Overview of Processing Activities under Article 30(1)GDPR Controller	Cover Page

Controller Details

Name and contact information of the individual / legal person / agency / body etc.

Name

Street

ZIP code

City

Telephone

E-Mail address

Internet URL

If applicable, Details of Joint Controllers

Name

Street

ZIP code

City

Telephone

E-Mail address

Details of Controller's Representative

Name and contact information of the individual / legal person / agency / body etc.

Name

Street

ZIP code

City

Telephone

E-Mail address

Details of the Data Protection Officer* (if external, provide street address)

* to the extent a DPO has been appointed under Article 37 GDPR

Form of address Title (e.g. Dr.)

Surname, First Name

Street

ZIP code

City

Telephone

E-Mail Address

Processing Activity: Title:_____	**Index No.:** _____
Commencement date:	Date of most recent modification:

Responsible Department Point of Contact Telephone E-Mail Address (Art. 30(1)(2)(a) GDPR)	
Purposes of the Processing(Art. 30(1)(2)(b) GDPR)	
Optional: Name of the process(es) employed	
Description of the Categories of affected Data Subjects (Art. 30(1)(2)(c) GDPR)	☐Employees ☐ Applicants ☐ Suppliers ☐ Customers ☐ Patients ☐ ☐ ☐
Description of the Categories of Personal Data (Art. 30(1)(2)(c) GDPR)	☐ ☐ ☐ Special Categories of Personal Data (Art. 9 GDPR): ☐

Categories of Recipients to whom Personal Data have been – or will be - disclosed (Art. 30(1)(2)(d) GDPR)	☐Internal Recipients (authorized users / users with access rights) Department / Function
	☐ External Recipients Categories of Recipients
	☐Third Countries or International Organizations (identify by category)
If applicable, Transfers of Personal Data to a Third Country or International Organization (Art. 30(1)(2)(e) GDPR)	☐Transfers do not occur and are not planned to occur ☐Transfers are made as follows:
Identification of Specific Transfer Recipients	☐Third Country or International Organization (identify by name)
To the extent that Transfers fall under Art. 49(1) para. 2 GDPR [*Note: These are one-time transfers affecting a "limited number" of individuals made on the basis of "compelling legitimate interests"*]:	Documentation of Sufficient Safeguards for Transfers
Retention/Deletion Periods for the Various Categories of Personal Data (Art. 30(1)(2)(f) GDPR)	

Technical and Organizational Measures (TOMs)implemented to ensure Information Security under Art. 32(1) GDPR (Art. 30(1)(2)(g) GDPR) *For guidance on describing Information Security TOMs, see points 6.7 and 6.8 of the Data Protection Conferences "Tips for the Index of Processing Activities"* (available [in German] here)

…… …… .....
Controller Date Signature

ΓΡΑΦΕΙΟ ΕΠΙΤΡΟΠΟΥ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

ΟΔΗΓΟΣ
ΣΥΜΠΛΗΡΩΣΗΣ ΑΡΧΕΙΟΥ ΔΡΑΣΤΗΡΙΟΤΗΤΩΝ ΕΠΕΞΕΡΓΑΣΙΑΣ

ΜΕΡΟΣ Α - Εισαγωγή

Στις 25 Μαΐου 2018, τίθεται σε εφαρμογή ο Κανονισμός (ΕΕ) 2016/679, για την προστασία των προσωπικών δεδομένων. Κάθε δημόσιος και ιδιωτικός οργανισμός, που επεξεργάζεται τέτοια δεδομένα, θα πρέπει να είναι σε συμμόρφωση με τον Κανονισμό. Μια κύρια υποχρέωση αφορά στην τήρηση Αρχείου Δραστηριοτήτων (**Άρθρο 30**). Σκοπός αυτού του Οδηγού, είναι να προσφέρει καθοδήγηση και να βοηθήσει στη συμπλήρωση του Πίνακα με τίτλο ΑΡΧΕΙΟ ΔΡΑΣΤΗΡΙΟΤΗΤΩΝ ΕΠΕΞΕΡΓΑΣΙΑΣ που επισυνάπτεται ως Παράρτημα και είναι αναρτημένος στην ιστοσελίδα του Γραφείου μας www.dataprotection.gov.cy . Ο Πίνακας αυτός πρέπει να τηρείται και σε ηλεκτρονική μορφή (**Άρθρο 30(3)**).

Ποιος έχει υποχρέωση να τηρεί Αρχείο Δραστηριοτήτων Επεξεργασίας; Η υποχρέωση βαραίνει οργανισμούς που ενεργούν ως υπεύθυνοι επεξεργασίας ή ως εκτελούντες την επεξεργασία. Ο υπεύθυνος επεξεργασίας (**Άρθρο 4(7)**) είναι το πρόσωπο που αποφασίζει το σκοπό και τον τρόπο μιας επεξεργασίας. Μπορεί να είναι φυσικό ή νομικό πρόσωπο. Για επιχειρήσεις, συνήθως, υπεύθυνος επεξεργασίας είναι ο ιδιοκτήτης ή ο διευθύνων σύμβουλος. Δεν αποκλείεται όμως, υπεύθυνος επεξεργασίας να είναι ένας υπάλληλος, ο οποίος αποφασίζει το σκοπό και τον τρόπο μιας ή περισσοτέρων πράξεων επεξεργασίας. Ο εκτελών την επεξεργασία (**Άρθρο 4(8)**) είναι ένα πρόσωπο, εκτός του οργανισμού, στον οποίο ο υπεύθυνος επεξεργασίας αναθέτει μια επεξεργασία και το οποίο ενεργεί κατ' εντολή και για λογαριασμό του υπεύθυνου επεξεργασίας. Για παράδειγμα, αν μια εταιρεία αποφασίσει να συμβληθεί με μια υπηρεσία σύννεφου (cloud), η υπηρεσία αυτή θα ενεργεί ως ο εκτελών την επεξεργασία. Στην περίπτωση που υπάρχουν από κοινού υπεύθυνοι επεξεργασίας (**Άρθρο 26**), ο Πίνακας συμπληρώνεται από έκαστο, στον βαθμό που τον αφορά. Αν ένας οργανισμός εδρεύει εκτός της Ευρωπαϊκής Ένωσης (ΕΕ) αλλά προσφέρει αγαθά ή υπηρεσίες σε πρόσωπα που βρίσκονται στην ΕΕ, ή παρακολουθεί τη συμπεριφορά τους, τότε έχει υποχρέωση να ορίσει εκπρόσωπο του στην ΕΕ (**Άρθρα 3(2), 27**). Σε τέτοια περίπτωση, την υποχρέωση συμπλήρωσης του Πίνακα έχει ο εκπρόσωπος του οργανισμού. Αν μια επιχείρηση έχει εγκατάσταση στην Κύπρο ή είναι μέλος ενός ομίλου επιχειρήσεων (**Άρθρο 4(19)**) και έχει την κύρια εγκατάσταση της στην Κύπρο (**Άρθρο 4(11)**), συστήνεται όπως το Αρχείο συμπληρωθεί σε συνεργασία με άλλες επιχειρήσεις του ομίλου που έχουν όμοιες ή παρόμοιες δραστηριότητες. Κατά κανόνα, μικρομεσαίες επιχειρήσεις με λιγότερους από 250 υπαλλήλους, δεν έχουν υποχρέωση να τηρούν Αρχείο Δραστηριοτήτων Επεξεργασίας. **Ωστόσο**, αν οι δραστηριότητες μιας μικρομεσαίας επιχείρησης συνεπάγονται ψηλό κίνδυνο για τους υπαλλήλους ή τους πελάτες της, τότε έχει υποχρέωση να τηρεί το Αρχείο αυτό (**Άρθρο 30(5)**). Η τήρηση αυτού του Αρχείου συστήνεται ακόμη και για οργανισμούς που δεν έχουν υποχρέωση να το τηρούν αφού είναι ένα χρήσιμο εργαλείο συμμόρφωσης με τον Κανονισμό.

