პერსონალურ მონაცემთა
დაცვის სამსახური

მსოფლიო პრაქტიკა

ივნისი / 2022

მთავარი სიახლეები

დიდი ბრიტანეთის საზედამხედველო ორგანო პოლიციას მოუწოდებს, შეწყვიტოს გაუპატიურებისა და მძიმე სექსუალური ძალადობის მსხვერპლთაგან პერსონალური მონაცემების „გადაჭარბებული შეგროვება“

იტალიის მონაცემთა დაცვის საზედამხედველო ორგანო აშშ-ში მონაცემთა გადაცემის სათანადო გარანტიების არარსებობის გამო “Google”- ის ანალიტიკის (“Google Analytics”) გამოყენებას კრძალავს

ევროპული საპარლამენტო კვლევითი სამსახური (EPRS) განცხადებას აკეთებს „მეტავერსის“ შესაძლებლობების, რისკებისა და პოლიტიკის შედეგების შესახებ

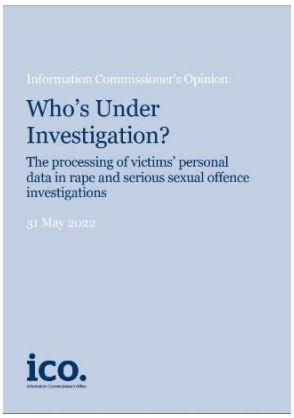
ირლანდიის საზედამხედველო ორგანომ დრონების გამოყენებით მონაცემთა დამუშავების შესახებ სახელმძღვანელო გამოაქვეყნა

დიდი ბრიტანეთის საზედამხედველო ორგანო პოლიციას მოუწოდებს, შეწყვიტოს გაუპატიურებისა და მძიმე სექსუალური ძალადობის მსხვერპლთაგან პერსონალური მონაცემების „გადაჭარბებული შეგროვება“

31.05.2022

დიდი ბრიტანეთის საზედამხედველო ორგანოს ხელმძღვანელმა, ინფორმაციის კომისარმა, სისხლის სამართლის მართლმსაჯულების სექტორს მოუწოდა დაუყოვნებლივ შეწყვიტოს გაუპატიურებისა და მძიმე სექსუალური ძალადობის მსხვერპლი პირებისაგან გადაჭარბებული ოდენობით პირადი ინფორმაციის შეგროვება.

მოწოდება გამოქვეყნებულია ინფორმაციის კომისრის დასკვნაში, რომელიც სისხლის სამართლის მართლმსაჯულების სექტორს აცნობებს, თუ როგორ გამოიყენოს მსხვერპლთა პერსონალური მონაცემები მონაცემთა დაცვის კანონმდებლობის შესაბამისად.



ფოტო: ico.org.uk

ამჟამად, დანაშაულის მსხვერპლისგან მოითხოვება, რომ დაუყოვნებლივ, თავდასხმის შემდეგ, განაცხადოს თანხმობა საკუთარი ცხოვრების შესახებ განსაკუთრებული ოდენობის ინფორმაციის გაცემის თაობაზე. მართლმსაჯულებაზე წვდომის წინაპირობად მსხვერპლისგან მოითხოვება წვდომის უზრუნველყოფა მათ სამედიცინო ისტორიაზე, სოციალური სამსახურისა და სასწავლებელში არსებულ ჩანაწერებზე, ასევე მათი მობილური ტელეფონის შინაარსზე. მსხვერპლებს ექცევიან ისე, როგორც ეჭვმიტანილებს.

ინფორმაციის კომისარს აქვს მოლოდინი, რომ აღნიშნული პრაქტიკა დაუყოვნებლივ შეწყდება და იძლევა დამატებით რეკომენდაციებს ინფორმაციის დამუშავების შესახებ:

1-ლი რეკომენდაცია

დიდი ბრიტანეთის მასშტაბით პოლიციის ყველა სამსახურს უნდა დაევალოს, რომ შეწყვიტონ იმგვარი განცხადებების ან ფორმების გამოყენება, რომლებიც მესამე პირის მასალების მოპოვებაზე საერთო თანხმობას ითვალისწინებს. მონაცემთა დაცვა არ წარმოადგენს მონაცემთა სამართლიანი და კანონიერი გაზიარებისა და მოპოვებისთვის ბარიერს, გასათვალისწინებელია მონაცემთა მინიმიზაცია. მსხვერპლთან დაკავშირებით მოპოვებული პერსონალური მონაცემი უნდა იყოს გამოძიების მიზნებისთვის ადეკვატური, რელევანტური, შესაბამისი და არ უნდა იყოს გადაჭარბებული.

მე-2 რეკომენდაცია

პროკურატურის ორგანოებმა უნდა უზრუნველყონ, რომ პროკურორები ინფორმირებულნი იყვნენ კომისრის აღნიშნული მოსაზრების თაობაზე. მათ

ინფორმაციის კომისრის მიერ მსხვერპლთა უფლებების დაცვის მიზნით განსაზღვრული პრინციპების შესაბამისად უნდა იმოქმედონ.

