

Εκπαίδευση, Δια Βίου Μάθηση, Έρευνα και Τεχνολογική Ανάπτυξη, Καινοτομία και Οικονομία

Τόμ. 1 (2016)

Πρακτικά Πρώτου Πανελληνίου Συνεδρίου



Εκτίμηση των Επιπτώσεων σχετικά με την Προστασία Δεδομένων σε έργα Ηλεκτρονικής Διακυβέρνησης

*Κωνσταντίνος Σιασιάκος, Σοφία Αναστασίου,
Κανέλλος Τούντας*

doi: [10.12681/elrie.817](https://doi.org/10.12681/elrie.817)

Εκτίμηση των Επιπτώσεων σχετικά με την Προστασία Δεδομένων σε έργα Ηλεκτρονικής Διακυβέρνησης

Κωνσταντίνος Σιασιάκος¹, Σοφία Αναστασίου², Κανέλλος Τούντας³

¹k.siassiakos@asep.gr, ²anastasiou@yahoo.com, ³kstoudas@gmail.com.

¹ Ανώτατο Συμβούλιο Επιλογής Προσωπικού (ΑΣΕΠ), Πουλίου 6., ² Σχολή Διοίκησης & Οικονομίας, ΤΕΙ Στερεάς Ελλάδας, 1ο χιλ. ΠΕΟ Θήβας – Ελευσίνας., ³ Εντεταλμένος Διδασκαλίας Εθνικού και Καποδιστριακού Πανεπιστημίου Αθηνών, Σοφοκλέους 1.

Περίληψη

Σύμφωνα με ανάλυση της Strategy Analytics, τα διακινούμενα (από συστήματα Τεχνολογιών Πληροφορικής και Επικοινωνιών - ΤΠΕ) δεδομένα στην αγορά των Η.Π.Α αυξήθηκαν κατά το εντυπωσιακό 300% το 1ο εξάμηνο του 2015 σε σχέση με το 2ο εξάμηνο του 2013. Σε αυτό το πλαίσιο, από την πλευρά της, η Ε.Ε έχοντας σκοπό να αντιμετωπίσει τους κινδύνους από την επεξεργασία προσωπικών δεδομένων, εξέδωσε Γενικό Κανονισμό για την Προστασία των Δεδομένων, σύμφωνα με τον οποίο, κάθε οργανισμός που επεξεργάζεται προσωπικά δεδομένα υποχρεούται να διενεργεί μια «εκτίμηση των επιπτώσεων σχετικά με την προστασία των δεδομένων» (Data Protection Impact Assessment). Στην ελληνική πραγματικότητα, το IOBE, στη δεύτερη έκθεσή του για το 2015, στο πλαίσιο των περιοδικών επισκοπήσεων της ελληνικής οικονομίας αναφέρει ότι όλο και περισσότερες κυβερνήσεις (περιλαμβανομένης και της Ελληνικής) σχεδιάζουν και εφαρμόζουν την υιοθέτηση των ΤΠΕ μέσω συγκεκριμένων στρατηγικών ψηφιακής ανάπτυξης. Η προτεινόμενη εργασία εξετάζει σφαιρικά την σημερινή κατάσταση σχετικά με την εναρμόνιση της ελληνικής πραγματικότητας της υλοποίησης της ηλεκτρονικής διακυβέρνησης με το γενικότερα θέμα της εκτίμησης των επιπτώσεων σχετικά με την προστασία των δεδομένων.

Λέξεις κλειδιά: Προστασία Δεδομένων, Ηλεκτρονική Διακυβέρνηση.

Abstract

According to the analysis of Strategy Analytics, trafficked (by ICT systems - ICT) data to the US market increased by an impressive 300% in the first half of 2015 compared with the second half of 2013. In this context, for its part, the EU having the aim to deal with the risks of the processing of personal data, adopted General Rules for data Protection, according to which, every organization that processes personal data required to carry out an "assessment impact on data protection » (Data Protection Impact Assessment). In the Greek reality, IOBE in the second report for 2015, in the periodic reviews of the Greek economy, indicates that more and more governments (including the Greek one) design and implement the adoption of ICT by specific digital development strategies. The proposed work comprehensively examines the current situation on the harmonization of Greek reality of the implementation of e-government with the general theme of the impact assessment regarding data protection

Keywords: Data Protection, E-Government

1. Εισαγωγή

Η ραγδαία ανάπτυξη που γνώρισε τα τελευταία χρόνια ο τομέας των ηλεκτρονικών υπηρεσιών σε συνδυασμό με την ευρεία χρήση του διαδικτύου και των social media, έχει συμβάλει σημαντικά στην εξέλιξη της οικονομίας και της κοινωνίας, ταυτόχρονα όμως έχει δημιουργήσει νέα προβλήματα που χρήζουν αντιμετώπισης, όπως αυτό της παραβίασης των προσωπικών δεδομένων. Η τεχνολογία έχει εισχωρήσει σε βάθος στις σύγχρονες κοινωνίες, οι οποίες είναι άμεσα εξαρτημένες από αυτή. Η ανάπτυξη συστημάτων ηλεκτρονικής διακυβέρνησης, ηλεκτρονικής υγείας και ηλεκτρονικού εμπορίου, σε συνδυασμό με την τάχιστα εξάπλωση του διαδικτύου και την εμφάνιση των social media, στηρίζουν τις σύγχρονες οικονομίες και πιο συγκεκριμένα τις επιχειρήσεις και τους κυβερνητικούς οργανισμούς που δραστηριοποιούνται σε αυτές. Πλέον, όλες σχεδόν οι υπηρεσίες που παρέχονται στους πολίτες εκτελούνται μέσω πληροφοριακών συστημάτων και ηλεκτρονικών μητρώων, κάτι που προϋποθέτει όμως και την διαχείριση προσωπικών δεδομένων. Ο όγκος της πληροφορίας που κυκλοφορεί εντός του διαδικτύου είναι δύσκολα μετρήσιμος και η κυκλοφορία των δεδομένων αυτών είναι απρόσκοπτη. Σύμφωνα με ανάλυση της Strategy Analytics, τα διακινούμενα (από συστήματα ΤΠΕ) δεδομένα στην αγορά των Η.Π.Α αυξήθηκαν κατά το εντυπωσιακό 300% το 1ο εξάμηνο του 2015 σε σχέση με το 2ο εξάμηνο του 2013. Όλη αυτή όμως η γρήγορη εξέλιξη των πληροφοριακών συστημάτων παροχής ηλεκτρονικών υπηρεσιών και οι τεράστιες πλέον ικανότητες του διαδικτύου, φέρουν μεγάλους κινδύνους για τα άτομα και τους οργανισμούς που αξιοποιούν ηλεκτρονικές υπηρεσίες στη καθημερινή τους ζωή. Η επεξεργασία – διαχείριση προσωπικών δεδομένων στο διαδίκτυο κρύβει πολλούς κινδύνους για την ασφάλεια των ατόμων, καθώς η υποκλοπή, η τροποποίηση ή η διαγραφή τους, μπορεί να προκαλέσει σοβαρές συνέπειες. Επομένως, είναι απαραίτητο ο κάθε οργανισμός που είναι κάτοχος προσωπικών δεδομένων, τα οποία τις περισσότερες φορές παρέχει σε φορείς-καταναλωτές των δεδομένων αυτών, να λαμβάνει μέτρα που να συμμορφώνονται με τους κανόνες ασφαλείας και να διασφαλίζουν την προστασία των ατόμων.

