ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ
ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΔΗΜΟΚΡΙΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΡΑΚΗΣ
ΤΜΗΜΑ ΝΟΜΙΚΗΣ

ΔΙΙΔΡΥΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ

Ο ΥΠΕΥΘΥΝΟΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΣΤΟΝ ΓΕΝΙΚΟ ΚΑΝΟΝΙΣΜΟ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΜΩΝ (ΕΚ) 679/2016

Διπλωματική Εργασία

της

Ελένης Κατσή

Θεσσαλονίκη, 23/10/2019

Ο ΥΠΕΥΘΥΝΟΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΣΤΟΝ ΓΕΝΙΚΟ ΚΑΝΟΝΙΣΜΟ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΜΩΝ (ΕΚ) 679/2016

Ελένη Κατσή

Πτυχίο Νομικής Δ.Π.Θ. 2015

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΟ ΔΙΚΑΙΟ & ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέπων Καθηγητής
Κ. Κομνηνός Κόμνιος

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 21/10/2019

…… …… ……..

…… …… ……

Ελένη Κατσή

ΠΕΡΙΛΗΨΗ

Με την παρούσα επιδιώκεται η παρουσίαση του νέου θεσμού του Υπευθύνου Προστασίας Δεδομένων, που πλέον με τον Κανονισμό (ΕΚ) 679/2016 έχει καταστεί υποχρεωτικός σε όλο το φάσμα του δημοσίου τομέα, των δημόσιων αρχών και σε ευρύ πεδίο στον ιδιωτικό τομέα. Ο θεσμός δεν αποτελεί μια εντελώς άγνωστη έννοια, ήδη ορισμένες χώρες, με χαρακτηριστικότερο παράδειγμα τη Γερμανία προέβλεπαν τον ορισμό του, όπως και στο ευρωπαϊκό νομικό γίγνεσθαι, προβλέπονταν ο ορισμός του άλλοτε υποχρεωτικά και άλλοτε προαιρετικά. Προτού αναλυθεί ο θεσμός του ΥΠΔ, στο Γενικό Κανονισμό, θα γίνει σύντομη αναφορά σε άλλες χώρες κράτη μέλη, όπου ήδη έχει ψηφιστεί και εφαρμοσθεί, εθνικός νόμος, εφαρμοστικός του Κανονισμού. Θα επισημανθούν, τυχόν διαφοροποιήσεις ή επιπλέον υποχρεώσεις που προέβλεψε ο εθνικό νομοθέτης του εκάστοτε κράτους μέλους, σχετικά με τον ορισμό ΥΠΔ, σε όσες διατάξεις παρέχεται αυτή η δυνατότητα, από τον κοινοτικό νομοθέτη. Παράλληλα, θα αναλυθούν ο ρόλος/ θέση του ΥΠΔ σε ένα οργανισμό, τα καθήκοντα που θα κληθεί να αναλάβει και τα εφόδια και τις ικανότητες που θα πρέπει να έχει, για να φέρει εις πέρας τον απαιτητικό του ρόλο. Τέλος, μέσω της ανάλυσης του θεσμού θα επιχειρηθεί να τονισθεί και να επισημανθεί, η σημασία της παρουσίας του ΥΠΔ σε έναν οργανισμό/οντότητα, υπό το νέο καθεστώς, όπως έχει διαμορφωθεί με την εφαρμογή του Κανονισμού, όπου ο Υπεύθυνος Προστασίας Δεδομένων καλείται να διαδραματίσει πρωταγωνιστικό ρόλο, ως ένα συμβουλευτικό όργανο.

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: υπεύθυνος προστασίας δεδομένων, Γενικός Κανονισμός, προσόντα/δεξιότητες, ρόλος/θέση, καθήκοντα,

ΠΕΡΙΕΧΟΜΕΝΑ

1.ΕΙΣΑΓΩΓΗ

Από τον Μάιο του 2018, τέθηκε σε ισχύ, μετά από μια διετή μεταβατική περίοδο, ο Κανονισμός 679/2016 για την Προστασία των Προσωπικών Δεδομένων, απόρροια των σύγχρονων τεχνολογικών και οικονομικών εξελίξεων, αφού είχαν προηγηθεί, τέσσερα έτη διαπραγματεύσεων και διαβουλεύσεων. Ο Κανονισμός (σε αντίθεση με την Οδηγία 95/46/ΕΚ που αντικατέστησε) έχει άμεση εφαρμογή σε όλα τα κράτη μέλη της ΕΕ. Ωστόσο, υπάρχουν περισσότερες από 50 σημεία/διατάξεις του GDPR, όπου προβλέπονται «ρήτρες ευελιξίας-ανοίγματος» και παρέχεται στα κράτη-μέλη η ευχέρεια, να νομοθετήσουν διαφορετικά, να αναπτύξουν δηλαδή διαφορετικές πρακτικές ερμηνείας και επιβολής του. Η πλειονότητα των χωρών, της Ευρωπαϊκής Ένωσης, έχει, ήδη ψηφίσει εθνικούς εφαρμοστικούς νόμους, σε τομείς που κατ' εξουσιοδότηση του Κανονισμού, επιτρέπονται οι παρεκκλίσεις ή προβλέπονται εξειδικεύσεις. Η Ελλάδα και η Σλοβενία, αποτελούσαν τις τελευταίες χώρες, χωρίς επικαιροποιημένη νομοθεσία στην Ευρωπαϊκή Ένωση, για την προστασία των προσωπικών δεδομένων. Το Σχέδιο Νόμου, στη χώρα μας, αρχικά είχε τεθεί προς διαβούλευση στο ελληνικό κοινοβούλιο, στις 20 Φεβρουαρίου 2018.

Η Ελλάδα είχε τύχει προειδοποιήσεως, από την Ευρωπαϊκή Επιτροπή, η οποία αποφάσισε, τον Ιανουάριο του 2019, να αποστείλει αιτιολογημένη γνώμη, στην χώρα μας, λόγω καθυστερήσεως θέσπισης εθνικού νόμου, που θα ενσωμάτωνε την Οδηγία 2016/680/ΕΕ, για την επεξεργασία προσωπικών δεδομένων από τις Αρχές ή αλλιώς «αστυνομική οδηγία», στην ελληνική έννομη τάξη. Η Ευρωπαϊκή Επιτροπή, κατόπιν της αδικαιολόγητης καθυστερήσεως, αποφάσισε να παραπέμψει την Ελλάδα, στο Δικαστήριο της ΕΕ και ο κίνδυνος επιβολής ενός δυσβάσταχτου προστίμου είναι, πλέον πραγματικότητα. Η ανωτέρω Οδηγία, θα περιλαμβάνονταν και αυτήν, στον εθνικό νόμο για τα προσωπικά δεδομένα, που είχε τεθεί υπό διαβούλευση. Στις 13 Αυγούστου 2019, ετέθη εκ νέου υπό δημόσια διαβούλευση το Σχέδιο Νόμου για τα Προσωπικά

Δεδομένα και την ενσωμάτωση της Οδηγίας 2016/680/ΕΕ. Εν τέλει, με την διαδικασία του κατεπείγοντος, υπό τη δαμόκλειο σπάθη της παραπομπής της χώρας, στο ευρωπαϊκό δικαστήριο, το νομοσχέδιο για την προστασία προσωπικών δεδομένων ψηφίστηκε, παρότι εκφράστηκαν έντονες ενστάσεις για ορισμένες διατάξεις.

Στον ανωτέρω αναφερόμενο Κανονισμό 679/2016, εισάγεται, ένας νέος ανεξάρτητος θεσμός, αυτός του Υπευθύνου Προστασίας Προσωπικών Δεδομένων (DPO), ο οποίος καλείται να διαδραματίσει ενεργό ρόλο, στην κατανόηση αλλά και στη συμμόρφωση, με το νέο Κανονισμό Προστασίας Δεδομένων. Ο θεσμός αυτός, δεν είναι παντελώς άγνωστος. Ήδη εφαρμόζεται σε άλλες χώρες, εδώ και δεκαετίες, δρώντας ως ανεξάρτητος αποκεντρωμένος, ελεγκτής για την εφαρμογή των διατάξεων περί προστασίας των προσωπικών δεδομένων. Στην Γερμανία, ήδη από το 1977, είναι υποχρεωτικός ο ορισμός ΥΠΔ στο δημόσιο αλλά, εν μέρει, και στον ιδιωτικό τομέα, γεγονός που μπορεί να αποτελέσει αρωγό στην κατανόηση, του ρόλου του νέου αυτού θεσμού και του τρόπου με τον οποίο καλείται να συνδράμει τους υπευθύνους επεξεργασίας και εκτελούντες, στην εφαρμογή του Κανονισμού.

Αλλά και από παλαιότερα, υπήρχε πρόβλεψη στην 95/46ΕΚ Οδηγία, για τον Υπεύθυνο Προστασίας Δεδομένων, εντούτοις, δεν ήταν υποχρεωτικός ο ορισμός του και η δυνατότητα αυτή δεν αξιοποιήθηκε από τον εθνικό νομοθέτη στον Ν.2472/1997 . Αντίθετα, στον Κανονισμό(ΕΚ) 45/2001,προβλέφθηκε η υποχρεωτικότητα ορισμού κοινοτικών ΥΠΔ στα όργανα και τους Οργανισμούς της Ευρωπαϊκής Κοινότητας. Θα μπορούσε να λεχθεί, επομένως, ότι έχει, ήδη, αποκτηθεί, στα πλαίσια της Ευρωπαϊκής Ένωσης, κάποια εμπειρία πάνω στο θεσμό αυτό, γεγονός που μπορεί να παρέχει την κατευθυντήρια γραμμή και το σχετικό παράδειγμα για τον τρόπο λειτουργίας του στο πλαίσιο του κάθε κράτους- μέλους.

Με το νέο Κανονισμό 679/2016, επιβάλλεται, για πρώτη φορά, υποχρεωτικότητα ως προς τον ορισμό υπεύθυνου προστασίας δεδομένων, σε όλο το δημόσιο τομέα και

τις δημόσιες αρχές και σε σημαντικό μέρος του ιδιωτικού τομέα, σε μία προσπάθεια πραγματικής υιοθέτησης και λειτουργίας του θεσμού και κατά συνέπεια, συμμόρφωσης με το ΓΚΠΔ. Είναι γεγονός ότι, η ευκολία, με την οποία προσωπικά δεδομένα, συλλέγονται και μεταφέρονται, ηλεκτρονικά έχει αυξηθεί δραματικά, στην ψηφιακή εποχή, αυξάνοντας τους κινδύνους για τα προσωπικά δεδομένα και για την προστασία των πληροφοριών. Δημιουργήθηκε έτσι, η ανάγκη επιβολής, ενός νέου ανεξάρτητου θεσμού, του Υπευθύνου Προστασίας Δεδομένων, ο οποίος θα κληθεί να διασφαλίσει ότι, τα θεμελιώδη δικαιώματα του υποκειμένου για την προστασία των δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής του ζωής, θα χαίρουν του αναγκαίου σεβασμού.

Ειδικότερα, ο Υπεύθυνος Προστασίας Δεδομένων, στο ΓΚΠΔ, επιφορτίζεται, με το καθήκον διευκόλυνσης εφαρμογής του. Καλείται, να διαδραματίσει εγγυητικό ρόλο, σχετικά με τη συμμόρφωση, των εκτελούντων και των υπευθύνων επεξεργασίας προσωπικών δεδομένων, στις διατάξεις του ΓΚΠΔ, στα πλαίσια της αρχής λογοδοσίας, που τους βαρύνει. Ο ΥΠΔ εντάσσεται, στο προσωπικό ενός οργανισμού ή μια επιχειρήσεως, δίχως να δεσμεύεται, όμως, από το διευθυντικό δικαίωμα ως προς την ενάσκηση των καθηκόντων του, δρα δηλαδή ανεξάρτητος. Οι αρμοδιότητές του, είναι συμβουλευτικές και όχι αποφασιστικές, ήτοι δεν έχει, τη δυνατότητα να επιβάλει την εφαρμογή του Κανονισμού, μέσα στον οργανισμό ή την επιχείρηση, που εργάζεται, ούτε να επιβάλλει κυρώσεις ή απαγορεύσεις.

Στην παρούσα μελέτη, αφού γίνει αναφορά στην Οδηγία και τον Κανονισμό που προαναφέρθηκαν και στους οποίους γίνεται ήδη μνεία του θεσμού, θα επιχειρηθεί μία πρώτη ανάλυση, του νέου θεσμού, θα γίνει αναφορά στις οντότητες που υποχρεούνται να διορίσουν Υπεύθυνο Προστασίας Δεδομένων, αλλά και στα προσόντα που πρέπει να διαθέτει ο ΥΠΔ, τη θέση του και τα καθήκοντα του κατά την

ενάσκηση των καθηκόντων του. Παράλληλα θα γίνει αναφορά και στο καθεστώς του ΥΠΔ σε άλλες χώρες της Ευρωπαϊκής Ένωσης.

2.ΙΣΤΟΡΙΚΟ ΥΠΟΒΑΘΡΟ ΘΕΣΜΟΥ

Ο θεσμός του ΥΠΔ, όπως προαναφέρθηκε δεν εισάγεται για πρώτη φορά, στο ευρωπαϊκό νομικό πλαίσιο. Ήδη με τη μητρική Οδηγία (ΕΚ) 95/46 «για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών» προβλέπονταν ο προαιρετικός ορισμός του. Αλλά και με τον Κανονισμό(ΕΚ) 45/2001 «για την προστασία των φυσικών προσώπων από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, από όργανα και οργανισμούς της Κοινότητας και σχετικά με την ελεύθερη κυκλοφορία των δεδομένων αυτών», ορίζεται ως υποχρεωτικός ο ΥΠΔ, στις υπηρεσίες της Ευρωπαϊκής Ένωσης και θεσπίζεται, η κεντρική ανεξάρτητη αρχή, του Ευρωπαίου Επόπτη Προστασίας Δεδομένων. Παράλληλα και σε άλλες ευρωπαϊκές υπηρεσίες προβλέπεται ο ορισμός ΥΠΔ, ενώ ο κεντρικός τους έλεγχος και η εποπτεία θα ασκείται από τον Ευρωπαίο Επόπτη Προστασίας Δεδομένων.

Ο ορισμός ΥΠΔ, είναι επίσης υποχρεωτικός για τις αρμόδιες αρχές, δυνάμει του άρθρου 32 της Οδηγίας (ΕΕ) 2016/680, του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών.

Το Συμβούλιο της Ε.Ε., έχει και αυτό το δικό του ΥΠΔ (Data protection commissioner) αλλά και στην εθνική νομοθεσία προβλέπεται, στον Ν. 3574/2008 και στον Ν. 3917/2011, ο Υπεύθυνος Διασφάλισης Απορρήτου και ο Υπεύθυνος Ασφαλείας Δεδομένων, αντίστοιχα, θεσμοί συγγενείς με αυτόν του ΥΠΔ. Στην Γερμανία, όπως προαναφέρθηκε ο θεσμός του ΥΠΔ, εφαρμόζεται ήδη, από το 1977, στον ιδιωτικό και δημόσιο τομέα, αποτελώντας την πρωτοπόρο χώρα, σε αυτό το θέμα.

Ι.ΟΙ ΠΡΟΑΙΡΕΤΙΚΟΙ ΥΠΕΥΘΥΝΟΙ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΣΤΗΝ ΟΔΗΓΙΑ (ΕΚ) 95/46

Στην 95/46ΕΚ Οδηγία, για την προστασία των φυσικών προσώπων από την επεξεργασία δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών, η οποία πλέον έχει καταργηθεί και αντικατασταθεί από τον Κανονισμό 679/2016, προβλέπονταν ως μια προαιρετική δυνατότητα από τους εθνικούς νομοθέτες, ο ορισμός ΥΠΔ .[1]

Συγκεκριμένα, στην Οδηγία θεσπίζονταν, η διοικητική υποχρέωση, του υπευθύνου επεξεργασίας να γνωστοποιεί, τυχόν επεξεργασία δεδομένων στην Αρχή. Στον καταργηθέντα νόμο 2472/1997, αντίστοιχη υποχρέωση προβλέπονταν στο άρθρο 6, σύμφωνα με το οποίο, ο υπεύθυνος επεξεργασίας θα πρέπει να γνωστοποιεί στην Αρχή, τα στοιχεία που αναφέρονται στο εν λόγω άρθρο, για να είναι νόμιμη η επεξεργασία, στην οποία προβαίνει.

Η αυστηρότητα με την οποία διατυπώνονταν, η διάταξη αυτή, στην Οδηγία, μετριάζονταν, με την πρόβλεψη στο άρθρο 18 παρ. 2. Τα κράτη θα μπορούν να προβλέπουν απλουστευμένη κοινοποίηση ή και εξαίρεση από την κοινοποίηση σε ορισμένες περιπτώσεις, οι οποίες προβλέπονταν στο εν λόγω άρθρο της Οδηγίας. Έτσι, ορίζεται ότι εφόσον, α) η επεξεργασία που γίνεται, δεν είναι δυνατόν, να θίξει τα δικαιώματα και τις ελευθερίες των προσώπων, στα οποία ανήκουν τα δεδομένα που υπόκεινται σε επεξεργασία και β) ο υπεύθυνος επεξεργασίας, ορίζει σύμφωνα με το εθνικό δίκαιο στο οποίο υπόκειται, έναν ΥΠΔ, ο οποίος θα διαφυλάττει την εφαρμογή της Οδηγίας στο εσωτερικό του κράτους και θα τηρεί μητρώο των επεξεργασιών που εκτελούνται, τότε τα κράτη θα μπορούν είτε να παραβλέπουν την κοινοποίηση είτε και

1.Λαζαράκος Γρηγόρης,2016, «Ο θεσμός του υπεύθυνου προστασίας προσωπικών δεδομένων (Data Protection Officer) στο νέο νομοθετικό πλαίσιο των προσωπικών δεδομένων μετά την υιοθέτηση του Κανονισμού (ΕΕ) 679/2016, Εφαρμογές Δημοσίου Δικαίου, σελ.244.

να εφαρμόζουν μία ποιο απλουστευμένη κοινοποίηση.

Παρατηρείται, λοιπόν, ότι εισάγονταν στο σημείο αυτό, στην Οδηγία ο προαιρετικός ορισμός ΥΠΔ, ο οποίος θα έχει ως καθήκον τη διασφάλιση της προστασίας των δεδομένων και τη τήρηση μητρώου, ως αντιστάθμισμα για τη χαλαρότητα, της ανάγκης κοινοποιήσεως στην Αρχή. Επομένως, αντί να κοινοποιείται το αρχείο, τηρείται από τον ΥΠΔ, σε μία προσπάθεια αποφόρτισης των αρμοδιοτήτων της Αρχής. Ο θεσμός, αυτός υιοθετήθηκε αρχικά, από ελάχιστα κράτη, στην πορεία, όμως, παρατηρήθηκε ότι και άλλα επέλεξαν, να προβλέψουν τον ορισμό ΥΠΔ. Μέχρι το 2005, πέντε κράτη, ήτοι η Γερμανία, η Ολλανδία, η Σουηδία, το Λουξεμβούργο και η Γαλλία, είχαν προβλέψει τον ορισμό ΥΠΔ.

Η πρόβλεψη ορισμού ΥΠΔ στην Οδηγία, όπου εφαρμόσθηκε, μπορεί να αποτελέσει, ένα χρήσιμο παράδειγμα για το τρόπο, που θα λειτουργήσει και το σκοπό που επιδιώκει να επιτύχει, η υποχρεωτικότητα, ορισμού ΥΠΔ, στο νέο Κανονισμό, ο οποίος αντικατέστησε την εν λόγω Οδηγία.

II. ΟΙ ΚΟΙΝΟΤΙΚΟΙ ΥΠΔ ΣΤΟΝ ΚΑΝΟΝΙΣΜΟ (ΕΚ) 45/2001

Με τον Κανονισμό (ΕΚ) 45/2001, για «την προστασία των φυσικών προσώπων από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, από όργανα και οργανισμούς της Κοινότητας και σχετικά με την ελεύθερη κυκλοφορία των δεδομένων αυτών», θεσπίστηκε η υποχρέωση για συμμόρφωση της ίδιας της Ε.Ε. με τη προστασία των προσωπικών δεδομένων. Αυτό επιδιώχθηκε, με την εισαγωγή ενός νέου κοινοτικού οργάνου, του Ευρωπαίου Επόπτη Προστασίας Δεδομένων, ο οποίος θα διαδραμάτιζε το ρόλο της κεντρικής Αρχής Προστασίας Δεδομένων και θα αναλάμβανε την κεντρική εποπτεία της προστασίας των προσωπικών δεδομένων.

Παράλληλα, ο Κανονισμός, εκτός του θεσμού του Ευρωπαίου Επόπτη Προστασίας Δεδομένων, εισάγει, επιπρόσθετα την υποχρέωση κάθε οργάνου και οργανισμού της Κοινότητας να διορίζει τουλάχιστον, έναν Υπεύθυνο Προστασίας Δεδομένων. Έναν τουλάχιστον διότι, λόγω του μεγέθους ορισμένων κοινοτικών οργάνων, θεωρήθηκε σκόπιμο, να ορίζεται και ένας αναπληρωτής ή βοηθός του ΥΠΔ. Ένα τέτοιο παράδειγμα αποτελεί, η Ευρωπαϊκή Επιτροπή, η οποία έχει διορίσει έναν «Συντονιστή Προστασίας Δεδομένων» σε κάθε γενική διεύθυνση της, επικεφαλής των οποίων ετέθη ο «Υπεύθυνος Προστασίας Δεδομένων».[2]

Στον Κανονισμό και συγκεκριμένα στο άρθρο 24, αναφέρονται και τα καθήκοντα του ΥΠΔ των κοινοτικών οργάνων και οργανισμών, τα οποία είναι πέντε: 1) το καθήκον ενημέρωσης, 2) η συνεργασία με την Εποπτική Αρχή, 3)η διασφάλιση συμμόρφωσης με τον Κανονισμό, 4)η τήρηση μητρώου επεξεργασιών δεδομένων, 5) η κοινοποίηση επικίνδυνων επεξεργασιών δεδομένων στον Ευρωπαίο Επόπτη Προστασίας Δεδομένων.

III. Ο ΥΠΕΥΘΥΝΟΣ ΔΙΑΣΦΑΛΙΣΗΣ ΑΠΟΡΡΗΤΟΥ ΚΑΙ Ο ΥΠΕΥΘΥΝΟΣ ΑΣΦΑΛΕΙΑΣ ΔΕΔΟΜΕΝΩΝ

Στον Νόμο 3674/2008, προβλέπεται ότι ο πάροχος δικτύου ηλεκτρονικών επικοινωνιών ή υπηρεσιών ηλεκτρονικών επικοινωνιών, θα πρέπει να ορίζει ένα στέλεχός του, ως Υπεύθυνο Διασφάλισης Απορρήτου. Καθήκον του ΥΔΑ είναι η διασφάλιση της εφαρμογής του σχεδίου πολιτικής ασφαλείας, που καταρτίζει ο πάροχος, σύμφωνα με τα προβλεπόμενα σε κανονισμούς της Αρχής Διασφάλισης του

2.Σωτηρόπουλος Βασίλης, 2017, «Υπεύθυνος Προστασίας Δεδομένων-Εργαλειοθήκη για τον νέο θεσμό σε δημόσιο και ιδιωτικό τομέα», Εκδόσεις Σάκκουλα, σελ. 70-72.

Απορρήτου των Επικοινωνιών(ΑΔΑΕ). Συγκεκριμένα, κάθε τετράμηνο εντός του πρώτου δεκαημέρου, υποβάλλεται στον πρόεδρο της ΑΔΑΕ, δήλωση, η οποία έχει υπογραφεί από τον πάροχο και τον ΥΔΑ, στην οποία γίνεται μνεία των βουλευμάτων και των διατάξεων, με τα οποία ζητείται η άρση του απορρήτου, καθώς και των αρχών που αιτούνται την άρση. Αν προκύψει παραβίαση του απορρήτου, ο ΥΔΑ οφείλει αμελλητί να ενημερώσει, εγγράφως για την παραβίαση και εάν αμελήσει να πράξει τούτο, προβλέπονται ποινικές κυρώσεις για τον ίδιο.

Αντίστοιχα στον Νόμο 3917/2011,προβλέπεται ο ορισμός Υπευθύνου Ασφαλείας Δεδομένων, από τον πάροχο διαθέσιμων στο κοινό υπηρεσιών, ηλεκτρονικών επικοινωνιών ή δημοσίου δικτύου επικοινωνιών. Ο ανωτέρω αναφερόμενος πάροχος, υποχρεούται να καταρτίζει ειδικό σχέδιο πολιτικής ασφαλείας, την εφαρμογή του οποίου αναθέτει στον ΥΑΔ.[3]

IV. ΥΠΔ ΣΤΗΝ ΓΕΡΜΑΝΙΑ ΥΠΟ ΤΟ ΠΡΟΗΓΟΥΜΕΝΟ ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ

Στον προηγούμενο γερμανικό ομοσπονδιακό νόμο, για την προστασία των προσωπικών δεδομένων (Bundesdatenschutzgesetz ή "BDSG") απαιτούνταν από δημόσιους και ιδιωτικούς οργανισμούς, να διορίζουν ΥΠΔ, εάν απασχολούσαν μόνιμα δέκα ή περισσότερα των δέκα ατόμων, στην αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα. Η υποχρέωση αυτή ίσχυε, επίσης και για εταιρείες και οργανισμούς, που απασχολούσαν 20 ή περισσότερα άτομα και προέβαιναν σε μη αυτοματοποιημένη επεξεργασία δεδομένων ή σε επεξεργασία δεδομένων που παρα-

3. Νόμος 3917/2011, άρθρο 7 παρ. 2 εδάφ. β':«Η εφαρμογή του σχεδίου αυτού ανατίθεται από τον πάροχο σε εξουσιοδοτημένο στέλεχος, το οποίο ορίζεται ως υπεύθυνος ασφάλειας δεδομένων».

βίαζε τόσο έντονα τα προσωπικά δικαιώματα και τις ελευθερίες των υποκειμένων, ώστε να απαιτείται, ο ΥΠΔ να προβεί σε επίσημη προκαταρκτική εξέταση του επιτρεπτού χαρακτήρα αυτής της επεξεργασίας δεδομένων(αντίστοιχη με την εκτίμηση αντικτύπου).[4] Σε περίπτωση παραβίασης της υποχρέωσης διορισμού ΥΠΔ, προβλέπονταν διοικητικά πρόστιμα, που ανέρχονταν στο ποσό των 50.000 ευρώ. Πολλές από τις διατάξεις, του προηγούμενο Νόμου για τα προσωπικά δεδομένα στην Γερμανία, φαίνεται να έχουν αποτελέσει πηγή έμπνευσης για τον νέο Κανονισμό αλλά και τον εφαρμοστικό νόμο που ψηφίστηκε πρόσφατα στην Ελλάδα.

4. Business and Technology Sourcing Review-Issue 16, 8/6/2011, «New Requirements for Data Protection Officers in Germany»<https://www.mayerbrown.com/en/perspectives-events/publications/2011/06/new-requirements-for-data-protection-officers-in-g >.

3. Ο ΘΕΣΜΟΣ ΤΟΥ ΥΠΔ ΣΤΙΣ ΧΩΡΕΣ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ

Τα περισσότερα κράτη μέλη, όπως προαναφέρθηκε, έχουν ψηφίσει εθνικούς εφαρμοστικούς νόμους, σε συμμόρφωση με τον Κανονισμό Προστασίας Προσωπικών Δεδομένων. Οι εθνικοί νόμοι, περιλαμβάνουν διατάξεις για τον ορισμό ΥΠΔ, που εισάγουν ορισμένες διαφοροποιήσεις ή προβλέπουν επιπλέον προϋποθέσεις, στα πλαίσια της διακριτικής ευχέρειας, που τους παρέχεται από τον ΓΚΠΔ.

Στην **Αυστρία**, ο εθνικός νόμος «DSG», στο πέμπτο τμήμα του, περιλαμβάνει κάποιους επιπλέον κανόνες, σε σχέση με αυτούς που προβλέπονται στον Κανονισμό, όσον αφορά τις υποχρεώσεις του ΥΠΔ. Συγκεκριμένα, απαιτείται ο ΥΠΔ και τα άτομα που εργάζονται γι αυτόν, να τηρούν απόρρητα τα στοιχεία της ταυτότητας των ατόμων, που έχουν επικοινωνήσει μαζί τους ή έχουν επεξεργαστεί προσωπικά τους δεδομένα και να διασφαλίζουν ότι δεν θα αποκαλυφθεί οποιαδήποτε πληροφορία που μπορεί να αποκαλύψει την ταυτότητα αυτών.[5] Το καθήκον εχεμύθειας, με το οποίο επιφορτίζεται ο ΥΠΔ, επεκτείνεται και στα μέλη του προσωπικού, που εργάζονται μαζί του και αφορά, οποιαδήποτε πληροφορία έχουν μάθει, λόγω της θέσης που κατέχουν. Οι επιπλέον αυτοί κανονισμοί, αφορούν τους δημόσιους οργανισμούς, μόνο.

Στο **Βέλγιο,** ο εθνικός νόμος «DPA»[6],προβλέπει ότι ο ορισμός του ΥΠΔ, θα εξαρτάται από την επιρροή που θα έχει η δραστηριότητα επεξεργασίας ενώ παράλληλα θα πρέπει να εξετάζεται και το ρίσκο που θα ενέχει αυτή, σύμφωνα με το άρθρο 35 του Κανονισμού, ιδίως όταν i) οργανισμός ιδιωτικού Δικαίου, επεξεργάζεται δεδομένα για λογαριασμό της κυβέρνησης ή η κυβέρνηση μεταφέρει προσωπικά δεδομένα, στο πλαίσιο αστυνομικής έρευνας, που διεξάγεται ή ii) η επεξεργασία υπερβαίνει τους

5. DLAPIPER, «Data Protection laws of the world», Austria-DPO.

6. DLA PIPER, «Data Protection laws of the world», Belgium-DPO.

σκοπούς, που απαιτούνται για τη συλλογή δεδομένων, για λόγους δημοσίου ενδιαφέροντος, επιστημονικούς, ιστορικής έρευνας ή για σκοπούς στατιστικούς. Ορισμένοι κυβερνητικοί οργανισμοί, οι οποίοι αναφέρονται στον εθνικό νόμο, όπως το Κέντρο για εξαφανισμένα και σεξουαλικώς κακοποιημένα παιδιά, απαιτείται να ορίσουν ΥΠΔ.

Στη **Βουλγαρία**, ο εθνικός νόμος, δεν προβλέπει κάποια διαφοροποίηση, σε σχέση με τον Κανονισμό. Εντούτοις, απαιτεί από τον υπεύθυνο επεξεργασίας δεδομένων, να ανακοινώνει, τα προσωπικά στοιχεία του ΥΠΔ και τα στοιχεία επικοινωνίας μαζί του, τα οποία θα πρέπει να τα δημοσιοποιεί, μάλιστα.[7] Κάθε αντικατάσταση του ΥΠΔ, θα πρέπει να γίνεται γνωστή. Ο τρόπος, το περιεχόμενο και η διαδικασία της ανακοίνωσης, πριν την εφαρμογή του εθνικού νόμου, θα καθορίζονταν από τον Κανονισμό της Επιτροπής και έπειτα θα εγκρίνονταν από τον εθνικό νόμο.

