პერსონალურ მონაცემთა
დაცვის სამსახური

მსოფლიო პრაქტიკა

იანვარი / 2023

მთავარი სიახლეები

ვროკავშირის მართლმსაჯულების სასამართლომ დაადგინა, რომ ყველა ადამიანს აქვს უფლება, იცოდეს ვის გაეგზავნა მისი პერსონალური მონაცემები

“EDPB”-მ საჯარო სექტორის მიერ „ღრუბლოვანი სერვისების“ გამოყენებისთვის რეკომენდაციები და “მზა-ჩანაწერების“ ბანერის სამუშაო ჯგუფის საქმიანობის შესახებ ანგარიში გამოაქვეყნა

ირლანდიის მონაცემთა დაცვის საზედამხედველო ორგანომ (“DPC”)“WhatsApp”-ის აპლიკაცია “GDPR”-ის მოთხოვნათა დარღვევის გამო დააჯარიმა

საფრანგეთის მონაცემთა დაცვის საზედამხედველო ორგანომ(“CNIL”) “TIKTOK”-ი ხუთი მილიონი ევროს ოდენობით დააჯარიმა

ევროკავშირის მართლმსაჯულების სასამართლომ დაადგინა, რომ ყველა ადამიანს აქვს უფლება, იცოდეს ვის გაეგზავნა მისი პერსონალური მონაცემები

12.01.2023

ევროკავშირის მართლმსაჯულების სასამართლომ საქმეზე C 154/21, დაადგინა, რომ ყველა ადამიანს აქვს უფლება იცოდეს, ვის გაეგზავნა მისი პერსონალური მონაცემები.

მიუხედავად ამისა, დამმუშავებელს შეუძლია, მონაცემთა სუბიექტს აცნობოს მხოლოდ მონაცემთა მიმღების კატეგორიების შესახებ, თუ შეუძლებელია მონაცემთა მიმღებების იდენტიფიცირება ან მოთხოვნა აშკარად უსაფუძვლო ან გადაჭარბებულია.

ფოტო: european-union.europa.eu

ფაქტობრივი გარემოებები: მოქალაქემ სთხოვა "Österreichische Post"-ს – საფოსტო და ლოგისტიკური მომსახურების მთავარ ოპერატორს ავსტრიაში, გაემჟღავნებინა მისთვის მონაცემთა იმ მიმღებთა ვინაობა, რომლებსაც საფოსტო ოპერატორმა მონაცემთა სუბიექტის მონაცემები გადასცა.

მონაცემთა სუბიექტი აღნიშნული მოთხოვნის წარდგენისას ევროკავშირის მონაცემთა დაცვის ზოგად რეგულაციას ("GDPR") დაეყრდნო. "GDPR"-ით გათვალისწინებულია, რომ მონაცემთა სუბიექტს უფლება აქვს, მონაცემთა დამმუშავებლისგან მიიღოს ინფორმაცია მონაცემების მიმღებთა ან მონაცემთა მიმღების კატეგორიების შესახებ, რომელთაც გადაეცათ ან მომავალში შეიძლება, გადაეცეთ მისი პერსონალური მონაცემები.

მოქალაქის მოთხოვნის საპასუხოდ, "Österreichische Post"-მა განაცხადა, რომ იგი, როგორც სატელეფონო წიგნების გამომცემელი, ამუშავებს პერსონალურ მონაცემებს კანონით განსაზღვრულ ფარგლებში და სავაჭრო პარტნიორებს აღნიშნულ მონაცემებს მარკეტინგული მიზნებისთვის სთავაზობს. შესაბამისად, მოქალაქემ "Österreichische Post"-ის წინააღმდეგ ავსტრიის სასამართლოებში სარჩელი შეიტანა.

სასამართლო პროცესზე, "Österreichische Post"-მა დამატებით აცნობა მოქალაქეს, რომ მისი მონაცემები გადაეგზავნა მომხმარებელს, მათ შორის რეკლამის განმთავსებლებს, რომლებიც საქმიანობას ფოსტისა და საკანცელარიო მაღაზიების გამოყენებით ახორციელებენ, ასევე, IT კომპანიებს, ელექტრონული ფოსტის მისამართების სიის პროვაიდერებს, საქველმოქმედო ორგანიზაციებს, არასამთავრობო ორგანიზაციებს, პოლიტიკურ პარტიებს.

კითხვები ევროკავშირის მართლმსაჯულების სასამართლოს წინაშე:

ავსტრიის უზენაესმა სასამართლომ, რომელიც განიხილავდა დავას, მიმართა ევროკავშირის მართლმსაჯულების სასამართლოს განმარტებისა და წინასწარი გადაწყვეტილების მიღების თხოვნით შემდეგ საკითხებთან დაკავშირებით:

- უზრუნველყოფს “GDPR”-ი მონაცემთა დამმუშავებლისთვის დისკრეციას, გაამჟღავნოს მონაცემების მიმღებთა კონკრეტული ვინაობა თუ მხოლოდ მონაცემთა მიმღების კატეგორიები?
- უზრუნველყოფს “GDPR”-ი მონაცემთა სუბიექტის უფლებას – იცოდეს მისი პერსონალური მონაცემების მიმღები პირების კონკრეტული ვინაობა?

ფოტო: shutterstock.com

სასამართლოს გადაწყვეტილება:

2023 წლის 12 იანვრის გადაწყვეტილებაში სასამართლომ განმარტა, რომ როდესაც პერსონალური მონაცემები გამჟღავნებულია ან მომავალში გამჟღავნდება მონაცემთა მიმღებისთვის, მონაცემთა დამმუშავებელი ვალდებულია, მოთხოვნის შემთხვევაში, მიაწოდოს მონაცემთა სუბიექტს ინფორმაცია მონაცემთა მიმღების რეალური ვინაობის შესახებ. ხოლო მაშინ, როდესაც შეუძლებელია მონაცემთა მიმღებთა იდენტიფიცირება, მონაცემთა დამმუშავებელს შეუძლია, მიუთითოს მხოლოდ მონაცემთა მიმღების კატეგორიებზე. აღნიშნული, ასევე, შესაძლებელია იმ შემთხვევაში, როდესაც მონაცემთა დამმუშავებელი წარმოაჩენს, რომ მოთხოვნა აშკარად უსაფუძვლო ან გადაჭარბებულია.

