პერსონალურ მონაცემთა
დაცვის სამსახური

პერსონალური მონაცემების თვითნებური ბასაჭარობა

მოსალოდნელი რისკები და რეკომენდაციები

ინტერნეტის ხელმისაწვდომობის ზრდისა და ტექნოლოგიური განვითარების შედეგად საზოგადოება ყოველდღიურად ეცნობა იმ ახალ საშუალებებსა და მიღწევებს, რომელიც ხშირად მათში სასიამოვნო გაკვირვებასა და ოპტიმისტურ განწყობას აყალიბებს. 90-იანი წლების შემდგომ თითოეული ჩვენგანი ტექნოლოგიური რევოლუციის არამხოლოდ მომსწრე, არამედ მონაწილეც არის. ონლაინ გამოცემები, ტელევიზიები, სხვა მედია საშუალებები მომენტალურად ავრცელებენ ინფორმაციას ამა თუ იმ ნოვაციის შესახებ, რომელიც უკავშირდება ჯანდაცვას, ბიოტექნოლოგიებს, ბლოკჩეინს, IOS თუ Android სისტემების განახლებებს, სოციალური ქსელების ახალ ფუნქციონალებს, 5G ტექნოლოგიებს, ხელოვნურ ინტელექტს, კვანტურ კომპიუტერებს, რობოტიკასა და ავტომატიზაციას. სამომხმარებლო პერსპექტივის გათვალისწინებით, საზოგადოების დიდი ნაწილი არსებულ სიახლეებს მხოლოდ შესაძლებლობების თვალსაზრისით აღიქვამს და ხშირად მეორე ხარისხოვანი ხდება ის რეალური აქტივი, რომელიც პერსონალურ მონაცემად არის ცნობილი. აღნიშნული საინფორმაციო ბლოგის ფარგლებში ყურადღება იქნება გამახვილებული სწორედ ამ კრიტიკულად მნიშვნელოვან საკითხებზე, რათა საზოგადოებას ეცნობოს რა რისკებს შეიძლება უკავშირდებოდეს პერსონალური მონაცემების თვითნებური გასაჯაროება.

პირადი ცხოვრების ხელშეუხებლობა ადამიანის ერთ-ერთი ფუნდამენტური უფლებაა და თითოეული ინდივიდის პერსონალური მონაცემები დაცული უნდა იყოს. აღსანიშნავია რომ, მონაცემები თანამედროვე მსოფლიოში ერთ-ერთ უმნიშვნელოვანეს ღირებულებას წარმოადგენს. სხვადასხვა ორგანიზაციების საქმიანობა, მათ შორის ციფრული ტექნოლოგიების სფეროს განვითარება, უმეტესად მონაცემთა დამუშავებას ეფუძნება. აღნიშნულ ინფორმაციას ხშირ შემთხვევაში უშუალოდ მონაცემთა სუბიექტი ან ზოგჯერ, მისი ახლობელი პირი ხდის ხელმისაწვდომს. პერსონალურ მონაცემთა გაზიარებისას ეს პირები შესაძლოა ვერ აღიქვამდნენ მოსალოდნელ საფრთხეებს და იმ ზიანს, რომელიც მათ/მათი ახლობლების პირადი ცხოვრების ხელშეუხებლობის, პერსონალურ მონაცემთა დაცვისა და სხვა ფუნდამენტურ უფლებებს შეიძლება მიადგეს.

ქვემოთ განვიხილავთ სწორედ იმ შემთხვევებსა და რისკებს, რაც პირის მიერ ნებაყოფლობით თავის ან ახლობლის შესახებ ინფორმაციის გაზიარებას და მონაცემთა ამგვარ დამუშავებას შეიძლება ახლდეს თან.

