მსოფლიო პრაქტიკა

პერსონალურ მონაცემთა დაცვის სამსახური

სიახლეები

საფრანგეთის მონაცემთა დაცვის საზედამხედველო ორგანო ("CNIL") მოხუცთა თავშესაფრებში ვიდეომეთვალყურეობის შესახებ რეკომენდაცია გამოაქვეყნა

გაერთიანებული სამეფოს მონაცემთა დაცვის საზედამხედველო ორგანომ გენერირებადი ხელოვნური ინტელექტის გამოყენებისთვის საჭირო წესების შემუშავების მესამე ეტაპი დაიწყო

ადამიანის უფლებათა ევროპულმა სასამართლომ ("ECtHR") პერსონალური მონაცემების განუსაზღვრელი ვადით შენახვის თაობაზე გადაწყვეტილება მიიღო

2024 წლის 16 აპრილს, ადამიანის უფლებათა ევროპულმა სასამართლომ ("ECtHR") საქმეზე "Borislav Tonchev v. Bulgaria"[1] მიიღო გადაწყვეტილება, რომელიც საპოლიციო სისტემაში პერსონალური მონაცემების განუსაზღვრელი ვადით შენახვას შეეხება.

EUROPEAN COURT OF HUMAN RIGHTS

მაისი 2024

- ფაქტობრივი გარემოებები:

მომჩივანს წარმოადგენს 1981 წელს დაბადებული, ბულგარეთის მოქალაქე. 2004 წლის ივნისში, იგი დაინიშნა ბადრაგის პოზიციაზე, რა მიზნითაც მან მარტის თვეში ნასამართლობის არარსებობის შესახებ ცნობა წარადგინა. საქმის ფაქტობრივი გარემოებების თანახმად, 2004 წლის მაისის თვეში, განმცხადებელი ალკოჰოლის ზემოქმედების ქვეშ მართავდა სატრანსპორტო საშუალებას, რის გამოც ადმინისტრაციული პასუხისმგებლობის სახით მას ჯარიმა დაეკისრა.

აღსანიშნავია, რომ სასამართლო სისტემის უსაფრთხოების უზრუნველყოფის მიზნით, 2012 წელს, ბულგარეთის იუსტიციის სამინისტრომ სხვადასხვა ვაკანტურ პოზიციაზე კონკურსი გამოაცხადა. კონკურსში მონაწილეობის მისაღებად, მომჩივანმა წარადგინა განაცხადი, რომლის საფუძველზეც დამსაქმებელმა ლოვეჩის რაიონული სასამართლოს კრიმინალური ჩანაწერების ბიუროდან (“Lovech District Court’s criminal records bureau”) განმცხადებლის სისხლისსამართლებრივი ჩანაწერების თაობაზე ინფორმაცია ელექტრონული ფორმით გამოითხოვა. დოკუმენტში ასახული იყო ნასვამ მდგომარეობაში ავტოსატრანსპორტო საშუალების მართვის გამო მომჩივანისთვის ადმინისტრაციული პასუხისმგებლობის დაკისრების შესახებ მონაცემები, რომლის საფუძველზე მას უარი ეთქვა კონკურსში მონაწილეობაზე. ამასთანავე, 2013 წელს მომჩივანი გაათავისუფლეს ბადრაგის პოზიციიდან იმ არგუმენტით, რომ წარსულში მასზე დაკისრებული ადმინისტრაციული პასუხისმგებლობა შეუთავსებელი იყო მის მოქმედ თანამდებობასთან.

გასათვალისწინებელია, რომ ბულგარეთის კანონმდებლობის თანახმად, პირის ადმინისტრაციულ პასუხისმგებლობასთან დაკავშირებული დოკუმენტაცია კანონით განსაზღვრულ ვადაში უნდა განადგურებულიყო, ხოლო ელექტრონული ფორმით შენახვაზე რაიმე მითითება არ არსებობდა.

აღნიშნული შემთხვევა შეაფასეს ბულგარეთის ადმინისტრაციულმა სასამართლომ და პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ. ბულგარეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილებით, მატერიალურ დოკუმენტაციასთან ერთად, ელექტრონული მონაცემებიც უნდა წაშლილიყო, რადგან ელექტრონული ფორმით მონაცემების განუსაზღვრელი ვადით შენახვა ეწინააღმდეგებოდა ბულგარეთის პერსონალურ მონაცემთა დაცვის კანონმდებლობას. ადმინისტრაციულმა სასამართლომ მომწესრიგებელ კანონმდებლობაზე დაყრდნობით მომჩივნის ადმინისტრაციული პასუხისმგებლობის შესახებ ინფორმაციის მოპოვება და აღნიშნული საფუძვლით მისი გათავისუფლება სადავოდ არ მიიჩნია.

- მომჩივნის მოთხოვნა:

„ადამიანის უფლებათა და ძირითად თავისუფლებათა დაცვის კონვენციის“ მე-8 მუხლზე („პირადი და ოჯახური ცხოვრების დაცულობის უფლება“) დაყრდნობით, მომჩივანი დაობდა ადმინისტრაციულ სახდელთან დაკავშირებული ინფორმაციის განუსაზღვრელი ვადით შენახვისა და აღნიშნული მონაცემების გამჟღავნების შესახებ, რადგან ბულგარეთის პერსონალურ მონაცემთა დაცვის მომწესრიგებელი კანონმდებლობის შესაბამისი ნორმა იყო ორაზროვანი.

- ადამიანის უფლებათა ევროპული სასამართლოს შეფასება:

ადამიანის უფლებათა ევროპულმა სასამართლომ პირადი ცხოვრების ხელშეუხებლობის უფლებაში ჩარევის მართლზომიერების შესაფასებლად შემდეგი წინაპირობები განიხილა:

კანონთან შესაბამისობა

პირადი ცხოვრების ხელშეუხებლობის უფლებაში ჩარევა უნდა იყოს „კანონის შესაბამისი“, რაც გულისხმობს, რომ ეროვნული კანონმდებლობა უნდა ითვალისწინებდეს უფლებაში ჩარევის შესაბამის სამართლებრივ საფუძველს. ამასთანავე, აღნიშნული კანონი უნდა იყოს ხელმისაწვდომი და განჭვრეტადი.

საქმის ფაქტობრივი გარემოებების გათვალისწინებით, ევროპულ სასამართლომ შეაფასა, ადმინისტრაციულ სანქციასთან დაკავშირებული პერსონალური მონაცემების შენახვის თაობაზე ბულგარეთის მომწესრიგებელი კანონმდებლობის განჭვრეტადობა. სასამართლომ აღნიშნა, რომ კანონმდებლობა ითვალისწინებდა ადმინისტრაციული სახდელის შესახებ მატერიალური ჩანაწერების შენახვის ვადას, თუმცა არ აწესრიგებდა ელექტრონულ მონაცემთა დამუშავების საკითხს.

