მსოფლიო პრაქტიკა

პერსონალურ მონაცემთა დაცვის სამსახური

სიახლეები

ევროკავშირის მართლმსაჯულების სასამართლოს გადაწყვეტილება „ლეგიტიმური ინტერესის“ განმარტების შესახებ

ევროპის მართლმსაჯულების სასამართლოს გადაწყვეტილება მედიკამენტების შესყიდვასთან დაკავშირებული მონაცემების დამუშავების შესახებ

გაერთიანებული სამეფოს პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება სამართალდამცავი ორგანოს მიერ მონაცემთა უსაფრთხოების დარღვევის შესახებ

გაერთიანებული სამეფოს პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ (“ICO”) ჩრდილოეთ ირლანდიის საპოლიციო სამსახურის (“The Police Service of Northern Ireland”) მიერ მონაცემთა უსაფრთხოების დარღვევასთან დაკავშირებით გადაწყვეტილება[1] მიიღო. საქმე შეეხებოდა ვებგვერდის მეშვეობით 9 483 პოლიციელისა და თანამშრომლის პერსონალური მონაცემების საჯარო გაზიარებას.[2]

ico.
Information Commissioner's Office

დეკემბერი 2024

ფაქტობრივი გარემოებები:
ჩრდილოეთ ირლანდიის საპოლიციო სამსახურის (“PSNI”) მონაცემთა ბაზა აერთიანებდა პოლიციის ოფიცრებისა და სამსახურის თანამშრომელთა პერსონალურ ინფორმაციას, კერძოდ: გვარი და სახელის ინიციალი; სამსახურებრივი მოვალეობა; დაკავებული თანამდებობა; დეპარტამენტი; სამუშაო ადგილსამყოფელი; თანამშრომელთან დადებული ხელშეკრულების სახე; სქესი; სამსახურის ნომერი.
საქმის ფაქტობრივი გარემოებების თანახმად, ჩრდილოეთ ირლანდიის საპოლიციო სამსახური მუდმივად განიხილავდა განმცხადებელთა მოთხოვნებს სამსახურში დასაქმებულ პირთა შესახებ საჯარო ინფორმაციის მიწოდების თაობაზე. აღნიშნული მიზნით იგი იყენებდა ზემოხსენებულ მონაცემთა ბაზას. აღსანიშნავია, რომ ადამიანური რესურსების ანალიზის მიზნებისთვის პოლიციის თანამშრომლების პერსონალური მონაცემები მუშავდებოდა საოფისე პროგრამა - “Excel”-ში.
2024 წლის 8 აგვისტოს, საჯარო ინფორმაციის მოთხოვნაზე პასუხის მომზადების პროცესში, სამსახურის თანამშრომლებისა და პოლიციის ოფიცერთა პერსონალური მონაცემები შეცდომით გამოქვეყნდა სამსახურის ვებგვერდზე. “Excel”-ის ცხრილში წარმოდგენილი იყო მრავალი გვერდი (მათ შორის, დაფარული გვერდები), რომელშიც ასახული იყო სამსახურის თანამშრომელთა პერსონალური მონაცემები.

გადაწყვეტილების დასაბუთება:
“ICO”-მ აღნიშნა, რომ საპოლიციო სამსახური, პერსონალური მონაცემების შემთხვევით გამოქვეყნებამდეც, არღვევდა გაერთიანებული სამეფოს „მონაცემთა დაცვის ძირითადი რეგულაციის“ მე-5(1)(f) (ვადის შეზღუდვის პრინციპი) და 32(1)(2)-ე (მონაცემთა დამუშავების უსაფრთხოება) მუხლებს. საზედამხედველო ორგანოს განმარტებით, მონაცემთა უსაფრთხოების დარღვევას შეიძლებოდა, ადგილი ჰქონოდა მითითებული დროის ნებისმიერ მონაკვეთში. აღნიშნული ძირითადად განპირობებული იყო შემდეგი გარემოებებით:

- საჯარო ინფორმაციის მოთხოვნის ფარგლებში სამსახურის მიერ თანამშრომელთა პერსონალური მონაცემების დამუშავების ფორმა და სიხშირე, რაც ზრდიდა პერსონალური ინფორმაციის გამჟღავნების რისკებს;
- “Excel”-ის ცხრილში მონაცემების ასახვა და გაზიარება, რომლითაც იზრდებოდა ადამიანური შეცდომის დაშვების ალბათობა;
- სამსახურის დაახლოებით 10 000 თანამშრომლისა და ოფიცრის პერსონალური ინფორმაციის დამუშავება, რაც წარმოშობდა რისკებს მათი უფლებებისა და თავისუფლებების დაცვის თვალსაზრისით;
- საჯარო ინფორმაციის მოთხოვნაზე პასუხების საჯაროდ ხელმისაწვდომობა;
- დამუშავებული პერსონალური მონაცემების სახეები, როგორიცაა მონაცემთა სუბიექტის თანამდებობა, სქესი, სამუშაო ადგილსამყოფელი, რაც იძლეოდა პირთა იდენტიფიცირების საშუალებას.

საზედამხედველო ორგანომ აგრეთვე აღნიშნა, რომ პერსონალური მონაცემების დამუშავების პროცესში არ იყო უზრუნველყოფილი სათანადო ტექნიკური და ორგანიზაციული უსაფრთხოების ზომები, მაგალითად, როგორიცაა: ადმინისტრაციული პერსონალის გადამზადება.

მიღებული გადაწყვეტილება:
გაერთიანებული სამეფოს პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ, ჯარიმის დაკისრებისას, გაითვალისწინა მონაცემთა უსაფრთხოების დარღვევის ხანგრძლივობა და სიმძიმე, რის გამოც ჩრდილოეთ ირლანდიის საპოლიციო სამსახურს დაეკისრა ჯარიმა 89 930 ევროს ოდენობით.