ფიზიკური პირის მიერ მონაცემთა გასაჯაროება

პერსონალური მონაცემების გასაჯაროება მოიაზრებს ყველა იმ შემთხვევას, როდესაც ეს ინფორმაცია სხვა მესამე პირებისთვის ხდება ხელმისაწვდომი. *მაგალითად, როდესაც ინდივიდი **პირისპირ კომუნიკაციის** ფარგლებში თავის ან მისთვის ნაცნობი, ახლობელი პირის შესახებ ინფორმაციას, როგორიცაა სახელი, გვარი, საცხოვრებელი მისამართი, ელექტრონული ფოსტა უზიარებს სხვა ფიზიკურ პირს ან ორგანიზაციას.*

2024 წლისთვის **სოციალური ქსელების მომხმარებელთა** რაოდენობამ 5 მილიარდს მიაღწია. მისი მეშვეობით მსოფლიოს გარშემო ყოველდღიურად ასი ათასობით ინფორმაცია ზიარდება, ხოლო მომხმარებლის მიერ შერჩეული პარამეტრების გათვალისწინებით, იგი შესაძლოა ხელმისაწვდომი გახდეს პირთა ფართო წრისთვის.

ფიზიკური პირის მიერ მონაცემთა სოციალური ქსელით გასაჯაროებაა, *როდესაც ინდივიდი სხვებისთვის ხელმისაწვდომს ხდის არა მხოლოდ საკუთარ, არამედ შვილის, მეგობრების ან სხვა მესამე პირის მონაცემებს. მაგალითად, როდესაც იგი პირად გვერდზე აზიარებს განათლების, სამუშაო ადგილის შესახებ ინფორმაციას, აზიარებს ფოტოსურათს, ასევე, როდესაც მის მიერ განთავსებულ პოსტზე მონიშნავს თავის და მასთან ერთად მყოფი პირების ზუსტ ადგილმდებარეობას და ა.შ.*

მონაცემთა გასაჯაროებად ასევე მიიჩნევა **სოციალური ქსელის ჯგუფებში** მონაცემთა განთავსებაც. *მაგალითად, როდესაც პირმა იპოვა სხვისი პირადობის მოწმობა და დახმარების მიზნით ეს მომხმარებელთა საერთო ჯგუფში განათავსა ან გააზიარა ვიდეოჩანაწერი, რომელზეც სხვა პირია გამოსახული.*

ინდივიდმა შესაძლოა პერსონალური მონაცემები გაუზიაროს ორგანიზაციას მისი **აპლიკაციის მომსახურებით** სარგებლობისას. *მაგალითად, აპლიკაციები, რომლებიც მომხმარებლის მიერ მიწოდებული ფოტოსურათების დამუშავებით, ხელოვნური ინტელექტის მეშვეობით ქმნის კონკრეტული თემატიკის ფოტოებს, ასევე სოციალური ქსელების აპლიკაციები, რომლებიც მომხმარებლის გარკვეულ მონაცემებს (როგორიცაა მისი ადგილმდებარეობა, კონტაქტები და სხვა) მათი პარამეტრებიდან გამომდინარე ამუშავებენ.*

თითქმის ყველა ზემოთ ჩამოთვლილ შემთხვევაში, ინფორმაციის ერთობლიობა, რომელსაც მომხმარებლები ციფრულ პლატფორმებზე აზიარებენ, მათ **„ციფრულ კვალს“** ქმნის. *მაგალითად, როდესაც სოციალურ ქსელში განთავსებულ პოსტს მოიწონებს, გააზიარებს ან დატოვებს მასზე კომენტარს, ასევე როდესაც მუსიკის ან ვიდეოპორტალის აპლიკაციები ინახავენ „მოსმენის/ყურების ისტორიას“ და სხვა.*

ფიზიკური პირის მიერ მონაცემთა გასაჯაროების რისკები/შედეგები

თანამედროვე სამყაროში ტექნოლოგიების შედეგად შექმნილი ონლაინ სივრცე არაერთ სარგებელს იძლევა, თუმცა წარმოშობს გარკვეულ რისკებს პირადი ცხოვრების ხელშეუხებლობისა და პერსონალური მონაცემების დაცვის თვალსაზრისით. მონაცემთა სუბიექტები საკუთარი, ახლობელი ან/და მესამე პირების პერსონალურ მონაცემებს ინტერნეტსივრცეში, სოციალური ქსელების მეშვეობით, ხშირად იმგვარად ასაჯაროებენ, რომ მათთვის უცნობია პოტენციური საფრთხისა და დამდგარი შედეგების შესახებ.