სტრასბურგის სასამართლომ ყურადღება გაამახვილა ეროვნული კანონმდებლობის შესახებ ადმინისტრაციული სასამართლოს და პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს შეფასებების სხვადასხვაობაზე.

ევროპულმა სასამართლომ აღნიშნა, რომ საკანონმდებლო მოწესრიგება, რომელიც არის ბუნდოვანი და წარმოშობს აზრთა სხვადასხვაობას, არ შეიძლება იყოს საკმარისად განჭვრეტადი. სასამართლოს შეფასებით, ეროვნულმა ადმინისტრაციულმა სასამართლომ არ იმსჯელა „შენახვის ვადის შეზღუდვის“ პრინციპთან მონაცემთა ელექტრონული ჩანაწერების განუსაზღვრელი ვადით შენახვის შესაბამისობაზე. აგრეთვე, ევროპულმა სასამართლომ არ გაიზიარა ეროვნული ადმინისტრაციული სასამართლოს მსჯელობა მასზედ, რომ ადმინისტრაციული სახდელის თაობაზე მონაცემების განუსაზღვრელი ვადით შენახვა აუცილებელი იყო იმ ლეგიტიმური მიზნის მისაღწევად, რომლის შესაბამისად დაუშვებელია, სამართალდამრღვევ პირს ერთი და იმავე დანაშაულისათვის განმეორებით დაედოს მსჯავრი. ევროპული სასამართლოს შეფასებით, ამგვარი მიზეზის არსებობა მაინც არ ამართლებდა მონაცემების განუსაზღვრელი ვადით შენახვას. შესაბამისად, სასამართლომ დაადგინა, რომ მომჩივნის მიმართ დაკისრებული ადმინისტრაციული პასუხისმგებლობის შესახებ მონაცემების განუსაზღვრელი ვადით შენახვა არ არის „კანონთან შესაბამისი“.

- დემოკრატიულ საზოგადოებაში აუცილებლობა:

მომჩივნის მტკიცებით, პერსონალური მონაცემების განუსაზღვრელი ვადით შენახვა, მიუხედავად მიზნისა, იყო არაპროპორციული. მოპასუხე სახელმწიფოს არგუმენტაციით, მონაცემების განუსაზღვრელი ვადით შენახვა იყო „აუცილებელი დემოკრატიულ საზოგადოებაში“ და ემსახურებოდა შესაბამის სამართლებრივ მიზანს.

ევროპულმა სასამართლომ აღნიშნა, ვინაიდან მოცემული შემთხვევის ფაქტობრივი გარემოებების საფუძველზე დადგინდა, რომ ადამიანის უფლებაში ჩარევა არ იყო „კანონთან შესაბამისი“, აღარ არსებობდა „დემოკრატიულ საზოგადოებაში აუცილებლობის“ შეფასების საჭიროება.

აღნიშნულის გათვალისწინებით, სასამართლომ საქმეზე “Borislav Tonchev v. Bulgaria” დაადგინა პირადი და ოჯახური ცხოვრების დაცულობის უფლების

ევროკავშირის მართლმსაჯულების სასამართლომ (“CJEU”) მონაცემთა უსაფრთხოების დარღვევაზე საზედამხედველო ორგანოს რეაგირების ვალდებულების შესახებ გენერალური ადვოკატის მოსაზრება გამოაქვეყნა

2024 წლის 11 აპრილს, ევროკავშირის მართლმსაჯულების სასამართლომ (“CJEU”) საქმეზე: “TR v Land Hessen” გენერალურ ადვოკატ პრიიტ პიკამაეს მოსაზრება გამოაქვეყნა,[1] რომელიც შეეხება საზედამხედველო ორგანოს ვალდებულებას, დაუყოვნებლივ იმოქმედოს მონაცემთა უსაფრთხოების დარღვევის ფაქტის (ინციდენტის) აღმოჩენის შემთხვევაში.

საქმის ფაქტობრივი გარემოებების თანახმად, გერმანიაში, ჰესენის ფედერალური მიწის ერთ-ერთი კომერციული ბანკის მომხმარებელმა (მონაცემთა სუბიექტმა), მისი პერსონალური მონაცემების უსაფრთხოების დარღვევისა და მონაცემთა უკანონოდ დამუშავების გამო, ჰესენის მონაცემთა დაცვის საზედამხედველო ორგანოს კომერციული ბანკის წინააღმდეგ, საჯარიმო ღონისძიებების განხორციელების განცხადებით მიმართა. კერძოდ, ბანკის თანამშრომლისთვის, შესაბამისი საფუძვლის გარეშე, მომხმარებლის პერსონალური მონაცემები გახდა ხელმისაწვდომი, რამაც მონაცემთა უკანონოდ დამუშავება გამოიწვია.

[1] ECtHR, Case of Borislav Tonchev V. Bulgaria, Appl. No. 40519/15, 16 April 2024,
<
<[1]https://www.edpb.europa.eu/news/news/2024/edpb-sets-out-priorities-2024-2027-and-clarifies-implementation-dpf-redress_en>.
[2] აღსანიშნავია, რომ 2022 წლის 28 აპრილს „მონაცემთა დაცვის ევროპულმა საბჭომ“ შეიმუშავა წინადადება ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ ეფექტიანი აღსრულების მიზნით საბჭოს წევრ მონაცემთა დაცვის საზედამხედველო ორგანოთა შორის თანამშრომლობის შესახებ. Statement on enforcement cooperation, adopted on 28 April 2022, <https://www.edpb.europa.eu/our-work-tools/our-documents/statements/statement-enforcement-cooperation_en>, [26.04.2024].
>.

ჰესენის მონაცემთა დაცვის საზედამხედველო ორგანომ კომერციული ბანკის ინსპექტირების შედეგად ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ დარღვევა დაადგინა. მიუხედავად აღნიშნულისა, ბანკს შესაბამისი პასუხისმგებლობა არ დააკისრა, ვინაიდან მას აღნიშნული თანამშრომლის მიმართ უკვე ჰქონდა დისციპლინური პასუხისმგებლობისათვის შესაბამისი ღონისძიებები განხორციელებული.

