29-ე მუხლის მონაცემთა დაცვის სამუშაო ჯგუფი

16/EN
WP242 rev.01

სახელმძღვანელო რეკომენდაცია
მონაცემთა პორტირების უფლების შესახებ

მიღების თარიღი: 2016 წლის 13 დეკემბერი
ბოლო გადახედვის თარიღი: 2017 წლის 5 აპრილი

სამუშაო ჯგუფი შექმნილია 95/46/EC დირექტივის 29-ე მუხლის საფუძველზე. იგი დამოუკიდებელი ევროპული საკონსულტაციო ორგანოა, რომელიც მუშაობს მონაცემთა დაცვისა და პირადი ცხოვრების ხელშეუხებლობის საკითხებზე. მისი ფუნქციები აღწერილია 95/46/EC დირექტივის 30-ე მუხლში და 2002/58/EC დირექტივის მე-15 მუხლში.

სამდივნო უზრუნველყოფილია ევროკომისიის ფუნდამენტური უფლებებისა და მოქალაქეობის დირექტორატის მიერ, მართლმსაჯულების გენერალური დირექტორატი, B-1049 ბრიუსელი, ბელგია, ოფისი No MO-59 05/35.

ვებგვერდი: http://ec.europa.eu/justice/data-protection/index_en.htm

წინამდებარე სახელმძღვანელო რეკომენდაციის თარგმანი მომზადდა გერმანიის საერთაშორისო თანამშრომლობის საზოგადოების (GIZ) საჯარო მმართველობის აღმოსავლეთ პარტნიორობის რეგიონული ფონდის პროექტის ფარგლებში და წარმოადგენს არაოფიციალურ თარგმანს.

სარჩევი

რეზიუმე **3**

I. შესავალი **4**

II. რომელია მონაცემთა პორტირების ძირითადი ელემენტები? **5**

III. რა შემთხვევაში გამოიყენება მონაცემთა პორტირება? **12**

IV. მონაცემთა პორტირებაზე როგორ ვრცელდება ზოგადი წესები, რომლებიც არეგულირებს მონაცემთა სუბიექტის უფლებების განხორციელებას? **20**

V. როგორ უნდა იქნას მიწოდებული პორტირებული მონაცემები? **24**

რეზიუმე

GDPR-ის მე-20 მუხლი ადგენს მონაცემთა პორტირების (გადატანის) ახალ უფლებას, რომელიც მჭიდროდ არის დაკავშირებული მონაცემებზე წვდომის უფლებასთან, თუმცა, ამ უფლებისგან არაერთი მიზეზის გამო განსხვავდება. იგი მონაცემთა სუბიექტებს საშუალებას აძლევს, სტრუქტურირებული, ფართოდ გამოყენებადი და ელექტრონულად წაკითხვადი ფორმით დამუშავებისთვის პასუხისმგებელი პირისგან მიიღონ ის მონაცემები, რომლებიც დამუშავებისთვის პასუხისმგებელ პირსდამუშავებისთვის პასუხისმგებელ პირს თავად მიაწოდეს. აღნიშნული ახალი უფლების მიზანია, გააძლიეროს მონაცემთა სუბიექტი და მას მისცეს საშუალება, უფრო მეტად აკონტროლოს საკუთარი პერსონალური მონაცემები.

ვინაიდან მონაცემთა პორტირების უფლება იძლევა პერსონალური მონაცემების დამუშავებისთვის პასუხისმგებელი ერთი პირისგან მეორე დამუშავებისთვის პასუხისმგებელი პირისთვის პირდაპირ გადაცემის შესაძლებლობას, იგი მნიშვნელოვანი ინსტრუმენტია, რომელიც ხელს უწყობს ევროკავშირში პერსონალური მონაცემების თავისუფალ მიმოცვლას და კონკურენციას დამუშავებისთვის პასუხისმგებელ პირებს შორის. მონაცემთა პორტირების უფლება მონაცემთა სუბიექტს საშუალებას აძლევს, მომსახურების ერთი მიმწოდებლიდან მეორე მიმწოდებელთან გადაინაცვლოს და იგი ხელს შეუწყობს ახალი სერვისების განვითარებას ერთიანი ციფრული ბაზრის სტრატეგიის კონტექსტში.

წინამდებარე დოკუმენტი უზრუნველყოფს სახელმძღვანელო ინსტრუქციებს GDPR-ით გათვალისწინებული მონაცემთა პორტირების (გადატანის) განმარტების და განხორციელების გზების შესახებ. მისი მიზანია, განიხილოს მონაცემთა პორტირების უფლება და მისი მოქმედების ფარგლები. იგი განმარტავს პირობებს, რომლის საფუძველზეც გამოიყენება ეს ახალი მუხლი, მონაცემთა დამუშავების სამართლებრივი საფუძვლის გათვალისწინებით (მონაცემთა სუბიქტის თანხმობა ან ხელშეკრულების შესრულების საჭიროება) და იმ ფაქტს, რომ აღნიშნული უფლების მოქმედება შემოიფარგლება მხოლოდ იმ პერსონალური მონაცემებით, რომლებიც დამუშავებისთვის პასუხისმგებელ პირს დამუშავებისთვის პასუხისმგებელ პირსმონაცემთა სუბიექტმა თავად მიაწოდა. წინამდებარე მოსაზრება, აგრეთვე, შეიცავს კონკრეტულ მაგალითებსა და კრიტერიუმებს იმ გარემოებების განსამარტად, რომლებშიც გამოიყენება მოცემული უფლება. ამ მხრივ, 29-ე მუხლის სამუშაო ჯგუფი (WP29) მიიჩნევს, რომ მონაცემთა პორტირების (გადატანის) უფლება მოიცავს მონაცემთა სუბიექტის მიერ წინასწარი შეცნობით და აქტიურად მიწოდებულ მონაცემებს, ისევე, როგორც პერსონალურ მონაცემებს, რომლებიც წარმოებულია მონაცემთა სუბიექტის აქტივობით. დაუშვებელია აღნიშნული ახალი უფლების დაკნინება და შეზღუდვა, რათა იგი გავრცელდეს მხოლოდ იმ პერსონალურ მონაცემებზე, რომელიც მონაცემთა სუბიექტმა პირდაპირ გადასცა დამუშავებისთვის პასუხისმგებელ პირს, მაგალითად, ონლაინ ფორმით.

კარგი პრაქტიკის სახით, მონაცემთა დამუშავებისთვის პასუხისმგებელი პირები ვალდებულები არიან, დაიწყონ იმ საშუალებების შემუშავება, რომელიც ხელს შეუწყობს მონაცემთა პორტირების მოთხოვნებზე რეაგირებას, როგორიცაა, ჩამოტვირთვის ინსტრუმენტები და აპლიკაციის პროგრამირების ინტერფეისები. მათ უნდა უზრუნველყონ პერსონალური მონაცემების გადაცემა სტრუქტურირებული, ფართოდ გამოყენებადი და ელექტრონულად წაკითხვადი ფორმატით. საჭიროა დამმუშავებლების წახალისება, რათა მონაცემთა პორტირების შესახებ მოთხოვნის პასუხად, მათ უზრუნველყონ მონაცემები ოპერაციულად თავსებად ფორმატში.

წინამდებარე მოსაზრება მონაცემთა დამმუშავებლებს ეხმარება, ნათლად გაიაზრონ თავიანთი ვალდებულებები და შეიცავს რეკომენდაციებს საუკეთესო პრაქტიკასთან და ინსტრუმენტებთან დაკავშირებით, რომელიც ხელს უწყობს მონაცემთა პორტირების უფლებასთან შესაბამისობას. და ბოლოს, წინამდებარე მოსაზრებაში წარმოდგენილი რეკომენდაციის თანახმად, მიზანშეწონილია წარმოების სფეროში მომუშავე დაინტერესებულმა მხარეებმა და სავაჭრო ასოციაციებმა ერთობლივად იმუშაონ საერთო სტანდარტებზე და ფორმატებზე ოპერაციულ თავსებადობასთან დაკავშირებით, მონაცემთა პორტირების უფლებასთან დაკავშირებული მოთხოვნების შესრულებისთვის.

I. შესავალი

მონაცემთა დაცვის ზოგადი რეგულაციის (GDPR) მე-20 მუხლი ითვალისწინებს მონაცემთა პორტირების ახალ უფლებას, რომელიც მონაცემთა სუბიექტებს საშუალებას აძლევს, სტრუქტურირებული, ფართოდ გამოყენებადი და ელექტრონულად წაკითხვადი ფორმით დამუშავებისთვის პასუხისმგებელი პირსგან მიიღონ ის მონაცემები, რომლებიც თავად მიაწოდეს და მოახდინონ ამ მონაცემების მეორე დამუშავებისთვის პასუხისმგებელი პირისთვის გადაცემა, დაუბრკოლებლად. აღნიშნული უფლება, რომელიც ექვემდებარება გარკვეულ პირობებს, მხარს უჭერს მონაცემთა სუბიექტების არჩევანს, მომხმარებლის მიერ საკუთარი მონაცემების გაკონტროლებას და მომხმარებლის გაძლიერებას.

ფიზიკური პირები, რომლებიც ახორციელებენ მონაცემებზე წვდომის უფლებას, მონაცემთა დაცვის 95/46/EC დირექტივის თანახმად, იზღუდებოდნენ იმ ფორმატით, რომელსაც მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი აირჩევდა მოთხოვნილი ინფორმაციის მიწოდებისას. **მონაცემთა პორტირების ახალი უფლება მიზნად ისახავს, გააძლიეროს მონაცემთა სუბიექტის კონტროლი საკუთარ პერსონალურ მონაცემებზე, ვინაიდან იგი ხელს უწყობს მონაცემთა სუბიექტის უფლებას, საკუთარი პერსონალური მონაცემები ერთი საინფორმაციო ტექნოლოგიების სფეროდან მეორეში გადაიტანოს, გადაწეროს ან გადასცეს, მარტივად** (საკუთარ სისტემების, ნდობით აღჭურვილი მესამე მხარეების სისტემების ან ახალი დამმუშავებლების სისტემების ფარგლებში).

განამტკიცებს რა ფიზიკური პირის პერსონალურ უფლებებს და კონტროლს საკუთარ პერსონალურ მონაცემებზე, მონაცემთა პორტირება, აგრეთვე, წარმოადგენს მონაცემთა სუბიექტებსა და დამუშავებისთვის პასუხისმგებელ პირებს შორის ურთიერთობის „ხელახლა დაბალანსების“ შესაძლებლობას.[1]

პერსონალური მონაცემების პორტირების უფლება, შესაძლოა, აგრეთვე ზრდიდეს კონკურენციას მომსახურებებს შორის (ხელს უწყობს ერთი მომსახურებიდან მეორეზე გადასვლას). თუმცა, GDPR არეგულირებს არა კონკურენციას, არამედ, პერსონალურ მონაცემებს. კერძოდ, მე-20 მუხლის თანახმად, პორტირებადი მონაცემები არ გულისხმობს მხოლოდ იმ მონაცემებს, რომლებიც აუცილებელია ან სასარგებლოა ერთი მომსახურებიდან მეორეზე გადასასვლელად.[2]

მონაცემთა პორტირება ახალი უფლებაა, თუმცა, სხვა სახის პორტირება უკვე არსებობს ან განიხილება კანონმდებლობის სხვა სფეროებში (მაგ., ხელშეკრულების შეწყვეტის საკომუნიკაციო სერვისების როუმინგისა და მომსახურებებზე ტრანსსასაზღვრო წვდომის კონტექსტებში[3]). ზოგიერთი სინერგიები და ის სარგებელიც კი, რასაც ფიზიკური პირები იღებენ, შესაძლოა, მომდინარეობდეს სხვადასხვა ტიპის პორტირებიდან, თუ პორტირებები ხორციელდება კომბინირებული მიდგომის საფუძველზე; თუმცა, ანალოგიების მიმართ მიზანშეწონილია ფრთხილი მიდგომის გამოყენება.

წინამდებარე მოსაზრება შეიცავს სახელმძღვანელო ინსტრუქციებს მონაცემთა დამუშავებისთვის პასუხისმგებელი პირისთვის, რათა მათ შეძლონ საკუთარი პრაქტიკების, პროცესებისა და პოლიტიკის განახლება, და განმარტავს მონაცემთა პორტირების მნიშვნელობას, რათა მონაცემთა სუბიექტებმა შეძლონ საკუთარი უფლების ეფექტურად გამოყენება.

II. რომელია მონაცემთა პორტირების ძირითადი ელემენტები?

GDPR-ი მონაცემთა პორტირების უფლებას 20(1) მუხლში განსაზღვრავს შემდეგნაირად:

---

[1] მონაცემთა პორტირების ძირითადი მიზანია, გაზარდოს ფიზიკური პირის კონტროლი საკუთარ პერსონალურ მონაცემებზე და უზრუნველყოს ფიზიკური პირის მიერ აქტიური როლის შესრულება მონაცემთა ეკოსისტემაში.

[2] მაგალითად, აღნიშნული უფლება შესაძლოა ბანკებს აძლევდეს საშუალებას, უზრუნველყონ დამატებითი მომსახურებები, მომხმარებლის კონტროლის ქვეშ, იმ პერსონალური მონაცემების გამოყენებით, რომელიც თავდაპირველად ელექტროენერგიის მიწოდების სერვისის ფარგლებში შეგროვდა.

[3] იხ. ევროკომისიის დღის წესრიგი ერთიან ციფრულ ბაზართან დაკავშირებით: https://ec.europa.eu/digital-agenda/en/digital- single-market, კერძოდ, პოლიტიკის განმსაზღვრელი პირველი სვეტი „ციფრულ პროდუქტებსა და სერვისებზე ონლაინ წვდომის გაუმჯობესება“.

„მონაცემთა სუბიექტს უფლება აქვს, დამუშავებისთვის პასუხისმგებელი პირისგან *სტრუქტურირებული, ფართოდ გამოყენებადი და ელექტრონულად წაკითხვადი ფორმით მიიღოს ის მონაცემები, რომლებიც თავადვე მიაწოდა მას, ყოველგვარი დაბრკოლების გარეშე გადაიტანოს აღნიშნული მონაცემები სხვა დამმუშავებელთან [...]"*

- პერსონალური მონაცემების მიღების უფლება

პირველ რიგში, მონაცემთა პორტირება არის **მონაცემთა სუბიექტის უფლება, მიიღოს პერსონალური მონაცემების ამონარიდი (subset),** რომელსაც დამუშავებისთვის პასუხისმგებელი პირიმის შესახებ ამუშავებს და ეს მონაცემები შეინახოს პირადი მიზნებით შემდგომი გამოყენებისთვის. ამგვარი შენახვა შესაძლოა განხორციელდეს კერძო მფლობელობაში არსებულ მოწყობილობაზე ან ღრუბლოვან სისტემაზე (cloud) ე, რაც შესაძლოა არ გულისხმობდეს მონაცემების სხვა დამუშავებისთვის პასუხისმგებელი პირისთვის გადაცემას.

ამ მხრივ, მონაცემთა პორტირება განამტკიცებს მონაცემებზე წვდომის უფლებას. მონაცემთა პორტირების ერთ-ერთი თავისებურება მდგომარეობს იმაში, რომ იგი უზრუნველყოფს მარტივ საშუალებებს, რათა მონაცემთა სუბიექტებმა თავად მართონ და გამოიყენონ პერსონალური მონაცემები. ეს მონაცემები მათ უნდა მიიღონ *„სტრუქტურირებულ, ფართოდ გამოყენებად და ელექტრონულად წაკითხვად ფორმატში".* მაგალითად, მონაცემთა სუბიექტი, შესაძლოა, დაინტერესებული იყოს, მოიპოვოს საკუთარი „ფლეილისტი" (ან მოსმენილი მუსიკალური კომპოზიციების ისტორია) მუსიკალური პლატფორმიდან, რათა დაადგინოს, თუ რამდენჯერ მოუსმინა კონკრეტულ კომპოზიციას ან განსაზღვროს, თუ რომელი მუსიკის შესყიდვა სურს ან რომელ მუსიკას სურს, რომ მოუსმინოს სხვა პლატფორმაზე. მომხმარებელს, შესაძლოა, აგრეთვე, სურდეს საკუთარი კონტაქტების სიის მოპოვება ვებმეილის აპლიკაციიდან, მაგალითად, ქორწილის სტუმრების სიის შესადგენად ან ინფორმაციის მიღება სხვადასხვა ლოიალობის ბარათების გამოყენებით განხორციელებული შესყიდვების შესახებ ან საკუთარი ნახშირბადის ანაბეჭდის შესაფასებლად.[4]

[4] ასეთ შემთხვევებში, მონაცემთა სუბიექტის მიერ მონაცემების დამუშავება ხვდება საყოფაცხოვრებო საქმიანობის სფეროში, რა შემთხვევაშიც დამუშავება ხორციელდება მხოლოდ და მხოლოდ მონაცემთა სუბიექტის კონტროლის ქვეშ, ან დამუშავებას შესაძლებელია ახორციელებდეს სხვა მხარე, მონაცემთა სუბიექტის საახელით. ამ შემთხვევაში, აღნიშნული სხვა მხარე წარმოადგენს დამუშავებისთვის პასუხისმგებელ პირს, მაშინაც კი, თუ დამუშავების ერთადერთი მიზანია პერსონალური მონაცემების შენახვა, და იგი ვალდებულია, დაიცვას GDPR-ით დადგენილი პრინციპები და ვალდებულებები.

