მსოფლიო პრაქტიკა

პერსონალურ მონაცემთა დაცვის სამსახური

სიახლეები

„ევროპის მონაცემთა დაცვის ზედამხედველის“ (“EDPS”) მოსაზრება ადმინისტრაციული წარმოების ფარგლებში დამუშავებული პერსონალური მონაცემების შენახვის ვადის განსაზღვრის შესახებ

საკომუნიკაციო პლატფორმა “Telegram“-მა კონფიდენციალობის პოლიტიკა განაახლა

საბერძნეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება გამჭვირვალობისა და მონაცემთა მინიმიზაციის პრინციპების დარღვევის შესახებ

საბერძნეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ (“HDPA”) საბერძნეთის მოქალაქეებისთვის ახალი ტიპის პირადობის მოწმობის შემოღებასთან დაკავშირებით გადაწყვეტილება მიიღო.

ნოემბერი 2024

საქმის ფაქტობრივი გარემოებები:

მონაცემთა სუბიექტმა საჩივრით მიმართა საზედამხედველო ორგანოს ბიომეტრიული მონაცემების შემცველი ახალი პირადობის მოწმობების საკითხის შესახებ. აღსანიშნავია, რომ განმცხადებელმა ასევე მიმართა საბერძნეთის „მოქალაქეთა დაცვის სამინისტროს“ (“Ministry of Citizen Protection”) მონაცემთა დამუშავების კანონიერების თაობაზე, თუმცა მის მიერ დასმულ კითხვებზე პასუხები მან მიიღო. აღნიშნულის საფუძველზე საზედამხედველო ორგანომ სამინისტროს მიერ ევროკავშირის „მონაცემთა დაცვის ძირითად რეგულაციასთან“ შესაბამისობის დადგენის მიზნით, საკითხის შესწავლა დაიწყო.
სამინისტრომ განმარტა, რომ ახალი პირადობის მოწმობების დანერგვასთან დაკავშირებით არაერთი ღონისძიება განხორციელდა, რომელთა შორისაა, მონაცემთა დაცვაზე ზეგავლენის შეფასება (“DPIA”), შესაბამისი რისკების იდენტიფიცირება და ბიომეტრიულ მონაცემთა დამუშავებასთან დაკავშირებული შესაბამისი გარანტიების დანერგვა.

საზედამხედველო ორგანოს გადაწყვეტილების დასაბუთება:

საქმის ფაქტობრივი გარემოებების შესწავლის შედეგად, საზედამხედველო ორგანომ დაადგინა მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის მიერ ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მე-12 მუხლის დარღვევის ფაქტი, რადგან სამინისტრომ ვერ უზრუნველყო პერსონალურ მონაცემთა შეგროვების კანონიერების, მიზნისა და ფარგლების შესახებ განმცხადებლისა და საზოგადოების დროული ინფორმირება. აგრეთვე, დადგინდა, რომ სამინისტრო სრულად არ იცავდა “GDPR”-ის 5(1)(გ) მუხლით გათვალისწინებულ მონაცემთა მინიმიზაციის პრინციპს. საზედამხედველო ორგანომ ეჭქვეშ დააყენა დამუშავებული ბიომეტრიული მონაცემების მოცულობის შესაბამისობა დამუშავების მიზანთან, რასაც მოცემულ შემთხვევაში პირადობის მოწმობების გაცემა წარმოადგენდა.

ბიომეტრიული მონაცემების დამუშავებით გამოწვეული ადამიანის უფლებათა შელახვის მაღალი რისკის გამო, საბერძნეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ ხაზი გაუსვა მონაცემთა დაცვაზე ზეგავლენის შეფასების (“DPIA”) აუცილებლობასაც. მართალია, სამინისტრომ განახორციელა შეფასება, თუმცა მან შესაბამისი დოკუმენტით გათვალისწინებული რისკის შემცირების ღონისძიებების, ძირითად რეგულაციასთან შესაბამისობა ვერ უზრუნველყო. ამასთანავე, საზედამხედველო ორგანომ გადაწყვეტილებაში ხაზგასმით აღნიშნა ანგარიშვალდებულების პრინციპის დაცვის აუცილებლობა და სამინისტროს ვალდებულება, უზრუნველყოს მოქალაქეთა ინფორმირება მონაცემთა დამუშავების პროცესის შესახებ.

საზედამხედველო ორგანოს დასკვნები:

საბერძნეთის მონაცემთა დაცვის საზედამხედველო ორგანომ დაადგინა, რომ „მოქალაქეთა დაცვის სამინისტრომ“ დაარღვია გამჭვირვალობისა და მონაცემთა მინიმიზაციას პრინციპები. კერძოდ, “GDPR”-ით გათვალისწინებული მოთხოვების შესაბამისად, სამინისტრომ ვერ უზრუნველყო დროული რეაგირება და ვერ მიაწოდა საზოგადოებას საკმარისი ინფორმაცია განსაკუთრებული კატეგორიის მონაცემთა დამუშავებასთან დაკავშირებით. ასევე, მან არ ჩაატარა მონაცემთა დაცვაზე ზეგავლენის შეფასება მონაცემთა დამუშავების დაწყებამდე, ხოლო შემდგომში, შეფასების

განხორციელებისას არ იქნა იდენტიფიცირებული მონაცემთა დამუშავებასთან დაკავშირებული რისკები.

მიღებული გადაწყვეტილება:
საბერძნეთის საზედამხედველო ორგანომ ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მე-13 და მე-14 მუხლების დარღვევისთვის „მოქალაქეთა დაცვის სამინისტრო“ დააჯარიმა 50 000 ევროს ოდენობით, ხოლო 35-ე მუხლის პირველი პუნქტის დარღვევისთვის — 100 000 ევროს ოდენობით.

სლოვენიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება დამუშავებისთვის პასუხისმგებელი პირის მიერ დასაქმებულების უკანონო ვიდეო-აუდიომონიტორინგისა და დამუშავებული პერსონალური მონაცემების ონლაინ გავრცელების დაუშვებლობის შესახებ

ფაქტობრივი გარემოებები:

დამუშავებისთვის პასუხისმგებელმა პირმა ვიდეომოწყობილობები კომპანიის სამუშაო სივრცეებში განათავსა, რომელთა საშუალებით იგი შენობაში აკვირდებოდა დასაქმებულთა საქმიანობას და ასევე, ახორციელებდა აუდიომონიტორინგს. მიღებულ მონაცემებს ეცნობოდა არა მხოლოდ დამუშავებისთვის პასუხისმგებელი პირი, არამედ კომპანიის მენეჯერი მობილური აპლიკაციისა და ვებგვერდის გამოყენებით, რომელშიც იტვირთებოდა დამუშავებული მონაცემები. საგულისხმოა, რომ მონაცემთა სუბიექტები არ იყვნენ ინფორმირებულნი დასაქმების ადგილას ვიდეო-აუდიომონიტორინგის მიმდინარეობის შესახებ. ამასთანავე, შენობის შესასვლელში არ იყო განთავსებული შესაბამისი გამაფრთხილებელი ნიშანი. უშუალოდ შენობაში, დასაქმებულებისთვის ხელმიუწვდომელ ადგილას, განთავსებული იყო მითითება ვიდეომონიტორინგის განხორციელების შესახებ, რომელიც არ შეიცავდა დამატებით აღნიშვნას, რომ ამავდროულად მიმდინარეობდა სამუშაო სივრცის აუდიომონიტორინგი.