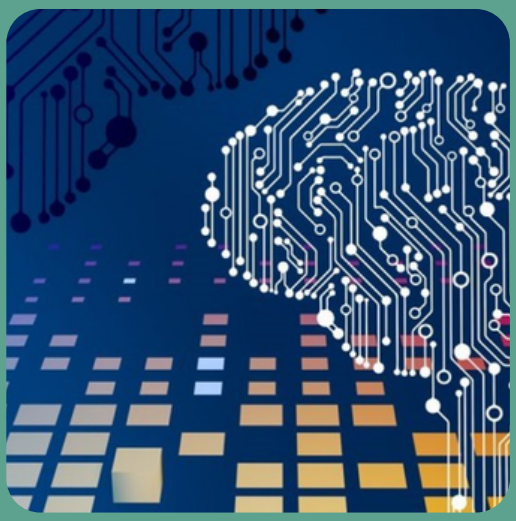
კომერციული ბანკის მომხმარებელმა (მონაცემთა სუბიექტმა) ჰესენის მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება გერმანიის ვისბადენის ადმინისტრაციულ სასამართლოში გაასაჩივრა, რომელმაც ევროკავშირის მართლმსაჯულების სასამართლოს მონაცემთა დარღვევის ფაქტის აღმოჩენის შემთხვევაში, „მონაცემთა დაცვის ძირითადი რეგულაციის“ მიხედვით საზედამხედველო ორგანოს უფლებამოსილებებისა და ვალდებულებების განმარტების თხოვნით მიმართა.
გენერალური ადვოკატის მოსაზრებით, პერსონალურ მონაცემთა დაცვის ეროვნული საზედამხედველო ორგანო ვალდებულია, დაუყოვნებლივ იმოქმედოს მონაცემთა უსაფრთხოების დარღვევის ფაქტის (ინციდენტის) გამოვლენის ან შესაბამისი ინფორმაციის მიღების შემთხვევაში. მონაცემთა სუბიექტის უფლებების დაცვის უზრუნველყოფის მიზნით, საზედამხედველო ორგანო ვალდებულია, დარღვევის სიმძიმის გათვალისწინებით, განახორციელოს სათანადო (“appropriate”), აუცილებელი (“necessary”) და პროპორციული (“proportionate”) ღონისძიება. იმ შემთხვევაში, თუკი აღარ იარსებებს აქტიური მოქმედებისა და სათანადო ღონისძიებების განხორციელების აუცილებლობა, საზედამხედველო ორგანოს აქვს დისკრეცია თავი შეიკავოს „მონაცემთა დაცვის ძირითადი რეგულაციით“ დადგენილი საჯარიმო ზომების გამოყენებისგან, განსაკუთრებით კი მაშინ, როდესაც დამუშავებისთვის პასუხისმგებელ პირს საკუთარი ინიციატივით აქვს მიღებული სათანადო ღონისძიებები. ასეთ შემთხვევაში, მონაცემთა სუბიექტსაც არ აქვს უფლება, მოითხოვოს რაიმე კონკრეტული ღონისძიების განხორციელება დამუშავებისთვის პასუხისმგებელი პირის მიმართ.

გენერალური ადვოკატის მოსაზრება ეყრდნობა „მონაცემთა დაცვის ძირითადი რეგულაციის“ 57-ე მუხლის პირველი პუნქტის „ა“ ქვეპუნქტს, რომლის თანახმად, საზედამხედველო ორგანო მისი ტერიტორიული მოქმედების ფარგლებში ზედამხედველობს რეგულაციის იმპლემენტაციისა და აღსრულების პროცესს. ასევე, მისი უფლებამოსილებაა მონაცემთა სუბიექტის მიერ რეგულაციის მე-80 მუხლის მიხედვით წარდგენილი განცხადების განხილვა და მასში მითითებული გარემოებების შესწავლა, აგრეთვე, განმცხადებლის გონივრულ ვადაში ინფორმირება საქმის მიმდინარეობის და შედეგების შესახებ. ამასთანავე, რეგულაციის 58-ე მუხლის მეორე პუნქტის „ა“ ქვეპუნქტის მიხედვით, საზედამხედველო ორგანო უფლებამოსილია განახორციელოს შესაბამისი პრევენციული ფუნქციაც. კერძოდ, გააფრთხილოს მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი ან დამუშავებაზე უფლებამოსილი პირი, რომ მონაცემთა დაგეგმილი დამუშავება სავარაუდოდ გამოიწვევს რეგულაციის დებულებათა დარღვევას.

გენერალური ადვოკატის დასკვნიდან გამომდინარეობს, რომ საზედამხედველო ორგანო ვალდებულია, დაუყოვნებლივ იმოქმედოს პერსონალური მონაცემების უსაფრთხოების დარღვევის ფაქტის (ინციდენტის) აღმოჩენისას, შეისწავლოს საკითხი, რის შემდეგაც იგი უფლებამოსილია, მიიღოს გადაწყვეტილება დამუშავებისთვის პასუხისმგებელი პირისთვის ადმინისტრაციული პასუხისმგებლობის დაკისრების შესახებ.
საგულისხმოა, რომ აღნიშნული საქმე განხილვის პროცესშია, ხოლო გენერალური ადვოკატის მოსაზრება ევროკავშირის მართლმსაჯულების სასამართლოსთვის არ არის სავალდებულო ძალის მქონე.

[1] CJEU publishes opinion on obligation of supervisory authorities to act on discovery of a data breach: Opinion of Advocate General Pikamäe, Case C-768/21, <dataguidance.com> [22.04.2024].

გაერთიანებული სამეფოს მონაცემთა დაცვის საზედამხედველო ორგანომ გენერირებადი ხელოვნური ინტელექტის გამოყენებისთვის საჭირო წესების შემუშავების მესამე ეტაპი დაიწყო



გაერთიანებული სამეფოს მონაცემთა დაცვის საზედამხედველო ორგანომ გენერირებადი ხელოვნური ინტელექტის გამოყენების შესახებ წესების შესამუშავებლად, საჯარო კონსულტაციები და სამუშაო შეხვედრები დაიწყო. აღნიშნული პროცესი რამდენიმე ეტაპს მოიცავს. დაგეგმილი კონსულტაციების მიზანია პერსონალურ მონაცემთა დაცვის სიზუსტის პრინციპთან, მონაცემთა დამუშავების ფორმასა და საფუძვლებთან მიმართებით ხელოვნური ინტელექტის გამოყენების შესწავლა.