Μια από της πιο αναγνωρισμένες σύγχρονες τεχνολογικές τάσεις είναι το «Διαδίκτυο των Πραγμάτων» (Internet of Things - IoT). Το IoT είναι μία έννοια που σχετίζεται με συσκευές της καθημερινότητας (π.χ wearable συσκευές) που χρησιμοποιούν ενσωματωμένους αισθητήρες για τη συλλογή δεδομένων και τη μετάδοσή τους με στόχο να προσφέρουν περισσότερες ηλεκτρονικές υπηρεσίες προστιθέμενης αξίας. Σύμφωνα με έκθεση της Ericsson Mobilit Report (2016) το IoT θα έχει εκθρονίσει τα κινητά τηλέφωνα από την κατηγορία των περισσότερων συνδεδεμένων συσκευών μέχρι το 2018. Από τα 28 δισεκατομμύρια συσκευών που θα έχουν συνδεθεί έως το 2021, σχεδόν 16 δισεκατομμύρια θα αντιπροσωπεύουν συσκευές IoT.

Στο σημερινό ψηφιακό περιβάλλον, τα συχνά κρούσματα μαζικής παραβίασης προσωπικών δεδομένων σε μεγάλους οργανισμούς δημιουργούν ανασφάλεια σε όλους τους πολίτες. Κάθε άνθρωπος έχει το δικαίωμα να προστατεύει τα προσωπικά του δεδομένα και έχει την ανάγκη να νιώθει εμπιστοσύνη για το πρόσωπο που τα επεξεργάζεται. Στη συνέχεια παρουσιάζονται κάποια στοιχεία που φανερώνουν το κλίμα αυτό:

- για το 2014 καταγράφηκαν περίπου 80.000 περιστατικά ασφάλειας (περιλαμβανομένων 2.122 επιβεβαιωμένων απωλειών δεδομένων) και

περισσότερες από 2.000 επιθέσεις, κατά τις οποίες τέθηκαν σε κίνδυνο προσωπικά δεδομένα, στοιχεία που αφορούσαν συνολικά 61 χώρες,

- κλοπή 80.000.000 ατομικών στοιχείων ασφαλισμένων από τη 2η μεγαλύτερη Αμερικανική εταιρεία ασφάλισης υγείας, τον Φεβρουάριο του 2015,
- επίθεση από *hackers* στην μεγαλύτερη τράπεζα της Αμερικής, JP Morgan Chase, όπου τέθηκαν σε κίνδυνο οι τραπεζικοί λογαριασμοί 76.000.000 πολιτών και 7.000.000 μικρών επιχειρήσεων,
- στην ελληνική πραγματικότητα, μείζον ζήτημα σχετικά με τα προσωπικά δεδομένα πολλών χιλιάδων οροθετικών και άλλων ασθενών έχει προκαλέσει ο χειρισμός των στοιχείων από το σύστημα «Taxis». Οι φάκελοι όσων αξιολογηθούν από τα Κέντρα Πιστοποίησης Αναπηρίας και λάβουν ποσοστό αναπηρίας περνούν αυτόματα στο «Taxis» και είναι προσβάσιμοι από υπαλλήλους της Εφορίας.

Έρευνα της εταιρίας Symantec Corp., με τίτλο: «Internet Security Threat Report» (2016) καταλήγει στο ότι:

- το 2015, ο αριθμός των τρωτών σημείων υπερδιπλασιάστηκε καταγράφοντας νέο ρεκόρ με 54 zero-days. Αύξηση 125% σε σύγκριση με το προηγούμενο έτος,
- το κακόβουλο λογισμικό αυξάνεται με εντυπωσιακό ρυθμό, αφού το 2015 ανακαλύφθηκαν 430 εκατ. νέες παραλλαγές *malware*,
- το 2015 έλαβε χώρα η μεγαλύτερη παραβίαση δεδομένων που έχει αναφερθεί ποτέ δημοσίως, με 191 εκατ. εγγραφές να βρίσκονται σε κίνδυνο σε ένα μόνο μεμονωμένο περιστατικό,
- επιπλέον, 429 εκατ. ταυτότητες εκτέθηκαν σε κίνδυνο, ενώ ο αριθμός των εταιρειών που επέλεξε να μην αναφέρει τον αριθμό των εγγραφών που έχει χάσει αυξήθηκαν κατά 85%.

Τα αποτελέσματα των παραπάνω αναφερόμενων ερευνών δείχνουν το μέγεθος, τη πολυδιάστατη σημασία και την πολυπλοκότητα του προβλήματος της παραβίασης προσωπικών δεδομένων, ενώ ταυτοχρόνως έρχονται να ενισχύσουν την σημαντικότητα της Εκτίμησης των Επιπτώσεων κατά την επεξεργασία Προσωπικών Δεδομένων.

Η Ε.Ε θέλοντας να αντιμετωπίσει τους κινδύνους κατά την επεξεργασία-διαχείριση προσωπικών δεδομένων και να εναρμονιστεί σε αυτό το πεδίο με τις σύγχρονες τεχνολογικές εξελίξεις, εξέδωσε τον Γενικό Κανονισμό για την Προστασία των Δεδομένων που αποτελεί το νομικό πλαίσιο της Ε.Ε για την προστασία των δεδομένων, και σύμφωνα με τον οποίο, κάθε οργανισμός που επεξεργάζεται προσωπικά δεδομένα υποχρεούται να διενεργεί μια «Εκτίμηση των Επιπτώσεων σχετικά με την Προστασία των Δεδομένων» (Data Protection Impact Assessment - DPIA).

Σκοπός της παρούσας εργασίας είναι να εξετάσει ολοκληρωμένα την σημερινή κατάσταση σχετικά με την εναρμόνιση της ελληνικής πραγματικότητας της υλοποίησης της ηλεκτρονικής διακυβέρνησης με το γενικότερα θέμα της Εκτίμησης των Επιπτώσεων σχετικά με την Προστασία των Δεδομένων. Επιχειρείται να αποτυπωθεί το ευρωπαϊκό και ελληνικό νομικό πλαίσιο για την προστασία των προσωπικών δεδομένων, να αναδειχθεί η σημασία του Γενικού Κανονισμού για την Προστασία των Δεδομένων της Ε.Ε και ιδιαίτερα το Άρθρο 33 και να αποτυπωθεί η ανάγκη για επείγουσα αναθεώρησή του. Προτείνεται μια διαδικασία για την διενέργεια εκτίμησης των επιπτώσεων κατά την επεξεργασία προσωπικών δεδομένων

σε εφαρμογές ηλεκτρονικής διακυβέρνησης (*e-government*). Τέλος, εξετάζεται το παράδειγμα του έργου e-ΑΣΕΠ, ενός έργου ηλεκτρονικής διακυβέρνησης, όπου η ορθή αντιμετώπιση θεμάτων προσωπικών δεδομένων αντιμετωπίζεται ως κυρίαρχη δραστηριότητα.

2. Το ευρωπαϊκό και ελληνικό νομικό πλαίσιο για την προστασία των προσωπικών δεδομένων

Σε αυτή την ενότητα γίνεται προσπάθεια να αποτυπωθεί το βασικό ευρωπαϊκό και ελληνικό νομικό πλαίσιο για την προστασία των προσωπικών δεδομένων. Από τη διεθνή βιβλιογραφία μπορεί εύκολα κανείς να καταλήξει στο συμπέρασμα ότι η ιδιωτική ζωή των φυσικών προσώπων προστατεύεται διεθνώς από συμβάσεις και νομοθεσίες, όπως:

- η Οικουμενική Διακήρυξη των Δικαιωμάτων του ανθρώπου του ΟΗΕ (ΟΗΕ,1948),
- η Ευρωπαϊκή Σύμβαση για τα Δικαιώματα του Ανθρώπου (ΕΣΔΑ), η οποία υπογράφηκε στη Ρώμη το 1950, καθώς και
- η Σύμβαση 108 του Συμβουλίου της Ευρώπης για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία δεδομένων.

