ივა კატიჩი*

მონაცემთა დაცვის ოფიცერი — „მონაცემთა დაცვის ძირითადი რეგულაციით“ განსაზღვრულ ამოცანებთან დაკავშირებული დარღვევების პრევენციის მექანიზმი

მონაცემთა დაცვის ოფიცრის მოთხოვნები დამატებით ტვირთს წარმოადგენს გუნდური სამუშაოებისთვის, რაც მონაცემთა დაცვის ოფიცრის სამუშაოს უკიდურესად ერთპიროვნულს ხდის. ამ პოზიციის ძირითადი არსი მდგომარეობს ყურადღების ფოკუსირებაში შიდა ორგანიზაციულ საკითხებზე, რათა არ მოხდეს მონაცემთა დაცვის კანონების დარღვევა, რაც ამ პოზიციას უკიდურესად დიდ პასუხისმგებლობას აკისრებს. სწორედ ზემოთ ხსენებულთან დაკავშირებით შეიძლება ითქვას, რომ ამოცანების ბუნებიდან გამომდინარე, მონაცემთა დაცვის ოფიცრებს შეუძლიათ, პრევენციული ზეგავლენა მოახდინონ ორგანიზაციაზე რაიმე დარღვევასთან დაკავშირებით, და შესაბამისად, ადამიანის ფუნდამენტური უფლებებისადმი პატივისცემაზე, განსაკუთრებით, პირად მონაცემთა დაცვის უფლებაზე.

საკვანძო სიტყვები: *მონაცემთა დაცვის ოფიცერი, პირად მონაცემთა დაცვა, დარღვევების პრევენცია.*

1. შესავალი

პერსონალური მონაცემები ყველგანაა. მართებულია, რომ კომპანიები კარგად დაფიქრდნენ მაშინაც კი, როცა ინფორმაცია ერთი შეხედვით არ კვალიფიცირდება როგორც პერსონალური მონაცემი.

სახელი, დაბადების თარიღი, სახლის და ელექტრონული მისამართი, ინტერნეტ პროტოკოლის (IP) მისამართი, პირადობის (ID) ნომერი, ჯანმრთელობის ცნობები, როგორიცაა ფიზიკური პირის დიოპტრიკა, თითის ანაბეჭდები, მანქანის რეგისტრაციის ნომერი, ფოტოსურათი და ბევრი სხვა სახის ინფორმაცია წარმოადგენს პირად მონაცემებს.

ევროპული კანონის მე-8 მუხლის შესაბამისად, პერსონალური მონაცემთა დაცვა აღიარებულია როგორც ადამიანის ცალკეული ფუნდამენტური უფლება ევროკავშირის ფუნდამენტურ უფლებათა ქარტიის მიხედვით.

---

* ზაგრების უნივერსიტეტის სამართლის მაგისტრი (LL.M.); ხორვატიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს — “Agencija za zaštitu osobnih podataka” სამდივნო.

„პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვისა და ასეთი მონაცემების თავისუფალი მიმოცვლის შესახებ“ ევროპარლამენტისა და საბჭოს 2016 წლის 27 აპრილის 2016/679 (EU) რეგულაცია („მონაცემთა დაცვის ძირითადი რეგულაცია“; შემდგომში GDPR), რომელიც აუქმებს 95/46/EC დირექტივას, ძალაში შესვლამდე პერსონალურ მონაცემთა დაცვის ძირითად სამართლებრივ დოკუმენტს წარმოადგენდა პერსონალურ მონაცემთა დაცვის დირექტივა.[1]

თუმცა, თანამედროვე ტექნოლოგიის განვითარების გამო საჭირო გახდა კანონმდებლობის რეფორმირება, რათა სამართლებრივმა ბაზამ შეძლოს შედარებით ეფექტურად გააკონტროლოს პერსონალურ მონაცემთა დამუშავება ციფრულ საუკუნეში.

ამის გამო, მონაცემთა დაცვის ძირითადი რეგულაცია ძალაში შევიდა როგორც ტექნოლოგიურად ნეიტრალური რეგულაცია, რომელიც გახდა პერსონალურ მონაცემთა დაცვის პიონერი და მისაბაძი მოდელი გლობალური მასშტაბით.

