Κατευθυντήριες γραμμές 3/2019 σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα μέσω βιντεοσυσκευών

Έκδοση 2.0

Εκδόθηκε στις 29 Ιανουαρίου 2020

Ιστορικό έκδοσης

Έκδοση 2.0	29 Ιανουαρίου 2020	Έκδοση κατευθυντήριων γραμμών μετά από δημόσια διαβούλευση
Έκδοση 1.0	10 Ιουλίου 2019	Έκδοση κατευθυντήριων γραμμών για δημόσια διαβούλευση

Πίνακας περιεχομένων

Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων

Έχοντας υπόψη το άρθρο 70 παράγραφος 1 στοιχείο ε) του κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (εφεξής «ΓΚΠΔ»),

Έχοντας υπόψη τη Συμφωνία για τον Ευρωπαϊκό Οικονομικό Χώρο και ιδίως το παράρτημα XI και το πρωτόκολλο 37, όπως τροποποιήθηκαν με την απόφαση της Μεικτής Επιτροπής του ΕΟΧ αριθ. 154/2018 της 6ης Ιουλίου 2018[1],

Έχοντας υπόψη το άρθρο 12 και το άρθρο 22 του εσωτερικού κανονισμού του,

ΕΞΕΔΩΣΕ ΤΙΣ ΑΚΟΛΟΥΘΕΣ ΚΑΤΕΥΘΥΝΤΗΡΙΕΣ ΓΡΑΜΜΕΣ

1 ΕΙΣΑΓΩΓΗ

1. Η εντατική χρήση βιντεοσυσκευών έχει αντίκτυπο στη συμπεριφορά των πολιτών. Η εκτεταμένη εφαρμογή αυτών των εργαλείων σε πολλές πτυχές της ανθρώπινης δραστηριότητας θα επιβαρύνει τον άνθρωπο στην προσπάθειά του να αποφευχθεί ο εντοπισμός συμπεριφοράς του η οποία θα μπορούσε να εκληφθεί ως παρατυπία. Στην πράξη, οι τεχνολογίες αυτές μπορούν να περιορίσουν τη δυνατότητα των ανθρώπων να διατηρούν την ανωνυμία τους όταν μετακινούνται και χρησιμοποιούν υπηρεσίες, και γενικότερα τη δυνατότητά τους να περνούν απαρατήρητοι. Οι επιπτώσεις για την προστασία των δεδομένων είναι τεράστιες.

2. Μολονότι οι άνθρωποι μπορεί να νιώθουν άνετα με τη βιντεοεπιτήρηση που υπηρετεί συγκεκριμένο σκοπό ασφαλείας, πρέπει ωστόσο να παρέχονται εγγυήσεις που θα διασφαλίζουν ότι η βιντεοεπιτήρηση δεν θα χρησιμοποιείται με αθέμιτο τρόπο για σκοπούς εντελώς διαφορετικούς ή μη αναμενόμενους για το υποκείμενο των δεδομένων (π.χ. για σκοπούς εμπορικής προώθησης, παρακολούθησης της απόδοσης εργαζομένων κ.λπ.). Επιπλέον, πολλά εργαλεία χρησιμοποιούνται πλέον για την εκμετάλλευση των εικόνων που καταγράφονται από τις κάμερες και για τη μετατροπή των παραδοσιακών καμερών σε έξυπνες κάμερες. Ο όγκος των δεδομένων που παράγονται μέσω της βιντεοσκόπησης, σε συνδυασμό με τα εν λόγω εργαλεία και τις τεχνικές, αυξάνουν τον κίνδυνο δευτερογενούς χρήσης των δεδομένων (είτε η χρήση αυτή συνδέεται με τον συγκεκριμένο σκοπό για τον οποίο δημιουργήθηκε το σύστημα είτε όχι), ή ακόμα και τον κίνδυνο αθέμιτης χρήσης των εν λόγω δεδομένων. Οι γενικές αρχές του ΓΚΠΔ (άρθρο 5) θα πρέπει πάντα να λαμβάνονται προσεκτικά υπόψη όταν διενεργείται βιντεοεπιτήρηση.

[1] Οι αναφορές στα «κράτη μέλη» στην παρούσα γνώμη θα πρέπει να νοούνται ως αναφορές στα «κράτη μέλη του ΕΟΧ».

3. Τα συστήματα βιντεοεπιτήρησης αλλάζουν σε πολλά επίπεδα τον τρόπο με τον οποίο επαγγελματίες του ιδιωτικού και του δημόσιου τομέα αλληλεπιδρούν σε ιδιωτικούς ή δημόσιους χώρους για σκοπούς ενίσχυσης της ασφάλειας, της λήψης δεδομένων ανάλυσης κοινού, της προβολής εξατομικευμένων διαφημίσεων κ.λπ. Η βιντεοεπιτήρηση έχει γίνει ιδιαίτερα αποτελεσματική χάρη στην αυξανόμενη χρήση της «έξυπνης» ανάλυσης του βιντεοσκοπημένου υλικού. Ορισμένες από αυτές τις τεχνικές είναι περισσότερο παρεμβατικές (π.χ. σύνθετες βιομετρικές τεχνολογίες) και άλλες λιγότερο παρεμβατικές (π.χ. απλοί υπολογιστικοί αλγόριθμοι). Γενικά, τα άτομα δυσκολεύονται ολοένα και περισσότερο να διατηρούν την ανωνυμία τους και να προστατεύουν την ιδιωτική τους ζωή. Τα ζητήματα προστασίας των δεδομένων που εγείρονται σε κάθε κατάσταση συχνά διαφέρουν· το ίδιο ισχύει και για την ανάλυση των νομικών ζητημάτων που ανακύπτουν όταν χρησιμοποιείται η μία ή η άλλη τεχνολογία.

4. Πέρα από τα ζητήματα ιδιωτικότητας, υπάρχουν και κίνδυνοι που σχετίζονται με την πιθανή δυσλειτουργία αυτών των συσκευών και την μεροληψία που είναι δυνατό να επιφέρουν. Οι ερευνητές αναφέρουν ότι το λογισμικό που χρησιμοποιείται για την ταυτοποίηση, την αναγνώριση ή την ανάλυση προσώπων «συμπεριφέρεται» διαφορετικά, ανάλογα με την ηλικία, το φύλο και την εθνότητα του προσώπου που ταυτοποιείται. Δεδομένου ότι οι αλγόριθμοι λειτουργούν βασισμένοι σε διαφορετικά δημογραφικά στοιχεία, η μεροληψία στην αναγνώριση προσώπου απειλεί να ενισχύσει τις προκαταλήψεις της κοινωνίας. Ως εκ τούτου, οι υπεύθυνοι επεξεργασίας πρέπει επίσης να διασφαλίζουν ότι η επεξεργασία βιομετρικών δεδομένων που παράγονται από βιντεοεπιτήρηση είναι αντικείμενο τακτικής αξιολόγησης για τη συνάφεια και επάρκειά της όσον αφορά τις εγγυήσεις που παρέχονται.

5. Η βιντεοεπιτήρηση δεν είναι εξ ορισμού αναγκαία εφόσον υπάρχουν άλλα μέσα για την επίτευξη του υποκείμενου σκοπού. Στην αντίθετη περίπτωση, υπάρχει ο κίνδυνος να μεταβληθούν οι πολιτισμικοί κανόνες και επομένως να εδραιωθεί ως γενική αρχή η έλλειψη της ιδιωτικότητας.

6. Οι παρούσες κατευθυντήριες γραμμές έχουν σκοπό να προσφέρουν καθοδήγηση για το πώς πρέπει να εφαρμόζεται ο ΓΚΠΔ σε σχέση με την επεξεργασία δεδομένων προσωπικού χαρακτήρα μέσω βιντεοσυσκευών. Τα παραδείγματα δεν είναι εξαντλητικά και η συλλογιστική που αναπτύσσεται στα περισσότερα από αυτά μπορεί να εφαρμοστεί σε όλους τους πιθανούς τομείς χρήσης.

2 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ[2]

2.1 Δεδομένα προσωπικού χαρακτήρα

7. Η συστηματική αυτοματοποιημένη παρακολούθηση συγκεκριμένου χώρου με οπτικά ή οπτικοακουστικά μέσα, κυρίως για τον σκοπό της προστασίας της περιουσίας ή για την προστασία της ζωής και της υγείας του ατόμου, αποτελεί σημαντικό φαινόμενο στις μέρες μας. Στο πλαίσιο αυτής της δραστηριότητας, συλλέγονται και διατηρούνται οπτικές ή οπτικοακουστικές πληροφορίες για όλα τα πρόσωπα που εισέρχονται στον παρακολουθούμενο χώρο, τα οποία μπορούν να ταυτοποιηθούν με βάση την εμφάνισή τους ή άλλα ειδικά στοιχεία. Η ταυτότητα αυτών των προσώπων μπορεί να εξακριβωθεί με βάση αυτά τα επιμέρους στοιχεία. Η συστηματική αυτοματοποιημένη παρακολούθηση επιτρέπει επίσης την περαιτέρω επεξεργασία των δεδομένων προσωπικού χαρακτήρα με βάση την παρουσία και τη συμπεριφορά των προσώπων στον εκάστοτε χώρο. Ο πιθανός κίνδυνος αθέμιτης χρήσης αυτών των δεδομένων αυξάνεται ως προς τις διαστάσεις του υπό παρακολούθηση χώρου και ως προς τον αριθμό των ατόμων που επισκέπτονται τον χώρο. Το γεγονός αυτό αποτυπώνεται στο άρθρο 35 παράγραφος 3 στοιχείο γ) του Γενικού Κανονισμού για την Προστασία των Δεδομένων, το οποίο προβλέπει τη διενέργεια εκτίμησης αντικτύπου για την προστασία δεδομένων στην περίπτωση συστηματικής παρακολούθησης δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα, καθώς και στο άρθρο 37 παράγραφος 1 στοιχείο β), το οποίο προβλέπει ότι οι υπεύθυνοι επεξεργασίας ορίζουν υπεύθυνο προστασίας δεδομένων αν η πράξη επεξεργασίας, λόγω της φύσης της, απαιτεί τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων.

8. Ωστόσο, ο κανονισμός δεν εφαρμόζεται στην επεξεργασία δεδομένων που δεν συνδέονται με συγκεκριμένο πρόσωπο, π.χ. όταν είναι αδύνατο να εξακριβωθεί άμεσα ή έμμεσα η ταυτότητα του προσώπου.

> Παράδειγμα: Ο ΓΚΠΔ δεν εφαρμόζεται στις εικονικές κάμερες (δηλαδή στις κάμερες που δεν λειτουργούν ως κάμερες και, ως εκ τούτου, δεν επεξεργάζονται δεδομένα προσωπικού χαρακτήρα). *Ωστόσο, σε ορισμένα κράτη μέλη η περίπτωση αυτή μπορεί να υπόκειται σε άλλη νομοθεσία.*
>
> Παράδειγμα: Η καταγραφή δεδομένων από μεγάλο ύψος εμπίπτει στο πεδίο εφαρμογής του ΓΚΠΔ μόνον αν, υπό τις συγκεκριμένες περιστάσεις, τα υπό επεξεργασία δεδομένα μπορούν να συσχετιστούν με συγκεκριμένο πρόσωπο.
>
> Παράδειγμα: Μια κάμερα είναι ενσωματωμένη σε αυτοκίνητο για να βοηθά τον οδηγό να σταθμεύσει. Αν η συσκευή έχει κατασκευαστεί ή τοποθετηθεί κατά τρόπο ώστε να μην συλλέγει πληροφορίες που συνδέονται με φυσικά πρόσωπα (όπως οι πινακίδες κυκλοφορίας ή πληροφορίες βάσει των οποίων θα μπορούσαν να ταυτοποιηθούν οι διερχόμενοι) ο ΓΚΠΔ δεν εφαρμόζεται.

9.

[2] Το ΕΣΠΔ σημειώνει ότι, εφόσον το επιτρέπει ο ΓΚΠΔ, ενδέχεται να ισχύουν ειδικές απαιτήσεις στην εθνική νομοθεσία.

2.2 Εφαρμογή της οδηγίας για την επιβολή του νόμου (ΕΕ) 2016/680

10. Ιδιαίτερα, η επεξεργασία δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, της διερεύνησης, της ανίχνευσης ή της δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων, συμπεριλαμβανομένης της προστασίας και πρόληψης έναντι κινδύνων που απειλούν τη δημόσια ασφάλεια, εμπίπτει στο πεδίο εφαρμογής της οδηγίας (ΕΕ) 2016/680.

2.3 Εξαίρεση της οικιακής δραστηριότητας

11. Σύμφωνα με το άρθρο 2 παράγραφος 2 στοιχείο γ), η επεξεργασία δεδομένων προσωπικού χαρακτήρα από φυσικό πρόσωπο στο πλαίσιο αποκλειστικά προσωπικής ή οικιακής δραστηριότητας, που μπορεί να περιλαμβάνει και επιγραμμική δραστηριότητα, δεν εμπίπτει στο πεδίο εφαρμογής του ΓΚΠΔ[3].

12. Αυτή η διάταξη –γνωστή και ως εξαίρεση της οικιακής δραστηριότητας– στο πλαίσιο της βιντεοεπιτήρησης πρέπει να ερμηνεύεται με τη στενή της έννοια. Ως εκ τούτου, όπως αποφάνθηκε το Ευρωπαϊκό Δικαστήριο, η αποκαλούμενη «εξαίρεση της οικιακής δραστηριότητας» πρέπει «*να ερμηνευθεί ως αφορώσα αποκλειστικά τις δραστηριότητες οι οποίες εντάσσονται στο πλαίσιο της ιδιωτικής ή οικογενειακής ζωής των ιδιωτών, πράγμα το οποίο προδήλως δεν ισχύει για την περίπτωση της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, η οποία συνίσταται στη δημοσίευσή τους στο Διαδίκτυο με συνέπεια να αποκτά πρόσβαση στα δεδομένα αυτά απροσδιόριστος αριθμός προσώπων*»[4]. Επιπροσθέτως, ένα σύστημα βιντεοεπιτήρησης, στον βαθμό που αυτό περιλαμβάνει τη διαρκή καταγραφή και αποθήκευση δεδομένων προσωπικού χαρακτήρα και εκτείνεται «*έστω και εν μέρει, στον δημόσιο χώρο και, ως εκ τούτου, εξέρχεται από την ιδιωτική σφαίρα αυτού που προβαίνει στην επεξεργασία των δεδομένων με το μέσο αυτό, δεν μπορεί να θεωρηθεί ως αποκλειστικώς "προσωπική ή οικιακή" δραστηριότητα κατά την έννοια του άρθρου 3, παράγραφος 2, δεύτερη περίπτωση, της οδηγίας 95/46*»[5].

13. Όσον αφορά στις βιντεοσυσκευές που λειτουργούν εντός ιδιωτικών εγκαταστάσεων, η χρήση τους μπορεί να εμπίπτει στην εξαίρεση της οικιακής δραστηριότητας. Θα πρέπει ωστόσο να συνυπολογίζονται πολλοί παράγοντες για να εξαχθεί σχετικό συμπέρασμα. Πέρα από τα προαναφερόμενα στοιχεία που καταγράφηκαν σε αποφάσεις του ΕΔ, ο χρήστης του συστήματος βιντεοεπιτήρησης στην ιδιωτική κατοικία πρέπει να εξετάζει κατά πόσον έχει οποιουδήποτε είδους προσωπική σχέση με το υποκείμενο των δεδομένων, κατά πόσον η κλίμακα ή η συχνότητα της επιτήρησης υποδηλώνει οποιουδήποτε είδους επαγγελματική δραστηριότητα από την πλευρά του καθώς και τον δυνητικό αρνητικό αντίκτυπο της επιτήρησης στα υποκείμενα των δεδομένων. Η παρουσία οποιουδήποτε από τα προαναφερόμενα στοιχεία δεν υποδηλώνει απαραιτήτως ότι η επεξεργασία δεν εμπίπτει στην εξαίρεση της οικιακής δραστηριότητας, καθώς πρέπει να διενεργηθεί σφαιρική αξιολόγηση για να προσδιοριστεί αν ισχύει εξαίρεση.

---

[3] Βλ. επίσης αιτιολογική σκέψη 18.

[4] Ευρωπαϊκό Δικαστήριο, απόφαση στην υπόθεση C-101/01, *υπόθεση Bodil Lindqvist*, 6 Νοεμβρίου 2003, σκέψη 47.

[5] Ευρωπαϊκό Δικαστήριο, απόφαση στην υπόθεση C-212/13, *František Ryneš v Úřad pro ochranu osobních údajů*, 11 Δεκεμβρίου 2014, σκέψη 33.

Παράδειγμα: Τουρίστας βιντεοσκοπεί τις διακοπές του τόσο μέσω του κινητού του τηλεφώνου όσο και μέσω βιντεοκάμερας. Δείχνει το οπτικοακουστικό υλικό σε φίλους και συγγενείς αλλά δεν το καθιστά προσβάσιμο σε απεριόριστο αριθμό προσώπων. Η ενέργεια αυτή εμπίπτει στην εξαίρεση της οικιακής δραστηριότητας.

Παράδειγμα: Ποδηλάτης βουνού θέλει να καταγράψει την κατάβασή της με κάμερα δράσης. Βρίσκεται σε απομακρυσμένη περιοχή και σκοπεύει να χρησιμοποιήσει το βιντεοσκοπημένο υλικό μόνο για προσωπική της ψυχαγωγία στο σπίτι. Και αυτή η περίπτωση εμπίπτει στην εξαίρεση της οικιακής δραστηριότητας, έστω και αν σε ορισμένο βαθμό υφίσταται επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Παράδειγμα: Κάποιος παρακολουθεί και καταγράφει με κάμερα τον κήπο του. Ο ιδιωτικός χώρος είναι περιφραγμένος και μόνον ο χειριστής και η οικογένειά του εισέρχονται στον κήπο σε τακτική βάση. Η περίπτωση αυτή εμπίπτει στην εξαίρεση της οικιακής δραστηριότητας εφόσον η βιντεοεπιτήρηση δεν εκτείνεται, ούτε εν μέρει, σε δημόσιο χώρο ή σε γειτονική ιδιοκτησία.

14.

3 ΝΟΜΙΜΟΤΗΤΑ ΤΗΣ ΕΠΕΞΕΡΓΑΣΙΑΣ

15. Πριν από τη χρήση του υλικού, οι σκοποί της επεξεργασίας πρέπει να διευκρινίζονται λεπτομερώς (άρθρο 5 παράγραφος 1 στοιχείο β)). Η βιντεοεπιτήρηση μπορεί να υπηρετεί πολλούς σκοπούς. Μεταξύ άλλων, μπορεί να συμβάλλει στην προστασία της ιδιοκτησίας και άλλων περιουσιακών στοιχείων, στην προστασία της ζωής και της σωματικής ακεραιότητας των ατόμων, στη συλλογή αποδεικτικών στοιχείων για αγωγές αστικού χαρακτήρα[6]. Οι εν λόγω σκοποί παρακολούθησης θα πρέπει να τεκμηριώνονται εγγράφως (άρθρο 5 παράγραφος 2) και πρέπει να διευκρινίζονται για κάθε κάμερα επιτήρησης που χρησιμοποιείται. Εφόσον διαφορετικές κάμερες χρησιμοποιούνται για τον ίδιο σκοπό από έναν και μόνο υπεύθυνο επεξεργασίας, μπορεί να παρέχεται κοινή τεκμηρίωση. Επιπλέον, τα υποκείμενα των δεδομένων πρέπει να ενημερώνονται για τους σκοπούς της επεξεργασίας σύμφωνα με το άρθρο 13 (*βλέπε Ενότητα 7, Υποχρεώσεις διαφάνειας και πληροφόρησης*). Η βιντεοεπιτήρηση που αποσκοπεί αποκλειστικά και μόνο στην «ασφάλεια» ή «για την ασφάλειά σας» δεν είναι επαρκώς συγκεκριμένη (άρθρο 5 παράγραφος 1 στοιχείο β)). Αντιβαίνει επίσης στην αρχή σύμφωνα με την οποία τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία με νομιμότητα, αντικειμενικότητα και διαφάνεια σε σχέση με το υποκείμενο των δεδομένων (βλέπε άρθρο 5 παράγραφος 1 στοιχείο α)).