სასამართლომ გამოყო შემდეგი რამდენიმე შემთხვევა:

- მონაცემთა სუბიექტის შესახებ ინფორმაცია გადაცემულია მონაცემთა მიმღებისთვის და მონაცემთა მიმღების იდენტიფიცირება შესაძლებელია;
- მონაცემთა მიმღების ვინაობის გამჟღავნება კონკრეტულ მომენტში არ არის შესაძლებელი;
- მონაცემთა მიმღების ვინაობის გამჟღავნების მოთხოვნა აშკარად უსაფუძვლო ან გადაჭარბებულია.

მონაცემთა სუბიექტის შესახებ ინფორმაცია გადაცემულია მონაცემთა მიმღებისთვის და მონაცემთა მიმღების იდენტიფიცირება შესაძლებელია:

სასამართლომ საკითხის სისტემური ინტერპრეტაციისთვის “GDPR”-ის რელევანტური ნორმები 5 საფეხურად განმარტა:

1. “GDPR”-ის მე-15 მუხლის პირველი პუნქტის „c“ ქვეპუნქტი ადგენს, რომ მონაცემთა სუბიექტს უფლება აქვს, მიიღოს მონაცემთა დამმუშავებლისგან დასტური, მუშავდება თუ არა მისი პერსონალური მონაცემები და დადებითი პასუხის შემთხვევაში, მიიღოს ინფორმაცია მონაცემთა მიმღების პერსონალური მონაცემებისა და მონაცემების მიმღებთა კატეგორიების შესახებ, რომლებსაც გადაეცა ან მომავალში შეიძლება, გადაეცეს მისი პერსონალური მონაცემები. აღსანიშნავია, რომ ტერმინები „მონაცემთა მიმღები“ და „მონაცემთა მიმღების კატეგორიები“ ამ დებულებაში გამოიყენება

თანმიმდევრულად, მათ შორის პრიორიტეტის დადგენის გარეშე.

“GDPR”-ის მე-15 მუხლის პირველი პუნქტის „c“ ქვეპუნქტის ფორმულირება ცალსახად არ ადგენს, აქვს თუ არა მონაცემთა სუბიექტს უფლება, მიიღოს ინფორმაცია მონაცემთა მიმღების კონკრეტული ვინაობის შესახებ, როდესაც მონაცემთა მიმღებს უკვე გადაეცა ან შეიძლება მომავალში გადაეცეს მისი პერსონალური მონაცემები.

რაც შეეხება “GDPR”-ის მე-15 მუხლის 1-ლი პუნქტის „c“ ქვეპუნქტის კონტექსტს, უნდა აღინიშნოს, რომ “GDPR”-ის პრეამბულის 63-ე პუნქტის თანახმად, მონაცემთა სუბიექტს უნდა ჰქონდეს უფლება, მიიღოს ინფორმაცია პერსონალური მონაცემების მიმღების შესახებ. ეს უფლება არ შეიძლება, შემოიფარგლოს მხოლოდ მონაცემთა მიმღებთა კატეგორიებით.

ფოტო: privacycompliancehub.com

2 ხელმისაწვდომობის უფლების პატივისცემის მიზნით, ფიზიკური პირების პერსონალური მონაცემების ყველა დამუშავება უნდა შეესაბამებოდეს “GDPR”-ის მე-5 მუხლით დადგენილ პრინციპებს.

აღნიშნული პრინციპები, მათ შორის “GDPR”-ის მე-5 მუხლის პირველი პუნქტის „a“ ქვეპუნქტით განსაზღვრული „გამჭვირვალობის პრინციპი“, “GDPR”-ის პრეამბულის 39-ე პუნქტის თანახმად, ადგენს მონაცემთა სუბიექტის ინფორმირების ვალდებულებას მისი პერსონალური მონაცემების დამუშავების მეთოდების შესახებ, ასევე, ინფორმაციის ადვილად ხელმისაწვდომობისა და განჭვრეტადობის ვალდებულებას.

3 გენერალურმა ადვოკატმა თავისი დასკვნის 21-ე პუნქტში განმარტა, რომ “GDPR”-ის მე-15 მუხლი განსაზღვრავს მონაცემთა სუბიექტისთვის ხელმისაწვდომობის უფლებას, რის შედეგად მონაცემთა სუბიექტს უნდა ჰქონდეს უფლება (როცა ეს შესაძლებელია), მოიპოვოს ინფორმაცია მონაცემთა კონკრეტული მიმღებთა შესახებ, რომლებისთვისაც იყო ან იქნება გამჟღავნებული მონაცემები, ან ინფორმაცია მონაცემთა მიმღების კატეგორიების შესახებ.

4 სასამართლოს დადგენილი პრაქტიკის თანახმად, ხელმისაწვდომობის უფლების განხორციელებამ უნდა მისცეს მონაცემთა სუბიექტს შესაძლებლობა, გადაამოწმოს არა მხოლოდ მასზე არსებული მონაცემების სისწორე, არამედ მათი დამუშავების კანონიერება და რომ ისინი გამჟღავნებულია ავტორიზებული მონაცემთა მიმღებისთვის. ხელმისაწვდომობის უფლება აუცილებელია იმისთვის, რომ მონაცემთა სუბიექტმა, გარემოებებიდან გამომდინარე, გამოიყენოს საკუთარი უფლება მონაცემთა შესწორების, წაშლის („დავიწყების უფლება“) ან დამუშავების შეზღუდვის შესახებ. ასევე, მონაცემთა სუბიექტს უნდა ჰქონდეს შესაძლებლობა, გაასაჩივროს მისი პერსონალური მონაცემების დამუშავება და

მოითხოვოს გარკვეული მოქმედების განხორციელება, როდესაც მონაცემთა სუბიექტს ზიანი მიადგა.

შესაბამისად, აღნიშნულ უფლებათა ეფექტიანობის უზრუნველყოფის მიზნით, როცა მონაცემთა სუბიექტის პირადი მონაცემები უკვე გამჟღავნებულია, იგი ინფორმირებული უნდა იყოს მონაცემთა კონკრეტული მიმღების ვინაობის შესახებ.

5 ასეთი ინტერპრეტაცია დასტურდება, "GDPR"-ის მე-19 მუხლის განმარტებიდან გამომდინარე. იგი ითვალისწინებს მონაცემთა დამმუშავებლის ვალდებულებას, აცნობოს მონაცემთა თითოეულ მიმღებს პერსონალური მონაცემების ნებისმიერი შესწორების, წაშლის ან დამუშავების შეზღუდვის შესახებ. მუხლის მეორე წინადადებაში განმარტებულია მონაცემთა დამმუშავებლის ვალდებულება, აცნობოს მონაცემთა სუბიექტს მონაცემთა მიმღების შესახებ, თუ მონაცემთა სუბიექტი ამას მოითხოვს.