Σε τι βοηθά η τήρηση του Αρχείου Δραστηριοτήτων Επεξεργασίας; Η συμπλήρωση αυτού του Αρχείου εξυπηρετεί πολλαπλούς σκοπούς. Πρώτο, ένας οργανισμός έχει υποχρέωση να θέσει το Αρχείο Δραστηριοτήτων στη διάθεση της Επιτρόπου, αν το ζητήσει. Δεύτερο, βοηθά να απαντηθούν ερωτήματα όπως ποίος είμαι, τι κάνω, πώς το κάνω και γιατί το κάνω. Είναι ένα εργαλείο αυτογνωσίας και αυτό-αξιολόγησης για τη συμμόρφωση με τον Κανονισμό. Τρίτο, βοηθά στην υιοθέτηση της πολιτικής προστασίας της ιδιωτικής ζωής (privacy policy), αν ένας οργανισμός χρειάζεται να διαθέτει τέτοια. Τέταρτο, βοηθά ένα οργανισμό να συμμορφώνεται με τις Αρχές της Λογοδοσίας (**Άρθρο 5(2)**) και της Διαφάνειας (**Άρθρο 5(1)(α)**). Πέμπτο, βοηθά στη διαμόρφωση πολιτικής ή μηχανισμών για την άσκηση των δικαιωμάτων των υποκειμένων των δεδομένων (**Άρθρο 12(1)**). Πολλοί οργανισμοί ρωτούν τι πρέπει να κάνουν για να είναι σε συμμόρφωση με τον Κανονισμό και από πού πρέπει να αρχίσουν. Ως πρώτο βήμα, συστήνεται η συμπλήρωση του Αρχείου αυτού. Η σωστή και πλήρης συμπλήρωσή του θα βοηθήσει τον οργανισμό να εντοπίσει κάποιες υποχρεώσεις που απορρέουν από τον Κανονισμό, με τις οποίες πρέπει να συμμορφωθεί. Η συμπλήρωση του Αρχείου Δραστηριοτήτων Επεξεργασίας δεν είναι στατική. Είναι μια συνεχής διαδικασία αφού, όταν διαφοροποιείται ή αλλάζει μια υφιστάμενη δραστηριότητα επεξεργασίας ή προστίθεται μια καινούργια, το Αρχείο πρέπει να επικαιροποιείται. Η τήρηση αυτού του Αρχείου συστήνεται ακόμη και για οργανισμούς που δεν έχουν υποχρέωση να το τηρούν αφού είναι ένα χρήσιμο εργαλείο συμμόρφωσης με τον Κανονισμό.

Τι πληροφορίες πρέπει να τηρούνται στο Αρχείο Δραστηριοτήτων Επεξεργασίας; Ένας υπεύθυνος επεξεργασίας ή ο εκπρόσωπός του, έχει υποχρέωση να τηρεί τις πληροφορίες που αναφέρονται στις στήλες 5-11 του Πίνακα (**Άρθρο 30(1)**). Ένας εκτελών την επεξεργασία ή ο εκπρόσωπός του, έχει υποχρέωση να τηρεί τις πληροφορίες που αναφέρονται στις στήλες 1, 4, 5, 8, και 10. Ωστόσο, τίποτε δεν τους εμποδίζει να τηρούν πρόσθετες πληροφορίες, για σκοπούς αυτογνωσίας, αυτό-αξιολόγησης, λογοδοσίας και διαφάνειας. Ο Πίνακας που επισυνάπτεται στο Παράρτημα και είναι αναρτημένος στην ιστοσελίδα του Γραφείου, ουσιαστικά αποτελεί ένα δείγμα, το οποίο κάθε οργανισμός μπορεί να προσαρμόζει με βάση τις δικές του ιδιαιτερότητες. Ένας οργανισμός, για τις δικές του ανάγκες, μπορεί να συμπληρώσει μόνο τα υποχρεωτικά πεδία του Πίνακα, ή να συμπληρώσει και κάποια μη υποχρεωτικά ή να προσθέσει και άλλα πεδία, ώστε να διαμορφωθεί μια σφαιρική εικόνα για το τι κάνει, πώς το κάνει και γιατί το κάνει, αλλά και για το τι πρέπει να κάνει για να είναι σε συμμόρφωση με τον Κανονισμό.

Ποιος πρέπει να συμπληρώσει τον Πίνακα; Όπως αναφέρεται πιο πάνω, την ευθύνη τήρησης του Αρχείου έχουν κατά περίπτωση, ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία ή οι τυχόν εκπρόσωποί τους. Ωστόσο, μπορούν να αναθέσουν αυτό το καθήκον σε κάποιο υπάλληλό τους ή σε κάποιο εξωτερικό ειδικό. Αν ο οργανισμός έχει υποχρέωση να ορίσει Υπεύθυνο Προστασίας Δεδομένων (ΥΠΔ) (**Άρθρα 37, 38, 39**) συστήνεται όπως ο Πίνακας συμπληρωθεί από τον ΥΠΔ. Σε κάθε περίπτωση, το πρόσωπο που θα αναλάβει αυτό το καθήκον πρέπει να έχει ολοκληρωμένη εικόνα για όλες τις δραστηριότητες του οργανισμού. Αν είναι υπάλληλος του οργανισμού, συστήνεται να είναι ψηλόβαθμο παρά χαμηλόβαθμο στέλεχος, αφού θα πρέπει να έχει συνεχή επαφή με τη διεύθυνση και πρόσβαση σε όλα τα τμήματα του οργανισμού, ώστε να καταγράψει όλες τις πράξεις επεξεργασίας προσωπικών δεδομένων. Αν είναι εξωτερικός συνεργάτης,

ο οργανισμός πρέπει να του παράσχει τις απαραίτητες διευκολύνσεις για τη σωστή συμπλήρωση του Πίνακα. Για μη σωστή συμπλήρωση του Πίνακα μπορεί να επιβληθεί διοικητική κύρωση (**Άρθρο 58**) σε ένα οργανισμό, ή διοικητικό πρόστιμο (**Άρθρο 83**). Αυτά, επιβάλλονται στον οργανισμό και όχι, στο πρόσωπο που συμπλήρωσε τον Πίνακα. Το πρόσωπο που θα συμπληρώσει τον Πίνακα δεν χρειάζεται κατ' ανάγκη να είναι νομικός ή τεχνικός πληροφορικής. Όμως, πρέπει να έχει γνώση του Κανονισμού και όλων των νομοθεσιών που εφαρμόζει ο οργανισμός ή που ρυθμίζουν τον τομέα στον οποίο δραστηριοποιείται, καθώς και στοιχειώδεις τουλάχιστο γνώσεις πληροφορικής.

Σε τι γλώσσα πρέπει να συμπληρωθεί ο Πίνακας; Ο Πίνακας πρέπει να συμπληρωθεί στα Ελληνικά. Για οργανισμούς που διενεργούν διασυνοριακές πράξεις επεξεργασίας (**Άρθρο 4(23)**) ή δραστηριοποιούνται σε πολλά Κράτη Μέλη της ΕΕ, ή παρέχουν υπηρεσίες της κοινωνίας των πληροφοριών (**Άρθρο 8**) ή παρέχουν πληροφόρηση στα υποκείμενα των δεδομένων (**Άρθρα 13, 14**) μέσω της ιστοσελίδας τους ή διαθέτουν στην ιστοσελίδα τους μηχανισμό άσκησης των δικαιωμάτων των υποκειμένων των δεδομένων (**Άρθρα 15-22**), συστήνεται όπως ο Πίνακας ή τουλάχιστο η στήλη 12, τηρείται και στην Αγγλική. Σε κάθε περίπτωση, η πληροφόρηση που δίνεται στους πελάτες, στους συνεργάτες ή στους υπαλλήλους, ενός οργανισμού πρέπει να είναι διαφανής, κατανοητή, σε εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή διατύπωση (**Άρθρο 12(1)**).