16. Καταρχήν, κάθε νομική βάση που εμπίπτει στο άρθρο 6 παράγραφος 1 μπορεί να αποτελέσει τη νομική βάση για την επεξεργασία δεδομένων βιντεοεπιτήρησης. Για παράδειγμα, το άρθρο 6 παράγραφος 1 στοιχείο γ) εφαρμόζεται εφόσον το εθνικό δίκαιο προβλέπει την υποχρέωση της διενέργειας βιντεοεπιτήρησης[7]. Ωστόσο, στην πράξη, οι διατάξεις που είναι περισσότερο πιθανόν να χρησιμοποιηθούν είναι

- Άρθρο 6 παράγραφος 1 στοιχείο στ) (έννομο συμφέρον).
- Άρθρο 6 παράγραφος 1 στοιχείο ε) (επεξεργασία απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας).

Σε μάλλον εξαιρετικές περιστάσεις, το άρθρο 6 παράγραφος 1 στοιχείο α) (συγκατάθεση) μπορεί να χρησιμοποιηθεί ως νομική βάση από τον υπεύθυνο επεξεργασίας.

3.1 Έννομο συμφέρον, άρθρο 6 παράγραφος 1 στοιχείο στ)

17. Η νομική αξιολόγηση του άρθρου 6 παράγραφος 1 στοιχείο στ) θα πρέπει να βασίζεται στα ακόλουθα κριτήρια σύμφωνα με την αιτιολογική σκέψη 47.

3.1.1 Ύπαρξη έννομων συμφερόντων

18. Η βιντεοεπιτήρηση είναι νόμιμη εάν είναι απαραίτητη για την επίτευξη του σκοπού του έννομου συμφέροντος 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 (άρθρο 6 παράγραφος 1 στοιχείο στ)). Τα έννομα συμφέροντα που επιδιώκει ο υπεύθυνος

[6] Οι κανόνες που διέπουν τη συλλογή αποδεικτικών στοιχείων για αγωγές αστικού χαρακτήρα ποικίλλουν στα κράτη μέλη.

[7] Στις παρούσες κατευθυντήριες γραμμές δεν αναλύονται ούτε εξετάζονται λεπτομέρειες της εθνικής νομοθεσίας που μπορεί να διαφέρουν μεταξύ κρατών μελών.

επεξεργασίας ή τρίτος μπορούν να είναι νομικά[8], οικονομικά ή μη υλικά συμφέροντα[9]. Ωστόσο, ο υπεύθυνος επεξεργασίας θα πρέπει να έχει υπόψη ότι εάν το υποκείμενο των δεδομένων εναντιώνεται στην επιτήρηση σύμφωνα με το άρθρο 21, ο υπεύθυνος επεξεργασίας μπορεί να προβεί στη βιντεοεπιτήρηση του εν λόγω υποκειμένου των δεδομένων μόνο εάν υπάρχει *επιτακτικό* έννομο συμφέρον που υπερισχύει των συμφερόντων, δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων ή για την κατοχύρωση, άσκηση ή υπεράσπιση νομικών αξιώσεων.

19. Εφόσον συντρέχει πραγματική και επικίνδυνη κατάσταση, ο σκοπός της προστασίας της περιουσίας από ληστεία, κλοπή ή βανδαλισμό μπορεί να συνιστά έννομο συμφέρον για τους σκοπούς της βιντεοεπιτήρησης.

20. Το έννομο συμφέρον πρέπει να υφίσταται πραγματικά και να αφορά παρόν ζήτημα (δηλαδή το συμφέρον δεν πρέπει να είναι πλασματικό ή υποθετικό)[10]. Πρέπει να υφίσταται πραγματική κατάσταση κινδύνου –όπως ζημιές ή σοβαρά συμβάντα στο παρελθόν– πριν από την έναρξη της επιτήρησης. Με βάση την αρχή της λογοδοσίας, οι υπεύθυνοι επεξεργασίας είναι χρήσιμο να καταγράφουν συναφή συμβάντα (ημερομηνία, τρόπος, οικονομική ζημία) και σχετικές ποινικές διώξεις. Αυτά τα καταγεγραμμένα συμβάντα μπορούν να αποτελέσουν ισχυρό τεκμήριο για την ύπαρξη έννομου συμφέροντος. Η ύπαρξη έννομου συμφέροντος, καθώς και η αναγκαιότητα της παρακολούθησης θα πρέπει να επαναξιολογούνται σε τακτικά χρονικά διαστήματα (π.χ. μία φορά ετησίως, ανάλογα με τις περιστάσεις).

> Παράδειγμα: Καταστηματάρχης σκοπεύει να ανοίξει νέο κατάστημα και επιθυμεί να εγκαταστήσει σύστημα βιντεοεπιτήρησης για την αποτροπή βανδαλισμών. Με τη βοήθεια στατιστικών στοιχείων μπορεί να αποδείξει ότι είναι πολύ πιθανό να σημειωθούν βανδαλισμοί στη γύρω περιοχή. Χρήσιμη είναι επίσης η εμπειρία γειτονικών καταστημάτων. Δεν είναι απαραίτητο να έχει υποστεί ζημιές ο εν λόγω υπεύθυνος επεξεργασίας. Αν οι καταστροφές στη γειτονιά υποδηλώνουν την ύπαρξη κινδύνου ή παρόμοιας απειλής, μπορούν παράλληλα να τεκμηριώσουν και την ύπαρξη έννομου συμφέροντος. Ωστόσο, η παρουσίαση εθνικών ή γενικών στατιστικών στοιχείων για την εγκληματική δραστηριότητα δεν αποτελεί επαρκές τεκμήριο αν δεν αναλυθούν παράλληλα η εν λόγω περιοχή ή οι κίνδυνοι για το συγκεκριμένο κατάστημα.

21.

22. Έννομο συμφέρον μπορούν επίσης να συνιστούν καταστάσεις επικείμενου κινδύνου οι οποίες εντοπίζονται σε τράπεζες ή καταστήματα που πωλούν πολύτιμα αγαθά (π.χ. κοσμηματοπωλεία) ή σε χώρους στους οποίους είναι γνωστό ότι διαπράττονται συχνά αδικήματα εναντίον περιουσίας (π.χ. βενζινάδικα).

23. Ο ΓΚΠΔ ορίζει επίσης σαφώς ότι οι δημόσιες αρχές δεν επιτρέπεται να επεξεργάζονται δεδομένα κατά την άσκηση των καθηκόντων τους στη βάση του έννομου συμφέροντος (άρθρο 6 παράγραφος 1 δεύτερη πρόταση).

---

[8] Ευρωπαϊκό Δικαστήριο, απόφαση στην υπόθεση C-13/16, *Rīgas satiksme case*, 4 Μαΐου 2017

[9] Βλέπε έγγραφο WP217, Ομάδα εργασίας του άρθρου 29.

[10] Βλέπε έγγραφο WP217, Ομάδα εργασίας του άρθρου 29, σ. 24 και επ. Βλέπε επίσης υπόθεση ΕΔ C-708/18, σ. 44

3.1.2 Αναγκαιότητα της επεξεργασίας

24. Τα δεδομένα προσωπικού χαρακτήρα θα πρέπει να είναι κατάλληλα, συναφή και να περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία («ελαχιστοποίηση των δεδομένων»), βλέπε άρθρο 5 παράγραφος 1 στοιχείο γ). Πριν από την εγκατάσταση συστήματος βιντεοεπιτήρησης, ο υπεύθυνος επεξεργασίας θα πρέπει πάντα να εξετάζει ενδελεχώς αν αυτό το μέτρο είναι, κατά πρώτον, κατάλληλο για την επίτευξη του επιθυμητού στόχου και, κατά δεύτερον, επαρκές και αναγκαίο για την επίτευξη των σκοπών του. Μέτρα βιντεοεπιτήρησης θα πρέπει να επιλέγονται μόνον εάν ο σκοπός της επεξεργασίας δεν θα μπορούσε εύλογα να εκπληρωθεί με άλλα μέσα, τα οποία θίγουν σε μικρότερο βαθμό τα θεμελιώδη δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων.

25. Αν υποτεθεί ότι ο υπεύθυνος επεξεργασίας επιθυμεί να αποτρέψει εγκλήματα εναντίον της ιδιοκτησίας του, αντί να εγκαταστήσει σύστημα βιντεοεπιτήρησης, μπορεί να λάβει εναλλακτικά μέτρα ασφάλειας, όπως π.χ. να περιφράξει την ιδιοκτησία του, να αναθέσει σε προσωπικό ασφαλείας την τακτική περιπολία του χώρου, να προσλάβει φύλακες, να βελτιώσει τον φωτισμό, να τοποθετήσει κλειδαριές ασφαλείας, απαραβίαστα παράθυρα και πόρτες ή να καλύψει τις επιφάνειες με επιστρώσεις ή μεμβράνες προστασίας από γκράφιτι. Αυτά τα μέτρα μπορούν να είναι εξίσου αποτελεσματικά με τα συστήματα βιντεοεπιτήρησης για την αποτροπή περιστατικών ληστείας, κλοπής και βανδαλισμού. Ο υπεύθυνος επεξεργασίας πρέπει να αξιολογεί κατά περίπτωση κατά πόσον αυτά τα μέτρα μπορούν να αποτελέσουν εύλογη λύση.

26. Πριν από τη λειτουργία του συστήματος βιντεοεπιτήρησης, ο υπεύθυνος επεξεργασίας είναι υποχρεωμένος να αξιολογεί πότε και πού τα μέτρα βιντεοεπιτήρησης είναι απολύτως αναγκαία. Συνήθως, ένα σύστημα βιντεοεπιτήρησης που λειτουργεί τη νύχτα, καθώς και εκτός του συνηθισμένου ωραρίου λειτουργίας, καλύπτει την ανάγκη του υπευθύνου επεξεργασίας να αποτρέψει οποιονδήποτε κίνδυνο απειλεί την ιδιοκτησία του.

27. Κατά κανόνα, η ανάγκη της βιντεοεπιτήρησης για την προστασία των εγκαταστάσεων του υπευθύνου επεξεργασίας τελειώνει στα όρια της ιδιοκτησίας.[11] Υπάρχουν ωστόσο και περιπτώσεις κατά τις οποίες η βιντεοεπιτήρηση της ιδιοκτησίας δεν αρκεί για την αποτελεσματική προστασία της ιδιοκτησίας. Σε ορισμένες μεμονωμένες περιπτώσεις, ενδέχεται να είναι αναγκαίο να επεκταθεί η βιντεοεπιτήρηση στις περιοχές που γειτνιάζουν με τις εγκαταστάσεις. Σε αυτήν την περίπτωση, ο υπεύθυνος επεξεργασίας θα πρέπει να χρησιμοποιεί φυσικά και τεχνικά μέσα, αφαιρώντας π.χ. από το βιντεοσκοπημένο υλικό τις μη συναφείς με τον σκοπό της επιτήρησης περιοχές ή παρουσιάζοντας τις εν λόγω περιοχές με εικονοψηφίδες.

> Παράδειγμα: Βιβλιοπώλης επιθυμεί να προστατεύσει το κατάστημά του από βανδαλισμό. Γενικά, οι κάμερες πρέπει να καταγράφουν μόνο το βιβλιοπωλείο καθώς, για τον σκοπό για τον οποίο χρησιμοποιούνται οι κάμερες, δεν είναι αναγκαίο να επιτηρούνται οι γειτονικές εγκαταστάσεις ή οι περιβάλλοντες δημόσιοι χώροι.

28.

29. Ερωτήματα που αφορούν την αναγκαιότητα της επεξεργασίας εγείρονται άλλωστε και για τον τρόπο με τον οποίο διατηρούνται τα στοιχεία. Σε ορισμένες περιπτώσεις ενδέχεται να είναι αναγκαίο να χρησιμοποιούνται λύσεις που προσομοιάζουν στο «μαύρο κουτί»: το οπτικοακουστικό υλικό διαγράφεται αυτομάτως αφού παρέλθει συγκεκριμένη περίοδος αποθήκευσης, και είναι προσβάσιμο μόνο σε περίπτωση συμβάντος. Σε άλλες περιπτώσεις, ενδέχεται να μην είναι αναγκαίο

[11] Η περίπτωση αυτή μπορεί επίσης να υπόκειται στην εθνική νομοθεσία σε ορισμένα κράτη μέλη.

να διατηρηθεί καθόλου το βιντεοσκοπημένο υλικό καθώς κρίνεται προσφορότερο να χρησιμοποιηθούν μέσα παρακολούθησης σε πραγματικό χρόνο. Η επιλογή μεταξύ των λύσεων του «μαύρου κουτιού» και της παρακολούθησης σε πραγματικό χρόνο πρέπει επίσης να βασίζεται στον επιδιωκόμενο σκοπό. Αν, για παράδειγμα, ο σκοπός της βιντεοεπιτήρησης είναι η διατήρηση αποδεικτικών στοιχείων, οι μέθοδοι επιτήρησης σε πραγματικό χρόνο δεν κρίνονται συνήθως κατάλληλες. Επίσης, σε ορισμένες περιπτώσεις η παρακολούθηση σε πραγματικό χρόνο μπορεί να είναι περισσότερο παρεμβατική από την αποθήκευση και την αυτόματη διαγραφή υλικού μετά την παρέλευση ορισμένου χρόνου (π.χ. όταν κάποιος παρακολουθεί συνεχώς την οθόνη μπορεί να παρεμβαίνει περισσότερο στην ιδιωτική ζωή των ατόμων από ό,τι αν δεν υπάρχει καθόλου οθόνη και το υλικό αποθηκεύεται απευθείας στο μαύρο κουτί). Σε αυτήν την περίπτωση πρέπει να λαμβάνεται υπόψη η αρχή της ελαχιστοποίησης των δεδομένων (άρθρο 5 παράγραφος 1 στοιχείο γ)). Θα πρέπει επίσης να ληφθεί υπόψη ότι ο υπεύθυνος επεξεργασίας, αντί για τη βιντεοεπιτήρηση έχει ενίοτε τη δυνατότητα να χρησιμοποιεί προσωπικό ασφαλείας, το οποίο μπορεί να αντιδράσει και να παρέμβει αμέσως.

3.1.3 Στάθμιση συμφερόντων

30. Αν υποτεθεί ότι η βιντεοεπιτήρηση είναι αναγκαία για την προστασία των έννομων συμφερόντων του υπευθύνου επεξεργασίας, το σύστημα βιντεοεπιτήρησης μπορεί να τεθεί σε λειτουργία μόνον εάν έναντι των έννομων συμφερόντων του υπευθύνου επεξεργασίας ή τρίτου (π.χ. προστασία ιδιωτικής περιουσίας ή σωματικής ακεραιότητας) δεν υπερισχύουν τα συμφέροντα ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων. Ο υπεύθυνος επεξεργασίας πρέπει να εξετάσει 1) κατά πόσον η παρακολούθηση θίγει τα συμφέροντα, τα θεμελιώδη δικαιώματα και τις ελευθερίες των ατόμων και 2) εάν η παρακολούθηση παραβιάζει ή έχει αρνητικές συνέπειες στα δικαιώματα του υποκειμένου των δεδομένων. Πράγματι, η στάθμιση των συμφερόντων είναι υποχρεωτική. Τα θεμελιώδη δικαιώματα και οι ελευθερίες, αφενός, και τα έννομα συμφέροντα του υπευθύνου επεξεργασίας, αφετέρου, πρέπει να αξιολογούνται και να σταθμίζονται με προσοχή.

> Παράδειγμα: Ιδιωτική εταιρεία στάθμευσης αντιμετωπίζει προβλήματα καθώς διαπράττονται συνεχώς κλοπές στα σταθμευμένα αυτοκίνητα. Ο χώρος στάθμευσης είναι ανοιχτός και εύκολα προσβάσιμος από οποιονδήποτε, αλλά εμφανώς σηματοδοτείται περιμετρικά με πινακίδες και οδοφράγματα. Η εταιρεία στάθμευσης έχει έννομο συμφέρον (αποτροπή κλοπών στα αυτοκίνητα των πελατών) να παρακολουθεί την περιοχή την ώρα της ημέρας που αντιμετωπίζει προβλήματα. Τα υποκείμενα των δεδομένων παρακολουθούνται για περιορισμένο χρόνο, δεν βρίσκονται στην περιοχή για σκοπούς ψυχαγωγίας, και επίσης, η αποτροπή των κλοπών είναι προς το συμφέρον τους. Σε αυτήν την περίπτωση το έννομο συμφέρον του υπευθύνου επεξεργασίας υπερισχύει του συμφέροντος των υποκειμένων των δεδομένων να μην παρακολουθούνται.
>
> Παράδειγμα: Εστιατόριο αποφασίζει να εγκαταστήσει βιντεοκάμερες στις τουαλέτες προκειμένου να ελέγχει την καθαριότητα στις εγκαταστάσεις υγιεινής. Σε αυτήν την περίπτωση τα δικαιώματα των υποκειμένων των δεδομένων υπερισχύουν σαφώς του συμφέροντος του υπευθύνου επεξεργασίας. Επομένως, δεν επιτρέπεται να εγκατασταθούν κάμερες.

31.

3.1.3.1 Λήψη αποφάσεων κατά περίπτωση

32. Καθώς η στάθμιση των συμφερόντων είναι υποχρεωτική σύμφωνα με τον κανονισμό, η απόφαση πρέπει να λαμβάνεται κατά περίπτωση (βλέπε άρθρο 6 παράγραφος 1 στοιχείο στ)). Ο συσχετισμός αφηρημένων καταστάσεων ή η σύγκριση παρεμφερών περιπτώσεων δεν είναι επαρκής. Ο υπεύθυνος

επεξεργασίας πρέπει να αξιολογεί τους κινδύνους παραβίασης των δικαιωμάτων των υποκειμένων των δεδομένων. Ως εκ τούτου, το καθοριστικό κριτήριο είναι η ένταση της παρέμβασης στα δικαιώματα και τις ελευθερίες του ατόμου.

33. Η ένταση εξαρτάται, μεταξύ άλλων, από το είδος των πληροφοριών που συγκεντρώνονται (περιεχόμενο των πληροφοριών), το πεδίο κάλυψης (πυκνότητα πληροφοριών, χωρική και γεωγραφική έκταση), τον αριθμό των ενδιαφερόμενων υποκειμένων των δεδομένων –είτε ως συγκεκριμένος αριθμός είτε ως αναλογία του σχετικού πληθυσμού– την υπό εξέταση κατάσταση, τα πραγματικά συμφέροντα της ομάδας των υποκειμένων των δεδομένων, τα εναλλακτικά μέσα, καθώς και τη φύση και το πεδίο εφαρμογής της αξιολόγησης των δεδομένων.

