პერსონალურ მონაცემთა
დაცვის სამსახური

მსოფლიო პრაქტიკა

ოქტომბერი / 2023

მთავარი სიახლეები

მონაცემთა დაცვის ევროპულმა საბჭომ (“EDPB”) საპოლიციო დირექტივის შესაბამისად პერსონალურ მონაცემთა გადაცემის შესახებ სახელმძღვანელო გამოაქვეყნა

ფინეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ “Yandex”-ის მონაცემების რუსეთში გადაცემის აკრძალვა გააუქმა

“EDPB”-მ და “EDPS”-მა ციფრული ევროს პროექტთან დაკავშირებით ერთობლივი მოსაზრება გამოაქვეყნეს

“GDPR”-ის დანაწესის დარღვევისთვის ირლანდიის ცენტრალურ ბანკს შესაძლოა რეკორდული ოდენობის ჯარიმა დაეკისროს

მონაცემთა დაცვის ევროპულმა საბჭომ (“EDPB”) საპოლიციო დირექტივის შესაბამისად პერსონალურ მონაცემთა გადაცემის შესახებ სახელმძღვანელო გამოაქვეყნა

27.09.2023

ფოტო: edpb.europa.eu

“EDPB”-მ საპოლიციო დირექტივის (“LED”) 37-ე მუხლთან დაკავშირებით სახელმძღვანელო შეიმუშავა.[1] “LED”-ის 37-ე მუხლი სათანადო გარანტიების საფუძველზე პერსონალურ მონაცემთა ტრანსსასაზღვრო გადაცემას ეხება. “EDPB”-ის მიერ მიღებული დოკუმენტი მიზნად ისახავს “LED”-ის 37-ე მუხლის გამოყენების თაობაზე ევროკავშირის წევრი სახელმწიფოების კომპეტენტური ორგანოების მიერ მესამე ქვეყნის შესაბამისი ორგანოების ან საერთაშორისო ორგანიზაციებისთვის პრაქტიკული მითითებების მიწოდებას.[2] კერძოდ, სახელმძღვანელო ეხება “LED”-ის 37-ე მუხლის პირველი პუნქტის (a) და (b) ქვეპუნქტების შესაბამისად სათანადო გარანტიების შესახებ კომპეტენტური ორგანოების მიერ გამოსაყენებელ სამართლებრივ სტანდარტებსა და გარანტიების არსებობის შეფასების საკითხებს.

სათანადო გარანტიების არსებითი ელემენტები

“EDPB”-იმ აღნიშნა, რომ “LED”-ის 35-ე მუხლის (პერსონალურ მონაცემთა გადაცემის ზოგადი პრინციპები) მე-3 პუნქტი ვრცელდება “LED”-ის 37-ე მუხლის საფუძველზე განხორციელებულ გადაცემებზე. სწორედ ამიტომ, “LED”-ის 37-ე მუხლი გამოყენებულ უნდა იქნას იმ პრინციპის გათვალისწინებით, რომ ევროკავშირში პერსონალურ მონაცემთა დაცვის დონე პერსონალური მონაცემების სხვა იურისდიქციაში გადაცემით არ უნდა დაირღვეს.

„EDPB“-იმ ასევე მიუთითა, რომ “LED”-ის 37-ე მუხლი მონაცემთა მიმღებ მესამე ქვეყანასა თუ საერთაშორისო ორგანიზაციაში მონაცემთა დაცვის არსებითად ეკვივალენტურ დონეს მოითხოვს. აღნიშნული მოთხოვნა კონკრეტულ მონაცემთა გადაცემას ან გადაცემების კატეგორიას ეხება. “LED”-ის 37-ე მუხლის თანახმად, დირექტივით გარანტირებული

[1] EDPB adopts Guidelines on data transfers subject to appropriate safeguards under the Law Enforcement Directive, <https://edpb.europa.eu/news/news/2023/edpb-adopts-guidelines-data-transfers-subject-appropriate-safeguards-under-law_en>, 24.10.2023.

[2] ევროპის პარლამენტისა და საბჭოს 2016 წლის 27 აპრილის დირექტივა (EU) 2016/680 უფლებამოსილი ორგანოების მიერ დანაშაულის პრევენციის, გამოძიების, დადგენის ან სისხლისსამართლებრივი დევნისა და სასჯელის აღსრულების მიზნით პერსონალური მონაცემების დამუშავებისას ფიზიკური პირების დაცვისა და ამგვარი მონაცემების თავისუფალი მიმოცვლის შესახებ.

დაცვის დონის არსებითი ეკვივალენტობა უზრუნველყოფილ უნდა იქნას ყოველ კონკრეტულ შემთხვევაში და არა აუცილებლად მესამე ქვეყანასა თუ საერთაშორისო ორგანიზაციაში მოქმედ მთელს კანონმდებლობასთან მიმართებით.

“EDPB”-მ უკვე შეიმუშავა რეკომენდაციები “LED”-თან შესაბამისობის შენიშვნებთან[3] დაკავშირებით, რომელიც აღნიშნულია, ევროკავშირის ჩარჩოსთან ეკვივალენტობის უზრუნველსაყოფად საჭირო მონაცემთა დაცვის პრინციპების შესახებ. “EDPB”-ი მიიჩნევს, რომ აღნიშნულ რეკომენდაციებში გადმოცემული პრინციპები და გარანტიები რელევანტურია “LED”-ის 37-ე მუხლის კონტექსტში, ანუ კონკრეტულ ტრანსფერთან ან გადაცემების კატეგორიასთან დაკავშირებით.

“LED”-ის 37-ე მუხლის პირველი პუნქტის (a) ქვეპუნქტი

“LED”-ის 37-ე მუხლის პირველი პუნქტის (a) ქვეპუნქტი ითვალისწინებს მონაცემთა ტრანსსასაზღვრო გადაცემას სამართლებრივად სავალდებულო ძალის მქონე ინსტრუმენტის საფუძველზე, რომლითაც, თავის მხრივ, უზრუნველყოფილია პერსონალურ მონაცემთა დაცვის სათანადო გარანტიები. მნიშვნელოვანია, რომ სამართლებრივად სავალდებულო ძალის მქონე ინსტრუმენტი გაფორმდეს იმ დაწესებულების მიერ, რომელიც უფლებამოსილია, აიღოს ვალდებულებები გათვალისწინებულ გარანტიებთან დაკავშირებით. ამდენად, საერთაშორისო შეთანხმებას უნდა ჰქონდეს კანონის ძალა. ამგვარი სამართლებრივად სავალდებულო ინსტრუმენტი შეიძლება აღსრულდეს მხარეთა და მონაცემთა სუბიექტების მიერ, რომელთა პერსონალური მონაცემების დამუშავებაც რეგულირდება შეთანხმებით. სამართლებრივად სავალდებულო ძალის მქონე ინსტრუმენტი უნდა ითვალისწინებდეს ყველა შესაბამის წესს, რათა მონაცემთა დაცვის თვალსაზრისით მესამე ქვეყნის ან საერთაშორისო ორგანიზაციის კანონმდებლობის ნებისმიერი ხარვეზი ან შეზღუდვა აღმოიფხვრას შესაბამისი გარანტიების დაწესებით, რომელიც უზრუნველყოფს მონაცემთა დაცვის არსებითად ეკვივალენტურ დონეს.

“EDPB” მიიჩნევს, რომ შესაბამისობის გადაწყვეტილების არარსებობის შემთხვევაში, მხარეებს შორის პერსონალური მონაცემების გადაცემის მარეგულირებელი სამართლებრივად სავალდებულო ძალის მქონე ინსტრუმენტის გამოყენება უპირატესი უნდა იყოს “LED”-ის 37-ე მუხლის პირველი პუნქტის (b) ქვეპუნქტის შესაბამისად (შეფასების მექანიზმთან მიმართებით). სამართლებრივად სავალდებულო ძალის მქონე ინსტრუმენტი უზრუნველყოფს უფრო მეტ სამართლებრივ განსაზღვრულობას, გამჭვირვალობას, განჭვრეტადობას, სტაბილურობას, თანმიმდევრულობასა და

[3] EDPB, Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive, 2021, <https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012021-adequacy-referential-under-law_en>, 24.10.2023.

მონაცემთა დაცვის გარანტიების ეფექტიან გამოყენებას.

ამ კონტექსტში, “EDPB”-მ მითითება გააკეთა საერთაშორისო შეთანხმებების, მათ შორის, გადაცემების შესახებ, 2021 წლის 13 აპრილს მის მიერ გავრცელებულ განცხადებზე. კერძოდ, განცხადების მიხედვით, “EDPB”-ი წევრ სახელმწიფოებს, პერსონალური მონაცემების ტრანსსასაზღვრო გადაცემასთან დაკავშირებით საერთაშორისო შეთანხმებების შეფასებასა და საჭიროების შემთხვევაში, მათ გადახედვას მოუწოდებდა. ასევე, “EDPB”-მ ხაზი გაუსვა შეთანხმებების დირექტივის მოთხოვნებთან შესაბამისობაში მოყვანის მნიშვნელობას.

