκληρωθεί πριν την επεξεργασία των προσωπικών δεδομένων και επομένως πριν την έναρξη εφαρμογής του Κανονισμού στις 25 Μαΐου 2018. Σε αυτήν την περίπτωση, συστήνεται στις επιχειρήσεις που αμφιταλαντεύονται σχετικά, να προχωρήσουν σε εκπόνηση ΕΑ, καθώς τα οφέλη που προκύπτουν είναι πολλαπλά:
Η εκπόνηση ΕΑ αποτελεί για μια διαδικασία κατά την οποία ο Υπεύθυνος Επεξεργασίας **εντοπίζει, αξιολογεί και μετριάζει τους κινδύνους που προκύπτουν από την επεξεργασία των δεδομένων**. Περιλαμβάνει: α) τη συστηματική περιγραφή των πράξεων και των σκοπών της επεξεργασίας, συμπεριλαμβανομένου του έννομου συμφέροντος που επιδιώκεται, β) την εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας σε συνάρτηση με τους σκοπούς, γ) την εκτίμηση των κινδύνων που προκύπτουν για τα υποκείμενα και δ) τα προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων, περιλαμβανομένων των εγγυήσεων, των μέτρων και μηχανισμών ασφάλειας, ώστε να διασφαλίζεται η προστασία των δεδομένων. Δηλαδή, η ΕΑ αποτελεί ένα ευέλικτο εργαλείο ανάλυσης κινδύνων για τις επιχειρήσεις, βοηθώντας τες 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 και αλλιώς θα έπρεπε να ακολουθούν.

Πόσο συχνά πρέπει η επιχείρηση να προβαίνει σε ΕΑ σχετικά με την προστασία δεδομένων;
Ο Κανονισμός δεν ορίζει ρητά πόσο συχνά πρέπει να εκπονείται μια ΕΑ. Ενδεχομένως, στον εφαρμοστικό Νόμο να υπάρξουν σχετικές προβλέψεις. Σε κάθε περίπτωση, αυτό που είναι σημαντικό να γίνει κατανοητό είναι ότι η ΕΑ αποτελεί μια δυναμική «άσκηση» για κάθε Υπεύθυνο Επεξεργασίας, δεν είναι μια μελέτη που εκπονείται “one-off”.
Ως «οδηγό» για τις επιχειρήσεις, με ιδιαίτερη προσοχή στην εφαρμογή της, μπορεί να χρησιμοποιηθεί η συμβουλή ότι, εφόσον δεν αλλάζει κάτι στις διαδικασίες της επιχείρησης, τότε δεν χρειάζεται η επικαιροποίηση της ΕΑ.

Είναι υποχρεωτικό να πιστοποιηθεί η επιχείρησή μου για την προστασία προσωπικών δεδομένων και ποια είναι η διαδικασία;
Τα άρθρα 42 και 43 του Κανονισμού αναφέρονται στη θέσπιση μηχανισμών πιστοποίησης προστασίας δεδομένων. Δηλαδή, ο Κανονισμός παροτρύνει την υιοθέτηση συστημάτων πιστοποίησης από τους Υπευθύνους Επεξεργασίας και τους Εκτελούντες την Επεξεργασία, δίχως ωστόσο να τη θέτει υποχρεωτική. Σημειώνεται ότι οι φορείς πιστοποίησης που θα προσφέρουν τις υπηρεσίες τους στο εν λόγω πεδίο θα πρέπει πρώτα να διαπιστευθούν ανάλογα με τις απαιτήσεις που θα ορίσει η αρμόδια εποπτική Αρχή (εν προκειμένω η ΑΠΔΧΠ) και ο οργανισμός διαπίστευσης (εν προκειμένω το Εθνικό Σύστημα Διαπίστευσης-ΕΣΥΔ). Επομένως, στην Ελλάδα είναι πρώιμο να γίνεται συζήτηση για πιστοποίηση προστασίας δεδομένων, είναι ζήτημα που θα απασχολήσει τις επιχειρήσεις μετά την έναρξη εφαρμογής του Κανονισμού και τις σχετικές αποφάσεις των ΑΠΔΧΠ και ΕΣΥΔ.

Οι προηγούμενες άδειες της ΑΠΔΧΠ έχουν ισχύ μετά την 25η Μαΐου 2018; Οι άδειες επεξεργασίας προσωπικών δεδομένων που έχει ήδη εκδώσει η Αρχή δεν θα έχουν πλέον κάποια τυπική ισχύ μετά την 25η Μαΐου 2018. Παρόλα αυτά, αναμένεται να αποτελούν ενισχυτικά στοιχεία για την απόδειξη της νομιμότητας προς την εποπτική Αρχή. Τέλος, εκτιμάται ότι στον εφαρμοστικό Νόμο του Κανονισμού θα υπάρχουν σχετικές προβλέψεις (π.χ. μεταβατικές διατάξεις, διευκρινίσεις).
Οι προηγούμενες γνωμοδοτήσεις της ΑΠΔΧΠ έχουν ισχύ μετά την 25η Μαΐου 2018; Ναι, εφόσον το περιεχόμενό τους δεν έρχεται σε αντίθεση με το πνεύμα του Κανονισμού.

