რა უნდა ვიცოდეთ ევროკავშირის მონაცემთა დაცვის რეგულაციის შესახებ

რა უნდა ვიცოდეთ ევროკავშირის მონაცემთა დაცვის რეგულაციის შესახებ

პერსონალურ მონაცემთა დაცვის
ინსპექტორის აპარატი

შესავალი

2018 წლის 25 მაისს ძალაში შევიდა ევროკავშირის მონაცემთა დაცვის ზოგადი რეგულაცია („General Data Protection Regulation“)[1]. რეგულაციას პერსონალურ მონაცემთა დაცვა სრულიად ახალ საფეხურზე გადაჰყავს და მიზნად ისახავს ტექნოლოგიური პროგრესისა და თანამედროვე გამოწვევების პირობებში ინდივიდების უფლებების სათანადო დაცვას. რეგულაცია ამკვიდრებს ისეთ ახალ პრინციპებს, როგორიცაა მონაცემთა დამმუშავებელი ორგანიზაციების ანგარიშვალდებულება, მონაცემთა პორტირება, მონაცემთა უსაფრთხოების დარღვევის შეტყობინების ვალდებულება და სხვა.

რეგულაცია ევროკავშირის წევრ ქვეყნებში პირდაპირ მოქმედებს და არ საჭიროებს ეროვნულ კანონმდებლობაში ასახვას[2]. იგი აწესებს ევროკავშირის მთელ ტერიტორიაზე მონაცემთა დაცვის ერთიან სავალდებულო წესებს, რაც გამორიცხავს ამა თუ იმ საკითხის რადიკალურად განსხვავებულ მოწესრიგებას. ეს მონაცემთა დამმუშავებელ ორგანიზაციებს გაუმარტივებს ევროკავშირის ტერიტორიაზე საქმიანობას და მონაცემთა დამუშავების წესების დაცვას.

---

1 ევროპარლამენტისა და საბჭოს 2016 წლის 27 აპრილის რეგულაცია (EU) 2016/679 პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვისა და ასეთი მონაცემების თავისუფალი მიმოცვლის შესახებ, რომელიც აუქმებს 95/46/EC დირექტივას. აღნიშნული რეგულაცია წარმოადგენს ევროკავშირის მონაცემთა დაცვის რეფორმის ნაწილს. რეფორმის ფარგლებში მიღებულია ასევე 2016 წლის 27 აპრილის დირექტივა (EU) 2016/680, რომელიც არეგულირებს სამართალდამცავი ორგანოების მიერ მონაცემთა დამუშავებას (ხელმისაწვდომია: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L0680) და მიმდინარეობს მუშაობა ელექტრონულ კომუნიკაციებში პერსონალურ მონაცემთა დაცვის შესახებ ახალ რეგულაციაზე (პროექტი ხელმისაწვდომია: http://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX%3A52017PC0010).

2 თუმცა, ევროკავშირის წევრ ქვეყნებს შეუძლიათ მიიღონ კანონები, სადაც კონკრეტულად იქნება მოწესრიგებული რეგულაციით გათვალისწინებული გარკვეული საკითხები. მაგალითად, იხ.: გერმანიის ფედერაციული რესპუბლიკის მონაცემთა დაცვის ფედერალური კანონი (ხელმისაწვდომია: https://www.bvdnet.de/wp-content/uploads/2017/08/BMI_Übersetzung_DSAnpUG-EU_mit_BDSG-neu.pdf).

მნიშვნელოვანია, რომ რეგულაცია ვრცელდება არა მხოლოდ ევროკავშირში რეგისტრირებულ, არამედ იმ ორგანიზაციებზეც, რომლებიც არ არიან რეგისტრირებული ევროკავშირში, თუმცა ამუშავებენ ევროკავშირში მყოფი პირების მონაცემებს. ევროკავშირთან გაღრმავებული სავაჭრო ურთიერთობების გათვალისწინებით, რეგულაცია ვრცელდება ცალკეულ ქართულ ორგანიზაციებზეც.

ვინაიდან რეგულაციის წესების დარღვევისთვის საკმაოდ მაღალი სანქციებია გათვალისწინებული, მნიშვნელოვანია, ორგანიზაციებმა იცოდნენ, რა ვალდებულებები ეკისრებათ და როგორ უნდა უზრუნველყონ მათი საქმიანობის რეგულაციასთან შესაბამისობა. ამ საინფორმაციო ბროშურის მიზანია, მოკლედ მოუყაროს თავი რეგულაციის მნიშვნელოვან დებულებებს და დაინტერესებულ პირებს მარტივი ფორმით მიაწოდოს ინფორმაცია ევროკავშირში არსებული ახალი საკანონმდებლო მოთხოვნების შესახებ.

