Finaluri

1) რას ნიშნავს მონაცემთა დამუშავება?

მონაცემთა დამუშავება არის ნებისმიერი ქმედება, რომელიც პერსონალური მონაცემების მიმართ ხორციელდება: შეგროვება; აღრიცხვა/ჩაწერა; ორგანიზება; სტრუქტურირება; შენახვა; ადაპტაცია ან შეცვლა; ამოღება; გაცნობა; გამოყენება; გამჟღავნება გადაცემით, გავრცელებით ან სხვაგვარი ხელმისაწვდომობით; დაჯგუფება ან კომბინირება; შეზღუდვა; წაშლა ან განადგურება. არსებობს 2 სახის : ავტომატური და არაავტომატური.

2) რა განსხვავებაა მონაცემთა მიმღებსა და მესამე პირს შორის?

ამ ორ პირს / ორგანიზაციას შორის მთავარი **განსხვავება** ისაა, თუ რა დამოკიდებულება და უფლებები აქვთ მონაცემთა დამმუშავებლის მიმართ - თუ რა დონის უფლება აქვთ, მიიღონ წვდომა დამმუშავებლის ხელში არსებულ ინფორმაციაზე.

მესამე პირი - არის ფიზიკური ან იურიდიული პირი, საჯარო უწყება, დაწესებულება ან სხვა პირი, მონაცემთა სუბიექტის, დამმუშავებლის, უფლებამოსილი ან იმ პირის გარდა, რომელსაც აქვს პერსონალური მონაცემების დამუშავების უფლებამოსილება დამმუშავებლის ან უფლებამოსილი პირის პირდაპირი დავალებით.

მონაცემთა მიმღებია - გულისხმობს ფიზიკურ ან იურიდიულ პირს, საჯარო დაწესებულებას, სააგენტოს ან სხვა უწყებას, რომელსაც გადაეცემა პერსონალური მონაცემები, მიუხედავად იმისა, მესამე პირია თუ არა.“ მონაცემთა მიმღები შეიძლება იყოს პირი, რომელიც არ არის დაკავშირებული მონაცემთა დამმუშავებელსა ან უფლებამოსილ პირთან (შესაბამისად, იგი მესამე პირად ჩაითვლება), ან პირიქით, უკავშირდება მათ (მაგ.: იმავე კომპანიის ან უწყების სხვა განყოფილების წარმომადგენელი).

მონაცემთა დამმუშავებლის ან უფლებამოსილი პირის თანამშრომელი შეიძლება იყოს პერსონალურ მონაცემთა მიმღები, რომელზეც დამატებითი სამართლებრივი მოთხოვნები არ ვრცელდება, თუკი ის ჩართულია დამმუშავებლის ან უფლებამოსილი პირის მიერ წარმოებულ მონაცემთა დამუშავების ოპერაციებში. ამავდროულად, მესამე პირს, რომელიც არ არის დაკავშირებული მონაცემთა დამმუშავებელსა ან უფლებამოსილ პირთან, არ აქვს მათ მიერ დამუშავებული მონაცემების გამოყენების უფლება, თუ კონკრეტულ საქმეში არ არსებობს სპეციფიკური სამართლებრივი საფუძვლები.

3) რას გულისხმობს მონაცემთა უსაფრთხოების მაღალი დონის უზრუნველყოფა?

მონაცემთა დამმუშავებელმა და უფლებამოსილმა პირმა უნდა მიიღონ სავარაუდო რისკების შესაბამისი ტექნიკური და ორგანიზაციული ზომები, უსაფრთხოების მაღალი დონის უზრუნველსაყოფად. ეს ზომები მოიცავს შემდეგ ასპექტებს: მონაცემთა ფსევდონიმიზაცია და დაშიფვრა; დამუშავების მუდმივი კონფიდენციალობა, ხელშეუხებლობა, ხელმისაწვდომობა და მოქნილობა; შესაბამისი ზომების ეფექტიანობის შეფასება და შემოწმება; ფიზიკური ან ტექნიკური ინციდენტის შემთხვევაში, დამუშავების პროცესის დროული აღდგენა.

მუდმივად უნდა ხდებოდეს დამუშავების კონფედენციალურობის დონის შემოწმება და ასევე იმის შემოწმება, თუ ესადაგება დაცვის იმჟამინდელი დონე, იმჟამინდელ □ტანდარტს. ინფორმაცია ისე უნდა დამუშავდეს, რომ მასში უცხო პირმა ვერ შეძლოს შეღწევა, ინფორმაციის შეცვლა, წაშლა, გაზიარება. ასევე უსაფრთოხების მაღალი დონე საჭიროა იმისთვისაც, რომ თუნდაც ავტორიზირებულმა პირმა ვერ შეძლოს მონაცემების იმგვარი დამუშავება, რომელიც სცდება დამუშავების მიზნების და ამოცანების ფარგლებს.