Κάποιες πρακτικές συμβουλές; Σε ορισμένους οργανισμούς, μικρούς ή μεγάλους, δημόσιους ή ιδιωτικούς, ίσως υπάρχει κάποια κουλτούρα μυστικοπάθειας. Ίσως υπάρχει ένα τμήμα ή ένα πρόσωπο που δεν μοιράζεται πληροφορίες με άλλα τμήματα ή συναδέλφους, για το τι κάνει, πώς το κάνει και γιατί το κάνει ή δεν μοιράζεται αρκετές πληροφορίες εύκολα. Ένας υπάλληλος ίσως νιώθει ότι, κοινοποιώντας τις πληροφορίες σε συναδέλφους του, θα θέσει σε κίνδυνο τη θέση του. Συστήνεται όπως, το πρόσωπο που θα αναλάβει τη συμπλήρωση του Πίνακα, έχει την ικανότητα επίλυσης τέτοιων προβλημάτων. Για τη συμπλήρωση του Πίνακα, το πρόσωπο που θα αναλάβει αυτό το καθήκον ίσως χρειαστεί τη συνδρομή των τεχνικών πληροφορικής και των νομικών συμβούλων του οργανισμού. Η επικοινωνία μεταξύ τεχνικών και νομικών δεν είναι πάντοτε εύκολη. Συστήνεται όπως, το πρόσωπο που θα αναλάβει τη συμπλήρωση του Πίνακα έχει επικοινωνιακές δεξιότητες ώστε να μπορεί να μεταφέρει τεχνικά θέματα στους νομικούς και νομικά θέματα στους τεχνικούς, αντίστοιχα.

Πιο κάτω, γίνεται αναλυτική περιγραφή των πληροφοριών που ενδείκνυται να καταγράφονται σε κάθε πεδίο του Πίνακα:

ΜΕΡΟΣ Β - Συμπλήρωση του Πίνακα

1. <u>Δραστηριότητα Επεξεργασίας</u>

Στη στήλη αυτή γίνεται μια σύντομη περιγραφή της κάθε δραστηριότητας του οργανισμού. Ως πρώτο βήμα, συστήνεται η επίσκεψη σε κάθε τμήμα του οργανισμού και η καταγραφή της κάθε δραστηριότητας που διενεργεί έκαστο. Αν ο οργανισμός έχει οργανόγραμμα, συμβουλευτείτε το. Κάποιες από αυτές τις δραστηριότητες συνεπάγονται επεξεργασία

προσωπικών δεδομένων. Αυτές πρέπει να καταγραφούν στη στήλη αυτή. Αν ένας οργανισμός, έχει τμήμα διεύθυνσης, τμήμα πωλήσεων, τμήμα μάρκετινγκ και τμήμα προσωπικού, συστήνεται όπως η στήλη αυτή χωριστεί σε τέσσερα αντίστοιχα τμήματα και όπως, κάτω από κάθε τμήμα, καταγραφούν οι δραστηριότητές του. Για κάθε δραστηριότητα, πρέπει να γίνει μια σύντομη περιγραφή. Για παράδειγμα, στο τμήμα προσωπικού μπορεί να καταγραφούν δύο δραστηριότητες. «Αρχείο υποψηφίων υπαλλήλων» και «Αρχείο προσωπικού». Για το πρώτο, η περιγραφή μπορεί να διατυπωθεί ως εξής: *Στο αρχείο αυτό τηρούνται τα βιογραφικά σημειώματα υποψήφιων για πρόσληψη* και για το δεύτερο: *Προσωπικοί φάκελοι υπαλλήλων*. Είναι σημαντικό να καταγραφούν όλες οι δραστηριότητες του οργανισμού. Αν το τμήμα μάρκετινγκ διαχειρίζεται την ιστοσελίδα του οργανισμού και συλλέγει στοιχεία πλοήγησης των επισκεπτών της στο διαδίκτυο, μέσω cookies, η διαχείριση της ιστοσελίδας θα πρέπει να γραφτεί ως ξεχωριστή δραστηριότητα, με την περιγραφή *παρακολούθηση ιστορικού πλοήγησης επισκεπτών της ιστοσελίδας*. Η χρήση κλειστού κυκλώματος βίντεο-παρακολούθησης πρέπει να καταγράφεται ως ξεχωριστή δραστηριότητα.

2. Κύρια ή Παρεπόμενη

Ο Κανονισμός ξεχωρίζει μεταξύ κύριων/ βασικών και παρεπόμενων δραστηριοτήτων και επιβάλλει κάποιες πρόσθετες υποχρεώσεις για τις πρώτες, όπως για παράδειγμα, τον ορισμό Υπεύθυνου Προστασίας Δεδομένων (**Άρθρο 37(1)(β),(γ)**). Αυτό δεν σημαίνει ότι, τα προσωπικά δεδομένα που τυγχάνουν επεξεργασίας στα πλαίσια παρεπόμενων δραστηριοτήτων είναι λιγότερης σημασίας ή ότι απολαμβάνουν χαμηλότερο επίπεδο προστασίας. Για παράδειγμα, κύρια δραστηριότητα ενός λογιστικού γραφείου είναι η παροχή λογιστικών υπηρεσιών και παρεπόμενη δραστηριότητά του είναι η τήρηση των φακέλων του προσωπικού. Παρόλο που το γραφείο δεσμεύεται από επαγγελματικό απόρρητο να προστατεύει τα προσωπικά δεδομένα του κάθε πελάτη του καθώς και τα δεδομένα των πελατών του κάθε πελάτη, τα δεδομένα υγείας που αναγράφονται στα ιατρικά πιστοποιητικά των υπαλλήλων που λαμβάνουν άδεια ασθενείας τυγχάνουν αυξημένης προστασίας (**Άρθρο 9**), έστω και αν η τήρηση τους συνιστά παρεπόμενη δραστηριότητα. Στη στήλη αυτή, δίπλα από την κάθε δραστηριότητα της πρώτης στήλης, θα πρέπει να γραφτεί αν αυτή είναι κύρια/ βασική ή παρεπόμενη δραστηριότητα. Η άσκηση αυτή βοηθά να εντοπιστούν άλλες υποχρεώσεις που ενδέχεται να βαραίνουν ένα οργανισμό, με βάση τον Κανονισμό.

3. Νομική Βάση

Κάθε δραστηριότητα επεξεργασίας πρέπει να έχει μια νομική βάση (**Άρθρα 6 και 9**). Στη στήλη αυτή καταγράφεται, το άρθρο του Κανονισμού στο οποίο βασίζεται η κάθε δραστηριότητα επεξεργασίας. Συνήθως, μια δραστηριότητα βασίζεται σε μία μόνο νομική βάση. Όμως, κάποιες δραστηριότητες μπορεί να έχουν διάφορες νομικές βάσεις. Για παράδειγμα, μια επιχείρηση στους προσωπικούς φακέλους του προσωπικού, έχει υποχρέωση να τηρεί δεδομένα για την απασχόληση και τη μισθοδοσία των υπαλλήλων της με βάση τη νομοθεσία των Υπηρεσιών Κοινωνικών Ασφαλίσεων και του Τμήματος Φορολογίας (**Άρθρο 6(1)(γ)**), τηρεί δεδομένα με βάση το συμβόλαιο εργοδότησης (**Άρθρο 6(1)(β)**) και έχει έννομο συμφέρον (**Άρθρο 6(1)(στ)**) να τηρεί πληροφορίες για την

απόδοση και την ανέλιξή τους. Εταιρείες που δραστηριοποιούνται στον τομέα των επενδύσεων ή στην παροχή Υπηρεσιών, με βάση τη νομοθεσία για ξέπλυμα χρήματος (Anti-Money Laundering AML), έχουν υποχρέωση να συλλέγουν πληροφορίες για να αξιολογούν την επικινδυνότητα των πελατών τους. Ανάλογα με τη ζητούμενη υπηρεσία, μπορεί να συλλέγουν και κάποιες πρόσθετες πληροφορίες που προβλέπονται στα συμβόλαια με τους πελάτες τους. Αν, για την παροχή μιας υπηρεσίας, χρειάζεται να συλλέξουν και πρόσθετες πληροφορίες, που δεν προβλέπονται από Νόμο ή στο συμβόλαιο, είτε από τους ίδιους τους πελάτες (**Άρθρο 13**) ή από τρίτους (**Άρθρο 14**), τηρούμενης της Αρχής της ελαχιστοποίησης των δεδομένων (**Άρθρο 5(1)(γ)**), αυτό πρέπει να γίνει με τη συγκατάθεση των πελατών (**Άρθρα 4(11), 6(1)(α), 7**). Η συμπλήρωση του πεδίου αυτού είναι πολύ σημαντική αφού ο Κανονισμός υποχρεώνει τους οργανισμούς να είναι διαφανείς σε σχέση με τη νομιμότητα της κάθε επεξεργασίας που διενεργούν (**Άρθρο 5(1)(α)**) και να επιδεικνύουν τη συμμόρφωση τους (**Άρθρο 5(2)**), σε κάθε στάδιο της επεξεργασίας. Για ορισμένους οργανισμούς, ίσως είναι πιο εύκολο όπως η στήλη αυτή συμπληρωθεί μετά τη συμπλήρωση της στήλης που αφορά στις κατηγορίες των υποκειμένων των δεδομένων.

