პერსონალურ მონაცემთა
დაცვის სამსახური

მსოფლიო პრაქტიკა

მარტი / 2024

მთავარი სიახლეები

ევროპარლამენტმა „ხელოვნური ინტელექტის შესახებ“ აქტი მიიღო

ევროპის მონაცემთა დაცვის ზედამხედველმა (“EDPS”) გამოძიების შედეგად დაადგინა რომ, ევროკომისიის მიერ “Microsoft 365“-ის გამოყენებამ დაარღვია ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაცია“ (“GDPR“)

ევროკავშირის მართლმსაჯულების სასამართლომ (“CJEU”) სარეკლამო მომსახურების განმახორციელებელი ასოციაცია თანადამუშავებისთვის პასუხისმგებელ პირად მიიჩნია

ევროკავშირის მართლმსაჯულების სასამართლომ (“CJEU”) არაკანონიერად დამუშავებული პერსონალური მონაცემების წაშლის თაობაზე გადაწყვეტილება მიიღო

ევროკავშირის მართლმსაჯულების სასამართლომ (“CJEU”) სარეკლამო მომსახურების განმახორციელებელი ასოციაცია თანადამუშავებისთვის პასუხისმგებელ პირად მიიჩნია

7.03.2024

ფოტო: european-union.europa.eu

ბელგიური არაკომერციული ასოციაცია “IAB ევროპა” კომპანიებს ციფრული რეკლამირებისა და მარკეტინგის სფეროში მომსახურებას უწევს. ასოციაციამ ევროკავშირის „მონაცემთა დაცვის ძირითად რეგულაციასთან“ (“GDPR”) შესაბამისობის მიზნით, მონაცემთა დამუშავების გამჭვირვალობისა და თანხმობის წესები შეიმუშავა, რომლის თანახმად, მომხმარებელს ვებგვერდზე ან აპლიკაციაში შესვლისთანავე მიეწოდება ინფორმაცია, რომელიც გენერირდება ავტომატურ რეჟიმში კომპანიების, ბროკერებისა და სარეკლამო პლატფორმის მონაცემთა საფუძველზე. აღნიშნული გულისხმობს პროფაილინგის განხორციელებას, მომხმარებლისთვის ცალკეული ინფორმაციის უპირატესად მიწოდების უზრუნველსაყოფად.

პროფაილინგის განსახორციელებლად, ვებგვერდზე შესვლისას მომხმარებელი ეცნობა პერსონალური მონაცემების დამუშავების პირობებს და გასცემს თანხმობას მონაცემთა დამუშავებაზე. გამჭვირვალობისა და თანხმობის წესი ასოციაციას შესაძლებლობას ანიჭებს, დაამუშავოს მონაცემთა სუბიექტის პერსონალური მონაცემი სულ მცირე ერთ სამართლებრივ საფუძველზე დაყრდნობით. მომხმარებლის თანხმობის შემთხვევაში, ონლაინ პლატფორმა მიღებულ ინფორმაციას უზიარებს მონაცემთა დამუშავებისთვის პასუხისმგებელ პირებს: კომპანიებს, რომლებსაც სურთ მათი მომსახურების შესახებ ინფორმაციის გაზიარება, ხოლო არაკომერციული ასოციაცია - “IAB ევროპა” პროფაილინგის განხორციელებით მოიაზრებოდა, როგორც მონაცემთა დამუშავებაზე უფლებამოსილი პირი, რომელიც მონაცემებს ამუშავებს შეთანხმებული ფორმითა და მოცულობით. ვებგვერდზე განთავსებული „მზა ჩანაწერების“ და კოდირების სპეციალური სისტემის გაერთიანებით შესაძლებელია, მომხმარებლის “IP” მისამართის მოძიება.

2022 წელს, ბელგიის მონაცემთა დაცვის საზედამხედველო ორგანოს გადაწყვეტილებით, არაკომერციული ასოციაცია “IAB ევროპა” მიჩნეულ იქნა მონაცემთა დამუშავებისთვის პასუხისმგებელ პირად, რომელიც არ ითვალისწინებდა ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ მოთხოვნებს. ხოლო კოდირების სპეციალური სისტემა, რომელსაც ასოციაცია იყენებდა, არ იყო რეგულაციასთან შესაბამისობაში. საზედამხედველო ორგანომ ასოციაცია

დააჯარიმა და კონკრეტული ღონისძიებების განხორციელება დააკისრა.

“IAB ევროპამ” საზედამხედველო ორგანოს გადაწყვეტილება გაასაჩივრა და მისი გაუქმების მოთხოვნით მიმართა ბრიუსელის სააპელაციო სასამართლოს. ასოციაცია ამტკიცებდა, რომ კოდირების სპეციალურ სისტემაში არსებული მონაცემები არ უკავშირდებოდა მომხმარებლის იდენტიფიცირებას და აღნიშნულ მონაცემთა “IP” მისამართთან დაკავშირება მხოლოდ გამჭვირვალობისა და თანხმობის წესთან შესაბამისობაში მყოფ კომპანიებს შეეძლოთ. ამიტომ, ასოციაცია დამუშავებისთვის პასუხისმგებელი პირების მითითებების შესაბამისი ფორმითა და მოცულობით დაამუშავებდა მონაცემებს. ამდენად, ასოციაცია არ უნდა მიჩნეულიყო დამუშავებისთვის პასუხისმგებელ პირად.

