

1. Ο υπεύθυνος επεξεργασίας

1.1. Υπεύθυνος επεξεργασίας των δεδομένων προσωπικού χαρακτήρα για το σύνολο των επεξεργασιών που διενεργούνται από τις υπηρεσίες του Οργανισμού Εσωτερικής Υπηρεσίας της ΕΕΑ είναι η Ελεήμων Εταιρεία Αθηνών, νομικό πρόσωπο ιδιωτικού δικαίου, όπως νόμιμα εκπροσωπείται (κατά τον ορισμό του άρθρου 4 αρ. 7 του Γενικού Κανονισμού Προστασίας Δεδομένων). Η Ελεήμων Εταιρεία Αθηνών καθορίζει τον σκοπό και τον τρόπο της επεξεργασίας δεδομένων από τις ανωτέρω υπηρεσίες.

1.2. Οι εργαζόμενοι, με οποιαδήποτε εργασιακή σχέση, στις ανωτέρω υπηρεσίες που επεξεργάζονται δεδομένα προσωπικού χαρακτήρα είναι “πρόσωπα που ενεργούν υπό την εποπτεία του υπεύθυνου επεξεργασίας” (κατά τον ορισμό του άρθρου 29 του Γ.Κ.Π.Δ.)

1.3. Άλλα φυσικά ή νομικά πρόσωπα που επεξεργάζονται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπεύθυνου επεξεργασίας είναι “εκτελούντες την επεξεργασία” (κατά τον ορισμό του άρθρου 4 αρ. 8 του Γ.Κ.Π.Δ.).

2. Ο υπεύθυνος προστασίας δεδομένων

2.1. Η Ελεήμων Εταιρεία Αθηνών έχει ορίσει Υπεύθυνο Προστασίας Δεδομένων (DPO) (άρθρο 37 Γ.Κ.Π.Δ.).

2.2. Καθήκοντα του DPO είναι:

α) Ενημερώνει και συμβουλεύει τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία και τους υπαλλήλους που επεξεργάζονται τις υποχρεώσεις τους που απορρέουν από τον Γ.Κ.Π.Δ. και από άλλες διατάξεις σχετικά με την προστασία δεδομένων,

β) παρακολουθεί τη συμμόρφωση με τον Γ.Κ.Π.Δ., με άλλες διατάξεις σχετικά με την προστασία δεδομένων και με τις πολιτικές του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία σε σχέση με την προστασία των δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων της ανάθεσης αρμοδιοτήτων, της ευαισθητοποίησης και της κατάρτισης των υπαλλήλων που συμμετέχουν στις πράξεις επεξεργασίας, και των σχετικών ελέγχων,

γ) παρέχει συμβουλές, όταν ζητείται, όσον αφορά την εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων και παρακολουθεί την υλοποίησή της σύμφωνα με το άρθρο 35 Γ.Κ.Π.Δ.,

δ) συνεργάζεται με την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα,

ε) ενεργεί ως σημείο επικοινωνίας για την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα για ζητήματα που σχετίζονται με την επεξεργασία, περιλαμβανομένης της προηγούμενης διαβούλευσης που αναφέρεται στο άρθρο 36 Γ.Κ.Π.Δ., και πραγματοποιεί διαβουλεύσεις, ανάλογα με την περίπτωση, για οποιοδήποτε άλλο θέμα.

3. Νομιμότητα επεξεργασιών δεδομένων από την ΕΕΑ

3.1. Η επεξεργασία προσωπικών δεδομένων από την ΕΕΑ επιτρέπεται μόνον εφόσον προβλέπεται από σχετικές διατάξεις, στις ακόλουθες περιπτώσεις.

3.2. Η επεξεργασία επιτρέπεται εφόσον είναι απαραίτητα για την εκτέλεση σύμβασης της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή για να ληφθούν μέτρα κατ' αίτηση του υποκειμένου πριν από τη σύναψη της σύμβασης (άρθρο 6 περ. β' Γ.Κ.Π.Δ.)

3.3. Η επεξεργασία επιτρέπεται εφόσον είναι απαραίτητη για τη συμμόρφωση της ΕΕΑ με έννομη υποχρέωσή της. Κατά κύριο λόγο, η ΕΕΑ επεξεργάζεται μόνο τα δεδομένα που είναι υποχρεωμένη να επεξεργάζεται για να ασκήσει τις προβλεπόμενες από την νομοθεσία αρμοδιότητές της (άρθρο 6 περ. γ' Γ.Κ.Π.Δ.). Όλες οι αρμοδιότητες που προβλέπονται ήδη από την νομοθεσία για την ΕΕΑ, εξακολουθούν να ασκούνται με νομική βάση της επεξεργασίας δεδομένων την διάταξη που ήδη τις προβλέπει.

3.4. Η επεξεργασία επιτρέπεται εφόσον είναι απαραίτητη για την διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου (άρθρο 6 περ. δ Γ.Κ.Π.Δ.)

3.5. Η επεξεργασία επιτρέπεται εφόσον είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση εξουσίας που έχει ανατεθεί στην ΕΕΑ (άρθρο 6 περ. ε Γ.Κ.Π.Δ.)

3.6. Κατ' αρχήν δεν επιτρέπεται επεξεργασία από την ΕΕΑ δεδομένων προσωπικού χαρακτήρα που βασίζεται στην "συγκατάθεση" του υποκειμένου των δεδομένων. Τέτοια συγκατάθεση δεν νοείται να παρέχει ο χρήστης στην ΕΕΑ. Οι χρήστες που παρέχουν τα δεδομένα τους για να ασκήσουν δικαιώματα ή να απολαύσουν παροχές από την ΕΕΑ, δεν το πράττουν στην βάση της συγκατάθεσής τους, αλλά στο πλαίσιο της υποχρέωσης της ΕΕΑ για ενάσκηση των αρμοδιοτήτων της, κατόπιν βεβαίως προηγούμενης ενημέρωσης των χρηστών. Ωστόσο, σε περιπτώσεις που μια υπηρεσία της ΕΕΑ παρέχεται στον χρήστη ως "υπηρεσία επιπρόσθετης αξίας", δηλαδή ο χρήστης μπορεί να την απολαύσει στην συμβατική της μορφή χωρίς συγκατάθεση ή και χωρίς καν να δώσει προσωπικά δεδομένα, αλλά η επιπρόσθετη αξία συνίσταται στην δυνατότητα ηλεκτρονικής ενεργοποίησης ή και παρακολούθησης, σε αυτές τις περιπτώσεις επιτρέπεται η επεξεργασία των προσωπικών δεδομένων επί τη βάσει της "συγκατάθεσης".