მე-3 რეკომენდაცია

მესამე მხარე ორგანიზაციებიდან პერსონალური ინფორმაციის გამოთხოვისას, შესაბამისმა ორგანოებმა პოლიციისთვის სათანადო რჩევები და დამხმარე ფორმები უნდა შეიმუშაონ. ფორმები უნდა შეესაბამებოდეს ინფორმაციის კომისრის მოსაზრებაში დადგენილ პრინციპებს. კერძოდ, ისინი უნდა:

- აძლევდეს მკაფიო რჩევებს პოლიციის მოთხოვნათა მიმღებ მესამე მხარეებს;
- განმარტავდეს, პოლიციის მოთხოვნები ნებაყოფლობითია თუ სავალდებულო;
- განმარტავდეს ინფორმაციის მოძიების მიზეზებს;
- განმარტავდეს, რომ მოძიებული ინფორმაცია შეიძლება, საბოლოოდ გაუმჟღავნდეს ბრალდებულს.

მე-4 რეკომენდაცია

ინფორმაციის კომისარმა რეკომენდაცია მისცა უშუალოდ დიდი ბრიტანეთის პოლიციის უფროსებს გაუპატიურებისა და მძიმე სექსუალური დანაშაულების მსხვერპლებთან დაკავშირებული ინფორმაციის დამუშავებისას მონაცემთა დაცვის კანონმდებლობასთან შესაბამისობის დემონსტრირების თაობაზე. საამისოდ უნდა განახლდეს სათანადო პოლიტიკის დოკუმენტები, სახელმძღვანელო მითითებები, სხვა სახის დოკუმენტაცია და შესაბამისი ტრენინგები. აღნიშნული უნდა ფარავდეს სულ მცირე შემდეგ საკითხებს:

- გარემოებები, როდესაც შესაძლებელია მიზანშეწონილი იყოს შესაბამის მასალებზე ხელმისაწვდომობა (i) მსხვერპლის ელექტრონული მოწყობილობებიდან, ან (ii) სხვა ორგანიზაციებიდან. როგორ შეუძლიათ გამოიყენონ მოპოვებული ინფორმაცია, ვის შეუძლიათ გაუმჟღავნონ იგი და როგორ უნდა უზრუნველყონ მონაცემთა დაცვა;
- იმ მასალების პარამეტრების ფორმულირება და აღრიცხვა, რომელთა მოპოვებაც პოლიციის თანამშრომლებს სურთ;
- მსხვერპლთან კონტაქტის მახასიათებლები და ასევე, ინფორმაცია, რომელიც მსხვერპლმა უნდა მიაწოდოს პოლიციის თანამშრომელს;
- ინფორმაცია, რომელიც უნდა მიეწოდოს მესამე პირს, რომლისგან პოლიციის თანამშრომლები ითხოვენ მასალას;
- როგორ უნდა მოიქცნენ იმ შემთხვევაში, როდესაც მესამე მხარე ინფორმაციის მიწოდებაზე უარს აცხადებს.

მე-5 რეკომენდაცია

დიდი ბრიტანეთის პოლიციის უფროსები უნდა გადამზადდნენ და ჰქონდეთ სათანადო პოლიტიკა, სახელმძღვანელო დოკუმენტები მსხვერპლთა პერსონალური მონაცემების მართვისა და შენახვის საკითხებზე. აღნიშნული ღონისძიებები უზრუნველყოფს უშუალოდ მსხვერპლისგან მოპოვებული ან მისი მოწყობილობებიდან ამოღებული, ან მესამე

პირებისგან მიღებული ინფორმაციის სათანადო მართვასა და დაცვას.

ირლანდიის საზედამხედველო ორგანომ ბავშვებისთვის პერსონალურ მონაცემთა დაცვის უფლებების შესახებ გზამკვლევები გამოაქვეყნა

25.05.2022

ირლანდიის საზედამხედველო ორგანომ ბავშვებისთვის GDPR-ის მიხედვით მონაცემთა დაცვისა და მათი უფლებების შესახებ სამი მოკლე გზამკვლევი მოამზადა. ეს დოკუმენტები, ძირითადად, გამიზნულია 13 წლისა და შედარებით უფროსი ბავშვებისთვის, რადგან ამ ასაკში მათ შეუძლიათ დამოუკიდებლად დაიწყონ სოციალური მედიის მრავალ პლატფორმაზე რეგისტრაცია.

ბავშვთა პერსონალური მონაცემების დაცვა ირლანდიის საზედამხედველო ორგანოსთვის მნიშვნელოვანი პრიორიტეტია და წარმოადგენს 2022-2027 წლების მარეგულირებელი სტრატეგიის ხუთი სტრატეგიული მიზნიდან ერთ-ერთს. ბოლო პერიოდში მათ, ასევე, გამოაქვეყნეს „საფუძვლები“ – სახელმძღვანელო ბავშვთა მონაცემთა დაცვის უფლებებთან დაკავშირებით, რათა დახმარებოდნენ ორგანიზაციებს მონაცემების დამუშავებისას ბავშვებთა უფლებების განსაკუთრებულ დაცვაში. თუმცა აღნიშნული ასევე გულისხმობს მათთვის იმგვარი ცოდნითა და ინსტრუმენტებით აღჭურვას, რომლებიც დაეხმარება მათ საკუთარი მონაცემების დაცვაში.