ვისზე ვრცელდება რეგულაცია

რეგულაციის მუხლები 2, 3 და 27

ევროკავშირის მონაცემთა დაცვის ზოგადი რეგულაცია ვრცელდება ევროკავშირში რეგისტრირებულ ნებისმიერ ორგანიზაციაზე, რომელიც საქმიანობის ფარგლებში ამუშავებს პერსონალურ მონაცემებს. სხვა ქვეყნებში, მათ შორის, საქართველოში რეგისტრირებულ ორგანიზაციებზე, რეგულაცია ვრცელდება იმ შემთხვევაში, თუ მათ აქვთ ფილიალი/წარმომადგენლობა ევროკავშირის ტერიტორიაზე ან:

- ამუშავებენ ევროკავშირის ტერიტორიაზე მყოფი პირების მონაცემებს მათთვის მომსახურების ან პროდუქციის შეთავაზების მიზნით, იმის მიუხედავად, ფასიანია თუ არა ეს მომსახურება ან პროდუქტი;

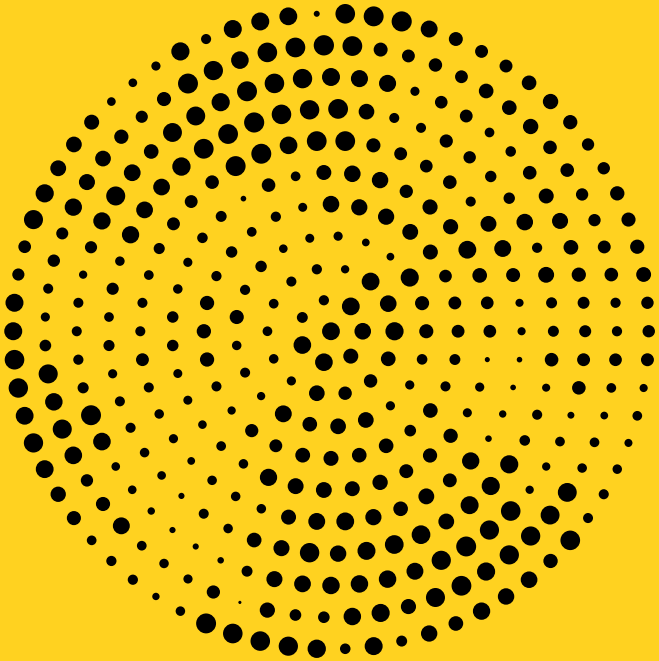
- მონიტორინგს უწევენ პირთა ქცევას ევროკავშირის ტერიტორიაზე.

რეგულაციის გავრცელების საკითხის შეფასებისას გასათვალისწინებელია შემდეგი ფაქტორები: აქვს თუ არა ორგანიზაციას ვებგვერდი ევროკავშირის რომელიმე ოფიციალურ ენაზე, პროდუქციის/მომსახურების ფასი დადგენილია თუ არა ევროკავშირში მოქმედ ვალუტაში, სთავაზობს თუ არა ორგანიზაცია მომხმარებლებს მიტანის სერვისს ევროკავშირის წევრი ქვეყნების ტერიტორიაზე და სხვა. ქცევის მონიტორინგად კი შეიძლება ჩაითვალოს ევროკავშირის ტერიტორიაზე მყოფ პირთა ქმედებებზე ონლაინ დაკვირვება მათი ინტერესებისა და დამოკიდებულებების შეფასების მიზნით; მაგალითად, თუ დეველოპერი მის მიერ შექმნილი აპლიკაციის მომხმარებელთა მონაცემებს მიზნობრივი მარკეტინგისთვის იყენებს, მასზე შესაძლოა გავრცელდეს რეგულაციის მოქმედება.

თუ ევროკავშირს გარეთ რეგისტრირებულ ორგანიზაციაზე ვრცელდება რეგულაცია, მან უნდა დანიშნოს წარმომადგენელი ევროკავშირში.

წარმომადგენლის დანიშვნის ვალდებულებისგან თავისუფლდებიან:

- საჯარო უწყებები;
- ის ორგანიზაციები, რომლებიც იშვიათად (ცალკეულ შემთხვევებში) ამუშავებენ ევროკავშირში მყოფი პირების პერსონალურ მონაცემებს, დიდი მოცულობით არ ამუშავებენ განსაკუთრებული კატეგორიის მონაცემებს და დამუშავება დიდი ალბათობით არ შეუქმნის საფრთხეს ინდივიდთა უფლებებს.



მონაცემთა დამუშავების პრინციპები

რეგულაციის მუხლი 5

მონაცემთა დაცვის ზოგადი რეგულაცია არსებითად არ ცვლის მონაცემთა დამუშავების 1995 წლის 95/46/EC დირექტივით[3] განსაზღვრულ პრინციპებს. ორგანიზაციებმა მონაცემები უნდა დაამუშავონ შემდეგი პრინციპების დაცვით:

- მონაცემები უნდა დამუშავდეს კანონიერად და სამართლიანად; დამუშავების შესახებ ინფორმაცია მარტივად ხელმისაწვდომი უნდა იყოს პირისთვის;

- მონაცემები უნდა შეგროვდეს მხოლოდ კონკრეტული, მკაფიოდ განსაზღვრული, კანონიერი მიზნებისათვის;

- მონაცემები უნდა დამუშავდეს მხოლოდ იმ მოცულობით, რომელიც აუცილებელია კონკრეტული კანონიერი მიზნის მისაღწევად;

- მონაცემები უნდა იყოს ზუსტი და, საჭიროების შემთხვევაში, განახლებული;

- იმ მიზნის მიღწევის შემდეგ, რომლისთვისაც მუშავდება მონაცემები, ისინი უნდა ინახებოდეს პირის იდენტიფიცირების გამომრიცხავი ფორმით;

- მონაცემების დამუშავებისას უზრუნველყოფილი უნდა იყოს მათი უსაფრთხოება და დაცვა უნებართვო ან უკანონო დამუშავებისგან, შემთხვევითი დაკარგვის, განადგურებისა და დაზიანებისგან.