4) რა არის მონაცემთა დაცვის ოფიცრის ფუნქცია?

მონაცემთა დაცვის ოფიცერი (DPO) არის პირი, რომელიც დამმუშავებელ ორგანიზაციას აწვდის რჩევებს მონაცემთა დაცვის წესებთან შესაბამისობაზე. ის „ანგარიშვალდებულების ქვაკუთხდია“, ვინაიდან ხელს უწყობს შესაბამისობას და, ამავდროულად, მოქმედებს, როგორც შუამავალი საზედამხედველო ორგანოებს, მონაცემთა სუბიექტებსა და დამნიშნავ ორგანიზაციას შორის.

ის ერთგვარი „ხიდია“ მონაცემთა დამმუშავებელს, მის ზედამხედველ ორგანიზაციებსა და იმ სუბიექტს შორის, ვისი პერსონალური ინფორმაციის დამუშავებაც ხდება. მონაცემთა ოფიცერს აქვს ვალდებულება, უზრუნველყოს რომ პირის პერსონალური ინფორმაცია მუშავდება კონვენციის მიერ გამოცემული კანონის თანახმად, დამამუშავებელი ორგანიზაციის მიერ.

5) რას ნიშნავს მონაცემთა დაცვის რისკების შეფასება?

მაშინ როდესაც მონაცემთა დამამუშავებელი ორგანიზაციები ამუშავებენ პირის პერსონალურ ინფორმაციას, იქმნება საფრთხე, რომ ეს ინფორმაცია გაიჟონოს, გადაკეთდეს, არაავტორიზებულ პირთა ხელში მოხვდეს და ასე შემდეგ... რისკები განსხვავდება და დამოკიდებულია დამუშავების ბუნებასა და მასშტაბზე. როგორც ევროპის საბჭო, ისე ევროკავშირი ავალდებულებს ხელშემკვრელ მხარეებს, რომ შეაფასონ ის რიკები, რომლებიც ზემოხსენებულმა საფრთხეება შეიძლება შეუქმნან მონაცემთა სუბიექტის უფლებებსა და ფუნდამენტურ თავისუფლებებს. პირველ რიგში, უნდა შეფასდეს რისკები, ამის შემდეგ კი უნდა იქნას შემუშავებული ისეთი მოდელი, რომელიც მაქსიმალურად მოახდენს რისკების თავიდან აცილებას ან მინიმუმამდე დაყვანას.

საქმე Y v. Turkey რა ტიპის შესაძლო დარღვევას ეხებოდა და სასამართლომ რა გადაწყვეტილება მიიღო?

განმცხადებელს ჰქონდა აივ დადებითი სტატუსი. კონკრეტული სიტუაციის შემდეგ, მისი საავადმყოფოში გადაყვანა გახდა საჭირო, სადაც ექიმებს მისი აივ სტატუსის გაცხადება მოუწიათ, რადგან განმაცხადებელი აღნიშნულ მომენტში უგონოდ იყო. განმცხადებელმა კი განცხადება გააკეთა იმიტომ, რომ არ სურდა, მისი აივ სტატუსი გასაჯაროებულიყო.

ამ საქმეში სასამართლომ განმცხადებლის უფლებები დარღვეულად არ სცნო, ვინაიდან განმაცხადებელი აღნიშნულ მომენტში უგონოდ იყო, საავადმყოფოს პერსონალს კი გადაუდებელი დახმარების გასაწევად მისი აივ სტატუსის გაცხადება დასჭირდა.

GDPR-ის მე-6 მუხლის თანახმად, სუბიექტის განსაკუთრებული კატეგორიის პერს. მონაცემების დამუშავება დაშვებულია იმ შემთხვევაში, თუ ეს მის სასიცოცხლო ინტერესებს იცავს. □ოწრედ ეს მუხლი გახდა საჩივრის გაბათილების საფუძველი.

