მსოფლიო პრაქტიკა

პერსონალურ მონაცემთა დაცვის სამსახური

სიახლეები

ლიეტუვის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება დამუშავებისთვის პასუხისმგებელი პირის მიერ მონაცემთა დამუშავების კანონიერების შესახებ

ფინეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება მონაცემთა უსაფრთხოების დარღვევის შესახებ

გაერთიანებული სამეფოს პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ მონაცემთა დაშიფვრის შესახებ ახალი სახელმძღვანელო რეკომენდაცია გამოაქვეყნა

2025 წლის 2 სექტემბერს გაერთიანებული სამეფოს პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ მონაცემთა დაშიფვრის (“ENCRYPTION”) შესახებ სახელმძღვანელო რეკომენდაციის განახლებული ვერსია გამოაქვეყნა.

საზედამხედველო ორგანო მონაცემთა დაშიფვრას განმარტავს პროცესად, რომელიც საიდუმლო გასაღების (“KEY”) საშუალებით წაკითხვად ტექსტს არაიდენტიფიცირებადს ხდის (რაც მხოლოდ შესაბამისი გასაღების მფლობელი და ავტორიზებული პირებისათვის არის გარჩევადი).

სექტემბერი 2025

აღნიშნულის საპირისპირო პროცესია გაშიფვრა (“DECRYPTION”) - ამ შემთხვევაში საიდუმლო გასაღები გამოიყენება ინფორმაციის წაკითხვად ფორმატში გადასაყვანად.[2] გასაღების გარეშე ინფორმაციის დაშიფვრა თეორიულად შესაძლებელია ყოველი სავარაუდო კომბინაციის მცდელობის გზით (“BRUTE FORCE ATTACK”), თუმცა აღნიშნული ფაქტობრივად შეუძლებელია გასაღების ტიპისა (“KEY TYPE”) და კომპიუტერული გამოთვლითი ფუნქციონალიდან (“COMPUTING POWER”) გამომდინარე. გასაღების ფლობის გარეშე, მონაცემთა დაშიფვრის პროცესის სირთულე მიანიშნებს დაშიფვრის, როგორც მონაცემთა დაცვის თვალსაზრისით გამოსაყენებელი ზომის, ეფექტურობაზე.

საჯარო და კერძო სექტორისათვის პერსონალურ მონაცემთა უსაფრთხოდ დამუშავება განსაკუთრებით მნიშვნელოვანია მონაცემთა სუბიექტების ნდობის მოპოვებისა და შენარჩუნების თვალსაზრისით. მონაცემთა დაშიფვრა აღნიშნული მიზნის მისაღწევად ეფექტური ტექნიკური საშუალებაა. მონაცემთა დაცვის მიზნებისათვის დაშიფვრის სხვადასხვა ფორმა ხშირად გამოიყენება, მაგალითად:
სხვადასხვა ტექნოლოგიის კოდით დაცვა (“PASSWORD PROTECTION”);
ვებგვერდის გამოყენება, რომელიც დაცულია დაშიფვრის პროტოკოლით (“HTTPS”). ამ შემთხვევაში მონაცემთა სუბიექტის პერსონალური მონაცემები (მაგალითად: პაროლი, პირადი ნომრები და სხვა) მონაცემთა გადაცემის პროცესში (ვებგვერდსა და მომხმარებლის მოწყობილობას შორის) დაშიფრული (“ENCRYPTED”) და დაცულია.

აღნიშნული დაცვის მექანიზმების გამოყენება საჭიროა იმისათვის, რომ მონაცემებზე წვდომა შეუძლებელი გახდეს არაავტორიზებული პირებისთვის, დადასტურდეს ვებგვერდის ავთენტურობა და მონაცემთა გადაცემის პროცესში დაცული იყოს მათი უსაფრთხოება უკანონო ზემოქმედებისგან, მაგალითად — არაავტორიზებული პირების მიერ ცვლილებებისაგან.
გაერთიანებული სამეფოს მონაცემთა დაცვის რეგულაცია არ ითვალისწინებს ორგანიზაციის ხელთ არსებული ყველა მონაცემის დაშიფვრის ვალდებულებას. დაშიფვრის საჭიროება დამოკიდებულია რისკზე, რომელიც განისაზღვრება მონაცემთა კატეგორიის, უსაფრთხოების დარღვევის ალბათობის, ტექნოლოგიისა და სხვა სათანადო ინფორმაციის შეფასების საფუძველზე. საზედამხედველო ორგანოს რეკომენდაციით, მონაცემთა დაშიფვრა საჭიროა მონაცემების ელექტრონულად გადაცემის პროცესში, მონაცემების სხვადასხვა მოწყობილობაში შენახვის დროს (მაგალითად, კომპიუტერში, მობილურ ტელეფონში და სხვა) და მონაცემთა მეხსიერების ბარათზე (“USB FLASH DRIVE”) შენახვისას.