Αξίζει να σημειωθεί ότι σε μεταγενέστερο στάδιο, το νομοθετικό πλαίσιο ενισχύθηκε με το βασικό Κανονισμό της Ε.Ε. για την προστασία των προσωπικών δεδομένων των ατόμων και πιο συγκεκριμένα με την Οδηγία 95/46/ΕΚ, η οποία εκδόθηκε το 1995 με στόχο την προστασία του δικαιώματος των ατόμων να προστατεύουν τα δεδομένα τους, αλλά και τη διασφάλιση της ελεύθερης ροής των προσωπικών δεδομένων στα πλαίσια της Ευρωπαϊκής Ένωσης. Η εν λόγω Οδηγία αποτέλεσε το έναυσμα για την ψήφιση του Ν.2472/1997, με τον οποίο η Ελλάδα έδειξε συμμόρφωση προς τον Ευρωπαϊκό Κανονισμό και συνάμα απέκτησε το δικό της εθνικό νομοθετικό πλαίσιο για την προστασία των προσωπικών δεδομένων (ΟΗΕ,1948), (Καμπούρης, 2015).

Η Ε.Ε. και κατά συνέπεια η Ελλάδα, ακολουθώντας την εξέλιξη της τεχνολογίας και την συνεχώς αυξανόμενη ανάγκη για τη λήψη μέτρων προστασίας, εκδίδουν ανανεωμένες Οδηγίες και νόμους που καλύπτουν τυχόν κενά στην προάσπιση των δικαιωμάτων των ατόμων. Η Οδηγία 97/66/ΕΚ περί επεξεργασίας δεδομένων προσωπικού χαρακτήρα και προστασίας της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα, συμπλήρωσε την προαναφερθείσα Οδηγία 95/46/ΕΚ. Επιπλέον, μια ακόμα σημαντική Οδηγία είναι η 2002/58/ΕΚ για την προστασία των δεδομένων και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών. Η Ελλάδα, όντας υποχρεωμένη να ακολουθήσει τις εξελίξεις, προχώρησε στη συνέχεια στη θέσπιση του Ν.2774/1999 για την προστασία των ατόμων στον τηλεπικοινωνιακό τομέα και του Ν.3471/2006, για την προστασία των δεδομένων στις ηλεκτρονικές επικοινωνίες. Στα πλαίσια της συνεχούς αναθεώρησης, εντάσσεται και η νομοθετική πρόταση του Ευρωπαϊκού Κοινοβουλίου στις 25/1/2012 (COM, 2012), που αποτελεί ανανέωση της Οδηγίας 95/46/ΕΚ και είναι ευρέως γνωστή ως «Γενικός Κανονισμός για την Προστασία των Δεδομένων» (General Data Protection Regulation) (Καμπούρης, 2015).

Τελευταία εξέλιξη αποτελεί το γεγονός ότι Κοινοβούλιο ενέκρινε (4/2016) το νέο θεσμικό πλαίσιο (Κανονισμός και Οδηγία) που θα διέπει τα προσωπικά δεδομένα. Έχει δοθεί διορία δύο ετών στα κράτη - μέλη για την ενσωμάτωση του. Ο νέος γενικός κανονισμός έχει σχεδιαστεί, ώστε να δώσει στους πολίτες μεγαλύτερο έλεγχο των

προσωπικών τους στοιχείων στο νέο ψηφιακό τοπίο των «έξυπνων» κινητών τηλεφώνων, των μέσων κοινωνικών δικτύωσης και του *Internet Banking*. Υπάρχει επίσης το λεγόμενο «δικαίωμα στη λήθη», όπου το υποκείμενο των δεδομένων έχει το δικαίωμα να ζητήσει από τον υπεύθυνο επεξεργασίας τη διαγραφή δεδομένων προσωπικού χαρακτήρα.

3. Ο Γενικός Κανονισμός για την Προστασία των Δεδομένων στην ΕΕ

Ο Γενικός Κανονισμός για την Προστασία των Δεδομένων έχει στόχο την προστασία των φυσικών προσώπων και ειδικότερα των θεμελιωδών δικαιωμάτων και ελευθεριών τους, έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και της ελεύθερης κυκλοφορίας αυτών. Πεδίο εφαρμογής του είναι η αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων ή η μη αυτοματοποιημένη επεξεργασία, της οποίας όμως τα δεδομένα πρόκειται να αρχειοθετηθούν, εντός των συνόρων της Ευρωπαϊκής Ένωσης (European Commission, 2012). Τα σημεία διαφοροποίησης του Κανονισμού από τις προηγούμενες Οδηγίες δίνουν άλλη διάσταση στην προστασία των ατόμων, ειδικότερα με το μέτρο της εκτίμησης των επιπτώσεων σχετικά με την προστασία των δεδομένων που αναφέρεται στο Άρθρο 33. Συνοπτικά οι προσθήκες που περιλαμβάνει ο νέος Κανονισμός είναι οι εξής (E-Lawyer, 2013):

- αρχή της διαφάνειας στην επεξεργασία και διευκρίνιση της αρχής της ελαχιστοποίησης των δεδομένων,
- η επεξεργασία δεδομένων παιδιών υπόκειται σε αυστηρές προϋποθέσεις,
- θέσπιση του δικαιώματος διαγραφής και του δικαιώματος φορητότητας των δεδομένων,
- δικαίωμα αντίρρησης στη δημιουργία *profile* ενός υποκειμένου,
- υποχρέωση των υπευθύνων να διενεργούν εκτίμηση των επιπτώσεων σχετικά με την προστασία των δεδομένων,
- διορισμός υπεύθυνου επεξεργασίας δεδομένων,
- συμμόρφωση με τις αρχές «*privacy by default*» και «*privacy by design*».

Το Άρθρο 33 του Γενικού Κανονισμού για την Προστασία των Δεδομένων

Το Άρθρο 33 του Γενικού Κανονισμού Προστασίας των Δεδομένων, όπως εκδόθηκε τον Ιανουάριο του 2012 από την Ευρωπαϊκή Επιτροπή, υποχρεώνει τους οργανισμούς να διενεργούν «εκτίμηση των επιπτώσεων σχετικά με την προστασία των δεδομένων» (*data protection impact assessment*), όπου η επεξεργασία περικλείει κινδύνους για τα προσωπικά δεδομένα των ατόμων. Η Επιτροπή είχε δείξει ήδη το ενδιαφέρον της σχετικά με την «εκτίμηση των επιπτώσεων σχετικά με την ιδιωτικότητα» (*privacy impact assessment*) από το 2009, ενώ ένα περαιτέρω παράδειγμα του ενδιαφέροντός της για την PIA (*privacy impact assessment*) ήταν η συμμετοχή στο PIAF project (*privacy impact assessment framework*).

Το Άρθρο 33 αναφέρεται στην εκτίμηση των επιπτώσεων σχετικά με την προστασία των δεδομένων όταν η επεξεργασία περικλείει συγκεκριμένους κινδύνους για το άτομο και δύναται να προσδιοριστούν η οικονομική του κατάσταση, οι προσωπικές του προτιμήσεις, θέματα υγείας ή συμπεριφοράς. Η εκτίμηση των επιπτώσεων διενεργείται

όταν επεξεργάζονται ευαίσθητα προσωπικά δεδομένα σχετικά με σεξουαλική ζωή, υγεία, φυλή, εθνική καταγωγή, παροχή υγειονομικής περίθαλψης, αλλά και δεδομένα παιδιών, βιομετρικά δεδομένα και γενετικά δεδομένα. Η εκτίμηση θα πρέπει τουλάχιστον να περιλαμβάνει τα εξής:

- γενική περιγραφή της διαδικασίας της επεξεργασίας,
- εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των προσώπων και μέτρα για την αντιμετώπισή τους,
- μέτρα ασφαλείας και μηχανισμούς, ώστε να διασφαλίζεται η προστασία των προσωπικών δεδομένων κατά την επεξεργασία αλλά και κατά τη διάρκεια παραμονής τους στον εκάστοτε φορέα.