ფოტო: edpb.europa.eu

“LED”-ის 37-ე მუხლის პირველი პუნქტის (b) ქვეპუნქტი

“LED”-ის 37-ე მუხლის პირველი პუნქტის (b) ქვეპუნქტის მიხედვით, მონაცემთა გადაცემა შესაძლებელია იმ შემთხვევაში, როდესაც მონაცემთა დამმუშავებელი პერსონალური მონაცემების გადაცემასთან დაკავშირებული გარემოებების შეფასების საფუძველზე ადგენს, რომ უზრუნველყოფილია პერსონალურ მონაცემთა დაცვის სათანადო გარანტიები. აღნიშნულ დებულებასთან დაკავშირებით, სახელმძღვანელოში აღნიშნულია, რომ კომპეტენტურ ორგანოებს შეუძლიათ, დაეყრდნონ შეფასების მექანიზმს მხოლოდ მაშინ, როდესაც იგი ეფუძნება შესაბამისი სამართლებრივი ბაზისა და პრაქტიკის გულმოდგინე ანალიზს. გარდა აღნიშნულისა, კომპეტენტურმა ორგანოებმა უნდა გამოიკვლიონ გადასაცემი პერსონალურ მონაცემთა დაცვის საკითხები იმ რისკების გათვალისწინებით, რომელიც მონაცემთა მესამე ქვეყნებისთვის გაზიარებას მოჰყვება მონაცემთა სუბიექტების ფუნდამენტური უფლებებისა და თავისუფლებების, ასევე, მათი და სხვა დაინტერესებული პირების ლეგიტიმური ინტერესების დაცვის თვალსაზრისით. განხორციელებულ ან განსახორციელებელ მონაცემთა გადაცემასთან დაკავშირებული გარემოებების დეტალური ცოდნა აუცილებელია იმისათვის, რომ შესაძლებელი იყოს ფიზიკური პირების უფლებებისა და თავისუფლებებისთვის შექმნილი რისკების იდენტიფიცირება და მათი შემცირების ნებისმიერი საშუალებების გამოვლენა.

მნიშვნელოვანია, რომ კომპეტენტურმა ორგანომ დეტალურად იცოდეს და გაითვალისწინოს მონაცემთა გადაცემის ბუნება, ფარგლები, შინაარსი და მიზნები. კერძოდ, კომპეტენტურ ორგანოებს შეუძლიათ მონაცემთა სუბიექტების ფუნდამენტურ უფლებებთან

დაკავშირებული რისკების შესაფასებლად მონაცემთა გადაცემის ოპერაციები გააანალიზონ და მათი კატეგორიზაცია მოახდინონ იმგვარი მახასიათებლების გათვალისწინებით, როგორიცაა: გადაცემის კონკრეტული მიზნები, გადაცემული მონაცემების რაოდენობა ან სისხლის სამართლის დანაშაულის სიმძიმე.

ზოგიერთ შემთხვევაში, შესაბამისი გარანტიები თავისთავად გამომდინარეობს მესამე ქვეყნის საერთაშორისო ვალდებულებებიდან, მისი კანონმდებლობიდან და პრაქტიკიდან. სხვა შემთხვევებში, კომპეტენტურ ორგანოებს, მათი უფლებამოსილების ფარგლებში, "LED"-ითა და ეროვნული კანონმდებლობით გათვალისწინებული დაცვის არსებითად ეკვივალენტური დონის უზრუნველსაყოფად, შესაძლებელია, დასჭირდეთ ზემოაღნიშნული კონკრეტული გადაცემის მახასიათებლების დამატებითი გარანტიები. ამასთანავე, აუცილებელია, რომ მესამე ქვეყნის მიმღებმა ორგანომ დამატებითი გარანტიების დაცვის ვალდებულება აიღოს.

გარანტიების მიზანშეწონილობის შესახებ გადაწყვეტილების მიღება

ის ფაქტი, რომ "LED"-ის 36-ე - 38-ე მუხლებით გათვალისწინებული გადაცემის მექანიზმები თანმიმდევრულად ფუნქციონირებს, იგი გავლენას ახდენს მონაცემთა დამმუშავებლის ანგარიშვალდებულებაზე. "LED"-ის 37-ე მუხლის პირველი პუნქტის (b) ქვეპუნქტთან დაკავშირებით მონაცემთა დამმუშავებლის ანგარიშვალდებულებასთან დაკავშირებული მოვალეობები, უზრუნველყოფილია 37-ე მუხლის მე-2 და მე-3 პუნქტებით იმდენად, რამდენადაც თავად მონაცემთა დამმუშავებელი განსაზღვრავს სათანადო გარანტიების არსებობის საკითხს. ეს კი გულისხმობს შესაბამისობის გადაწყვეტილებებისა თუ სამართლებრივად სავალდებულო ძალის მქონე ინსტრუმენტების საფუძველზე განხორციელებულ გადაცემებთან შედარებით შეუსაბამობების უფრო მაღალ საფრთხეებს, ნაკლებ გამჭვირვალობასა და სამართლებრივ განსაზღვრულობას მონაცემთა სუბიექტებისთვის.

"LED"-ის 37-ე მუხლის მე-2 პუნქტით დაკისრებულ ვალდებულებასთან დაკავშირებით და ამ დებულების მიღების მიზეზის გათვალისწინებით, კომპეტენტურმა ორგანოებმა მონაცემთა დაცვის საზედამხედველო ორგანოებს რეგულარულად უნდა აცნობონ მათ მიერ "LED"-ის 37-ე მუხლის პირველი პუნქტის (b) ქვეპუნქტის საფუძველზე განხორციელებული მონაცემთა გადაცემების კატეგორიების შესახებ. აგრეთვე, საზედამხედველო ორგანოსთვის წარდგენილი ინფორმაცია უნდა შეიცავდეს მონაცემებს მიმღები კომპეტენტური ორგანოებისა და მონაცემთა გადაცემის რაოდენობის შესახებ.[4]

[4] EDPB, Guidelines 01/2023on Article 37 Law Enforcement Directive, Version 1.0, 2023, 2-3, <https://edpb.europa.eu/system/files/2023-09/edpb-guidelines_202301_art_37_led_en_2.pdf>, 25.10.2023.

გაერთიანებული სამეფოს მონაცემთა დაცვის საზედამხედველო ორგანომ (“ICO”) დასაქმებულ პირთა კანონიერი მონიტორინგის თაობაზე სახელმძღვანელო გამოაქვეყნა

04.10.2023

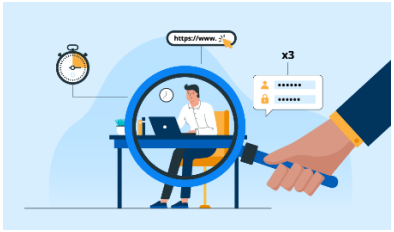
ფოტო: ico.org.uk

2023 წლის 4 ოქტომბერს, გაერთიანებული სამეფოს მონაცემთა დაცვის საზედამხედველო ორგანომ (“ICO”) სახელმძღვანელო გამოაქვეყნა,[5] რომელიც სამუშაო სივრცეში დამსაქმებლების მხრიდან დასაქმებული პირების მიმართ მონიტორინგის განხორციელებას შეეხება. დოკუმენტში განხილულია დასაქმებულთა მონიტორინგის პროცესში მონაცემთა დაცვის კანონმდებლობის შესაბამისად გასათვალისწინებელი საკითხები.

სახელმძღვანელო, ძირითადად, შემუშავებულია დამსაქმებელთათვის და მისი მიზანია დასაქმებულთა პერსონალური მონაცემების დაცვა. მასში ხაზგასმულია, რომ დასაქმებულ პირთა მონიტორინგის მიზანს გაწეული სამუშაოს შესრულების ხარისხისა და მოცულობის შემოწმება, ასევე, ჯანმრთელობისა და უსაფრთხოების დაცვა უნდა წარმოადგენდეს.

დასაქმებული პირების მიმართ გადაჭარბებულმა მონიტორინგმა შესაძლოა, უარყოფითი გავლენა იქონიოს მათი უფლებებისა და თავისუფლებების დაცვაზე, რასაც შედეგად პირადი ცხოვრების დაცულობის უფლებაში არამართლზომიერი ჩარევა მოჰყვება. “ICO” გამოყოფს გარემოებებს, როდესაც რთულია სამსახურებრივი ინფორმაციის და პირადისაგან გამიჯვნა. ერთ-ერთი ამგვარი შემთხვევაა დისტანციურად მუშაობა, იმის გათვალისწინებით, რომ სამუშაოს შესასრულებლად შეიძლება, გამოყენებული იქნას პერსონალური მოწყობილობა.

დამატებით, სახელმძღვანელოში აღნიშნულია, რომ დამსაქმებელს შეიძლება, დასჭირდეს დასაქმებულების თაობაზე მოპოვებული პერსონალური ინფორმაციის სამართალდამცავი ორგანოებისთვის გაზიარება. მაგალითად, როდესაც გამოავლენს, რომ არსებობს სისხლისსამართლებრივი დანაშაულის ჩადენასთან დაკავშირებული ეჭვი, როგორიცაა: თაღლითობა, ქურდობა და სხვა.