ევროკავშირის მართლმსაჯულების სასამართლოს გადაწყვეტილება „ლეგიტიმური ინტერესის“ განმარტების შესახებ

ევროკავშირის მართლმსაჯულების სასამართლომ (“CJEU”) (Case C-621/22[1]) ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ (“GDPR”) მე-6 მუხლის პირველი პუნქტის “f” ქვეპუნქტის („მონაცემთა დამუშავება აუცილებელია მონაცემთა დამმუშავებლის ან მესამე პირის კანონიერი ინტერესების დასაცავად, გარდა იმ შემთხვევისა, როდესაც აღნიშნულ ინტერესებს აღემატება იმ მონაცემთა სუბიექტის ინტერესები ან ფუნდამენტური უფლებები და თავისუფლებები, რომელიც მოითხოვს მონაცემთა დაცვას, განსაკუთრებით თუ მონაცემთა სუბიექტი ბავშვია“) ფარგლებში „ლეგიტიმური ინტერესის“ განმარტებასთან დაკავშირებით იმსჯელა.[2]

- **საქმის ფაქტობრივი გარემოებები:**

2018 წელს, ჩოგბურთის ფედერაციამ, რომელიც წარმოადგენს დამუშავებისთვის პასუხისმგებელ პირს, ორ სპონსორს (სპორტული აღჭურვილობის მიმწოდებელი და ონლაინ ტოტალიზატორის კომპანია), თანხის გადახდის სანაცვლოდ, ფედერაციის წევრების პერსონალური მონაცემები გადასცა. სპონსორები აღნიშნულ მონაცემებს მარკეტინგული მიზნებისთვის ამუშავებდნენ.

მონაცემთა სუბიექტებმა (ფედერაციის წევრები) საჩივარი შეიტანეს ჰოლანდიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოში, რომელმაც დაადგინა დამუშავებისთვის პასუხისმგებელი პირის მიერ “GDPR”-ის მე-6 მუხლის („მონაცემთა დამუშავების კანონიერება“) პირველი პუნქტის “a” („მონაცემთა დამუშავება კანონიერია მხოლოდ იმ შემთხვევაში და იმ მოცულობით, თუ მონაცემთა სუბიექტი განაცხადებს თანხმობას მისი პერსონალური მონაცემების დამუშავებაზე ერთი ან ერთზე მეტი კონკრეტული მიზნისთვის“) და “f” („მონაცემთა დამუშავება აუცილებელია მონაცემთა დამმუშავებლის ან მესამე პირის კანონიერი ინტერესების დასაცავად, გარდა იმ შემთხვევისა, როდესაც აღნიშნულ ინტერესებს აღემატება იმ მონაცემთა სუბიექტის ინტერესები ან ფუნდამენტური უფლებები და თავისუფლებები, რომელიც მოითხოვს მონაცემთა დაცვას, განსაკუთრებით თუ მონაცემთა სუბიექტი ბავშვია“) ქვეპუნქტების დარღვევა.

ამასთან, საზედამხედველო ორგანოს შეფასებით, დაირღვა “GDPR”-ის მე-5 მუხლის პირველი პუნქტის “a” ქვეპუნქტი („პერსონალური მონაცემები უნდა დამუშავდეს კანონიერად, სამართლიანად და გამჭვირვალედ მონაცემთა სუბიექტთან მიმართებით“), ვინაიდან ჩოგბურთის ფედერაციამ სპონსორებს პერსონალური ინფორმაცია მონაცემთა სუბიექტების თანხმობისა და სხვა სამართლებრივი საფუძვლის არსებობის გარეშე გაუზიარა. შესწავლილი გარემოებებიდან გამომდინარე, ჰოლანდიის საზედამხედველო ორგანომ დამუშავებისთვის პასუხისმგებელი პირი 525 000 ევროს ოდენობით დააჯარიმა.

დამუშავებისთვის პასუხისმგებელმა პირმა საზედამხედველო ორგანოს გადაწყვეტილება ამსტერდამის სასამართლოში გაასაჩივრა, ძირითადი რეგულაციის მე-6 მუხლის პირველი პუნქტის “f” ქვეპუნქტის შესაბამისად, ფედერაციის წევრების პერსონალური მონაცემების გაზიარებისთვის ლეგიტიმური ინტერესის არსებობაზე მითითებით. დამატებით, იგი ამტკიცებდა, რომ ლეგიტიმური ინტერესი გულისხმობდა მონაცემთა სუბიექტებისთვის სპონსორების მხრიდან ფასდაკლებების შეთავაზებას, რათა ჩოგბურთის თამაშის შესაძლებლობა უფრო ხელმისაწვდომი ფასებით ჰქონოდათ.
2022 წლის 22 სექტემბერს, ამსტერდამის სასამართლომ, „ლეგიტიმური ინტერესების“ განმარტების თხოვნით ევროკავშირის მართლმსაჯულების სასამართლოს მიმართა, რათა დაეზუსტებინა შეიძლება თუ არა, რომ ნებისმიერი ინტერესი ლეგიტიმურ ინტერესად შეფასდეს, თუ იგი არ ეწინააღმდეგება კანონს.

- **ევროკავშირის მართლმსაჯულების სასამართლოს გადაწყვეტილება:**

სასამართლომ, უპირველეს ყოვლისა, აღნიშნა, რომ ლეგიტიმური ინტერესის სამართლებრივი საფუძველი უნდა განიმარტოს ვიწროდ, ვინაიდან პერსონალური მონაცემები მონაცემთა სუბიექტის თანხმობის გარეშე მუშავდება. სასამართლოს განმარტებით, “GDPR”-ის პრეამბულის 47-ე პუნქტის თანახმად, აუცილებელი არ არის, რომ ლეგიტიმური ინტერესის შინაარსი არ შემოიფარგლება კანონით. დამატებით, ამავე პუნქტის შესაბამისად, პირდაპირი მარკეტინგის მიზნებით პერსონალური მონაცემების დამუშავება შეიძლება ჩაითვალოს კანონიერი ინტერესის საფუძველზე დამუშავებად. “CJEU”-მ განმარტა, რომ ლეგიტიმური ინტერესი უნდა შეფასდეს კანონმდებლობისა და განსახილველი საქმის ფაქტობრივი გარემოებების ანალიზის საფუძველზე. სასამართლომ აღნიშნა, რომ ლეგიტიმური ინტერესების უზრუნველსაყოფად პერსონალური მონაცემების დამუშავება, მიზნის გათვალისწინებით, უნდა იყოს აუცილებელი. ასევე, დაცული უნდა იქნას ბალანსი მონაცემთა სუბიექტის უფლებებსა და თავისუფლებებს და დამუშავებისთვის პასუხისმგებელი პირის ლეგიტიმურ ინტერესებს შორის. პერსონალური მონაცემების დამუშავება უნდა იყოს აუცილებელი მიზნის მისაღწევად და არ უნდა არსებობდეს სხვა, ნაკლებად მზღუდავი საშუალებები.