ხუთზე მეტი წლის წინ, მონაცემთა დაცვის ძირითადმა რეგულაციამ გამოიწვია დიდი საზოგადოებრივი ინტერესი და აიძულა ბევრი სუბიექტი, რომ რენტგენზე გაეტარებინათ თავიანთი ორგანიზაციები.

მონაცემთა დაცვის კანონმდებლობის შესასრულებლად მონაცემთა დამმუშავებელს განვითარებული უნდა ჰქონდეს კანონით გათვალისწინებული ყველა დავალების შესრულების უნარი.

ბოლო წლებში, ცხადი გახდა, რამდენად ღირებულია ორგანიზაციისათვის მონაცემთა დაცვის ოფიცრის როლი.

განსაკუთრებით რეკომენდებულია დაინიშნოს ორგანიზაციაში მონაცემთა დაცვის ოფიცერი, რომელსაც შეუძლია, ძლიერი პრევენციული ზეგავლენა მოახდინოს ორგანიზაციაზე, სადაც იგი მუშაობს.

მონაცემთა დაცვის სათანადო ოფიცრის დანიშვნას შეუძლია, შეამციროს პერსონალურ მონაცემების უსაფრთხოებასთან დაკავშირებული დარღვევებისა და არაკანონიერი წვდომის შესაძლებლობები.

2. მონაცემთა დაცვის ოფიცრის როლის პრევენციული გავლენა ორგანიზაციაში

წარმოვიდგინოთ მონაცემთა სუბიექტის საჩივარი კომპანიის წინააღმდეგ, მონაცემთა სუბიექტის პერსონალური მონაცემების კომპანიის ვებგვერდზე განთავსების გამო.

გამოქვეყნებული მონაცემები შეიცავდა სუბიექტის ავტომანქანის იდენტიფიკაციის ნომერს (შასის ნომერი), ზოგად ინფორმაციას ავტომობილის შესახებ და მონაცემებს მისი დაზიანების შესახებ კონკრეტული ნომრის მიხედვით.

ერთი შეხედვით, ჩვეულებრივ ფიზიკური პირი განაცხადებდა, რომ გამოქვეყნებული ინფორმაცია არ წარმოადგენს პერსონალურ მონაცემებს, თუმცა შასის ნომრის რამდენიმე ვებგვერდზე შეყვანით, პიროვნებას შეუძლია, მიიღოს ინფორმაცია ტრანსპორტის შესახებ, როგორიცაა ძრავის ნიშნები, ფერის კოდი ან წარმოების თარიღი და სხვა.

[1] ევროპარლამენტისა და საბჭოს 1995 წლის 24 ოქტომბრის დირექტივა 95/46/EC „პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვისა და ასეთი მონაცემების თავისუფალ მიმოცვლასთან დაკავშირებით“.

თავდაპირველად, პიროვნებას არ შეუძლია გაიგოს ბევრი რამ ავტომანქანის მეპატრონის შესახებ, მაგრამ შასის ნომერი ტრანსპორტის მფლობელის თუნდაც ზუსტი ვინაობის გაგების საშუალებაა.

წარმოვიდგინოთ, რომ კომპანიამ არ დაინიშნა მონაცემთა დაცვის ოფიცერი და ამტკიცებს, რომ შასის ნომერი არ წარმოადგენს პერსონალურ მონაცემს.

როგორ შეასრულებს ეს კომპანია გამჭვირვალობის ვალდებულებას, რომელიც დადგენილია მონაცემთა დაცვის კანონით?

კომპანიაში ვინმეს უნდა განესაზღვრა შასის ნომერი, როგორც პერსონალური მონაცემი, დაედგინა დამუშავების სამართლებრივი ბაზა და დაეცვა გამჭვირვალობის ვალდებულება, რისთვისაც საჭიროა მონაცემთა დამუშავების სამართლებრივი ბაზის შესახებ ინფორმაციის შეტანა შეტყობინებაში პირადი ცხოვრების ხელშეუხებლობის შესახებ.