34. Σημαντικοί παράγοντες στάθμισης μπορεί να είναι το μέγεθος του χώρου που βρίσκεται υπό επιτήρηση και ο αριθμός των υπό επιτήρηση υποκειμένων των δεδομένων. Η χρήση βιντεοεπιτήρησης σε απομακρυσμένη περιοχή (π.χ. για την παρακολούθηση άγριας πανίδας ή για την προστασία ζωτικών υποδομών όπως ιδιωτική ραδιοφωνική κεραία) πρέπει να αξιολογείται με διαφορετικό τρόπο από ό,τι η βιντεοεπιτήρηση σε πεζοδρομημένη περιοχή ή σε εμπορικό κέντρο.

> Παράδειγμα: Αν εγκατασταθεί κάμερα-ταμπλό σε όχημα (π.χ. με σκοπό τη συλλογή στοιχείων σε περίπτωση ατυχήματος), είναι σημαντικό να διασφαλιστεί ότι αυτή η κάμερα δεν καταγράφει συνεχώς ούτε την κυκλοφορία, ούτε και τα παρακείμενα πρόσωπα. Ειδάλλως, η βιντεοσκόπηση και η χρησιμοποίηση του βιντεοσκοπημένου υλικού ως αποδεικτικό στοιχείο στην πλέον θεωρητική περίπτωση τροχαίου ατυχήματος δεν μπορεί να αιτιολογήσει αυτή τη σοβαρή παρέμβαση στα δικαιώματα των υποκειμένων των δεδομένων[11].

35.

3.1.3.2 Εύλογες προσδοκίες των υποκειμένων των δεδομένων

36. Σύμφωνα με την αιτιολογική σκέψη 47, η ύπαρξη έννομου συμφέροντος χρειάζεται προσεκτική αξιολόγηση. Κατά την αξιολόγηση πρέπει να λαμβάνονται υπόψη οι εύλογες προσδοκίες του υποκειμένου των δεδομένων τόσο κατά τη στιγμή όσο και στο πλαίσιο της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα που το αφορούν. Όσον αφορά τη συστηματική παρακολούθηση, η σχέση μεταξύ του υποκειμένου των δεδομένων και του υπευθύνου επεξεργασίας μπορεί να ποικίλλει σημαντικά και να επηρεάζει το είδος των εύλογων προσδοκιών του υποκειμένου των δεδομένων. Η ερμηνεία της έννοιας των εύλογων προσδοκιών δεν θα πρέπει να βασίζεται μόνο στις εν λόγω υποκειμενικές προσδοκίες. Αντιθέτως, το αποφασιστικό κριτήριο πρέπει να είναι εάν ένας αντικειμενικός τρίτος θα μπορούσε λογικά να αναμένει και να συμπεράνει ότι υπόκειται σε παρακολούθηση στην εκάστοτε κατάσταση.

37. Για παράδειγμα, ένας εργαζόμενος στον χώρο εργασίας του στις περισσότερες περιπτώσεις δεν αναμένει να παρακολουθείται από τον εργοδότη του[12]. Επιπλέον, δεν πρέπει να αναμένεται παρακολούθηση σε ιδιωτικό κήπο, σε χώρους διαβίωσης ή σε αίθουσες εξετάσεων και θεραπείας. Στο ίδιο πνεύμα, κανένας δεν θεωρεί εύλογο να παρακολουθείται σε εγκαταστάσεις υγιεινής ή σάουνας – η παρακολούθηση σε αυτούς τους χώρους αποτελεί έντονη προσβολή των δικαιωμάτων του υποκειμένου των δεδομένων. Τα υποκείμενα των δεδομένων θεωρούν εύλογα ότι δεν θα υπάρχει βιντεοεπιτήρηση σε αυτούς τους χώρους. Ωστόσο, ο πελάτης μιας τράπεζας μπορεί να αναμένει ότι θα παρακολουθείται εντός της τράπεζας ή στην αυτόματη ταμειολογιστική μηχανή (ATM).

[12] Βλέπε επίσης: Ομάδα εργασίας του άρθρου 29, γνώμη 2/2017 σχετικά με την επεξεργασία δεδομένων στην εργασία, WP 249, 8 Ιουνίου 2017.

38. Τα υποκείμενα των δεδομένων μπορούν επίσης να αναμένουν ότι δεν θα παρακολουθούνται εντός δημοσίως προσβάσιμων χώρων, πολύ δε περισσότερο αν οι χώροι αυτοί χρησιμοποιούνται κατά κανόνα για ανάρρωση, αποκατάσταση και δραστηριότητες ελεύθερου χρόνου, καθώς και εντός χώρων στους οποίους οι άνθρωποι αναπαύονται και/ή επικοινωνούν, όπως καθιστικοί χώροι, τραπέζια σε εστιατόρια, πάρκα, κινηματογράφοι και γυμναστήρια. Σε αυτήν την περίπτωση, τα συμφέροντα ή τα δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων συχνά υπερισχύουν των έννομων συμφερόντων του υπευθύνου επεξεργασίας.

> Παράδειγμα: Στις τουαλέτες τα υποκείμενα των δεδομένων αναμένουν ότι δεν θα παρακολουθούνται. Η βιντεοεπιτήρηση που χρησιμοποιείται π.χ. για την πρόληψη ατυχημάτων δεν χαρακτηρίζεται από αναλογικότητα.

39.

40. Οι πινακίδες που ενημερώνουν τα υποκείμενα των δεδομένων για τη βιντεοεπιτήρηση δεν πρέπει να λαμβάνονται υπόψη όταν εξετάζεται τι αντικειμενικά πρέπει να αναμένουν τα υποκείμενα των δεδομένων και τι όχι. Με άλλα λόγια, ένας καταστηματάρχης δεν μπορεί να βασιστεί στο ότι οι πελάτες του *αντικειμενικά* έχουν εύλογες προσδοκίες ότι θα παρακολουθούνται επειδή μια πινακίδα στην είσοδο του καταστήματός του ενημερώνει τους πελάτες για την επιτήρηση.

3.2 Ανάγκη εκπλήρωσης καθήκοντος το οποίο εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας (άρθρο 6 παράγραφος 1 στοιχείο ε))

41. Τα δεδομένα προσωπικού χαρακτήρα θα μπορούσαν να υποβληθούν σε επεξεργασία μέσω βιντεοεπιτήρησης σύμφωνα με το άρθρο 6 παράγραφος 1 στοιχείο ε) εάν η επεξεργασία είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας[13]. Κατά την άσκηση δημόσιας εξουσίας ενδέχεται να μην επιτρέπεται τέτοια επεξεργασία. Ωστόσο, άλλες νομικές βάσεις, όπως η «υγεία και ασφάλεια» για την προστασία επισκεπτών και εργαζομένων μπορεί να παρέχουν στον υπεύθυνο επεξεργασίας περιορισμένο πεδίο να επεξεργαστεί δεδομένα, με γνώμονα πάντα τις υποχρεώσεις και τα δικαιώματα των υποκειμένων των δεδομένων σύμφωνα με τον ΓΚΠΔ.

42. Τα κράτη μέλη έχουν το δικαίωμα να διατηρήσουν ή να θεσπίσουν ειδική εθνική νομοθεσία για τη βιντεοεπιτήρηση προκειμένου να προσαρμόσουν την εφαρμογή των κανόνων του ΓΚΠΔ, προσδιορίζοντας με μεγαλύτερη ακρίβεια ειδικές απαιτήσεις για την επεξεργασία εφόσον αυτές είναι σύμφωνες με τις αρχές που προβλέπει ο ΓΚΠΔ (π.χ. περιορισμοί ως προς την αποθήκευση, αναλογικότητα).

3.3 Συγκατάθεση, άρθρο 6 παράγραφος 1 στοιχείο α)

43. Η συγκατάθεση πρέπει να είναι ελεύθερη, συγκεκριμένη, ρητή και να παρέχεται με πλήρη επίγνωση, όπως περιγράφεται στις κατευθυντήριες γραμμές για τη συγκατάθεση[14].

---

[13] Η νομική βάση της εν λόγω επεξεργασίας ορίζεται σύμφωνα με το δίκαιο της Ένωσης ή το δίκαιο του κράτους μέλους και είναι αναγκαία «για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας» (άρθρο 6 παράγραφος 3).

[14] Ομάδα εργασίας του άρθρου 29, Κατευθυντήριες γραμμές σχετικά με τη συγκατάθεση βάσει του κανονισμού 2016/679 (WP 259 αναθ. 01). - εκδόθηκαν από το ΕΣΠΔ

44. Όσον αφορά τη συστηματική παρακολούθηση, η συγκατάθεση του υποκειμένου των δεδομένων μπορεί να αποτελέσει νομική βάση σύμφωνα με το άρθρο 7 (βλέπε αιτιολογική σκέψη 43) μόνο σε εξαιρετικές περιπτώσεις. Η ταυτόχρονη παρακολούθηση άγνωστου αριθμού ανθρώπων αποτελεί εγγενές χαρακτηριστικό της τεχνολογίας της βιντεοεπιτήρησης. Ο υπεύθυνος επεξεργασίας δύσκολα μπορεί να αποδείξει ότι το υποκείμενο των δεδομένων συγκατατέθηκε εκ των προτέρων για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν (άρθρο 7 παράγραφος 1). Αν υποτεθεί ότι το υποκείμενο των δεδομένων ανακαλεί τη συγκατάθεσή του θα είναι δύσκολο ο υπεύθυνος επεξεργασίας να αποδείξει ότι τα δεδομένα προσωπικού χαρακτήρα δεν υποβάλλονται πλέον σε επεξεργασία (άρθρο 7 παράγραφος 3).

> Παράδειγμα: Αθλητές ζητούν να παρακολουθούνται κατά τη διάρκεια ατομικών ασκήσεων ώστε να μελετήσουν τις τεχνικές και την απόδοσή τους. Ωστόσο, αν ένας αθλητικός σύλλογος αναλάβει την πρωτοβουλία να παρακολουθήσει μια ολόκληρη ομάδα για τον ίδιο σκοπό, η συγκατάθεση τις περισσότερες φορές δεν θα είναι έγκυρη, καθώς οι αθλητές μπορεί να αισθάνονται πίεση να δώσουν τη συγκατάθεσή τους, ούτως ώστε η άρνηση συγκατάθεσης να μην επηρεάσει αρνητικά τους συναθλητές τους.

45.

46. Αν ο υπεύθυνος επεξεργασίας επιθυμεί να βασιστεί στη συγκατάθεση, είναι υποχρέωσή του να βεβαιωθεί ότι κάθε υποκείμενο των δεδομένων που εισέρχεται στον επιτηρούμενο χώρο έχει δώσει τη συγκατάθεσή του. Η συγκατάθεση αυτή πρέπει να πληροί τις προϋποθέσεις του άρθρου 7. Η είσοδος σε σηματοδοτημένο παρακολουθούμενο χώρο (π.χ. όταν οι άνθρωποι καλούνται να διασχίσουν ειδικό χώρο υποδοχής ή πύλη για να εισέλθουν σε παρακολουθούμενο χώρο) δεν αποτελεί δήλωση ή σαφή θετική ενέργεια, όπως απαιτείται για τη συγκατάθεση, εκτός εάν αυτή πληροί τα κριτήρια των άρθρων 4 και 7, όπως περιγράφεται στις κατευθυντήριες γραμμές για τη συγκατάθεση[15].

47. Με δεδομένη την ανισορροπία ισχύος μεταξύ εργοδοτών και εργαζομένων, στις περισσότερες περιπτώσεις οι εργοδότες δεν θα πρέπει να βασίζονται στη συγκατάθεση των εργαζομένων όταν επεξεργάζονται δεδομένα προσωπικού χαρακτήρα, καθώς η συγκατάθεση αυτή είναι απίθανο να έχει δοθεί ελεύθερα. Εν προκειμένω θα πρέπει να λαμβάνονται υπόψη οι κατευθυντήριες γραμμές σχετικά με τη συγκατάθεση.

48. Η νομοθεσία των κρατών μελών ή οι συλλογικές συμβάσεις, συμπεριλαμβανομένων των «συμβάσεων έργων/εργασίας», μπορεί να προβλέπουν ειδικούς κανόνες για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα των εργαζομένων στο πλαίσιο της απασχόλησης (βλέπε άρθρο 88).

[15] Ομάδα εργασίας του άρθρου 29, Κατευθυντήριες γραμμές σχετικά με τη συγκατάθεση βάσει του κανονισμού 2016/679 (WP 259) - εκδόθηκαν από το ΕΣΠΔ και θα πρέπει να λαμβάνονται υπόψη.

4 ΚΟΙΝΟΛΟΓΗΣΗ ΒΙΝΤΕΟΣΚΟΠΗΜΕΝΟΥ ΥΛΙΚΟΥ ΣΕ ΤΡΙΤΟΥΣ

49. Καταρχήν, οι γενικοί κανόνες του ΓΚΠΔ εφαρμόζονται στην κοινολόγηση βιντεοσκοπημένου υλικού σε τρίτους.

4.1 Κοινολόγηση βιντεοσκοπημένου υλικού σε τρίτους γενικά

50. Η κοινολόγηση ορίζεται στο άρθρο 4(2) ως διαβίβαση (π.χ. μεμονωμένη κοινοποίηση), διάδοση (π.χ. ηλεκτρονική δημοσίευση) ή κάθε άλλη μορφή διάθεσης. Οι τρίτοι ορίζονται στο άρθρο 4(10). Όταν η κοινολόγηση γίνεται προς τρίτες χώρες ή διεθνείς οργανισμούς εφαρμόζονται επίσης οι ειδικές διατάξεις του άρθρου 44 και επόμενες.

51. Κάθε κοινολόγηση δεδομένων προσωπικού χαρακτήρα αποτελεί ξεχωριστό είδος επεξεργασίας δεδομένων προσωπικού χαρακτήρα για την οποία ο υπεύθυνος επεξεργασίας πρέπει να διαθέτει νομική βάση στο πλαίσιο του άρθρου 6.

> Παράδειγμα: Υπεύθυνος επεξεργασίας που επιθυμεί να αναρτήσει βιντεοσκοπημένο υλικό στο διαδίκτυο πρέπει να βασιστεί σε νομική βάση για αυτή την επεξεργασία και να εξασφαλίσει π.χ. τη συγκατάθεση του υποκειμένου των δεδομένων σύμφωνα με το άρθρο 6 παράγραφος 1 στοιχείο α).

52.

53. Η διαβίβαση βιντεοσκοπημένου υλικού σε τρίτους για σκοπό άλλο από αυτόν για τον οποίο έχουν συλλεγεί τα δεδομένα είναι δυνατή υπό τους κανόνες του άρθρου 6 παράγραφος 4.

> Παράδειγμα: Σε μπάρα (χώρου στάθμευσης) εγκαθίσταται σύστημα βιντεοεπιτήρησης για να εξετάζονται νομικά οι περιπτώσεις επίλυσης ζημιών. Προκαλείται ζημιά και το βιντεοσκοπημένο υλικό διαβιβάζεται σε δικηγόρο για την έναρξη διαδικασίας. Σε αυτήν την περίπτωση, ο σκοπός της βιντεοσκόπησης είναι ο ίδιος με τον σκοπό της διαβίβασης του υλικού.
>
> Παράδειγμα: Σε μπάρα (χώρου στάθμευσης) εγκαθίσταται σύστημα βιντεοεπιτήρησης για να εξετάζονται νομικά οι περιπτώσεις επίλυσης ζημιών. Το βιντεοσκοπημένο υλικό δημοσιεύεται διαδικτυακά για καθαρά ψυχαγωγικούς σκοπούς. Σε αυτήν την περίπτωση ο σκοπός έχει αλλάξει και δεν είναι συμβατός με τον αρχικό σκοπό. Επίσης, είναι δύσκολο να εντοπιστεί νομική βάση για αυτήν την επεξεργασία (δημοσίευση).

54.

55. Ο τρίτος-αποδέκτης θα πρέπει να διενεργήσει δική του νομική ανάλυση, προσδιορίζοντας ιδίως τη νομική βάση σύμφωνα με το άρθρο 6 για την επεξεργασία που πραγματοποιεί (π.χ. παραλαβή του υλικού).

4.2 Κοινολόγηση βιντεοσκοπημένου υλικού σε αρχές επιβολής του νόμου

56. Η κοινολόγηση βιντεοσκοπημένου υλικού σε αρχές επιβολής του νόμου είναι και αυτή ανεξάρτητη διαδικασία, η οποία απαιτεί χωριστή αιτιολόγηση εκ μέρους του υπευθύνου επεξεργασίας.

57. Σύμφωνα με το άρθρο 6 παράγραφος 1 στοιχείο γ), η επεξεργασία είναι σύννομη όταν είναι απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση του υπευθύνου επεξεργασίας. Μολονότι το εφαρμοστέο αστυνομικό δίκαιο υπόκειται στον αποκλειστικό έλεγχο των κρατών μελών, υπάρχουν τις περισσότερες φορές γενικοί κανόνες που ρυθμίζουν σε κάθε κράτος μέλος τη διαβίβαση αποδεικτικών στοιχείων στις αρχές επιβολής του νόμου. Η επεξεργασία εκ μέρους του υπευθύνου επεξεργασίας που παραδίδει τα δεδομένα ρυθμίζεται από τον ΓΚΠΔ. Αν η εθνική νομοθεσία απαιτεί

από τον υπεύθυνο επεξεργασίας να συνεργάζεται με τις αρχές επιβολής του νόμου (π.χ. κατά την έρευνα), η νομική βάση για την παράδοση των δεδομένων είναι η έννομη υποχρέωση σύμφωνα με το άρθρο 6 παράγραφος 1 στοιχείο γ).

58. Ως εκ τούτου, ο περιορισμός του σκοπού στο άρθρο 6 παράγραφος 4 δεν αποτελεί συχνά πρόβλημα, εφόσον η κοινολόγηση αναφέρεται ρητώς στο δίκαιο του κράτους μέλους. Δεν είναι επομένως αναγκαίο να λαμβάνονται υπόψη οι ειδικές απαιτήσεις για την αλλαγή σκοπού υπό την έννοια των στοιχείων α) έως ε).

59. Παράδειγμα: Καταστηματάρχης καταγράφει με βίντεο την είσοδο του καταστήματός του. Στο βιντεοσκοπημένο υλικό διακρίνεται ένα άτομο να κλέβει ένα πορτοφόλι. Η αστυνομία ζητεί από τον υπεύθυνο επεξεργασίας να παραδώσει το υλικό προκειμένου να διευκολυνθεί στην έρευνά της. Σε αυτήν την περίπτωση, ο καταστηματάρχης μπορεί να χρησιμοποιήσει τη νομική βάση του άρθρου 6 παράγραφος 1 στοιχείο γ) (έννομη υποχρέωση) σε συνδυασμό με το σχετικό εθνικό δίκαιο για την επεξεργασία της διαβίβασης.

60. Παράδειγμα: Σε κατάστημα εγκαθίσταται κάμερα για λόγους ασφαλείας. Ο καταστηματάρχης πιστεύει ότι έχει καταγράψει κάτι ύποπτο στο υλικό του και αποφασίζει να στείλει το υλικό στην αστυνομία (χωρίς να έχει καμία ένδειξη ότι βρίσκεται υπό εξέλιξη οποιαδήποτε έρευνα). Σε αυτήν την περίπτωση, ο καταστηματάρχης πρέπει να αξιολογήσει αν πληρούνται, κατά βάση, οι όροι του άρθρου 6 παράγραφος 1 στοιχείο στ). Αυτό ισχύει συνήθως αν ο καταστηματάρχης έχει εύλογες υπόνοιες ότι έχει διαπραχθεί αδίκημα.