განსახილველ საქმეში, დამუშავებისთვის პასუხისმგებელ პირს უნდა მიეწოდებინა ფედერაციის წევრებისთვის ინფორმაცია, რომ მარკეტინგული მიზნებისთვის გეგმავდა მათი პერსონალური მონაცემების სპონსორებისთვის გადაცემას და გადაცემამდე თითოეულის თანხმობის მოპოვება. დამატებით, სასამართლომ აღნიშნა, რომ ისეთი სპონსორებისთვის, რომლებიც მართავენ კაზინოებისა და აზარტული თამაშების ვებგვერდებს, პერსონალური მონაცემების გადაცემას შეიძლებოდა, ჰქონოდა ნეგატიური გავლენა მონაცემთა სუბიექტებზე (მაგალითად, აზარტულ თამაშებზე დამოკიდებულება). “CJEU”-მ შეაფასა მონაცემთა სუბიექტის მოლოდინი ფედერაციაში გასაწევრიანებლად წარდგენილი ინფორმაციის შემდგომში მესამე მხარისათვის მარკეტინგული მიზნებისთვის, თანხის გადახდის სანაცვლოდ გადაცემასთან დაკავშირებით.
სასამართლომ დაადგინა, რომ სავალდებულო არ არის, რომ ლეგიტიმური ინტერესი ეფუძნებოდეს სამართლებრივ ნორმას, თუმცა უნდა იყოს კანონიერი. ლეგიტიმური ინტერესი “GDPR”-ის მე-6 მუხლის პირველი პუნქტის “f” ქვეპუნქტთან იმ შემთხვევაში იქნება შესაბამისი, თუ სახეზეა მონაცემთა დამუშავების მწვავე საჭიროება და მონაცემთა სუბიექტის უფლებები და თავისუფლებები არ გადაწონის აღნიშნულს.

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.

ევროპის მართლმსაჯულების სასამართლოს გადაწყვეტილება მედიკამენტების შესყიდვასთან დაკავშირებული მონაცემების დამუშავების შესახებ

ევროპის მართლმსაჯულების სასამართლოს 2024 წლის 4 ოქტომბრის გადაწყვეტილების[1] თანახმად, მომხმარებელთა მიერ სააფთიაქო პროდუქციის შეკვეთისას მითითებული პერსონალური მონაცემები ჯანმრთელობის შესახებ ინფორმაციას წარმოადგენს. ამასთან, დამუშავებისთვის პასუხისმგებელი პირის კონკურენტ კომპანიებს უფლება აქვთ მიმართონ სასამართლოს მის მიერ მონაცემთა დამუშავებასთან დაკავშირებული დარღვევების, როგორც აკრძალული არაკეთილსინდისიერი კომერციული პრაქტიკის თაობაზე.

საქმის ფაქტობრივი გარემოებები:
გერმანული აფთიაქი, სახელწოდებით “Lindenapotheke”, ინტერნეტმაღაზიის, “Amazon”-ის საშუალებით ყიდდა ისეთ მედიკამენტებს, რომლებიც ურეცეპტოდ გაიცემა. “Lindenapotheke” ამუშავებდა მომხმარებელთა პერსონალურ მონაცემებს (სახელი, მისამართი, შეძენილი მედიკამენტი და სხვა საჭირო ინფორმაცია მედიკამენტის მომხმარებლის საჭიროებაზე მორგებისთვის) პერსონალიზებული სარეკლამო შეთავაზებების გაგზავნის მიზნით.

კონკურენტმა აფთიაქმა “Lindenapotheke”-ს წინააღმდეგ გერმანიის რეგიონულ სასამართლოში შეიტანა სარჩელი, რომლის თანახმადაც კომპანია უკანონოდ, მონაცემთა სუბიექტების თანხმობის გარეშე, ამუშავებდა მომხმარებელთა პერსონალურ მონაცემებს პირდაპირი მარკეტინგის მიზნებისთვის. მოსარჩელე ითხოვდა “Lindenapotheke”-ს მიერ მედიკამენტების პლატფორმა Amazon-ზე გაყიდვის შეწყვეტას.

განსაკუთრებული კატეგორიის მონაცემთა დამუშავებისათვის მკაფიოდ გამოხატული თანხმობის მიღების აუცილებლობა:

ჯანმრთელობის შესახებ მონაცემების, როგორც განსაკუთრებული კატეგორიის მონაცემთა დამუშავება ევროპის მონაცემთა დაცვის ძირითადი რეგულაციის მე-9 მუხლის შესაბამისად, მონაცემთა სუბიექტების მიერ გაცემული თანხმობის მაღალ სტანდარტს საჭიროებს. რეგიონულმა სასამართლომ დაადგინა, რომ, განსაკუთრებული კატეგორიის პერსონალური მონაცემების მარკეტინგული მიზნით დამუშავებისათვის აფთიაქს უნდა მოეპოვებინა მომხმარებელთა თანხმობა მონაცემთა ამგვარ დამუშავებაზე.

მარკეტინგი და ინფორმაცია ჯანმრთელობის შესახებ:
პერსონალურ მონაცემთა დამუშავება მარკეტინგის მიზნებისათვის, მათ შორის, მომხმარებელთა „პროფაილინგისთვის“, ნებადართულია მხოლოდ მონაცემთა სუბიექტის მიერ ინფორმირებული, კონკრეტული და აშკარა თანხმობის გამოხატვის შემდგომ. ჯანმრთელობასთან დაკავშირებული მონაცემების შემთხვევაში, მონაცემთა სუბიექტის თანხმობა უნდა იყოს თავისუფლად გაცემული, კონკრეტული, ინფორმირებული და მკაფიო. ასეთად, არ უნდა მივიჩნიოთ მომხმარებლის მიერ მომსახურების ზოგად პირობებზე დათანხმება, უმოქმედობა თუ წინასწარ მონიშნული თანხმობის გრაფა.