სიახლეს წარმოადგენს ***ანგარიშვალდებულების პრინციპი***, რომელიც მკაფიოდ მიუთითებს, რომ ორგანიზაცია პასუხისმგებელია დამუშავების ყველა პრინციპის დაცვაზე და უნდა შეეძლოს ამის დადასტურება.

---

3 ევროპარლამენტისა და საბჭოს 1995 წლის 24 ოქტომბრის 95/46/EC დირექტივა პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვისა და ამ მონაცემთა თავისუფალი მიმოცვლის შესახებ (ხელმისაწვდომია: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046)

- რეგულაციის პრინციპების დასაცავად რეკომენდირებულია:
  - მონაცემთა დაცვის/ინფორმაციული უსაფრთხოების პოლიტიკის შემუშავება;
  - პერსონალური მონაცემების, დამუშავების საფუძვლებისა და მონაცემთა მიმართ შესრულებული მოქმედებების აღრიცხვა;
  - მონაცემთა დამუშავების პროცესში ჩართული თანამშრომლების ინფორმირება/გადამზადება;
  - მონაცემთა დამუშავებასთან დაკავშირებული დოკუმენტების (მაგალითად, პირის წერილობითი თანხმობა მონაცემთა დამუშავებაზე) განსაზღვრული ვადით შენახვა;
  - მონაცემთა დამუშავებასთან დაკავშირებული რისკების შეფასება;
  - მონაცემთა შენახვის ვადებისა და შესაბამისი პროცედურების განსაზღვრა;
  - ქცევის კოდექსის შემუშავება ან საქმიანობის სფეროში უკვე დამტკიცებულ ქცევის კოდექსთან მიერთება;
  - ნებაყოფლობითი სერტიფიცირება.

მონაცემთა დამუშავების საფუძვლები

რეგულაციის მუხლები 6 და 9

ახალი რეგულაციის მიხედვით, მონაცემთა დამუშავება კანონიერია, თუ ის ხორციელდება ერთ-ერთი შემდეგი საფუძვლით:

- პირმა გამოხატა თანხმობა მისი მონაცემების ერთი ან მეტი კონკრეტული მიზნით დამუშავებაზე;
- დამუშავება აუცილებელია პირთან დადებული ხელშეკრულების შესასრულებლად, ან მისივე თხოვნით ხელშეკრულების მოსამზადებლად;
- დამუშავება აუცილებელია ორგანიზაციისთვის კანონმდებლობით დაკისრებული მოვალეობის შესასრულებლად;
- დამუშავება აუცილებელია პირის სასიცოცხლო ინტერესების დასაცავად;
- დამუშავება აუცილებელია საჯარო ინტერესიდან გამომდინარე ფუნქციების ან ორგანიზაციისთვის კანონით მინიჭებული უფლებამოსილების განსახორციელებლად;
- დამუშავება აუცილებელია ორგანიზაციის ან მესამე პირის კანონიერი ინტერესების დასაცავად.

განსაკუთრებული კატეგორიის მონაცემთა[4] დამუშავების საფუძვლების ჩამონათვალი 10-პუნქტიანია და რეგულაციაში მას ცალკე მუხლი აქვს დათმობილი. თუმცა, ევროკავშირს გარეთ რეგისტრირებული ორგანიზაციებისთვის შესაძლოა რელევანტური იყოს რამდენიმე მათგანი:

- პირი ნათლად და მკაფიოდ გამოხატავს თანხმობას მონაცემთა დამუშავებაზე;
- დამუშავება აუცილებელია პირის სასიცოცხლო ინტერესების დასაცავად და მას არ შესწევს უნარი თანხმობა გამოხატოს მონაცემთა დამუშავებაზე;
- დამუშავება აუცილებელია სამართალწარმოების მიზნით;
- პირმა თავად გაასაჯაროვა მონაცემები, მათი გამოყენების აშკარა აკრძალვის გარეშე.

- განსაკუთრებული კატეგორიის მონაცემების დამუშავებისთვის პირის თანხმობის მოპოვებისას მიზანშეწონილია თანხმობა გამოხატულ იქნას წერილობით, ელექტრონული ფორმით ან სხვა ისეთი საშუალებით, რომლითაც ნათლად დადგინდება პირის ნება.

4 განსაკუთრებული კატეგორიის მონაცემებია, მაგალითად, რასობრივი ან ეთნიკური წარმომავლობა, პოლიტიკური შეხედულებები, რელიგიური მრწამსი, ჯანმრთელობასთან დაკავშირებული მონაცემები, გენეტიკური და ბიომეტრული მონაცემები.