საზედამხედველო ორგანოს ოფიციალურ განცხადებაში აღნიშნულია, რომ ხელოვნური ინტელექტის მეშვეობით მონაცემთა დამუშავების სიზუსტის პრინციპის გაუთვალისწინებლობამ, შეიძლება ყალბი, უკანონო და მონაცემთა სუბიექტის რეპუტაციის შემლახველი ინფორმაციის გავრცელება გამოიწვიოს. საკითხის უკეთ შესასწავლად შესაბამისი სამუშაო ჯგუფი მსოფლიოში წამყვან ტექნოლოგიურ ორგანიზაციებთან არაერთი სისტემატური ხასიათის შეხვედრის ორგანიზებას გეგმავს.
გენერირებადი ხელოვნური ინტელექტის გამოყენების მიზნით, სათანადო წესების შემუშავებისთვის მოსაზრებების მიღება მიმდინარე წლის 10 მაისამდეა შესაძლებელი. ამ პერიოდში გაიმართება სამუშაო შეხვედრები, რომლებშიც მონაწილეობის მიღება მონაცემთა სუბიექტებს, მონაცემთა დამუშავებისთვის პასუხისმგებელ და უფლებამოსილ პირებს, დარგის სპეციალისტებსა და დაინტერესებულ პირებს შეეძლებათ. დღესდღეობით, საზედამხედველო ორგანოს შესწავლილი აქვს მონაცემთა დამუშავების მიზნის შეზღუდვის პრინციპის მოქმედება გენერირებადი ხელოვნური ინტელექტის შექმნისას. მიმდინარე წლის ზაფხულში დაგეგმილი კონსულტაციები მონაცემთა დამუშავების შესახებ მონაცემთა სუბიექტის მიერ ინფორმაციის მიღების უფლებას დაეთმობა.

აღსანიშნავია, რომ თანამედროვე ტენდენციების გათვალისწინებით, საქართველოს პერსონალურ მონაცემთა დაცვის სამსახური აქტიურად შეისწავლის ევროკავშირის „ხელოვნური ინტელექტის აქტს“.[1] ასევე, ხელოვნური ინტელექტის გამოყენებით პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებულ სხვადასხვა საკითხებს. ამასთანავე, აღსანიშნავია, რომ მიმდინარე წლის 19 აპრილს სამსახურის წარმომადგენლებმა შეხვედრა გამართეს საქართველოს ხელოვნური ინტელექტის ასოციაციის წევრებთან, რომლის ფარგლებშიც განხილულ იქნა საქართველოს პერსონალურ მონაცემთა დაცვის სამართლის საკანონმდებლო ცვლილებების გავლენა ტექნოლოგიების სფეროზე.

წყარო:
https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/04/information-commissioner-s-office-seeks-views-on-accuracy-of-generative-ai-models/

საფრანგეთის მონაცემთა დაცვის საზედამხედველო ორგანო (“CNIL”) მოხუცთა თავშესაფრებში ვიდეომეთვალყურეობის შესახებ რეკომენდაცია გამოაქვეყნა

2024 წლის 2 მაისს, საფრანგეთის მონაცემთა დაცვის საზედამხედველო ორგანომ (“CNIL”) გამოაქვეყნა რეკომენდაცია მოხუცთა თავშესაფრებში ვიდეოთვალთვალის განხორციელების შესახებ.[1] ვიდეომეთვალყურეობის სისტემების დამონტაჟება შესაძლებელია იმ შემთხვევაში, როდესაც არსებობს დასაბუთებული ეჭვი მოხუცთა თავშესაფრის ბენეფიციარების მიმართ არასათანადო მოპყრობის შესახებ. რეკომენდაციაში განმარტებულია ის პირობები, რომლებსაც უნდა აკმაყოფილებდეს ვიდეომონიტორინგის მეშვეობით პერსონალურ მონაცემთა დამუშავების პროცესი. მიზანშეწონილია, რომ სამეთვალყურეო სისტემების დამონტაჟებამდე, მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირებმა:

- დროთა განმავლობაში შეზღუდონ სისტემის აქტივაცია;
- ბენეფიციართა ახლობლების ვიზიტის განმავლობაში განახორციელონ ვიდეოკამერების დეაქტივაცია (გარდა იმ შემთხვევისა, როდესაც არსებობს არასათანადო მოპყრობის დასაბუთებული ეჭვი);
- განსაზღვრონ ვიდეოსათვალთვალო მოწყობილობის დამონტაჟების მიზანი და შეიმუშაონ გამოყენების პირობების შიდა რეგულაცია;
- ვიდეოსათვალთვალო მოწყობილობების დამონტაჟების შესახებ აცნობონ თანამშრომლებს;
- მოიპოვონ ბენეფიციართა თანხმობა;
- უზრუნველყონ ვიდეოგამოსახულების გაბუნდოვანება ისეთი სივრცის მეთვალყურეობისას, სადაც სუბიექტს პირადი ცხოვრების დაცულობის გონივრული მოლოდინი აქვს;
- უზრუნველყონ აღნიშნული სისტემების მართვასა და დანერგვაზე პასუხისმგებელი პერსონალის ცნობიერების ამაღლება და გადამზადება.

შემუშავებულ რეკომენდაციაში საფრანგეთის მონაცემთა დაცვის საზედამხედველო ორგანომ (“CNIL”) აღნიშნა, რომ სავალდებულოა მონაცემთა დაცვის ზეგავლენის შეფასება (“Data Protection Impact Assessment”)[2], როდესაც შესაძლებელია, პერსონალური მონაცემების დამუშავებამ გამოიწვიოს ფიზიკური პირების უფლებებისა და თავისუფლებების დარღვევის მაღალი რისკი. სარეკომენდაციო დოკუმენტში აღნიშნულია, რომ ვიდეომონიტორინგი წარმოშობს ამგვარ რისკს და, შესაბამისად, დამუშავებისთვის პასუხისმგებელ პირებს მართებთ, სათანადოდ შეაფასონ მონაცემთა დამუშავების პროცესის შესაძლო გავლენა ადამიანის ძირითად უფლებებსა და თავისუფლებებზე[3].

[1] https://www.dataguidance.com/news/france-cnil-publishes-recommendation-surveillance

[2] აღსანიშნავია, რომ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 31-ე მუხლი ითვალისწინებს დამუშავებისთვის პასუხისმგებელი პირის ვალდებულებას, წინასწარ განახორციელოს მონაცემთა დაცვაზე ზეგავლენის შეფასება, თუ მონაცემთა დამუშავებისას ახალი ტექნოლოგიების, მონაცემთა კატეგორიის, მოცულობის, მონაცემთა დამუშავების მიზნებისა და საშუალებების გათვალისწინებით, მაღალი ალბათობით იქმნება ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის საფრთხე.

[3] ასევე, პერსონალურ მონაცემთა დაცვის სამსახურის რეკომენდაციები ვიდეომონიტორინგის და აუდიომონიტორინგის განხორციელების თაობაზე, იხ. ბმულზე.

