ევროკავშირის მართლმსაჯულების სასამართლოს პრეცედენტული სამართალი

ევროკავშირის მართლმსაჯულების სასამართლოს 2023 წლის 14 დეკემბრის გადაწყვეტილება *VB v. Natsionalna agentsia za prihodite, C-340/21, ECLI:EU:C:2023:986*

მოკლე მიმოხილვა:

2019 წლის 15 ივლისს ბულგარეთის მედიაში გავრცელდა ინფორმაცია კიბერთავდასხმის შესახებ. ცნობების თანახმად, ბულგარეთის შემოსავლების ეროვნული სააგენტოს (Natsionalna agentsia za prihodite, შემდგომ NAP)[1] IT სისტემაში ადგილი ჰქონდა უნებართვო წვდომასა და მასში დაცული პერსონალური მონაცემების ინტერნეტში გამოქვეყნებას. აღნიშნული მოვლენა შეეხო ექვს მილიონზე მეტ ადამიანს, რომელთაგან შვიდასმა, მათ შორის, აპელანტმა, NAP-ის წინააღმდეგ ეროვნულ სასამართლოში შეიტანა სარჩელი. მონაცემთა დაცვის ზოგადი რეგულაციის (GDPR) 82-ე მუხლისა და ეროვნული კანონმდებლობის საფუძველზე აპელანტი ითხოვდა ზიანის ანაზღაურებას.

საგულისხმოა, რომ, მონაცემთა დაცვის ზოგადი რეგულაციის (GDPR) 24-ე და 32-ე მუხლების მიხედვით, მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია მიიღოს სათანადო ზომები მონაცემთა უსაფრთხოების დასაცავად. მოცემულ საქმეზე ბულგარეთის ეროვნულ სასამართლოში ერთ-ერთ სადავო საკითხს აღნიშნული პირის პასუხისმგებლობა წარმოადგენდა. კერძოდ, მესამე პირის მიერ უნებართვო წვდომა ან ამავე პირის მიერ მონაცემების უნებართვო გამჟღავნება ნიშნავდა თუ არა იმას, რომ მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის მიერ მიღებული ტექნიკური და ორგანიზაციული ზომები მონაცემთა დაცვის ზოგადი რეგულაციის (GDPR) 24-ე და 32-ე მუხლების მიხედვით არ იყო „სათანადო“? წინასწარი გადაწყვეტილების პროცედურის ფარგლებში, ეროვნულმა სასამართლომ აღნიშნული შეკითხვით მიმართა ევროკავშირის მართლმსაჯულების სასამართლოს.

ევროკავშირის მართლმსაჯულების სასამართლოს განმარტებით, მონაცემთა დაცვის ზოგადი რეგულაციის (GDPR) 24-ე და 32-ე მუხლები უნდა განიმარტოს ისე, რომ მესამე პირის მიერ პერსონალური მონაცემების უნებართვო გამჟღავნება ან ამ მონაცემებზე უნებართვო წვდომა, ამ რეგულაციის მე-4(10)[2] მუხლის მნიშვნელობით, თავისთავად არ უნდა ჩაითვალოს საკმარისად იმის დასადგენად, რომ მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის მიერ მიღებული ტექნიკური და ორგანიზაციული ზომები, რეგულაციის 24-ე და 32-ე მუხლების მნიშვნელობით, არ იყო სათანადო.

მნიშვნელოვანი ამონარიდები გადაწყვეტილებიდან:

24 [...] უნდა აღინიშნოს, რომ მონაცემთა დაცვის ზოგადი რეგულაციის (GDPR) 24-ე მუხლი პერსონალურ მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის მიმართ ადგენს ზოგად ვალდებულებას, რომ მან მიიღოს სათანადო ტექნიკური და ორგანიზაციული ზომები მონაცემთა ამ რეგულაციის შესაბამისად დამუშავების უზრუნველსაყოფად და შეძლოს მონაცემთა დამუშავების ამ რეგულაციასთან შესაბამისობის დადასტურება.