მონაცემთა დაცვის ძირითადი რეგულაციის მიხედვით, მონაცემთა სუბიექტი არის პირდაპირ ან არაპირდაპირ იდენტიფიცირებული ან იდენტიფიცირებადი ფიზიკური პირი. იდენტიფიკაციას ხელს უწყობენ გარკვეული ფაქტორები, რომლებიც დაკავშირებულია ფიზიკური პირის ფიზიკურ, ფიზიოლოგიურ, გენეტიკურ, გონებრივ, ეკონომიკურ, კულტურულ ან სოციალურ იდენტობასთან.[2]

ავტომანქანის მძღოლის ვინაობა შესაძლოა შემდგომში დადგინდეს დამატებითი ინფორმაციის საშუალებით, არაპირდაპირ, კონკრეტული პიროვნებისთვის დამახასიათებელი ერთი ან მეტი ფაქტორით, ფაქტებით ადგილმდებარეობის შესახებ და ა.შ. აქედან გამომდინარე, ტრანსპორტის შასის ნომერი შეიძლება მიჩნეული იყოს პერსონალური მონაცემად.

მონაცემთა დაცვის ოფიცერი (თუ დანიშნულია ან სათანადოდ არის შერჩეული) ამოიცნობდა კავშირს „შასის ნომრის“ მიღმა მყოფ პირთან და ეცოდინებოდა პერსონალური მონაცემების განმარტება. პერსონალური მონაცემების იდენტიფიკაციის შემდეგ მონაცემთა დაცვის ოფიცერი დაადგენდა სამართლებრივ ბაზას მონაცემთა დამუშავებისათვის გასაჯაროებამდე და შემდეგ, მონაცემთა მინიმიზაციის[3] პრინციპის შესაბამისად, გასცემდა რჩევას, რომ მხოლოდ საჭიროების შემთხვევაში გაესაჯაროებინათ პერსონალური მონაცემები და მიეწოდებინათ ინფორმაცია მონაცემთა სუბიექტისთვის ასეთი მონაცემების დამუშავების შესახებ.

მონაცემთა დაცვის ოფიცერი ან თანამშრომელია ან გარე ექსპერტი, რომელსაც გააჩნია მაღალი პროფესიონალური ეთიკა და ცოდნა მონაცემთა დაცვის კანონის შესახებ.

მონაცემთა დაცვის ოფიცერმა აუცილებლად უნდა იცოდეს ვალდებულებები, რომლებსაც მას აკისრებს მონაცემთა დაცვის კანონი და უნდა აკონტროლებდეს ევროპის ეკონომიკური სივრცის ფარგლებში ზედამხედველი ორგანოების მიერ და ევროპის კავშირის მართლმსაჯულების სასამართლოს მიერ მიღებულ გადაწყვეტილებებს, ზედამხედველი ორგანოების რეკომენდაციებსა და

[2] ევროპარლამენტისა და საბჭოს 2016 წლის 27 აპრილის რეგულაცია (EU)2016/679 „პერსონალურ მონაცემთა დამუშავებისას პიზიკურ პირთა დაცვისა და ასეთი მონაცემების მიმოცვლის შესახებ“, რომელიც აუქმებს დირექტივას 95/46/EC (მონაცემთა დაცვის ძირითადი რეგულაცია, მუხლი 4, პარაგრაფი 1).

[3] იქვე, მუხლი 5, პარ. 1.

შეხედულებებს და ასევე მონაცემთა დაცვის ევროპული საბჭოს სახელმძღვანელო მითითებებს.

მონაცემთა დაცვის ოფიცერი წარმოადგენს ერთგვარ ინსპექციას ორგანიზაციის ფარგლებში. ამიტომ, ძალიან მნიშვნელოვანია, რომ ის ფლობდეს ცოდნას ორგანიზაციის შიდა სტრუქტურის შესახებ. მონაცემთა დაცვის ოფიცრისთვის ნაცნობი უნდა იყოს ორგანიზაციის მიერ მართული პროცესები, ასევე მონაცემთა დამუშავების საშუალებები.

ფიზიკური პირი, რომელიც განიხილება როგორც ორგანიზაციის ინსპექტორი, უნდა შეეძლოს წარმატებული კომუნიკაციის წარმართვა სამთავრობო წარმომადგენელთან. მონაცემთა დაცვის ოფიცერს ნამდვილად მოუწევს შეეწინააღმდეგოს ისეთ იდეებს, რომლებიც კონფლიქტშია მონაცემთა დაცვის კანონთან. გარდა ამისა, ყველა ადამიანს არ შეუძლია კოლეგების გაკრიტიკება და პერსონალურ მონაცემთა დაცვის შესახებ კანონის დებულებების დაცვის მოთხოვნა.