ირლანდიის საზედამხედველო ორგანოს მიერ გამოქვეყნებული გზამკვლევები შემდეგ საკითხებს შეეხება:

მონაცემთა დაცვა - რა საკითხებს ეხება?

ეს გზამკვლევი ბავშვებსა და ახალგაზრდებს აცნობს პერსონალური მონაცემებისა და მონაცემთა დაცვის იდეას და რატომ არის მათთვის მნიშვნელოვანი ამის ცოდნა.

ფოტო: dataprotection.ie

ჩემი მონაცემების დაცვის უფლებები

დოკუმენტში მოცემულია გზამკვლევები მონაცემთა დაცვის სხვადასხვა უფლების შესახებ, ასევე, ინფორმაცია მათი გამოყენების თაობაზე. დოკუმენტი პასუხობს იმგვარ საკითხებს, როგორიცაა:

- რატომ არის მონაცემთა დაცვის უფლებები მნიშვნელოვანი?
- იცოდე, რა ემართება შენს მონაცემებს;
- შენი მონაცემების ასლების მიღება;
- შენი მონაცემების წაშლა;
- უთხარით „არა“ მესამე პირებს, რომლებიც იყენებენ თქვენს მონაცემებს.

ფოტო: dataprotection.ie

ძირითადი რჩევები თქვენი მონაცემების ონლაინ უსაფრთხოების შესანარჩუნებლად

სახელმძღვანელო შეიცავს 15 რჩევას, რომელიც დაეხმარება ბავშვებს და არა მხოლოდ მათ, დაიცვან საკუთარი პერსონალური მონაცემები ინტერნეტ სივრცეში.

ფოტო: dataprotection.ie

ევროპული საპარლამენტო კვლევითი სამსახური (EPRS) განცხადებას აკეთებს „მეტავერსის“ შესაძლებლობების, რისკებისა და პოლიტიკის შედეგების შესახებ

24.07.2022

“EPRS”-მა გამოაქვეყნა ინსტრუქცია, სახელწოდებით – „მეტავერსი: შესაძლებლობები, რისკები და პოლიტიკის შედეგები“. ინსტრუქციაში შეჯამებულია კვლევა „მეტავერსის“ პოტენციური ზემოქმედების შესახებ სხვადასხვა საკითხებზე, კერძოდ: კონკურენციის, მონაცემთა დაცვის, ვალდებულებების, ფინანსური ტრანზაქციების, კიბერუსაფრთხოების, ჯანმრთელობის, ხელმისაწვდომობისა და ინკლუზიურობის შესახებ.

მონაცემთა დაცვასთან დაკავშირებით ინსტრუქციაში ხაზგასმულია, რომ „მეტავერსში“ გამოყენებულ მონაცემთა დიდი მოცულობა, აჩენს მონაცემთა დაცვისა და კიბერუსაფრთხოების რიგ რისკებს.

ინსტრუქციაში ასევე ნახსენებია, რომ „მეტავერსზე“ კონფიდენციალურობისა და მონაცემთა დაცვის ჩარჩო ვრცელდება და ევროპის პარლამენტმა მოუწოდა ევროპის კომისიას, უზრუნველყოს „მეტავერსში“ ოპერირებადი კომპანიების ზემოაღნიშნულთან შესაბამისობა.

ამასთანავე, ინსტრუქცია შეიცავს მოწოდებას მონაცემთა დაცვის ზოგადი რეგულაციის (GDPR) გადახედვისა და განახლების თაობაზე, რათა გადაიჭრას „მეტავერსით“ წამოჭრილი იმგვარი გამოწვევა, როგორიცაა არაცნობიერი ქცევის ან ხელოვნურ ინტელექტთან (“AI”) ინტერაქციის დროს შეგროვებული მონაცემების რეგულირების საჭიროება.

ფოტო: freepik.com

„მეტავერსი“ შეიძლება შეფასდეს, როგორც რეალობასთან მიმსგავსებული და უწყვეტი ვირტუალური 3D სამყარო, სადაც ადამიანები ურთიერთობენ „ავატარის“ საშუალებით აქტივობების ფართო სპექტრის განსახორციელებლად.

იტალიის მონაცემთა დაცვის საზედამხედველო ორგანო აშშ-ში მონაცემთა გადაცემის სათანადო გარანტიების არარსებობის გამო “Google”-ის ანალიტიკის (“Google Analytics”) გამოყენებას კრძალავს

23.06.2022

ფოტო: garanteprivacy.it

იტალიის მონაცემთა დაცვის საზედამხედველო ორგანომ, ევროპის მონაცემთა დაცვის საზედამხედველო ორგანოებთან ერთად, შეისწავლა უწყებაში წარმოდგენილი საჩივართა გარემოებები, რის შედეგად გამოიკვეთა, რომ ვებგვერდის ოპერატორები იყენებდნენ “Google”-ის ანალიტიკას, მზა ჩანაწერებს, დათვალიერებულ გვერდებსა და შეთავაზებულ სერვისებს.