წინამდებარე საქმის გერმანიის რეგიონულ *(Oberlandesgericht Naumburg – OLG Naumburg)* და ფედერალურ სასამართლოებში *(*Bundesgerichtshof - BGH*)* განხილვის შემდგომ, *BGH*-მა ევროპის მართლმსაჯულების სასამართლოს *(CJEU)* ევროპის მონაცემთა დაცვის ძირითადი რეგულაციის მოქმედების თაობაზე წინასწარი შეკითხვებით *(preliminary questions)* მიმართა.
მართლმსაჯულების სასამართლოს უნდა შეეფასებინა *:*

1. მიიჩნევა თუ არა ონლაინ აფთიაქის მომხმარებლის სააფთიაქო შეკვეთებთან დაკავშირებული ინფორმაცია ჯანმრთელობის შესახებ ინფორმაციას *GDPR*-ის მე-*9 (1)* მუხლის შესაბამისად. აღნიშნულ საკითხზე მსჯელობისას სასამართლომ შეაფასა რამდენად იყო შესაძლებელი აფთიაქის მიერ დამუშავებული ინფორმაციის საფუძველზე მონაცემთა სუბიექტის ჯანმრთელობაზე დასკვნების გაკეთება.
2. მონაცემთა დაცვის ძირითადი რეგულაციისა და კონკურენციის სამართლის ურთიერთქმედების საკითხი. კერძოდ, სასამართლომ განიხილა დაშვებულია თუ არა კონკურენტი კომპანიის წინააღმდეგ მონაცემთა დაცვის კანონმდებლობის დარღვევების, როგორც არაკეთილსინდისიერი კომერციული პრაქტიკის, თაობაზე სასამართლოში სარჩელის შეტანა.

რა ითვლება ჯანმრთელობის შესახებ ინფორმაციად*:*
სასამართლოს მსჯელობის თანახმად, თუ მედიკამენტების შესყიდვასთან დაკავშირებული მონაცემები შეიძლება გამოყენებულ იქნას იდენტიფიცირებული ან იდენტიფიცირებადი ფიზიკური პირის ჯანმრთელობის მდგომარეობის თაობაზე დასკვნების გამოსატანად, *GDPR*-ის შესაბამისად, იგი მიიჩნევა ჯანმრთელობის შესახებ განსაკუთრებული კატეგორიის მონაცემებად.

მართლმსაჯულების სასამართლომ აღნიშნა, რომ „სამედიცინო მონაცემი“ ფართოდ განიმარტება - მონაცემის სიზუსტის, დამუშავებაზე პასუხისმგებელი პირის ვინაობის და მისი დამუშავების მიზნის მიუხედავად. ინტერნეტმაღაზიისთვის მედიკამენტების შესყიდვის მიზნით მიწოდებული ინფორმაციის საფუძველზე შესაძლოა გაკეთდეს დასკვნა მომხმარებლის *(*მონაცემთა სუბიექტის*)* ჯანმრთელობის მდგომარეობის შესახებ, მიუხედავად მომხმარებლის მიერ მიწოდებული ინფორმაციის სისწორისა. სასამართლომ გადაწყვიტა, რომ მნიშვნელობა არ აქვს შეძენილი მედიკამენტის ტიპს, ასევე, საჭიროებს თუ არა მისი შეძენა ექიმის დანიშნულებას, რადგან მხოლოდ მედიკამენტების შესყიდვების შესახებ ინფორმაციის საფუძველზე შესაძლებელია მონაცემთა სუბიექტის ჯანმრთელობის მდგომარეობის შესახებ დასკვნის გაკეთება. სასამართლოს მსჯელობის თანახმად, მედიკამენტის შესყიდვასთან დაკავშირებული მონაცემები განსაკუთრებული კატეგორიის პერსონალური მონაცემებია.

კონკურენციის სამართლისა და *GDPR*-ის ურთიერთმიმართება*:*[2]
CJEU-მ განიხილა კონკურენციის კანონმდებლობისა და მონაცემთა დაცვის რეგულაციების ურთიერთდამოკიდებულების საკითხი. სასამართლომ დაადგინა, რომ დამუშავებისთვის პასუხისმგებელი პირის წინააღმდეგ მონაცემთა დაცვის რეგულაციების დარღვევისთვის სასამართლოში სარჩელის შეტანის უფლებამოსილება არა მხოლოდ საზედამხედველო ორგანოებს, არამედ კონკურენტ კომპანიებსაც გააჩნიათ, თუ ეს ეროვნული კონკურენციის სამართლით აკრძალული არაა. სასამართლოს მიერ მიღებული გადაწყვეტილება მნიშვნელოვანია, ვინაიდან იგი წარმოადგენს პრეცედენტს, რომლის საფუძველზეც კომპანიები უფლებამოსილნი არიან მონაცემთა დაცვის კანონმდებლობის დარღვევების საფუძველზე სასამართლოს კონკურენტი კომპანიის წინააღმდეგ მიმართონ.[3]

გადაწყვეტილების მნიშვნელობა:
გადაწყვეტილება აქტუალურია არა მხოლოდ სააფთიაქო ბიზნესებისათვის, არამედ ნებისმიერი ორგანიზაციისთვის, რომელიც ჯანმრთელობის შესახებ მონაცემებს მარკეტინგული მიზნებისათვის ამუშავებს.