Στην **Κροατία**, δεν υπάρχει κάποια διαφοροποίηση, ως προς τις προβλέψεις του Κανονισμού, για τους ΥΠΔ.

Στην **Κύπρο**, προβλέπεται ότι, ο Επίτροπος, θα δημοσιεύει και θα καθιστά προσιτή, μία λίστα με τις λειτουργίες επεξεργασίας ή άλλων περιπτώσεων, που θα καθιστούν απαραίτητο τον ορισμό ΥΠΔ, από τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία.[8] Λίστα με τα ονόματα των υπευθύνων επεξεργασίας ή εκτελούντων που έχουν προσλάβει ΥΠΔ, θα δημοσιεύεται στην ιστοσελίδα (website) του Επιτρόπου, υπό την προϋπόθεση ότι συναινούν, είτε ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία, ανάλογα με το ποιος βαρύνεται με την υποχρέωση ορισμού.

---

7. DLA PIPER, «Data Protection laws of the world», Bulgaria-DPO.

8. DLA PIPER, «Data Protection laws of the world», Cyprus-DPO.

Στην **Τσεχία**, δεν προβλέπεται κάποια διαφοροποίηση ως προς τον ΥΠΔ, στον εθνικό νόμο.

Στην **Δανία**, ο ΥΠΔ, υπό τον εθνικό νόμο (Danish Data Protection Act), υπόκειται σε καθήκον εχεμύθειας. Απαγορεύεται, να μεταφέρει και να εκμεταλλεύεται δεδομένα, που απέκτησε λόγω της ιδιότητάς του, ως ΥΠΔ.

Στην **Εσθονία**, ο εθνικός νόμος (PDPA), δεν προβλέπει παρεκκλίσεις ή πρόσθετες απαιτήσεις, ως προς τον Κανονισμό.[9]

Στην **Φιλανδία,** ο εθνικός νόμος δεν περιλαμβάνει επιπλέον, ειδικές προϋποθέσεις για τον ΥΠΔ. Ωστόσο, ορισμένοι άλλοι εθνικοί νόμοι και διατάγματα, προβλέπουν τον υποχρεωτικό ορισμό ΥΠΔ. Για παράδειγμα, όλες οι μονάδες υγειονομικής περίθαλψης και ευημερίας, όπως τα φαρμακεία, πρέπει να ορίσουν ΥΠΔ, σύμφωνα με την «Acton Electronic Prescriptions 2007/61». Όπως επίσης και κατά την «Act on Electronic Processing of Client Information in Social Welfare and Healthcare 2007/159», ΥΠΔ, θα πρέπει να ορισθεί, σε όλες τις λειτουργικές ενότητες, της δημόσιας κοινωνικής πρόνοιας και υγειονομικής περίθαλψης, όπως επίσης και στον Οργανισμό Φιλανδικής Κοινωνικής Ασφάλισης (“KELA”). Εντούτοις, ήδη, έχουν προταθεί τροποποιήσεις στην«Acton Electronic Processing of Client Information in Social Welfare and Healthcare», γεγονός που θα επιφέρει τροποποιήσεις και στο κομμάτι που αφορά τον ΥΠΔ, όπου πλέον η υποχρέωση ορισμού του, θα καλύπτεται από την εφαρμογή του Κανονισμού.[10]

Στη **Γαλλία,** ο υπεύθυνος προστασίας δεδομένων, που επεξεργάζεται, δεδομένα, στο πλαίσιο της Οδηγίας « EU Data Protection Directive on Police and Criminal Justice

9. DLA PIPER, «Data Protection laws of the world», Denmark-DPO.

10. DLA PIPER, «Data Protection laws of the world», Finland-DPO.

Cooperation», θα πρέπει να ορίσει ΥΠΔ, με εξαίρεση τα δικαστήρια που ενεργούν στο πλαίσιο της δικαιοδοτικής τους αρμοδιότητας. Το «Decree» (νόμος στη Γαλλία) συγκεκριμενοποιεί τις απαραίτητες πληροφορίες, που θα πρέπει να δημοσιευθούν στην Εποπτική Αρχή (CNIL) από τους υπευθύνους επεξεργασίας και τους εκτελούντες την επεξεργασία, στο έντυπο κοινοποιήσεως του ΥΠΔ. Στην Γαλλία, ήδη υπήρχαν, σε ορισμένες εταιρίες οι "CIL" (οι ανταποκριτές υπολογιστών και ελευθερίας), οι οποίοι ήταν, άτομα που αποτελούν το σύνδεσμο-δίαυλο επικοινωνίας της Γαλλικής Αρχής Προστασίας Δεδομένων (CNIL),με τις επιχειρήσεις. Ο ρόλος των ανωτέρω, θα μπορούσε να αναβαθμιστεί και να παρέχουν πλέον, τις υπηρεσίες τους ως ΥΠΔ.[11]

Στην **Γερμανία,** το όριο για τον ορισμό ενός υπεύθυνου προστασίας δεδομένων (DPO) είναι πιο αυστηρό, σύμφωνα με τον «Budesdatenschutzgesetz-BDSG». Ο υπεύθυνος επεξεργασίας και ο υπεύθυνος επεξεργασίας, πρέπει να ορίσουν ΥΠΔ, εάν χρησιμοποιούν τουλάχιστον δέκα άτομα, που απασχολούνται στην αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα (38 εδάφιο α' BDSG).[12] Η έννοια της «αυτοματοποιημένης επεξεργασίας» ερμηνεύεται ευρέως από τις γερμανικές αρχές. Βασικά καλύπτει κάθε εργαζόμενο, που εργάζεται με υπολογιστή. Εφόσον, το όριο των δέκα ατόμων, δεν καλύπτεται, (Κεφ. 38 δεύτερη φράση), ο εθνικός νόμος («BDSG») προβλέπει, επιπλέον του άρθρου 37 του Κανονισμού (GDPR), ότι ΥΠΔ, πρέπει να ορίζεται σε περίπτωση που ο υπεύθυνος της επεξεργασίας ή ο εκτελών της επεξεργασία, αναλάβει τη διεξαγωγή επεξεργασίας, η οποία υπόκειται σε αξιολόγηση αντίκτυπου για την προστασία των δεδομένων, σύμφωνα με το άρθρο 35 του Κανονισμού (GDPR) ή εάν επεξεργάζονται για εμπορικούς σκοπούς, δεδομένα προσωπικού χαρακτήρα. Επιπλέον, στον εθνικό νόμο, θεσπίζεται ένα προστατευτικό

11. DLA PIPER, «Data Protection laws of the world», France-DPO.

12. DLA PIPER, «Data Protection laws of the world», Germany-DPO.

πλέγμα όσον αφορά τον ΥΠΔ. Ο ΥΠΔ, δεν απολύεται, εκτός εάν, υπάρχουν γεγονότα, που δίνουν στον δημόσιο φορέα την δυνατότητα, να τερματίσει τη συνεργασία του, χωρίς προειδοποίηση. Αφού απολυθεί ο ΥΠΔ, δεν απομακρύνεται αμέσως, από το χώρο εργασίας του, αλλά παραμένει στη θέση του, για ένα έτος επιπλέον, εκτός εάν ο δημόσιος φορέας δικαιολογημένα αποφάσισε να τερματισθεί, η συνεργασία τους, χωρίς προειδοποίηση. Επιπλέον, ο εθνικός νόμος («BDSG») ορίζει, ότι ο υπεύθυνος προστασίας δεδομένων, δεσμεύεται από το απόρρητο, όσον αφορά την ταυτότητα των προσώπων, στα οποία αναφέρονται τα δεδομένα και τις περιστάσεις που επιτρέπουν την αναγνώριση των υποκειμένων των δεδομένων, υπό την ρητή εξαίρεση, κατά την οποία το υποκείμενο, στο οποίο αναφέρονται τα δεδομένα, τους απαλλάσσει από αυτή την υποχρέωση. Επιπλέον, οι γερμανικές αρχές, απαιτούν από τον υπεύθυνο προστασίας δεδομένων να γνωρίζει, τη γλώσσα των αρμόδιων αρχών και των υποκειμένων των δεδομένων, δηλαδή την γερμανική, ή τουλάχιστον να διαβεβαιώνεται η δυνατότητα, άμεσης μετάφρασης.

Στην **Ουγγαρία**, δεν υπάρχει κάποια ειδική πρόβλεψη, σχετικά με τον ορισμό του ΥΠΔ.

Στην **Ιρλανδία**, το άρθρο 34 του εθνικού νόμου, επιτρέπει στον Υπουργό, μετά από διαβούλευση με άλλους Υπουργούς της Κυβέρνησης και εφόσον κρίνεται σκόπιμο και με την Επιτροπή, να θεσπίζει κανόνες βάσει των οποίων, οι υπεύθυνοι επεξεργασίας δεδομένων, οι εκτελούντες την επεξεργασία, ή άλλοι οργανισμοί που εκπροσωπούν κατηγορίες υπεύθυνων ή εκτελούντων επεξεργασίας, θα έχουν την υποχρέωση να ορίσουν ΥΠΔ.[13]

13.DLA PIPER, «Data Protection laws of the world», Ireland-DPO.

Στην **Ιταλία**, εφαρμόζεται ο Κανονισμός δίχως παρέκκλιση όσον αφορά τις προβλέψεις για τον ΥΠΔ. [14]

Στην **Λετονία**, ο εθνικός νόμος «Personal Data Processing Law», δεν προβλέπει παρέκκλιση από τις απαιτήσεις του GDPR, όσον αφορά τους υπευθύνους προστασίας δεδομένων.

Στην **Λιθουανία,** επίσης, ο νόμος περί προστασίας δεδομένων, δεν καθορίζει παρεκκλίσεις από τις απαιτήσεις που ορίζονται στο GDPR όσον αφορά τους υπευθύνους προστασίας δεδομένων.

Στο **Λουξεμβούργο**, το άρθρο 65, του εθνικού νόμου, της 1ης Αυγούστου 2018, προβλέπει ειδική υποχρέωση για την εθνική επιτροπή προστασίας δεδομένων, ορισμού ΥΠΔ, στο πλαίσιο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα για επιστημονικούς ή ιστορικούς σκοπούς ή για στατιστικούς σκοπούς.[15] Ο ορισμός, αυτός πρέπει να γίνεται σύμφωνα με τη φύση, το πεδίο, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους για τα δικαιώματα και τις ελευθερίες, των υποκειμένων, στα οποία αναφέρονται τα δεδομένα. Σε περίπτωση που ο υπεύθυνος επεξεργασίας, επιλέξει να μην ορίσει υπεύθυνο προστασίας δεδομένων, τότε πρέπει να τεκμηριώνει επισήμως και να αιτιολογεί την επιλογή του, να μην ορίσει έναν ΥΠΔ, για κάθε εργασία που εκτελεί και περιλαμβάνει επεξεργασία δεδομένων προσωπικού χαρακτήρα, για επιστημονικούς ή ιστορικούς σκοπούς ή για στατιστικούς σκοπούς.

Στην **Μάλτα**, εφαρμόζεται ότι προβλέπεται στον Κανονισμό, δίχως παρέκκλιση.

---

14. Legislative Decree 101/2018, που τέθηκε σε ισχύ στις 19/09/2018.

15. DLA PIPER, «Data Protection laws of the world», Luxembourg-DPO.

Στην **Ολλανδία**, ο εκτελεστικός νόμος, παρέχει λεπτομερέστερες πληροφορίες σχετικά με την υποχρέωση τήρησης του απορρήτου, που προβλέπεται στο άρθρο 38 παράγραφος 5 του ΓΚΠΔ, ορίζοντας ότι ο ΥΠΔ πρέπει να τηρεί το απόρρητο, κάθε πληροφορίας, η οποία του γνωστοποιείται, μέσω καταγγελίας ή κάποιου αιτήματος, του υποκειμένου των δεδομένων, εκτός εάν το υποκείμενο των δεδομένων συμφωνεί, με την αποκάλυψη των δεδομένων που το αφορούν.[16]

Στην **Νορβηγία**, εφαρμόζεται χωρίς διαφοροποίηση ο Κανονισμός.

Στην **Πολωνία**, σύμφωνα με τον εθνικό νόμο (PDPA), ο ορισμός ενός υπεύθυνου προστασίας δεδομένων (DPO) πρέπει να κοινοποιηθεί στην εποπτική αρχή, εντός 14 ημερών.[17] Η κοινοποίηση, πρέπει να περιλαμβάνει, το όνομα και τη διεύθυνση ηλεκτρονικού ταχυδρομείου του ΥΠΔ ή τον αριθμό τηλεφώνου του. Οποιεσδήποτε διαφοροποιήσεις, στις παρεχόμενες πληροφορίες ή η απόλυση ενός ΥΠΔ, πρέπει επίσης, να κοινοποιούνται εντός 14 ημερών. Η οντότητα, που όρισε τον ΥΠΔ, πρέπει να καθιστά προσπελάσιμα, τα στοιχεία του ΥΠΔ στον ιστότοπό της ή οπουδήποτε αλλού είναι εφικτό (εάν δεν έχει δικό της wesbite). Σύμφωνα με επίσημες οδηγίες της πολωνικής DPA, τα στοιχεία επικοινωνίας του ΥΠΔ πρέπει να είναι εύκολα προσβάσιμα και σε εμφανές μέρος. Παράλληλα, προβλέπεται, η δυνατότητα ορισμού ενός ατόμου, που θα αντικαθιστά τον ΥΠΔ, κατά την απουσία του (π.χ. προσωρινή απουσία). Ωστόσο, είναι απαραίτητο, να ενημερωθεί, η πολωνική DPA, σχετικά με τα στοιχεία και του αντικαταστάτη. Όλοι οι κανόνες, που ισχύουν για τον ΥΠΔ, θα ισχύουν και για το πρόσωπο, που θα τον αναπληρώνει. Εφόσον, ένα άτομο έχει ορισθεί, ως «Information Security Officer» (ABI), υπό τον προηγούμενο νόμο, αυτομάτως, το άτομο αυτό θα αναλάμβανε, το ρόλο του ΥΠΔ, υπό την προϋπόθεση, ότι ο ορισμός θα ανακοινώνονταν

16. DLA PIPER, «Data Protection laws of the world», Holland-DPO.

17. DLA PIPER, «Data Protection laws of the world», Poland-DPO.

στον «President of the Office» μέχρι τον Σεπτέμβριο του 2018. Εφόσον συνέβαινε αυτό, έπειτα, θα εξακολουθούσε να απασχολείται ως ΥΠΔ. Εάν ο υπεύθυνος επεξεργασίας δεδομένων, είναι υποχρεωμένος να ορίσει ΥΠΔ, υπό το άρθρο 37 του Κανονισμού και δεν είχε ορίσει, υπό τον προηγούμενο εθνικό νόμο, θα έπρεπε να είχε ορίσει ΥΠΔ, και να κοινοποιήσει τα στοιχεία του, στον «President of the Office», μέχρι τις 31 Ιουλίου, 2018. Τίθεται δηλαδή χρονικός περιορισμός, ορισμού ΥΠΔ από την εθνική Αρχή.

Στην **Πορτογαλία**, ο νόμος για την προστασία των δεδομένων προσωπικού χαρακτήρα δεν προβλέπει, την απαίτηση ορισμού των υπευθύνων προστασίας δεδομένων. Ως εκ τούτου, μέχρι την ημερομηνία εφαρμογής του GDPR, οι οργανισμοί δεν ήταν υποχρεωμένοι να ορίζουν υπεύθυνο προστασίας δεδομένων.[18] Ωστόσο, μετά την εφαρμογή, του GDPR, ο ορισμός ΥΠΔ κατέστη επιβεβλημένος, υπό τις προϋποθέσεις, που προβλέπονται στον εν λόγω Κανονισμό. Σύμφωνα με την πρόταση του εθνικού νόμου: α) ο ΥΠΔ ορίζεται βάσει επαγγελματικών προσόντων και εξειδικευμένων γνώσεων, που έχει, σχετικά με το δίκαιο και τις πρακτικές προστασίας των δεδομένων και την ικανότητα εκπλήρωσης των νομικών του καθηκόντων (δεν απαιτείται επαγγελματική πιστοποίηση για τους σκοπούς αυτούς), β) ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία, ορίζει ΥΠΔ, σε κάθε περίπτωση, κατά την οποία η βασική δραστηριότητα τους : i) συνίσταται σε πράξεις επεξεργασίας που, λόγω της φύσης τους, του πεδίου εφαρμογής ή των σκοπών τους, απαιτούν τακτική και συστηματική παρακολούθηση των δεδομένων, σε μεγάλη κλίμακα ή ii) συνίσταται στην επεξεργασία σε μεγάλη κλίμακα ειδικών κατηγοριών δεδομένων ή δεδομένων προσωπικού χαρακτήρα, που αφορούν ποινικές καταδίκες και αξιόποινες πράξεις. Για τους σκοπούς της υποχρεωτικής κοινοποίησης του ορισμού του ΥΠΔ, στην εποπτική

18. DLA PIPER, «Data Protection laws of the world», Portugal-DPO.

αρχή, στο πλαίσιο του άρθρου 37 παράγραφος 7 του GDPR, η εποπτική αρχή, καθόρισε την εφαρμοστέα διαδικασία κοινοποίησης. Θα πρέπει, επομένως, να συμπληρωθεί και να υποβληθεί ηλεκτρονικά, ένα συγκεκριμένο έντυπο που θα διατίθεται από την εποπτική αρχή, στην ιστοσελίδα της.[19]

Στη **Ρουμανία**, εκτός από τις απαιτήσεις, που προβλέπονται από το GDPR, στα άρθρα 37 έως 39, ο νόμος 190/2018 προβλέπει ότι, ΥΠΔ, πρέπει να ορίζεται κάθε φορά που ο φορέας, που ενεργεί ως υπεύθυνος επεξεργασίας, επεξεργάζεται έναν εθνικό αριθμό αναγνώρισης, συμπεριλαμβανομένης της συλλογής ή της επεξεργασίας εγγράφων, που φέρουν τον εν λόγω εθνικό αριθμό αναγνώρισης, όταν η επεξεργασία είναι αναγκαία για τους σκοπούς και τα έννομα συμφέροντα που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, σύμφωνα με τις διατάξεις του άρθρου 6 παράγραφος 1 στοιχείο στ' του GDPR.[20]

Στην **Σλοβενία**, δεν έχει ακόμα εφαρμοσθεί εσωτερικός νόμος. Στις 6 Μαρτίου 2019, όμως, το Υπουργείο Δικαιοσύνης της Σλοβενίας, δημοσίευσε ένα σχέδιο νόμου για την προστασία των προσωπικών δεδομένων. Βάσει του σχεδίου, απαιτείται ο ΥΠΔ να έχει τουλάχιστον τριετή επαγγελματική πείρα, που θα αποδεικνύεται από τις δηλώσεις των υπαλλήλων του.[21] Εναλλακτικά, ο ΥΠΔ θα μπορεί να υποβάλει εθνικά ή διεθνή πιστοποιητικά σχετικά με τη γνώση και την εκπαίδευση του, στον τομέα της προστασίας δεδομένων. Δεν είναι σαφές, ακόμα, εάν η τριετής επαγγελματική πείρα μπορεί επίσης, να αποδειχθεί από οργανισμούς, με τους οποίους συνεργάστηκε ο ΥΠΔ με σύμβαση διαφορετική από σύμβαση εργασίας (π.χ. ως ανεξάρτητος σύμβουλος).

19.Το έντυπο διατίθεται στην ιστοσελίδα <https://www.cnpd.pt/DPO/DPOiniciar.aspx>.

20.DLA PIPER, «Data Protection laws of the world», Romania-DPO.

21.Euro Cloud Europe, 19/03/2019, «Data Protection Officers under Slovenia's Draft Personal Data Protection Act(ZVOP-2)».

Σύμφωνα με το σχέδιο, ο ΥΠΔ ενός κρατικού φορέα (ο όρος κρατικός φορέας δεν σχετίζεται με κάθε οργανισμό του δημόσιου τομέα) θα πρέπει να απασχολείται στον δημόσιο τομέα, όχι όμως κατ 'ανάγκη στον κρατικό φορέα, που τον έχει ορίσει ως ΥΠΔ, υπό τη ρητή εξαίρεση, των υπουργείων, όπου ο ΥΠΔ, θα πρέπει να απασχολείται από το εν λόγω υπουργείο που τον όρισε ή από έναν από τους φορείς του υπουργείου. Άλλοι φορείς και οργανισμοί του δημόσιου τομέα, θα μπορούν να ορίσουν ΥΠΔ, που δεν απασχολείται στον δημόσιο τομέα, αλλά μόνο αν δεν μπορούν να βρουν κατάλληλο πρόσωπο που απασχολείται στον δημόσιο τομέα.

Μια άλλη απόκλιση από τον Γενικό Κανονισμό, είναι η δυνατότητα για τους υπεύθυνους επεξεργασίας και τους εκτελούντες, να ορίσουν έναν αναπληρωτή ΥΠΔ για την ώρα της απουσίας του ΥΠΔ. Δεν καθορίζονται, όμως, απαιτήσεις σχετικά με την επαγγελματική πείρα, του αναπληρωτή-ΥΠΔ.

Τέλος, προκειμένου να διευκολυνθεί η άσκηση των δικαιωμάτων των ατόμων, το σχέδιο νόμου, προτρέπει επίσης, να δημοσιευθούν τα ονόματα των ΥΠΔ, μαζί με τα ονόματα των αντίστοιχων υπευθύνων επεξεργασίας και εκτελούντων την επεξεργασία, στην ιστοσελίδα της Αρχής Προστασίας Δεδομένων της Σλοβενίας.

Στην **Ισπανία**, ο εθνικός νόμος «NLOPD», περιλαμβάνει έναν μακροσκελή κατάλογο, οργανώσεων και εταιρειών, που καλούνται να ορίσουν ΥΠΔ.[22] Κατά συνέπεια, οι ασφαλιστικές ή αντασφαλιστικές εταιρείες, τα χρηματοπιστωτικά πιστωτικά ιδρύματα, τα εκπαιδευτικά ιδρύματα, οι διανομείς ηλεκτρικού και φυσικού αερίου, καθώς και οι εταιρείες διαφήμισης και εμπορίου, μεταξύ άλλων, καλούνται να ορίσουν έναν ΥΠΔ. Ο εθνικός νόμος, προβλέπει επίσης, τη δυνατότητα, οι οργανισμοί και οι εταιρείες, να ορίζουν οικειοθελώς, έναν ΥΠΔ. Σε κάθε περίπτωση, ο

22. DLAPIPER, «Data Protection laws of the world», Spain-DPO.

ορισμός του ΥΠΔ πρέπει να κοινοποιείται στην Εποπτική Αρχή «AEPD».

Στην **Σουηδία**, δεν προβλέπονται παρεκκλίσεις, εκτός του ότι ο Σουηδικός νόμος που αφορά την πρόσβαση σε πληροφορίες και το απόρρητο (2009: 400), εφαρμόζεται όσον αφορά, την υποχρέωση περί εμπιστευτικότητας και τήρησης απορρήτου, του ΥΠΔ στο δημόσιο τομέα, αντί του άρθρου 37 του GDPR.[23]

Οι περισσότεροι από τους αντίστοιχους νόμους, περί προστασίας δεδομένων εκτός Ευρώπης, δεν κάνουν ρητή αναφορά στην ανάγκη ορισμού ΥΠΔ. Ωστόσο, ορισμένες Αρχές προστασίας δεδομένων, επισημαίνουν ότι, ο διορισμός ενός ΥΠΔ, μπορεί να αποτελέσει καίριο στοιχείο απόδειξης, σεβασμού των προσωπικών δεδομένων και συμμόρφωσης με τις αρχές προστασίας δεδομένων, στα πλαίσια της εφαρμογής της αρχής της λογοδοσίας.

23. DLA PIPER, «Data Protection laws of the world», Sweden-DPO.

4.Ο ΥΠΟΧΡΕΩΤΙΚΟΣ ΔΙΟΡΙΣΜΟΣ ΥΠΔ ΣΤΟΝ ΓΚΠΔ

Στο άρθρο 37, του ΓΚΠΔ προβλέπονται, οι περιπτώσεις εκείνες, στις οποίες είναι υποχρεωτικός, ο ορισμός ΥΠΔ, από τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Οι περιπτώσεις αυτές είναι τρείς. Ειδικότερα, οι υπεύθυνοι επεξεργασίας και εκτελούντες την επεξεργασία, υποχρεούνται να ορίσουν ΥΠΔ:

1)όταν η επεξεργασία προσωπικών δεδομένων, διενεργείται από δημόσια αρχή ή φορέα, με εξαίρεση των δικαστηρίων, όταν ενεργούν υπό τη δικαιοδοτική τους αρμοδιότητα.

2)όταν οι βασικές δραστηριότητές του υπευθύνου ή εκτελούντος την επεξεργασία, αφορούν επεξεργασία δεδομένων που απαιτούν τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων, σε μεγάλη κλίμακα

3)όταν οι βασικές δραστηριότητες του υπευθύνου ή εκτελούντος την επεξεργασία, αφορούν την επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα και δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα.

Σημειώνεται, ότι το δίκαιο της Ένωσης ή των κρατών μελών είναι δυνατόν να επιβάλλει, τον υποχρεωτικό ορισμό υπευθύνου προστασίας δεδομένων και σε άλλες περιπτώσεις.

Στον εθνικό εφαρμοστικό νόμο, παρόλο που δίνεται η ευχέρεια από τον ευρωπαίο νομοθέτη, τα κράτη μέλη στο πλαίσιο της δικαιοδοτικής τους αρμοδιότητας, να προβλέψουν επιπλέον περιπτώσεις περί επιβολής του ΥΠΔ, εκτός του άρθρου 37 του ΓΚΠΔ, παρατηρείται ότι δεν αξιοποιήθηκε αυτή η δυνατότητα και ο έλληνας νομοθέτης περιορίστηκε στην ανάλυση του ορισμού ΥΠΔ, μόνο στο δημόσιο τομέα.

Ο υποχρεωτικός διορισμός ΥΠΔ, προβλέπεται και στο άρθρο 32 της Οδηγίας (ΕΕ) 2016/680, εκτός του ΓΚΠΔ, σύμφωνα με το οποίο ο υπεύθυνος επεξεργασίας, διορίζει ΥΠΔ, με τη δυνατότητα εξαίρεσης από αυτή την υποχρέωση, των δικαστηρίων και άλλων ανεξάρτητων αρχών, όταν ενεργούν υπό τη δικαιοδοτική τους αρμοδιότητα.

Ο ορισμός του ΥΠΔ μπορεί να γίνει και σε εθελοντική βάση, οπότε και σε αυτή την περίπτωση, θα ισχύουν οι ίδιες απαιτήσεις και προϋποθέσεις, ως εάν ο ορισμός να ήταν υποχρεωτικός.

Με εξαίρεση την περίπτωση, που είναι προφανές, ότι δεν απαιτείται από έναν οργανισμό να ορίσει ΥΠΔ, η Ομάδα Εργασίας, του άρθρου 29 συνιστά, οι υπεύθυνοι επεξεργασίας δεδομένων και οι εκτελούντες την επεξεργασία, να τεκμηριώσουν την απόφαση να μην διορίσουν ΥΠΔ, διεξάγοντας εσωτερική ανάλυση και έρευνα για να προσδιορίσουν, εάν κρίνεται απαραίτητος για τον οργανισμό. Θα πρέπει να σημειωθεί, ότι δεν χρειάζεται να διορίσουν έναν ΥΠΔ, τον οποίο θα απασχολούν κατά αποκλειστικότητα. Υπάρχει η δυνατότητα, ένας οργανισμός, να «μοιράζεται» τον ΥΠΔ με έτερους οργανισμούς. Αυτό θα συμβεί για παράδειγμα, εάν επιλέγει ως ΥΠΔ, ένας τρίτος, ανεξάρτητος πάροχος υπηρεσιών, ήτοι μια εξειδικευμένη συμβουλευτική ή νομική εταιρεία, της οποίας ο ρόλος θα είναι να παρέχει συμβουλές σε οργανισμούς για την επίτευξη της συμμόρφωσης τους με τις απαιτήσεις του ΓΚΠΔ.

Σε κάθε περίπτωση, οι οργανισμοί θα πρέπει να λαμβάνουν υπόψη ορισμένους παράγοντες, για να αποφασίσουν αν θα διορίσουν ΥΠΔ, όπως το μέγεθος του [24] οργα-

---

24. Cryan Michael, 3/07/2018,«Do small businesses need to appoint a DPO under GDPR?», Το μέγεθος και η δομή μιας εταιρίας δεν την αποκλείουν,αυτομάτως από την υποχρέωση ορισμού ΥΠΔ. Εάν μια εταιρεία ανεξάρτητα από το μέγεθός της, επεξεργάζεται ειδικές κατηγορίες δεδομένων, υπάρχει υποχρέωση για ορισμό ΥΠΔ. Συνιστάται η διοίκηση μιας εταιρείας να διεξάγει μια εσωτερική ανάλυση, από όπου θα μπορεί να προσδιορισθεί και η φύση των δεδομένων, που υποβάλλονται σε επεξεργασία, ώστε να καθορισθεί, εάν απαιτείται ΥΠΔ.

νισμού, την πολυπλοκότητα των δεδομένων που επεξεργάζεται και σε ποια κλίμακα διεξάγεται η επεξεργασία αυτή, την ποσότητα των προσωπικών πληροφοριών που διαχειρίζεται, τον ευαίσθητο χαρακτήρα των δεδομένων και την προστασία που απαιτείται για την επεξεργασία αυτών.

Ειδικότερα, οι τρεις επιμέρους περιπτώσεις, υποχρεωτικότητας ορισμού ΥΠΔ, στο ΓΚΠΔ:

Ι) ΟΙ ΔΗΜΟΣΙΕΣ ΑΡΧΕΣ Ή ΦΟΡΕΙΣ

Στο ΓΚΠΔ δεν διευκρινίζεται, ποιες ακριβώς, είναι οι δημόσιες αρχές ή φορείς, οι οποίοι οφείλουν να συμμορφωθούν με τις επιταγές του άρθρου 37 του Κανονισμού. Σύμφωνα με την ομάδα του άρθρου 29, ο καθορισμός των δημόσιων αρχών και φορέων, εναπόκειται στη δικαιοδοτική εξουσία, του κάθε κράτους.[25,26] Παράλληλα, αναφέρεται ότι ως δημόσιες αρχές νοούνται, οι εθνικές, περιφερειακές καθώς και οι τοπικές αρχές.

Στον πρόσφατα ψηφισθέντα εθνικό Νόμο 4624/2029, για την Προστασία Προσωπικών Δεδομένων, στο άρθρο 4 περ. α' ορίζεται ότι «δημόσιος φορέας» είναι: «οι δημόσιες αρχές, οι ανεξάρτητες και ρυθμιστικές διοικητικές αρχές, τα νομικά πρόσωπα δημοσίου δικαίου, οι οργανισμοί τοπικής αυτοδιοίκησης πρώτου και δεύτε-

25. Στην Ισλανδία,ο ορισμός της δημόσιας αρχής ή οργανισμού, προκύπτει από το νόμο37/1993,περί διοικητικών διαδικασιώνάρ.1. Ο όρος δημόσια αρχή αναφέρεται σε όλα τα μέρη, τα θεσμικά όργανα, τις επιτροπές κλπ. που διέπονται από το κράτος και τη τοπική κυβέρνηση. Είναι επιθυμητό, οι εταιρείες, που έχουν αναλάβει ορισμένα έργα, για το δημόσιο συμφέρον να ορίσουν ΥΠΔ, για τα έργα αυτά.