ზემოაღნიშნული კონტექსტური ანალიზიდან გამომდინარეობს, რომ "GDPR"-ის მე-15 მუხლის პირველი პუნქტის „c" ქვეპუნქტი მიზნად ისახავს მონაცემთა სუბიექტის მიმართ გამჭვირვალობის უზრუნველყოფას და მონაცემთა სუბიექტს აძლევს საშუალებას, განახორციელოს "GDPR"-ის მე-16, მე-19, 21-ე, 79-ე და 82-ე მუხლებით გათვალისწინებული უფლებები.

შესაბამისად, "GDPR"-ის მე-15 მუხლის 1-ლი პუნქტის „c" ქვეპუნქტით გათვალისწინებული ხელმისაწვდომობის უფლების თანახმად, მონაცემთა სუბიექტისთვის მიწოდებული ინფორმაცია მაშინ უნდა იყოს მაქსიმალურად ზუსტი, როდესაც ეს ობიექტურად არის შესაძლებელი.

მონაცემთა მიმღების ვინაობის გამჟღავნება შეუძლებელია:

"GDPR"-ის პრეამბულის მე-4 პუნქტის თანახმად, პერსონალური მონაცემების დაცვის უფლება არ არის აბსოლუტური უფლება. აღნიშნული უფლება უნდა განიხილებოდეს საზოგადოებაში მის ფუნქციასთან მიმართებით და სხვა ფუნდამენტურ უფლებებთან „პროპორციულობის პრინციპის" შესაბამისად დაბალანსდეს.

ამგვარად, ცალკეულ გარემოებებში შესაძლებელია, ვერ მოხერხდეს კონკრეტულ მონაცემთა მიმღების შესახებ ინფორმაციის მონაცემთა სუბიექტისთვის მიწოდება. შესაბამისად, წვდომის უფლება შეიძლება, შემოიფარგლოს მონაცემთა მიმღების კატეგორიების შესახებ ინფორმაციით.

მონაცემთა მიმღების ვინაობის გამჟღავნების მოთხოვნა აშკარად უსაფუძვლო ან გადაჭარბებულია:

გასათვალისწინებელია, რომ "GDPR"-ის მე-12 მუხლის მე-5 პუნქტის „b" ქვეპუნქტის თანახმად, მონაცემთა დამმუშავებელს შეუძლია, რეგულაციის მე-5 მუხლის მე-2 პუნქტსა და პრეამბულის 74-ე პუნქტში მითითებული პასუხისმგებლობის პრინციპის შესაბამისად, უარი განაცხადოს, მონაცემთა სუბიექტის მოთხოვნისამებრ მოქმედებაზე, თუ იგი აშკარად უსაფუძვლო ან გადაჭარბებულია. ასეთ შემთხვევაში მონაცემთა დამმუშავებელზეა მტკიცების ტვირთი.

ევროკავშირის მართლმსაჯულების სასამართლომ უფლების დაცვის ადმინისტრაციული და სამოქალაქო მექანიზმების ერთდროულად გამოყენების თაობაზე იმსჯელა

12.01.2023

ერთ-ერთ საქმეზე (C-132/21) ევროკავშირის მართლმსაჯულების სასამართლომ დაადგინა, რომ მონაცემთა დაცვის ზოგადი რეგულაციით გათვალისწინებული უფლების დაცვის ადმინისტრაციული და სამოქალაქო მექანიზმების გამოყენება შეიძლება ერთდროულად და ერთმანეთისგან დამოუკიდებლად.

სასამართლოს განმარტების თანახმად, წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ ამ საშუალებების პარალელურმა რეალიზებამ ზიანი არ მიაყენოს "GDPR"-ის თანმიმდევრულ და ერთგვაროვან გამოყენებას.

ფაქტობრივი გარემოებები:

2019 წლის აპრილში, აქციონერი "BE", შეზღუდული პასუხისმგებლობის საზოგადოების საერთო კრებას დაესწრო, რომელზეც მან კითხვებით მიმართა დირექტორთა საბჭოს წევრებსა და სხვა მონაწილეებს. იგი მოითხოვდა მისთვის საერთო კრების აუდიოჩანაწერის გაგზავნას. თუმცა კომპანიამ მას ჩანაწერის მხოლოდ ის ნაწყვეტები გაუზიარა, რომელიც მხოლოდ აქციონერ "BE"-ის განაცხადებსა და დასმულ კითხვებს ასახავდა. ჩანაწერში სხვა მონაწილეთა პასუხები ასახული არ იყო.

"BE"-მ უნგრეთის საზედამხედველო ორგანოს მიმართა, რათა შესაბამისი კომპანიისთვის დაევალებინა "BE"-სთვის ჩანაწერის სრული სახით გაგზავნა. საზედამხედველო ორგანომ უარი განაცხადა "BE"-ს მოთხოვნის დაკმაყოფილებაზე.

"BE"-მ ეროვნულ სასამართლოს ადმინისტრაციული საჩივრით მიმართა და მონაცემთა დაცვის საზედამხედველო ორგანოს უარი მისი მოთხოვნის დაკმაყოფილებაზე გაასაჩივრა. ამავდროულად, მან უნგრეთის სამოქალაქო სასამართლოებს მიმართა და კომპანიის გადაწყვეტილება სამოქალაქო წესით გაასაჩივრა.

აღნიშნული სამართალწარმოება ეფუძნებოდა "GDPR"-ის დებულებას, რომელიც მონაცემთა სუბიექტს სამართლებრივი დაცვის ეფექტიანი საშუალების გამოყენების შესაძლებლობას ანიჭებს, თუკი მას მიაჩნია, რომ დაირღვა მისი უფლებები. მართალია, ადმინისტრაციულ სასამართლოში საკითხის განხილვა არ დასრულებულა, მაგრამ უნგრეთის სამოქალაქო სასამართლოებმა, საბოლოო გადაწყვეტილებით უკვე დაადგინეს, რომ აღნიშნულმა კომპანიამ დაარღვია "BE"-ს პერსონალურ მონაცემებზე წვდომის უფლება.

კითხვები ევროკავშირის მართლმსაჯულების სასამართლოს წინაშე:

ბუდაპეშტის ზემდგომმა სასამართლომ ევროკავშირის მართლმსაჯულების სასამართლოს შემდეგი საკითხების განმარტების თხოვნით მიმართა:

- ეროვნული საზედამხედველო ორგანოს გადაწყვეტილების ადმინისტრაციული წესით კანონიერების განხილვის კონტექსტში, არის თუ არა სამოქალაქო სასამართლოების მიერ მიღებული

საბოლოო გადაწყვეტილება იმავე ფაქტებსა და სავარაუდო დარღვევასთან დაკავშირებით სავალდებულო ძალის მქონე?