- ჯანმრთელობის შესახებ მონაცემთა დამუშავებისას, განსაკუთრებით, მარკეტინგული მიზნებისათვის, საჭიროა მონაცემთა სუბიექტების თანხმობა, რომელიც შესაბამისობაში უნდა იყოს მონაცემთა დაცვის ძირითადი რეგულაციის მიერ დაწესებულ თანხმობის კრიტერიუმებთან;
- კომპანიების უფლება აქვთ მიმართონ სასამართლოს კონკურენტი კომპანიის წინააღმდეგ, მონაცემთა დამუშავებასთან დაკავშირებული დარღვევების საფუძვლით;
- თუ ინფორმაციის საფუძველზე შესაძლოა მონაცემთა სუბიექტის ჯანმრთელობის შესახებ დასკვნის გამოტანა, აღნიშნული ჯანმრთელობის შესახებ ინფორმაციას წარმოადგენს.

„მონაცემთა დაცვის ევროპული საბჭოს“ (“EDPB") მოსაზრება მონაცემთა დამუშავებისთვის პასუხისმგებელი პირისა და დამუშავებისთვის პასუხისმგებელი პირის ქვე-დამმუშავებლის (“Sub-Processor”) ვალდებულებების შესახებ

2024 წლის 7 ოქტომბერს „მონაცემთა დაცვის ევროპულმა საბჭომ“ გამოაქვეყნა მოსაზრება[1] მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის და დამუშავებისთვის პასუხისმგებელი პირის ქვე-კონტრაქტორის ან ქვე-დამმუშავებლის (“Sub-Processor”) შესახებ.

საბჭოს მოსაზრება შეეხება მონაცემთა დამუშავებისთვის პასუხისმგებელ პირსა და მის თანა-დამმუშავებელთან, აგრეთვე ქვე-დამმუშავებელთან ურთიერთობების საკითხებს.
ქვე-კონტრაქტორი ან ქვე-დამმუშავებელი დამუშავებაზე უფლებამოსილი პირის დავალების მიხედვით მოქმედი პირია,[2] რომელიც პერსონალურ მონაცემებს ამუშავებს დამუშავებაზე უფლებამოსილი პირისათვის. ქვე-დამმუშავებელი შეიძლება იყოს იურიდიული პირი, მაგალითად, მცირე და საშუალო ბიზნესი, საჯარო დაწესებულება, სააგენტო ან სხვა ორგანო.

[1]GDPR-ის64(2) მუხლის საფუძველზე, ნებისმიერ საზედამხედველო ორგანოს აქვს უფლებამოსილება თხოვნით მიმართოს საბჭოს მისთვის საინტერესო და საჭირო თემატიკაზე მოსაზრების გამოცემის შესახებ, ისეთ საკითხებთან მიმართებით, რომელიც აქტუალურია ერთზე მეტ სახელმწიფოში მაინც.
[2] What is a data Controller, https://www.edpb.europa.eu/sme-data-protection-guide/data-controller-data-processor_en.

ქვე-დამმუშავებლის დანიშვნა:

ქვე-დამმუშავებლის დასანიშნად აუცილებელი წინაპირობაა წერილობითი თანხმობა, რომელიც გაიცემა მონაცემთა დამუშავებისთვის უფლებამოსილი პირის ან თანა-დამმუშავებლის მიერ. დამუშავებისთვის პასუხისმგებელმა პირმა უნდა შეადგინოს ხელშეკრულება ქვე-დამმუშავებელთან, რომლითაც განისაზღვრება ქვე-დამმუშავებელის ვალდებულებები.
წინამდებარე ხელშეკრულება დამუშავებაზე უფლებამოსილ პირსა და ქვე-დამმუშავებელს შორის უნდა უზრუნველყოფდეს მონაცემთა სუბიექტების უფლებების დაცვის იგივე ხარისხს, რაც უზრუნველყოფილია მონაცემთა დამუშავებისთვის უფლებამოსილ პირსა და დამუშავებაზე პასუხისმგებელ პირს შორის არსებული ხელშეკრულებით.

საბჭოს მიერ მომზადებულ სარეკომენდაციო ხასიათის დოკუმენტში განხილულია სხვადასხვა შემთხვევა, როდესაც საჭიროა დამუშავებისთვის პასუხისმგებელი პირის გარკვეული უფლებებისა და მოვალეობების განმარტების საკითხი, აგრეთვე, მხარეთა შორის დასადები ხელშეკრულების ტექსტის შედგენის საკითხი.[1]
საბჭოს მოსაზრება შეიცავს პრაქტიკულ ინფორმაციას მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის ვალდებულებების შესახებ.

საკონტაქტო ინფორმაციის შენახვის ვალდებულება:

მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს, უნდა ჰქონდეს ყველა დამუშავებაზე უფლებამოსილი პირისა და ქვე-დამმუშავებელის შესახებ ინფორმაცია (მაგალითად, სახელი, მისამართი, საკონტაქტო პირის ვინაობა). [2]

უსაფრთხოების გარანტიებთან შესაბამისობის შემოწმების ვალდებულება:
დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, გადაამოწმოს დამუშავებაზე უფლებამოსილი პირის და ქვე-დამმუშავებლის მიერ მონაცემთა უსაფრთხოების დაცვის სათანადო გარანტიებთან შესაბამისობის საკითხი.

გადამოწმების ვალდებულება წარმოიშვება განუსაზღვრელად იმისა, აყენებს თუ არა დამუშავების პროცესი მონაცემთა სუბიექტების უფლებებს და თავისუფლებებს მაღალი რისკის ქვეშ.

მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი, როგორც გადაწყვეტილების მიმღები პირი:
დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, მიაღწიოს შეთანხმებას ქვე-დამმუშავებელთან „უსაფრთხოების დაცვის სათანადო გარანტიების“ შესახებ, თუმცა, წინამდებარე საკითხებზე საბოლოო გადაწყვეტილებების მიღების ვალდებულება და მისგან მომდინარე პასუხისმგებლობები ქვე-დამმუშავებელთან თანამშრომლობის თვალსაზრისით, კვლავ მონაცემთა დამუშავებისთვის უფლებამოსილი პირის (და არა დამუშავებაზე პასუხისმგებელი პირის) ვალდებულების ნაწილში ექცევა.