შესაძლებელია გამოვყოთ ფიზიკური პირების მიერ მონაცემთა გასაჯაროების სოციალური ურთიერთობების, ქცევითი, სახელშეკრულებო და შინაარსობრივი რისკები. კერძოდ, სოციალური ურთიერთობების რისკი უკავშირდება ონლაინ შეხვედრებში მონაწილეობას, რამაც შესაძლოა გამოიწვიოს ციფრული თაღლითობა, შევიწროება, ადევნება, პირადი ინფორმაციის მოპოვება, მასზე კონტროლი და ა.შ. უკანონო ციფრული მარკეტინგის შეტყობინებების მიღება, ეკონომიკური და უსაფრთხოების რისკები, რომლებიც „ციფრულ მარკეტში“ აქტიურ მონაწილეობას მიემართება, თავის მხრივ, სახელშეკრულებო რისკებში ერთიანდება. რაც შეეხება ქცევით რისკებს, აღნიშნული შესაძლოა გამოიხატებოდეს უკანონო საქმიანობაში ჩართვის, საზიანო მასალების გაზიარების და სხვა მსგავსი ქმედების განხორციელებაში. ხოლო, შინაარსობრივი რისკები გულისხმობს შეტყობინებების, ინფორმაციის მიღებას, რომელიც არასასურველი რეკლამის, საზიანო ან აგრესიული შინაარსის მატარებელი შეიძლება იყოს.[1]

მნიშვნელოვანია მხედველობაში იქნეს მიღებული ის შედეგები, რაც მონაცემთა გასაჯაროებას შეიძლება მოჰყვეს. ციფრული ტექნოლოგიის ეპოქაში განსაკუთრებით ფართოა იმ საფრთხეებისა და ზიანის ჩამონათვალი, რაც პირის პერსონალური მონაცემების გასაჯაროებით მის უფლებებსა და თავისუფლებებს ემუქრება. *აღნიშნული რისკებიდან შეიძლება გამოვყოთ შემდეგი:*

[1] ციფრულ გარემოში ბავშვის პერსონალურ მონაცემთა დაცვის გზამკვლევი, პერსონალურ მონაცემთა დაცვის სამსახური, თბილისი, 2022, 4. <https://shorturl.at/psFdl>.

პიროვნების ქურდობა (Identity theft)

სახელი, გვარი, პირადი ნომერი, დაბადების თარიღი და საცხოვრებელი მისამართი იძლევა საკმარის ინფორმაციას სუბიექტის შესახებ. აღნიშნული ინფორმაცია, შესაძლოა გამოყენებულ იქნეს პირის იდენტობის მითვისებისთვის და შემდგომ მისი სახელით იმგვარი ქმედებების განხორციელებისთვის, რაც მისთვის ფინანსური თუ რეპუტაციული ზიანის მომტანი იქნება, პირვანდელი მდგომარეობის აღდგენას შეიძლება დიდი დრო და ძალისხმევა დასჭირდეს, ცალკეულ შემთხვევებში კი შეუძლებელიც კი აღმოჩნდეს.

პირის იდენტობა შეიძლება გამოყენებული იყოს მის მაგივრად სხვადასხვა მომსახურების მიღებისთვის, რაც მხოლოდ სუბიექტის მინიმალური ინფორმაციის დამუშავებას საჭიროებს *(მაგალითად, ონლაინ განაცხადის მეშვეობით სწრაფი სესხის აღებისთვის).*

განსაკუთრებით საყურადღებოა შემთხვევები, როდესაც პიროვნების ქურდობის მსხვერპლი არასრულწლოვანია. ბავშვები მეტად მოწყვლადნი არიან მათი პერსონალური მონაცემების დაცვის კუთხით, რადგან უმეტეს შემთხვევებში მათ ინფორმაციას *(ფოტოსურათს, სახელს, გვარს, სასწავლო დაწესებულებას, ასაკს და სხვა)* ასაჯაროებენ მშობლები, ოჯახის წევრები და ახლობლები. არასრულწლოვნებს არ აქვთ შესაბამისი ცოდნა, გამოცდილება ან საშუალება, რომ გავლენა იქონიონ აღნიშნულ პროცესებზე. შესაბამისად მნიშვნელოვანია, რომ ზრდასრულმა პირებმა **განსაკუთრებული სიფრთხილე** გამოიჩინონ ბავშვების მონაცემების, მათ შორის, ფოტოსურათების გასაჯაროებისას.