61. Η επεξεργασία των δεδομένων προσωπικού χαρακτήρα από τις αρχές επιβολής του νόμου καθαυτές δεν βασίζεται στον ΓΚΠΔ (βλέπε άρθρο 2 παράγραφος 2 στοιχείο δ)), αλλά βασίζεται στην οδηγία σχετικά με την επιβολή του νόμου (ΕΕ) 2016/680.

5 ΕΠΕΞΕΡΓΑΣΙΑ ΕΙΔΙΚΩΝ ΚΑΤΗΓΟΡΙΩΝ ΔΕΔΟΜΕΝΩΝ

62. Τα συστήματα βιντεοεπιτήρησης συλλέγουν συνήθως τεράστιο όγκο προσωπικών δεδομένων τα οποία ενδέχεται να αποκαλύψουν δεδομένα πολύ προσωπικής φύσης, ακόμη και ειδικών κατηγοριών δεδομένα. Ενδέχεται δηλαδή μη σημαντικά δεδομένα, που συλλέγονται αρχικά μέσω βίντεο, να χρησιμοποιηθούν για την εξαγωγή άλλων πληροφοριών για την επίτευξη διαφορετικού σκοπού (π.χ. για την χαρτογράφηση των συνηθειών ενός ατόμου). Ωστόσο, δεν πρέπει πάντα να θεωρείται ότι η βιντεοεπιτήρηση ισοδυναμεί με επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα.

63. Παράδειγμα: Βιντεοσκοπημένο υλικό που δείχνει υποκείμενο των δεδομένων να φοράει γυαλιά ή να χρησιμοποιεί αναπηρικό καροτσάκι δεν αποτελεί καθεαυτό ειδική κατηγορία δεδομένων προσωπικού χαρακτήρα.

64. Ωστόσο, αν το υλικό αυτό υποβληθεί σε επεξεργασία προκειμένου να εξαχθούν συμπεράσματα για ειδικές κατηγορίες δεδομένων, τότε εφαρμόζεται το άρθρο 9.

65. Παράδειγμα: Από εικόνες που δείχνουν ταυτοποιήσιμα υποκείμενα των δεδομένων να συμμετέχουν σε εκδήλωση, απεργία κ.λπ., θα μπορούσαν να εξαχθούν συμπεράσματα για τα πολιτικά φρονήματα αυτών των ατόμων. Η περίπτωση αυτή εμπίπτει στο άρθρο 9.

Παράδειγμα: Όταν σε νοσοκομείο εγκαθίσταται βιντεοκάμερα για να παρακολουθείται η κατάσταση της υγείας ασθενούς, θεωρείται ότι γίνεται επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα (άρθρο 9).

66. Κατά κανόνα, όταν εγκαθίσταται σύστημα βιντεοεπιτήρησης θα πρέπει να εξετάζεται προσεκτικά η αρχή της ελαχιστοποίησης των δεδομένων. Ως εκ τούτου, ακόμη και σε περιπτώσεις όπου δεν εφαρμόζεται το άρθρο 9 παράγραφος 1, ο υπεύθυνος επεξεργασίας των δεδομένων θα πρέπει πάντα να προσπαθεί να ελαχιστοποιεί τον κίνδυνο λήψης υλικού που αποκαλύπτει άλλα ευαίσθητα δεδομένα (πέραν του άρθρου 9), ανεξαρτήτως του σκοπού.

67. Παράδειγμα: Σύστημα βιντεοεπιτήρησης που παρακολουθεί εκκλησία δεν υπόκειται εξ ορισμού στο άρθρο 9. Ωστόσο, ο υπεύθυνος επεξεργασίας οφείλει να διενεργήσει ιδιαίτερα προσεκτική αξιολόγηση στο πλαίσιο του άρθρου 6 παράγραφος 1 στοιχείο στ), λαμβάνοντας υπόψη τη φύση των δεδομένων αλλά και τον κίνδυνο αποκάλυψης άλλων ευαίσθητων δεδομένων (πέραν του άρθρου 9) κατά την αξιολόγηση των συμφερόντων του υποκειμένου των δεδομένων.

68. Αν το σύστημα βιντεοεπιτήρησης χρησιμοποιείται για να γίνει επεξεργασία ειδικών κατηγοριών δεδομένων, ο υπεύθυνος επεξεργασίας πρέπει να προσδιορίσει τόσο την εξαίρεση που αφορά την επεξεργασία ειδικών κατηγοριών δεδομένων σύμφωνα με το άρθρο 9 (π.χ. εξαίρεση από τον γενικό κανόνα ότι δεν θα πρέπει κανένας να επεξεργάζεται ειδικές κατηγορίες δεδομένων), όσο και τη νομική βάση σύμφωνα με το άρθρο 6.

69. Για παράδειγμα, ο υπεύθυνος επεξεργασίας θα μπορούσε –θεωρητικά και κατ' εξαίρεση– να χρησιμοποιήσει ως νομική βάση το άρθρο 9 παράγραφος 2 στοιχείο γ) («[...] *η επεξεργασία είναι απαραίτητη για την προστασία των ζωτικών συμφερόντων του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου* [...]»), αλλά θα πρέπει να τεκμηριώσει ότι η επεξεργασία είναι απολύτως

αναγκαία για να προστατευθούν τα ζωτικά συμφέροντα του προσώπου και να αποδείξει ότι «[...] *το υποκείμενο των δεδομένων είναι σωματικά ή νομικά ανίκανο να συγκατατεθεί*.». Επιπροσθέτως, ο υπεύθυνος επεξεργασίας δεν επιτρέπεται να χρησιμοποιήσει το σύστημα για κανέναν άλλο λόγο.

70. Είναι σημαντικό να επισημανθεί σε αυτό το σημείο ότι η επίκληση οποιασδήποτε εξαίρεσης που αναφέρεται στο άρθρο 9 για να αιτιολογηθεί η επεξεργασία ειδικών κατηγοριών δεδομένων μέσω βιντεοεπιτήρησης είναι τις περισσότερες φορές αδύνατη. Ειδικότερα, οι υπεύθυνοι που επεξεργάζονται αυτά τα δεδομένα στο πλαίσιο βιντεοεπιτήρησης δεν μπορούν να επικαλεστούν το άρθρο 9 παράγραφος 2 στοιχείο ε), το οποίο επιτρέπει την επεξεργασία δεδομένων προσωπικού χαρακτήρα που έχουν προδήλως δημοσιοποιηθεί από το υποκείμενο των δεδομένων. Το γεγονός και μόνο ότι το υποκείμενο των δεδομένων εμπίπτει στην εμβέλεια της κάμερας δεν συνεπάγεται πρόθεσή του να δημοσιοποιήσει ειδικές κατηγορίες δεδομένων που το αφορούν.

71. Επιπλέον, η επεξεργασία ειδικών κατηγοριών δεδομένων απαιτεί αυξημένη και συνεχή επαγρύπνηση σε σχέση με ορισμένες υποχρεώσεις. Παραδείγματος χάρη, όπου κρίνεται αναγκαίο, θα πρέπει να διενεργούνται υψηλού επιπέδου εκτιμήσεις αντικτύπου για την ασφάλεια και την προστασία δεδομένων.

> Παράδειγμα: Ο εργοδότης δεν πρέπει να χρησιμοποιεί το υλικό του συστήματος βιντεοεπιτήρησης για να ταυτοποιεί απεργούς που συμμετέχουν σε πορείες.

72.

5.1 Γενικές παράμετροι κατά την επεξεργασία βιομετρικών δεδομένων

73. Η χρήση βιομετρικών δεδομένων, και ιδίως η αναγνώριση προσώπου, εγκυμονεί αυξημένους κινδύνους για τα δικαιώματα των υποκειμένων των δεδομένων. Τα τεχνολογικά αυτά μέσα πρέπει οπωσδήποτε να χρησιμοποιούνται με γνώμονα τις αρχές της νομιμότητας, της αναγκαιότητας, της αναλογικότητας και της ελαχιστοποίησης δεδομένων όπως προβλέπονται στον ΓΚΠΔ. Μολονότι η χρήση αυτών των τεχνολογιών μπορεί να θεωρείται ιδιαίτερα αποτελεσματική, οι υπεύθυνοι επεξεργασίας θα πρέπει πρώτα από όλα να αξιολογούν τον αντίκτυπο που έχουν τα τεχνολογικά αυτά μέσα στα θεμελιώδη δικαιώματα και τις ελευθερίες και να εξετάζουν τη χρήση λιγότερο παρεμβατικών μέσων για να επιτυγχάνουν τον νόμιμο σκοπό της επεξεργασίας.

74. Η επεξεργασία ανεπεξέργαστων δεδομένων όπως τα φυσικά, βιολογικά ή συμπεριφορικά χαρακτηριστικά φυσικού προσώπου, για να χαρακτηριστεί επεξεργασία βιομετρικών δεδομένων όπως ορίζεται στον ΓΚΠΔ, πρέπει να υποδηλώνει μέτρηση αυτών των χαρακτηριστικών. Εφόσον τα βιομετρικά δεδομένα είναι αποτέλεσμα τέτοιων μετρήσεων, ο ΓΚΠΔ ορίζει στο άρθρο 4(14) ότι *«[...] προκύπτουν από ειδική τεχνική επεξεργασία συνδεόμενη με φυσικά, βιολογικά ή συμπεριφορικά χαρακτηριστικά φυσικού προσώπου και τα οποία επιτρέπουν ή επιβεβαιώνουν την αδιαμφισβήτητη ταυτοποίηση του εν λόγω φυσικού προσώπου [...]».* Ωστόσο, το υλικό βιντεοσκόπησης που απεικονίζει άτομα δεν μπορεί να θεωρηθεί ότι αποτελεί καθαυτό βιομετρικό δεδομένο σύμφωνα με το άρθρο 9, εάν προηγουμένως το υλικό δεν έχει υποβληθεί σε ειδική τεχνική επεξεργασία προκειμένου να συμβάλει η επεξεργασία αυτή στην ταυτοποίηση των ατόμων[16].

[16] Η αιτιολογική σκέψη 51 του ΓΚΠΔ στηρίζει αυτό το σκεπτικό, καθώς αναφέρεται ότι «*[...] Η επεξεργασία φωτογραφιών δεν θα πρέπει συστηματικά να θεωρείται ότι είναι επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα, καθώς αυτές καλύπτονται από τον ορισμό των βιομετρικών δεδομένων μόνο σε περίπτωση επεξεργασίας μέσω ειδικών τεχνικών μέσων που επιτρέπουν την αδιαμφισβήτητη ταυτοποίηση ή επαλήθευση της ταυτότητας ενός φυσικού προσώπου.* [...]».

75. Η επεξεργασία βιομετρικών δεδομένων, για να λογίζεται ως επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα (άρθρο 9), πρέπει να έχει «σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου».

76. Συνοπτικά, υπό το πρίσμα του άρθρου 4(14) και του άρθρου 9, πρέπει να λαμβάνονται υπόψη τρία κριτήρια:

- **Φύση των δεδομένων:** δεδομένα που σχετίζονται με τα φυσικά, βιολογικά ή συμπεριφορικά χαρακτηριστικά φυσικού προσώπου,
- **Μέσα και τρόπος επεξεργασίας**: δεδομένα τα οποία «προκύπτουν από ειδική τεχνική επεξεργασία»,
- **Σκοπός της επεξεργασίας:** τα δεδομένα πρέπει να χρησιμοποιούνται με σκοπό την αδιαμφισβήτητη ταυτοποίηση φυσικού προσώπου.

77. Η χρήση συστημάτων βιντεοεπιτήρησης που περιλαμβάνουν και λειτουργίες βιομετρικής αναγνώρισης τις οποίες εγκαθιστούν ιδιωτικές οντότητες για δικούς τους σκοπούς (π.χ. για σκοπούς εμπορικής προώθησης, στατιστικής ή ακόμη και ασφάλειας) προϋποθέτει τις περισσότερες φορές τη ρητή συγκατάθεση όλων των υποκειμένων των δεδομένων (άρθρο 9 παράγραφος 2 στοιχείο α)), μολονότι και σε αυτήν την περίπτωση μπορεί να ισχύει άλλη νόμιμη εξαίρεση του άρθρου 9.

Παράδειγμα: Για να βελτιώσει τις υπηρεσίες της, ιδιωτική εταιρεία αντικαθιστά τα σημεία ελέγχου ταυτοποίησης επιβατών του αεροδρομίου (παράδοση αποσκευών, επιβίβαση) με συστήματα βιντεοεπιτήρησης, τα οποία χρησιμοποιούν τεχνικές αναγνώρισης προσώπου για να εξακριβώνεται η ταυτότητα των επιβατών που έχουν επιλέξει να δώσουν τη συγκατάθεσή τους για αυτήν τη διαδικασία. Δεδομένου ότι η επεξεργασία εμπίπτει στο άρθρο 9, οι επιβάτες που έχουν ήδη δώσει τη ρητή και με πλήρη επίγνωση συγκατάθεσή τους για να υποβληθούν σε επεξεργασία, πρέπει να εγγραφούν, παραδείγματος χάρη, σε αυτόματο τερματικό σταθμό προκειμένου να δημιουργήσουν και να καταχωρίσουν το πρότυπο του προσώπου τους, το οποίο θα συσχετιστεί με την κάρτα επιβίβασης και την ταυτότητά τους. Τα σημεία ελέγχου με αναγνώριση προσώπου πρέπει να διαχωρίζονται σαφώς από τις υπόλοιπες εγκαταστάσεις. Για παράδειγμα, το σύστημα πρέπει να είναι εγκατεστημένο εντός αψίδας ελέγχου ώστε να μη λαμβάνονται τα βιομετρικά πρότυπα προσώπων που δεν έχουν δώσει τη συγκατάθεσή τους. Μόνον οι επιβάτες που έχουν ήδη δώσει τη συγκατάθεσή τους και έχουν ολοκληρώσει την εγγραφή τους μπορούν να χρησιμοποιούν την αψίδα ελέγχου με το βιομετρικό σύστημα.

Παράδειγμα: Υπεύθυνος επεξεργασίας ελέγχει την πρόσβαση στο κτίριό του με τη μέθοδο της αναγνώρισης προσώπου. Τα άτομα μπορούν να χρησιμοποιήσουν αυτόν τον τρόπο πρόσβασης μόνον αν έχουν δώσει προηγουμένως τη ρητή και με πλήρη επίγνωση συγκατάθεσή τους (σύμφωνα με το άρθρο 9 παράγραφος 2 στοιχείο α)). Ωστόσο, για να μην απεικονίζονται τα πρόσωπα ατόμων που δεν έδωσαν τη συγκατάθεσή τους, η μέθοδος αναγνώρισης προσώπου θα πρέπει να ενεργοποιείται από το ίδιο το υποκείμενο των δεδομένων, π.χ. με το πάτημα ενός κουμπιού. Για να είναι νόμιμη η επεξεργασία, ο υπεύθυνος επεξεργασίας πρέπει πάντα να προσφέρει εναλλακτικό τρόπο πρόσβασης στο κτίριο κατά τον οποίο δεν θα διενεργείται επεξεργασία βιομετρικών δεδομένων, όπως π.χ. κάρτες εισόδου ή κλειδιά.

78.

79. Σε αυτού του είδους τις περιπτώσεις, στις οποίες δημιουργούνται βιομετρικά πρότυπα, οι υπεύθυνοι επεξεργασίας μεριμνούν ώστε, από τη στιγμή που υπάρξει ή δεν υπάρξει αντιστοιχία στη βάση δεδομένων, να διαγράφουν αμέσως και με ασφάλεια όλα τα ενδιάμεσα πρότυπα που δημιουργήθηκαν στη διάρκεια της διαδικασίας (με τη ρητή και με πλήρη επίγνωση συγκατάθεση του υποκειμένου των δεδομένων) για να αντιπαραβληθούν με τα πρότυπα που δημιούργησαν τα υποκείμενα των δεδομένων κατά τη στιγμή της εγγραφής τους. Τα πρότυπα που δημιουργούνται για την εγγραφή θα πρέπει να διατηρούνται μόνο για την εκπλήρωση του σκοπού της επεξεργασίας και να μην αποθηκεύονται ή να αρχειοθετούνται.

80. Ωστόσο, όταν ο σκοπός της επεξεργασίας είναι π.χ. να διακριθεί μια κατηγορία ανθρώπων από μια άλλη, και όχι η αδιαμφισβήτητη ταυτοποίηση προσώπου, η επεξεργασία δεν εμπίπτει στο άρθρο 9.

Παράδειγμα: Καταστηματάρχης επιθυμεί να προσαρμόσει το διαφημιστικό του υλικό στα χαρακτηριστικά (φύλο και ηλικία) του πελάτη που απεικονίζεται σε σύστημα βιντεοεπιτήρησης. Αν αυτό το σύστημα δεν δημιουργεί βιομετρικά πρότυπα με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, αλλά εντοπίζει απλώς αυτά τα φυσικά χαρακτηριστικά προκειμένου να ταξινομήσει το πρόσωπο, τότε η επεξεργασία δεν εμπίπτει στο άρθρο 9 (εφόσον δεν υποβάλλονται σε επεξεργασία άλλα είδη ειδικών κατηγοριών δεδομένων).

81.

82. Το άρθρο 9 ισχύει, ωστόσο, αν ο υπεύθυνος επεξεργασίας αποθηκεύει βιομετρικά δεδομένα – τις περισσότερες φορές μέσω προτύπων που παράγονται μετά την επεξεργασία βασικών χαρακτηριστικών των ανεπεξέργαστων βιομετρικών δεδομένων (π.χ. τη μέτρηση από εικόνα των διαστάσεων των προσώπων) – με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου. Εάν ο υπεύθυνος επεξεργασίας θέλει να εντοπίσει υποκείμενο των δεδομένων που επανέρχεται στον χώρο ή που εισέρχεται σε νέο χώρο (ώστε να προβάλλεται συνεχώς εξατομικευμένο διαφημιστικό υλικό), τότε ο σκοπός θα είναι η αδιαμφισβήτητη ταυτοποίηση φυσικού προσώπου, και έτσι η πράξη εμπίπτει εξαρχής στο άρθρο 9. Αυτό συμβαίνει όταν π.χ. υπεύθυνος επεξεργασίας αποθηκεύει τα παραγόμενα πρότυπα για να προβάλλονται συνεχώς εξατομικευμένες διαφημίσεις στις διάφορες πινακίδες που βρίσκονται σε διαφορετικά σημεία εντός του καταστήματος. Εφόσον το σύστημα χρησιμοποιεί φυσικά χαρακτηριστικά τόσο για τον εντοπισμό συγκεκριμένων ατόμων που επιστρέφουν στο πεδίο λήψης της κάμερας (όπως οι επισκέπτες εμπορικού κέντρου), όσο και για την ιχνηλάτησή τους, πρόκειται για μέθοδο βιομετρικής ταυτοποίησης επειδή η διαδικασία αποσκοπεί στην ταυτοποίηση με τη χρήση ειδικής τεχνικής επεξεργασίας.