- პერსონალური მონაცემების დამუშავებისთვის პასუხისმგებელი ერთი პირისგან მეორე დამუშავებისთვის პასუხისმგებელ პირთან გადატანის უფლება

მეორე, 20(1) მუხლი მონაცემთა სუბიექტებს ანიჭებს **პერსონალური მონაცემების** დამუშავებისთვის პასუხისმგებელი **ერთი** პირისგან მეორე დამუშავებისთვის პასუხისმგებელ პირთან **გადატანის უფლებას,** „დაბრკოლების გარეშე." მონაცემების ერთი დამმუშავებლიდან პირდაპირ მეორისთვის გადაცემა შესაძლებელია მონაცემთა სუბიექტის მოთხოვნის საფუძველზე და იმ შემთხვევაში, თუ ეს ტექნიკურად შესაძლებელია (მუხლი 20(2)). ამ მხრივ, პრეამბულის 68-ე პუნქტი დამმუშავებლებს მოუწოდებს, შეიმუშაონ ოპერაციულად თავსებადი ფორმატები, რომლებიც მონაცემთა პორტირებას[5] შეუწყობს ხელს. ამავდროულად, აღნიშნული უნდა განხორციელდეს ისე, რომ დამმუშავებლებს არ დაეკისროთ ტექნიკურად თავსებადი დამუშავების სისტემების დანერგვის ან შენარჩუნების ვალდებულება.[6] თუმცა, GDPR-ი დამუშავებისთვის პასუხისმგებელ პირს უკრძალავს მონაცემთა გადაცემისთვის ბარიერების შექმნას.

არსებითად, მონაცემთა პორტირების აღნიშნული ელემენტი ითვალისწინებს მონაცემთა სუბიექტების შესაძლებლობას, არა მხოლოდ მოიპოვონ და გამოიყენონ საკუთარი პერსონალური მონაცემები, არამედ, აგრეთვე მოახდინონ მონაცემთა ერთი პროვაიდერიდან მეორე პროვაიდერისთვის გადაცემა (ბიზნესის იმავე ან სხვა სექტორში). მონაცემთა პორტირება მომხმარებლის პოზიციას განამტკიცებს და ახდენს მომხმარებლის ერთ მიმწოდებელთან „ჩაკეტვის" პრევენციას. ამავდროულად, არსებობს მოლოდინი, რომ მონაცემთა პორტირების უფლება ხელს შეუწყობს ინოვაციის შესაძლებლობებს და პერსონალური მონაცემების გაზიარებას მონაცემთა დამმუშავებლებს შორის, უსაფრთხო ფორმით, მონაცემთა სუბიექტის კონტროლის ქვეშ.[7] მონაცემთა პორტირება ხელს შეუწყობს მომხმარებელთა მიერ ორგანიზაციებს შორის საკუთარი პერსონალური მონაცემების კონტროლირებად და ლიმიტირებულ გაზიარებას და ამ გზით, გაამდიდრებს სერვისებს და მომხმარებლის გამოცდილებებს.[8] მონაცემთა პორტირება ხელს შეუწყობს მომხმარებლების შესახებ პერსონალური მონაცემების გადაცემას და ხელახლა გამოყენებას იმ სხვადასხვა სერვისების მიერ, რომელთა მიმართაც ინტერესი გააჩნიათ მომხმარებლებს.

---

[5] ასევე, იხ. სექცია V.

[6] შედეგად, განსაკუთრებული ყურადღება უნდა მიექცეს გადაცემული მონაცემების ფორმატს, რათა გარანტირებული იყოს მონაცემთა ხელახლა გამოყენების შესაძლებლობა, მინიმალური ძალისხმევით, მონაცემთა სუბიექტის ან მონაცემთა სხვა დამმუშავებლის მიერ. ასევე, იხ. სექცია V.

[7] იხ. ევროპაში ექსპერიმენტალური გამოყენების რამოდენიმე მაგალით, MiData გაერთიანებულ სამეფოში, MesInfos / SelfData by FING საფრანგეთში.

[8] ყოველდღიური ცხოვრების სხვადასხვა ასპექტების თვით-მონიტორინგთან (Quantified self) და საგნების ინტერნეტთან დაკავშირებული ინდუსტრიები წარმოაჩენს სხვადასხვა სარგებელს და რისკებს, რომლებიც მოაქვს ფიზიკური პირის ცხოვრების სხვადასხვა ასპექებთან დაკავშირებული პერსონალური მონაცემების (მაგ., ფიტნესი, აქტივობა, კალორიების მიღება) გამოყენებას ფიზიკური პირის ცხოვრების შესახებ ყოველმხრივი სურათის შექმნის კუთხით.

- დამუშავებისთვის პასუხისმგებელი პირის ვალდებულებები

მონაცემთა პორტირება უზრუნველყოფს პერსონალური მონაცემების მიღების და მათი დამუშავების უფლებას, მონაცემთა სუბიექტის სურვილის შესაბამისად.[9]

მონაცემთა დამუშავებისთვის პასუხისმგებელი პირები, რომლებიც რეაგირებენ მონაცემთა პორტირების შესახებ მოთხოვნებზე, მე-20 მუხლში დადგენილი პირობების შესაბამისად, არ არიან პასუხისმგებელი დამუშავებაზე, რომელსაც ახორციელებს მონაცემთა სუბიექტი ან სხვა კომპანია, რომელიც იღებს პერსონალურ მონაცემებს. ისინი მოქმედებენ მონაცემთა სუბიექტის სახელით, მათ შორის, სხვა დამუშავებისთვის პასუხისმგებელი პირისთვის პერსონალური მონაცემების პირდაპირ გადაცემის შემთხვევაში. ამ მხრივ, დამუშავებისთვის პასუხისმგებელი პირი არ არის ვალდებული, უზრუნველყოს მიმღები დამუშავებისთვის პასუხისმგებელი პირის შესაბამისობა მონაცემთა დაცვის კანონმდებლობასთან, იმის გათვალისწინებით, რომ მიმღებ დამუშავებისთვის პასუხისმგებელ პირს არ ირჩევს გამგზავნი დამუშავებისთვის პასუხისმგებელი პირი. ამავდროულად, დამმუშავებელმა უნდა დანერგოს დაცვის გარანტიები, რომლებიც რეალურად იმოქმედებს მონაცემთა სუბიექტის სასარგებლოდ. მაგალითად, დამუშავებისთვის პასუხისმგებელ პირს შეუძლია დანერგოს პროცედურები, რათა უზრუნველყოს, რომ გადაცემული პერსონალური მონაცემების სწორედ ის მონაცემებია, რომლის გადაცემაც სურს მონაცემთა სუბიექტს. აღნიშნულის განხორციელება შესაძლებელია მონაცემთა სუბიექტისგან დასტურის მოპოვების გზით, გადაცემამდე ან მანამდე, დამუშავებაზე თავდაპირველი თანხმობის მოპოვებისას ან ხელშეკრულებისთვის საბოლოო სახის მიცემისას.

დამმუშავებლები, რომლებიც პასუხობენ მონაცემთა პორტირების შესახებ მოთხოვნას, არ არიან ვალდებულები, უზრუნველყონ მონაცემთა ხარისხის შემოწმება გადაცემამდე. რა თქმა უნდა, აღნიშნული მონაცემები უკვე უნდა იყოს ზუსტი და განახლებული, GDPR-ის 5(1) მუხლში დადგენილი პრინციპების შესაბამისად. ამას გარდა, მონაცემთა პორტირება დამუშავებისთვის პასუხისმგებელ პირს არ აკისრებს ვალდებულებას, პერსონალური მონაცემები შეინახოს იმაზე მეტ ხანს, ვიდრე ეს აუცილებელია ან შენახვის კონკრეტული პერიოდის მიღმა.[10] აღსანიშნავია, რომ არ მოქმედებს დამატებითი მოთხოვნა მონაცემების ჩვეულებრივ მოქმედ ვადებზე მეტი

[9] მონაცემთა პორტირების უფლება არ შემოიფრაგლება მხოლოდ იმ პერსონალური მონაცემებით, რომლებიც აუცილებელი და რელევანტურია მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის კონკურენტების მიერ უზრუნველყოფილი მსგავსი მომსახურებისთვის.

[10] ზემოაღნიშნულ მაგალითში, თუ დამუშავებისთვის პასუხისმგებელი პირი არ ინახავს იმ სიმღერების ჩანაწერებს, რომელსაც მომხმარებელი უსმენდა, მაშინ შეუძლებელი იქნება აღნიშნული პერსონალური მონაცემების გათვალისწინება მონაცემთა პორტირების შესახებ მოთხოვნაში.

ხნით შენახვასთან დაკავშირებით, მხოლოდ იმიტომ, რომ დაკმაყოფილდეს მომავალში მონაცემთა პორტირების რაიმე პოტენციური მოთხოვნა.

როდესაც მოთხოვნილ პერსონალურ მონაცემებს ამუშავებს **დამუშავებაზე** უფლებამოსილი პირი, GDPR-ის 28-ე მუხლის თანახმად დადებული ხელშეკრულება უნდა ითვალისწინებდეს **დამუშავებაზე** უფლებამოსილი პირის „სათანადო ტექნიკური და ორგანიზაციული ზომებით“ დახმარების ვალდებულებას, რათა მან „უპასუხოს მონაცემთა სუბიექტის უფლებების განხორციელების შესახებ მოთხოვნებს.“ ამრიგად, დამმუშავებელმა უნდა დანერგოს კონკრეტული პროცედურები, უფლებამოსილ პირებთან თანამშრომლობის საფუძველზე, მონაცემთა პორტირების შესახებ მოთხოვნებზე რეაგირების კუთხით. ერთობლივი დამმუშავებლების შემთხვევაში, ხელშეკრულება მკაფიოდ უნდა განსაზღვრავდეს თითოეული დამუშავებისთვის პასუხისმგებელი პირის მოვალეობას მონაცემთა პორტირების შესახებ მოთხოვნების დამუშავების კუთხით.

ამას გარდა, მიმღები დამუშავებისთვის პასუხისმგებელი პირი[11] ვალდებულია, უზრუნველყოს, რომ პორტირებული მონაცემები არის რელევანტური და არ არის გადაჭარბებული მონაცემთა ახალი დამუშავების ჭრილში. მაგალითად, თუ მონაცემთა პორტირების შესახებ მოთხოვნა წარედგინა ვებმეილის სერვისს, ხოლო მოთხოვნის საფუძველზე მონაცემთა სუბიექტს სურს ელ.ფოსტის მიღება და დაარქივების დაცული პლატფორმისთვის გადაგზავნა, არ არის საჭირო, რომ მონაცემთა ახალმა დამმუშავებელმა დაამუშავოს მონაცემთა სუბიექტის კორესპონდენტთა საკონტაქტო მონაცემები. თუ ეს ინფორმაცია არ არის რელევანტური ახალი დამუშავების მიზნისთვის, არ უნდა მოხდეს მისი შენახვა და დამუშავება. ნებისმიერ შემთხვევაში, მიმღები დამუშავებისთვის პასუხისმგებელი პირი არ არის ვალდებული, მიიღოს და დაამუშავოს პერსონალური მონაცემები, რომელთა გადაცემაც მოხდა მონაცემთა პორტირების მოთხოვნის საფუძველზე. მსგავსად აღნიშნულისა, თუ მონაცემთა სუბიექტი ითხოვს მისი საბანკო ტრანზაქციების შესახებ დეტალების გადაცემას ისეთი მომსახურებისთვის, რომელიც ითვალისწინებს ბიუჯეტის მართვაში დახმარებას, მიმღები დამუშავებისთვის პასუხისმგებელი პირი არ არის ვალდებული, მიიღოს ყველა მონაცემი ან შეინახოს ტრანზაქციებთან დაკავშირებული ყველა დეტალი მას შემდეგ, რაც მოხდება მონაცემთა კატეგორიზება ახალი მომსახურების მიზნებისთვის. სხვა სიტყვებით რომ ვთქვათ, მიღებული და შენახული მონაცემები უნდა იყოს მხოლოდ ის მონაცემები, რომლებიც მიმღები დამუშავებისთვის პასუხისმგებელი პირის მიერ უზრუნველყოფილი მომსახურებისთვის აუცილებელი და რელევანტურია.

„მიმღები“ ორგანიზაცია ხდება მონაცემთა ახალი დამუშავებისთვის პასუხისმგებელი პირი ამ პერსონალურ მონაცემებთან მიმართებით და იგი ვალდებულია, დაიცვას

[11] ე.ი., რომელიც იღებს პერსონალურ მონაცემებს, მას შემდეგ, რაც მონაცემთა სუბიექტი სხვა დამუშავებისთვის პასუხისმგებელ პირს მიმართავს მონაცემთა პორტირების მოთხოვნით.

GDPR-ის მე-5 მუხლში დადგენილი პრინციპები. შესაბამისად, „ახალმა“ დამმუშავებელმა მკაფიოდ და პირდაპირ უნდა განაცხადოს ახალი დამუშავების მიზანი მანამ, სანამ მოხდება პორტირებადი მონაცემების გადაცემის შესახებ მოთხოვნის წარდგენა, მე-14 მუხლით დადგენილი გამჭვირვალობის მოთხოვნების შესაბამისად.[12] რაც შეეხება მონაცემთა დამუშავებას ამ პასუხისმგებლობის ფარგლებში, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, იხელმძღვანელოს მე-5 მუხლით დადგენილი პრინციპებით, როგორიცაა, კანონიერება, სამართლიანობა და გამჭვირვალობა, მიზნის შეზღუდვა, მონაცემთა მინიმიზაცია, სიზუსტე, უსაფრთხოება და კონფიდენციალობა, შენახვის შეზღუდვა და ანგარიშვალდებულება.[13]

მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი, რომელიც ინახავს პერსონალურ მონაცემებს, მზად უნდა იყოს, ხელი შეუწყოს მონაცემთა სუბიექტის მონაცემთა პორტირების უფლების განხორციელებას. დამუშავებისთვის პასუხისმგებელ პირს, აგრეთვე, შეუძლია თანხმობა განაცხადოს მონაცემთა სუბიექტისგან მონაცემების მიღებაზე, თუმცა, მას არ აქვს აღნიშნული ვალდებულება.

- მონაცემთა პორტირება vs. მონაცემთა სუბიექტის სხვა უფლებები

ფიზიკურმა პირმა მონაცემთა პორტირების უფლება უნდა განახორციელოს ისე, რომ ზიანი არ მიადგეს რომელიმე სხვა უფლებას (იგივე ვრცელდება GDPR-ით გათვალისწინებულ სხვა უფლებებზე). მონაცემთა სუბიექტს შეუძლია გააგრძელოს დამუშავებისთვის პასუხისმგებელი პირის მომსახურების გამოყენება და მისით სარგებლობა მას შემდეგაც კი, რაც განხორციელდება მონაცემთა პორტირებასთან დაკავშირებული ოპერაცია. მონაცემთა პორტირება ავტომატურად არ იწვევს მონაცემების წაშლას[14] მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის სისტემებიდან და იგი გავლენას არ ახდენს შენახვის თავდაპირველ ვადაზე, რომელსაც გადაცემული მონაცემები ექვემდებარება. მონაცემთა სუბიექტს თავისი უფლებების

---

[12] ამას გარდა, მონაცემთა ახალმა დამუშავებისთვის პასუხისმგებელმა პირმა არ უნდა დაამუშაოს პერსონალური მონაცემები, რომლებიც არ არის რელევანტური, ხოლო დამუშავება უნდა შემოიფარგლებოდეს მხოლოდ იმით, რაც აუცილებელია ახალი მიზნებისთვის, მაშინაც კი, თუ პერსონალური მონაცემები გლობალური მონაცემთა წყების ნაწილია, რომელთა გადაცემაც ხდება პორტირების პროცესის საშუალებით. პერსონალური მონაცემები, რომლებიც არ არის აუცილებელი ახალი დამუშავების მიზნის მისაღწევად, დაუყოვნებლივ უნდა წაიშალოს.

[13] მას შემდეგ, რაც დამუშავებისთვის პასუხისმგებელი პირი მიიღებს პერსონალურ მონაცემებს, რომელთა გაგზავნაც მოხდა მონაცემთა პორტირების უფლების ფარგლებში, ეს მონაცემები ჩაითვლება მონაცემთა სუბიექტის მიერ „მიწოდებულ“ მონაცემებად და შესაძლებელი იქნება მათი ხელახლა გადაცემა, მონაცემთა პორტირების უფლების შესაბამისად, იმ პირობით, თუ დაკმაყოფილებულია ამ უფლებასთან დაკავშირებული სხვა პირობები (ე.ი., დამუშავების სამართლებრივი საფუძველი, ...).