- ადმინისტრაციული და სამოქალაქო-სამართლებრივი უფლების დაცვის საშუალებების პარალელურმა გამოყენებამ შეიძლება თუ არა, გამოიწვიოს ურთიერთგამომრიცხავი გადაწყვეტილებების მიღების საფრთხე?
- შესაძლებელია აღნიშნული უფლების დაცვის საშუალებებიდან რომელიმესთვის პრიორიტეტის მინიჭება?

ფოტო: econonet.net

სასამართლოს გადაწყვეტილება:

მართლმსაჯულების სასამართლოს განმარტებით, "GDPR"-ი საზღვრავს უფლების დაცვის განსხვავებულ საშუალებებს იმ პირებისთვის, რომლებიც ამტკიცებენ, რომ რეგულაციის დებულებები დაირღვა, თუმცა თითოეული ეს საშუალება ისე უნდა იქნეს გამოყენებული, რომ სხვებს არ აყენებდეს ზიანს.

"GDPR"-ი არ ითვალისწინებს რაიმე პრიორიტეტულ ან ექსკლუზიურ კომპეტენციას, იურისდიქციას ან პრიორიტეტის მინიჭების რაიმე წესს საზედამხედველო ორგანოს ან სასამართლოს მიერ განხორციელებულ შეფასებასთან დაკავშირებით.

სასამართლო აღნიშნავს, რომ "GDPR"-ით გათვალისწინებული ადმინისტრაციული და სამოქალაქო დაცვის საშუალებები შეიძლება, განხორციელდეს ერთდროულად და ერთმანეთისგან დამოუკიდებლად.

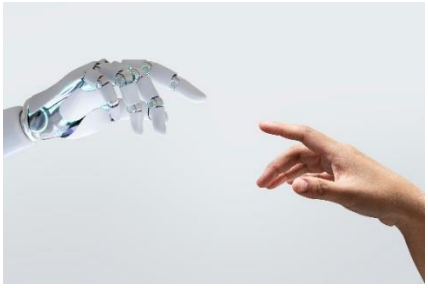
რაც შეეხება მიღებული გადაწყვეტილების შეუსაბამობის რისკს, სასამართლომ ხაზგასმით აღნიშნა, რომ საკუთარი ავტონომიის ფარგლებში თითოეულ წევრ სახელმწიფოს ევალება, უზრუნველყოს მონაცემთა სუბიექტის უფლებების დაცვა აუცილებელი პროცედურული წესების მიღებით. აღნიშნული გამომდინარეობს იქიდან, რომ ერთდროული და ერთმანეთისგან დამოუკიდებელი სამართლებრივი დაცვის საშუალებები "GDPR"-ით გარანტირებული უფლებების ეფექტიან დაცვას, მისი დებულებების თანმიმდევრულ და ერთგვაროვან გამოყენებას ან სასამართლოს წინაშე სამართლებრივი დაცვის ეფექტიან განხორციელებას კითხვის ნიშნის ქვეშ არ აყენებდეს.

"ICO"-ს აღმასრულებელი დირექტორის - *სტეფან ბონერის* ბლოგი ხელოვნური ინტელექტის გამოყენებასთან დაკავშირებული პოტენციური რისკების შესახებ

19.01.2023

ცენტრალურ და ადგილობრივ დონეზე არსებული მმართველობის ორგანოებს პერსონალურ მონაცემებზე მუდმივად მიუწვდებათ ხელი. ეს შეიძლება იყოს ისეთი კატეგორიის მონაცემები,

როგორებიცაა: სახელი, დაბადების თარიღი, პირადი ან ფინანსური ისტორია ან ჯანმრთელობის მდგომარეობის შესახებ ინფორმაცია.



ფოტო: www.freepik.com

მოსახლეობა უნდა დარწმუნდეს, რომ აღნიშნული მონაცემები მუშავდება კანონიერად და სამართლიანად მუშავდება.

გაერთიანებული სამეფოს საინფორმაციო კომისარმა ("ICO") ჩაატარა გამოკითხვა ალგორითმის და მსგავსი სისტემების განვითარების, მიზნისა და ფუნქციების შესასწავლად.

გამოკითხვაში გაერთიანებული სამეფოს თერთმეტმა ადგილობრივი ხელისუფლების ორგანომ მიიღო მონაწილეობა.

გამოკითხვის ფარგლებში ვერ იქნა აღმოჩენილი მტკიცებულება, რომელიც მიუთითებს იმაზე, რომ პირები, რომელთა მონაცემი ხელოვნური ინტელექტის მეშვეობით მუშავდება, განიცდიან რაიმე ზიანს ალგორითმების ან მსგავსი ტექნოლოგიების გამოყენების შედეგად. გამოკითხვის ფარგლებში სერვისის არაერთმა მიმწოდებელმა დაადასტურა, რომ ხელოვნური ინტელექტის ან მანქანური სწავლების გამოყენება ადმინისტრაციული დატვირთვის შემცირებას ემსახურება და არა შინაარსობრივი გადაწყვეტილების მიღებას.

"ICO"-ს ფუნქცია არ არის ტექნოლოგიის გამოყენების შესახებ ნებართვის გაცემა ან ტექნოლოგიის გამოყენების აკრძალვა. თუმცა ვინაიდან ხელოვნური ინტელექტის გამოყენების მასშტაბები ყოველდღიურად იზრდება, "ICO" უფლებამოსილია, ზედამხედველობა გაუწიოს პერსონალურ მონაცემთა დაცვის პრინციპების შესაბამისად ხელოვნური ინტელექტის გამოყენების პროცესს.