საქმის განხილვა საზედამხედველო ორგანოში:

შესაფასებელი მუხლები:

ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“:

·მე-5 მუხლის პირველი პუნქტის „ა“ ქვეპუნქტი — პერსონალური მონაცემები უნდა დამუშავდეს კანონიერად, სამართლიანად და გამჭვირვალედ მონაცემთა სუბიექტთან მიმართებით (კანონიერება, სამართლიანობა, გამჭვირვალობა);

·მე-6 მუხლის პირველი პუნქტის „ა“ ქვეპუნქტი — მონაცემთა დამუშავება კანონიერია მხოლოდ იმ შემთხვევაში და იმ მოცულობით, თუ მონაცემთა სუბიექტი განაცხადებს თანხმობას მისი პერსონალური მონაცემების დამუშავებაზე ერთი ან მეტი კონკრეტული მიზნისათვის;

·მე-13 მუხლის პირველი პუნქტის „ა“ ქვეპუნქტი — მონაცემთა უშუალოდ მონაცემთა სუბიექტისგან შეგროვებისას, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, აცნობოს მას დამუშავებისთვის პასუხისმგებელი პირის და მისი წარმომადგენლის (ასეთის არსებობის შემთხვევაში) ვინაობა და საკონტაქტო ინფორმაცია.

საზედამხედველო ორგანოს შეფასება:

საზედამხედველო ორგანომ განიხილა დამუშავებისთვის პასუხისმგებელი პირისა და მენეჯერის ინდივიდუალური პასუხისმგებლობის საკითხი, რის შედეგადაც გადაწყვიტა, რომ მათზე თანაბრად გაევრცელებინა პასუხისმგებლობა. დამუშავებისთვის პასუხისმგებელმა პირმა სამუშაო სივრცის უკანონო ვიდეო-აუდიომონიტორინგის განხორციელებით დაარღვია დასაქმებულთა, როგორც მონაცემთა სუბიექტების უფლებები. იქიდან გამომდინარე, რომ კომპანიამ დაარღვია ვიდეო და აუდიომონიტორინგის განხორციელების წესი, მენეჯერის მიერ პერსონალური მონაცემების შემდგომი გავრცელება ასევე დაუშვებელი იყო. დადგინდა, რომ ვიდეო-აუდიოჩაწერის ერთადერთი მიზანი იყო შენობის მთელს სივრცეში თანამშრომლების თვალთვალი და მიყურადება, რაც საზედამხედველო ორგანოს შეფასებით, არ იყო დამუშავების ლეგიტიმური საფუძველი, ხოლო ამ ფორმით მიღებული პერსონალური მონაცემების ვებგვერდზე ონლაინ განთავსება, ასევე, წარმოადგენდა სამართალდარღვევას.

მიღებული გადაწყვეტილება:

სლოვენიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ დამუშავებისთვის პასუხისმგებელი პირი, მასთან დასაქმებულების უკანონო ვიდეო- და აუდიო- მონიტორინგის განხორციელებისა და ამ ფორმით მიღებული პერსონალური მონაცემების ონლაინ გავრცელების გამო, 25 000 ევროს ოდენობით, ხოლო მენეჯერი — 1750 ევროს ოდენობით დააჯარიმა.

ევროკავშირის მართლმსაჯულების სასამართლოს გადაწყვეტილება პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს მიერ დარღვევის გამოსასწორებელი ზომების მიღების შესახებ

ევროკავშირის მართლმსაჯულების სასამართლოს გადაწყვეტილება (C 768/21) შეეხება ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ (“GDPR”) 57(1)(a)(f)-ე (საზედამხედველო ორგანოს ფუნქციები), 58(2)-ე (საზედამხედველო ორგანოს უფლებამოსილებები) და 77(1)-ე (საზედამხედველო ორგანოში საჩივრის წარდგენის უფლება) მუხლების ინტერპრეტაციას. სასამართლოს ძირითად განსახილველ საკითხს წარმოადგენდა პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს კომპეტენცია, დარღვევის გამოსასწორებელი ზომების მიღების კონტექსტში.[1]

·საქმის ფაქტობრივი გარემოებები:
ჰესენის ფედერალური მიწის კომერციული ბანკი (“Savings Bank”) არის საზოგადოებრივი ინსტიტუტი, რომლის ძირითადი ამოცანაა საბანკო და საკრედიტო ტრანზაქციების განხორციელება. 2019 წლის 15 ნოემბერს, ბანკმა “GDPR”-ის 33-ე მუხლის შესაბამისად, მონაცემთა უსაფრთხოების დარღვევის (ინციდენტის) თაობაზე ინფორმაცია წარუდგინა ჰესენის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს (“HBDI”)[2]. მონაცემთა უსაფრთხოების დარღვევა გამოიხატებოდა ბანკის თანამშრომლის მიერ ერთ-ერთი მომხმარებლის (“TR”) პერსონალურ მონაცემზე კანონიერი საფუძვლის გარეშე წვდომაში. აღსანიშნავია, რომ თავის მხრივ ბანკმა არ უზრუნველყო მომხმარებლის ინფორმირება მონაცემთა უსაფრთხოების დარღვევის თაობაზე.

მას შემდეგ, რაც მომხმარებელმა შეიტყო საკუთარ პერსონალურ მონაცემებზე უკანონო წვდომის შესახებ, 2020 წლის 27 ივლისს, “GDPR”-ის 77-ე მუხლის საფუძველზე, მან საჩივრით მიმართა მონაცემთა დაცვის საზედამხედველო ორგანოს, რომელმაც რეგულაციის 34-ე მუხლის („მონაცემთა სუბიექტისათვის მონაცემთა უსაფრთხოების დარღვევის შეტყობინება“) დარღვევაზე მიუთითა. ამავდროულად, მიუთითა, რომ დასაქმებულებს ჰქონდათ ამ მონაცემებზე წვდომის უფლება.

საჩივარში ფაქტების განხილვის შემდეგ, საზედამხედველო ორგანო გაეცნო დამუშავებისთვის პასუხისმგებელი პირის — ბანკის პოზიციას, რომლის თანახმად, მონაცემთა უსაფრთხოების დარღვევის თაობაზე მომხმარებლის ინფორმირება არ იქნა უზრუნველყოფილი იმდენად, რამდენადაც მონაცემთა დაცვის ოფიცერმა მიიჩნია, რომ არ არსებობდა მაღალი რისკი მონაცემთა სუბიექტის უფლებებისა და თავისუფლებების დაცვის თვალსაზრისით. ბანკმა დისციპლინური ზომები გაატარა დასაქმებული პირის მიმართ, რომელმაც წერილობით დაადასტურა, რომ მას არასდროს გადაუღია პერსონალური მონაცემების ასლები, ასევე, არ შეუნახავს, არ გადაუცია მესამე მხარისთვის და არც სამომავლოდ გეგმავდა მსგავსი ქმედებების განხორციელებას.

·პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება:

2020 წლის 3 სექტემბრის გადაწყვეტილებით, ჰესენის მონაცემთა დაცვის საზედამხედველო ორგანომ ბანკის მომხმარებელს აცნობა, რომ კომერციულმა ბანკმა არ დაარღვია ძირითადი რეგულაციის 34-ე მუხლი, რამდენადაც ბანკმა სწორად მიიჩნია, რომ მონაცემთა უსაფრთხოების დარღვევა არ გამოიწვევდა მაღალ რისკს მონაცემთა სუბიექტის უფლებებისა და თავისუფლებების დაცვის თვალსაზრისით. მიუხედავად იმისა, რომ დასაქმებულს ჰქონდა წვდომა მომხმარებლის პირად ინფორმაციაზე, არ არსებობდა რაიმე მტკიცებულება მონაცემების მესამე მხარის გადაცემისა ან სხვაგვარად გამოყენების შესახებ. აგრეთვე, საზედამხედველო ორგანომ მოსთხოვა ბანკს მონაცემებზე წვდომების შესახებ ინფორმაცია შეენახა 3 თვეზე მეტი ვადით. რაც შეეხება კომერციული ბანკის თანამშრომლის მიერ პერსონალურ მონაცემებზე წვდომას, საზედამხედველო ორგანომ არ გაიზიარა მომხმარებლის მოთხოვნა და აღნიშნა, რომ მონაცემებზე წვდომა შეიძლება დასაშვები იყოს, თუკი მომხმარებელი წვდომის პირობების შესახებ ინფორმირებულია. აღნიშნულიდან გამომდინარე, მონაცემებზე ყველა სახის წვდომის სისტემატური შეფასება და განხილვა არ არის აუცილებელი.

მომხმარებელმა საზედამხედველო ორგანოს გადაწყვეტილება გაასაჩივრა გერმანიის ადმინისტრაციულ სასამართლოში, საზედამხედველო ორგანოს მიერ კომერციული ბანკის წინააღმდეგ შესაბამისი ზომების მიღების მოთხოვნით.

·გერმანიის ადმინისტრაციული სასამართლოს შეფასება:
მომხმარებელმა საკუთარი პოზიციის გასამყარებლად აღნიშნა, რომ მონაცემთა დაცვის საზედამხედველო ორგანომ მისი საჩივარი “GDPR”-ის მოთხოვნების დაცვის შესაბამისად არ განიხილა. სანქციის სახით საზედამხედველო ორგანოს კომერციული ბანკისთვის ძირითადი რეგულაციის მე-5, მე-12(3), მე-15(1)(c) და 33(1)(3)-ემუხლების დარღვევის გამო უნდა დაეკისრებინა ჯარიმა. მომხმარებელმა განაცხადა, რომ საზედამხედველო ორგანოს არ ჰქონდა დისკრეციული უფლებამოსილება მოცემულ შემთხვევაში მიიღებდა თუ არა შესაბამის ზომებს, არამედ დისკრეცია უნდა გამოხატულიყო კონკრეტული ღონისძიების განსაზღვრაში.

ზემოაღნიშნულ არგუმენტებზე დაყრდნობით, ადმინისტრაციული სასამართლოს უნდა შეეფასებინა:

—როდესაც დადგინდება ძირითადი რეგულაციის დებულებათა დარღვევა, ავალდებულებს თუ არა “GDPR”-ი საზედამხედველო ორგანოს, მიიღოს შესაბამისი, გამოსასწორებელი ზომები, მაგალითად, როგორიცაა: ჯარიმის განსაზღვრა?

—გააჩნია თუ არა საზედამხედველო ორგანოს დისკრეცია, კონკრეტული გარემოებების გათვალისწინებით, თავი შეიკავოს შესაბამისი, გამოსასწორებელი ზომების მიღებისგან?
სასამართლომ პირველ საკითხთან მიმართებით, აღნიშნა, საზედამხედველო ორგანო უფლებამოსილია მონაცემთა სუბიექტის უფლების დარღვევის იდენტიფიცირების შემთხვევაში, მიიღოს გამოსასწორებელი ზომები, რომელთა მიზანია პირვანდელი მდგომარეობის აღდგენა. ამდენად, “GDPR”-ის 58(2)-ე მუხლი (საზედამხედველო ორგანოს მიერ შესაბამისი ღონისძიების გატარების უფლებამოსილება) უნდა განიმარტოს როგორც სტანდარტი, რომელიც ავალდებულებს საზედამხედველო ორგანოს, მიიღოს დარღვევის გამოსასწორებლად შესაბამისი ღონისძიება. ამდენად, როდესაც ადგილი აქვს მონაცემთა უსაფრთხოების დარღვევას, საზედამხედველო ორგანო ვალდებულია, მიიღოს შესაბამისი, გამოსასწორებელი ღონისძიებები. მისი დისკრეცია შეზღუდულია კონკრეტულ სიტუაციაში გამოსასწორებელი ზომის მოცულობის განსაზღვრის ფარგლებში.

საგულისხმოა, რომ ადმინისტრაციული სასამართლო არ იყო დარწმუნებული საკუთარი პოზიციის მართებულობაში. მაშინაც კი, როდესაც “GDPR”-ის 57(1)(f)-ე მუხლის შესაბამისად, საზედამხედველო ორგანოს გააჩნია ვალდებულება, განახორციელოს მონაცემთა სუბიექტის საჩივრის სიღრმისეული შესწავლა მას შესაძლოა, არ ევალებოდეს ყველა სიტუაციაში შესაბამისი, გამოსასწორებელი ზომების მიღება. აღნიშნულიდან გამომდინარე, ადმინისტრაციულმა სასამართლომ მიიღო გადაწყვეტილება საქმის წარმოებაში დატოვების შესახებ და მიმართა ევროკავშირის მართლმსაჯულების სასამართლოს (“CJEU”).

·გერმანიის ადმინისტრაციული სასამართლოს მიერ ევროკავშირის მართლმსაჯულების სასამართლოსთვის დასმული კითხვა:

ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ 57(1)(a)(f)-ე, 58(2)(a)(j)-ე და 77(1)-ე მუხლები უნდა იქნეს თუ არა განმარტებული იმ მნიშვნელობით, რომ როდესაც მონაცემთა დაცვის საზედამხედველო ორგანო დაადგენს მონაცემთა სუბიექტის უფლებების დარღვევას, აუცილებელია, ყველა შემთხვევაში მიიღოს გამოსასწორებელი ზომა “GDPR”-ის 58-ე მუხლის მე-2 პუნქტის შესაბამისად.