[14] GDPR-ის მე-17 მუხლის შესაბამისად.

განხორციელება შეუძლია მანამ, სანამ მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი ჯერ კიდევ ამუშავებს მონაცემებს.

მსგავსად აღნიშნულისა, თუ მონაცემთა სუბიექტს სურს განხორციელოს თავისი უფლება მონაცემთა წაშლაზე („დავიწყების უფლება“, მე-17 მუხლის თანახმად), დამუშავებისთვის პასუხისმგებელი პირი მონაცემთა პორტირებას ვერ გამოიყენებს როგორც მიზეზს მონაცემთა წაშლის გაჭიანურებისთვის ან წაშლაზე უარის თქმისთვის.

თუ მონაცემთა სუბიექტი აღმოაჩენს, რომ მონაცემთა პორტირების უფლების საფუძველზე მოთხოვნილი პერსონალური მონაცემები სრულად ვერ აკმაყოფილებს მის მოთხოვნას, პერსონალური მონაცემების შემდგომი მოთხოვნა, რომელიც განხორციელდა მონაცემებზე წვდომის უფლების ფარგლებში, სრულად უნდა დაკმაყოფილდეს, GDPR-ის მე-15 მუხლის შესაბამისად.

ამას გარდა, თუ კონკრეტულ ევროპულ სახელმწიფოში ან წევრ სახელმწიფოში სხვა სფეროში მოქმედი სამართალი ითვალისწინებს იგივე მონაცემთა პორტირების გარკვეულ ფორმას, ამ სპეციფიურ სამართალში დადგენილი პირობები აგრეთვე უნდა იქნას მხედველობაში მიღებული GDPR-ის საფუძველზე მონაცემთა პორტირების მოთხოვნის დაკმაყოფილებისას. პირველი, თუ მონაცემთა სუბიექტის მოთხოვნიდან ნათელია, რომ მის განზრახვას წარმოადგენს არა GDPR-ით გათვალისწინებული უფლებების, არამედ სექტორული კანონმდებლობით გათვალისწინებული უფლებების განხორციელება, მაშინ ამ მოთხოვნაზე ვერ გავრცელდება GDPR-ის დებულებები მონაცემთა პორტირების შესახებ.[15] მეორეს მხრივ, თუ მოთხოვნა მონაცემთა პორტირებას ისახავს მიზნად, GDPR-ის შესაბამისად, ამგვარი სპეციფიური კანონმდებლობის არსებობა არ გამორიცხავს მონაცემთა პორტირების პრინციპის ზოგად გამოყენებას ნებისმიერი დამუშავებისთვის პასუხისმგებელი პირის მიმართ, GDPR-ის შესაბამისად. არამედ, თითოეულ ინდივიდუალურ შემთხვევაში უნდა შეფასდეს, თუ რა გავლენა აქვს (ან აქვს თუ არა საერთოდ გავლენა) ამგვარ სპეციფიურ კანონმდებლობას მონაცემთა პორტირების უფლებაზე.

[15] მაგალითად, თუ მონაცემთა სუბიექტის მოთხოვნა ითვალისწინებს საინფორმაციო სერვისის პროვაიდერის მიერ მისი საბანკო ანგარიშის ისტორიაზე წვდომის უზრუნველყოფას, „გადახდის სერვისების შესახებ მე-2 დირექტივით“ (PSD2) გათვალისწინებული მიზნებისთვის, წვდომა აღნიშნული დირექტივის დებულებების საფუძველზე უნდა იქნას უზრუნველყოფილი.

III. რა შემთხვევაში გამოიყენება მონაცემთა პორტირება?

- დამუშავებასთან დაკავშირებულ ოპერაციებს რა შემთხვევაში მოიცავს მონაცემთა პორტირების უფლება?

GDPR-თან შესაბამისობისთვის, დამმუშავებლებს უნდა გააჩნდეთ პერსონალური მონაცემების დამუშავების მკაფიო სამართლებრივი საფუძველი.

GDPR-ის 20(1)(a) მუხლის შესაბამისად, **იმისათვის, რომ დამუშავება ხვდებოდეს მონაცემთა პორტირების უფლების მოქმედების ქვეშ,** იგი უნდა ეფუძნებოდეს:

- მონაცემთა სუბიექტის თანხმობას (6(1)(a) მუხლის შესაბამისად, ან 9(2)(a) მუხლის თანახმად, განსაკუთრებული კატეგორიების პერსონალური მონაცემების დამუშავების შემთხვევაში);
- ან, ხელშეკრულებას, რომლის ერთ-ერთი მხარეც არის მონაცემთა სუბიექტი, 6(1)(b) მუხლის შესაბამისად.

მაგალითად, ფიზიკური პირის მიერ წიგნების ონლაინ მაღაზიაში ნაყიდი წიგნის სათაურები ან ის სიმღერები, რომელთაც ფიზიკური პირი უსმენს მუსიკალურ პლატფორმაზე წარმოადგენს პერსონალური მონაცემების მაგალითებს, რომლებიც, როგორც წესი, მონაცემთა პორტირების უფლების მოქმედების ქვეშ ხვდებიან, ვინაიდან მათი დამუშავება ხდება იმ ხელშეკრულების შესრულების ფარგლებში, რომლის ერთ-ერთი მხარეც არის მონაცემთა სუბიექტი.

GDPR-ი არ ადგენს მონაცემთა პორტირების ზოგად უფლებას ისეთ შემთხვევებში, როდესაც პერსონალური მონაცემების დამუშავება არ ეფუძნება თანხმობას ან ხელშეკრულებას.[16] მაგალითად, ფინანსური დაწესებულებები არ არიან ვალდებულები, უპასუხონ მონაცემთა პორტირების მოთხოვნებს იმ პერსონალურ მონაცემებთან დაკავშირებით, რომელსაც ამუშავებენ ფულის გათეთრების ან სხვა ფინანსური დანაშაულების პრევენციისა და გამოვლენის ვალდებულების ფარგლებში.

[16] იხ. GDPR-ის პრეამბულის 68-ე პუნქტი და 20(3) მუხლი. აღნიშნული დებულებების თანახმად, მონაცემთა პორტირება არ ვრცელდება, როდესაც მონაცემთა დამუშავება აუცილებელია საჯარო ინტერესის სფეროში შემავალი ფუნქციების/ამოცანების შესასრულებლად ან დამმუშავებლისათვის კანონით მინიჭებული უფლებამოსილების განსახორციელებლად, ან როდესაც მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი ახორციელებს მის საჯარო მოვალეობებს ან ასრულებს მის სამართლებრივ ვალდებულებას. შესაბამისად, მონაცემთა დამმუშავებლები არ არიან ვალდებულები უზრუნველყონ მონაცემთა პორტირება ასეთ შემთხვევებში. ამავდროულად, კარგი პრაქტიკის თანახმად, მიზანშეწონილია იმგვარი პროცესების შემუშავება, რომელიც უზრუნველყოფს მონაცემთა პორტირების შესახებ მოთხოვნებზე ავტომატური პასუხის გაცემას, მონაცემთა პორტირების უფლების მარეგულირებელი პრინციპების შესაბამისად. მაგალითად: სახელმწიფო სამსახური უზრუნველყოფს წარდგენილი საგადასახადო დეკლარაციების ადვილად ჩამოტვირთვის შესაძლებლობას. ლეგიტიმური ინტერესების შესახებ WP29-ის დასკვნაში 6/2014 (WP2017, გვ.გვ. 47-48) შეგიძლიათ იხილოთ ინფორმაცია კარგი პრაქტიკის შესახებ, როცა მონაცემთა დამუშავება ეფუძნება ლეგიტიმურ ინტერესს და არსებულ მოხალისეობრივ სქემებთან დაკავშირებით.

აღნიშნულის მსგავსად, მონაცემთა პორტირება არ მოიცავს პროფესიული ხელშეკრულების დეტალებს, რომელთა დამუშავებაც ხდება ბიზნესებს შორის ურთიერთობის ფარგლებში, ისეთ შემთხვევებში, როდესაც დამუშავება არ ეფუძნება მონაცემთა სუბიექტის თანხმობას ან ხელშეკრულებას, რომლის ერთ-ერთი მხარეც არის მონაცემთა სუბიექტი.

როდესაც საქმე ეხება დასაქმებულთა მონაცემებს, მონაცემთა პორტირების უფლება, როგორც წესი, ვრცელდება მხოლოდ იმ შემთხვევაში, თუ დამუშავება ეფუძნება ხელშეკრულებას, რომლის ერთ-ერთი მხარეც არის მონაცემთა სუბიექტი. ხშირად, თანხმობა ამ კონტექსტში არ მიიჩნევა ნებაყოფლობითად იმ ძალაუფლების დისბალანსის გათვალისწინებით, რომელიც არსებობს დასაქმებულსა და დამსაქმებელს შორის.[17] ნაცვლად ამისა, ადამიანურ რესურსების მართვის ჭრილში მონაცემების დამუშავება ზოგ შემთხვევაში, ეფუძნება ლეგიტიმური ინტერესის სამართლებრივ საფუძველს, ან წარმოადგენს აუცილებლობას დასაქმების სფეროში კონკრეტულ სამართლებრივ მოვალეობებთან შესრულებისთვის. პრაქტიკაში, ადამიანური რესურსების მართვის კონტექსტში ეჭვგარეშეა, რომ მონაცემთა პორტირების უფლება ვრცელდება დამუშავების გარკვეულ ოპერაციებზე (მაგ., ხელფასის და კომპენსაციის გადახდა, შიდა რეკრუტირება), თუმცა, არაერთ სიტუაციაში, საჭიროა ინდივიდუალური მიდგომა, რათა გადამოწმდეს მონაცემთა პორტირების უფლებასთან დაკავშირებულ პირობებთან შესაბამისობა.

და ბოლოს, მონაცემთა პორტირების უფლება მოქმედებს მხოლოდ იმ შემთხვევაში, როდესაც მონაცემთა დამუშავება „ავტომატური საშუალებით ხორციელდება“. შესაბამისად, ეს უფლება ძირითადად არ მოქმედებს ფიზიკური (ქაღალდის) ფაილების შემთხვევაში.

- რა სახის პერსონალურ მონაცემებზე ვრცელდება პორტირების უფლება?

20(1) მუხლის თანახმად, მონაცემთა პორტირების უფლებას ექვემდებარება:

- პერსონალური მონაცემები მონაცემთა სუბიექტის შესახებ,

- რომელიც მონაცემთა სუბიექტმა დამუშავებისთვის პასუხისმგებელ პირს თავად *მიაწოდა*.

20(4) მუხლის თანახმად, აღნიშნულ უფლებასთან შესაბამისობამ არ უნდა იქონიოს რაიმე უარყოფითი გავლენა სხვების უფლებებზე და თავისუფლებებზე.

<u>პირველი პირობა: მონაცემთა სუბიექტის პერსონალური მონაცემები</u>

[17] WP29-ის დასკვნა 8/2001, 2001 წლის 13 სექტემბერი (WP48).

პორტირებას ექვემდებარება მხოლოდ პერსონალური მონაცემები. შესაბამისად, ნებისმიერი მონაცემები, რომლებიც ანონიმიზებულია[18] ან არ ეხება მონაცემთა სუბიექტს, არ ექვემდებარება პორტირებას. ამავდროულად, შესაძლებელია იმ ფსევდონიმიზებული მონაცემების პორტირების მოთხოვნა, რომელთა მკაფიოდ დაკავშირებაც შესაძლებელია მონაცემთა სუბიექტთან (მაგ., თუ სუბიექტი წარმოადგენს დამატებით ინფორმაციას, რომელიც მისი იდენტიფიცირების საშუალებას იძლევა, cf. მუხლი 11(2)).

ხშირად დამუშავებისთვის პასუხისმგებელი პირები ამუშავებენ ინფორმაციას, რომელიც შეიცავს რამდენიმე მონაცემთა სუბიექტის პერსონალურ მონაცემებს. ასეთ შემთხვევაში, დამუშავებისთვის პასუხისმგებელმა პირმა არ უნდა იხელმძღვანელონ წინადადების „პერსონალური მონაცემები მონაცემთა სუბიექტის შესახებ“ ზედმეტად შემზღუდველი ინტერპრეტაციით. მაგალითად, სატელეფონო ზარების, ინტერპერსონალური შეტყობინებების ან VoIP ჩანაწერები შესაძლოა მოიცავდეს (გამომწერის პროფილის ისტორიაში) დეტალურ მონაცემებს მესამე მხარეების შესახებ, შემომავალი ან გამავალი ზარების კონტექსტში. შესაბამიმსად, ჩანაწერები შეიცავს ერთზე მეტი ადამიანის პერსონალურ მონაცემებს. თუმცა, გამომწერებს უნდა შეეძლოთ ამ ჩანაწერების მიღება მონაცემთა პორტირების შესახებ მოთხოვნის საფუძველზე, რადგან ჩანაწერები (აგრეთვ) ეხება მონაცემთა სუბიექტს. ამავდროულად, თუ ასეთი ჩანაწერები ახალ დამუშავებისთვის პასუხისმგებელ პირს გადაეცემა, ამ უკანასკნელმა არ უნდა დაამუშავოს ისინი იმ მიზნით, რომელიც უარყოფით გავლენას იქონიებს მესამე მხარეების უფლებებზე და თავისუფლებებზე (იხ. ქვემოთ: მესამე პირობა).

<u>მეორე პირობა: მონაცემთა სუბიექტის მიერ მიწოდებული მონაცემები</u>

მეორე პირობის თანახმად, პორტირების უფლება ვრცელდება მონაცემთა სუბიექტის „მიერ მიწოდებულ“ მონაცემებზე.

არაერთი მაგალითი არსებობს პერსონალური მონაცემების, რომლებიც მონაცემთა სუბიექტმა წინასწარი შეცნობით და აქტიურად მიაწოდა დამუშავებისთვის პასუხისმგებელ პირს, მაგალითად, მომხმარებლის დასარეგისტრირებლად საჭირო მონაცემები (საფოსტო მისამართი, მომხმარებელის სახელი, ასაკი), რომელთა მიწოდებაც ხდება ონლაინ ფორმების საშუალებით. ამავდროულად, „მონაცემთა სუბიექტის მიერ მიწოდებული“ მონაცემები, აგრეთვე, მოიცავს მონაცემთა სუბიექტის აქტივობის დაკვირვების შედეგად მოპოვებულ მონაცემებს. შესაბამისად, WP29 თვლის, რომ ამ ახალი უფლების სრულფასოვნების უზრუნველყოფა საჭიროებს, რომ „მონაცემთა სუბიექტის მიერ მიწოდებული“ მონაცემები, აგრეთვე, მოიცავდეს პერსონალურ მონაცემებს, რომლებიც მოპოვებულია მომხმარებელთა აქტივობების დაკვირვების შედეგად, როგორიცაა, პირველადი მონაცემები (raw data), რომელსაც

[18]http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

ამუშავებს „სმარტმეტრი“ და სხვა მსგავსი ტიპის ნივთები,[19] „აქტივობის ჟურნალი“, ვებსაიტის გამოყენების ისტორია ან საძიებო აქტივობები.

მონაცემთა ეს უკანასკნელი კატეგორია არ მოიცავს მონაცემებს, რომელთაც ქმნის მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი (დაკვირვების შედეგად მოპოვებული ან პირდაპირ მიწოდებული ინფორმაციის საფუძელზე), როგორიცაა, მომხმარებლის პროფილი, რომელიც შექმნილია „სმარტმეტრით“ შეგროვებული პირველადი მონაცემებით.

წარმომავლობის მიხედვით ერთმანეთისაგან განარჩევენ სხვადასხვა კატეგორიის მონაცემებს, რომლის საფუძველზეც განისაზღვრება, თუ რამდენად ექვემდებარებიან ისინი მონაცემთა პორტირების უფლებას. ქვემოთ წარმოდგენილი კატეგორიები „მონაცემთა სუბიექტის მიერ მიწოდებული“ მონაცემების კატეგორიებს განეკუთვნება:

- **მონაცემები, რომლებიც დამუშავებისთვის პასუხისმგებელ პირს აქტიურად და წინასწარ შეცნობით მიაწოდა მონაცემთა სუბიექტმა** (მაგ., საფოსტო მისამართი, მომხმარებლის სახელი, ასაკი და ა.შ.)
- **დაკვირვების შედეგად მიღებული მონაცემები, რომლებიც დამუშავებისთვის პასუხისმგებელ პირს მონაცემთა სუბიექტმა მიაწოდა მომსახურების ან მოწყობილობის გამოყენების შედეგად.** მაგალითად, საძიებო ისტორია, ტრეფიკის მონაცემები და ადგილმდებარეობის აღმნიშვნელი მონაცემები. აღნიშნული, შესაძლოა, აგრეთვე, მოიცავდეს პირველად მონაცემებს, როგორიცაა გულის ცემის აღმნიშვნელი მონაცემები, რომელსაც მონიტორინგს უწევს ტარებადი მოწყობილობა.