ფოტო: exodus.co.tz

[5] ICO, Information Commissioner’s Office: <https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/employment-information/employment-practices-and-data-protection-monitoring-workers-1-0.pdf>, [27.10.2023].

“ICO”-ს მიერ შემუშავებული დოკუმენტი ფოკუსირებულია რეგულარულ მეთვალყურეობაზე. თუმცა, დოკუმენტში ასევე წარმოდგენილია საკითხები მოკლევადიან მონიტორინგთან დაკავშირებით. ამ უკანასკნელის მაგალითი შეიძლება იყოს სავარაუდო ქურდობის გამოვლენა.

მონიტორინგის ტექნოლოგიებსა და საშუალებებში შეიძლება, მოიაზრებოდეს:

- ☑ კამერები, რომლის მიზანია ჯანმრთელობისა და უსაფრთხოების დაცვა;
- ☑ ვებკამერები და ეკრანის ფოტოსურათები (“screenshots”);
- ☑ დროის აღრიცხვის ან დაშვების კონტროლის ტექნოლოგიები;
- ☑ კლავიატურის გამოყენებაზე კონტროლი;
- ☑ დასაქმებულთა პროდუქტიულობის შეფასების ინსტრუმენტები;
- ☑ ინტერნეტ საქმიანობა;
- ☑ სხეულზე სატარებელი მოწყობილობები, რათა გაკონტროლდეს დასაქმებულთა ადგილმდებარეობა;
- ☑ ფარული აუდიო მონიტორინგი.

“ICO”-ს განმარტებით, დამსაქმებლების მიერ გამოყენებული ტექნოლოგიები დასაქმებულთა კონტროლის მიზნით დღითიდღე იცვლება და ვითარდება. მიუხედავად ტექნოლოგიური ცვლილებებისა, აუცილებელია მონაცემთა დაცვის პრინციპების გათვალისწინება. დოკუმენტში გაერთიანებული სამეფოს მონაცემთა დაცვის საზედამხედველო ორგანომ გამოყო საკითხთან დაკავშირებული აქტუალური კითხვები და მოკლედ განმარტა თითოეული მათგანი.

შეიძლება თუ არა დასაქმებული პირების მონიტორინგი?

მონაცემთა დაცვის კანონმდებლობა დამსაქმებელს არ ზღუდავდეს დასაქმებულ პირებზე მეთვალყურეობის უფლებას, თუმცა აუცილებელია, რომ აღნიშნული განხორციელდეს მონაცემთა დაცვის მოთხოვნების შესაბამისად. აღნიშნული განსაკუთრებით მნიშვნელოვანია დისტანციური მუშაობის თვალსაზრისით. კერძოდ, დასაქმებულს პირადი ცხოვრების დაცულობის განცდა გაცილებით მაღალი აქვს სახლში ყოფნის დროს, რაც მეტად ზრდის პირადი ცხოვრების ხელშეუხებლობის უფლებაში ჩარევასთან დაკავშირებულ რისკებს. ამასთან, აუცილებელია, რომ მონაცემთა დაცვის სტანდარტების შესაბამისად, დაბალანსდეს დამსაქმებლის ბიზნესინტერესები და დასაქმებულის უფლებები და თავისუფლებები. მონიტორინგის არამართლზომიერად განხორციელების შემთხვევაში, შეილახება დასაქმებულის პირადი ცხოვრების ხელშეუხებლობის უფლება. ასევე, აღნიშნული გავლენას იქონიებს დასაქმებულსა და დამსაქმებელს შორის ნდობაზე. გასათვალისწინებელია, რომ მონიტორინგის დროს კონკრეტული მიზნის მისაღწევად გამოყენებული უნდა იქნას ნაკლებად ინვაზიური საშუალება.

მაგალითი:

დამსაქმებელმა აღმოაჩინა, რომ დისტანციურად მომუშავე რამდენიმე

თანამშრომელმა მუშაობა დაიწყო იმაზე გვიან, ვიდრე ასახეს „დროის ფურცელში“. ამ მიზეზით, დამსაქმებელმა დაიწყო შესაბამისი მოწყობილობების კონტროლი, რომლის მეშვეობითაც პირთა მუშაობის მონიტორინგისთვის მენეჯმენტს წვდომა ჰქონდა ვებკამერაზე.

წარმოდგენილი მაგალითი, დიდი ალბათობით, გამოიწვევს მონაცემთა დაცვის კანონმდებლობის დარღვევას, რადგან არის არაპროპორციული. ასევე, არსებობს კონტროლის ნაკლებად ინვაზიური საშუალებები.

როგორ უნდა გაკონტროლდნენ დასაქმებულები კანონიერად?

დასაქმებულ პირთა მონაცემების კანონიერად დამუშავების მიზნით, აუცილებელია შესაბამისი სამართლებრივი საფუძვლის არსებობა. საყურადღებოა, რომ ამ პროცესში არსებობს განსაკუთრებული კატეგორიის ინფორმაციის მოპოვების შესაძლებლობა. ამგვარი ინფორმაცია, მისი სენსიტიური ბუნებიდან გამომდინარე, საჭიროებს გაძლიერებულ დაცვას.

რა ვადით ინახება დასაქმებულის შესახებ მოპოვებული ინფორმაცია?

დამსაქმებელმა დასაქმებულის შესახებ მოპოვებული პერსონალური ინფორმაცია არ უნდა შეინახოს იმაზე დიდი ხნით, ვიდრე აღნიშნული საჭიროა კონკრეტული მიზნის მისაღწევად. ამასთან, უნდა იქნას გათვალისწინებული შესაბამისი სტანდარტები და სამართლებრივი ვალდებულებები.

როგორ უნდა იქნას უზრუნველყოფილი მოპოვებული პერსონალური ინფორმაციის უსაფრთხოება?

პერსონალური ინფორმაციის უსაფრთხოება მონაცემთა დაცვის კანონმდებლობის ძირითად პრინციპს წარმოადგენს. აქედან გამომდინარე, დამსაქმებელმა უნდა მიიღოს შესაბამისი ორგანიზაციული და ტექნიკური ზომები, რათა დაიცვას დასაქმებულის პერსონალური მონაცემები. აღნიშნულ პროცესში უნდა შეფასდეს მონაცემთა უსაფრთხოებასთან დაკავშირებული რისკები და ინფორმაციაზე წვდომა მაქსიმალურად უნდა შეიზღუდოს.

ფოტო: linkedin.com

შეიძლება თუ არა ფარული მეთვალყურეობის განხორციელება?

ფარული მეთვალყურეობა გულისხმობს დასაქმებულთა წინასწარი ცოდნის გარეშე მონიტორინგს. ჩვეულებრივ პირობებში, ამ სახის კონტროლი ნაკლებად გამართლებულია, თუმცა არსებობს საგამონაკლისო შემთხვევები, მაგალითად, სავარაუდო სისხლისსამართლებრივი დანაშაულის ან უხეში გადაცდომის პრევენცია ან გამოვლენა.

ფარული კონტროლის პროცესში აუცილებელია შემდეგ გარემოებათა გათვალისწინება:

- ☑ ამგვარი მონიტორინგი უნდა განხორციელდეს უფლებამოსილი პირების მხრიდან;
- ☑ უნდა განხორციელდეს მონაცემთა დაცვაზე ზეგავლენის შეფასება;
- ☑ უნდა არსებობდეს სისხლისსამართლებრივი დანაშაულის ჩადენის შესახებ ეჭვი;
- ☑ კონკრეტული საქმის მოკვლევის დასრულების შემდეგ, აღარ უნდა გაგრძელდეს ფარული მეთვალყურეობა;
- ☑ არ უნდა იქნას გამოყენებული ფარული აუდიო ან ვიდეო მონიტორინგი იმ სივრცეებში, რომლებშიც დასაქმებულებს ექნებათ პირადი სივრცის დაცულობის აღქმა, როგორიცაა: საპირფარეშო ან გამოსაცვლელი ოთახები;
- ☑ უმეტეს შემთხვევაში, არ უნდა გაკონტროლდეს პირადი კომუნიკაცია, მაგალითად, პერსონალური ელექტრონული ფოსტა, რადგან პირებს აქვთ პირადი სივრცის დაცულობის გონივრული განცდა;
- ☑ მოპოვებული ინფორმაცია მხოლოდ განსაზღვრული მიზნისთვის უნდა გამოიყენებოდეს;
- ☑ უნდა განისაზღვროს მკაფიო წესები ინფორმაციის გამჟღავნებასა და მასზე წვდომასთან მიმართებით;
- ☑ ყველა ეტაპზე უნდა იქნას გათვალისწინებული დასაქმებულთა მონაცემთა დაცვის უფლებები.

შეუძლიათ თუ არა დასაქმებულებს საკუთარ პერსონალურ ინფორმაციაზე წვდომის მოთხოვნა?