26. Στην Ιταλία, οι δημόσιες αρχές και οι φορείς που είναι υποχρεωμένοι να ορίσουν ΥΠΔ είναι αυτοί που απαριθμούνται στα άρθρα 18-22 του ιταλικού κώδικα προστασίας δεδομένων, όπως: η κρατική διοίκηση, οι εθνικές, περιφερειακές, τοπικές μη κερδοσκοπικοί οργανισμοί, περιφερειακές ή τοπικές Αρχές, Πανεπιστήμια, Εθνικοί φορείς υγείας, ανεξάρτητες Αρχές, Εμπορικά Επιμελητήρια, βιομηχανίες.

ρου βαθμού και τα νομικά πρόσωπα και οι επιχειρήσεις αυτών, οι κρατικές ή δημόσιες επιχειρήσεις και οργανισμοί, τα νομικά πρόσωπα ιδιωτικού δικαίου που ανήκουν στο κράτος ή επιχορηγούνται κατά 50% τουλάχιστον του ετήσιου προϋπολογισμού τους ή η διοίκησή τους ορίζεται από αυτό.»

Η μοναδική εξαίρεση, που εισάγεται στον Κανονισμό, από την υποχρέωση ορισμού ΥΠΔ, αφορά τα κατά τόπους δικαστήρια, όπως προβλέπονταν και στην Οδηγία(ΕΕ) 2016/680, στο πλαίσιο ενάσκησης της δικαιοδοτικής τους αρμοδιότητος. Το ίδιο προβλέπεται και στον εθνικό Νόμο 4624/2019, στο άρθρο 8 παρ.2. Έτσι, μπορεί να εξαχθεί το συμπέρασμα ότι, οι Γραμματείες των Δικαστηρίων, οφείλουν να έχουν ορίσει ΥΠΔ, διότι η αρχειοθέτηση, δεν αποτελεί δικαιοδοτική λειτουργία.

Στην Οδηγία(ΕΕ) 2016/680, αναφέρεται επιπρόσθετα, ότι ΥΠΔ οφείλουν να ορίζουν οι αρχές που εφαρμόζουν την αντεγκληματική πολιτική, ήτοι οι αστυνομικές αρχές, οι λιμενικές κλπ.

Εκτός των ανωτέρω, δημόσιοι φορείς θεωρούνται και φορείς ιδιωτικού δικαίου, που έχουν αναλάβει δημόσιες αρμοδιότητες. Τέτοιοι φορείς, σύμφωνα με την Ομάδα του άρθρου 29[27] είναι αυτοί, που παρέχουν υπηρεσίες δημόσιων μεταφορών, υπηρεσίες ύδρευσης, παροχής ενέργειας, υπηρεσίες οδικών υποδομών, η δημόσια ραδιοτηλεόραση, η κατασκευή εργατικών κατοικιών π.χ. ΟΛΠ, ΣΤΑΣΥ, ΕΥΔΑΠ, ΔΕΔΔΗΕ, ΕΡΤ, ΔΣΘ, ΤΕΕ. Ο λόγος που η υποχρέωση ορισμού ΥΠΔ, επεκτείνεται και σε αυτούς τους φορείς, είναι το γεγονός ότι μπορεί να επεξεργάζονται προσωπικά δεδομένα, υποκειμένων κατά τον ίδιο τρόπο, που πράττει και μία δημόσια αρχή ή φορέας, με αποτέλεσμα το υποκείμενο να μπορεί να βρεθεί σε παρόμοια θέση, όπως όταν η επεξεργασία διεξάγεται από δημόσιους φορείς.

27. Κατευθυντήριες γραμμές για ΥΠΔ, της Ομάδας Εργασίας του άρθρου 29, σελ. 8.

Η Ομάδα Εργασίας του άρθρου 29, για τον ορισμό της έννοιας του δημόσιου φορέα, παραπέμπει στην Οδηγία 2003/98/ΕΚ, όπου στο άρθρο 2 παράγραφος 1 και 2 αναφέρεται το εξής: «Ως φορείς του δημοσίου τομέα, νοούνται οι κρατικές, περιφερειακές, οι τοπικές αρχές, οι οργανισμοί δημοσίου δικαίου και οι ενώσεις οι σχηματιζόμενες από μία ή περισσότερες από τις αρχές αυτές ή από έναν ή περισσότερους από τους εν λόγω οργανισμούς δημοσίου δικαίου. Ως «οργανισμός δημοσίου δικαίου»: νοείται κάθε οργανισμός: α) που έχει συσταθεί με συγκεκριμένο σκοπό την κάλυψη αναγκών γενικού συμφέροντος που δεν έχουν βιομηχανικό ή εμπορικό χαρακτήρα, και β) που έχει νομική προσωπικότητα, και γ) του οποίου, είτε η δραστηριότητα χρηματοδοτείται κατά κύριο λόγο από το κράτος, τις περιφερειακές ή τοπικές αρχές ή άλλους οργανισμούς δημοσίου δικαίου· είτε η διαχείρισή του υπόκειται στην εποπτεία των ανωτέρω· είτε διοικείται, διευθύνεται ή εποπτεύεται από όργανο του οποίου περισσότερα από τα μισά μέλη διορίζονται από το κράτος, τις περιφερειακές ή τοπικές αρχές, ή άλλους οργανισμούς δημοσίου δικαίου.»

Ο καθορισμός του τρόπου και του σκοπού της επεξεργασίας γίνεται, από τον εκάστοτε υπεύθυνο επεξεργασίας. Έτσι, εφόσον, ο υπεύθυνος εξεργασίας, ορίζει το σκοπό και τον τρόπο, που θα γίνεται η επεξεργασία δεδομένων σε ένα συγκεκριμένο τμήμα ή μία διεύθυνση, σκόπιμο θα ήταν γι αυτό το συγκεκριμένο τμήμα να ορίζεται και ένας ΥΠΔ, και όχι ένας ΥΠΔ, για ολόκληρη την δημόσια αρχή ή φορέα.[28]

Το γεγονός ότι, μία αρχή ή φορέας εντάσσεται στον ευρύτερο χώρο του δημοσίου, δε σημαίνει ότι, ένας μόνο ΥΠΔ, θα οριστεί για όλο το δημόσιο τομέα. Ένα

28. Σωτηρόπουλος Βασίλης, 2017, «Υπεύθυνος Προστασίας Δεδομένων-Εργαλειοθήκη για τον νέο θεσμό σε δημόσιο και ιδιωτικό τομέα», Εκδόσεις Σάκκουλα, σελ. 85-86.

χρήσιμο αντίστοιχο παράδειγμα, αποτελεί η Ευρωπαϊκή Επιτροπή, που έχει ορίσει έναν συντονιστή ΥΠΔ, για κάθε Γενική Διεύθυνση της και έναν ΥΠΔ σε κεντρικό επίπεδο.

Εντούτοις, στο άρθρο 37 του ΓΚΠΔ στην παρ. 3, αναφέρεται ρητά ότι εάν ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία προσωπικών δεδομένων είναι δημόσια αρχή ή δημόσιος φορέας, ένας μόνο ΥΠΔ μπορεί να ορίζεται, για πολλές τέτοιες αρχές ή πολλούς τέτοιους φορείς, λαμβάνοντας υπόψη την οργανωτική δομή και το μέγεθός τους. Αυτό που θα πρέπει, να εξασφαλίζεται είναι η εύκολη και άμεση προσβασιμότητα των ενδιαφερόμενων υποκειμένων, στον ΥΠΔ .

Η ίδια πρόβλεψη συμπεριλαμβάνεται στον εθνικό εφαρμοστικό του ΓΚΠΔ, Νόμο 4624/2019 για τα Προσωπικά Δεδομένα, στο άρθρο 6 παρ. 2, υπό τη ρητή προϋπόθεση ότι θα λαμβάνεται, πάντοτε υπόψη η οργανωτική δομή και το μέγεθος των δημοσίων φορέων.

ΙΙ) ΟΝΤΟΤΗΤΕΣ ΠΟΥ ΔΙΕΞΑΓΟΥΝ ΤΑΚΤΙΚΗ ΚΑΙ ΣΥΣΤΗΜΑΤΙΚΗ ΠΑΡΚΟΛΟΥΘΗΣΗ ΣΕ ΜΕΓΑΛΗ ΚΛΙΜΑΚΑ

Η δεύτερη κατηγορία στην οποία προβλέπεται η υποχρεωτικότητα ορισμού ΥΠΔ, αφορά τον ιδιωτικό τομέα. Ειδικότερα, οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία, που οι βασικές τους δραστηριότητες, συνίστανται στην επεξεργασία προσωπικών δεδομένων, που απαιτούν τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων, οφείλουν να ορίσουν ΥΠΔ.

Η θέσπιση της υποχρεωτικότητας, περί ορισμού ΥΠΔ και στον ιδιωτικό τομέα, αποτελεί μια καινοτόμα διάταξη, που εισάγεται με τον Γενικό Κανονισμό. Αρχικά, είχε

προταθεί από την Ευρωπαϊκή Επιτροπή, η επιβολή της υποχρέωσης ορισμού ΥΠΔ, σε υπευθύνους επεξεργασίας, που απασχολούν, περισσότερους των 250 εργαζομένων, πρόβλεψη που απαλείφθηκε από το τελικό κείμενο του Κανονισμού.

Σύμφωνα με την από 6.5.2003 Σύσταση της Επιτροπής, την οποία προφανώς έλαβε υπόψη στην πρόταση της ,πολύ μικρές, μικρές και μεσαίες είναι οι επιχειρήσεις, που απασχολούν λιγότερους από 250 εργαζομένους και ο ετήσιος κύκλος εργασιών τους, δεν υπερβαίνει τα 50 εκατομμύρια ευρώ ή το σύνολο του ισολογισμού τους, δεν υπερβαίνει τα 43 εκατομμύρια ευρώ.[29] Στον Κανονισμό, εν τέλει ο αριθμός των 250 εργαζομένων, εμφανίζεται ως το όριο, βάσει του οποίου καθορίζεται ποιες επιχειρήσεις, έχουν υποχρέωση να τηρούνε αρχείο των δραστηριοτήτων επεξεργασίας, στις οποίες προβαίνουν (α. 30 παρ.5 ΓΚΠΔ). Ο αριθμός των απασχολούμενων εργαζομένων σε μία επιχείρηση, δεν αποτελεί, στον Γενικό Κανονισμό, κριτήριο για τον ορισμό ΥΠΔ, όπως αντίθετα προβλέπεται στην Γερμανία.

Σκόπιμο είναι να αναφερθεί και να τονισθεί το γεγονός, ότι οι οντότητες του ιδιωτικού τομέα, που υποχρεώνονται να ορίσουν ΥΠΔ, θα πρέπει να ασκούν ως <u>βασική και κύρια δραστηριότητα</u>, την επεξεργασία δεδομένων προσωπικού χαρακτήρα, που απαιτεί την τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων και όχι, ως παρεπόμενη και δευτερεύουσα.

Η Ομάδα Εργασίας του άρθρου 29, στις κατευθυντήριες γραμμές για τους ΥΠΔ, αναφέρει ότι ως <u>βασικές δραστηριότητες</u> θα πρέπει να θεωρηθούν, οι πράξεις αυτές, που είναι καθοριστικές και αναγκαίες για την επίτευξη των στόχων του υπευθύνου και του εκτελούντος την επεξεργασία. Στις βασικές δραστηριότητες, εντάσσονται και αυτές που αποτελούν αναπόσπαστο μέρος, της δραστηριότητας του

29. 2003/361/ΕΚ Σύσταση της Επιτροπής της 6ης Μαΐου 2003, σχετικά με τον ορισμό των πολύ μικρών, των μικρών και των μεσαίων επιχειρήσεων.

υπευθύνου και του εκτελούντος την επεξεργασία. Ως παράδειγμα, αναφέρεται από την Ομάδα Εργασίας του άρθρου 29, το νοσοκομείο, βασική δραστηριότητα του οποίου είναι η παροχή υγειονομικής περίθαλψης.[30] Ωστόσο, για να εκτελεί αποτελεσματικά αυτή τη δραστηριότητα, θα πρέπει να επεξεργάζεται, τα ιατρικά δεδομένα των ασθενών. Η επεξεργασία αυτή, θεωρείται βασική και καίρια, για την ορθή λειτουργία του νοσοκομείου, επομένως, τα νοσοκομεία υποχρεούνται να διορίσουν ΥΠΔ.

Ένα πρόσθετο παράδειγμα που επικαλείται η Ομάδα Εργασίας του άρθρου 29, είναι αυτό των εταιρειών που παρέχουν υπηρεσίες φύλαξης, ιδιωτικών και δημόσιων χώρων, οι οποίες ως βασική δραστηριότητα, έχουν τη φύλαξη των χώρων αυτών. Η δραστηριότητα αυτή, όμως είναι άρρηκτα συνδεδεμένη με την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Υπάρχουν και δραστηριότητες, που τελούνται στο πλαίσιο αρκετών οργανισμών, όπως για παράδειγμα, η επεξεργασία δεδομένων για την καταβολή της μισθοδοσίας των υπαλλήλων τους, οι οποίες κρίνονται αναγκαίες για την υποστήριξη της βασικής δραστηριότητα της οντότητας. Οι δραστηριότητες αυτές, όμως θεωρούνται δευτερεύουσες, παρεπόμενες και όχι βασικές και έτσι, δεν κρίνεται απαραίτητος ο ορισμός ΥΠΔ. Εάν, όμως, η μισθοδοσία έχει ανατεθεί σε άλλη επιχείρηση μηχανοργάνωσης, η οποία έχει ως κύρια και βασική δραστηριότητα την επεξεργασία δεδομένων, τότε θα πρέπει να ορίσει ΥΠΔ.

Ένας άλλος όρος, που χρήζει διευκρινίσεως, είναι αυτός της «μεγάλης κλίμακας», στην οποία διεξάγεται, επεξεργασία των προσωπικών δεδομένων, ώστε να επιτάσσεται ο ορισμός ΥΠΔ. Από το ΓΚΠΔ δεν διευκρινίζεται σε τι συνίσταται η επεξε-

30. Κατευθυντήριες γραμμές για ΥΠΔ, της Ομάδας Εργασίας του άρθρου 29,σελ. 9.

ργασία προσωπικών δεδομένων, σε μεγάλη κλίμακα.

Δεν έχει προβλεφθεί κάποιο ποσοτικό κριτήριο, ούτε σχετικά με τα εν δυνάμει εμπλεκόμενα πρόσωπα, ούτε σχετικά με την ποσότητα των δεδομένων, που υπόκεινται σε επεξεργασία, ώστε να υπάρχει ένα κοινό κριτήριο, που να μπορεί να εφαρμοσθεί σε όλες τις περιπτώσεις. Από την πρακτική εφαρμογή επισημαίνει, η Ομάδα του άρθρου 29 «Στις κατευθυντήριες Γραμμές για τους ΥΠΔ», μπορούν να αναπτυχθούν πρότυπα και κριτήρια.

Η Ομάδα Εργασίας του άρθρου 29, βέβαια, έχει προβλέψει ορισμένους παράγοντες, που δύνανται να παίξουν καθοριστικό ρόλο, στον καθορισμό, του αν μία επεξεργασία, διεξάγεται σε **μεγάλη κλίμακα** :

Α) ο αριθμός των εμπλεκόμενων υποκειμένων των δεδομένων, είτε ως συγκεκριμένος αριθμός είτε ως ποσοστό επί του συναφούς πληθυσμού,
Β) ο όγκος των δεδομένων και/ή το εύρος των διαφόρων στοιχείων δεδομένων που υφίστανται επεξεργασία,
Γ) η διάρκεια ή ο μόνιμος χαρακτήρας της δραστηριότητας επεξεργασίας δεδομένων,
Δ) η γεωγραφική έκταση της δραστηριότητας επεξεργασίας.

Η ***Εσθονική Αρχή Προστασίας Δεδομένων*** εξέδωσε κατευθυντήριες γραμμές σχετικά με το πότε υφίσταται επεξεργασία σε «**μεγάλη κλίμακα**», η οποία θεμελιώνει, υποχρέωση ορισμού ΥΠΔ αλλά και διεξαγωγής εκτίμησης αντίκτυπου επεξεργασίας δεδομένων.[31] Επισημαίνει ότι, η επεξεργασία δεδομένων, διεξάγεται σε «μεγάλη κλίμακα» , όταν περιλαμβάνει:

1)Ειδικές κατηγορίες προσωπικών δεδομένων ή δεδομένων που αφορούν ποινικά

31. Cloud Privacy Check (CPC), 2/08/2018, «The Estonian data protection authority issued guidance on the definition of “large scale” processing».

αδικήματα, 5.000 και πλέον ατόμων,

2)Προσωπικά δεδομένα υψηλού κινδύνου 10.000 ατόμων και πλέον,

3)Άλλα προσωπικά δεδομένα 50.000 ατόμων και πλέον.

Οι προτάσεις αυτές, της Εσθονικής Αρχής Προστασίας Δεδομένων, σχετικά με τον ποσοτικό καθορισμό της «μεγάλης κλίμακας», προέκυψαν βάσει των ακόλουθων συλλογισμών:

1)Το ποσοτικό κριτήριο των 5.000 και πλέον ατόμων, που αφορά ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα ή προσωπικά δεδομένα σχετικά με ποινικά αδικήματα, βάσει της αιτιολογικής σκέψης 91, του GDPR.

Το εν λόγω άρθρο, προβλέπει ότι η επεξεργασία δεδομένων προσωπικού χαρακτήρα, δεν πρέπει να θεωρείται ότι διεξάγεται σε μεγάλη κλίμακα, όταν αφορά τα προσωπικά δεδομένα των ασθενών ενός ιδιώτη ιατρού ή άλλου επαγγελματία του τομέα υγείας. Στην Εσθονία, ιδιώτης ιατρός, είναι ο οικογενειακός ιατρός. Σύμφωνα με τον εκεί ισχύοντα νόμο, ο μέγιστος αριθμός ατόμων-ασθενών, που μπορεί να περιλαμβάνονται σε κατάλογο οικογενειακού ιατρού, μπορεί να είναι 2.000 άτομα. Το όριο των 5.000 ατόμων, περιλαμβάνει επομένως δύο με τρεις οικογενειακούς ιατρούς, με βάσει τα ισχύοντα, στην Εσθονία. Η αιτιολογική σκέψη, του άρθρου 91 του GDPR, αναφέρεται επίσης σε ιδιώτες δικηγόρους, αλλά δεν υπάρχουν αξιόπιστα στοιχεία σχετικά με τον ακριβή αριθμό πελατών, που μπορεί να έχει ένας ιδιώτης δικηγόρος. Διαφορετική, θα είναι, η αντιμετώπιση ιατρικού κέντρου, όπου είναι πολύ πιθανό, να υφίσταται επεξεργασία δεδομένων σε μεγάλη κλίμακα. Η Εσθονική Αρχή Προστασίας Δεδομένων, παρατήρησε ότι, τα όρια για κάποιες ειδικές κατηγορίες προσωπικών δεδομένων, στο GDPR, είναι αυστηρότερα από τον προηγούμενο, εθνικό νόμο για την προστασία των προσωπικών δεδομένων και αυτός είναι ο λόγος για τον οποίο, θεώρησε εύλογο το

όριο για ειδικές κατηγορίες προσωπικών δεδομένων, να είναι μικρότερο από αυτό που προβλέπεται, για άλλα πιο ευαίσθητα δεδομένα (δεδομένα υψηλού κινδύνου).

2) Το ποσοτικό κριτήριο των 10.000 και πλέον ατόμων που αφορά προσωπικά δεδομένα υψηλού κινδύνου, βάσει της αιτιολογικής σκέψης 75, του GDPR.

Η Εσθονική Αρχή Προστασίας Δεδομένων, επικαλείται τα ακόλουθα παραδείγματα, όπου μπορεί να υφίσταται επεξεργασία προσωπικών δεδομένων, υψηλού κινδύνου: **α)**την κλοπή ταυτότητας ή την πιθανή απάτη (ιδίως σε σχέση με υπηρεσίες ψηφιακής εμπιστοσύνης και παρόμοιες υπηρεσίες διαχείρισης ταυτότητας), **β)** τις οικονομικές απώλειες(ιδίως μέσω τραπεζικών και πιστωτικών καρτών), **γ)** την παραβίαση απορρήτου γραπτής συνομιλίας (ειδικά σε περίπτωση επικοινωνιακών υπηρεσιών), **δ)**την παρακολούθηση της θέσης ενός ατόμου σε πραγματικό χρόνο (ειδικά σε περίπτωση υπηρεσιών επικοινωνιών), **ε)**την παραβίαση του απορρήτου της οικονομικής κατάστασης ενός προσώπου (ιδίως των φορολογικών δεδομένων, των τραπεζικών δεδομένων και των δεδομένων αξιολόγησης πιστοληπτικής ικανότητας, ωστόσο, δεν περιλαμβάνει τη χρήση δημόσιων δεδομένων), **ζ)** τη διάκριση με νομικές συνέπειες ή ισοδύναμο αποτέλεσμα (συμπεριλαμβανομένων των υπηρεσιών για την τοποθέτηση θέσεων εργασίας και των υπηρεσιών αξιολόγησης που μπορούν να επηρεάσουν τις ευκαιρίες μισθών και σταδιοδρομίας), **η)**την επεξεργασία προσωπικών δεδομένων παιδιών (σε υπηρεσίες που απευθύνονται σε παιδιά), **θ)**την κοινοποίηση πληροφοριών που προστατεύονται από το απόρρητο, που πηγάζει απευθείας από το νόμο (πληροφορίες στις οποίες έχουν πρόσβαση, ελάχιστα άτομα, πληροφορίες που προστατεύονται από το επαγγελματικό απόρρητο).

Κατά τον καθορισμό του κατώτατου ορίου των 10.000 ατόμων, η Εσθονική Αρχή Προστασίας Δεδομένων, προφανώς έχει επηρεαστεί, από άλλες σημαντικές υπηρεσίες, στις οποίες χρησιμοποιείται, επίσης ως κριτήριο, το όριο των 10.000 ατόμων, στο εσθονικό δίκαιο, π.χ. στις καλωδιακές υπηρεσίες, στην υπηρεσία

διανομής ηλεκτρικής ενέργειας που παρέχεται ως ζωτικής σημασίας υπηρεσία, στην υπηρεσία δικτύου διανομής φυσικού αερίου, που παρέχεται ως ζωτικής σημασίας υπηρεσία, επίσης.

Η Ομάδα Εργασίας του άρθρου 29, στις Κατευθυντήριες Γραμμές για τους ΥΠΔ, που εξέδωσε, περιλαμβάνει ορισμένα παραδείγματα επεξεργασίας σε μεγάλη κλίμακα τα οποία είναι τα ακόλουθα:

• η επεξεργασία δεδομένων ασθενών στο πλαίσιο της συνήθους λειτουργίας ενός νοσοκομείου,

• η επεξεργασία δεδομένων μετακίνησης φυσικών προσώπων που χρησιμοποιούν το σύστημα δημόσιων μεταφορών μιας πόλης (π.χ., παρακολούθηση μέσω καρτών πολλαπλών διαδρομών)

• η επεξεργασία σε πραγματικό χρόνο δεδομένων γεωγραφικού εντοπισμού πελατών διεθνούς αλυσίδας ταχυφαγείων για στατιστικούς σκοπούς από εκτελούντα την επεξεργασία που ειδικεύεται στην παροχή τέτοιου είδους υπηρεσιών,

• η επεξεργασία δεδομένων πελατών στο πλαίσιο της συνήθους λειτουργίας μιας ασφαλιστικής εταιρίας η μιας τράπεζας ,

• η επεξεργασία δεδομένων προσωπικού χαρακτήρα για σκοπούς συμπεριφορικής διαφήμισης από μηχανή αναζήτησης,

• η επεξεργασία δεδομένων (περιεχόμενο, κίνηση, θέση) από παρόχους υπηρεσιών τηλεφωνίας ή διαδικτύου.

Παραδείγματα που **δεν** συνιστούν επεξεργασία μεγάλης κλίμακας είναι, μεταξύ άλλων, τα ακόλουθα, σύμφωνα πάλι με την Ομάδα Εργασίας του άρθρου 29:

•η επεξεργασία δεδομένων ασθενών από ιδιώτη ιατρό,

• η επεξεργασία δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα από ιδιώτη δικηγόρο.

Ένα άλλο στοιχείο που απαιτεί ο Κανονισμός, να εμφανίζουν οι οντότητες που υποχρεούνται να διορίσουν ΥΠΔ, είναι να διεξάγουν συστηματική και τακτική παρακολούθηση. Δεν αρκεί η μεγάλη κλίμακα, αλλά θα πρέπει παράλληλα, να συντρέχει και αυτό το στοιχείο επιπρόσθετα. Και στη δεδομένη περίπτωση, δεν ορίζεται από το ΓΚΠΔ, τι συνιστά την έννοια της τακτικής και συστηματικής παρακολούθησης.

Η Ομάδα Εργασίας του άρθρου 29, επιχειρεί να ερμηνεύσει τους όρους **τακτική και συστηματική** παρακολούθηση, στις κατευθυντήριες γραμμές που δίνει.

Συγκεκριμένα, η Ομάδα του άρθρου 29 δίδει στο επίθετο «**τακτική**» μία ή περισσότερες από τις ακόλουθες ερμηνείες:

1)η επεξεργασία προσωπικών δεδομένων, η οποία λαμβάνει χώρα, σε συνεχή βάση ή σε συγκεκριμένα χρονικά διαστήματα για συγκεκριμένη χρονική περίοδο,
2)η λαμβάνουσα χώρα τακτικά ή κατ' επανάληψη σε σταθερές χρονικές στιγμές,
3) η λαμβάνουσα χώρα αδιαλείπτως ή περιοδικά.

Η Ομάδα του άρθρου 29 δίδει στο επίθετο «**συστηματική**» μία ή περισσότερες από τις ακόλουθες ερμηνείες:

1) η επεξεργασία προσωπικών δεδομένων η οποία λαμβάνει χώρα, σύμφωνα με κάποιο σύστημα
2)η προκαθορισμένη, οργανωμένη ή μεθοδική,
3)η λαμβάνουσα χώρα στο πλαίσιο γενικότερου σχεδίου για τη συλλογή δεδομένων,
4) διενεργούμενη στο πλαίσιο στρατηγικής.

Ως παραδείγματα, τακτικής και συστηματικής παρακολούθησης, η Ομάδα Εργασίας του άρθρου 29, επικαλείται τη λειτουργία δικτύου τηλεπικοινωνιών, την παροχή υπηρεσιών τηλεπικοινωνιών, την προώθηση διαφημιστικών μηνυμάτων ηλεκτρονικού ταχυδρομείου, την προώθηση γενικώς προϊόντων, με τη χρήση

προσωπικών δεδομένων, τη διαμόρφωση προφίλ και βαθμολόγηση για σκοπούς εκτίμησης κινδύνου (π.χ. για σκοπούς βαθμολόγησης πιστοληπτικής ικανότητας), τον εντοπισμό τοποθεσίας, για παράδειγμα, μέσω εφαρμογών για κινητά τηλέφωνα, προγράμματα επιβράβευσης αφοσιωμένων πελατών, τη συμπεριφορική διαφήμιση, τη φυσική κατάσταση και την υγεία μέσω φορητών συσκευών κ.λπ.

Τα κριτήρια "τακτικής συστηματικής και μεγάλης κλίμακας", θα πρέπει να ισχύουν σωρευτικά, για την ενεργοποίηση του υποχρεωτικού διορισμού ενός ΥΠΔ.

III) ΟΝΤΟΤΗΤΕΣ ΠΟΥ ΕΠΕΞΕΡΓΑΖΟΝΤΑΙ ΜΕΓΑΛΗΣ ΚΛΙΜΑΚΑΣ ΕΥΑΙΣΘΗΤΑ ΔΕΔΟΜΕΝΑ

Η δεύτερη περίπτωση, οντοτήτων του ιδιωτικού τομέα, που θα πρέπει να ορίσει ΥΠΔ, είναι αυτή που έχει ως βασική δραστηριότητα, την επεξεργασία σε μεγάλη κλίμακα ειδικών κατηγοριών δεδομένων και δεδομένων που αφορούν σε ποινικές καταδίκες και αδικήματα.

Στο άρθρο 9 του ΓΚΠΔ, αναφέρονται οι ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα, η επεξεργασία των οποίων, σε μεγάλη κλίμακα απαιτεί τον ορισμό ΥΠΔ. Ειδικότερα, σε αυτά περιλαμβάνονται, αυτά που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και η επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων, με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένων που αφορούν την υγεία ή δεδομένων που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή το γενετήσιο προσανατολισμό του.

Στο άρθρο 10 του ΓΚΠΔ, προβλέπεται ότι χρήζουν αυξημένης προστασίας, τα δεδομένα που αφορούν ποινικές καταδίκες και αδικήματα, ως ειδικότερη κατηγορία δεδομένων.

Η Ομάδα Εργασίας του άρθρου 29, προβαίνει σε μία διευκρίνηση όσο αφορά, το συμπλεκτικό σύνδεσμο «και», ανάμεσα στις δύο κατηγορίες δεδομένων, ήτοι τις ειδικές κατηγορίες δεδομένων και των δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα, αναφέροντας ότι θα πρέπει να εκληφθεί ως διάζευξη. Δεν απαιτείται δηλαδή, η επεξεργασία και των δύο κατηγοριών δεδομένων ταυτόχρονα αλλά η επεξεργασία είτε της μίας είτε της άλλης κατηγορίας, ώστε να κριθεί απαραίτητος ο ορισμός ΥΠΔ.[32]

Ορισμένα παραδείγματα, της συγκεκριμένης κατηγορίας, οντοτήτων αποτελούν τα εξής: α) ΜΚΟ που ασχολούνται με θέματα μετανάστευσης ή προσφύγων ή με θέματα υγείας, β)Πολιτικά κόμματα, γ)Συνδικαλιστικές οργανώσεις κ.α.

Στο εθνικό εφαρμοστικό Νόμο 4624/2019, για τα Προσωπικά Δεδομένα, που πρόσφατα ψηφίσθηκε, στο άρθρο 22, προβλέπεται ότι κατά παρέκκλιση των οριζομένων στην παρ. 1 του άρθρου 9 του ΓΚΠΔ, θα είναι δυνατή η επεξεργασία των ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα, που αναφέρονται στο εν λόγω άρθρο, από δημόσιους και ιδιωτικούς φορείς υπό ορισμένους όρους και υπό την προϋπόθεση, ότι θα λαμβάνονται όλα τα κατάλληλα και ειδικά μέτρα διασφάλισης των θεμελιωδών δικαιωμάτων και ατομικών ελευθεριών των υποκειμένων των δεδομένων. Λαμβάνοντας υπόψη κάποιους παράγοντες, στην παράγραφο 3 του ίδιου άρθρου 22, αναφέρονται ενδεικτικά ορισμένα μέτρα διασφάλισης, που θα μπορούν να ληφθούν ανάμεσα στα οποία, περιλαμβάνεται ο ορισμός ΥΠΔ.

32. Κατευθυντήριες γραμμές για ΥΠΔ, της Ομάδας Εργασίας του άρθρου 29.