მეორეს მხრივ, ნავარაუდევი მონაცემები და წარმოებული მონაცემები „მონაცემთა სუბიექტის მიერ მიწოდებული მონაცემების“ საფუძველზე დამუშავებისთვის პასუხისმგებელი პირის მიერ შექმნილი მონაცემებია. მაგალითად, მომხმარებლის ჯანმრთელობის შესახებ შეფასების შედეგი ან რისკის მართვის და ფინანსური რეგულაციის კონტექსტში შექმნილი პროფილი (მაგ., საკრედიტო ქულის მისანიჭებლად ან ფულის გათეთრებასთან ბრძოლის წესებთან შესაბამისობისთვის) ვერ იქნება მიჩნეული, როგორც მონაცემთა სუბიექტის „მიერ მიწოდებული“ მონაცემები. მართალია, ამგვარი მონაცემები დამუშავებისთვის პასუხისმგებელი პირის მიერ წარმოებული პროფილის შემადგენელი ნაწილია და ივარაუდება ან იწარმოება მონაცემთა სუბიექტის მიერ მიწოდებული (მაგ., საკუთარი ქმედებების საშუალებით) მონაცემების ანალიზის საფუძველზე, როგორც წესი, აღნიშნული მონაცემები ვერ იქნება მიჩნეული „მონაცემთა სუბიექტის მიერ მიწოდებულ“

[19] თავისი აქტივობის დაკვირვების შედეგად შექმნილი მონაცემების მოპოვების შესაძლებლობა მონაცემთა სუბიექტს საშუალებას მისცემს, უკეთ აღიქვას დაკვირვების შედეგად მიღებული მონაცემების მასშტაბი და უკეთეს მდგომარეობაში იქნება იმისათვის, რომ აირჩიოს, თუ რა სახის მონაცემების მიწოდებისთვის არის მზად მსგავსი მომსახურების მისაღებად. მონაცემთა სუბიექტს ეცოდინება, თუ რამდენადაა დაცული მისი პირადი ცხოვრების ხელშეუხებლობის უფლება.

მონაცემებად და ამრიგად, ისინი არ შედის აღნიშნული ახალი უფლების მოქმედების სფეროში.[20]

ზოგადად, მონაცემთა პორტირების უფლების ამოცანებიდან გამომდინარე, ტერმინი „მონაცემთა სუბიექტის მიერ მიწოდებული“ ფართოდ უნდა განიმარტოს და უნდა გამორიცხავდეს „ნავარაუდევ მონაცემებს“ და „წარმოებულ მონაცემებს“, რომელიც მოიცავს მომსახურების მიმწოდებლის მიერ შექმნილ პერსონალურ მონაცემებს (მაგ., ალგორითმული შედეგები). დამუშავებისთვის პასუხისმგებელი პირი უფლებამოსილია, ნავარაუდევი მონაცემები გამორიცხოს, თუმცა, მან უნდა შეიტანოს ყველა სხვა დარჩენილი პერსონალური მონაცემი, რომელსაც მონაცემთა სუბიექტი დამუშავებისთვის პასუხისმგებელ პირს აწვდის დამუშავებისთვის პასუხისმგებელი პირის მიერ უზრუნველყოფილი ტექნიკური საშუალებების გამოყენების შედეგად.[21]

ამრიგად, ტერმინი „მონაცემთა სუბიექტის მიერ მიწოდებული“ მოიცავს პერსონალურ მონაცემებს, რომლებიც დაკავშირებულია მონაცემთა სუბიექტის აქტივობასთან ან შექმნილია ფიზიკური პირის ქცევის დაკვირვების შედეგად, თუმცა, არ მოიცავს ამ ქცევის შემდგომი ანალიზის შედეგად შექმნილ მონაცემებს. მეორეს მხრივ, პერსონალური მონაცემები, რომლებიც დამმუშავებელმა შექმნა მონაცემთა დამუშავების ფარგლებში, მაგ/. პერსონალიზაციის ან რეკომენდაციის პროცესის შედეგად, მომხმარებელთა კატეგორიზაციის ან პროფილირების გზით, წარმოადგენს მონაცემთა სუბიექტის მიერ მიწოდებული პერსონალური მონაცემების საფუძველზე წარმოებულ ან ნავარაუდევ მონაცემებს და მათზე არ ვრცელდება მონაცემთა პორტირების უფლება.

<u>მესამე პირობა: მონაცემთა პორტირების უფლებამ არ უნდა იქონიოს უარყოფითი გავლენა სხვების უფლებებზე და თავისუფლებებზე</u>

სხვა მონაცემთა სუბიექტების შესახებ პერსონალურ მონაცემებთან დაკავშირებით:

---

[20] ამავდროულად, მონაცემთა სუბიექტები კვლავ შეძლებენ, გამოიყენონ მათი უფლება *„მიიღონ მათი პერსონალური მონაცემების დამუშავების დადასტურება და დამუშავებული მონაცემები“* და მიიღონ ინფორმაცია: *„გადაწყვეტილების ავტომატიზებულად მიღების, მათ შორის, 22-ე მუხლის პირველი და მე-4 პუნქტებით გათვალისწინებული „პროფილირების“, და ამგვარ შემთხვევებში სულ მცირე მნიშვნელოვანი/არსებითი ინფორმაცია გამოყენებული ლოგიკის/კრიტერიუმების, საჭიროების და მონაცემთა სუბიექტისთვის შესაძლო შედეგების შესახებ“,* GDPR-ის მე-15 მუხლის შესაბამისად (რომელიც მიუთითებს წვდომის უფლებაზე).

[21] აღნიშნული მოიცავს ყველა მონაცემებს, რომელიც შექმნილია მონაცემთა სუბიექტის დაკვირვების შედეგად, იმ აქტივობების განხორციელების პროცესში, რომელთა მიზნითაც ხდება მონაცემების შეგროვება, როგორიცაა, ტრანზაქციების ისტორია და „შესვლის ჩანაწერები“. მონაცემები, რომელთა შეგროვებაც ხდება მონაცემთა სუბიექტის მონიტორინგის და ჩაწერის შედეგად (როგორიცაა, აპლიკაციები, რომლებიც იწერს გულის ცემას ან ტექნოლოგია, რომელიც გამოიყენება ბრაუზინგის მონიტორინგისთვის), აგრეთვე, მიჩნეული უნდა იქნას, როგორც მონაცემთა სუბიექტის მიერ მიწოდებული მონაცემები, მაშინაც კი, თუ მონაცემების გადაცემა არ ხდება აქტიურად ან ცნობიერად.

მესამე პირობის მიზანია, თავიდან აიცილოს სხვა მონაცემთა სუბიექტების (რომელთაც თანხმობა არ გაუციათ) პერსონალური მონაცემების შემცველი მონაცემების მოპოვება და ახალი დამუშავებისთვის პასუხისმგებელი პირისთვის გადაცემა ისეთ შემთხვევებში, როდესაც აღნიშნული მონაცემები სავარაუდოდ, დამუშავდება იმგვარად, რაც უარყოფით გავლენას მოახდენს სხვა მონაცემთა სუბიექტების უფლებებზე და თავისუფლებებზე (GDPR-ის 20(4) მუხლი).[22]

ამგვარ უარყოფით გავლენას გავლენა ექნება თუ, მაგალითად, მონაცემების ერთი დამუშავებისთვის პასუხისმგებელი პირისგან მეორე დამუშავებისთვის პასუხისმგებელი პირისთვის გადაცემა მესამე მხარეებს შეუზღუდავს GDPR-ით გათვალისწინებული მონაცემთა სუბიექტის უფლებების განხორციელების შესაძლებლობას (მაგ., ინფორმაციის მიღების უფლება, წვდომის უფლება და ა.შ.).

მონაცემთა სუბიექტი, რომელიც ახდენს საკუთარი მონაცემების სხვა დამუშავებისთვის პასუხისმგებელი პირისთვის გადაცემის ინიცირებას, თანხმობას აძლევს ახალ დამუშავებისთვის პასუხისმგებელ პირს დამუშავებისთვის ან მასთან აფორმებს ხელშეკრულებას. როდესაც მონაცემთა წყება შეიცავს მესამე მხარეების პერსონალურ მონაცემებს, საჭიროა დამუშავების სხვა სამართლებრივი საფუძვლის იდენტიფიცირება. მაგ., დამუშავებისთვის პასუხისმგებელი პირი შესაძლოა ესწრაფვოდეს 6(1)(f) მუხლით გათვალისწინებული ლეგიტიმური ინტერესის განხორციელებას, განსაკუთრებით, როდესაც დამუშავებისთვის პასუხისმგებელი პირის მიზანია, მონაცემთა სუბიექტს მიაწოდოს მომსახურება, რომელიც ამ უკანასკნელს საშუალებას აძლევს, მონაცემები დაამუშაოს ცალსახად პირადი ან ოჯახური საქმიანობის ფარგლებში. დამუშავების ოპერაციები, რომლებიც ინიცირებულია მონაცემთა სუბიექტის მიერ, პირადი საქმიანობის კონტექსტში და სავარაუდოდ გავლენას ახდენს მესამე მხარეებზე, მონაცემთა სუბიექტის პასუხისმგებლობას წარმოადგენს იმდენად, რამდენადაც ამგვარი დამუშავების შესახებ გადაწყვეტილებას არ იღებს მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი, რაიმე ფორმით.

მაგალითად, ვებმეილის სერვისის გამოყენებით შესაძლებელია მონაცემთა სუბიექტის კონტაქტების, მეგობრების, ნათესავების, ოჯახის წევრებისა და ფართო გარემოს ცნობარის შექმნა. ვინაიდან მონაცემები ეხება იდენტიფიცირებად პირს (და შექმნილია იდენტიფიცირებადი პირის მიერ), რომელსაც სურს განახორციელოს მონაცემთა პორტირების უფლება, მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, მონაცემთა სუბიექტს გადასცეს შემომავალი და გამავალი ელ. ფოსტის მთლიანი ცნობარი.

---

[22] პრეამბულის 68-ე პუნქტის თანახმად: „როცა გარკვეული პერსონალური მონაცემები მონაცემთა ერთზე მეტი სუბიექტს ეხება, პერსონალური მონაცემების მიღების უფლება არ უნდა უგულებელყოფდეს მონაცემთა სხვა სუბიექტების უფლებებსა და თავისუფლებებს ამ რეგულაციის თანახმად.“

მსგავსად აღნიშნულისა, მონაცემთა სუბიექტის საბანკო ანგარიში შესაძლოა შეიცავდეს არა მხოლოდ ანგარიშის მფლობელის, არამედ, სხვა პირების ტრანზაქციებთან დაკავშირებულ მონაცემებს (მაგ., თუ ისინი ფულს ურიცხავენ ანგარიშის მფლობელს). მესამე მხარეთა უფლებებზე და თავისუფლებებზე, სავარაუდოდ, უარყოფით გავლენას არ მოახდენს საბანკო ანგარიშის შესახებ ინფორმაციის ანგარიშის მფლობელისთვის გადაცემა, მონაცემთა პორტირების მოთხოვნის საფუძველზე - იმ პირობით, რომ ორივე მაგალითში მონაცემები ერთი და იგივე მიზნისთვის გამოიყენება (ე.ი., საკონტაქტო მისამართი, რომელსაც მხოლოდ მონაცემთა სუბიექტი იყენებს ან მონაცემთა სუბიექტის საბანკო ანგარიშის ისტორია).

მეორეს მხრივ, მესამე მხარეების უფლებები და თავისუფლებები არ იქნება დაცული, თუ ახალი დამუშავებისთვის პასუხისმგებელი პირი მათ პერსონალურ მონაცემებს სხვა მიზნებისთვის გამოიყენებს, მაგ., თუ მიმღები დამუშავებისთვის პასუხისმგებელი პირი მარკეტინგული მიზნებისთვის იყენებს მონაცემთა სუბიექტის კონტაქტების ბაზაში არსებული სხვა ფიზიკური პირების პერსონალურ მონაცემებს.

შესაბამისად, მესამე მხარეზე უარყოფითი გავლენის თავიდან აცილების მიზნით, სხვა დამუშავებისთვის პასუხისმგებელი პირის მიერ ამგვარი პერსონალური მონაცემების დამუშავება დაშვებულია მხოლოდ იმ პირობით, რომ მონაცემები მხოლოდ იმ მომხმარებლის კონტროლის ქვეშ დარჩება, რომელმაც წარადგინა მოთხოვნა და მონაცემების მართვა მოხდება ცალსახად პირადი ან ოჯახური საჭიროებების მიზნით. „ახალ“ დამუშავებისთვის პასუხისმგებელ პირს (ვისაც მომხმარებლის მოთხოვნის საფუძველზე გადაეცემა მონაცემები) ეკრძალება გადაცემული მესამე მხარის მონაცემების საკუთარი მიზნებისთვის გამოყენება, მაგ., მესამე მხარეებისათვის (მონაცემთა სუბიექტებისთვის) მარკეტინგული პროდუქტების და სერვისების შეთავაზებისთვის. მაგალითად, აღნიშნული ინფორმაცია არ უნდა იქნას გამოყენებული მესამე მხარის შესახებ პროფილის განვრცობისთვის და მისი სოციალური გარემოს შექმნისთვის, მისი ინფორმირების და თანხმობის გარეშე.[23] ამ მონაცემების გამოყენება, აგრეთვე, დაუშვებელია მესამე მხარეების შესახებ ინფორმაციის მოპოვებისა და სპეციფიური პროფილების შექმნის მიზნით, მაშინაც კი, თუ მათი პერსონალური მონაცემები უკვე ინახება მონაცემთა დამმუშავებელთან. სხვა შემთხვევაში, ამგვარი დამუშავება იქნება უკანონო და უსამართლო, განსაკუთრებით, თუ მესამე მხარე არ არის ინფორმირებული და არ აქვს თავისი, როგორც მონაცემთა სუბიექტის უფლებების განხორციელების შესაძლებლობა.

ამას გარდა, ყველა მონაცემთა დამუშავებისთვის პასუხისმგებელი პირისთვის („გამგზავნი“ და „მიმღები“ მხარეებისთვის) წამყვან პრაქტიკას წარმოადგენს იმ ინსტრუმენტების დანერგვა, რომლებიც მონაცემთა სუბიექტებს საშუალებას აძლევს,

[23] სოციალური პლატფორმები მონაცემთა პორტირების საფუძველზე გადაცემული მონაცემების გამოყენებით მომხმარებელთა პროფილის განვრცობას არ უნდა ახორციელებდეს გამჭვირვალობის ფუნდამენტური პრინციპის დაუცველად. მათ, აგრეთვე, უნდა უზრუნველყონ ამ კონკრეტული დამუშავებისთვის სათანადო სამართლებრივი საფუძვლის გამოყენება.

შეარჩიონ შესაბამისი მონაცემები, რომელთა მიღება და გადაცემაც სურთ და საჭიროების შესაბამისად, გამორიცხონ სხვა ფიზიკური პირების მონაცემები. აღნიშნული ხელს შეუწყობს რისკების შემცირებას იმ მესამე მხარეებისთვის, რომელთა პერსონალური მონაცემები შესაძლოა პორტირებას დაექვემდებაროს.

ამას გარდა, დამმუშავებლებმა უნდა დანერგონ თანხმობის მექანიზმები სხვა მონაცემთა სუბიექტებისთვის, რათა გაადვილდეს მონაცემთა გადაცემა ისეთ შემთხვევებში, სადაც აღნიშნული მხარეები მზად არიან, გასცენ თანხმობა, ე.ი., თუ მათაც სურთ საკუთარი მონაცემების გადატანა სხვა დამმუშავებელთან. ასეთი სიტუაცია წარმოიშვება, მაგალითად, სოციალურ ქსელებთან დაკავშირებით, თუმცა, თავად დამუშავებისთვის პასუხისმგებელი პირი იღებს გადაწყვეტილებას იმის შესახებ, თუ რომელ წამყვან პრაქტიკას უნდა მისდიოს.