Παράδειγμα: Καταστηματάρχης έχει εγκαταστήσει σύστημα αναγνώρισης προσώπου στο κατάστημά του προκειμένου να προβάλλονται εξατομικευμένες διαφημίσεις στους πελάτες. Ο υπεύθυνος επεξεργασίας πρέπει να λάβει τη ρητή και με πλήρη επίγνωση συγκατάθεση όλων των υποκειμένων των δεδομένων προτού χρησιμοποιήσει αυτό το βιομετρικό σύστημα και προβάλει εξατομικευμένο διαφημιστικό υλικό. Το σύστημα δεν είναι νόμιμο εάν καταγράφει επισκέπτες ή διερχομένους που δεν έχουν δώσει τη συγκατάθεσή τους για τη δημιουργία του βιομετρικού τους προτύπου, ακόμη και αν αυτό το πρότυπο διαγράφεται το συντομότερο δυνατό. Πράγματι, αυτά τα προσωρινά πρότυπα συνιστούν βιομετρικά δεδομένα, τα οποία υποβάλλονται σε επεξεργασία με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπων. Τα πρόσωπα αυτά ωστόσο ενδέχεται να μην επιθυμούν να γίνουν δέκτες στοχευμένων διαφημίσεων.

83.

84. Το ΕΣΠΔ παρατηρεί ότι ορισμένα βιομετρικά συστήματα είναι εγκατεστημένα σε μη ελεγχόμενα περιβάλλοντα[17], γεγονός το οποίο σημαίνει ότι το σύστημα απεικονίζει, στο πλαίσιο της διαδικασίας, τα πρόσωπα όλων των ατόμων που διέρχονται από το πεδίο λήψης της κάμερας. Μεταξύ αυτών, υπάρχουν και άτομα που δεν έχουν δώσει τη συγκατάθεσή τους για να καταγραφούν από τη βιομετρική συσκευή και ούτε, επομένως, για τη δημιουργία βιομετρικών προτύπων. Τα πρότυπα αυτά αντιπαραβάλλονται με τα πρότυπα των υποκείμενων των δεδομένων που έδωσαν τη συγκατάθεσή τους κατά τη διάρκεια της εγγραφής τους (στην προκειμένη περίπτωση πρόκειται για τους χρήστες της βιομετρικής συσκευής), ώστε ο υπεύθυνος επεξεργασίας να γνωρίζει εάν το πρόσωπο είναι χρήστης βιομετρικής συσκευής ή όχι. Στην περίπτωση αυτή, το σύστημα είναι συχνά ειδικά σχεδιασμένο ώστε να διαχωρίζει τα άτομα που επιθυμεί να αναγνωρίσει από μια βάση δεδομένων, από τα άτομα που δεν έχουν εγγραφεί. Εφόσον ο σκοπός είναι η αδιαμφισβήτητη ταυτοποίηση φυσικών προσώπων, πρέπει σε κάθε περίπτωση να ισχύει μία από τις εξαιρέσεις του άρθρου 9 παράγραφος 2 του ΓΚΠΔ για <u>οποιονδήποτε</u> παρακολουθείται από την κάμερα.

<u>Παράδειγμα:</u> Ξενοδοχείο χρησιμοποιεί σύστημα βιντεοεπιτήρησης που ειδοποιεί αυτομάτως τον διευθυντή του ξενοδοχείου όταν φθάσει ένα πολύ σημαντικό πρόσωπο (VIP), εφόσον βέβαια το πρόσωπο του επισκέπτη αναγνωρίζεται από το σύστημα. Αυτά τα σημαντικά πρόσωπα έχουν δώσει τη ρητή τους συγκατάθεση για τη χρήση αναγνώρισης προσώπου πριν καταγραφούν σε βάση δεδομένων που δημιουργείται για αυτόν τον σκοπό. Τα εν λόγω συστήματα επεξεργασίας βιομετρικών δεδομένων είναι παράνομα εάν όλοι οι άλλοι επισκέπτες που παρακολουθούνται (προκειμένου να ταυτοποιηθούν τα πολύ σημαντικά πρόσωπα) δεν έχουν δώσει τη συγκατάθεσή τους για την επεξεργασία σύμφωνα με το άρθρο 9 παράγραφος 2 στοιχείο α) του ΓΚΠΔ.

<u>Παράδειγμα</u>: Ο υπεύθυνος επεξεργασίας εγκαθιστά σύστημα βιντεοεπιτήρησης με αναγνώριση προσώπου στην είσοδο του συναυλιακού χώρου που διαχειρίζεται. Ο υπεύθυνος επεξεργασίας πρέπει να προβλέψει σαφώς διαχωρισμένες εισόδους: μία είσοδο με βιομετρικό σύστημα και μία είσοδο χωρίς βιομετρικό σύστημα (στην οποία οι θεατές θα μπορούν π.χ. να σαρώνουν το εισιτήριό τους). Οι είσοδοι που διαθέτουν βιομετρικές συσκευές πρέπει να είναι διαμορφωμένες και προσβάσιμες κατά τρόπο ο οποίος αποτρέπει το σύστημα από την καταγραφή των βιομετρικών προτύπων των θεατών που δεν έχουν δώσει τη συγκατάθεσή τους για να υποβληθούν σε επεξεργασία.

85.

86. Τέλος, όταν η συγκατάθεση προβλέπεται στο άρθρο 9 του ΓΚΠΔ, ο υπεύθυνος επεξεργασίας δεν πρέπει να συνδέει την πρόσβαση στις υπηρεσίες του με την αποδοχή της βιομετρικής επεξεργασίας. Με άλλα λόγια, όταν η επεξεργασία βιομετρικών δεδομένων χρησιμοποιείται για τον σκοπό της εξακρίβωσης της ταυτότητας, ο υπεύθυνος επεξεργασίας πρέπει να προσφέρει εναλλακτική λύση η οποία δεν περιλαμβάνει την βιομετρική επεξεργασία – χωρίς περιορισμούς ή πρόσθετο κόστος για το υποκείμενο των δεδομένων. Αυτή η εναλλακτική λύση απαιτείται επίσης τόσο για τα άτομα που δεν πληρούν τις απαιτήσεις της βιομετρικής συσκευής (αδύνατη εγγραφή ή ανάγνωση των βιομετρικών δεδομένων, αναπηρία που δυσχεραίνει τη χρήση κ.λπ.) όσο και στις περιπτώσεις κατά τις οποίες η βιομετρική συσκευή δεν είναι διαθέσιμη (π.χ. δυσλειτουργία της συσκευής). Στις περιπτώσεις αυτές πρέπει να εφαρμόζεται «εφεδρική λύση» προκειμένου να διασφαλίζεται η αδιάλειπτη χρήση της

[17] Αυτό σημαίνει ότι η βιομετρική συσκευή είναι τοποθετημένη σε χώρο ανοιχτό για το κοινό και μπορεί να λειτουργήσει για κάθε διερχόμενο, σε αντίθεση με τα βιομετρικά συστήματα σε ελεγχόμενα περιβάλλοντα που μπορούν να χρησιμοποιηθούν μόνο με τη συμμετοχή του προσώπου που συγκατατίθεται.

προτεινόμενης υπηρεσίας, μολονότι η λύση αυτή πρέπει να χρησιμοποιείται σε εξαιρετικές μόνο περιστάσεις. Σε εξαιρετικές περιπτώσεις, η επεξεργασία βιομετρικών δεδομένων ενδέχεται να είναι η βασική δραστηριότητα υπηρεσίας που παρέχεται στο πλαίσιο σύμβασης. Τέτοιες περιπτώσεις είναι π.χ. οι επιδείξεις συσκευών αναγνώρισης προσώπου που διοργανώνουν μουσεία για να εξηγήσουν πώς λειτουργούν οι συσκευές αυτές, στην οποία περίπτωση ωστόσο το υποκείμενο των δεδομένων δεν μπορεί να εναντιωθεί στην επεξεργασία βιομετρικών δεδομένων εάν επιθυμεί να συμμετάσχει στην επίδειξη. Και στην περίπτωση αυτή πάντως, ισχύει η συγκατάθεση που προβλέπεται στο άρθρο 9, εάν πληρούνται οι απαιτήσεις του άρθρου 7.

5.2 Προτεινόμενα μέτρα για την ελαχιστοποίηση των κινδύνων κατά την επεξεργασία βιομετρικών δεδομένων

87. Με γνώμονα την αρχή της ελαχιστοποίησης δεδομένων, οι υπεύθυνοι επεξεργασίας πρέπει να διασφαλίζουν ότι τα δεδομένα που εξάγονται από ψηφιακή εικόνα για τη δημιουργία προτύπου δεν θα είναι υπερβολικά και θα περιέχουν μόνο τις πληροφορίες που απαιτούνται για τον συγκεκριμένο σκοπό, αποτρέποντας επομένως κάθε πιθανή περαιτέρω επεξεργασία. Θα πρέπει να ληφθούν μέτρα προκειμένου να διασφαλίζεται ότι θα είναι αδύνατη η διαβίβαση προτύπων μεταξύ βιομετρικών συστημάτων.

88. Η ταυτοποίηση και η εξακρίβωση/επαλήθευση της ταυτότητας είναι πιθανόν να απαιτούν την αποθήκευση του προτύπου προκειμένου να χρησιμοποιηθεί σε μεταγενέστερη αντιπαραβολή. Ο υπεύθυνος επεξεργασίας πρέπει να εξετάζει την καταλληλότερη τοποθεσία αποθήκευσης των δεδομένων. Σε ένα ελεγχόμενο περιβάλλον (οριοθετημένοι χώροι υποδοχής ή σημεία ελέγχου) τα πρότυπα πρέπει να αποθηκεύονται σε ατομική συσκευή ή μέσο που τηρεί ο χρήστης και βρίσκεται υπό τον αποκλειστικό του έλεγχο (έξυπνο κινητό τηλέφωνο ή ταυτότητα) ή –όταν αυτό απαιτείται για ειδικούς σκοπούς και εφόσον συντρέχουν αντικειμενικές ανάγκες– αποθηκεύονται σε κεντρική βάση δεδομένων σε κρυπτογραφημένη μορφή, με μυστικό κωδικό που βρίσκεται αποκλειστικά στα χέρια του χρήστη, προκειμένου να αποτρέπεται η μη εξουσιοδοτημένη πρόσβαση στο πρότυπο ή στην τοποθεσία αποθήκευσης. Εάν δεν μπορεί να αποτρέψει την πρόσβαση τρίτων στα πρότυπα, ο υπεύθυνος επεξεργασίας πρέπει να λάβει κατάλληλα μέτρα ώστε να διασφαλίζει την ασφάλεια των αποθηκευόμενων δεδομένων. Στα μέτρα αυτά συγκαταλέγεται και η κρυπτογράφηση του προτύπου με κρυπτογραφικό αλγόριθμο.

89. Σε κάθε περίπτωση, ο υπεύθυνος επεξεργασίας λαμβάνει όλα τα απαραίτητα προληπτικά μέτρα ώστε να διαφυλάξει τη διαθεσιμότητα, την ακεραιότητα και την εμπιστευτικότητα των υπό επεξεργασία δεδομένων. Για τον σκοπό αυτό, ο υπεύθυνος επεξεργασίας λαμβάνει κυρίως τα ακόλουθα μέτρα: διαχωρίζει τα δεδομένα κατά τη διάρκεια της διαβίβασης και της αποθήκευσής τους, αποθηκεύει τα βιομετρικά πρότυπα και τα ανεπεξέργαστα δεδομένα ή τα δεδομένα ταυτότητας σε χωριστές βάσεις δεδομένων, κρυπτογραφεί τα βιομετρικά δεδομένα, κυρίως τα βιομετρικά πρότυπα, και καθορίζει πολιτική για την κρυπτογράφηση και τη διαχείριση των κλειδιών κρυπτογράφησης, ενσωματώνει οργανωτικά και τεχνικά μέτρα για τον εντοπισμό περιστατικών απάτης, συσχετίζει κωδικό ακεραιότητας με τα δεδομένα (για παράδειγμα, υπογραφή ή ετικέτα) και απαγορεύει κάθε εξωτερική πρόσβαση στα βιομετρικά δεδομένα. Τα μέτρα αυτά θα πρέπει να συμβαδίζουν με την πρόοδο της τεχνολογίας.

90. Άλλωστε, οι υπεύθυνοι επεξεργασίας δεδομένων θα πρέπει να διαγράφουν ανεπεξέργαστα δεδομένα (απεικόνιση προσώπου, σήματα ομιλίας, βάδισμα κ.λπ.) και να διασφαλίζουν την αποτελεσματικότητα της διαγραφής. Εάν δεν υφίσταται πλέον νομική βάση για την επεξεργασία, τα ανεπεξέργαστα δεδομένα πρέπει να διαγράφονται. Πράγματι, στον βαθμό που τα βιομετρικά πρότυπα απορρέουν από αυτά τα δεδομένα, θα μπορούσαμε να ισχυριστούμε ότι η δημιουργία βάσεων δεδομένων μπορεί να αποτελέσει ισοδύναμη, αν όχι μεγαλύτερη απειλή (σε αντίθεση με τα ανεπεξέργαστα δεδομένα, που αποτελούν τα συστατικά στοιχεία του κάθε προτύπου, το βιομετρικό πρότυπο δεν είναι πάντα εύκολο να αναγνωστεί χωρίς να γνωρίζουμε πώς έγινε ο προγραμματισμός του). Σε περίπτωση που ο υπεύθυνος επεξεργασίας δεδομένων χρειάζεται να διατηρήσει αυτά τα δεδομένα, θα πρέπει να διερευνήσει τη χρήση μεθόδων προσθετικού θορύβου (όπως η υδατοσήμανση), οι οποίες καθιστούν αναποτελεσματική τη δυνατότητα δημιουργίας του προτύπου. Ο υπεύθυνος επεξεργασίας πρέπει επίσης να διαγράφει βιομετρικά δεδομένα και πρότυπα σε περίπτωση μη εξουσιοδοτημένης πρόσβασης στο τερματικό ανάγνωσης-σύγκρισης ή στον διακομιστή αποθήκευσης και να διαγράφει όλα τα δεδομένα που δεν είναι χρήσιμα για περαιτέρω επεξεργασία στο τέλος του κύκλου ζωής της βιομετρικής συσκευής.

6 ΔΙΚΑΙΩΜΑΤΑ ΤΟΥ ΥΠΟΚΕΙΜΕΝΟΥ ΤΩΝ ΔΕΔΟΜΕΝΩΝ

91. Λόγω του χαρακτήρα της επεξεργασίας δεδομένων κατά τη χρήση βιντεοεπιτήρησης ορισμένα δικαιώματα του υποκειμένου των δεδομένων σύμφωνα με τον ΓΚΠΔ πρέπει να διευκρινιστούν περαιτέρω. Ωστόσο, αυτό το κεφάλαιο δεν είναι εξαντλητικό και κατά την επεξεργασία δεδομένων προσωπικού χαρακτήρα μέσω βιντεοεπιτήρησης ισχύουν όλα τα δικαιώματα που προβλέπονται στον ΓΚΠΔ.

6.1 Δικαίωμα πρόσβασης

92. Το υποκείμενο των δεδομένων έχει το δικαίωμα να ζητεί επιβεβαίωση από τον υπεύθυνο επεξεργασίας ως προς το αν τα δεδομένα προσωπικού χαρακτήρα που το αφορούν υποβάλλονται σε επεξεργασία. Όσον αφορά τη βιντεοεπιτήρηση, αυτό σημαίνει ότι εάν δεν αποθηκεύονται ή δεν διαβιβάζονται με κανέναν τρόπο δεδομένα, τότε από τη στιγμή που θα παρέλθει η στιγμή της παρακολούθησης σε πραγματικό χρόνο ο υπεύθυνος επεξεργασίας μπορεί μόνο να δώσει την πληροφορία ότι κανένα δεδομένο προσωπικού χαρακτήρα δεν υποβάλλεται πλέον σε επεξεργασία (πέραν των γενικών υποχρεώσεων πληροφόρησης σύμφωνα με το άρθρο 13, βλέπε *Ενότητα 7 - Υποχρεώσεις διαφάνειας και πληροφόρησης*). Αν ωστόσο εξακολουθεί να γίνεται επεξεργασία δεδομένων τη στιγμή του αιτήματος (δηλ. αν τα δεδομένα αποθηκεύονται ή υποβάλλονται σε συνεχή επεξεργασία με οποιονδήποτε άλλον τρόπο), το υποκείμενο των δεδομένων θα πρέπει να λάβει πρόσβαση και πληροφόρηση σύμφωνα με το άρθρο 15.

93. Το δικαίωμα πρόσβασης μπορεί ωστόσο να περιορίζεται σε ορισμένες περιπτώσεις.

- Το άρθρο 15 παράγραφος 4 του ΓΚΠΔ, επηρεάζει δυσμενώς τα δικαιώματα άλλων

94. Δεδομένου ότι στην ίδια αλληλουχία βιντεοεπιτήρησης μπορεί να καταγραφεί απροσδιόριστος αριθμός υποκειμένων των δεδομένων, ο έλεγχος του βιντεοσκοπημένου υλικού θα έχει ως αποτέλεσμα την πρόσθετη επεξεργασία δεδομένων προσωπικού χαρακτήρα άλλων υποκειμένων των δεδομένων. Τυχόν επιθυμία του υποκειμένου των δεδομένων να λάβει αντίγραφο του υλικού (άρθρο 15 παράγραφος 3) θα μπορούσε να επηρεάσει δυσμενώς τα δικαιώματα και τις ελευθερίες άλλων υποκειμένων των δεδομένων που απεικονίζονται στο υλικό. Ως εκ τούτου, για να αποτρέψει αυτό το ενδεχόμενο, ο υπεύθυνος επεξεργασίας θα πρέπει να λαμβάνει υπόψη ότι, λόγω του παρεμβατικού χαρακτήρα του βιντεοσκοπημένου υλικού, σε ορισμένες περιπτώσεις δεν θα πρέπει να διανέμει βιντεοσκοπημένο υλικό στο οποίο μπορούν να ταυτοποιηθούν άλλα υποκείμενα των δεδομένων. Ωστόσο, η προστασία των δικαιωμάτων τρίτων μερών δεν πρέπει να χρησιμοποιείται ως δικαιολογία για να μην ικανοποιούνται θεμιτά αιτήματα πρόσβασης. Ο υπεύθυνος επεξεργασίας θα πρέπει εν προκειμένω να χρησιμοποιεί τεχνικά μέτρα για να ανταποκριθεί στο αίτημα πρόσβασης (π.χ. τεχνικές επεξεργασίας εικόνων, όπως απόκρυψη ή αλλοίωση). Ωστόσο, οι υπεύθυνοι επεξεργασίας δεν είναι υποχρεωμένοι να χρησιμοποιούν τα εν λόγω τεχνικά μέτρα αν μπορούν με άλλον τρόπο να ανταποκριθούν σε αίτημα του άρθρου 15 εντός του χρονικού περιθωρίου που ορίζει το άρθρο 12 παράγραφος 3.

- Άρθρο 11 παράγραφος 2 του ΓΚΠΔ, ο υπεύθυνος επεξεργασίας δεν είναι σε θέση να εξακριβώσει την ταυτότητα του υποκειμένου των δεδομένων

95. Εάν στο βιντεοσκοπημένο υλικό είναι αδύνατο να αναζητηθούν δεδομένα προσωπικού χαρακτήρα (για την ακρίβεια, ο υπεύθυνος επεξεργασίας πρέπει πιθανότατα να επεξεργαστεί μεγάλο όγκο αποθηκευμένου υλικού για να εντοπίσει το εκάστοτε υποκείμενο των δεδομένων), ο υπεύθυνος επεξεργασίας μπορεί να μην είναι σε θέση να εξακριβώσει την ταυτότητα του υποκειμένου των δεδομένων.