5.ΟΡΙΣΜΟΣ ΕΝΟΣ ΥΠΔ

Σύμφωνα με το άρθρο 37 του ΓΚΠΔ, ΥΠΔ υποχρεούται να διορίσει αναλόγως με το ποιος πληροί τα κριτήρια, είτε ο υπεύθυνος επεξεργασίας, είτε ο εκτελών την επεξεργασία. Αυτό συνεπάγεται, ότι σε περίπτωση που, ο υπεύθυνος επεξεργασίας, βάσει των προαπαιτούμενων, που ορίζει ο ΓΚΠΔ, οφείλει να ορίσει ΥΠΔ, δεν συνεπάγεται δίχως άλλο, ότι την ίδια υποχρέωση θα έχει και ο εκτελών την επεξεργασία, αν και σύμφωνα με την Ομάδα Εργασίας του άρθρου 29, θα κρίνονταν σκόπιμο, να γινόταν κάτι ανάλογο.

Επιπρόσθετα, στην περίπτωση των ομίλων επιχειρήσεων- εταιριών, στο άρθρο 37 παρ. 2 του ΓΚΠΔ, ορίζεται ότι, μπορεί να ορισθεί ένας μόνο ΥΠΔ, υπό την προϋπόθεση ότι, κάθε εγκατάσταση του ομίλου, θα έχει εύκολη πρόσβαση στον ΥΠΔ, ο οποίος καλείται να αποτελέσει δίαυλο επικοινωνίας, για τα υποκείμενα των δεδομένων, την εποπτική αρχή, τον υπεύθυνο επεξεργασίας και τον εκτελούντα.

Για να είναι εφικτή, η άμεση πρόσβαση στον ΥΠΔ θα πρέπει τα στοιχεία επικοινωνίας του, να είναι δημοσιευμένα, όπως απαιτεί ο ΓΚΠΔ στο άρθρο 37 παρ.7.

Χρήσιμο θα ήταν, τα στοιχεία του ΥΠΔ να αναρτώνται στην ιστοσελίδα της οντότητας, για λογαριασμό της οποίας έχει διορισθεί ο ΥΠΔ, καθώς επίσης, και σε όλους τους τηλεφωνικούς καταλόγους ή καταλόγους των προσώπων που υπηρετούν στην οντότητα, ώστε να καθίσταται πιο ευχερής, η εύρεση του, από όποιον το επιθυμεί. Δεν απαιτείται να δημοσιεύεται και το όνομα του ΥΠΔ, στα στοιχεία επικοινωνίας, αν και θα αποτελούσε μία καλή και χρήσιμη πρακτική.

Με τη συνδρομή και των συνεργατών του ΥΠΔ, όπου έχουν ορισθεί, θα πρέπει να εξασφαλίζεται και να είναι εγγυημένη, η αποτελεσματική επικοινωνία, με τα υποκείμενα των δεδομένων και η συνεργασία με τις αρμόδιες εποπτικέ αρχές.

Κρίσιμο θεωρείται, η επικοινωνία αυτή να διεξάγεται σε γλώσσα, η οποία θα είναι κατανοητή, από τις εποπτικές αρχές και τα υποκείμενα των δεδομένων.

Επιπρόσθετα των ανωτέρω, για επιπλέον ένα λόγο, τα στοιχεία επικοινωνίας του ΥΠΔ, κατά το άρθρο 37 παρ. 7, θα πρέπει να δημοσιεύονται και να καθίστανται προσιτά, για να υπάρχει η δυνατότητας άμεσης και εύκολης επικοινωνίας με τον ίδιο τον ΥΠΔ, χωρίς την παρεμβολή άλλων ατόμων. Έτσι, θα εξασφαλίζεται η εμπιστευτικότητα- μυστικότητα της επικοινωνίας, για να εξαλείφονται τυχόν δισταγμοί και αναστολές των υποκειμένων των δεδομένων, που θα υπήρχαν εξαιτίας, για παράδειγμα, της παρεμβολής τρίτων ατόμων, στην προσπάθεια επικοινωνίας με τον ΥΠΔ.

Σύμφωνα με την ΟΕ του α.29, ο ΥΠΔ θα πρέπει να είναι εγκατεστημένος εντός Ε.Ε. ανεξάρτητα από το εάν ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία, είναι εγκατεστημένοι στην Ε.Ε., προκειμένου να καθίσταται εφικτή η πρόσβαση σε αυτόν από όποιον το επιθυμεί.

Διάταγμα, που εκδόθηκε, στη Γαλλία σχετικά με τον ορισμό ΥΠΔ, επαναλαμβάνει την πρόβλεψη του Γενικού Κανονισμού, σύμφωνα με την οποία, πολλές επιχειρήσεις θα έχουν τη δυνατότητα να ορίσουν έναν μόνο ΥΠΔ.[33]

Στην παράγραφο 3 του ίδιου άρθρου (37), ορίζεται ακριβώς το ίδιο και για τις δημόσιες αρχές και φορείς, στις οποίες παρόλο το μέγεθος τους και τη δομή τους, θα μπορεί να διοριστεί, ένας υπεύθυνος προστασίας δεδομένων. Ο ίδιος, ο υπεύθυνος επεξεργασίας, ή ο εκτελών την επεξεργασία, θα πρέπει να διασφαλίζει, ότι ένας μόνος ΥΠΔ, για πολλούς δημόσιους φορείς και αρχές, θα μπορέσει να επιτελέσει αποτελεσμα-

33.Smith Reed, 12/2018, «Overview of the latest developments regarding the national implementation of the GDPR requirements», IP Tech & Data, General Data Protection Regulation.

τικά τα καθήκοντά του, έχοντας βέβαια τη συνδρομή ειδικής ομάδας, όπου απαιτείται και κρίνεται απαραίτητο.

Αλλά και στο άρθρο 6 παρ. 2 του εθνικού εφαρμοστικού Νόμου για τα Προσωπικά Δεδομένα, όπως προεκτέθηκε, αναφέρεται ότι ένας μόνο ΥΠΔ για περισσότερους δημόσιους φορείς θα ορίζεται λαμβανομένου πάντοτε υπόψη της οργανωτικής δομής και του μεγέθους τους. Επαναλαμβάνεται, λοιπόν αυτούσια η διάταξη του ΓΚΠΔ (37 παρ. 3).

Η ανωτέρω διάταξη επαναλαμβάνεται και στο άρθρο 32 παρ. 3 της Οδηγίας (ΕΕ) 2016/680,για τους ΥΠΔ των διωκτικών αρχών: « ένας μοναδικός υπεύθυνος προστασίας δεδομένων, μπορεί να διοριστεί για περισσότερες της μίας αρμόδιες αρχές, ανάλογα με την οργανωτική δομή και το μέγεθός τους».

Επομένως, εφόσον είναι εγγυημένη, η ανά πάσα στιγμή διαθεσιμότητα του ΥΠΔ και εξασφαλίζεται η άμεση και ανενόχλητη επικοινωνία μαζί του, τότε και όμιλοι επιχειρήσεων και δημόσιοι φορείς και αρχές θα μπορούν να ορίσουν ένα ΥΠΔ, εφόσον βέβαια έχουν ληφθεί προηγουμένως υπόψη παράγοντες, όπως η οργανωτική δομή και το μέγεθός τους.

6. ΠΡΟΣΟΝΤΑ ΚΑΙ ΔΕΞΙΟΤΗΤΕΣ ΔΙΟΡΙΣΜΟΥ ΥΠΔ/ ΠΙΣΤΟΠΟΙΗΣΕΙΣ

Στην παράγραφο 5 του άρθρου 37 του ΓΚΠΔ, γίνεται μνεία στα προσόντα και τις δεξιότητες τις οποίες θα πρέπει να φέρει ο ΥΠΔ. Σύμφωνα λοιπόν με την εν λόγω διάταξη, ο ΥΠΔ «διορίζεται βάσει επαγγελματικών προσόντων και ιδίως βάσει της εμπειρογνωσίας, που διαθέτει στον τομέα του δικαίου και των πρακτικών περί προστασίας δεδομένων, καθώς και βάσει της ικανότητας εκπλήρωσης των καθηκόντων που αναφέρονται στο άρθρο 39».

Στο άρθρο 6 παρ. 3 του εθνικού Νόμου 4624/2019, για την Προστασία των Προσωπικών Δεδομένων, επαναλαμβάνεται η διατύπωση του Γενικού Κανονισμού χωρίς καμία περαιτέρω εξειδίκευση. Συγκεκριμένα αναφέρεται ότι: «ο ΥΠΔ επιλέγεται βάσει επαγγελματικών προσόντων και ιδίως βάσει εξειδικευμένων γνώσεων του στο δίκαιο της προστασίας δεδομένων προσωπικού χαρακτήρα και των πρακτικών περί προστασίας δεδομένων προσωπικού χαρακτήρα, καθώς και βάσει των ικανοτήτων του να εκπληρώσει τα καθήκοντα του άρθρου 8».

Στον Κανονισμό, δεν εξειδικεύονται τα επαγγελματικά προσόντα, που απαιτείται να φέρει ένας ΥΠΔ, ώστε να μπορεί να επιτελέσει το έργο του, αλλά ούτε και ο βαθμός, εμπειρογνωσίας-εξειδίκευσης.

Στην αιτιολογική σκέψη 97, του Προοιμίου του ΓΚΠΔ, αναφέρεται, ότι το αναγκαίο επίπεδο εμπειρογνωσίας θα πρέπει να καθορίζεται, ανάλογα με τις πράξεις επεξεργασίας δεδομένων, που διενεργούνται και από την προστασία την οποία απαιτούν, τα δεδομένα προσωπικού χαρακτήρα, που υφίστανται επεξεργασία.

Η Ομάδα Εργασίας του άρθρου 29, αναφέρει ότι η εμπειρία και το επίπεδο γνώσεων ενός ΥΠΔ, θα πρέπει να είναι ανάλογο με τις υποθέσεις, που καλείται να διαχειριστεί. Δηλαδή, όσο πιο μεγάλο βαθμό επικινδυνότητας, όγκου και πολυπλοκότητας εμφανίζει η επεξεργασία δεδομένων από μία οντότητα, τόσο μεγαλύτερη και πληρέστερη κατάρτιση οφείλει να έχει ο ΥΠΔ.[34]

Ούτε τα επαγγελματικά προσόντα, τα απαραίτητα για έναν ΥΠΔ προσδιορίζονται, όπως προαναφέρθηκε, απλά θεωρείται αυτονόητο, ότι θα πρέπει να διαθέτει νομικές γνώσεις και άριστη γνώση του ΓΚΠΔ. Η γνώση του Κανονισμού,

---

34.Λαζαράκος Γρηγόρης,2016, «Ο θεσμός του υπεύθυνου προστασίας προσωπικών δεδομένων (Data Protection Officer) στο νέο νομοθετικό πλαίσιο των προσωπικών δεδομένων μετά την υιοθέτηση του Κανονισμού (ΕΕ) 679/2016, Εφαρμογές Δημοσίου Δικαίου-ΙΙΙ, σελ.249.

θα αφορά και θα εξειδικεύεται, στο τομέα, που απασχολείται ο υπεύθυνος επεξεργασίας, κάθε φορά.

Ο ΥΠΔ, θα πρέπει να είναι σε θέση να αντιλαμβάνεται τις πράξεις επεξεργασίας, που διενεργούνται, τα συστήματα πληροφορικής και τις ανάγκες του υπευθύνου επεξεργασίας, σε επίπεδο ασφάλειας και προστασίας δεδομένων.[35] Ιδιαίτερα χρήσιμο θα ήταν, ο ΥΠΔ, να είχε γνώσεις πληροφορικής, ώστε να μπορεί να διαχειρίζεται με μεγαλύτερη ευχέρεια, τυχόν παραβιάσεις ασφάλειας δεδομένων.

Ένα ακόμη σημαντικό στοιχείο για την επιλογή του ΥΠΔ, είναι, σύμφωνα με την Ομάδα Εργασίας του άρθρου 29, η ικανότητα εκπλήρωσης των καθηκόντων που βαρύνουν τον υπεύθυνο προστασίας δεδομένων.[36] Η ικανότητα αυτή, αναφέρεται τόσο στην προσωπική επάρκεια και γνώση του ΥΠΔ, όσο και στη θέση που θα κατέχει εντός του οργανισμού.

Ειδικότερα, ορισμένες από τις ιδιότητες και τις γνώσεις, που ο ΥΠΔ, θα ήταν ευκταίο ανάλογα με το συγκεκριμένο ρόλο, που καλείται να διαδραματίσει να έχει[37]: α)Πτυχίο Νομικής, ιδανικά με εξειδίκευση στη προστασία των προσωπικών δεδομένων, β)Εμπειρία στην εφαρμογή μέτρων προστασίας δεδομένων, γ)Εμπειρία διαχείρισης των βασικών συστημάτων και διαδικασιών, που αφορούν στη διασφάλιση και προστασία προσωπικών δεδομένων, δ)Εμπειρία σε πρότυπα διαχείρισης κινδύνου, ε)Εμπειρία και γνώση της ασφάλειας των πληροφοριών, της διαχείρισης και της βασικής ασφάλειας στον κυβερνοχώρο.

Στην περίπτωση δημόσιας αρχής ή δημόσιου φορέα, ο υπεύθυνος προστασίας

35, 36. Κατευθυντήριες γραμμές για ΥΠΔ από την ομάδα Εργασίας άρθρου 29,σελ.15,σελ. 13.

37. IT Governance Privacy team, Publishing 2017, «EU General Data Protection Regulation(GDPR)- An Implementation and Compliance Guide», Second edition,σελ.2.

δεδομένων θα πρέπει να έχει επιπλέον, καλή γνώση των διοικητικών κανόνων και διαδικασιών του οργανισμού.

Είναι πιθανό, οι δεξιότητες αυτές και οι γνώσεις να είναι δύσκολο να βρεθούν σε ένα μόνο άτομο γι αυτό επιθυμητό θα ήταν, να υπάρχει μία ομάδα ειδικών, που θα συνδράμουν τον ΥΠΔ, στο έργο του.[38,39] Άλλωστε, ο ρόλος που καλείται να διαδραματίσει ο ΥΠΔ, του θεματοφύλακα, της ορθής και συνετής εφαρμογής και συμμόρφωσης με τον ΓΚΠΔ, εντός του οργανισμού είναι ιδιαίτερα απαιτητικός. Θα πρέπει να κατορθώσει να εξασφαλίσει ότι εντός της επιχειρήσεως, έχει καταστεί κατανοητή, η σημασία της διατήρησης υψηλού επιπέδου ασφαλείας των δεδομένων.

Στην Ιρλανδία, ο Ιρλανδός Επίτροπος Προστασίας Δεδομένων, έχει εκδώσει οδηγίες, σχετικά με τα κατάλληλα προσόντα, που θα πρέπει να έχει ένας ΥΠΔ.[40] Τα προσόντα "θα καθορίζονται ανάλογα, με τις διεργασίες δεδομένων προσωπικού χαρακτήρα που πραγματοποιούνται, την πολυπλοκότητα και την κλίμακα επεξεργασίας δεδομένων, την ευαισθησία που παρουσιάζουν τα επεξεργασμένα δεδομένα και την προστασία που απαιτείται για την επεξεργασία των δεδομένων". Η Εθνική Αρχή Προστασίας Δεδομένων («DPC») επισημαίνει ότι οι οργανισμοί που επεξεργάζονται δεδομένα, περισσότερα σύνθετα ενδέχεται να χρειάζονται έναν ΥΠΔ με "υψηλότερο επίπεδο εμπειρογνωμοσύνης και υποστήριξης". Επίσης, αναφέρει ορισμένες χρήσιμες δεξιότητες, που θα πρέπει να κατέχει ο ΥΠΔ, όπως η βαθιά γνώση των ευρωπαϊκών νόμων για την προστασία των δεδομένων, η "κατανόηση των τεχνολογιών των πληροφοριών και της ασφάλειας των δεδομένων" και η "ικανότητα προώθησης μιας

38.Γιαννακάκης Ιωάννης,11/01/2017, «Ο Ρόλος και η ευθύνη του Data Protection Officer σύμφωνα με το νέο Γενικό Κανονισμό Προσωπικών Δεδομένων (GDPR)» , The DPO Academy.

39. Comments by the Centre for Information Policy Leadership on the Article 29 Data Protection Working Party's "Guidelines on Data Protection Officers (DPOs)" adopted on 13 December 2016,σελ.5

40.DLA PIPER , «Data Protection laws of the world», Ireland-DPO.

κουλτούρας προστασίας δεδομένων εντός του οργανισμού". Παράλληλα επισημαίνει ότι, οι εταιρείες/οργανισμοί, θα πρέπει να έχουν γνώση των διαθέσιμων επιλογών κατάρτισης και να εξετάζουν "το περιεχόμενο και τα μέσα της κατάρτισης και της αξιολόγησης, την κατάρτιση που οδηγεί στην πιστοποίηση και αν η παρεχόμενη εκπαίδευση και η πιστοποίηση αναγνωρίζονται διεθνώς. "

Στον Κανονισμό, δεν προβλέπεται, ούτε τίθεται καμιά υποχρέωση ή προϋπόθεση, απόκτησης πιστοποιήσεως, που θα πιστοποιεί τις γνώσεις και τις ικανότητες ενός ΥΠΔ. Εντούτοις πληθώρα, πιστοποιήσεων, παρέχονται από διάφορα ιδρύματα.

Η Ελληνική ΑΠΔΠΧ (9/08/2017)σε ανακοίνωση που εξέδωσε, δεν θέτει κάποια υποχρεωτική απαίτηση για πιστοποίηση του ΥΠΔ, ούτε καν ενθαρρύνει σε προαιρετική βάση τέτοια πιστοποίηση. «Μέχρι σήμερα κανένας φορέας στην Ελλάδα δεν έχει διαπιστευθεί για να πιστοποιεί τα επαγγελματικά προσόντα/δεξιότητες ενός DPO. Συνεπώς, οι προτεινόμενες πιστοποιήσεις DPO δεν εμπίπτουν στην κατηγορία των υφιστάμενων επίσημων ελληνικών πιστοποιήσεων». Η Αρχή ουδεμία ευθύνη φέρει για την εκπαιδευτική ύλη και την ποιότητα των εν λόγω προγραμμάτων.[41] Δύο παραδείγματα, τέτοιων φορέων πιστοποίησης, στη Ελλάδα, από τους ποικίλους που πλέον παρέχουν πιστοποιήσεις για ΥΠΔ, αποτελούν οι TUV Hellas και IAPP.

Το ίδιο και η Βελγική ΑΠΔΠΧ, στην υπ' αρίθμ.4/2017γνωμοδότηση της επισήμανε ότι για τον διορισμό του ΥΠΔ δεν απαιτείται, από τον Κανονισμό κανένα δίπλωμα ή ειδική πιστοποίηση.

Αλλά και στην Κύπρο, ο Επίτροπος Προστασίας Δεδομένων Προσωπικού Χαρα-

41.Michalopoulou &Associates LawGroup, «Ο υπεύθυνος προστασίας δεδομένων -dpo- και το υπάρχον πλαίσιο Πιστοποίησης υπό τον GDPR».

κτήρα, προέβη σε ανακοίνωση, κατόπιν πληθώρας ερωτημάτων σχετικά με τις παρεχόμενες πιστοποιήσεις διευκρινίζοντας, ότι η ενημέρωση που παρέχεται από τα διάφορα εκπαιδευτικά προγράμματα/σεμινάρια, συμβάλει μόνο, στην ευαισθητοποίηση γύρω από τις απαιτήσεις του ΓΚΠΔ, καθώς δεν τίθεται από τον Κανονισμό καμία νομική υποχρέωση,[42] για απόκτηση πιστοποιήσεως και παράλληλα επισήμανε ότι, τίθεται εν αμφιβόλω η εγκυρότητα αυτών των πιστοποιήσεων, διότι κανένας φορέας στην Κυπριακή Δημοκρατία, δεν είναι διαπιστευμένος για την παροχή τέτοιων πιστοποιήσεων.

Στο άρθρο 42 του Γενικού Κανονισμού Προστασίας Δεδομένων, γίνεται ρητή αναφορά, για τις δυνατότητες πιστοποίησης με μέγιστη διάρκεια τα τρία έτη, η οποία όμως, πιστοποίηση αφορά μόνο τον υπεύθυνο επεξεργασίας δεδομένων και τον εκτελούντα την επεξεργασία και <u>όχι τον ΥΠΔ</u>.[43] Αυτό, που πιστοποιείται είναι η τήρηση/ συμμόρφωση με τα κριτήρια που ορίζονται, στον Γενικό Κανονισμό Προστασίας Δεδομένων, χωρίς να προβλέπεται υποχρέωση λήψης της πιστοποιήσεως.

Ανεξαρτήτως των ανωτέρω, οι αρμόδιοι φορείς για τη χορήγηση πιστοποιήσεως, για να δρουν νομίμως και συνετά, θα πρέπει να έχουν διαπιστευθεί, όπως ρητά και με σαφήνεια ορίζεται στο άρθρο 43 του ΓΚΠΔ, από ένα ή αμφότερα τα ακόλουθα: α) την εποπτική αρχή που είναι αρμόδια, (στην Ελλάδα, επομένως την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα), β) τον εθνικό οργανισμό διαπίστευσης σύμφωνα με τον κανονισμό (ΕΚ) αρίθμ. 765/2008 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, δηλαδή το Εθνικό Σύστημα Διαπίστευσης της Ελλάδας (Ε.ΣΥ.Δ.) που έχει ορισθεί ως ο Εθνικός Οργανισμός Διαπίστευσης στην Ελλάδα, σύμφωνα και με τις απαιτήσεις του άρθρου 4 του Κανονισμού (ΕΚ) αρίθμ. 765/2008 .

---

42. <www.lawspot.gr> ,3/04/2018, «Διευκρινίσεις για τις πιστοποιήσεις dpo και στην Κύπρο».

43.Τσόλιας Γρηγόρης, 6/10/2017, «Ο Υπεύθυνος Προστασίας Δεδομένων (DPO) στον GDPR» - itSecurity.

Στον Εθνικό εφαρμοστικό Νόμο 4624/2019, για την Προστασία Προσωπικών Δεδομένων, στο άρθρο 37 αναφέρεται ότι η διαπίστευση των φορέων που χορηγούν πιστοποιήσεις, θα πραγματοποιείται από Εθνικό Σύστημα Διαπίστευσης (Ε.ΣΥ.Δ.), με βάση το πρότυπο EN-ISO/IEC 17065/2012 και σύμφωνα με συμπληρωματικές απαιτήσεις της Αρχής. Επιπλέον, προβλέπεται η δυνατότητα του « Ε.ΣΥ.Δ. να ανακαλεί διαπίστευση αν ενημερωθεί από την Αρχή ότι δεν πληρούνται πλέον οι απαιτήσεις διαπίστευσης ή ο φορέας πιστοποίησης παραβαίνει τον ΓΚΠΔ και τις διατάξεις του παρόντος».

Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων, επίσης, εξέδωσε κατευθυντήριες οδηγίες (1/2018), σχετικά με τις πιστοποιήσεις πράξεων επεξεργασίας (άρθρο 42-43 ΓΚΠΔ) και τα κριτήρια πιστοποιήσεων.[44] Ειδικότερα, επισημαίνει ότι η πιστοποίηση ενός ατόμου εντός ενός Φορέα, δεν αποδεικνύει τη συμμόρφωση του Φορέα αυτού, μπορεί όμως να αποτελέσει στοιχείο, το οποίο θα χρησιμοποιηθεί για να αποδειχθεί η συμμόρφωση, με τον Κανονισμό. Ως δυνατές επιλογές, για κάθε Εποπτική Αρχή, ώστε να χορηγεί πιστοποιήσεις, αναφέρει τις εξής: 1)Να χορηγεί η Αρχή, δική της πιστοποίηση, σύμφωνα με το δικό της σύστημα πιστοποίησης, 2)Να χορηγεί η Αρχή δική της πιστοποίηση, σύμφωνα με το δικό της σύστημα πιστοποίησης αλλά να αναθέτει ολόκληρο ή μέρος της διαδικασίας αξιολόγησης σε τρίτα μέρη, 3)Να δημιουργήσει η Αρχή, το δικό της σύστημα πιστοποίησης και να αναθέσει σε οργανισμούς πιστοποίησης τη διαδικασία πιστοποίησης οι οποίοι θα εκδίδουν την πιστοποίηση, 4) Να ενθαρρύνει η Αρχή την αγορά να αναπτύξει μηχανισμούς πιστοποίησης. Επομένως, οι πιστοποιήσεις θα μπορούν να εκδίδονται και από οργανισμούς πιστοποίησης κράτους μέλους, σύμφωνα πάντα, με τα κριτήρια που θα έχουν εγκριθεί από την αρμόδια εποπτική αρχή, του εκάστοτε κράτους μέλους.

---

44. Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679.

Εκτός των ανωτέρω αναφερόμενων και άλλες χώρες έχουν ασχοληθεί με το θέμα των πιστοποιήσεων των ΥΠΔ.

Η Γαλλική Αρχή Προστασίας Δεδομένων (CNIL)εξέδωσε, ανακοίνωση στις 11 Οκτωβρίου του 2018, σύμφωνα με την οποία υιοθετεί δύο κατευθυντήριες γραμμές, σχετικά με τις πιστοποιήσεις των ΥΠΔ, οι οποίες, όμως θα έχουν εφαρμογή, μόνο, στους ΥΠΔ που βρίσκονται στην Γαλλία ή που μιλούν τη γαλλική γλώσσα και είναι ιδιώτες.[45] Οι πιστοποιήσεις δεν θα χορηγούνται από την CNIL, αλλά από πιστοποιημένους από αυτήν οργανισμούς. Επισημαίνεται, ότι η πιστοποίηση βάσει των αναφορών αυτών της CNIL(κατευθυντήριες γραμμές), **δεν** εμφανίζουν υποχρεωτικό χαρακτήρα, για να γίνει κάποιος ΥΠΔ, είναι μια καθαρά εθελοντική διαδικασία, που βοηθά στην απόδειξη της συμμόρφωσης με τις απαιτήσεις του GDPR Οι κατευθυντήριες γραμμές αυτές περιλαμβάνουν: 1)πιστοποιητικό όπου καθορίζονται οι όροι για το παραδεκτό, των αιτήσεων των ΥΠΔ, και απαριθμούνται 17 προσόντα, που θα πρέπει να φέρει ο ΥΠΔ, προκειμένου να διαπιστευθεί από οργανισμό διαπίστευσης, εγκεκριμένο από την CNIL, 2) αναφορά των κριτηρίων, που πρέπει να πληρούν οι οργανισμοί για να είναι διαπιστευμένοι από την CNIL, ως οργανισμοί διαπίστευσης.

Παράλληλα, υποστηρίζεται ότι, οι υποψήφιοι ΥΠΔ, για να πληρούν τα απαιτούμενα κριτήρια, ώστε να αποκτήσουν την πιστοποίηση θα πρέπει: 1) να έχουν επαγγελματική εμπειρία τουλάχιστον δύο ετών, σε δραστηριότητες ή καθήκοντα, σχετικά με την προστασία των προσωπικών δεδομένων και σε καθήκοντα σχετικά με τη θέση του ΥΠΔ ή 2) θα πρέπει να έχουν επαγγελματική εμπειρία τουλάχιστον δύο ετών σε οποιοδήποτε τομέα, με τουλάχιστον 35 ώρες κατάρτισης, στην προστασία των προσωπικών δεδομένων από αντίστοιχο οργανισμό κατάρτισης. Επιπρόσθετα, οι υπο-

45. Privacy & Information Security Law Blog,18/10/2018,«CNIL Adopts Referentials on DPO Certification».

ψήφιοι θα κληθούν να συμπληρώσουν ένα γραπτό τεστ που θα περιλαμβάνει, τουλάχιστον 100 ερωτήσεις πολλαπλής επιλογής, το 30% των οποίων θα παρουσιάζεται με τη μορφή των περιπτωσιολογικών μελετών (case studies). Με την πρακτική αυτή, επιδιώκεται να ελεγχθούν οι ικανότητες του υποψηφίου ΥΠΔ. Όσοι επιτύχουν, θα αποκτήσουν μία πιστοποίηση για τρία έτη, οπότε και θα κληθούν εκ νέου να εξετασθούν, και όλα αυτά στα πλαίσια του προαιρετικού αυτού μηχανισμού, που παρέχεται, μόνο, για τους ομιλούντες γαλλικά ή τους ΥΠΔ στην Γαλλία.

Η Ισπανική Αρχή Προσωπικών Δεδομένων (AEPD), σε συνεργασία με τον Ισπανικό Εθνικό Φορέα Διαπίστευσης (ENAC's) και μια σειρά άλλων ειδικών στην προστασία των προσωπικών δεδομένων, είναι η πρώτη στην Ευρώπη, που θέσπισε κανονισμούς, για τη λειτουργία ενός συστήματος πιστοποίησης των ΥΠΔ, με τρόπο αντίστοιχο με τα πρότυπα του ISO 17024.[46] Όποιος επιθυμεί να γίνει ΥΠΔ θα πρέπει να λάβει την αντίστοιχη πιστοποίηση, υπό το προβλεπόμενο σύστημα. Παράλληλα, εξέδωσε οδηγίες και για τους οργανισμούς, που θα παρέχουν τις πιστοποιήσεις, οι οποίοι θα μπορούν να λειτουργούν μόνο, με την έγκυρη έγκριση του ENAC's. Όσοι, λοιπόν, θα επιθυμούν, να αποκτήσουν πιστοποίηση DPO, θα πρέπει, αρχικά να πληρούν μία από τις κάτωθι προϋποθέσεις:1) τουλάχιστον πέντε έτη επαγγελματικής εμπειρίας σε αντίστοιχη θέση/έργο που αφορά την προστασία των προσωπικών δεδομένων, ή 2) τουλάχιστον τρία έτη εμπειρίας στο ίδιο τομέα όπως προαναφέρθηκε και τουλάχιστον εξήντα (60) ώρες αναγνωρισμένης εξειδικευμένης εκπαίδευσης, ή 3)τουλάχιστον δύο έτη εμπειρίας και εκατό (100) ώρες εκπαίδευσης ή 4) σε περίπτωση μηδαμινής ή ανύπαρκτης εμπειρίας τουλάχιστον εκατό ογδόντα(180) ώρες εκπαίδευσης.

---

46. IAPP ,31/10/2017,«Here's what it takes to be a certified DPO in Spain».

Η εκπαίδευση/εξειδίκευση, δεν είναι απαραίτητο να έχει αποκτηθεί στην Ισπανία, αλλά και οπουδήποτε αλλού στην Ευρώπη, απλά θα πρέπει να αναγνωριστεί από τον αντίστοιχο φορέα κατάρτισης της Ισπανίας. Η πιστοποίηση, θα διαρκεί για τρία έτη, με το πέρας των οποίων, θα πρέπει να επανεξετασθεί η εγκυρότητα της. Η Ισπανική Αρχή Προστασίας Δεδομένων, παρέχει μία μακροσκελή λίστα με τις απαιτούμενες ικανότητες (20), που θα πρέπει να φέρει κάποιος που επιθυμεί να γίνει ΥΠΔ, η οποία μπορεί να αποτελέσει έναν χρήσιμο οδηγό και για όσους επιθυμούν και σε οποιαδήποτε άλλη χώρα της Ευρωπαϊκής Ένωσης, να γίνουν ΥΠΔ. Επιπλέον, οι υποψήφιοι ΥΠΔ στην χώρα της Ισπανίας, θα κληθούν να υπογράψουν έναν κώδικα ηθικής, παραβιάσεις του οποίου μπορούν να οδηγήσουν σε αναστολή της πιστοποίησης, για πάνω από έξι μήνες. Ποικίλες άλλες παραβιάσεις ή επαναλαμβανόμενες παραβιάσεις, θα μπορούν να οδηγήσουν, μέχρι και σε αφαίρεση της πιστοποιήσεως.