·ევროკავშირის მართლმსაჯულების სასამართლოს გადაწყვეტილება:

ევროკავშირის მართლმსაჯულების სასამართლომ აღნიშნა, რომ “GDPR”-ის 57(1)(f) მუხლის თანახმად, პერსონალურ მონაცემთა დაცვის თითოეული საზედამხედველო ორგანო ვალდებულია, საკუთარ ტერიტორიაზე განიხილოს საჩივრები რეგულაციის 77-ე მუხლის პირველი პუნქტის შესაბამისად: „თითოეული მონაცემთა სუბიექტი უფლებამოსილია, სასამართლოს ან ადმინისტრაციული ორგანოს მეშვეობით უფლებების დაცვის გარდა, საჩივრით მიმართოს საზედამხედველო ორგანოს წევრ სახელმწიფოში საკუთარი საცხოვრებელი ადგილის, სამუშაო ადგილის ან სავარაუდო დარღვევის ჩადენის ადგილის მიხედვით, თუ მონაცემთა სუბიექტი მიიჩნევს, რომ მისი მონაცემების დამუშავება ხორციელდება რეგულაციის დარღვევით.“

ამასთანავე, საზედამხედველო ორგანო, რომელსაც წარედგინა საჩივარი, ვალდებულია, აცნობოს საჩივრის წარმდგენს მისი განცხადების განხილვის მიმდინარეობისა და შედეგების შესახებ, მათ შორის, სასამართლოს მეშვეობით უფლების დაცვის/აღდგენის თაობაზე. საზედამხედველო ორგანომ საჩივარი უნდა განიხილოს სათანადო გულისხმიერებით.

სასამართლომ აღნიშნა, რომ საჩივრის განსახილველად, “GDPR”-ის 58-ე მუხლის პირველი პუნქტის შესაბამისად, საზედამხედველო ორგანოს გააჩნია მნიშვნელოვანი საგამოძიებო უფლებამოსილებები. საკითხის შესწავლის შემდეგ, თუ საზედამხედველო ორგანო დაადგენს რეგულაციის დარღვევას, მისი ვალდებულებაა, იმოქმედოს გამოვლენილ ნაკლოვანებათა გამოსწორების მიზნით. საზედამხედველო ორგანოს მიერ მიღებული ნებისმიერი ზომა უნდა იყოს შესაბამისი, აუცილებელი და პროპორციული რეგულაციასთან შესაბამისობის უზრუნველყოფის თვალსაზრისით. ამასთან, უნდა იქნას გათვალისწინებული თითოეული განსახილველი საქმის სპეციფიკა. ძირითადი რეგულაციის 58-ე მუხლის მე-2 პუნქტით გათვალისწინებულია სხვადასხვა გამოსასწორებელი ზომა, რომლის მიღების უფლებამოსილებაც გააჩნია საზედამხედველო ორგანოს.

ამდენად, *“GDPR”*-ის *58*-ე მუხლის მე-*2* პუნქტის გათვალისწინებით, საზედამხედველო ორგანოს, მათ შორის, შეუძლია: დამუშავებისთვის პასუხისმგებელი პირის მიმართ შენიშვნის გამოცხადება, როდესაც მონაცემთა დამუშავების ოპერაციები ეწინააღმდეგება ძირითად რეგულაციას; დამუშავებისთვის პასუხისმგებელ ან დამუშავებაზე უფლებამოსილ პირს მოსთხოვოს, იმოქმედონ მონაცემთა სუბიექტის მოთხოვნის შესაბამისად, რათა უზრუნველყოფილ იქნას რეგულაციით განსაზღვრული უფლებების რეალიზება; დამუშავებისთვის პასუხისმგებელ ან დამუშავებაზე უფლებამოსილ პირს მოსთხოვოს დამუშავების პროცესის რეგულაციასთან შესაბამისობაში მოყვანა, საჭიროების შემთხვევაში, სათანადო ფორმითა და შესაბამისი ვადის დაწესებით. ამასთან, საზედამხედველო ორგანო უფლებამოსილია, თითოეული საქმის გარემოების გათვალისწინებით, სანქციის სახით გამოიყენოს ადმინისტრაციული ჯარიმა. ამდენად, საჩივრის განხილვის პროცედურა წარმოადგენს ეფექტიან მექანიზმს მონაცემთა სუბიექტების უფლებებისა და თავისუფლებების დაცვის თვალსაზრისით.

მართლმსაჯულების სასამართლომ ყურადღება გაამახვილა ჰესენის მონაცემთა დაცვის საზედამხედველო ორგანოს მიერ მიღებულ გადაწყვეტილებაზე, რომლითაც დადასტურდა კომერციულ ბანკში მონაცემთა უსაფრთხოების დარღვევა. აღნიშნული მართალია, მოიაზრებდა ბანკში დასაქმებულ პირთა მიერ მომხმარებლის პერსონალური მონაცემების ხელმისაწვდომობას, თუმცა საზედამხედველო ორგანოს შეფასებით, *“GDPR”*-ის *58*-ე მუხლის მე-*2* პუნქტის მიხედვით, არ არსებობდა კომერციული ბანკის წინააღმდეგ რაიმე სახის გამოსასწორებელი ზომების მიღების აუცილებლობა. აღნიშნულთან დაკავშირებით ევროკავშირის მართლმსაჯულების სასამართლომ აღნიშნა, რომ ძირითადი რეგულაცია საზედამხედველო ორგანოს გამოვლენილი ნაკლოვანების გამოსწორების ფარგლებში ანიჭებს დისკრეციას იმდენად, რამდენადაც ძირითადი რეგულაციის *58*-ე მუხლის მე-*2* პუნქტით გათვალისწინებულია სხვადასხვა გამოსასწორებელი ზომა, რომლის მიღების უფლებამოსილებაც გააჩნია საზედამხედველო ორგანოს. შესაბამისად, მისი პრეროგატივაა განსაზღვროს, თუ რომელი ღონისძიება იქნება შესაბამისი და აუცილებელი კონკრეტული საქმის სპეციფიკის გათვალისწინებით. თუმცა, აღნიშნული დისკრეციული უფლებამოსილება შეზღუდულია პერსონალური მონაცემების თანმიმდევრული და ეფექტიანი დაცვის საჭიროებით.

რაც შეეხება ადმინისტრაციულ ჯარიმას, იგი უნდა იქნას დაწესებული თითოეული ინდივიდუალური შემთხვევიდან გამომდინარე *(“GDPR”*-ის *83*-ე მუხლის მე-*2* პუნქტი*)*, რეგულაციით დადგენილ ზომებთან ერთად ან მათ სანაცვლოდ. ასევე, *83*-ე მუხლის მე-*2* პუნქტით დაზუსტებულია, რომ ადმინისტრაციული ჯარიმის დაწესებისას, მონაცემთა დამუშავების მიზნის და მოცულობის გათვალისწინებით უნდა განისაზღვროს დარღვევის სახე, სიმძიმე და ხანგძლივობა ისევე, როგორც დაზარალებული მონაცემთა სუბიექტების რაოდენობა და ზიანი. შესაბამისად, ევროკავშირის კანონმდებლობის განსაზღვრული სანქციის სისტემა საშუალებას აძლევს საზედამხედველო ორგანოებს თითოეული ინდივიდუალური შემთხვევის შესაბამისად განსაზღვრონ შესაბამისი სახდელის სახე.