25 ამ მიზნით, 24(1)-ე მუხლში ჩამოთვლილია ის კრიტერიუმები, რომლებიც მხედველობაში უნდა იქნეს მიღებული ასეთი ზომების სათანადოობის შეფასებისთვის, სახელდობრ, დამუშავების ხასიათი, მოცულობა, კონტექსტი და მიზანი, ისევე, როგორც სხვადასხვა ხარისხით სავარაუდო და სხვადასხვა სიმძიმის რისკები ფიზიკური პირის უფლებებთან და თავისუფლებებთან მიმართებით. ნახსენები

[1] NAP არის ბულგარეთის ფინანსთა სამინისტროსთან დაკავშირებული უწყება, რომლის უფლებამოსილებებიც, სხვებს შორის, მოიცავს სახელმწიფო ვალის იდენტიფიცირებას, უზრუნველყოფასა და ამოღებას და რომელიც წარმოადგენს მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს მონაცემთა დაცვის ზოგადი რეგულაციის (GDPR) მე-4(7) მუხლის მნიშვნელობით.

[2] მონაცემთა დაცვის ზოგადი რეგულაციის (GDPR) მე-4(10) მუხლი განმარტავს „მესამე პირის“ ცნებას.

დებულების დამატებითი პირობაა, რომ საჭიროების შემთხვევაში ეს ზომები გადაიხედოს და განახლდეს.

26 აღნიშნული თვალსაზრისიდან გამომდინარე, მონაცემთა დაცვის ზოგადი რეგულაციის (GDPR) 32-ე მუხლი ადგენს მონაცემთა დამუშავებისთვის პასუხისმგებელი პირისა და შესაძლო დამუშავებაზე უფლებამოსილი პირის ვალდებულებებს ასეთი დამუშავების უსაფრთხოებასთან დაკავშირებით. ამგვარად, აღნიშნული მუხლის 1-ელი პუნქტი განსაზღვრავს, რომ მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა და დამუშავებაზე უფლებამოსილმა პირმა უნდა მიიღონ სათანადო ტექნიკური და ორგანიზაციული ზომები, რათა უზრუნველყონ ამ გადაწყვეტილების წინა პუნქტში მითითებული რისკების სათანადო უსაფრთხოების ხარისხი, უახლესი ტექნოლოგიების, განხორციელების ხარჯების, დამუშავების ხასიათის, მოცულობის, კონტექსტისა და მიზნების გათვალისწინებით.

27 ანალოგიურად, აღნიშნული მუხლის მე-2 პუნქტი ადგენს, რომ უსაფრთხოების სათანადო ხარისხის შეფასებისას განსაკუთრებით გასათვალისწინებელია ის რისკები, რომლებიც გამოწვეულია პერსონალური მონაცემების დამუშავებით, კონკრეტულად, მათი შემთხვევითი ან უკანონო განადგურებით, დაკარგვით, შეცვლით, უნებართვო გამჟღავნებით ან მათზე უნებართვო წვდომით.

[...]

29 მონაცემთა დაცვის ზოგადი რეგულაციის (GDPR) 32(1)-ე და 32(2)-ე მუხლებში „რისკის შესაბამის უსაფრთხოების ხარისხზე“ და „უსაფრთხოების შესაბამის ხარისხზე“ გაკეთებული მითითება აჩვენებს, რომ რეგულაცია აყალიბებს რისკის მართვის სისტემას და რომ ის არანაირად არ ისახავს მიზნად პერსონალურ მონაცემთა დაცვის წესების დარღვევის რისკების აღმოფხვრას.