პრაქტიკაში მთავარ პრობლემას წარმოადგენს არაკვალიფიციური პირის დანიშვნა, როდესაც მონაცემთა დაცვის ოფიცრის დანიშვნა ატარებს ფორმალურ ხასიათს, ორგანიზაციას იგი სარგებლობას ვერ მოუტანს.

2.1. საზედამხედველო ვალდებულების ზეგავლენა დარღვევების პრევენციაზე

მონაცემთა დაცვის ოფიცერი უნდა ასრულებდეს კონსულტანტის როლს. ორგანიზაციაში ახალი პროცედურის ან ტექნოლოგიის დანერგვისას მონაცემთა დაცვის ოფიცერი ჩართული უნდა იყოს პროექტში რათა შესაძლებელი იყოს პრევენციული ზემოქმედება იმ მექანიზმებზე, რომლებიც უსაფრთხოებასთან დაკავშირებული დარღვევებისა და არაკანონიერი წვდომის რისკის ქვეშ დააყენებს პერსონალურ მონაცემებს.

გადამწყვეტი მნიშვნელობა აქვს პროექტში დროულ ჩართვას. ახალი ტექნოლოგიის დამუშავების პროცესში, კარგი ექსპერტი მხედველობაში მიიღებს მონაცემთა დაცვას - მომსახურების შექმნის პროცესში (design) და პირველად პარამეტრად (default)[4] და გააერთიანებს უსაფრთხოების ზომებს როგორიცაა მონაცემის წაშლის შესაძლებლობა მისი შენახვის პერიოდის გასვლის შემდეგ, უზრუნველყოფს რომ პერსონალურ მონაცემებზე წვდომა შეიზღუდოს იმ პერსონალამდე, რომელმაც უნდა შეასრულოს ამ პერსონალური მონაცემებით კონკრეტული დავალება და მხოლოდ იმ კონკრეტული ტიპის პერსონალურ მონაცემებამდე, რომლის ცოდნაც საჭიროა ამ დავალების შესასრულებლად, ასევე უზრუნველყოფს რომ შეუძლებელი იყოს მონაცემების წაკითხვა, გადაწერა, შეცვლა ან ამოშლა უფლებამოსილების გარეშე (მაგ. ცოდნის - საჭიროების საფუძველზე), მონაცემებზე წვდომა შესაძლებელი იყოს მხოლოდ უფლებამოსილი პერსონალის წარმატებული იდენტიფიკაციისა და ავთენტიფიკაციის შემდეგ, და ა.შ.

მონაცემთა დაცვის ძირითადი რეგულაცია რისკზე დაფუძნებული კანონია. მონაცემთა დაცვის ოფიცერმა გამუდმებით უნდა შეაფასოს რისკები, რათა შესაძლებელი იყოს ორგანიზაციაში იმ მონაცემთა დამუშავების დადგენა რომლებიც შეიძლება პრობლემური იყოს. მაგ. თუ კომპანიის პერსონალური მონაცემები სისტემატურად და ფართოდ პროფილირდება ან ახალი ტექნოლოგიური გადაჭრის გზები გამოიყენება პერსონალურ მონაცემთა დამუშავებაში, როგორიცაა „საგნების

[4] იქვე, მუხლი 25. პარ. 1.

ინტერნეტის“ გამოყენება, ან პერსონალური მონაცემები მუშავდება მრავალი წყაროდან მიღებული მსგავსებების ერთმანეთთან დაკავშირებით, შედარებით და შემოწმებით, მონაცემთა დაცვის ოფიცერმა უნდა „ააფრიალოს წითელი დროშა“ - დაადგინოს ან ყურადღება გაამახვილოს პრობლემაზე.

მონაცემთა დაცვის ოფიცრები არ წარმოადგენენ კომპანიისთვის ტვირთს. მათ დანიშნულებას არ წარმოადგენს პერსონალურ მონაცემთა დამუშავების აკრძალვა. მათი მიზანია უზრუნველყონ პერსონალურ მონაცემთა დამუშავების შესაბამისობა მონაცემთა დაცვის რეგულაციის მოთხოვნებთან.

თუმცა, თუ კომპანიას არ მიაჩნია, რომ მონაცემთა დაცვის ოფიცრისგან რჩევების მიღება და მათი ჩართვა პროექტში, რომელიც ითვალისწინებს მონაცემთა დამუშავებას, მათთვის სარგებლობის მომტანია, მან მხედველობაში უნდა მიიღოს რომ შესაძლებელია დაიწყოს გამოძიება ამ მოთხოვნის შეუსრულებლობის გამო.