ამდენად, ძირითადი რეგულაციის *58(2)*-ე და *83*-ე მუხლები პერსონალურ მონაცემთა უსაფრთხოების დარღვევის შემთხვევაში, საზედამხედველო ორგანოს ყოველთვის არ ავალდებულებს გამოსასწორებელი ზომების მიღებას, კერძოდ, ადმინისტრაციული ჯარიმის დაწესებას. მისი ვალდებულებაა, რომ გამოვლენილი ნაკლოვანების გამოსასწორებლად იმოქმედოს სათანადოდ. მოცემულ შემთხვევაში, როგორც გენერალური ადვოკატის მოსაზრებაშია წარმოდგენილი, მომჩივანს, რომლის უფლებებიც იქნა დარღვეული, არ გააჩნია უფლებამოსილება, მოსთხოვოს საზედამხედველო ორგანოს, რომ დამუშავებისთვის პასუხისმგებელ პირს დააკისროს ჯარიმა.

ძირითადი რეგულაციის *58(2)* და *83*-ე მუხლებიც ცხადყოფს, რომ საზედამხედველო ორგანოს, მონაცემთა უსაფრთხოების დარღვევის დადგენის შემთხვევაში, ყოველთვის არ მოეთხოვება *“GDPR”*-ის *58*-ე მუხლის მე-*2* პუნქტის შესაბამისი, გამოსასწორებელი ზომების გატარება. ამგვარი ღონისძიების მიღება შეიძლება არ იყოს აუცილებელი, როდესაც ადგილი ჰქონდა *“GDPR”*-ის დარღვევას, თუმცა უკვე უზრუნველყოფილია რეგულაციის მოთხოვნებთან შესაბამისობა.

მაშასადამე, “GDPR”-ის 83-ე მუხლის („ადმინისტრაციული ჯარიმის დაკისრების ზოგადი წესები“) მიზანია ადმინისტრაციული ჯარიმების დაწესება რეგულაციის აღსასრულებლად. თუმცა, “GDPR”-ის პრეამბულის 148-ე პუნქტის შესაბამისად, როდესაც ჯარიმა არაპროპორციულ ტვირთს აკისრებს ფიზიკურ პირს, საზედამხედველო ორგანო უფლებამოსილია, თავი შეიკავოს ადმინისტრაციული ჯარიმის დაკისრებისგან და სანაცვლოდ,სანქციის სახით გამოიყენოს შენიშვნა (“reprimand”).

მართლმსაჯულების სასამართლომ მიუთითა განსახილველი საქმის ფაქტობრივ გარემოებებზე, რომლის თანახმად, კომერციულმა ბანკმა მომხმარებლის მონაცემთა უსაფრთხოების დარღვევის შესახებ ინფორმაცია მიაწოდა ჰესენის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს. ასევე, საზედამხედველო ორგანომ განაცხადა, რომ დასაქმებულის წინააღმდეგ მიღებული იქნა დისციპლინური ზომები და უნდა შეცვლილიყო მონაცემებზე წვდომის აღრიცხვასთან დაკავშირებული ინფორმაციის შენახვის ვადები. აღნიშნულის საფუძველზე, საზედამხედველო ორგანომ თავი შეიკავა “GDPR”-ის 58-ე მუხლის მე-2 პუნქტით გათვალისწინებული გამოსასწორებელი ზომების (მაგალითად, ადმინისტრაციული ჯარიმის დაწესება) მიღებისგან. ამასთანავე, მართლმსაჯულების სასამართლომ აღნიშნა, რომ საზედამხედველო ორგანოს მიერ მიღებული გადაწყვეტილება ექვემდებარება ეროვნული სასამართლოს განხილვას, შესაბამისად, გერმანიის ადმინისტრაციულ სასამართლოს უნდა შეეფასებინა, თუ რამდენად სათანადოდ და კანონის მოთხოვნათა დაცვით განიხილა საზედამხედველო ორგანომ საჩივარი.

·ევროკავშირის მართლმსაჯულების სასამართლომ დაადგინა:

ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ 57(1)(a)(f)-ე, 58(2)-ე და 77(1)-ე მუხლები უნდა განიმარტოს იმ მნიშვნელობით, რომ პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებული საკანონმდებლო მოთხოვნების დარღვევის შემთხვევაში, საზედამხედველო ორგანოს არ ეკისრება ვალდებულება მიიღოს “GDPR”-ის 58-ე მუხლის მე-2 პუნქტით გათვალისწინებული გამოსასწორებელი ზომები, კერძოდ, სანქციის სახით გამოიყენოს ჯარიმა მაშინ, როდესაც ამგვარი ზომა არ არის სათანადო, აუცილებელი, პროპორციული გამოვლენილი ნაკლოვანების გამოსასწორებლად და რეგულაციასთან შესაბამისობის უზრუნველსაყოფად.

„ევროპის მონაცემთა დაცვის ზედამხედველის“ (“EDPS”) მოსაზრება ადმინისტრაციული წარმოების ფარგლებში დამუშავებული პერსონალური მონაცემების შენახვის ვადის განსაზღვრის შესახებ

„ევროპის მონაცემთა დაცვის ზედამხედველმა“ (“EDPS”) გამოაქვეყნა მოსაზრება (“opinion”), რომელიც შეეხება ადმინისტრაციული წარმოების ფარგლებში დამუშავებული პერსონალური მონაცემების შენახვის ვადის განსაზღვრის შესახებ ევროპოლის მმართველი საბჭოს (“Europol Management Board Decision”) გადაწყვეტილების პროექტს.

ევროკავშირის მონაცემთა დაცვის რეგულაციის — “EUDPR”[2] მე-2(1) მუხლის თანახმად, რეგულაციის მოქმედება ასევე ვრცელდება ევროპოლის მიერ პერსონალური მონაცემების დამუშავების პროცესზე.

“EUDPR”-ის მე-4(1)(ე) ქვეპუნქტის შესაბამისად, ევროპოლი, როგორც მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი, ვალდებულია ადმინისტრაციული წარმოების ფარგლებში განსაზღვროს კონკრეტული მიზნით დამუშავებული პერსონალური მონაცემების შენახვის მაქსიმალური ვადა, რომელიც აუცილებელი და პროპორციული უნდა იყოს მონაცემთა დამუშავების მიზანთან მიმართებით („შენახვის ვადის შეზღუდვა“). ანგარიშვალდებულების პრინციპის თანახმად, მნიშვნელოვანია, რომ ევროპოლმა უზრუნველყოს კანონშესაბამისობა. ამასთანავე, “EUDPR”-ის შესაბამისად, ორგანიზაციამ უნდა განსაზღვროს თითოეული ფაილის შენახვის ვადა და მონაცემთა დამუშავების პროცესში მიიღოს სათანადო ტექნიკურ-ორგანიზაციული ზომები.