ბრიუსელის სააპელაციო სასამართლოს მიმართვის საფუძველზე, ევროკავშირის მართლმსაჯულების სასამართლომ განმარტა,[1] რომ კოდირების სპეციალური სისტემა პერსონალური მონაცემია, რომელიც აერთიანებს მომხმარებლის “IP” მისამართს და მომხმარებლის მიერ გაცხადებული თანხმობის საფუძველზე შესაძლებელს ხდის მის ამოცნობას, მიუხედავად იმისა, აქვს თუ არა წვდომა “IAB ევროპას” მასზე. სასამართლომ იმსჯელა ასოციაციის მონაცემთა დამუშავებისთვის პასუხისმგებელ პირად მიჩნევის საკითხზე - განსაზღვრავდა იგი თუ არა მონაცემთა დამუშავების მიზნებსა და საშუალებებს. სასამართლომ აღნიშნა, რომ “IAB ევროპის” მიერ შედგენილი გამჭვირვალობისა და თანხმობის წესი ხელს უწყობს კომპანიებს სარეკლამო სივრცის ათვისებაში, რომელიც მონაცემთა სუბიექტებისა და მონაცემთა დამუშავებისთვის პასუხისმგებელი პირებისთვის მონაცემთა დაცვის გარკვეულ სტანდარტს ადგენდა. კოდირების სპეციალური სისტემა იმგვარად იმართებოდა, რომ ასოციაციას მისი კონტროლის მექანიზმი ჰქონდა, კერძოდ, პროფაილინგის დაწყების, შეჩერებისა და დასრულების თვალსაზრისით, მათ შორის, მომხმარებლის თანხმობისა და უარყოფის საპასუხო დამუშავების შესაძლებლობა.

სასამართლომ დაასკვნა, რომ “IAB ევროპა” თავისი მოქმედებით გავლენას ახდენდა მონაცემთა დამუშავებაზე და მისი მომსახურების დამკვეთ კომპანიებთან ერთად განსაზღვრავდა მონაცემთა დამუშავების მიზნებსა და საშუალებებს, რის გამოც სასამართლომ იგი თანადამუშავებისთვის პასუხისმგებელ პირად მიიჩნია. გადაწყვეტილებაში აღინიშნა, თუ რა მნიშვნელობა აქვს დამუშავებისთვის პასუხისმგებელ პირსა და

[1] Judgment of the Court, In Case C-604/22, 7 March 2024, <https://curia.europa.eu/juris/document/document.jsf;jsessionid=56AC13792375F19613F0200AE8680B42?text=&docid=283529&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=4314797>, [25.03.2024].

დამუშავებაზე უფლებამოსილ პირს შორის დადებული ხელშეკრულების შესაბამისობას ევროკავშირის „მონაცემთა დაცვის ძირითად რეგულაციასთან“. მათ შორის, თუ როდის შეიძლება მიჩნეულ იქნეს დამუშავებაზე უფლებამოსილი პირი თანადამუშავებისთვის პასუხისმგებელ პირად.[2]

გაერთიანებული სამეფოს მონაცემთა დაცვის საზედამხედველო ორგანომ სამართალდარღვევის ჩადენისთვის პასუხისმგებლობის დაკისრების სახელმძღვანელო რეკომენდაცია გამოაქვეყნა

18.03.2024

ფოტო: twitter.com

სახელმძღვანელო რეკომენდაცია[3] პერსონალური მონაცემების დამუშავებასთან დაკავშირებული ადმინისტრაციული სამართალდარღვევისთვის ჯარიმის დაკისრების და შესაბამისი ოდენობების განსაზღვრის ინსტრუქციას წარმოადგენს. იგი უზრუნველყოფს მონაცემთა დაცვის საზედამხედველო ორგანოს საქმიანობის გამჭვირვალობას და საჯაროობას. მისი მიზანია საზედამხედველო ორგანოს თანამშრომლებს, მონაცემთა სუბიექტებს, მონაცემთა დამუშავებისთვის პასუხისმგებელ, დამუშავებაზე უფლებამოსილ და სხვა დაინტერესებულ პირებს მიაწოდოს ინფორმაცია ჯარიმის დაკისრების უფლებამოსილებისა და საგამონაკლისო შემთხვევების შესახებ. აღსანიშნავია, რომ გამოქვეყნებამდე ერთი წლით ადრე, სახელმძღვანელო მითითებების პროექტი ღია იყო შენიშვნებისა და სარეკომენდაციო წინადადებებისთვის.

ინსტრუქციაში მოცემულია საკანონმდებლო საფუძვლები, რომლებსაც ეყრდნობა საზედამხედველო ორგანო პერსონალური მონაცემების დამუშავებასთან დაკავშირებული სამართალდარღვევის დადგენისა და სახდელის სახით ჯარიმის დაკისრებისას. მასში ჩამოყალიბებულია საკანონმდებლო ცნებებისა და მოწესრიგების ერთგვაროვანი განმარტებები მონაცემთა სუბიექტების უფლებების, მონაცემთა დამმუშავებლების უფლება-მოვალეობების და სხვა საკითხების

[2] Court of Justice of the European Union (“CJEU”), Judgment of the Court in Case C-604/22, PRESS RELEASE No 44/24 Luxembourg, 7 March 2024, <https://curia.europa.eu/jcms/upload/docs/application/pdf/2024-03/cp240044en.pdf[25.03.2024].

[3] Information Commissioner’s Office (“ICO”), Data Protection Fining Guidance, <https://ico.org.uk/about-the-ico/our-information/policies-and-procedures/data-protection-fining-guidance/>, [25.03.2024].

შესახებ. დოკუმენტის ძირითადი ნაწილი ეთმობა მეთოდოლოგიას, რომელიც გამოიყენება სამართალდარღვევის შესაბამისი ჯარიმის გამოსათვლელად.

დოკუმენტი აერთიანებს ნაწილებს:

1. „გაერთიანებული სამეფოს მონაცემთა დაცვის ძირითადი რეგულაციის“ და „მონაცემთა დაცვის კანონის“ მოთხოვნათა დარღვევები, რისთვისაც საზედამხედველო ორგანოს შეუძლია, მონაცემთა დამუშავებისთვის პასუხისმგებელ ან დამუშავებაზე უფლებამოსილ პირს დააკისროს ჯარიმა;
2. გარემოებები, რომლებიც გასათვალისწინებელია საჯარიმო შეტყობინების გაცემის და ოდენობის განსაზღვრის შესახებ გადაწყვეტილების მიღებისას, კერძოდ, რა შემთხვევაში უნდა გამოსცეს ორგანომ შეტყობინება;
3. ჯარიმის მაქსიმალური ოდენობა „გაერთიანებული სამეფოს მონაცემთა დაცვის ძირითადი რეგულაციის“ და „მონაცემთა დაცვის კანონის“ მიხედვით;
4. მონაცემთა დამუშავებისთვის პასუხისმგებელი და დამუშავებაზე უფლებამოსილი პირებისთვის (ორგანიზაციებისთვის) ჯარიმის განსაზღვრისა და დაკისრების კონცეფცია;
5. საზედამხედველო ორგანოს შეხედულება ჯარიმებთან დაკავშირებით, დამუშავებისთვის პასუხისმგებელი ან დამუშავებაზე უფლებამოსილი პირების მიერ ერთზე მეტი სამართალდარღვევის ჩადენის შემთხვევაში;
6. საჯარიმო ცნობების გაცემასთან დაკავშირებული შეზღუდვები;
7. შემთხვევები, როდესაც საზედამხედველო ორგანო მიზანშეწონილად მიიჩნევს საჯარიმო შეტყობინების გამოცემას:
   - პერსონალური მონაცემების დამუშავებასთან დაკავშირებული დარღვევის სიმძიმე;
   - პასუხისმგებლობის დამამძიმებელი ან შემამსუბუქებელი გარემოებების არსებობა;
   - მონაცემთა დაცვის საზედამხედველო ორგანოს ეფექტიანი, პროპორციული და დროული მოქმედების საჭიროება;
8. ჯარიმის ოდენობის განსაზღვრისთვის მხედველობაში მიიღება:
   - დარღვევის სიმძიმე;
   - ორგანიზაციის ფინანსური ბრუნვა;
   - დარღვევის ჩადენის საწყისი ეტაპის დადგენა და განგრძობადი ხასიათი;
   - პასუხისმგებლობის დამამძიმებელი და შემამსუბუქებელი გარემოებები;

- ჯარიმის უკვე განსაზღვრული ოდენობის შესწორების საგამონაკლისო შემთხვევები;

9. ჯარიმის შემცირება ორგანიზაციის მიერ მისი გადახდის დროებითი შეუძლებლობის შემთხვევაში.

ამდენად, გაერთიანებული სამეფოს მონაცემთა დაცვის საზედამხედველო ორგანოს მიერ მიღებული სახელმძღვანელო რეკომენდაცია უზრუნველყოფს „გაერთიანებული სამეფოს მონაცემთა დაცვის ძირითადი რეგულაციის“ და „მონაცემთა დაცვის“ კანონის მოთხოვნათა ზუსტ და ერთგვაროვან განმარტებას ადმინისტრაციული სამართალ-დარღვევისთვის შესაბამისი პასუხისმგებლობის დაკისრების მიზნით.

გაერთიანებული სამეფოს მონაცემთა დაცვის საზედამხედველო ორგანომ ორგანიზაცია მონაცემთა პირდაპირი მარკეტინგის მიზნით მონაცემთა დამუშავებისთვის დააჯარიმა

07.03.2024

ფოტო: 1stformations.co.uk

მონაცემთა დამუშავებაზე უფლებამოსილმა ორგანიზაციამ ჯანმრთელობის დაზღვევის მომსახურების შეთავაზების, პირდაპირი მარკეტინგის მიზნით, მონაცემთა სუბიექტებთან არასასურველი ზარი 47 998-ჯერ განახორციელა. განხორციელებულ ზარებს ჰქონდა მუდმივი, მიზანმიმართული და შეცდომაში შემყვანი ხასიათი. მოქალაქეები ინფორმაციის მიღებაზე უარის განცხადების მიუხედავად, კვლავ იღებდნენ შეტყობინებებს.[4]

გაერთიანებული სამეფოს მონაცემთა დაცვის საზედამხედველო ორგანომ დაადგინა, რომ მონაცემთა დამუშავებაზე უფლებამოსილი პირი, კერძოდ, ორგანიზაციის ოპერატორები კვლავ უკავშირდებოდნენ მონაცემთა

[4] Information Commissioner's Office ("ICO"), CO fines Wigan-based Pinnacle Life £80,000 for "predatory" spam call campaign, 07 March 2024, <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/03/ico-fines-wigan-based-pinnacle-life-80-000-for-predatory-spam-call-campaign/>, [25.03.2024].

სუბიექტებს მომსახურების შეთავაზების მიზნით და მოქალაქეებს აწვდიდნენ მცდარ ინფორმაციას დამუშავებისთვის პასუხისმგებელი იმ პირის სახელით მოქმედების შესახებ, რომლისგანაც მომხმარებლებს ადრე უკვე ჰქონდათ მიღებული შესაბამისი მომსახურება.

აღსანიშნავია, რომ მონაცემთა დაცვის საზედამხედველო ორგანომ საკითხის შესწავლა დაიწყო ერთ-ერთი მოქალაქის მიმართვის საფუძველზე, რის შემდეგაც გამოვლინდა 47 998 ზარის განხორციელების ფაქტი. მოქალაქე აღნიშნავდა, რომ განხორციელებული ზარის ფარგლებში ორგანიზაციის ოპერატორი ეკითხებოდა სახელს, გვარსა და მისამართს, ხოლო პასუხზე, რომ იგი უკვე სარგებლობდა ჯანმრთელობის დაზღვევით და აღარ სურდა საუბრის გაგრძელება, ორგანიზაციის წარმომადგენელი ზარის დასრულების შემდეგ, კვლავ ცდილობდა მასთან დაკავშირებას. ამის შემდეგ რამდენიმე მოქალაქემ საზედამხედველო ორგანოს მიმართა. ისინი აღნიშნავდნენ, რომ უარის მიუხედავად, ორგანიზაციის წარმომადგენლებმა მათთან საუბრისას დააფიქსირეს, რომ დაკავშირება გაგრძელდებოდა იქამდე, ვიდრე არ დაეთანხმებოდნენ შეთავაზებულ პირობებს. მოქალაქეები ყურადღებას ამახვილებდნენ სატელეფონო საუბრისას ოპერატორების უხეშ და შეურაცხმყოფელ დამოკიდებულებაზეც.