ფინეთის მონაცემთა დაცვის საზედამხედველო ორგანომ მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი მონაცემთა განუსაზღვრელი ვადით შენახვისთვის დააჯარიმა

ფინეთის მონაცემთა დაცვის საზედამხედველო ორგანომ მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი მონაცემთა განუსაზღვრელი ვადით შენახვისთვის 856 000 ევროს ოდენობით დააჯარიმა.[1]

საქმის ფაქტობრივი გარემოებების თანახმად, საცალო ვაჭრობის ონლაინ კომპანია (შემდგომ - დამუშავებისთვის პასუხისმგებელი პირი) განუსაზღვრელი ვადით ინახავდა მომხმარებელთა პერსონალურ მონაცემებს. კერძოდ, მომსახურების მისაღებად მომხმარებელი რეგისტრირდებოდა კომპანიის ვებგვერდზე და ქმნიდა ანგარიშს, რომლის გარეშე შეუძლებელი იყო შესაბამისი მომსახურების მიღება.[2] მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს არ ჰქონდა განსაზღვრული მონაცემების შენახვის ვადა და არც ვებგვერდზე რეგისტრაციის ეტაპზე იყო აღნიშნული რაიმე სახის მითითება. დამუშავებისთვის პასუხისმგებელი პირის განმარტებით, მომხმარებელს ნებისმიერ დროს შეეძლო ანგარიშის გაუქმება, თუმცა თუკი კვლავ აპირებდა კომპანიის მომსახურებით სარგებლობას, აქტიური ანგარიშის საფუძველზე მისი მონაცემები განუსაზღვრელი ვადით ინახებოდა.

საზედამხედველო ორგანომ აღნიშნა, რომ აქტიური ანგარიშის მქონე მომხმარებლის ინფორმაციის მუდმივად შენახვა არღვევს მონაცემთა სუბიექტის უფლებებს. ამასთანავე, სავალდებულო რეგისტრაცია მომეტებულ პასუხისმგებლობას აკისრებს მომხმარებელს, რომ მრავალჯერადი მომსახურების მისაღებად შექმნას ინდივიდუალური, თუმცა ავტომატური დამუშავებისთვის საჭირო მუდმივი ანგარიში.

საზედამხედველო ორგანოს აღნიშნული გადაწყვეტილება გამომდინარეობს ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მე-5 მუხლის პირველი პუნქტიდან, რომლის თანახმად, პერსონალური მონაცემი უნდა იყოს შენახული ისეთი ფორმით, რომელიც იძლევა მონაცემთა სუბიექტების იდენტიფიცირების შესაძლებლობას არაუმეტეს იმ დროისა, რაც აუცილებელია მონაცემთა დამუშავების მიზნებისათვის და აგრეთვე, რეგულაციის 25-ე მუხლის მე-2 პუნქტიდან, რომლის მიხედვით, მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა უნდა მიიღოს იმგვარი ტექნიკური და ორგანიზაციული ღონისძიებები, რომ ავტომატურად დამუშავდეს მხოლოდ ის მონაცემი, რომელიც აუცილებელია დამუშავების კონკრეტული მიზნისთვის.[3]

ამდენად, ფინეთის საზედამხედველო ორგანომ დამუშავებისთვის პასუხისმგებელი პირი დააჯარიმა და ყურადღება გაამახვილა მომსახურების მისაღებად ვებგვერდზე მომხმარებლის რეგისტრაციის პირობებზე. კომპანიას დაევალა მონაცემების შენახვის პერიოდის განსაზღვრა და სავალდებულო რეგისტრაციის პრაქტიკის გადახედვა. აღსანიშნავია, რომ დამუშავებისთვის პასუხისმგებელმა პირმა არ გაიზიარა საზედამხედველო ორგანოს გადაწყვეტილება და გეგმავს მის გასაჩივრებას.

ესპანეთის მონაცემთა დაცვის საზედამხედველო ორგანომ (“AEPD”) კომპანია უსაფრთხოების შესაბამისი ზომების არარსებობისა და მონაცემთა უსაფრთხოების დარღვევის შესახებ დაგვიანებული შეტყობინების გამო დააჯარიმა

2024 წლის 8 მაისს, ესპანეთის მონაცემთა დაცვის საზედამხედველო ორგანომ (“AEPD”) მიიღო გადაწყვეტილება,[1] რომელიც მონაცემთა დამუშავების უსაფრთხოებისა და საზედამხედველო ორგანოსათვის მონაცემთა უსაფრთხოების დარღვევის (ინციდენტის) შესახებ შეტყობინების ვალდებულების საკითხებს შეეხება.

ფაქტობრივი გარემოებები:

მონაცემთა დაცვის საზედამხედველო ორგანოს 2023 წლის 12 მაისს გაეგზავნა შეტყობინება მონაცემთა უსაფრთხოების დარღვევის (ინციდენტის) თაობაზე, რომელიც 2023 წლის 20 აპრილს იქნა აღმოჩენილი. მონაცემთა უსაფრთხოების დარღვევაში მოიაზრებოდა საზიანო პროგრამული უზრუნველყოფა, რომელიც შექმნილია კომპიუტერულ სისტემაზე წვდომის დაბლოკვის მიზნით გამოსასყიდის გადახდის პირობით (“ransomware attack”). აღსანიშნავია, რომ დარღვევამ გავლენა იქონია პერსონალური მონაცემების ხელმისაწვდომობასა და კონფიდენციალობაზე, მათ შორის, საკონტაქტო ინფორმაციაზე, მაიდენტიფიცირებელ მონაცემებსა და პაციენტთა ჯანმრთელობასთან დაკავშირებულ მონაცემებზე.

მონაცემთა დაცვის საზედამხედველო ორგანოს დასკვნები:

საკითხის შესწავლის შედეგად “AEPD”-მ დაადგინა, რომ კომპანიას არ ჰქონდა დანერგილი “GDPR”-ის 32-ე მუხლით გათვალისწინებული მონაცემთა უსაფრთხოების სათანადო მექანიზმები. ამასთანავე, კომპიუტერულ პროგრამებზე არ იყო დამონტაჟებული საკმარისად ძლიერი ანტივირუსი. კერძოდ, კომპანიის განმარტებით, განხორციელდა მონაცემთა დაცვაზე ზეგავლენის შეფასება, რომელიც მოიაზრებდა რისკის შესამცირებლად განსახორციელებელ რიგ ღონისძიებებს. თუმცა აღნიშნული ფაქტი კომპანიამ ვერ დაადასტურა.