ბელგიის მონაცემთა დაცვის ორგანომ[5] ინსპექტირება ჩაატარა ტურიზმის რეგიონულ სამთავრობო სააგენტოში, რის შედეგადაც სააგენტოს გამოუცხადეს საყვედური, რადგან მონაცემთა დაცვის ოფიცერი არ იყო პროაქტიულად ჩართული კანონით გათვალისწინებული დავალების დამუშავებაში, დაირღვა მონაცემთა დაცვის ძირითადი რეგულაციის 38(1) და 39(1) მუხლები.

2.2. სამართლებრივ დებულებებთან შესაბამისობის მონიტორინგი, როგორც დარღვევების პრევენციის მექანიზმი

მონაცემთა დაცვის ოფიცერი უფლებამოსილია ჩაატაროს აუდიტი, რომელიც შეიძლება ინიციირებული იყოს ან გარეგანი შეტყობინების საფუძველზე, მაგ., როდესაც ფიზიკური პირი წარუდგენს კომპანიას საჩივარს და მონაცემთა დაცვის ოფიცერი შეისწავლის საჩივართან დაკავშირებულ გარემოებებს, ან შინაგანი ინიციატივით - პროფკავშირის კომისრის, შრომის საბჭოს, ინფორმატორის ან ნებისმიერი თანამშრომლის საჩივრის ან შეტყობინების საფუძველზე.

კომპანია ვალდებულია, მიაწოდოს მონაცემთა დაცვის ოფიცერს ყველა რესურსი და მისცეს წვდომა აუდიტის ჩასატარებლად. კომპანიამ უნდა აცნობოს თანამშრომლებს ინსპექტირების ჩატარებაზე მონაცემთა დაცვის ოფიცრის უფლებამოსილების შესახებ (კარგი იქნება თუ გასცემს მკაფიო ინსტრუქციებს კომპანიის შიდა წესების გამოყენებით). შეტყობინება ცნობილი უნდა გახდეს საგარეო სერვისების პროვაიდერებისთვის, მომმარაგებლებისთვის, ზედამხედველი კომიტეტის წევრებისა და ყველასთვის, ვისაც აქვს შეხება პერსონალურ მონაცემებთან კომპანიაში.

რეგულარული აუდიტის ჩატარებას შეუძლია (დროულად) აღმოაჩინოს პერსონალურ მონაცემთა დამუშავებაში არსებული პრობლემები და თავიდან აიცილოს პერსონალურ მონაცემთა უსაფრთხოებასთან დაკავშირებული დარღვევები.

[5] <https://gdprhub.eu/index.php?title=APD/GBA_(Belgium)_-_162/2022> [30.09.2023].

2.3. დამუშავების ოპერაციებში ჩართული პერსონალის ცნობიერების ამაღლება და ტრენინგი

პერსონალურ მონაცემებთან დაკავშირებული დარღვევები უმეტესად სათავეს მონაცემთა დამმუშავებლის თანამშრომლების მიერ დაშვებული შეცდომებიდან იღებს, რასაკვირველია, შეცდომის რისკი არსებობს, თუმცა შეიძლება შეცდომის თავიდან აცილება თანამშრომლების სათანადო კვალიფიკაციის ამაღლებით.

ნორვეგიაში[6] ერთმა კომპანიამ შეცდომით შეამოწმა მეორე კომპანიის ერთ-ერთი მფლობელის კრედიტი, რის შედეგადაც დაჯარიმდა 200 000 ნორვეგიული კრონით. დარღვევა გამოწვეული იყო იმ სისტემის არცოდნით, რომელიც გამოიყენებოდა საკრედიტო ანგარიშების მოთხოვნისთვის.

შემთხვევა მოხდა კვიპროსში[7], სადაც კლიენტის მონაცემების განახლების პროცესში ბეჭდვითი შეცდომა იქნა დაშვებული პასპორტის ნომერში ჰელენიკ ბანკში. გარკვეული დროის შემდეგ, სხვა პირმა შეამოწმა ინფორმაცია და ნახა, რომ თავის ახალ პასპორტს მიენიჭა ის ნომერი, რომელიც ბანკის თანამშრომელმა შეცდომით შეიყვანა წინა მომხმარებლის პასპორტის ნომრად, ამგვარად, ვებ-ბანკინგის პლატფორმის გამოყენებით სხვა კლიენტს ჰქონდა ნაწილობრივი წვდომა მეორე მომხმარებლის პერსონალურ და ფინანსურ მონაცემებზე.