რაც შეეხება მონაცემებს, რომელთაც მოიცავს ინტელექტუალური საკუთრება და კომერციული საიდუმლოება:

20(4) მუხლი მიუთითებს სხვების უფლებებზე და თავისუფლებებზე, რაც მათ შორის, მოიცავს *„სავაჭრო საიდუმლოებებს ან ინტელექტუალურ საკუთრებას, კერძოდ, პროგრამული უზრუნველყოფის დამცავი ინტელექტუალური საკუთრების უფლებას“*. აღნიშნული უფლებები გათვალისწინებული უნდა იქნას მონაცემთა პორტირების შესახებ მოთხოვნის განხილვისას, თუმცა, *„ამ ფაქტორების გათვალისწინების შედეგად, დამმუშავებელმა მონაცემთა სუბიექტს არ უნდა უთხრას უარი ნებისმიერი მოთხოვნილი ინფორმაციის მიწოდებაზე“*. ამას გარდა, დამმუშავებელმა მონაცემთა პორტირების შესახებ მოთხოვნის დაკმაყოფილებაზე უარი არ უნდა თქვას იმ საფუძვლით, რომ აღნიშნული სხვა სახელშეკრულებო უფლებას არღვევს (მაგ., არსებული დავალიანება, ან კომერციული ინტერესების კონფლიქტი სხვა მონაცემთა სუბიექტთან).

მონაცემთა პორტირების უფლება არ გულისხმობს ფიზიკური პირის მიერ ინფორმაციის ბოროტად გამოყენებას, იმგვარად, რაც შეიძლება ჩაითვალოს უსამართლო პრაქტიკად ან წარმოადგენს ინტელექტუალური საკუთრების უფლებების დარღვევას.

ამავდროულად, პოტენციური ბიზნეს-რისკი, ცალკე აღებული, ვერ ჩაითვლება პორტირების შესახებ მოთხოვნის დაკმაყოფილებაზე უარის თქმის საფუძვლად, ხოლო მონაცემთა დამმუშავებლებს მონაცემთა სუბიექტების მიერ მიწოდებული პერსონალური მონაცემების გადაცემა შეუძლიათ იმ ფორმით, რაც არ ამჟღავნებს კომერციული საიდუმლოებით ან ინტელექტუალური საკუთრების უფლებით დაცულ ინფორმაციას.

IV. მონაცემთა პორტირებაზე როგორ ვრცელდება ზოგადი წესები, რომლებიც არეგულირებს მონაცემთა სუბიექტის უფლებების განხორციელებას?

- წინასწარ რა ინფორმაცია უნდა წარმოადგინოს მონაცემთა სუბიექტმა?

მონაცემთა პორტირების ახალ უფლებასთან შესაბამისობის მიზნით, დამმუშავებლებმა მოანცემთა სუბიექტებს უნდა შეატყობინონ პორტირების ახალი უფლების არსებობის შესახებ. თუ პერსონალური მონაცემების შეგროვება ხდება პირდაპირ მონაცემთა სუბიექტისგან, აღნიშნული უნდა განხორციელდეს „პერსონალური მონაცემების მოპოვების დროს“. თუ პერსონალური მონაცემების მოპოვება არ ხდება მონაცემთა სუბიექტისგან, მაშინ დამმუშავებელმა ინფორმაციის მიწოდება უნდა მოახდინოს 13(2)(b) და 14(2)(c) მუხლების შესაბამისად.

„თუ პერსონალური მონაცემები მონაცემთა სუბიექტისგან არ არის მოპოვებული“, 14(3) მუხლის თანახმად, ინფორმირება უნდა განხორციელდეს გონივრულ ვადაში, მაგრამ არა უმეტეს მონაცემთა მოპოვებიდან ერთი თვისა, მონაცემთა სუბიექტთან კავშირის პირველად დამყარებისას, ან თუ მონაცემები სხვა მიმღებს უნდა გადაეცეს, არა უგვიანეს მონაცემების პირველად გადაცემის მომენტისა.[24]

საჭირო ინფორმაციის მიწოდებისას, დამმუშავებელმა უნდა უზრუნველყოს პორტირების უფლების სხვა უფლებებისგან გამიჯვნა. შესაბამისად, WP29-ის რეკომენდაციის თანახმად, დამმუშავებლებმა მკაფიოდ უნდა განმარტონ, თუ რა განსხვავება არსებობს იმ სხვადასხვა ტიპის მონაცემებს შორის, რომელთა მიღებაც მონაცემთა სუბიექტს შეუძლია მონაცემებზე წვდომის უფლებით და მონაცემთა პორტირების უფლებით.

ამას გარდა, სამუშაო ჯგუფის რეკომენდაციის თანახმად, დამმუშავებლებმა მონაცემთა სუბიექტს ყოველთვის უნდა მიაწოდონ ინფორმაცია მონაცემთა პორტირების უფლების შესახებ მანამ, სანამ მონაცემთა სუბიექტი დახურავს საკუთარ ანგარიშს. ეს მომხმარებელს საშუალებას აძლევს, შეაფასონ საკუთარი პერსონალური მონაცემები და ადვილად გადაიტანონ ეს მონაცემები საკუთარ მოწყობილობაზე ან სხვა პროვაიდერთან, ხელშეკრულების შეწყვეტამდე.

და ბოლოს, WP29-ის რეკომენდაციის თანახმად, კარგი პრაქტიკის სახით, მიზანშეწონილია, რომ „მიმღებმა“ დამმუშავებლებმა მონაცემთა სუბიექტებს მიაწოდონ სრული ინფორმაცია, თუ რა ტიპის პერსონალური მონაცემები არის

[24] მე-12 მუხლის თანახმად, დამუშავებისთვის პასუხისმგებელ პირს მოეთხოვება, რომ ნებისმიერი კომუნიკაცია წარმართოს *„მოკლე, გამჭვირვალე, გასაგები და მარტივად ხელმისაწვდომი ფორმით, ნათელი და მარტივი ენით, განსაკუთრებით მაშინ, როდესაც აღნიშნული ეხება არასრულწლოვანისთვის მიწოდებულ ინფორმაციას.“*

რელევანტური მათი მომსახურების მიწოდებისთვის. გარდა იმისა, რომ აღნიშნული სამართლიან დამუშავებას უწყობს ხელს, იგი მომხმარებლებს აგრეთვე, საშუალებას აძლევს, შეამცირონ რისკები მესამე მხარეების სასარგებლოდ და შეზღუდონ პერსონალური მონაცემების არასაჭირო დუბლირება მაშინაც კი, თუ ეს არ ეხება სხვა მონაცემთა სუბიექტებს.

- როგორ მოახდენს დამუშავებისთვის პასუხისმგებელი პირი მონაცემთა სუბიექტის იდენტიფიცირებას მანამ, სანამ უპასუხებს მის მოთხოვნას?

GDPR-ი არ ითვალისწინებს რაიმე პრესკრიფციულ მოთხოვნებს მონაცემთა სუბიექტის იდენტიფიცირებასთან დაკავშირებით. ამავდროულად, 12(2) მუხლის თანახმად, დამმუშავებელმა არ უნდა თქვას უარი მონაცემთა სუბიექტის მოთხოვნაზე საკუთარი უფლების განხორციელების შესახებ (მონაცემთა პორტირების უფლების ჩათვლით), გარდა იმ შემთხვევისა, როცა იგი პერსონალურ მონაცემებს ამუშავებს მიზნისთვის, რომელიც არ საჭიროებს მონაცემთა სუბიექტის იდენტიფიცირებას და დამუშავებისთვის პასუხისმგებელ პირს შეუძლია დემონსტრირება იმისა, რომ მას არ აქვს მონაცემთა სუბიექტის იდენტიფიცირების საშუალება. ამავდროულად, 11(2) მუხლის მიხედვით, ასეთ გარემოებებში მონაცემთა სუბიექტს შეუძლია წარმოადგინოს დამატებითი ინფორმაცია, რომელიც მისი იდენტიფიცირების შესაძლებლობას იძლევა. 12(6) მუხლი, აგრეთვე, ადგენს, რომ თუ დამუშავებისთვის პასუხისმგებელ პირს გონივრული ეჭვები აქვს მონაცემთა სუბიექტის ვინაობასთან დაკავშირებით, მას შეუძლია, მოითხოვოს დამატებითი ინფორმაცია მონაცემთა სუბიექტის ვინაობის დასადასტურებლად. თუ მონაცემთა სუბიექტი წარმოადგენს დამატებით ინფორმაციას, რომელიც მისი იდენტიფიცირების შესაძლებლობას იძლევა, დამმუშავებელმა არ უნდა თქვას უარი მოთხოვნის დაკმაყოფილებაზე. თუ ონლაინ შეგროვებული მონაცემები და ინფორმაცია დაკავშირებულია ფსევდონიმებთან ან უნიკალურ იდენტიფიკატორებთან, დამუშავებისთვის პასუხისმგებელ პირს შეუძლია დანერგოს სათანადო პროცედურები, რომელიც ფიზიკურ პირს მისცემს საშუალებას, დამუშავებისთვის პასუხისმგებელ პირს მიმართოს პორტირების მოთხოვნით და მიიღოს მასთან დაკავშირებული მონაცემები. ნებისმიერ შემთხვევაში, დამმუშავებელმა უნდა დანერგოს იდენტიფიცირების პროცედურა, რათა მყარად დაადგინოს იმ მონაცემთა სუბიექტის ვინაობა, რომელიც საკუთარ პერსონალურ მონაცემებს ითხოვს ან ზოგადად, ახორციელებს GDPR-ით მინიჭებულ უფლებებს.

ეს პროცედურები ხშირად, უკვე არსებობს. მონაცემთა სუბიექტები, ხშირად, უკვე იდენტიფიცირებულია მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის მიერ, მანამ, სანამ მოხდება ხელშეკრულების გაფორმება ან დამუშავებაზე თანხმობის მოპოვება. შედეგად, პერსონალური მონაცემები, რომლებიც შესაბამისი პირის დასარეგისტრირებლად გამოიყენება, შესაძლებელია, რომ აგრეთვე გამოყენებული

იქნას, როგორც მტკიცებულება მონაცემთა სუბიექტის იდენტიფიცირებისთვის, მონაცემთა პორტირების მიზნებისთვის.[25]

აღნიშნულ შემთხვევებში, მონაცემთა სუბიექტის წინასწარ იდენტიფიცირება, შესაძლოა, საჭიროებდეს მათი სამართლებრივი იდენტობის დამადასტურებელ მტკიცებულებას, თუმცა, ამგვარი ვერიფიკაცია, შესაძლოა, არ იყოს რელევანტური მონაცემებსა და შესაბამის პირს შორის არსებული კავშირის შესაფასებლად, რადგან ეს კავშირი პირის ოფიციალურ ან სამართლებრივ იდენტობასთან არ არის დაკავშირებული. არსებითად, მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის შესაძლებლობა, მოითხოვოს დამატებითი ინფორმაცია პირის იდენტიფიცირებისთვის, არ უნდა იწვევდეს გადაჭარბებულ მოთხოვნებს და პერსონალური მონაცემების შეგროვებას, რომელიც არ არის რელევანტური ან აუცილებელი ფიზიკურ პირსა და მოთხოვნილ პერსონალურ მონაცემებს შორის კავშირის გასამყარებლად.

უმეტეს შემთხვევაში, იდენტიფიცირების ამგვარი პროცედურები ისედაც არსებობს. მაგალითად, მომხმარებლის სახელები და პაროლები ხშირად გამოიყენება იმისათვის, რომ ფიზიკურ პირებს ჰქონდეთ წვდომა მონაცემებზე, რომლებიც ხელმისაწვდომია თავიანთ ელ-ფოსტის ანგარიშებში, სოციალურ ქსელებში არსებულ პროფილებში და იმ ანგარიშებში, რომელიც გამოიყენება სხვადასხვა სერვისებისთვის, ხოლო ზოგიერთი სერვისის მიღებას ფიზიკური პირები საკუთარი სრული სახელისა და ვინაობის გამჟღავნების გარეშე არჩევენ.

იმ შემთხვევაში, თუ მონაცემთა სუბიექტის მიერ მოთხოვნილი მონაცემების მოცულობა პრობლემურს ხდის მონაცემთა გადაცემას ინტერნეტის საშუალებით, მოთხოვნის დაკმაყოფილების ვადის მაქსიმალურ ვადამდე (სამ თვემდე) გაზრდის ნაცვლად,[26] მიზანშეწონილია, რომ დამუშავებისთვის პასუხისმგებელმა პირმა განიხილოს მონაცემთა მიწოდების ალტერნატიული გზები, როგორიცაა, სტრიმინგი ან მონაცემების შენახვა CD და DVD დისკებზე ან სხვა შესანახ მოწობილობაზე, ან პერსონალური მონაცემების სხვა დამუშავებისთვის პასუხისმგებელი პირისთვის პირდაპირ გადაცემა (GDRP-ის 20(2) მუხლის შესაბამისად, თუ ეს ტექნიკურად შესაძლებელია).

- პორტირების შესახებ მოთხოვნას რა ვადაში უნდა გაეცეს პასუხი?

12(3) მუხლის თანახმად, დამუშავებისთვის პასუხისმგებელმა პირმა მონაცემთა სუბიექტს ინფორმაცია „მოთხოვნის საფუძველზე განხორციელებული ქმედებების შესახებ“ უნდა მიაწოდოს „დაუყოვნებლივ ან ნებისმიერ შემთხვევაში, მოთხოვნის

[25] მაგალითად, როდესაც მონაცემთა დამუშავება დაკავშირებულია მომხმარებლის ანგარიშთან, მომხმარებლის სახელის და პაროლის მიწოდება, შესაძლოა, საკმარისი იყოს მონაცემთა სუბიექტის იდენტიფიცირებისთვის.

[26] მუხლი 12(3): „დამუშავებისთვის პასუხისმგებელმა პირმა მონაცემთა სუბიექტს ... უნდა მიაწოდოს ინფორმაცია ... მოთხოვნის საფუძველზე განხორციელებული ქმედებების შესახებ.“

მიღებიდან ერთი თვის ვადაში“. ეს ვადა შეიძლება გაგრძელდეს სამი თვით, მოთხოვნის სირთულიდან გამომდინარე, იმ პირობით, თუ მონაცემთა სუბიექტს დამუშავებისთვის პასუხისმგებელი პირი მიაწვდის ინფორმაციას დაყოვნების მიზეზების შესახებ, თავდაპირველი მოთხოვნის წარდგენიდან ერთი თვის ვადაში.

დამუშავებისთვის პასუხისმგებელი პირები, რომლებიც ახორციელებენ საინფორმაციო საზოგადოების მომსახურების მიწოდებას, სავარაუდოდ, უკეთ იქნებიან აღჭურვილი იმისათვის, რომ მოთხოვნის შესრულება მოხდეს შედარებით მოკლე ვადაში. მომხმარებლის მოლოდინების დასაკმაყოფილებლად, კარგ პრაქტიკას წარმოადგენს პორტირების შესახებ მოთხოვნებზე რეაგირების მიზნით, კონკრეტული ვადის განსაზღვრა და ამ ინფორმაციის მიწოდება მონაცემთა სუბიექტებისთვის.

თუ დამუშავებისთვის პასუხისმგებელი პირი უარს ამბობს პორტირების მოთხოვნის შესრულებაზე, 12(4) მუხლის თანახმად, იგი ვალდებულია, მონაცემთა სუბიექტს დაუყოვნებლივ ან მოთხოვნის მიღებიდან არაუგვიანეს ერთი თვის ვადაში აცნობოს *„მოთხოვნაზე უარის მიზეზების შესახებ და ასევე აცნობოს აღნიშნულის საზედამხედველო ორგანოში ან სასამართლოში გასაჩივრების შესაძლებლობის შესახებ.“*

მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, პატივი სცეს მოთხოვნაზე დადგენილ ვადებში რეაგირების ვალდებულებას, მაშინაც კი, თუ იგი უარს იტყვის მოთხოვნის დაკმაყოფილებაზე. სხვა სიტყვებით რომ ვთქვათ, დაუშვებელია დამუშავებისთვის პასუხისმგებელი პირის დუმილი, როდესაც მას მიმართავენ მონაცემთა პორტირების შესახებ მოთხოვნით.

- რა შემთხვევაშია შესაძლებელი მონაცემთა პორტირების შესახებ მოთხოვნის უარყოფა ან საფასურის დაწესება?

მე-12 მუხლის თანახმად, პერსონალური მონაცემების გაცემა უნდა განხორციელდეს უსასყიდლოდ, გარდა იმ შემთხვევისა, როდესაც დამუშავებისთვის პასუხისმგებელ პირს შეუძლია დემონსტრირება, რომ მოთხოვნები არის ცალსახად დაუსაბუთებელი ან გადაჭარბებული, „განსაკუთრებით, მათი განმეორებითი ხასიათის გამო“. საინფორმაციო საზოგადოების მომსახურების მიმწოდებელს, რომლის სპეციალიზაციასაც წარმოადგენს პერსონალური მონაცემების ავტომატური დამუშავება და რომელიც ახორციელებს ისეთ ავტომატურ სისტემებს, როგორიცაა „აპლიკაციის პროგრამირების ინტერფეისები“ (API)[27], შეუძლია ხელი შეუწყოს მონაცემთა სუბიექტთან კომუნიკაციას, რაც შეამცირებს განმეორებითი მოთხოვნებიდან მომდინარე პოტენციურ ტვირთს. შესაბამისად, ძალიან მცირე იქნება იმ შემთხვევების რაოდენობა, სადაც დამუშავებისთვის პასუხისმგებელი პირი

[27] „აპლიკაციის პროგრამირების ინტერფეისი“ (Application Programming Interface – API) აღნიშნავს აპლიკაციების ან ვებ-სერვისების ინტერფეისებს, რომლებსაც დამუშავებისთვის პასუხისმგებელი პირი ხდის ხელმისაწვდომს, რათა სხვა სისტემებს ან აპლიკაციებს შეეძლოთ მათ სისტემებთან დაკავშირება და მათთან ერთად მუშაობა.