დადგინდა, რომ 2021 წლის 5 მაისიდან 1 წლის განმავლობაში, მონაცემთა დამუშავებაზე უფლებამოსილმა ორგანიზაციამ საჯარო სატელეკომუნიკაციო სერვისის გამოყენებით სულ მცირე არასასურველი პირდაპირი მარკეტინგული ზარი 47 998-ჯერ განახორციელა. მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი არ ფლობდა ინფორმაციას, რომ მონაცემთა დამუშავებაზე უფლებამოსილი პირი მისი სახელით უკავშირდებოდა მომხმარებლებს. აღნიშნული ორგანიზაციის მიერ განხორციელებული მოქმედებები მიჩნეულ იქნა, როგორც მონაცემთა პირდაპირი მარკეტინგის მიზნით დამუშავებასთან დაკავშირებული საკანონმდებლო მოწესრიგების დარღვევა. აღნიშნულის გათვალისწინებით, მონაცემთა დაცვის საზედამხედველო ორგანომ მონაცემთა დამუშავებაზე უფლებამოსილი პირი 80 000 £-ით დააჯარიმა და მნიშვნელოვნად მიიჩნია პირდაპირი მარკეტინგული ზარებისა და შეტყობინებების მომწესრიგებელ აქტში - „პირადი ცხოვრების ხელშეუხებლობისა და ელექტრონული კომუნიკაციების“ 2003 წლის რეგულაციაში ცვლილებების შეტანა.[5]

[5] აღნიშნული რეგულაცია წარმოადგენს გაერთიანებული სამეფოს საკანონმდებლო აქტს, ხოლო ევროკავშირის დონეზე მოქმედებს ევროპის პარლამენტისა და საბჭოს 2002 წლის 12 ივლისის დირექტივა „ელექტრონული კომუნიკაციის სექტორში პერსონალური მონაცემის დამუშავებისა და პირადი ცხოვრების ხელშეუხებლობის დაცვის შესახებ“.

ევროპარლამენტმა „ხელოვნური ინტელექტის შესახებ“ აქტი მიიღო

13.03.2024

ფოტო: setav.org

2024 წლის 13 მარტს, ევროპარლამენტმა პლენარულ სესიაზე მხარი დაუჭირა ევროკომისიის წინადადებას ხელოვნური ინტელექტის შესახებ ჰარმონიზებული წესების (“AI Act”) განმსაზღვრელი რეგულაციის მიღების თაობაზე (523 - მხარდამჭერი; 46 - მოწინააღმდეგე; 49-მ შეიკავა).[6]

„ხელოვნური ინტელექტის აქტი" (“AI Act”)[7] სავალდებულო ძალის მქონე დოკუმენტია, რომლის მიზანია, სამართლებრივი მოწესრიგების ფარგლებში მოაქციოს ხელოვნური ინტელექტის სისტემების შექმნის, განვითარებისა და გამოყენების პროცესი. აქტის მოქმედება ვრცელდება ევროკავშირის მასშტაბით, წევრ ქვეყნებზე და მოიცავს როგორც საჯარო, ისე კერძო სექტორს. თუმცა, არსებობს გამონაკლისებიც - ხელოვნური ინტელექტის აქტი არ ვრცელდება სამხედრო, თავდაცვითი, ეროვნული უსაფრთხოების, კვლევისა და განვითარებისთვის შექმნილ ხელოვნური ინტელექტის სისტემებზე.

აქტით განსაზღვრულია სხვადასხვა ვალდებულება ხელოვნური ინტელექტის სისტემების პოტენციური რისკებისა და ზემოქმედების დონის მიხედვით. მასში კლასიფიცირებულია “AI” სისტემების სამი ძირითადი ჯგუფი, რომელთა მიმართაც განსხვავებული მოთხოვნები და ვალდებულებებია დადგენილი (“unacceptable-risk, high-risk, limited-risk”).

💡 დაუშვებელი რისკი (“unacceptable-risk”) მოიაზრებს იმგვარ პროგრამებს, რომლებიც აშკარა საფრთხეს უქმნის ადამიანის ფუნდამენტურ უფლებებს მათ შორისაა: ემოციების ამომცნობი, ადამიანთა ქცევებით მანიპულირების პროგრამები. აგრეთვე, იმგვარი სისტემები, რომლითაც შესაძლებელია სახის ამოცნობის მიზნით ადამიანების გამოსახულებების არამიზნობრივი შეგროვება; დანაშაულის პროგნოზირება, მომსახურების მიმწოდებელი ორგანიზაციების მიერ საჯარო სივრცეში რეალურ დროში ბიომეტრიული მონაცემების გამოყენება და სხვა.

💡 მაღალი რისკი (“high-risk”) - ადამიანის უსაფრთხოებისა და ჯანმრთელობისთვის მაღალი რისკის შემცველი სისტემები. ამგვარი კატეგორიის სისტემები, რომელთა

[6] “Data Guidance”, EU: European Parliament adopts AI Act, 13 March 2024, <https://www.dataguidance.com/news/eu-european-parliament-adopts-ai-act>, [25.03.2024].

[7] Council of the European Union, <https://data.consilium.europa.eu/doc/document/ST-5662-2024-INIT/en/pdf>, [25.03.2024]. აქტი აერთიანებს 12 თავსა და 85 მუხლს.

მიმართ გამოიყენება მკაცრი მოთხოვნები: ფუნდამენტურ უფლებებზე ზეგავლენის შეფასება; ხელოვნური ინტელექტის სისტემის რეგისტრაცია ევროკავშირის მონაცემთა საჯარო ბაზაში, სიზუსტის, მდგრადობისა და გამჭვირვალობის ვალდებულებები. ამგვარი სისტემები შეიძლება იყოს: სამედიცინო მოწყობილობები, ემოციების ამომცნობი სისტემები, საგანმანათლებლო და პროფესიულ ტრენინგებში გამოყენებული სხვადასხვა სისტემა და სხვა.

💡 დაბალი რისკი ("limited-risk") მოიაზრებს სხვადასხვა ტექსტებისა და ფოტოების მაგენერირებელ „ჩატბოტებსა" და სხვა მსგავს პროგრამებს. ისინი ლიმიტირებული რისკით ხასიათდება, ამიტომაც მათ გამჭვირვალობის მაღალი სტანდარტის დაცვის ვალდებულება არ გააჩნიათ.