ფოტო: www.freepik.com

მიუხედავად იმისა, რომ "ICO"-მ არ გამოავლინა ხელოვნური ინტელექტის გამოყენებისას დისკრიმინაციის ან მისი უკანონო გამოყენების შემთხვევა, აშკარაა ხელოვნური ინტელექტის გამოყენებასთან დაკავშირებული რიგი საფრთხეების არსებობა. "ICO"-ს მოსაზრებით, რისკების შესამცირებლად, მონაცემთა დაცვის კანონმდებლობის შესაბამისად ტექნოლოგიების გამოყენების მიზნით, შესაძლოა ადგილობრივი და ცენტრალური ხელისუფლების მხრიდან რიგი პრაქტიკული ღონისძიებების განხორციელება:

1. **მონაცემთა დაცვის სტანდარტების გათვალისწინება ახალი პროდუქტის ან მომსახურების შექმნისას ("by design") და მონაცემთა დაცვა პირველად პარამეტრად ("by default")**

ადგილობრივი ხელისუფლების წარმომადგენლები, როგორც მონაცემთა დამმუშავებლები, ვალდებულები არიან, უზრუნველყონ მონაცემთა დამუშავების შესაბამისობა დიდი ბრიტანეთის მონაცემთა დაცვის ზოგად რეგულაციასთან ("UK GDPR"). ეს ნიშნავს, რომ საჭიროა, მკაფიოდ განისაზღვროს, თუ რა პერსონალური მონაცემები ინახება და რატომ არის მათი შენახვა საჭირო, რა ვადით ინახება და ასევე წაშლის ვალდებულება, როცა აღარ იქნება მათი შენახვის საჭიროება.

ალგორითმების მეშვეობით დამუშავებული მონაცემები, მონაცემთა ანალიტიკა და მსგავსი სისტემები რეაქტიულად და პროაქტიულად უნდა გადაიხედოს იმის შესამოწმებლად, რომ ისინი სწორია და იმ დროისთვის რელევანტურია. ეს წესი ასევე ვრცელდება ყველა კომპანიაზე ან ორგანიზაციაზე, რომელიც ადგილობრივი ხელისუფლების სახელით ამუშავებს მონაცემებს. თუკი ადგილობრივი ხელისუფლების წარმომადგენლები შეარჩევენ მესამე პირებს ინფორმაციის დასამუშავებლად ალგორითმების, მონაცემთა ანალიტიკის ან ხელოვნური ინტელექტის მეშვეობით, ისინი ვალდებული არიან, შეარჩიონ ისეთი კომპანია, რომელიც მონაცემებს გაერთიანებული სამეფოში მოქმედი მონაცემთა დაცვის ზოგადი რეგულაციის შესაბამისად ("UK GDPR") დაამუშავებს.

2. ინდივიდებისთვის გამჭვირვალე უნდა იყოს, თუ როგორ გამოიყენება მათი პერსონალური მონაცემები

ადგილობრივმა ხელისუფლებამ რეგულარულად უნდა გადახედოს კონფიდენციალურობის პოლიტიკას და განსაზღვროს გასაუმჯობესებელი სფეროები. გარკვეული ტიპის ინფორმაციის გაცემის ვალდებულება მუდმივად არსებობს, ხოლო ზოგიერთი ტიპის ინფორმაციის მიწოდება დამოკიდებულია ორგანიზაციაში არსებულ კონკრეტულ გარემოებებზე და იმაზე, თუ როგორ და რატომ გამოიყენება პერსონალური მონაცემები.

3. პირის კონფიდენციალურობისთვის პოტენციური რისკების დადგენა

ადგილობრივმა ხელისუფლებამ მიზანშეწონილია, ჩაატაროს მონაცემთა დაცვაზე ზეგავლენის შეფასება ("Data Protection Impact Assessments" ("DPIA")) ალგორითმის გამოყენებასთან, ხელოვნურ ინტელექტთან და მონაცემთა ანალიტიკასთან დაკავშირებულ მონაცემთა დაცვის რისკების იდენტიფიცირებისა და შემცირების მიზნით. "DPIA" უნდა შეაფასოს შესაბამისობის, ასევე, ადამიანის უფლებებისა და თავისუფლებათა დაცვასთან დაკავშირებული რისკი და სოციალური ან ეკონომიკური გავლენა.

აშკარაა ხელოვნური ინტელექტის პოტენციური სარგებელი. მას შეუძლია პროცესების გამარტივება, ხარჯების შემცირება, მომსახურებების გაუმჯობესება. თუმცა ამ ინოვაციების ეკონომიკური და სოციალური სარგებლის პარალელურად, მნიშვნელოვანია საზოგადოების ნდობის შენარჩუნება. აუცილებელია ადგილობრივი ხელისუფლების მიერ ხელოვნური

ინტელექტის სამართლიანად, კანონის შესაბამისად გამოყენება.

საფრანგეთის მონაცემთა დაცვის საზედამხედველო ორგანომ (“CNIL”) ხელოვნური ინტელექტის დეპარტამენტი შექმნა

26.01.2023

საფრანგეთის საზედამხედველო ორგანოში (“CNIL”) ხელოვნური ინტელექტის დეპარტამენტის შეიქმნა.

ფოტო: www.cnil.fr

დეპარტამენტში სამართლებრივი ექსპერტები და სპეციალიზებული ინჟინრები იმუშავებენ. ეს დეპარტამენტი “CNIL”-ის ტექნოლოგიისა და ინოვაციების დირექტორატის ნაწილია. ხელოვნური ინტელექტის დეპარტამენტის ფუნქციებია:

- ხელოვნური ინტელექტის სისტემების გაგების გაუმჯობესება;
- “CNIL”-ის შესაძლებლობების გაძლიერება პირადი ცხოვრების დაცულობასთან დაკავშირებული რისკების იდენტიფიცირებისა და პრევენციის მიმართულებით;
- ევროპის ხელოვნური ინტელექტის რეგულაციის (რომელიც ამჟამად შემუშავების პროცესშია ევროპის დონეზე) იმპლემენტაციისთვის მზადება;
- საუნივერსიტეტო სივრცის წარმომადგენლებთან, კომპანიებთან, ე. წ. “start-up”-ებთან კოორდინაციის გაუმჯობესება.

ხელოვნური ინტელექტის დეპარტამენტი, “CNIL”-ის სხვა დეპარტამენტებთან კოორდინაციით, ხელოვნური ინტელექტის გამოყენებასთან დაკავშირებულ საკითხებზე იმუშავებს. იგი ევროპის მონაცემთა დაცვის საბჭოს (“EDPB”) ექსპერიმენტული პროექტების განხორციელებაში დაეხმარება. ეს ცვლილება ეხმიანება საფრანგეთის სახელმწიფო საბჭოს 2022 წლის 30 აგვისტოს კვლევას მმართველობით ორგანოებში ხელოვნური ინტელექტის გამოყენების თაობაზე. საბჭო მხარს უჭერს “CNIL”-ის ხელოვნური ინტელექტის სისტემების საზედამხედველო ორგანოდ განსაზღვრას და ასევე მის როლს ხელოვნური ინტელექტის რეგულაციის კოორდინაციის თვალსაზრისით.