ზემოაღნიშნულ პროცესში, გროვდებოდა არაერთი მონაცემი, მათ შორის, მომხმარებლის IP მისამართი და ინფორმაცია ბრაუზერის, მომუშავე სისტემის, არჩეული ენის, გვერდის დათვალიერების თარიღისა და დროის შესახებ, რომელიც გადაეცემოდა აშშ-ს. იტალიის მონაცემთა დაცვის საზედამხედველო ორგანომ აღნიშნა, რომ IP მისამართი წარმოადგენს პერსონალურ მონაცემებს. საზედამხედველო ორგანომ განაცხადა, რომ ვებგვერდი, რომელიც იყენებს “Google”-ის ანალიტიკას GDPR-ში წარმოდგენილი გარანტიების არარსებობის გარეშე, არღვევს მონაცემთა დაცვის კანონმდებლობას. აღნიშნულის მიზეზს წარმოადგენს ის გარემოება, რომ მომხმარებლის მონაცემები გადაიცემა აშშ-ში, სადაც პერსონალური მონაცემები შესაბამისად არ არის დაცული.

ფოტო: freepik.com

საზედამხედველო ორგანოს მიერ, ასევე, ხაზი გაესვა, რომ აშშ-ში არსებულ სამთავრობო და სადაზვერვო უწყებებისთვის ხელმისაწვდომია იმგვარი პერსონალური მონაცემები, რომლებიც გადაცემულია სათანადო გარანტიების არარსებობით.

მონაცემთა გადაცემის თვალსაზრისით, “Google”-ის მიერ მიღებული ზომები არ უზრუნველყოფდა მომხმარებლის პერსონალური მონაცემების ადეკვატურ დაცვას.

- იტალიის მონაცემთა დაცვის საზედამხედველო ორგანოს სურს, რომ მიიპყროს როგორც საჯარო, ისე კერძო ვებგვერდების ოპერატორთა ყურადღება, “Google”-ის ანალიტიკის მეშვეობით აშშ-ში მონაცემების გადაცემის თაობაზე. საზედამხედველო ორგანო მოუწოდებს ყველა დამმუშავებელს, რომ მათ ვებგვერდებზე მზა ჩანაწერებისა და მონიტორინგის ინსტრუმენტები შესაბამისობაში მოიყვანოს მონაცემთა დაცვის კანონმდებლობასთან.

იტალიის მონაცემთა დაცვის საზედამხედველო ორგანომ, აღნიშნულ

გარემოებათა გათვალისწინებით, ვებგვერდის ოპერატორს დაავალა მონაცემთა დამუშავების GDPR-თან შესაბამისობაში მოყვანა 90 დღის განმავლობაში. თუ აღნიშნული ვადა საკმარისი არ აღმოჩნდა, “Google”-ის ანალიტიკასთან დაკავშირებული მონაცემების გადაცემა აშშ-ში უნდა შეჩერდეს.

ევროკავშირის მართლმსაჯულების სასამართლომ (CJEU) ტერორისტული და მძიმე დანაშაულების პრევენციის, გამოვლენის, გამოძიებისა და დამნაშავეთა დასჯის მიზნით, მგზავრთა პირადი მონაცემების (PNR) გამოყენების დირექტივის თაობაზე მიიღო გადაწყვეტილება

21.06.2022

დირექტივა ტერორისტული და მძიმე დანაშაულების პრევენციის, გამოვლენის, გამოძიებისა და დამნაშავეთა დასჯის მიზნით მგზავრთა პირადი მონაცემების (PNR) გამოყენების შესახებ, ევროკავშირის წევრი სახელმწიფოების მიერ მესამე ქვეყნის უფლებამოსილი უწყებებისათვის PNR მონაცემების გადასაცემად ადგენს სამართლებრივ ჩარჩოს. აღნიშნულის მიზანია ტერორისტული და მძიმე დანაშაულების პრევენცია, გამოვლენა, გამოძიება და დამნაშავეთა დასჯა.

მესამე ქვეყნის სახელმწიფო ორგანოებისათვის PNR მონაცემების გადაცემა ექვემდებარება ინდივიდუალურ შეფასებას, რომლის ფარგლებშიც უნდა განისაზღვროს, თუ რამდენად მოდის გადაცემა დირექტივის მიზნებთან შესაბამისობაში და განხორციელდა თუ არა ფუნდამენტურ უფლებათა დაცვით.

2022 წლის 21 ივნისს, ევროკავშირის მართლმსაჯულების სასამართლომ მიიღო გადაწყვეტილება, რომელშიც ზემოაღნიშნულ დირექტივასთან დაკავშირებით იმსჯელა. გადაწყვეტილება შეეხება ბელგიის საკონსტიტუციო სასამართლოს მიერ ევროკავშირის მართლმსაჯულების სასამართლოსთვის დასმულ სხვადასხვა კითხვას, რომლებიც, სხვა საკითხებთან ერთად, PNR დირექტივის მოქმედებას და 2016 წლის 25 დეკემბრის კანონის ევროკავშირის კანონმდებლობასთან თავსებადობას შეეხება .

ფოტო: european-union.europa.eu

- სასამართლომ განაცხადა, რომ PNR დირექტივა იწვევს სერიოზულ ჩარევას უფლებებში, რომლებიც გარანტირებულია ევროკავშირის ძირითად უფლებათა ქარტიის მე-6 და მე-8 მუხლებით, რადგან დირექტივით დადგენილია მეთვალყურეობის იმგვარი რეჟიმი, რომელიც განგრძობადი და სისტემატურია და არ არის გამიზნული/მიმართული კონკრეტულ პირთა წრეზე. ამ თვალსაზრისით აღინიშნა, რომ ჩარევა უნდა შეფასდეს მისი მნიშვნელობით/სერიოზულობით.