3.7. Δεν νοείται επεξεργασία δεδομένων από την ΕΕΑ δεδομένων προσωπικού χαρακτήρα που βασίζεται σε "έννομο συμφέρον" που υπερέχει των δικαιωμάτων και ελευθεριών του ατόμου (άρθρο 6 in. fin. Γ.Κ.Π.Δ.)

4. Διαφάνεια και ενημέρωση

4.1. Με την ανακοίνωση της παρούσας Πολιτικής Προστασίας Προσωπικών Δεδομένων της ΕΕΑ, τα υποκείμενα των δεδομένων ενημερώνονται για τους όρους υπό τους οποίους η ΕΕΑ επεξεργάζεται τα δεδομένα που τα αφορούν (άρθρο 12 Γ.Κ.Π.Δ.)

4.2. Στην περίπτωση που η ΕΕΑ συλλέγει δεδομένα από το ίδιο το υποκείμενο των δεδομένων, όπως π.χ. όταν το υποκείμενο του υποβάλλει μια αίτηση ή διαθέτει τα στοιχεία του για να αποκτήσει πρόσβαση σε μια υπηρεσία ή παροχή ή να ασκήσει κάποιο σχετικό δικαίωμα, η υπηρεσία παρέχει τις εξής πληροφορίες στο υποκείμενο των δεδομένων, με ευδιάκριτη σήμανση στο ίδιο το έντυπο της αίτησης ή στην ηλεκτρονική μορφή επικοινωνίας του χρήστη με την υπηρεσία:

α) Την ταυτότητα και τα στοιχεία επικοινωνίας του υπευθύνου επεξεργασίας και, κατά περίπτωση, του εκπροσώπου του υπευθύνου επεξεργασίας,

β) τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων, κατά περίπτωση,

γ) τους σκοπούς της επεξεργασίας για τους οποίους προορίζονται τα δεδομένα προσωπικού χαρακτήρα, καθώς και τη νομική βάση για την επεξεργασία,

δ) τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων προσωπικού χαρακτήρα, εάν υπάρχουν,

ε) κατά περίπτωση, την πρόθεση του υπευθύνου επεξεργασίας να διαβιβάσει δεδομένα προσωπικού χαρακτήρα σε τρίτη χώρα ή διεθνή οργανισμό και την ύπαρξη ή την απουσία απόφασης επάρκειας της Επιτροπής ή, όταν πρόκειται για τις διαβιβάσεις που αναφέρονται στο άρθρο 46 ή 47 ή στο άρθρο 49 παράγραφος 1 δεύτερο εδάφιο, αναφορά στις ενδεδειγμένες ή κατάλληλες εγγυήσεις και τα μέσα για να αποκτηθεί αντίγραφο τους ή στο πού διατέθηκαν,

στ) το χρονικό διάστημα για το οποίο θα αποθηκευτούν τα δεδομένα προσωπικού χαρακτήρα ή, όταν αυτό είναι αδύνατο, τα κριτήρια που καθορίζουν το εν λόγω διάστημα,

ζ) την ύπαρξη δικαιώματος υποβολής αιτήματος στον υπεύθυνο επεξεργασίας για πρόσβαση και διόρθωση ή διαγραφή των δεδομένων προσωπικού χαρακτήρα ή περιορισμό της επεξεργασίας που αφορούν το υποκείμενο των δεδομένων ή δικαιώματος αντίταξης στην επεξεργασία, καθώς και δικαιώματος στη φορητότητα των δεδομένων,

η) όταν η επεξεργασία βασίζεται στην συγκατάθεση, την ύπαρξη του δικαιώματος να ανακαλέσει τη συγκατάθεσή του οποτεδήποτε, χωρίς να θιγεί η νομιμότητα της επεξεργασίας που βασίστηκε στη συγκατάθεση πριν από την ανάκλησή της,

θ) το δικαίωμα υποβολής καταγγελίας στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα,

ι) κατά πόσο η παροχή δεδομένων προσωπικού χαρακτήρα αποτελεί νομική ή συμβατική υποχρέωση ή απαίτηση για τη σύναψη σύμβασης, καθώς και κατά πόσο το υποκείμενο των δεδομένων υποχρεούται να παρέχει τα δεδομένα προσωπικού χαρακτήρα και ποιες ενδεχόμενες συνέπειες θα είχε η μη παροχή των δεδομένων αυτών,

ια) την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ, που αναφέρεται στο άρθρο 22 παράγραφοι 1 και 4 και, τουλάχιστον στις περιπτώσεις αυτές, σημαντικές πληροφορίες σχετικά με τη λογική που ακολουθείται, καθώς και τη σημασία και τις προβλεπόμενες συνέπειες της εν λόγω επεξεργασίας για το υποκείμενο των δεδομένων.

4.3. Στην περίπτωση που η ΕΕΑ συλλέγει δεδομένα από άλλες πηγές και όχι από το ίδιο το υποκείμενο των δεδομένων, παρέχει στο υποκείμενο των δεδομένων τις ακόλουθες πληροφορίες, εκτός αν η συλλογή τους προβλέπεται ρητά στην νομοθεσία, οπότε δεν είναι υποχρεωμένη να προβεί στην σχετική ενημέρωση του υποκειμένου περί:

α) Την ταυτότητα και τα στοιχεία επικοινωνίας του υπευθύνου επεξεργασίας και, κατά περίπτωση, του εκπροσώπου του υπευθύνου επεξεργασίας,

β) τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων, κατά περίπτωση,

γ) τους σκοπούς της επεξεργασίας για τους οποίους προορίζονται τα δεδομένα προσωπικού χαρακτήρα, καθώς και τη νομική βάση για την επεξεργασία,

δ) τις σχετικές κατηγορίες δεδομένων προσωπικού χαρακτήρα,

ε) τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων προσωπικού χαρακτήρα, ενδεχομένως,

