სახელმძღვანელო რეკომენდაცია **3/2019** პერსონალური მონაცემების ვიდეომოწყობილობებით დამუშავების შესახებ

ვერსია 2.0

მიღებულია 2020 წლის 29 იანვარს

წინამდებარე სახელმძღვანელო რეკომენდაციის თარგმანი მომზადდა გერმანიის საერთაშორისო თანამშრომლობის საზოგადოების (GIZ) საჯარო მმართველობის აღმოსავლეთ პარტნიორობის რეგიონული ფონდის პროექტის ფარგლებში და წარმოადგენს არაოფიციალურ თარგმანს.

ვერსიების შესახებ

ვერსია 2.1	2020 წლის 26 თებერვალი	მასალაში არსებული შეცდომების შესწორება
ვერსია 2.0	2020 წლის 29 იანვარი	სახელმძღვანელო პრინციპების მიღება საჯარო კონსულტაციების შემდგომ
ვერსია 1.0	2019 წლის 10 ივლისი	სახელმძღვანელო პრინციპების მიღება საჯარო კონსულტაციებისთვის

სარჩევი

ევროპის მონაცემთა დაცვის საბჭო:

ითვალისწინებს რა, ევროპარლამენტისა და საბჭოს 2016 წლის 27 აპრილის რეგულაციას (EU) 2016/679 პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვისა და ასეთი მონაცემების თავისუფალი მიმოცვლის შესახებ, რომელიც აუქმებს 95/46/EC დირექტივას (შემდგომში, „GDPR“), კერძოდ, მის 70(1e) მუხლს;

ითვალისწინებს რა ევროპის ეკონომიკური ზონის შესახებ (EEA) შეთანხმებას, კერძოდ, მის XI დანართსა და 37-ე პროტოკოლს, რომელიც შესწორებულია EEA ერთობლივი კომიტეტის 2018 წლის 6 ივლისის N154/2018 გადაწყვეტილებით[1];

ითვალისწინებს რა საკუთარი რეგლამენტის მე-12 და 22-ე მუხლებს;

ამტკიცებს ქვემოთ წარმოდგენილ სახელმძღვანელო პრინციპებს.

1. შესავალი

1. ვიდეომოწყობილობების ინტენსიურ გამოყენებას გავლენა აქვს მოქალაქეთა ქცევაზე. ამგვარი ინსტრუმენტების მნიშვნელოვანი განხორციელება ფიზიკურ პირთა ცხოვრების სხვადასხვა სფეროში დამატებით ზეწოლას ქმნის ფიზიკურ პირზე, რათა მან სცადოს, დარჩეს შეუმჩნეველი მაშინ, თუ შესაძლებელია, რომ მისი ქმედებები ანომალიად იქნას მიჩნეული. ფაქტობრივად, ეს ტექნოლოგიები შესაძლოა, ზღუდავდეს ანონიმური მოძრაობისა და სერვისების ანონიმური გამოყენების შესაძლებლობას და ზოგადად, ზღუდავდეს შეუმჩნევლად დარჩენის შესაძლებლობას. მონაცემთა დაცვაზე ამ ტექნოლოგიებს ფართომასშტაბიანი გავლენა აქვს.

2. როდესაც ფიზიკური პირისთვის დისკომფორტს არ წარმოადგენს, მაგალითად, უსაფრთხოების გარკვეული მიზნით ვიდეომეთვალყურეობის მოწყობა, გარანტიები უნდა იქნას მიღებული აბსოლუტურად განსხვავებული და - მონაცემთა სუბიექტისათვის - მოულოდნელი მიზნებისთვის ბოროტად გამოყენების თავიდან ასაცილებლად (მაგ., მარკეტინგის მიზანი, დასაქმებულთა საქმიანობის მონიტორინგი და ა.შ.). ამას გარდა, არაერთი ინსტრუმენტის დანერგვა ხდება დაფიქსირებული გამოსახულებების ექსპლუატაციისთვის და ტრადიციული კამერების ჭკვიან კამერებად გადაქცევის მიზნით. ვიდეოს საშუალებით გენერირებული (წარმოებული) მონაცემების მოცულობა, ამ ინსტრუმენტებთან და ტექნიკებთან ერთობლიობაში, ზრდის მეორეული გამოყენების რისკებს (რაც შესაძლოა უკავშირდებოდეს ან არ უკავშირდებოდეს სისტემისთვის თავდაპირველად მინიჭებულ მიზანს) ან ბოროტად გამოყენების რისკებსაც კი. GDPR-ის ზოგადი პრინციპები (მუხლი 5) ყოველთვის

[1] წინამდებარე დოკუმენტში „წევრ სახელმწიფოებზე“ მითითება გაგებული უნდა იქნას, როგორც ევროპის ეკონომიკური ზონის (EEA) წევრ სახელმწიფოებზე მითითება.

სიფრთხილით უნდა იქნას გათვალისწინებული, როდესაც საქმე ეხება ვიდეომეთვალყურეობას.

3. ვიდეომეთვალყურეობის სისტემებმა მნიშვნელოვნად შეცვალა კერძო და საჯარო სექტორის წარმომადგენელი სპეციალისტების ინტერაქცია კერძო და საზოგადოებრივ ადგილებში, უსაფრთხოების გაუმჯობესების, აუდიტორიის ანალიზის მოპოვების, პერსონალიზებული რეკლამის მიწოდების და ა.შ. მიზნით. ვიდეომეთვალყურეობის ეფექტურობა მნიშვნელოვნად გაიზარდა ინტელექტუალური ვიდეოანალიზის (intelligent video analysis) მზარდი განხორციელების ფონზე. აღნიშნული ტექნიკები, შესაძლოა, უფრო მეტად (მაგ., კომპლექსური ბიომეტრიული ტექნოლოგიები) ან უფრო ნაკლებად (მაგ., თვლის მარტივი ალგორითმები) ერეოდეს ფიზიკურ პირთა უფლებებში. ანონიმურად დარჩენა და კონფიდენციალობის დაცვა, ზოგადად, სულ უფრო და უფრო მეტად რთული ხდება. ასეთ სიტუაციაში წარმოიშობა მონაცემთა დაცვასთან დაკავშირებული განსხვავებული საკითხები. შესაბამისად, განსხვავდება ამ სხვადასხვა ტექნოლოგიების გამოყენების სამართლებრივი ანალიზიც.

4. კონფიდენციალობის საკითხების გარდა, არსებობს, აგრეთვე, რისკები, რომლებიც დაკავშირებულია აღნიშნული მოწყობილობების შესაძლო დისფუნქციასთან და იმ მიკერძოებებთან, რომლებსაც ეს მოწყობილობები იწვევს. მკვლევრების თანახმად, კომპიუტერული პროგრამა, რომელიც გამოიყენება სახის იდენტიფიკაციის, ამოცნობის ან ანალიზისთვის განსხვავებულად ფუნქციონირებს იმ პირის ასაკის, გენდერის ან ეთნიკური წარმომავლობის მიხედვით, ვის იდენტიფიცირებასაც ახდენს იგი. ალგორითმები მუშაობს სხვადასხვა დემოგრაფიული მახასიათებლების საფუძველზე. შესაბამისად, მიკერძოება სახის ამოცნობაში საზოგადოებაში მიკერძოების გამყარების საფრთხეს ქმნის. სწორედ ამიტომ, დამუშავებისთვის პასუხისმგებელმა პირებმა უნდა უზრუნველყონ ვიდეომეთვალყურეობის საფუძველზე განხორციელებული ბიომეტრიულ მონაცემთა დამუშავება დაექვემდებაროს რეგულარულ შეფასებას მის რელევანტურობასთან დაკავშირებით და საკმარისი გარანტიები იქნას უზრუნველყოფილი.

5. ვიდეომეთვალყურეობა არ წარმოადგენს ავტომატურ აუცილებლობას, როდესაც არსებობს დასახული მიზნის მიღწევის სხვა საშუალებები. წინააღმდეგ შემთხვევაში, შესაძლებელია, წარმოიშვას კულტურული ნორმების შეცვლის რისკი, რაც გამოიწვევს ზოგადი პრაქტიკის სახით კონფიდენციალობის (მონაცემთა დაცვის) ნაკლებობის მიმღებლობას.

6. წინამდებარე სახელმძღვანელო პრინციპები მიზნად ისახავს, წარმოადგინოს ინსტრუქციები GDPR-ის გამოყენების შესახებ, ვიდეომოწყობილობების საშუალებით პერსონალური მონაცემების დამუშავებასთან დაკავშირებით. ეს მაგალითები არ არის ამომწურავი, თუმცა, ზოგადი პრინციპების გამოყენება შესაძლებელია ელექტრონული მოწყობილობების გამოყენების ყველა პოტენციური სფეროს მიმართ.

2. გამოყენების ფარგლები[2]

2.1 პერსონალური მონაცემები

7. გარკვეული სივრცის ოპტიკური ან აუდიოვიზუალური საშუალებებით სისტემატური ავტომატური მონიტორინგი, ძირითადად, საკუთრების დაცვის მიზნებისთვის, ან ფიზიკური პირის სიცოცხლის და ჯანმრთელობის დასაცავად, ჩვენს დროში მნიშვნელოვანი ფენომენი გახდა. ეს აქტივობა გულისხმობს გამოსახულებითი ან აუდიოვიზუალური ინფორმაციის შეგროვებას და შენახვას ყველა იმ პირის შესახებ, რომელიც შედის იმ ადგილას, სადაც მონიტორინგი ხორციელდება, ხოლო მათი იდენტიფიცირება შესაძლებელია მათი გარეგნობის ან სხვა სპეციფიკური ელემენტების მიხედვით. ამ ადამიანთა ვინაობის დადგენა შესაძლებელია ამ დეტალების საფუძველზე. აღნიშნული, აგრეთვე, შესაძლებელს ხდის პერსონალური მონაცემების შემდგომ დამუშავებას, მოცემულ სივრცეში პირთა ყოფნისა და მათი ქცევის ჭრილში. ამ მონაცემთა ბოროტად გამოყენების პოტენციური რისკი იზრდება მონიტორინგს დაქვემდებარებული სივრცის განზომილების და აგრეთვე, იმ ადამიანთა რაოდენობის პროპორციულად, რომლებიც ხშირად იმყოფებიან ამ სივრცეში. აღნიშნული ფაქტი ასახულია მონაცემთა დაცვის ძირითადი რეგულაციის (GDPR) 35(3)(c) მუხლში, რომლის მიხედვითაც საჯაროდ ხელმისაწვდომი მონაცემების ფართომასშტაბიანი, სისტემატური მონიტორინგისას საჭიროა მონაცემთა დაცვაზე ზეგავლენის შეფასება, და 37(1)(b) მუხლში, რომლის თანახმადაც დამუშავებისთვის პასუხისმგებელ პირს მოეთხოვება მონაცემთა დაცვის ოფიცრის დანიშვნა, თუ დამუშავების ოპერაცია, არსებითად, მოიცავს მონაცემთა სუბიექტების რეგულარულ და სისტემატურ მონიტორინგს.

8. ამავდროულად, რეგულაცია არ ვრცელდება მონაცემთა დამუშავებაზე, რომელიც არ არის დაკავშირებული კონკრეტულ პირთან, მაგ., თუ პირის იდენტიფიცირება შეუძლებელია, პირდაპირ ან ირიბად.

9.

> <u>მაგალითი:</u> GDPR-ი არ ვრცელდება სათამაშო კამერებზე (ე.ი., რომელიც არ ფუნქციონირებს, როგორც კამერა და შესაბამისად, არ ამუშავებს პერსონალურ მონაცემებს). *ამავდროულად, ზოგიერთ წევრ სახელმწიფოში, შესაძლოა, აღნიშნული დაექვემდებაროს სხვა კანონმდებლობას.*
>
> <u>მაგალითი:</u> დიდი სიმაღლიდან განხორციელებული ჩაწერა GDPR-ის მოქმედების სფეროში ხვდება მხოლოდ იმ შემთხვევაში, თუ მოცემულ სიტუაციაში, დამუშავებული მონაცემების დაკავშირება შესაძლებელია კონკრეტულ პირთან.

[2] EDPB-ის თანახმად, თუ GDPR-ი ამის ნებას რთავს, ეროვნულ კანონმდებლობაში შესაძლებელია, მოქმედებდეს კონკრეტული მოთხოვნები.

მაგალითი: ვიდეოკამერა, რომელიც ინტეგრირებულია მანქანაში, უზრუნველყოფს დახმარებას მანქანის დაპარკირების კუთხით. თუ კამერა შექმნილია ან კონფიგურირებულია იმგვარად, რომ იგი არ აგროვებს ფიზიკური პირის შესახებ ინფორმაციას (როგორიცაა, მანქანის სანომრე ნიშნები ან ინფორმაცია, რომლითაც შესაძლებელია გამვლელის იდენტიფიცირება), მაშინ GDPR-ი არ გავრცელდება.

2.2 სამართალდამცავი ორგანოების მიერ მონაცემთა დამუშავების შესახებ დირექტივის გამოყენება, LED (EU2016/680)

10. აღსანიშნავია, რომ პერსონალური მონაცემების დამუშავება შესაბამისი ორგანოების მიერ, სისხლის სამართლის დანაშაულების პრევენციის, გამოძიების, გამოვლენის ან სამართლებრივი დევნის მიზნებისთვის ან სისხლის სამართლებრივი სანქციების აღსრულებისთვის, მათ შორის, საზოგადოებრივი საფრთხისგან დასაცავად და ამგვარი საფრთხის პრევენციისთვის, ხვდება EU2016/680 დირექტივის მოქმედების სფეროში.

2.3 გამონაკლისი მონაცემთა ოჯახური საქმიანობის ფარგლებში დამუშავებასთან დაკავშირებით

11. 2 (2) (c) მუხლის თანახმად, ფიზიკური პირის მიერ პერსონალური მონაცემების დამუშავება, ცალსახად პირადი ან ოჯახური საქმიანობის ფარგლებში, რაც შესაძლოა მოიცავდეს ონლაინ აქტივობას, GDPR-ის მოქმედების სფეროში არ ხვდება.[3]

12. აღნიშნული დებულება - ე.წ. გამონაკლისი მონაცემთა ოჯახური საქმიანობის ფარგლებში დამუშავებასთან დაკავშირებით - ვიდეომეთვალყურეობის კონტექსტში, ვიწროდ უნდა იქნას განმარტებული. ამავდროულად, მართლმსაჯულების ევროპული სასამართლოს თანახმად, ე.წ. „მონაცემთა ოჯახური საქმიანობის ფარგლებში დამუშავების“ გამონაკლისი *„განმარტებული უნდა იქნას იმგვარად, რომ იგი დაკავშირებულია მხოლოდ იმ აქტივობებთან, რომლებიც ხორციელდება ფიზიკური პირების კერძო ან ოჯახური ცხოვრების ფარგლებში, რაც ცალსახად არ ეხება პერსონალური მონაცემების დამუშავებას ინტერნეტში გამოქვეყნებულ მასალაში, რათა ეს მონაცემები ხელმისაწვდომი იყოს ადამიანთა განუსაზღვრელი რაოდენობისთვის.“*[4] ამავდროულად, თუ ვიდეომეთვალყურეობის სისტემა, იმ შემთხვევაში, თუ გულისხმობს პერსონალური მონაცემების მუდმივად ჩაწერას და შენახვას და მოიცავს *„ნაწილობრივაც კი, საზოგადოებრივ სივრცეს და შესაბამისად, სცდება იმ პირის კერძო გარემოს ფარგლებს, რომელიც ამგვარ მონაცემებს ამუშავებს,*

[3] ასევე, იხ. პრეამბულის მე-18 პუნქტი.

[4] მართლმსაჯულების ევროპული სასამართლო, გადაწყვეტილება საქმეში C-101/01, Bodil Linquist-ის საქმე, 2003 წლის 6 ნოემბერი, პ.47

ვერ ჩაითვლება აქტივობად, რომელიც ცალსახად 'პირადი ან ოჯახური საქმიანობის' ფარგლებში ხორციელდება, 95/46 დირექტივის 3(2) მუხლის მეორე აბზაცის მიზნებისთვის."[5]

13. რაც შეეხება იმ ვიდეომოწყობილობებს, რომლებიც ოპერირებენ კერძო პირის ტერიტორიის შიგნით, ისინი შესაძლოა, ხვდებოდნენ „ოჯახური საქმიანობის ფარგლებში განხორციელებული დამუშავების" გამონაკლისის ქვეშ. აღნიშნული დამოკიდებულია რამდენიმე ფაქტორზე, ხოლო დასკვნის გაკეთებისთვის საჭიროა ყველა ფაქტორის გათვალისწინება. ECJ-ის გადაწყვეტილებებში იდენტიფიცირებული ზემოაღნიშნული ელემენტების გარდა, როდესაც სახლში მოიხმარენ ვიდეომეთვალყურეობას, გათვალისწინებული უნდა იქნას, აქვს თუ არა რაიმე პერსონალური ურთიერთობა ვიდეომეთვალყურეობის მომხმარებელს მონაცემთა სუბიექტთან, მეთვალყურეობის მასშტაბი ან სიხშირე ხომ არ მიუთითებს მისი მხრიდან რაიმე სახის პროფესიულ აქტივობაზე, და რა შესაძლო უარყოფითი გავლენა ექნება მეთვალყურეობას მონაცემთა სუბიექტზე. ზემოაღნიშნული რომელიმე ელემენტის არსებობა ავტომატურად არ ნიშნავს, რომ დამუშავება ოჯახური საქმიანობის გამონაკლისის გარეთ ხვდება, არამედ, ამის დასადგენად საჭიროა ზოგადი შეფასების განხორციელება.

14.

> <u>მაგალითი:</u> ტურისტი ახდენს ვიდეოების ჩაწერას საკუთარი მობილური ტელეფონის და ვიდეოკამერის საშუალებით, არდადეგების დოკუმენტირების მიზნით. მან ჩანაწერი აჩვენა მეგობრებს და ოჯახის წევრებს. ამასთან, ჩანაწერი ადამიანთა განუსაზღვრელი რაოდენობისთვის არ არის ხელმისაწვდომი. აღნიშნული ოჯახური საქმიანობის გამონაკლისის ქვეშ ხვდება.
>
> მაგალითი: ველოსიპედისტს სურს, კამერა „actioncam"-ის საშუალებით ჩაიწეროს გარკვეულ ტერიტორიაზე საკუთარი მოძრაობა. იგი დაუსახლებელ ტერიტორიაზე გადაადგილდება ველოსიპედით და აპირებს ჩანაწერები გამოიყენოს სახლში, პირადი, გასართობი მიზნებისთვის. აღნიშნული ხვდება ოჯახური საქმიანობის გამონაკლისის ქვეშ.
>
> მაგალითი: ფიზიკური პირი საკუთარ ბაღზე ახორციელებს მონიტორინგს და ჩაწერას. საკუთრება შემოღობილია და ბაღში რეგულარულად შედიან მხოლოდ დამუშავებისთვის პასუხისმგებელი პირი და მისი ოჯახის წევრები. აღნიშნული ხვდება ოჯახური საქმიანობის გამონაკლისის ქვეშ იმ შემთხვევაში, თუ ვიდეომეთვალყურეობა ნაწილობრივაც კი არ ვრცელდება საზოგადოებრივ ადგილზე ან მეზობლად მდებარე საკუთრებაზე.