დასაქმებულ პირებს, მოთხოვნის შემთხვევაში, უნდა ჰქონდეთ წვდომა მათ შესახებ მონიტორინგის შედეგად მოპოვებულ პერსონალურ ინფორმაციაზე.

დასაქმებულებს აქვთ თუ არა უფლება უარი განაცხადონ მათ მიმართ მონიტორინგის განხორციელებაზე?

კონკრეტულ შემთხვევებში, დასაქმებულ პირებს უფლება აქვთ უარი განაცხადონ მათი პერსონალური მონაცემების დამუშავებაზე. მიზეზი, სხვა საკითხებთან ერთად, შეიძლება იყოს საჯარო ამოცანის შესრულება ან ლეგიტიმური ინტერესი.

ფოტო: flaticon.com

რა უნდა იცოდეს დამსაქმებელმა, როდესაც დისტანციურად მომუშავე დასაქმებულს აკონტროლებს?

დასაქმებულების მხრიდან დისტანციურად მუშაობის დროს პირადი ცხოვრების დაცულობის შესახებ მოლოდინი უფრო მაღალია, ვიდრე სამუშაო ადგილზე. თუმცა, არსებობს ოჯახისა და პირადი ცხოვრების შესახებ ინფორმაციის გაუფრთხილებლად მოპოვების ალბათობა. მოცემულ

შემთხვევაში, საჭიროა მონაცემთა დაცვაზე ზეგავლენის შეფასება.

შეიძლება თუ არა დასაქმებულების სატელეფონო ზარებზე მონიტორინგის განხორციელება?

ყველა შემთხვევაში, სატელეფონო ზარების მონიტორინგი ან შინაარსის ჩაწერა არაპროპორციულია. ბიზნეს სატელეფონო ზარების მონიტორინგი შესაძლებელია იმ შემთხვევაში, თუ ეს საჭიროა ბიზნეს ტრანზაქციებთან დაკავშირებით მტკიცებულებების მოსაპოვებლად ან ხარისხის კონტროლის მიზნებისთვის.

შეიძლება თუ არა ელექტრონული ფოსტისა და მიმოწერების კონტროლი?

სამუშაო ანგარიშების მეშვეობით ელექტრონული ფოსტისა და შეტყობინებების მონიტორინგის დროს ნათლად უნდა იქნას განსაზღვრული მიზანი და დამსაქმებელი უნდა დარწმუნდეს, რომ მონიტორინგი აუცილებელი და მიზნის პროპორციულია. ამასთან, აუცილებელია, რომ დასაქმებულს მიეწოდოს ინფორმაცია მონიტორინგის ნებისმიერი მიზნის თაობაზე. გარდა ამისა, უნდა განხორციელდეს მონაცემთა დაცვაზე ზეგავლენის შეფასება. აღნიშნულის მიზეზია დასაქმებულთა უფლებებსა და თავისუფლებებთან მიმართებით მაღალი რისკის არსებობა და ასევე, განსაკუთრებული კატეგორიის ინფორმაციის მოპოვების ალბათობა. ამ შემთხვევაში, მოთხოვნის არარსებობის მიუხედავად, მიზანშეწონილია, რომ განხორციელდეს მონაცემთა დაცვაზე ზეგავლენის შეფასება.

შეიძლება თუ არა დასაქმებულების ვიდეო-აუდიო მონიტორინგი?

შესაძლებელია, რომ აღნიშნულ პროცესში დამუშავდეს განსაკუთრებული კატეგორიის ინფორმაცია, მაგალითად, “CCTV” სისტემების მეშვეობით შესაძლებელია:

- ვიდეო და აუდიო ჩაწერა;
- სახის ამოცნობა;
- დასაქმებულთა პროდუქტიულობის შესაფასებლად და ემოციური ანალიზის განსახორციელებლად ხელოვნურ ინტელექტთან ერთად მუშაობა.

მონიტორინგის განხორციელებამდე, თუ არსებობს ვარაუდი, რომ ამ პროცესში გამოვლინდება განსაკუთრებული კატეგორიის პერსონალური ინფორმაცია, დამსაქმებელმა უნდა განახორციელოს მონაცემთა დაცვაზე ზეგავლენის შეფასება.

ფოტო: infolawcentre.blogs.sas.ac.uk

შეიძლება თუ არა სამსახურის სატრანსპორტო საშუალების მონიტორინგი?

სამსახურის სატრანსპორტო საშუალების მონიტორინგი დასაშვებია. თუმცა, თუკი დასაქმებულს უფლება აქვს, რომ

ტრანსპორტი გამოიყენოს მათ შორის პირადი მიზნით, მონიტორინგის განხორციელების გამართლება გარკვეულ სირთულეებთან არის დაკავშირებული.

ზოგიერთი დამსაქმებელი კანონით ვალდებულია, რომ სატრანსპორტო საშუალებებში გამოიყენოს „ტაქოგრაფები“, რათა ჩაიწეროს ინფორმაცია მგზავრობის დროის, სიჩქარისა და მანძილის შესახებ. აღნიშნული მოწყობილობის გამოყენების მიზანია დასაქმებულის სამუშაო საათებთან დაკავშირებული წესების დაცვა. ასეთ შემთხვევაში, უნდა არსებობდეს შესაბამისი სამართლებრივი საფუძველი.

ფოტო: safer-internet.net

შეიძლება თუ არა ბიომეტრიული მონაცემების გამოყენება დროისა და დასწრების კონტროლის მიზნებისთვის?

ბიომეტრიული მონაცემების დამუშავება (მაგალითად, თითის ანაბეჭდი) შესაძლოა, იყოს მოსახერხებელი გზა დასაქმებულთათვის სამუშაო სივრცეზე წვდომის უზრუნველსაყოფად. დამსაქმებელმა უნდა გაითვალისწინოს არსებობს თუ არა ნებისმიერი სხვა ალტერნატივა ბიომეტრიული მონაცემების გამოყენებასთან მიმართებით. ბიომეტრიული მონაცემების დამუშავებისას უსაფრთხოების დარღვევის შემთხვევაში ზიანის რისკი მეტად მაღალია. შესაბამისად, დამსაქმებელმა უნდა გაითვალისწინოს სჭირდება თუ არა დამატებითი უსაფრთხოების ზომები ბიომეტრიული მონაცემების შეგროვების, გამოყენებისა და შენახვის პროცესში.

ბიომეტრიული მონაცემების გამოყენებით დასაქმებული პირის მიმართ მონიტორინგის დროს საჭიროა თუ არა მონაცემთა დაცვაზე ზეგავლენის შეფასება?

ბიომეტრიული მონაცემების დამუშავებისას აუცილებელია მონაცემთა დაცვაზე ზეგავლენის შეფასება. აღნიშნულის მიზეზს წარმოადგენს ის გარემოება, რომ ამგვარი მონაცემების დამუშავება მეტად მაღალ რისკთან არის დაკავშირებული. შესაბამისად, დამსაქმებელი ვალდებულია, რომ დაასრულოს მონაცემთა დაცვაზე ზეგავლენის შეფასება ბიომეტრიული მონაცემების დამუშავებამდე.

გარდა მითითებული საკითხებისა, “ICO”-ს მიერ შემუშავებულ სახელმძღვანელოში წარმოდგენილია დამსაქმებელის მიერ დასაქმებულის მიმართ მონიტორინგის განხორციელებისას გასათვალისწინებელი კრიტერიუმების ჩამონათვალი (“checklists”).

დასაქმებულთა მონიტორინგის პროცესში მონაცემთა დასაცავად მნიშვნელოვანია:

☑ შემოწმდეს, რომ დასაქმებულთა მონიტორინგი დასახული მიზნის მისაღწევად აუცილებელია და არ არსებობს ნაკლებად ინვაზიური გზა;

- ☑ მონაცემთა დაცვაზე ზეგავლენის შეფასების საჭიროების განსაზღვრა;
- ☑ დასაქმებულ პირთა ინტერესების გათვალისწინება მონაცემთა დაცვაზე ზეგავლენის შეფასებასთან დაკავშირებით გადაწყვეტილების მიღებისას;
- ☑ შესაბამისი კანონიერი საფუძვლის არსებობა;
- ☑ განსაკუთრებული კატეგორიის მონაცემთა დამუშავებასთან დაკავშირებული საკითხების გათვალისწინება;
- ☑ დამუშავებული პერსონალური ინფორმაციის აღრიცხვა;
- ☑ შესაბამისი პოლიტიკის დოკუმენტის არსებობა;
- ☑ მონაცემთა დაცვის კონტექსტში შესაბამისი ვალდებულებების გათვალისწინება, როგორიცაა: მონაცემთა მინიმიზაცია, უსაფრთხოება და ა.შ.;
- ☑ მონაცემთა დაცვის საკითხების გათვალისწინება მონიტორინგის სისტემის შექმნისა და დანერგვის პროცესში;
- ☑ მონაცემთა საერთაშორისო გადაცემისთვის შესაბამისი წესების არსებობა.