ესპანეთის მონაცემთა დაცვის საზედამხედველო ორგანომ აღნიშნა, რომ კომპანიამ ვერ დააკმაყოფილა “GDPR”-ის 33-ე მუხლით განსაზღვრული 72-საათიანი ვადა საზედამხედველო ორგანოსთვის მონაცემთა უსაფრთხოების დარღვევის შეტყობინებისთვის. შეტყობინება განხორციელდა ინციდენტის აღმოჩენიდან 22 დღეში, რასთან დაკავშირებითაც კომპანიამ ზემოხსენებული ვადის დარღვევა ვერ დაასაბუთა.
საქმის ფაქტობრივი გარემოების შეფასების შედეგად, მონაცემთა დამუშავების სათანადო უსაფრთხოების უზრუნველყოფისა და საზედამხედველო ორგანოსათვის ინციდენტის თაობაზე შეტყობინების ვალდებულებების დარღვევის გამო, ესპანეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ დაადგინა კომპანიის მიერ “GDPR”-ის 32-ე და 33-ე მუხლების დარღვევა. შედეგად, კომპანიას დაეკისრა ჯარიმა 20 000 ევროს ოდენობით.

[1] Data Guidance, Spain: AEPD fines Dentalcuadros €20,000 for lack of security measures and delayed breach notification, <https://www.dataguidance.com/news/spain-aepd-fines-dentalcuadros-20000-lack-security>.

გაერთიანებული სამეფოს მონაცემთა დაცვის საზედამხედველო ორგანომ (“ICO”) ჯანდაცვის სფეროში პერსონალური მონაცემების დამუშავებისას გამჭვირვალობის უზრუნველყოფის თაობაზე სახელმძღვანელო გამოაქვეყნა

2024 წლის 15 აპრილს, გაერთიანებული სამეფოს მონაცემთა დაცვის საზედამხედველო ორგანომ (“ICO”) ჯანდაცვის სექტორში პერსონალურ მონაცემთა დამუშავების შესახებ სახელმძღვანელო გამოაქვეყნა,[1] რომლის ძირითადი მიზანი გამჭვირვალობის უზრუნველყოფაა. იგი განკუთვნილია იმ ორგანიზაციებისთვის, რომლების ჯანდაცვის სფეროში პერსონალურ მონაცემებს ამუშავებენ. სახელმძღვანელო შედგება შემდეგი ძირითადი თავებისგან: გამჭვირვალობის მნიშვნელობა; გამჭვირვალობის უზრუნველყოფა; გამჭვირვალობისა და პირადი ცხოვრების ხელშეუხებლობის თაობაზე ინფორმაციის მიწოდება; გამჭვირვალობის შეფასება.
სახელმძღვანელოში აღნიშნულია, რომ ჯანდაცვის სექტორში მუდმივად მუშავდება ფიზიკური პირის ჯანმრთელობასა და მის პირად ცხოვრებასთან დაკავშირებული მონაცემები. აღნიშნული ინფორმაცია ჯანდაცვის მომსახურების მიღების მიზნით, მონაცემთა სუბიექტის მიერ გაიცემა. გასათვალისწინებელია, რომ ამგვარი ინფორმაცია წარმოადგენს განსაკუთრებული კატეგორიის პერსონალურ მონაცემს, რომელიც თავისი ბუნებით არის სენსიტიური ხასიათის და საჭიროებს გაძლიერებულ დაცვას.

გაერთიანებული სამეფოს კანონმდებლობის თანახმად, გამჭვირვალობა ერთ-ერთ ძირითად პრინციპს წარმოადგენს. ამასთან, აღიარებულია განსაკუთრებული კატეგორიის პერსონალური მონაცემების დაცვის მნიშვნელობა. სახელმძღვანელოზე დაყრდნობით, ამგვარი მონაცემების დასაცავად აუცილებელია დამატებითი საზედამხედველო მექანიზმის შემუშავება, რათა მონაცემთა სუბიექტს ჰქონდეს ნდობა ჯანდაცვის სფეროს წარმომადგენლის მიმართ საკუთარი პერსონალური მონაცემების გაზიარებისას.

სახელმძღვანელოში განხილულია პოტენციური საფრთხეები ინდივიდთა მონაცემების დამუშავების პროცესში. კერძოდ, არსებობს მონაცემთა სუბიექტების მიმართ ფიზიკური, მატერიალური და არამატერიალური ზიანის მიდგომის რისკი. ამდენად აუცილებელია, მონაცემთა სუბიექტებს მიეწოდოთ დეტალური ინფორმაცია მათი პერსონალური მონაცემების გამოყენების ფარგლებთან დაკავშირებით, მათ შორის, პირადი ინფორმაციის დამუშავების მიზნის შესახებ.
სახელმძღვანელოში, ასევე, წარმოდგენილია პრაქტიკული მაგალითები და ჯანდაცვის სექტორში პერსონალური მონაცემების დამუშავებისას გამჭვირვალობის უზრუნველსაყოფად გასათვალისწინებელი პუნქტები (“Checklist”).

[1] ICO (Information Commissioner’s Office), Transparency in health and social care, 15 April 2024, <https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/transparency-in-health-and-social-care-1-0.pdf>.

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

ადამიანის უფლებათა ევროპულმა სასამართლომ სამართალდამცავი ორგანოების მიერ ელექტრონულ საკომუნიკაციო სისტემაზე უსაფუძვლო და განუსაზღვრელი წვდომის დაუშვებლობის შესახებ გადაწყვეტილება მიიღო

2024 წლის 13 თებერვალს, ადამიანის უფლებათა ევროპულმა სასამართლომ საქმეზე Podchasov v. Russia გადაწყვეტილება მიიღო,[1] რომელიც სამართალდამცავი ორგანოების მიერ ელექტრონულ საკომუნიკაციო სისტემებზე განუსაზღვრელი ფარგლებითა და ვადით წვდომის საკითხს შეეხება, კერძოდ, მიმოწერათა „სუსტი დაშიფვრის სისტემისა“ (“encryption mechanism”) და მათ შინაარსზე ხელმისაწვდომობის საკითხს.

ფაქტობრივი გარემოებები:
რუსეთის ფედერაციის სისხლის სამართლის საპროცესო კოდექსისა და ოპერატიულ-სამძებრო საქმიანობის აქტის საფუძველზე, ელექტრონული კომუნიკაციის კომპანიებს დაევალათ საკომუნიკაციო მონაცემების ერთი წლის ვადით, ხოლო მათი შინაარსის — ექვსი თვის განმავლობაში შენახვა. აღნიშნული მონაცემი, მათ შორის ნებისმიერი ისეთი ინფორმაცია, რომელიც სამართალდამცავ ორგანოებს კომუნიკაციების გაშიფვრაში დაეხმარებოდათ, ელექტრონული კომუნიკაციის კომპანიებს მოთხოვნისთანავე უნდა წარედგინათ.
საქმის ფაქტობრივი გარემოებების თანახმად, რუსეთის სახელმწიფო უსაფრთხოების ფედერალურმა სამსახურმა ელექტრონული კომუნიკაციის კომპანია “Telegram”-ს მოსთხოვა, წარედგინა სისტემური ინფორმაცია, რომელიც სამსახურს ექვსი მობილური ნომრის კომუნიკაციის გაშიფვრაში დაეხმარებოდა. აღსანიშნავია, რომ მობილური ნომრების მომხმარებლები, შეტყობინებათა დაშიფვრის მიზნით, პლატფორმა “Telegram”-ის „საიდუმლო მიმოწერის“ ფუნქციას იყენებდნენ.