„ევროპოლის მმართველი საბჭოს“ (“Europol Management Board Decision”) გადაწყვეტილების პროექტთან დაკავშირებით “EDPS”-ის მიერ გაიცა შემდეგი რეკომენდაციები:

·“EUDPR”-ის მე-4(1)(ე) და მე-4(2) მუხლებთან შესაბამისობის უზრუნველსაყოფად, “EDPS” მიზანშეწონილად მიიჩნევს, რომ საბჭოს გადაწყვეტილების პროექტის შენახვის ცხრილის შესახებ დანართში აისახოს ის კრიტერიუმები და ელემენტები, რომლებიც ადასტურებს დამუშავებული პერსონალური მონაცემების შენახვის განსაზღვრულ ვადას;

·მონაცემთა კატეგორიების მიხედვით შენახვის ვადის სწორად განსაზღვრის მიზნით, მიზანშეწონილია, ევროპოლმა გადახედოს მონაცემთა დამუშავების შესახებ არსებულ ჩანაწერებს;

·შენახვის პერიოდების უსაფრთხოდ დანერგვისა და შემდგომ მისი შემოწმების მიზნით, მიზანშეწონილია, ევროპოლი დარწმუნდეს, რომ მისი საინფორმაციო სისტემები სათანადოდ არის განახლებული.

„ევროპის მონაცემთა დაცვის ზედამხედველი“ მიესალმება იმ ფაქტს, რომ გადაწყვეტილების პროექტი ითვალისწინებს შენახვის ვადის შეზღუდვის პრინციპს. პროექტის მე-3 მუხლის თანახმად, ადმინისტრაციული წარმოების ფარგლებში დამუშავებული პერსონალური მონაცემების შენახვა შესაძლებელია საგამონაკლისო შემთხვევებში, პროექტით დადგენილ ვადაზე მეტი ხნით, თუკი მონაცემები მუშავდება არქივირებისთვის ან თუკი არსებობს საჯარო ინტერესი, სამეცნიერო ან ისტორიული კვლევის ან სტატისტიკის წარმოების მიზნები. ამასთანავე, “EUDPR”-ის მე-13 მუხლის მიხედვით, მონაცემთა სუბიექტების უფლებებისა და თავისუფლებების დასაცავად უნდა არსებობდეს შესაბამისი გარანტიები.

აღნიშნულთან დაკავშირებით, „ევროპის მონაცემთა დაცვის ზედამხედველის“ რეკომენდაციის თანახმად, ევროპოლმა გადაწყვეტილების პროექტის მე-3 მუხლში სასურველია მკაფიოდ განაცხადოს, რომ ხსენებული მიზნებისთვის პერსონალური მონაცემების შენახვის ვადის გაზრდის საგამონაკლისო შემთხვევები სრულად შეესაბამება “EUDPR”-ის მე-13 მუხლის მოთხოვნებს.

ასევე, “EDPS” მიზანშეწონილად მიიჩნევს, რომ პროექტის მე-3 მუხლის მე-4 პუნქტი ითვალისწინებდეს მონაცემთა კატეგორიების მიხედვით შენახვის ვადის განსაზღვრის შესახებ კრიტერიუმების დოკუმენტირების ვალდებულებას. ზედამხედველის შეფასებით, მნიშვნელოვანია, რომ მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს დაეკისროს იმ კრიტერიუმების ანალიზის ვალდებულება, რომლითაც ხორციელდება ადმინისტრაციული წარმოების ფარგლებში დამუშავებული პერსონალური მონაცემების შენახვის ვადის გაგრძელების აუცილებლობის დადგენა და ასევე, განსაზღვროს შეფასების განხორციელების სიხშირე.

გადაწყვეტილების პროექტის დანართი ითვალისწინებს საზოგადოებასთან ურთიერთობის, მარკეტინგის, პრესისა და მსგავს საქმიანობასთან დაკავშირებული მონაცემების შენახვის სამწლიან ვადას. “EDPS”-ის მოსაზრებით, მნიშვნელოვანია განისაზღვროს ვადის ათვლის ზუსტი თარიღი და დასაბუთდეს მონაცემების შენახვის სამწლიანი ვადის მიზანშეწონილობა.

„ევროპის მონაცემთა დაცვის ზედამხედველი“ დადებითად აფასებს მონაცემთა სუბიექტის წვდომის უფლებასთან მიმართებით შენახვის სამწლიან ვადას, თუმცა იგი ამასთანავე საჭიროდ მიიჩნევს, რომ განისაზღვროს ვადის ათვლის თარიღი.
აღსანიშნავია, რომ „ევროპის მონაცემთა დაცვის ზედამხედველმა“ ევროპოლის მმართველი საბჭოს გადაწყვეტილების პროექტთან დაკავშირებით 33 რეკომენდაცია გასცა. ანგარიშვალდებულების პრინციპის შესაბამისად, მონაცემთა დაცვის ზედამხედველი იმედოვნებს, რომ აღნიშნული რეკომენდაციები გათვალისწინებული იქნება და გადაიდგმება შესაბამისი ნაბიჯები მონაცემთა დაცვის კანონმდებლობასთან შესაბამისობის უზრუნველსაყოფად.

საკომუნიკაციო პლატფორმა “Telegram“-მა კონფიდენციალობის პოლიტიკა განაახლა

მსოფლიოში ერთ-ერთი ყველაზე პოპულარული სოციალური მედიის პლატფორმა “Telegram” მომხმარებლებს პირადი მიმოწერის შესახებ კონფიდენციალობის სერვისით უზრუნველყოფს (“end-to-end encryption”). აღნიშნული მოდელი იცავს მომხმარებლებს პირად საკომუნიკაციო ინფორმაციის გამჟღავნებისგან და სთავაზობს მათ პერსონალურ მონაცემთა დაცვის მაღალი დონის გარანტიას.

მიუხედავად ამისა, საკომუნიკაციო პლატფორმა “Telegram”-ის სხვადასხვა არხზე არაერთხელ დაიდენტიფიცირებულა დიდი რაოდენობით არალეგალური მასალა, მაგალითად, პლატფორმის მეშვეობით, მომხმარებლებს აქვთ შესაძლებლობა შეიძინონ იარაღი, ნარკოტიკი, ჰქონდეთ წვდომა ბავშვებზე ძალადობის ამსახველ მასალაზე.

“Telegram”-ის კონფიდენციალობის პოლიტიკის ცვლილება ამავე კომპანიის ხელმძღვანელის — პაველ დუროვის დაპატიმრებას უკავშირდება. მიმდინარე წლის 25 აგვისტოს, იგი საფრანგეთის ერთ-ერთ აეროპორტში უკანონო ვაჭრობის, ნარკოტიკების კონტრაბანდის, თაღლითობისა და ბავშვთა სექსუალური ძალადობის ამსახველი მასალის ვებგვერდზე გავრცელებაში თანამონაწილეობის საფუძველზე დააკავეს.