96. Για αυτούς τους λόγους το υποκείμενο των δεδομένων θα πρέπει (πέρα από την ταυτοποίηση που πραγματοποιεί το ίδιο, συμπεριλαμβανομένης της ταυτοποίησης με έγγραφο ταυτότητας ή με προσωπική επαφή) να διευκρινίζει στο αίτημα που αποστέλλει στον υπεύθυνο επεξεργασίας τον χρόνο – εντός εύλογου χρονικού πλαισίου ανάλογα βέβαια και με τον αριθμό των υποκειμένων των δεδομένων που έχουν καταγραφεί – κατά τον οποίο εισήλθε στον υπό παρακολούθηση χώρο. Ο υπεύθυνος επεξεργασίας θα πρέπει να γνωστοποιεί εκ των προτέρων στο υποκείμενο των δεδομένων ποιες πληροφορίες χρειάζεται ο ίδιος για να ικανοποιήσει το αίτημα. Αν ο υπεύθυνος επεξεργασίας μπορεί να αποδείξει ότι δεν είναι σε θέση να εξακριβώσει την ταυτότητα του υποκειμένου των δεδομένων, ο υπεύθυνος επεξεργασίας πρέπει να ενημερώσει το υποκείμενο των δεδομένων αναλόγως, εφόσον αυτό είναι δυνατό. Σε αυτήν την περίπτωση, στην απάντησή του προς το υποκείμενο των δεδομένων ο υπεύθυνος επεξεργασίας θα πρέπει να το ενημερώσει για τον ακριβή χώρο παρακολούθησης, την επαλήθευση των καμερών που ήταν σε χρήση κ.λπ. ώστε το υποκείμενο των δεδομένων να γνωρίζει ακριβώς ποια δεδομένα προσωπικού χαρακτήρα που το αφορούν μπορεί να έχουν υποβληθεί σε επεξεργασία.

Παράδειγμα: Αν υποκείμενο των δεδομένων ζητήσει αντίγραφο των δεδομένων προσωπικού χαρακτήρα που το αφορούν, τα οποία υποβάλλονται σε επεξεργασία μέσω βιντεοεπιτήρησης στην είσοδο εμπορικού κέντρου με 30 000 επισκέπτες ημερησίως, το υποκείμενο των δεδομένων θα πρέπει να διευκρινίσει τη χρονική στιγμή (συν/πλην μία ώρα) κατά την οποία διήλθε από τον υπό παρακολούθηση χώρο. Εάν ο υπεύθυνος επεξεργασίας εξακολουθεί να επεξεργάζεται το υλικό θα πρέπει να παρασχεθεί αντίγραφο του βιντεοσκοπημένου υλικού. Εάν άλλα υποκείμενα των δεδομένων μπορούν να ταυτοποιηθούν στο ίδιο υλικό, ο υπεύθυνος επεξεργασίας θα πρέπει να καταστήσει «ανώνυμο» αυτό το μέρος του υλικού (θολώνοντας π.χ. το αντίγραφο ή μέρη αυτού) προτού παραδώσει το αντίγραφο στο υποκείμενο των δεδομένων που υπέβαλε το αίτημα.

Παράδειγμα: Εάν ο υπεύθυνος επεξεργασίας διαγράφει αυτομάτως το σύνολο του οπτικοακουστικού υλικού, για παράδειγμα εντός 2 ημερών, δεν μπορεί να παραδώσει οπτικοακουστικό υλικό στο υποκείμενο των δεδομένων μετά την παρέλευση των 2 αυτών ημερών. Εάν ο υπεύθυνος επεξεργασίας λάβει αίτημα μετά από τις 2 αυτές ημέρες, το υποκείμενο των δεδομένων θα πρέπει να ενημερωθεί αναλόγως.

97.

- Άρθρο 12 του ΓΚΠΔ, υπερβολικά αιτήματα

98. Σε περίπτωση υπερβολικών ή προδήλως αβάσιμων αιτημάτων από υποκείμενο των δεδομένων, ο υπεύθυνος επεξεργασίας μπορεί είτε να επιβάλει την καταβολή εύλογου τέλους σύμφωνα με το άρθρο 12 παράγραφος 5 στοιχείο α) του ΓΚΠΔ ή να αρνηθεί να δώσει συνέχεια στο αίτημα (άρθρο 12 παράγραφος 5 στοιχείο β) του ΓΚΠΔ). Ο υπεύθυνος επεξεργασίας πρέπει να μπορεί να αποδείξει τον προδήλως αβάσιμο ή υπερβολικό χαρακτήρα του αιτήματος.

6.2 Δικαίωμα διαγραφής και δικαίωμα εναντίωσης

6.2.1 Δικαίωμα διαγραφής («Δικαίωμα στη λήθη»)

99. Εάν ο υπεύθυνος επεξεργασίας συνεχίσει να επεξεργάζεται δεδομένα προσωπικού χαρακτήρα πέρα από την παρακολούθηση σε πραγματικό χρόνο (π.χ. αποθήκευση) το υποκείμενο των δεδομένων μπορεί να ζητήσει τη διαγραφή των δεδομένων προσωπικού χαρακτήρα σύμφωνα με το άρθρο 17 του ΓΚΠΔ.

100. Κατόπιν αιτήματος, ο υπεύθυνος επεξεργασίας υποχρεούται να διαγράψει τα δεδομένα προσωπικού χαρακτήρα χωρίς αδικαιολόγητη καθυστέρηση εφόσον συντρέχει μια από τις περιστάσεις που αναφέρονται στο άρθρο 17 παράγραφος 1 του ΓΚΠΔ (και δεν ισχύει καμία από τις εξαιρέσεις που αναφέρονται στο άρθρο 17 παράγραφος 3 του ΓΚΠΔ). Στο πλαίσιο αυτό προβλέπεται η υποχρέωση διαγραφής δεδομένων προσωπικού χαρακτήρα, όταν αυτά δεν είναι πλέον αναγκαία για τον σκοπό για τον οποίο είχαν αρχικά αποθηκευτεί ή όταν η επεξεργασία είναι παράνομη (βλέπε επίσης *Ενότητα 8 - Περίοδοι αποθήκευσης και υποχρέωση διαγραφής*). Επιπλέον, ανάλογα με τη νομική βάση επεξεργασίας, τα δεδομένα προσωπικού χαρακτήρα θα πρέπει να διαγράφονται:

- *για λόγους συγκατάθεσης*, όταν ανακαλείται η συγκατάθεση (και δεν υπάρχει άλλη νομική βάση για την επεξεργασία)
- για λόγους *έννομου συμφέροντος*:
    - όταν το υποκείμενο των δεδομένων ασκεί το δικαίωμα εναντίωσης (βλέπε *Ενότητα 6.2.2*) και δεν υπερισχύουν άλλοι επιτακτικοί και νόμιμοι λόγοι για την επεξεργασία ή
    - σε περίπτωση άμεσης εμπορικής προώθησης (περιλαμβανομένης της κατάρτισης προφίλ) όταν το υποκείμενο των δεδομένων αντιτίθεται στην επεξεργασία.

101. Εάν ο υπεύθυνος επεξεργασίας έχει δημοσιοποιήσει το βιντεοσκοπημένο υλικό (π.χ. ραδιοτηλεοπτική μετάδοση ή διαδικτυακή μετάδοση συνεχούς ροής), πρέπει να ληφθούν εύλογα μέτρα προκειμένου να ενημερωθούν άλλοι υπεύθυνοι επεξεργασίας (που επίσης επεξεργάζονται τα εν λόγω δεδομένα προσωπικού χαρακτήρα) για το αίτημα σύμφωνα με το άρθρο 17 παράγραφος 2 του ΓΚΠΔ. Τα εύλογα μέτρα θα πρέπει να περιλαμβάνουν τεχνικά μέτρα ενώ πρέπει να λαμβάνεται υπόψη η διαθέσιμη τεχνολογία και το κόστος εφαρμογής. Στον βαθμό του εφικτού, ο υπεύθυνος επεξεργασίας θα πρέπει να ενημερώνει –με τη διαγραφή των δεδομένων προσωπικού χαρακτήρα– κάθε πρόσωπο στο οποίο τα δεδομένα προσωπικού χαρακτήρα γνωστοποιήθηκαν στο παρελθόν, σύμφωνα με το άρθρο 19 του ΓΚΠΔ.

102. Πέρα από την υποχρέωση του υπευθύνου επεξεργασίας να διαγράφει δεδομένα προσωπικού χαρακτήρα κατόπιν αιτήματος του υποκειμένου των δεδομένων, ο υπεύθυνος επεξεργασίας υποχρεούται σύμφωνα με τις γενικές αρχές του ΓΚΠΔ να περιορίσει τα αποθηκευμένα δεδομένα προσωπικού χαρακτήρα (βλέπε *Ενότητα 8*).

103. Όσον αφορά τη βιντεοεπιτήρηση, αξίζει να σημειωθεί ότι όταν π.χ. θολώνεται η εικόνα και δεν υπάρχει πλέον η δυνατότητα να ανακτηθούν τα δεδομένα προσωπικού χαρακτήρα που περιείχε προηγουμένως η εικόνα, τα δεδομένα προσωπικού χαρακτήρα θεωρείται ότι έχουν διαγραφεί σύμφωνα με τον ΓΚΠΔ.

Παράδειγμα: Παντοπωλείο αντιμετωπίζει προβλήματα βανδαλισμού, ιδίως στον εξωτερικό του χώρο, και για τον λόγο αυτό επιτηρείται η είσοδός του μέσω καμερών που έχουν τοποθετηθεί στους τοίχους εξωτερικά του καταστήματος. Διερχόμενος ζητεί, από εκείνη τη στιγμή και μετά, τη διαγραφή όλων των δεδομένων προσωπικού χαρακτήρα που τον αφορούν. Ο υπεύθυνος επεξεργασίας είναι υποχρεωμένος να ανταποκριθεί στο αίτημα χωρίς αδικαιολόγητη καθυστέρηση και το αργότερο εντός ενός μηνός. Εφόσον το εν λόγω οπτικοακουστικό υλικό δεν υπηρετεί πλέον τον σκοπό για τον οποίο είχε αρχικά αποθηκευτεί (δεν συνέβη βανδαλισμός κατά τον χρόνο διέλευσης του υποκειμένου των δεδομένων), δεν υπάρχει, τη στιγμή του αιτήματος, έννομο συμφέρον αποθήκευσης των δεδομένων που να υπερισχύει των συμφερόντων των υποκειμένων των δεδομένων. Ο υπεύθυνος επεξεργασίας πρέπει να διαγράψει τα δεδομένα προσωπικού χαρακτήρα.

104.

6.2.2 Δικαίωμα εναντίωσης

105. Όσον αφορά τη βιντεοεπιτήρηση που βασίζεται σε *έννομο συμφέρον* (άρθρο 6 παράγραφος 1 στοιχείο στ) του ΓΚΠΔ) ή την ανάγκη εκπλήρωσης καθήκοντος που εκτελείται προς το *δημόσιο συμφέρον* (άρθρο 6 παράγραφος 1 στοιχείο ε) του ΓΚΠΔ) το υποκείμενο των δεδομένων έχει το δικαίωμα –ανά πάσα στιγμή– να εναντιωθεί, για λόγους που αφορούν την ιδιαίτερή του κατάσταση, στην επεξεργασία σύμφωνα με το άρθρο 21 του ΓΚΠΔ. Αν ο υπεύθυνος επεξεργασίας δεν αποδείξει ότι συντρέχουν επιτακτικοί και νόμιμοι λόγοι που υπερισχύουν των δικαιωμάτων και των συμφερόντων του υποκειμένου των δεδομένων, η επεξεργασία των δεδομένων του ατόμου που προέβαλε αντίρρηση πρέπει να σταματήσει. Ο υπεύθυνος επεξεργασίας είναι υποχρεωμένος να ανταποκριθεί σε αιτήματα που υποβάλλει το υποκείμενο των δεδομένων χωρίς αδικαιολόγητη καθυστέρηση και το αργότερο εντός ενός μηνός.

106. Στο πλαίσιο της βιντεοεπιτήρησης, αυτή η αντίρρηση θα μπορούσε να διατυπωθεί κατά την είσοδο στον παρακολουθούμενο χώρο, κατά τη διάρκεια της παραμονής σε αυτόν ή μετά την αποχώρηση από αυτόν. Στην πράξη, αυτό σημαίνει ότι, εάν ο υπεύθυνος επεξεργασίας δεν έχει επιτακτικούς και νόμιμους λόγους, η παρακολούθηση χώρου κατά την οποία μπορεί να εξακριβωθεί η ταυτότητα φυσικών προσώπων είναι νόμιμη μόνον εάν

    (1) ο υπεύθυνος επεξεργασίας μπορεί να σταματήσει αμέσως την κάμερα από την επεξεργασία δεδομένων προσωπικού χαρακτήρα όταν λάβει σχετικό αίτημα, ή

    (2) η πρόσβαση στον παρακολουθούμενο χώρο είναι πολύ αυστηρά ελεγχόμενη ώστε ο υπεύθυνος επεξεργασίας να μπορεί να διασφαλίσει την έγκριση του υποκειμένου των δεδομένων πριν το υποκείμενο των δεδομένων εισέλθει στον χώρο και εφόσον δεν πρόκειται για χώρο στον οποίο το υποκείμενο των δεδομένων έχει δικαίωμα πρόσβασης ως πολίτης.

107. Οι παρούσες κατευθυντήριες γραμμές δεν έχουν σκοπό να προσδιορίσουν τι θεωρείται *επιτακτικό* έννομο συμφέρον (άρθρο 21 του ΓΚΠΔ).

108. Όταν χρησιμοποιείται βιντεοεπιτήρηση για τους σκοπούς της άμεσης εμπορικής προώθησης, το υποκείμενο των δεδομένων έχει το δικαίωμα να εναντιωθεί στην επεξεργασία κατά τη διακριτική του ευχέρεια, καθώς το δικαίωμα εναντίωσης είναι απόλυτο σε αυτό το πλαίσιο (άρθρο 21 παράγραφοι 2 και 3 του ΓΚΠΔ).

Παράδειγμα: Εταιρεία αντιμετωπίζει δυσκολίες λόγω της παραβίασης της ασφάλειας της δημόσιας εισόδου της και, επικαλούμενη το έννομο συμφέρον της, χρησιμοποιεί σύστημα βιντεοεπιτήρησης προκειμένου να συλλαμβάνονται τα άτομα που εισέρχονται παράνομα. Επισκέπτης της εταιρείας εναντιώνεται στην επεξεργασία των δεδομένων που τον αφορούν μέσω του συστήματος βιντεοεπιτήρησης για λόγους που σχετίζονται με την ιδιαίτερή του κατάσταση. Η εταιρεία ωστόσο σε αυτήν την περίπτωση απορρίπτει το αίτημα με το σκεπτικό ότι το αποθηκευμένο οπτικοακουστικό υλικό είναι αναγκαίο λόγω εσωτερικής έρευνας που είναι σε εξέλιξη. Ως εκ τούτου, η εταιρεία έχει επιτακτικούς και νόμιμους λόγους να συνεχίσει να επεξεργάζεται τα δεδομένα προσωπικού χαρακτήρα.

109.

7 ΥΠΟΧΡΕΩΣΕΙΣ ΔΙΑΦΑΝΕΙΑΣ ΚΑΙ ΠΛΗΡΟΦΟΡΗΣΗΣ[18]

110. Η ευρωπαϊκή νομοθεσία για την προστασία των δεδομένων είναι επί μακρόν συνυφασμένη με την αρχή ότι τα υποκείμενα των δεδομένων θα πρέπει να γνωρίζουν ότι λειτουργεί σύστημα βιντεοεπιτήρησης. Τα άτομα πρέπει να ενημερώνονται λεπτομερώς όσον αφορά τους χώρους που παρακολουθούνται[19]. Στο πλαίσιο του ΓΚΠΔ οι γενικές υποχρεώσεις διαφάνειας και πληροφόρησης ορίζονται στο άρθρο 12 του ΓΚΠΔ και επόμενα. Οι «Κατευθυντήριες γραμμές σχετικά με τη διαφάνεια βάσει του κανονισμού 2016/679 (WP260)» της Ομάδας εργασίας του άρθρου 29 που εγκρίθηκαν από το ΕΣΠΔ στις 25 Μαΐου 2018 περιλαμβάνουν περαιτέρω λεπτομέρειες. Σύμφωνα με τις κατευθυντήριες γραμμές WP260 παρ. 26, εφαρμόζεται το άρθρο 13 του ΓΚΠΔ εάν τα δεδομένα προσωπικού χαρακτήρα συλλέγονται «[...] από ένα υποκείμενο των δεδομένων μέσω παρατήρησης (π.χ. χρησιμοποιώντας συσκευές καταγραφής δεδομένων ή λογισμικό καταγραφής δεδομένων όπως κάμερες [...]».

111. Με βάση τον όγκο πληροφοριών που απαιτείται να παρασχεθούν στο υποκείμενο των δεδομένων, οι υπεύθυνοι επεξεργασίας δεδομένων μπορούν να ακολουθούν μια προσέγγιση πολλαπλών επιπέδων όταν επιλέγουν να χρησιμοποιήσουν έναν συνδυασμό μεθόδων για την εξασφάλιση διαφάνειας (έγγραφο WP260, παρ. 35, έγγραφο WP89, παρ. 22). Όσον αφορά τη βιντεοεπιτήρηση, οι πιο σημαντικές πληροφορίες θα πρέπει να αναγράφονται στην προειδοποιητική πινακίδα σήμανσης (πρώτο επίπεδο) ενώ οι συμπληρωματικές υποχρεωτικές πληροφορίες μπορούν να παρέχονται με άλλα μέσα (δεύτερο επίπεδο).

7.1 Πληροφορίες πρώτου επιπέδου (προειδοποιητική πινακίδα σήμανσης)

112. Το πρώτο επίπεδο αφορά τον κύριο τρόπο με τον οποίο ο υπεύθυνος επεξεργασίας επικοινωνεί σε πρώτο στάδιο με το υποκείμενο των δεδομένων. Σε αυτό το στάδιο, οι υπεύθυνοι επεξεργασίας έχουν τη δυνατότητα να χρησιμοποιήσουν προειδοποιητική πινακίδα σήμανσης που περιλαμβάνει τις σχετικές πληροφορίες. Οι πληροφορίες αυτές μπορούν να παρέχονται σε συνδυασμό με εικονίδια προκειμένου να δίνεται με ευδιάκριτο, κατανοητό και ευανάγνωστο τρόπο μια ουσιαστική επισκόπηση της σκοπούμενης επεξεργασίας (άρθρο 12 παράγραφος 7 του ΓΚΠΔ). Οι διαστάσεις των ενημερωτικών πινακίδων πρέπει να είναι ανάλογες των χώρων (έγγραφο WP89 παρ. 22).

7.1.1 Τοποθέτηση της προειδοποιητικής πινακίδας σήμανσης

113. Η προειδοποιητική πινακίδα σήμανσης θα πρέπει να είναι τοποθετημένη κατά τρόπο ώστε το υποκείμενο των δεδομένων να μπορεί εύκολα να αναγνωρίζει τις συνθήκες της βιντεοεπιτήρησης προτού εισέλθει στον παρακολουθούμενο χώρο (περίπου στο επίπεδο των ματιών). Δεν είναι υποχρεωτικό να αποκαλύπτεται η θέση της κάμερας εφόσον δεν υπάρχει αμφιβολία ως προς το ποιες περιοχές υπόκεινται σε παρακολούθηση και εφόσον οι συνθήκες της επιτήρησης διευκρινίζονται με σαφήνεια (έγγραφο WP89, παρ. 22). Το υποκείμενο των δεδομένων πρέπει να είναι σε θέση να εκτιμήσει ποια περιοχή υπόκειται σε παρακολούθηση από κάμερα ώστε να είναι σε θέση να αποφύγει την επιτήρηση ή να προσαρμόσει τη συμπεριφορά του εάν είναι απαραίτητο.