ფიშინგი

ფიშინგი ერთ-ერთი ყველაზე გავრცელებული ინტერნეტ თაღლითობაა, როდესაც რეალობას მიმსგავსებული შეტყობინებებისა თუ სხვაგვარი კომუნიკაციის მეშვეობით დამნაშავეები ცდილობენ მოიპოვონ ინფორმაცია პირის შესახებ. უმეტეს შემთხვევებში, ისინი მსხვერპლს აწვდიან რაიმე ბმულს *(მაგალითად, სატრანსპორტო კომპანიის, ქსელური მარკეტის, გათამაშების და სხვა),* რომელიც გამოიყურება რეალურად, თუმცა მომხმარებელი გადაჰყავს თაღლითურ ვებგვერდზე. ამგვარად, მომხმარებელს აქვს რწმენა, რომ იმყოფება სანდო ვებგვერდზე, რის შემდეგაც შეჰყავს მოთხოვნილი ინფორმაცია, პაროლები, პირადი ან საბანკო დეტალები. აღნიშნული მონაცემები თაღლითების ხელში აღმოჩნდება, რომელთაც მონაცემთა გაყიდვის ან სხვაგვარად გამოყენების შესაძლებლობა ეძლევათ.

დისკრიმინაცია და სტიგმატიზაცია

ხშირად ინტერნეტსივრცეში პირის მიერ გაზიარებულ ფოტოსურათებზე, ვიდეოში გამოსახული სხვა პიროვნება შესაძლოა საზოგადოების მხრიდან დაცინვის, დისკრიმინაციის ან სტიგმატიზაციის ობიექტი გახდეს. აღნიშნული რისკები განსაკუთრებით იზრდება, როდესაც ამ ინფორმაციის გაზიარება ხდება არა კონკრეტული პირებისთვის *(მაგალითად, სამეგობრო წრისთვის),* არამედ ფართო საზოგადოებისთვის, რა დროსაც მოსალოდნელია სხვადასხვაგვარი რეაქციები.

განსაკუთრებით საგულისხმოა **არასრულწლოვნის** მონაწილეობით ვიდეოჩანაწერებისა და ფოტოსურათების გასაჯაროება, რამაც ცალკეულ შემთხვევებში, კონტექსტიდან გამომდინარე, შესაძლოა გამოიწვიოს მისი ღირსების შელახვა, სტიგმატიზაცია, ბულინგი, დისკრიმინაცია ან ნეგატიური გავლენა იქონიოს მის ემოციურ მდგომარეობასა და განვითარებაზე.

ემოციური წნეხი, შანტაჟი და გამოძალვა

ზოგიერთ შემთხვევაში სუბიექტი თანმდევი რისკების გათვითცნობიერების გარეშე უზიარებს საკუთარ მონაცემებს, *მათ შორის განსაკუთრებული კატეგორიის მონაცემებსაც*, მისთვის არცთუ ისე სანდო პირებს. აღნიშნული ინფორმაცია შესაძლოა გამოყენებული იქნეს შანტაჟის ან გამოძალვის მიზნებისთვის, რასაც თან ახლავს სუბიექტის ემოციური წნეხი.

მონაცემთა ავტომატური დამუშავება (Data Scraping)

მონაცემთა ავტომატური დამუშავება, ე.წ. *„ვებსკრეიპინგი“* ან *„მონაცემთა სკრეიპინგი“*, მონაცემთა შეგროვების თანამედროვე ციფრული მეთოდია, რომელიც სხვადასხვა სფეროში გამოიყენება. აღნიშნული გულისხმობს ინტერნეტიდან, *მაგალითად სოციალური მედიიდან,* მონაცემების ჩამოტვირთვას და ელექტრონულ ფორმატში მის შენახვას/შეგროვებას. ამ მეთოდით შესაძლებელი ხდება დიდი რაოდენობით მონაცემების *(მათ შორის, პერსონალური მონაცემების)* ერთდროულად, მოკლე დროში, განსაკუთრებული ძალისხმევის გარეშე შეგროვება. აღნიშნული ტექნოლოგიების შესაძლებლობა, ერთიანად შეაგროვოს დიდი რაოდენობით მონაცემთა სუბიექტების მონაცემები, მონაცემთა დაცვის რისკებს ქმნის. ამ გზით მოპოვებული ინფორმაცია შესაძლოა სხვადასხვა

მიზნებისთვის *(მაგალითად, მიზნობრივი კიბერშეტევები, პიროვნების ქურდობა, მონიტორინგი/პროფაილინგი)* იყოს გამოყენებული და ზიანის მომატანი იყოს სუბიექტისთვის.