Ασάφειες του Άρθρου 33

Προσεκτική μελέτη του Άρθρου 33 οδηγεί στις κάτωθι διαπιστώσεις σχετικά με τις ασάφειες που το χαρακτηρίζουν:

- δεν γίνεται αναφορά στην περιγραφή της ροής της πληροφορίας (ποιος συλλέγει τις πληροφορίες, τι πληροφορίες είναι αυτές, ποιος έχει πρόσβαση σε αυτές, κλπ.),
- δεν αποσαφηνίζεται το αν χρειάζεται να δημοσιευτεί η αναφορά της εκτίμησης των επιπτώσεων,
- δεν προβλέπει την καταγραφή των ωφελειών από τη διενέργεια εκτίμησης των επιπτώσεων, καθώς εστιάζει μόνο στους ενεχόμενους κινδύνους,
- δεν αναφέρεται στην ανάγκη συνεχούς αναθεώρησης της αναφοράς, λόγω μεταβολής των παραγόντων που επηρεάζουν την επεξεργασία,
- δεν προσδιορίζει το ποιος θα διενεργεί την επικύρωση και τον έλεγχο της τελικής έκθεσης, αλλά αφήνεται αόριστα στη δικαιοδοσία της Επιτροπής να ορίσει τα πρότυπα και τις διαδικασίες.

Όλες οι παραπάνω ελλείψεις στις οδηγίες του Άρθρου 33 τονίζουν την άμεση αναθεώρησή του, ώστε να καλυφθούν τα θολά σημεία και οι παραλείψεις που στοιχίζουν σε ποιότητα και ασφάλεια όσον αφορά την επεξεργασία προσωπικών δεδομένων (Wright *et al*, 2013).

4. Εκτίμηση των επιπτώσεων σχετικά με την προστασία των δεδομένων

Σύμφωνα με τον Γενικό Κανονισμό για την Προστασία των Προσωπικών Δεδομένων και πιο συγκεκριμένα σύμφωνα με αυτά που ορίζονται στο Άρθρο 33, «...κάθε δημόσιος ή ιδιωτικός οργανισμός που επεξεργάζεται συγκεκριμένα προσωπικά δεδομένα, υποχρεούται να εκτελεί μια εκτίμηση για τις πιθανές επιπτώσεις των κινδύνων που ενδέχεται να προκύψουν από την επεξεργασία των δεδομένων αυτών». Η διαδικασία της «Εκτίμησης των Επιπτώσεων σχετικά με την Προστασία των Δεδομένων - (Data Protection Impact Assessment – DPIA) ορίζεται πολύ περιληπτικά στον τελευταίο Γενικό Κανονισμό, χωρίς όμως να ακολουθεί συγκεκριμένες γραμμές, αφήνοντας μεγάλα περιθώρια διαμόρφωσης. Στη συνέχεια προτείνεται μια διαδικασία για την διενέργεια εκτίμησης των επιπτώσεων κατά την επεξεργασία προσωπικών δεδομένων σε εφαρμογές ηλεκτρονικής διακυβέρνησης (e-government). Η διαδικασία αυτή που προτείνεται, περιλαμβάνει χρήσιμα βήματα για την αναγνώριση και την

αντιμετώπιση των κινδύνων και βασίστηκε στο περίγραμμα της εφαρμογής εκτίμησης των επιπτώσεων σε μετρικά συστήματα και έξυπνα δίκτυα (*Data protection impact assessment template for smart grid and smart metering systems*, 2014) καθώς και στο Privacy impact assessment framework project της Ευρωπαϊκής Ένωσης (PIAF EU Project, 2012). Η εκτίμηση των επιπτώσεων σχετικά με την προστασία των δεδομένων αποτελεί στην ουσία μια διαδικασία η οποία διενεργείται κυρίως κατά το αρχικό στάδιο σχεδίασης της εφαρμογής. Αποτέλεσμα αυτής της διαδικασίας είναι η σύνταξη μιας έκθεσης στην οποία περιέχονται όλα τα στοιχεία και χαρακτηριστικά της επεξεργασίας, η εκτίμηση των πιθανών κινδύνων καθώς και προτεινόμενα μέτρα ασφαλείας ώστε να επιτυγχάνεται ο περιορισμός ή η εξάλειψη αυτών. Η έκθεση αυτή υπόκειται σε έλεγχο από την εκάστοτε Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, ώστε να εκδώσει την απαραίτητη άδεια επεξεργασίας των συγκεκριμένων δεδομένων, όπως προβλέπεται από τον Γενικό Κανονισμό για την Προστασία των Δεδομένων. Αυτή η *ex-ante* εκτίμηση του όλου εγχειρήματος της επεξεργασίας ενισχύει την πιθανότητα επιρροής της DPIA στην σχεδίαση της εφαρμογής, πληρώνοντας με αυτό τον τρόπο το κριτήριο της ιδιωτικότητας κατά την σχεδίαση (*privacy by design*). Η DPIA πρέπει να θεωρείται ένα κομμάτι από μια ευρύτερη διαδικασία διαχείρισης κινδύνων (*risk management*) που οφείλει να εφαρμόζει ένας οργανισμός (European Commission – Directorate General Justice, 2012).

Εκτέλεση της DPIA

Με σκοπό να εφαρμοστεί η DPIA σε ένα νέο πληροφοριακό σύστημα επεξεργασίας δεδομένων, διατυπώνεται στη συνέχεια μια διαδικασία σε βήματα, η οποία θα αποτελείται από τις κατάλληλες δραστηριότητες, ώστε η εκτίμηση των επιπτώσεων σχετικά με τη προστασία των δεδομένων να εκτελείται με όσον το δυνατόν περισσότερη ευκολία και μεθοδικότητα. Σημειώνεται πως η προτεινόμενη διαδικασία είναι απλά μια ενδεικτική διαδικασία εκτέλεσης της σχετικής εκτίμησης προοριζόμενη για εφαρμογές ηλεκτρονικής διακυβέρνησης (*e-government*).

Η διαδικασία αυτή αποτελείται από τα εξής βήματα:

- καθορισμός της ανάγκης για την διενέργεια της DPIA (Τι είδους προσωπικά δεδομένα επεξεργάζονται; Ποιος ο υπεύθυνος επεξεργασίας; Ενδέχεται να υπάρξουν αρνητικές επιπτώσεις για τα φυσικά πρόσωπα; Έχουν ληφθεί μέτρα προστασίας;),
- προσδιορισμός της ομάδας εκτέλεσης της DPIA,
- αναγνώριση και περιγραφή της εφαρμογής / διαδικασίας (Περιγραφή του σχεδιασμού της εφαρμογής και των διεπαφών της με άλλα συστήματα και της διαδικασίας, της ροής των δεδομένων, των εμπλεκόμενων χρηστών και των επιμέρους υποσυστημάτων της εφαρμογής),
- σύσκεψη με τους εμπλεκόμενους (Ατομα από το εσωτερικό και εξωτερικό του οργανισμού επισημαίνουν τους κινδύνους που αφορούν το δικό τους πεδίο εξειδίκευσης),
- αναγνώριση των σχετικών κινδύνων (Αναγνώριση των συνθηκών και των πιθανών κινδύνων που μπορεί να απειλήσουν τα προσωπικά δεδομένα των ατόμων και να επηρεάσουν την ιδιωτικότητά τους),

- διαχείριση των κινδύνων (Αξιολόγηση των ενδεχόμενων απειλών και των δυσμενών γεγονότων που έχουν αρνητικές επιπτώσεις για τα φυσικά πρόσωπα, Λήψη μέτρων αντιμετώπισης και ασφάλειας),
- έλεγχος νομοθετικής συμμόρφωσης,
- τεκμηρίωση και ολοκλήρωση της σχετικής έκθεσης,
- εξωτερικός έλεγχος και ανασκόπηση.