στ) κατά περίπτωση, ότι ο υπεύθυνος επεξεργασίας προτίθεται να διαβιβάσει δεδομένα προσωπικού χαρακτήρα σε αποδέκτη σε τρίτη χώρα ή διεθνή οργανισμό και την ύπαρξη ή την απουσία απόφασης επάρκειας της Επιτροπής ή, όταν πρόκειται για τις διαβιβάσεις που αναφέρονται στο άρθρο 46 ή 47 ή στο άρθρο 49 παράγραφος 1 δεύτερο εδάφιο, αναφορά στις ενδεδειγμένες ή κατάλληλες εγγυήσεις και τα μέσα για να αποκτηθεί αντίγραφο τους ή στο πού διατέθηκαν,

ζ) το χρονικό διάστημα για το οποίο θα αποθηκευτούν τα δεδομένα προσωπικού χαρακτήρα ή, όταν αυτό είναι αδύνατο, τα κριτήρια που καθορίζουν το εν λόγω χρονικό διάστημα,

η) την ύπαρξη δικαιώματος υποβολής αιτήματος στον υπεύθυνο επεξεργασίας για πρόσβαση και διόρθωση ή διαγραφή των δεδομένων προσωπικού χαρακτήρα ή περιορισμό της επεξεργασίας που αφορά το υποκείμενο των δεδομένων και δικαιώματος αντίταξης στην επεξεργασία, καθώς και δικαιώματος στη φορητότητα των δεδομένων,

θ) όταν η επεξεργασία βασίζεται στην συγκατάθεση, την ύπαρξη του δικαιώματος να ανακαλέσει τη συγκατάθεσή του οποτεδήποτε, χωρίς να θιγεί η νομιμότητα της επεξεργασίας που βασίστηκε στη συγκατάθεση πριν από την ανάκλησή της,

ι) το δικαίωμα υποβολής καταγγελίας στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα,

ια) την πηγή από την οποία προέρχονται τα δεδομένα προσωπικού χαρακτήρα και, ανάλογα με την περίπτωση, εάν τα δεδομένα προήλθαν από πηγές στις οποίες έχει πρόσβαση το κοινό,

ιβ) την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ, που προβλέπεται στο άρθρο 22 παράγραφοι 1 και 4 και, τουλάχιστον στις περιπτώσεις αυτές, σημαντικές πληροφορίες σχετικά με τη λογική που ακολουθείται, καθώς και τη σημασία και τις προβλεπόμενες συνέπειες της εν λόγω επεξεργασίας για το υποκείμενο των δεδομένων.

4.4. Η ΕΕΑ υποχρεούται να διαθέσει όλες τις πληροφορίες που προβλέπονται από τα παρακάτω δικαιώματα στο υποκείμενο των δεδομένων εντός μηνός από την παραλαβή του αιτήματος. Η προθεσμία μπορεί να παραταθεί κατά δύο ακόμη μήνες, εφόσον απαιτείται λαμβανομένων υπόψη της πολυπλοκότητας του αιτήματος και του αριθμού των αιτημάτων. Η ΕΕΑ ενημερώνει το υποκείμενο των δεδομένων για την παράταση εντός μηνός από την παραλαβή του αιτήματος, καθώς και για τους λόγους της καθυστέρησης. Εάν το υποκείμενο των δεδομένων υποβάλει το αίτημα με ηλεκτρονικά μέσα, η ενημέρωση παρέχεται με ηλεκτρονικά μέσα.

5. Δικαίωμα πρόσβασης

5.1. Το υποκείμενο των δεδομένων έχει το δικαίωμα να λαμβάνει από τον υπεύθυνο επεξεργασίας επιβεβαίωση για το κατά πόσον ή όχι τα δεδομένα προσωπικού χαρακτήρα που το αφορούν φέρονται επεξεργασία και, εάν συμβαίνει τούτο, το δικαίωμα πρόσβασης στα δεδομένα προσωπικού χαρακτήρα και στις ακόλουθες πληροφορίες:

α) Τους σκοπούς της επεξεργασίας,

β) τις σχετικές κατηγορίες δεδομένων προσωπικού χαρακτήρα,

γ) τους αποδέκτες ή τις κατηγορίες αποδεκτών στους οποίους κοινολογήθηκαν ή πρόκειται να κοινολογηθούν τα δεδομένα προσωπικού χαρακτήρα, ιδίως τους αποδέκτες σε τρίτες χώρες ή διεθνείς οργανισμούς,

δ) εάν είναι δυνατόν, το χρονικό διάστημα για το οποίο θα αποθηκευτούν τα δεδομένα προσωπικού χαρακτήρα ή, όταν αυτό είναι αδύνατο, τα κριτήρια που καθορίζουν το εν λόγω διάστημα,

ε) την ύπαρξη δικαιώματος υποβολής αιτήματος στον υπεύθυνο επεξεργασίας για διόρθωση ή διαγραφή δεδομένων προσωπικού χαρακτήρα ή περιορισμό της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα που αφορά το υποκείμενο των δεδομένων ή δικαιώματος αντίταξης στην εν λόγω επεξεργασία,

στ) το δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή,

ζ) όταν τα δεδομένα προσωπικού χαρακτήρα δεν συλλέγονται από το υποκείμενο των δεδομένων, κάθε διαθέσιμη πληροφορία σχετικά με την προέλευσή τους,

η) την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ, που προβλέπεται στο άρθρο 22 παράγραφοι 1 και 4 Γ.Κ.Π.Δ. και, τουλάχιστον στις περιπτώσεις αυτές, σημαντικές πληροφορίες σχετικά με τη λογική που ακολουθείται, καθώς και τη σημασία και τις

προβλεπόμενες συνέπειες της εν λόγω επεξεργασίας για το υποκείμενο των δεδομένων.

5.2. Όταν δεδομένα προσωπικού χαρακτήρα διαβιβάζονται σε τρίτη χώρα ή σε διεθνή οργανισμό, το υποκείμενο των δεδομένων έχει το δικαίωμα να ενημερώνεται για τις κατάλληλες εγγυήσεις σύμφωνα με το άρθρο 46 σχετικά με τη διαβίβαση.