4(α),(β). <u>Υπεύθυνος ή Εκτελών την Επεξεργασία ή τυχόν εκπρόσωπός τους</u>

Στη στήλη 4(α) καταγράφεται η ιδιότητα ενός οργανισμού σε σχέση με κάθε δραστηριότητα επεξεργασίας, δηλαδή, αν ενεργεί ως υπεύθυνος επεξεργασίας, ως εκτελών την επεξεργασία, ή ως εκπρόσωπος του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία. Στη στήλη 4(β) καταγράφεται το όνομα και τα στοιχεία επαφής του προσώπου που καταγράφτηκε στη στήλη 4(α) και όπου υπάρχει, τα στοιχεία επαφής του Υπεύθυνου Προστασίας Δεδομένων. Ένας οργανισμός μπορεί να παρέχει διάφορες υπηρεσίες. Για ορισμένες από αυτές μπορεί να ενεργεί ως υπεύθυνος επεξεργασίας ενώ για άλλες ως εκτελών την επεξεργασία. Για παράδειγμα, ένα γραφείο εξεύρεσης εργασίας, μπορεί να δραστηριοποιείται στην τοποθέτηση υποψηφίων σε εργοδότες αλλά και να διενεργεί συνεντεύξεις σε υποψήφιους πελατών του, για λογαριασμό του κάθε πελάτη του. Στην πρώτη περίπτωση, το εν λόγω Γραφείο ενεργεί ως υπεύθυνος επεξεργασίας ενώ, στη δεύτερη, ως εκτελών την επεξεργασία. Σε άλλη περίπτωση, μια επιχείρηση μπορεί να δραστηριοποιείται στην παροχή συμβουλευτικών υπηρεσιών για τα συστήματα αρχειοθέτησης (**Άρθρο 4(6)**) που τηρούν οι πελάτες της. Ταυτόχρονα, μπορεί να προσφέρει και υπηρεσίες φύλαξης ηλεκτρονικών και έντυπων εγγράφων των πελατών της. Στην πρώτη περίπτωση η εταιρεία ενεργεί ως υπεύθυνος επεξεργασίας ενώ στη δεύτερη ως εκτελών. Μια υπεραγορά αναθέτει σε μια εταιρεία μάρκετινγκ τη διενέργεια έρευνας ικανοποίησης των πελατών της. Στη στήλη αυτή θα πρέπει να γραφτούν το όνομα και τα στοιχεία επαφής του υπεύθυνου επεξεργασίας της υπεραγοράς καθώς και της εταιρείας μάρκετινγκ, ως ο εκτελών την επεξεργασία. Η καταγραφή της ιδιότητας του οργανισμού, ως υπεύθυνου ή ως εκτελούντα, για κάθε ξεχωριστή δραστηριότητα, είναι πολύ σημαντική αφού ο Κανονισμός θέτει διαφορετικές υποχρεώσεις για τον υπεύθυνο επεξεργασίας (**Άρθρα 24, 25(2)**) και διαφορετικές για τον εκτελούντα την επεξεργασία (**Άρθρο 28**), ιδιαίτερα όσον αφορά στη διαχείριση, και ανακοίνωση παραβιάσεων προσωπικών δεδομένων (**Άρθρα 33, 34**). Σε ορισμένες περιπτώσεις, δύο ή περισσότεροι οργανισμοί μπορεί να ενεργούν ως από κοινού υπεύθυνοι επεξεργασίας (**Άρθρο 26**) και να αποφασίζουν, από κοινού, το σκοπό και τον τρόπο επεξεργασίας. Τέτοια περίπτωση

μπορεί να είναι, για παράδειγμα όταν, αριθμός επιχειρήσεων ταχυφαγίας, για να μειώσουν τα κόστη τους, αποφασίζουν από κοινού, τη δημιουργία ενός τηλεφωνικού κέντρου για να δέχεται παραγγελίες και να εκτελεί την παράδοση τους. Όταν ένας οργανισμός εδρεύει εκτός της ΕΕ αλλά προσφέρει αγαθά ή υπηρεσίες σε πρόσωπα στην ΕΕ, ή παρακολουθεί τη συμπεριφορά τους, έχει υποχρέωση να ορίσει εκπρόσωπο του στην ΕΕ (**Άρθρα 3(2), 27**). Αν ο οργανισμός αυτός έχει ορίσει εκπρόσωπό του στην Κύπρο, στη στήλη 4(α) θα πρέπει να γραφτεί η ιδιότητά του και στη στήλη 4(β) το όνομα και τα στοιχεία επαφής του. Η συμπλήρωση της στήλης αυτής θα βοηθήσει κα στη συμπλήρωση της στήλης (11), αφού η ιδιότητα του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία και, όπου υπάρχουν, οι αντίστοιχες αρμοδιότητες των από κοινού υπεύθυνων επεξεργασίας, παίζουν σημαντικό ρόλο στη διενέργεια εκτίμησης αντίκτυπου (**Άρθρο 34**) και στη διαδικασία προηγούμενης διαβούλευσης (**Άρθρο 35**).

5. Σκοπός της Επεξεργασίας

Στη στήλη αυτή γίνεται μια σύντομη περιγραφή του σκοπού της κάθε επεξεργασίας. Η στήλη αυτή είναι απόλυτα συνυφασμένη με τη στήλη 2 που αφορά στο αν μια επεξεργασία είναι κύρια/ βασική ή παρεπόμενη, τη στήλη 3 που αφορά στη νομική βάση της κάθε επεξεργασίας και με τις στήλες 6(β) και 9 που αφορούν στις κατηγορίες των δεδομένων προσωπικού χαρακτήρα και στην προβλεπόμενη προθεσμία διαγραφής τους, αντίστοιχα. Αν μια δραστηριότητα εξυπηρετεί διάφορους σκοπούς, στη στήλη αυτή θα πρέπει να καταγραφεί έκαστος σκοπός και η περιγραφή του. Για παράδειγμα, μια υπεραγορά έχει, ως παρεπόμενη επεξεργασία σύστημα δωροκάρτας (loyalty card) το οποίο χρησιμοποιεί μόνο για σκοπούς παροχής προνομίων ή δώρων στους πελάτες της. Στο σύστημα δεν το καταχωρούνται οι αγορές του κάθε πελάτη. Μια δεύτερη υπεραγορά, διατηρεί παρόμοιο σύστημα, το οποίο όμως χρησιμοποιεί για σκοπούς παροχής προνομίων ή δώρων αλλά και για σκοπούς αποστολής μηνυμάτων sms στους πελάτες της για προσφορές. Για το σκοπό αυτό, συλλέγει και τον αριθμό του κινητού τηλεφώνου των πελατών της. Μια τρίτη υπεραγορά έχει διαφορετικό σύστημα το οποίο χρησιμοποιεί για την παροχή προνομίων ή δώρων, την αποστολή διαφημιστικών sms αλλά και για την κατάρτιση προφίλ (**Άρθρο 4(4)**) των πελατών τους, με βάση τις καταναλωτικές τους συνήθειες, δηλαδή τι αγοράζουν, πότε το αγοράζουν, προτιμήσεις σε προϊόντα, ποσότητες, τρόπος πληρωμής κλπ, για σκοπούς προγραμματισμού των παραγγελιών της και προσφοράς εξατομικευμένων προσφορών. Και οι τρεις υπεραγορές συλλέγουν τα προσωπικά δεδομένα, με τη συγκατάθεση των πελατών τους. Για τις δύο πρώτες, η δραστηριότητα αυτή μπορεί να θεωρηθεί ως παρεπόμενη αλλά, για την τρίτη, η δραστηριότητα θα πρέπει να θεωρηθεί ως κύρια/ βασική. Στη στήλη αυτή, η κάθε υπεραγορά θα πρέπει να καταγράψει τους σκοπούς που επιδιώκει με το δικό της σύστημα δωροκάρτας. Ο Κανονισμός επιβάλλει σε οργανισμούς όπως ενημερώνουν κατάλληλα τα υποκείμενα των δεδομένων για τους σκοπούς της κάθε επεξεργασίας. Γι' αυτό, η συμπλήρωση της στήλης αυτής θα βοηθήσει και στη συμπλήρωση της τελευταίας στήλης που αφορά στην πληροφόρηση που δίνεται στα υποκείμενα των δεδομένων, για κάθε ξεχωριστή δραστηριότητα. Στο πιο πάνω παράδειγμα, αν οι δύο πρώτες υπεραγορές, αποφασίσουν σε κάποιο στάδιο να εγκαταστήσουν σύστημα δωροκάρτας παρόμοιο με της τρίτης, θα πρέπει να εξετάσουν αν οι καινούργιοι σκοποί που επιδιώκουν είναι συμβατοί με τους αρχικούς (**Άρθρο 5(1)(β)**) και αν η επεξεργασία των προσωπικών δεδομένων των υφιστάμενων πελατών τους