თანხმობა

რეგულაციის მუხლები 4(11), 6(1)(a), 7, 8 და 9(2)(a)

თანხმობა მონაცემთა დამუშავების ერთ-ერთი ყველაზე გავრცელებული საფუძველია. რეგულაცია აწესებს კონკრეტულ მოთხოვნებს, რომლებიც ორგანიზაციამ პირისგან თანხმობის მოპოვებისას უნდა დაიცვას:

- თანხმობა უნდა იყოს ნებაყოფლობითი, ინფორმირებული და მკაფიოდ გამოხატული;
- თანხმობის გამოხატვამდე პირს გასაგებ ენაზე უნდა მიეწოდოს ამომწურავი ინფორმაცია მონაცემთა დამუშავების შესახებ;
- პირმა თანხმობა უნდა გამოხატოს აქტიური მოქმედებით; დუმილი, უმოქმედობა ან წინასწარ მონიშნული გრაფები არ ჩაითვლება თანხმობად;
- თანხმობა გაცემული უნდა იყოს კონკრეტული მიზნით/ მიზნებით მონაცემთა დამუშავებაზე;
- თუ მონაცემები ერთზე მეტი მიზნით დამუშავდება, საჭიროა, პირმა თანხმობა გამოხატოს მონაცემთა თითოეული მიზნით დამუშავებაზე;
- დოკუმენტებში თანხმობის პირობები გამოყოფილი უნდა იყოს სხვა ტექსტისგან და ჩამოყალიბებული უნდა იყოს მარტივი და გასაგები ენით;

- პირს უფლება აქვს, ნებისმიერ დროს გაითხოვოს თანხმობა. პროცედურა ისეთივე მარტივი უნდა იყოს, როგორც თანხმობის გამოხატვა. ამ უფლების შესახებ პირი წინასწარ უნდა იყოს ინფორმირებული;
- 16 წლამდე[5] არასრულწლოვანისათვის მომსახურების ელექტრონულად შეთავაზებისას, თანხმობას გასცემს მშობელი ან კანონიერი წარმომადგენელი[6];

5 შესაძლოა, ევროკავშირის წევრმა სახელმწიფომ თავისი კანონმდებლობით დაადგინოს უფრო დაბალი ზღვარი, თუმცა, ის არ შეიძლება იყოს 13 წელზე ნაკლები.

6 დამატებითი ინფორმაცია თანხმობასთან დაკავშირებით შეგიძლიათ იხილოთ ევროკავშირის პერსონალურ მონაცემთა დაცვის სამუშაო ჯგუფის (ე.წ. „29-ე მუხლის სამუშაო ჯგუფი“) სახელმძღვანელოში, რომელიც ხელმისაწვდომია: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

პირის უფლებები

რეგულაცია აძლიერებს ინდივიდის უფლებებს და განსაზღვრავს მონაცემთა სუბიექტის ახალ შესაძლებლობებს, მონაცემთა დამმუშავებელ ორგანიზაციებს კი აკისრებს შესაბამის ვალდებულებებს.

მონაცემებთან წვდომის უფლება

რეგულაციის მუხლი 15

- ორგანიზაციას აქვს ვალდებულება, პირს აცნობოს, ამუშავებს თუ არა მის შესახებ მონაცემებს.
- მოთხოვნის შემთხვევაში, პირს უნდა განემარტოს დამუშავების მიზნები, დამუშავებულ მონაცემთა კატეგორიები, მონაცემთა შენახვის ვადები და სხვა.
- ინფორმაციის მოთხოვნის პირველ შემთხვევაში პირს მონაცემთა ასლები უფასოდ უნდა მიეწოდოს. ინფორმაციის/დოკუმენტების განმეორებით მოთხოვნის შემთხვევაში, ორგანიზაციამ შესაძლოა დააწესოს გონივრული საფასური.

მონაცემთა წაშლის უფლება („დავიწყების უფლება“)

რეგულაციის მუხლი 17

ორგანიზაცია ვალდებულია წაშალოს მონაცემები, თუ, მაგალითად:

- მონაცემები აღარ არის საჭირო იმ მიზნის მისაღწევად, რისთვისაც მოხდა მათი შეგროვება ან დამუშავება;
- დამუშავება განხორციელდება არაკანონიერად;
- პირი გაითხოვს თანხმობას, რომლის საფუძველზეც მუშავდებოდა მონაცემები.

თუ ეს არ მოითხოვს არაპროპორციულად დიდ ძალისხმევას, ორგანიზაციამ უნდა აცნობოს მონაცემთა ყველა მიმღებს მონაცემთა წაშლის საჭიროების თაობაზე, ხოლო როდესაც ორგანიზაციას პირის მოთხოვნის საფუძველზე ევალება საჯაროდ (მაგალითად ინტერნეტში) გამოქვეყნებული მონაცემების წაშლა, მან ამის შესახებ, არსებული ტექნოლოგიებისა და ხარჯების გათვალისწინებით, უნდა აცნობოს სხვა ორგანიზაციებს, რომლებიც ამავე მონაცემებს ამუშავებენ.

მონაცემთა დაბლოკვა[7]

რეგულაციის მუხლი 18

- რეგულაცია ორგანიზაციებს მონაცემთა დაბლოკვას რამდენიმე შემთხვევაში ავალდებულებს. მაგალითად, თუ პირი ითხოვს მონაცემების შესწორებას, ორგანიზაციამ მონაცემები უნდა დაბლოკოს, ვიდრე არ გადაწყდება მონაცემთა სიზუსტის/ნამდვილობის საკითხი. ასევე, თუ პირი ითხოვს მონაცემთა დამუშავების შეწყვეტას, ორგანიზაციამ უნდა უზრუნველყოს მათი დაბლოკვა დამუშავების აღმატებული კანონიერი ინტერესის არსებობის დადგენამდე. ორგანიზაციამ მონაცემები უნდა დაბლოკოს იმ შემთხვევაშიც, როდესაც მონაცემთა დამუშავების არაკანონიერება დადგენილია, მაგრამ პირს არ სურს მათი წაშლა.