Στη Λετονία, ορίζεται ότι για να γίνει κάποιος ΥΠΔ, θα πρέπει να περάσει μια διαδικασία εξετάσεων, το περιεχόμενο των οποίων, το κόστος τους και οι υπόλοιπες λεπτομέρειες, θα καθορίζονται, από ειδική αντιπροσωπεία, που θα συσταθεί στο Υπουργικό Συμβούλιο. Ωστόσο, η εξέταση αυτή θα είναι προαιρετική, εν αντιθέσει με το προηγούμενο καθεστώς, που ίσχυε στη χώρα. Έτσι, ο υπεύθυνος επεξεργασίας και ο εκτελών, θα έχουν τη δυνατότητα να ορίσουν, οποιοδήποτε άτομο ως ΥΠΔ, εφόσον συγκεντρώνει τα απαραίτητα προσόντα, σύμφωνα με το Γενικό Κανονισμό, ανεξαρτήτως εάν κατέχει πιστοποίηση.[47] Ο εφαρμοστικός νόμος στη Λετονία, προβλέπει μία μεταβατική διάταξη, σύμφωνα με την οποία, το Υπουργικό Συμβούλιο, θα αξιολογήσει τη χρησιμότητα της απόκτησης πιστοποιήσεως από τους ΥΠΔ και θα υποβάλει την αξιολόγησή του σχετικά με τη χρησιμότητα αυτής της εξέτασης, στο

47. DLA PIPER, «Data Protection laws of the world», Latvia-DPO.

κοινοβούλιο, μέχρι τις 30 Ιουνίου 2021 .

Στην Ιταλία, στις 13 Σεπτεμβρίου 2018, το ιταλικό διοικητικό δικαστήριο της Friuli Venezia Giulia Regiuon, εξέδωσε μία πολύ σημαντική απόφαση, σχετικά με τις απαιτήσεις, που πρέπει να πληροί ένας ΥΠΔ. Το δικαστήριο έκρινε, ότι η τοπική υγειονομική αρχή συμπεριέλαβε, εσφαλμένα την πιστοποίηση «ISO / IEC 27001 Lead Auditor» ως απαραίτητη προϋπόθεση για τον ορισμό κάποιου ως ΥΠΔ. Το Δικαστήριο, στην απόφασή του, αναγνωρίζει ρητά ότι: "Η σχολαστική γνώση και η εφαρμογή των κανονισμών του Γενικού Κανονισμού Προστασίας Δεδομένων, είναι ανεξάρτητη, από την κατοχή της εν λόγω πιστοποίησης."[48,49]Η απόφαση αυτή, είναι ιδιαίτερα σημαντική, καθώς, αποσαφηνίζει το ελάχιστο επίπεδο δεξιοτήτων και προσόντων, που θα πρέπει να διαθέτει ένας ΥΠΔ, ώστε να πληρούνται οι προϋποθέσεις του ΓΚΠΔ, ήτοι, η εμπειρογνωμοσύνη, όσο αναφορά την εθνική και ευρωπαϊκή νομοθεσία και η σε βάθος κατανόηση του ΓΚΠΔ. Η απόκτηση πιστοποίησης, μπορεί να θεωρηθεί ως ένα επιπλέον προσόν, αλλά όχι ως απαίτηση.

Σε γενικές γραμμές, παρόλο που δεν θεσπίζεται η υποχρέωση απόκτησης πιστοποίησης από τον Γενικό Κανονισμό, η απόκτηση της δύναται να αποτελέσει τεκμήριο γνώσης, κατάρτισης και συμμόρφωσης, του ΥΠΔ, με τις διατάξεις του Γενικού Κανονισμού και απόδειξη για τον υπεύθυνο επεξεργασίας ή τον εκτελούντα που θέλει να προσλάβει τον ΥΠΔ, ότι αυτός είναι κατάλληλα εκπαιδευμένος και καταρτισμένος.

Άλλωστε και στις οδηγίες σχετικά με τα επαγγελματικά πρότυπα για ένα ΥΠΔ,[50]

---

48. Lexology,21/09/2018,«Italian court decision on DPO requirements and new Belgian privacy law».

49.Oberschelp de Meneses Anna and Van Quathem Kristof , 25/10/2018, «Italian Court decides that a data protection officer does not have to be a certified ISO 27001», posted in DATA PRIVACY, DATA PROTECTION, EUROPEAN UNION.

50. Επαγγελματικά Πρότυπα για DPOs από τον Ευρωπαίο Επόπτη για την Προστασία Δεδομένων (EDPS), υπό τον Κανονισμό (ΕΕ) 45/2001, 14/10/2010.

βάσει του Κανονισμού (ΕΕ) 45/2001, αναφέρεται ότι η απόκτηση πιστοποίησης από τους ΥΠΔ θα αξιολογείται, ως ένα σημαντικό προσόν, από τα όργανα ή τους οργανισμούς της ΕΕ κατά την επιλογή του ΥΠΔ.

7.ΚΟΙΝΟΠΟΙΗΣΗ ΤΩΝ ΣΤΟΙΧΕΙΩΝ ΤΟΥ ΥΠΔ

Σύμφωνα με το άρθρο 37 παρ. 7 ΓΚΠΔ, ο υπεύθυνος ή ο εκτελών την επεξεργασία, δημοσιεύουν τα στοιχεία επικοινωνίας του ΥΠΔ και τα ανακοινώνουν στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

Στο άρθρο 6 παρ. 5 του εθνικού εφαρμοστικού Νόμου 4624/2019, για τα Προσωπικά Δεδομένα, επαναλαμβάνεται η πρόβλεψη του Κανονισμού, αλλά επιπλέον εισάγεται και μία ρητή εξαίρεση από την υποχρέωση κοινοποιήσεως των στοιχείων του ΥΠΔ που ορίζεται σε δημόσιο φορέα και αφορά την περίπτωση που δεν επιτρέπεται η κοινοποίηση, για λόγους εθνικής ασφάλειας ή λόγω τήρησης του καθήκοντος εχεμύθειας (εμπιστευτικότητας), όπως προβλέπεται στον νόμο.

Σκοπός της ανακοινώσεως αυτής των στοιχείων του ΥΠΔ, είναι να καταστούν γνωστά τα στοιχεία επικοινωνίας του, ώστε οποιοσδήποτε επιθυμεί, να μπορεί να έρθει σε επαφή μαζί του. Παράλληλα, επιδιώκεται η εξασφάλιση του απορρήτου της επικοινωνίας με τον ΥΠΔ, ώστε τυχόν δισταγμοί και αναστολές, λόγω αμφιβολιών τήρησης της μυστικότητας και εμπιστευτικότητας να κάμπτονται.

Άλλωστε, ο ΥΠΔ, δεσμεύεται από το απόρρητο όσον αφορά την ενάσκηση των καθηκόντων του, βάσει του άρθρου 38 παρ. 5 ΓΚΠΔ.

Στα στοιχεία επικοινωνίας του ΥΠΔ, ώστε να καθίσταται δυνατή και εύκολη η ανεύρεση του, από όποιον επιθυμεί, συγκαταλέγονται τα εξής:

-Ονοματεπώνυμο

-Ταχυδρομική Διεύθυνση

-Αποκλειστικός τηλεφωνικός αριθμός

-Διεύθυνση ηλεκτρονικού ταχυδρομείου

-Λογαριασμοί σε μέσα κοινωνικής δικτύωσης

Ο Γενικός Κανονισμός, δεν απαιτεί στα δημοσιευμένα στοιχεία επικοινωνίας του ΥΠΔ, να περιλαμβάνεται και το όνομα του. Εντούτοις, θα αποτελούσε καλή και χρήσιμη πρακτική η δημοσίευση του ονόματός του. Ο υπεύθυνος επεξεργασίας, καλείται να αποφασίσει, αλλά και ο ΥΠΔ, για το πότε είναι απαραίτητο ή χρήσιμο, να δημοσιεύεται το όνομα του ΥΠΔ, αναλόγως τη συγκεκριμένη περίπτωση.

Χρήσιμο θα ήταν, η οντότητα να ενημερώνει τους υπαλλήλους της, για το όνομα και τα στοιχεία επικοινωνίας του ΥΠΔ. Για παράδειγμα, το όνομα και τα στοιχεία επικοινωνίας του ΥΠΔ μπορούν να δημοσιευθούν, εντός του οργανισμού, στο εσωτερικό του δίκτυο, στον εσωτερικό τηλεφωνικό κατάλογο.

Στην Ελλάδα, προβλέπεται η υποχρέωση για τον υπεύθυνο και εκτελούντα την επεξεργασία να ανακοινώνουν στην εποπτική αρχή στοιχεία, που αφορούν στον ορισμό του ΥΠΔ.[51] Στο πλαίσιο αυτό, η Αρχή έχει αναρτήσει στην ιστοσελίδα της ειδικό έντυπο, το οποίο καλούνται να συμπληρώνουν οι υπεύθυνοι και εκτελούντες την επεξεργασία προκειμένου να ανακοινώσουν στην Αρχή τον ορισμό του υπευθύνου προστασίας. Το έντυπο πρέπει να αποσταλεί ηλεκτρονικά στη διεύθυνση, «dpo announcement@dpa.gr». Η υποχρέωση ανακοίνωσης ορισμού ΥΠΔ, ικανοποιείται μόνο, με την υποβολή του συγκεκριμένου εντύπου. Οποιαδήποτε προηγούμενη δήλωση (πριν την 25η Μαΐου 2018) στοιχείων υπευθύνου προστασίας

51. Υπεύθυνος Προστασίας Δεδομένων ,<www.dpa.gr> .

δεδομένων, που έχει υποβληθεί στην Αρχή δεν λαμβάνεται υπόψη. Ο υπεύθυνος επεξεργασίας ενημερώνει την Αρχή, με email, σε περίπτωση αντικατάστασης ή κατάργησης του ΥΠΔ. Στην πρώτη περίπτωση (αντικατάστασης),ο υπεύθυνος επεξεργασίας συμπληρώνει εκ νέου το σχετικό έντυπο με τα στοιχεία του νέου DPO και το αποστέλλει στην ανωτέρω αναφερόμενη διεύθυνση, ενώ το παλιό έντυπο καταργείται αυτομάτως. Στη δεύτερη περίπτωση (κατάργησης), ο υπεύθυνος επεξεργασίας ενημερώνει με απλό email, στην ανωτέρω αναφερόμενη διεύθυνση ότι καταργείται ο DPO και δεν αντικαθίσταται.

Ορισμένες Εποπτικές Αρχές έχουν ορίσει προθεσμίες για την ολοκλήρωση της κοινοποίησης. Η Ολλανδία και η Πολωνία είναι δύο από τα σημαντικότερα παραδείγματα, με προθεσμίες κοινοποίησης, που είχαν καθορισθεί, από τον Ιούνιο έως τον Σεπτέμβριο του 2018. Οι περισσότερες άλλες αρχές, δεν έχουν ορίσει ρητά προθεσμίες.[52]

Διάταγμα στη Γαλλία, απαιτεί, τα στοιχεία επικοινωνίας του ΥΠΔ και οι τυχόν τροποποιήσεις τους, να κοινοποιούνται, το συντομότερο δυνατόν, στη γαλλική Αρχή.[53]Η «CNIL», η γαλλική αρχή Προστασίας Δεδομένων, έχει δημιουργήσει ένα ηλεκτρονικό έντυπο για τη διευκόλυνση των φορέων, που επιθυμούν να διορίσουν έναν ΥΠΔ. Το εν λόγω έντυπο, το οποίο αποτελείται από 4 βήματα, επιτρέπει τον διορισμό ενός ΥΠΔ, χωρίς την ανάγκη εκτέλεσης πρόσθετων διοικητικών διατυπώσεων. Για ομίλους επιχειρήσεων, η διαδικασία θα πρέπει να επαναληφθεί, για κάθε οντότητα χωριστά, για τον ορισμό του ΥΠΔ της. Η «CNIL» τηρεί μητρώο των δημόσιων

52. Alston and Bird, June 17 2018, «EU Supervisory Authorities Disclose DPO Notification Tools», Privacy & Data Security Team.

53. Gastaud Florent 23 août 2018, «Comment designer un Data Protection Officer (DPO) en France ?», Mon DPO externe.

στοιχείων επικοινωνίας, όλων των ΥΠΔ που ορίζονται, μαζί.

Η Πολωνική Αρχή Προστασίας Δεδομένων, αναφέρει ότι, ο υπεύθυνος επεξεργασίας οφείλει να κοινοποιήσει τον ορισμό του ΥΠΔ. Τα απαραίτητα στοιχεία της κοινοποίησης είναι τα εξής: α) Όνομα, διεύθυνση ηλεκτρονικού ταχυδρομείου και αριθμός τηλεφώνου, β) Διεύθυνση κατοικίας, εάν ο ΥΠΔ είναι φυσικό πρόσωπο, γ) Η επιχείρηση και η διεύθυνση της όπου ο υπεύθυνος επεξεργασίας ή ο εκτελών, που διευθύνει την επιχείρηση είναι φυσικό πρόσωπο, δ) Ονοματεπώνυμο και διεύθυνση της έδρας, εφόσον ο υπεύθυνος επεξεργασίας ή ο εκτελών δεν είναι φυσικό πρόσωπο, ε) Στατιστικό αριθμό, εάν δόθηκε στον υπεύθυνο επεξεργασίας ή στον εκτελούντα την επεξεργασία.Εάν μια ομάδα εταιρειών αποφασίσει να διορίσει έναν ΥΠΔ για ολόκληρο τον όμιλο, κάθε εταιρεία που ανήκει στον όμιλο υποχρεούται να γνωστοποιήσει στην αρμόδια αρχή, τον διορισμό του ΥΠΔ, χωριστά από τις άλλες εταιρείες του ομίλου. Η κοινοποίηση μπορεί να γίνει **μόνο σε ηλεκτρονική μορφή**.[54] Η ηλεκτρονική κοινοποίηση, απαιτεί την κατοχή κατάλληλης ηλεκτρονικής υπογραφής ή υπογραφής που επιβεβαιώνεται από το προφίλ ePUAP (ένα αξιόπιστο προφίλ που προσφέρουν οι πολωνικές αρχές). Και οι δύο αυτές μέθοδοι επαλήθευσης ταυτότητας, μπορεί να είναι δύσκολο να χρησιμοποιηθούν από άτομα που βρίσκονται εκτός της χώρας της Πολωνίας. Επιπρόσθετα, όπως και στην Ελλάδα, σε περίπτωση αλλαγής των προσωπικών στοιχείων του ΥΠΔ ή ακύρωσης του διορισμού και ορισμού νέου ΥΠΔ, πρέπει να υποβληθούν οι αλλαγές αυτές, στην αρμόδια αρχή, εντός 14 ημερών από την ημερομηνία της αλλαγής.

Στην Ιρλανδία, προβλέπεται η συμπλήρωση ενός ηλεκτρονικού εγγράφου, για τον ορισμό του ΥΠΔ, το οποίο κατόπιν κοινοποιείται στην αρμόδια αρχή (DPC).[55]

54.DLA PIPER, «Data Protection laws of the world», Poland-DPO.

55. Data Protection Officers | Data Protection Commissioner.

Αλλά και στη Βουλγαρία, [56] απαιτείται ο υπεύθυνος επεξεργασίας δεδομένων, να ανακοινώνει, τα προσωπικά στοιχεία του ΥΠΔ και τα στοιχεία επικοινωνίας μαζί του, όπως και οποιαδήποτε τροποποίηση των στοιχείων αυτών.

Η σημασία της ανακοίνωσης και της γνώσης των στοιχείων του ΥΠΔ, αναδύεται ιδιαίτερα, σε περίπτωση παραβιάσεως δεδομένων προσωπικού χαρακτήρα, όπου ο υπεύθυνος επεξεργασίας, θα πρέπει να την γνωστοποιήσει αμελλητί και σε κάθε περίπτωση εντός 72 ωρών, από τη γνώση της παραβιάσεως, στην αρμόδια Αρχή.[57]

Μεταξύ των απαραίτητων πληροφοριών, που θα πρέπει να μεταφέρει ο υπεύθυνος επεξεργασίας, συγκαταλέγονται το όνομα και τα στοιχεία επικοινωνίας του ΥΠΔ, από τον οποίον θα μπορούν να ληφθούν περισσότερες πληροφορίες. Στο Ηνωμένο Βασίλειο, επισημαίνεται ότι θα πρέπει να γνωστοποιείται το όνομα του ΥΠΔ, σε περίπτωση παραβίασης προσωπικών δεδομένων, στην αρμόδια αρχή « ICO» και στα άτομα που αφορά η παραβίαση.[58]

Επιπλέον, όταν βάσει του άρθρου 35 ΓΚΠΔ, διαφαίνεται ότι η επεξεργασία προσωπικών δεδομένων, θα προκαλέσει υψηλό κίνδυνο και ο υπεύθυνος επεξεργασίας ζητά τη γνώμη της Αρχής, πριν από την επεξεργασία, ανάμεσα στα άλλα στοιχεία που θα πρέπει να γνωστοποιήσει στην Αρχή, είναι και τα στοιχεία του ΥΠΔ.

Μια ενδιαφέρουσα πρακτική, όσον αναφορά τα προσωπικά στοιχεία του ΥΠΔ, που θα μπορούσε να υιοθετηθεί από τις αρμόδιες κατά τόπους Αρχές, είναι αυτή που

---

56. DLA PIPER , «Data Protection laws of the world», Bulgaria-DPO.

57. Ψαρουδάκη Μαριάνα, Αύγουστος-Σεπτέμβριος 2018, «Υπεύθυνος Προστασίας Δεδομένων (DPO)-Το πλαίσιο των καθηκόντων του και της ευθύνης του», ΕΠΙΧΕΙΡΗΣΗ 151/2018, σελ.733.

58.Ιστοσελίδα Information Commissioner' s Office Ηνωμένου Βασιλείου.

τηρείται από τον Ευρωπαίο Επόπτη Προστασίας Δεδομένων. Στην ιστοσελίδα του Επόπτη, υπάρχει πλήρη λίστα των ΥΠΔ, που υπηρετούν στα ευρωπαϊκά όργανα και τις υπηρεσίες της ΕΕ.[59]

8. ΥΠΔ ΜΕΛΟΣ ΤΟΥ ΠΡΟΣΩΠΙΚΟΥ ΤΗΣ ΟΝΤΟΤΗΤΑΣ Ή ΕΞΩΤΕΡΙΚΟΣ ΣΥΝΕΡΓΑΤΗΣ

Ο ΥΠΔ, θα μπορεί να αποτελεί μέλος του προσωπικού, του υπευθύνου επεξεργασίας ή του εκτελούντος ή να ασκεί τα καθήκοντα του, ως εξωτερικός συνεργάτης της οντότητας βάσει συμβάσεως παροχής υπηρεσιών, κατά το άρθρο 37 παρ. 7 του ΓΚΠΔ.

Το ίδιο προβλέπεται και στο άρθρο 6 παρ. 4 του Νόμου 4624/2019, για τα Προσωπικά Δεδομένα για τους δημόσιους φορείς, όπου ΥΠΔ θα ορίζεται είτε υπάλληλος του δημοσίου φορέα με οποιαδήποτε σχέση εργασίας είτε τρίτος βάσει σύμβασης παροχής υπηρεσιών.

Οι δύο επιλογές, εμφανίζουν η καθεμία τα δικά της θετικά στοιχεία. Βεβαία, η καλύτερη και σωστότερη επιλογή εξαρτάται από την ad hoc περίπτωση.

Για παράδειγμα, μια εταιρεία που δεν διαθέτει υψηλά ειδικευμένο προσωπικό στον τομέα της προστασίας δεδομένων και των κανονισμών ασφαλείας του συστήματος πληροφοριών, θα επωφεληθεί, από την ύπαρξη ενός τρίτου, εμπειρογνώμονα, που θα απασχολείται αποκλειστικά στο συγκεκριμένο τομέα, αφιερώνοντας όλο το χρόνο του εκεί. Εντούτοις, και μια εταιρεία με το αυτό αντικείμενο δραστηριοποίησης, μπορεί επίσης να επιλέξει να αναθέσει σε εξωτερικούς

59. DLAPIPER, «Data Protection laws of the world», Cyprus-DPO, Στην Κύπρο, προβλέπεται η ύπαρξη λίστας με τα ονόματα των υπεύθυνων επεξεργασίας δεδομένων και των εκτελούντων την επεξεργασία, που έχουν ορίσει ΥΠΔ, υπό την προϋπόθεση ότι επιθυμούν να συμπεριληφθούν σε αυτήν.

συνεργάτες τη λειτουργία του ΥΠΔ, για ρεαλιστικούς λόγους, όπως για παράδειγμα για να εξασφαλίσει την απόλυτη ανεξαρτησία και τεχνογνωσία, του υπεύθυνου προστασίας δεδομένων.

Σε κάθε περίπτωση, καθίσταται σαφές ότι, ο ΥΠΔ, ο οποίος εργάζεται ήδη στην οντότητα, στην οποία καλείται να παρέχει τις υπηρεσίες του ως ΥΠΔ, θα έχει[60] πληρέστερη και άμεση εικόνα, των πρακτικών της οντότητας, της επεξεργασίας των δεδομένων, που διενεργείται, ώστε αμέσως να είναι σε θέση να διαπιστώσει το βαθμό συμμορφώσεως της, με το ΓΚΠΔ.

Η «Facebook» για παράδειγμα, όρισε ως ΥΠΔ, για όλες τις εταιρίες της «οικογένειας» (Instagram και WhatsApp), ένα μέλος της εταιρίας, που ήταν επιφορτισμένο με αυξημένης αρμοδιότητας καθήκοντα, το οποίο με τη συνδρομή μίας αφοσιωμένης και εξειδικευμένης ομάδας, ανέλαβε τον απαιτητικό ρόλο του ΥΠΔ.[61]

Το ανωτέρω, αποτελεί ίσως και το μοναδικό θετικό στοιχείο, διότι, εφόσον ο ΥΠΔ, είναι ήδη μέλος της οντότητας, ήδη θα είναι επιφορτισμένος με καθήκοντα, που υπάρχει ενδεχόμενο, να έρχονται σε σύγκρουση με αυτά του ΥΠΔ. Αυτό συνέβη στην Γερμανία, όπου ως ΥΠΔ, ορίσθηκε ο IT manager της εταιρίας, με αποτέλεσμα, η Βαυαρική ΑΠΔΠΧ, να επιβάλλει πρόστιμο 50.000 ευρώ στην εταιρία, αξιώνοντας παράλληλα και την αντικατάσταση του ΥΠΔ. Η θέση ενός διαχειριστή ΤΠ είναι ασυμβίβαστη με τη θέση του ΥΠΔ, διότι ο ΥΠΔ θα πρέπει, στην ουσία να παρακολουθεί τον εαυτό του, να διαπιστώνει δηλαδή, κατά πόσον οι δραστηριότητές του ως υπεύθυνου πληροφορικής συμμορφώνονται με τον νόμο περί προστασίας δεδομένων. Αντίστοιχη σύγκρουση συμφερόντων, θα μπορούσε επίσης να διαπιστωθεί, εάν ο ΥΠΔ

---

60. Σωτηρόπουλος Βασίλης,2017, «Υπεύθυνος Προστασίας Δεδομένων-Εργαλειοθήκη για τον νέο θεσμό σε δημόσιο και ιδιωτικό τομέα», Εκδόσεις Σάκκουλα, σελ. 108.

61.IAPP,24/05/2018,«Facebook names Deadman first DPO».

είναι επικεφαλής άλλων υπηρεσιών που εμπλέκονται σε μεγάλο βαθμό με την επεξεργασία προσωπικών δεδομένων, όπως το τμήμα μάρκετινγκ.

Ακόμα και αν δεν συντρέχει τέτοια περίπτωση, ενδέχεται, τα έτερα καθήκοντα, που έχει ο ΥΠΔ, να τον αποσπούν από την απρόσκοπτη ενάσκηση των καθηκόντων του, ως ΥΠΔ ή ακόμα θα μπορούσε να βρεθεί σε δίλλημα και να μπει στον πειρασμό να δώσει προτεραιότητα σε άλλες δραστηριότητες (επιχειρηματικές, οργανωτικές κ. α)από εκείνες που σχετίζονται με την προστασία των δεδομένων. Για το λόγο αυτό, κρίνεται θεμιτό, να απαλλάσσεται των έτερων καθηκόντων του, ώστε να μπορεί να αφιερωθεί και να αφοσιωθεί στο έργο του, αναπόσπαστα, έχοντας στη διάθεση του, όσο χρόνο απαιτείται για την ενασχόληση με το απαιτητικό τομέα της προστασίας των προσωπικών δεδομένων. [62]

Ένα ακόμα αρνητικό σημείο, της ανάδειξης ως ΥΠΔ, μέλος του προσωπικού της οντότητας, είναι το γεγονός ότι, θα έχει αναπτύξει ήδη φιλικές- συναδελφικές σχέσεις, αλλά και σχέσεις εμπιστοσύνης με τους προϊσταμένους του, γεγονός που μπορεί να δρα ανασταλτικά, στην ανεπηρέαστη και απρόσκοπτη ενάσκηση των καθηκόντων του.[63] Ίσως να είναι εξαιρετικά δύσκολο, να διοριστεί ένας εσωτερικός ΥΠΔ που τα καθήκοντα, τα οποία ήδη έχει αναλάβει εντός της οντότητας, δεν θα έρχονται σε σύγκρουση, με τις άλλες λειτουργίες του, ως ΥΠΔ.

Από την άλλη πλευρά, εφόσον ως ΥΠΔ, επιλεγεί τρίτο πρόσωπο σε σχέση με την οντότητα, είτε αυτό είναι φυσικό πρόσωπο είτε άλλος οργανισμός/νομική οντότητα, θεωρείται δεδομένο, ότι θα διαθέτει την απαιτούμενη εξειδίκευση, γνώση και κατά-

---

62. Ψαρουδάκη Μαριάνα, Αύγουστος-Σεπτέμβριος 2018, «Υπεύθυνος Προστασίας Δεδομένων (DPO)-Το πλαίσιο των καθηκόντων του και της ευθύνης του», ΕΠΙΧΕΙΡΗΣΗ 151/2018, σελ.729

63.Σωτηρόπουλος Βασίλης, 2017, «Υπεύθυνος Προστασίας Δεδομένων-Εργαλειοθήκη για τον νέο θεσμό σε δημόσιο και ιδιωτικό τομέα», Εκδόσεις Σάκκουλα, σελ. 108-109

ρτιση, απασχολούμενος μόνο στο συγκεκριμένο τομέα, συμβάλλοντας έτσι τα μέγιστα, στην επίτευξη της συμμόρφωσης με το ΓΚΠΔ.[64] Έτσι, θα επωφεληθεί ο οργανισμός, διότι δεν θα χρειασθεί να αφιερώσει χρόνο και χρήμα, για την περαιτέρω εκπαίδευση και κατάρτιση, ενός ήδη υπάρχοντος μέλους της οντότητας, για να φτάσει στο επιθυμητό επίπεδο εμπειρογνωσίας, ώστε να αναλάβει τον απαιτητικό ρόλο του ΥΠΔ .Επιπρόσθετα, οι πιθανότητες να προκύψουν, τυχόν συγκρούσεις συμφερόντων εκμηδενίζονται. Άλλωστε ρητά προβλέπεται στο άρθρο 38 παρ. 6 του ΓΚΠΔ, ότι ο ΥΠΔ θα πρέπει να είναι ανεξάρτητος κατά την εκτέλεση των καθηκόντων του, δεν θα πρέπει να αναλαμβάνει καθήκοντα και να εκτελεί αποστολές, που ενδέχεται να έρχονται σε σύγκρουση συμφερόντων, με την ιδιότητα του ως ΥΠΔ.

Η ομάδα Εργασίας του άρθρου 29, στις κατευθυντήριες γραμμές για τους ΥΠΔ έχει επίσης, επισημάνει ότι ορισμένες θέσεις (διευθυντής μάρκετινγκ κ.α.)θα είναι ασύμβατες, με το ρόλο του ΥΠΔ και η ανάληψη τους παράλληλα με τα καθήκοντα του ΥΠΔ, θα οδηγούν σε σύγκρουση συμφερόντων.[65] Ο διορισμός ενός εξωτερικού ΥΠΔ, θα εξαλείφει εντελώς ,αυτό το ενδεχόμενο.

Ο εξωτερικός ΥΠΔ, κατά την ενάσκηση των καθηκόντων του, θα χαίρει των προστατευτικών διατάξεων του Κανονισμού (δεν θα μπορεί, δηλαδή, να γίνει αποδέκτης καταχρηστικής καταγγελίας της σύμβασης παροχής υπηρεσιών για την άσκηση δραστηριοτήτων που εμπίπτουν στην ιδιότητα του ΥΠΔ, ούτε οποιοδήποτε μέλος του οργανισμού που ασκεί καθήκοντα ΥΠΔ δεν θα μπορεί να τύχει καταχρηστικής απολύσεως, δεν θα υφίσταται κυρώσεις για την τέλεση των καθηκόντων του).

---

64. IT Governance Blog, 17/07/2018, «The DPO role and why you should consider out sourcing it».

65. Κατευθυντήριες γραμμές για ΥΠΔ της Ομάδας Εργασίας του άρθρου 29,σελ. 22.