[5] მართლმსაჯულების ევროპული სასამართლო, გადაწყვეტილება საქმეში C-212/13, František Ryneš v Úřad pro ochranu osobních údajů, 2014 წლის 11 დეკემბერი, პ.33

3. დამუშავების კანონიერება

15. გამოყენებამდე, საჭიროა დეტალურად მიეთითოს დამუშავების მიზნები (მუხლი 5(1)(b)). ვიდეომეთვალყურეობას შესაძლოა, ჰქონდეს სხვადასხვა მიზანი, მაგ., საკუთრების და სხვა აქტივების დაცვა, ფიზიკური პირების სიცოცხლის და ფიზიკური ხელშეუხებლობის დაცვის მხარდაჭერა, მტკიცებულების შეგროვება სამოქალაქო პრეტენზიებისთვის.[6] საჭიროა მონიტორინგის აღნიშნული მიზნების წერილობითი ფორმით დოკუმენტირება (მუხლი 5(2)) და მითითება თითოეული სამეთვალყურეო კამერისთვის. კამერები, რომლებიც გამოიყენება ერთი და იგივე მიზნისთვის, ერთი და იგივე დამუშავებისთვის პასუხისმგებელი პირის მიერ, შესაძლებელია, რომ ერთად იქნას დოკუმენტირებული. ამას გარდა, მონაცემთა სუბიექტებს უნდა მიეწოდოთ ინფორმაცია დამუშავების მიზნ(ებ)ის შესახებ, მე-13 მუხლის შესაბამისად (*იხ. სექცია 7, გამჭვირვალობასთან და ინფორმაციასთან დაკავშირებული ვალდებულებები).* როდესაც ვიდეომეთვალყურეობა ეფუძნება მხოლოდ „უსაფრთხოების“ და „თქვენი უსაფრთხოების“ მიზანს, ეს მიზანი არ არის საკმარისად კონკრეტული (მუხლი 5(1)(b). ამასთან, იგი ეწინააღმდეგება იმ პრინციპს, რომ პერსონალური მონაცემები უნდა დამუშავდეს კანონიერად, სამართლიანად და გამჭვირვალედ, მონაცემთა სუბიექტთან მიმართებით (იხ. მუხლი 5(1)(a)).

16. არსებითად, 6(1) მუხლით გათვალისწინებული თითოეული სამართლებრივი საფუძველი შესაძლებელია, რომ უზრუნველყოფდეს კანონიერ საფუძველს ვიდეომეთვალყურეობის შედეგად მოპოვებული მონაცემების დამუშავებისთვის. მაგალითად, 6(1)(c) მუხლი მოქმედებს, თუ ეროვნული კანონი ადგენს ვიდეომეთვალყურეობის განხორციელების მოვალეობას.[7] ამავდროულად, პრაქტიკაში დებულებები, რომლებიც ყველაზე ხშირად გამოიყენება, მოიცავს:

    - მუხლი 6(1)(f) (ლეგიტიმური ინტერესი),
    - მუხლი 6(1)(e) (დამუშავება აუცილებელია აუცილებელია საჯარო ინტერესის სფეროში შემავალი ამოცანების შესასრულებლად ან დამუშავებისთვის პასუხისმგებელი პირისთვის მინიჭებული ოფიციალური უფლებამოსილების განსახორციელებლად).

    გამონაკლის შემთხვევებში, დამუშავებისთვის პასუხისმგებელმა პირმა, შესაძლოა გამოიყენოს 6(1)(a) მუხლიც (თანხმობა), როგორც სამართლებრივი საფუძველი.

[6] სამოქალაქო საჩივრებისთვის მტკიცებულების შეგროვების წესები განსხვავდება წევრი სახელმწიფოების მიხედვით.

[7] წინამდებარე სახელმძღვანელო პრინციპები არ აანალიზებს და დეტალურად არ განიხილავს განსხვავებულ ეროვნულ კანონებს, რომლებიც შესაძლოა მოქმედებდნენ წევრ სახელმწიფოებში.

3.1 ლეგიტიმური ინტერესი, მუხლი 6(1)(f)

17. 6(1)(f) მუხლის სამართლებრივი შეფასება უნდა ეფუძნებოდეს ქვემოთ წარმოდგენილ კრიტერიუმებს, პრეამბულის 47-ე პუნქტის შესაბამისად.

3.1.1 ლეგიტიმური ინტერესების არსებობა

18. ვიდეომეთვალყურეობა კანონიერია, თუ იგი აუცილებელია დამუშავებისთვის პასუხისმგებელი პირის ან მესამე მხარის მიერ დასახული ლეგიტიმური ინტერესის დასაკმაყოფილებლად, გარდა იმ შემთხვევისა, როდესაც ამგვარ ინტერესებს გადაწონის მონაცემთა სუბიექტის ინტერესები ან ფუნდამენტური უფლებები ან თავისუფლებები (მუხლი 6(1)(f)). დამუშავებისთვის პასუხისმგებელი პირის ან მესამე მხარის ლეგიტიმური ინტერესები შესაძლოა იყოს სამართლებრივი[8], ეკონომიკური ან არა-მატერიალური.[9] ამავდროულად, დამუშავებისთვის პასუხისმგებელმა პირმა უნდა გაითვალისწინოს, რომ თუ მონაცემთა სუბიექტი მოსთხოვს ვიდეომეთვალყურეობის შეწყვეტას, 21-ე მუხლის შესაბამისად, დამუშავებისთვის პასუხისმგებელ პირს მეთვალყურეობის გაგრძელება შეუძლია იმ შემთხვევაში, თუ იარსებებს *დამაჯერებელი* ლეგიტიმური ინტერესი, რომელიც გადაწონის მონაცემთა სუბიექტის ინტერესებს, უფლებებს და თავისუფლებებს ან სამართლებრივი პრეტენზიების დადგენისთვის, განხორციელებისთვის ან დაცვისთვის.

19. რეალური და საფრთხის შემცველი სიტუაციის გათვალისიწნებით, საკუთრების ძარცვისგან, ქურდობისგან ან ვანდალიზმისგან დაცვის მიზანი შესაძლოა, წარმოადგენდეს ვიდეომეთვალყურეობის ლეგიტიმურ ინტერესს.

20. ლეგიტიმური ინტერესი რეალურად უნდა არსებობდეს და უნდა იყოს საკითხი, რომელიც მოცემულ მომენტში დგას (ე.ი., იგი არ უნდა იყოს ფიქციური ან სპეკულაციური).[10] მეთვალყურეობის დაწყებამდე, მოცემულ მომენტში უნდა არსებობდეს რეალური პრობლემური სიტუაცია - როგორიცაა, ზიანი ან სერიოზული ინციდენტები წარსულში. ანგარიშვალდებულების პრინციპის თანახმად, მიზანშეწონილია, რომ დამუშავებისთვის პასუხისმგებელმა პირებმა მოახდინონ ინციდენტების (თარიღი, ფორმა, ფინანსური ზიანი) და შესაბამისი სისხლის სამართლებრივი ბრალდებების დოკუმენტირება. აღნიშნული დოკუმენტირებული ინციდენტები მყარ მტკიცებულებას შექმნის ლეგიტიმური ინტერესის არსებობასთან დაკავშირებით. ლეგიტიმური ინტერესის არსებობა და მონიტორინგის აუცილებლობა პერიოდული ინტერვალებით უნდა შეფასდეს (მაგ., წელიწადში ერთხელ, გარემოებებისდა შესაბამისად).

21.

---

[8] მართლმსაჯულების ევროპული სასამართლო, გადაწყვეტილება საქმეში C-13/16, Rīgas satiksme-ს საქმე, 2017 წლის 4 მაისი.

[9] იხ. WP2017, 29-ე მუხლის სამუშაო ჯგუფი.

[10] იხ. WP217, 29-ე მუხლის სამუშაო ჯგუფი, გვ.24 seq. ასევე, იხ. ECJ-ის საქმე C-708/18, გვ.44

მაგალითი: მაღაზიის მფლობელს სურს, რომ გახსნას ახალი მაღაზია და დაამონტაჟოს ვიდეომეთვალყურეობის სისტემა, ვანდალიზმის პრევენციის მიზნით. მას შეუძლია, წარმოადგინოს სტატისტიკა და დაადასტუროს მოცემულ რაიონში ვანდალიზმის მაღალი მაჩვენებლის არსებობა. ამ კუთხით, სასარგებლოა მეზობლად მდებარე მაღაზიების გამოცდილებაც. იმისათვის, რომ მონაცემთა ამგვარი დამუშავება დასაშვებად ჩაითვალოს, არ არის აუცილებელი, რომ დამუშავებისთვის პასუხისმგებელ პირს მიადგეს ზიანი. თუ ახლოს მდებარე ობიექტების გამოცდილებიდან ჩანს ვანდალიზმის საფრთხე ან სხვა მსგავსი რისკი, ეს შესაძლოა ლეგიტიმური ინტერესის არსებობაზე მიუთითებდეს. ამავდროულად, არ არის საკმარისი ეროვნული ან ზოგადი სისხლის სამართლებრივი სტატისტიკის წარდგენა, მოცემული ტერიტორიის/რაიონის და იმ საფრთხეების გაანალიზების გარეშე, რომელიც კონკრეტულად ამ მაღაზიას ემუქრება.

22. გარდაუვალი საფრთხის სიტუაციები, შესაძლოა, წარმოადგენდეს ლეგიტიმურ ინტერესს. ასეთი ინტერესი არსებობს იმ ბანკების და მაღაზიების შემთხვევაში, რომლებიც ყიდიან ძვირფას საქონელს (მაგ., საიუვილერო მაღაზიები) ან იმ ტერიტორიებზე, სადაც ხშირია საკუთრების მიმართ დანაშაულის შემთხვევები (მაგ., ბენზინგასამართი სადგურები).

23. GDPR-ი მკაფიოდ აცხადებს, რომ სახელმწიფო ორგანოები მონაცემთა დამუშავებას ვერ დააფუძნებენ ლეგიტიმურ ინტერესს, თუ დამუშავებას ახორციელებენ თავიანთი ამოცანების შესრულების მიზნით (მე-6 მუხლის 1-ლი პუნქტი, მე-2 წინადადება).

3.1.2 დამუშავების აუცილებლობა

24. პერსონალური მონაცემები უნდა იყოს დამუშავების მიზანთან მიმართებით ადეკვატური, რელევანტური და უნდა დამუშავდეს მხოლოდ იმ მოცულობით, რომელიც აუცილებელია დამუშავების მიზნის მისაღწევად (‘მონაცემთა მინიმიზაცია’), იხ. მუხლი 5(1)(c). ვიდეომეთვალყურეობის სისტემის დამონტაჟებამდე, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, ყოველთვის კრიტიკულად შეაფასოს, თუ რამდენად შესაფერისია ეს ზომა სასურველი მიზნის მისაღწევად და რამდენად ადეკვატური და აუცილებელია იგი ამ მიზნისთვის. ვიდეომეთვალყურეობის ზომები არჩეული უნდა იქნას იმ შემთხვევაში, თუ დამუშავების მიზანი, გონივრულობის ფარგლებში, ვერ იქნება მიღწეული სხვა საშუალებებით, რომლებიც ნაკლებად ზღუდავს მონაცემთა სუბიექტის ფუნდამენტურ უფლებებს და თავისუფლებებს.

25. იმის გათვალისწინებით, რომ დამუშავებისთვის პასუხისმგებელ პირს სურს, მოახდინოს საკუთრებასთან დაკავშირებული დანაშაულების პრევენცია, ნაცვლად ვიდეომეთვალყურეობის სისტემის დამონტაჟებისა, მას შეუძლია მიიღოს უსაფრთხოების ალტერნატიული ზომები, როგორიცაა, საკუთრების შემოღობვა, უსაფრთხოების თანამშრომლების დაქირავება, დარაჯების გამოყენება, უკეთესი

განათების უზრუნველყოფა, უსაფრთხოების საკეტების, მყარი ფანჯრების და კარების დამონტაჟება ან კედლების გრაფიტის საწინააღმდეგო საშუალებებით დამუშავება. აღნიშნული ზომები, შესაძლოა, ისეთივე ეფექტური იყოს ძარცვის, ქურდობის და ვანდალიზმის წინააღმდეგ, როგორც ვიდეომეთვალყურეობა. დამუშავებისთვის პასუხისმგებელმა პირმა ყოველ ინდივიდუალურ შემთხვევაში უნდა შეაფასოს, თუ რამდენად გონივრულ გადაწყვეტას წარმოადგენს ამგვარი ზომები.

26. ვიდეომეთვალყურეობის სისტემის ამოქმედებამდე, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, შეაფასოს, თუ სად და როდის არის ვიდეომეთვალყურეობის ზომები მკაცრად აუცილებელი. როგორც წესი, ვიდეომეთვალყურეობის სისტემა, რომელიც ოპერირებს ღამით და სამუშაო საათების მიღმა, დააკმაყოფილებს დამუშავებისთვის პასუხისმგებელი პირის ინტერესს, საფრთხე აცილოს საკუთრებას.

27. ზოგადად, დამუშავებისთვის პასუხისმგებელი პირის ტერიტორიის დასაცავად ვიდეომეთვალყურეობის გამოყენების აუცილებლობა სრულდება საკუთრების საზღვრებთან.[11] ამავდროულად, ზოგ შემთხვევაში, საკუთრების მონიტორინგი არ არის საკმარისი მისი ეფექტური დაცვისთვის. ზოგ ინდივიდუალურ შემთხვევებში, შესაძლებელია, საჭირო იყოს ვიდეომეთვალყურეობის გავრცელება ტერიტორიის გარემომცველ ადგილებზე. ამ კონტექსტში, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, გაითვალისწინოს ფიზიკური და ტექნიკური საშუალებები, მაგალითად, არარელევანტური ტერიტორიების დაბლოკვა ან პიქსელიზაცია.

28.

> <u>მაგალითი:</u> წიგნების მაღაზიას სურს, საკუთარი ტერიტორია ვანდალიზმისგან დაიცვას. ზოგადად, კამერები მხოლოდ ტერიტორიას უნდა იღებდეს, რადგან არ არის აუცილებელი მეზობლად მდებარე ტერიტორიების ან საზოგადოებრივი ადგილების მონიტორინგი წიგნების მაღაზიის გარშემო, აღნიშნული მიზნით.

29. კითხვები, რომლებიც ეხება დამუშავების აუცილებლობას, აგრეთვე, წარმოიშვება მტკიცებულების შენახვასთან დაკავშირებით. ზოგ შემთხვევაში, შესაძლოა აუცილებელი იყოს „შავი ყუთის“ გადაწყვეტების გამოყენება, როდესაც ჩანაწერი ავტომატურად იშლება შენახვის გარკვეული პერიოდის შემდეგ და მათზე წვდომის განხორციელება შესაძლებელია მხოლოდ ინციდენტის შემთხვევაში. სხვა სიტუაციებში, შესაძლოა აუცილებელი არ იყოს ვიდეომასალის ჩაწერა და უფრო შესაფერის საშუალებას წარმოადგენდეს რეალურ დროში მონიტორინგი. „შავი ყუთის“ გადაწყვეტასა და რეალურ დროში მონიტორინგს შორის არჩევანი უნდა გაკეთდეს დასახული მიზნის საფუძველზე. თუ მაგალითად, ვიდეომეთვალყურეობა

[11] აღნიშნული, შესაძლოა, აგრეთვე დაექვემდებაროს ზოგიერთ წევრ სახელმწიფოში მოქმედ ეროვნულ კანონმდებლობას.

ემსახურება მტკიცებულების შენახვას, რეალურ დროში მონიტორინგის მეთოდები, როგორც წესი, არ არის შესაფერისი. ზოგ შემთხვევაში, რეალურ დროში მონიტორინგი, შესაძლოა, უფრო მეტად ზღუდავდეს უფლებებს, ვიდრე მასალის შენახვა და ავტომატურად წაშლა გარკვეული ვადის გასვლის შემდეგ (მაგ., თუ ვინმე მუდმივად უყურებს მონიტორინგს, ეს შესაძლოა უფრო მეტად ზღუდავდეს მონაცემთა სუბიექტის უფლებებს, ვიდრე მონიტორინგის არ არსებობა და მასალის პირდაპირ შენახვა შავ ყუთში). ამ შემთხვევაში, გამოყენებული უნდა იქნას მონაცემთა მინიმიზაციის პრინციპი (მუხლი 5(1)(c)). აგრეთვე, გათვალისწინებული უნდა იქნას, რომ შესაძლებელია დამუშავებისთვის პასუხისმგებელმა პირმა გამოიყენოს უსაფრთხოების თანამშრომლები, ვიდეომეთვალყურეობის ნაცვლად, რომლებსაც შეუძლიათ დაუყოვნებლივ რეაგირება და ჩარევა.

3.1.3 ინტერესების დაბალანსება

30. თუ ჩავთვლით, რომ ვიდეომეთვალყურეობა აუცილებელია დამუშავებისთვის პასუხისმგებელი პირის ლეგიტიმური ინტერესების დასაცავად, ვიდეომეთვალყურეობის სისტემის ამოქმედება შესაძლებელია მხოლოდ იმ შემთხვევაში, თუ აღნიშნული პირის ან მესამე მხარის ლეგიტიმურ ინტერესებს (მაგ., საკუთრების ან ფიზიკური ხელშეუხებლობის დაცვა) არ გადაწონის მონაცემთა სუბიექტის ინტერესები ან ფუნდამენტური უფლებები და თავისუფლებები. დამუშავებისთვის პასუხისმგებელმა პირმა უნდა გაითვალისწინოს: 1) რამდენად ახდენს მონიტორინგი გავლენას ფიზიკური პირების ინტერესებზე, ფუნდამენტურ უფლებებზე და თავისუფლებებზე და 2) იწვევს თუ არა ეს დარღვევებს ან ნეგატიურ შედეგებს მონაცემთა სუბიექტის უფლებებთან მიმართებით. უფრო მეტიც, ინტერესების დაბალანსება აუცილებელია. ერთის მხრივ, ფუნდამენტური უფლებები და თავისუფლებები და მეორეს მხრივ, დამუშავებისთვის პასუხისმგებელი პირის ლეგიტიმური ინტერესები უნდა შეფასდეს და სიფრთხილით დაბალანსდეს.

31.

> <u>მაგალითი:</u> პარკინგის კერძო კომპანია ახდენს დაპარკირებულ მანქანებში ქურდობის გახშირებული შემთხვევების დოკუმენტირებას. პარკინგის ტერიტორია არის ღია სივრცე, სადაც ნებისმიერ პირს შეუძლია შესვლა, თუმცა, ამ სივრცის გარშემო განთავსებულია მკაფიო ნიშნები და გზის დამაბრკოლებელი საშუალებები. პარკინგის კომპანიას აქვს ლეგიტიმური ინტერესი (მომხმარებელთა მანქანების გაქურდვის პრევენცია), განახორციელოს ტერიტორიის მონიტორინგი დროის იმ პერიოდში, როდესაც ადგილი აქვს აღნიშნულ შემთხვევებს. მონაცემთა სუბიექტების მონიტორინგი ხორციელდება დროის შეზღუდულ პერიოდში, ისინი ტერიტორიაზე რეკრეაციული მიზნებით არ იმყოფებიან და აგრეთვე, მათ ინტერესებშია ქურდობის შემთხვევების პრევენცია. მონაცემთა სუბიექტების

ინტერესს, არ დაექვემდებარონ მონიტორინგს, ამ შემთხვევაში, გადაწონის დამუშავებისთვის პასუხისმგებელი პირის ლეგიტიმური ინტერესი.