“Telegram”-ის შეცვლილი კონფიდენციალობის პოლიტიკის თანახმად[1], გააქტიურდა შესაძლო არაკანონიერი ქმედებების შესახებ შეტყობინების გაგზავნის ფუნქცია (“Report”), რომლის მეშვეობით პლატფორმას შეეძლება დახურულ ჯგუფებსა და საკომუნიკაციო არხებში არსებული მონაცემების დამუშავება და კანონიერი მოთხოვნის შემთხვევაში, ამ მონაცემების სამართალდამცავი ორგანოებისთვის მიწოდება. საგულისხმოა, რომ “Telegram”-მა წაშალა ხშირად დასმული კითხვების (“FAQ”) სექციიდან ტექსტი, რომლის მიხედვით პლატფორმა უარს აცხადებდა მომხმარებელთა უკანონო ქმედებების შესახებ შეტყობინების საფუძველზე მიმოწერის გაცნობას.

ირლანდიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ ავიაკომპანია „რაინეარის“მონაცემთა დამუშავებისა და ვერიფიკაციის სისტემის შესწავლა დაიწყო

ირლანდიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ განაცხადა,[1] რომ დაიწყო ავიაკომპანია „რაინეარის“ მონაცემთა დამუშავების პრაქტიკის და კლიენტთა ვერიფიკაციის სისტემის შესწავლა. სისტემა გამოიყენება „რაინეარის“ იმ მომხმარებლებთან მიმართებით, რომლებიც ფრენებს ტურისტული სააგენტოების ან მესამე მხარის ვებგვერდების გამოყენებით ჯავშნიან.

საქმის შესწავლის დაწყების საფუძველი:

საზედამხედველო ორგანომ საქმის შესწავლა არაერთი მონაცემთა სუბიექტის საჩივრის საფუძველზე, კომპანია „რაინეარის“ მიერ, დამატებით დოკუმენტის სახით, პირადობის დამადასტურებელი მოწმობის მოთხოვნის შესახებ დაიწყო.

საქმის ფაქტობრივი გარემოებების თანახმად, „რაინეარი“ მომხმარებლებს ბილეთების მისი ვებგვერდის გამოყენებით დაჯავშნის შემთხვევაში, ვერიფიკაციას არ სთხოვდა. შესაბამისად, მათ დამატებით არც პირადობის დამადასტურებელი დოკუმენტების გაგზავნა მოეთხოვებოდათ. თუმცა, ბილეთების მესამე მხარის ვებგვერდების გამოყენებით დაჯავშნის შემთხვევაში, მონაცემთა სუბიექტების ვერიფიკაციის მიზნით, „რაინეარი“ სხვადასხვა დოკუმენტის (მათ შორის, ბიომეტრიულ მონაცემებს) წარდგენას ითხოვდა. შესაბამისად, ავიაკომპანიის მიერ გამოყენებული მეთოდები მოიცავდა მონაცემთა სუბიექტების ბიომეტრიულ მონაცემებზე დაყრდნობით, სახის ამომცნობი სისტემით ვერიფიკაციასაც.
ირლანდიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანო უახლოს მომავალში გამოაქვეყნებს გადაწყვეტილებას ავიაკომპანიის მონაცემთა დამუშავების პროცესის ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მოთხოვნებთან შესაბამისობის თაობაზე.

„მონაცემთა დაცვის ევროპული საბჭოს“ მოსაზრება ბიომეტრიულ მონაცემთა გამოყენებასთან დაკავშირებით:

აღსანიშნავია, რომ 2024 წლის მაისში „მონაცემთა დაცვის ევროპულმა საბჭომ“ გამოსცა მოსაზრება,[2] რომელშიც კიდევ ერთხელ იქნა განხილული ბიომეტრიულ მონაცემთა გამოყენებასთან დაკავშირებული საფრთხეები და შესაბამისი რისკები. საბჭომ ყურადღება გაამახვილა სახის ამომცნობ ტექნოლოგიაზე, რომლის გამოყენებამაც მონაცემთა სუბიექტების უფლებებზე და თავისუფლებებზე შესაძლოა ნეგატიური ზეგავლენა მოახდინოს.
საბჭო მიიჩნევს, რომ სახის ამომცნობ ტექნოლოგიებთან ასოცირებული მაღალი რისკის გამო, მათი გამოყენება უნდა მოხდეს მხოლოდ აუცილებელი საჭიროებების დროს და სიფრთხილის განსაკუთრებული ზომების დაცვით.

ესპანეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს მიერ კომპანია „გლოვოს“ დაჯარიმების შესახებ

ესპანეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ საკვების მიმწოდებელი კომპანია „გლოვო“, მონაცემთა სუბიექტის ინფორმაციაზე წვდომის მოთხოვნის უპასუხოდდატოვებისათვის, 15 000 ევროს ოდენობით დააჯარიმა.
საქმის ფაქტობრივი გარემოებები:

მონაცემთა სუბიექტი (პოლონეთის მოქალაქე, მძღოლი და საკვების მიმწოდებელი), რომელსაც მიწოდებასთან დაკავშირებით პრობლემა შეექმნა, დაუკავშირდა კომპანია „გლოვოს“ მომხმარებელთა დახმარების ჯგუფს და გაესაუბრა წინამდებარე ჯგუფის თანამშრომელს. მონაცემთა სუბიექტი კომპანიის წინააღმდეგ სასამართლოსადმი აპირებდა მიმართვას. აღნიშნული მიზნით, მან მომხმარებელთა დახმარების ჯგუფისაგან მოითხოვა საუბრის ჩანაწერების გაზიარება. ჩანაწერის გადაცემაზე უარის მიღების შემდგომ, მონაცემთა სუბიექტმა კომპანიას მძღოლებისათვის განკუთვნილი „დახმარების მომსახურეობის პორტალიდან“ გაუგზავნა ინფორმაციის მიწოდებაზე მოთხოვნა. მოთხოვნის წინამდებარე ფორმით მიღების შემდგომ, კომპანიამ კვლავ უარი განაცხადა საუბრის ჩანაწერის მიწოდებაზე.

მონაცემთა სუბიექტმა საჩივარი „გლოვოს“ წინააღმდეგ პოლონეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოში შეიტანა, თუმცა, ვინაიდან კომპანიის დაფუძნების ადგილი ესპანეთია, საქმე განსახილველად ესპანეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაეცა.

მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის განცხადებით, იგი არ იყო ვალდებული ეპასუხა ინფორმაციის მოთხოვნაზე, ვინაიდან იგი დაფიქსირდა არა სპეციალურად შექმნილი ელექტრონული ფოსტის მისამართზე, არამედ სხვა ფორმით, კერძოდ, მძღოლებისათვის განკუთვნილი „დახმარების მომსახურეობის პორტალის“ საშუალებით.