Μία αποτελεσματική πρακτική, για την πληρέστερη και αποδοτικότερη ενάσκηση των καθηκόντων του εξωτερικού ΥΠΔ, θα μπορούσε να αποτελέσει η σύσταση μίας εξειδικευμένης ομάδας εντός της οντότητας, τα μέλη της οποίας, θα συνδράμουν τον ΥΠΔ στο δύσκολο και επίπονο έργο του. Έχοντας γνώση της εσωτερικής λειτουργίας του οργανισμού, θα συνεργάζονται μαζί του υπό τις οδηγίες του, καθώς αυτός θα είναι ο επικεφαλής της ομάδας και ο άμεσα υπεύθυνος για το έργο της. Οι αρμοδιότητες του κάθε μέλους, χρήσιμο θα ήταν να καθορίζονται εκ των προτέρων, ώστε να διευκολύνεται το έργο της ομάδας. [66,67]

66.Λαζαράκος Γρηγόρης,2016, «Ο θεσμός του υπεύθυνου προστασίας προσωπικών δεδομένων (Data Protection Officer) στο νέο νομοθετικό πλαίσιο των προσωπικών δεδομένων μετά την υιοθέτηση του Κανονισμού (ΕΕ) 679/2016, Εφαρμογές Δημοσίου Δικαίου-ΙΙΙ, σελ. 25

67. Comments by the Centre for Information Policy Leadership on the Article 29 Data Protection Working Party's "Guidelines on Data Protection Officers (DPOs)" adopted on 13 December 2016, σελ.5

9. Ο ΡΟΛΟΣ-ΘΕΣΗ ΤΟΥ ΥΠΕΥΘΥΝΟΥ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

Ο ΥΠΔ, χαίρει προστασίας από τον Γενικό Κανονισμό, είναι ανεξάρτητος και ο ρόλος του είναι συμβουλευτικός. Στο άρθρο 38 παρ. 1 ΓΚΠΔ αναφέρεται : «Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία διασφαλίζουν ότι ο υπεύθυνος προστασίας δεδομένων συμμετέχει, δεόντως και εγκαίρως, σε όλα τα ζητήματα τα οποία σχετίζονται με την προστασία δεδομένων προσωπικού χαρακτήρα». Παράλληλα, παρέχονται οι κατάλληλες θεσμικές εγγυήσεις και πόροι για τη διασφάλιση του θεσμού του ΥΠΔ, για την απρόσκοπτη και ακώλυτη εκτέλεση των καθηκόντων του. Είναι ζωτικής σημασίας να συμμετέχει ο ΥΠΔ και να γνωμοδοτεί όσο το δυνατόν σε πιο πρώιμο στάδιο, σε οποιοδήποτε ζήτημα σχετίζεται, με τα δεδομένα προσωπικού χαρακτήρα.[68]

1) ΣΥΜΜΕΤΟΧΗ ΣΤΗ ΛΗΨΗ ΑΠΟΦΑΣΕΩΝ

Όπως προαναφέρθηκε, ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία διασφαλίζουν ότι ο υπεύθυνος προστασίας δεδομένων «συμμετέχει, δεόντως και εγκαίρως, σε όλα τα ζητήματα τα οποία σχετίζονται με την προστασία δεδομένων προσωπικού χαρακτήρα». Η Ομάδα Εργασίας του άρθρου 29 για τους ΥΠΔ, επισημαίνει ότι, η από το πρωταρχικό στάδιο, ενημέρωση από τον υπεύθυνο προστασίας δεδομένων για την επεξεργασία δεδομένων και η διαβούλευση μαζί του, θα διευκολύνουν και θα συμβάλουν στη συμμόρφωση, με τον ΓΚΠΔ. Κατά αυτόν τον τρόπο, ήδη από το στάδιο του σχεδιασμού, θα μπορέσει να διασφαλισθεί και η τήρηση της ιδιωτικότητας και μυστικότητας.

68.Faller Pierre , «GDPR DPO's (Data Protection Officer) role within organization»,<advisera.com>.

Χαρακτηριστικό της καίριας θέσης του ΥΠΔ και της ανάγκης να συμμετέχει από το αρχικό στάδιο, σε οποιαδήποτε πράξη ενέχει επεξεργασία δεδομένων, αποτελεί το γεγονός ότι, κατά τη διενέργεια εκτίμησης αντικτύπου, σχετικά με την προστασία των δεδομένων(αρ.35 παρ.2)ο ΓΚΠΔ απαιτεί ρητώς, την έγκαιρη συμμετοχή του υπευθύνου προστασίας δεδομένων. Ο υπεύθυνος επεξεργασίας δεδομένων, επιπλέον, οφείλει να ζητήσει τη γνώμη του υπευθύνου προστασίας δεδομένων, κάθε φορά που διενεργείται εκτίμηση αντικτύπου, σχετικά με την προστασία των δεδομένων.

Η Ομάδα Εργασίας του άρθρου 29 αναφέρει ότι είναι σημαντικό, ο ΥΠΔ να αντιμετωπίζεται ως συνομιλητής, εντός της οντότητας.[69] Γι αυτό, θα πρέπει να διασφαλίζεται ότι έχει προσκληθεί, να παρακολουθεί τις συνεδριάσεις, ειδικά όταν λαμβάνονται αποφάσεις με επιπτώσεις στην προστασία δεδομένων. Η αναγκαιότητα συμμετοχής του, θα μπορούσε να φτάσει μέχρι το σημείο να ζητήσει αναβολή στη λήψη απόφασης επί θέματος, για το οποίο ο ίδιος, θα χρειάζεται μεγαλύτερο χρονικό διάστημα, για να προετοιμαστεί. Εφόσον η οντότητα, παραλείψει να τηρήσει, κάτι από τα ανωτέρω, παραβιάζει το άρθρο 38 παρ.1 του Γενικού Κανονισμού και καθίσταται έκθετη ενώπιον της Αρχής. Επιπλέον, στην περίπτωση που, η γνώμη που θα διατυπώσει ο ΥΠΔ, δεν ληφθεί υπόψη ή δεν υιοθετηθεί, θα πρέπει να καταγράφονται οι λόγοι για τους οποίους δεν ακολουθήθηκε και δεν υιοθετήθηκε η συμβουλή του ΥΠΔ.

Η συμμετοχή του ΥΠΔ, θα πρέπει να διασφαλίζεται αδιακρίτως, του ζητήματος για το οποίο καλείται να αποφασίσει η οντότητα είτε αυτό είναι διοικητικής φύσεως, είτε τεχνικής, εφόσον προβλέπεται ότι θα έχει επιπτώσεις στην προστασία προσωπικών δεδομένων. Αυτό συνεπάγεται, ότι ο ΥΠΔ προηγουμένως θα έχει τύχει της κατάλληλης

69. Κατευθυντήριες γραμμές για ΥΠΔ της Ομάδας Εργασίας του άρθρου 29,σελ. 18.

ενημέρωσης, για το ζήτημα, για το οποίο επρόκειτο να διεξαχθεί η συζήτηση, ώστε να μπορεί ενεργά και έγκαιρα, στα πλαίσια των συμβουλευτικών του καθηκόντων, να συμμετέχει.

Εν ολίγοις, θα πρέπει να γίνει κατανοητό, ότι ο ΥΠΔ, στα πλαίσια μίας οντότητας θα πρέπει να διαδραματίζει καθοριστικό και ενεργό ρόλο, ώστε να επιτευχθεί η συμμόρφωση με τον Κανονισμό και να αποφευχθούν τυχόν αστοχίες, που θα μπορούσαν να οδηγήσουν, την οντότητα στην οικονομική καταστροφή, με την επιβολή δυσβάστακτων προστίμων.

2) ΠΑΡΟΧΗ ΠΡΟΣΒΑΣΗΣ ΣΕ ΔΕΔΟΜΕΝΑ-ΠΟΡΟΥΣ

Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία, στηρίζουν τον ΥΠΔ στην άσκηση των καθηκόντων του, παρέχοντας του απαραίτητους πόρους για την άσκηση αυτών, πρόσβαση σε δεδομένα προσωπικού χαρακτήρα και σε πράξεις επεξεργασίας, καθώς και πόρους απαραίτητους για την διατήρηση της εμπειρογνωσίας του (άρθρο 38 παρ. 2 ΓΚΠΔ). Το ίδιο ακριβώς, προβλέπεται και στην Οδηγία (ΕΕ) 2016/680 .

Ιδιαίτερα σημαντικό κρίνεται αρχικά, ο ΥΠΔ να αμείβεται επιπρόσθετα, για την ενάσκηση των καθηκόντων του ως ΥΠΔ, σε περίπτωση που είναι ήδη μέλος του προσωπικού της οντότητας, στην οποία θητεύει. Είναι βασικό, ώστε να εξασφαλίζεται ότι θα εκτελέσει τα καθήκοντα του, επιμελώς. Η ανάθεση καθηκόντων ΥΠΔ, χωρίς μισθολογική αναπροσαρμογή συνιστά παραβίαση του Γενικού Κανονισμού. [70]

70.Σωτηρόπουλος Βασίλης,2017, «Υπεύθυνος Προστασίας Δεδομένων-Εργαλειοθήκη για τον νέο θεσμό σε δημόσιο και ιδιωτικό τομέα», Εκδόσεις Σάκκουλα, σελ.116

Στις «Κατευθυντήριες Γραμμές για τους ΥΠΔ» η Ομάδα Εργασίας του άρθρου 29 αναφέρει, ότι απαραίτητοι πόροι για την εκτέλεση των καθηκόντων του ΥΠΔ αποτελούν τα ακόλουθα.[71]

-Η ενεργητική υποστήριξη της λειτουργίας του ΥΠΔ από τα υψηλότερα στελέχη της διοίκησης

- Ο επαρκής χρόνος για τον ΥΠΔ προκειμένου να εκπληρώσει τα καθήκοντά του.

- Η επαρκής υποστήριξη ως προς τους οικονομικούς πόρους, τις υποδομές και το προσωπικό όπου είναι αναγκαίο.

-Η επίσημη ανακοίνωση του ορισμού ΥΠΔ προς όλο το προσωπικό, ώστε να γίνει γνωστή η ύπαρξή του στο πλαίσιο του φορέα

-Η αναγκαία πρόσβαση σε άλλες υπηρεσίες (ανθρώπινο δυναμικό, νομική υπηρεσία, πληροφορική)ώστε να λαμβάνει υποστήριξη

-Η συνεχής εκπαίδευση και κατάρτιση.

-Αναλόγως του μεγέθους και της δομής του οργανισμού, μπορεί ενδεχομένως να απαιτείται η σύσταση ομάδας υπευθύνου προστασίας δεδομένων (να υπάρχει δηλαδή υπεύθυνος προστασίας δεδομένων με δικό του προσωπικό).

Γενικότερα, όσο μεγαλύτερη πολυπλοκότητα και όσο πιο ευαίσθητα είναι τα δεδομένα, που υπόκειντο σε επεξεργασία, τόσο περισσότεροι πόροι, θα πρέπει να διατίθεντο στον ΥΠΔ, ώστε να εκτελεί αποτελεσματικά το έργο του.

Ειδικότερα, μία προτεινόμενη και αρμόζουσα πρακτική, σχετικά με τους πόρους, που θα πρέπει να διατίθεντο στον ΥΠΔ, περιλαμβάνει, πρωτίστως, την διαμόρφωση

71. Κατευθυντήριες γραμμές για ΥΠΔ της Ομάδας Εργασίας του άρθρου 29,σελ. 19.

ειδικού χώρου-γραφείου, αποκλειστικά για τον ΥΠΔ, ακόμη και αν είναι εξωτερικός συνεργάτης. Ανάλογα με την έκταση και τη μορφή της οντότητας, θα πρέπει να παρέχεται και αυτοτελής γραμματειακή υποστήριξη στον ΥΠΔ, που για λόγους προστασίας απορρήτου, δεν πρέπει να έχει παράλληλα καθήκοντα. Δεν είναι νοητή η άσκηση των καθηκόντων του ΥΠΔ, χωρίς την κατάλληλα τεχνική υποδομή. Είναι αυτονόητο, ότι για την ενάσκηση των καθηκόντων του ο ΥΠΔ, θα έχει το δικό του, ηλεκτρονικό υπολογιστή με πρόσβαση στο Διαδίκτυο και στο εσωτερικό δίκτυο, όπως και τα άλλα απαραίτητα περιφερειακά εργαλεία(σαρωτή, εκτυπωτή) καθώς επίσης και τα πιο προηγμένα λογισμικά ασφάλειας δικτύου και του συστήματος του γραφείου του. Η παροχή πρόσβασης σε δεδομένα προσωπικού χαρακτήρα αποτελεί, επίσης υποχρέωση της οντότητας απέναντι στον ΥΠΔ. Δεν υπάρχει κανενός είδους απόρρητο για τον ΥΠΔ και πρέπει να είναι σαφές ότι για την ενάσκηση των καθηκόντων του, θα πρέπει να έχει πρόσβαση σε κάθε προσωπικό δεδομένο, εντός της οντότητας, ακόμη και εκείνα της νομικής υπηρεσίας.

Παράλληλα, για την συνεχή εκπαίδευση και κατάρτιση του ΥΠΔ, και τη διατήρηση της εμπειρογνωσίας του, που κρίνεται απαραίτητη, θα πρέπει να εξασφαλίζεται η πρόσβαση του σε σεμινάρια, συνέδρια, εκδηλώσεις στο εσωτερικό και το εξωτερικό, σε βιβλία, μελέτες, επιστημονικά περιοδικά, να του παρέχονται συνδρομές σε νομικές εκδόσεις και ψηφιακές βάσεις δεδομένων.

Τα ανωτέρω όλα, αποτελούν μια σειρά από κρίσιμα και χρήσιμα, κονδύλια-εφόδια τα οποία, θα πρέπει να παρέχονται στον ΥΠΔ, ώστε να εκτελεί, το έργο του, απρόσκοπτα, άρτια, αποτελεσματικά, εξοπλισμένος, με τα απαραίτητα εφόδια.

3) ΑΝΕΞΑΡΤΗΣΙΑ ΣΕ ΣΧΕΣΗ ΜΕ ΤΟΝ Υ.Ε. ΚΑΙ Ε.Ε.

Ο ΥΠΔ δεν λαμβάνει εντολές κατά την άσκηση των καθηκόντων του, δεν απολύεται ούτε υφίσταται κυρώσεις, από τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία. (α. 38 παρ. 3 ΓΚΠΔ). Με αυτές τις διατάξεις εξαιρείται ο ΥΠΔ από το διευθυντικό δικαίωμα του εργοδότη ή την ιεραρχική σχέση με τον προϊστάμενό του και απολαμβάνει την ανεξαρτησία, που του παρέχεται κατά την ενάσκηση των καθηκόντων του. Επομένως, δεν θα πρέπει να δέχεται πιέσεις ή να καθοδηγείται, ώστε να χειριστεί μια υπόθεση με συγκεκριμένο τρόπο ή για να λάβει μία συγκεκριμένη θέση.

Στην αιτιολογική σκέψη του αρ. 97 του Προοιμίου του ΓΚΠΔ, αναφέρεται επιπροσθέτως ότι οι υπεύθυνοι προστασίας δεδομένων, «ανεξάρτητα από το κατά πόσον είναι υπάλληλοι του υπευθύνου επεξεργασίας, θα πρέπει να είναι σε θέση να εκτελούν τις υποχρεώσεις και τα καθήκοντά τους με ανεξάρτητο τρόπο». Όπως επίσης και η Οδηγία (ΕΚ) 95/46, στο άρθρο 18 παρ. 2 αναφερόταν στον προαιρετικό τότε ΥΠΔ ότι θα διασφάλιζε, κατ' ανεξάρτητο τρόπο, την εσωτερική εφαρμογή των εθνικών διατάξεων που θεσπίζονταν με την εν λόγω οδηγία. Αντίστοιχη και η ρύθμιση του άρθρου 24 παρ. 1 γ', του Κανονισμού (ΕΚ) 45/2001 για τον κοινοτικό ΥΠΔ, όπου επισημαίνεται ότι θα διασφαλίζει, κατά τρόπο ανεξάρτητο, την εσωτερική εφαρμογή του ανωτέρω Κανονισμού.

Η απαγόρευση απόλυσης και κυρώσεων, αναφορικά με την ενάσκηση των καθηκόντων του, ενδυναμώνει την ανεξαρτησία του ΥΠΔ. Βέβαια, μπορεί να απολυθεί για άλλους λόγους, που δεν συνδέονται ευθέως, με τα καθήκοντά του ως ΥΠΔ όπως κάθε άλλος εργαζόμενος, ωστόσο ο Κανονισμός δεν διευκρινίζει πως και πότε μπορεί ένας ΥΠΔ να απολυθεί ή να αντικατασταθεί. Εντούτοις, καθίσταται σαφές ότι, όσες περισσότερες εγγυήσεις παρέχονται, στον ΥΠΔ κατά της καταχρηστικής του απολύσεως τόσο, πιο ανεξάρτητος και αυτόνομος, θα καθίσταται. Για παράδειγμα, στον εθνικό

εφαρμοστικό Νόμο 4624/2029, στο άρθρο 7 παρ. 4, για τα Προσωπικά Δεδομένα, αναφέρεται ότι «η καταγγελία της συμβάσεώς του ή η ανάκληση των καθηκόντων του στην περίπτωση που και αυτός είναι υπάλληλος του δημοσίου φορέα, επιτρέπεται μόνον για σπουδαίο λόγο. Μετά τη λήξη της σύμβασης εργασίας του ως ΥΠΔ, δεν μπορεί να απολυθεί για ένα έτος μετά το πέρας του διορισμού του, εκτός αν ο δημόσιος φορέας έχει σπουδαίο λόγο να προβεί στην καταγγελία της σύμβασης.»

Σύμφωνα και με τις κατευθυντήριες γραμμές για τους ΥΠΔ[72], η ανεξαρτησία που επιτάσσει ο ΓΚΠΔ, σημαίνει ότι οι ΥΠΔ δεν πρέπει να καθοδηγούνται για το πως θα χειριστούν μια υπόθεση, πως να εξετάσουν μια καταγγελία ή να εξαναγκάζονται να λάβουν ορισμένη θέση για ένα θέμα. Ωστόσο, αυτή η ανεξαρτησία που απολαμβάνουν, σε καμία περίπτωση, δεν θα πρέπει να ερμηνευτεί ως μία ευκαιρία για να δρουν ανεξέλεγκτα και ασύδοτα και ως πρόφαση για να λαμβάνουν αποφάσεις καθ' υπέρβαση των καθηκόντων τους.

Σχετικά με το συγκεκριμένο θέμα, το άρθρο 38 παράγραφος 3 του ΓΚΠΔ, προβλέπει ότι ο υπεύθυνος προστασίας δεδομένων «λογοδοτεί απευθείας στο ανώτατο διοικητικό επίπεδο του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία». Συμφώνα με την Ομάδα Εργασίας του άρθρου 29, με την απευθείας λογοδοσία, διασφαλίζεται η πλήρης ενημέρωση της ανώτερης διοίκησης, για τις συμβουλές και τις συστάσεις που διατυπώνει ο ΥΠΔ στο πλαίσιο του καθήκοντός του, να ενημερώνει και να συμβουλεύει τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία.[73] Αν ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία, λαμβάνει αποφάσεις που έρχονται σε σύγκρουση με τον ΓΚΠΔ και με τις συμβουλές του ΥΠΔ, τότε ο ΥΠΔ, θα πρέπει να έχει τη δυνατότητα να γνωστοποιήσει την αντίθετη γνώμη

72. Κατευθυντήριες γραμμές για ΥΠΔ της Ομάδας Εργασίας του άρθρου 29,σελ. 20.

73. Κατευθυντήριες γραμμές για ΥΠΔ της Ομάδας Εργασίας του άρθρου 29,σελ. 20.

του, στο ανώτατο διοικητικό επίπεδο του οργανισμού και στους υπεύθυνους λήψης των αποφάσεων.

Επιπρόσθετα, με την απευθείας λογοδοσία, στο ανώτατο διοικητικό επίπεδο του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, καταγράφεται, η δράση του και οι ενέργειες στις οποίες προβαίνει. Έτσι, ισοσταθμίζεται, η απόλυτη ελευθερία και ανεξαρτησία της οποίας χαίρει, ο ΥΠΔ.

Η υποχρέωση λογοδοσίας, του ΥΠΔ, σύμφωνα με την Ομάδα Εργασίας του άρθρου 29, μπορεί να ικανοποιείται και με την κατάρτιση ετήσιας έκθεσης δραστηριοτήτων από τον ΥΠΔ και την υποβολή της στο ανώτατο διοικητικό επίπεδο.[74]Η έκθεση αυτή, ενδεικτικά, μπορεί να περιλαμβάνει μια εισαγωγή με παράθεση του θεσμικού πλαισίου που παρακολουθεί ο ΥΠΔ, στοιχεία για τον ορισμό του, περιγραφή των κοινοποιήσεων παραβάσεων στην Αρχή, αποτελέσματα ελέγχων που διεξήχθησαν, αναφορά των καταγγελιών που έχουν ληφθεί αλλά και προτάσεις για τη βελτίωση της προστασίας των προσωπικών δεδομένων.

4)ΕΠΙΚΟΙΝΩΝΙΑ

Σύμφωνα με το άρθρο 38 παρ. 4 ΓΚΠΔ, τα υποκείμενα των δεδομένων μπορούν να επικοινωνούν και να συμβουλεύονται τον ΥΠΔ, για κάθε ζήτημα σχετικό με την επεξεργασία των δεδομένων τους και με την άσκηση των δικαιωμάτων τους δυνάμει του παρόντος κανονισμού. Η διάταξη αυτή, αντιστοιχεί και στο καθήκον του ΥΠΔ να ανταποκρίνεται στην επικοινωνία των υποκειμένων των δεδομένων, αλλά τίθεται και στο άρθρο 38,που ορίζει τη θέση του ΥΠΔ. Ο ΥΠΔ, λοιπόν δε δρα, αποκομμένος από την

74. Κατευθυντήριες γραμμές για ΥΠΔ της Ομάδας Εργασίας του άρθρου 29,σελ. 20.

υπόλοιπη οντότητα, αντίθετα θα πρέπει να είναι εύκολη η ανεύρεση των στοιχείων επικοινωνίας μαζί του, από οποιοδήποτε υποκείμενο το επιθυμεί. Ως εκ τούτου αποτελεί υποχρέωση του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία να διαμορφώσουν τις πρακτικές εκείνες και να φροντίσουν, ώστε τα υποκείμενα να αναγνωρίζουν τον ΥΠΔ ως «πρόσωπο επικοινωνίας», για θέματα προστασίας δεδομένων και να μην διστάζουν να επικοινωνήσουν μαζί του. Αυτό μπορεί να επιτευχθεί δημοσιεύοντας τα στοιχεία επικοινωνίας του, όπως έχει αναφερθεί, με τη δημιουργία ειδικού ηλεκτρονικού ταχυδρομείου ή τη δημιουργία ειδικής τηλεφωνικής γραμμής, εντός της οντότητας.

5) ΑΠΟΡΡΗΤΟ ΚΑΙ ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ

Η διάταξη του άρθρου 38 παρ. 5 ΓΚΠΔ εισάγει την μόνη περίπτωση ευθύνης του ΥΠΔ. Σύμφωνα με την ανωτέρω διάταξη, ο ΥΠΔ δεσμεύεται από την τήρηση του απορρήτου ή της εμπιστευτικότητας σχετικά με την εκτέλεση των καθηκόντων του, σύμφωνα με το δίκαιο της Ένωσης ή Κράτους μέλους.

Σε περίπτωση που, ο ΥΠΔ δεν παρέχει ορθές συμβουλές, κατά τα συμβουλευτικά καθήκοντά του, δεν μπορεί να απολυθεί ή να του επιβληθούν κυρώσεις. Ωστόσο, η δέσμευση που φέρει ο ΥΠΔ, ως προς την τήρηση των κανόνων απορρήτου και της εμπιστευτικότητας, συνεπάγεται ατομική του ευθύνη.[75] Η ατομική του ευθύνη αυτή, μπορεί να φτάσει μέχρι το σημείο της απολύσεώς του.

Οι κανόνες προστασίας προσωπικών δεδομένων πρέπει να χαίρουν σεβασμού

75. Σωτηρόπουλος Βασίλης,2017, «Υπεύθυνος Προστασίας Δεδομένων-Εργαλειοθήκη για τον νέο θεσμό σε δημόσιο και ιδιωτικό τομέα», Εκδόσεις Σάκκουλα, σελ. 128

και να τηρούνται και από τον ίδιο τον ΥΠΔ, για τις επεξεργασίες δεδομένων στις οποίες προβαίνει κατά την ενάσκηση των καθηκόντων του. Το γεγονός, ότι δεν υφίσταται κυρώσεις για τις αποφάσεις και τις συμβουλές, που παρέχει κατά την ενάσκηση των καθηκόντων του, δεν συνεπάγεται ότι μπορεί να δρα ανεξέλεγκτα. Έτσι εφόσον, παραβεί, το καθήκον εχεμύθειας και απορρήτου, που προβλέπεται στον Γενικό Κανονισμό τότε, βάσει των θεσμοθετημένων διατάξεων,στο εσωτερικό δίκαιο του κάθε κράτους, μπορεί να του επιβληθούν κυρώσεις. Πρόκειται, λοιπόν, για την μόνη εξαίρεση από τον κανόνα, της μη επιβολής κυρώσεων στον ΥΠΔ κατά την ενάσκηση των καθηκόντων του.

Στο άρθρο 39 παρ. 6, του Σχεδίου Νόμου για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα στην Ελλάδα, που είχε τεθεί υπό δημόσια διαβούλευση, προβλέπονταν ότι, «ο υπεύθυνος προστασίας δεδομένων που παραβιάζει την υποχρέωση εχεμύθειας που τον βαρύνει στο πλαίσιο του επαγγελματικού απορρήτου ανακοινώνοντας ή αποκαλύπτοντας σε άλλον γεγονότα ή πληροφορίες που περιήλθαν σε γνώση του από τη θέση του κατά την εκτέλεση των καθηκόντων του ή επ’ ευκαιρία αυτών, με σκοπό να ωφεληθεί ο ίδιος ή τρίτος, ή για να βλάψει τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία ή το υποκείμενο των δεδομένων ή οποιονδήποτε τρίτο, τιμωρείται με ποινή φυλάκισης τουλάχιστον ενός (1) έτους και χρηματική ποινή από δέκα χιλιάδες (10.000) ευρώ έως εκατό χιλιάδες (100.000) ευρώ, εάν η πράξη δεν τιμωρείται βαρύτερα από άλλες διατάξεις». Εν τέλει εν λόγω διάταξη απαλείφθηκε, διότι θεωρήθηκε ότι μπορεί να αποτελέσει ανασταλτικό παράγοντα για την ανάληψη καθηκόντων του ΥΠΔ.

Στο άρθρο 7 παρ.5 του εφαρμοστικού Νόμου 4624/2019, που εν τέλει ψηφίσθηκε, ρητά προβλέπεται ότι ο «ΥΠΔ είναι υποχρεωμένος να διατηρεί εμπιστευτικότητα ως προς την ταυτότητα των υποκειμένων των δεδομένων και σχετικά με τις περιστάσεις, που επιτρέπουν την εξαγωγή συμπερασμάτων, ως προς το

υποκείμενο των δεδομένων, εκτός αν η ταυτότητα του υποκειμένου αποκαλύπτεται από αυτό». Παράλληλα, ορίζεται ότι σε περίπτωση που, κατά την ενάσκηση του έργου του, λάβει γνώση δεδομένων προσωπικού χαρακτήρα, για το οποία ο επικεφαλής του δημοσίου φορέα, έχει το δικαίωμα να αρνηθεί να καταθέσει ως μάρτυρας, για επαγγελματικούς λόγους, το ίδιο θα ισχύει και για τον ΥΠΔ αλλά και για τους βοηθούς του.

Στην περίπτωση παραβίασης της υποχρεώσεως αυτής του ΥΠΔ, θα μπορούσε να τύχει αναλογικής εφαρμογής το άρθρο 371 παρ. 1, του ΠΚ, όπου προβλέπονται ποινικές κυρώσεις, για την παραβίαση της επαγγελματικής εχεμύθειας από ορισμένους επαγγελματίες, όπου λόγω της φύσεως του επαγγέλματός τους, συνήθως τους εμπιστεύονται ιδιωτικά απόρρητα. Συγκεκριμένα, στο εν λόγω άρθρο προβλέπεται: « Κληρικοί, δικηγόροι και κάθε είδους νομικοί παραστάτες, συμβολαιογράφοι, γιατροί, μαίες, νοσοκόμοι, φαρμακοποιοί και άλλοι στους οποίους κάποιοι εμπιστεύονται συνήθως, λόγω του επαγγέλματος τους ή της ιδιότητάς τους ιδιωτικά απόρρητα, καθώς και οι βοηθοί των προσώπων αυτών, τιμωρούνται με χρηματική ποινή ή με φυλάκιση μέχρι ενός έτους, αν φανερώσουν ιδιωτικά απόρρητα, που τους τα εμπιστεύτηκαν ή που τα έμαθαν, λόγω του επαγγέλματός τους ή της ιδιότητάς τους».

Και σε άλλα κράτη μέλη, όπου έχει θεσμοθετηθεί, εσωτερικός εφαρμοστικός νόμος, του Κανονισμού, έχει προβλεφθεί ως ειδικότερη διάταξη η υποχρέωση του ΥΠΔ, να τηρεί το απόρρητο, κατά την ενάσκηση των καθηκόντων του.

Ειδικότερα, στην **Αυστρία**, απαιτείται ο ΥΠΔ και τα άτομα, που εργάζονται γι αυτόν, να τηρούν απόρρητα τα στοιχεία της ταυτότητας των ατόμων,[76] που έχουν επικοινωνήσει μαζί τους ή έχουν επεξεργαστεί προσωπικά τους δεδομένα και να

76. DLA PIPER, Data Protection laws of the world, Austria-DPO.

διασφαλίζουν ότι, δεν θα αποκαλυφθεί οποιαδήποτε πληροφορία, που μπορεί να προδώσει την ταυτότητα αυτών.

Στην **Δανία**, επίσης, προβλέπεται, ειδικότερη ρύθμιση, βάσει της οποίας, ο ΥΠΔ, υπό τον εθνικό νόμο (Danish Data Protection Act), υπόκειται σε καθήκον εχεμύθειας και απαγορεύεται, να μεταφέρει και να εκμεταλλεύεται δεδομένα, που απέκτησε λόγω της ιδιότητάς του, ως ΥΠΔ.[77]

Στην **Γερμανία,** ο εθνικός νόμος (η BDSG) ορίζει, ότι ο υπεύθυνος προστασίας δεδομένων δεσμεύεται από το απόρρητο, όσον αφορά την ταυτότητα των προσώπων στα οποία αναφέρονται τα δεδομένα και τις περιστάσεις που επιτρέπουν την αναγνώριση της ταυτότητας, των υποκειμένων των δεδομένων, υπό την ρητή εξαίρεση, που το υποκείμενο, στο οποίο αναφέρονται τα δεδομένα, τους απαλλάσσει από αυτή την υποχρέωση. [78]

Στην **Ολλανδία,** ο εσωτερικός νόμος, παρέχει λεπτομερέστερες πληροφορίες σχετικά με την υποχρέωση τήρησης του απορρήτου, ορίζοντας ότι ο ΥΠΔ πρέπει να τηρεί το απόρρητο, κάθε πληροφορίας, η οποία του γνωστοποιείται, μέσω καταγγελίας ή κάποιου αιτήματος, του υποκειμένου των δεδομένων, εκτός εάν το υποκείμενο των δεδομένων συμφωνεί, με την αποκάλυψη των δεδομένων που το αφορούν.[79]

6) ΣΥΓΚΡΟΥΣΗ ΣΥΜΦΕΡΟΝΤΩΝ

Ο ΥΠΔ μπορεί να επιτελεί έτερα καθήκοντα και να αναλαμβάνει και άλλες

77.DLA PIPER, Data Protection laws of the world, Denmark-DPO.

78.DLA PIPER, Data Protection laws of the world, Germany-DPO.

79. IP, Tech & Data, General Data Protection Regulation, «Overview of the latest developments regarding the national implementation of the GDPR requirements».

υποχρεώσεις, εκτός αυτών του ΥΠΔ. Ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία, θα πρέπει να διασφαλίζουν ότι, τα εν λόγω καθήκοντα και υποχρεώσεις, δεν συνεπάγονται σύγκρουση συμφερόντων, βάσει του άρθρου 38 παρ. 6 του ΓΚΠΔ.