7.1.2 Περιεχόμενο του πρώτου επιπέδου

114. Το πρώτο επίπεδο σήμανσης (προειδοποιητική πινακίδα σήμανσης) θα πρέπει σε γενικές γραμμές να παρέχει τις πλέον σημαντικές πληροφορίες, όπως τις λεπτομέρειες των σκοπών της επεξεργασίας,

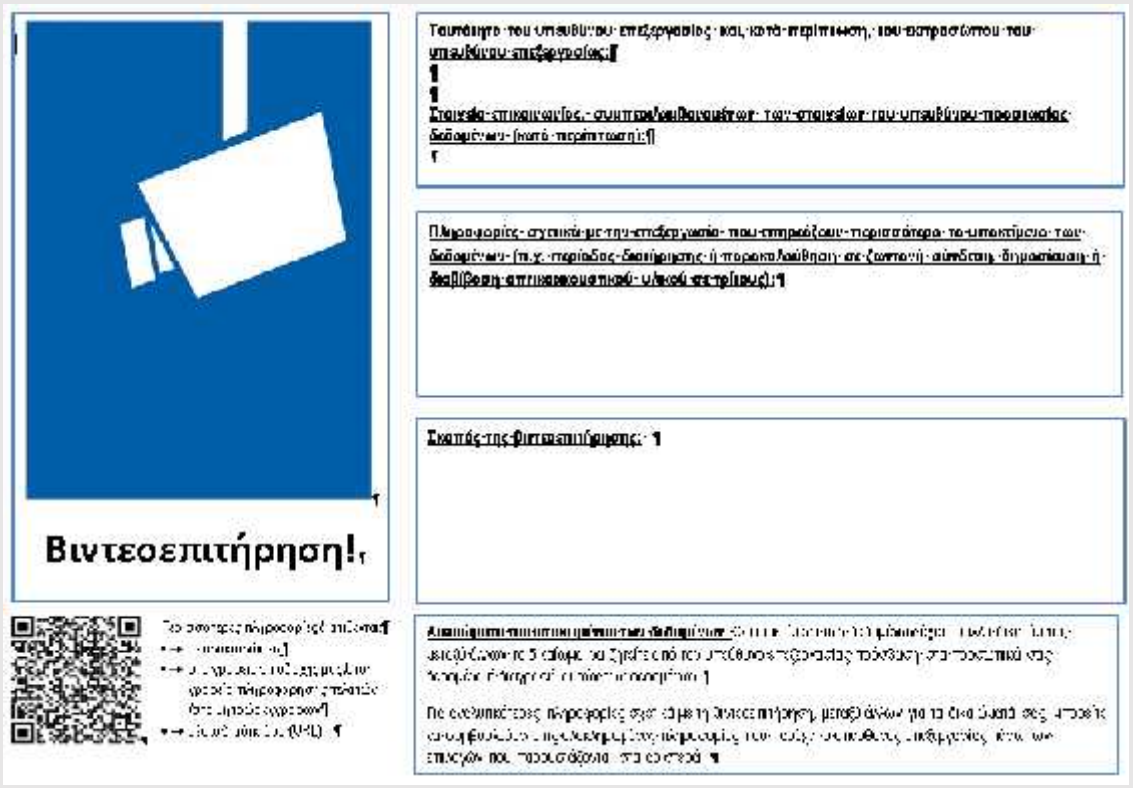
[18] Ειδικές απαιτήσεις ενδέχεται να ισχύουν σύμφωνα με την εθνική νομοθεσία.

[19] Βλέπε έγγραφο WP89, Γνωμοδότηση 4/2004 για την επεξεργασία προσωπικών δεδομένων μέσω βιντεοεπιτήρησης της Ομάδας εργασίας του άρθρου 29.

την ταυτότητα του υπευθύνου επεξεργασίας και την ύπαρξη των δικαιωμάτων του υποκειμένου των δεδομένων, μαζί με πληροφορίες σχετικά με την επεξεργασία που θα έχει τον μεγαλύτερο αντίκτυπο[20]. Στο πλαίσιο αυτό μπορούν π.χ. να αναφέρονται τα έννομα συμφέροντα στα οποία βασίζεται ο υπεύθυνος επεξεργασίας (ή τρίτος) και τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων (κατά περίπτωση). Επιπλέον, πρέπει να γίνεται λεπτομερέστερη αναφορά στο δεύτερο επίπεδο πληροφοριών, και συγκεκριμένα αναφορά σχετικά με τον τόπο και τον τρόπο πρόσβασης σε αυτές τις πληροφορίες.

115. Επιπλέον, η πινακίδα θα πρέπει να περιλαμβάνει κάθε πληροφορία που θα μπορούσε να προκαλέσει έκπληξη στο υποκείμενο των δεδομένων (WP260, παρ. 38). Τέτοιες πληροφορίες είναι π.χ. η διαβίβαση σε τρίτους, ιδίως εάν βρίσκονται εκτός της ΕΕ, ακόμα και η περίοδος αποθήκευσης. Εάν οι πληροφορίες αυτές δεν αναγράφονται, τότε το φυσικό πρόσωπο θα μπορεί ευλόγως να υποθέσει ότι η παρακολούθηση γίνεται μόνο σε πραγματικό χρόνο (χωρίς καταγραφή δεδομένων ή διαβίβαση σε τρίτους).

Παράδειγμα (μη δεσμευτική πρόταση):



116.

7.2 Πληροφόρηση δεύτερου επιπέδου

117. Οι πληροφορίες δεύτερου επιπέδου πρέπει επίσης να παρουσιάζονται σε χώρο με εύκολη πρόσβαση για το υποκείμενο των δεδομένων. Μεταξύ άλλων, οι πληροφορίες μπορούν να παρουσιάζονται σε πλήρες ενημερωτικό φυλλάδιο που διανέμεται σε κεντρική τοποθεσία (π.χ. γραφείο πληροφοριών, υποδοχή ή ταμείο) ή να προβάλλονται σε εύκολα προσβάσιμη αφίσα. Όπως προαναφέρθηκε, στην προειδοποιητική πινακίδα σήμανσης του πρώτου επιπέδου πρέπει να γίνεται ρητή αναφορά στην πληροφόρηση δεύτερου επιπέδου. Επιπλέον, είναι προτιμότερο η πληροφόρηση πρώτου επιπέδου

[20] Βλέπε έγγραφο WP260, παρ. 38.

να παραπέμπει στην ψηφιακή πηγή του δεύτερου επιπέδου (π.χ. QR-κώδικας ή διεύθυνση ιστοσελίδας). Ωστόσο, οι πληροφορίες θα πρέπει να είναι εύκολα διαθέσιμες και σε μη ψηφιακή μορφή. Το υποκείμενο των δεδομένων θα πρέπει να μπορεί να αποκτήσει πρόσβαση στην πληροφόρηση δεύτερου επιπέδου χωρίς να εισέλθει στον επιτηρούμενο χώρο, εάν μάλιστα οι πληροφορίες παρέχονται ψηφιακά (η προσθήκη συνδέσμου θα βοηθούσε προς την κατεύθυνση αυτή). Άλλο πρόσφορο μέσο είναι και η χρήση ειδικού τηλεφωνικού αριθμού. Όπως και να παρέχονται οι πληροφορίες, πρέπει να περιλαμβάνουν όλα τα στοιχεία που είναι υποχρεωτικά σύμφωνα με το άρθρο 13 του ΓΚΠΔ.

118. Πέραν αυτών των επιλογών, και με γνώμονα την αύξηση της αποτελεσματικότητας, το ΕΣΠΔ ενθαρρύνει τη χρήση τεχνολογικών μέσων για την πληροφόρηση των υποκειμένων των δεδομένων. Στα μέσα αυτά μπορεί να περιλαμβάνονται για παράδειγμα οι κάμερες εντοπισμού γεωγραφικής θέσης και η προσθήκη πληροφοριών σε εφαρμογές ή δικτυακούς τόπους χαρτογράφησης ώστε οι ενδιαφερόμενοι να μπορούν εύκολα, αφενός, να εντοπίζουν και να διευκρινίζουν τις πηγές βίντεο που σχετίζονται με την άσκηση των δικαιωμάτων τους, και αφετέρου, να λαμβάνουν αναλυτικότερες πληροφορίες για τη διαδικασία της επεξεργασίας.

> Παράδειγμα: Καταστηματάρχης παρακολουθεί το κατάστημά του. Για να συμμορφωθεί με το άρθρο 13 αρκεί να τοποθετήσει προειδοποιητική πινακίδα σήμανσης σε ευδιάκριτο σημείο της εισόδου του καταστήματός του με τις πληροφορίες του πρώτου επιπέδου. Επιπλέον, πρέπει να διανέμει ενημερωτικό φυλλάδιο με τις πληροφορίες δεύτερου επιπέδου στο ταμείο ή σε άλλο κεντρικό και εύκολα προσβάσιμο σημείο στο κατάστημά του.

119.

8 ΠΕΡΙΟΔΟΙ ΑΠΟΘΗΚΕΥΣΗΣ ΚΑΙ ΥΠΟΧΡΕΩΣΗ ΔΙΑΓΡΑΦΗΣ

120. Τα δεδομένα προσωπικού χαρακτήρα δεν επιτρέπεται να αποθηκεύονται για διάστημα μεγαλύτερο από ό,τι είναι αναγκαίο για τους σκοπούς για τους οποίους γίνεται η επεξεργασία των δεδομένων προσωπικού χαρακτήρα (άρθρο 5 παράγραφος 1 στοιχεία γ) και ε) του ΓΚΠΔ). Σε ορισμένα κράτη μέλη, ενδέχεται να υφίστανται ειδικές διατάξεις για τις περιόδους αποθήκευσης όσον αφορά τη βιντεοεπιτήρηση σύμφωνα με το άρθρο 6 παράγραφος 2 του ΓΚΠΔ.

121. Το κατά πόσον είναι αναγκαία η αποθήκευση των δεδομένων προσωπικού χαρακτήρα ή όχι θα πρέπει να ελέγχεται το συντομότερο δυνατό. Γενικά, νόμιμοι σκοποί για τη βιντεοεπιτήρηση είναι συχνά η προστασία της περιουσίας ή η διατήρηση αποδεικτικών στοιχείων. Συνήθως οι ζημίες που σημειώνονται μπορούν να αναγνωριστούν εντός μίας ή δύο ημερών. Για να διευκολυνθεί η απόδειξη της συμμόρφωσης με το πλαίσιο προστασίας των δεδομένων, είναι προς το συμφέρον του υπευθύνου επεξεργασίας να προβαίνει εκ των προτέρων σε οργανωτικές ρυθμίσεις (π.χ. να ορίζει, εφόσον είναι αναγκαίο, εκπρόσωπο για τη διαλογή και την προστασία του βιντεοσκοπημένου υλικού). Λαμβάνοντας υπόψη τις αρχές του άρθρου 5 παράγραφος 1 στοιχεία γ) και ε) του ΓΚΠΔ, και ιδίως την ελαχιστοποίηση δεδομένων και τους περιορισμούς αποθήκευσης, τα δεδομένα προσωπικού χαρακτήρα θα πρέπει στις περισσότερες περιπτώσεις (π.χ. για τον σκοπό του εντοπισμού βανδαλισμών) να διαγράφονται, ιδανικά αυτομάτως, έπειτα από μερικές ημέρες. Όσο μεγαλύτερη είναι η καθορισμένη περίοδος αποθήκευσης (ιδίως όταν αυτή υπερβαίνει τις 72 ώρες) τόσο περισσότερα επιχειρήματα πρέπει να προβάλλονται υπέρ της νομιμότητας του σκοπού και της αναγκαιότητας της αποθήκευσης. Εάν ο υπεύθυνος επεξεργασίας δεν χρησιμοποιεί τη βιντεοεπιτήρηση μόνο για την παρακολούθηση των εγκαταστάσεών του, αλλά σκοπεύει επίσης να αποθηκεύσει τα δεδομένα, πρέπει να διασφαλίσει ότι η αποθήκευση αυτή είναι πραγματικά αναγκαία για την επίτευξη του σκοπού. Αν η αποθήκευση είναι όντως αναγκαία, η περίοδος αποθήκευσης πρέπει να καθορίζεται σαφώς και μεμονωμένα για κάθε ιδιαίτερο σκοπό. Είναι ευθύνη του υπευθύνου επεξεργασίας να καθορίζει την περίοδο διατήρησης σύμφωνα με τις αρχές της αναγκαιότητας και της αναλογικότητας και να αποδεικνύει τη συμμόρφωση με τις διατάξεις του ΓΚΠΔ.

Παράδειγμα: Μια πράξη βανδαλισμού γίνεται συνήθως αντιληπτή από ιδιοκτήτη μικρού καταστήματος την ίδια ημέρα. Συνεπώς, η συνήθης περίοδος αποθήκευσης των 24 ωρών είναι επαρκής. Αν ωστόσο μεσολαβεί Σαββατοκύριακο ή μεγαλύτερη περίοδος αργίας, είναι λογικό η περίοδος αποθήκευσης να επιμηκυνθεί. Αν ο ιδιοκτήτης εντοπίσει ζημιά μπορεί επίσης να χρειαστεί να αποθηκεύσει το βιντεοσκοπημένο υλικό για μεγαλύτερη περίοδο προκειμένου να προσφύγει νομικά κατά του δράστη.

122.

9 ΤΕΧΝΙΚΑ ΚΑΙ ΟΡΓΑΝΩΤΙΚΑ ΜΕΤΡΑ

123. Όπως αναφέρεται στο άρθρο 32 παράγραφος 1 του ΓΚΠΔ, η επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τη βιντεοεπιτήρηση δεν πρέπει μόνο να είναι νομικά επιτρεπτή αλλά ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία πρέπει επίσης να τη διασφαλίζουν επαρκώς. Τα εφαρμοζόμενα **οργανωτικά και τεχνικά μέτρα** πρέπει να είναι **ανάλογα προς τους κινδύνους για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων**. Οι κίνδυνοι αυτοί απορρέουν από την τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, άνευ αδείας κοινολόγηση ή προσπέλαση δεδομένων προσωπικού χαρακτήρα που προέκυψαν μέσω βιντεοεπιτήρησης. Σύμφωνα με τα άρθρα 24 και 25 του ΓΚΠΔ, οι υπεύθυνοι επεξεργασίας πρέπει να εφαρμόζουν τεχνικά και οργανωτικά μέτρα προκειμένου να διαφυλάσσουν όλες τις αρχές προστασίας δεδομένων στη διάρκεια της επεξεργασίας

και να θεσπίζουν μέσα βάσει των οποίων τα υποκείμενα των δεδομένων μπορούν να ασκήσουν τα δικαιώματά τους όπως ορίζεται στα άρθρα 15-22 του ΓΚΠΔ. Οι υπεύθυνοι επεξεργασίας δεδομένων θα πρέπει να θεσπίζουν εσωτερικό πλαίσιο και πολιτικές που διασφαλίζουν αυτήν την εφαρμογή τόσο κατά τη στιγμή του καθορισμού των μέσων επεξεργασίας όσο και κατά τη στιγμή της επεξεργασίας, διενεργώντας μεταξύ άλλων εκτιμήσεις αντικτύπου σχετικά με την προστασία δεδομένων, εφόσον κρίνεται αναγκαίο.

9.1 Επισκόπηση του συστήματος βιντεοεπιτήρησης

124. Το σύστημα βιντεοεπιτήρησης (video surveillance system - VSS)[21] αποτελείται από αναλογικές και ψηφιακές συσκευές καθώς και από λογισμικό, και έχει σκοπό την απεικόνιση σκηνών, τη διαχείριση των εικόνων και την εμφάνισή τους στον χειριστή. Τα στοιχεία από τα οποία αποτελείται το σύστημα ταξινομούνται στις ακόλουθες κατηγορίες:

- Περιβάλλον βίντεο: απεικόνιση, διασυνδέσεις και διαχείριση εικόνων:
  - σκοπός της απεικόνισης είναι η δημιουργία εικόνας του πραγματικού κόσμου σε τέτοια μορφή που να μπορεί να χρησιμοποιηθεί από το υπόλοιπο σύστημα,
  - οι διασυνδέσεις περιγράφουν το σύνολο της διαβίβασης δεδομένων εντός του περιβάλλοντος βίντεο, δηλ. συνδέσεις και επικοινωνία. Παραδείγματα συνδέσεων είναι τα καλώδια, τα ψηφιακά δίκτυα και η ασύρματη διαβίβαση. Οι επικοινωνίες περιγράφουν όλα τα σήματα δεδομένων βίντεο και ελέγχου που θα μπορούσαν να είναι αναλογικά ή ψηφιακά,
  - η διαχείριση εικόνων περιλαμβάνει την ανάλυση, αποθήκευση και παρουσίαση εικόνας ή σειράς εικόνων.
- Από την οπτική της διαχείρισης του συστήματος, το σύστημα VSS επιτελεί τις ακόλουθες λογικές λειτουργίες:
  - διαχείριση δεδομένων και διαχείριση δραστηριοτήτων, η οποία περιλαμβάνει τη διαχείριση εντολών του χειριστή και των δραστηριοτήτων που παράγει το σύστημα (διαδικασίες συναγερμού, προειδοποίηση των χειριστών),
  - οι διεπαφές με άλλα συστήματα μπορεί να συμπεριλαμβάνουν τη σύνδεση με άλλα συστήματα ασφαλείας (έλεγχος πρόσβασης, συναγερμός πυρκαγιάς) ή μη ασφαλείας (συστήματα διαχείρισης κτιρίων, αυτόματη αναγνώριση πινακίδων κυκλοφορίας).
- Η ασφάλεια των συστημάτων VSS συνίσταται στην εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα του συστήματος και των δεδομένων:
  - η ασφάλεια του συστήματος περιλαμβάνει τη φυσική ασφάλεια όλων των στοιχείων του συστήματος και τον έλεγχο πρόσβασης στο σύστημα VSS,
  - η ασφάλεια των δεδομένων περιλαμβάνει την αποτροπή απώλειας ή αθέμιτης χρήσης των δεδομένων.

[21] Ο ΓΚΠΔ δεν περιλαμβάνει τον ορισμό του, ωστόσο τεχνικός ορισμός διατίθεται για παράδειγμα στο έγγραφο «EN 62676-1-1:2014 Video surveillance systems for use in security applications – Part 1-1: Video system requirements».

125.