- თუ მონაცემების გადაცემა მოხდა მესამე პირებისათვის, ორგანიზაციამ უნდა შეატყობინოს მონაცემთა ყველა მიმღებს მონაცემთა დაბლოკვის თაობაზე, თუ ეს შესაძლებელია და არ მოითხოვს არაპროპორციულად დიდ ძალისხმევას.

მონაცემთა პორტირების უფლება

რეგულაციის მუხლი 20

- პირს აქვს უფლება, ორგანიზაციისგან მიიღოს მის შესახებ მონაცემები (რომელიც ორგანიზაციას თავად მიაწოდა) სტრუქტურირებულად, ელექტრონულად წაკითხვად ფორ-

7 მონაცემთა დაბლოკვა გულისხმობს მონაცემთა დამუშავების დრებით შეჩერებას.

მატში და გადასცეს იგი სხვა ორგანიზაციას მაშინ, როდესაც:

- *მონაცემთა დამუშავება ხდება პირის თანხმობით ან სახელშეკრულებო ვალდებულებიდან გამომდინარე; და*
- *მონაცემთა დამუშავება ხდება ავტომატური საშუალებებით.*

- თუ ეს ტექნიკურად შესაძლებელია, პირს შეუძლია მოსთხოვოს ორგანიზაციას მისი პერსონალური მონაცემების პირდაპირ სხვა ორგანიზაციისთვის გადაცემა[8].

დამუშავების შეწყვეტის მოთხოვნის უფლება

რეგულაციის მუხლი 21

- პირის მოთხოვნის შემთხვევაში, ორგანიზაციამ უნდა შეწყვიტოს მონაცემთა დამუშავება, თუ არ არსებობს დამუშავების აღმატებული კანონიერი ინტერესი. მაგალითად, მონაცემების დამუშავება დანაშაულის გამოძიების მიზნებისთვის განიხილება აღმატებულ კანონიერ ინტერესად და ამ შემთხვევაში მონაცემთა დამუშავება არ შეწყდება.

- მონაცემების პირდაპირი მარკეტინგის მიზნებისათვის დამუშავების დროს, პირის მოთხოვნის შემთხვევაში, დროულად უნდა მოხდეს მათი ამ მიზნით დამუშავების შეწყვეტა.

ორგანიზაციამ აღნიშნული ვალდებულებები უნდა შეასრულოს დაუყოვნებლივ, მაგრამ არაუგვიანეს 1 თვისა. გამონაკლისის სახით, ვადის გაგრძელება შესაძლებელია.

თუ ორგანიზაცია ვერ ახერხებს მოთხოვნის შესრულებას, პირს უნდა აცნობოს შესაბამისი მიზეზები.

8 დამატებითი ინფორმაცია პორტირების უფლებასთან დაკავშირებით შეგიძლიათ იხილოთ ევროკავშირის პერსონალურ მონაცემთა დაცვის სამუშაო ჯგუფის (ე.წ. „29-ე მუხლის სამუშაო ჯგუფი“) სახელმძღვანელოში, რომელიც ხელმისაწვდომია: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233

- **თუ პირი თხოვნას ელექტრონული ფორმით წარადგენს, პასუხიც ელექტრონული ფორმით უნდა გაიცეს, თუ თავად პირი არ მოითხოვს სხვაგვარად.**

გადაწყვეტილების ავტომატიზებული მიღება და „პროფილირება“

რეგულაციის მუხლი 22

პროფილირება არის პერსონალურ მონაცემთა ავტომატური საშუალებით დამუშავება იმ მიზნით, რომ გაანალიზდეს ან წინასწარ განისაზღვროს მისი ფინანსური მდგომარეობა, ინტერესები, ქცევა და სხვა. მაგალითად, პირის მონაცემების დამუშავება საკრედიტო სარეიტინგო ქულის ავტომატიზებულად გამოსათვლელად.

- თუ გადაწყვეტილება პირისთვის სამართლებრივი ან სხვა მნიშვნელოვანი შედეგის მომტანია, მას აქვს უფლება, მის შესახებ გადაწყვეტილება არ იქნას მიღებული მხოლოდ ავტომატიზებული საშუალებებით, ადამიანური რესურსის ჩარევის გარეშე.

პროფილირება დასაშვებია, თუ:

- აუცილებელია ხელშეკრულების დასადებად ან მის შესასრულებლად;
- ნებადართულია ევროკავშირის ან მისი წევრი ქვეყნის კანონმდებლობით;
- პირმა მკაფიოდ გამოხატა თანხმობა პროფილირებაზე[9].

9 დამატებითი ინფორმაცია პროფილირებასთან დაკავშირებით შეგიძლიათ იხილოთ ევროკავშირის პერსონალურ მონაცემთა დაცვის სამუშაო ჯგუფის (ე.წ. „29-ე მუხლის სამუშაო ჯგუფი“) სახელმძღვანელოში, რომელიც ხელმისაწვდომია: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

მონაცემთა დაცვის სტანდარტების გათვალისწინება ახალი პროდუქტის ან მომსახურების შექმნის პროცესში („PRIVACY BY DESIGN“) და მონაცემთა დაცვა პირველად პარამეტრად („PRIVACY BY DEFAULT“)

რეგულაციის მუხლი 25

მონაცემთა კატეგორიის, მოცულობის, დამუშავების მიზნების, საფუძვლების, ტექნიკური საშუალებებისა და რისკების გათვალისწინებით, ორგანიზაციებს ევალებათ მონაცემთა დაცვისთვის საჭირო ტექნიკური და ორგანიზაციული ზომების მიღება დამუშავების საშუალებების განსაზღვრის ეტაპზევე. ამ ზომების მიღება (მაგალითად, ფსევდონიმიზაცია[10]) უნდა მოხდეს უშუალოდ დამუშავების საშუალებების, მაგალითად, ელექტრონული პროგრამის შექმნისას.