საინფორმაციო კომისიის აპარატმა[8] საყვედური გამოუცხადა იუსტიციის სამინისტროს კონფიდენციალურობის დარღვევისთვის, რადგან რამდენიმე პირს ჰქონდა წვდომა ციხის კამერაში დარჩენილ კონფიდენციალურ დოკუმენტებზე.

პოლონეთის მონაცემთა დაცვის ორგანომ[9] 6387 ევროს ოდენობით დააჯარიმა რაიონული სასამართლო, რადგან თანამშრომელმა დაკარგა სამი USB-დისკი, რომელიც შეიცავდა რეზოლუციის პროექტს და ფიზიკური პირების დაუზუსტებელი რაოდენობის პერსონალურ მონაცემებს.

მნიშვნელოვანია, ხაზი გავუსვათ ფაქტს, რომ ერთ-ერთ ვალდებულებას რომელიც განსაზღვრულია მონაცემთა დაცვის ძირითადი რეგულაციით[10] წარმოადგენს სათანადო ორგანიზაციული დამცავი ზომების მიღება, რომელიც მოიცავს ორგანიზაციის შიგნით ცნობიერების ამაღლებას და არა მარტო.

დამმუშავებლის აღნიშნული ვალდებულება დაკავშირებულია პერსონალური მონაცემების დაცვის ოფიცრის ვალდებულებებთან, რომლის ამოცანაა თანამშრომელთა ცოდნის ამაღლება და პერსონალისთვის ტრენინგების ჩატარება მონაცემებთან დაკავშირებული დარღვევების თავიდან ასაცილებლად.

უამრავი მაგალითი არსებობს პრაქტიკაში, სადაც მონაცემთა დაცვის ოფიცერი მოახდენდა პრევენციულ გავლენას პერსონალურ მონაცემებთან დაკავშირებულ დარღვევებზე, ორგანიზაციაში პერსონალური მონაცემების დაცვის მნიშვნელობაზე ცნობიერების ამამაღლებელი აქტივობები რომ განხორციელებულიყო.

როცა საქმე ეხება თანამშრომელთა შეცდომას, პერსონალურ მონაცემთა დაცვის განზრახ დარღვევა არ არის ხშირი. როგორც წესი, თანამშრომლებს წარმოდგენა არა აქვთ რისკების წარმოშობასა და შეცდომებზე. მათ ასევე არ იციან, რომ ინციდენტთან

[6] <https://gdprhub.eu/index.php?title=Datatilsynet_(Norway)_-_20/04401> [30.09.2023].

[7] <https://gdprhub.eu/index.php?title=Commissioner_(Cyprus)_-_12.10.001.011.001> [30.09.2023].

[8] <https://gdprhub.eu/index.php?title=ICO_(UK)_-_Ministry_of_Justice_(1)> [30.09.2023].

[9] <https://gdprhub.eu/index.php?title=UODO_(Poland)_-_DKN.5131.12.2020> [30.09.2023].

[10] ევროპარლამენტისა და საბჭოს 2016 წლის 27 აპრილის რეგულაცია (EU)2016/679 „პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვისა და ასეთი მონაცემების მიმოცვლის შესახებ“, რომელიც აუქმებს დირექტივას 95/46/EC (მონაცემთა დაცვის ძირითადი რეგულაცია, მუხლი 32, პარაგრაფი 1).

დაკავშირებით უნდა გაკეთდეს შეტყობინება, რათა ლეგიტიმურად იმოქმედონ იმ ზეგავლენაზე რომელსაც ეს დარღვევა მოახდენს მონაცემთა სუბიექტზე.

2.4. კონსულტაციების გაწევა მონაცემთა დაცვაზე ზემოქმედების შეფასების პროცესში

მონაცემთა დაცვის ძირითადი რეგულაციის[11] მიხედვით, სადაც ერთგვარი დამუშავების, კერძოდ, ახალი ტექნოლოგიის გამოყენებისა, და დამუშავების ბუნების, სფეროს, კონტექსტის და მიზნის მხედველობაში მიღების შედეგად შეიძლება ფიზიკური პირების უფლებები და თავისუფლებები რისკის ქვეშ დადგეს, დამმუშავებელი ვალდებულია, დამუშავებამდე განახორციელოს დამუშავების ოპერაციების პერსონალური მონაცემების დაცვაზე ზეგავლენის შეფასება.