რა უნდა იცოდეს დამსაქმებელმა, როდესაც მონიტორინგი მხოლოდ ავტომატური საშუალებებით ხორციელდება?

- ☑ გაითვალისწინოს შესაბამისი საკანონმდებლო მოთხოვნები;
- ☑ გაითვალისწინოს სხვა ალტერნატივის არსებობა, მაგალითად, გადაწყვეტილების მიღების პროცესში ადამიანური რესურსის ჩართვა;
- ☑ განახორციელოს სისტემატური შემოწმება, რათა დარწმუნდეს, რომ სისტემა გამართულად მუშაობს.

მონიტორინგის განსახორციელებლად გასათვალისწინებელი სხვა მნიშვნელოვანი საკითხები:

- ☑ წინასწარ, ნათლად უნდა განისაზღვროს მიზანი და არ უნდა შეგროვდეს იმაზე მეტი პერსონალური ინფორმაცია, ვიდრე საჭიროა აღნიშნული მიზნის მისაღწევად;
- ☑ ელექტრონული ფოსტისა და მიმოწერის შემოწმებამდე უნდა განხორციელდეს მონაცემთა დაცვაზე ზეგავლენის შეფასება;
- ☑ დამსაქმებლებმა უნდა გამიჯნონ ქსელთან დაკავშირებული მონაცემები და შინაარსი. შინაარსზე წვდომა უნდა განხორციელდეს საგამონაკლისო შემთხვევებში და აღნიშნულის შესახებ ინფორმაცია დასაქმებულმა უნდა იცოდეს წინასწარ;
- ☑ მნიშვნელოვანია შესაბამისი კანონიერი საფუძვლის განსაზღვრა;
- ☑ უნდა შემუშავდეს პოლიტიკის დოკუმენტი;
- ☑ დასაქმებულებს უნდა მიეწოდოთ ინფორმაცია მონიტორინგის ხასიათის, მოცულობისა და საჭიროების თაობაზე;
- ☑ უნდა შემუშავდეს მონაცემთა შენახვის პოლიტიკის დოკუმენტი.

“EDPB”-მ და “EDPS”-მა ციფრული ევროს პროექტთან დაკავშირებით ერთობლივი მოსაზრება გამოაქვეყნეს

18.10.2023

2023 წლის 18 ოქტომბერს „“მონაცემთა დაცვის ევროპულმა საბჭომ“ (“EDPB”) და „ევროკავშირის მონაცემთა დაცვის ზედამხედველმა“ (EDPS”) ციფრული ევროს პროექტთან დაკავშირებით ერთობლივი მოსაზრება გამოაქვეყნეს.[6]

2023 წლის 29 ივნისს ევროკომისიამ მიმართა “EDPB”-ისა და “EDPS”-ს ერთობლივი მოსაზრების წარდგენის მოთხოვნით ევროკავშირის EU 2018/1725 რეგულაციის (“EUDPR“) 42-ე მუხლის მე-2 პუნქტის შესაბამისად შექმნილ ორ პროექტთან დაკავშირებით, რომლებიც წარმოადგენს „ერთიანი ვალუტის პაკეტის“ ნაწილს. აღნიშნული საკანონმდებლო პაკეტი მოიცავს:

- ციფრული ევროს დაარსების შესახებ რეგულაციის პროექტს (შემდგომში — „პროექტი“);
- რეგულაციის პროექტს ციფრული ევროს მომსახურების მიწოდების შესახებ საგადახდო მომსახურების მიმწოდებლების მიერ, რომლებიც გაერთიანებულია წევრ ქვეყნებში და რომელთა ვალუტა ევრო არ არის. რეგულაციის აღნიშნული პროექტი ცვლის ევროპარლამენტისა და ევროპული საბჭოს რეგულაცია EU 2021/1230-ს.

აღნიშნული ორი პროექტი, მიზნად ისახავს ციფრული ევროს დაარსებას და ევროპელებისთვის როგორც ნაღდი ფულის, ასევე ციფრული გადახდის ვარიანტების უზრუნველყოფას ცენტრალური ბანკის მიერ წარმოებული ვალუტით. “EDPB”-ისა და “EDPS”-ის ერთობლივი მოსაზრების ფარგლებში განხილულია რეგულაციის პროექტთან დაკავშირებით ციფრული ევროს დაარსების შესახებ რეკომენდაციები.

პროექტი ევროპის ცენტრალური ბანკის (“ECB”) მიერ ციფრული ევროს მიღებისა და გამოშვებისთვის საკანონმდებლო ჩარჩოს ადგენს და ძირითადად ეფუძნება “ECB”-ის მიერ 2023 წლის აპრილში გამოქვეყნებული პროგრესის მესამე ანგარიშით გათვალისწინებულ მიდგომებს.

ფოტო: edps.europa.eu

ციფრული ევროს მიღების ისტორია

2023 წლის 28 ივნისს ევროკომისიამ მიიღო საკანონმდებლო პაკეტი ციფრული ევროს შესახებ, რომელიც მოიცავდა პროექტს ციფრული ევროს საკანონმდებლო ბაზის შექმნის შესახებ. აღნიშნული პროექტი

[6] EDPB-EDPS Joint Opinion 02/2023 on the Proposal for a Regulation of the European Parliament and of the Council on the establishment of the digital euro, https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-022023-proposal_en [27.10.2023]

მიზნად ისახავს ციფრული ევროს არსებითი ასპექტების ჩამოყალიბებასა და რეგულირებას, რომლის გამოშვება "ECB"-ის პრეროგატივაა. ციფრული ევროს პროექტი აღნიშნული საკანონმდებლო პაკეტის მიღებამდე დაიწყო.

ცენტრალური ბანკის ციფრული ვალუტების მიმართ მზარდი ინტერესის გათვალისწინებით, "ECB"-მ 2020 წლის ოქტომბერში წამოიწყო საჯარო კონსულტაციები შესაძლო ციფრული ევროს, ცენტრალური ბანკის ციფრული ვალუტის ახალი ფორმის შესახებ, რომელიც საცალო გადახდებში გამოიყენება და მიზნად ისახავს, შეავსოს მატერიალური, ნაღდი ფულის სახით არსებული ევრო. ციფრული ევროს დაარსების პოლიტიკის მიზანია, უზრუნველყოს ევროკავშირის მოქალაქეების მუდმივი ხელმისაწვდომობა ცენტრალური ბანკის ვალუტაზე ნაღდი ფულის გამოყენების შემცირების კონტექსტში, ფინანსური ჩართულობის ხელშეწყობა, აგრეთვე, გადახდებთან დაკავშირებით ევროკავშირში ინოვაციებისა და სტრატეგიული ავტონომიის უზრუნველყოფა.

2021 წლის აპრილში "ECB"-მ გამოაქვეყნა ანგარიში საჯარო კონსულტაციის შედეგად არსებულ გამოხმაურებასთან დაკავშირებით. ანგარიშის თანახმად, კონფიდენციალურობა ციფრული ევროსთვის ყველაზე მნიშვნელოვან მახასიათებლად მიიჩნია გამოკითხულთა 43%-მა, როგორც მოქალაქეებში, ასევე — სფეროს ექსპერტებში.

ფოტო: edpb.europa.eu

2021 წლის 18 ივნისს "EDPB"-მ წერილი გაუგზავნა ევროპულ ინსტიტუტებს შესაძლო ციფრული ევროს პირადი ცხოვრების ხელშეუხებლობისა და მონაცემთა დაცვის ასპექტების შესახებ. აღნიშნულ წერილში "EDPB"-მ ხაზგასმით მიუთითა, რომ ევროპულმა ინსტიტუტებმა უნდა იმუშაონ ციფრულ ევროზე, რომელიც სრულად მოიცავს მიდგომას პირადი ცხოვრების ხელშეუხებლობასა და მონაცემთა დაცვის დიზაინით და პირველად პარამეტრად გათვალისწინების შესახებ ("privacy and data protection by design and by default approach"). გარდა ამისა, "EDPB"-მ ხაზი გაუსვა ამგვარი პროექტისთვის დამახასიათებელ რისკებს პირადი ცხოვრების ხელშეუხებლობისა და სხვა ფუნდამენტური უფლებებისა და თავისუფლებებისთვის, თუ ციფრული ევრო არ იქნება სათანადო დაცვის გარანტიებით აღჭურვილი. კერძოდ, "EDPB"-მ ყურადღება გაამახვილა ტრანზაქციების ზოგადი მეთვალყურეობის (Tracking), ციფრული ევროს გამოყენებით მოქალაქეების გადაჭარბებული იდენტიფიკაციისა და გადახდის მონაცემების უსაფრთხოების რისკებზე და შესთავაზა კანონმდებლებს დახმარება აღნიშნული გამოწვევების საპასუხოდ. უფრო მეტიც, "EDPB" წერილში ემხრობოდა შესაძლებლობას, რომ

გარიგებების ნაწილი ანონიმურად განხორციელებულიყო ან, სულ მცირე, გამოყენებული ყოფილიყო ფსევდონიმიზაციის მაღალი დონე. “EDPB”-მ ასევე აღნიშნა, რომ ფიზიკური ნაღდი ფული იყო შესაბამისი საორიენტაციო ნიშანი ციფრული ევროს დიზაინისთვის, ერთი მხრივ, პირადი ცხოვრების ხელშეუხებლობასა და მონაცემთა დაცვასა და მეორე მხრივ, ფულის გათეთრებასა და ტერორიზმის დაფინანსების წინააღმდეგ ბრძოლას შორის (შემდგომში — “AML/CFT”) ბალანსის დასამყარებლად.