ორგანიზაციებს საწყის ეტაპზევე ევალებათ კონკრეტულ კანონიერ მიზანთან მონაცემთა მოცულობისა და დამუშავების ვადის შესაბამისობის უზრუნველყოფა. მონაცემები თავისთავად („by default“) არ უნდა იყოს ხელმისაწვდომი პირთა განუსაზღვრელი წრისთვის. მაგალითად, სოციალური ქსელის ან აპლიკაციის ოპერატორმა უნდა უზრუნველყოს, რომ მომხმარებლის მიერ ფოტოს გამოქვეყნებისას პირველადი პარამეტრი იყოს პრივატული და მხოლოდ მაშინ გახდეს საჯარო, თუ პირი თავად შეცვლის შესაბამის პარამეტრს.

10 ფსევდონიმიზაცია გულისხმობს მონაცემთა დამუშავებას იმგვარად, რომ გამოირიცხება მონაცემების მიკუთვნება კონკრეტული პირისთვის, დამატებითი ინფორმაციის გამოყენების გარეშე. ეს დამატებითი ინფორმაცია კი ინახება განცალკევებით, უსაფრთხოდ.

მონაცემთა დამუშავების რისკების შეფასება

რეგულაციის მუხლები 35-36

მონაცემთა დამუშავებამ რიგ შემთხვევებში (მაგალითად, ახალი ტექნოლოგიების გამოყენების დროს) შესაძლოა საფრთხე შეუქმნას მონაცემების დაცულობას და შესაბამისად - პირთა უფლებებს. თუ მონაცემთა დამუშავება დიდი ალბათობით წარმოშობს პირთა უფლებების დარღვევის საფრთხეს, ორგანიზაციებს მოეთხოვებათ, დამუშავების დაწყებამდე შეაფასონ არსებული რისკები, მათი გავლენა პირის უფლებებზე და წინასწარვე განსაზღვრონ აღმოფხვრის/შემცირების გზები.

რეგულაციის მიხედვით, შეფასების პროცესი უნდა მოიცავდეს სულ მცირე შემდეგს:

- მონაცემთა დაგეგმილი დამუშავების პროცესის და მიზნების აღწერას;
- მონაცემთა დამუშავების საჭიროებისა და პროპორციულობის შეფასებას;
- პირთა უფლებებთან დაკავშირებული რისკების შეფასებას;
- იმ ღონისძიებათა ჩამონათვალს, რომლებიც ამცირებს რისკებს და უზრუნველყოფს რეგულაციასთან შესაბამისობას.

თუ შეფასების პროცესში გამოვლინდება რისკი, რომლის შემცირება ან აღმოფხვრა შეუძლებელია, საჭიროა ორგანიზაციამ კონსულტაციისთვის მიმართოს მონაცემთა დაცვის საკითხებზე ზედამხედველობის განმახორციელებელ ორგანოს და გაითვალისწინოს მისი მითითებები.

- ევროკავშირის წევრი ქვეყნების საზედამხედველო ორგანოებმა შესაძლოა დაადგინონ დამუშავების იმ სახეების სია, რომელიც წინასწარ საჭიროებს ან არ საჭიროებს გავლენის შეფასებას. მაგალითად, დიდი ბრიტანეთის მონაცემთა დაცვის საზედამხედველო ორგანოს მითითების თანახმად, თუ ორგანიზაცია გეგმავს დიდი მოცულობით განსაკუთრებული კატეგორიის მონაცემების დამუშავებას ან არასრულწლოვანთა მონაცემების პროფილირების მიზნით დამუშავებას, გავლენის შეფასება სავალდებულოა.[11]

- ევროკავშირის პერსონალურ მონაცემთა დაცვის საკითხებზე მომუშავე საერთაშორისო ჯგუფის, ე.წ. „29-ე მუხლის სამუშაო ჯგუფის“ რეკომენდაცია მიუთითებს, რომ დამუშავების რისკების შეფასება აუცილებელია მხოლოდ რეგულაციის ამოქმედების შემდეგ დაგეგმილ დამუშავებაზე. თუმცა, თუ დამუშავება უკვე მიმდინარეობს და იზრდება მონაცემთა დამუშავების რისკები, შეფასება ამ შემთხვევაშიც იქნება საჭირო[12].

11 იხ.: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

12 დამატებითი ინფორმაცია მონაცემთა დამუშავების რისკების შეფასებასთან დაკავშირებით შეგიძლიათ იხილოთ ევროკავშირის პერსონალურ მონაცემთა დაცვის სამუშაო ჯგუფის (ე.წ. „29-ე მუხლის სამუშაო ჯგუფი“) სახელმძღვანელოში, რომელიც ხელმისაწვდომია: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

მონაცემთა დაცვის ოფიცერი

რეგულაციის მუხლები 37-39

მონაცემთა დაცვის ოფიცერი არის პირი, რომელიც ორგანიზაციის შიგნით აკონტროლებს მონაცემთა დამუშავების პროცესის შესაბამისობას რეგულაციით დადგენილ მოთხოვნებთან. მონაცემთა დაცვის ოფიცრის დანიშვნა სავალდებულოა, თუ ორგანიზაცია:

- რეგულარულად და სისტემატურად ახდენს დიდი რაოდენობით პირთა მონიტორინგს;
- ამუშავებს დიდი მოცულობით განსაკუთრებული კატეგორიის ან ნასამართლობასთან დაკავშირებულ მონაცემებს;
- ამას ითვალისწინებს ევროკავშირის წევრი ქვეყნის კანონმდებლობა.