ფოტო: www.freepik.com

მეორე მხრივ, ხელოვნური ინტელექტის დეპარტამენტის შექმნა სოციალურ მოთხოვნას შეესაბამება. ხელოვნური ინტელექტის შესწავლა მნიშვნელოვანია მონაცემთა სუბიექტების უფლებების

დასაცავად, რომელთა მონაცემები ტექნოლოგიების გამოყენებით მუშავდება. აგრეთვე მისი შესწავლა აუცილებელია როგორც მონაცემთა დამმუშავებლისთვის, ასევე ამ დარგის მარეგულირებლებისთვის, რათა სწორად განისაზღვროს ხელოვნური ინტელექტის მიერ მონაცემთა დამუშავებაზე კონტროლის და ინსპექტირების მექანიზმები.

“CNIL”-ი ხელოვნური ინტელექტის საკითხებზე 2017 წლიდან მუშაობს და ამ დრომდე მის მიერ აქტივობები შემდეგი სამი მიმართულებით განხორციელდა:

- ხელოვნურ ინტელექტთან დაკავშირებული ეთიკური და სამართლებრივი საკითხების იდენტიფიცირება;
- ხელოვნურ ინტელექტთან დაკავშირებული რისკების მართვა;
- ხელოვნური ინტელექტის გამოყენებასთან დაკავშირებით რეკომენდაციების გაცემა აღნიშნული ტექნოლოგიის გამოყენების გაუმჯობესების მიზნით.

საფრანგეთის მონაცემთა დაცვის საზედამხედველო ორგანომ (“CNIL”) “TIKTOK”-ი ხუთი მილიონი ევროს ოდენობით დააჯარიმა

12.01.2023

2022 წლის 29 დეკემბერს, საფრანგეთის მონაცემთა დაცვის საზედამხედველო ორგანომ (“CNIL”) სოციალურ ქსელ “TIKTOK”-ს ხუთი მილიონი ევროს ოდენობის ჯარიმა დაუწესა ორი მიზეზის გამო:

1. “tiktok.com”-ის მომხმარებლებს „მზა-ჩანაწერებზე“ (ე. წ. “cookies”) უარის თქმა ისევე მარტივად არ შეეძლოთ, როგორც მათზე დათანხმება;
2. მომხმარებლები სხვადასხვა „მზა-ჩანაწერის“ მიზნების შესახებ საკმარისად არ იყვნენ ინფორმირებულნი.

ინფორმაცია საქმის შესწავლის შესახებ

2020 წლის მაისიდან ივნისამდე პერიოდში, “CNIL”-მა ონლაინკვლევები ჩაატარა “tiktok.com” ვებგვერდისა და კომპანიისგან გამოთხოვილი დოკუმენტების საფუძველზე. კვლევა მხოლოდ “TIKTOK”-ის ვებგვერდზე ჩატარდა, თუმცა არა მობილურ აპლიკაციაში.

შემოწმების შედეგად მიღებული დასკვნების საფუძველზე, საზედამხედველო ორგანომ მიიჩნია, რომ “TIKTOK Information Technologies UK Limited”-მა (“TIKTOK UK”) და “TIKTOK Technology Limited”-მა (“TIKTOK Ireland”) საფრანგეთის „მონაცემთა დაცვის შესახებ“ აქტის 82-ე მუხლის მოთხოვნები დაარღვიეს.

ფოტო: freepik.com

დაკისრებული ჯარიმის ოდენობა გამოვლენილი დარღვევების, დაინტერესებულ პირთა რაოდენობის (მათ

შორის, არასრულწლოვნების) მიხედვით განისაზღვრა. აგრეთვე, აღნიშნულის საფუძველს “CNIL”-ის არაერთი წინმსწრები კომუნიკაცია წარმოადგენდა იმის შესახებ, რომ „მზა-ჩანაწერების“ უარყოფა ისეთივე მარტივი უნდა იყოს, როგორც მათზე დათანხმება.

ფოტო: freepik.com

საფრანგეთის მონაცემთა დაცვის შესახებ აქტის დარღვევა

კომპანიები “TIKTOK UK” და “TIKTOK IRELAND” მომხმარებლებს „მზა-ჩანაწერების“ დაუყოვნებლივ მიღების ღილაკს სთავაზობდნენ, თუმცა მსგავსი სახის გადაწყვეტა (ღილაკი ან სხვა მექანიზმი) შემოთავაზებაზე მარტივად უარყოფისთვის, გათვალისწინებული არ იყო. კერძოდ, ყველა „მზა-ჩანაწერის“ უარყოფას რამდენიმე მონიშვნა სჭირდებოდა მაშინ, როდესაც მათი მიღება ერთი დადასტურებით იყო შესაძლებელი.

“CNIL”-მა მიიჩნია, რომ უარის თქმის მექანიზმის კომპლექსურობა, „მზა-ჩანაწერებზე“ უარის თქმას ართულებდა და მომხმარებელს „ყველაფრის მიღების“ ღილაკისკენ უბიძგებდა. 2022 წლის თებერვალში უარყოფის ღილაკის ამოქმედებამდე, 2021 წლის ივნისში ონლაინ კვლევის ჩატარების პროცესში “CNIL”-მა დაასკვნა, რომ აღნიშნული ინტერნეტ მომხმარებელთა ნების თავისუფლებას არღვევდა და საფრანგეთის მონაცემთა დაცვის შესახებ აქტის 82-ე მუხლის დარღვევას წარმოადგენდა. გარდა ამისა, მომხმარებლები არ იყვნენ საკმარისად ინფორმირებულნი „მზა-ჩანაწერების“ მიზნების შესახებ.

“CNIL”-ის უფლებამოსილების ფარგლები

“CNIL”-ი უფლებამოსილია, გადაამოწმოს „მზა-ჩანაწერებთან“ დაკავშირებული ოპერაციები, ასევე, დააწესოს სანქციები, თუკი „მზა-ჩანაწერები“ კომპანიების მიერ საფრანგეთში მყოფ ინტერნეტ მომხმარებელთა მოწყობილობებზეა განთავსებული. ამ შემთხვევაში “GDPR”-ით გათვალისწინებული თანამშრომლობის მექანიზმი არ გამოიყენება, რადგან იდენტიფიკატორების გამოყენებასთან დაკავშირებული ოპერაციები „ePrivacy“ დირექტივის რეგულირების ფარგლებში ექცევა, რაც ასევე ასახულია საფრანგეთის მონაცემთა დაცვის შესახებ აქტის 82-ე მუხლში.