დამმუშავებლის ეს ვალდებულება დაკავშირებულია პერსონალურ მონაცემთა დაცვის ოფიცრის ამოცანებთან, რომელსაც ევალება მონაცემთა დაცვაზე ზემოქმედების შეფასების შესახებ საჭირო კონსულტაციის ჩატარება.

მონაცემთა დაცვაზე ზემოქმედების შეფასება ხელს უწყობს ფიზიკური პირების უფლებებსა და თავისუფლებების მიმართ მაღალი რისკის დადგენას პერსონალური მონაცემების დამუშავების დროს.

ზოგიერთი ფაქტორი,[12] რომელიც შესაძლოა, შეიცავდეს მაღალ რისკებს შემდეგია: ფინანსური დაწესებულებები, რომლებიც ახდენენ თავიანთი კლიენტების შემოწმებას ფულის გათეთრების საწინააღმდეგო (AML) ან თაღლითობის მონაცემთა ბაზის მეშვეობით, ბიოტექნოლოგიური კომპანია, რომელიც მომხმარებლებს სთავაზობს გენეტიკურ ტესტებს ავადმყოფობის/ჯანმრთელობის რისკების შეფასების და პროგნოზირების მიზნით, კომპანია, რომელიც ქმნის ქცევით ან მარკეტინგულ პროფაილებს თავიანთი ვებსაიტების გამოყენების ან ნავიგაციის მეშვეობით, ზოგადი პროფილის საავადმყოფო, რომელშიც შენახულია პაციენტების ისტორიები, კერძო გამომძიებელი, რომელიც ინახავს დეტალებს ნასამართლობებსა და კანონდარღვევებზე, გენეალოგიური ინფორმაციის ფართო კოლექციებს იმ პიროვნებების ოჯახებზე რომლებიც მიეკუთვნებიან კონკრეტულ რელიგიურ ჯგუფებს, დამუშავება იმ მონაცემებისა, რომლებიც მიღებულია ე.წ. „ნივთების ინტერნეტის“ აპლიკაციების გამოყენებით თუ მონაცემების გამოყენება მნიშვნელოვან გავლენას ახდენს (ან შესაძლოა მოახდინოს) ინდივიდების ყოველდღიურ და პირად ცხოვრებაზე.

შესაფასებელი რისკები დაკავშირებულია არა მარტო პერსონალური მონაცემების დაცვის უფლებასთან, არამედ სხვა უფლებებსა და ფუნდამენტურ თავისუფლებებთან, როგორიცაა პირადი და ოჯახური ცხოვრების უფლება, გამოხატვის თავისუფლებისა და ინფორმაციის უფლება და ა.შ.

ამიტომ, მაგალითად, თუ კომპანიას სურს მოძებნოს თანამშრომლის ტრანსპორტის მდებარეობა, არსებობს პერსონალური მონაცემების დამუშავების რისკი არასამუშაო დროს თანამშრომლის ადგილმდებარეობის შესახებ, რადგანაც ამან შეიძლება გავლენა მოახდინოს მის პირად და ოჯახურ ცხოვრებაზე.

[11] იქვე, მუხლი 35, პარ. 1.
[12] <https://azop.hr/wp-content/uploads/2023/09/DPO-prirucnik.pdf> [30.09.2023].

როდესაც მაღალი რისკი დადგენილია, საჭიროა, შეფასდეს შესაძლებელია თუ არა მისი შესუსტება სათანადო ტექნიკური და ორგანიზაციული დამცავი ზომების გამოყენებით. თუ რისკის შემსუბუქება არ არის შესაძლებელი, მაშინ მიზანშეწონილია პერსონალური მონაცემების დამუშავებაზე უარის თქმა.

ამ პროცესში პერსონალური მონაცემების დაცვის ოფიცერი თამაშობს საკვანძო როლს, რამდენადაც მის რეკომენდაციაზეა დამოკიდებული პერსონალური მონაცემების უსაფრთხოებასთან დაკავშირებული დარღვევებისა და არაკანონიერი წვდომის წარმატებით (ან წარუმატებლად) თავიდან აცილება.