2021 წლის 14 ივლისს “ECB”-მ ციფრული ევროს პროექტის გამოკვლევის ეტაპი დაიწყო. აღნიშული 24-თვიანი ეტაპი მიზნად ისახავდა ევროს ციფრული ფორმის დიზაინისა და განთავსების ძირითადი საკითხების, ასევე, ბაზარზე ციფრული ევროს შესაძლო გავლენის შეფასებას. მოკვლევის სხვა მიზნებს წარმოადგენდა დიზაინის ვარიანტების იდენტიფიცირება პირადი ცხოვრების ხელშეუხებლობის უზრუნველსაყოფად და რისკების თავიდან აცილების მიზნით ევროზონის მოქალაქეების, შუამავლებისა და მთლიანი ეკონომიკისთვის. ევროპის ინსტიტუტებისთვის აღნიშნულ საკითხებზე სამართლებრივი დახმარების ფარგლებში, “EDPB”-მ მონაწილეობა მიიღო გამოკვლევის ეტაპის საკონსულტაციო პროცესში და გამართა რამდენიმე შეხვედრა “ECB”-ის ექსპერტებთან. საჯაროდ გამოთქმული პოზიციების გარდა, “EDPB” ატარებდა რეგულარულ შიდა შეხვედრებს აღნიშნულ საკითხთან დაკავშირებით, რომლებშიც მონაწილეობდნენ ევროკომისიის ექსპერტები.

2022 წლის აპრილში კომისიამ წამოიწყო საჯარო კონსულტაცია, რომელიც მიზნად ისახავდა დამატებითი ინფორმაციის მოპოვებას რიგ ასპექტებზე, მათ შორის, მომხმარებელთა საჭიროებებსა და მოლოდინებზე, ციფრული ევროს განთავსების საკვანძო ინდუსტრიებზე მოსალოდნელ ზემოქმედებაზე, ასევე, პირადი ცხოვრების ხელშეუხებლობასა და მონაცემთა დაცვაზე. “EDPB”-მ აღნიშნულ კონსულტაციას უპასუხა 2022 წლის ივნისში. თავის წერილში “EDPB”-მ კიდევ ერთხელ გააჟღერა პოზიცია “AML/CFT” შემოწმების სრული არარსებობის სასარგებლოდ დაბალი ღირებულების ტრანზაქციებთან დაკავშირებით და მიუთითა ტრანზაქციების ცენტრალიზაციის თავიდან არიდების აუცილებლობაზე ნებისმიერი ისეთი საზოგადოების ან კერძო პირის მიერ, რომელიც მხარს უჭერს ტრანზაქციის შესახებ მონაცემების ადგილობრივ დამუშავებასა და შენახვას. გარდა ამისა, “EDPB”-მ ხაზგასმით აღნიშნა, რომ “ECB”-ისა და ეროვნული ცენტრალური ბანკების (შემდგომში — „ევრო სისტემა“) ნებისმიერი წვდომა ტრანზაქციის მონაცემებზე თაღლითობის თავიდან არიდების ან საგადასახადო წესების აღსრულების მიზნით, უნდა იქნეს აცილებული. “EDPB”-მ აღნიშნა, რომ შენახვის ლიმიტების ან საფასურის ზღვარის შემოღება გავლენას მოახდენს მონაცემთა სუბიექტების უფლებებსა და თავისუფლებებზე, რადგან აღნიშნული საჭიროებს მონაცემთა დამატებით შეგროვებასა და კონტროლს.

2022 წლის სექტემბერში, “ECB”-მ გამოაქვეყნა მის მიერ ჩატარებული გამოკვლევის ეტაპის პროგრესის პირველი ანგარიში, რომლითაც წარადგინა მონაცემთა დაცვისა და პირადი ცხოვრების ხელშეუხებლობის დიზაინის რამდენიმე ვარიანტი ციფრული ევროსთვის. “ECB”-მ ასევე განმარტა, რომ კანონმდებლების მიერ დაწესებული მარეგულირებელი ჩარჩო იქნება ძირითადი საკითხი ციფრული ევროს პირადი ცხოვრების ხელშეუხებლობის ასპექტებთან დაკავშირებით. კერძოდ, “ECB”-მ წარადგინა საბაზისო სცენარი, რომელიც გულისხმობს ციფრული ევროს იმგვარ განვითარებას, რომ უზრუნველყოფილი იყოს მისი ხელმისაწვდომობა ფინანსური შუამავლების მიერ დამოწმებულ ყველა ელექტრონულ ტრანზაქციაში. წარდგენილი პირველადი მოსაზრების თანახმად, ციფრული ევროს განთავსების პროცესი სრულად გამჭვირვალე უნდა იყოს ფინანსური შუამავლებისთვის ციფრული ევროს პირველი გამოშვებიდან მოყოლებული. „შერჩევითი კონფიდენციალურობის“ (“selective privacy”) ორი ვარიანტი, რომლის თანახმადაც პირადი ცხოვრების ხელშეუხებლობის უფრო მაღალი ხარისხით იქნება უზრუნველყოფილი დაბალი ღირებულების/დაბალი რისკის ელექტრონული (“online”) გადახდებისა და არაელექტრონული (“offline”) მოდალობისთვის.

2022 წლის 10 ოქტომბერს, “EDPB”-მ გამოაქვეყნა განცხადება, რომელშიც განმარტა, რომ აუცილებელია, თავიდან იქნეს აცილებული ტრანზაქციის სისტემატური მიკვლევა (“tracing”). მან განმარტა, რომ ციფრული ევროს მეშვეობით განხორციელებული ყველა ტრანზაქციის დადასტურება შესაძლოა, არ შეესაბამებოდეს მონაცემთა დაცვის კანონმდებლობით განსაზღვრულ აუცილებლობისა და პროპორციულობის ცნებებს, ევროკავშირის მართლმსაჯულების სასამართლოს პრეცედენტული სამართლის შესაბამისად. “EDPB”-მ განმარტა, რომ პირადი ცხოვრების ხელშეუხებლობის ერთგვარი ბარიერის შემოღება დაბალი ღირებულების ტრანზაქციებისთვის, რომლებიც არ უნდა დაექვემდებაროს მიკვლევას (“tracing”) აუცილებელი იყო აღნიშნული რისკის შესამცირებლად ციფრული ევროს როგორც ელექტრონული (“online”), ისე არაელექტრონული (“offline”) მოდალობისთვის. გარდა ამისა, “EDPB”-მ რეკომენდაცია გასცა საჯარო და დემოკრატიული დებატების გამართვაზე.

რაც შეეხება ციფრული ევროს “AML/CFT” რეჟიმს, “EDPB”-მ აღნიშნა, რომ ელექტრონული გადახდების მოქმედი საკანონმდებლო ბაზა არ არის შესაფერისი ისეთი ინსტრუმენტისთვის, როგორიცაა ციფრული ევრო, რომელსაც პოლიტიკის მიზნების თვალსაზრისით ფუნდამენტურად განსხვავებული მახასიათებლები აქვს და განიხილა საჯარო კონსულტაციების დროს გამოთქმული მოლოდინების დასაკმაყოფილებლად საჭირო ნდობის ხარისხი.

აღნიშნულიდან გამომდინარე, “EDPB” მხარს უჭერდა ციფრული ევროსთვის სპეციფიკური სამართლებრივი რეჟიმის შექმნას და მიზანშეწონილად მიიჩნევდა ერთდროულად პირადი ცხოვრების

ხელშეუხებლობისა და ასევე “AML/CFT” რისკების შეფასებას.

ფოტო: ecb.europa.eu

“EDPB”-ისა და “EDPS”-ის რეკომენდაციები

“ECB”-ის მიერ ციფრული ევროს გამოშვების მოკვლევის ფაზის დაწყებიდან ორი წლის შემდეგ, ევროპარლამენტი და ევროპული საბჭო უახლოეს თვეებში განიხილავს რეგულაციის პროექტს, რომელიც ციფრულ ევროს ცენტრალური ბანკის ციფრულ ვალუტად დაადგენს. ციფრული ევროს განსაკუთრებული მნიშვნელობის გათვალისწინებით პირადი ცხოვრების ხელშეუხებლობის ფუნდამენტური უფლებისა და პერსონალური მონაცემების დაცვის მიზნით, ევროკომისიამ მოითხოვა, რომ “EDPB”-სა და “EDPS”-ს გამოეთქვა ერთობლივი მოსაზრება აღნიშნულ პროექტთან დაკავშირებით.