“EDPB”-მ საჯარო სექტორის მიერ „ღრუბლოვანი სერვისების“ * გამოყენებისთვის რეკომენდაციები და “მზა-ჩანაწერების“ ბანერის სამუშაო ჯგუფის საქმიანობის შესახებ ანგარიში გამოაქვეყნა

18.01.2023

ფოტო: edpb.europa.eu

მონაცემთა დაცვის ევროპულმა საბჭომ (“EDPB”) კოორდინირებული სააღსრულებო მოქმედების შესახებ 2022 წლის ანგარიში გამოაქვეყნა, რომელიც საჯარო სექტორის მიერ ე. წ. „ღრუბელზე დაფუძნებული“ (“cloud-based”) სერვისების გამოყენებაზეა ფოკუსირებული. “EDPB”-მ აღნიშნა საჯარო ორგანოების მიერ “GDPR”-ის სრული დაცვით მოქმედების აუცილებლობა. მან საჯარო სექტორის ორგანიზაციებისთვის ღრუბელზე დაფუძნებული პროდუქტების, ასევე, სერვისების გამოყენებასთან დაკავშირებით რეკომენდაციები გასცა. მონაცემთა დაცვის საზედამხედველო ორგანოების მიერ „ღრუბლოვანი გამოთვლების“ (“cloud computing”) სფეროში უკვე განხორციელებული ღონისძიებების შესახებ ინფორმაცია უკვე ხელმისაწვდომია.

“EDPB”-ის თავმჯდომარემ განაცხადა: „კოორდინირებული აღსრულების ჩარჩო (“CEF”) აწესებს მონაცემთა დაცვის საზედამხედველო ორგანოებს შორის უფრო ღრმა თანამშრომლობის მეთოდებს მეტი ეფექტიანობისა და თანმიმდევრულობის მიზნით. ევროპის მასშტაბით, საჯარო სექტორის ორგანიზაციები მიმართავენ „ღრუბლოვან სერვისებს“ და მათ უჭირთ “GDPR”-ის შესაბამისი სერვისებისა თუ პროდუქტების უზრუნველყოფა. საჯარო სამსახურების მიერ დამუშავებული პერსონალური მონაცემების მიმართ საჭიროა განსაკუთრებული სიფრთხილის გამოჩენა, განსაკუთრებით კი მაშინ, როდესაც დამუშავება მესამე მხარის მიერ ხორციელდება. ამისთვის “EDPB”-ის 2022 წლის “CEF”-ის ანგარიში იძლევა გამოსადეგ საზომს და მჯერა, რომ იგი გახდება მნიშვნელოვანი სტანდარტი საჯარო ორგანოებისთვის, რომელთაც “GDPR”-თან შესაბამისი ღრუბლოვანი სერვისების უზრუნველყოფა სურთ.“

ფოტო: freepik.com

* ტერმინი „ღრუბლოვანი სერვისები“ მოიაზრებს სერვისების ფართო სპექტრს, რომლებიც კომპანიებსა და მომხმარებლებს ინტერნეტის საშუალებით მიეწოდება. აღნიშნული სერვისები შექმნილია, შესაბამისი ინფრასტრუქტურის ან მოწყობილობების საჭიროების გარეშე, აპლიკაციებსა და რესურსებზე მარტივი წვდომის უზრუნველსაყოფად. დამატებით იხ., <www.citrix.com/solutions/digital-workspace/what-is-a-cloud-service.html>, <www.redhat.com/en/topics/cloud-computing/what-are-cloud-services>.

2022 წელს მონაცემთა დაცვის ოცდაორმა საზედამხედველო ორგანომ (მათ შორის, “EDPS”) ევროპის ეკონომიკური ზონის მასშტაბით საჯარო სექტორის მიერ ღრუბელზე დაფუძნებული სერვისების გამოყენების შესახებ კოორდინირებული კვლევა დაიწყო. ამ პროცესში ასამდე საჯარო ორგანო მონაწილეობდა, მათ შორის, ევროპული ინსტიტუტები, რომლებიც სექტორების ფართო სპექტრს ფარავს (მაგალითად, როგორიცაა: ჯანდაცვა, ფინანსები, გადასახადები, განათლება, IT სერვისების მომწოდებლები და სხვა).

2021-2023 წლების სტრატეგიის მიხედვით „კოორდინირებული აღსრულების ჩარჩო“ (“CEF”) არის “EDPB”-ის ძირითადი აქტივობა. მისი მიზანი მონაცემთა დაცვის საზედამხედველო ორგანოებს შორის თანამშრომლობისა და აღსრულების გამარტივებაა. 2023 წლის ძირითადი აქტივობა მონაცემთა დაცვის ოფიცრის (“DPO”) დანიშვნასა და როლს შეეხება.

გარდა ამისა, “EDPB”-მ „მზა-ჩანაწერების ბანერის სამუშაო ჯგუფის“ (“Cookie Banner Task Force”) საქმიანობის შესახებ ანგარიში გამოაქვეყნა. სამუშაო ჯგუფი 2021 წლის სექტემბერში შეიქმნა. მისი მიზანია ევროპის ეკონომიკური ზონის მასშტაბით „მზა-ჩანაწერების“ ბანერებთან დაკავშირებით თანმიმდევრული მიდგომის უზრუნველსაყოფად მონაცემთა დაცვის საზედამხედველო ორგანოებს შორის თანამშრომლობის, ინფორმაციის და საუკეთესო პრაქტიკის გაზიარების ხელშეწყობა. ანგარიშის მიხედვით, მონაცემთა დაცვის საზედამხედველო ორგანოები შეთანხმდნენ “ePrivacy” დირექტივისა და “GDPR”-ის დებულებების განმარტებათა საერთო აღნიშვნაზე: „უარყოფის ღილაკები“, „წინასწარ მონიშნული ველები“, „ბანერის დიზაინი“ და სხვა.

ირლანდიის მონაცემთა დაცვის საზედამხედველო ორგანომ (“DPC”) “WhatsApp”-ის აპლიკაცია “GDPR”-ის მოთხოვნათა დარღვევის გამო დააჯარიმა

19.01.2023

ფოტო: www.dataprotection.ie

2023 წლის 19 იანვარს, ირლანდიის მონაცემთა დაცვის საზედამხედველო ორგანომ (“DPC”) პლატფორმა “WhatsApp”-ი “GDPR”-ის მოთხოვნების დარღვევის გამო 5.5 მილიონი ევროს ოდენობით დააჯარიმა.