მაღალი რისკების შემთხვევაში, რომლებიც ტექნიკური და ორგანიზაციული ზომების გატარებით არ შეიძლება შემცირდნენ „დასაშვებ რისკამდე“, უნდა შესრულდეს ვალდებულება, რომელიც განსაზღვრულია მონაცემთა დაცვის ძირითადი რეგულაციის 36-ე მუხლით, რაც ითვალისწინებს ზედამხედველ ორგანოსთან წინასწარ კონსულტაციას.

2.5. თანამშრომლობა ზედამხედველ ორგანოსთან

მონაცემთა დაცვის ოფიცერმა უნდა ითანამშრომლოს ზედამხედველ ორგანოსთან. თანამშრომლობა იწყება საკუთარი ან ზედამხედველი ორგანოს ინიციატივით.

მონაცემთა დაცვის ოფიცრის ურთიერთობას ზედამხედველ ორგანოსთან შეუძლია ზეგავლენა მოახდინოს პერსონალურ მონაცემთა დაცვის რეგულაციების დაცვაზე.

3. დასკვნა

ორგანიზაციაში მონაცემთა დაცვის ოფიცრის დანიშვნამ შესაძლოა იმოქმედოს, როგორც მონაცემთა დაცვის წესების დარღვევების თავიდან არიდების მექანიზმმა, რომელიც გამომდინარეობს დასახული ამოცანების ბუნებიდან. სხვა მოთხოვნებთან ერთად, მონაცემთა დაცვის ოფიცერმა კონსულტაცია უნდა გაუწიოს მონაცემთა დამმუშავებლებს და იმ თანამშრომლებს, რომლებიც ახორციელებენ მონაცემთა დამუშავებას, ხელი უნდა შეუწყოს პერსონალურ მონაცემთა დაცვის უფლებისადმი პატივისცემის კულტურის დანერგვას ორგანიზაციაში და მონიტორინგი გაუწიოს მონაცემთა დაცვის რეგულაციების შესრულებას. მათი დანიშვნით, რაც იძლევა ვალდებულებების დროულად შესრულების საშუალებას მათი რჩევების გათვალისწინებით, შეუძლია უზრუნველყოს, რომ არ დაირღვეს პერსონალურ მონაცემთა კანონი. მონაცემთა დაცვის ოფიცერსა და პრევენციულ მექანიზმს შორის კავშირი კანონის დარღვევასთან დაკავშირებით ზოგადად დამოკიდებულია რისკზე დაფუძნებულ ქმედებებზე, რაც (იმ შემთხვევაში თუ მონაცემთა დაცვის ოფიცერი კვალიფიციურია) ორი წინ გადადგმული ნაბიჯია, თუ მოვიფიქრებთ როგორ გავაუმჯობესოთ კანონის დაცვის სტანდარტი და შევამციროთ რისკები, დავაბალანსოთ ბიზნეს აქტივობები პერსონალურ მონაცემთა დაცვის უფლების მოთხოვნასთან.

ბიბლიოგრაფია:

1. ევროპარლამენტისა და საბჭოს 1995 წლის 24 ოქტომბრის დირექტივა 95/46/EC „პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვისა და ასეთი მონაცემების თავისუფალ მიმოცვლასთან დაკავშირებით“ (ძალადაკარგულია).
2. ევროპარლამენტისა და საბჭოს 2016 წლის 27 აპრილის რეგულაცია (EU)2016/679 „პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვისა და ასეთი მონაცემების მიმოცვლის შესახებ“.
3. <https://gdprhub.eu/index.php?title=APD/GBA_(Belgium)_-_162/2022> [30.09.2023].
4. <https://gdprhub.eu/index.php?title=Datatilsynet_(Norway)_-_20/04401> [30.09.2023].
5. <https://gdprhub.eu/index.php?title=Commissioner_(Cyprus)_-_12.10.001.011.001> [30.09.2023].
6. <https://gdprhub.eu/index.php?title=ICO_(UK)_-_Ministry_of_Justice_(1)> [30.09.2023].
7. <https://gdprhub.eu/index.php?title=UODO_(Poland)_-_DKN.5131.12.2020> [30.09.2023].
8. <https://azop.hr/wp-content/uploads/2023/09/DPO-prirucnik.pdf> [30.09.2023].