5.3. Ο υπεύθυνος επεξεργασίας παρέχει αντίγραφο των δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία. Για επιπλέον αντίγραφα που ενδέχεται να ζητηθούν από το υποκείμενο των δεδομένων, ο υπεύθυνος επεξεργασίας μπορεί να επιβάλει την καταβολή εύλογου τέλους για διοικητικά έξοδα. Εάν το υποκείμενο των δεδομένων υποβάλλει το αίτημα με ηλεκτρονικά μέσα και εκτός εάν το υποκείμενο των δεδομένων ζητήσει κάτι διαφορετικό, η ενημέρωση παρέχεται σε ηλεκτρονική μορφή που χρησιμοποιείται συνήθως.

5.4. Το δικαίωμα να λαμβάνεται αντίγραφο που αναφέρεται στην παράγραφο 5.3 δεν επηρεάζει δυσμενώς τα δικαιώματα και τις ελευθερίες άλλων.

6. Δικαίωμα διόρθωσης

Το υποκείμενο των δεδομένων έχει το δικαίωμα να απαιτήσει από τον υπεύθυνο επεξεργασίας χωρίς αδικαιολόγητη καθυστέρηση τη διόρθωση ανακριβών δεδομένων προσωπικού χαρακτήρα που αφορούν. Έχοντας υπόψη τους σκοπούς της επεξεργασίας, το υποκείμενο των δεδομένων έχει το δικαίωμα να απαιτήσει τη συμπλήρωση ελλιπών δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων μέσω συμπληρωματικής δήλωσης.

7. Δικαίωμα διαγραφής (“δικαίωμα στη λήθη”)

7.1. Το υποκείμενο των δεδομένων έχει το δικαίωμα να ζητήσει από τον υπεύθυνο επεξεργασίας τη διαγραφή δεδομένων προσωπικού χαρακτήρα που το αφορούν χωρίς αδικαιολόγητη καθυστέρηση και ο υπεύθυνος επεξεργασίας υποχρεούται να διαγράψει δεδομένα προσωπικού χαρακτήρα χωρίς αδικαιολόγητη καθυστέρηση, εάν ισχύει ένας από τους ακόλουθους λόγους:

α) Τα δεδομένα προσωπικού χαρακτήρα δεν είναι πλέον απαραίτητα σε σχέση με τους σκοπούς για τους οποίους συλλέχθηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία,

β) το υποκείμενο των δεδομένων ανακαλεί τη συγκατάθεση επί της οποίας βασίζεται η επεξεργασία και δεν υπάρχει άλλη νομική βάση για την επεξεργασία,

γ) το υποκείμενο των δεδομένων αντιτίθεται στην επεξεργασία σύμφωνα με το άρθρο 21 παράγραφος 1 Γ.Κ.Π.Δ. (επεξεργασία για σκοπούς ενάσκησης καθήκοντος που αφορά το δημόσιο συμφέρον ή ενάσκηση δημόσιας εξουσίας) και δεν υπάρχουν επιτακτικοί και νόμιμοι λόγοι για τη νεπεξεργασία ή το υποκείμενο των δεδομένων αντιτίθεται στην επεξεργασία σύμφωνα με το άρθρο 21 παράγραφος 2 Γ.Κ.Π.Δ. (απευθείας εμπορική προώθηση προϊόντων ή υπηρεσιών),

δ) τα δεδομένα προσωπικού χαρακτήρα υποβλήθηκαν σε επεξεργασία παράνομα,

ε) τα δεδομένα προσωπικού χαρακτήρα πρέπει να διαγραφούν, ώστε να τηρηθεί νομική υποχρέωση βάσει του ενωσιακού δικαίου ή του δικαίου κράτους μέλους, στην οποία υπόκειται ο υπεύθυνος επεξεργασίας,

στ) τα δεδομένα προσωπικού χαρακτήρα έχουν συλλεχθεί σε σχέση με την προσφορά υπηρεσιών της κοινωνίας των πληροφοριών με συγκατάθεση από παιδί.

7.2. Όταν ο υπεύθυνος επεξεργασίας έχει δημοσιοποιήσει τα δεδομένα προσωπικού χαρακτήρα και υποχρεούται σύμφωνα με την παράγραφο 1 να διαγράψει τα δεδομένα προσωπικού χαρακτήρα, ο υπεύθυνος επεξεργασίας, λαμβάνοντας υπόψη τη διαθέσιμη τεχνολογία και το κόστος εφαρμογής, λαμβάνει εύλογα μέτρα, συμπεριλαμβανομένων των τεχνικών μέτρων, για να ενημερώσει τους υπευθύνους επεξεργασίας που επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα, ότι το υποκείμενο

των δεδομένων ζήτησε τη διαγραφή από αυτούς τους υπευθύνους επεξεργασίας τυχόν συνδέσμων με τα δεδομένα αυτά ή αντιγράφων ή αναπαραγωγών των εν λόγω δεδομένων προσωπικού χαρακτήρα.

7.3. Οι παράγραφοι 1 και 2 δεν εφαρμόζονται στον βαθμό που η επεξεργασία είναι απαραίτητη:

- α) Για την άσκηση του δικαιώματος ελευθερίας της έκφρασης και του δικαιώματος στην ενημέρωση,
- β) για την τήρηση νομικής υποχρέωσης που επιβάλλει την επεξεργασία βάσει του δικαίου της Ένωσης ή του δικαίου κράτους μέλους στο οποίο υπάγεται ο υπεύθυνος επεξεργασίας ή για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο της επεξεργασίας,
- γ) για λόγους δημόσιου συμφέροντος στον τομέα της δημόσιας υγείας σύμφωνα με το άρθρο 9 παράγραφος 2 στοιχεία η) και θ), καθώς και το άρθρο 9 παράγραφος 3 Γ.Κ.Π.Δ.,
- δ) για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς σύμφωνα με το άρθρο 89 παράγραφος 1, εφόσον το δικαίωμα που αναφέρεται στην παράγραφο 1 είναι πιθανόν να καταστήσει αδύνατη ή να εμποδίσει σε μεγάλο βαθμό την επίτευξη σκοπών της εν λόγω επεξεργασίας, ή
- ε) για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων.