საბჭოს მოსაზრებით, ევროპის „მონაცემთა დაცვის ძირითადი რეგულაცია“ არ ავალდებულებს მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს სისტემატიურად მოითხოვოს ხელშეკრულებების ასლები, რათა შეამოწმოს, თუ რამდენად გაითვალისწინეს მასთან თანამშრომლობაში მყოფმა ქვე-დამმუშავებლებმა მონაცემთა დაცვის შესაბამისი კანონმდებლობის მიერ განსაზღვრული ვალდებულებები.

მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა უნდა შეაფასოს, სიტუაციიდან გამომდინარე, საჭიროა თუ არა ხელშეკრულებების ასლების მოთხოვნა და გაცნობა, რათა შეძლოს ევროპის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მოთხოვნებთან შესაბამისობის უზრუნველყოფა უფლებამოსილი პირებისა და საზედამხედველო ორგანო(ები)სათვის.

ვალდებულებები მონაცემთა საერთაშორისო გადაცემასთან მიმართებით:
თუ ქვე-დამმუშავებელი პერსონალურ მონაცემებს ევროპის ეკონომიკური სივრცის გარეთ გადასცემს, დამუშავებისთვის პასუხისმგებელმა პირმა უნდა მოამზადოს შესაბამისი დოკუმენტი, სადაც გადაცემის შესახებ ყველა საკითხი დეტალურად იქნება გათვალისწინებული.

მონაცემთა გადაცემის შესახებ დოკუმენტში საჭიროა აღიწეროს მონაცემთა გადაცემის ფორმა, გადაცემის მონაცემთა სუბიექტების უფლებებზე ზეგავლენის შეფასება და მონაცემთა უსაფრთხოების უზრუნველსაყოფად განხორციელებული ზომების შესახებ ინფორმაცია.[
ამავდროულად, მონაცემთა დაცვის საზედამხედველო ორგანოს მოთხოვნის საფუძველზე, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, ადაადასტუროს მონაცემთა დაცვის სათანადო გარანტიებთან შესაბამისობა.[2] მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა აღნიშნული დოკუმენტი, მოთხოვნისამებრ, უნდა მიაწოდოს საზედამხედველო ორგანოს.

ევროპის მონაცემთა დაცვის საბჭოს („EDPB”) გზამკვლევის პროექტი „მონაცემთა დამუშავების ლეგიტიმურ ინტერესის შესახებ“

2024 წლის 7 ოქტომბერს „ევროპის მონაცემთა დაცვის საბჭომ“ გამოსცა რეკომენდაციის პროექტი[1] მონაცემთა დამუშავების ლეგიტიმურ ინტერესთან დაკავშირებით.
პროექტის თანახმად, მონაცემთა დამუშავებისთვის პასუხისმგებელი პირების მიერ მონაცემთა კანონიერების ფარგლებში, დასამუშავებლად აუცილებელია შესაბამისი სამართლებრივი საფუძვლის არსებობა.ლეგიტიმური ინტერესი კი ერთ-ერთ სამართლებრივ საფუძველს წარმოადგენს. შესაბამისად, გზამკვლევის პროექტი ეხება დამუშავებისთვის პასუხისმგებელ პირების მიერ ლეგიტიმური ინტერესის საფუძველზე მონაცემთა დამუშავებას.

ინტერესის ლეგიტიმურობის შესახებ:
ლეგიტიმურად შესაძლოა მიჩნეულ იქნას მხოლოდ კანონიერი ინტერესი, რომელიც ჩამოყალიბებულია ნათლად და გარკვევით, არის რეალური და ამჟამინდელი, რეალურ დროში არსებული. მაგალითად, კომპანიას, რომელიც მონაცემთა დამუშავებისთვის პასუხისმგებელი პირია და მონაცემთა სუბიექტს მომსახურებას უწევს შესაძლოა ჰქონდეს მონაცემთა სუბიექტის პერსონალური მონაცემების დამუშავების ლეგიტიმური ინტერესი.

მონაცემთა დამუშავების „აუცილებლობის“ სტანდარტი:
თუ მონაცემთა დამუშავების მიზნის მიღწევა შესაძლებელია სხვა უფრო ადეკვატური და ეფექტიანი ალტერნატივის მეშვეობით, დამუშავება ვერ მიიჩნევა აუცილებელ მეთოდად. დამუშავების აუცილებლობის სტანდარტი უნდა შეფასდეს მონაცემთა მინიმიზაციის პრინციპის გათვალისწინებით.

ინტერესთა ურთიერთბალანსი:
დაუშვებელია დამუშავებისთვის პასუხისმგებელი პირის იმგვარი ლეგიტიმური ინტერესით პერსონალური მონაცემების დამუშავება, რომელიც ხელყოფს მონაცემთა სუბიექტის უფლებებსა და თავისუფლებებს. ლეგიტიმური ინტერესის განსაზღვრისას მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია გაითვალისწინოს მონაცემთა სუბიექტის გონივრული მოლოდინები და უზრუნველყოს დამუშავების რისკთან შესაბამისი მონაცემთა უსაფრთხოების ზომების გატარება.

რეკომენდაცია მიმოიხილავს მონაცემთა დამუშავებისთვის პასუხისმგებელი პირების მიერ მონაცემთა დამუშავების ლეგიტიმური ინტერესის არსებობის შეფასების საკითხს. კერძოდ, რეკომენდაციებში წარმოდგენილია მონაცემთა დამუშავების სხვადასხვა კონტექსტი და მიზანი, როგორიცაა: თაღლითობის პრევენცია, პირდაპირი მარკეტინგი და ინფორმაციის უსაფრთხოება. დოკუმენტი, განიხილავს კავშირს მონაცემთა დამუშავების სამართლებრივ საფუძველსა და ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციით“ გათვალისწინებულ მონაცემთა სუბიექტის უფლებებს შორის.

მონაცემთა ლეგიტიმური დამუშავების განმსაზღვრელი კრიტერიუმები:
რეკომენდაციებში წარმოდგენილია მონაცემთა დაცვის კანონიერად, ლეგიტიმური ინტერესის საფუძველზე დამუშავების კრიტერიუმების[1] ანალიზი.[2]იმისათვის, რომ მონაცემთა დამუშავების სამართლებრივ საფუძველად ლეგიტიმური ინტერესი ჩაითვალოს, ერთდოულად უნდა დაკმაყოფილდეს შემდეგი სამი ძირითადი პირობა:

1.პერსონალურ მონაცემთა დამუშავების ლეგიტიმური ინტერესის არსებობა;
2.მონაცემთა დამუშავების ინტერესის მკაფიოდ და გარკვევით ჩამოყალიბება;
3.დამუშავების ინტერესის რეალურ დროში არსებობა.