Το παρόν συντάχθηκε από τον Τομέα Επιχειρηματικού Περιβάλλοντος και Ρυθμιστικών Πολιτικών του ΣΕΒ, αξιοποιώντας στοιχεία που παράχθηκαν στο πλαίσιο του έργου «Μηχανισμός παρακολούθησης των αλλαγών και υποστήριξης των δράσεων ανάπτυξης και προσαρμοστικότητας της βιομηχανίας», το οποίο συγχρηματοδοτείται από την Ελλάδα και την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο) μέσω του ΕΠ «Ανταγωνιστικότητα, Επιχειρηματικότητα και Καινοτομία».

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο

ΕΠΑνΕΚ 2014-2020
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ
ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ
ΚΑΙΝΟΤΟΜΙΑ

ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

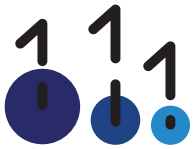
Οικονομικά μεγέθη μελών ΣΕΒ

ΕΝΕΡΓΗΤΙΚΟ
€368 δισ.
67% συνόλου*

ΙΔΙΑ ΚΕΦΑΛΑΙΑ
€60 δισ.
51% συνόλου*

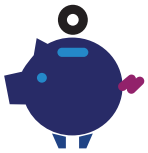
ΠΩΛΗΣΕΙΣ
€62 δισ.
43% συνόλου*

ΠΡΟ ΦΟΡΩΝ ΚΕΡΔΗ
€2,4 δισ. **
30% συνόλου**



ΕΡΓΑΖΟΜΕΝΟΙ
190.000
11% συνόλου ασφαλισμένων στο ΙΚΑ

ΜΙΣΘΟΙ
€4,8 δισ.
20% συνόλου***



ΑΣΦΑΛΙΣΤΙΚΕΣ ΕΙΣΦΟΡΕΣ
€2,1 δισ.
20% συνόλου***

ΦΟΡΟΣ ΕΠΙ ΚΕΡΔΩΝ
€0,8 δισ.
29% συνόλου****

*20.500 δημοσιευμένοι ισολογισμοί χρήσης 2015 που περιλαμβάνονται στη βάση της ICAP
**σύνολο κερδών κερδοφόρων επιχειρήσεων
***% επί του συνόλου τακτικών αποδοχών (χωρίς bonus και υπερωρίες)/ασφαλιστικών εισφορών ασφαλισμένων στο ΙΚΑ
****% επί του συνόλου εσόδων από φόρο εισοδήματος νομικών προσώπων

Όραμα

Οραματιζόμαστε την Ελλάδα ως τη χώρα, που κάθε πολίτης του κόσμου θα θέλει και θα μπορεί να επισκεφθεί, να ζήσει και να επενδύσει.
Οραματιζόμαστε μια ανοιχτή, κοινωνικά υπεύθυνη και οικονομικά φιλελεύθερη χώρα-μέλος της Ευρωπαϊκής Ένωσης, που προτάσσει την ισχυρή ανάπτυξη ως παράγοντα κοινωνικής συνοχής. Θέλουμε μια Ελλάδα δυναμικό κέντρο της ευρωπαϊκής περιφέρειας, με στέρεους θεσμούς, ελκυστικό κοινωνικό και οικονομικό περιβάλλον, που προάγει τις εξαγωγές, την καινοτόμο επιχειρηματικότητα, την παραγωγή και τις ποιοτικές υπηρεσίες, τη βιώσιμη ανάπτυξη, τη γνώση, τη συνοχή, τις ίσες ευκαιρίες και το κράτος δικαίου.

Αποστολή

Ηγεσία & Γνώση

Ο ΣΕΒ διαδραματίζει ηγετικό ρόλο στον μετασχηματισμό της Ελλάδας σε μια παραγωγική, εξωστρεφή και ανταγωνιστική οικονομία, ως ανεξάρτητος και υπεύθυνος εκπρόσωπος της ιδιωτικής οικονομίας.

Κοινωνικός Εταίρος

Ο ΣΕΒ, ως κοινωνικός εταίρος που πιστεύει στη λειτουργία των θεσμών, προωθεί στα αρμόδια όργανα της Πολιτείας και της Ε.Ε. τις απόψεις και θέσεις της επιχειρηματικής κοινότητας.

Ισχυρός Εκπρόσωπος

Ο ΣΕΒ διαμορφώνει θέσεις, αναλύσεις και προτάσεις πολιτικής για την οικονομία, τη βιομηχανία, την καινοτομία, την απασχόληση, την παιδεία και τις εργασιακές δεξιότητες, τον κοινωνικό διάλογο, τη βιώσιμη ανάπτυξη, την εταιρική υπευθυνότητα.

Φορέας Δικτύωσης

Ο ΣΕΒ δικτυώνει τα μέλη του μεταξύ τους & με τα κέντρα αποφάσεων (εγχώρια και διεθνή), με στόχο τη δημιουργία προστιθέμενης αξίας.

ΣΕΒ
Σύγχρονες Επιχειρήσεις, Σύγχρονη Ελλάδα

ΣΕΒ σύνδεσμος επιχειρήσεων και βιομηχανιών

Ξενοφώντος 5, 105 57 Αθήνα
T: 211 5006 000
F: 210 3222 929
E: info@sev.org.gr
www.sev.org.gr

SEV Hellenic Federation of Enterprises

168, Avenue de Cortenbergh
B-1000 Bruxelles
M: +32 (0) 494 46 95 24
E: sevbrussels@proximus.be

ΑΚΟΛΟΥΘΗΣΤΕ ΜΑΣ ΣΤΑ ΜΕΣΑ ΚΟΙΝΩΝΙΚΗΣ ΔΙΚΤΥΩΣΗΣ