<u>მაგალითი:</u> რესტორანმა გადაწყვიტა, განათავსოს ვიდეოკამერები საპირფარეშოში, რათა გააკონტროლოს სანიტარული წერტილების სისუფთავე. ამ შემთხვევაში ცხადია, რომ მონაცემთა სუბიექტების უფლებები გადაწონის დამუშავებისთვის პასუხისმგებელი პირის ინტერესს. შესაბამისად, დაუშვებელია მითითებულ ადგილას კამერების განთავსება.

3.1.3.1 ინდივიდუალური გადაწყვეტილებების მიღება

32. ვინაიდან ინტერესთა დაბალანსება რეგულაციის მიხედვით აუცილებელია, გადაწყვეტილება მიღებული უნდა იქნას ინდივიდუალური შემთხვევის გარემოებების გათვალისწინებით (იხ. მუხლი 6(1)(f)). აბსტრაქტულ სიტუაციებზე მითითება ან მსგავსი შემთხვევების ერთმანეთისთვის შედარება არასაკმარისია. დამუშავებისთვის პასუხისმგებელმა პირმა უნდა შეაფასოს მონაცემთა სუბიექტის უფლებებში ჩარევის რისკები; ამ შემთხვევაში, გადამწყვეტი კრიტერიუმი არის ფიზიკური პირის უფლებებსა და თავისუფლებებში ინტერვენციის ინტენსივობა.

33. ინტენსივობა შესაძლოა, inter alia, განისაზღვროს შემდეგი ფაქტორების მიხედვით: რა ტიპის ინფორმაციის შეგროვება ხდება (ინფორმაციის შინაარსი), ინფორმაციის ფარგლები (საინფორმაციო სიმჭიდროვე, სივრცითი და გეოგრაფიული მასშტაბი), მონაცემთა სუბიექტების რაოდენობა, რომელთა უფლებებშიც ერევიან, მონაცემთა სუბიექტების ჯგუფის რეალური ინტერესები, ალტერნატიული საშუალებები და მონაცემთა შეფასების ხასიათი და ფარგლები.

34. დაბალანსებისთვის მნიშვნელოვანი ფაქტორებია: ტერიტორიის ზომა, სადაც ხორციელდება მეთვალყურეობა და იმ მონაცემთა სუბიექტების რაოდენობა, რომლებიც მეთვალყურეობას ექვემდებარებიან. ვიდეომეთვალყურეობის გამოყენება მოშორებით მდებარე ტერიტორიებზე (მაგ., ხანძრებზე მონიტორინგის ან კრიტიკული ინფრასტრუქტურის - მაგ., რადიო ანტენა, რომელიც კერძო მფლობელობაშია - დაცვის მიზნით) უნდა შეფასდეს განსხვავებულად, ვიდრე ვიდეომეთვალყურეობა, რომელიც ხორციელდება სავაჭრო ცენტრში ან ფეხით მოსიარულეთა ზონაში.

35.

<u>მაგალითი:</u> მანქანაში ვიდეორეგისტრატორის დამონტაჟების შემთხვევაში (მაგ., უბედური შემთხვევის დროს მტკიცებულების შეგროვების მიზნით) მნიშვნელოვანია, რომ კამერა მუდმივად არ იწერდეს მანქანების მოძრაობას და აგრეთვე, გზასთან ახლოს მყოფ ადამიანებს. სხვა შემთხვევაში, ვიდეოჩანაწერების სახით მტკიცებულების ქონა უბედური შემთხვევის თეორიულ შემთხვევაში ვერ გაამართლებს მონაცემთა სუბიექტების უფლებებში ჩარევის სიმძიმეს.[11]

3.1.3.2 მონაცემთა სუბიექტების გონივრული მოლოდინები

36. პრეამბულის 47-ე პუნქტის მიხედვით, ლეგიტიმური ინტერესის არსებობა საჭიროებს ზედმიწევნით შეფასებას. ამ შემთხვევაში, გათვალისწინებული უნდა იქნას მონაცემთა სუბიექტის მოლოდინები იმ დროს და პერსონალური მონაცემების დამუშავების კონტექსტი. სისტემატურ მონიტორინგთან დაკავშირებით, მონაცემთა სუბიექტსა და დამუშავებისთვის პასუხისმგებელ პირს შორის ურთიერთობა, შესაძლოა, მნიშვნელოვნად განსხვავდებოდეს და გავლენას ახდენდეს იმაზე, თუ რა გონივრული მოლოდინები შეიძლება ჰქონდეს მონაცემთა სუბიექტს. გონივრული მოლოდინების ინტერპრეტაცია არ უნდა დაეფუძნოს მხოლოდ მოცემული პირის სუბიექტურ მოლოდინებს, არამედ, გადამწყვეტი კრიტერიუმი მდგომარეობს, თუ რა გონივრული მოლოდინები შეიძლება ჰქონდეს ობიექტურ მესამე მხარეს და მისი აზრით, რა ექვემდებარება მონიტორინგს მოცემულ სიტუაციაში.

37. მაგალითად, უმეტეს შემთხვევებში, დასაქმებულს სამუშაო ადგილზე არ ექნება მოლოდინი, რომ მის მონიტორინგს განახორციელებს მისი დამსაქმებელი.[12] ამასთან, მონაცემთა სუბიექტი მონიტორინგს არ ელის საკუთარ ბაღში, საცხოვრებელ სივრცეებში ან გასინჯვის და მკურნალობის ოთახებში. მსგავსად აღნიშნულისა, არ შეიძლება არსებობდეს სანიტარული კვანძების და საუნების მონიტორინგის გონივრული მოლოდინი - ასეთი სივრცეების მონიტორინგი წარმოადგენს მონაცემთა სუბიექტის უფლებებში ინტენსიურ ჩარევას. მონაცემთა სუბიექტების გონივრული მოლოდინები მდგომარეობს იმაში, რომ აღნიშნულ სივრცეებში ადგილი არ ექნება მეთვალყურეობას. მეორეს მხრივ, ბანკის მომხმარებელს შესაძლოა ჰქონდეს მოლოდინი, რომ მასზე ხორციელდება ვიდეომეთვალყურეობა ბანკში ან ბანკომატთან.

38. მონაცემთა სუბიექტი, აგრეთვე, მოელის, რომ საზოგადოებრივ ადგილებში, განსაკუთრებით, ისეთ ადგილებში, რომელიც გამოიყენება გამოჯანმრთელებასთან, რეგენერაციასთან და დასვენებასთან დაკავშირებული აქტივობებისთვის და ასევე იმ ადგილებში, სადაც ფიზიკური პირების რჩებიან და/ან ახორციელებენ კომუნიკაციას, მაგალითად, დასაჯდომი სივრცეები, მაგიდები რესტორნებში, პარკებში, კინოები და ფიტნეს დაწესებულებები, იგი არ დაექვემდებარება მონიტორინგს. ამ შემთხვევაში, მონაცემთა სუბიექტის უფლებები და თავისუფლებები ხშირად გადაწონის დამუშავებისთვის პასუხისმგებელი პირის ლეგიტიმურ ინტერესებს.

39.

[12] ასევე, იხ. 29-ე მუხლის სამუშაო ჯგუფი, დასკვნა 2/2017 სამუშაო ადგილას მონაცემთა დამუშავების შესახებ, WP249, მიღებულია 2017 წლის 8 ივნისს.

<u>მაგალითი:</u> ტუალეტებში მონაცემთა სუბიექტი მოელის, რომ იგი არ დაექვემდებარება მონიტორინგს. ვიდეომეთვალყურეობა, მაგალითად, უბედური შემთხვევების თავიდან ასარიდებლად, არ არის პროპორციული.

40. ნიშნები, რომლებიც მონაცემთა სუბიექტს აფრთხილებს ვიდეომეთვალყურეობის შესახებ, არ არის რელევანტური, როდესაც ხდება მონაცემთა სუბიექტის ობიექტური მოლოდინების განსაზღვრა. ეს ნიშნავს, რომ მაგალითად, მაღაზიის მფლობელი ვერ დაეყრდნობა მომხმარებლებს, რომლებსაც *ობიექტურად* გააჩნიათ გონივრული მოლოდინი, რომ ისინი დაექვემდებარებიან მონიტორინგს მხოლოდ იმიტომ, რომ შესასვლელთან განთავსებული ნიშანი პირს ატყობინებს მეთვალყურეობის შესახებ.

3.2 დამუშავება აუცილებელია საჯარო ინტერესის სფეროში შემავალი ამოცანების შესასრულებლად ან დამუშავებისთვის პასუხისმგებელი პირისთვის მინიჭებული ოფიციალური უფლებამოსილების განსახორციელებლად, მუხლი 6(1)(e)

41. პერსონალური მონაცემების დამუშავება შესაძლებელია ვიდეომეთვალყურეობის საშუალებით, 6(1)(e) მუხლის საფუძველზე, თუ ეს აუცილებელია საჯარო ინტერესის სფეროში შემავალი ამოცანების შესასრულებლად ან დამუშავებისთვის პასუხისმგებელი პირისთვის მინიჭებული ოფიციალური უფლებამოსილების განსახორციელებლად.[13] ოფიციალური უფლებამოსილების განხორციელება, შესაძლოა, ამგვარ დამუშავებას არ ითვალისწინებდეს, თუმცა, სხვა საკანონმდებლო საფუძვლები, როგორიცაა „ჯანმრთელობა და უსაფრთხოება“ ვიზიტორების ან დასაქმებულების დასაცავად, შესაძლოა, იძლეოდეს დამუშავებას შეზღუდულ ფარგლებში. ამავდროულად, გათვალისწინებული უნდა იქნას GDPR-ით დადგენილი ვალდებულებები და მონაცემთა სუბიექტის უფლებები.

42. წევრ სახელმწიფოებს შესაძლოა ჰქონდეთ ან შესაძლოა დანერგონ კონკრეტული კანონები ვიდეომეთვალყურეობის შესახებ, GDPR-ით განსაზღვრული წესების გამოყენების ადგილობრივ კონტექსტზე ადაპტაციის მიზნით. კერძოდ, ამგვარი კანონები შესაძლოა მეტი სიზუსტით განსაზღვრავდეს დამუშავების კონკრეტულ მოთხოვნებს იმ პირობით, თუ ეს შესაბამისობაშია GDPR-ით დადგენილ პრინციპებთან (მაგ., შენახვის შეზღუდვა, პროპორციულობა).

[13] დამუშავების საფუძველს უნდა ადგენდეს თანამეგობრობის სამართალი ან წევრი სახელმწიფოს კანონი და „აუცლებელი უნდა იყოს საჯარო ინტერესის სფეროში შემავალი ამოცანების შესასრულებლად ან დამუშავებისთვის პასუხისმგებელი პირისთვის მინიჭებული ოფიციალური უფლებამოსილების განსახორციელებლად“ (მუხლი 6(3)).

3.3 თანხმობა, მუხლი 6(1)(a)

43. თანხმობა უნდა იყოს ნებაყოფლობითი, კონკრეტული, ინფორმირებული და მკაფიო, რაც აღწერილია არის თანხმობის შესახებ სახელმძღვანელო პრინციპებში.[14]

44. სისტემატურ მონიტორინგთან დაკავშირებით, მონაცემთა სუბიექტის თანხმობა მე-7 მუხლის თანახმად (იხ. პრეამბულის 43-ე პუნქტი) მხოლოდ გამონაკლის შემთხვევებში იქნება სამართლებრივი საფუძველი. ვიდეომეთვალყურეობის ბუნებიდან გამომდინარე, ტექნოლოგია ერთდროულად ადამიანთა უცნობი რაოდენობის მონიტორინგს ახორციელებს. დამუშავებისთვის პასუხისმგებელი პირი ვერ შეძლებს დაამტკიცოს, რომ მონაცემთა სუბიექტმა გასცა თანხმობა მისი პერსონალური მონაცემების დამუშავებამდე (მუხლი 7(1)). იმ შემთხვევაში, თუ მონაცემთა სუბიექტი უკან გაიხმობს თანხმობას, დამუშავებისთვის პასუხისმგებელი პირისთვის რთული იქნება, დაამტკიცოს, რომ მისი პერსონალური მონაცემების დამუშავება აღარ ხორციელდება (მუხლი 7(3)).

45.

> <u>მაგალითი:</u> სპორტსმენმა, შესაძლოა, ინდივიდუალური ვარჯიშის დროს ითხოვოს მონიტორინგი, რათა შეძლოს საკუთარი ტექნიკის და მომზადების ანალიზი. მეორეს მხრივ, როდესაც სპორტული კლუბი გადაწყვეტს, ამავე მიზნით განახორციელოს მთლიანი გუნდის მონიტორინგი, თახმობა როგორც წესი, არ იქნება ლეგიტიმური, ვინაიდან ცალკეულმა სპორტსმენებმა, შესაძლოა, ვალდებულად ჩათვალონ თავი, გასცენ თანხმობა, რათა მათმა უარმა უარმა უარყოფითი გავლენა არ მოახდინოს მათ გუნდელებზე.

46. თუ დამუშავებისთვის პასუხისმგებელ პირს სურს, დაეყრდნოს თანხმობას, იგი ვალდებულია, უზრუნველყოს, რომ თითოეული მონაცემთა სუბიექტი, რომელიც შედის ვიდეომეთვალყურეობას დაქვემდებარებულ ტერიტორიაზე, გასცემს თანხმობას. ეს თანხმობა უნდა აკმაყოფილებდეს მე-7 მუხლით დადგენილ პირობებს. მონიშნულ ტერიტორიაზე შესვლა (მაგ., როდესაც ადამიანები გადიან ჰოლს ან ჭიშკარს იმისათვის, რომ შევიდნენ მონიტორინგს დაქვემდებარებულ ტერიტორიაზე) არ წარმოადგენს განცხადებას ან აქტიურად გამოხატულ მკაფიო ქმედებას, რომელიც საჭიროა თანხმობისთვის, გარდა იმ შემთხვევისა, თუ ის აკმაყოფილებს მე-4 და მე-7 კრიტერიუმებს (იხ. სახელმძღვანელო პრინციპები თანხმობის შესახებ[15]).

47. იმ ძალთა დისბალანსის გათვალისწინებით, რომელიც არსებობს დამსაქმებლებსა და დასაქმებულებს შორის, უმეტეს შემთხვევაში, დამსაქმებლები არ უნდა დაეყრდნონ

[14] 29-ე მუხლის სამუშაო ჯგუფი (Art. 29 WP), „სახელმძღვანელო პრინციპები თანხმობის შესახებ, 2016/679 რეგულაციის მიხედვით“ (WP 259 rev. 01) - აღიარებულია EDPB-ის მიერ.

[15] 29-ე მუხლის სამუშაო ჯგუფი (Art. 29 WP), „სახელმძღვანელო პრინციპები თანხმობის შესახებ, 2016/679 რეგულაციის მიხედვით“ (WP 259) - აღიარებულია EDPB-ის მიერ.

თანხმობას პერსონალური მონაცემების დამუშავებისას, რადგან ეს თანხმობა ნებაყოფლობითად ვერ ჩაითვლება. ამ კონტექსტში გათვალისწინებული უნდა იქნას თანხმობის შესახებ სახელმძღვანელო პრინციპები.

48. წევრი სახელმწიფოს კანონმდებლობა ან კოლექტიური შეთანხმებები, მათ შორის, „შრომითი ხელშეკრულებები' შესაძლოა ითვალისწინებდეს კონკრეტულ წესებს დასაქმებულთა პერსონალური მონაცემების დამუშავების შესახებ, დასაქმების კონტექსტში (იხ. მუხლი 88).

4. ვიდეოჩანაწერის მესამე მხარეებისთვის გამჟღავნება

49. არსებითად, ვიდეოჩანაწერის მესამე მხარეებისთვის გამჟღავნების (გადაცემის) შემთხვევებზე ვრცელდება GDPR-ის ძირითადი რეგულაციები.

4.1 ვიდეოჩანაწერის გადაცემა მესამე მხარეებისთვის, ზოგადი საკითხები

50. 4(2) მუხლის თანახმად, გამჟღავნება ნიშნავს გადაცემას (მაგ., ინდივიდუალური კომუნიკაცია), გავრცელებას (მაგ., ონლაინ გამოქვეყნება) ან მონაცემთა ხელმისაწვდომობის სხვაგვარად უზრუნველყოფას. მესამე მხარეები განმარტებულია 4(10) მუხლში. მონაცემების მესამე ქვეყნებისთვის ან საერთაშორისო ორგანიზაციებისთვის გამჟღავნებისას, აგრეთვე, მოქმედებს 44-ე მუხლის სპეციალური დებულებები.

51. პერსონალური მონაცემების გამჟღავნება არის პერსონალური მონაცემების დამუშავების ცალკე შემთხვევა, რისთვისაც დამუშავებისთვის პასუხისმგებელ პირს უნდა ჰქონდეს მე-6 მუხლით განსაზღვრული სამართლებრივი საფუძველი.

52.

> <u>მაგალითი:</u> დამუშავებისთვის პასუხისმგებელი პირი, რომელსაც სურს ინტერნეტში ჩანაწერის ატვირთვა, უნდა დაეყრდნოს ამგვარი დამუშავების შესაბამის სამართლებრივ საფუძველს - მაგ., მონაცემთა სუბიექტისგან თანხმობის მოპოვება 6(1)(a) მუხლის შესაბამისად.

53. 6(4) მუხლით გათვალისწინებული წესების თანახმად, დასაშვებია ვიდეოჩანაწერის მესამე მხარეებისთვის გამჟღავნება იმ მიზნით, რომელიც განსხვავდება მონაცემთა შეგროვების მიზნისგან.

54.

მაგალითი: პარკინგის ტერიტორიაზე, დამონტაჟდა ვიდეომეთვალყურეობის სისტემა, რომლის მიზანიც არის მანქანის დაზიანების ფაქტების დაფიქსირება. ადგილი ჰქონდა მანქანის დაზიანებას, ხოლო ჩანაწერი გადაეცა ადვოკატს, საქმის აღძვრის მიზნით. ამ შემთხვევაში, ჩაწერისა და გადაცემის მიზნები არის ერთი და იგივე.

მაგალითი: პარკინგის ტერიტორიაზე, დამონტაჟდა ვიდეომეთვალყურეობის სისტემა, რომლის მიზანიც არის მანქანის დაზიანების ფაქტების დაფიქსირება. კამერის ჩანაწერი გამოქვეყნდა ონლაინ, გასართობი მიზნით. ამ შემთხვევაში, მიზანი შეიცვალა და იგი შეუთავსებელია თავდაპირველ მიზანთან. ამასთან, პრობლემური იქნება მსგავსი დამუშავებისთვის (გამოქვეყნება) სამართლებრივი საფუძვლის იდენტიფიცირება.

55. მესამე მხარემ თავად უნდა განახორციელოს სამართლებრივი ანალიზი, კერძოდ, მოახდინოს სამართლებრივი საფუძვლის იდენტიფიცირება დამუშავებისთვის, მე-6 მუხლის შესაბამისად (მაგ., მასალის მიღება).

4.2 ვიდეოჩანაწერის გამჟღავნება სამართალდამცავი ორგანოსთვის

56. სამართალდამცავი ორგანოსთვის ვიდეოჩანაწერის გადაცემა, აგრეთვე, დამოუკიდებელი პროცესია, რომელიც მოითხოვს ცალკე დასაბუთებას დამუშავებისთვის პასუხისმგებელი პირის მიერ.