მაგალითისთვის, ერთ-ერთი ყველაზე ცნობილი სახის ამომცნობი ტექნოლოგიების კომპანია "Clearview AI" თავის მონაცემთა ბაზას სწორედ სოციალური მედიიდან მომხმარებლების შესახებ არსებული ინფორმაციის „ავტომატური წამოღების" მეშვეობით ქმნიდა. აღნიშნული მონაცემთა დამუშავების პროცესი, მიუხედავად ამ ინფორმაციის საჯაროობისა, არაერთმა ევროპულმა საზედამხედველო ორგანომ[2][3] მონაცემთა დაცვის ზოგადი რეგულაციის (GDPR) დარღვევად მიიჩნია და კომპანიას ადმინისტრაციული სახდელი დააკისრა.

„ვებსკრეიპინგით" პერსონალურ მონაცემთა შეგროვებისას მონაცემთა სუბიექტებს არ შეუძლიათ რაიმე სახის გავლენა იქონიონ მათ შემდგომ დამუშავებაზე, რაც უმეტესად სრულიად სცდება მათ მიერ ამ მონაცემების თავდაპირველი გასაჯაროების მიზნებს.

სოციალური ქსელების მეშვეობით ინტერნეტსივრცეში გაზიარებული პერსონალური მონაცემები შესაძლოა გამოყენებულ იქნეს მონაცემთა სუბიექტის ინფორმირების, თანხმობის გარეშე, სოციალური კვლევების, პირდაპირი მარკეტინგის, საარჩევნო კამპანიის[4] მიზნებისთვის. საგულისხმოა, რომ ტექნოლოგიური პროგრესის პირობებში პერსონალური მონაცემების დამუშავება ხელოვნური ინტელექტის (AI) მეშვეობითაც აქტიურად ხდება. ამდენად, ფიზიკურმა პირებმა მონაცემთა გასაჯაროებამდე უნდა გაითვალისწინონ მოსალოდნელი რისკები და წინასწარ განსაზღვრონ შესაძლო უარყოფითი შედეგების დადგომის შესაძლებლობა.

---

[2] *Autoriteit Persoonsgegevens,* Decision fines and orders subject to a penalty Clearview, 16.05.2024, <https://www.autoriteitpersoonsgegevens.nl/en/system/files?file=2024-09/Decision%20fines%20and%20orders%20subject%20to%20a%20penalty%20Clearview.pdf>.

[3] Decision by the Austrian SA against Clearview AI Infringements, 10.05.2023, <https://www.edpb.europa.eu/news/national-news/2023/decision-austrian-sa-against-clearview-ai-infringements-articles-5-6-9-27_en>.

[4] მაგალითად, 2010 წელს ერთ-ერთმა ბრიტანულმა კომპანიამ ("Cambridge Analytica") სოციალური ქსელის, "Facebook"-ის მილიონობით მომხმარებლის პერსონალური მონაცემები, მათი თანხმობის გარეშე, პოლიტიკური მიზნებისთვის გამოიყენა. *იხ. The Guardian,* "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach", 17.03.2018, <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>, [07.10.2024].