მონაცემთა დაცვის ოფიცრის ფუნქციებში უნდა შედიოდეს სულ მცირე:

- ორგანიზაციის და დამუშავების პროცესში ჩართული თანამშრომლების ინფორმირება მათი უფლება-მოვალეობების შესახებ;
- ორგანიზაციაში მონაცემთა დამუშავების პროცესის შიდა კონტროლი;
- საჭიროებისას მონაცემთა დამუშავების რისკების შეფასებაში მონაწილეობა და ამ პროცესის ზედამხედველობა;
- პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოსთან თანამშრომლობა;
- პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოსთან ურთიერთობისას და პერსონალურ მონაცემთა დაცვასთან წამოჭრილ საკითხებთან დაკავშირებით საკონტაქტო პირის ფუნქციის შესრულება.

- კომპანიათა ჯგუფს შეუძლია დანიშნოს ერთი მონაცემთა დაცვის ოფიცერი, რომელიც ჯგუფში შემავალი ყველა კომპანიისთვის შეასრულებს ოფიცრის ფუნქციებს.
- მონაცემთა დაცვის ოფიცრის საკონტაქტო მონაცემები უნდა იყოს საჯაროდ ხელმისაწვდომი.
- მონაცემთა დაცვის ოფიცერი ანგარიშვალდებული უნდა იყოს პირდაპირ უმაღლესი დონის მმართველ რგოლთან, თუმცა, თავის საქმიანობაში უნდა იყოს დამოუკიდებელი.

! თუ ორგანიზაცია ვერ ასრულებს რეგულაციის პირობებს, პასუხისმგებლობა ეკისრება ორგანიზაციას და არა მონაცემთა დაცვის ოფიცერს[13].

13 დამატებითი ინფორმაცია მონაცემთა დაცვის ოფიცერთან დაკავშირებით შეგიძლიათ იხილოთ ევროკავშირის პერსონალურ მონაცემთა დაცვის სამუშაო ჯგუფის (ე.წ. „29-ე მუხლის სამუშაო ჯგუფი“) სახელმძღვანელოში, რომელიც ხელმისაწვდომია: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048

მონაცემთა უსაფრთხოების დარღვევის შესახებ შეტყობინება

რეგულაციის მუხლები 33-34

მონაცემთა უსაფრთხოების დარღვევა არის ინციდენტი, რომელმაც გამოიწვია პერსონალურ მონაცემთა შემთხვევითი ან არაკანონიერი განადგურება, დაკარგვა, შეცვლა, გამჟღავნება ან მათზე უკანონო წვდომა.

თუ დაირღვა მონაცემთა უსაფრთხოება, ორგანიზაციამ:

- დარღვევის აღმოჩენიდან არაუგვიანეს 72 საათისა უნდა შეატყობინოს პერსონალურ მონაცემთა საზედამხედველო ორგანოს;
- დარღვევის შესახებ უნდა შეატყობინოს იმ პირებს, ვის მონაცემებსაც შეეხო ინციდენტი, თუ ეს დიდი ალბათობით გამოიწვევს ამ პირთა უფლების შელახვას.

საზედამხედველო ორგანოსათვის შეტყობინება უნდა მოიცავდეს სულ მცირე შემდეგს:

- მონაცემთა უსაფრთხოების დარღვევის ხასიათი - მათ შორის, თუ შესაძლებელია, იმ პირთა რაოდენობა, ვისი მონაცემებიც არაკანონიერად გამჟღავნდა, დაიკარგა, განადგურდა და ა.შ.; აგრეთვე იმ მონაცემთა რაოდენობა და კატეგორიები, რომლებსაც შეეხო ინციდენტი;
- მონაცემთა უსაფრთხოების დარღვევის სავარაუდო შედეგები;
- ორგანიზაციის მიერ მიღებული ან დაგეგმილი ღონისძიებები სავარაუდო ზიანის შესამცირებლად;
- ინციდენტის შესახებ მეტი ინფორმაციის მისაღებად საკონტაქტო პირის მონაცემები.

- ორგანიზაციამ უნდა აღრიცხოს მონაცემთა უსაფრთხოების დარღვევის ყველა შემთხვევა, შედეგები და გატარებული ზომები.

- ორგანიზაციამ უნდა შეიმუშავოს მონაცემთა უსაფრთხოების დარღვევის შეტყობინების პოლიტიკა, ინციდენტების გამოვლენისა და მათზე რეაგირების გეგმა.

- მიზანშეწონილია ისეთი ზომების მიღება, რომლებიც არაავტორიზებული წვდომის შემთხვევაში შეამცირებს მონაცემების მეშვეობით პირის იდენტიფიცირების რისკს (მაგალითად, დაშიფვრა)[14].