8. Δικαίωμα περιορισμού της επεξεργασίας

8.1. Το υποκείμενο των δεδομένων δικαιούται να εξασφαλίζει από τον υπεύθυνο επεξεργασίας τον περιορισμό της επεξεργασίας, όταν ισχύει ένα από τα ακόλουθα:

- α) Η ακρίβεια των δεδομένων προσωπικού χαρακτήρα αμφισβητείται από το υποκείμενο των δεδομένων, για χρονικό διάστημα που επιτρέπει στον υπεύθυνο επεξεργασίας να επαληθεύσει την ακρίβεια των δεδομένων προσωπικού χαρακτήρα,
- β) η επεξεργασία είναι παράνομη και το υποκείμενο των δεδομένων αντιτάσσεται στη διαγραφή των δεδομένων προσωπικού χαρακτήρα και ζητεί, αντ' αυτής, τον περιορισμό της χρήσης τους,
- γ) ο υπεύθυνος επεξεργασίας δεν χρειάζεται πλέον τα δεδομένα προσωπικού χαρακτήρα για τους σκοπούς της επεξεργασίας, αλλά τα δεδομένα αυτά απαιτούνται από το υποκείμενο των δεδομένων για τη θεμελίωση, την άσκηση ή την υποστήριξη νομικών αξιώσεων,
- δ) το υποκείμενο των δεδομένων έχει αντιρρήσεις για την επεξεργασία σύμφωνα με το άρθρο 21 παράγραφος 1 Γ.Κ.Π.Δ., εν αναμονή της επαλήθευσης του κατά πόσον οι νόμιμοι λόγοι του υπευθύνου επεξεργασίας υπερισχύουν έναντι των λόγων του υποκειμένου των δεδομένων.

8.2. Όταν η επεξεργασία έχει περιοριστεί σύμφωνα με την παράγραφο 8.1, τα εν λόγω δεδομένα προσωπικού χαρακτήρα, εκτός της αποθήκευσης, υφίστανται επεξεργασία μόνο με τη συγκατάθεση του υποκειμένου των δεδομένων ή για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων ή για την προστασία των δικαιωμάτων άλλου φυσικού ή νομικού προσώπου ή για λόγους σημαντικού δημόσιου συμφέροντος της Ένωσης ή κράτους μέλους.

8.3. Το υποκείμενο των δεδομένων το οποίο έχει εξασφαλίσει τον περιορισμό της επεξεργασίας σύμφωνα με την παράγραφο 8.1 ενημερώνεται από τον υπεύθυνο επεξεργασίας πριν από την άρση του περιορισμού επεξεργασίας.

9. Δικαίωμα στην φορητότητα των δεδομένων

9.1. Το υποκείμενο των δεδομένων έχει το δικαίωμα να λαμβάνει τα δεδομένα προσωπικού χαρακτήρα που το αφορούν, και τα οποία έχει παράσχει σε υπεύθυνο επεξεργασίας, σε δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα μορφότυπο, καθώς και το δικαίωμα να διαβιβάζει τα

εν λόγω δεδομένα σε άλλον υπεύθυνο επεξεργασίας χωρίς αντίρρηση από τον υπεύθυνο επεξεργασίας στον οποίο παρασχέθηκαν τα δεδομένα προσωπικού χαρακτήρα, όταν:

α) η επεξεργασία βασίζεται σε συγκατάθεση σύμφωνα με το άρθρο 6 παράγραφος 1 στοιχείο α) ή το άρθρο 9 παράγραφος 2 στοιχείο α) ή σε σύμβαση σύμφωνα με το άρθρο 6 παράγραφος 1 στοιχείο β) Γ.Κ.Π.Δ. και

β) η επεξεργασία διενεργείται με αυτοματοποιημένα μέσα.

9.2. Κατά την άσκηση του δικαιώματος στη φορητότητα των δεδομένων σύμφωνα με την παράγραφο 9.1, το υποκείμενο των δεδομένων έχει το δικαίωμα να ζητά την απευθείας διαβίβαση των δεδομένων προσωπικού χαρακτήρα από έναν υπεύθυνο επεξεργασίας σε άλλον, σε περίπτωση που αυτό είναι τεχνικά εφικτό.

9.3. Το δικαίωμα που αναφέρεται στην παράγραφο 9.1 του παρόντος άρθρου ασκείται με την επιφύλαξη του άρθρου 17 Γ.Κ.Π.Δ. (δικαίωμα διαγραφής). Το εν λόγω δικαίωμα δεν ισχύει για την επεξεργασία που είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας.

9.4. Το δικαίωμα που αναφέρεται στην παράγραφο 9.1 δεν επηρεάζει δυσμενώς τα δικαιώματα και τις ελευθερίες άλλων.

10. Δικαίωμα εναντίωσης

10.1. Το υποκείμενο των δεδομένων δικαιούται να αντιτάσσεται, ανά πάσα στιγμή και για λόγους που σχετίζονται με την ιδιαίτερη κατάστασή του, στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που το αφορούν, η οποία βασίζεται στο άρθρο 6 παράγραφος 1 στοιχείο ε) Γ.Κ.Π.Δ., περιλαμβανομένης της κατάρτισης προφίλ βάσει των εν λόγω διατάξεων. Ο υπεύθυνος επεξεργασίας δεν υποβάλλει πλέον τα δεδομένα προσωπικού χαρακτήρα σε επεξεργασία, εκτός εάν ο υπεύθυνος επεξεργασίας καταδείξει επιτακτικούς και νόμιμους λόγους για την επεξεργασία οι οποίοι υπερিশχύουν των συμφερόντων, των δικαιωμάτων και των ελευθεριών του υποκειμένου των δεδομένων ή για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων.

10.2. Εάν δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία για σκοπούς απευθείας εμπορικής προώθησης, το υποκείμενο των δεδομένων δικαιούται να αντιταχθεί ανά πάσα στιγμή στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν για την εν λόγω εμπορική προώθηση, περιλαμβανομένης της κατάρτισης προφίλ, εάν σχετίζεται με αυτήν την απευθείας εμπορική προώθηση.

10.3. Όταν τα υποκείμενα των δεδομένων αντιτίθενται στην επεξεργασία για σκοπούς απευθείας εμπορικής προώθησης, τα δεδομένα προσωπικού χαρακτήρα δεν υποβάλλονται πλέον σε επεξεργασία για τους σκοπούς αυτούς.