Αυτό σημαίνει ότι ο ΥΠΔ δεν μπορεί να κατέχει, εντός της οντότητας, θέση από την οποία θα μπορεί να καθορίζει τα μέσα και τους σκοπούς, της επεξεργασίας προσωπικών δεδομένων, ενεργώντας σαν να ήταν ο αυτός, ο υπεύθυνος επεξεργασίας. Στις «Κατευθυντήριες γραμμές» της Ομάδας Εργασίας του άρθρου 29, αναφέρεται ότι, η σύγκρουση συμφερόντων, πρέπει να εξετάζεται ανά περίπτωση, εάν συντρέχει.[80] Παράλληλα, επισημαίνεται ότι, περισσότερες πιθανότητες να προκύψει σύγκρουση συμφερόντων, υπάρχουν όταν το άτομο που ορίζεται ως ΥΠΔ, κατέχει εντός του οργανισμού, ήδη θέση ανώτερου στελέχους. Υπάρχει όμως, πιθανότητα, ακόμα και αν πρόκειται για θέσεις ιεραρχικά κατώτερες στην οργανωτική δομή μίας οντότητας, να μπορεί να καθορισθεί από αυτές, ο σκοπός και τα μέσα τις επεξεργασίας δεδομένων, με αποτέλεσμα, η σύγκρουση συμφερόντων να φαντάζει πιθανή. Ακόμα και στην περίπτωση που, έχει ορισθεί εξωτερικός ΥΠΔ, εφόσον αυτός κληθεί να εκπροσωπήσει σε κάποια νομική διαδικασία, τον υπεύθυνο/εκτελούντα την επεξεργασία, ενώπιον δικαστηρίων για παραβίαση προσωπικών δεδομένων, τότε ενδέχεται να προκύψει μία κατάσταση, που θα ενέχει σοβαρό κίνδυνο πρόκλησης σύγκρουσης συμφερόντων.

Ο ΥΠΔ, όπως προαναφέρθηκε, χαίρει λειτουργικής και οικονομικής ανεξαρτησίας, αυτονομίας και ασυλίας. Ως βασική του προτεραιότητα, θα πρέπει να έχει τα καθήκοντα του ως ΥΠΔ και δεν πρέπει να αναλαμβάνει άλλα καθήκοντα που έρχονται σε σύγκρουση με αυτά.

---

80. Κατευθυντήριες γραμμές για ΥΠΔ της Ομάδας Εργασίας του άρθρου 29,σελ.22.

Για παράδειγμα, όπως προαναφέρθηκε δεν μπορεί να διορισθεί, ως ΥΠΔ, ο IT μάνατζερ της εταιρίας/οργανισμού, γεγονός που συνέβη, στη Βαυαρία. Η BayLDA (Βαυαρική Αρχή) υποστήριξε ότι, η θέση ενός διαχειριστή ΤΠ, είναι ασυμβίβαστη με τη θέση του ΥΠΔ, διότι ο ΥΠΔ θα πρέπει να παρακολουθεί τον εαυτό του, δηλαδή κατά πόσον οι δραστηριότητές του, ως υπευθύνου πληροφορικής συμμορφώνονται με τον νόμο περί προστασίας δεδομένων. Αυτή η αυτοπαρακολούθηση αντιφάσκει, με την απαιτούμενη ανεξαρτησία που αναμένεται από τον ΥΠΔ.

Αντίστοιχη σύγκρουση συμφερόντων, θα μπορούσε επίσης, να διαπιστωθεί εάν ο ΥΠΔ είναι επικεφαλής σε άλλους τομείς, που εμπλέκονται σε μεγάλο βαθμό με την επεξεργασία προσωπικών δεδομένων, όπως είναι το νομικό τμήμα ή το τμήμα μάρκετινγκ, μιας εταιρίας.

Στον ισχύοντα γερμανικό νόμου περί προστασίας δεδομένων, προβλέπεται ότι ο ΥΠΔ, δεν θα πρέπει να αναλαμβάνει καθήκοντα, που να αντιβαίνουν στις υποχρεώσεις παρακολούθησης του ΥΠΔ.

Η Αρχή Προστασίας Δεδομένων της Βαυαρίας (BayLDA) σε πρόσφατη έκθεσή της, αναφέρει ότι τα μέλη της νομικής υπηρεσίας, μιας εταιρίας, ενδέχεται σε ορισμένες περιπτώσεις, να κληθούν να αναλάβουν καθήκοντα, που μπορεί να επιφέρουν μία πιθανή σύγκρουση συμφερόντων, γεγονός που αποκλείει, αυτομάτως τα άτομα αυτά, από την ανάληψη του ρόλου του ΥΠΔ.[81] Ειδικότερα, εάν ο νομικός σύμβουλος, εκπροσωπεί την εταιρεία σε μια νομική-δικαστική διαδικασία (ιδίως όσον αφορά τις νομικές ενέργειες εναντίον εργαζομένων ή πελατών, οι οποίες ενδέχεται να αφορούν ζητήματα σχετικά με την προστασία της ιδιωτικής ζωής), και παράλληλα, δρα ως ΥΠΔ της εταιρίας, τότε ο δικηγόρος υπόκειται σε σύγκρουση συμφερόντων και σε

81. Kaufmann Julia and Guenther Jan-Philipp, 9/01/2018 and 21/11/2016,«Germany: Data Protection Officer must not have a conflict of interests-Global Compliance News».

καμία περίπτωση δεν μπορεί να είναι ένας ανεξάρτητος ΥΠΔ. Έτσι, όμως, αυτόματα μειώνονται σημαντικά οι πιθανοί υποψήφιοι, για το ρόλο του ΥΠΔ, από το εσωτερικό της οντότητας.

Κατ 'αρχήν, ένα μέλος της εσωτερικής ομάδας νομικών συμβούλων της εταιρείας, θα είναι κατάλληλος υποψήφιος για ΥΠΔ, ειδικά εάν αυτός ο νομικός σύμβουλος έχει εμπειρία προστασίας προσωπικών δεδομένων. Επιπλέον, οι δεξιότητες ενός δικηγόρου μπορούν να βοηθήσουν, στην αντιμετώπιση των ζητημάτων προστασίας δεδομένων. Εντούτοις, μια εταιρεία που προτίθεται να διορίσει μέλος της νομικής υπηρεσίας της, ως ΥΠΔ πρέπει να διασφαλίσει, πρώτα ότι αυτός ο εσωτερικός νομικός, αποκλείεται από την εκπροσώπηση της εταιρείας, σε οποιαδήποτε νομική διαδικασία, που μπορεί να προκαλέσει πιθανή σύγκρουση συμφερόντων.

Η Ομάδα Εργασίας του άρθρου 29, αναφέρει ότι τα άτομα με ανώτερη διευθυντική θέση, όπως ο προϊστάμενος γενικά ενός τμήματος, ο προϊστάμενος χρηματοπιστωτικού ιδρύματος, ο προϊστάμενος ιατρός, ο προϊστάμενος του τμήματος μάρκετινγκ, ο προϊστάμενος του τμήματος ανθρώπινων πόρων ή ο προϊστάμενος των τμημάτων πληροφορικής, μπορεί να έχουν σύγκρουση συμφερόντων και ως εκ τούτου δεν είναι κατάλληλα για τη θέση του DPO.[82]

Η Ομάδα Εργασίας του άρθρου 29, επιπρόσθετα, έχει καταγράψει, ορισμένες πρακτικές[83],οι οποίες αναλόγως των δραστηριοτήτων, του μεγέθους και της δομής του οργανισμού, μπορούν να αποτελέσουν για τους υπεύθυνους επεξεργασίας ή τους εκτελούντες την επεξεργασία, σημαντικό αρωγό, ώστε να αποφύγουν μια ενδεχόμενη σύγκρουση συμφερόντων εντός του οργανισμού. Ειδικότερα, 1) χρήσιμο θα ήταν να

82. Κατευθυντήριες γραμμές για ΥΠΔ της Ομάδας Εργασίας του άρθρου 29,σελ.22.

83. Κατευθυντήριες γραμμές για ΥΠΔ της Ομάδας Εργασίας του άρθρου 29,σελ. 22-23.

εντοπίζουν, εκ των προτέρων, τις θέσεις που είναι ενδεχομένως ασύμβατες με τα καθήκοντα του υπευθύνου προστασίας δεδομένων, 2) να καταρτίζουν εσωτερικό κανονισμό για τον συγκεκριμένο σκοπό, με γνώμονα την αποτροπή των συγκρούσεων συμφερόντων, 3) να παρέχουν μια ενδελεχή επεξήγηση των συγκρούσεων συμφερόντων, 4) να ανακοινώνουν ότι δεν υφίσταται σύγκρουση συμφερόντων για τον υπεύθυνο προστασίας δεδομένων που έχουν ορίσει, όσον αφορά την άσκηση των καθηκόντων του υπό τη συγκεκριμένη ιδιότητα, ως έναν τρόπο ενίσχυσης της ευαισθητοποίησης γύρω από τη συγκεκριμένη απαίτηση, 5) να συμπεριλαμβάνουν στον εσωτερικό κανονισμό του οργανισμού, εγγυήσεις και να διασφαλίζουν ότι η ανακοίνωση για την πλήρωση της θέσης του υπευθύνου προστασίας δεδομένων ή η σύμβαση παροχής υπηρεσιών είναι επαρκώς ακριβείς και λεπτομερείς, ώστε να αποτρέπονται οι συγκρούσεις συμφερόντων.

Στις 9 Νοεμβρίου 2018, ο Επίτροπος Πληροφοριών της Σλοβενίας, δημοσίευσε στην επίσημη ιστοσελίδα του, συστάσεις σχετικά με το ρόλο του ΥΠΔ, που περιλαμβάνουν κατάλογο καθηκόντων, η ανάληψη των οποίων από τον ΥΠΔ, θα οδηγεί σε σύγκρουση συμφερόντων.[84] Ανάμεσα σε αυτά τα καθήκοντα, που θα δημιουργούν, κίνδυνο σύγκρουσης καθηκόντων, περιλαμβάνονται αυτά που αφορούν: 1)τη λήψη αποφάσεων για τα δικαιώματα και τις υποχρεώσεις ενός ατόμου,2) τη λήψη αποφάσεων, για τη δημιουργία νέων συστημάτων αρχειοθέτησης, καθορίζοντας τους σκοπούς και το εύρος της επεξεργασίας, 3)τη λήψη αποφάσεων σχετικά με οργανωτικά και τεχνικά μέτρα για την ασφάλεια των προσωπικών δεδομένων, 4)τη λήψη αποφάσεων, σχετικά με τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες ή σε διεθνείς οργανισμούς, 5)την απόφαση για τη διεξαγωγή αξιολόγησης αντικτύπου προστασίας δεδομένων (DPIA), 6) τη λήψη απόφασης για τη δημιουργία ή

84.Euro Cloud Europe, 23/11/2018, «Slovenia’s ICO defines DPO’s additional tasks that could result in a conflict of interests».

την ενημέρωση ενός μητρώου δραστηριοτήτων επεξεργασίας, και 7) άλλα καθήκοντα, που περιλαμβάνουν τη λήψη αποφάσεων σχετικά με τα προσωπικά δεδομένα, όπου ο ΥΠΔ θα βρεθεί σε κατάσταση, όπου θα πρέπει να ελέγξει τις δικές του αποφάσεις.

Όταν διαπιστωθεί η ύπαρξη σύγκρουσης συμφερόντων τότε, ο ίδιος ο ΥΠΔ, θα πρέπει να ενημερώσει τα ανώτατα στελέχη της οντότητας και επιπρόσθετα, θα πρέπει να προτείνει ο ίδιος, λύσεις για να διευθετηθεί το ζήτημα της συγκρούσεως, δεδομένου, φυσικά ότι ο υπεύθυνος επεξεργασίας και ο εκτελών, έχουν ήδη πράξει ότι απαιτείται, για να την αποφύγουν και έχουν λάβει όλα τα προληπτικά μέτρα. Σε μία τέτοια περίπτωση, εάν δεν φροντίσει να ενημερώσει ο ΥΠΔ, τότε ιδρύεται, βάσιμος και δικαιολογημένος λόγος, για την αντικατάστασή του.

10. ΤΑ ΚΑΘΗΚΟΝΤΑ ΤΟΥ ΥΠΔ

Ο ΥΠΔ, έχει όσα καθήκοντα αναφέρονται στο άρθρο 39 του ΓΚΠΔ. Η απαρίθμηση αυτή όμως, δεν είναι περιοριστική αλλά ενδεικτική. Τα κράτη μέλη, στις εθνικές νομοθεσίες τους, έχουν τη δυνατότητα να προβλέψουν πρόσθετα καθήκοντα για τον ΥΠΔ, ώστε να φέρει εις πέρας το απαιτητικό του έργο, τη διασφάλιση δηλαδή, της εφαρμογής των κανόνων προστασίας προσωπικών δεδομένων.

Στον εθνικό εφαρμοστικό Νόμο 4624/2019, για τα Προσωπικά Δεδομένα στη στο άρθρο 8 εισάγεται διάταξη, που προβλέπει επιπλέον καθήκοντα για τον ΥΠΔ, με τη ρητή επιφύλαξη ότι αυτά δεν θα οδηγήσουν σε σύγκρουση συμφερόντων. Ειδικότερα τα καθήκοντα αυτά είναι τα ακόλουθα:

«α) να ενημερώνει και να συμβουλεύει τον δημόσιο φορέα και τους εργαζομένους που διενεργούν την επεξεργασία σχετικά με τις υποχρεώσεις τους, σύμφωνα με τις διατάξεις του παρόντος και κάθε άλλης νομοθεσίας για την προστασία δεδομένων προσωπικού χαρακτήρα· β) να παρακολουθεί την τήρηση των διατάξεων του παρόντος και κάθε άλλης νομοθεσίας για την προστασία δεδομένων προσωπικού χαρακτήρα, και των πολιτικών του δημόσιου φορέα σε σχέση με την προστασία των δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων της λογοδοσίας, καθώς και των σχετικών ελέγχων· γ) να παρέχει συμβουλές όσον αφορά την εκτίμηση αντικτύπου για την προστασία των δεδομένων προσωπικού χαρακτήρα και να παρακολουθεί την εφαρμογή της σύμφωνα με το άρθρο 65·δ) να συνεργάζεται με την Αρχή· ε) να ενεργεί ως σημείο επαφής με την Αρχή σε θέματα, που αφορούν την επεξεργασία, συμπεριλαμβανομένης της προηγούμενης διαβούλευσης, που αναφέρεται στο άρθρο 67, και να τη συμβουλεύεται, κατά περίπτωση, σχετικά με οποιοδήποτε άλλο θέμα.»

Κατά την ενάσκηση αυτών των καθηκόντων του ο ΥΠΔ, θα πρέπει να λαμβάνει υπόψη παραμέτρους, όπως το κίνδυνο που παρουσιάζει η επεξεργασία, τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας. Λαμβάνοντας

υπόψη αυτούς τους παράγοντες, θα πρέπει να δίνει προτεραιότητα στην εξέταση και ενασχόληση με τις πράξεις επεξεργασίας, που συνδέονται με υψηλό κίνδυνο.[85]

Ο ΥΠΔ, κατ' αρχήν συνδράμει τον υπεύθυνο επεξεργασίας ή τον εκτελούντα στα ζητήματα που αφορούν την προστασία προσωπικών δεδομένων. Επιπλέον, οφείλει να ενημερώνει τον οργανισμό, για τις βαρύτατες συνέπειες, που επισύρει η μη συμμόρφωση με τον Κανονισμό. Οποιαδήποτε αστοχία, ή λάθος εκτίμηση, μπορεί να επιφέρει, στον οργανισμό, μεγάλο κόστος, όχι μόνο οικονομικό αλλά και εν γένει επιχειρηματικό. Έτσι, ο ΥΠΔ καλείται να παρέχει συμβουλές, σχετικά με τις βέλτιστες πρακτικές, για την προστασία των προσωπικών δεδομένων, που υπόκεινται σε επεξεργασία, από τον εκάστοτε οργανισμό ή οντότητα. Καθίσταται σαφές, λοιπόν, ότι ο ρόλος του ΥΠΔ, θα είναι προληπτικός και όχι κατασταλτικός, θα παρέχει συμβουλές προληπτικά, πριν προκύψει οποιοδήποτε ζήτημα παραβίασης προσωπικών δεδομένων.

1)ΕΝΗΜΕΡΩΤΙΚΟΣ Ή ΣΥΜΒΟΥΛΕΥΤΙΚΟΣ ΧΑΡΑΚΤΗΡΑΣ

Σύμφωνα με το άρθρο 39 παρ.1 περ. α' του ΓΚΠΔ, ο υπεύθυνος προστασίας ενημερώνει και συμβουλεύει τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία και τους υπαλλήλους που επεξεργάζονται για τις υποχρεώσεις τους, που απορρέουν από τον παρόντα Κανονισμό και από άλλες διατάξεις της Ένωσης ή του κράτους μέλους σχετικά με την προστασία δεδομένων.

Αρχικά, θα πρέπει να γίνει κατανοητό ότι, ο ΓΚΠΔ, παρόλο που είναι ένας ευρωπαϊκός νόμος, εφαρμόζεται και σε οποιονδήποτε, οπουδήποτε στον κόσμο, που

85.Τσόλιας Γρηγόρης, σε Κοτσαλής Λεωνίδας/Μενουδάκος Κωνσταντίνος (επ.),2018, «Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων (GDPR), Νομική διάσταση και πρακτική εφαρμογή», Νομική Βιβλιοθήκη, σελ. 211.

που επεξεργάζεται προσωπικά δεδομένα, κατοίκων της Ευρωπαϊκής Ένωσης. [86]

Προκειμένου λοιπόν, να ενημερώνει έγκυρα και έγκαιρα, ο ΥΠΔ θα πρέπει να παρακολουθεί στενά, τις εξελίξεις στην προστασία δεδομένων, καταγράφοντας αποφάσεις και οδηγίες που εκδίδονται από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, τις γνωμοδοτήσεις της Ομάδας του άρθρου 29, τα κείμενα του Ευρωπαίου Επόπτη Προστασίας Δεδομένων, τη νομολογία των εθνικών δικαστηρίων, των δικαστηρίων άλλων κρατών μελών, αλλά και κρατών ανά το κόσμο.

Κατ' αυτόν το τρόπο, θα κατορθώσει να αποκτήσει, παγκόσμια και σφαιρική γνώση, σχετικά με την προστασία δεδομένων, την οποία θα διοχετεύει και θα εφαρμόζει στον οργανισμό, ευθυγραμμίζοντας τις δραστηριότητές του, με τις βέλτιστες πρακτικές, που θα οδηγήσουν, στην ελαχιστοποίηση των κινδύνων, που συνεπάγεται η επεξεργασία των προσωπικών δεδομένων.

Στα πλαίσια της συνεχούς καταρτίσεως, ο ΥΠΔ, επιβάλλεται να παρακολουθεί ημερίδες, συνέδρια και σεμινάρια που διοργανώνονται και αφορούν την προστασία προσωπικών δεδομένων. Για αυτό ακριβώς το λόγο, η οντότητα στην οποία θητεύει, θα πρέπει να του παρέχει τους απαραίτητους οικονομικούς πόρους(όπως προδιατυπώθηκε). Με αυτό τον τρόπο, θα διατηρεί τις γνώσεις του σε ικανοποιητικό επίπεδο, φροντίζοντας παράλληλα, να εμπλουτίζει και να διευρύνει συνεχώς, το γνωστικό του πεδίο, όσον αναφορά την προστασία των προσωπικών δεδομένων για να επιτελεί αποτελεσματικά το έργο του.

Ειδικότερα, το περιεχόμενο του ενημερωτικού και συμβουλευτικού ρόλου του υπευθύνου προστασίας δεδομένων, περιλαμβάνει την ενημέρωση και την υπενθύμιση

86. Taylor Sarah (Author), 29/3/2018, «Data Protection Officer (DPO)» e-book, Kindle Cloud Reader,σελ.12-13.

των υποχρεώσεων του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία, που απορρέουν από τον ισχύοντα Κανονισμό 679/2016 και από την Οδηγία (ΕΕ) 2016/680, στο πλαίσιο της δημιουργίας μίας κουλτούρας προστασίας προσωπικών δεδομένων, εντός της επιχείρησης.

Θα πρέπει, λοιπόν στα πλαίσια του καθήκοντος του αυτού, να ενημερώνει για τους κανόνες που διέπουν την επεξεργασία δεδομένων, όπως η αρχή της νομιμότητας, αντικειμενικότητας και διαφάνειας των δεδομένων, η αρχή της ελαχιστοποίησης των δεδομένων, η αρχή της λογοδοσίας, η αρχή του περιορισμού του σκοπού επεξεργασίας των δεδομένων.

Επίσης, έχει υποχρέωση να ενημερώσει τον υπεύθυνο επεξεργασίας, για τις περιοριστικά απαριθμούμενες περιστάσεις, του άρθρου 6 παρ. 1 του ΓΚΠΔ, υπό τις οποίες επιτρέπεται η επεξεργασία των δεδομένων. Σύμφωνα με το ανωτέρω άρθρο, η επεξεργασία είναι σύννομη μόνο όταν, συντρέχει, τουλάχιστον μία από τις ακόλουθες προϋποθέσεις: α) το υποκείμενο των δεδομένων έχει συναινέσει στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα του για έναν ή περισσότερους συγκεκριμένους σκοπούς,

β) η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή για να ληφθούν μέτρα κατ' αίτηση του υποκειμένου των δεδομένων πριν από τη σύναψη σύμβασης,

γ) η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση του υπευθύνου επεξεργασίας,

δ) η επεξεργασία είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου,

ε) η επεξεργασία είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας, που έχει ανατεθεί στον υπεύθυνο επεξεργασίας,

στ) η επεξεργασία είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, εκτός εάν έναντι των συμφερόντων αυτών υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων, που επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα, ιδίως εάν το υποκείμενο των δεδομένων είναι παιδί.

Το στοιχείο στ), δεν εφαρμόζεται στην επεξεργασία που διενεργείται από δημόσιες αρχές κατά την άσκηση των καθηκόντων τους.

Επιπρόσθετα, το καθήκον ενημέρωσης, επεκτείνεται και στην πληροφόρηση για την υποχρέωση ύπαρξης της νόμιμης συγκατάθεσης, που προβλέπεται στα άρθρα 7 και 8 του ΓΚΠΔ, του υποκειμένου των δεδομένων, όπου αυτή απαιτείται.

Αλλά και για τα ευαίσθητα δεδομένα, τα οποία απαγορεύεται να υποστούν επεξεργασία, πλην ορισμένων περιπτώσεων, θα πρέπει να ενημερώσει, τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία, ο ΥΠΔ. Στο άρθρο 9 του ΓΚΠΔ, αναφέρονται οι κατηγορίες δεδομένων, που θεωρούνται, ευαίσθητα, αλλά και οι εξαιρέσεις υπό τις οποίες αίρεται, η απαγόρευση επεξεργασίας των δεδομένων αυτών. Όσον αφορά, τις αρχές επιβολής του νόμου, εφαρμόζεται η Οδηγία (ΕΕ) 2016/680 και συγκεκριμένα το άρθρο 10, βάσει του οποίου επιτρέπεται από τις αρχές αυτές, η επεξεργασία των ευαίσθητων δεδομένων, υπό τις προϋποθέσεις που απαριθμούνται στο εν λόγω άρθρο ήτοι: α) να επιτρέπεται η επεξεργασία τους, από το δίκαιο της Ένωσης ή των κρατών μελών· β) να επιβάλλεται για την προστασία των ζωτικών συμφερόντων του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου ή γ) η

επεξεργασία αυτή να αφορά σε δεδομένα τα οποία έχουν προδήλως, δημοσιοποιηθεί από το υποκείμενο των δεδομένων.

Ο ΥΠΔ, οφείλει να ενημερώσει την οντότητα και για την νέα υποχρέωση, που θεσπίζει ο ΓΚΠΔ (άρθρα 16, 17 παρ. 1 και 18 ΓΚΠΔ), ήτοι για την υποχρέωση του υπευθύνου επεξεργασίας να ανακοινώνει κάθε διόρθωση ή διαγραφή δεδομένων προσωπικού χαρακτήρα ή περιορισμό της επεξεργασίας των δεδομένων που διενεργείται, σε κάθε αποδέκτη στον οποίο γνωστοποιήθηκαν αυτά τα δεδομένα και για τις εξαιρέσεις που προβλέπονται από τον Κανονισμό και από τα εθνικά δίκαια.

Ανάμεσα στις υποχρεώσεις του ΥΠΔ, συγκαταλέγεται και η υποχρέωση να ενημερώσει, βάσει του άρθρου 32 του ΓΚΠΔ, για τις υποχρεώσεις ασφαλείας, καθώς επίσης και για την υποχρέωση του υπευθύνου επεξεργασίας, σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα, να γνωστοποιήσει αυτή (την παραβίαση) στην Αρχή. Η γνωστοποίηση, πρέπει να γίνει αμέσως («αμελλητί») και αν αυτό δεν είναι δυνατόν, οπωσδήποτε εντός 72 ωρών, από τη στιγμή, που ο υπεύθυνος επεξεργασίας αποκτά γνώση της παραβίασης. Δεν στοιχειοθετείται αυτοτελής ευθύνη του ΥΠΔ, για να γνωστοποιήσει την παραβίαση των δεδομένων στην Αρχή, όπως συμβαίνει με τον «υπεύθυνο διασφάλισης απορρήτου». Απλώς, ο ΥΠΔ, οφείλει να ενημερώσει τον υπεύθυνο επεξεργασίας ή τον εκτελούντα γι αυτή την υποχρέωση που φέρουν.

Παράλληλα, οφείλει να ενημερώσει τον υπεύθυνο επεξεργασίας και για την ετέρα υποχρέωση του, να γνωστοποιήσει στο υποκείμενο των δεδομένων, ότι η επεξεργασία δεδομένων του, ενδέχεται να θέσει σε υψηλό κίνδυνο, τα δικαιώματα και τις ελευθερίες του.

Τέλος, ο ΥΠΔ θα πρέπει να διασφαλίζει ότι, ο υπεύθυνος επεξεργασίας είναι ενήμερος, σχετικά με τις διατάξεις που ρυθμίζουν την έκταση και τις προϋποθέσεις της

ευθύνης του, ώστε βάσει τις ευθύνης που φέρει να φροντίζει να λαμβάνει και τα κατάλληλα τεχνικά και οργανωτικά μέτρα. Έτσι, θα αποδεικνύεται και η συμμόρφωση του, με τις υποχρεώσεις που απορρέουν από τον ΓΚΠΔ.

Ο τρόπος με τον οποίο, ο ΥΠΔ, θα φέρει εις πέρας την ανωτέρω αποστολή του, ενημέρωσης του υπευθύνου επεξεργασίας και του εκτελούντα, δεν καθορίζεται. Αρωγός στην εκπλήρωση του ανωτέρω καθήκοντος του ΥΠΔ, μπορεί να σταθούν τα έγγραφα βέλτιστων πρακτικών για τους κοινοτικούς ΥΠΔ, οι οποίοι είναι επιφορτισμένοι με την ίδια υποχρέωση.

Για παράδειγμα στις κατευθυντήριες οδηγίες, για τα προσόντα του ΥΠΔ, βάσει του Κανονισμού (ΕΕ) 45/2001, αναφέρεται ότι θα πρέπει, οι ΥΠΔ να προσφέρουν κατάρτιση στους υπεύθυνους επεξεργασίας και στο προσωπικό τους, που θα εστιάζει, συγκεκριμένα στα πρακτικά μέτρα, που θα πρέπει να λάβουν προκειμένου να συμμορφωθούν με τις απαιτήσεις προστασίας δεδομένων κατά την άσκηση των καθηκόντων τους, στο πλαίσιο του αντίστοιχου οργάνου ή οργανισμού.[87] Η εκπαίδευση και η ενημέρωση, πρέπει να επαναλαμβάνεται σε τακτική βάση, ώστε να εξασφαλίζεται ότι και όλοι οι νεοεισερχόμενοι υπάλληλοι, θα λάβουν την κατάλληλη ενημέρωση. Επίσης, θα πρέπει να διοργανώνονται ειδικές συνεδριάσεις κατάρτισης-πληροφόρησης για τις διάφορες ομάδες προσωπικού, με παρόμοιες δραστηριότητες επεξεργασίας δεδομένων. Επιπρόσθετα, καλούνται να αναπτύξουν, όπου χρειάζεται, σε συνεργασία με τους υπεύθυνους επεξεργασίας, κατευθυντήριες γραμμές για την προστασία των δεδομένων, εάν σημαντικός αριθμός ατόμων εντός του οργανισμού, ασχολείται με την επεξεργασία, προσωπικών δεδομένων, προκειμένου να διασφαλίσει ότι αυτή γίνεται με συνέπεια και σύμφωνα με όλες τις απαιτήσεις του Κανονισμού.

87. Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001,14 October 2010.

2)ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΣΥΜΜΟΡΦΩΣΗΣ

Ο ΥΠΔ έχει ως καθήκον, επίσης να παρακολουθεί τη συμμόρφωση με τον ΓΚΠΔ και με άλλες διατάξεις της Ένωσης σχετικά με την προστασία των δεδομένων και με τις πολιτικές του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία, σε σχέση με την προστασία των δεδομένων προσωπικού χαρακτήρα, σύμφωνα με το άρθρο 39 παρ.1 του ΓΚΠΔ.

Στο άρθρο 97 του Προοιμίου του Κανονισμού, αναφέρεται ότι θα πρέπει να συνδράμει τον υπεύθυνο επεξεργασίας και τον εκτελούντα την επεξεργασία, στην παρακολούθηση της εσωτερικής συμμόρφωσης, με τις διατάξεις του Γενικού Κανονισμού. Ειδικότερα, το καθήκον αυτό του ΥΠΔ, περιλαμβάνει ιδίως, τη συλλογή πληροφοριών για να καθοριστούν οι επεξεργασίες των δεδομένων, την ανάλυση και τον έλεγχο της συμμόρφωσης ως προς τις επεξεργασίες δεδομένων, την πληροφόρηση, την παροχή συμβουλών και συστάσεων προς τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία.[88]Η δυνατότητα αυτή του ΥΠΔ, να διεξάγει αυτοβούλως προληπτικούς ελέγχους (άνευ καταγγελίας) για τη συμμόρφωση με τον Κανονισμό συνιστά απόρροια, της ανεξαρτησίας και της αντικειμενικότητας του.[89]

Η συμμόρφωση με τους κανόνες της προστασίας δεδομένων, αποτελεί εταιρική ευθύνη, την οποία επωμίζεται ο υπεύθυνος επεξεργασίας. Ο ΥΠΔ δεν είναι προσωπικά υπεύθυνος, όταν συντρέχει, εντός της οντότητας, περιστατικό μη συμμόρφωσης. Άλλωστε, όπως προαναφέρθηκε, δεν φέρει προσωπική ευθύνη για τυχόν αστοχίες, κατά την εκτέλεση των καθηκόντων του.

---

88. Άρθρο 97 του Προοιμίου του Κανονισμού (ΕΕ) 2016/679.

89.Τσόλιας Γρηγόρης, σε Κοτσαλής Λεωνίδας/Μενουδάκος Κωνσταντίνος (επ.),2018, «Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων (GDPR), Νομική διάσταση και πρακτική εφαρμογή», Νομική Βιβλιοθήκη, σελ. 208.

Αξίζει να σημειωθεί ότι δεν θα πρέπει να θεωρείται ότι, η συμμόρφωση έχει επιτευχθεί, μόνο, όταν τηρούνται και εφαρμόζονται όσες υποχρεώσεις, προβλέπονται στο θεσμικό πλαίσιο. Θα πρέπει, επιπλέον, να λαμβάνονται υπόψη και να ικανοποιούνται τα δικαιώματα των υποκειμένων των δεδομένων. Η κατανόηση, της ανάγκης σεβασμού των δικαιωμάτων των υποκειμένων, θα αποτελέσει σημαντικό δείγμα συμμορφώσεως με τον Κανονισμό.