Το κόστος εφαρμογής της DPIA

Η υποχρέωση των εκτελούντων της επεξεργασίας προσωπικών δεδομένων να διενεργούν εκτίμηση των επιπτώσεων σχετικά με την προστασία των δεδομένων (DPIA), όπου η επεξεργασία φαίνεται να παρουσιάζει κινδύνους για τα δικαιώματα και τις ελευθερίες των ατόμων, επιφέρει ένα επιπλέον κόστος για τον εκάστοτε οργανισμό, με την έννοια ότι χρειάζεται πόρους για να εκτελέσει την εν λόγω εκτίμηση. Η εκτίμηση του πιθανού κόστους της DPIA εξαρτάται από έναν σημαντικό αριθμό παραγόντων. Το μέγεθος και η αυστηρότητα της DPIA θα εξαρτηθούν κυρίως από το πώς ο οργανισμός αντιλαμβάνεται τους κινδύνους αλλά και τη σοβαρότητα με την οποία τους αντιμετωπίζει. Η εκτίμηση του πιθανού κόστους της DPIA εξαρτάται από τους ενδεικτικά κάτωθι συναφείς παράγοντες:

- μέγεθος της εκτίμησης,
- αυστηρότητα της νομοθεσίας,
- συμμετοχή των εμπλεκόμενων μερών,
- πρόσληψη ειδικού στελέχους για την εκτέλεση της εκτίμησης.

Προσθέτοντας όλες τις παραπάνω πιθανές δαπάνες γίνεται κατανοητό πως η DPIA αποτελεί μια διαδικασία που κοστίζει αρκετά. Το ζήτημα που εγείρεται είναι αν το όφελος από την DPIA όντως καλύπτει το κόστος της, κάτι που μπορεί να εξακριβωθεί από μια ανάλυση κόστους-οφέλους, λαμβάνοντας όμως υπόψη και επιπλέον ποιοτικούς παράγοντες (Καμπούρης, 2015).

Οφέλη από την εκτέλεση της DPIA

Από την εκτέλεση και την ολοκλήρωση της εκτίμησης των επιπτώσεων σχετικά με την προστασία των προσωπικών δεδομένων προκύπτουν σημαντικά πλεονεκτήματα ουσιαστικής σημασίας για τον οργανισμό. Αυτά τα πλεονεκτήματα αφορούν το εσωτερικό και εξωτερικό περιβάλλον του οργανισμού και θα μπορούσαν να καταγραφούν ως εξής (European Commission – Directorate General Justice, 2012; Smart Grid Task Force, 2014; Information Commissioner's Office, 2014):

- Εσωτερικά:
 - ο διαχείριση του κινδύνου (αναγνώριση και περιορισμός),
 - ο αποφυγή κοστοβόρων επαναπροσδιορισμών της διαδικασίας επεξεργασίας αλλά και της ίδιας της εφαρμογής εάν από την αρχή έχουν προσδιοριστεί οι ενδεχόμενοι κίνδυνοι και απειλές,
 - ο αποφυγή επιβολής κυρώσεων αλλά και αποφυγή της διακοπής ή απαγόρευσης του εγχειρήματος από την αρμόδια Αρχή Προστασίας Προσωπικών Δεδομένων λόγω μη συμμόρφωσης στους υφιστάμενους κανονισμούς και στη νομοθεσία της Ε.Ε,
 - ο βελτίωση της προστασίας των προσωπικών δεδομένων και της αποδοτικότητας της συγκεκριμένης υπηρεσίας,
 - ο βελτίωση του τρόπου διαχείρισης των δεδομένων γνωρίζοντας τις πιθανές απειλές και αστοχίες,

- αύξηση της ασφάλειας του συστήματος όσον αφορά την προστασία των δεδομένων και των γενικότερων λειτουργιών του οργανισμού που βασίζονται σε αυτό,
 - βελτίωση της τεχνογνωσίας σε θέματα προστασίας προσωπικών δεδομένων και ασφάλειας πληροφοριακών συστημάτων.
- Εξωτερικά:
- ενίσχυση της αξιοπιστίας του οργανισμού από την πλευρά των εμπλεκόμενων μερών και προώθηση του *e-government*,
 - υπόδειξη συμμόρφωσης με την νομοθεσία περί προστασίας προσωπικών δεδομένων και επιβεβαίωση ότι η ασφάλεια λαμβάνεται σοβαρά υπόψη.

5. Μελέτη περίπτωσης: η περίπτωση του έργου e-ΑΣΕΠ

Το Ανώτατο Συμβούλιο Επιλογής Προσωπικού (ΑΣΕΠ), συστάθηκε με το Ν. 2190/1994, ως Ανεξάρτητη Αρχή, επιφορτισμένη με τον έλεγχο της ορθής εφαρμογής των διατάξεων που διέπουν τις προσλήψεις στο δημόσιο τομέα. Αποτελεί το θεσμικό εγγυητή του δικαιώματος προς εργασία, στο δημόσιο τομέα, με συνθήκες απόλυτης διαφάνειας, δημοσιότητας, αντικειμενικότητας και αξιοκρατίας και τη διασφάλιση ίσων ευκαιριών για όλους τους πολίτες. Για την εκπλήρωση της αποστολής του, το ΑΣΕΠ έχει ήδη από τον ιδρυτικό του νόμο εξοπλιστεί με ειδικές εγγυήσεις ανεξαρτησίας. Τα μέλη του χαρακτηρίζονται ανώτατοι κρατικοί λειτουργοί που απολαμβάνουν προσωπικής και λειτουργικής ανεξαρτησίας. Κατά την εικοσαετή και πλέον λειτουργία του το ΑΣΕΠ πέτυχε να ανατρέψει παγιωμένες νοοτροπίες και πρακτικές, καταδεικνύοντας τη δυνατότητά του ως ανεξάρτητης αρχής να εκπληρώσει με επιτυχία το θεσμικό της ρόλο και να διασφαλίσει αμεροληψία και διαφάνεια στον κρίσιμο και ευαίσθητο τομέα της απασχόλησης στη δημόσια διοίκηση, καταξιώθηκε δε ως ουσιαστικός μηχανισμός ελέγχου των προσλήψεων στο Δημόσιο με γνώμονα τη διαφύλαξη της αρχής της αξιοκρατίας και τη θωράκιση του κράτους δικαίου. [ΑΣΕΠ, 2016]

Στο πλαίσιο του Επιχειρησιακού Προγράμματος «Ψηφιακή Σύγκλιση 2007-2013» στο Α.Σ.Ε.Π. υλοποιήθηκε το έργο: «Αναβάθμιση ψηφιακών υπηρεσιών Ανώτατου Συμβουλίου Επιλογής Προσωπικού (ΑΣΕΠ)» εν συντομία e-ΑΣΕΠ (ΚτΠ Α.Ε, 2013). Αντικείμενο του έργου ήταν η υλοποίηση όλων των απαιτούμενων ενεργειών για την αναβάθμιση των ψηφιακών υπηρεσιών του Α.Σ.Ε.Π., την υλοποίηση νέων ψηφιακών υπηρεσιών και την προμήθεια και εγκατάσταση του απαιτούμενου εξοπλισμού και λογισμικού. Ενδεικτικά, το συγκεκριμένο έργο περιλαμβάνει (ΑΣΕΠ, 2015):