57. 6(1)(c) მუხლის თანახმად, დამუშავება არის კანონიერი, თუ ის აუცილებელია დამუშავებისთვის პასუხისმგებელი პირის სამართლებრივი ვალდებულების შესასრულებლად. პოლიციის შესახებ კანონის მიღება წევრი სახელმწიფოს ექსკლუზიურ უფლებამოსილებას წარმოადგენს. ამავდროულად, მაღალი ალბათობით, წევრ სახელმწიფოებში მოქმედებს გარკვეული ზოგადი წესები, რომლებიც არეგულირებს მტკიცებულების გადაცემას სამართალდამცავი ორგანოებისთვის. GDPR-ი დამუშავებას არეგულირებს დამუშავებისთვის პასუხისმგებელი პირის შემთხვევაში, რომელიც ახდენს მონაცემების გადაცემას. თუ ეროვნული კანონმდებლობით დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, ითანამშრომლოს სამართალდამცავ ორგანოებთან (მაგ., გამოძიება), მონაცემთა გადაცემის სამართლებრივ საფუძველს წარმოადგენს 6(1)(c) მუხლით გათვალისწინებული სამართლებრივი მოვალეობა.

58. ამ შემთხვევაში, მიზნის შეზღუდვა, რომელსაც 6(4) მუხლი ითვალისწინებს, არ არის პრობლემური, რადგან ამგვარი გამჟღავნება, ცალსახად რეგულირდება წევრი სახელმწიფოს კანონმდებლობით. შესაბამისად, აღარ მოქმედებს (a)-(e) ქვეპუნქტებით დადგენილი სპეციალური პირობების გათვალისწინების მოთხოვნა.

59.

> <u>მაგალითი:</u> მაღაზიის პატრონს შესასვლელთან განთავსებული აქვს კამერა. ჩანაწერში ჩანს, თუ როგორ ჰპარავს ერთი ადამიანი მეორეს საფულეს. გამოძიების ფარგლებში, პოლიციამ დამუშავებისთვის პასუხისმგებელ პირს მოსთხოვა კამერის ჩანაწერები. ამ შემთხვევაში, მონაცემთა გადასაცემად, მაღაზიის მეპატრონე დაეყრდნობა სამართლებრივ საფუძველს, რომელსაც ითვალისწინებს 6(1)(c) მუხლი (სამართლებრივი ვალდებულება), წაკითხული შესაბამის ეროვნულ კანონთან ერთობლიობაში.

60.

> <u>მაგალითი:</u> მაღაზიაში დამონტაჟებულია კამერა, უსაფრთხოების მიზნებისთვის. მაღაზიის მეპატრონეს სჯერა, რომ კამერამ რაღაც საეჭვო დააფიქსირა და გადაწყვიტა, მასალა პოლიციისთვის გაეგზავნა (ისე, რომ გამოძიება არ არის დაწყებული). ამ შემთხვევაში, მაღაზიის მეპატრონემ უნდა შეაფასოს, თუ რამდენადაა სახეზე 6(1)(f) მუხლით გათვალისწინებული პირობები. როგორც წესი, აღნიშნული პირობები სახეზეა, თუ მაღაზიის მეპატრონეს გონივრული ეჭვი აქვს, რომ დანაშაული იქნა ჩადენილი.

61. სამართალდამცავი ორგანოების მიერ პერსონალური მონაცემების დამუშავება, როგორც ასეთი, რეგულირდება არა GDPR-ით (იხ. მუხლი 2(2)(d)), არამედ, სამართალდამცავი ორგანოების მიერ მონაცემთა დამუშავების შესახებ დირექტივით (EU2016/680).

5. განსაკუთრებული კატეგორიის მონაცემთა დამუშავება

62. ვიდეომეთვალყურეობის სისტემები, როგორც წესი, მასობრივი მოცულობის პერსონალური მონაცემების შეგროვებას ითვალისწინებს, რაც, შესაძლოა მოიცავდეს უაღრესად პერსონალურ მონაცემებს და განსაკუთრებული კატეგორიის მონაცემებსაც კი. მართლაც, თავდაპირველად ვიდეოს საშუალებით შეგროვებული, ერთი შეხედვით უმნიშვნელო მონაცემების საფუძველზე შესაძლებელია სხვა ინფორმაციის დედუცირება, რომელიც გამოყენებული იქნება განსხვავებული მიზნის მისაღწევად (მაგ., პირის ჩვევების განსაზღვრა). ამავდროულად, ეს არ ნიშნავს, რომ ვიდეომეთვალყურეობის საშუალებით ყოველთვის მუშავდება განსაკუთრებული კატეგორიის პერსონალური მონაცემები.

63.

მაგალითი: ვიდეოჩანაწერი ასახავს მონაცემთა სუბიექტს, რომელსაც სათვალეები უკეთია ან იყენებს ხელჯოხს. ამგვარი მონაცემები, როგორც ასეთი, არ მიიჩნევა განსაკუთრებული კატეგორიის პერსონალურ მონაცემებად.

64. ამავდროულად, თუ ვიდეოჩანაწერის დამუშავება ხდება განსაკუთრებული კატეგორიის მონაცემების დედუცირების მიზნით, მოქმედებს მე-9 მუხლი.

65.

მაგალითი: იმ სურათებზე დაყრდნობით, რომელიც ასახავს იდენტიფიცირებადი მონაცემთა სუბიექტების მიერ გარკვეულ ღონისძიებაში, გაფიცვაში და ა.შ. მონაწილეობის მიღებას, შესაძლებელია მათი პოლიტიკური შეხედულებების დედუცირება. აღნიშნული ხვდება მე-9 მუხლის მოქმედების ქვეშ.

მაგალითი: საავადმყოფო, სადაც დამონტაჟებულია ვიდეოკამერა, პაციენტის ჯანმრთელობის მდგომარეობაზე დაკვირვების მიზნით, ამუშავებს განსაკუთრებული კატეგორიის პერსონალურ მონაცემებს (მუხლი 9).

66. ზოგადი პრინციპის სახით, ვიდეომეთვალყურეობის სისტემის დამონტაჟებისას, განსაკუთრებული ყურადღება უნდა მიექცეს მონაცემთა მინიმიზაციის პრინციპს. ამრიგად, მაშინაც კი, თუ 9(1) მუხლი არ მოქმედებს, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, ყოველთვის მინიმუმამდე შეამციროს ვიდეოკამერის მიერ იმგვარი კადრების დაფიქსირება, რომელიც შეიცავს სხვა სახის მგრძნობიარე მონაცემებს (მე-9 მუხლის მიღმა), მიზნის მიუხედავად.

67.

მაგალითი: ვიდეომეთვალყურეობის სისტემა, რომელიც ეკლესიაშია დამონტაჟებული, როგორც ასეთი, მე-9 მუხლის მოქმედების სფეროში არ ხვდება. თუმცა, დამუშავებისთვის პასუხისმგებელმა პირმა განსაკუთრებული სიფრთხილით უნდა შეაფასოს აღნიშნული, 6(1)(f) მუხლის საფუძველზე, მონაცემთა ხასიათისა და სხვა მგრძნობიარე მონაცემების დაფიქსირების რისკის გათვალისწინებით (მე-9 მუხლის მიღმა), მონაცემთა სუბიექტის ინტერესების შეფასებისას.

68. იმ შემთხვევაში, თუ ვიდეომეთვალყურეობის სისტემა გამოიყენება განსაკუთრებული კატეგორიის მონაცემების დამუშავებისთვის, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, მოახდინოს განსაკუთრებული კატეგორიის მონაცემთა დამუშავებისთვის მე-9 მუხლით გათვალისწინებული გამონაკლისის იდენტიფიცირება, (ე.ი., განსაკუთრებული კატეგორიის მონაცემთა დამუშავების

აკრძალვის შესახებ მოქმედი წესიდან გამონაკლისი) და განსაზღვროს მე-6 მუხლით გათვალისწინებული სამართლებრივი საფუძველი.

69. მაგალითად, 9(2)(c) მუხლი („[...] მონაცემთა დამუშავება საჭიროა მონაცემთა სუბიექტის ან სხვა ფიზიკური პირის სასიცოცხლო ინტერესების დასაცავად“ [...]) შესაძლებელია - თეორიულად და გამონაკლისის სახით - გამოყენებული იქნას, თუმცა, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, დაამტკიცოს, რომ ეს აბსოლუტურად აუცილებელია პირის სასიცოცხლო ინტერესების დასაცავად, ხოლო „[...] სუბიექტს *ფიზიკურად ან სამართლებრივად არ შესწევს უნარი, თანხმობა განაცხადოს დამუშავებაზე.“* ამას გარდა, დამუშავებისთვის პასუხისმგებელ პირს არ ექნება უფლება, სისტემა რაიმე სხვა მიზნით გამოიყენოს.

70. მნიშვნელოვანია, აღინიშნოს, რომ მე-9 მუხლით გათვალისწინებული გამონაკლისი, სავარაუდოდ, არ იქნება გამოსადეგი იმისათვის, რომ დამუშავებისთვის პასუხისმგებელმა პირმა დაასაბუთოს განსაკუთრებული კატეგორიის მონაცემთა დამუშავება ვიდეომეთვალყურეობის საშუალებით. კერძოდ, დამუშავებისთვის პასუხისმგებელი პირები, რომლებიც ამ მონაცემებს ამუშავებენ ვიდეომეთვალყურეობის კონტექსტში, ვერ დაეყრდნობიან 9(2)(e) მუხლს, რომლის თანახმადაც დასაშვებია მონაცემთა სუბიექტის მიერ ცალსახად გამოქვეყნებული პერსონალური მონაცემების დამუშავება. მხოლოდ ის ფაქტი, რომ მონაცემთა სუბიექტი კამერების დაფარვის ზონაში შევიდა, არ გულისხმობს, რომ მონაცემთა სუბიექტი აპირებს, საჯარო გახადოს მასთან დაკავშირებული განსაკუთრებული კატეგორიის მონაცემები.

71. ამას გარდა, განსაკუთრებული კატეგორიის მონაცემთა დამუშავება საჭიროებს გარკვეული ვალდებულებების ზედმიწევნით და უწყვეტად დაცვას; მაგალითად, უსაფრთხოების მაღალი დონე და მონაცემთა დაცვაზე ზეგავლენის შეფასება, საჭიროების შესაბამისად.

72.

> <u>მაგალითი:</u> დამსაქმებელმა გაფიცულთა იდენტიფიცირების მიზნით არ უნდა გამოიყენოს ვიდეომეთვალყურეობის სისტემიდან ამოღებული ჩანაწერი, რომელიც ასახავს დემონსტრაციას.

5.1 ბიომეტრიული მონაცემების დამუშავებისას გასათვალისწინებელი ზოგადი საკითხები

73. ბიომეტრიული მონაცემების გამოყენება, კერძოდ, სახის ამოცნობა მომეტებულ რისკებს უქმნის მონაცემთა სუბიექტის უფლებებს. უაღრესად მნიშვნელოვანია, რომ ამგვარი ტექნოლოგიების გამოყენება განხორციელდეს GDPR-ით დადგენილი

კანონიერების, აუცილებლობის, პროპორციულობის და მონაცემთა მინიმიზაციის პრინციპების სათანადო პატივისცემის საფუძველზე. იმ შემთხვევაში, თუ აღნიშნული ტექნოლოგიების გამოყენება განსაკუთრებით ეფექტურ საშუალებად არის მიჩნეული, დამუშავებისთვის პასუხისმგებელმა პირმა, პირველ რიგში, უნდა შეაფასოს ტექნოლოგიების ზეგავლენა ფუნდამენტურ უფლებებსა და თავისუფლებებზე და უფლებების ყველაზე ნაკლებად შემზღუდავი საშუალება გამოიყენოს დამუშავების ლეგიტიმური მიზნის მისაღწევად.

74. იმისათვის, რომ მონაცემები მიჩნეული იქნას ბიომეტრიულ მონაცემებად (GDPR-ის განმარტების შესაბამისად), პირველადი („ნედლი“) მონაცემების დამუშავება, როგორიცაა ფიზიკური პირის ფიზიკური, ფიზიოლოგიური ან ქცევითი მახასიათებლები, ამ მახასიათებლების შეფასებას („გაზომვას“) უნდა გულისხმობდეს. ვინაიდან ბიომეტრიული მონაცემები ამგვარი შეფასების შედეგია, GDPR-ის 4.14 მუხლში წარმოდგენილი განმარტების თანახმად, ბიომეტრიული მონაცემები *„ნიშნავს პერსონალურ მონაცემებს, რომლებიც მიიღება ფიზიკური პირის ფიზიკური, ფიზიოლოგიური ან ქცევითი მონაცემების კონკრეტული ტექნიკური დამუშავების შედეგად და რომელიც იძლევა ფიზიკური პირის უნიკალურად იდენტიფიცირების ან იდენტიფიკაციის დადასტურების საშუალებას“*. ამავდროულად, ფიზიკური პირის ვიდეოჩანაწერი, როგორც ასეთი, ვერ იქნება მიჩნეული ბიომეტრიულ მონაცემებად, მე-9 მუხლის შესაბამისად, თუ მისი კონკრეტული ტექნიკური დამუშავება არ ემსახურება ფიზიკური პირის იდენტიფიცირების მიზანს.[16]

75. ბიომეტრიული მონაცემები უნდა მუშავდებოდეს „ფიზიკური პირის უნიკალური იდენტიფიცირების მიზნით“ იმისათვის, რომ დამუშავება ჩაითვალოს განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავებად (მუხლი 9).

76. მოკლედ რომ შევაჯამოთ, მე-4 მუხლის მე-14 პუნქტისა და მე-9 მუხლის მიხედვით, გათვალისწინებული უნდა იქნას შემდეგი სამი კრიტერიუმი:

    - მონაცემების ხასიათი: მონაცემები, რომლებიც დაკავშირებულია ფიზიკური პირის ფიზიკურ, ფსიქოლოგიურ ან ქცევით მახასიათებლებთან;
    - დამუშავების საშუალებები და გზა: „კონკრეტული ტექნიკური დამუშავების შედეგად“ მიღებული მონაცემები;
    - დამუშავების მიზანი: მონაცემები გამოყენებული უნდა იქნას ფიზიკური პირის უნიკალური იდენტიფიცირების მიზნით.

[16] GDPR-ის პრეამბულის 51-ე პუნქტი მხარს უჭერს აღნიშნულ ანალიზს. კერძოდ, ამ პუნქტის თანახმად: *„[...] ფოტოების დამუშავება შეიძლება არ ჩაითვალოს განსაკუთრებული კატეგორიის პერსონალურ მონაცემთა დამუშავებად, ვინაიდან ფოტოები შეესაბამება ბიომეტრიული მონაცემების განმარტებას მხოლოდ მაშინ, როცა მათ დამუშავება ხდება სპეციალური ტექნიკური საშუალებებით, რომლებიც ფიზიკური პირის ამოცნობის ან დადგენის საშუალებას იძლევა. ამგვარი მონაცემები არ უნდა დამუშავდეს გარდა ამ რეგულაციით განსაზღვრული შემთხვევებისა. [...]“*

77. ვიდეომეთვალყურეობის გამოყენება, მათ შორის, ბიომეტრიული ამოცნობის ფუნქცია, რომელიც დამონტაჟებულია კერძო პირების მიერ, საკუთარი მიზნებისთვის (მაგ., მარკეტინგული, სტატისტიკური ან უსაფრთხოების მიზნებისთვის), უმეტეს შემთხვევაში, ყველა მონაცემთა სუბიექტისგან ცალსახა თანხმობას საჭიროებს (მუხლი 9(2)(a)). ამავდროულად, შესაძლებელია გამოყენებული იქნას მე-9 მუხლით გათვალისწინებული გამონაკლისი.

78.

> <u>მაგალითი:</u> საკუთარი მომსახურების გაუმჯობესების მიზნით, კერძო კომპანიამ აეროპორტში, გამსვლელ პუნქტებში, სადაც ხდება მომხმარებელთა იდენტიფიცირება (ბარგის ჩაბარებისას, ბორტზე ასვლისას) განათავსა ვიდეომეთვალყურეობის სისტემები, რომელიც სახის ამოცნობის ტექნიკის გამოყენებით ახდენს იმ მგზავრების იდენტიფიცირებას, რომლებიც დაეთანხმდნენ ამგვარ პროცედურას. ვინაიდან დამუშავება მე-9 მუხლის მოქმედების სფეროში შედის, მგზავრები, რომელთაც გასცეს ცალსახა და ინფორმირებული თანხმობა, უნდა გამოცხადდნენ, მაგალითად, ავტომატურ ტერმინალთან, რათა შექმნან და დაარეგისტრირონ თავიანთი სახის ნიმუში (facial template), რომელიც დაუკავშირდება მათ ჩასხდომის ბარათს და ვინაობას. ის გამსვლელი პუნქტები, სადაც განთავსებულია სახის ამოცნობის ტექნოლოგია, მკაფიოდ უნდა იყოს განცალკევებული, მაგ., სისტემა უნდა დამონტაჟდეს სპეციალური სტრუქტურის ფარგლებში, რათა იმ პირთა ბიომეტრიული შაბლონები, რომელთაც თანხმობა არ გაუციათ, არ დაფიქსირდეს აღნიშნული სისტემის მიერ. ბიომეტრიული სისტემით აღჭურვილი სტრუქტურის (პორტალის) გამოყენებას შეძლებენ მხოლოდ ის მგზავრები, რომელთაც გამოხატეს თანხმობა და დაარეგისტრირეს თავიანთი სახის ნიმუში.
>
> <u>მაგალითი:</u> დამუშავებისთვის პასუხისმგებელი პირი საკუთარ შენობებში ადამიანების შესვლას აკონტროლებს სახის ამოცნობის მეთოდის გამოყენებით. ადამიანებს ამ საშუალების გამოყენება შენობაში შესასვლელად შეუძლიათ იმ შემთხვევაში, თუ წინასწარ გასცემენ მკაფიო ინფორმირებულ თანხმობას, 9(2)(a) მუხლის შესაბამისად. ამავდროულად, იმისათვის, რომ სახის ამოცნობის სისტემაში არ დაფიქსირდეს ისეთი ადამიანი, ვისაც თანხმობა არ გაუცია, სისტემის ამოქმედება უნდა მოხდეს თავად მონაცემთა სუბიექტის მიერ, მაგალითად, ღილაკზე ხელის მიჭერით. დამუშავების კანონიერების უზრუნველყოფისთვის, დამუშავებისთვის პასუხისმგებელმა პირმა ყოველთვის უნდა უზრუნველყოს შენობაში შესვლის ალტერნატიული საშუალება, ბიომეტრიული დამუშავების გარეშე, როგორიცაა, სამკერდე ნიშანი ან გასაღები.

79. ამ ტიპის შემთხვევაში, როდესაც ბიომეტრიული ნიმუშების გენერირება ხდება, დამუშავებისთვის პასუხისმგებელმა პირებმა უნდა უზრუნველყონ, რომ შედეგის

(„დაემთხვა“ ან „არ დაემთხვა“) მიღებისთანავე, სწრაფად და უსაფრთხოდ უნდა წაიშალოს ყველა შუალედური ნიმუში, რომელიც შეიქმნა ადგილზე, ფიზიკური პირის მკაფიო და ინფორმირებული თანხმობის საფუძველზე რეგისტრაციის დროს გენერირებულ ნიმუშთან შედარების მიზნით. რეგისტრაციისთვის შექმნილი ნიმუშები უნდა შენარჩუნდეს მხოლოდ და მხოლოდ დამუშავების მიზნის რეალიზებისთვის და დაუშვებელია მათი შენახვა ან დაარქივება.