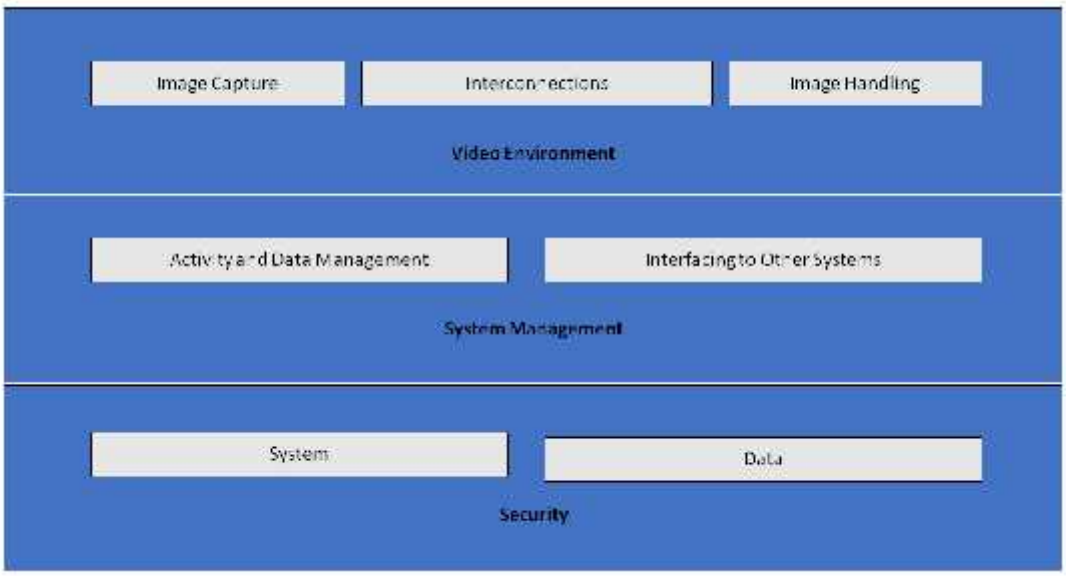


Image Capture	Απεικόνιση
Interconnections	Διασυνδέσεις
Image Handling	Διαχείριση εικόνων
Video Environment	Περιβάλλον βίντεο
Activity and Data Management	Διαχείριση δεδομένων και δραστηριοτήτων
Interfacing to Other Systems	Διεπαφή με άλλα συστήματα
System Management	Διαχείριση συστήματος
System	Σύστημα
Data	Δεδομένα
Security	Ασφάλεια

Σχήμα 1- σύστημα βιντεοεπιτήρησης

9.2 Προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού

126. Όπως αναφέρεται στο άρθρο 25 του ΓΚΠΔ, οι υπεύθυνοι επεξεργασίας πρέπει να εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα προστασίας των δεδομένων από τη στιγμή που προγραμματίζουν τη βιντεοεπιτήρηση – προτού ξεκινήσουν τη συλλογή και επεξεργασία βιντεοσκοπημένου υλικού. Αυτές οι αρχές αναδεικνύουν την ανάγκη χρησιμοποίησης ενσωματωμένων τεχνολογιών που ενισχύουν την ιδιωτικότητα, την ανάγκη χρήσης των προεπιλεγμένων ρυθμίσεων που ελαχιστοποιούν την επεξεργασία δεδομένων καθώς και την ανάγκη απόκτησης των αναγκαίων εργαλείων που θα επιτρέψουν τη μεγαλύτερη δυνατή προστασία των δεδομένων προσωπικού χαρακτήρα[22].

127. Οι υπεύθυνοι επεξεργασίας πρέπει να αναπτύξουν συστήματα προστασίας δεδομένων και προστασίας της ιδιωτικής ζωής όχι μόνο στις προδιαγραφές σχεδιασμού της τεχνολογίας αλλά και στις οργανωτικές τους πρακτικές. Όσον αφορά τις οργανωτικές πρακτικές, οι υπεύθυνοι επεξεργασίας θα πρέπει να θεσπίζουν κατάλληλο πλαίσιο διαχείρισης, να καθορίζουν και να εφαρμόζουν πολιτικές

[22] Έγγραφο WP 168, Γνώμη σχετικά με «Το μέλλον της προστασίας της ιδιωτικής ζωής», κοινή συνεισφορά της Ομάδας εργασίας του άρθρου 29 για την προστασία δεδομένων και της Ομάδας εργασίας για την αστυνομία και τη δικαιοσύνη στη διαβούλευση της Ευρωπαϊκής Επιτροπής σχετικά με το νομικό πλαίσιο για το θεμελιώδες δικαίωμα προστασίας των δεδομένων προσωπικού χαρακτήρα (εκδόθηκε την 1η Δεκεμβρίου 2009).

και διαδικασίες σχετικά με τη βιντεοεπιτήρηση. Από τεχνική άποψη, οι προδιαγραφές και ο σχεδιασμός του συστήματος θα πρέπει να περιλαμβάνουν απαιτήσεις για την επεξεργασία δεδομένων προσωπικού χαρακτήρα σύμφωνα με τις αρχές που ορίζονται στο άρθρο 5 του ΓΚΠΔ (νομιμότητα της επεξεργασίας, σκοπός και περιορισμός δεδομένων, ελαχιστοποίηση δεδομένων εξ ορισμού υπό την έννοια του άρθρου 25 παράγραφος 2 του ΓΚΠΔ, ακεραιότητα και εμπιστευτικότητα, λογοδοσία κ.λπ.). Σε περίπτωση που ο υπεύθυνος επεξεργασίας σχεδιάζει να αποκτήσει εμπορικό σύστημα βιντεοεπιτήρησης, πρέπει να συμπεριλάβει αυτές τις απαιτήσεις στις προδιαγραφές της αγοράς. Ο υπεύθυνος επεξεργασίας πρέπει να διασφαλίσει τη συμμόρφωση με αυτές τις απαιτήσεις, εφαρμόζοντας τις απαιτήσεις σε όλα τα στοιχεία του συστήματος και σε όλα τα δεδομένα που αυτό επεξεργάζεται, σε ολόκληρη τη διάρκεια του κύκλου ζωής του.

9.3 Συγκεκριμένα παραδείγματα σχετικών μέτρων

128. Τα περισσότερα από τα μέτρα που μπορούν να χρησιμοποιηθούν για την προστασία της βιντεοεπιτήρησης, ειδικά όταν χρησιμοποιείται ψηφιακός εξοπλισμός και λογισμικό, δεν διαφέρουν από τα μέτρα που χρησιμοποιούνται σε άλλα συστήματα τεχνολογίας πληροφοριών. Ωστόσο, ανεξάρτητα από τη λύση που επιλέγεται, ο υπεύθυνος επεξεργασίας πρέπει να προστατεύει επαρκώς όλα τα στοιχεία του συστήματος βιντεοεπιτήρησης και τα δεδομένα σε όλα τα στάδια, δηλ. κατά την αποθήκευση (δεδομένα σε αδράνεια), τη μετάδοση (δεδομένα σε διαμετακόμιση) και την επεξεργασία (δεδομένα σε χρήση). Για αυτόν τον σκοπό, είναι απαραίτητο οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία να συνδυάζουν οργανωτικά και τεχνικά μέτρα.

129. Όταν επιλέγει τεχνικές λύσεις, ο υπεύθυνος επεξεργασίας θα πρέπει να εξετάζει τη χρήση τεχνολογιών φιλικών προς την ιδιωτικότητα επειδή, μεταξύ άλλων, οι εν λόγω τεχνολογίες ενισχύουν την ασφάλεια. Παραδείγματα τέτοιων τεχνολογιών είναι τα συστήματα που επιτρέπουν την απόκρυψη ή την αλλοίωση χώρων που δε σχετίζονται με την επιτήρηση, ή τα συστήματα που επιτρέπουν την αφαίρεση εικόνων τρίτων ατόμων όταν παρέχεται βιντεοσκοπημένο υλικό σε υποκείμενα των δεδομένων[23]. Από την άλλη πλευρά, οι επιλεγόμενες λύσεις δεν θα πρέπει να παρέχουν λειτουργίες που δεν είναι αναγκαίες (π.χ. απεριόριστη κίνηση της κάμερας, δυνατότητα μεταβολής εστιακής απόστασης/zoom, ραδιομετάδοσης, ανάλυση και εγγραφές ήχου). Οι παρεχόμενες λειτουργίες που δεν είναι αναγκαίες πρέπει να απενεργοποιούνται.

130. Υπάρχει μεγάλη βιβλιογραφία σχετικά με το θέμα αυτό, μεταξύ άλλων διεθνή πρότυπα και τεχνικές προδιαγραφές για τη φυσική ασφάλεια των πολυμεσικών συστημάτων[24]και την ασφάλεια των πληροφοριακών συστημάτων γενικά[25]. Ως εκ τούτου, στην παρούσα ενότητα παρουσιάζονται μόνο συνοπτικά οι βασικές πτυχές του θέματος.

9.3.1 Οργανωτικά μέτρα

131. Πέρα από τη δυνητική ανάγκη για διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων (βλέπε Ενότητα 10), οι υπεύθυνοι επεξεργασίας θα πρέπει να εξετάζουν τα ακόλουθα θέματα όταν δημιουργούν δικές τους πολιτικές και διαδικασίες βιντεοεπιτήρησης:

---

[23] Η χρήση τέτοιων τεχνολογιών ενδέχεται να είναι ακόμη και υποχρεωτική σε ορισμένες περιπτώσεις προκειμένου να εξασφαλίζεται η συμμόρφωση με το άρθρο 5 παράγραφος 1 στοιχείο γ). Σε κάθε περίπτωση, οι τεχνολογίες αυτές μπορούν να αποτελέσουν παραδείγματα βέλτιστης πρακτικής.

[24] IEC TS 62045 — Multimedia security - Guideline for privacy protection of equipment and systems in and out of use.

[25] ISO/IEC 27000 — Information security management systems series.

- Ποιος είναι υπεύθυνος για τη διαχείριση και τον χειρισμό του συστήματος βιντεοεπιτήρησης.
- Σκοπός και πεδίο εφαρμογής του σχεδίου βιντεοεπιτήρησης.
- Ενδεδειγμένη και απαγορευμένη χρήση (πότε και πού επιτρέπεται η βιντεοεπιτήρηση και πότε και πού δεν επιτρέπεται, π.χ. χρήση κρυφών καμερών και ήχου επιπλέον της βιντεοσκόπησης)[26].
- Μέτρα διαφάνειας όπως αναφέρονται στην Ενότητα 7 *(Υποχρεώσεις διαφάνειας και πληροφόρησης)*.
- Πώς γίνεται η βιντεοσκόπηση και για πόση διάρκεια –συμπεριλαμβάνεται εν προκειμένω η αποθήκευση σε αρχείο βιντεοσκοπημένου υλικού που αφορά συμβάντα ασφάλειας.
- Ποιος πρέπει να λάβει σχετική κατάρτιση και πότε.
- Ποιος έχει πρόσβαση στο βιντεοσκοπημένο υλικό και για ποιους σκοπούς.
- Επιχειρησιακές διαδικασίες (π.χ. από ποιον και από πού παρακολουθείται η βιντεοεπιτήρηση, τι πρέπει να γίνει σε περίπτωση συμβάντος παραβίασης δεδομένων).
- Ποιες διαδικασίες πρέπει να ακολουθούν εξωτερικά μέρη προκειμένου να ζητήσουν βιντεοσκοπημένο υλικό και διαδικασίες απόρριψης ή αποδοχής τέτοιων αιτημάτων.
- Διαδικασίες προμήθειας, εγκατάστασης και συντήρησης συστημάτων VSS.
- Διαχείριση συμβάντων και διαδικασίες αποκατάστασης.

9.3.2 Τεχνικά μέτρα

132. **Ασφάλεια συστήματος** σημαίνει **φυσική ασφάλεια** όλων των εξαρτημάτων του συστήματος και ακεραιότητα συστήματος, δηλαδή **προστασία και ανθεκτικότητα σε περίπτωση σκόπιμης ή ακούσιας παρεμπόδισης των κανονικών λειτουργιών** και **ελέγχου της πρόσβασης**. Ασφάλεια δεδομένων σημαίνει **εμπιστευτικότητα** (τα δεδομένα είναι προσπελάσιμα μόνο σε όσους έχει παραχωρηθεί πρόσβαση), **ακεραιότητα** (προλαμβάνεται η απώλεια ή η παραποίηση δεδομένων) και **διαθεσιμότητα** (τα δεδομένα είναι προσπελάσιμα όταν απαιτείται).

133. Η **φυσική ασφάλεια** είναι ζωτικό μέρος της προστασίας δεδομένων και βρίσκεται στην πρώτη γραμμή άμυνας, συντελώντας στην προστασία του εξοπλισμού του συστήματος VSS από κλοπές, βανδαλισμούς, φυσικές καταστροφές, ανθρωπογενείς καταστροφές και τυχαίες βλάβες (π.χ. ηλεκτρικές υπερτάσεις, ακραίες θερμοκρασίες, τυχαία εισχώρηση καφέ στο σύστημα). Στα αναλογικά συστήματα η φυσική ασφάλεια διαδραματίζει τον κεντρικό ρόλο στην προστασία τους.

134. **Η ασφάλεια συστήματος και δεδομένων**, δηλαδή η προστασία από σκόπιμη ή ακούσια παρεμβολή στις συνήθεις λειτουργίες του μπορεί να περιλαμβάνει:

- Προστασία ολόκληρης της υποδομής του συστήματος VSS (συμπεριλαμβανομένων των καμερών με απομακρυσμένη σύνδεση, των καλωδιώσεων και της τροφοδοσίας) από φυσική παραβίαση και κλοπή.
- Προστασία της διαβίβασης οπτικοακουστικού υλικού με ασφαλείς διαύλους επικοινωνίας ενάντια σε υποκλοπή.
- Κρυπτογράφηση δεδομένων.
- Χρήση λύσεων βασισμένων στο υλικό και το λογισμικό όπως τείχη προστασίας, συστήματα καταπολέμησης ιών ή ανίχνευσης εισβολών για την προστασία από κυβερνοεπιθέσεις.
- Ανίχνευση δυσλειτουργιών των εξαρτημάτων, του λογισμικού και των διασυνδέσεων του συστήματος.
- Μέσα αποκατάστασης της διαθεσιμότητας και της πρόσβασης στο σύστημα σε περίπτωση φυσικού ή τεχνικού συμβάντος.

[26] Μπορεί να εξαρτάται από τις εθνικές νομοθεσίες και τους κανονισμούς σε επίπεδο τομέων.

135. **Ο έλεγχος της πρόσβασης** διασφαλίζει ότι μόνο εξουσιοδοτημένα άτομα μπορούν να έχουν πρόσβαση στο σύστημα και στα δεδομένα και ότι η πρόσβαση απαγορεύεται σε όλους τους μη εξουσιοδοτημένους χρήστες. Στο πλαίσιο των μέτρων που στηρίζουν τον έλεγχο φυσικής και λογικής πρόσβασης περιλαμβάνονται:

- Διασφαλίζεται ότι όλες οι εγκαταστάσεις στις οποίες εκτελείται παρακολούθηση με βιντεοεπιτήρηση και στις οποίες αποθηκεύεται βιντεοσκοπημένο υλικό προστατεύονται από μη εποπτευόμενη πρόσβαση τρίτων.
- Τοποθετούνται οθόνες κατά τρόπο ώστε μόνο χειριστές που έχουν σχετική άδεια να μπορούν να τις βλέπουν (κυρίως όταν οι οθόνες βρίσκονται σε ανοιχτούς χώρους, όπως σε αίθουσα υποδοχής).
- Καθορίζονται και εφαρμόζονται διαδικασίες για τη χορήγηση, μεταβολή και ανάκληση φυσικής και λογικής πρόσβασης.
- Εφαρμόζονται μέθοδοι και μέσα εξακρίβωσης ταυτότητας και εξουσιοδότησης χρήστη, π.χ. οι μυστικοί κωδικοί πρόσβασης πρέπει να έχουν συγκεκριμένο μέγεθος και πρέπει να αλλάζουν συχνά.
- Οι ενέργειες που εκτελεί ο χρήστης (τόσο στο σύστημα όσο και στα δεδομένα) καταγράφονται και ελέγχονται τακτικά.
- Η παρακολούθηση και η ανίχνευση αποτυχιών πρόσβασης γίνεται σε διαρκή βάση και οι αδυναμίες που διαπιστώνονται αντιμετωπίζονται το συντομότερο δυνατόν.

10 ΕΚΤΙΜΗΣΗ ΕΠΙΠΤΩΣΕΩΝ ΣΧΕΤΙΚΑ ΜΕ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ

136. Σύμφωνα με το άρθρο 35 παράγραφος 1 του ΓΚΠΔ, όταν ένα είδος επεξεργασίας ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας πρέπει να διενεργεί εκτίμηση των επιπτώσεων για την προστασία δεδομένων. Το άρθρο 35 παράγραφος 3 στοιχείο γ) του ΓΚΠΔ ορίζει ότι οι υπεύθυνοι επεξεργασίας υποχρεούνται να διενεργούν εκτιμήσεις αντικτύπου σχετικά με την προστασία δεδομένων εάν η επεξεργασία αποτελεί συστηματική παρακολούθηση δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα. Επιπλέον, σύμφωνα με το άρθρο 35 παράγραφος 3 στοιχείο β) του ΓΚΠΔ η εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων είναι αναγκαία όταν ο υπεύθυνος επεξεργασίας σκοπεύει να επεξεργαστεί ειδικές κατηγορίες δεδομένων σε μεγάλη κλίμακα.

137. Οι κατευθυντήριες γραμμές για την εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων[27] περιλαμβάνουν περαιτέρω συμβουλές και πιο αναλυτικά παραδείγματα σχετικά με τη βιντεοεπιτήρηση (π.χ. σε σχέση με τη «χρήση συστήματος βιντεοσκόπησης για την παρακολούθηση της οδικής συμπεριφοράς σε αυτοκινητοδρόμους»). Το άρθρο 35 παράγραφος 4 του ΓΚΠΔ ορίζει ότι κάθε εποπτική αρχή πρέπει να καταρτίζει κατάλογο με τα είδη των πράξεων επεξεργασίας που υπόκεινται στην απαίτηση για διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων εντός της οικείας χώρας. Αυτοί οι κατάλογοι διατίθενται συνήθως στους δικτυακούς τόπους των αρχών. Δεδομένου ότι η βιντεοεπιτήρηση υπηρετεί συνήθως συγκεκριμένους σκοπούς (προστασία ατόμων και περιουσίας, εντοπισμός, πρόληψη και έλεγχος αδικημάτων, συλλογή αποδεικτικών στοιχείων και βιομετρική ταυτοποίηση υπόπτων), είναι εύλογο να υποθέσουμε ότι σε πολλές περιπτώσεις βιντεοεπιτήρησης θα πρέπει να διενεργείται εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων. Ως εκ τούτου, οι υπεύθυνοι επεξεργασίας θα πρέπει να συμβουλεύονται προσεκτικά αυτά τα έγγραφα για να εξακριβώσουν αν χρειάζεται η εκτίμηση αυτή και, εφόσον χρειάζεται, να τη διενεργούν. Στο αποτέλεσμα της διενεργούμενης εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων θα πρέπει να προσδιορίζονται τα εφαρμοστέα μέτρα προστασίας δεδομένων που επιλέγονται από τον υπεύθυνο επεξεργασίας.

138. Είναι επίσης σημαντικό να σημειωθεί ότι αν στα αποτελέσματα της εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων αναφέρεται ότι η επεξεργασία θα μπορούσε να επιφέρει υψηλό κίνδυνο παρά τα μέτρα ασφαλείας που σχεδιάζει να λάβει ο υπεύθυνος επεξεργασίας, τότε είναι απαραίτητο να πραγματοποιηθεί διαβούλευση με την αρμόδια εποπτική αρχή πριν από την επεξεργασία. Λεπτομέρειες σχετικά με την προηγούμενη διαβούλευση διατίθενται στο άρθρο 36.

Για το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων

Η Πρόεδρος

(Andrea Jelinek)

---

[27] WP248 αναθ.01, «Κατευθυντήριες γραμμές για την εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) και καθορισμός του κατά πόσον η επεξεργασία "ενδέχεται να επιφέρει υψηλό κίνδυνο" για τους σκοπούς του κανονισμού 2016/679» - εκδόθηκαν από το ΕΣΠΔ