სახელმძღვანელო რეკომენდაციის წინა რედაქციაში განხილულ იქნა დაშიფვრის სხვადასხვა პროტოკოლის, მაგალითად: “TLS”, “SSL” - შესახებ ინფორმაცია, თუმცა განსხვავებით განახლებული რედაქციისაგან, იგი დაშიფვრის პროტოკოლის (“HTTPS”) ვებგვერდის ყველა ნაწილში გამოყენების შესახებ რეკომენდაციას არ ითვალისწინებდა. სახელმძღვანელო რეკომენდაცია შეიცავს ორ ძირითად სიახლეს:
განახლებულია სახელმძღვანელო რეკომენდაციის ნაწილი, რომელიც მონაცემთა გადაცემის პროცესში დაშიფვრის პროტოკოლის (“HTTPS”) გამოყენებას ითვალისწინებს. საზედამხედველო ორგანოს განმარტებით, რეკომენდებულია, დაწესებულების ან ორგანიზაციის მიერ ვებგვერდის ფლობის შემთხვევაში, ვებგვერდი სრულად იქნეს დაცული დაშიფვრის პროტოკოლით (“HTTPS”). აღნიშნული სიახლე განსაკუთრებით მნიშვნელოვანია პერსონალური მონაცემების, მაგალითად, ავტორიზაციისთვის საჭირო მონაცემების, საბანკო (გადახდის შესახებ) ინფორმაციის და სხვა განსაკუთრებული კატეგორიის მონაცემების დაცვის თვალსაზრისით, რომლებსაც მომხმარებლები ვებგვერდზე უთითებენ;

სახელმძღვანელო რეკომენდაციის პირველ ვერსიაში ნათლად არ იყო გამიჯნული მონაცემთა დამუშავებისთვის პასუხისმგებელი პირების მიერ სავალდებულოდ შესასრულებელი და სარეკომენდაციო ხასიათის საკითხები. შესაბამისად, მონაცემთა დაშიფვრასთან დაკავშირებული ვალდებულებებისა და საუკეთესო პრაქტიკის მეტი სიცხადით გასამიჯნად, სახელმძღვანელო რეკომენდაციის ახალ ვერსიაში ყურადღება გამახვილდა მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის ვალდებულებებსა და სარეკომენდაციო ხასიათის საკითხებზე.

გაერთიანებული სამეფოს მონაცემთა დაცვის ძირითადი რეგულაციის მონაცემთა უსაფრთხოების შესახებ დებულებების თანახმად, საჭიროა მონაცემთა დაშიფვრის თვალსაზრისით დანერგილი ტექნიკური და ორგანიზაციული ზომების ეფექტურობა და კანონმდებლობასთან შესაბამისობის საკითხი პერიოდულად შემოწმდეს, შესაბამისად, რეკომენდებულია განისაზღვროს, თუ რა პერიოდულობით გადაიხედება დაშიფვრის გამოყენების წესის შესახებ კომპანიის ან დაწესებულების მიერ განსაზღვრული ტექნიკური და ორგანიზაციული ზომების დანერგვის საკითხი.

ფინეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება მონაცემთა უსაფრთხოების დარღვევის შესახებ

ფინეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ მსხვილი ფინური ონლაინ აფთიაქის (“YLIOPISTON APTEEKKI”) მიერ მონაცემთა დამუშავების კანონიერების შესწავლა მონაცემთა სუბიექტის (დოქტორანტურის სტუდენტ-მკვლევარი) მიმართვის საფუძველზე დაიწყო.