შეძლებს, მოთხოვნილი ინფორმაციის მიწოდებაზე უარი დაასაბუთოს, მაშინაც კი, როდესაც საქმე ეხება მონაცემთა პორტირების ერთზე მეტ მოთხოვნას.

ამას გარდა, იმ პროცესების საერთო ღირებულება, რომლებიც შექმნილია მონაცემთა პორტირების შესახებ მოთხოვნებზე რეაგირებისთვის, არ უნდა იქნას გათვალისწინებული მოთხოვნის გადაჭარბებული მოთხოვნის გადაჭარბებულობის შეფასებისას. უფრო მეტიც, GDPR-ის მე-12 მუხლი ხაზს უსვამს ერთი მონაცემთა სუბიექტის მიერ წარდგენილ მოთხოვნებს და არა მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის მიერ მიღებული მოთხოვნების საერთო რაოდენობას. შესაბამისად, მონაცემთა სუბიექტს დამუშავებისთვის პასუხისმგებელმა პირმა არ უნდა დაუწესოს ზოგადად სისტემის განხორციელებასთან დაკავშირებული ხარჯების ანაზღაურების მოთხოვნა და აღნიშნული არ უნდა იქნას გამოყენებული პორტირების მოთხოვნის დაკმაყოფილებაზე უარის თქმის დასაბუთებისთვის.

V. როგორ უნდა იქნას მიწოდებული პორტირებული მონაცემები?

- მონაცემთა მიწოდებისთვის დამუშავებისთვის პასუხისმგებელმა პირმა რა საშუალებები უნდა გამოიყენოს?

GDPR-ის 20(1) მუხლის თანახმად, დამუშავებისთვის პასუხისმგებელ პირს უფლება აქვს, მონაცემები გადასცეს სხვა დამუშავებისთვის პასუხისმგებელ პირს ისე, რომ აღნიშნული არ დააბრკოლოს იმ დამმუშავებელმა, ვისაც მონაცემთა სუბიექტმა მიაწოდა პერსონალური მონაცემები.

ამგვარი დაბრკოლება მოიაზრებს ნებისმიერ სამართლებრივ, ტექნიკურ ან ფინანსურ დაბრკოლებას, რომელსაც აწესებს დამუშავებისთვის პასუხისმგებელი პირი იმისათვის, რომ გამორიცხოს ან გააჭიანუროს მონაცემთა სუბიექტის ან სხვა დამუშავებისთვის პასუხისმგებელი პირის მიერ მონაცემებზე წვდომა, მათი გადაცემა ან ხელახლა გამოყენება. აღნიშნული დაბრკოლების მაგალითებია: მონაცემთა მიწოდებაზე საფასურის დაწესება, მონაცემთა ფორმატის, API-ს ან მიწოდებული ფორმატის ოპერაციული თავსებადობის ან მისაწვდომობის ნაკლებობა; გადაჭარბებული გაჭიანურება ან მონაცემთა სრული ფორმით მოპოვების სირთულე; მონაცემების მიზანმიმართულად გაბუნდოვანება; ან სპეციფიური და დაუსაბუთებელი ან გადაჭარბებული სტანდარტიზაციის ან აკრედიტაციის სექტორული მოთხოვნების დაწესება.[28]

[28] შესაძლოა წარმოიშვას გარკვეული ლეგიტიმური დაბრკოლებები, როგორიცაა, მაგალითად, სხვების უფლებებთან და თავისუფლებებთან დაკავშირებული დაბრკოლებები, როგორც ეს 20(4) მუხლშია მითითებული, ან დამმუშავებლის სისტემების უსაფრთხოებასთან დაკავშირებული დაბრკოლებები.

20(2) მუხლი დამუშავებისთვის პასუხისმგებელ პირებს ავალდებულებს, პორტირებული მონაცემები სხვა დამუშავებისთვის პასუხისმგებელ პირს გადასცენ პირდაპირ, „თუ ეს ტექნიკურად შესაძლებელია.“

მონაცემების ერთი დამუშავებისთვის პასუხისმგებელი პირისგან პირდაპირ მეორე დამუშავებისთვის პასუხისმგებელი პირისთვის გადაცემის ტექნიკური შესაძლებლობა, მონაცემთა სუბიექტის კონტროლის ქვეშ, უნდა შეფასდეს ინდივიდუალურად. პრეამბულის 68-ე პუნქტი დამატებით განმარტავს „ტექნიკური შესაძლებლობის“ საზღვრებს და მიუთითებს, რომ იგი „არ უნდა ავალდებულებდეს დამუშავებისთვის პასუხისმგებელ პირს, რომ აითვისოს ან შეინარჩუნოს დამუშავების სისტემები, რომლებიც ტექნიკურად თავსებადია.“

დამუშავებისთვის პასუხისმგებელი პირების მიმართ არსებობს მოლოდინი, რომ მათ პერსონალური მონაცემების გადაცემა უნდა უზრუნველყონ ოპერაციულად თავსებად ფორმატში, თუმცა, ეს სხვა დამუშავებისთვის პასუხისმგებელ პირებს არ აკისრებს ამ ფორმატებთან თავსებადობის უზრუნველყოფის ვალდებულებას. მონაცემების ერთი დამუშავებისთვის პასუხისმგებელი პირიდან პირდაპირ მეორე დამუშავებისთვის პასუხისმგებელი პირისთვის გადაცემა განხორციელდება, თუ ორ სისტემას შორის შესაძლებელია კომუნიკაციის დამყარება, უსაფრთხოდ,[29] და როდესაც მიმღებ სისტემას გააჩნია ტექნიკური შესაძლებლობა, მიიღოს შემოსული მონაცემები. თუ ტექნიკური დაბრკოლებები აფერხებს პირდაპირ გადაცემას, დამუშავებისთვის პასუხისმგებელმა პირმა ეს დაბრკოლებები უნდა განუმარტოს მონაცემთა სუბიექტებს. წინააღმდეგ შემთხვევაში, მის გადაწყვეტილებას ექნება ისეთივე შედეგი, რაც აქვს მონაცემთა სუბიექტის მოთხოვნასთან დაკავშირებით ქმედების განხორციელებაზე უარის თქმას (მუხლი 12(4)).

ტექნიკურ დონეზე, დამუშავებისთვის პასუხისმგებელმა პირებმა უნდა გამოიკვლიონ და შეაფასონ ორი განსხვავებული და ურთიერთდამხმარე საშუალებები, რომლებიც უზრუნველყოფს პორტირებადი მონაცემების ხელმისაწვდომობას მონაცემთა სუბიექტებისათვის ან სხვა დამუშავებისთვის პასუხისმგებელი პირისთვის:

- პორტირებადი მონაცემების მთლიანი ჩანაწერის (dataset) (ან გლობალური ჩანაწერიდან ექსტრაქტირებული მონაცემების) პირდაპირ გადაცემა;

- ავტომატური ინსტრუმენტი, რომელიც შესაბამისი მონაცემების ექსტრაქტირების შესაძლებლობას იძლევა.

მონაცემთა კომპლექსური და მოცულობითი ჩანაწერების შემთხვევაში, დამუშავებისთვის პასუხისმგებელი პირები მეორე საშუალებას ამჯობინებენ, რადგან

დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, დაასაბუთოს, რომ დაბრკოლება არის ლეგიტიმური და არ წარმოადგენს დაბრკოლებას, 20(1) მუხლის მნიშვნელობის შესაბამისად.

[29] იმგვარი კომუნიკაციით, სადაც დადგენილია მხარეთა ვინაობა და გამოიყენება მონაცემთა დაშიფრვის სათანადო დონე.

იგი მონაცემთა ჩანაწერიდან იმ მონაცემების ექსტრაქტირების შესაძლებლობას იძლევა, რომელიც მონაცემთა სუბიექტისათვის რელევანტურია, მისი მოთხოვნიდან გამომდინარე. აღნიშნული ხელს შეუწყობს რისკის მინიმუმამდე შემცირებას და სავარაუდოდ, მონაცემთა სინქრონიზაციის მექანიზმების გამოყენებას[30] (მაგ., დამუშავებისთვის პასუხისმგებელ პირებს შორის რეგულარული კომუნიკაციის კონტექსტში). ეს აგრეთვე, საუკეთესო გზაა „ახალი“ დამუშავებისთვის პასუხისმგებელი პირის შესაბამისობის უზრუნველსაყოფად და წარმოადგენს კარგ პრაქტიკას თავდაპირველი დამუშავებისთვის პასუხისმგებელი პირის მიერ პირადი ცხოვრების ხელშეუხებლობის რისკების შესამცირებლად.

შესაბამისი პორტირებადი მონაცემების მიწოდების აღნიშნული ორი განსხვავებული და ურთიერთდამხმარე საშუალების განხორციელება შესაძლებელია მონაცემთა ხელმისაწვდომობის სხვადასხვა საშუალებებით უზრუნველყოფის გზით, როგორიცაა, მაგალითად, დაცული შეტყობინებების გაგზავნა, SFTP სერვერი, დაცული WebAPI ან WebPortal. მონაცემთა სუბიექტებს უნდა მიეცეთ შესაძლებლობა, ისარგებლონ პერსონალური მონაცემების შენახვის მომსახურებით, პერსონალური ინფორმაციის მართვის სისტემით[31] ან სხვა სახის მომსახურებით, რომელსაც უზრუნველყოფს ნდობით აღჭურვილი მესამე მხარე, რათა შეინახონ და შეინარჩუნონ პერსონალური მონაცემები და დამმუშავებლებს მისცენ პერსონალურ მონაცემებზე წვდომისა და მათი დამუშავების ნებართვა, საჭიროების შესაბამისად.

- როგორი უნდა იყოს მონაცემების ფორმატი?

GDPR-ის თანახმად, დამუშავებისთვის პასუხისმგებელ პირებს მოეთხოვებათ, ფიზიკური პირის მიერ მოთხოვნილი პერსონალური მონაცემების მიწოდება უზრუნველყონ ისეთ ფორმატში, რომელიც ხელახლა გამოყენების საშუალებას იძლევა. კერძოდ, GDPR-ის 20(1) მუხლის თანახმად, პერსონალური მონაცემების მიწოდება უნდა მოხდეს „სტრუქტურებული, ფართოდ გამოყენებადი და ელექტრონულად წაკითხვადი ფორმატით“. პრეამბულის 68-ე პუნქტი დამატებით განმარტავს, რომ ეს ფორმატი უნდა იყოს ოპერაციულად თავსებადი, ხოლო ევროკავშირში[32] ეს ტერმინი განიმარტება როგორც:

---

[30] სინქრონიზაციის მექანიზმი ხელს შეუწყობს GDPR-ის მე-5 მუხლით დადგენილი ზოგადი ვალდებულებების შესრულებას. კერძოდ, ამ მუხლის თანახმად, „პერსონალური მონაცემები უნდა იყოს (...) ზუსტი და უნდა იყოს ზუსტი და საჭიროებისამებრ განახლდეს.“

[31] პერსონალური ინფორმაციის მართვის სისტემების შესახებ იხ., მაგალითად: EDPS-ის დასკვნა 9/2016, ხელმისაწვდომია: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-10-20_PIMS_opinion_EN.pdf.

[32] მე-2 მუხლი, ევროპარლამენტის და საბჭოს 2009 წლის 16 სექტემბრის No 922/2009/EC გადაწყვეტილება ევროპის საჯარო ადმინისტრაციებს შორის ოპერაციული თავსებადობის გადაწყვეტების შესახებ (ISA) OJ 260, 03.10.2009, გვ.20.

განსხვავებული და მრავალფეროვანი ორგანიზაციების შესაძლებლობა, დაამყარონ ინტერაქცია ურთიერთსასარგებლო და შეთანხმებული საერთო მიზნების მისაღწევად, რაც მოიცავს ინფორმაციისა და ცოდნის გაზიარებას ორგანიზაციებს შორის, მათ მიერ მხარდაჭერილი ბიზნეს პროცესების საშუალებით, თავიანთ საინფორმაციო და საკომუნიკაციო ტექნოლოგიების (ICT) სისტემებს შორის მონაცემთა გაზიარების გზით.

ტერმინები „სტრუქტუირებული“, „ფართოდ გამოყენებადი“ და „ელექტრონულად წაკითხვადი“ ის მინიმალური მოთხოვნებია, რომლებიც ხელს შეუწყობს დამუშავებისთვის პასუხისმგებელი პირის მიერ მიწოდებული მონაცემთა ფორმატის ოპერაციულ თავსებადობას. ამრიგად, „სტრუქტუირებული, ფართოდ გამოყენებადი და ელექტრონულად წაკითხვადი“ საშუალებების სპეციფიკაციებია, ხოლო ოპერაციული თავსებადობა კი სასურველი შედეგია.

2013/37/EU დირექტივაში[33] [34], პრეამბულის 21-ე პუნქტი „ელექტრონულად წაკითხვადს“ განმარტავს შემდეგნაირად:

ფაილის ფორმატი, რომლის სტრუქტურაც იმგვარია, რომ კომპიუტერულ აპლიკაციებს მარტივად შეუძლიათ სპეციფიური მონაცემების, მათ შორის, ფაქტის შემცველი ინდივიდუალური განცხადებების, და მათი შიდა სტრუქტურის იდენტიფიცირება, აღიარება და ექსტრაქტირება. მონაცემები, რომლებიც კოდირებულია ელექტრონულად წაკითხვადი ფორმატის მქონე ფაილებში, ელექტრონულად წაკითხვადი მონაცემებია. ელექტრონულად წაკითხვადი ფორმატები შესაძლოა იყოს საჯარო (ღია) ან კერძო; ისინი, შესაძლოა, წარმოადგენდნენ (ან არ წარმოადგენდნენ) ფორმალურ სტანდარტებს. დოკუმენტები, რომლებიც კოდირებულია ფაილის იმგვარ ფორმატში, რომელიც ზღუდავს ავტომატურ დამუშავებას იმის გამო, რომ ამ დოკუმენტებიდან შეუძლებელია მონაცემების (ადვილად) ექსტრაქტირება, არ უნდა იქნას მიჩნეული ელექტრონულად წაკითხვადი ფორმატის მქონე დოკუმენტებად. წევრმა სახელმწიფოებმა, საჭიროების შესაბამისად, უნდა წაახალისონ საჯარო (ღია) ელექტრონულად წაკითხვადი ფორმატების გამოყენება.

მონაცემთა შესაძლო ტიპების ფართო სპექტრის გათვალისწინებით, რომელთა დამუშავებაც მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს შეუძლია, GDPR-ი არ ადგენს კონკრეტულ რეკომენდაციებს იმის შესახებ, თუ რა ფორმატში უნდა იქნას მიწოდებული პერსონალური მონაცემები. შესაფერისი ფორმატები განსხვავდება

[33] რომლითაც შესწორდა 2003/98/EC დირექტივა საჯარო სექტორში დაცული ინფორმაციის ხელახლა გამოყენების შესახებ.

[34] ევროკავშირის ლექსიკონი (http://eur-lex.europa.eu/eli-register/glossary.html) შეიცავს დამატებით განმარტებებს იმ მოლოდინების შესახებ, რომელიც წინამდებარე სახელმძღვანელო პრინციპებში გამოყენებულ კონცეფციებს უკავშირდება, როგორიცაა: *ელექტრონულად წაკითხვადი, ოპერაციულად თავსებადი, ღია (საჯარო) ფორმატი, სტანდარტული, მეტამონაცემები.*

სექტორების მიხედვით, ხოლო ადექვატური ფორმატები, შესაძლოა, უკვე არსებობდეს. ადექვატური ფორმატი ყოველთვის უნდა აირჩეს ოპერაციული თავსებადობის და მონაცემთა პორტირებადობის მაღალი ხარისხის მიზნის გათვალისწინებით. როგორც ასეთი, ფორმატები, რომლებიც ექვემდებარება ძვირადღირებული ლიცენზირების შეზღუდვებს, ადექვატურ მიდგომას არ წარმოადგენს.