მომჩივნის მოთხოვნა:
მომჩივანი აცხადებდა, რომ სამართალდამცავი ორგანოების მიერ ელექტრონულ საკომუნიკაციო სისტემაზე განუსაზღვრელი ფარგლებითა და ვადით წვდომა ეწინააღმდეგებოდა ადამიანის უფლებათა ევროპული კონვენციის მე-8 მუხლს.

ადამიანის უფლებათა ევროპული სასამართლოს შეფასება:
ევროპულმა სასამართლომ ყურადღება გაამახვილა ციფრულ ეპოქაში ელექტრონული კომუნიკაციების კონფიდენციალობის უზრუნველყოფის მექანიზმებზე, მათ შორის, მიმოწერის დაშიფვრის ღონისძიებებზე, რაც ხელს უწყობს სხვა ძირითადი უფლებით სარგებლობას. კომუნიკაციის დაშიფვრა მომხმარებლებს საშუალებას აძლევს, დაიცვან საკუთარი მონაცემები და აირიდონ კონფიდენციალური ინფორმაციის გამჟღავნება. სტრასბურგის სასამართლომ დაადგინა, რომ ელექტრონულ საკომუნიკაციო სისტემაში დაცული მონაცემების გაშიფვრის მოთხოვნა იყო არაპროპორციული, რამდენადაც ეროვნული კანონმდებლობა არ ითვალისწინებდა შესაბამისი და სათანადო დასაბუთების ვალდებულებას.

სასამართლომ აღნიშნა, რომ პერსონალური მონაცემების დაცვას არსებითი მნიშვნელობა აქვს ინდივიდის პირადი და ოჯახური ცხოვრების პატივისცემის უფლებით სარგებლობისთვის. ეროვნული კანონმდებლობით უზრუნველყოფილი უნდა იყოს შესაბამისი გარანტიები, რათა თავიდან იქნეს არიდებული პერსონალური მონაცემების კონვენციის მე-8 მუხლთან შეუსაბამოდ დამუშავება. ამგვარ ღონისძიებათა არსებობა მნიშვნელოვანია პერსონალური მონაცემების ავტომატური დამუშავების პროცესში — განსაკუთრებით კი მაშინ, როდესაც მონაცემები სამართალდამცავი მიზნებისთვის გამოიყენება. სასამართლომ განმარტა, რომ თანამედროვე ტექნოლოგიების დაბალანსებული გამოყენების გარეშე სამართალდამცავი მიზნებისათვის კონვენციის მე-8 მუხლით დაცულ სფეროში ჩარევა, არაპროპორციულ ზომას წარმოადგენს. შესაბამისად, პერსონალური მონაცემების დამუშავების კონტექსტში აუცილებელია, არსებობდეს მკაფიო და დეტალური წესები მონაცემთა შენახვის, გამოყენებისა და მათზე წვდომის შესახებ. ხოლო მონაცემთა შენახვის ვადა უნდა განისაზღვროს შეგროვების კანონიერი მიზნის პროპორციულად.

საქმის ფაქტობრივი გარემოებების შეფასების საფუძველზე, ადამიანის უფლებათა ევროპულმა სასამართლომ აღნიშნა, რომ სისტემაში არსებული ყველა მონაცემისა და მეტამონაცემის ხანგრძლივი ვადით შენახვა გავლენას ახდენდა ინტერნეტ- კომუნიკაციების ყველა მომხმარებელზე, მიუხედავად იმისა, არსებობდა თუ არა რაიმე ეჭვი დანაშაულებრივ ქმედებებში პირის მონაწილეობის შესახებ. შესაბამისად, სასამართლომ დაადგინა, რომ მონაცემთა შენახვისა და ხელმისაწვდომობის მოთხოვნა არღვევდა მონაცემთა კონფიდენციალობას, აგრეთვე, არ ითვალისწინებდა მონაცემთა სუბიექტის უფლების დაცვის სათანადო გარანტიებს.
ზემოაღნიშნულიდან გამომდინარე, სასამართლომ დაადგინა, რომ ეროვნული კანონმდებლობა, რომელიც ითვალისწინების ყველა ინტერნეტ-მომხმარებლის კომუნიკაციის შენახვას, ასევე, ელექტრონულ საკომუნიკაციო სისტემაზე უსაფრთხოების სამსახურის პირდაპირ წვდომას, მონაცემთა დაცვის ადეკვატური გარანტიების არსებობის გარეშე, ვერ იქნება მიჩნეული, როგორც აუცილებელი დემოკრატიულ საზოგადოებაში. შესაბამისად, სასამართლომ დაადგინა ადამიანის უფლებათა ევროპული კონვენციის მე-8 მუხლის დარღვევა.

[1] Case of Podchasov v. Russia, Application no. 33696/19, 13 February 2024, <https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-230854%22]}> [15.04.2024].

ჰონგ-კონგის მონაცემთა დაცვის საზედამხედველო ორგანომ (“PCPD”) პროექტ “Worldcoin”-ის ფარგლებში პერსონალურ მონაცემთა დაცვის კანონმდებლობის დარღვევა დაადგინა

2024 წლის 22 მაისს, ჰონგ-კონგის მონაცემთა დაცვის საზედამხედველო ორგანომ (“PCPD”) გამოაქვეყნა გადაწყვეტილება,[1] რომელიც პროექტ “Worldcoin”-ის[2] ფარგლებში პერსონალური მონაცემების დამუშავების კანონიერების შესწავლას შეეხება.

საზედამხედველო ორგანომ ინსპექტირება 2024 წლის იანვარში დაიწყო, რათა დაედგინა ჰონგ-კონგში განხორციელებული პროექტ “Worldcoin”-ის ფარგლებში მონაცემთა დამუშავების ოპერაციების შესაბამისობა პერსონალურ მონაცემთა დაცვის კანონმდებლობასთან. ადგილზე შემოწმებები საზედამხედველო ორგანომ განახორციელა იმ ორგანიზაციებში, რომლებიც “Worldcoin”-ის პროექტში იყვნენ ჩართულნი. შესწავლილი ფაქტობრივი გარემოებების საფუძველზე დადგინდა, რომ პროექტ “Worldcoin”-ის ფარგლებში მუშავდებოდა მონაცემთა სუბიექტების სახისა და თვალის ფერადი გარსის ფოტოსურათები, მათი იდენტიფიცირების მიზნით. აღნიშნული კი წარმოადგენდა “Worldcoin”-ის მონეტისა და კრიპტოვალუტის მიღების წინაპირობას. “Worldcoin”-ის პროექტის მონაწილე ერთ-ერთმა კომპანიამ, როგორც მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა, დაადასტურა, რომ მონაცემთა სუბიექტების ვერიფიკაციისთვის, სისტემაში 8 302 ფიზიკური პირის სახისა და თვალის გარსის დასკანერებული ვერსია ინახებოდა.