1. “EDPB”-მ და “EDPS-მა განმარტეს, რომ ციფრული ევროს განსაკუთრებული ღირებულება უაღრესად კონკურენტული გადახდების საშუალებებს შორის, ძირითადად, მის კონფიდენციალურ ბუნებაში მდგომარეობს. “EDPB” და “EDPS” მიესალმებიან, რომ ციფრულ მომხმარებლებს ყოველთვის ექნებათ არჩევანი, გადაიხადონ ციფრული ევროს თუ ნაღდი ფულის გამოყენებით, ასევე, მიდგომას, რომლის თანახმად, ციფრული ევრო არ იქნება ე. წ. „პროგრამირებადი ფული“. აღსანიშნავია პროექტის მიზანი, უზრუნველყოს პირადი ცხოვრების ხელშეუხებლობა და მონაცემთა დაცვის მაღალი სტანდარტი ციფრული ევროსთვის და გაწეული ძალისხმევა, განსაკუთრებით კი ინტერნეტზე წვდომის გარეშე მოქმედ არაელექტრონული (“offline”) მოდალობის შემოღებით, რათა შემცირდეს პერსონალურ მონაცემთა დამუშავება ციფრულ ევროსთან დაკავშირებით, ასევე ინტეგრირდეს მონაცემთა დაცვის დიზაინის და მონაცემთა დაცვის ნაგულისხმევ პარამეტრად გათვალისწინების (“data protection by design and by default”) ფუნქციები ციფრული ევროს შინაარსში.

2. თუმცა, “EDPB” და “EDPS“ კანონმდებლების ყურადღებას ამახვილებენ პერსონალურ მონაცემთა დაცვასთან დაკავშირებულ არაერთ პრობლემაზე, რომლებმაც შეიძლება, უარყოფითად იმოქმედოს მოქალაქეების ნდობაზე მომავალში ციფრულ ევროსა და მის სოციალურ ათვისებასთან დაკავშირებით, თუ აღნიშნულ გამოწვევათა გადაჭრის გზები გათვალისწინებული არ იქნება პროექტით.

3. მიუხედავად იმისა, რომ “EDPB” და “EDPS” მიესალმებიან ციფრული ევროს განთავსებას „დეცენტრალიზებული წესით“, ანუ ფინანსური შუამავლების და არა უშუალოდ ევრო სისტემის მიერ, ისინი მიიჩნევენ, რომ შემდგომი განმარტებები ციფრული ევროს განთავსების მოდალობასთან დაკავშირებით

საკანონმდებლო ტექსტში უნდა იყოს შეტანილი.

4. უფრო მეტიც, “EDPB” და “EDPS” მიიჩნევენ, რომ მეტად უნდა განიმარტოს ციფრული ევროს უნიკალური იდენტიფიკატორების ერთიანი წვდომის წერტილის აუცილებლობისა და პროპორციულობის საკითხები, ასევე თუ როგორ უნდა განხორციელდეს მონაცემთა დაცვა დიზაინით და ნაგულისხმევ პარამეტრად გათვალისწინებით (“data protection by design and by default”). გარდა ამისა, საკანონმდებლო ტექსტი უნდა შეიცავდეს განმარტებებს, თუ როგორ უნდა დამუშავდეს პერსონალური მონაცემები გადახდის მომსახურების მომწოდებლების (“PSP”) მიერ, რათა პრაქტიკაში დაცული იქნეს შენახვის ლიმიტები. მეტი სიცხადე ასევე მოითხოვება “PSP”-ების მიერ პერსონალური მონაცემების დამუშავებასთან დაკავშირებით მოთხოვნილი მოსაკრებლების ლიმიტების აღსრულების მიზნით.

5. რაც შეეხება ანგარიშსწორების ინფრასტრუქტურას, რომელიც უზრუნველყოფილი და მართული იქნება “ECB”-ის მიერ, “EDPB” და “EDPS” მიიჩნევენ, რომ პროექტის ამოქმედების პირობები უნდა შეიცავდეს ვალდებულებას, რომელიც უზრუნველყოფს “ECB”-სა და ეროვნულ ცენტრალურ ბანკებს შორის არსებული ყველა ტრანზაქციის მონაცემების ფსევდონიმიზაციას.

6. “EDPB” და “EDPS” ასევე მიიჩნევენ, რომ თაღლითობის გამოვლენისა და პრევენციის ზოგად მექანიზმთან (“FDPM”) დაკავშირებული დებულებები, რომელიც “ECB”-მ შეიძლება აირჩიოს “PSP”-ების მიერ თაღლითობის გამოვლენისა და პრევენციის გასაადვილებლად, არ არის განჭვრეტადი. აღნიშნული კი საფრთხეს უქმნის სამართლებრივ განსაზღვრულობასა და შესაძლებლობას, შეფასდეს ასეთი მექანიზმის დანერგვის აუცილებლობა. გაურკვეველია, კონკრეტულად, რა ამოცანებს შეასრულებს “ECB” (როგორც “PSP”-ების მიერ განხორციელებული თაღლითობის შესაძლო ზედამხედველი) და რომელ ამოცანებს (და მასთან დაკავშირებულ მონაცემთა დამუშავებას) შეასრულებენ “PSP”-ები. ამიტომ, “EDPB” და “EDPS” კანონმდებლებს მოუწოდებენ, წარმოაჩინონ ამგვარი მექანიზმის დანერგვის აუცილებლობა და უზრუნველყონ მკაფიო და ზუსტი წესები, რომლებიც არეგულირებს “FDPM”-ის ფარგლებსა და გამოყენებას, მათ შორის, “ECB”-ის მიერ “PSP”-ების მხარდაჭერის თვალსაზრისით. თუ ამგვარი აუცილებლობა არ გამოვლინდა, “EDPB” და “EDPS” რეკომენდაციას უწევენ, მონაცემთა დაცვის პერსპექტივიდან ნაკლებად შემზღუდველი ზომების დანერგვას, სათანადო გარანტიების განხორციელებასთან ერთად.

7. გარდა ამისა, აღნიშნულ ერთობლივ მოსაზრებაში “EDPB” და “EDPS” აღიარებენ იმ პოტენციურ რისკებს, რომელთა წინაშეც შეიძლება, აღმოჩნდეს ციფრული ევრო ინფორმაციული ტექნოლოგიებისა და კიბერუსაფრთხოების პერსპექტივიდან გამომდინარე და რეკომენდაციას უწევენ პროექტის პრეამბულაში მკაფიოდ მიეთითოს კიბერუსაფრთხოების შესახებ მოქმედ საკანონმდებლო ბაზაზე.

8. რაც შეეხება ციფრული ევროსთან დაკავშირებულ პირადი ცხოვრების ხელშეუხებლობისა და მონაცემთა დაცვის ასპექტებს, “EDPS” და “EDPB” დადებითად ეხმაურებიან პროექტის VIII თავსა და გაწეულ ძალისხმევას, რათა დადგინდეს პერსონალური მონაცემების დამუშავების მიზნები და კატეგორიები თითოეული მოქმედი პირის მიერ ციფრული ევროს გამოშვებისა და გამოყენებისთვის განხორციელებულ მონაცემთა დამუშავების მოქმედებასთან დაკავშირებით. ამასთან, კანონმდებლებმა უნდა უზრუნველყონ დამატებითი განმარტებები აღნიშნული დამუშავების მოქმედებების სამართლებრივ საფუძვლებთან, პასუხისმგებლობების განაწილებასა და თითოეული მოქმედი პირის მიერ დასამუშავებელი პერსონალური მონაცემების ტიპებთან დაკავშირებით.

9. “EDPB” და “EDPS” სინანულს გამოთქვამენ, რომ პროექტით უარყოფილია „შერჩევითი კონფიდენციალურობის“ მიდგომა დაბალი ღირებულების ელექტრონული გადახდის ოპერაციებისთვის. ამასთან დაკავშირებით, უნდა აღინიშნოს, რომ “AML/CFT” რისკის დონე ელექტრონული ციფრული ევროსთვის დამოკიდებული იქნება გამოყენებულ ტექნოლოგიასა და კონცეფციის შემუშავების ეტაპზე გაკეთებულ დიზაინის არჩევანზე. ამგვარი რისკის შესამცირებლად, “EDPB” და “EDPS” ურჩევენ კანონმდებლებს არაელექტრონულ (“offline”) მოდალობაზე გაავრცელონ მოქმედი სპეციალური რეჟიმი დაბალი ღირებულების ტრანზაქციების ელექტრონულ (“online”) მოდალობაზე, იმ ზღვარის შემოღებით, რომლის ქვემოთაც არ იქნება ტრანზაქციების კვალიფიკაცია “AML/CFT” მიზნებისთვის მნიშვნელოვანი.