პირობა I. მონაცემთა დამუშავების ლეგიტიმური ინტერესის არსებობა:
უპირველეს ყოვლისა, მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი უნდა დარწმუნდეს, რომ მისი ინტერესი „ლეგიტიმურია“. აქვე, უნდა აღინიშნოს, რომ არ არსებობს დამუშავების ლეგიტიმური ინტერესების ამოწურვადი ჩამონათვალი და „მონაცემთა დაცვის ძირითადი რეგულაცია“ ლეგიტიმური ინტერესის კონკრეტულ განმარტებას არ შეიცავს.
აგრეთვე, საგულისხმოა, რომ დამუშავებისთვის პასუხისმგებელი პირის ლეგიტიმური „ინტერესი“ მონაცემთა დამუშავებისათვის განსხვავდება მონაცემთა დამუშავების „მიზნისაგან“.[3] დამუშავებისთვის პასუხისმგებელ პირს, შესაძლოა ჰქონდეს მის მიერ წარმოებული პროდუქტის ან მომსახურეობის რეკლამირების ინტერესი, რაც შესაძლოა, პირდაპირი მარკეტინგის მიზნით მონაცემთა დამუშავების გზით განხორციელდეს.

GDPR-ის, აგრეთვე, ევროპის მართლმსაჯულების სასამართლოს პრაქტიკის ანალიზზე დაყრდნობით, ლეგიტიმური ინტერესების მაგალითებია:

·ინტერნეტში არსებულ ინფორმაციაზე ხელმისაწვდომობა;
·საჯარო ვებგვერდებზე წვდომა;
·ქონებრივი ზიანის მიმყენებელი პირის მონაცემებზე წვდომა, ზიანის ანაზღაურების მიზნით.
·მაცხოვრებელთა უძრავი ქონების, ჯანმრთელობის და სიცოცხლის დაცვის ინტერესი;
·პროდუქტის გაუმჯობესების ინტერესი, მონაცემთა სუბიექტების კრედიტის გადახდის უნარიანობის შემოწმება, და სხვა.

პირობა II. კანონიერია, ჩამოყალიბებულია „ნათლად“ და „გარკვევით“:
ლეგიტიმურად მიიჩნევა ინტერესი, რომელიც კანონიერია, ჩამოყალიბებულია ნათლად და გარკვევით, არის რეალური და ამჟამინდელი (ახლანდელ დროში არსებული). მაგალითად, მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს, როგორც მომსახურების გამწევს, უნდა გააჩნდეს მონაცემთა დამუშავების ლეგიტიმური ინტერესი.

„კანონიერების“ კრიტერიუმი მაგალითი:
კრიტერიუმი მაგალიბამესის საფუხელწოდებაელექტრო სიგარეტის მწარმოებელ ევროპულ კომპანიას სურს წარმოებული პროდუქციის რეკლამირება, რისთვისაც ესაჭიროება, ევროპაში მცხოვრებ მომხმარებლებთან სარეკლამო შეტყობინებების გაგზავნა. აღნიშნული მიზნის განსახორციელებლად, იგი ამუშავებს მომხმარებელთა პერსონალურ მონაცემებს. პირდაპირი მარკეტინგის მიზნებისათვის პერსონალურ მონაცემთა დამუშავების ინტერესი შესაძლოა, ზოგიერთ შემთხვევაში, მონაცემთა დამუშავების ლეგიტიმურ ინტერესად ჩაითვალოს, თუმცა აუცილებელია მონაცემთა დამუშავების კონტექსტის გათვალისწინება.

მოცემულ შემთხვევაში, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, შეამოწმოს მონაცემთა კონკრეტული მიზნით დამუშავების კანონიერება. იმის გათვალისწინებით, რომ ევროკავშირში აკრძალულია ელექტრო სიგარეტის რეკლამა, ევროპული თამბაქოს დირექტივის და მასთან ასოცირებული კანონმდებლობის საფუძველზე, კომპანიას ვერ ექნება ლეგიტიმური ინტერესი პერსონალურ მონაცემთა დამუშავებისათვის, მონაცემთა დამუშავების „კანონიერების ელემენტის“ არარსებობის გამო.

პირობა III. „ნათლად“ და „გარკვევით“ ჩამოყალიბების კრიტერიუმის მაგალითი:
ორგანიზაციას „სამეზობლოს მცველები“ წევრებმა გადაწყვიტეს, რომ სამეზობლოში განათავსონ ვიდეო მეთვალყურეობის სისტემა, საცხოვრებელ პერიმეტრზე პოტენციური კრიმინალური ქმედებების კონტროლის მიზნით.

მიუხედავად იმისა, რომ შესაძლოა ლეგიტიმურ ინტერესად იქნას მიჩნეული ქონების, ჯანმრთელობის და სიცოცხლის დაცვა, ამ კონკრეტულ შემთხვევაში, მეთვალყურეობის სისტემის დასაყენებლად ხსენებული მიზეზი მეტად ზოგადია და არ მიუთითებს კონკრეტული უსაფრთხოების პრობლემაზე, რის საპასუხოდაც პროპორციული იქნებოდა მეთვალყურეობის სისტემის განთავსება. შესაბამისად, ორგანიზაციის ინტერესი ვერ აკმაყოფილებს სამ საფეხურიანი შეფასების კრიტერიუმს.