მონაცემთა დამუშავების კანონიერების შესწავლის შედეგად, “PCPD”-მ აღნიშნა, რომ დაირღვა მონაცემთა დაცვის ძირითადი პრინციპები, ასევე, მონაცემთა სუბიექტის წვდომისა და გასწორების უფლებები. კერძოდ, საზედამხედველო ორგანომ დაადგინა, რომ:

- პროექტ “Worldcoin”-ის ფარგლებში არ არსებობდა სახისა და თვალის ფერადი გარსის სურათების შეგროვების საჭიროება, რაც მონაცემთა გადაჭარბებული მოცულობით დამუშავებას წარმოადგენდა;
- პროექტის ფარგლებში პერსონალური მონაცემების დამუშავების თაობაზე „კონფიდენციალობის შესახებ“ განაცხადი მონაცემთა სუბიექტებისათვის არ იყო ჩინურ ენაზე ხელმისაწვდომი ისევე, როგორც „ბიომეტრიულ მონაცემთა დამუშავების შესახებ“ თანხმობის ფორმა. ამასთან, მონაცემთა დამუშავების მიზანი არ იყო მკაფიოდ განმარტებული და მონაცემთა სუბიექტებს არ ჰქონდათ ინფორმაცია ბიომეტრიული მონაცემების დამუშავებასთან დაკავშირებული შესაძლო რისკების თაობაზე;
- პერსონალური მონაცემების შეგროვებამდე, მონაცემთა სუბიექტები არ იყვნენ სრულად ინფორმირებულნი მათი პერსონალური მონაცემების დამუშავების მიზნის, მესამე პირებისათვის მონაცემთა შესაძლო გადაცემის, მათი უფლებების, მათ შორის, პერსონალურ მონაცემებზე წვდომისა და გასწორების შესახებ;
- “Worldcoin”-ის ფარგლებში პერსონალური მონაცემების 10 წლის ვადით შენახვა არ იყოს დამუშავების მიზნის პროპორციული;

- პერსონალურ მონაცემთა დაცვის პოლიტიკა და პრაქტიკა არ იყო მონაცემთა სუბიექტებისათვის საკმარისად გამჭვირვალე და ჩინურ ენაზე ხელმისაწვდომი, რის გამოც დაინტერესებული პირები მოკლებულნი იყვნენ შესაძლებლობას, მიეღოთ სრულყოფილი ინფორმაცია პროექტის შესახებ.
-

აღნიშნულიდან გამომდინარე, ჰონგ-კონგის მონაცემთა დაცვის საზედამხედველო ორგანომ დაავალა მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს, რომ ჰონგ-კონგში განხორციელებული პროექტ “Worldcoin”-ის ფარგლებში შეეწყვიტა მონაცემთა სუბიექტების სახისა და თვალის ფერადი გარსის სურათების დამუშავება.

„გერმანიის მონაცემთა დაცვის დამოუკიდებელ ორგანოთა კონფერენციამ“ (“DSK”) პაციენტის მონაცემთა დაცვის შესახებ რეზოლუცია გამოაქვეყნა

2024 წლის 15 მაისს, გერმანიის მონაცემთა დაცვის კონფერენციამ (“DSK”) გამოაქვეყნა რეზოლუცია, რომელიც პაციენტების მონაცემთა დაცვის გარანტიებს შეეხება.[1] კონფერენციაზე აღინიშნა, რომ სამედიცინო დაწესებულების ფუნქციონირების შეწყვეტისას დამუშავებული მონაცემების შენახვისა და წაშლის წესების არარსებობა წარმოადგენს ერთგვარ გამოწვევას.
საკითხის გადასაწყვეტად, გერმანიის მონაცემთა დაცვის კონფერენციაზე განხილულ იქნა რამდენიმე რეკომენდაცია:

- ჩრდილოეთ რაინ-ვესტფალიასა და ჰესენში არსებული რეგულაციების თანახმად, საავადმყოფოებმა უნდა შეიმუშაონ სამოქმედო გეგმა იმ შემთხვევებისთვის, თუ ისინი გადახდისუუნარობის ან მოულოდნელი ლიკვიდაციის საშიშროების წინაშე აღმოჩნდებიან და წარუდგინონ აღნიშნული დოკუმენტი უფლებამოსილ საზედამხედველო ორგანოს;
- სახელმწიფომ, საჭიროების შემთხვევაში, უნდა მოიძიოს დაფინანსების სხვადასხვა შესაძლებლობა, რათა უზრუნველყოფილი იყოს გადაუდებელ სიტუაციებში პაციენტის პერსონალურ მონაცემის შენახვა, ხოლო სარეზერვო ასლების უზრუნველსაყოფად დაფინანსება გაგრძელდეს გარდამავალი პერიოდის განმავლობაში;
- დღესდღეობით სამედიცინო დაწესებულების ლიკვიდაციის შემთხვევაში, პერსონალურ მონაცემთა შენახვის, წაშლისა და გადაცემის საკითხები კანონმდებლობით ზუსტად არ არის მოწესრიგებული. ამდენად, მნიშვნელოვანია, რომ საავადმყოფოს მენეჯმენტმა შეიმუშავოს და უზრუნველყოს მონაცემთა სუბიექტების სამედიცინო ჩანაწერების მოკლევადიანი უსაფრთხო შენახვის მექანიზმები.

ჯანდაცვის მინისტრთა კონფერენცია აღნიშნულ საკითხს მომავალ შეხვედრაზე განიხილავს და შესაბამის გადაწყვეტილებას მიიღებს, რათა უზრუნველყოფილი იყოს ჯანდაცვის სფეროში მონაცემთა სუბიექტების განსაკუთრებული კატეგორიის მონაცემების დაცვის სათანადო გარანტიები.

[1] “DSK” წარმოადგენს გერმანიის ფედერალურ მიწათა დამოუკიდებელი პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოების ყოველწლიურ კონფერენციას <https://www.dataguidance.com/news/germany-dsk-publishes-resolution-patient-data>, [28.05.2024].

(+ 995 32) 242
1000 o ce@pdps.ge
w w w.pdps.ge