სასამართლომ აღნიშნა, რომ PNR-ის დირექტივით გათვალისწინებული მგზავრთა პირადი მონაცემების გადაცემა, დამუშავება და შენახვა, უნდა შეიზღუდოს მკაცრი საჭიროებით, კერძოდ, ტერორიზმსა და სერიოზულ დანაშაულთან ბრძოლის მიზნებით. შესაბამისად, დირექტივით გათვალისწინებული უფლებამოსილებები უნდა იქნას განხილული შეზღუდულად.

კანადის პირადი ცხოვრების ხელშეუხებლობის კომისრის ოფისმა, სხვა მონაცემთა დაცვის საერთაშორისო საზედამხედველო ორგანოებთან ერთად, კიბერუსაფრთხოების საკითხზე სახელმძღვანელო გამოსცა

30.06.2022

კანადის პირადი ცხოვრების ხელშეუხებლობის კომისრის ოფისმა, სხვა მონაცემთა დაცვის საერთაშორისო საზედამხედველო ორგანოებთან ერთად, გამოსცა სახელმძღვანელო, რათა დაეხმაროს პირებს კიბერ საფრთხეებისგან დასაცავად. აღნიშნული დოკუმენტი შემუშავდა „პირადი ცხოვრების ხელშეუხებლობის გლობალური ასამბლეის“ (“GPA”) სამუშაო ჯგუფის ფარგლებში.

დოკუმენტი იკვლევს ზოგად ტენდენციებს სხვადასხვა ანგარიშზე ერთი და იმავე მომხმარებლის სახელის, ელ-ფოსტის მისამართებისა და პაროლების ხელმეორედ გამოყენების თვალსაზრისით. ამგვარი პრაქტიკა კიბერ თავდამსხმელებს აძლევთ შესაძლებლობას, დაარღვიონ მონაცემთა უსაფრთხოება სხვადასხვა ონლაინ გვერდზე. ერთ-ერთი კვლევის თანახმად, ყოველდღიურად ასობით მილიონ მსგავს შემთხვევას აქვს ადგილი.

სახელმძღვანელოს მიზანია, დაეხმაროს პირებს და კომერციულ ორგანიზაციებს, რათა გამოავლინონ კიბერთავდასხმა ან მოახდინონ აღნიშნულის პრევენცია. დოკუმენტი ეხმარება ორგანიზაციებს, გაითვალისწინონ მონაცემთა დაცვისა და პირადი ცხოვრების ხელშეუხებლობის კანონმდებლობა, რომელთა შესაბამისად უნდა უზრუნველყონ პერსონალური ინფორმაციის დაცვა.

ფოტო: flaticon.com

სახელმძღვანელოში წარმოდგენილ ინფორმაციაზე დაყრდნობით, შემდეგი გარემოებებია გასათვალისწინებელი:

- ანგარიშის მფლობელებმა თავიდან უნდა აირიდონ პროგნოზირებადი პაროლები და შესაძლებლობების ფარგლებში, უნდა გამოიყენონ მრავალეტაპიანი იდენტიფიკაცია;
- ონლაინ ანგარიშის გატეხვის შემთხვევაში, პირებმა უნდა შეცვალონ პაროლები დაუყოვნებლივ, ასევე იმ

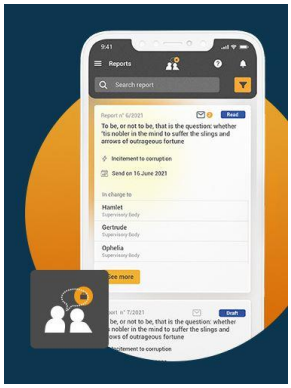
ანგარიშებზე, სადაც გამოყენებულია იგივე ან მსგავსი პაროლი;

პირები დაუყოვნებლივ უნდა დაუკავშირდნენ შესაბამის ფინანსურ უწყებებს, რომლებსაც შესაძლებლობა აქვთ, მოძებნონ ნებისმიერი ფინანსური ინფორმაცია იმ ანგარიშთან დაკავშირებით, რომელიც „გატეხილია“ ან არსებობს ეჭვი აღნიშნულის თაობაზე.