სტუდენტი სამეცნიერო საქმიანობის ფარგლებში ქსელურ კომუნიკაციას იკვლევდა (“NETWORK TRAFFIC ANALYSIS”). კერძოდ, მომხმარებლის მიერ გამოყენებულ ტექნიკურ საშუალებასა (მობილური ტელეფონი, კომპიუტერი და სხვა) და კონკრეტულ ონლაინ მომსახურებას (ამ შემთხვევაში, ონლაინ აფთიაქს) შორის მონაცემთა მიმოცვლის პროცესს სწავლობდა. აღნიშნულ პროცესში მან მონაცემთა დაცვის კანონმდებლობასთან შესაბამისობის (კერძოდ, კანონით გათვალისწინებული მონაცემთა უსაფრთხოების ზომების დაცვის) თვალსაზრისით ხარვეზები აღმოაჩინა.

აფთიაქის მომხმარებლებს გაცემული ჰქონდათ თანხმობა პერსონალურ მონაცემთა დამუშავების შესახებ, თუმცა, „მზა ჩანაწერები“ (“COOKIES”) ონლაინ აფთიაქის მიზნებისათვის იმგვარი ფორმით გამოიყენებოდა, რომ მომხმარებელთა საიტზე განხორციელებული აქტივობის შესახებ ინფორმაცია (მაგალითად: კონკრეტული პროდუქტის დათვალიერება, ყიდვის პროცესის წამოწყება და ასე შემდეგ) მესამე პირებს, კერძოდ, მომსახურების მიმწოდებლებს (“Google”,“Meta" და სხვები) გადაეცემოდათ.

მომხმარებლის აქტივობის შესახებ ინფორმაციასთან ერთად, ასევე, „მომხმარებელთა ინტერნეტ პროტოკოლის მისამართების“ (“IP ADDRESS”) შესახებ მონაცემი გადაიცემოდა, რომელთა გამოყენებით ინდივიდუალურ მომხმარებელთა იდენტიფიცირება იყო შესაძლებელი. [2] აღნიშნულ კომპანიებს (“GOOGLE” და “META”) მომხმარებელთა იდენტიფიკაცია შეეძლოთ იმ შემთხვევაში, თუ ონლაინ აფთიაქის გამოყენების დროს მომხმარებელს ავტორიზაცია “Google”-ის ან “Facebook”-ის ანგარიშის საშუალებით (“LOGGED IN”) ჰქონდა გავლილი.
ზემოაღნიშნული მომსახურების მიმწოდებლებთან გადაცემული ინფორმაცია:

- არ იყო სათანადოდ (ფსევდონიმიზაციის ან ანონიმიზაციის გამოყენებით) დაფარული (“MASKED”).
- ცალკეულ შემთხვევებში ინფორმაცია არ იყო დაშიფრული (“ENCRYPTED”), რაც მომსახურეობის მიმწოდებლების ან სხვა მესამე პირების მიერ მომხმარებელთა იდენტიფიკაციის, ასევე მომსახურების მიმწოდებლების მიერ მონაცემების შემდგომი (სხვა პირებისათვის) გადაცემის რისკს წარმოშობდა.

საზედამხედველო ორგანოს გადაწყვეტილებით „მზა ჩანაწერების“ ტექნოლოგიის გამოყენება შესაძლოა ადმინისტრაციული ჯარიმის დაკისრების საფუძველი გახდეს იმ შემთხვევაში, თუ:

- კომპანიის ვებგვერდზე არსებული „მზა ჩანაწერები“ იმგვარად გამოიყენება, რომ მონაცემთა სუბიექტების პერსონალური მონაცემები შესაძლოა ხელმისაწვდომი გახდეს მესამე პირთათვის ან/და;
- „მზა ჩანაწერები“ ტექნოლოგიის შესაბამისი დაცვის მექანიზმების (როგორიცაა მაგალითად, მონაცემთა მინიმიზაციის პრინციპი) დანერგვის გარეშე გამოყენება.[3]

აქედან გამომდინარე, საჭიროა კომპანიას წინასწარ ჰქონდეს განსაზღვრული, თუ რა პერსონალური მონაცემები შესაძლოა გახდეს ხელმისაწვდომი მესამე პირთათვის და რა დაცვის მექანიზმები უნდა დაინერგოს, რათა მონაცემები მესამე პირებთან (მაგალითად, მომსახურების მიმწოდებლებთან), მონაცემთა დაცვის კანონმდებლობის მოთხოვნათა გათვალისწინებით გაზიარდეს.