კომპანიის განცხადებით, მან მონაცემთა სუბიექტის მოთხოვნა მონაცემთა დაცვის საზედამხედველო ორგანოსგან შეიტყო. კომპანიამ აგრეთვე ხაზი გაუსვა შიდა პროცედურული წესების არსებობას, რომელთა საფუძველზე თანამშრომლებს ევალებათ, მონაცემთა დაცვასთან დაკავშირებული საკითხების მონაცემთა დაცვის ოფიცერთან გადამისამართება არ განხორციელდა მხოლოდ ერთი თანამშრომლის – განმცხადებლის მიერ. შესაბამისად, რეაგირება წინამდებარე ინფორმაციის მოთხოვნის შემთხვევასთან დაკავშირებით დაგვიანდა.

ესპანეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება:

საზედამხედველო ორგანომ არ გაიზიარა კომპანიის არგუმენტი მასზედ, რომ მონაცემთა სუბიექტმა მოთხოვნა არასწორი კომუნიკაციის არხის გამოყენებით დააფიქსირა.

საზედამხედველო ორგანოს მოსაზრებით, თუ თანამშრომელს თავად არ შეეძლო ინფორმაციის მოთხოვნაზე რეაგირება, იგი ვალდებული იყო მოთხოვნის თაობაზე ინფორმაცია დამუშავებისთვის პასუხისმგებელი პირის (კომპანიის) შესაბამისი დეპარტამენტისათვის მიეწოდებინა. კომპანია მონაცემთა სუბიექტთან საინფორმაციო მოთხოვნების მისაღებად საკომუნიკაციო ფორმის განსაზღვრის ნაწილში თავისუფალია. თუმცა, წინამდებარე დისკრეცია არ ათავისუფლებს მას პასუხისმგებლობისაგან უპასუხოს მონაცემთა სუბიექტების იმ მოთხოვნებს, რომლებიც სხვა არხების საშუალებით და სხვა ფორმით მიიღო.

საზედამხედველო ორგანომ გადაწყვეტილებაში მიუთითა „ევროპის მონაცემთა დაცვის საბჭოს“ გზამკვლევი, რომელიც მონაცემთა სუბიექტების ინფორმაციაზე წვდომის უფლებას შეეხება. წინამდებარე გზამკვლევი მონაცემთა დამუშავებისთვის პასუხისმგებელ პირებს ავალდებულებს, რომ უზრუნველყონ ზოგად საკონტაქტო არხებზე მიღებული განცხადებების იმ დეპარტამენტთან გადამისამართება, რომელიც რეაგირებს მონაცემთა სუბიექტების მოთხოვნებზე. საზედამხედველო ორგაონომ დაადგინა, რომ მხოლოდ ერთ-ერთი თანამშრომლის გულგრილი ქმედება არ გამორიცხავს კომპანიის პასუხისმგებლობას.

ისლანდიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება სამართალდაცვითი მიზნებისთვის განხორციელებული ვიდეოთვალთვალის კანონიერების შესახებ

ფაქტობრივი გარემოებები:

ისლანდიის მოქალაქე, მონაცემთა სუბიექტმა, მიმართა ისლანდიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს ადგილობრივი პოლიციის თანამშრომლის მიერ განხორციელებული მოქმედებების შესწავლის მიზნით. განმცხადებლის მითითებით, დამუშავებისთვის პასუხისმგებელმა პირმა, საკუთარი მობილური მოწყობილობით, დაამუშავა სამართალდაცვითი მიზნებისთვის განხორციელებული ვიდეოთვალთვალის შედეგად მიღებული ჩანაწერები. აღნიშნული ჩანაწერი გაუზიარა სხვა პოლიციელებსა და მათ შორის, მონაცემთა სუბიექტის დამსაქმებელს. განმცხადებელი შესაბამისი მტკიცებულებების მითითების გარეშე აღნიშნავდა, რომ მის პერსონალურ მონაცემებზე წვდომა მოიპოვეს არაავტორიზებულმა პირებმა, რითაც დაირღვა მისი, როგორც მონაცემთა სუბიექტის უფლებები.

საქმის განხილვა საზედამხედველო ორგანოში:

პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ გამოკვეთა ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ და მონაცემთა დაცვის ეროვნული კანონმდებლობის დარღვევის შესაძლო შემთხვევების შესწავლის მნიშვნელობა. საზედამხედველო ორგანომ დაადგინა, რომ დამუშავებისთვის პასუხისმგებელ პირს საერთაშორისო და ეროვნული კანონმდებლობის მოთხოვნები არ დაურღვევია.[1]

საზედამხედველო ორგანოს შეფასება:

საზედამხედველო ორგანოს შეფასებით, დამუშავებისთვის პასუხისმგებელმა პირმა განმცხადებლის მონაცემები საკუთარი საქმიანობის ფარგლებში შეაგროვა. შესაბამისად, მონაცემების დამუშავება დასაშვები იყო დანაშაულებრივი საქმიანობის ზოგადი ანალიზისა და სხვადასხვა გამოვლენილ დანაშაულთა შორის კავშირის დადგენის მიზნით. მასში მოიაზრებოდა მონაცემთა სუბიექტის ადგილმდებარეობის, ქცევისა და გადაადგილების მონიტორინგი. დამუშავებისთვის პასუხისმგებელმა პირმა სამართალდაცვითი მიზნებისთვის განხორციელებული ვიდეოთვალთვალის ჩანაწერები შეინახა შესაბამისი ფაილის სახით. ამ ფაილზე სხვა პოლიციელების წვდომა ასევე, უზრუნველყოფილი იყო მათი საქმიანობის განხორციელების მიზნებით. ვიდეოსათვალთვალო მოწყობილობები განთავსებული იყო საჯარო CCTV მოწყობილობების ფორმით.

საზედამხედველო ორგანოს განმარტებით, აღნიშნულ ჩანაწერებთან დაკავშირებით მონაცემთა სუბიექტს მტკიცების ტვირთი გააჩნია. გამომდინარე იქიდან, რომ მონაცემთა სუბიექტი შესაბამისი მტკიცებულებების გარეშე, განცხადებაში და ზოგადად, ზეპირსიტყვიერად აღნიშნავდა ინფორმაციის გადაცემის შემთხვევას, ეს არ შეიძლება მიჩნეულიყო უტყუარ მტკიცებულებად მონაცემთა სხვა პირისთვის გადაცემის დასადასტურებლად. მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის კომპიუტერული სისტემების მონიტორინგის შედეგად, საზედამხედველო ორგანოს არ აღმოუჩენია განცხადებაში აღნიშნული ფაილის არაავტორიზებული პირებისთვის გადაცემის ფაქტი.

საზედამხედველო ორგანოს გადაწყვეტილება:
ისლანდიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ დაადგინა, რომ მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის მიერ სამართალდაცვითი მიზნებისთვის განხორციელებული ვიდეოთვალთვალი იყო კანონიერი.
[

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