პირობა III. „რეალურ დროში არსებული“ კრიტერიუმის მაგალითი:
გაზეთის მენეჯმენტს სურს შექმნას მონაცემთა ბაზა, რომელშიც გაერთიანდება ინფორმაცია იმ გამომწერთა შესახებ, რომელთაც შესაბამისი ვადის ამოწურვის შემდგომ, არ მოისურვეს გაზეთის ხელახალი გამოწერა. მონაცემთა ბაზის შექმნის საჭიროებას გაზეთის მენეჯმენტი იმ არგუმენტით ასაბუთებს, რომ მომავალში, ახალი გაზეთის გამოცემის შემთხვევაში, პრაქტიკული იქნება ძველი გამომწერების შესახებ ინფორმაციაზე წვდომა. საგულისხმოა, რომ ახალი გაზეთის ჩამოყალიბების იდეა მხოლოდ ჰიპოთეტური ფორმით არსებობს. მოცემულ შემთხვევაში, მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის ინტერესი ვერ იქნება აღქმული როგორც „რეალური და ამჟამინდელი“ ინტერესი, ვინაიდან ახალი გაზეთის შექმნის საკითხი მხოლოდ სავარაუდოა. აქედან გამომდინარე, მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის ინტერესი ლეგიტიმურად ვერ იქნება მიჩნეული.

რეკომენდაციის პრაქტიკული დანიშნულება:
რეკომენდაცია მონაცემთა დამუშავებისთვის პასუხისმგებელ პირებს დაეხმარება ლეგიტიმური ინტერესის საფუძველზე პერსონალური მონაცემების კანონიერად დამუშავებაში.
დამუშავებისთვის პასუხისმგებელი პირები, რეკომენდაციის საშუალებით, დეტალურად გაეცნობიან იმ პირობებსა და კრიტერიუმებს, რომელთა გათვალისწინება და დაკმაყოფილება აუცილებელია პერსონალურ მონაცემთა ლეგიტიმური ინტერესის საფუძველზე დასამუშავებლად.

ნორვეგიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება აგდერის უნივერსიტეტის დაჯარიმების შესახებ

ნორვეგიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანომ აგდერის უნივერსიტეტი დააჯარიმა თანამშრომელთა მიერ ინფორმაციაზე წვდომის შეზღუდვის ვალდებულებისა და მონაცემთა უსაფრთხოების წესების დაუცველობისათვის.

დაჯარიმების საფუძველი:
2024 წლის თებერვალში, აგდერის უნივერსიტეტის თანამშრომელმა აღმოაჩინა, რომ სისტემატურად ირღვეოდა პერსონალურ მონაცემთა შემცველი დოკუმენტების შენახვის წესი. პერსონალურ მონაცემთა შემცველი დოკუმენტები “Microsoft Teams”-ის პლატფორმაზე (საქაღალდეებში) ინახებოდა და მასზე წვდომა განურჩევლად საჭიროებისა. ყველა თანამშრომელს ჰქონდა.[1] მონაცემთა უსაფრთხოების დარღვევა იყო დენადი ხასიათის, 2018 წლის აგვისტოდან მოყოლებული (როდესაც უნივერსიტეტის თანამშრომლებმა პროგრამა Microsoft Teams-ის გამოყენება დაიწყეს) 2024 წლის თებერვლამდე პერიოდს მოიცავდა.

საზედამხედველო ორგანოს მთავარი მიგნებები:
2018 წლის აგვისტოდან 2024 წლის თებერვლამდე, თანამშრომელთათვის “Microsoft Teams”-ის სისტემაში, კერძოდ, საქაღალდეებში, თანამშრომლების, სტუდენტების და გარეშე პირების პერსონალური მონაცემების შემცველი ინფორმაცია ღიად იყო ხელმისაწვდომი, და თანამშრომლებს მასზე წვდომამარტივად, პროგრამა “Microsoft Teams”-ის საქაღალდეებში საძიებო ფუნქციის გამოყენებით ჰქონდათ.

ინფორმაციული უსაფრთხოების აღნიშნული დარღვევა შეეხო 16 000 მონაცემთა სუბიექტის პერსონალურ მონაცემებს, კერძოდ: სახელებს, საიდენტიფიკაციო ნომრებს, სხვადასხვა სტუდენტის საჭიროებაზე მორგებული (ადაპტირებული) გამოცდების შესახებ ინფორმაციას; ინფორმაციას დამატებით გამოცდაზე სტუდენტის გასვლის შესახებ და რა სპეციალური ღონისძიებები ან/და მოწყობილობები იქნა გამოყენებული გამოცდის პროცესში ზოგიერთი სტუდენტის განსაკუთრებული საჭიროებების დაკმაყოფილებისათვის.

მონაცემთა უსაფრთხოების დარღვევა შეეხოთ ასევე უნივერსიტეტთან ასოცირებული, ლტოლვილის სტატუსის მქონე პირების შესახებ ინფორმაციასაც, რაც მოიცავდა მათ საკონტაქტო ინფორმაციას, ასევე, მონაცემებს მათი განათლების და ნორვეგიაში ცხოვრების უფლების შესახებ.

მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილება:
ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ დარღვევის გამო, კერძოდ, პერსონალურ მონაცემთა უსაფრთხოების ზომების დაუცველობისათვის, ნორვეგიის მონაცემთა დაცვის საზედამხედველო ორგანომ მიიღო გადაწყვეტილება აგდერის უნივერსიტეტის 12 700 ევროს ოდენობით დაჯარიმების შესახებ.

საზედამხედველო ორგანოს შეფასების თანახმად, უნივერსიტეტს ჰქონდა ვალდებულება დაეცვა პერსონალურ მონაცემთა შემცველი ინფორმაციის უსაფრთხოება, კერძოდ, უზრუნველეყო მისი დაცვა არაავტორიზებული წვდომისაგან. აღნიშნულ ინფორმაციაზე წვდომის განხორციელება შესაძლებელი უნდა ყოფილიყო მხოლოდ იმ თანამშრომლებისათვის, რომელთაც ეს აუცილებლად სჭირდებოდათ მათზე დაკისრეული სამუშაოს შესასრულებლად. თანამშრომლებს უნდა ჰქონოდათ წვდომა ინფორმაციაზე მხოლოდ იმ მოცულობით, რაც აუცილებელი იყო მათზე დაკისრებული კონკრეტული სამუშაოს შესრულებისთვის, მონაცემთა მინიმიზაციის პრინციპის გათვალისწინებით.

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