ხელოვნური ინტელექტის აქტით, ასევე, მოწესრიგებულია სანქციების სახეთა განსაზღვრის და დაკისრების საკითხები: ჯარიმა, გაფრთხილება და არაფულადი ღონისძიებები. მნიშვნელოვანია, რომ გათვალისწინებული სანქცია უნდა იყოს ეფექტიანი და დარღვევის პროპორციული, ასევე, მისი განსაზღვრისას მიზანშეწონილია მცირე და საშუალო ბიზნესის ინტერესებისა და ეკონომიკური მდგომარეობის გათვალისწინება.

რაც შეეხება უშუალოდ ჯარიმებს, აკრძალული სისტემების გამოყენებისთვის, აქტით გათვალისწინებულია ფულადი ჯარიმა €35 მილიონამდე ან კომპანიის წლიური ბრუნვის 7%-ის ოდენობით.

ფოტო: europarl.europa.eu

აღსანიშნავია, რომ "AI აქტი" ჯერ კიდევ გადის ენობრივ რედაქტირებას. საბოლოო ვერსიის მომზადების შემდეგ, აქტი სრულად ამოქმედდება გამოქვეყნებიდან 24 თვეში, თუმცა მისი ძალაში შესვლა იგეგმება ეტაპობრივად. პირველ 6 თვეში, გათვალისწინებულია „აკრძალულ სისტემებთან" დაკავშირებული წესების ამოქმედება, რომელიც აერთიანებს სოციალური შეფასების, აგრეთვე, სახის და ემოციის ამომცნობი ცალკეული სისტემების, ასევე, სამართალდამცავი ორგანოების მიერ საჯარო თავშეყრის ადგილებში, რეალურ დროში დისტანციური ბიომეტრიული იდენტიფიკაციის სისტემების გამოყენების აკრძალვას და სხვა.

გაერთიანებული სამეფოს მონაცემთა დაცვის საზედამხედველო ორგანო საქველმოქმედო ორგანიზაციებს პირდაპირი მარკეტინგის წესების დაცვისკენ მოუწოდებს

5.03.2024

ფოტო: ico.org.uk

გაერთიანებული სამეფოს მონაცემთა დაცვის საზედამხედველო ორგანომ მოუწოდა საქველმოქმედო ორგანიზაციებს, შეწყვიტონ პირდაპირი მარკეტინგის მიზნით, არასასურველი მოკლეტექსტური შეტყობინებების გაგზავნა იმ პირებისთვის, რომლებსაც თანხმობა არ განუცხადებიათ აღნიშნულის თაობაზე.[8]

გაერთიანებულ სამეფოში დაფუძნებული საქველმოქმედო ორგანიზაცია "Penny Appeal"-ის წარმომადგენლებმა 460 000-ზე მეტ პირს გაუგზავნეს არასასურველი შეტყობინება, ხოლო ათი დღის განმავლობაში - 52 000 პირს, რომელთაც თანხმობა არასდროს განუცხადებიათ აღნიშნულის თაობაზე ან აშკარა ფორმით უარი თქვეს მათ მიღებაზე. მოკლეტექსტური შეტყობინებები იგზავნებოდა 2022 წლის აპრილიდან მაისამდე, რამადანის პერიოდის განმავლობაში, რათა ყოველდღიურად შეეხსენებინათ პირებისთვის შემოწირულობის გაღების შესახებ.

შედეგად, გაერთიანებული სამეფოს მონაცემთა დაცვის საზედამხედველო ორგანომ მიიღო 354 განაცხადი. განმცხადებლებმა მონაცემთა დაცვის საზედამხედველო ორგანოს შეატყობინეს, რომ მათი სურვილის მიუხედავად, მაინც იღებდნენ მოკლეტექსტურ შეტყობინებებს საქველმოქმედო ორგანიზაციისგან და მოითხოვეს აღნიშნულის შეწყვეტა.

"ICO"-მ შესწავლის შედეგად დაადგინა, რომ საქველმოქმედო ორგანიზაციამ შექმნა მონაცემთა ახალი ბაზა, რომელშიც შეუძლებელი იყო მონაცემთა სუბიექტების უარის აღრიცხვა. შესაბამისად, შეტყობინებები ეგზავნებოდა ყველას, ვისაც ბოლო ხუთი წლის განმავლობაში შეხება ჰქონდა ორგანიზაციასთან.

"ICO"-ს განცხადებით, საქველმოქმედო ორგანიზაციას განესაზღვრა 30 დღიანი ვადა, რათა შეეწყვიტა მარკეტინგული შინაარსის შეტყობინებების გაგზავნა მონაცემთა სუბიექტის თანხმობის გარეშე.

მონაცემთა დაცვის საზედამხედველო ორგანო შეახსენებს ყველა საქველმოქმედო ორგანიზაციას, მათ

[8] Information Commissioner's Office ("ICO"), ICO warns charities about direct marketing rules as it orders Penny Appeal to stop sending spam texts, 05 March 2024, <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/03/ico-warns-charities-about-direct-marketing-rules-as-it-orders-penny-appeal-to-stop-sending-spam-texts/>, [25.03.2024].

შორის, მონაცემთა დამუშავებაზე სხვა პასუხისმგებელ პირებს, მონაცემთა სუბიექტის წინასწარ გამოხატული თანხმობის გარეშე მარკეტინგული შინაარსის შეტყობინებების, ზარების ან ელ. ფოსტის გაგზავნის კანონსაწინააღმდეგო ხასიათის შესახებ. გარდა ამისა, თანხმობა, არ შეიძლება იყოს აღქმული, როგორც მომსახურების მიღების პირობა. ვინაიდან იგი უნდა იყოს მონაცემთა სუბიექტის თავისუფალი ნების საფუძველზე გაცემული.

ევროკავშირის მართლმსაჯულების სასამართლომ ("CJEU") არაკანონიერად დამუშავებული პერსონალური მონაცემების წაშლის თაობაზე გადაწყვეტილება მიიღო

14.03.2024

ფოტო: european-union.europa.eu

2024 წლის 14 მარტს, ევროკავშირის მართლმსაჯულების სასამართლომ ("CJEU") პერსონალურ მონაცემთა წაშლის საკითხებთან დაკავშირებით მიიღო გადაწყვეტილება.[9]

ფაქტობრივი გარემოებები:

უნგრეთის მუნიციპალურმა ადმინისტრაციამ ("Újpest administration") გადაწყვიტა, რომ ფინანსური დაეხმარება გაეწია იმ პირებისთვის, რომლებიც დაზარალდნენ "Covid-19" პანდემიის შედეგად და აკმაყოფილებდნენ დახმარების გასაწევად საჭირო კრიტერიუმებს. ამ მიზნით, მუნიციპალურმა ადმინისტრაციამ ორი სხვადასხვა უწყებისგან მოიპოვა მონაცემთა სუბიექტთა პერსონალური მონაცემები, რომლებიც საჭირო იყო შესაბამისი კრიტერიუმების დასადასტურებლად.