10. “EDPB” და “EDPS” განმარტავენ, რომ ციფრული ევროს გამოყენებით მონაცემთა ყველა დამმუშავებელმა უნდა ჩაატაროს მონაცემთა დაცვაზე ზეგავლენის შეფასება “GDPR“-ის 35-ე მუხლის ან “EUDPR”-ის 39-ე მუხლის მოთხოვნების შესაბამისად. გარდა ამისა, პროექტი უნდა მოიცავდეს პირადი ცხოვრების ხელშეუხებლობისა და მონაცემთა დაცვის ვალდებულებას დიზაინით და პირველად პარამეტრად (“privacy and data protection by design and by default”) საოპერაციო დიზაინისა და ტექნოლოგიური არჩევანის დადგენისას.

ციფრული ევროს შესახებ კანონმდებლობის მიღების შემდეგ, “EDPB” და “EDPS” თითოეული თავისი პასუხისმგებლობის ფარგლებში, გააგრძელებენ ციფრული ევროს განთავსების მონიტორინგს და მზად იქნებიან, გაუწიონ რეკომენდაცია კანონმდებლებს, “ECB”-ს ციფრულ ევროსთან დაკავშირებით პერსონალური მონაცემთა დაცვის ასპექტების შესახებ.

“GDPR”-ის დანაწესის დარღვევისთვის ირლანდიის ცენტრალურ ბანკს შესაძლოა რეკორდული ოდენობის ჯარიმა დაეკისროს

16.10.2023

ფოტო: centralbanking.com

“GDPR“-ის (მონაცემთა დაცვის ზოგადი რეგულაციის) მოთხოვნათა დარღვევის გამო, ირლანდიის ცენტრალურ ბანკი რეკორდული ოდენობის ჯარიმის დაკისრების რისკის ქვეშაა.[7]

ირლანდიის ცენტრალური ბანკი წარმოადგენს მონაცემთა მსხვილ დამმუშავებელს, რომელიც ათასობით ბენეფიციარის პირად ინფორმაციას ამუშავებს და ინახავს. როგორც ირლანდიის მონაცემთა დაცვის კომისრის (“DPC”) მიერ ჩატარებული მოკვლევით დადგინდა, ბანკი ინახავდა მონაცემთა სუბიექტების შესახებ ინფორმაციას იმაზე მეტ ხანს, ვიდრე ეს “GDPR”-ით არის დაშვებული. სულ მცირე 20 000 პირის საკრედიტო ისტორია ხელმისაწვდომი იყო ბანკისთვის მაშინ, როდესაც აღნიშნული მონაცემი უნდა წაეშალათ.

საკითხთან დაკავშირებით, “DPC”-ის მიერ დაიწყო ყოვლისმომცველი მოკვლევა ცენტრალური ბანკის დარღვევის შესახებ. დარღვევის შედეგად, ბანკს შესაძლოა დაეკისროს ერთ-ერთი ყველაზე მსხვილი ჯარიმა, რაც კი ოდესმე ყოფილა გამოყენებული საჯარო ორგანოს მიმართ მონაცემთა სუბიექტის უფლებების დარღვევისთვის. ირლანდიის კანონმდებლობის მიხედვით, მონაცემთა დაცვის საზედამხედველო ორგანოს შეუძლია, რომ მონაცემთა არამართლზომიერი შენახვისთვის საჯარო ორგანო 1 მილიონი ევროს ოდენობით დააჯარიმოს.

აღნიშნული დარღვევა უკავშირდება ცენტრალურმა ბანკის მიერ ცენტრალურ საკრედიტო რეესტრში (CCR) ბენეფიციარების მონაცემების შენახვას დასაშვებზე 3 თვით მეტი დროით. ნაცვლად იმისა, რომ 2018 წლის მაისში, ივნისსა და ივლისში დამუშავებული მონაცემები ხუთწლიანი ვადის გასვლის შედეგად წაშლილიყო, მიმდინარე წლის 1 ივნისიდან 7 აგვისტომდე მდგომარეობით, ისინი კვლავ ხელმისაწვდომი იყო ბანკისთვის და შესაბამისად, იყო ასახული გაცემულ საკრედიტო ანგარიშებში. აღნიშნულმა დარღვევამ ზეგავლენა მოახდინა სულ მცირე 50 საკრედიტო გადაწყვეტილებაზე და ამ მიზეზით, ბენეფიციარებს შესაძლოა, უარი ეთქვათ სესხის მიღებაზე.

[7]იხ. ელექტრონული წყარო: <Central Bank faces historic fine for major GDPR breach | Business Post>.

ირლანდიის ცენტრალური ბანკი სინანულს გამოხატავს ამ შემთხვევასთან დაკავშირებით და მის მიერ დაშვებული შეცდომის გამო საზოგადოებას ბოდიშს უხდის. ამასთან, ბანკის მმართველობა პასუხისმგებლობას იღებს დარღვევასთან დაკავშირებით და გეგმავს აუცილებელი ზომების მიღებას მომავალში მსგავსი შემთხვევის თავიდან ასაცილებლად.

ფინეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ "Yandex"-ის მონაცემების რუსეთში გადაცემის აკრძალვა გააუქმა

15.10.2023

ფოტო: Wikipedia

ფინეთის მონაცემთა დაცვის საზედამხედველო ორგანომ გააუქმა "Yandex"-ისა და მისი ჰოლანდიელი პარტნიორის — "Ridetech"-ის მიმართ გამოცემული ბრძანება მონაცემთა დამუშავების დროებითი აკრძალვის თაობაზე.[8]

აკრძალვა განპირობებული იყო რუსეთის ფედერაციის უსაფრთხოების სამსახურის მიერ ფინელ მომხმარებელთა პერსონალურ მონაცემებზე შესაძლო წვდომით. ფინეთის მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება მიღებული იყო ტაქსის მომსახურების შესახებ რუსეთის ფედერაციის ახალი კანონის საპასუხოდ, გადაუდებელი პროცედურების ფარგლებში, რომელსაც ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაცია" ("GDPR") ითვალისწინებს.

ფინეთის პერსონალურ მონაცემთა დაცვის ომბუცმენის ოფისის განცხადებით, აღნიშნული გადაწყვეტილება არ მოწმობს იმას, რომ რუსეთში მონაცემთა გადაცემა "GDPR"-ის შესაბამისად ხორციელდება ან რომ რუსეთის ფედერაციაში სათანადოდ არის უზრუნველყოფილი პერსონალურ მონაცემთა დაცვა.[9] განცხადებაში აღნიშნულია, რომ მიმდინარე წლის ოქტომბერში საზედამხედველო ორგანოს მიერ მიღებული გადაწყვეტილება მონაცემთა გადაცემის აკრძალვის თაობაზე იყო შუალედური; "Yango"-სთან დაკავშირებით საბოლოო გადაწყვეტილების მიღების უფლებამოსილება ფინეთის მონაცემთა დაცვის საზედამხედველო ორგანოს არ აქვს. როგორც აღნიშნულია გამოქვეყნებულ განცხადებაში, საბოლოო გადაწყვეტილება უნდა გამოიტანოს იმ მონაცემთა დაცვის საზედამხედველო ორგანომ, რომელიც პასუხისმგებელია

[8] იხ. ელექტორნული ბმული: <https://gdprbuzz.com/news/finland-lifts-ban-on-transferring-yandex-data-to-russia/>.

[9] იხ. ფინეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს განცხადება: <The Data Protection Ombudsman's decision does not address the legality of data transfers to Russia – the matter remains under investigation | Data Protection Ombudsman's Office (tietosuoja.fi)>.

საქმეზე. აქვე საგულისხმოა, რომ “Yango”-ს საქმის შესწავლა კვლავ მიმდინარეობს. “Yango”-ს მიერ მონაცემთა გადაცემის კანონიერების შეფასება და საბოლოო გადაწყვეტილების მიღება განხორციელდება „ტრანსსასაზღვრო პროცედურის“ (cross-border procedure”) ფარგლებში, რომლის მიხედვითაც, ევროკავშირის მონაცემთა დაცვის საზედამხედველო ორგანოები საკითხის შესწავლისას ურთიერთთანამშრომლობენ. აღნიშნული შეფასების ძირითადი კომპონენტი რუსეთში მონაცემთა დაცვის სათანადო დონის არსებობის შემოწმებაა.

განსახილველ საქმეზე საბოლოო გადაწყვეტილების მომზადებაზე პასუხისმგებელი უწყება ნიდერლანდების პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოა (როგორც წამყვანი საზედამხედველო ორგანო). მიუხედავად აღნიშნულისა, ფინეთის პერსონალურ მონაცემთა დაცვის ომბუცმენის ოფისი საკითხის შესწავლის ყველა ეტაპზე მიიღებს მონაწილეობას. თუკი საკითხის გადაწყვეტისას საზედამხედველო ორგანოები ვერ შეთანხმდებიან, საქმე განსახილველად „მონაცემთა დაცვის ევროპულ საბჭოს“ (“EDPB”) გადაეცემა — აღნიშნულია ფინეთის მონაცემთა დაცვის საზედამხედველო ორგანოს განცხადებაში.

(+ 995 32) 242 1000
office@pdps.ge
www.pdps.ge