10.4. Το αργότερο κατά την πρώτη επικοινωνία με το υποκείμενο των δεδομένων, το δικαίωμα που αναφέρεται στις παραγράφους 10.1 και 10.2 επισημαίνεται ρητώς στο υποκείμενο των δεδομένων και περιγράφεται με σαφήνεια και χωριστά από οποιαδήποτε άλλη πληροφορία.

10.5. Στο πλαίσιο της χρήσης υπηρεσιών της κοινωνίας των πληροφοριών και με την επιφύλαξη της οδηγίας 2002/58/ΕΚ, το υποκείμενο των δεδομένων μπορεί να ασκεί το δικαίωμά του να αντιταχθεί με αυτοματοποιημένα μέσα τα οποία χρησιμοποιούν τεχνικές προδιαγραφές.

10.6. Όταν δεδομένα προσωπικού χαρακτήρα υφίστανται επεξεργασία για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς κατά το άρθρο 89 παράγραφος 1, το υποκείμενο των δεδομένων δικαιούται να αντιταχθεί, για λόγους που σχετίζονται με την ιδιαίτερη κατάστασή του, στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν, εκτός εάν η επεξεργασία είναι απαραίτητη για την εκτέλεση καθήκοντος που ασκείται για λόγους δημόσιου συμφέροντος.

11. Αυτοματοποιημένη λήψη απόφασης

11.1. Το υποκείμενο των δεδομένων έχει το δικαίωμα να μην υπόκειται σε απόφαση που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας, συμπεριλαμβανομένης της κατάρτισης προφίλ, η οποία παράγει έννομα αποτελέσματα που το αφορούν ή το επηρεάζει σημαντικά με παρόμοιο τρόπο.

11.2. Η παράγραφος 11.1 δεν εφαρμόζεται όταν η απόφαση:

- α) Είναι αναγκαία για τη σύναψη ή την εκτέλεση σύμβασης μεταξύ του υποκειμένου των δεδομένων και του υπευθύνου επεξεργασίας των δεδομένων,
- β) επιτρέπεται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους στο οποίο υπόκειται ο υπεύθυνος επεξεργασίας και το οποίο προβλέπει επίσης κατάλληλα μέτρα για την προστασία των δικαιωμάτων, των ελευθεριών και των έννομων συμφερόντων του υποκειμένου των δεδομένων ή
- γ) βασίζεται στη ρητή συγκατάθεση του υποκειμένου των δεδομένων.

11.3. Στις περιπτώσεις που αναφέρονται στην παράγραφο 11.2 στοιχεία α) και γ), ο υπεύθυνος επεξεργασίας των δεδομένων εφαρμόζει κατάλληλα μέτρα για την προστασία των δικαιωμάτων, των ελευθεριών και των έννομων συμφερόντων του υποκειμένου των δεδομένων, τουλάχιστον του δικαιώματος εξασφάλισης ανθρώπινης παρέμβασης από την πλευρά του υπευθύνου επεξεργασίας, έκφρασης άποψης και αμφισβήτησης της απόφασης.

11.4. Οι αποφάσεις που αναφέρονται στην παράγραφο 11.2 δεν βασίζονται στις ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα που αναφέρονται στο άρθρο 9 παράγραφος 1, εκτός αν ισχύει το άρθρο 9 παράγραφος 2 στοιχείο α) ή ζ) και αν υφίστανται κατάλληλα μέτρα για την προστασία των δικαιωμάτων, των ελευθεριών και των έννομων συμφερόντων του υποκειμένου των δεδομένων.

12. Αρχεία των δραστηριοτήτων της επεξεργασίας

12.1. Η ΕΕΑ Πειραιώς τηρεί “Αρχείο των δραστηριοτήτων της επεξεργασίας”. Σε αυτό καταγράφεται κάθε ιδιαίτερη περίπτωση επεξεργασίας δεδομένων, υπό τους όρους του άρθρου 30του Γ.Κ.Π.Δ. Το “Αρχείο των δραστηριοτήτων της επεξεργασίας” τηρείται στην Διεύθυνση Πληροφορικής.

12.2. Όταν μία υπηρεσία της ΕΕΑ προτίθεται να εκκινήσει την διενέργεια μιας νέας επεξεργασίας δεδομένων προσωπικού χαρακτήρα, με οποιαδήποτε νομική βάση, υποχρεούται να φροντίζει για την σχετική επικαιροποίηση του “Αρχείου των δραστηριοτήτων της επεξεργασίας”. Συγκεκριμένα, υποχρεούται να υποβάλλει έγγραφο με τα εξής στοιχεία:

- α) Την επωνυμία και τα στοιχεία επικοινωνίας της υπηρεσίας και, κατά περίπτωση, του από κοινού υπευθύνου επεξεργασίας, του εκπροσώπου του υπευθύνου επεξεργασίας και του υπευθύνου προστασίας δεδομένων,
- β) τους σκοπούς της επεξεργασίας,
- γ) περιγραφή των κατηγοριών υποκειμένων των δεδομένων και των κατηγοριών δεδομένων προσωπικού χαρακτήρα,

δ) τις κατηγορίες αποδεκτών στους οποίους πρόκειται να γνωστοποιηθούν ή γνωστοποιήθηκαν τα δεδομένα προσωπικού χαρακτήρα, περιλαμβανομένων των αποδεκτών σε τρίτες χώρες ή διεθνείς οργανισμούς,

ε) όπου συντρέχει περίπτωση, τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα σε τρίτη χώρα ή διεθνή οργανισμό, συμπεριλαμβανομένων του προσδιορισμού της εν λόγω τρίτης χώρας ή του διεθνούς οργανισμού και, σε περίπτωση διαβιβάσεων που αναφέρονται στο άρθρο 49 παράγραφος 1 δεύτερο εδάφιο, της τεκμηρίωσης των κατάλληλων εγγυήσεων,

στ) όπου είναι δυνατό, τις προβλεπόμενες προθεσμίες διαγραφής των διάφορων κατηγοριών δεδομένων,

ζ) όπου είναι δυνατό, γενική περιγραφή των τεχνικών και οργανωτικών μέτρων ασφάλειας που αναφέρονται στο άρθρο 32 παράγραφος 1 του Γ.Κ.Π.Δ.

13. Γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

13.1. Ως “παραβίαση δεδομένων προσωπικού χαρακτήρα”, νοείται η παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία (άρθρο 4 αρ. 12 του Γ.Κ.Π.Δ.). Σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα, ο υπεύθυνος επεξεργασίας γνωστοποιεί αμελλητί και, αν είναι δυνατό, εντός 72 ωρών από τη στιγμή που αποκτά γνώση του γεγονότος την παραβίαση των δεδομένων προσωπικού χαρακτήρα στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, εκτός εάν η παραβίαση δεδομένων προσωπικού χαρακτήρα δεν ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Όταν η γνωστοποίηση στην Αρχή δεν πραγματοποιείται εντός 72 ωρών, συνοδεύεται από αιτιολόγηση για την καθυστέρηση. Κάθε πρόσωπο που απασχολείται στην ΕΕΑ, εφόσον διαπιστώσει τέτοια παραβίαση οφείλει αμελλητί να την γνωστοποιήσει στην Διεύθυνση Πληροφορικής. Η Διεύθυνση Πληροφορικής είναι αρμόδια για την γνωστοποίηση της παραβίασης στην Αρχή.

13.2. Ο εκτελών την επεξεργασία ενημερώνει τον υπεύθυνο επεξεργασίας αμελλητί, μόλις αντιληφθεί παραβίαση δεδομένων προσωπικού χαρακτήρα.

Η γνωστοποίηση που αναφέρεται στην παράγραφο 13.1 κατ' ελάχιστο:

α) Περιγράφει τη φύση της παραβίασης δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων, όπου είναι δυνατό, των κατηγοριών και του κατά προσέγγιση αριθμού των επηρεαζόμενων υποκειμένων των δεδομένων, καθώς και των κατηγοριών και του κατά προσέγγιση αριθμού των επηρεαζόμενων αρχείων δεδομένων προσωπικού χαρακτήρα,

β) ανακοινώνει το όνομα και τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων ή άλλου σημείου επικοινωνίας από το οποίο μπορούν να ληφθούν περισσότερες πληροφορίες,

γ) περιγράφει τις ενδεχόμενες συνέπειες της παραβίασης των δεδομένων προσωπικού χαρακτήρα,

δ) περιγράφει τα ληφθέντα ή τα προτεινόμενα προς λήψη μέτρα από τον υπεύθυνο επεξεργασίας για την αντιμετώπιση της παραβίασης των δεδομένων προσωπικού χαρακτήρα, καθώς και, όπου ενδείκνυται, μέτρα για την άμβλυνση ενδεχόμενων δυσμενών συνεπειών της.

13.3. Σε περίπτωση που και εφόσον δεν είναι δυνατόν να παρασχεθούν οι πληροφορίες ταυτόχρονα, μπορούν να παρέχονται σταδιακά χωρίς αδικαιολόγητη καθυστέρηση.

13.4. Ο υπεύθυνος επεξεργασίας τεκμηριώνει κάθε παραβίαση δεδομένων προσωπικού χαρακτήρα, που συνίστανται στα πραγματικά περιστατικά που αφορούν την παραβίαση δεδομένων προσωπικού χαρακτήρα, τις συνέπειες και τα ληφθέντα διορθωτικά μέτρα. Η εν λόγω τεκμηρίωση επιτρέπει στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα να επαληθεύει τη συμμόρφωση προς το παρόν άρθρο.

13.5. Το άρθρο αυτό εφαρμόζεται με λήψη υπόψη των “Κατευθυντήριων γραμμών σχετικά με τη

γνωστοποίηση παραβιάσεων δεδομένων προσωπικού χαρακτήρα δυνάμει του Κανονισμού 2016/679” της Ομάδας Εργασίας του Άρθρου 29 για την Προστασία των Δεδομένων (εκδόθηκε 3.10.2017, αναθεωρήθηκε και εκδόθηκε τις 6.2.2018.

14. Ανακοίνωση παραβίασης δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων

14.1. Όταν η παραβίαση δεδομένων προσωπικού χαρακτήρα ενδέχεται να θέσει σε υψηλό κίνδυνο δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας ανακοινώνει αμελλητί την παραβίαση των δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων.

14.2. Στην ανακοίνωση στο υποκείμενο των δεδομένων η οποία αναφέρεται στην παράγραφο 14.1 του παρόντος άρθρου περιγράφεται με σαφήνεια η φύση της παραβίασης των δεδομένων προσωπικού χαρακτήρα και περιέχονται τουλάχιστον οι πληροφορίες και τα μέτρα που αναφέρονται στο άρθρο 13 παράγραφος 3 στοιχεία β), γ) και δ).

14.3. Η ανακοίνωση στο υποκείμενο των δεδομένων η οποία αναφέρεται στην παράγραφο 14.1 δεν απαιτείται, εάν πληρείται οποιαδήποτε από τις ακόλουθες προϋποθέσεις:

α) Ο υπεύθυνος επεξεργασίας εφάρμοσε κατάλληλα τεχνικά και οργανωτικά μέτρα προστασίας, και τα μέτρα αυτά εφαρμόστηκαν στα επηρεαζόμενα από την παραβίαση δεδομένα προσωπικού χαρακτήρα, κυρίως μέτρα που καθιστούν μη κατανοητά τα δεδομένα προσωπικού χαρακτήρα σε όσους δεν διαθέτουν άδεια πρόσβασης σε αυτά, όπως η κρυπτογράφηση,

β) ο υπεύθυνος επεξεργασίας έλαβε στη συνέχεια μέτρα που διασφαλίζουν ότι δεν είναι πλέον πιθανό να προκύψει ο αναφερόμενος στην παράγραφο 1 υψηλός κίνδυνος για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων,

γ) προϋποθέτει δυσανάλογες προσπάθειες. Στην περίπτωση αυτή, γίνεται αντ' αυτής δημόσια ανακοίνωση ή υπάρχει παρόμοιο μέτρο με το οποίο τα υποκείμενα των δεδομένων ενημερώνονται με εξίσου αποτελεσματικό τρόπο.

14.4. Εάν ο υπεύθυνος επεξεργασίας δεν έχει ήδη ανακοινώσει την παραβίαση των δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων, η εποπτική αρχή μπορεί, έχοντας εξετάσει την πιθανότητα επέλευσης υψηλού κινδύνου από την παραβίαση των δεδομένων προσωπικού χαρακτήρα, να του ζητήσει να το πράξει ή μπορεί να αποφασίσει ότι πληρούται οποιαδήποτε από τις προϋποθέσεις που αναφέρονται στην παράγραφο 3.