აღნიშნულ შემთხვევასთან დაკავშირებით დადგინდა „მონაცემთა დაცვის ძირითადი რეგულაციის“ (“GDPR”) შემდეგი მუხლების დარღვევა:

- მუხლი 32 (მონაცემთა უსაფრთხოება);
- მუხლი 5.1.ვ. (მონაცემთა დამუშავების პრინციპები - მონაცემთა უსაფრთხოდ, შესაბამისი ტექნიკური და ორგანიზაციული ზომების შესაბამისად დამუშავება);

ზემოაღნიშნული დარღვევების გათვალისწინებით, კომპანიას დაეკისრა ადმინისტრაციული ჯარიმა 1.1 მილიონი ევროს ოდენობით[4], ამასთან, მიიღო გაფრთხილება ონლაინ აფთიაქის ფუნქციონირების შედეგად შეგროვებული და დამუშავებული პერსონალური მონაცემების უსაფრთხოების ზომების უზრუნველყოფასთან დაკავშირებით.

საზედამხედველო ორგანომ აფთიაქის მიერ მონაცემთა დამუშავების კანონიერების საკითხი 2018 წლის მაისიდან 2022 წლის სექტემბრამდე შეისწავლა. აფთიაქის განცხადებით, მათ კომპანიებთან („GOOGLE“ და „META“) მზა ჩანაწერების საშუალებით ინფორმაციის გადაცემის პრაქტიკა 2022 წლის სექტემბერში შეწყვიტეს.

ევროკავშირის მონაცემთა დაცვის ზედამხედველის (“EDPS”) და მონაცემთა დაცვის ევროპული საბჭოს (“EDPB”) ერთობლივი მოსაზრება მონაცემთა დაცვის ძირითად რეგულაციაში” (“GDPR”) ცვლილებების შეტანის შესახებ

ევროკავშირის მონაცემთა დაცვის ზედამხედველმა (“EDPS”) და მონაცემთა დაცვის ევროპულმა საბჭომ (“EDPB”) ევროკომისიის მიერ შეთავაზებული საკანონმდებლო ცვლილებების შესახებ მოსაზრება გამოაქვეყნეს. ევროკომისიის წინადადება[1] საკანონმდებლო აქტებში, მათ შორის, ,,მონაცემთა დაცვის ძირითად რეგულაციაში” (“GDPR”)[2] მცირე და საშუალო ზომის საწარმოთათვის ცვლილებების შეტანას ისახავდა მიზნად.

ევროკომისიის წინადადების თანახმად, რეკომენდებულია, რომ ძირითადი რეგულაციის 30-ე მუხლის მეხუთე პუნქტში შევიდეს ცვლილება. აღნიშნული პუნქტი აწესებს გამონაკლისს მონაცემთა დამუშავების მოქმედებების შესახებ ინფორმაციის აღრიცხვის ვალდებულების თაობაზე. ამჟამად, წინამდებარე პუნქტით განსაზღვრული გამონაკლისი ვრცელდება მხოლოდ იმ საწარმოებსა და ორგანიზაციებზე, რომლებშიც 250-ზე ნაკლები დასაქმებულია, გარდა კანონით (ძირითადი რეგულაციის 30-ე მუხლის მეხუთე პუნქტი) განსაზღვრული ცალკეული გამონაკლისებისა. ევროკომისიის მოსაზრებით, რეკომენდებულია, ინფორმაციის აღრიცხვის ვალდებულებიდან გამონაკლისი ვრცელდებოდეს იმ საწარმოებსა და ორგანიზაციებზე, რომლებიც 750-ზე ნაკლებ თანამშრომელს ასაქმებენ იმ პირობით, თუ მათ მიერ განხორციელებული დამუშავების მოქმედებები (ძირითადი რეგულაციის 35-ე მუხლის მოთხოვნათა შესაბამისად) მონაცემთა სუბიექტების უფლებებისა და თავისუფლებების შეზღუდვის მაღალ რისკს არ ქმნის.