რეკომენდაციები

პერსონალურ მონაცემთა დამუშავება უმეტესად შესაძლოა უშუალოდ სუბიექტის ან სხვა ფიზიკური პირის მიერ ამ ინფორმაციის პირადი მიზნით გასაჯაროებას ეფუძნებოდეს. მონაცემთა გაზიარებისას მხედველობაში არ არის მიღებული ამ ქმედებებიდან გამომდინარე საფრთხეები. იმისათვის, რომ ზემოთ განხილული შემთხვევები თავიდან იქნეს არიდებული, მნიშვნელოვანია შემდეგი რეკომენდაციების გათვალისწინება:

- ციფრული პლატფორმებისთვის მომხმარებელმა შექმნას **„ძლიერი პაროლი“** და ისარგებლოს ორმაგი ავთენტიფიკაციის მეთოდით *(თუ აპლიკაცია ამის შესაძლებლობას იძლევა).* სასურველია არ გამოიყენოთ თქვენთან დაკავშირებული ინფორმაცია, რომელიც მესამე პირებისთვისაცაა ცნობილი ან მარტივად არის ხელმისაწვდომი *(თქვენს მიერ საჯაროდ გავრცელებული ინფორმაციიდან). მაგალითად, მომხმარებლის სახელი, გვარი, დაბადების თარიღი/ადგილი, შინაური ცხოველის სახელი და სხვა.* სხვა პირის მიერ მომხმარებლის ანგარიშზე წვდომა გულისხმობს, რომ მისთვის ხელმისაწვდომი იქნება ყველა ინფორმაცია, რასაც ეს პირი სოციალურ ქსელში განათავსებს (აღნიშნულში მოიაზრება პირადი მიმოწერებიც);
- ე.წ. „ფიშინგის“ თავიდან ასაცილებლად, მაგალითად, საბანკო ტრანზაქციების ონლაინ პლატფორმების მეშვეობით განხორციელებამდე, მომხმარებელი უნდა დარწმუნდეს ვებგვერდის სანდოობასა და ამავე პლატფორმის შესაბამისი საბანკო დაწესებულებისადმი კუთვნილებაში;
- სოციალურ ქსელში გაეცნოს და ისარგებლოს **„კონფიდენციალურობის პარამეტრებით“** (Privacy Settings). განსაზღვროს თუ მის რა მონაცემებზე ექნება წვდომა აპლიკაციას *(ადგილმდებარეობა, კონტაქტები, ოჯახური მდგომარეობის შესახებ ინფორმაცია და სხვა),* პირთა წრე, ვისთვისაც მის მიერ გაზიარებული ინფორმაცია იქნება ხელმისაწვდომი. უმჯობესია, რომ პირმა მონაცემები გაუზიაროს მხოლოდ მის მიერ წინასწარ განსზღვრულ ვიწრო წრეს;
- აუცილებელია, რომ სხვა პირების მონაცემთა გაზიარებისას მათი სურვილი იყოს გათვალისწინებული. მეტად საყურადღებოა სხვადასხვა ჯგუფებში პირთა ფართო ან განუსაზღვრელი წრისათვის ამ ინფორმაციის გასაჯაროება;
- განსაკუთრებული სიფრთხილით მოპყრობას საჭიროებს **ბავშვების პერსონალური მონაცემები**, რადგან ისინი მეტად მოწყვლადნი შეიძლება იყვნენ მონაცემთა ბოროტად გამოყენებისადმი;

- მოერიდეთ **განსაკუთრებული კატეგორიის მონაცემების** გაზიარებას სხვა პირებისთვის, შანტაჟის, გამოძალვის თუ სხვა ემოციური წნეხის მომტანი ქმედებების თავიდან ასაცილებლად;
- დაფიქრდით სანამ მონაცემებს **უცხო პირს გაუზიარებთ**, დააზუსტეთ მათი სანდოობა და მონაცემთა დამუშავების მიზნები.

დემოკრატიული საზოგადოების თითოეული წევრის პერსონალურ მონაცემთა დაცვისთვის უმნიშვნელოვანესია არა მხოლოდ კანონმდებლობის ფარგლებში ან მისი მექანიზმებით აღნიშნული უფლების დაცვის უზრუნველყოფა, არამედ სოციუმში, პირად ურთიერთობებში მონაცემთა დაცვისა და პატივისცემის კულტურის ამაღლება. აღნიშნული შესაძლებელს გახდის ზემოთ ჩამოთვლილი საფრთხეებისა და ადამიანის უფლებებისადმი ზიანის თავიდან არიდებას.

მის.: საქართველო, თბილისი, ნ. ვაჩნაძის N7, 0105
ბათუმი, ბაქოს N 48, 6010

ტელ.: (+995 32) 242 1000
E-mail: office@pdps.ge
www.pdps.ge