μπορεί να βασιστεί στη συγκατάθεση που αρχικά είχαν δώσει (**Άρθρο 6(4)**). Αν η εκπλήρωση ενός σκοπού βασίζεται στο έννομο συμφέρον που επιδιώκει ο οργανισμός (**Άρθρο 6(1)στ)**), συστήνεται όπως, στο πεδίο αυτό καταγραφτεί το σκεπτικό γιατί το συμφέρον αυτό υπερέχει των συμφερόντων, θεμελιωδών δικαιωμάτων και ελευθεριών των υποκειμένων των δεδομένων. Η συμπλήρωση της στήλης αυτής είναι ιδιαίτερα σημαντική και για δημόσιες Αρχές που προσφέρουν αριθμό υπηρεσιών ή επιδομάτων στη βάση διαφορετικών νομοθεσιών και πρέπει να συλλέγουν, στα έντυπα των αιτήσεων, εκείνα τα δεδομένα που είναι απαραίτητα, με βάση την οικεία νομοθεσία.

6(α),(β). <u>Κατηγορίες υποκειμένων των δεδομένων και κατηγορίες προσωπικών δεδομένων</u>

Στη στήλη 6(α) καταγράφεται η κατηγορία των υποκειμένων των δεδομένων στην οποία αφορά η κάθε επεξεργασία. Κατηγορίες δεδομένων μπορεί να είναι πελάτες, προμηθευτές, συνεργάτες, υπάλληλοι, επισκέπτες της ιστοσελίδας κλπ, ανάλογα με τον τομέα δραστηριότητας του κάθε οργανισμού. Για δημόσιες Αρχές, μια κατηγορία υποκειμένων των δεδομένων μπορεί να είναι τα πρόσωπα που αιτούνται μια συγκεκριμένη υπηρεσία ή επίδομα. Αν μια κατηγορία αφορά παιδιά ή αν σε αυτή περιλαμβάνονται και παιδιά, συστήνεται όπως αυτό καταγραφτεί στη στήλη 6(α), αφού ο Κανονισμός θεσπίζει ειδικές πρόνοιες για παιδιά (**Άρθρα 6(1)(στ), 8, 12, 40(2)(ζ) και αιτιολογικές σκέψεις 38, 58, 65, 71 και 75**). Η συμπλήρωση της στήλης 6(α) θα βοηθήσει και στη συμπλήρωση της τελευταίας στήλης του Πίνακα που αφορά στην πληροφόρηση που δίνεται στα υποκείμενα των δεδομένων, για κάθε ξεχωριστή δραστηριότητα ενός οργανισμού. Στη στήλη 6(β) καταγράφονται τα προσωπικά δεδομένα που αφορούν στην κάθε κατηγορία υποκειμένων των δεδομένων. Για παράδειγμα, αν η κατηγορία των υποκειμένων των δεδομένων αφορά στους υπαλλήλους του οργανισμού, στη στήλη 6(β) θα πρέπει να καταγραφούν όλα τα δεδομένα που η εταιρεία τηρεί για αυτούς. Σε κάθε περίπτωση, τα προσωπικά δεδομένα που επεξεργάζεται ένας οργανισμός πρέπει να περιορίζονται στο μέτρο του αναγκαίου για τους σκοπούς που εξυπηρετεί η κάθε ξεχωριστή δραστηριότητα του οργανισμού (**Άρθρο 6(1)(γ**). Η συλλογή υπερβολικών πληροφοριών για τους σκοπούς της κάθε επεξεργασίας παραβαίνει τον Κανονισμό και δημιουργεί αχρείαστο κόστος για ένα οργανισμό. Η άσκηση της στήλης 6(β) μπορεί να βοηθήσει στον εντοπισμό αχρείαστων πληροφοριών που ένας οργανισμός συνέλεγε βάσει παλαιότερων πρακτικών.

7. <u>Κατηγορίες αποδεκτών</u>

Στη στήλη 7 καταγράφονται οι κατηγορίες των αποδεκτών (**Άρθρο 4(9)**) στους οποίους ενδέχεται να γνωστοποιούνται τα προσωπικά δεδομένα των υποκειμένων των δεδομένων. Για παράδειγμα, ένα ταξιδιωτικό γραφείο που κλείνει αεροπορικά εισιτήρια και δωμάτια ξενοδοχείων σε πελάτες του, στη στήλη αυτή θα πρέπει να καταγράψει, ως κατηγορίες αποδεκτών, τις αεροπορικές εταιρίες και τα ξενοδοχεία. Αν μια επιχείρηση έχει εκ του νόμου υποχρέωση να γνωστοποιεί πληροφορίες που αφορούν πελάτες ή υπαλλήλους της σε κάποιες δημόσιες Αρχές, στη στήλη αυτή θα πρέπει να καταγραφεί η γενική κατηγορία, «Δημόσιες Αρχές». Για παράδειγμα, αν μια επιχείρηση που δραστηριοποιείται στον τομέα των επενδύσεων ή στον τομέα της παροχής διοικητικών υπηρεσιών έχει νομική υποχρέωση να γνωστοποιεί σε ρυθμιστικές Αρχές στις οποίες υπάγεται, πληροφορίες για κάποιες κατηγορίες πελατών της, στο πεδίο αυτό, θα πρέπει να καταγραφτεί η κατηγορία

των ρυθμιστικών Αρχών. Σημειώνεται ότι, δεν θεωρείται αποδέκτης μια δημόσια Αρχή που ζητεί από ένα οργανισμό, πληροφορίες για κάποιο πελάτη του, στα πλαίσια συγκεκριμένης έρευνας για τον πελάτη αυτό. Παρόλο ο Κανονισμός δεν υποχρεώνει την καταγραφή συγκεκριμένων αποδεκτών αλλά μόνο κατηγοριών τους, αν αυτό είναι εύκολο, συστήνεται ως καλή πρακτική, αφού μπορεί να βοηθήσει τον οργανισμό να έχει μια πιο σφαιρική εικόνα και αφού θα είναι σε θέση να παράσχει καλύτερη ενημέρωση στα επηρεαζόμενα πρόσωπα. Σημειώνεται ότι, στη στήλη αυτή καταγράφονται και οι κατηγορίες αποδεκτών στους οποίους τα ίδια τα υποκείμενα ζητούν από τον οργανισμό, όπως γνωστοποιήσει τα δεδομένα τους. Τέτοια μπορεί να είναι, για παράδειγμα, η περίπτωση όπου, επιχείρηση, κατόπιν αιτήματος των πελατών της αποστέλλει στις τράπεζες τους, αγορά-πωλητήρια ή άλλα έγγραφα, για σκοπούς χρηματοδότησης (financing) ή δανειοδότησης. Σε αυτή την περίπτωση, θα πρέπει να καταγραφτεί, ως κατηγορία πελατών «τράπεζες των πελατών». Στη στήλη αυτή θα πρέπει να περιληφθούν και οι κατηγορίες αποδεκτών που βρίσκονται σε τρίτες χώρες και στους οποίους διαβιβάστηκαν ή πρόκειται να διαβιβαστούν προσωπικά δεδομένα των υποκειμένων των δεδομένων.