ზემოაღნიშნულ ფაქტებთან მიმართებით, პერსონალური მონაცემების კანონიერი დამუშავების საკითხებზე, უნგრეთის მონაცემთა დაცვის საზედამხედველო ორგანომ საკუთარი ინიციატივით დაიწყო შესწავლა. საზედამხედველო ორგანომ დაადგინა, რომ უნგრეთის მუნიციპალურმა ადმინისტრაციამ დაარღვია "GDPR"-ის მე-5, მე-14 და მე-12(1) მუხლების დებულებები, რადგან მონაცემთა სუბიექტებს, 1 თვის განმავლობაში არ მიაწოდა ინფორმაცია „დახმარების პროგრამის" ფარგლებში დამუშავებული პერსონალური მონაცემების კატეგორიების, მონაცემთა დამუშავების მიზნებისა და მათი უფლებების განხორციელების შესახებ.

[9] CJEU, Judgment of the Court (Fifth Chamber), 14 March 2024, Case C-46/23, <https://curia.europa.eu/juris/document/document.jsf;jsessionid=2403574B62BE828E89CA4D50028427 10?text=&docid=283833&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=5273970>, [24.03.2024].

✓ ყოველივე აღნიშნულიდან გამომდინარე, მონაცემთა დაცვის საზედამხედველო ორგანომ უნგრეთის მუნიციპალურ ადმინისტრაციას, "GDPR"-ის 58(2)(d) მუხლზე დაყრდნობით, დაავალა მონაცემთა სუბიექტების მონაცემთა წაშლა.

უნგრეთის მუნიციპალურმა ადმინისტრაციამ მონაცემთა დაცვის საზედამხედველო ორგანოს მიერ მიღებული გადაწყვეტილება ბუდაპეშტის სასამართლოში გაასაჩივრა ("Budapest Hight Court"). ადმინისტრაციის მტკიცებით, მონაცემთა დაცვის საზედამხედველო ორგანოს, "GDPR"-ის 58(2)(d)-ე და მე-17 მუხლების შესაბამისად, არ ჰქონდა უფლებამოსილება, დაევალებინა პერსონალურ მონაცემთა წაშლა მონაცემთა სუბიექტის მოთხოვნის არარსებობის გამო.

"GDPR"-ის დებულებებთან დაკავშირებით განმარტებების მიღების მიზნით, ბუდაპეშტის სასამართლომ "CJEU"-ს შემდეგი კითხვებით მიმართა:

? ანიჭებს თუ არა "GDPR"-ის 58(2)(c)(d)(g)-ე მუხლი მონაცემთა დაცვის საზედამხედველო ორგანოს უფლებას, რომ "GDPR"-ის მე-17 მუხლის შესაბამისად დაავალოს მონაცემთა დამუშავებისთვის პასუხისმგებელ და დამუშავებაზე უფლებამოსილ პირებს უკანონოდ დამუშავებული პერსონალური მონაცემების წაშლა, მონაცემთა სუბიექტის გამოხატული მოთხოვნის არსებობის მიუხედავად?

? კითხვაზე დადებითი პასუხის შემთხვევაში, ენიჭება თუ არა რაიმე მნიშვნელობა პერსონალური მონაცემების მოპოვების წყაროს (მაგ., მონაცემები მოპოვებული იქნა უშუალოდ მონაცემთა სუბიექტისგან თუ სხვა წყაროსგან)?

❶ პირველ კითხვასთან მიმართებით, სასამართლომ ყურადღება გაამახვილა "GDPR"-ის მე-17(1) მუხლზე, რომლის საფუძველზე მონაცემთა სუბიექტს უფლება აქვს, მოითხოვოს მის შესახებ არსებული მონაცემების წაშლა, ხოლო თავის მხრივ, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, წაშალოს ისინი გაუმართლებელი დაყოვნების გარეშე. აღნიშნული ეხება, მათ შორის, იმ შემთხვევასაც, როდესაც მონაცემების დამუშავება განხორციელდა უკანონოდ ("GDPR"-ის მე-17(1)(d)).

დამატებით, აღინიშნა "GDPR"-ის 58(2)(d)-ე მუხლი, რომლის თანახმად მონაცემთა დაცვის საზედამხედველო ორგანოს წარმოეშობა უფლებამოსილება, დაავალოს დამუშავებისთვის პასუხისმგებელ ან დამუშავებაზე უფლებამოსილ პირებს მონაცემთა დამუშავების პროცესის "GDPR"-თან შესაბამისობაში მოყვანა, საჭიროების შემთხვევაში, სათანადო ფორმითა და შესაბამისი ვადის დაწესებით.

ამასთან, "GDPR"-ის 58(2)(g)-ე მუხლის ფარგლებში საზედამხედველო ორგანო უფლებამოსილია, მოითხოვოს მონაცემთა შესწორება, წაშლა ან დამუშავების შეზღუდვა "GDPR"-ის მე-

16, მე-17 და მე-18 მუხლების შესაბამისად და აღნიშნულის თაობაზე უზრუნველყოს პერსონალური მონაცემების მიმღებთა ინფორმირება “GDPR”-ის მე-17(2) და მე-19 მუხლების ფარგლებში.