პრეამბულის 68-ე პუნქტი განმარტავს: *„მონაცემთა სუბიექტის უფლება, რომ გადასცეს ან მიიღოს მასთან დაკავშირებული პერსონალური მონაცემები, არ უნდა ავალდებულებდეს დამუშავებისთვის პასუხისმგებელ პირს, რომ აითვისოს ან შეინარჩუნოს დამუშავების სისტემები, რომლებიც ტექნიკურად თავსებადია.“* **ამრიგად, პორტირების მიზანია ოპერაციულად თავსებადი და არა თავსებადი სისტემების შექმნა[35].**

პერსონალური მონაცემების მიწოდება უნდა მოხდეს ისეთ ფორმატებში, რომლებიც მინიმალურად არის დაკავშირებული შიდა ან კერძო ფორმატთან. როგორც ასეთი, მონაცემთა პორტირება გულისხმობს დამუშავებისთვის პასუხისმგებელი პირის მიერ მონაცემთა დამუშავების დამატებით შრეს, რათა განხორციელდეს მონაცემთა ექსტრაქტირება პლატფორმიდან და პორტირების ფარგლებს გარეთ არსებული პერსონალური მონაცემების გაფილტვრა, როგორიცაა, ნავარაუდევი მონაცემები ან სისტემების უსაფრთხოებასთან დაკავშირებული მონაცემები. ამრიგად, დამუშავებისთვის პასუხისმგებელი პირები შეძლებენ, წინასწარ მოახდინონ საკუთარ სისტემებში იმ მონაცემების იდენტიფიცირება, რომლებიც პორტირებას ექვემდებარება. ამგვარი დამატებითი დამუშავება განხილული იქნება, როგორც ძირითადი დამუშავების დამხმარე აქტივობა, ვინაიდან მისი განხორციელება არ ხდება დამუშავებისთვის პასუხისმგებელი პირის მიერ განსაზღვრული ახალი მიზნის მისაღწევად.

იმ შემთხვევაში, თუ მოცემულ ინდუსტრიაში ან კონტექსტში არ არსებობს ფართოდ გამოყენებადი ფორმატები, დამუშავებისთვის პასუხისმგებელმა პირებმა **პერსონალური მონაცემების მიწოდება უნდა მოახდინონ ფართოდ გამოყენებადი ღია (საჯარო) ფორმატების გამოყენებით (მაგ., XML, JSON, CSV, ...),** სასარგებლო **მეტამონაცემებთან ერთად, რომელიც იქნება მაქსიმალურად დეტალიზებული,** და ამავდროულად, შენარჩუნებული უნდა იქნას აბსტრაქციის მაღალი დონე. როგორც ასეთი, გამოყენებული უნდა იქნას სათანადო მეტამონაცემები, რომლებიც ზუსტად აღწერს გაცვლილი ინფორმაციის მნიშვნელობას. ეს მეტამონაცემები საკმარისი უნდა იყოს მონაცემთა ფუნქციონირებისა და ხელახლა გამოყენებისთვის, თუმცა, რა თქმა უნდა, კომერციული საიდუმლოების გამჟღავნების გარეშე. ნაკლებად სავარაუდოა,

[35] ISO/IEC 2382-01 განმარტების თანახმად, ოპერაციული თავსებადობა არის: „სხვადასხვა ფუნქციონალურ განყოფილებებს შორის კომუნიკაციის, პროგრამების განხორციელების ან მონაცემთა გადაცემის შესაძლებლობა, იმგვარად, რაც მოითხოვს მომხმარებლის მინიმალურ ინფორმირებას (ან საერთოდ არ მოითხოვს მომხმარებლის ინფორმირებას) ამ განყოფილებების უნიკალური მახასიათებლების შესახებ.“

რომ ფიზიკური პირისათვის ელექტრონული საფოსტო ყუთის PDF ვერსიების მიწოდება უზრუნველყოფს საკმარისად სტრუქტუირებულ და თვალსაჩინო მონაცემებს, ხელმეორე გამოყენებისთვის. ნაცვლად აღნიშნულისა, ელ-ფოსტის მონაცემების მიწოდება უნდა მოხდეს ისეთ ფორმატში, სადაც შენარჩუნებული იქნება ყველა მეტამონაცემი, რაც მონაცემთა ეფექტურ ხელმეორე გამოყენებას შეუწყობს ხელს. როგორც ასეთი, მონაცემთა მიწოდების ფორმატის შერჩევისას, დამუშავებისთვის პასუხისმგებელმა პირმაუნდა გაითვალისწინოს, ეს ფორმატი როგორ შეუწყობს ხელს ან დააბრკოლებს ფიზიკური პირის უფლებას მონაცემთა ხელმეორე გამოყენებაზე. თუ დამუშავებისთვის პასუხისმგებელ პირს შეუძლია, მონაცემთა სუბიექტს მისცეს საშუალება თავად გააკეთოს არჩევანი პერსონალური მონაცემების ფორმატებს შორის, მან მკაფიოდ უნდა განმარტოს თითოეული არჩევანის შედეგი. ამავდროულად, დამატებითი მეტამონაცემების დამუშავება იმ ერთადერთი მოტივით, რომ ეს მონაცემები შესაძლოა საჭირო ან სასურველი იყოს მონაცემთა პორტირების მოთხოვნაზე რეაგირებისთვის, არ წარმოადგენს ამგვარი დამუშავების ლეგიტიმურ საფუძველს.

29-ე მუხლის სამუშაო ჯგუფი მტკიცედ უჭერს მხარს თანამშრომლობას შესაბამის ინდუსტრიაში მოქმედ დაინტერესებულ მხარეებსა და სავაჭრო ასოციაციებს შორის, რათა მათ ერთობლივად განსაზღვრონ ოპერაციული თავსებადობის სტანდარტები და ფორმატები, მონაცემთა პორტირების უფლებასთან დაკავშირებული მოთხოვნების განსახორციელებლად. აღნიშნულ გამოწვევას, აგრეთვე, გამოეხმაურა ევროპის ოპერაციული თავსებადობის ჩარჩო (EIF), რომელმაც შექმნა შეთანხმებული მიდგომა იმ ორგანიზაციების ოპერაციულ თავსებადობასთან დაკავშირებით, რომელთაც საჯარო სერვისების ერთობლივად მიწოდება სურთ. აღნიშნული ჩარჩო მისი მოქმედების სფეროში ადგენს გარკვეულ საერთო ელემენტებს, როგორიცაა: ლექსიკონი, კონცეფციები, პრინციპები, პოლიტიკის მიმართულებები, სახელმძღვანელო მითითებები, რეკომენდაციები, სტანდარტები, მახასიათებლები და პრაქტიკები.[36]

- რა მიდგომები უნდა გამოვიყენოთ პერსონალური მონაცემების ფართო ან კომპლექსურ ჩანაწერთან მიმართებით?

GDPR-ი არ განმარტავს ისეთ მოთხოვნებზე რეაგირების გზებს, რომლებიც დაკავშირებულია მონაცემთა ფართო ჩანაწერთან, მონაცემთა კომპლექსურ სტრუქტურასთან ან სხვა ტექნიკურ პრობლემებთან, რომლებიც გარკვეულ სირთულეებს ქმნიან დამუშავებისთვის პასუხისმგებელი პირებისთვის ან მონაცემთა სუბიექტებისთვის.

ამავდროულად, ნებისმიერ შემთხვევაში, უაღრესად მნიშვნელოვანია, რომ ფიზიკურ პირს შეეძლოს, სრულფასოვნად გაიაზროს იმ პერსონალური მონაცემების განმარტება, სქემა და სტრუქტურა, რომლის მიწოდებაც დამუშავებისთვის პასუხისმგებელ პირს შეუძლია. მაგალითად, თავდაპირველად მონაცემების მიწოდება შესაძლებელია

[36] წყარო: http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf.

შემოკლებული ფორმით, დაფების (dashboards) გამოყენებით, რაც მონაცემთა სუბიექტს საშუალებას მისცემს, მოახდინოს პერსონალური მონაცემების ამონარიდების (ქვეჯგუფის) პორტირება, ნაცვლად მთლიანი მონაცემებისა. დამუშავებისთვის პასუხისმგებელ პირს უნდა შეეძლოს ზოგადი მიმოხილვის მიწოდება „მოკლე, გამჭვირვალე, გასაგები და მარტივად ხელმისაწვდომი ფორმით, ნათელი და მარტივი ენით“ (იხ. GDPR-ის 12(1) მუხლი), იმგვარად, რომ მონაცემთა სუბიექტს ყოველთვის ჰქონდეს მკაფიო ინფორმაცია იმის შესახებ, თუ რა მონაცემები უნდა ჩამოტვირთოს ან გადასცეს სხვა დამუშავებისთვის პასუხისმგებელ პირს, დამუშავებისთვის პასუხისმგებელ პირსკონკრეტულ მიზანთან მიმართებით. მაგალითად, მონაცემთა სუბიექტებს უნდა შეეძლოს კომპიუტერული აპლიკაციების გამოყენება, რათა აპლიკაციებიდან სპეციფიური მონაცემების ადვილად იდენტიფიცირება, ცნობა და დამუშავება შეძლონ.

როგორც ზემოთ ითქვა, მონაცემთა პორტირების მოთხოვნებზე რეაგირების პრაქტიკულ გზას წარმოადგენს დამუშავებისთვის პასუხისმგებელი პირის მიერ სათანადოდ დაცული და დოკუმენტირებული API-ს შეთავაზება. აღნიშნული ფიზიკურ პირებს საშუალებას მისცემს, დამუშავებისთვის პასუხისმგებელ პირებს მიმართონ საკუთარი პერსონალური მონაცემების მისაღებად, საკუთარი ან მესამე მხარის კომპიუტერული პროგრამით ან სხვებს მისცენ ნებართვა, მონაცემთა სუბიექტის სახელით მოითხოვონ მისი მონაცემები (მათ შორის, სხვა დამუშავებისთვის პასუხისმგებელ პირს), GDPR-ის 20(2) მუხლის შესაბამისად. გარედან ხელმისაწვდომი API-ს საშუალებით მონაცემებზე წვდომის მინიჭებით, შესაძლებელია წვდომის უფრო დახვეწილი სისტემის შეთავაზება, რომელიც ფიზიკურ პირებს საშუალებას აძლევს, შემდგომაც მოითხოვონ მონაცემები, მონაცემთა სრულად ჩამოტვირთვით ან დელტა ფუნქციის სახით, რომელიც შეიცავს მხოლოდ ბოლო ჩამოტვირთვის შემდგომ განხორციელებულ ცვლილებებს, ხოლო აღნიშნული დამატებითი მოთხოვნები დამუშავებისთვის პასუხისმგებელ პირს არ დააკისრებს ტვირთს.

- როგორ დავიცვათ პორტირებადი მონაცემები?

ზოგადად, GDPR-ის 5(1)(f) მუხლის თანახმად, დამუშავებისთვის პასუხისმგებელმა პირებმა უნდა უზრუნველყონ მონაცემების სათანადო უსაფრთხოება, მათ შორის, უკანონო და არაუფლებამოსილი პირების მიერ დამუშავების, შემთხვევით დაკარგვის, განადგურების ან დაზიანებისგან დაცვა, სათანადო ტექნიკური ან ორგანიზაციული ზომების გამოყენებით.

ამავდროულად, მონაცემთა სუბიექტისათვის პერსონალური მონაცემების გადაცემა, შესაძლოა, წარმოშობდეს უსაფრთხოებასთან დაკავშირებულ გარკვეულ პრობლემებს:

<u>როგორ უნდა უზრუნველყოს</u> დამუშავებისთვის პასუხისმგებელმა პირმა <u>პერსონალური მონაცემების უსაფრთხოდ მიწოდება შესაბამისი პირისთვის?</u>

ვინაიდან მონაცემთა პორტირების მიზანია, პერსონალური მონაცემები დამუშავებისთვის პასუხისმგებელი პირის საინფორმაციო სისტემიდან გადაიტანოს, გადაცემამ შესაძლოა აღნიშნულ მონაცემებს გარკვეული საფრთხე შეუქმნას (კერძოდ, გადაცემის დროს შესაძლოა დარღვეული იქნას მონაცემთა უსაფრთხოება). დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია, მიიღოს უსაფრთხოების ყველა ის ზომა, რომელსაც მოითხოვს შესაბამისი მხარისათვის პერსონალური მონაცემების უსაფრთხოდ გადაცემა (გამოიყენოს ვინაობის დადგენის მყარი ზომები და გამჭოლი (end-to-end) დაშიფრვა ან მონაცემთა დაშიფრვა). ამავდროულად, მან უნდა გააგრძელოს იმ პერსონალური მონაცემების დაცვა, რომელიც რჩება მათ სისტემებში და გამჭვირვალე პროცედურების გამოყენება მონაცემთა უსაფრთხოების დარღვევის შესაძლო შემთხვევებზე რეაგირებისთვის.[37] როგორც ასეთი, დამუშავებისთვის პასუხისმგებელმა პირმა უნდა შეაფასოს ის კონკრეტული რისკები, რომლებიც დაკავშირებულია მონაცემთა პორტირებასთან და მიიღოს სათანადო ზომები რისკის შესამცირებლად.

რისკის შემცირების ზომები, შესაძლოა, მოიცავდეს შემდეგს: თუ საჭიროა მონაცემთა სუბიექტის ვინაობის დადგენა, ვინაობის დასადგენად დამატებითი ინფორმაციის გამოყენება, როგორიცაა, საერთო საიდუმლო ან ამოცნობის სხვა ფაქტორი, როგორიცაა, ერთჯერადი პაროლი; გადაცემის შეწყვეტა ან „გაყინვა“ ანგარიშის გატეხვის შემთხვევაში; პერსონალური მონაცემების ერთი დამუშავებისთვის პასუხისმგებელი პირის მიერ მეორესთვის პირდაპირ გადაცემის შემთხვევაში, გამოყენებული უნდა იქნას სავალდებულო ამოცნობა, როგორიცაა, ტოკენზე დაფუძნებული ამოცნობა.

უსაფრთხოების ამგვარი ზომები არსებითად არ უნდა ქმნიდეს დაბრკოლებას და მომხმარბელებს არ უნდა უზღუდავდეს თავიანთი უფლებების განხორციელების შესაძლებლობას, მაგ., დამატებითი საფასურის დაწესების გზით.

<u>როგორ დავეხმაროთ მომხმარებლებს თავიანთ სისტემებში საკუთარი პერსონალური მონაცემების უსაფრთხოდ დაცვის კუთხით?</u>

როდესაც საქმე ეხება ონლაინ მომსახურებიდან მომხმარებლის მიერ საკუთარი პერსონალური მონაცემების მიღებას, ყოველთვის არსებობს რისკი, რომ მომხმარებელი ამ მონაცემებს შეინახავს სისტემაში, რომელიც ონლაინ მომსახურების სისტემასთან შედარებით, ნაკლებად არის დაცული. საჭიროა მომხმარებლის ინფორმირება აღნიშნულის შესახებ, რათა მან გადადგას ნაბიჯები მიღებული ინფორმაციის დასაცავად. საუკეთესო პრაქტიკის მაგალითის სახით, დამუშავებისთვის პასუხისმგებელი პირები რეკომენდაციას უწევენ სათანადო ფორმატ(ებ)ს, დაშიფრვის ინსტრუმენტებს და უსაფრთხოების სხვა ზომებს, რომლებიც მონაცემთა სუბიექტს ამ მიზნის მიღწევაში დაეხმარება.

[37] (EU) 2016/1148 დირექტივის შესაბამისად, რომელიც ეხება ევროკავშირში საინფორმაციო სისტემებისა და ქსელის უსაფრთხოების საერთო ზომებს.

შესრულებულია ბრიუსელში, 2016 წლის 13 დეკემბერს

სამუშაო ჯგუფის სახელით,

თავმჯდომარე

ისაბელ ფალკე-პიეროტინი

ბოლო გადახედვისა და მიღების თარიღი: 2017 წლის 5 აპრილი

სამუშაო ჯგუფის სახელით,

თავმჯდომარე

ისაბელ ფალკე-პიეროტინი

სახელმძღვანელო რეკომენდაცია მონაცემთა პორტირების უფლების შესახებ

WP242 rev.01 / მიღების თარიღი: 2016 წლის 13 დეკემბერი

დანართი: ხშირად დასმული კითხვები

1. რა მიზანი აქვს მონაცემთა პორტირების უფლებას?

მონაცემთა პორტირება მონაცემთა სუბიექტებს შესაძლებლობას აძლევს, მოიპოვონ და ხელახლა გამოიყენონ „თავიანთი“ მონაცემები, საკუთარი მიზნებისთვის და სხვადასხვა მომსახურებებთან დაკავშირებით. ეს უფლება ხელს უწყობს მათ შესაძლებლობას, პერსონალური მონაცემები და მათი ასლები ადვილად გადაიტანონ ერთი IT (საინფორმაციო-ტექნოლოგიური) გარემოდან მეორე გარემოში, დაბრკოლების გარეშე. იგი განამტკიცებს მომხმარებლის პოზიციას, რადგან გამორიცხავს მონაცემების ერთ მომწოდებელთან შეჩერების შესაძლებლობას და ამავდროულად, ხელს უწყობს ინოვაციის შესაძლებლობებს და პერსონალური მონაცემების გაზიარებას დამუშავებისთვის პასუხისმგებელ პირებს შორის, უსაფრთხო და დაცული ფორმით, მონაცემთა სუბიექტის კონტროლის ქვეშ.