- την αναβάθμιση των υφιστάμενων ηλεκτρονικών υπηρεσιών του ΑΣΕΠ και ειδικότερα:
 - ηλεκτρονικό αίτημα φορέα για πρόσληψη προσωπικού,
 - ηλεκτρονική αίτηση υποψηφίου για συμμετοχή του σε διαγωνισμό,
 - ηλεκτρονική ένσταση και ηλεκτρονική αίτηση θεραπείας υποψηφίου,
 - υπηρεσία παρακολούθησης πορείας της αίτησης συμμετοχής σε διαγωνισμό, της ένστασης και της αίτησης θεραπείας του υποψηφίου.
- την υλοποίηση νέων ψηφιακών υπηρεσιών του ΑΣΕΠ:

- ο δημιουργία **Ηλεκτρονικού Μητρώου** υποψηφίων με καταχωρήσεις δικαιολογητικών των υποψηφίων,
- ο δημιουργία **Ηλεκτρονικού Μητρώου** Υπαλλήλων Φορέων,
- ο διαλειτουργικότητα του Α.Σ.Ε.Π. με Φορείς που εκδίδουν/πιστοποιούν έγγραφα ή Συστήματα, οι οποίοι διαχειρίζονται τα δικαιολογητικά, που απαιτούνται για την υποβολή της ηλεκτρονικής αίτησης συμμετοχής σε διαγωνισμό,
- ο δημιουργία συστήματος εξυπηρέτησης των πολιτών που περιλαμβάνει όλα τα διαθέσιμα κανάλια επικοινωνίας,
- ο δημιουργία συστήματος διαχείρισης Περιεχομένου Ηλεκτρονικών Υπηρεσιών,
- ο υλοποίηση συστήματος διοικητικής πληροφόρησης.

Από την παραπάνω περιγραφή του έργου e-ΑΣΕΠ, γίνεται εύκολα κατανοητό ότι βασικό αλλά και καινοτόμο εργαλείο για την ηλεκτρονική παροχή υπηρεσιών του ΑΣΕΠ, αποτελεί τόσο το Ηλεκτρονικό Μητρώο υποψηφίων και υπαλλήλων φορέων, όσο και η επίτευξη διαλειτουργικότητα μεταξύ του Α.Σ.Ε.Π. και Φορέων που εκδίδουν / πιστοποιούν έγγραφα ή Συστήματα, οι οποίοι διαχειρίζονται τα δικαιολογητικά, που απαιτούνται για την υποβολή της ηλεκτρονικής αίτησης συμμετοχής σε διαγωνισμό του ΑΣΕΠ. Απουσία ολοκληρωμένης παραγωγικής λειτουργίας του έργου «Ερμής» στην καθημερινότητα της ελληνική δημόσια διοίκησης καθιστά το παραπάνω αναφερόμενο έργο του ΑΣΕΠ κομβικής σημασίας υλοποίηση ηλεκτρονικής διακυβέρνησης στην ελληνική δημόσια διοίκηση [Ερμής, 2016].

Για την «νομική θωράκιση» των παραπάνω αναφερόμενων ηλεκτρονικών υπηρεσιών του ΑΣΕΠ ψηφίστηκε ο Νόμος 4325/15 με τίτλο: «Εκδημοκρατισμός της Διοίκησης – Καταπολέμηση Γραφειοκρατίας και Ηλεκτρονική Διακυβέρνηση. Αποκατάσταση αδικιών και άλλες διατάξεις» (ΦΕΚ 47/11-5-2015). Με το άρθρο 11, με τίτλο: Ηλεκτρονικές Υπηρεσίες ΑΣΕΠ, δημιουργείται και τηρείται από το Α.Σ.Ε.Π. ηλεκτρονικό αρχείο (μητρώο) υποψηφίων, στο οποίο θα καταχωρούνται στοιχεία και τυχόν δικαιολογητικά:

- ενδιαφερομένων που θα ανταποκριθούν σε σχετική πρόσκληση του ΑΣΕΠ ασχέτως συμμετοχής σε κάποια προκήρυξη,
- όλων των υποψηφίων που θα συμμετάσχουν στο εξής σε διαδικασίες αρμοδιότητας ΑΣΕΠ, και
- ορισμένων κατηγοριών παλαιών υποψηφίων που θα επιλεγθούν από το ΑΣΕΠ γιατί πιθανολογείται γι' αυτούς ότι θα επανέλθουν σε επόμενες διαδικασίες.

Με αυτόν τον τρόπο καθιερώνεται η ηλεκτρονική υποβολή, μία μόνο φορά, των δικαιολογητικών τεκμηρίωσης των προσόντων των υποψηφίων χωρίς να απαιτείται πλέον επαν-υποβολή τους σε κάθε μελλοντική διαδικασία. Όπως επίσης δίνεται η δυνατότητα τα δικαιολογητικά αυτά να ελέγχονται μόνο μια φορά από το ΑΣΕΠ και όχι πολλές φορές που γινόταν στο παρελθόν. Επιπλέον, με το άρθρο αυτό, δημιουργείται αντίστοιχο μητρώο για τους υπαλλήλους φορέων που συνεργάζονται με το ΑΣΕΠ και παρέχεται εξουσιοδότηση στην Ολομέλεια του ΑΣΕΠ για ρύθμιση θεμάτων που αφορούν στον χρόνο τήρησης του αρχείου/μητρώου, την εγγραφή σε αυτό και λοιπά σχετικά θέματα (Νόμος υπ' αρ. 4325, ΦΕΚ 47/11-5-2015; ΦΕΚ 2849/24-12-2015).

Με την υπ' αριθμό 13/2015, Κανονιστική Απόφαση της Ολομέλειας του ΑΣΕΠ, που δημοσιεύεται στο ΦΕΚ 2849/24-12-2015, ρυθμίζονται «Θέματα τήρησης στο ΑΣΕΠ αρχείου/μητρώου υποψηφίων και υπαλλήλων φορέων». Με αυτό τον τρόπο εξασφαλίστηκε η «νομική προστασία» της τήρησης στο ΑΣΕΠ του αρχείου/μητρώου υποψηφίων και υπαλλήλων φορέων και της δυνατότητας διαλειτουργικότητας του ΑΣΕΠ με άλλους Φορείς (ΦΕΚ 2849/24 -12-2015).

Επιπρόσθετη ουσιαστική θωράκιση από πλευράς ασφάλειας των ηλεκτρονικών υπηρεσιών του ΑΣΕΠ αποτελεί τόσο το αναλυτικό Σχέδιο Πολιτικής Ασφάλειας & Ιδιωτικότητας, όσο και η Μελέτη ανάλυσης & αποτίμησης επικινδυνότητας που έχουν εκπονηθεί. Μέσα στη συνολικότερη προσέγγιση της ασφάλειας εκπονήθηκε Σχέδιο Επιχειρησιακής Συνέχειας και Σχέδιο Ανάκαμψης από Καταστροφές. Στόχος των προτάσεων αυτών είναι η εύρεση γενικότερων στρατηγικών και τεχνικών λύσεων για την διασφάλιση των αρχών ασφάλειας (εμπιστευτικότητας, ακεραιότητας, διαθεσιμότητας, αυθεντικοποίησης, μη άρνηση ευθύνης, υπευθυνότητας) των νέων ηλεκτρονικών υπηρεσιών του ΑΣΕΠ (ΚτΠ Α.Ε, 2014).