8. <u>Διαβίβαση σε τρίτες χώρα/ διεθνή οργανισμό</u>

Αν ένας οργανισμός διαβιβάζει προσωπικά δεδομένα σε τρίτη χώρα, δηλαδή εκτός της ΕΕ ή σε διεθνή οργανισμό (**Άρθρο 4(26)**), σε αυτό το πεδίο θα πρέπει να καταγράψει τα σχετικά με αυτές τις διαβιβάσεις, δηλαδή, τι διαβιβάζει, σε ποιον τα διαβιβάζει και που βρίσκεται ο παραλήπτης των δεδομένων. Διαβίβαση δεδομένων μπορεί να γίνεται από υπεύθυνο επεξεργασίας ή από εκτελούντα την επεξεργασία που βρίσκεται στην Κύπρο, σε υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία που βρίσκεται σε τρίτη χώρα ή σε διεθνή οργανισμό. Η διαβίβαση μπορεί να γίνεται από και προς επιχειρήσεις ενός ομίλου επιχειρήσεων ή από μια επιχείρηση σε άλλη ή από μια δημόσια σε Αρχή σε άλλη στα πλαίσια διοικητικής συνεργασίας. Ο Κανονισμός προσφέρει αριθμό εργαλείων που μπορεί να αποτελέσουν τη νομική βάση για την πραγματοποίηση τέτοιων διαβιβάσεων. Τέτοια εργαλεία είναι οι Αποφάσεις Επάρκειας (**Άρθρο 45**), οι κατάλληλες εγγυήσεις (**Άρθρο 46**) και οι δεσμευτικοί εταιρικοί κανόνες (**Άρθρο 47**), οι οποίοι, κατά κανόνα, χρησιμοποιούνται από ομίλους επιχειρήσεων. Ορισμένα από αυτά τα εργαλεία απαιτούν να ληφθεί η έγκριση της Επιτρόπου. Ο κάθε οργανισμός μπορεί να επιλέξει το νομικό εργαλείο που τον εξυπηρετεί καλύτερα, ανάλογα με τις ανάγκες του και το σκοπό και το είδος της διαβίβασης. Αν ένας οργανισμός είναι σε θέση να αποδείξει ότι, δεν μπορεί ή δεν ενδείκνυται να χρησιμοποιήσει κάποια από αυτά τα νομικά εργαλεία, μπορεί να διαβιβάσει δεδομένα στη βάση παρεκκλίσεων για ειδικές καταστάσεις. Ωστόσο, λόγω ψηλού κινδύνου πρέπει να χρησιμοποιούνται ως το έσχατο μέτρο για την πραγματοποίηση της διαβίβασης. Για διαβίβαση στη βάση παρεκκλίσεων ένας οργανισμός ίσως να πρέπει να διενεργήσει εκτίμηση αντίκτυπου (**Άρθρο 35**) και ή να διαβουλευτεί με την Επίτροπο (**Άρθρο 36**) πριν πραγματοποιηθεί η προβλεπόμενη διαβίβαση. Η εκτίμηση αντίκτυπου πρέπει να προβλέπει μέτρα μετριασμού του κινδύνου που συνεπάγεται η διαβίβαση στη βάση των παρεκκλίσεων. Η Επίτροπος θα καταρτίσει και θα δημοσιεύσει κατάλογο των πράξεων επεξεργασίας για τις οποίες θα απαιτείται η διενέργεια εκτίμησης αντίκτυπου και μπορεί να δημοσιεύσει και κατάλογο πράξεων για τις οποίες δεν θα χρειάζεται τέτοια εκτίμηση (**Άρθρα 35(4),(5)**). Μια περιστασιακή διαβίβαση που δεν είναι επαναλαμβανόμενη και αφορά περιορισμένο αριθμό υποκειμένων των δεδομένων, μπορεί να πραγματοποιηθεί

χωρίς να βασίζεται σε κάποιο από τα προαναφερόμενα νομικά εργαλεία, μόνο για επιτακτικούς νόμιμους σκοπούς που επιδιώκει ένας οργανισμός, νοουμένου ότι, οι σκοποί αυτοί υπερέχουν των συμφερόντων, δικαιωμάτων και ελευθεριών των υποκειμένων των δεδομένων. Σε τέτοια περίπτωση, ο οργανισμός πρέπει να εκτιμήσει τους κινδύνους που συνεπάγεται η διαβίβαση και να λάβει τις δέουσες εγγυήσεις. Στη στήλη αυτή πρέπει να καταγράφεται, υποχρεωτικά, η εκτίμηση που έχει γίνει και οι δέουσες εγγυήσεις που έχουν ληφθεί. Ωστόσο, συστήνεται όπως, καταγράφεται το νομικό εργαλείο που χρησιμοποιείται για κάθε ξεχωριστή διαβίβαση, δηλαδή αν αυτή βασίζεται σε απόφαση επάρκειας, ή σε επαρκείς εγγυήσεις, ή σε δεσμευτικούς εταιρικούς κανόνες, αφού ο οργανισμός θα πρέπει να ενημερώσει κατάλληλα τα υποκείμενα των δεδομένων (**Άρθρα 13(1)(στ), 14(1)(στ)**) για κάθε διαβίβαση. Η συμπλήρωση της στήλης αυτής θα βοηθήσει και στη συμπλήρωση της τελευταίας στήλης του Πίνακα, που αφορά στην πληροφόρηση που δίνεται στα υποκείμενα των δεδομένων. Επίσης, ένας οργανισμός ίσως χρειάζεται να δημοσιεύσει κάποιες πληροφορίες για τη νομιμότητα των διαβιβάσεων που πραγματοποιεί, για να επιδείξει τη συμμόρφωσή του με τον Κανονισμό, σύμφωνα με τις Αρχές της Λογοδοσίας και της Διαφάνειας.

9. <u>Διαγραφή των δεδομένων</u>

Με βάση την Αρχή του περιορισμού της αποθήκευσης (**Άρθρο 5(1)(ε)**), όταν εκπληρωθεί ο σκοπός μιας επεξεργασίας, η κατηγορία των δεδομένων που αφορούν στη συγκεκριμένη επεξεργασία, πρέπει να διαγράφονται. Στη στήλη αυτή καταγράφεται η προβλεπόμενη προθεσμία διαγραφής των δεδομένων που αφορούν σε κάθε ξεχωριστή δραστηριότητα επεξεργασίας Ορισμένες φορές, η προθεσμία είναι εύκολο να καθοριστεί, για παράδειγμα, όταν προβλέπεται από νόμο. Π.χ. για τη διαγραφή δεδομένων πελατών, μετά το πέρας της πελατειακής σχέσης, θα πρέπει να ληφθεί υπόψη η νομοθεσία του Τμήματος Φορολογίας και για τη διαγραφή δεδομένων υπαλλήλων, μετά το πέρας της σχέσης εργασίας, η νομοθεσία των Υπηρεσιών Κοινωνικών Ασφαλίσεων, αντίστοιχα. Δημόσιες Υπηρεσίες θα πρέπει να εξετάσουν την οικεία νομοθεσία που εφαρμόζουν και το Νόμο του Κρατικού Αρχείου. Οργανισμοί που δραστηριοποιούνται σε ορισμένους τομείς δραστηριοτήτων, όπως τον επενδυτικό και τον χρηματοπιστωτικό θα πρέπει να εξετάσουν τις οικείες νομοθεσίες που εφαρμόζουν, για τον καθορισμό της προθεσμίας διαγραφής. Ορισμένες φορές όμως, θα είναι δύσκολο να καθοριστεί εκ των προτέρων η προθεσμία διαγραφής κάποιων κατηγοριών προσωπικών δεδομένων, ιδίως όταν προκύψει ανάγκη, μια κατηγορία δεδομένων, να τύχει περαιτέρω επεξεργασίας (**Άρθρα 5(1)(β), 6(4)**) για κάποιο νόμιμο σκοπό που επιδιώκει ένας οργανισμός. Όπου είναι δυνατό, πρέπει να καταγράφεται ή ακριβής προθεσμία διαγραφής. Όπου αυτό δεν είναι δυνατό, ή είναι δύσκολο να καθοριστεί, πρέπει να υπολογίζεται και να καταγράφεται, η εκτιμώμενη προθεσμία διαγραφής. Σε κάθε περίπτωση, ο οργανισμός θα πρέπει να είναι σε θέση να αιτιολογήσει, είτε την ακριβή, είτε την εκτιμώμενη προθεσμία. Με βάση τον Κανονισμό, σε ορισμένες περιπτώσεις, πριν τη διαγραφή μιας κατηγορίας δεδομένων, ο οργανισμός ίσως έχει υποχρέωση να απομονώσει κάποια δεδομένα ή να περιορίσει την επεξεργασία τους (**Άρθρο 18**) ή να τα κρυπτογραφήσει ή να τα ψευδωνυμοποιήσει (**Άρθρα 4(5), 6(4)(ε), 25, 40(2)(δ), 89**), ιδίως όταν δεν είναι πλέον απαραίτητη η εξακρίβωση της ταυτότητας των υποκειμένων των δεδομένων (**Άρθρο 11**) ή όταν αυτό απαιτείται από εγκεκριμένο Κώδικα δεοντολογίας στον οποίο υπόκειται ένας οργανισμός (**Άρθρο 40(2)(δ)**). Παρόλο που δεν