Σε περίπτωση που, τα υποκείμενα των δεδομένων, αιτηθούν την ικανοποίηση κάποιου δικαιώματός τους, από τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία και δεν ικανοποιηθεί το αίτημά τους, τότε θα υπάρχει δυνατότητα με καταγγελία, να απευθυνθούν στον ΥΠΔ. Στο πλαίσιο του καθήκοντός του, για παρακολούθηση της συμμόρφωσης με το Γενικό Κανονισμό, μπορεί να εξετάζει την καταγγελία και αν υπάρχει πρόβλημα να απευθύνει σύσταση, στον υπεύθυνο επεξεργασίας, με σκοπό να συμμορφωθεί με τις διατάξεις του Κανονισμού, επανεξετάζοντας τη στάση του. Ο ΥΠΔ, θα πρέπει, όμως να εξετάσει τους λόγους, για τους οποίους δεν ικανοποιήθηκε το υποκείμενο και το ενδεχόμενο η άρνηση να εμπίπτει σε κάποια από τις εξαιρέσεις.[90,91]Επιπλέον, θα πρέπει να εξετάσει την εξέλιξη, που θα λάβει η αρνητική στάση, στην ικανοποίηση του αιτήματος του υποκειμένου, στην περίπτωση που το υποκείμενο απευθυνθεί στην Αρχή.

90.Στη **Σουηδία,** ο εκτελών την επεξεργασία προσωπικών δεδομένων, ακόμα και στη περίπτωση που δεν είναι δημόσια αρχή, μπορεί να μην παρέχει πρόσβαση στα προσωπικά δεδομένα, στα οποία ζητά, το υποκείμενο δεδομένων, εάν τα δεδομένα αυτά θα ήταν εμπιστευτικά και απόρρητα, σύμφωνα με το Σουηδικό Νόμο για την ελευθερία της πληροφόρησης και της τήρησης των επίσημων απορρήτων,(SFS 2009: 400). Στο Νόμο αυτόν προβλέπεται ότι, ο υπεύθυνος επεξεργασίας των προσωπικών δεδομένων, θα πρέπει να είναι δημόσια αρχή για να αρνηθεί την πρόσβαση στα προσωπικά δεδομένα ενός υποκειμένου.(DLA PIPER,Data Protection laws of the world, Sweden-DPO).

91. Στον εθνικό εφαρμοστικό Νόμο 4624/2019, προβλέπονται εξαιρέσεις από την ικανοποίηση των δικαιωμάτων των υποκειμένων των δεδομένων, ειδικότερα όσο αφορά δικαίωμα πρόσβασης, την ανακοίνωση παραβίασης δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων, το δικαίωμα διαγραφής και το δικαίωμα εναντίωσης.

Ειδικότερα, ανάμεσα στα δικαιώματα των υποκειμένων, τα οποία θα πρέπει να τύχουν σεβασμού από τον υπεύθυνο επεξεργασίας ή τον εκτελούντα, και θα πρέπει να ικανοποιηθούν, συγκαταλέγονται: 1) το δικαίωμα ενημέρωσης (άρθρα 13, 14 GDPR)ο υπεύθυνος επεξεργασίας υποχρεούται να παράσχει στο υποκείμενο μια σειρά από πληροφορίες, 2) το δικαίωμα πρόσβασης(άρθρο 15 GDPR) του υποκειμένου των δεδομένων, δηλαδή το δικαίωμα να διακριβώσει αν τα δεδομένα του υφίστανται επεξεργασία, 3) το δικαίωμα διόρθωσης(άρθρο 16 GDPR), ανακριβών δεδομένων που αφορούν το υποκείμενο, 4) το δικαίωμα διαγραφής (« δικαίωμα στη λήθη») (άρθρο 17 GDPR), δεδομένων που αφορούν το υποκείμενο, 5)το δικαίωμα περιορισμού της επεξεργασίας (άρθρο 18 GDPR), 6) το δικαίωμα στη φορητότητα των δεδομένων (άρθρο 20 GDPR), που το αφορούν, δηλαδή το δικαίωμα να λαμβάνει τα δεδομένα που το αφορούν από τον υπεύθυνο επεξεργασίας αλλά και να τα διαβιβάζει σε άλλον υπεύθυνο επεξεργασίας. Επίσης, ένα ακόμα δικαίωμα του υποκειμένου είναι το 7) δικαίωμα εναντίωσης στην επεξεργασία των δεδομένων του (άρθρο 21 GDPR). Τέλος, 8) το υποκείμενο έχει δικαίωμα να παρεμβαίνει σε οποιαδήποτε απόφαση, που το αφορά και λαμβάνεται αποκλειστικά, βάσει αυτοματοποιημένης επεξεργασίας, συμπεριλαμβανομένης της κατάρτισης προφίλ, η οποία πρόκειται να παράγει έννομα αποτελέσματα ή πρόκειται να το επηρεάσει σημαντικά (άρθρο 22 GDPR).

Υποστηρίζεται από τον Τσόλια ότι, ο ρόλος του ΥΠΔ στο πλαίσιο του καθήκοντος του αυτού, να παρακολουθεί τη συμμόρφωση, προσομοιάζει με αυτόν μιας «εσωτερικής εποπτικής αρχής».[92]

92. Τσόλιας Γρηγόρης, σε Κοτσαλής Λεωνίδας/Μενουδάκος Κωνσταντίνος (επ.),2018, «Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων (GDPR), Νομική διάσταση και πρακτική εφαρμογή», Νομική Βιβλιοθήκη, σελ. 208.

3) ΕΚΤΙΜΗΣΗ ΑΝΤΙΚΤΥΠΟΥ

Όταν ένα είδος επεξεργασίας ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες φυσικών προσώπων, ο υπεύθυνος επεξεργασίας, διενεργεί πριν από την επεξεργασία, εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία των δεδομένων προσωπικού χαρακτήρα. Στο άρθρο 35 παρ. 2 αναφέρεται ρητά ότι ο υπεύθυνος επεξεργασίας δεδομένων ζητεί τη γνώμη του ΥΠΔ, κατά τη διενέργεια εκτίμησης αντικτύπου, σχετικά με την προστασία δεδομένων και οι συμβουλές του θα πρέπει να τεκμηριώνονται. [93,94]

Μια δραστηριότητα επεξεργασίας, ειδικά, εάν χρησιμοποιεί νέες τεχνολογίες, είναι πιο πιθανό να ελλοχεύει υψηλό ρίσκο, για τα δικαιώματα και τις ελευθερίες, του υποκειμένου των δεδομένων.

Η Εποπτική Αρχή, οφείλει να καταρτίζει και να δημοσιοποιεί κατάλογο, με τα είδη των πράξεων επεξεργασίας δεδομένων, που υπόκεινται στην απαίτηση για διενέργεια εκτίμησης αντικτύπου, αλλά και για όσες πράξεις δεν είναι απαραίτητη η διενέργεια εκτίμησης αντικτύπου. [95]

Η εκτίμηση, θα πρέπει να περιέχει τουλάχιστον, συστηματική περιγραφή των

---

93. Ψαρουδάκη Μαριάνα, Αύγουστος-Σεπτέμβριος 2018, «Υπεύθυνος Προστασίας Δεδομένων (DPO)-Το πλαίσιο των καθηκόντων του και της ευθύνης του», ΕΠΙΧΕΙΡΗΣΗ 151/2018, Ψηφιακή Νομική Βιβλιοθήκη, σελ. 740.

94. Λουκάς Νικόλαος, 2017, «Η έννοια και η διαχείριση του « Κινδύνου» στον Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR)», Δίκαιο Μέσων Ενημέρωσης και Επικοινωνίας, σελ. 548.

95. Η ΑΠΔΠΧ, κατήρτισε σχέδιο καταλόγου με τα είδη των πράξεων επεξεργασίας, που υπόκεινται σε ΕΑΠΔ, για το οποίο το ΕΣΠΔ, εξέδωσε την με αρίθμ. 7/2018 γνώμη του. Με την με αρίθμ.65/2018 απόφαση της η ΑΠΔΠΧ, τροποποίησε τον κατάλογο ΕΑΠΔ που εξεδόθη, βάσει των συστάσεων που περιλαμβάνονται στην γνώμη 7/2018 της ΕΣΠΔ.

προβλεπόμενων πράξεων επεξεργασίας και των σκοπών της επεξεργασίας, εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας, εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων και τα μέτρα αντιμετώπισης των κινδύνων, περιλαμβανομένων των εγγυήσεων, των μέτρων και μηχανισμών ασφαλείας ώστε να διασφαλίζεται η προστασία των δεδομένων και να αποδεικνύεται η συμμόρφωση προς τον Γενικό Κανονισμό. Η Ομάδα Εργασίας του άρθρου 29, έχει δημοσιεύσει τις «Κατευθυντήριες γραμμές για την Εκτίμηση Αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΔΠ)» και για τον καθορισμό περί του «ποια επεξεργασία ενδέχεται να επιφέρει υψηλό κίνδυνο» κατά την έννοια του Κανονισμού 2016/679.[96]

Ο ΥΠΔ καλείται να αναλάβει ένα δύσκολο εξισορροπητικό ρόλο.[97]Θα πρέπει, δηλαδή να κατανοεί την ανάγκη του οργανισμού, στα πλαίσια του επιχειρηματικού ρίσκου, να επιχειρήσει κάποιες ενέργειες, που ίσως, θέτουν σε κίνδυνο τα προσωπικά δεδομένα υποκειμένων, και να επιδιώξει, να εξισορροπήσει την ανάγκη αυτή του οργανισμού, με τις προσδοκίες, της Εποπτικής Αρχής για την ασφάλεια των δεδομένων. Ένας οργανισμός μπορεί, για παράδειγμα, να είναι πρόθυμος να αναλάβει, ορισμένους κινδύνους, τους οποίους η Εποπτική Αρχή δεν αποδέχεται.

Ο ΥΠΔ και στην εν λόγω περίπτωση, δεν θα φέρει προσωπική ευθύνη, ούτε θα υφίσταται κυρώσεις, σχετικά με τη διενέργεια εκτίμησης αντικτύπου. Την ευθύνη θα φέρει αποκλειστικά, ο υπεύθυνος επεξεργασίας. Ο ΥΠΔ, σύμφωνα και με τα ανωτέρω, καλείται να συνδράμει τον υπεύθυνο επεξεργασίας, παρέχοντας του χρήσιμες συμβουλές και παρακολουθώντας την υλοποίηση αυτών.

---

96. «Κατευθυντήριες γραμμές για την Εκτίμηση Αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΔΠ)», της Ομάδας Εργασίας του άρθρου 29.

97. IT Governance, Publishing 2017, «EU General Data Protection Regulation (GDPR) An Implementation and Compliance Guide», Second edition,σελ.81.

4) ΣΥΝΕΡΓΑΣΙΑ ΚΑΙ ΔΙΑΒΟΥΛΕΥΣΗ ΜΕ ΤΗΝ ΑΡΧΗ

Ο ΥΠΔ ενεργεί, ως σημείο επικοινωνίας με την Εποπτική Αρχή για ζητήματα που σχετίζονται με την επεξεργασία δεδομένων, συμπεριλαμβανομένης της προηγούμενης διαβούλευσης, που αναφέρεται στο άρθρο 36 του ΓΚΠΔ, και πραγματοποιεί διαβουλεύσεις, ανάλογα με την περίπτωση, για οποιοδήποτε άλλο θέμα, σύμφωνα με το άρθρο 39 παρ.1δ' του ΓΚΠΔ.

Στα πλαίσια του καθήκοντός της συνεργασίας και επικοινωνίας, ο ΥΠΔ διευκολύνει την πρόσβαση της Αρχής στα έγγραφα και τις πληροφορίες του οργανισμού, προκειμένου να ασκήσει τις αδειοδοτικές, διορθωτικές, ελεγκτικές και συμβουλευτικές αρμοδιότητές της. Η υποχρέωση τήρησης απορρήτου, που δεσμεύει τον ΥΠΔ, δεν απαγορεύει την επικοινωνία και τη λήψη συμβουλών, από την Εποπτική Αρχή, στα πλαίσια της καλής και αγαστής συνεργασίας, για την εφαρμογή του Γενικού Κανονισμού.

Το καθήκον συνεργασίας με την Εποπτική Αρχή, δεν συνεπάγεται ότι ο ΥΠΔ είναι φερέφωνο, της Αρχής ή του Ευρωπαίου Επόπτη Προστασίας Δεδομένων. Αντίθετα εργάζεται και πασχίζει, για να επιτύχει την πλήρη συμμόρφωση του οργανισμού, με τις διατάξεις του Γενικού Κανονισμού. Σημαντικότατος αρωγός στην προσπάθεια αυτή, μπορεί να σταθεί, η καλή συνεργασία με την Αρχή, η ανταλλαγή απόψεων και πληροφοριών με αυτή.[98]

Ο ΥΠΔ, θα πρέπει να είναι σε ετοιμότητα και να απαντάει άμεσα, σε αιτήματα της Εποπτικής Αρχής, που απευθύνονται σε αυτόν και να εξασφαλίζει, παράλληλα, ότι τα αιτήματα της εποπτεύουσας αρχής, που έχουν ως αποδέκτες τους υπεύθυνους

98. Σωτηρόπουλος Βασίλης,2017, «Υπεύθυνος Προστασίας Δεδομένων-Εργαλειοθήκη για τον νέο θεσμό σε δημόσιο και ιδιωτικό τομέα», Εκδόσεις Σάκκουλα, σελ. 186.

επεξεργασίας, γίνονται κατανοητά από αυτούς και εφαρμόζονται.

Σε ενδεχόμενη παραβίαση των δεδομένων, ιδιαίτερη σημασία, θα διαδραματίσει, ο διαμεσολαβητικός ρόλος, που έχει αναλάβει ο ΥΠΔ, μεταξύ της Εποπτικής Αρχής και του υπεύθυνου επεξεργασίας. Λειτουργώντας ως ενδιάμεσος, θα συμβάλει ώστε να ικανοποιηθούν οι απαιτήσεις του άρθρου 33 του ΓΚΠΔ (Γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα στην εποπτική αρχή[99]), ενώ ο υπεύθυνος επεξεργασίας, ανενόχλητος θα μπορεί να εστιάζει και να επιδιώκει, την επανόρθωση και αποκατάσταση της δημιουργηθείσας κατάστασης, λόγω της παραβίασης των δεδομένων.

Καθήκον του ΥΠΔ είναι επίσης, να ενεργεί ως σημείο επικοινωνίας για ζητήματα επεξεργασίας, συμπεριλαμβανομένης της προηγούμενης διαβούλευσης με την Αρχή, βάσει του άρθρου 36 του ΓΚΠΔ.Ο υπεύθυνος επεξεργασίας, ζητεί την γνώμη της Αρχής αφού έχει εκπονήσει ΕΑΠΔ (σύμφωνα με το άρθρο 35 ΓΚΠΔ) η οποία θα υποδεικνύει αν οι υπολειπόμενοι κίνδυνοι, που απορρέουν από την επεξεργασία είναι υψηλοί, παρά τη λήψη μέτρων μετριασμού του κινδύνου από τον υπεύθυνο επεξεργασίας. Ο υπεύθυνος επεξεργασίας, θα πρέπει να παρέχει στην Αρχή τους σκοπούς και τα μέσα της σχεδιαζόμενης επεξεργασίας, τα μέτρα και τις εγγυήσεις για την προστασία των δεδομένων, καθώς και κάθε άλλη πληροφορία που ζητεί, ώστε να διατυπώσει γνώμη.

Από την ΑΠΔΠΧ προβλέπεται ότι, το αίτημα για προηγούμενη διαβούλευση με την Αρχή, βάσει του άρθρου 36 του ΓΚΠΔ, από τον υπεύθυνο επεξεργασίας πραγματοποιείται σε ηλεκτρονική μορφή, με αποστολή στην ηλεκτρονική διεύθυνση,

---

99. Άρθρο 33 παρ. 3 περ. β’ ΓΚΠΔ: «(Ο υπεύθυνος επεξεργασίας) ανακοινώνει το όνομα και τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων ή άλλου σημείου επικοινωνίας από το οποίο μπορούν να ληφθούν περισσότερες πληροφορίες».

«**prior_consultation@dpa.gr»** και μόνο σε εξαιρετικές περιπτώσεις, οι οποίες θα πρέπει αναλυτικά να περιγράφονται, θα μπορεί το συμπληρωμένο έντυπο να υποβληθεί με άλλο τρόπο.[100] Παράλληλα, στις οδηγίες συμπλήρωσης του ηλεκτρονικού εντύπου, που παρέχονται στην ιστοσελίδα της ΑΠΔΠΧ, επισημαίνεται ότι η Αρχή για την εξέταση του αιτήματος προηγούμενης διαβούλευσης, ενδέχεται να χρειαστεί διευκρινίσεις ή περαιτέρω στοιχεία, τα οποία θα λαμβάνει, μέσω της επικοινωνίας με τον ΥΠΔ, όπου αυτός έχει ορισθεί. Κρίνεται απαραίτητο έτσι, να συμπληρωθούν στο αντίστοιχο πεδίο και τα στοιχεία του ΥΠΔ, εφόσον έχει ορισθεί, για να διευκολυνθεί η επικοινωνία με την Αρχή.

100. Οδηγίες για υπευθύνους επεξεργασίας-Προηγούμενη διαβούλευση με την Αρχήhttps://www.dpa.gr

11) ΕΠΙΛΟΓΟΣ

Ο ΥΠΔ, αποτελεί το θεσμό, που καλείται να διαδραματίσει πρωταγωνιστικό και καίριο ρόλο, στην εφαρμογή και τήρηση του Κανονισμού (ΕΕ)2016/679. Ο ρόλος του θα είναι πρωτίστως συμβουλευτικός και υποστηρικτικός. Θα αποτελέσει ένα εργαλείο στα χέρια κάθε επιχείρησης, διασφαλίζοντας μέσω τη δράσης του, ότι οι οργανισμοί/επιχειρήσεις θα ανταπεξέλθουν στις αυξημένες ευθύνες, με τις οποίες έχουν επιφορτισθεί ως υπεύθυνοι επεξεργασίας και εκτελούντες την επεξεργασία.

Η κατάρτιση ενός ισχυρού προγράμματος συμμόρφωσης με τον ΓΚΠΔ, εποπτευόμενο από έναν κατάλληλα καταρτισμένο ΥΠΔ, μπορεί να συμβάλει στην ελαχιστοποίηση του κινδύνου παραβίασης προσωπικών δεδομένων και συνεπώς στην αποφυγή προστίμων και λοιπών κυρώσεων από την Αρχή, αλλά και τυχόν αξιώσεων αποζημίωσης από τα υποκείμενα των δεδομένων, σε πιθανές περιπτώσεις παραβίασης των προσωπικών τους δεδομένων .

Παράλληλα, όμως, υπεύθυνοι επεξεργασίας και εκτελούντες την επεξεργασία κατά αυτόν τον τρόπο, θα κατορθώσουν να ενισχύσουν τη φήμη της επιχειρήσεως τους, την αξιοπιστία της και θα έχουν τη δυνατότητα να διεκδικήσουν νέες ευκαιρίες, έχοντας στρατηγικό πλεονέκτημα έναντι των υπολοίπων οργανισμών/επιχειρήσεων, που δεν έχουν ορίσει ΥΠΔ και δεν έχουν, επομένως τακτοποιήσει τα ζητήματα, τα σχετικά με την προστασία των δεδομένων.

Στις ημέρες μας, δεδομένου ότι τα σύγχρονα μέσα ψηφιακής τεχνολογίας, βασίζονται κατά κύριο λόγο, στην επεξεργασία προσωπικών δεδομένων (συλλογή, ανταλλαγή δεδομένων) είναι σύνηθες και καθημερινό φαινόμενο, οι αυθαιρεσίες και οι παραβιάσεις των δεδομένων αυτών. Παράλληλα, τα ίδια τα άτομα έχοντας άγνοια των κινδύνων και επιπτώσεων, δημοσιοποιούν πληθώρα προσωπικών πληροφοριών στο διαδίκτυο καθημερινά, καθιστώντας τις προσιτές σε παγκόσμιο επίπεδο. Αναδύεται, λοιπόν, σήμερα, περισσότερο από ποτέ, η ανάγκη ύπαρξης αυτού του

ανεξάρτητου ατόμου εντός της επιχειρήσεως, που θα εγγυάται την νόμιμη χρήση και επεξεργασία των προσωπικών δεδομένων και θα καταδεικνύει στα υποκείμενα των δεδομένων ότι, η επιχείρηση λαμβάνει σοβαρά υπόψη της, την προστασία των δεδομένων τους.

Άλλωστε, η διασφάλιση υψηλού επιπέδου προστασίας των δεδομένων προσωπικού χαρακτήρα και σεβασμού της ιδιωτικής ζωής, αποτελούν θεμελιώδη δικαιώματα, του υποκειμένου που προβλέπονται και κατοχυρώνονται, σε ευρωπαϊκά κείμενα, στο άρθρο 8 και 7 του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και στο άρθρο 16 παρ.1 της Συνθήκης για τη Λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ) και πρέπει να χαίρουν σεβασμού από όλους ανεξαιρέτως. Ο θεσμός του ΥΠΔ, λοιπόν, θα γίνει πιο εύκολα κατανοητός και αποδεκτός, εφόσον αναλογιστεί κανείς τη σημασία της προστασίας των προσωπικών δεδομένων μας, τους κινδύνους που υπάρχουν και τον εγγυητικό ρόλο, που καλείται να διαδραματίσει ο ΥΠΔ.

Παρόλο που, ο θεσμός του ΥΠΔ, δεν εμφανίζεται σε άλλα νομικά κείμενα χωρών εκτός της Ευρώπης ως μία υποχρέωση, την οποία πρέπει να εκπληρώσουν υπεύθυνοι επεξεργασίας και εκτελούντες, εντούτοις, έχει γίνει αναφορά από ορισμένες αρχές προστασίας δεδομένων, σε αυτόν, ως ένα βασικό στοιχείο, που μπορεί να αποδείξει τη συμμόρφωση, με τις αρχές προστασίας δεδομένων. Η εφαρμογή του θεσμού στην Ευρώπη, μπορεί να αποτελέσει το παράδειγμα για το τρόπο, που θα λειτουργήσει και θα δράσει ο ΥΠΔ, εντός μίας οντότητας, σε πρακτικό επίπεδο και αφορμή για να επικαιροποίησουν τη νομοθεσία τους.

ΒΙΒΛΙΟΓΡΑΦΙΑ-ΑΡΘΡΟΓΡΑΦΙΑ

1. Βασίλης Σωτηρόπουλος, 2017, «Υπεύθυνος Προστασίας Δεδομένων-Εργαλειοθήκη για τον νέο θεσμό σε δημόσιο και ιδιωτικό τομέα», Εκδόσεις Σάκκουλα
2. Κοτσαλής Λεωνίδας, Μενουδάκος Κωνσταντίνος,2018, «Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων (GDPR), Νομική διάσταση και πρακτική εφαρμογή», Νομική Βιβλιοθήκη, σελ. 193-216
3. Λαζαράκος Γρηγόρης,2016, «Ο θεσμός του υπεύθυνου προστασίας προσωπικών δεδομένων (Data Protection Officer) στο νέο νομοθετικό πλαίσιο των προσωπικών δεδομένων μετά την υιοθέτηση του Κανονισμού (ΕΕ) 679/2016, Εφαρμογές Δημοσίου Δικαίου-ΙΙΙ, σελ.243 επ.
4. Λουκάς Νικόλαος, 2017, «Η έννοια και η διαχείριση του « Κινδύνου» στον Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR)», Δίκαιο Μέσων Ενημέρωσης και Επικοινωνίας, σελ. 544 επ.
5. Ψαρουδάκη Μαριάνα, Αύγουστος-Σεπτέμβριος 2018, «Υπεύθυνος Προστασίας Δεδομένων (DPO)- Το πλαίσιο των καθηκόντων του και της ευθύνης του», ΕΠΙΧΕΙΡΗΣΗ 151/2018, σελ. 722 επ.
6. IT Governance, Publishing 2017,«EUGeneralDataProtectionRegulation (GDPR) An Implementation and Compliance Guide», Second edition, σελ.53-83

ΗΛΕΚΤΡΟΝΙΚΑ ΒΙΒΛΙΑ (E-BOOKS)

1. Taylor Sarah (Author), 29/3/2018, «Data Protection Officer (DPO)» e-book, Kindle Cloud Reader,https://read.amazon.com/

ΠΗΓΕΣ ΑΠΟ ΤΟ ΔΙΑΔΙΚΤΥΟ

1. Ανακοίνωση Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα για DPOs, 9/08/2017
2. Γιαννακάκης Ιωάννης,11/01/2017 «Ο Ρόλος και η ευθύνη του DataProtectionOfficer σύμφωνα με το νέο Γενικό Κανονισμό Προσωπικών Δεδομένων (GDPR)», The DPO Academy,<https://www.cyberinsurancegreece.com/news/o-rolos-kai-oi-eythyni-toy-data-protection-officer-symfona-me-to-neo-geniko-kanonismo-prosopikon-dedomenon-gdpr-toy-ioanni-e-giannakaki-dikigoroy-nomikoy-symvoyloy>
3. Γνωμοδότηση 7/2017, Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, 3/11/2017
4. Επαγγελματικά Πρότυπα για DPOs από τον Ευρωπαίο Επόπτη για την Προστασία Δεδομένων (EDPS), υπό τον Κανονισμό (ΕΕ) 45/2001, 14/10/2010
5. Ιστοσελίδα Αρχής Προστασίας Προσωπικών Δεδομένων Ιρλανδίας, <https://www.dataprotection.ie/en/organisations/know-your-obligations/data-protection-officers>
6. Ιστοσελίδα Information Commissioner' s Office Ηνωμένου Βασιλείου, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/?lspt_context=gdpr>
7. Κατευθυντήριες γραμμές Ομάδας Εργασίας Άρθρου 29, σχετικά με τους υπεύθυνους προστασίας δεδομένων, 5 Απριλίου 2017
8. Νόμος 4624/2019 για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα σε εφαρμογή του Κανονισμού (ΕΕ) 2016/679και αιτιολογική έκθεση

9. Τσόλιας Γρηγόρης,6/10/2017,«Ο Υπεύθυνος Προστασίας Δεδομένων (DPO) στον GDPR» - itSecurity,<https://www.itsecuritypro.gr/o-ypefthynos-prostasias-dedomenon-dpo-ston-gdpr/>

10. Alston and Bird, June 17, 2018, «EU Supervisory Authorities Disclose DPO Notification Tools» | Privacy & Data Security Team,<https://www.alstonprivacy.com/eu-supervisory-authorities-disclose-dpo-notification-tools/>

11. Business and technology sourcing review-Issue 16, 8/6/2011, «New Requirements for Data Protection Officers in Germany»

12. Cloud Privacy Check (CPC), 2/08/2018, «The Estonian data protection authority issued guidance on the definition of "large scale" processing», <https://eurocloud.org/news/article/the-estonian-data-protection-authority-issued-guidance-on-the-definition-of-large-scale-processing/>

13. Comments by the Centre for Information Policy Leadership on the Article 29 Data Protection Working Party's "Guidelines on Data Protection Officers (DPOs)" adopted on 13 December 2016

14. Cryan Michael,3/07/2018«Do small businesses need to appoint a DPO under GDPR?»,<https://www.compliancejunction.com/small-business-dpo-gdpr/>

15. Data Protection Officers | Data Protection Commissioner,<https://www.dataprotection.ie/en/organisations/know-your obligations /data-protection-officers>

16. DLAPIPER, DataProtectionlawsoftheworld,<https://www.dlapiperdataprotection.com/>

17. Αρχή Προστασίας Δεδομένων, οδηγίες για υπευθύνους επεξεργασίας<www.dpa.gr>

18. EuroCloud Europe,23/11/2018, «Slovenia's ICO defines DPO's additional tasks that could result in a conflict of

interests»<https://staraudit.org/news/article/slovenias-ico-defines-dpos-additional-tasks-that-could-result-in-a-conflict-of-interests/>

19. Euro Cloud Europe, 19/03/2019, «Data Protection Officers under Slovenia's Draft Personal Data Protection Act(ZVOP-2)», <https://eurocloud.org/news/article/data-protection-officers-under-slovenias-draft-personal-data-protection-act-zvop-2/>

20. Faller Pierre,«GDPR DPO's (Data Protection Officer) role within organization»,<https://advisera.com/eugdpracademy/knowledgebase/the-role-of-the-dpo-in-light-of-the-general-data-protection-regulation/>

21. Gastaud Florent, 23 août 2018, «Comment désigner un Data Protection Officer (DPO) en France?», Mon DPO externe,<https://mon-dpo-externe.com/comment-designer-dpo-france/>

22. Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679

23. IAPP, 24/05/2018, «Facebook names Deadman first DPO»,<https://iapp.org/news/a/facebook-names-deadman-first-dpo/>

24. IAPP, 31/10/2017, «Here's what it takes to be a certified DPO in Spain»,<https://iapp.org/news/a/heres-what-it-takes-to-be-a-certified-dpo-in-spain/>

25. IP, Tech & Data, General Data Protection Regulation, «Overview of the latest developments regarding the national implementation of the GDPR requirements»

26. IT Governance Blog, 17/07/2018, «The DPO role and why you should consider outsourcing it»,<https://www.itgovernance.eu/blog/en/the-dpo-role-and-why-you-should-consider-outsourcing-it>

27. Kaufmann Julia and Guenther Jan-Philipp, 9/01/2018 and 21/11/2016, «Germany: Data Protection Officer must not have a conflict of interests-Global Compliance News»,<https://globalcompliancenews.com/germany-

data-protection-officer-conflict-of-interest-20161121/>,<https://globalcompliancenews.com/data-protection-officers-conflict-interest-20180109/>

28. lawspot.gr, 3/04/2018, «Διευκρινήσεις για τις πιστοποιήσεις dpo και στη Κύπρο»,<https://www.lawspot.gr/nomika-nea/gdpr-dieykriniseis-gia-tis-pistopoiiseis-dpo-kai-stin-kypro>

29. Lexology, 21/09/2018, «Italian court decision on DPO requirements and new Belgian privacy law», <https://www.lexology.com/library/detail.aspx?g=2dd363cb-e4a7-49de-81c7-0297d9d29776>

30. Michalopoulou &Associates LawGroup, «Ο υπεύθυνος προστασίας δεδομένων -dpo- και το υπάρχον πλαίσιο Πιστοποίησης υπό τον GDPR»

31. Oberschelp de MenesesAnna and Van QuathemKristof , 25/10/2018, «Italian Court decides that a data protection officer does not have to be a certified ISO 27001», posted in DATA PRIVACY,DATA PROTECTION, EUROPEAN UNION

32. Privacy & Information Security Law Blog, 18/10/2018, «CNIL Adopts Referentials on DPO Certification»,<https://www.huntonprivacyblog.com/2018/10/18/cnil-adopts-referentials-dpo-certification/>

33. Recommandationn°04/2017 du 24 mai 2017,<https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/recommandation_04_2017.pdf>

34. Smith Reed, 12/2018, «Overview of the latest developments regarding the national implementation of the GDPR requirements»,IP, Tech & Data. General Data Protection Regulation

35. 2003/361/ΕΚ Σύσταση της Επιτροπής της 6ης Μαΐου 2003, σχετικά με τον ορισμό των πολύ μικρών, των μικρών και των μεσαίων επιχειρήσεων