Επιπλέον, στο πλαίσιο του έργου: «Υπηρεσίες Προσδιορισμού, Παρακολούθησης & Αποτίμησης των απαιτούμενων μέτρων ασφάλειας του ΑΣΕΠ» (ΑΣΕΠ, 2013):

- εξετάστηκε και ελέγχθηκε η παραπάνω αναφερόμενη Πολιτική Ασφάλειας με χρήση διεθνώς αναγνωρισμένων προτύπων, μεθοδολογιών, test cases και εργαλείων διείσδυσης και ανάλυσης επικινδυνότητας,
- εκπονήθηκε μελέτη προστασίας της ιδιωτικότητας και βελτίωση του σχεδιασμού της πολιτικής ασφάλειας του συστήματος
- πιστοποιήθηκε η καλή λειτουργία του συστήματος ως προς την ασφάλεια των δεδομένων μέσω σχετικών διαδικασιών «*penetration testing*», και τέλος
- εκπονήθηκε σχέδιο προτάσεων βελτιστοποίησης / επικαιροποίησης των μέτρων ασφάλειας.

Τέλος θα πρέπει να σημειωθεί ότι τόσο η «νομική θωράκιση», όσο και η «τεχνική θωράκιση» (μελέτη ασφάλειας κλπ) του έργου e-ΑΣΕΠ και των ηλεκτρονικών του υπηρεσιών, επιτεύχθηκε με τη άριστη συνεργασία και υποστήριξη της Αρχής Προστασίας Προσωπικών Δεδομένων.

Συμπεράσματα

Οι ραγδαίες τεχνολογικές εξελίξεις που επηρεάζουν άμεσα και τάχιστα τις επιχειρήσεις - οργανισμούς και ιδιαίτερα ο γενικότερος αυξημένος όγκος της ανταλλαγής και της συλλογής δεδομένων έχουν δημιουργήσει νέες προκλήσεις σχετικά με την προστασία των δεδομένων. Η τεχνολογία έχει μεταλλάξει ριζικά τόσο την οικονομία, όσο και την κοινωνική ζωή. Η Ευρωπαϊκή Ένωση σε αυτό το οικονομικό-κοινωνικό πλαίσιο, έχοντας ως στόχο την ενίσχυση της προστασίας των δεδομένων και της ιδιωτικής ζωής των ατόμων, προχώρησε στην ανανέωση της σχετικής Οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου. Επικαιροποίηση της αποτελεί ο Γενικός Κανονισμός για την Προστασία των Δεδομένων, καινοτομία του οποίου είναι το Άρθρο 33, που ορίζει την υποχρεωτική εκτέλεση Εκτίμησης Επιπτώσεων σχετικά με την Προστασία των Δεδομένων. Το Άρθρο 33, με τη σημερινή του μορφή, αφήνει μεγάλα περιθώρια όσον αφορά τον τρόπο διαμόρφωσης της διαδικασίας εκτίμησης των επιπτώσεων, αλλά και του περιεχομένου της. Η συγκεκριμένη εκτίμηση στηρίζεται στο γεγονός ότι η μη ύπαρξη μιας διαδικασίας με σαφείς προϋποθέσεις και συγκεκριμένα στάδια εκτέλεσης, δίνει

το δικαίωμα στον εκάστοτε οργανισμό επεξεργασίας δεδομένων να αναπτύσσει τη δική του μεθοδολογική προσέγγιση. Αξίζει να σημειωθεί ότι η έλλειψη συνοχής που χαρακτηρίζει το συγκεκριμένο Άρθρο 33, δημιουργεί προβλήματα και στους ίδιους τους οργανισμούς, οι οποίοι καλούνται να διενεργήσουν την εν λόγω εκτίμηση με ασαφείς οδηγίες και να τηρήσουν έναν νόμο μη ολοκληρωμένο. Επιπροσθέτως, από σύγκρισή που έγινε μεταξύ των όσων προβλέπει το Άρθρο 33 και της διαδικασίας της PIA (Privacy Impact Assessment), προκύπτει πως η εκτίμηση των επιπτώσεων που αναφέρεται στο εν λόγω Άρθρο 33, χαρακτηρίζεται από μεγάλη αοριστία και ασάφεια, γεγονός που δημιουργεί πρόβλημα στη διατύπωση της διαδικασίας. Αρχικά, το πρόβλημα ξεκινά από την αναγκαιότητα εκτέλεσης της εν λόγω εκτίμησης. Ο Γενικός Κανονισμός αναφέρει πως είναι απαραίτητο να διενεργείται εκτίμηση των επιπτώσεων όταν η επεξεργασία των δεδομένων ενέχει συγκεκριμένους κινδύνους. Καθώς δεν γίνεται εκτενής αναφορά στους συγκεκριμένους κινδύνους, η εφαρμογή της DPIA γενικεύεται. Το συγκεκριμένο σημείο χρήζει διευκρίνισης για να αποφευχθεί η διενέργεια μιας DPIA άσκοπα, επιβαρύνοντας τον οργανισμό με μεγάλο κόστος. Μια πληρέστερη και ευρύτερη λίστα κινδύνων που καθιστούν απαραίτητη την DPIA, ναι μεν θα στένυνε το πεδίο εφαρμογής της, όμως θα την έκανε πιο στοχευόμενη, ενώ ταυτόχρονα θα ενίσχυε τη σημαντικότητα άλλων κινδύνων που θέτουν σε κίνδυνο την επεξεργασία (Καμπούρης, 2015). Σύμφωνα με τα παραπάνω προτείνεται η ανάγκη αναθεώρησης του Αρθρου 33 και η αντικατάστασή του με ένα πλαίσιο σαφές και αναλυτικό, που να ορίζει με ακρίβεια τα στάδια της διαδικασίας και το περιεχόμενο της σχετικής έκθεσης, ενώ ταυτόχρονα δεν θα αφήνει περιθώρια απόκλισης.

Μια επιπλέον πρόταση που μπορεί να αναδειχθεί, προς τον εκσυγχρονισμό των εποπτικών και ελεγκτικών Αρχών, είναι ο ρόλος της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, να λάβει και συμβουλευτικό χαρακτήρα (εκτός από εποπτικός και ελεγκτικός), διευκολύνοντας με αυτό τον τρόπο την διαδικασία της εκτίμησης των επιπτώσεων για τους οργανισμούς και διαφωτίζοντας ταυτόχρονα τα θολά σημεία του Αρθρου 33. Η παροχή συμβουλών σχετικά με το περιεχόμενο της τελικής αναφοράς της εκτίμησης, τις ανάγκες σε πόρους και το επιθυμητό επίπεδο ασφάλειας της επεξεργασίας, ώστε να επιτυγχάνεται η νομοθετική συμμόρφωση, θα διευκόλυνε τους οργανισμούς επεξεργασίας και θα αύξανε την εποπτική αποτελεσματικότητα της Αρχής (Καμπούρης, 2015).