υπάρχει υποχρέωση καταγραφής τέτοιων προθεσμιών στη στήλη αυτή, συστήνεται ως καλή πρακτική, αφού θα βοηθήσει και στη συμπλήρωση της στήλης (10) που αφορά στα τεχνικά και οργανωτικά μέτρα ασφάλειας.

10. Τεχνικά και οργανωτικά μέτρα ασφάλειας

Κάθε οργανισμός έχει υποχρέωση να λαμβάνει τα απαραίτητα τεχνικά και οργανωτικά μέτρα για την ασφάλεια της επεξεργασίας (**Άρθρο 32**), είτε ενεργεί ως υπεύθυνος επεξεργασίας (**Άρθρο 24(1)**) είτε ως εκτελών την επεξεργασία (**Άρθρο 28(1)**), ιδίως όταν είναι επιχείρηση τεχνολογίας που σχεδιάζει και αναπτύσσει (**Άρθρο 25**) συστήματα αρχειοθέτησης (**Άρθρο 4(6)**) για λογαριασμό των πελατών της, λαμβάνοντας υπόψη, μεταξύ άλλων, τη φύση και το σκοπό της επεξεργασίας και τους κινδύνους που αυτή συνεπάγεται. Στη στήλη αυτή καταγράφονται αυτά τα μετρά ασφάλειας, ανάλογα με την ιδιότητα του οργανισμού (**δείτε στήλη 4(α)**). Τεχνικά μέτρα ασφάλειας μπορεί να είναι για παράδειγμα, η κρυπτογράφηση και ψευδωνυμοποίηση (**Άρθρα 4(5), 6(4)(ε), 25, 40(2)(δ), 89**) και ο περιορισμός της επεξεργασίας (**Άρθρο 18**), η αποθήκευση αντιγράφων αρχείων (back ups), η ανάκτηση αρχείων σε περίπτωση καταστροφής (disaster recovery) και η εφαρμογή firewalls για προστασία συστημάτων συνδεδεμένων με το διαδίκτυο από κακόβουλα λογισμικά (malware). Οργανωτικό μέτρο ασφάλειας μπορεί να είναι η παροχή, σε μέλη ενός οργανισμού, δυνατότητας πρόσβασης στο σύστημα αρχειοθέτησης του, ανάλογα με την ιεραρχία τους (κάθετη πρόσβαση) και τα καθήκοντά τους (οριζόντια) πρόσβαση, ώστε να διασφαλιστεί ότι το κάθε μέλος έχει πρόσβαση μόνο σε εκείνα τα δεδομένα που απαιτεί η θέση και τα καθήκοντά του. Άλλα οργανωτικά μέτρα μπορεί να περιλαμβάνουν τη φύλαξη του χώρου που είναι εγκατεστημένος ο εξυπηρετητής (server) και ποιοι θα έχουν πρόσβαση στο χώρο αυτό. Για κλειστά κυκλώματα βίντεο-παρακολούθησης, τα οργανωτικά μέτρα ασφάλειας επιβάλλουν, μεταξύ άλλων, να καταγραφεί ο χώρος που βρίσκεται η οθόνη (monitor) παρακολούθησης, ποιος θα έχει πρόσβαση σε αυτή και υπό ποιες προϋποθέσεις. Σύμφωνα με τις Καθοδηγητικές Γραμμές της Ομάδας Εργασίας του Άρθρου 29, για τη γνωστοποίηση παραβίασης προσωπικών δεδομένων στην Επίτροπο (**Άρθρα 4(12), 33**) και την ενημέρωση των επηρεαζόμενων υποκειμένων των δεδομένων (‘**Άρθρο 34**), τα τεχνικά και τα οργανωτικά μέτρα ασφάλειας θα πρέπει να διασφαλίζουν τη διαθεσιμότητα (accessibility), την γνησιότητα (authenticity) και την ακεραιότητά (integrity) και την εμπιστευτικότητα (confidentiality) των δεδομένων (Προοίμιο, αναφορά 49). Αν ένας οργανισμός δραστηριοποιείται στην παροχή υπηρεσιών της κοινωνίας της πληροφορίας, τα τεχνικά μέτρα ασφάλειας θα πρέπει να διασφαλίζουν και τη συνεχιζόμενη προσφορά των υπηρεσιών (cyber resilience). Τεχνικά μέτρα πρέπει να λαμβάνονται και για την ασφαλή άσκηση του δικαιώματος φορητότητας των δεδομένων (**Άρθρο 20**), κατόπιν αίτησης του υποκειμένου των δεδομένων. Σε περίπτωση όπου ένας οργανισμός χρησιμοποιεί σύστημα για την κατάρτιση προφίλ (**Άρθρο 4(4)**) ή για την αυτοματοποιημένη λήψη αποφάσεων, περιλαμβανομένης της κατάρτισής προφίλ (**Άρθρο 22**), τα οργανωτικά μέτρα ασφάλειας πρέπει να προβλέπουν την ανθρώπινη παρέμβαση, όπου απαιτείται. Η συμπλήρωση τη στήλης αυτής θα βοηθήσει και στη συμπλήρωση της τελευταίας στήλης του Πίνακα, που αφορά στην στοιχειώδη πληροφόρηση που πρέπει να δίνεται στα υποκείμενα των δεδομένων για τα τεχνικά και οργανωτικά μέτρα ασφάλειας, χωρίς να αποκαλύπτονται πληροφορίες που μπορεί να υπονομεύουν την ασφάλεια της αυτοματοποιημένης επεξεργασίας ή να προσβάλλουν το δικαίωμα διανοητικής ιδιοκτησίας

(intellectual property rights). Επίσης, μπορεί να βοηθήσει στην ικανοποίηση αιτημάτων άσκησης άλλων δικαιωμάτων, ιδίως αυτών που αφορούν στην πρόσβαση (**Άρθρο 15**) και στην εναντίωση (**Άρθρο 21**).