გამოქვეყნებული ერთობლივი მოსაზრების შესაბამისად, ევროკავშირის მონაცემთა დაცვის ზედამხედველი და მონაცემთა დაცვის ევროპული საბჭო ევროკომისიის მხრიდან მიიღებენ დამატებით დასაბუთებას ინფორმაციის აღრიცხვის ვალდებულებისაგან გამონაკლისის დაწესების თვალსაზრისით, ახალი რიცხობრივი მაჩვენებლის განსაზღვრის საჭიროების შესახებ.

აგრეთვე, ევროკომისიის ინიციატივით, ძირითადი რეგულაციის მეოთხე მუხლში უნდა განიმარტოს ტერმინები: „მცირე და საშუალო ზომის საწარმოები“ (“Small and Medium-sized Enterprises-SME”) და „მცირე და საშუალო კაპიტალიზაციის საწარმოები“ (“Small Mid-Caps Enterprises-SMC”). ამასთან, ძირითადი რეგულაციის მე-40(1) და 42(1)-ე მუხლების (სერტიფიცირებისა და ქცევის კოდექსის შესახებ) მოქმედების ფარგლები უნდა გავრცელდეს მცირე და საშუალო კაპიტალიზაციის საწარმოებზეც. არსებული მდგომარეობით, სერტიფიცირებისა და ქცევის კოდექსის დოკუმენტები, საწარმოებისა და ორგანიზაციებისთვის წარმოადგენს დამხმარე საშუალებას, “GDPR”-თან შესაბამისობის უზრუნველყოფის თვალსაზრისით. თუმცა, გასათვალისწინებელია, რომ აღნიშნული დოკუმენტები მიემართება მხოლოდ მცირე და საშუალო ზომის საწარმოების საჭიროებებს.

ამავდროულად, ევროკავშირის მონაცემთა დაცვის ზედამხედველი და მონაცემთა დაცვის ევროპული საბჭო აღნიშნავენ, რომ ახალი გამონაკლისის დაწესებისათვის (30-ე მუხლის მეხუთე პუნქტთან დაკავშირებით, რომელიც შეეხება იმ საწარმოებსა და ორგანიზაციებს, რომლებიც 750-ზე ნაკლებ თანამშრომელს ასაქმებენ) აუცილებელია აისახოს ტერმინთა განახლებული განმარტებები, კერძოდ: „მცირე და საშუალო ზომის საწარმოები“ და მცირე და „საშუალო კაპიტალიზაციის საწარმოები“. აგრეთვე, რეკომენდებულია, წინადადებაში ევროკომისიამ მიუთითოს, რომ ტერმინ „ორგანიზაციაში“, 30-ე მუხლის მეხუთე პუნქტის კონტექსტში, არ მოიაზრება საჯარო დაწესებულებები და ინსტიტუციები.

ლიეტუვის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება დამუშავებისთვის პასუხისმგებელი პირის მიერ მონაცემთა დამუშავების კანონიერების შესახებ

2025 წლის 1-ელ აგვისტოს, ლიეტუვის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ (“VDAI”) მიიღო გადაწყვეტილება[1] ონლაინ მაღაზიის მიერ მონაცემთა დამუშავების კანონიერების შესახებ.

საქმის ფაქტობრივი გარემოებები

საქმის ფაქტობრივი გარემოებების თანახმად, მონაცემთა სუბიექტი დარეგისტრირდა მეორეული ტანსაცმელებისა და აქსესუარების ყიდვა-გაყიდვის ონლაინ მაღაზიის ვებგვერდზე (“Vinted”). მომხმარებლის ახალი ანგარიშის შექმნისას ტელეფონის ნომრის მითითება საჭირო არ იყო, თუმცა მოგვიანებით დამუშავებისთვის პასუხისმგებელმა პირმა (ონლაინ მაღაზია) მონაცემთა სუბიექტს მოსთხოვა ტელეფონის ნომრის დამატება. ამგვარი მონაცემის შეგროვების მიზნად მაღაზიამ დაასახელა თაღლითობის პრევენცია, “Vinted” პლატფორმისა და მისი მომხმარებლების უსაფრთხოების უზრუნველყოფა. მონაცემთა სუბიექტმა დამუშავებისთვის პასუხისმგებელი პირის მოთხოვნა დაუსაბუთებლად მიიჩნია, თუმცა საბოლოოდ მაინც გააზიარა ტელეფონის ნომერი, ვინაიდან წინააღმდეგ შემთხვევაში საკუთარ ანგარიშზე წვდომა შეეზღუდებოდა.