30 მონაცემთა დაცვის ზოგადი რეგულაციის (GDPR) 24-ე და 32-ე მუხლებიდან ცხადია, რომ ისინი მონაცემთა დამუშავებისთვის პასუხისმგებელი პირისგან მოითხოვს, შესაძლებლობის ფარგლებში, ისეთი ტექნიკური და ორგანიზაციული ზომების მიღებას, რომელთა მიზანია პერსონალურ მონაცემთა დამუშავების ნებისმიერი დარღვევის თავიდან აცილება. ასეთი ზომების სათანადოობა უნდა შეფასდეს კონკრეტულ შემთხვევაში იმის შემოწმებით, მიიღო თუ არა მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა ზომები აღნიშნულ ნორმებში მითითებული სხვადასხვა კრიტერიუმების, ამ დამუშავებისთვის დამახასიათებელი მონაცემთა დაცვის საჭიროებების და მისგან მომდინარე რისკების გათვალისწინებით.

31 შესაბამისად, მონაცემთა დაცვის ზოგადი რეგულაციის (GDPR) 24-ე და 32-ე მუხლები არ შეიძლება განიმარტოს იმგვარად, რომ მესამე პირის მიერ პერსონალურ მონაცემთა უნებართვო გამჟღავნება ან მათზე უნებართვო წვდომა საკმარისი იყოს მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის მიერ მიღებული ზომების არასათანადოდ მისაჩნევად, [...], მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის მიერ საწინააღმდეგო მტკიცებულების წარდგენის შესაძლებლობის გარეშე.

32 ასეთი სახის განმარტება მით უფრო აუცილებელია, რადგან მონაცემთა დაცვის ზოგადი რეგულაციის (GDPR) 24-ე მუხლი აშკარად ითვალისწინებს, რომ მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს უნდა ჰქონდეს იმის დადასტურების შესაძლებლობა, რომ მის მიერ მიღებული ზომები შეესაბამება აღნიშნულ რეგულაციას, ანუ შესაძლებლობას, რომელსაც ის მოკლებული იქნებოდა, თუ დაუშვებდნენ უცილობელ პრეზუმფციას.

ეროვნული კანონმდებლობის ნორმის ევროკავშირის კანონმდებლობასთან დაახლოების საფუძველი	საქართველო-ევროკავშირის ასოცირების შესახებ შეთანხმების დანართი I
ევროკავშირის სამართლებრივი აქტი, რომელთანაც მოხდა ეროვნული ნორმის დაახლოება	ევროპარლამენტისა და საბჭოს 2016 წლის 27 აპრილის რეგულაცია (EU) 2016/679 „პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვისა და ასეთი მონაცემების თავისუფალი მიმოცვლის შესახებ, რომელიც აუქმებს დირექტივას 95/46/EC (მონაცემთა დაცვის ზოგადი რეგულაცია (GDPR))“
ევროკავშირის დებულება	რეგულაციის 2016/679 24-ე და 32-ე მუხლები
ეროვნული ნორმა, რომლის დაახლოება ევროკავშირის სამართლებრივ აქტთან უკვე მოხდა	„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 27-ე მუხლის 1-ელი, მე-2, მე-3 და მე-6 პუნქტები *(სარეგისტრაციო კოდი 010100000.05.001.020936; 13/05/2025 კონსოლიდირებული ვერსია)*

საკვანძო ტერმინი	სათანადო ორგანიზაციული და ტექნიკური ზომები
ევროკავშირის მართლმსაჯულების სასამართლოს (CJEU) პრეცედენტული სამართალი	2023 წლის 14 დეკემბრის გადაწყვეტილება *VB v. Natsionalna agentsia za prihodite, C-340/21, ECLI:EU:C:2023:986*

ინფორმაცია დამუშავებულია საქართველოს იუსტიციის სამინისტროს ევროკავშირის სამართლის დეპარტამენტის მიერ, ევროკავშირის მართლმსაჯულების სასამართლოს გადაწყვეტილებათა ანალიზის საფუძველზე. ანალიზი განკუთვნილია მხოლოდ საინფორმაციო და საგანმანათლებლო მიზნებისთვის და არ ასახავს რომელიმე ორგანიზაციის, დაწესებულების ან სუბიექტის შეხედულებებს.