80. ამავდროულად, როდესაც დამუშავების მიზანია, მაგალითად, ადამიანთა ორი სხვადასხვა კატეგორიის ერთმანეთისგან გარჩევა და არა რომელიმე კონკრეტული პირის უნიკალურად იდენტიფიცირება, დამუშავება არ ხვდება მე-9 მუხლის მოქმედების ფარგლებში.

81.

> <u>მაგალითი:</u> მაღაზიის მეპატრონეს სურს, რომ თავისი რეკლამა მოარგოს მომხმარებელთა სხვადასხვა კატეგორიებს, მათი გენდერული და ასაკობრივი მახასიათებლების მიხედვით, ხოლო ამ მახასიათებლებს აფიქსირებს ვიდეომეთვალყურეობის სისტემა. თუ ეს სისტემა არ ახდენს ბიომეტრიული ნიმუშების გენერირებას ადამიანთა უნიკალურად იდენტიფიცირებისთვის, არამედ, მხოლოდ ახდენს აღნიშნული ფიზიკური მახასიათებლების გამოვლენას, ადამიანთა სხვადასხვა კატეგორიებად დაყოფისთვის, მაშინ დამუშავება არ მოხვდება მე-9 მუხლის მოქმედების სფეროში (თუ არ მუშავდება სხვა ტიპის განსაკუთრებული კატეგორიის მონაცემები).

82. ამავდროულად, მე-9 მუხლი მოქმედებს, თუ დამუშავებისთვის პასუხისმგებელი პირი ბიომეტრიულ მონაცემებს ინახავს (როგორც წესი, ნიმუშების გამოყენებით, რომლებიც შექმნილია „ნედლი“ ბიომეტრიული მონაცემებიდან ძირითადი მახასიათებლების ამოღებით - მაგ., გამოსახულებიდან ამოღებული სახის ზომები), პირის უნიკალურად იდენტიფიცირების მიზნით. თუ დამუშავებისთვის პასუხისმგებელ პირს სურს, რომ გამოავლინოს მონაცემთა სუბიექტის მიერ ტერიტორიაზე განმეორებით შესვლა ან სხვა ტერიტორიაზე შესვლა (მაგ., მისთვის უწყვეტი პერსონალიზებული რეკლამის ჩვენების მიზნით), ამ შემთხვევაში, მიზანი იქნება ფიზიკური პირის უნიკალურად იდენტიფიცირება, რაც ნიშნავს იმას, რომ აღნიშნული ოპერაცია თავიდანვე მე-9 მუხლის მოქმედების სფეროში შევა. ასეთ შემთხვევას ადგილი აქვს, როდესაც დამუშავებისთვის პასუხისმგებელი პირი წარმოებულ ნიმუშებს ინახავს მაღაზიაში განთავსებულ რამდენიმე დაფაზე პერსონალიზებული რეკლამის მოთავსების მიზნით. ვინაიდან სისტემა იყენებს ფიზიკურ მახასიათებლებს კონკრეტული პირების კამერის დაფარვის არეალში დაბრუნების გამოსავლენად (მაგ., სავაჭრო ცენტრის ვიზიტორები) და მათი მონიტორინგისთვის, აღნიშნული წარმოადგენს ბიომეტრიული იდენტიფიცირების მეთოდს, რადგან იგი მიმართულია სპეციფიკური ტექნიკური დამუშავების გამოყენებით ფიზიკური პირების ამოცნობისკენ.

83.

> მაგალითი: მაღაზიის მეპატრონემ დაამონტაჟა სახის ამოცნობის სისტემა, რეკლამის პერსონალიზების მიზნებისთვის. დამუშავებისთვის პასუხისმგებელმა პირმა მკაფიო და ინფორმირებული თანხმობა უნდა მოიპოვოს ყველა მონაცემთა სუბიექტისგან, ბიომეტრიული სისტემის გამოყენებამდე და პერსონალიზებული რეკლამის მიწოდებამდე. სისტემა უკანონო იქნება, თუ იგი აფიქსირებს ვიზიტორებს ან გამვლელებს, რომელთაც თანხმობა არ გაუციათ მათი ბიომეტრიული ნიმუშის შექმნაზე, მაშინაც კი, თუ ნიმუშის წაშლა ხდება მაქსიმალურად მოკლე ვადაში. მართლაც, ეს დროებითი ნიმუშები წარმოადგენს ბიომეტრიულ მონაცემებს, რომელთა დამუშავებაც ხდება იმ პირის უნიკალურად იდენტიფიცირებისთვის, რომელსაც შესაძლოა სურდეს პერსონალიზებული (მიზნობრივი) რეკლამის მიღება.

84. EDPB-ის დაკვირვებით, ზოგიერთი ბიომეტრიული სისტემის დამონტაჟება ხდება უკონტროლო გარემოში[17], რაც ნიშნავს იმას, რომ სისტემა გულისხმობს ადგილზე ყველა იმ პირის სახის დაფიქსირებას, რომელიც გაივლის კამერის დაფარვის არეალში, მათ შორის, იმ პირებისა, რომელთაც არ გაუციათ თანხმობა ბიომეტრიულ მოწყობილობაზე და შესაბამისად, ბიომეტრიული ნიმუშების შექმნაზე. აღნიშნული ნიმუშები დარდება იმ ნიმუშებს, რომლებიც მონაცემთა სუბიექტებმა (ე.ი., ბიომეტრიული მოწყობილობის მომხმარებლებმა) შექმნეს რეგისტრაციის პროცესში, იმისათვის, რომ დამუშავებისთვის პასუხისმგებელმა პირმა შეძლოს იმის დადგენა, არის თუ არა პირი ბიომეტრიული მოწყობილობის მომხმარებელი. ამ შემთხვევაში, სისტემა ხშირად შექმნილია იმისათვის, რომ ერთმანეთისაგან გაარჩიოს პირები, რომელთა ამოცნობაც უნდა მოახდინოს სისტემამ და ისინი, ვინც არ არიან დარეგისტრირებულები. ვინაიდან მიზანს წარმოადგენს ფიზიკური პირების უნიკალურად იდენტიფიცირება, 9(2) მუხლით გათვალისწინებული გამონაკლისის პირობები დაცული უნდა იქნას ყველა იმ პირის შემთხვევაში, რომელსაც კამერა აფიქსირებს.

85.

> მაგალითი: სასტუმრო იყენებს ვიდეომეთვალყურეობას, რათა სასტუმროს მენეჯერს ავტომატურად შეატყობინოს VIP სტუმრის შემოსვლის შესახებ, მას შემდეგ, რაც მოხდება სტუმრის სახის ამოცნობა. VIP სტუმრები წინასწარ გასცემენ თანხმობას სახის ამოცნობის გამოყენებაზე, ხოლო შემდგომ ხდება ამ მიზნით შექმნილ მონაცემთა ბაზაში მათი მონაცემების დაფიქსირება. ბიომეტრიული მონაცემების

[17] ეს ნიშნავს, რომ ბიომეტრიული მოწყობილობა განთავსებულია საზოგადოებრივ სივრცეში და აფიქსირებს ნებისმიერ გამვლელს, ხოლო კონტროლირებად გარემოში განთავსებული ბიომეტრიული სისტემების გამოყენება შესაძლებელია მხოლოდ იმ პირის მიერ, რომელმაც გასცა თანხმობა.

დამუშავების აღნიშნული სისტემები უკანონო იქნება, თუ VIP სტუმრების იდენტიფიცირების მიზნით მიმდინარე მონიტორინგს დაქვემდებარებულ სხვა სტუმრებს არ გაუციათ თანხმობა დამუშავებაზე, 9(2)(a)მუხლის შესაბამისად.

<u>მაგალითი:</u> დამუშავებისთვის პასუხისმგებელმა პირმა, საკონცერტო დარბაზის შესასვლელში, რომელსაც იგი მართავს, დაამონტაჟა სახის ამომცნობი ვიდეომეთვალყურეობის სისტემა. დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, მოაწყოს ერთმანეთისგან მკაფიოდ გამიჯნული ორი შესასვლელი; ერთ შესასვლელს ექნება ბიომეტრიული სისტემა, მეორეს კი არა (ხოლო ბიომეტრიული მონაცემების დამუშავების ნაცვლად, მომხმარებლები, მაგალითად, დაასკანერებენ ბილეთებს). ბიომეტრიული მოწყობილობებით აღჭურვილი შესასვლელები უნდა მოეწყოს იმგვარად, რომ სისტემამ არ დააფიქსიროს იმ მომხმარებელთა ბიომეტრიული მონაცემები, რომელთაც თანხმობა არ გაუციათ.

86. და ბოლოს, როდესაც GDPR-ის მე-9 მუხლი ითხოვს თანხმობას, დამუშავებისთვის პასუხისმგებელმა პირმა სერვისებზე წვდომა არ უნდა დაუკავშიროს ბიომეტრიულ დამუშავებაზე თანხმობის გაცემას. სხვა სიტყვებით რომ ვთქვათ და განსაკუთრებით მაშინ, როდესაც ბიომეტრიული დამუშავება გამოიყენება ვინაობის დადგენის მიზნით, დამუშავებისთვის პასუხისმგებელმა პირმა უნდა უზრუნველყოს ალტერნატიული გზა, რომელიც არ გულისხმობს ბიომეტრიული მონაცემების დამუშავებას - ისე, რომ მონაცემთა სუბიექტი არ დაექვემდებაროს რაიმე შეზღუდვებს ან დამატებით ხარჯებს. ალტერნატიული გზა, აგრეთვე, საჭიროა იმ პირებისთვის, რომლებიც ვერ აკმაყოფილებენ ბიომეტრიული მოწყობილობის მოთხოვნებს (დარეგისტრირება ან ბიომეტრიული მონაცემების წაკითხვა შეუძლებელია, შეზღუდული შესაძლებლობა ართულებს ბიომეტრიული მოწყობილობის გამოყენებას და ა.შ.). ამასთან, თუ ბიომეტრიული მოწყობილობა არ იქნება ხელმისაწვდომი (მაგ., თუ მოწყობილობა გაუმართავია), უნდა არსებობდეს „ალტერნატიული გზა“, რაც სერვისის უწყვეტობას უზრუნველყოფს. თუმცა, აღნიშნული გზა გამონაკლის შემთხვევებში უნდა იქნას გამოყენებული. გამონაკლის შემთხვევებში, შესაძლებელია, რომ ბიომეტრიული მონაცემების დამუშავება ხელშეკრულებით გათვალისწინებული მომსახურების ძირითად აქტივობას წარმოადგენდეს, მაგ., მუზეუმმა მოაწყო გამოფენა, რომელიც ახდენს სახის ამომცნობი მოწყობილობის გამოყენების დემონსტრირებას, რა შემთხვევაშიც მონაცემთა სუბიექტი ვერ შეძლებს ბიომეტრიული მონაცემების დამუშავებაზე უარის თქმას, თუ მას გამოფენაში მონაწილეობის მიღება სურს. ასეთ შემთხვევაში, მე-9 მუხლის თანახმად მოპოვებული თანხმობა ლეგიტიმური იქნება, თუ სრულდება მე-7 მუხლით დადგენილი მოთხოვნები.

5.2 ბიომეტრიული მონაცემების დამუშავებისას რისკების შესამცირებელი ზომები

87. მონაცემთა მინიმიზაციის პრინციპის შესაბამისად, დამუშავებისთვის პასუხისმგებელმა პირებმა უნდა უზრუნველყონ, რომ ნიმუშის შესაქმნელად ციფრული გამოსახულებიდან ამოღებული მონაცემების გამოყენება არ მოხდება გადაჭარბებულად და ეს მონაცემები შეიცავს მხოლოდ იმ ინფორმაციას, რომელიც კონკრეტული მიზნისთვის არის საჭირო, რაც ხელს შეუწყობს შესაძლო შემდგომი დამუშავების თავიდან აცილებას. საჭიროა, დაინერგოს ზომები, რომელიც მოახდენს ბიომეტრიულ სისტემებს შორის ნიმუშების გადაცემის პრევენციას.

88. იდენტიფიცირება და ავთენტურობის დადგენა/ვერიფიკაცია, როგორც წესი, მოითხოვს ნიმუშის შენახვას, რომლის გამოყენებაც მოხდება მოგვიანებით, შედარების მიზნით. დამუშავებისთვის პასუხისმგებელმა პირმა უნდა გაითვალისწინოს, თუ რა იქნება ყველაზე შესაფერისი ადგილი მონაცემების შესანახად. კონტროლირებად გარემოში (დელიმიტირებული ჰოლები ან გამსვლელი პუნქტები), ნიმუშები შენახული უნდა იქნას ინდივიდუალურ მოწყობილობაზე, რომელიც იქნება მომხმარებლის ხელთ და მისი ექსკლუზიური კონტროლის ქვეშ (სმარტფონში ან ID ბარათში), ან კონკრეტული მიზნებისა და ობიექტური საჭიროებების გათვალისწინებით, შესაძლებელია მონაცემების შენახვა ცენტრალიზებულ მონაცემთა ბაზაში, დაშიფრული ფორმით, ხოლო გასაღები მუდმივად იქნება მომხმარებლის ხელთ, რაც უზრუნველყოფს ნიმუშზე ან შესანახ ადგილზე არაავტორიზებული წვდომის პრევენციას. თუ ნიმუშებზე დამუშავებისთვის პასუხისმგებელი პირის წვდომა გარდაუვალია, მაშინ, მან სათანადო ნაბიჯები უნდა გადადგას შენახული მონაცემების უსაფრთხოებისთვის. ეს შესაძლოა, მოიცავდეს ნიმუშის დაშიფვრას კრიპტოგრაფული ალგორითმის გამოყენებით.

89. ნებისმიერ შემთხვევაში, დამუშავებისთვის პასუხისმგებელმა პირმა სიფრთხილის ყველა საჭირო ზომა უნდა მიიღოს იმისათვის, რომ დაცული იქნას დამუშავებული მონაცემების ხელმისაწვდომობა, ხელშეუხებლობა და კონფიდენციალურობა. ამ მიზნით, დამუშავებისთვის პასუხისმგებელმა პირმა უნდა მიიღოს შემდეგი ზომები: გადაცემის და შენახვის დროს მონაცემების დაყოფა კატეგორიებად (compartmentalize); ბიომეტრიული ნიმუშების და პირველადი („ნედლი“) მონაცემების ან ვინაობის აღმნიშვნელი მონაცემების შენახვა ცალკე მონაცემთა ბაზაში; ბიომეტრიული მონაცემების დაშიფვრა, განსაკუთრებით, ბიომეტრიული ნიმუშების; და დაშიფვრისა და გასაღების მართვის პოლიტიკის განსაზღვრა; ორგანიზაციული და ტექნიკური ზომების დანერგვა (ინტეგრაცია) თაღლითობის გამოსავლენად; მონაცემთა უსაფრთხოების კოდის ასოცირება მონაცემებთან (მაგ., ხელმოწერა ან ჰეშ-კოდი) და ბიომეტრიულ მონაცემებზე გარე წვდომის აკრძალვა. ასეთი ზომები ტექნოლოგიების წინსვლასთან ერთად უნდა განვითარდეს.

90. ამას გარდა, დამუშავებისთვის პასუხისმგებელმა პირებმა უნდა უზრუნველყონ პირველადი („ნედლი“) მონაცემების (სახის გამოსახულებები, მეტყველებითი სიგნალები, ანაბეჭდი და ა.შ.) წაშლა და წაშლის ეფექტურობა. თუ დამუშავებისთვის კანონიერი საფუძველი აღარ არსებობს, პირველადი („ნედლი“) მონაცემები უნდა წაიშალოს. მართლაც, იმდენად, რამდენადაც ბიომეტრიული ნიმუშები ამგვარი მონაცემებიდან იწარმოება, შეიძლება ითქვას, რომ მონაცემთა ბაზის შექმნა იგივე საფრთხეს ქმნის (შესაძლოა, უფრო მეტ საფრთხესაც), ვიდრე ბიომეტრიული ნიმუშის წაკითხვა, ვინაიდან ბიომეტრიული ნიმუშის ინტერპრეტაცია იმ ინფორმაციის გარეშე, თუ როგორ მოხდა მისი დაპროგრამება, შესაძლოა რთული იყოს, მაშინ, როდესაც პირველადი მონაცემები ნებისმიერი ნიმუშის ფუნდამენტურ კომპონენტებს ქმნის. თუ საჭიროა, რომ დამუშავებისთვის პასუხისმგებელმა პირმა ამგვარი მონაცემები შეინახოს, მიზანშეწონილია გათვალისწინებული იქნას მონაცემებისთვის „ხმაურის დამატების მეთოდების“ (noise-additive methods) გამოყენების შესაძლებლობა (მაგ., „წყლის ნიშნის“ დატანა), რაც შეუძლებელს გახდის ეფექტური ნიმუშის შექმნას. ამასთან, დამუშავებისთვის პასუხისმგებელმა პირმა უნდა წაშალოს ბიომეტრიული მონაცემები და ნიმუშები, წაკითხვა-შედარების ტერმინალზე ან მონაცემთა შესანახ სერვერზე არაავტორიზებული წვდომის შემთხვევაში და მას შემდეგ, რაც ამოიწურება ბიომეტრიული მოწყობილობის ოპერაციულ სიცოცხლე, წაშალოს ნებისმიერი მონაცემი, რომელიც შემდგომი დამუშავებისთვის არ გამოდგება.

6. მონაცემთა სუბიექტის უფლებები

91. ვიდეომეთვალყურეობის გამოყენებისას მონაცემთა დამუშავების ხასიათის გათვალისწინებით, GDPR-ით დადგენილი მონაცემთა სუბიექტის ზოგიერთი უფლება საჭიროებს დამატებით განმარტებას. თუმცა, წინამდებარე თავი არ არის ამომწურავი და GDPR-ით გათვალისწინებული ყველა უფლება ვრცელდება პერსონალური მონაცემების დამუშავებაზე ვიდეომეთვალყურეობის გზით.

6.1 მონაცემებზე წვდომის უფლება

92. მონაცემთა სუბიექტს უფლება აქვს, დამუშავებისთვის პასუხისმგებელი პირისგან მოიპოვოს დადასტურება, მუშავდება თუ არა მისი მონაცემები. ვიდეომეთვალყურეობის შემთხვევაში, აღნიშნული ნიშნავს, რომ თუ არ ხდება მონაცემების შენახვა ან გადაცემა, რეალურ დროში მონიტორინგის მომენტის გასვლის შემდეგ, დამუშავებისთვის პასუხისმგებელი პირი შეძლებს, გასცეს ინფორმაცია, რომ პერსონალური მონაცემების დამუშავება აღარ ხდება (იმ ინფორმაციის გარდა, რომლის მონაცემთა სუბიექტისათვის მიწოდების ვალდებულებასაც ადგენს მე-13 მუხლი, იხ. მე-7 სექცია - გამჭვირვალობასთან და ინფორმაციის მიწოდებასთან დაკავშირებული ვალდებულებები). ამავდროულად, თუ მოთხოვნის წარდგენის

მომენტში, მონაცემთა დამუშავება გრძელდება (ე.ი., თუ მონაცემები ინახება ან უწყვეტად მუშავდება, რაიმე სხვა ფორმით), მონაცემთა სუბიექტი უზრუნველყოფილი უნდა იქნას წვდომითა და ინფორმაციით, მე-15 მუხლის შესაბამისად.

93. ამავდროულად, მოქმედებს რამდენიმე შეზღუდვა, რომელიც ზოგ შემთხვევაში ვრცელდება მონაცემებზე წვდომის უფლებაზე.