იტალიის საზედამხედველო ორგანომ პერუჯის საჯარო საავადმყოფო და IT მომსახურების განმახორციელებელი კომპანია მხილების პორტალის დაცვის გარანტიების გარეშე ფუნქციონირებისთვის დააჯარიმა

10.06.2022

[იტალიის საზედამხედველო ორგანომ შეამოწმა მხილების განცხადებების მართვის ყველაზე ხშირად გამოყენებადი სისტემის მიერ მონაცემების დამუშავების შესაბამისობა GDPR-ის მოთხოვნებთან.] ინსპექტირების შედეგად გამოვლინდა, რომ პერუჯის საჯარო საავადმყოფოს მიერ გამოყენებული მხილების განცხადებების მართვის აპლიკაცია მონაცემთა დამუშავების მოთხოვნებს არ შეესაბამებოდა. დადგინდა, რომ მხილების განცხადებების მართვის ელექტრონული სისტემა ადგენდა თუ რომელი პროგრამული უზრუნველყოფის (“Software”) საშუალებით უკავშირდებოდა მომხმარებელი მხილების განცხადებების მართვის აპლიკაციას, ხოლო ქსელური დაცვა (“Firewall”) აღრიცხავდა მომხმარებელთა მიერ აპლიკაციაში განხორციელებულ აქტივობებს. შედეგად, შესაძლებელი ხდებოდა აპლიკაციის მომხმარებელთა, როგორც პოტენციურ მამხილებელთა, ვინაობის დადგენა. აპლიკაციის მომხმარებლებს არ მიეწოდებოდათ ინფორმაცია მონაცემთა დამუშავების შესახებ.



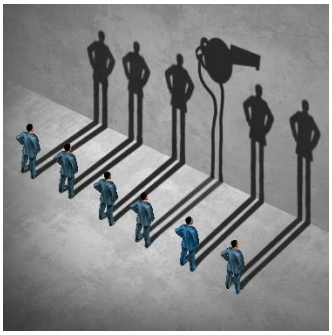
ფოტო: digitalpa.net

იტალიის საზედამხედველო ორგანომ დაადგინა, რომ მონაცემთა დამმუშავებლის მიერ:

- არ ჩატარებულა მონაცემთა დამუშავების ზეგავლენის შეფასება;
- არ აღრიცხულა მონაცემთა დამუშავების შემთხვევები GDPR-ის 30-ე მუხლის შესაბამისად;
- მონაცემებზე წვდომის მქონე პირებმა აპლიკაციაში ავთენტიფიკაციის გავლასთან დაკავშირებული მონაცემები გამოიყენეს GDPR-ის მოთხოვნების გაუთვალისწინებლად.

იტალიის საზედამხედველო ორგანომ განმარტა, რომ მხილების მომწესრიგებელი შიდა რეგულაციები სპეციალური კანონმდებლობის ქვეშ ექცევა, რომელიც GDPR-ის 88(1) მუხლის შესაბამისად, შრომითი საქმიანობის კონტექსტში მიზნად ისახავს დასაქმებულთა

(პოტენციურ მამხილებელთა) პერსონალური მონაცემების დამუშავებასთან დაკავშირებული უფლებებისა და თავისუფლებების დაცვას. კერძოდ, მხილება გულისხმობს მამხილებლის, მხილებული პირების, მოწმეებისა და მესამე პირების პერსონალური მონაცემების დამუშავებას. ამასთან, მონაცემთა დაცვის სპეციალური რეჟიმი ვრცელდება მხილების პროცესზე, რაც გულისხმობს მამხილებლის იდენტობის გამჟღავნებისგან დაცვას.



ფოტო: hsf.org

პერუჯის საჯარო საავადმყოფომ ვერ შეძლო ადეკვატური ტექნიკური და ორგანიზაციული ზომების მიღება, კერძოდ, მხილების განცხადებების მართვის აპლიკაციის მონაცემთა დაცვაზე ორიენტირებული დიზაინისა და პირველადი არჩევანის სახით მომხმარებლისთვის პერსონალურ მონაცემთა დაცვაზე ორიენტირებული მიდგომის შეთავაზება.

იტალიის საზედამხედველო ორგანომ პერუჯის საჯარო საავადმყოფო და IT კომპანია 40 000 ევროს ოდენობით დააჯარიმა.

საფრანგეთის საზედამხედველო ორგანომ (CNIL) “Google Analytics”-ის გამოყენებისა და აშშ-ში მონაცემთა გადაცემასთან დაკავშირებით ინფორმაცია და ხშირად დასმული კითხვები გამოაქვეყნა

07.06.2022

საფრანგეთის საზედამხედველო ორგანომ (CNIL) “Google Analytics”-ის გამოყენებისა და აშშ-ში მონაცემთა გადაცემასთან დაკავშირებით ინფორმაცია და ხშირად დასმული კითხვები გამოაქვეყნა. “Google Analytics” არის სერვისი, რომელიც შესაძლებელია ვებსაიტებში იქნეს ინტეგრირებული ინტერნეტ-მომხმარებლების ვიზიტების რაოდენობის დათვლის მიზნით. თითოეულ ვიზიტორს ენიჭება უნიკალური იდენტიფიკატორი, რომელიც პერსონალურ მონაცემს წარმოადგენს და მასთან დაკავშირებულ მონაცემებთან ერთად, “Google Analytics” მიერ აშშ-ს გადაეცემა.

ფოტო: commons.wikimedia.org

საფრანგეთის საზედამხედველო ორგანომ მიიღო არაერთი საჩივარი ციფრული უფლებების ევროპული ცენტრ – “NOYB” ასოციაციისგან “Google Analytics”-ის გამოყენებით ვებგვერდებზე შეგროვებული მონაცემების აშშ-ში გადაცემის თაობაზე. საერთო ჯამში, “NOYB”-მა 101 საჩივარი წარადგინა ევროკავშირის 27 წევრ ქვეყანასა და ევროპის ეკონომიკური ზონის (“EEA”) სამ სხვა ქვეყანაში მონაცემთა 101 დამმუშავებლის წინააღმდეგ, რომლებიც

“Google Analytics”-ის გამოყენებით, სავარაუდოდ, აშშ-ს პერსონალურ მონაცემებს გადასცემდნენ.