Dalshe

1) შეიძლება თუ არა ზოგადად განსაკუთრებული კატეგორიის მონაცემების დამუშავება? ზოგადად, განსაკუთრებული კატეგორიის მონაცემების დამუშავება აკრძალულია. გარდა გამონაკლისი შემთხვევებისა:

- როცა პირის განსაკუთრებული კატეგორიის მონაცემების დამუშავება აუცილებელია მისივე სასიცოცხლო ინტერესებისთვის ან მნიშვნელოვანი საჯარო ინტერესებისთვის.
- არსებობს მონაცემთა სუბიექტის მკაფიო თანხმობა დამუშავებაზე;
- მონაცემებს ამუშავებს არაკომერციული ორგანიზაცია
- დამუშავება მოიცავს ისეთ მონაცემებს, რომლებიც თვითონ სუბიექტმა საჯაროდ გამოაქვეყნა;
- მონაცემთა სუბიექტის მკაფიო თანხმობა
- მონაცემთა სუბიექტის სასიცოცხლო ინტერესები
- საქველმოქმედო ან არაკომერციული ორგანიზაციები
- მონაცემთა სუბიექტის მიერ ცალსახად საჯაროდ გამოქვეყნებული მონაცემები
- სამართლებრივი მოთხოვნები

2) რა შემთხვევაში მიიჩნევა მონაცემთა სუბიექტის მიერ მონაცემები ცალსახად საჯაროდ გამოქვეყნებულად?

ცალსახად საჯაროდ გამოქვეყნებული მონაცემების შინაარსი უნდა გავიგოთ, როგორც მონაცემთა სუბიექტის მიერ საკუთარი მონაცემების განზრახ გამოქვეყნება საჯაროდ. იმ

შემთხვევაში, თუ მონაცემთა სუბიექტიოს მეერ გამოქვეყნებულ ინფორმაციას ცალსასხად ეტყობა, რომ ის მისი გაცნობიერებული სურვილითაა გამოქვეყნებული. მაგ: სოც ქსელში ატვირთული კონტენტი და სხვა...

3) შესაძლოა თუ არა სამართლებრივი მოთხოვნის საფუძველზე განსაკუთრებული კატეგორიის მონაცემების დამუშავება?

კი, ვროპის საბჭოს 108-ე კონვენცია, გარდა იმისა, რომ უზრუნველყოფს პერსონალურ მონაცემთა დამუშავების გარანტიებისა და უსაფრთხოების ვალდებულებებს, კრძალავს განსაკუთრებული კატეგორიის მონაცემთა (როგორიცაა: პიროვნების რასობრივი კუთვნილება, პოლიტიკური შეხედულებები, ჯანმრთელობის მდგომარეობა, რელიგია, სქესობრივი ცხოვრება და ნასამართლობა) დამუშავებას დაცვის სათანადო სამართლებრივი მექანიზმის გარეშე. გარდა შემთხვევებისა როცა დამმუშავებელმა თავისი ნებით გაასაჯორვა ინფორმაცია.

4) რას გულისხმობს მნიშვნელოვანი საჯარო ინტერესის საფუძველზე განსაკუთრებული კატეგორიის მონაცემების დამუშავება?

GDPR-ის მე-9 მუხლის 2(ზ) პუნქტის თანახმად, წევრი სახელმწიფოს დაშვების საფუძველზე დაშვებულია განსაკუთრებული კატეგორიის მონაცემთა დამუშავება, თუკი: ეს აუცილებელია მნიშვნელოვანი საჯარო ინტერესიდან გამომდინარე;

5) მონაცემთა სუბიქტის სასიცოცხლო ინტერესის გათვალისწინებით შეიძლება თუ არა განსაკუთრებული კატეგორიის მონაცემების დამუშავება?

თუ მონაცემთა სუბიექტის სასიცოცხლო ინტერესებს საფრთხე ემუქრება და თვით მონაცემთა სუბიექტს არ აქვს საშუალება, განაცხადოს თანხმობა (უგონოდაა, მიუწვდომელია, არ იმყოფება საღ გონებაზე და ა.ს.შ) შესაძლებელია. ევროკავშირის სამართალში GDPR-ის მე-6 მუხლის 1(დ) პუნქტის თანახმად, მონაცემთა დამუშავება კანონიერია, თუ ეს „აუცილებელია მონაცემთა სუბიექტის ან სხვა ფიზიკური პირის სასიცოცხლო ინტერესების დასაცავად.“ ამ კანონიერი საფუძვლის გამოყენება შესაძლებელია მხოლოდ იმ შემთხვევაში, თუ დამუშავება „ცალსახად ვერ მოხდება სხვა სამართლებრივი საფუძვლით.“ ზოგჯერ, ასეთი დამუშავება შესაძლოა დაეფუძნოს როგორც საჯარო ინტერესებს, ისე მონაცემთა სუბიექტის ან სხვა პირის სასიცოცხლო ინტერესებს (მაგ.: ეპიდემიებისა და მათ განვითარებაზე მონიტორინგის, ან ჰუმანიტარული კრიზისის შემთხვევაში).