Επιπλέον, ένα ακόμα θέμα προς συζήτηση που προκύπτει από την ανάπτυξη της διαδικασίας εκτίμησης των επιπτώσεων και ενδιαφέρει άμεσα τους οργανισμούς επεξεργασίας, είναι αυτό του κόστους εφαρμογής της. Όπως έγινε φανερό από την προτεινόμενη διαδικασία, η διενέργειά της απαιτεί χρόνο και ανθρώπινους πόρους με εξειδικευμένες γνώσεις, κάτι που συνεπάγεται επιπλέον κόστος. Το κόστος συμμόρφωσης θα ήταν δυσβάσταχτο για μερικούς οργανισμούς, ενώ παράλληλα αποτελεί αντικίνητρο εφαρμογής της εκτίμησης των επιπτώσεων. Η απλοποίηση της συγκεκριμένης διαδικασίας ίσως συνέβαλε στην μείωση του κόστους εφαρμογής της εκτίμησης, χωρίς να μειώνεται η ποιότητα και η ασφάλεια της επεξεργασίας. Επίσης, η εκτενέστερη αναφορά στους κινδύνους που απαιτούν εκτίμηση επιπτώσεων θα εξαιρούσε αρκετές επιχειρήσεις από την κοστοβόρα διαδικασία της DPIA, περιορίζοντας την υποχρέωσή τους σε μια απλή ανάλυση κινδύνων. Η κίνηση αυτή θα αποτελούσε ευνοϊκή εξέλιξη ειδικά για τις μικρομεσαίες επιχειρήσεις, οι οποίες είναι αμφίβολο το αν θα αντέξουν το υψηλό κόστος εφαρμογής (Καμπούρης, 2015).

Λαμβάνοντας υπόψη τα όσα αναφέρθηκαν στην εν λόγω εργασία και την επικείμενη εφαρμογή του Γενικού Κανονισμού για την Προστασία των Δεδομένων, οι αλλαγές στον τομέα της προστασίας δεδομένων αναμένεται να είναι ριζικές. Η εφαρμογή της

DPIA αλλάζει τον τρόπο διευθέτησης των κινδύνων από τους οργανισμούς αλλά και τον τρόπο εποπτείας τους από τις αρμόδιες Αρχές. Για πρώτη φορά, εφαρμόζεται ένας Κανονισμός για την προστασία των δεδομένων ο οποίος έχει ενιαία νομική βάση, παρακάμπτοντας το πρόβλημα της διαφορετικότητας των εθνικών νομικών πλαισίων. Η Ευρώπη έχει ανάγκη από έναν Κανονισμό με μακρά διάρκεια, που θα συμβάλει ουσιαστικά στην ενίσχυση της ανάπτυξης σε αυτή τη δύσκολη εποχή που διανύει.

Ευχαριστίες

Η συγκεκριμένη εργασία βασίστηκε στη Μεταπτυχιακή Διπλωματική Εργασία με τίτλο: «Εκτίμηση των Επιπτώσεων Σχετικά με την Προστασία των Δεδομένων», του φοιτητή Αναστάσιου Καμπούρη, που εκπονήθηκε στο πλαίσιο του Διαπανεπιστημιακού Προγράμματος Μεταπτυχιακών Σπουδών: «ΤΕΧΝΟ – ΟΙΚΟΝΟΜΙΚΑ ΣΥΣΤΗΜΑΤΑ», του ΕΜΠ & Πανεπιστημίου Πειραιώς, υπό την επίβλεψη του Δρ. Κωνσταντίνου Σιασιάκου, Επιστημονικό Συνεργάτη Ε.Μ.Π.

Βιβλιογραφία

Ελληνική

- Καμπούρης, Α. (2015) *Εκτίμηση των Επιπτώσεων Σχετικά με την Προστασία των Δεδομένων*, Μεταπτυχιακή Διπλωματική Εργασία στο πλαίσιο του Διαπανεπιστημιακού Προγράμματος Μεταπτυχιακών Σπουδών: «ΤΕΧΝΟ – ΟΙΚΟΝΟΜΙΚΑ ΣΥΣΤΗΜΑΤΑ», ΕΜΠ-Πανεπιστήμιο Πειραιώς.
- ΑΣΕΠ (2015) 2015 Ετήσια Έκθεση – Έκθεση Πεπραγμένων και Συνοπτική Ανασκόπηση της πορείας του ΑΣΕΠ – Ανεξάρτητη Αρχή.
- ΚτΠ Α.Ε (2013) *Διακήρυξη του έργου: Αναβάθμιση ψηφιακών υπηρεσιών Ανώτατου Συμβουλίου Επιλογής Προσωπικού* (ΑΣΕΠ), 9/2016, http://www.ktpae.gr/index.php?option=com_ktpcontests&task=Details&id=387&Itemid=13
- ΚτΠ Α.Ε (2014) *Διακήρυξη του έργου: Υπηρεσίες Προσδιορισμού, Παρακολούθησης & Αποτίμησης των απαιτούμενων μέτρων ασφάλειας του ΑΣΕΠ*, διαθέσιμο στην ιστοσελίδα: http://www.ktpae.gr/index.php?option=com_ktpcontests&task=Details&id=433&Itemid=13
- Φαρσαρώτας, Ι. και Σινανιώτη-Μαρούδη, Α. (2005) *Ηλεκτρονική Τραπεζική*, Αθήνα: Εκδόσεις Αντ. Ν. Σάκκουλα.
- Οργανισμός Ηνωμένων Εθνών (ΟΗΕ) (1948) *Οικουμενική διακήρυξη για τα Ανθρώπινα Δικαιώματα*, 9/2016, διαθέσιμο στην ιστοσελίδα: http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/grk.pdf
- E-Lawyer (2013) *Η αναθεώρηση του θεσμικού πλαισίου προστασίας δεδομένων από την Ευρωπαϊκή Ένωση*, 9/2016, Διαθέσιμο στην ιστοσελίδα: http://elawyer.blogspot.gr/2013/02/blog-post_2.html.

Ξενόγλωσση

Ericsson Mobilit Report: On the Pulse of the Networked Society (June 2016).
ERICSSON

European Commission (2012) *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, COM (2012), 11 final, 25 January, Brussels, 9/2016, διαθέσιμο στην ιστοσελίδα:
<http://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52012PC0011&from=EL>

European Commission – Directorate General Justice (2012) *Recommendations for a privacy impact assessment framework for the European Union (PIAF)*, 12 November, Brussels – London, διαθέσιμο στην ιστοσελίδα:
http://www.piafproject.eu/ref/PIAF_D3_final.pdf

Information Commissioner's Office (2014). *Conducting Privacy Impact Assessments code of practice*, February.

Internet Security Threat Report (ISTR) (2016). Symantec Corp.

Smart Grid Task Force (2014) *Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems*, 18 March, 9/2016, διαθέσιμο στην ιστοσελίδα:
https://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf

Wright, D., Finn, R. and Rodrigues, R. (2013), A Comparative Analysis of Privacy Impact Assessment in Six Countries, *Journal of Contemporary European Research*. 9 (1), 160-180.

Πηγές

ΑΠΔΠΧ (2016) Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, Ανεξάρτητη Αρχή, 9/2016, <http://www.dpa.gr/>

Ερμής (2016) Κεντρική Διαδικτυακή Πύλη της Δημόσιας Διοίκησης, 9/2016, <http://www.ermis.gov.gr/>

ΑΣΕΠ (2016) Ανώτατο Συμβούλιο Επιλογής Προσωπικού, ΑΣΕΠ, Ανεξάρτητη Αρχή, 9/2016, <http://www.asep.gr/>

Θεσμικά κείμενα

Νόμος υπ' αριθμό 4325, ΦΕΚ 47/11-5-2015, *Εκδημοκρατισμός της Διοίκησης – Καταπολέμηση Γραφειοκρατίας και Ηλεκτρονική Διακυβέρνηση. Αποκατάσταση αδικιών και άλλες διατάξεις*.

ΦΕΚ 2849/24-12-2015, *Αποφάσεις: Θέματα τήρησης στο ΑΣΕΠ Αρχείου/Μηρώου υποψηφίων και υπαλλήλων φορέων*.