- GDPR-ის 15(4) მუხლი, უარყოფითი გავლენა სხვების უფლებებზე

94. იმის გათვალისწინებით, რომ ვიდეომეთვალყურეობის ჩანაწერებში, შესაძლოა, დაფიქსირდეს ერთზე მეტი მონაცემთა სუბიექტი, ამ ჩანაწერების ჩვენება გამოიწვევს სხვა მონაცემთა სუბიექტების პერსონალური მონაცემების დამატებით დამუშავებას. თუ მონაცემთა სუბიექტი მოუსურვებს, მიიღოს მასალის ასლი (მუხლი 15(3)), ამან, შესაძლოა, უარყოფითი გავლენა მოახდინოს ამავე მასალაში ასახული სხვა მონაცემთა სუბიექტის უფლებებზე და თავისუფლებებზე. აღნიშნული შედეგის თავიდან ასაცილებლად, დამუშავებისთვის პასუხისმგებელმა პირმა უნდა გაითვალისწინოს, რომ ვიდეოჩანაწერის ინვაზიური ბუნების გათვალისწინებით, ზოგ შემთხვევაში, არ უნდა მოხდეს ისეთი ვიდეოჩანაწერის გაცემა, რომელშიც შესაძლებელია სხვა მონაცემთა სუბიექტების იდენტიფიცირება. ამავდროულად, მესამე მხარეთა უფლებების დაცვა არ უნდა იქნას გამოყენებული, როგორც ფიზიკურ პირთა ლეგიტიმურ მოთხოვნებზე უარის თქმის საფუძველი. ასეთ შემთხვევებში, დამუშავებისთვის პასუხისმგებელმა პირმა უნდა განახორციელოს ტექნიკური ზომები, მონაცემებზე წვდომის შესახებ მოთხოვნის შესასრულებლად (მაგ., გამოსახულების რედაქტირება - შენიღბვა ან ე.წ. „scrambling“). ამავდროულად, დამუშავებისთვის პასუხისმგებელი პირები არ არიან ვალდებულები, განხორციელონ ამგვარი ტექნიკური ზომები, თუ მათ სხვაგვარად შეუძლიათ უზრუნველყონ მე-15 მუხლის საფუძველზე წარდგენილი მოთხოვნის შესრულება, 12(3) მუხლით დადგენილ ვადაში.

- GDPR-ის 11(2) მუხლი, დამუშავებისთვის პასუხისმგებელი პირს არ შეუძლია მონაცემთა სუბიექტის იდენტიფიცირება

95. თუ ვიდეოჩანაწერში შეუძლებელია პერსონალური მონაცემების მოძიება (ე.ი., დამუშავებისთვის პასუხისმგებელმა პირმა მთლიანად უნდა დაათვალიეროს დიდი ოდენობით შენახული მასალა იმისათვის, რომ იპოვოს შესაბამისი მონაცემთა სუბიექტი), მაშინ ითვლება, რომ დამუშავებისთვის პასუხისმგებელ პირს არ შეუძლია მონაცემთა სუბიექტის იდენტიფიცირება.

96. აღნიშნული მიზეზების გამო, მონაცემთა სუბიექტმა (საიდენტიფიკაციო დოკუმენტის გამოყენებით ან პირადად, საკუთარი თავის იდენტიფიცირების გარდა) ვალდებულია, მოთხოვნაში მიუთითოს, თუ როდის შევიდა იმ ტერიტორიაზე, სადაც მონიტორინგი მიმდინარეობს - მან უნდა მიუთითოს დროის გონივრული ინტერვალი,

ვიდეოჩანაწერში მოხვედრილი მონაცემთა სუბიექტების რაოდენობის პროპორციულად. დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, მონაცემთა სუბიექტს წინასწარ შეატყობინოს, თუ რა სახის ინფორმაციაა საჭირო იმისათვის, რომ დამუშავებისთვის პასუხისმგებელმა პირმა შეძლოს მოთხოვნის შესრულება. თუ დამუშავებისთვის პასუხისმგებელი პირი შეძლებს დაადასტუროს, რომ მას არ შეუძლია მონაცემთა სუბიექტის იდენტიფიცირება, მან მონაცემთა სუბიექტს უნდა მიაწოდოს შესაბამისი ინფორმაცია, თუ ეს შესაძლებელია. ასეთ სიტუაციაში, მონაცემთა სუბიექტის საპასუხოდ, დამუშავებისთვის პასუხისმგებელმა პირმა მონაცემთა სუბიექტს უნდა მიაწოდოს ინფორმაცია, თუ ზუსტად რომელ ტერიტორიაზე ხორციელდება მონიტორინგი, რომელი კამერები გამოიყენებოდა და ა.შ., რათა მონაცემთა სუბიექტს ჰქონდეს სრულფასოვანი წარმოდგენა იმის შესახებ, თუ სავარაუდოდ რა სახის პერსონალური მონაცემები დამუშავდა.

97.

> <u>მაგალითი:</u> თუ მონაცემთა სუბიექტი ითხოვს სავაჭრო ცენტრის შესასვლელში განთავსებული ვიდეომეთვალყურეობის საშუალებით დამუშავებული საკუთარი პერსონალური მონაცემების ასლს, ხოლო ამ სავაჭრო ცენტრს დღეში 30,000 ადამიანი სტუმრობს, იგი ვალდებულია, დაახლოებით ერთსაათიანი ინტერვალით მიუთითოს იმ ტერიტორიაზე გავლის დრო, სადაც მონიტორინგი ხორციელდება. თუ დამუშავებისთვის პასუხისმგებელი პირი კვლავ ამუშავებს აღნიშნულ მასალას, იგი ვალდებულია, ვიდეოჩანაწერის ასლი გადასცეს მონაცემთა სუბიექტს. თუ ამავე მასალაში შესაძლებელია სხვა მონაცემთა სუბიექტების იდენტიფიცირება, მაშინ აუცილებელია მასალის ამ ნაწილის ანონიმიზება (მაგ., მასალის ან შესაბამისი ნაწილების გაბუნდოვანება), მანამ, სანამ ასლი გადაეცემა მონაცემთა სუბიექტს, რომელმაც წარადგინა მოთხოვნა.
>
> <u>მაგალითი:</u> თუ დამუშავებისთვის პასუხისმგებელი პირი ავტომატურად შლის ყველა ჩანაწერს, მაგალითად, 2 დღის შემდეგ, იგი ვერ შეძლებს ამ ორი დღის გასვლის შემდეგ, ვიდეოჩანაწერის მონაცემთა სუბიექტისთვის გადაცემას. თუ დამუშავებისთვის პასუხისმგებელი პირი მოთხოვნას ორი დღის გასვლის შემდეგ მიიღებს, მონაცემთა სუბიექტს უნდა მიაწოდოს შესაბამისი ინფორმაცია.

- GDPR-ის მე-12 მუხლი, გადაჭარბებული მოთხოვნები

98. მონაცემთა სუბიექტის მხრიდან გადაჭარბებული ან ცალსახად დაუსაბუთებელი მოთხოვნების შემთხვევაში, დამუშავებისთვის პასუხისმგებელ პირს შეუძლია, მონაცემთა სუბიექტს მოსთხოვოს გონივრული საფასურის გადახდა, GDPR-ის 12(5)(a) მუხლის შესაბამისად, ან უარი თქვას მოთხოვნაზე რეაგირების განხორციელებაზე (GDPR-ის 12(5)(b) მუხლი). დამუშავებაზე პასუხისმგებელმა პირმა უნდა შეძლოს დემონსტრირება იმისა, რომ მოთხოვნა არის ცალსახად დაუსაბუთებელი ან გადაჭარბებული.

6.2 მონაცემთა წაშლის უფლება და დამუშავების შეწყვეტის მოთხოვნის უფლება

6.2.1 წაშლის უფლება (დავიწყების უფლება)

99. თუ დამუშავებისთვის პასუხისმგებელი პირი გააგრძელებს პერსონალური მონაცემების დამუშავებას რეალურ დროში მონიტორინგის მიღმა (მაგ., შენახვა), მონაცემთა სუბიექტს უფლება აქვს, მოითხოვოს მონაცემთა წაშლა, GDPR-ის მე-17 მუხლის შესაბამისად.

100. მოთხოვნის შემთხვევაში, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, ზედმეტი დაყოვნების გარეშე წაშალოს პერსონალური მონაცემები, იმ შემთხვევაში, თუ სახეზეა 17(1) მუხლით გათვალისწინებული რომელიმე გარემოება (და არ იკვეთება GDPR-ის 17(3) მუხლით გათვალისწინებული რომელიმე გამონაკლისი). აღნიშნული მოიცავს პერსონალური მონაცემების წაშლის ვალდებულებას მაშინ, როდესაც მონაცემები აღარ არის საჭირო იმ მიზნით, რა მიზნითაც მოხდა მათი თავდაპირველად შენახვა ან როდესაც დამუშავება უკანონოა (იხ. სექცია 8 - შენახვის ვადები და წაშლის მოვალეობა). ამას გარდა, დამუშავების სამართლებრივი საფუძვლის მიხედვით, პერსონალური მონაცემები უნდა წაიშალოს:

- თანხმობის საფუძვლის შემთხვევაში, როდესაც ხდება თანხმობის უკან გახმობა (და დამუშავების სამართლებრივი საფუძველი აღარ არსებობს)

- ლეგიტიმური ინტერესის შემთხვევაში:

  - როდესაც მონაცემთა სუბიექტი ახორციელებს მონაცემთა დამუშავების შეწყვეტის მოთხოვნის უფლებას (იხ. სექცია 6.2.2) და არ არსებობს აღმატებული ლეგიტიმური საფუძველი დამუშავებისთვის, ან

  - პირდაპირი მარკეტინგის შემთხვევაში (პროფილირების ჩათვლით), როდესაც მონაცემთა სუბიექტი ითხოვს დამუშავების შეწყვეტას.

101. თუ დამუშავებისთვის პასუხისმგებელმა პირმა ვიდეოჩანაწერი გახადა საჯარო (მაგ., მაუწყებლობის ან ონლაინ სტრიმინგის გზით), გონივრული ნაბიჯები უნდა გადაიდგას იმისათვის, რომ დამუშავებისთვის პასუხისმგებელ სხვა პირებს (რომლებიც ამჟამად ამუშავებენ მოცემულ პერსონალურ მონაცემებს) მიეწოდოთ ინფორმაცია მოთხოვნის შესახებ, GDPR-ის 17(2) მუხლის შესაბამისად. გონივრული ნაბიჯები უნდა მოიცავდეს ტექნიკურ ზომებს და ითვალისწინებდეს ხელმისაწვდომ ტექნოლოგიას და განხორციელების ღირებულებას. იმდენად, რამდენადაც შესაძლებელია, დამუშავებისთვის პასუხისმგებელმა პირმა - პერსონალური მონაცემების წაშლის შემთხვევაში - ინფორმაცია უნდა მიაწოდოს ყველას, ვისაც გადაეცა პერსონალური მონაცემები, GDPR-ის მე-19 მუხლის შესაბამისად.

102. გარდა დამუშავებისთვის პასუხისმგებელი პირის ვალდებულებისა, წაშალოს პერსონალური მონაცემები მონაცემთა სუბიექტის მოთხოვნის საფუძველზე, დამუშავებისთვის პასუხისმგებელი პირი GDPR-ის ზოგადი პრინციპების თანახმად ვალდებულია, მაქსიმალურად შეამციროს შენახული პერსონალური მონაცემები (იხ. სექცია 8).

103. ვიდეომეთვალყურეობასთან დაკავშირებით, აღსანიშნავია, რომ მაგალითად, სურათის გაბუნდოვანება, რის შედეგადაც შეუძლებელი ხდება სურათიდან რეტროაქტიულად იმ პერსონალური მონაცემების ამოღება, რომელიც მანამდე მასზე ინახებოდა, პერსონალური მონაცემები ითვლება წაშლილად, GDPR-ის შესაბამისად.

104.

> <u>მაგალითი:</u> მაღაზია ხშირად განიცდის ვანდალიზმის შემთხვევებს, რაც განსაკუთრებით ეხება მის გარეთა ფასადს. შესაბამისად, მაღაზიამ შესასვლელთან დაამონტაჟა ვიდეომეთვალყურეობის სისტემა, რომელიც პირდაპირ კედლებს უყურებს. ერთ-ერთი გამვლელი ითხოვს, წაშალონ მისი პერსონალური მონაცემები, რომელიც სისტემამ კონკრეტულ მომენტში დააფიქსირა. დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, მოთხოვნას პასუხი გასცეს ყოველგვარი შეუსაბამო დაყოვნების გარეშე და მაქსიმუმ 1 თვის ვადაში. ვინაიდან ვიდეოჩანაწერი ვეღარ აკმაყოფილებს იმ მიზანს, რისთვისაც იგი თავდაპირველად ინახებოდა (იმ მომენტში, როდესაც მონაცემთა სუბიექტმა ჩაიარა, ვანდალიზმს ადგილი არ ჰქონია), მოთხოვნის დროს აღარ არსებობს მონაცემთა შენახვის ლეგიტიმური ინტერესი, რომელიც აღემატება მონაცემთა სუბიექტების ინტერესებს. დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, წაშალოს პერსონალური მონაცემები.

6.2.2 დამუშავების შეწყვეტის მოთხოვნის უფლება

105. როდესაც ვიდეომეთვალყურეობა ეფუძნება ლეგიტიმურ ინტერესს (GDPR-ის 6(1)(f) მუხლი) ან საზოგადოებრივ ინტერესში შემავალი ფუნქციის განხორციელებასთან დაკავშირებულ აუცილებლობას (GDPR-ის 6(1)(e) მუხლი), მონაცემთა სუბიექტს უფლება აქვს - ნებისმიერ დროს - მოითხოვოს დამუშავების შეწყვეტა, მისი ინდივიდუალური გარემოებებიდან გამომდინარე, GDPR-ის 21-ე მუხლის შესაბამისად. გარდა იმ შემთხვევისა, როდესაც დამუშავებისთვის პასუხისმგებელი პირი წარმოადგენს დამაჯერებელ ლეგიტიმურ საფუძველს, რომელიც აღემატება მონაცემთა სუბიექტის უფლებებს და ინტერესებს, იმ პირის მონაცემთა დამუშავება, რომელთაც მოითხოვა დამუშავების შეწყვეტა, უნდა შეწყდეს. დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, მონაცემთა სუბიექტის მოთხოვნებს უპასუხოს გაჭიანურების გარეშე, მაქსიმუმ 1 თვის ვადაში.

106. ვიდეომეთვალყურეობის კონტექსტში, დამუშავების შეწყვეტის მოთხოვნა შესაძლებელია მონიტორინგს დაქვემდებარებულ ტერიტორიაზე შესვლისას, ტერიტორიაზე ყოფნის დროს ან ტერიტორიიდან გამოსვლისას. პრაქტიკაში, ეს ნიშნავს იმას, რომ გარდა იმ შემთხვევისა, როდესაც დამუშავებისთვის პასუხისმგებელ პირს გააჩნია დამაჯერებელი ლეგიტიმური საფუძველი, იმ ტერიტორიის მონიტორინგი, სადაც ფიზიკური პირების იდენტიფიცირება შესაძლებელია, კანონიერად მიიჩნევა მხოლოდ იმ შემთხვევაში, თუ:

(1) დამუშავებისთვის პასუხისმგებელ პირს შეუძლია, დაუყოვნებლივ შეწყვიტოს პერსონალური მონაცემების დამუშავება კამერის მიერ, მოთხოვნის შემთხვევაში, ან

(2) მონიტორინგს დაქვემდებარებულ ტერიტორიაზე შესვლა იმდენად შეზღუდულია, რომ დამუშავებისთვის პასუხისმგებელ პირს შეუძლია, უზრუნველყოს მონაცემთა სუბიექტისგან თანხმობის მიღება ტერიტორიაზე შესვლამდე, ხოლო მონიტორინგს დაქვემდებარებული ტერიტორია არ წარმოადგენს ტერიტორიას, სადაც შესვლის უფლება აქვს მონაცემთა სუბიექტს, როგორც მოქალაქეს.

107. წინამდებარე სახელმძღვანელო პრინციპები მიზნად არ ისახავს მოახდინოს იდენტიფიცირება, თუ რა წარმოადგენს *დამაჯერებელ* ლეგიტიმურ ინტერესს (GDPR-ის 21-ე მუხლი).

108. პირდაპირი მარკეტინგის მიზნებისთვის ვიდეომეთვალყურეობის გამოყენებისას, მონაცემთა სუბიექტს უფლება აქვს, მოითხოვოს დამუშავების შეწყვეტა, საკუთარი დისკრეციის საფუძველზე, რადგან ამ კონტექსტში, დამუშავების შეწყვეტის მოთხოვნის უფლება არის აბსოლუტური (GDPR-ის 21-ე მუხლის მე-2 და მე-3 პუნქტები).

109.

მაგალითი: კომპანიის შენობაში გახშირდა საზოგადოებრივი შესასვლელიდან გარეშე პირთა შესვლის შემთხვევები. ამასთან დაკავშირებით, ლეგიტიმური ინტერესის საფუძველზე, კომპანიამ შენობის შესასვლელში დაამონტაჟა ვიდეომეთვალყურეობის სისტემა, რათა მოახდინოს იმ ადამიანთა იდენტიფიცირება, რომლებიც შენობაში უკანონოდ შედის. ერთ-ერთმა ვიზიტორმა გააპროტესტა ვიდეომეთვალყურეობის სისტემის საშუალებით თავისი მონაცემების დამუშავება, თავისი ინდივიდუალური გარემოებებიდან გამომდინარე. თუმცა, კომპანიამ უარი თქვა დამუშავების შეწყვეტის მოთხოვნის დაკმაყოფილებაზე იმ მოტივით, რომ შენახული ჩანაწერი საჭიროა მიმდინარე შიდა გამოძიების მიზნებისთვის. ამრიგად, კომპანიას აქვს დამაჯერებელი ლეგიტიმური საფუძველი, რათა გააგრძელოს პერსონალური მონაცემების დამუშავება.

7. გამჭვირვალობის და ინფორმაციის მიწოდების ვალდებულებები[18]

110. ევროპის მონაცემთა დაცვის სამართალი დიდი ხანია ადგენს, რომ მონაცემთა სუბიექტები უნდა იყვნენ ინფორმირებულები იმის შესახებ, რომ მიმდინარეობს ვიდეომეთვალყურეობა. მათ უნდა მიეწოდოთ დეტალური ინფორმაცია, თუ რომელი ადგილები ექვემდებარება მონიტორინგს.[19] GDPR-ში, გამჭვირვალობასთან და ინფორმაციის მიწოდებასთან დაკავშირებული ვალდებულებები წარმოდგენილია მე-12 და შემდგომ მუხლებში. 29-ე მუხლის სამუშაო ჯგუფის „სახელმძღვანელო პრინციპები გამჭვირვალობის შესახებ, 2016/679 რეგულაციის (WP260) მიხედვით, რომელიც EDPB-მ დაამტკიცა 2018 წლის 25 მარტს, ითვალისწინებს დამატებით დეტალებს. WP260-ის 26-ე პუნქტის თანახმად, GDPR-ის მე-13 მუხლი, რომელიც მოქმედებს, თუ პერსონალური მონაცემების შეგროვება ხდება „[...] მონაცემთა სუბიექტისგან დაკვირვების გზით (მაგ., მონაცემთა შეგროვების ავტომატიზებული მოწყობილობების ან მონაცემთა შეგროვების კომპიუტერული პროგრამების გამოყენების გზით [...]“.