14 დამატებითი ინფორმაცია მონაცემთა უსაფრთხოების დარღვევის შესახებ შეტყობინებებთან დაკავშირებით შეგიძლიათ იხილოთ ევროკავშირის პერსონალურ მონაცემთა დაცვის სამუშაო ჯგუფის (29-ე მუხლის სამუშაო ჯგუფი) სახელმძღვანელოში, რომელიც ხელმისაწვდომია:
http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

მონაცემთა საერთაშორისო გადაცემა

რეგულაციის მუხლები 44-49

მონაცემთა გადაცემა ევროკავშირის წევრი ერთი ქვეყნიდან მეორეში, ასევე, იმ ქვეყნებსა და საერთაშორისო ორგანიზაციებში, რომელთა მიმართაც არსებობს ე.წ. „შესაბამისობის გადაწყვეტილება“,[15] არ საჭიროებს სპეციალურ ნებართვას.

მონაცემთა იმ ქვეყნებში გადაცემა, რომელთა მიმართაც არ არის მიღებული „შესაბამისობის გადაწყვეტილება“, დაშვებულია მხოლოდ მაშინ, თუ ორგანიზაცია უზრუნველყოფს მონაცემთა დაცვის სათანადო გარანტიებს. სათანადო გარანტიები შესაძლოა მოცემული იყოს მათ შორის, შემდეგ დოკუმენტებში:

- *საჯარო უწყებებს შორის დადებული ხელშეკრულებები (მაგალითად, საერთაშორისო ან ორმხრივი შეთანხმება);*
- *ტრანსნაციონალური კომპანიების შიდა კორპორაციული წესები;*
- *ევროკომისიის ან საზედამხედველო ორგანოს მიერ შემუშავებული მონაცემთა დაცვის სტანდარტული დებულებები.*

სათანადო გარანტიების არარსებობის შემთხვევაში, გადაცემა გამონაკლისის სახით დასაშვებია, მათ შორის, შემდეგ შემთხვევებში:

- მიუხედავად რისკების შესახებ გაფრთხილებისა, პირმა ნათლად გამოთქვა თანხმობა მონაცემთა გადაცემაზე;
- მონაცემთა გადაცემა აუცილებელია პირსა და ორგანიზაციას შორის დადებული ხელშეკრულების შესასრულებლად ან მისივე თხოვნით ხელშეკრულების მოსამზადებლად;

15 ევროკომისია აფასებს ქვეყნებსა და საერთაშორისო ორგანიზაციებში პირთა უფლებების დაცვის სტანდარტს (განსაკუთრებით, მონაცემთა დაცვის სფეროში) და თუ სათანადო გარანტიები უზრუნველყოფილია, მიიღება ე.წ. „შესაბამისობის გადაწყვეტილება“.

- მონაცემთა გადაცემა აუცილებელია პირის ინტერესებიდან გამომდინარე, ორგანიზაციასა და სხვა ფიზიკურ/იურიდიულ პირს შორის დადებული ხელშეკრულების შესასრულებლად;
- მონაცემთა გადაცემა აუცილებელია მნიშვნელოვანი საჯარო ინტერესებიდან გამომდინარე;
- მონაცემთა გადაცემა აუცილებელია სამართლებრივი მოთხოვნის დასადგენად, განსახორციელებლად ან დასაცავად;
- მონაცემთა სუბიექტის სასიცოცხლო ინტერესების დასაცავად, თუ მას არ შესწევს უნარი გამოხატოს თანხმობა მონაცემთა გადაცემაზე.

ჯარიმები

რეგულაციის წესების დარღვევები იყოფა ორ კატეგორიად:

დარღვევების პირველი კატეგორია:

- ორგანიზაციამ არ შეასრულა მონაცემთა უსაფრთხოების დარღვევისას შეტყობინების ვალდებულება;
- ევროკავშირის ტერიტორიის გარეთ დარეგისტრირებულმა ორგანიზაციამ არ დანიშნა წარმომადგენელი ევროკავშირში;
- დამუშავების საშუალებების შექმნის პროცესში არ მოხდა მონაცემთა დაცვის სტანდარტების გათვალისწინება;
- არ აღირიცხა მონაცემთა მიმართ განხორციელებული მოქმედებები.
- და სხვა

ამ კატეგორიის დარღვევებისთვის ჯარიმის მაქსიმალური ოდენობა არის 10,000,000 ევრო ან კომპანიის წლიური ბრუნვის 2%.

დარღვევების მეორე კატეგორია:

- ორგანიზაციამ დაარღვია პირის თანხმობასთან დაკავშირებული წესები;
- დაირღვა პირის უფლებები;
- დაირღვა მონაცემთა საერთაშორისო გადაცემასთან დაკავშირებული წესები;

- ორგანიზაციამ არ შეასრულა საზედამხედველო ორგანოს მითითება ან ხელი შეუშალა შემოწმების პროცესს;
- და სხვა

ამ კატეგორიის დარღვევებისათვის ჯარიმის მაქსიმალური ოდენობა არის 20,000,000 ევრო ან კომპანიის წლიური ბრუნვის 4%[16].

16 დამატებითი ინფორმაცია სანქციებთან დაკავშირებით შეგიძლიათ იხილოთ ევროკავშირის პერსონალურ მონაცემთა დაცვის სამუშაო ჯგუფის (ე.წ. „29-ე მუხლის სამუშაო ჯგუფი“) სახელმძღვანელოში, რომელიც ხელმისაწვდომია: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237