2. რას ითვალისწინებს მონაცემთა პორტირების უფლება?

პირველ რიგში, იგი მოიცავს იმ პერსონალური მონაცემების მიღების უფლებას („სტრუქტურირებული, ფართოდ გამოყენებადი და ელექტრონულად წაკითხვადი ფორმით“), რომელსაც ამუშავების დამუშავებისთვის პასუხისმგებელი პირი და კერძო მოწყობილობაზე შენახვის უფლებას, შემდგომი პირადი გამოყენებისთვის, მონაცემების დამუშავებისთვის პასუხისმგებელი ერთი პირისგან მეორე პასუხისმგებელი პირისთვის გადაცემის გარეშე. ეს უფლება მონაცემთა სუბიექტებს უადვილებს საკუთარი პერსონალური მონაცემების დამოუკიდებლად მართვას.

მეორე, ეს უფლება მონაცემთა სუბიექტებს აძლევს საკუთარი პერსონალური მონაცემების დამუშავებისთვის პასუხისმგებელი ერთი პირისგან მეორე პასუხისმგებელი პირისთვის გადაცემის შესაძლებლობას, „დაბრკოლების გარეშე“, და ხელს უწყობს მათ შესაძლებლობას, პერსონალური მონაცემები და მათი ასლი ადვილად გადაიტანონ ერთი IT (საინფორმაციო-ტექნოლოგიური) გარემოდან მეორე გარემოში.

3. რა ინსტრუმენტების გამოყენებაა მიზანშეწონილი მონაცემთა პორტირების შესახებ მოთხოვნებზე რეაგირებისთვის?

პირველ რიგში, დამუშავებისთვის პასუხისმგებელი პირი მონაცემთა სუბიექტს უნდა სთავაზობდეს მონაცემთა პირდაპირ ჩამოტვირთვის შესაძლებლობას. მეორე, იგი

მონაცემთა სუბიექტებს უნდა აძლევდეს მონაცემების სხვა პასუხისმგებელი პირისთვის პირდაპირ გადაცემის შესაძლებლობას. აღნიშნულის განხორციელება შესაძლებელია, მაგალითად, „აპლიკაციის პროგრამირების ინტერფეისის“ ხელმისაწვდომობის უზრუნველყოფით.

მონაცემთა სუბიექტებს შეუძლიათ გამოიყენონ მათთვის სანდო მესამე მხარის მომსახურება მონაცემთა შენახვის კუთხით. კერძოდ, მესამე მხარე შეინახავს მათ პერსონალურ მონაცემებს და საჭიროების მიხედვით, დამუშავებაზე პასუხისმგებელ პირს მისცემს მონაცემებზე წვდომისა და მათი დამუშავების შესაძლებლობას. აღნიშნული გააადვილებს მონაცემთა გადაცემას დამუშავებისთვის პასუხისმგებელი ერთი პირისგან მეორე პასუხისმგებელი პირისთვის.

4. დამუშავებისთვის პასუხისმგებელი პირები რამდენად არიან პასუხისმგებლები მონაცემთა პორტირების უფლების განხორციელების შედეგად მიღებულ ან გადაცემულ მონაცემებზე?

დამუშავებისთვის პასუხისმგებელი პირი, რომელიც ასრულებს მონაცემთა პორტირების შესახებ მოთხოვნას, არ არის პასუხისმგებელი მონაცემთა სუბიექტის ან მონაცემთა მიმღები სხვა კომპანიის მიერ პერსონალური მონაცემების დამუშავებაზე. ამავდროულად, დამუშავებისთვის პასუხისმგებელი პირი, რომელიც იღებს მონაცემებს, ვალდებულია, უზრუნველყოს, რომ პორტირებული მონაცემები არის რელევანტური და არ არის გადაჭარბებული, მონაცემთა ახალ დამუშავებასთან მიმართებით; მკაფიოდ მიაწოდოს მონაცემთა სუბიექტს ინფორმაცია ახალი დამუშავების მიზნის შესახებ და ზოგადად, დამუშავების პროცესში მონაცემთა დაცვის პრინციპები გამოიყენოს GDPR-ის დებულებების შესაბამისად.

5. მონაცემთა პორტირების უფლების განხორციელება ახდენს თუ არა გავლენას მონაცემთა სუბიექტის სხვა უფლებებზე?

როდესაც ფიზიკური პირი ახორციელებს მონაცემთა პორტირების უფლებას (ან GDPR-ით გათვალისწინებულ სხვა უფლებას), ამით ზიანი არ ადგება მის სხვა უფლებებს. მონაცემთა სუბიექტი უფლებამოსილია, განახორციელოს თავისი უფლებები მანამ, სანამ დამუშავებისთვის პასუხისმგებელი პირი ამუშავებს მონაცემებს. მაგალითად, მონაცემთა სუბიექტს შეუძლია, მონაცემთა დამუშავებისთვის პასუხისმგებელი პირის მომსახურება გამოიყენოს და მიიღოს სარგებელი მას შემდეგაც კი, რაც განხორციელდება მონაცემთა პორტირებასთან დაკავშირებული ოპერაცია. თუ მონაცემთა სუბიექტს სურს, განახორციელოს წაშლის უფლება, საკუთარ პერსონალურ მონაცემებზე წვდომის უფლება, მანამდე ან ამის შემდგომ მონაცემთა პორტირების უფლების განხორციელება ვერ იქნება გამოყენებული დამუშავებისთვის პასუხისმგებელი პირის მიერ, როგორც მონაცემთა სუბიექტის სხვა უფლებებზე რეაგირების გაჭიანურების ან რეაგირებაზე უარის თქმის მიზეზი. ამას გარდა,

მონაცემთა პორტირება ავტომატურად არ განაპირობებს დამუშავებისთვის პასუხისმგებელი პირის სისტემებიდან მონაცემების წაშლას და არ ახდენს გავლენას შენახვის თავდაპირველ ვადაზე, რომელიც ვრცელდება მონაცემთა პორტირების უფლების შესაბამისად გადაცემულ მონაცემებზე.

6. როდის მოქმედებს მონაცემთა პორტირების უფლება?

აღნიშნული **ვრცელდება 3 პირობის ერთდროულად არსებობის შემთხვევაში.**

პირველი, პერსონალური მონაცემები უნდა მუშავდებოდეს ავტომატური საშუალებით (რაც გამორიცხავს მატერიალურ ფაილებს), მონაცემთა სუბიექტის მიერ გაცემულ თანხმობაზე დაყრდნობით ან იმ ხელშეკრულების შესრულების პროცესში, რომლის მხარეც არის მონაცემთა სუბიექტი.

მეორე, პერსონალური მონაცემები უნდა ეხებოდეს მონაცემთა სუბიექტს და მის მიერ უნდა იქნას მოწოდებული. WP29-ის რეკომენდაციის თანახმად, დამუშავებისთვის პასუხისმგებელმა პირებმა ზედმეტად ვიწროდ არ უნდა განმარტონ წინადადება „პერსონალური მონაცემები მონაცემთა სუბიექტის შესახებ“, როდესაც მესამე მხარეთა მონაცემებს შეიცავს მონაცემთა ერთობლიობა, რომელიც ეხება მონაცემთა სუბიექტს, ხოლო აღნიშნული მონაცემთა ერთობლიობა მოწოდებულია მონაცემთა სუბიექტის მიერ და გამოიყენება მონაცემთა სუბიექტის პირადი მიზნებისთვის. ამგვარი (მესამე მხარის მონაცემების შემცველი) მონაცემების მაგალითებია სატელეფონო ჩანაწერები (რომელიც შეიცავს შემოსულ და გამავალ ზარებს), რომელთა მიღებაც სურს მონაცემთა სუბიექტს ან საბანკო ანგარიშის ისტორია, რომელიც მოიცავს მესამე მხარეებისგან მიღებული თანხების შესახებ ინფორმაციას.

პერსონალური მონაცემები ითვლება მონაცემთა სუბიექტის მიერ მოწოდებულად, როდესაც ისინი წინასწარი შეცნობით და აქტიურად „არის უზრუნველყოფილი“ მონაცემთა სუბიექტის მიერ, როგორიცაა, ანგარიშის შესახებ მონაცემები (მაგ., საფოსტო მისამართი, მომხმარებლის სახელი, ასაკი), რომლის მიწოდებაც ხდება ონლაინ ფორმების საშუალებით; ასევე, როდესაც მონაცემები წარმოებულია და შეგროვებულია მომხმარებელთა აქტივობების საფუძველზე, მათ მიერ მომსახურების ან მოწყობილობის გამოყენების შედეგად. მეორეს მხრივ, პერსონალურ მონაცემებზე, რომლებიც წარმოებულია ან ნავარაუდევია მონაცემთა სუბიექტის მიერ მოწოდებული მონაცემების საფუძველზე, როგორიცაა, მომხმარებლის პროფილი, რომელიც ჭკვიან მოწყობილობებში არსებული მონაცემების ანალიზის საფუძველზე შეიქმნა, არ ვრცელდება მონაცემთა პორტირების უფლების მოქმედების სფერო, ვინაიდან ისინი არ წარმოადგენენ მონაცემთა სუბიექტის მიერ მიწოდებულ მონაცემებს, არამედ, დამუშავებისთვის პასუხისმგებელი პირის მიერ შექმნილი მონაცემებია.

მესამე პირობის თანახმად, აღნიშნული ახალი უფლების განხორციელებამ უარყოფითი გავლენა არ უნდა იქონიოს მესამე მხარეთა უფლებებზე და თავისუფლებებზე. მაგალითად, თუ მონაცემთა სუბიექტის მოთხოვნის საფუძველზე

გადაცემული მონაცემები შეიცავს სხვა პირებთან დაკავშირებულ პერსონალურ მონაცემებს, ახალმა დამუშავებისთვის პასუხისმგებელმა პირმა ეს მონაცემები უნდა დაამუშაოს მხოლოდ იმ შემთხვევაში, თუ მას სათანადო სამართლებრივი საფუძველი ექნება. როგორც წესი, ასეთი მონაცემების დამუშავება დაშვებულია მხოლოდ პირადი ან ოჯახური აქტივობების ფარგლებში, მხოლოდ მონაცემთა სუბიექტის კონტროლის ქვეშ.

7. როგორ უნდა მოხდეს მონაცემთა სუბიექტების ინფორმირება აღნიშნული ახალი უფლების შესახებ?

დამუშავებისთვის პასუხისმგებელმა პირებმა მონაცემთა სუბიექტებს მონაცემთა პორტირების უფლების არსებობის შესახებ უნდა შეატყობინონ „მოკლე, გამჭვირვალე, გასაგები და მარტივად ხელმისაწვდომი ფორმით, ნათელი და მარტივი ენით". ამ მხრივ, WP29-ის რეკომენდაციის თანახმად, დამუშავებისთვის პასუხისმგებელმა პირებმა მკაფიოდ უნდა განმარტონ მონაცემთა იმ სხვადასხვა ტიპებს შორის არსებული განსხვავება, რომელთა მიღებაც მონაცემთა სუბიექტს შეუძლია მონაცემთა პორტირების უფლების ან მონაცემებზე წვდომის უფლების საშუალებით. დამუშავებისთვის პასუხისმგებელმა პირმა მონაცემთა სუბიექტს სპეციფიური ინფორმაცია მონაცემთა პორტირების უფლების შესახებ, აგრეთვე, უნდა მიაწოდოს ანგარიშის დახურვამდე, რათა მონაცემთა სუბიექტმა შეძლოს მისი პირადი მონაცემების მოპოვება და შენახვა.

ამას გარდა, დამუშავებისთვის პასუხისმგებელი პირები, რომლებიც მონაცემთა სუბიექტის მოთხოვნის საფუძველზე პორტირებულ მონაცემებს იღებენ, საუკეთესო პრაქტიკის სახით, მონაცემთა სუბიექტებს აწვდიან სრულ ინფორმაციას, თუ რა სახის პერსონალური მონაცემებია რელევანტური მათი სერვისების მიწოდებისთვის.

8. დამუშავებისთვის პასუხისმგებელი პირი როგორ მოახდენს მონაცემთა სუბიექტის ვინაობის დადგენას მანამ, სანამ პასუხს გასცემს მის მოთხოვნას?

WP29-ის რეკომენდაციის თანახმად, დამუშავებისთვის პასუხისმგებელმა პირმა უნდა დანერგოს სათანადო პროცედურები, რომლებიც ფიზიკურ პირებს მისცემს შესაძლებლობას, წარადგინონ მონაცემთა პორტირების შესახებ მოთხოვნა და მიიღონ მათ შესახებ მონაცემები. დამუშავებისთვის პასუხისმგებელ პირს უნდა გააჩნდეს მონაცემთა სუბიექტის ავთენტიფიკაციის პროცედურა, რომლის საფუძველზეც იგი მყარად მოახდენს იმ მონაცემთა სუბიექტის დადგენას, რომელიც ითხოვს თავის პერსონალურ მონაცემებს ან ზოგადად, GDPR-ით გათვალისწინებულ უფლებებს ახორციელებს.

9. რა ვადაში უნდა განხორციელდეს რეაგირება მონაცემთა პორტირების მოთხოვნაზე?

მონაცემთა დაცვის ძირითადი რეგულაციის მე-12 მუხლი დამუშავებისთვის პასუხისმგებელ პირს უკრძალავს პერსონალური მონაცემების უზრუნველყოფისთვის რაიმე საფასურის დაწესებას, გარდა იმ შემთხვევისა, თუ დამუშავებისთვის პასუხისმგებელ პირს შეუძლია დაადასტუროს, რომ მოთხოვნა არის ცალსახად დაუსაბუთებელი ან გადაჭარბებული, *„განსაკუთრებით, მისი განმეორებითი ხასიათის გამო.“* საინფორმაციო საზოგადოებისთვის ან მსგავსი ონლაინ სერვისების შემთხვევაში, რომლებიც პერსონალური მონაცემების ავტომატური დამუშავების სფეროში საქმიანობენ, მონაცემთა პორტირების რამდენიმე მოთხოვნაზე რეაგირება იშვიათად თუ ჩაითვლება გადაჭარბებული ტვირთის მომცველად. ასეთ შემთხვევებში, WP29-ის რეკომენდაციის თანახმად, მიზანშეწონილია გონივრული ვადის განსაზღვრა, რომელიც ადაპტირებული იქნება კონტექსტთან და მის შესახებ ინფორმაციის მიწოდება მონაცემთა სუბიექტებისთვის.

10. როგორ უნდა მოხდეს პორტირებული მონაცემების მიწოდება?

პერსონალური მონაცემების გადაცემა უნდა მოხდეს სტრუქტურირებული, ფართოდ გამოყენებადი და ელექტრონულად წაკითხვადი ფორმით. აღნიშნული სპეციფიკაციები, რომლებიც მონაცემთა გადაცემის საშუალებებზე ვრცელდება, უნდა უზრუნველყოფდეს დამუშავებისთვის პასუხისმგებელი პირის მიერ მიწოდებული მონაცემთა ფორმატის ოპერაციულ თავსებადობას. სასურველ შედეგს წარმოადგენს სწორედ ოპერაციული თავსებადობა. ამავდროულად, აღნიშნული არ ნიშნავს იმას, რომ დამუშავებისთვის პასუხისმგებელ პირებს უნდა ჰქონდეთ თავსებადი სისტემები. ამას გარდა, დამუშავებისთვის პასუხისმგებელმა პირებმა მონაცემებთან ერთად უნდა უზრუნველყონ მაქსიმალურად ბევრი მეტა-მონაცემები, მაქსიმალური სიზუსტითა და დეტალურობით, რაც შეინარჩუნებს გაცვლილი ინფორმაციის ზუსტ მნიშვნელობას.

მონაცემთა პოტენციური ტიპების ფართო სპექტრის გათვალისწინებით, რომელთა დამუშავებაც შესაძლებელია დამუშავებისთვის პასუხისმგებელი პირის მიერ, GDPR-ი არ ითვალისწინებს რაიმე სპეციალურ რეკომენდაციებს, თუ რა ფორმატში უნდა იქნას მონაცემები მიწოდებული. ყველაზე შესაფერისი ფორმატი განსხვავდება სექტორების მიხედვით, ხოლო ადეკვატური ფორმატები შესაძლოა უკვე არსებობდეს, თუმცა, მათი არჩევა ყოველთვის უნდა მოხდეს ოპერაციული თავსებადობის მიზნის მისაღწევად.

WP29-ის რეკომენდაციის თანახმად, მიზანშეწონილია, რომ წარმოების სფეროში მომუშავე დაინტერესებულმა მხარეებმა და სავაჭრო ასოციაციებმა ერთობლივად იმუშაონ საერთო სტანდარტებზე და ფორმატებზე ოპერაციულ თავსებადობასთან დაკავშირებით, მონაცემთა პორტირების უფლებასთან დაკავშირებული მოთხოვნების შესრულებისთვის.