ფაქტობრივი გარემოებათა თანახმად, მომჩივანი აცხადებდა, რომ მომსახურების გაუმჯობესებისა და უსაფრთხოების უზრუნველყოფის მიზნით, აპლიკაცია მომხმარებლებს მათი პერსონალური მონაცემების დამუშავებაზე დათანხმებას ავალდებულებდა. კერძოდ, “WhatsApp”-მა მომხმარებლებს აცნობა, რომ თუკი სურდათ აპლიკაციის გამოყენება, შესაბამის ღილაკზე დაჭერით, მათ უნდა დაედასტურებინათ მომსახურების პირობებზე თანხმობა. წინააღმდეგ შემთხვევაში ისინი პლატფორმით ვერ

ისარგებლებდნენ. მომჩივანი ამტკიცებდა, რომ აღნიშნული “GDPR”-ის დებულებებს ეწინააღმდეგებოდა.

საზედამხედველო ორგანომ “GDPR“-ის სავარაუდო დარღვევასთან დაკავშირებული საკითხი შეისწავლა, რის შედეგად გამჭვირვალობის უზრუნველყოფის ვალდებულების დარღვევა გამოავლინა. ხაზგასასმელია, რომ საზედამხედველო ორგანომ წინა შემთხვევაშიც “WhatsApp”-ი გამჭვირვალობის ვალდებულებების დარღვევისთვის დააჯარიმა 225 მილიონი ევროს ოდენობით. სწორედ ამიტომ, საწყის ეტაპზე საზედამხედველო ორგანომ საჭიროდ აღარ მიიჩნია ჯარიმის ხელმეორედ დაწესება, თუმცა “EDPB”-ის მითითების შედეგად, მან კვლავ დაუწესა აპლიკაციას ჯარიმა 5.5 მილიონის ევროს ოდენობით. ასევე, “WhatsApp”-ს “GDPR -თან შესაბამისობის უზრუნველსაყოფად ექვსი თვე განესაზღვრა.

ფოტო: freepik.com

“EDPB”-მ საზედამხედველო ორგანოს დაავალა, რომ “WhatsApp”-ის მიერ მონაცემთა დამუშავების ოპერაციებთან დაკავშირებით დამატებითი შესწავლა ჩაეტარებინა “GDPR”-თან შესაბამისობის ხარისხი დადგენის მიზნით. საზედამხედველო ორგანო მიიჩნია, რომ “EDPB”-ს არ ჰქონდა მსგავსი დავალების გაცემის უფლებამოსილება. შესაბამისად, იგი გეგმავს დავალების ევროკავშირის მართლმსაჯულების სასამართლოში გასაჩივრებას.

თავის მხრივ “WhatsApp”-ის წარმომადგენელმა აღნიშნა, რომ პლატფორმის მომსახურების პირობები სრულად შეესაბამება “GDPR”-ით დადგენილ სტანდარტებს და ამიტომაც აპირებენ საზედამხედველო ორგანოს გადაწყვეტილების გასაჩივრებას.

გაერთიანებული სამეფოს მონაცემთა დაცვის საზედამხედველო ორგანომ (“ICO”) სკოლებში სახის ამომცნობი ტექნოლოგიების გამოყენებაზე იმსჯელა

31.01.2023

ფოტო: ico.org.uk

2023 წლის 31 იანვარს, გაერთიანებული სამეფოს მონაცემთა დაცვის საზედამხედველო ორგანომ ჩრდილოეთ აირშირის საბჭოს (“North Ayrshire Council”) წარუდგინა წერილი, რომელიც სკოლებში სახის ამომცნობი ტექნოლოგიის გამოყენებას შეეხებოდა. აღნიშნული ტექნოლოგიის გამოყენების მიზანს სკოლის სასადილოებში „უნაღდო კვების“ (“cashless catering”) მართვა წარმოადგენდა.

ფოტო: freepik.com

“ICO”-მ განაცხადა, რომ საგანმანათლებლო დაწესებულებებში სახის ამომცნობი და სხვა ახალი ტექნოლოგიები, მართალია, უზრუნველყოფს სარგებელს, თუმცა მისი მეშვეობით განსაკუთრებული კატეგორიის პერსონალური მონაცემები მუშავდება. აღნიშნული კი წარმოშობს გარკვეულ რისკებს. შესაბამისად, ამ პროცესში მეტად მნიშვნელოვანია ბავშვების მონაცემებისა და მათი უფლებების დაცვა.

წერილზე დაყრდნობით, “ICO”-მ ჩრდილოეთ აირშირის საბჭოსთან თანამშრომლობით მონაცემთა დამუშავების კანონმდებლობასთან შესაბამისობა შეაფასა და დაადგინა, რომ “GDPR”-ის შესაბამისი დებულებების გათვალისწინებით, სახის ამომცნობი ტექნოლოგიების განლაგება მონაცემთა დაცვის სტანდარტებს არღვევდა:

- კანონიერება, სამართლიანობა და გამჭვირვალობა (“GDPR”-ის მე-5 მუხლის პირველი პუნქტის “a” ქვეპუნქტი, მე-6, მე-9 და მე-12 მუხლები);
- ინფორმირების უფლება (“GDPR”-ის მე-13 მუხლი);
- შენახვა (“GDPR”-ის მე-5 მუხლის პირველი პუნქტის „e” ქვეპუნქტი);
- მონაცემთა დაცვის რისკების შეფასება (“GDPR”-ის 35-ე მუხლი).

“ICO”-მ ჩრდილოეთ აირშირის საბჭოს რეკომენდაციები წარუდგინა, რომელთა მიხედვით:

- უნდა არსებობდეს მონაცემთა დამუშავების კანონიერი საფუძველი – “ICO”-მ აღნიშნა, რომ თანხმობა წარმოადგენს ბავშვების განსაკუთრებული კატეგორიის ბიომეტრიული მონაცემების დამუშავების კანონიერ საფუძველს;
- დამუშავება უნდა იყოს გამჭვირვალე – “ICO”-მ განაცხადა, რომ ჩრდილოეთ აირშირის საბჭომ გასაგები ენით უნდა განმარტოს, თუ როგორ გროვდება, გამოიყენება და ინახება ბავშვების პერსონალური მონაცემები, ასევე, თუ რა რისკები ახლავს მათი მონაცემების დამუშავებას;
- მონაცემთა დამუშავების დაწყებამდე წინასწარ უნდა შეფასდეს მონაცემთა დაცვის რისკები, რომლებიც ითვალისწინებს დამუშავების აუცილებლობას და პროპორციულობას.

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