111. ინფორმაციის მოცულობის გათვალისწინებით, რომლის მიწოდებაც აუცილებელია მონაცემთა სუბიექტისათვის, დამუშავებისთვის პასუხისმგებელი პირები უფლებამოსილები არიან, გამოიყენონ მრავალშრიანი მიდგომა, რომლის თანახმადაც ისინი გამჭვირვალობის უზრუნველყოფის მიზნით სხვადასხვა მეთოდებს გამოიყენებენ (WP260, პ.35; WP89, პ.22). ვიდეომეთვალყურეობასთან დაკავშირებით, ყველაზე მნიშვნელოვანი ინფორმაცია წარმოდგენილი უნდა იქნას თავად გამაფრთხილებელ ნიშანზე (პირველი შრე), ხოლო დამატებითი სავალდებულო დეტალების მიწოდება შესაძლებელია სხვა საშუალებებით (მეორე შრე).

7.1 ინფორმაციის პირველი შრე (გამაფრთხილებელი ნიშანი)

112. პირველი შრე ეხება დამუშავებისთვის პასუხისმგებელი პირის პირველ კონტაქტს მონაცემთა სუბიექტთან. ამ ეტაპზე, დამუშავებისთვის პასუხისმგებელი პირი იყენებს გამაფრთხილებელ ნიშანს, რომელიც რელევანტურ ინფორმაციას შეიცავს. წარმოდგენილი ინფორმაციის მიწოდება შესაძლებელია პიქტოგრამასთან ერთად, რათა ინფორმაცია დაგეგმილი დამუშავების შესახებ მონაცემთა სუბიექტს მიეწოდოს ადვილად აღსაქმელი, გასაგები და მკაფიოდ წაკითხვადი ფორმით (GDPR-ის 12(7) მუხლი). ინფორმაციის ფორმატი უნდა მოერგოს ინდივიდუალურ ადგილმდებარეობას (WP89, პ.22).

[18] შესაძლოა, მოქმედებდეს ეროვნული კანონმდებლობის სპეციფიკური მოთხოვნები.

[19] იხ. WP89, დასკვნა 4/2004 პერსონალური მონაცემების ვიდეომეთვალყურეობის საშუალებით დამუშავების შესახებ, 29-ე მუხლის სამუშაო ჯგუფი.

7.1.1 გამაფრთხილებელი ნიშნის ადგილმდებარეობა

113. ინფორმაცია პოზიციონირებული უნდა იქნას იმგვარად, რომ მონაცემთა სუბიექტს ადვილად შეეძლოს ვიდეომეთვალყურეობის გარემოებების აღქმა მანამ, სანამ იგი მონიტორინგს დაქვემდებარებულ ტერიტორიაზე შევა (დაახლოებით, თვალის დონეზე). არ არის აუცილებელი კამერის მდებარეობის გამჟღავნება, თუ არ იარსებებს ეჭვი იმასთან დაკავშირებით, თუ რომელი ტერიტორია ექვემდებარება მონიტორინგს და მეთვალყურეობის კონტექსტი იქნება მკაფიოდ განმარტებული (WP 89, პ.22). მონაცემთა სუბიექტს უნდა შეეძლოს, თავად განსაზღვროს, თუ რომელ ტერიტორიას მოიცავს კამერა, რათა მან შეძლოს, თავი აარიდოს მეთვალყურეობას ან მოახდინოს საკუთარი ქცევის ადაპტირება, საჭიროების შესაბამისად.

7.1.2 პირველი შრის შინაარსი

114. ინფორმაციის პირველი შრე (გამაფრთხილებელი ნიშანი), როგორც წესი, უნდა ასახავდეს ყველაზე მნიშვნელოვან ინფორმაციას, მაგ. დამუშავების მიზნების შესახებ დეტალური ინფორმაცია, დამუშავებისთვის პასუხისმგებელი პირის ვინაობა და მონაცემთა სუბიექტის უფლებების არსებობა, იმ ინფორმაციასთან ერთად, რომელიც ასახავს დამუშავების ყველაზე მნიშვნელოვან გავლენებს.[20] ეს შესაძლებელია, რომ მოიცავდეს, მაგალითად, დამუშავებისთვის პასუხისმგებელი პირის (ან მესამე მხარის) ლეგიტიმურ ინტერესებს და მონაცემთა დაცვის ოფიცრის საკონტაქტო დეტალებს (ასეთის არსებობის შემთხვევაში). ინფორმაციის პირველი შრე, აგრეთვე, უნდა შეიცავდეს მითითებას ინფორმაციის უფრო დეტალურ, მეორე შრეზე და მონაცემთა სუბიექტს განუმარტავდეს, თუ სად და როგორ იპოვოს იგი.

115. ამას გარდა, ნიშანი უნდა შეიცავდეს ყველა იმ ინფორმაციას, რაც შესაძლოა მოულოდნელი იყოს მონაცემთა სუბიექტისთვის (WP260, პ.38). მაგალითად, მონაცემების გადაცემა მესამე მხარისთვის, განსაკუთრებით, თუ იგი მდებარეობს ევროკავშირის ფარგლებს გარეთ, და შენახვის ვადა. ამ ინფორმაციის არ მითითება მონაცემთა სუბიექტს მიანიშნებს, რომ მონიტორინგი მხოლოდ ცოცხალ რეჟიმში ხორციელდება (და მონაცემთა ჩაწერა ან მესამე მხარეებისათვის გადაცემა არ ხდება).

116.

<u>მაგალითი (არასავალდებულო რეკომენდაცია):</u>	
	<u>დამუშავებისთვის პასუხისმგებელი პირის და საჭიროების შემთხვევაში, მისი წარმომადგენლის ვინაობა:</u> <u>საკონტაქტო მონაცემები (თუ არსებობს მონაცემთა დაცვის ოფიცერი, მისი საკონტაქტო მონაცემებიც):</u>

[20] იხ. WP260, p.38.

 **ვიდეომეთვალყურეობა!**	<u>ინფორმაცია დამუშავების შესახებ, რომელსაც ყველაზე მნიშვნელოვანი გავლენა ექნება მონაცემთა სუბიექტზე (მაგ., შენახვის ვადა ან ცოცხალ რეჟიმში მონიტორინგი, ვიდეოჩანაწერის გამოქვეყნება ან მესამე მხარეებისთვის გადაცემა):</u> <u>ვიდეომეთვალყურეობის მიზანი ან მიზნები:</u>
[შტრიხკოდი] დამატებითი ინფორმაცია ხელმისაწვდომია: • შეტყობინებით • მიმღებ/საინფორმაციო/სარეგისტრაციო განყოფილებაში • ინტერნეტის საშუალებით (URL)...	<u>მონაცემთა სუბიექტის უფლებები:</u> როგორც მონაცემთა სუბიექტს, თქვენ გენიჭებათ რამდენიმე უფლება. კერძოდ, თქვენ გაქვთ უფლება, დამუშავებისთვის პასუხისმგებელ პირს მოსთხოვოთ თქვენს პერსონალურ მონაცემებზე წვდომა ან მათი წაშლა. ვიდეომეთვალყურეობის შესახებ დეტალური ინფორმაციის მისაღებად, მათ შორის, თქვენი უფლებების შესახებ, იხ. დამუშავებისთვის პასუხისმგებელი პირის მიერ უზრუნველყოფილი სრული ინფორმაცია, მარცხენა მხარეს წარმოდგენილი ვარიანტების საშუალებით.

7.2 ინფორმაციის მეორე შრე

117. ინფორმაციის მეორე შრე უნდა განთავსდეს ისეთ ადგილას, რომელიც მონაცემთა სუბიექტისათვის ადვილად იქნება ხელმისაწვდომი, მაგალითად, სრული საინფორმაციო დოკუმენტი, რომელიც ხელმისაწვდომია ცენტრალურ ლოკაციაზე (მაგ., საინფორმაციო ცენტრი, მიმღები განყოფილება ან სალარო) ან ადვილად მისაწვდომ პოსტერზე უნდა იყოს წარმოდგენილი. როგორც ზემოთ ითქვა, პირველი შრე (გამაფრთხილებელი ნიშანი) მკაფიოდ უნდა მიუთითებდეს ინფორმაციის მეორე შრეზე. ამას გარდა, უმჯობესია, თუ პირველი შრე მიუთითებს ციფრულ წყაროზე (მაგ., QR კოდი ან ვებგვერდის მისამართი). ამავდროულად, ინფორმაცია ადვილად უნდა იყოს ხელმისაწვდომი არაციფრული ფორმით. ინფორმაციის მეორე შრის ნახვა შესაძლებელი უნდა იყოს მონიტორინგს დაქვემდებარებულ ტერიტორიაზე შესვლის გარეშე, განსაკუთრებით მაშინ, თუ ინფორმაცია მიწოდებულია ციფრული ფორმით

(აღნიშნულის მიღწევა შესაძლებელია, მაგალითად, ბმულის საშუალებით). სხვა შესაბამისი საშუალებები მოიცავს ტელეფონის ნომერს (მონაცემთა სუბიექტს შეუძლია ნომერზე დარეკოს ინფორმაციის მისაღებად). ამავდროულად, წარმოდგენილი ინფორმაცია უნდა შეიცავდეს ყველა იმ ელემენტს, რომელიც მე-13 მუხლის თანახმად სავალდებულოა.

118. ამ ვარიანტების გარდა და იმისათვის, რომ გაიზარდოს მათი ეფექტურობა, EDPB ხელს უწყობს ტექნოლოგიური საშუალებების გამოყენებას მონაცემთა სუბიექტებისთვის ინფორმაციის მიწოდებისთვის. ეს შესაძლოა მოიცავდეს, მაგალითად, გეოლოკაციის განმსაზღვრელ კამერებს და ინფორმაციის დატანას რუკების შემცველ აპლიკაციებსა თუ ვებგვერდებზე, რათა ფიზიკურმა პირებმა, ერთის მხრივ, ადვილად შეძლონ მათი უფლებების განხორციელებასთან დაკავშირებული ვიდეოწყაროების იდენტიფიცირება და მკაფიოდ განსაზღვრა და მეორეს მხრივ, მოიპოვონ უფრო დეტალური ინფორმაცია დამუშავების ოპერაციის შესახებ.

119.

> <u>მაგალითი:</u> მაღაზიის მეპატრონე ახორციელებს საკუთარი მაღაზიის მონიტორინგს. მე-13 მუხლთან შესაბამისობისთვის, საკმარისია გამაფრთხილებელი ნიშნის განთავსება გამოსაჩენ ადგილას, მაღაზიის შესასვლელში, ხოლო ეს ნიშანი უნდა შეიცავდეს ინფორმაციის პირველ შრეს. ამას გარდა, მაღაზიის მეპატრონემ უნდა უზრუნველყოს საინფორმაციო ფურცელი, რომელიც ინფორმაციის მეორე შრეს შეიცავს და განთავსებული იქნება სალაროსთან ან ნებისმიერ სხვა ცენტრალურ და ადვილად მისაწვდომ ადგილას, მის მაღაზიაში.

8. შენახვის ვადები და წაშლის ვალდებულება

120. პერსონალური მონაცემების შენახვა დაუშვებელია იმაზე მეტი ხნით, რაც აუცილებელია იმ მიზნებისთვის, რისთვისაც მუშავდება პერსონალური მონაცემები (GDPR-ის 5(1)(c) და (e) ქვეპუნქტები). ზოგიერთ წევრ სახელმწიფოში, შესაძლოა, არსებობდეს სპეციფიკური დებულებები მონაცემთა შენახვის ვადებთან დაკავშირებით, ვიდეომეთვალყურეობის ჭრილში, GDPR-ის 6(2) მუხლის შესაბამისად.

121. გადაწყვეტილებები პერსონალური მონაცემების შენახვის საჭიროების შესახებ მიღებული უნდა იქნას მოკლე ვადაში. ზოგადად, ვიდეომეთვალყურეობის ლეგიტიმური მიზანია საკუთრების დაცვა ან მტკიცებულების შენახვა. როგორც წესი, დამდგარი ზიანის გაცნობიერება შესაძლებელია 1 ან 2 დღის ვადაში. მონაცემთა დაცვის ჩარჩოსთან შესაბამისობის სადემონსტრაციოდ, დამუშავებისთვის პასუხისმგებელი პირის ინტერესში შედის წინასწარ ორგანიზაციული ზომების მიღება

(მაგ., საჭიროების შემთხვევაში, წარმომადგენლის ნომინირება, რომელიც უზრუნველყოფს მასალის დათვალიერებას და უსაფრთხოების დაცვას). GDPR-ის 5(1) პუნქტის (c) და (e) პუნქტებით დაცული პრინციპების - კერძოდ, მონაცემთა მინიმიზაციისა და შენახვის ვადის შეზღუდვის პრინციპების გათვალისწინებით, უმეტეს შემთხვევაში (მაგ., როდესაც მიზანია ვანდალიზმის გამოვლენა), პერსონალური მონაცემები უნდა წაიშალოს, იდეალურ შემთხვევაში, რამდენიმე დღეში. რაც უფრო მეტია შენახვის ვადა (განსაკუთრებით, თუ იგი 72 საათს აღემატება), მით უფრო მეტი არგუმენტებია საჭირო შენახვის აუცილებლობისა და მიზნის ლეგიტიმურობის დასაბუთებისთვის. თუ დამუშავებისთვის პასუხისმგებელი პირი იყენებს ვიდეომეთვალყურეობას, არა მხოლოდ საკუთარი ტერიტორიის მონიტორინგის მიზნით, არამედ, აგრეთვე აპირებს მონაცემების შენახვას, დამუშავებისთვის პასუხისმგებელმა პირმა უნდა უზრუნველყოს, რომ შენახვა რეალურად არის საჭირო მიზნის მისაღწევად. ასეთ შემთხვევაში, შენახვის პერიოდი მკაფიოდ უნდა განისაზღვროს და ინდივიდუალურად უნდა დადგინდეს თითოეულ მიზანთან მიმართებით. დამუშავებისთვის პასუხისმგებელი პირის მოვალეობაში შედის შენახვის ვადის განსაზღვრა აუცილებლობისა და პროპორციულობის პრინციპების შესაბამისად და GDPR-ის დებულებებთან შესაბამისობის დემონსტრირება.

122.

> <u>მაგალითი:</u> მაღაზიის მეპატრონე, როგორც წესი, იმავე დღეს ამჩნევს ვანდალიზმის შემთხვევას. შესაბამისად, ჩანაწერის 24 საათით შენახვა საკმარისია. ამავდროულად, თუ მაღაზია შაბათ-კვირას დაკეტილია ან ხანგრძლივი დღესასწაულების დროს, შესაძლებელია, რომ მონაცემები უფრო მეტი ხნით იქნას შენახული. თუ გამოვლინდა დაზიანება, შესაძლებელია, რომ ვიდეოჩანაწერი უფრო მეტი ხნით იქნას შენახული, დამნაშავის მიმართ სამართლებრივი ქმედების განხორციელების მიზნით.

9. ტექნიკური და ორგანიზაციული ზომები

123. როგორც GDPR-ის 32(1) მუხლშია მითითებული, პერსონალური მონაცემების დამუშავება ვიდეომეთვალყურეობის დროს არა მხოლოდ სამართლებრივად დასაშვები უნდა იყოს, არამედ, დამუშავებისთვის პასუხისმგებელ პირებმა და უფლებამოსილმა პირებმა სათანადოდ უნდა დაიცვან მონაცემები. განხორციელებული **ორგანიზაციული და ტექნიკური ზომები** უნდა იყოს იმ **რისკების პროპორციული, რომელიც ფიზიკურ პირთა უფლებებს და თავისუფლებებს ექმნება,** ვიდეომეთვალყურეობის შედეგად მოპოვებული მონაცემების შემთხვევითი ან

უკანონო განადგურების, დაკარგვის, შეცვლის, არაავტორიზებული გაცემის ან წვდომის შედეგად. GDPR-ის 24-ე და 25-ე მუხლების თანახმად, დამუშავებისთვის პასუხისმგებელმა პირებმა უნდა განახორციელონ ტექნიკური და ორგანიზაციული ზომები, რათა დამუშავების პროცესში დაიცვან მონაცემთა დაცვის ყველა პრინციპი და შექმნან საშუალებები მონაცემთა სუბიექტების მიერ საკუთარი უფლებების განსახორციელებლად, GDPR-ის 15-22 მუხლების შესაბამისად. დამუშავებისთვის პასუხისმგებელმა პირებმა უნდა დანერგონ შიდა ჩარჩო და პოლიტიკა, რომელიც უზრუნველყოფს აღნიშნულის განხორციელებას როგორც დამუშავების საშუალებების განსაზღვრისას, ისე თავად დამუშავების დროს, რაც მათ შორის, უნდა მოიცავდეს მონაცემთა დაცვაზე ზეგავლენის შეფასებებს (data protection impact assessments), საჭიროების შესაბამისად.

9.1 ვიდეომეთვალყურეობის სისტემის მიმოხილვა

124. ვიდეომეთვალყურეობის სისტემა (VSS)[21] აერთიანებს ანალოგურ და ციფრულ მოწყობილობებს და პროგრამულ ნაწილს, რომელთა მიზანიც არის რაიმე ადგილის გამოსახულებების აღბეჭდვა, გამოსახულებების დამუშავება და მათი ოპერატორისთვის წარდგენა. ვიდეომეთვალყურეობის სისტემის კომპონენტები შესაძლებელია, დაიყოს რამდენიმე კატეგორიად:

- ვიდეო გარემო: გამოსახულების აღბეჭდვა, ურთიერთკავშირები და გამოსახულების დამუშავება:

    i. გამოსახულების აღბეჭდვის მიზანია რეალური სამყაროს გამოსახულების გენერირება იმგვარ ფორმატში, რომლის გამოყენებაც შესაძლებელია დანარჩენი სისტემის მიერ,

    ii. ურთიერთკავშირები (interconnections) გულისხმობს მონაცემთა მიმოცვლას ვიდეო გარემოში (ე.ი., კავშირები და კომუნიკაციები). კავშირების მაგალითებია: კაბელები, ციფრული ქსელები და უკაბელო ტრანსმისიები. კომუნიკაციები აღწერს ყველა ვიდეო და საკონტროლო მონაცემთა სიგნალებს, რომელიც შესაძლოა იყოს ციფრული ან ანალოგური,

    iii. გამოსახულების დამუშავება მოიცავს გამოსახულების ან გამოსახულებათა ერთობლიობის ანალიზს, შენახვას და წარდგენას.

[21] GDPR-ი არ შეიცავს განმარტებას, თუმცა, ტექნიკური აღწერა ხელმისაწვდომია, მაგალითად დოკუმენტში EN 62676-1-1:2014, ვიდეომეთვალყურეობის სისტემები, რომლებიც გამოიყენება უსაფრთხოების მიზნით - ნაწილი 1-1: ვიდეოსისტემის მოთხოვნები.

- სისტემის მართვის პერსპექტივიდან, VSS-ს აქვს შემდეგი ლოგიკური ფუნქციები:

    i. მონაცემთა მართვა და აქტივობის მართვა, რაც მოიცავს ოპერატორის ბრძანებებზე რეაგირებას და სისტემის მიერ გენერირებულ აქტივობებს (განგაშის პროცედურები, შეტყობინების ოპერაციები),

    ii. სხვა სისტემებთან დამაკავშირებელი ინტერფეისები, შესაძლოა, მოიცავდეს უსაფრთხოების (წვდომის კონტროლი, სახანძრო განგაში) და არაუსაფრთხოების (შენობის მართვის სისტემები, ავტომობილის სანომრე ნიშნების ავტომატური ამოცნობა) სისტემებთან კავშირს.