“CJEU”-ს შეფასებით, “GDPR”-ის სტანდარტების დაცვის უზრუნველსაყოფად, არსებითად მნიშვნელოვანია, მონაცემთა დაცვის საზედამხედველო ორგანოს ჰქონდეს უფლებამოსილება, გადადგას შესაბამისი ქმედითი ნაბიჯები. საზედამხედველო ორგანომ ღონისძიებები შეიძლება, განახორციელოს საკუთარი ინიციატივით (“GDPR”-ის 58(2) მუხლი). შესაბამისად, თუ მონაცემთა დაცვის საზედამხედველო ორგანო მიიჩნევს, რომ მონაცემთა დამუშავება არ აკმაყოფილებს “GDPR”-ის მოთხოვნებს, მონაცემთა სუბიექტის წინასწარი მოთხოვნის არსებობის მიუხედავად, მიღებულ უნდა იქნეს შესაბამისი ზომები გამოვლენილი დარღვევების გამოსასწორებლად.

“CJEU”-ს შეფასებით, “GDPR”-ის 58(2)(d)(g)-ე მუხლი უნდა იქნას განმარტებული იმგვარად, რომ წევრი სახელმწიფოს მონაცემთა დაცვის საზედამხედველო ორგანო უფლებამოსილია, დაავალოს მონაცემთა დამუშავებისთვის პასუხისმგებელ და დამუშავებაზე უფლებამოსილ პირებს უკანონოდ დამუშავებული პერსონალური მონაცემების წაშლა, მიუხედავად მონაცემთა სუბიექტის წინასწარი მოთხოვნისა.

მეორე კითხვასთან დაკავშირებით სასამართლომ აღნიშნა, რომ “GDPR”-ის 58(2)-ე მუხლი არ აწესრიგებს პერსონალური მონაცემების მოპოვების წყაროსთან დაკავშირებულ საკითხს, საზედამხედველო ორგანოს მიერ ღონისძიებების განხორციელების კონტექსტში. აღნიშნულის მსგავსად, “GDPR”-ის მე-17(1) მუხლი, რომელიც განსაზღვრავს მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის ვალდებულებას, წაშალოს უკანონოდ დამუშავებული პერსონალური მონაცემები, არ ითვალისწინებს რაიმე მოთხოვნას შეგროვებული პერსონალური მონაცემების მოპოვების წყაროსთან მიმართებით.

“CJEU”-ს გადაწყვეტილებით, “GDPR”-ის 58(2)-ე მუხლი უნდა განიმარტოს იმ მნიშვნელობით, რომ წევრი სახელმწიფოს მონაცემთა დაცვის საზედამხედველო ორგანოს უფლებამოსილება, უკანონოდ დამუშავებული პერსონალური მონაცემების წაშლის მოთხოვნასთან მიმართებით, გავრცელდეს როგორც მონაცემთა სუბიექტის მიერ მიღებულ, ისე სხვა წყაროდან მოპოვებულ ინფორმაციაზე.

გაეროს გენერალურმა ასამბლეამ ხელოვნური ინტელექტის სისტემებთან დაკავშირებით რეზოლუცია მიიღო

11.03.2024

ფოტო: undocs.org

2024 წლის 11 მარტს, გაეროს გენერალურმა ასამბლეამ მიიღო რეზოლუცია,[10] რომელიც შეეხება ხელოვნური ინტელექტის სისტემების უსაფრთხო, დაცულ და სანდო გამოყენებას. გენერალური ასამბლეა აცნობიერებს, რომ გაუმართავი ხელოვნური ინტელექტის სისტემები შეიძლება, გახდეს როგორც ქვეყნის შიგნით, ისე სახელმწიფოთა შორის დავის საგანი. დამატებით, არსებობს ალბათობა იმისა, რომ ხელოვნური ინტელექტის არასათანადო გამოყენებამ შესაძლოა, წარმოშვას დისკრიმინაცია და შელახოს ადამიანის უფლებები და ძირითადი თავისუფლებები, მათ შორის, პირადი ცხოვრების ხელშეუხებლობა.

რეზოლუციას მხარი დაუჭირა 120-ზე მეტმა წევრმა სახელმწიფომ, მათ შორის საქართველომ. მხარდამჭერ სახელმწიფოთა მიზანია, ხელოვნური ინტელექტი გახდეს ფიზიკურ პირებზე მორგებული, მარტივად გასაგები, ეთიკური, ასევე, უზრუნველყოს პირადი ცხოვრების ხელშეუხებლობა და ორიენტირებული იყოს მდგრადი განვითარების მიზნებზე.

აღსანიშნავია, რომ რეზოლუცია არ მიემართება სამხედრო მიზნით ხელოვნური ინტელექტის სისტემების გამოყენებას.

გენერალური ასამბლეის რეზოლუციის მიზანია:

- ☑ წევრი სახელმწიფოების, კერძო სექტორის, სამოქალაქო საზოგადოების, კვლევითი ორგანიზაციების და მედიის წახალისება, რათა შეიმუშაონ წესები ხელოვნური ინტელექტის უსაფრთხო, დაცულ და სანდო გამოყენებასთან დაკავშირებით;
- ☑ მოუწოდოს წევრ სახელმწიფოებს, რათა დაეხმარონ განვითარებად ქვეყნებს ხელოვნური ინტელექტის სისტემების გამოყენებაში;
- ☑ მოუწოდოს სახელმწიფოებს, რათა თავი შეიკავონ ან შეწყვიტონ ხელოვნური ინტელექტის სისტემების გამოყენება, რომლებიც ვერ აკმაყოფილებს ადამიანის უფლებათა დაცვის საერთაშორისო სტანდარტებს და რისკს უქმნის ადამიანის უფლებებსა და თავისუფლებებს;
- ☑ წაახალისოს წევრი სახელმწიფოები იმისათვის, რომ ხელი შეუწყონ

[10] United Nations, General Assembly, Resolution: "Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development", 11 March 2024, <https://documents.un.org/doc/undoc/ltd/n24/065/92/pdf/n2406592.pdf?token=I8c0wH9wcYcqFwValV&fe=true>, [25.03.2024].