11(α),(β). Εκτίμηση αντίκτυπου και προηγούμενη διαβούλευση

Για ορισμένες πράξεις επεξεργασίας που ενέχεται να ελλοχεύουν ψηλούς κινδύνους, ιδίως όταν αφορούν στη χρήση νέας τεχνολογίας, πριν την εφαρμογή της, επιβάλλεται να διενεργηθεί εκτίμηση αντίκτυπου (**Άρθρο 35**), ώστε ο οργανισμός να λάβει κατάλληλα μέτρα μετριασμού των κινδύνων. Αν, ο οργανισμός δεν είναι σίγουρος ότι τα σχεδιαζόμενα μέτρα μετριάζουν τους κινδύνους αποτελεσματικά ή αν δεν μπορεί να σκεφτεί κάποια αποτελεσματικά μέτρα, τότε έχει υποχρέωση να υποβάλει την εκτίμηση αντίκτυπου στην Επίτροπο για προηγούμενη διαβούλευση (**Άρθρο 36**). Στη στήλη 11(α) καταγράφονται τα σχετικά με τις εκτιμήσεις αντίκτυπου και στη στήλη 11(β) τα σχετικά με τις προηγούμενες διαβουλεύσεις. Η εκτίμηση αντίκτυπου γίνεται σε τέσσερα στάδια και γι' αυτό, στη στήλη 11(α) θα πρέπει να καταγραφτούν τα εξής: (ι) Περιγραφή της προβλεπόμενης πράξης επεξεργασίας και της νομικής βάσης στην οποία αυτή βασίζεται. (ιι) Πώς η προβλεπόμενη επεξεργασία υπακούει τις Αρχές του περιορισμού του σκοπού και της ελαχιστοποίησης των δεδομένων (**Άρθρα 5(1)(β),(γ)**). (ιιι) τους κινδύνους που ενδέχεται να ελλοχεύει αυτή η πράξη για τα υποκείμενα των δεδομένων και (ιν) τα σχεδιαζόμενα μέτρα για τον μετριασμό των κινδύνων αυτών. Αν βοηθά, η στήλη 11(α) μπορεί να χωριστεί σε 4 υπό-στήλες (ι), (ιι), (ιιι) και (ιν). Αν ο οργανισμός έχει ορίσει υπεύθυνο προστασίας δεδομένων (δείτε στήλες 4(α),(β)), ο υπεύθυνος επεξεργασίας ζητεί την γνώμη του για την εκτίμηση αντίκτυπου (**Άρθρο 35(2)**). Γι' αυτό, συστήνεται όπως στη στήλη 11(α) καταγράφεται και μια περίληψη της γνώμης του υπεύθυνου προστασίας των δεδομένων. Στη στήλη 11(β) καταγράφονται (ι) οι πληροφορίες που ο οργανισμός έχει υποχρέωση να δώσει στην Επίτροπο (**Άρθρο 36(3)**) για να ζητήσει τη συμβουλή της και (ιι) τη συμβουλή που έλαβε από την Επίτροπο (**Άρθρο 36(2)**). Αν βοηθά, η στήλη 11(β) μπορεί να χωριστεί σε 2 υπό-στήλες (ι) και (ιι). Η συμπλήρωση της στήλης (11) μπορεί να βοηθήσει και στη συμπλήρωση της στήλης (8) που αφορά στη διαβίβαση δεδομένων, ιδιαίτερα όταν αυτή είναι περιστασιακή και αφορά περιορισμένο αριθμό υποκειμένων των δεδομένων, της στήλης (10) που αφορά στη λήψη τεχνικών και οργανωτικών μέτρων ασφάλειας, καθώς και της στήλης (12), που αφορά στην ενημέρωση των υποκειμένων των δεδομένων.

12. Ενημέρωση των υποκειμένων των δεδομένων

Η κατάλληλη ενημέρωση των υποκειμένων των δεδομένων (**Άρθρα 13, 14**) επιβάλλεται από τις Αρχές τις διαφάνειας και της λογοδοσίας (**Άρθρα 5(1)(α), 5(2), 12**) και αποτελεί την πεμπτουσία του Κανονισμού. Η ενημέρωση είναι ιδιαίτερα σημαντική όταν μια πράξη επεξεργασίας βασίζεται στη συγκατάθεση του υποκειμένου των δεδομένων (**Άρθρο 4(11)**) ή όταν το υποκείμενο των δεδομένων αποδέχεται τους όρους που περιλαμβάνονται σε ένα συμβόλαιο (**Άρθρο 7(4)**) ή όταν η επεξεργασία βασίζεται σε ένα έννομο συμφέρον που επιδιώκει ένας οργανισμός. Ανάλογα με την κατηγορία των υποκειμένων των δεδομένων, η ενημέρωση πρέπει να είναι διαφανής, κατανοητή, σε εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή διατύπωση (**Άρθρο 12(1)**), ιδιαίτερα όταν δίνεται σε παιδιά (**Άρθρα 6(1)(στ) και 8, Προοίμιο αναφορές 58 και 71**). Στη στήλη αυτή πρέπει να

καταγράφεται ένα σύντομο κείμενο ενημέρωσης, το οποίο ο Οργανισμός προτίθεται να δίνει σε κάθε κατηγορία υποκειμένων των δεδομένων, για κάθε ξεχωριστή πράξη επεξεργασίας. Αν οι υπόλοιπες στήλες του Πίνακα έχουν συμπληρωθεί σωστά, η συμπλήρωση αυτής της στήλης θα είναι μια σχετικά εύκολη δουλειά. Αν ένας οργανισμός επιθυμεί, ή χρειάζεται να έχει πολιτική προστασίας της ιδιωτικής ζωής (privacy policy) η συμπλήρωση αυτής της στήλης θα συμβάλει στη σύνταξη και στη διαμόρφωσή της. Τέτοιες πολιτικές μπορεί να είναι εσωτερικές, δηλαδή να αφορούν στους υπαλλήλους του οργανισμού ή εξωτερικές, δηλαδή να αφορούν πελάτες, συνεργάτες, προμηθευτές του οργανισμού, ή χρήστες ή επισκέπτες της ιστοσελίδας του. Για παράδειγμα, αν μια δραστηριότητα αφορά στην χρήση συστήματος GPS σε οχήματα μιας επιχείρησης, στη στήλη αυτή θα πρέπει να καταγραφεί ότι, «*η θέση και κίνηση των οχημάτων δύναται να παρακολουθείται και ή να καταγράφεται μέσω συστήματος GPS*». Στην αντίστοιχη εσωτερική πολιτική προστασίας της ιδιωτικής ζωής μπορεί να καταγραφεί το εξής κείμενο: «*Η χρήση των οχημάτων της επιχείρησης επιτρέπεται μόνο για υπηρεσιακούς σκοπούς. Η θέση και η κίνηση των οχημάτων ενδέχεται να καταγράφεται και/ ή να παρακολουθείται από τον διαχειριστή (administrator) εκ μέρους της διεύθυνσης, μέσω συστήματος GPS».* Αν μια πράξη επεξεργασίας βασίζεται σε υποχρέωση του οργανισμού που απορρέει από Νόμο, το κείμενο της ενημέρωσης θα πρέπει να αναφέρει ότι, τα δεδομένα που αφορούν στη συγκεκριμένη πράξη συλλέγονται με βάση το συγκεκριμένο νόμο. Όταν ένας οργανισμός κοινοποιεί δεδομένα σε μια κατηγορία αποδεκτών, στο κείμενο της ενημέρωσης θα πρέπει να αναφέρει το σκοπό της κοινοποίησης σε αυτούς του αποδέκτες. Στο κείμενο της ενημέρωσης πρέπει να περιλαμβάνεται στοιχειώδης πληροφόρηση για τα τεχνικά και οργανωτικά μέτρα ασφάλειας που λαμβάνει ένας οργανισμός, χωρίς να αποκαλύπτονται πληροφορίες που μπορεί να υπονομεύσουν την ασφάλεια της επεξεργασίας ή να προσβάλλουν το δικαίωμα διανοητικής ιδιοκτησίας του οργανισμού.

ΜΕΡΟΣ Γ - Χρήσιμες πληροφορίες

Ο Πίνακας αυτός σχεδιάστηκε για να εξυπηρετήσει την πλειοψηφία των οργανισμών στην Κύπρο. Ο κάθε οργανισμός μπορεί να τον προσαρμόσει, με βάση τις δικές του ανάγκες και ιδιαιτερότητες. Αν ένας οργανισμός έχει απορίες για τη συμπλήρωση κάποιων πεδίων, μπορεί να επικοινωνήσει τηλεφωνικώς με το Γραφείο μας. Ωστόσο, το Γραφείο μας μπορεί να δώσει μόνο γενική καθοδήγηση, αφού, για την συγκεκριμένη συμπλήρωση του Πίνακα, απαιτείται ενδελεχής και εις βάθος γνώση για το ποιος είναι ο οργανισμός, τι ακριβώς κάνει και πώς το κάνει. Ο Πίνακας αυτός ενδέχεται να τροποποιηθεί μερικώς μετά την υιοθέτηση του Νόμου για την καλύτερη εφαρμογή ορισμένων διατάξεων του Κανονισμού, ώστε να καλύψει και κάποιες πρόσθετες υποχρεώσεις που μπορεί να προβλέπει ο Νόμος αυτός. Σε κάθε περίπτωση, ο επισυνημμένος Πίνακας καλύπτει σε μεγάλος μέρος τις υποχρεώσεις των οργανισμών και η συμπλήρωσή του αποτελεί ένα καλό πρώτο βήμα για συμμόρφωση τους, με τις διατάξεις του Κανονισμού.