“CNIL”-მა, ევროპელ კოლეგებთან თანამშრომლობით, გააანალიზა გარემოებები “Google Analytics”-ის გამოყენებით შეგროვებული მონაცემების აშშ-სთვის გადაეცემის თაობაზე და განსაზღვრა დაკავშირებული პირებისთვის არსებული რისკები. “CNIL”-ი მიზნად ისახავდა ევროკავშირის მართლმსაჯულების სასამართლოს 2020 წლის 16 ივლისის გადაწყვეტილების “Schrems II” შედეგების გათვალისწინებას, რომლითაც გაუქმდა ე. წ. „პირადი ცხოვრების ხელშეუხებლობის ფარი“. გადაწყვეტილებაში სასამართლომ ხაზი გაუსვა ამერიკული დაზვერვის სამსახურების მიერ აშშ-ში გადაცემულ პერსონალურ მონაცემებზე წვდომის მიღების საფრთხეზე, თუკი მონაცემთა გადაცემა სათანადოდ არ იქნება რეგულირებული.

ფოტო: linkedin.com

“CNIL”-მა დაასკვნა, რომ აშშ-ში მონაცემთა გადაცემა ამჟამად საკმარისად არ არის რეგულირებული. კერძოდ, მონაცემთა გადაცემასთან დაკავშირებით „შესაბამისობის გადაწყვეტილების“ (ამგვარი გადაწყვეტილებით დგინდება რომ კონკრეტული ქვეყნის კანონმდებლობით უზრუნველყოფილია GDPR-ით განსაზღვრული უფლების დაცვის გარანტიების ტოლფასი მექანიზმები) არარსებობის პირობებში მონაცემთა გადაცემა შეიძლება, განხორციელდეს მხოლოდ იმ შემთხვევაში, თუ უზრუნველყოფილია უფლების დაცვის სათანადო გარანტიები მონაცემთა კონკრეტული ნაკადისთვის.

“CNIL”-მა არასაკმარისად ჩათვალა შემდეგი ზომების განხორციელება:

- ✗ “Google Analytics” ინსტრუმენტის კონფიგურაცია ისე, რომ არ გადაიტანოს პერსონალური მონაცემები აშშ-ში – “Google Analytics”-ის პასუხის თანახმად, იმ შემთხვევაშიც კი, თუ მონაცემთა გადაცემა არ გახდება საჭირო, კომპანიებს შეიძლება დასჭირდეთ წვდომა უზრუნველყონ მესამე ქვეყნის ხელისუფლებისთვის, ვინაიდან “Google Analytics”-ის ყველა მონაცემი იმართება აშშ-დან;
- ✗ “Google Analytics” ინსტრუმენტის კონფიგურაცია ისე, რომ მხოლოდ ანონიმიზირებული მონაცემების გადაცემა გახდეს შესაძლებელი აშშ-ში – “Google Analytics”-ის თანახმად, ინსტრუმენტი იყენებს ფსევდონიმიზაციასა და არა ანონიმიზაციას, IP მისამართის ანონიმიზაციის ფუნქციის გამოყენება ყველა სახის მონაცემთა გადაცემისთვის შეუძლებელი იქნება;
- ✗ დაშიფვრა.

“CNIL”-ის თანახმად, შესაძლებელია შექმნილი ვითარებიდან გამოსავალს წარმოადგენდეს შუამავალი სერვერების (“proxy server”) გამოყენება იმ დათქმით, რომ აღნიშნული შესაბამისობაში იქნება “EDPB”-ს 01/2020 გადაწყვეტილებასთან, კერძოდ, ფსევდონიმიზირებული

მონაცემების დამუშავება არ უნდა იძლეოდეს მონაცემთა სუბიექტის იდენტიფიცირების შესაძლებლობას.

ფოტო: flaticon.com

მოთხოვნები, რომლებსაც შუამავალი სერვერი უნდა აკმაყოფილებდეს:

- IP მისამართის გადაცემის შეუძლებლობა მონაცემთა მაჩვენებელი/საზომი ინსტრუმენტების სერვერებზე;
- მომხმარებლის იდენტიფიკატორის ჩანაცვლება შუამავალი სერვერით;
- ძირითად საიტზე არსებული ყველა დამატებითი მონაცემის წაშლა;
- შეგროვებულ "URL"-ებში არსებული ნებისმიერი პარამეტრის წაშლა;
- ინფორმაციის ხელახალი დამუშავება, რომელსაც შეუძლია ხელი შეუწყოს „მომხმარებლის აგენტების" წარმოქმნას, უიშვიათესი კონფიგურაციების გამორიცხვა, რამაც შეიძლება გამოიწვიოს მომხმარებლის ხელახალი იდენტიფიკაცია;
- იდენტიფიკატორების რაიმე სახის კრებულით არსებობის გამორიცხვა;
- ნებისმიერი სხვა მონაცემის წაშლა, რამაც შეიძლება გამოიწვიოს ხელახალი იდენტიფიკაცია.