- VSS-ის უსაფრთხოება მოიცავს სისტემის და მონაცემების კონფიდენციალობას, დაცულობას და ხელმისაწვდომობას:

    i. სისტემის უსაფრთხოება მოიცავს სისტემის ყველა კომპონენტის ფიზიკურ უსაფრთხოებას და VSS-ზე წვდომის კონტროლს,

    ii. მონაცემთა უსაფრთხოება მოიცავს მონაცემების დაკარგვის ან მონაცემებით მანიპულაციის პრევენციას.

125.

გამოსახულების აღბეჭდვა	ურთიერთკავშირები (interconnections)	გამოსახულების დამუშავება
ვიდეო გარემო		
აქტივობის და მონაცემების მართვა		სხვა სისტემებთან დამაკავშირებელი ინტერფეისები
სისტემის მართვა		
სისტემა		მონაცემები
უსაფრთხოება		

სურათი 1 - ვიდეომეთვალყურეობის სისტემა

9.2 მონაცემთა მეტად დაფარვის პრიორიტეტი, როგორც ალტერნატიული მიდგომის არჩევამდე ავტომატურად გამოყენებული საწყისი მეთოდი ახალი პროდუქტის ან მომსახურების შექმნისას

126. როგორც GDPR-ის 25-ე მუხლშია მითითებული, დამუშავებისთვის პასუხისმგებელმა პირებმა უნდა მიიღონ მონაცემთა დაცვის სათანადო ტექნიკური და ორგანიზაციული ზომები, როგორც კი დაგეგმავენ ვიდეომეთვალყურეობას და მანამ, სანამ დაიწყებენ ვიდეოჩანაწერის შეგროვებას და დამუშავებას. აღნიშნული

პრინციპები ხაზს უსვამს მონაცემთა დაცვის ინტეგრირებული (built-in) ტექნოლოგიების საჭიროებას, ავტომატური პარამეტრების (default settings) დანერგვას, რომელიც მინიმუმამდე ამცირებს მონაცემთა დამუშავებას და საჭირო ინსტრუმენტების უზრუნველყოფას, რომელიც ხელს უწყობს პერსონალური მონაცემების ყველაზე მაღალი შესაძლო სტანდარტით დაცვას.[22]

127. დამუშავებისთვის პასუხისმგებელმა პირებმა უნდა დანერგონ მონაცემთა დაცვის გარანტიები არა მხოლოდ ტექნოლოგიური საშუალების დიზაინის სპეციფიკაციებში, არამედ, აგრეთვე, ორგანიზაციულ პრაქტიკაში. როდესაც საქმე ეხება ორგანიზაციულ პრაქტიკას, დამუშავებისთვის პასუხისმგებელმა პირებმა უნდა დანერგონ მართვის სათანადო ჩარჩო, შექმნან და აღასრულონ ვიდეომეთვალყურეობასთან დაკავშირებული პოლიტიკა და პროცედურები. ტექნიკური თვალსაზრისით, სისტემის სპეციფიკაცია და დიზაინი უნდა მოიცავდეს პერსონალური მონაცემების GDPR-ის მე-5 მუხლით დადგენილი პრინციპების შესაბამისად დამუშავების მოთხოვნებს (დამუშავების კანონიერება, მიზნის და მონაცემების შეზღუდვა, მონაცემთა ავტომატური მინიმიზაცია GDPR-ის 25(2) მუხლით გათვალისწინებული მნიშვნელობის ფარგლებში, უსაფრთხოება და კონფიდენციალობა, ანგარიშვალდებულება და ა.შ.). თუ დამუშავებისთვის პასუხისმგებელი პირი აპირებს, შეიძინოს ვიდეომეთვალყურეობის კომერციული სისტემა, მან აღნიშნული მოთხოვნები შესყიდვის სპეციფიკაციებში უნდა გაითვალისწინოს. დამუშავებისთვის პასუხისმგებელმა პირმა უნდა უზრუნველყოს აღნიშნულ მოთხოვნებთან შესაბამისობა, მათი გავრცელება სისტემის ყველა კომპონენტზე და მის მიერ დამუშავებულ ყველა მონაცემზე, ცხოვრების მთლიანი ციკლის მანძილზე.

9.3 შესაბამისი ზომების კონკრეტული მაგალითები

128. იმ ზომების უმეტესობა, რომელიც შესაძლებელია გამოყენებული იქნას ვიდეომეთვალყურეობის უსაფრთხოებისთვის, განსაკუთრებით, ციფრული აპარატურის და პროგრამის გამოყენების შემთხვევაში, არ განსხვავდება იმ ზომებისგან, რომლებიც გამოიყენება სხვა საინფორმაციო ტექნოლოგიების (IT) სისტემებში. ამავდროულად, არჩეული გადაწყვეტის მიუხედავად, დამუშავებისთვის პასუხისმგებელმა პირმა ადეკვატურად უნდა დაიცვას ვიდეომეთვალყურეობის სისტემის ყველა კომპონენტი და მონაცემები ყველა ეტაპზე, ე.ი. შენახვის ეტაპზე (არსებული მონაცემები), გადაცემის ეტაპზე (მონაცემები გადაცემის პროცესში) და დამუშავების ეტაპზე (მონაცემები გამოყენების პროცესში). ამისთვის საჭიროა

[22] WP 168, დასკვნა „მონაცემთა დაცვის მომავლის შესახებ“, 29-ე მუხლის სამუშაო ჯგუფი და პოლიციისა და მართლმსაჯულების საკითხებზე მომუშავე ჯგუფი, რომელიც კონსულტაციას უწევს ევროკომისიას პერსონალური მონაცემების დაცვის ფუნდამენტური უფლების სამართლებრივი ჩარჩოს შესახებ (მიღებულია 2009 წლის 1 დეკემბერს).

დამუშავებისთვის პასუხისმგებელი პირების და უფლებამოსილი პირების მიერ ორგანიზაციული და ტექნიკური ზომების ერთობლივი გამოყენება.

129. ტექნიკური გადაწყვეტების არჩევისას, დამუშავებისთვის პასუხისმგებელმა პირმა უნდა გაითვალისწინოს „მონაცემთა დაცვისადმი მეგობრული“ ტექნოლოგიები, ვინაიდან აღნიშნული აუმჯობესებს უსაფრთხოებას. ამგვარი ტექნოლოგიების მაგალითებია: სისტემები, რომლებიც იმ ტერიტორიების შენიღბვის ან ე.წ. scrambling-ის შესაძლებლობას იძლევა, რომლებიც არ არიან მნიშვნელოვანი მეთვალყურეობისთვის, ან მესამე პირთა გამოსახულებების რედაქტირება ვიდეოჩანაწერის მონაცემთა სუბიექტებისთვის გადაცემისას.[23] მეორეს მხრივ, არჩეული გადაწყვეტები არ უნდა ითვალისწინებდეს არასაჭირო (ზედმეტ) ფუნქციებს (მაგ., კამერების ულიმიტო მოძრაობა, მიახლოების შესაძლებლობა, რადიო ტრანსმისია, ანალიზი და აუდიო ჩანაწერები). უზრუნველყოფილი უნდა იქნას არასაჭირო (ზედმეტი) ფუნქციების დეაქტივაცია.

130. ამ თემაზე ფართო ლიტერატურაა ხელმისაწვდომი, მათ შორის, საერთაშორისო სტანდარტები და ტექნიკური სპეციფიკაციები მულტიმედია სისტემების ფიზიკური უსაფრთხოების[24] და ზოგადი საინფორმაციო-ტექნოლოგიური სისტემების უსაფრთხოების შესახებ.[25] ამრიგად, წინამდებარე სექცია მოცემულ თემას მხოლოდ ზედაპირულად მიმოიხილავს.

9.3.1 ორგანიზაციული ზომები

131. მონაცემთა დაცვაზე შესაძლო ზემოქმედების შეფასების (DPIA) გარდა (იხ. სექცია 10), დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, გაითვალისწინოს ქვემოთ ჩამოთვლილი თემები, ვიდეომეთვალყურეობის პოლიტიკის და პროცედურების შემუშავებისას:

- ვინ არის პასუხისმგებელი ვიდეომეთვალყურეობის სისტემის მართვაზე და ოპერირებაზე;
- ვიდეომეთვალყურეობის პროექტის მიზანი და მოქმედების სფერო.

[23] ამგვარი ტექნოლოგიების გამოყენება, შესაძლოა, სავალდებულოც იყოს ზოგიერთ შემთხვევაში, 5(1)(c) მუხლის მოთხოვნების შესასრულებლად. ნებისმიერ შემთხვევაში, ისინი კარგი პრაქტიკის მაგალითებს წარმოადგენენ.

[24] IEC TS 62045 - მულტიმედია უსაფრთხოება - მოწყობილობებისა და სისტემების უსაფრთხოების დაცვის სახელმძღვანელო პრინციპები, გამოყენების დროს და გამოყენების შემდგომ.

[25] ISO/IEC 27000 - საინფორმაციო უსაფრთხოების მართვის სისტემების სერია.

- სათანადო და აკრძალული გამოყენება (სად და როდის არის ვიდეომეთვალყურეობა დაშვებული და სად და როდის არ არის; მაგ., ფარული კამერების ან აუდიოჩაწერის გამოყენება, ვიდეოჩაწერასთან ერთად).[26]
- გამჭვირვალობის ზომები, რომლებზეც მიუთითებს მე-7 სექცია (გამჭვირვალობასთან და ინფორმირებასთან დაკავშირებული ვალდებულებები).
- როგორ ხდება ვიდეოს ჩაწერა და რა ხანგრძლივობით, მათ შორის, უსაფრთხოების ინციდენტებთან დაკავშირებული ვიდეოჩანაწერების დაარქივება/შენახვა.
- ვინ უნდა გაიაროს ტრენინგი და როდის.
- ვის აქვს წვდომა ვიდეოჩანაწერებზე და რა მიზნებით.
- საოპერაციო პროცედურები (მაგ., ვინ და საიდან აკონტროლებს ვიდეომეთვალყურეობას, რა უნდა გაკეთდეს მონაცემთა უსაფრთხოების დარღვევის ინციდენტის დროს).
- რა პროცედურებს საშუალებით შეძლებს გარეშე პირი ვიდეოჩანაწერის მოთხოვნის წარდგენას და ამგვარი მოთხოვნის დაკმაყოფილების ან უარყოფის პროცედურები.
- VSS შესყიდვის, დამონტაჟების და მოვლა-პატრონობის პროცედურები.
- ინციდენტის მართვისა და აღდგენის პროცედურები.

9.3.2 ტექნიკური ზომები

132. **სისტემის უსაფრთხოება** ნიშნავს სისტემის ყველა კომპონენტის **ფიზიკურ უსაფრთხოებას** და სისტემის ხელშეუხებლობას (მთლიანობას), ე.ი., **მის ჩვეულებრივ მუშაობაში** და **სისტემაზე წვდომის კონტროლში განზრახ და უნებლიე ჩარევის შემთხვევებისგან დაცვას და ასეთ შემთხვევებში სისტემის მედეგობას (სიმტკიცეს).** მონაცემთა უსაფრთხოება ნიშნავს **კონფიდენციალობას** (მონაცემები ხელმისაწვდომია მხოლოდ მათთვის, ვისაც აქვს მათზე წვდომის უფლება), **დაცულობას** (მონაცემთა დაკარგვის ან მონაცემებით მანიპულაციის პრევენცია) და **ხელმისაწვდომობას** (მონაცემები ხელმისაწვდომია საჭიროების შესაბამისად).

133. **ფიზიკური უსაფრთხოება** მონაცემთა დაცვის უმნიშვნელოვანესი ნაწილია და დაცვის ფუნდამენტურ (პირველად) შრეს წარმოადგენს იმის გათვალისწინებით, რომ იგი იცავს VSS მოწყობილობებს ქურდობისგან, ვანდალიზმისგან, სტიქიური უბედურებისგან, ადამიანების მიერ შექმნილი კატასტროფებისგან და შემთხვევითი

[26] ეს შესაძლოა, დამოკიდებული იყოს ეროვნულ კანონებზე და სექტორულ რეგულაციებზე.

დაზიანებისგან (მაგ., ელექტრონული ძაბვის მოვარდნის, ექსტრემალური ტემპერატურების და ყავის დაქცევის შედეგად). ანალოგზე დაფუძნებული სისტემების შემთხვევაში, ფიზიკური უსაფრთხოება ძირითად როლს ასრულებს მათ დაცვაში.

134. **სისტემის და მონაცემების უსაფრთხოება,** ე.ი., სისტემის ჩვეულებრივ საქმიანობაში განზრახ და უნებლიე ჩარევის შემთხვევებისგან დაცვა:

- მთლიანი VSS ინფრასტრუქტურის დაცვა (მათ შორის, დისტანციური კამერები, კაბელები და დენის წყარო) ფიზიკური ხელყოფისგან და ქურდობისგან.
- ჩანაწერის გადაცემის პროცესის დაცვა იმგვარი საკომუნიკაციო არხებით, რომელიც მიყურადებას გამორიცხავს.
- მონაცემთა დაშიფვრა.
- კომპიუტერულ მოწყობილობებზე და პროგრამებზე დაფუძნებული გადაწყვეტების გამოყენება, მაგალითად, firewall, ანტივირუსი ან შეჭრის აღმოჩენის სისტემები, რომლებიც მოქმედებს კიბერთავდასხმების წინააღმდეგ.
- კომპონენტების, პროგრამების და ურთიერთკავშირების ხარვეზების გამოვლენა.
- სისტემის ხელმისაწვდომობის და მასზე წვდომის აღდგენის საშუალებები ფიზიკური ან ტექნიკური ინციდენტის შემთხვევაში.

135. **წვდომაზე კონტროლი** უზრუნველყოფს სისტემაზე და მონაცემებზე მხოლოდ ავტორიზებული პირების წვდომას და გამორიცხავს სხვა პირების წვდომას. ზომები, რომლებიც ხელს უწყობენ ფიზიკური და ლოგიკური წვდომის კონტროლს, მოიცავს:

- ყველა იმ ტერიტორიის დაცვას მესამე მხარეთა უკონტროლო წვდომისგან, სადაც ხორციელდება ვიდეომეთვალყურეობა და ინახება ვიდეოჩანაწერები.
- მონიტორების განთავსება იმგვარად (განსაკუთრებით მაშინ, როდესაც ისინი ღია სივრცეშია განთავსებული, მაგ., მისაღები), რომ მათი ნახვა მხოლოდ ავტორიზებულმა ოპერატორებმა შეძლონ.
- ფიზიკური და ლოგიკური წვდომის მინიჭების, შეცვლისა და გაუქმების პროცედურების განსაზღვრა და აღსრულება.
- ხორციელდება მომხმარებლის ავტორიზების და ავთენტურობის (ნამდვილობის) დადგენის მეთოდები და საშუალებები, როგორიცაა, მაგალითად, პაროლის სიგრძე და შეცვლის სიხშირე.
- ხორციელდება მომხმარებლის მიერ განხორციელებული ქმედებების (სისტემასთან და მონაცემებთან მიმართებით) ჩაწერა და რეგულარული გადახედვა.

- წვდომის წარუმატებლობის შემთხვევების მონიტორინგი და გამოვლენა ხორციელდება უწყვეტად, ხოლო სუსტი მხარეების იდენტიფიცირების შემთხვევაში, ხდება სწრაფი რეაგირება.

10. მონაცემთა დაცვაზე ზეგავლენის შეფასება

136. GDPR-ის 35(1) მუხლის თანახმად, დამუშავებისთვის პასუხისმგებელ პირებს მოეთხოვებათ მონაცემთა დაცვაზე ზეგავლენის შეფასების (DPIA) განხორციელება, როდესაც მონაცემთა დამუშავების გარკვეული ტიპი, სავარაუდოდ, მაღალ რისკს შეუქმნის ფიზიკურ პირთა უფლებებს და თავისუფლებებს. GDPR-ის 35(3)(c) მუხლის თანახმად, დამუშავებისთვის პასუხისმგებელ პირებს მოეთხოვებათ მონაცემთა დაცვაზე ზეგავლენის შეფასება, თუ დამუშავება გულისხმობს საჯარო სივრცის სისტემატურ და ფართომასშტაბიან მონიტორინგს. ამას გარდა, GDPR-ის 35(3)(b) მუხლის თანახმად, მონაცემთა დაცვაზე ზეგავლენის შეფასება საჭიროა მაშინაც, როდესაც დამუშავებისთვის პასუხისმგებელი პირი აპირებს განსაკუთრებული კატეგორიის მონაცემთა დამუშავებას დიდი მასშტაბით.

137. მონაცემთა დაცვაზე ზეგავლენის შეფასების სახელმძღვანელო პრინციპები[27] უზრუნველყოფს დამატებით ინსტრუქციებს და უფრო დეტალურ მაგალითებს, რომლებიც რელევანტურია ვიდეომეთვალყურეობის კონტექსტში (მაგ., „გზატკეცილზე მანქანის ტარების მონიტორინგის მიზნით ვიდეოსისტემის გამოყენება“). GDPR-ის 35(4) მუხლის თანახმად, თითოეულმა საზედამხედველო ორგანომ უნდა გამოაქვეყნოს დამუშავების ოპერაციების ჩამონათვალი, რომელიც ექვემდებარება სავალდებულო DPIA-ს შესაბამის ქვეყანაში. ასეთი ჩამონათვალები, როგორც წესი, ხელმისაწვდომია შესაბამისი ორგანოების ვებგვერდზე. ვიდეომეთვალყურეობის ტიპური მიზნების გათვალისწინებით (ადამიანების და საკუთრების დაცვა, დანაშაულთა გამოვლენა, პრევენცია და კონტროლი, მტკიცებულების შეგროვება და ეჭვმიტანილთა ბიომეტრიული იდენტიფიკაცია), გონივრულია ჩავთვალოთ, რომ ვიდეომეთვალყურეობა ხშირ შემთხვევაში, მოითხოვს DPIA-ს. შესაბამისად, დამუშავებისთვის პასუხისმგებელი პირები ყურადღებით უნდა გაეცნონ აღნიშნულ დოკუმენტებს, რათა განსაზღვრონ, თუ რამდენად საჭიროა ამგვარი შეფასება და საჭიროების შესაბამისად განახორციელონ იგი. DPIA-ს შედეგებზე დაყრდნობით დამუშავებისთვის პასუხისმგებელი პირი ირჩევს მონაცემთა დაცვის განსახორციელებელ ზომებს.

138. მნიშვნელოვანია აღინიშნოს, რომ თუ DPIA-შედეგები მიუთითებს, რომ დამუშავება მაღალ რისკს შეუქმნის მონაცემთა დაცვას, დამუშავებისთვის

[27] WP248 rev.01, სახელმძღვანელო პრინციპები მონაცემთა დაცვაზე ზეგავლენის შეფასების შესახებ და იმის განსაზღვრა, თუ რამდენად „შეუქმნის მაღალ რისკს“ დამუშავება 2016/679 რეგულაციის მიზნებს - აღიარებულია EDPB-ის მიერ.

პასუხისმგებელი პირის მიერ დაგეგმილი უსაფრთხოების ზომების მიუხედავად, მაშინ დამუშავებამდე აუცილებელია შესაბამის საზედამხედველო ორგანოებთან კონსულტაციის გავლა. წინასწარი კონსულტაციის შესახებ დეტალური ინფორმაცია ხელმისაწვდომია 36-ე მუხლში.

მონაცემთა დაცვის ევროპული საბჭოს სახელით

თავმჯდომარე

(ანდრეა იელინეკი)