თავის მხრივ, მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა მიუთითა “Vinted”-ის მომსახურების პირობებზე, სადაც ნათლად იყო განმარტებული, რომ ანგარიშის უსაფრთხოების უზრუნველყოფისა და თაღლითობის პრევენციის მიზნით, მომხმარებლის ტელეფონის ნომერი ანგარიშის ვერიფიკაციის ერთ-ერთ მეთოდს წარმოადგენდა. აღნიშნულის საფუძველზე დამუშავებისთვის პასუხისმგებელი პირი აცხადებდა, რომ ანგარიშის ვერიფიკაციისთვის ტელეფონის ნომრის შეგროვება ეფუძნებოდა ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მე-6 მუხლის 1-ელი პუნქტის „ბ“ ქვეპუნქტით გათვალისწინებულ სამართლებრივ საფუძველს, რომლის თანახმად, მონაცემთა დამუშავება კანონიერია, თუ აუცილებელია მონაცემთა სუბიექტის მიერ დადებული ხელშეკრულების შესასრულებლად ან სუბიექტის თხოვნით ხელშეკრულების გაფორმებამდე გარკვეული ზომების მისაღებად. დამატებით, მომხმარებელთა ანგარიშის უსაფრთხოების უზრუნველყოფა ხელშეკრულების განუყოფელ ნაწილს წარმოადგენდა. აღნიშნულიდან გამომდინარე, პერსონალური მონაცემების შეგროვება ანგარიშის ვერიფიკაციის მიზნით მომხმარებელთა ლეგიტიმურ მოლოდინებთან შესაბამისობაში იყო.

საზედამხედველო ორგანოს შეფასება

ლიეტუვის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ დაადგინა, რომ მომხმარებელთა ანგარიშების ვერიფიკაცია დამუშავებისთვის პასუხისმგებელ პირსა და მონაცემთა სუბიექტს შორის გაფორმებული ხელშეკრულების არსებით ასპექტს არ წარმოადგენდა. ამ მიზეზით, საზედამხედველო ორგანომ მიიჩნია, რომ მონაცემთა დამუშავება ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ (“GDPR”) მე-6 მუხლის 1-ელი პუნქტის „ა“ და „ბ“ ქვეპუნქტს ვერ დაეფუძნებოდა. საზედამხედველო ორგანომ მიუთითა მონაცემთა დაცვის ევროპული საბჭოს (“EDPB”) სახელმძღვანელო რეკომენდაციაზე და აღნიშნა, რომ აღნიშნული ნორმის აუცილებლობის კრიტერიუმი ვიწროდ უნდა იქნეს განმარტებული.

საზედამხედველო ორგანომ, ასევე, აღნიშნა, რომ მომსახურების პირობების მიხედვით, დამუშავებისთვის პასუხისმგებელი პირის მიერ ტელეფონის ნომრის დამუშავება ვერიფიკაციის ერთ-ერთ შესაძლო საშუალებას წარმოადგენდა. აღნიშნული გარემოება საკმარისი იყო იმის დასადგენად, რომ პერსონალური მონაცემების დამუშავება ვერ აკმაყოფილებდა ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მე-6 მუხლის 1-ელი პუნქტის ფარგლებში დადგენილ აუცილებლობის კრიტერიუმს.

საზედამხედველო ორგანოს გადაწყვეტილება

საზედამხედველო ორგანომ დაადგინა, რომ მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის მიერ დაირღვა ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მე-6 მუხლის 1-ელი პუნქტის „ა“ და „ბ“ ქვეპუნქტი - კანონიერი საფუძვლის გარეშე შეაგროვა მომხმარებელთა პერსონალური მონაცემები. აღნიშნულიდან გამომდინარე, კომპანიას დაევალა ვერიფიკაციის მიზნით ტელეფონის ნომრების შეგროვების შეწყვეტა და უკანონოდ მოპოვებული მონაცემების წაშლა.

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