6) რა ტიპის პერსონალური მონაცემები შეიძლება მივიჩნიოთ განსაკუთრებული კატეგორიის პერსონალურ მონაცემებად?

როგორც ევროკავშირის, ისე ევროპის საბჭოს კანონმდებლობის მიხედვით, არსებობს პერსონალურ მონაცემთა განსაკუთრებული კატეგორიები, რომლებიც, თავიანთი ბუნებიდან გამომდინარე, დამუშავებისას შეიძლება შეიცავდეს რისკებს მონაცემთა

სუბიექტებისათვის. შესაბამისად, ისინი საჭიროებს გაძლიერებულ დაცვას. ამგვარ მონაცემებზე ვრცელდება აკრძალვის პრინციპი და მათი დამუშავება კანონის თანახმად ნებადართულია მხოლოდ შეზღუდული რაოდენობით. ეს შეიძლება იყოს: პიროვნების რასობრივი კუთვნილება, პოლიტიკური შეხედულებები, ჯანმრთელობის მდგომარეობა, რელიგია, სქესობრივი ცხოვრება და ნასამართლობა.

7) რას გულისხმობს მონაცემთა ავტომატური დამუშავება?

ევროკავშირის სამართალში მონაცემთა ავტომატური დამუშავება გულისხმობს ქმედებებს, რომლებიც ხორციელდება „მონაცემთა მიმართ სრულად ან ნაწილობრივ ავტომატური საშუალებებით.195 მოდერნიზებული 108-ე კონვენცია შეიცავს ასეთივე განმარტებას. პრაქტიკაში ეს ნიშნავს, რომ პერსონალურ მონაცემთა ნებისმიერი სახის დამუშავებაზე ავტომატური საშუალებებით (მაგ.: პერსონალური კომპიუტერის, მობილური მოწყობილობის ან როუტერის დახმარებით) ვრცელდება როგორც ევროკავშირის, ისე ევროპის საბჭოს მონაცემთა დაცვის წესები.

8) რას ნიშნავს მონაცემთა არაავტომატური დამუშავება?

მონაცემთა არაავტომატური დამუშავება ასევე საჭიროებს მონაცემთა დაცვას. ევროკავშირის სამართლის თანახმად, მონაცემთა დამუშავება მხოლოდ ავტომატური დამუშავებით არ შემოიფარგლება. შესაბამისად, ამ კანონმდებლობით, მონაცემთა დაცვა ეხება პერსონალური მონაცემების დამუშავებას არაავტომატურ ფაილურ სისტემაში - სპეციალური სტრუქტურის მქონე საქაღალდეში. სტრუქტურიზებული ფაილური სისტემა უზრუნველყოფს პერსონალურ მონაცემთა კატეგორიზაციას და მათზე ხელმისაწვდომობას გარკვეული კრიტერიუმების საფუძველზე. მაგალითად, თუ დამსაქმებელი აწარმოებს საქაღალდეს „დასაქმებულთა შვებულება“, რომელიც შეიცავს დეტალურ ინფორმაციას გასული წლის განმავლობაში თანამშრომელთა შვებულების შესახებ, დალაგებულს ანბანის მიხედვით, ასეთი ფაილი ითვლება არაავტომატურ ფაილურ სისტემად, რომელზეც ვრცელდება ევროკავშირის მონაცემთა დაცვის წესები. ამას რამდენიმე მიზეზი აქვს. კერძოდ:

- ფაილების სტრუქტურიზება შესაძლებელია იმგვარად, რომ მოხერხდეს ინფორმაციის სწრაფად და ადვილად მოძიება;
- პერსონალური მონაცემების შენახვა საქაღალდეებში აიოლებს იმ შეზღუდვების აცილებას, რომლებიც კანონმდებლობით გათვალისწინებულია მონაცემთა ავტომატური დამუშავებისათვის.

9) რა განსხვავებაა მონაცემთა დამმუშავებელსა და უფლებამოსილ პირს შორის?