14.5. Το άρθρο αυτό εφαρμόζεται με λήψη υπόψη των “Κατευθυντήριων γραμμών σχετικά με τη γνωστοποίηση παραβιάσεων δεδομένων προσωπικού χαρακτήρα δυνάμει του Κανονισμού 2016/679” της Ομάδας Εργασίας του Άρθρου 29 για την Προστασία των Δεδομένων (εκδόθηκε 3.10.2017, αναθεωρήθηκε και εκδόθηκε τις 6.2.2018.

15. Εκτίμηση αντικτύπου

15.1. Όταν πρόκειται να εφαρμοστεί για πρώτη φορά ένα είδος επεξεργασίας δεδομένων προσωπικού χαρακτήρα, ιδίως με χρήση νέων τεχνολογιών (π.χ. λογισμικό, λειτουργία καμερών) και συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, η υπηρεσία ενημερώνει την Μηχανογράφηση. Η ΕΕΑ διενεργεί, πριν από την επεξεργασία, εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα. Σε μία εκτίμηση μπορεί να εξετάζεται ένα σύνολο παρόμοιων πράξεων επεξεργασίας οι οποίες ενέχουν παρόμοιους υψηλούς κινδύνους.

15.2. Η ΕΕΑ ζητεί τη γνώμη του Υπευθύνου Προστασίας Δεδομένων, κατά τη διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων.

15.3. Η αναφερόμενη στην παράγραφο 1 εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων απαιτείται ιδίως στην περίπτωση:

α) Συστηματικής και εκτενούς αξιολόγησης προσωπικών πτυχών σχετικά με φυσικά πρόσωπα, η οποία βασίζεται σε αυτοματοποιημένη επεξεργασία, περιλαμβανομένης της κατάρτισης προφίλ, και στην οποία βασίζονται αποφάσεις που παράγουν έννομα αποτελέσματα σχετικά με το φυσικό πρόσωπο ή ομοίως επηρεάζουν σημαντικά το φυσικό πρόσωπο,

β) μεγάλης κλίμακας επεξεργασίας των ειδικών κατηγοριών δεδομένων που αναφέρονται στο άρθρο 9 παράγραφος 1 Γ.Κ.Π.Δ. ή δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα που αναφέρονται στο άρθρο 10 Γ.Κ.Π.Δ. ή

γ) συστηματικής παρακολούθησης δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα.

15.4. Η εκτίμηση περιέχει τουλάχιστον:

α) Συστηματική περιγραφή των προβλεπόμενων πράξεων επεξεργασίας και των σκοπών της επεξεργασίας, περιλαμβανομένου, κατά περίπτωση, του έννομου συμφέροντος που επιδιώκει ο υπεύθυνος επεξεργασίας,

β) εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας σε συνάρτηση με τους σκοπούς,

γ) εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων που αναφέρονται στην παράγραφο 1 και

δ) τα προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων, περιλαμβανομένων των εγγυήσεων, των μέτρων και μηχανισμών ασφάλειας, ώστε να διασφαλίζεται η προστασία των δεδομένων προσωπικού χαρακτήρα και να αποδεικνύεται η συμμόρφωση προς τον παρόντα κανονισμό, λαμβάνοντας υπόψη τα δικαιώματα και τα έννομα συμφέροντα των υποκειμένων των δεδομένων και άλλων ενδιαφερόμενων προσώπων.

15.5. Η ΕΕΑ ζητεί τη γνώμη της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα πριν από την επεξεργασία, όταν η δύναμη του παρόντος άρθρου και του άρθρου 35 Γ.Κ.Π.Δ. εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων υποδεικνύει ότι η επεξεργασία θα προκαλούσε υψηλό κίνδυνο ελλείψει μέτρων μετριασμού του κινδύνου από τον υπεύθυνο επεξεργασίας.

16. Ασφάλεια των δεδομένων

16.1. Λαμβάνοντας υπόψη τις τελευταίες εξελίξεις, το κόστος εφαρμογής και τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, η ΕΕΑ εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων, περιλαμβανομένων, μεταξύ άλλων, κατά περίπτωση:

α) Της ψευδωνυμοποίησης και της κρυπτογράφησης δεδομένων προσωπικού χαρακτήρα,

β) της δυνατότητας διασφάλισης του απορρήτου, της ακεραιότητας, της διαθεσιμότητας και της αξιοπιστίας των συστημάτων και των υπηρεσιών επεξεργασίας σε συνεχή βάση,

γ) της δυνατότητας αποκατάστασης της διαθεσιμότητας και της πρόσβασης σε δεδομένα προσωπικού χαρακτήρα σε εύθετο χρόνο σε περίπτωση φυσικού ή τεχνικού συμβάντος,

δ) διαδικασίας για την τακτική δοκιμή, εκτίμηση και αξιολόγηση της αποτελεσματικότητας των τεχνικών και των οργανωτικών μέτρων για τη διασφάλιση της ασφάλειας της επεξεργασίας.

16.2. Κατά την εκτίμηση του ενδεδειγμένου επιπέδου ασφάλειας λαμβάνονται ιδίως υπόψη οι κίνδυνοι που απορρέουν από την επεξεργασία, ιδίως από τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, άνευ αδείας κοινολόγηση ή προσπέλαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν,

αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία.

16.3. Η ΕΕΑ λαμβάβει μέτρα ώστε να διασφαλίζεται ότι κάθε φυσικό πρόσωπο που ενεργεί υπό την εποπτεία του το οποίο έχει πρόσβαση σε δεδομένα προσωπικού χαρακτήρα τα επεξεργάζεται μόνο κατ' εντολή του υπευθύνου επεξεργασίας, εκτός εάν υποχρεούται προς τούτο από το δίκαιο της Ένωσης ή του κράτους μέλους. Ειδικότερα, τα εν λόγω μέτρα διασφαλίζουν ότι, εξ ορισμού, τα δεδομένα προσωπικού χαρακτήρα δεν καθίστανται προσβάσιμα χωρίς την παρέμβαση του φυσικού προσώπου σε αόριστο αριθμό φυσικών προσώπων.