ირლანდიის საზედამხედველო ორგანომ დრონების გამოყენებით მონაცემთა დამუშავების შესახებ სახელმძღვანელო გამოაქვეყნა

24.06.2022

ირლანდიის საზედამხედველო ორგანოს ხელმძღვანელის მოადგილემ, 2022 წლის 24 ივნისს LInkdin-ზე განაცხადა, რომ გამოქვეყნდა დრონების გამოყენებით მონაცემთა დამუშავების შესახებ სახელმძღვანელო. სახელმძღვანელოში განმარტებულია, რომ დრონები წარმოადგენენ უპილოტო საფრენი აპარატების იმ ფართო კატეგორიას, რომლებიც დისტანციურად იმართებიან და აღჭურვილი არიან სურათების, ვიდეოების, ხმებისა ან/და სხვა ინფორმაციის შეგროვების ტექნოლოგიით (მონაცემთა შეგროვების სისტემა), რასაც შემდგომ ჭკვიან მოწყობილობებს გადასცემენ (მაგალითად, ღრუბლოვან საცავებს ე. წ. "cloud storage"-ს). დრონებს შეუძლიათ, გადაიქცნენ მობილურ სათვალთვალო სისტემად და დაამუშაონ გამვლელთა (მონაცემთა სუბიექტების) პერსონალური მონაცემები.

ფოტო: flaticon.com

აღნიშნულიდან გამომდინარე, ირლანდიის საზედამხედველო ორგანო დრონის ოპერატორებს განიხილავს როგორც მონაცემთა დამმუშავებლებს (გარდა იმ შემხვევებისა, როდესაც დრონი გამოიყენება მხოლოდ საოჯახო-სამეურნეო

ან პირადი მიზნებისთვის) და მათ გარკვეულ ვალდებულებებს აკისრებს, რათა თავიდან აირიდონ მონაცემთა სუბიექტის უფლებების შეუქცევადი დარღვევა. სახელმძღვანელო არ ვრცელდება დრონების სამართალდაცვითი მიზნებისთვის გამოყენებაზე.

ირლანდიის საზედამხედველო ორგანო დრონის ოპერატორებს მონაცემთა დამუშავების კანონიერების ტესტს სთავაზობს. მონაცემთა დამუშავების ყველაზე გავრცელებული საფუძვლის – თანხმობის გამოყენება დრონებთან მიმართებით ნაკლებად აქტუალურია, ვინაიდან, როგორც წესი, დრონის ოპერატორი მოკლებულია შესაძლებლობას, მიიღოს თანხმობა ყველა იმ პირისგან, რომლის მონაცემები დრონის მეშვეობით მუშავდება.

როდესაც მონაცემთა დამმუშავებელი იყენებს დრონს და აღნიშნულს არ აქვს ცალსახად პირადი ან საოჯახო-სამეურნეო ხასიათი, მას ეკისრება ვალდებულება დაასაბუთოს, რომ:

- მონაცემთა დამუშავება მონაცემთა სუბიექტის ინტერესში შედიოდა;
- დრონის გამოყენება საჭიროა ლეგიტიმური მიზნის მისაღწევად;
- რომ მას არ აქვს არაპროპორციული ზეგავლენა მონაცემთა სუბიექტზე, მაგალითად, გამოყენებული იქნება ავტომატური გაბუნდოვანების ფუნქცია და სხვა.

საოჯახო-სამეურნეო მიზნებისთვის დრონის გამოყენების შემთხვევაში, საზედამხედველო ორგანომ მოუწოდა დრონის ოპერატორებს, მონაცემთა დამუშავების ფარგლების განსაზღვრისას, იხელმძღვანელონ „გონივრულობის პრინციპით“, მოერიდონ სახეებისა და სხვისი პირადი სივრცის გადაღებას.

ფოტო: sutterstock.com

საზედამხედველო ორგანომ მონაცემთა დამმუშავებლებს, რიგი გარემოებებიდან გამომდინარე, შეიძლება ვალდებულებად განუსაზღვროს მონაცემთა დამუშავების ზეგავლენის შეფასების წარმოება და პირადი ცხოვრების ხელშეუხებლობის პოლიტიკის შემუშავება.

ასევე, მიზანშეწონილია, მონაცემთა დამმუშავებლებმა გაითვალისწინონ:

- კარგად გაეცნონ დრონების მართვის მარეგულირებელ კანონმდებლობას (მაგალითად, კერძო საკუთრებაში უნებართვო შეღწევის შესახებ);
- განსაზღვრონ მონაცემთა დამუშავების თავდაპირველი და შემდგომი მიზნები;
- მონაცემთა სუბიექტის მხრიდან ინფორმაციის მოთხოვნის შემთხვევაში, მიაწოდონ მას ამომწურავი ინფორმაცია მონაცემთა დამუშავების მიზნების, კანონიერებისა და სუბიექტის უფლებების შესახებ;
- გაითვალისწინოს მონაცემთა მინიმიზაციის პრინციპი, ანონიმიზაციისა და ფსევდონიმიზაციის შესაძლებლობა მონაცემთა არამიზნობრივი (გადაჭარბებული) დამუშავების ასარიდებლად.