ხელოვნური ინტელექტის სისტემების უსაფრთხო, დაცულ და სანდო გამოყენებას შემდეგი აქტივობების შესრულებით:

- ხელოვნური ინტელექტის სისტემების იდენტიფიკაციის, კლასიფიკაციის, შეფასებისა და შემოწმების უზრუნველსაყოფად შესაბამისი ღონისძიებების განხორციელება;
- მომხმარებელთა უკუკავშირის მიღების მექანიზმის შემუშავება;
- რისკის მართვის მექანიზმების, მათ შორის, პერსონალურ მონაცემთა დაცვის პოლიტიკის შემუშავება და დანერგვა;
- საერთაშორისო დონეზე გამოყენებადი ტექნიკური ინსტრუმენტებისა და სტანდარტების შემუშავება;
- ხელოვნური ინტელექტის სისტემების შემოწმებისა და შეფასებისას პირადი ცხოვრების ხელშეუხებლობისა და პერსონალურ მონაცემთა დაცვის უფლებების გათვალისწინება;
- ხელოვნური ინტელექტის სისტემების გამჭვირვალობის, განჭვრეტადობის, სანდოობისა და ინდივიდთა მიერ ზედამხედველობის განხორციელების ხელშეწყობა.
- საუკეთესო პრაქტიკის გაზიარება და საერთაშორისო თანამშრომლობის ხელშეწყობა;
- ხელოვნური ინტელექტის სისტემებთან დაკავშირებით ანალიტიკური კვლევების წახალისება.[11]

ევროპის მონაცემთა დაცვის ზედამხედველმა (“EDPS”) გამოძიების შედეგად დაადგინა რომ, ევროკომისიის მიერ “Microsoft 365“-ის გამოყენებამ დაარღვია ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაცია“ (“GDPR“)

11.03.2024

ფოტო: edps.europa.eu

ევროპის მონაცემთა დაცვის ზედამხედველმა[12] (“EDPS”) შესწავლის

[11] “Data Guidance”, International: UN General Assembly adopted resolution on AI systems, 22 March 2024, <https://www.dataguidance.com/news/international-un-general-assembly-adopted-resolution-ai>, [25.03.2024].

[12] “EDPS”, Press Release, Brussels, 11 March 2024, European Commission’s use of “Microsoft 365” infringes data protection law for EU institutions and bodies, <https://www.edps.europa.eu/system/files/2024-03/EDPS-2024-05-European-Commission_s-use-of-M365-infringes-data-protection-rules-for-EU-institutions-and-bodies_EN.pdf>, [25.03.2024].

შედეგად დაადგინა, რომ ევროკომისიამ “Microsoft 365“-ის გამოყენებისას დაარღვია მონაცემთა დაცვის რამდენიმე წესი. “EDPS”-მა დაადგინა, რომ ევროკომისიამ დაარღვია “GDPR”-ის რამდენიმე დებულება; ევროკავშირის მონაცემთა დაცვის სამართალი; ევროკავშირის ინსტიტუტების, ორგანოების, ოფისებისა და სააგენტოებისთვის, მათ შორის, პერსონალური მონაცემების ევროკავშირის/ევროპის ეკონომიკური ზონის გარეთ პერსონალური მონაცემების გადაცემის შესახებ სამართლებრივი ჩარჩოს დებულებები. კერძოდ, ევროკომისიამ ვერ უზრუნველყო მონაცემთა დაცვის შესაბამისი გარანტიები ევროკავშირის ფარგლებს გარეთ გადაცემულ ინფორმაციასთან მიმართებით. გარდა ამისა, “Microsoft 365”-თან დადებულ ხელშეკრულებაში ევროკომისიამ საკმარისად არ დააკონკრეტა, თუ რა კატეგორიის პერსონალური მონაცემები უნდა დამუშავებულიყო, ასევე, რა მიზნები განისაზღვრა “Microsoft 365”-ის გამოყენებისას. გამოვლენილი დარღვევები, ასევე, ეხებოდა მონაცემთა დამუშავებასა და პერსონალური მონაცემების გადაცემას.

ევროპის მონაცემთა დაცვის ზედამხედველმა, ვოიჩეკ ვიევიოროვსკიმ განაცხადა, რომ: „ევროკავშირის ინსტიტუტების, ორგანოების, ოფისებისა და სააგენტოების პასუხისმგებლობაა, უზრუნველყონ, შესაბამისი დაცვის გარანტიები პერსონალური მონაცემების ნებისმიერი დამუშავებისას ევროკავშირის/EEA-ს ფარგლებში თუ ფარგლებს გარეთ, ღრუბლოვან სისტემაზე დაფუძნებული სერვისების კონტექსტში. აღნიშნული აუცილებელია იმის უზრუნველსაყოფად, რომ მონაცემთა სუბიექტის ინფორმაცია დაცული იყოს, რეგულაციის შესაბამისად.“

ზემოაღნიშნულიდან გამომდინარე, “EDPS”-მა დაავალა ევროკომისიას შეეწყვიტა ნებისმიერი პერსონალური მონაცემების მიმოცვლა “Microsoft”-თან და მის შვილობილ კომპანიებთან, რომლებსაც არ გააჩნდათ დაცვის შესაბამისი გარანტიები, მიუხედავად იმისა ვრცელდებოდა თუ არა მათზე “GDPR“. აღნიშნული დავალების შესრულების ვადად 2024 წლის 9 დეკემბერი განისაზღვრა.

“EDPS”-მა მიიჩნია, რომ მის მიერ განსაზღვრული ღონისძიებები არის შესაბამისი, აუცილებელი და პროპორციული აღმოჩენილი დარღვევების სერიოზულობისა და ხანგრძლივობის გათვალისწინებით.

მნიშვნელოვანია აღინიშნოს, რომ “EDPS”-მა გაითვალისწინა ევროკომისიის მიერ საზოგადოებრივი ინტერესის შესრულებისა და კომისიისთვის მინიჭებული ოფიციალური უფლებამოსილების განხორციელების შესაძლებლობა. სწორედ ამიტომ ევროკომისიას მიეცა სათანადო დრო, რათა უზრუნველეყო მონაცემთა დამუშავების რეგულაციასთან შესაბამისობა.

აღნიშნულ შესწავლას, წინ უძღოდა 2020 წლის 16 ივლისის ევროკავშირის მართლმსაჯულების სასამართლოს “Schrems II” გადაწყვეტილება. მისი

მიზანი იყო ევროკავშირის ინსტიტუტებისა და ორგანოების მიერ “Microsoft”-ის პროდუქტებისა და სერვისების გამოყენების შესახებ, “EDPS”-ის მიერ გაცემულ რეკომენდაციებთან შესაბამისობის შეფასება.

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