მონაცემთა დამმუშავებელსა და უფლებამოსილ პირს შორის მნიშვნელოვანი განსხვავებაა: პირველი გახლავთ იურიდიული ან ფიზიკური პირი, რომელიც განსაზღვრავს დამუშავების მიზნებსა და საშუალებებს, მეორე კი - იურიდიული ან ფიზიკური პირი, რომელიც მონაცემებს ამუშავებს დამმუშავებლის სახელით, მკაცრად განსაზღვრული ინსტრუქციების

საფუძველზე. ზოგადად, დამუშავებაზე კონტროლი მონაცემთა დამმუშავებელმა უნდა განახორციელოს, სწორედ მას ეკისრება პასუხისმგებლობა ამ საკითხზე, მათ შორის, სამართლებრივიც. თუმცა, მონაცემთა დაცვის წესების რეფორმასთან ერთად, უფლებამოსილ პირებს დაეკისრათ იმ არაერთი მოთხოვნის შესრულების ვალდებულება, რომლებიც მონაცემთა დამმუშავებლებზე ვრცელდება.

10) რას ნიშნავს მონაცემთა ერთობლივი დამუშავება?

პერსონალურ მონაცემებს ამუშავებს ფიზიკური პირი/პირები ან ორაგნიზაცია/ორგანიზაციები. როდესაც ინფორმაციას ამუშავებს ერთზე მეტი პიროვნება ან ორგანიზაცია, ამას ეწოდება ერთობლივი დამუშავება. სახსენებელია რომ იმ პირებმა/ორგანიზაციებმა, რომლებიც ერთობლივად ამუშავებენ ინფორმაციას, აუცილებლად უნდა აკონტროლონ ერთმანეთი - კანონთან მიმართებაში, ვინაიდან იმ შემთხვევაშიც, თუ ერთ ერთი მაინც ჩაიდენს რაიმე - მარეგულირებელი კანონის საწინააღმდეგოს, ორივე/ყველა მათგანი თანაბრად მიიღებს სასჯელს, მიუხედავად იმისა თუ რა თანაბრობით აქვთ საქმე გადანაწილებული კომპანიებს.

11) რას გულისხმობს უსაფრთხოების უზრუნველყოფის ტექნიკური ზომები?

მონაცემები ისეთ გარემოში უნდა დამუშავდნენ და შეინახონ, რომელიც დაცული იქნება არაავტორიზირებული წვდომისგან, დაკარგვისგან, გაჟონვისაგან. უნდა მოხდეს ინფორმაციის ფსევდონიმიზაცია, დაფარვა, ანონიმიზაცია მუდმივად უნდა ხდებოდეს დამუშავების კონფედენციალურობის დონის შემოწმება და ასევე იმის შემოწმება, თუ ესადაგება დაცვის იმჟამინდელი დონე, იმჟამინდელ სტანდარტს.

12) რას ნიშნავს უსაფრთხოების უზრუნველყოფის ორგანიზებული ზომები?

ყველა თანამშრომლისთათვის ინფორმაციის მუდმივ რეჟიმში და ამომწურავად მიწოდებას იმის შესახებ თუ როგორ უნდა დამუშავდეს პირის ინფორმაცია, მისი კონფედენციალურობის დაცვით + ამის გარანტის გაცემა. პასუხისმგებლობის მკაფიოდ ჩამოყალიბება და გადანაწილება, იმაზე ხაზის გასმა, რომ პირის, ინფორმაცია უნდა დამუშავდეს მხოლოდ უფლებამოსილი პირების ან ზოგადი წესის მიხედვით, პერს. ინფორმაციაზე წვდომა მხოლოდ უფლებამოსილ პირებს, ამ წვდომის აღრიცხვა ელექტრონული საშუალებებით და ა.ს.შ.

13) რა არის უსაფრთხოების მაღალი დონის უზრუნველყოფის მიზანი?

მონაცემთა დამმუშავებელმა და უფლებამოსილმა პირმა უნდა მიიღონ სავარაუდო რისკების შესაბამისი ტექნიკური და ორგანიზაციული ზომები, უსაფრთხოების მაღალი დონის უზრუნველსაყოფად. ეს ზომები მოიცავს შემდეგ ასპექტებს: მონაცემთა ფსევდონიმიზაცია და დაშიფვრა; დამუშავების მუდმივი კონფიდენციალობა, ხელშეუხებლობა, ხელმისაწვდომობა და მოქნილობა; შესაბამისი ზომების ეფექტიანობის შეფასება და შემოწმება; ფიზიკური ან ტექნიკური ინციდენტის შემთხვევაში, დამუშავების პროცესის დროული აღდგენა.

მუდმივად უნდა ხდებოდეს დამუშავების კონფედენციალურობის დონის შემოწმება და ასევე იმის შემოწმება, თუ ესადაგება დაცვის იმჟამინდელი დონე, იმჟამინდელ □ტანდარტს. ინფორმაცია ისე უნდა დამუშავდეს, რომ მასში უცხო პირმა ვერ შეძლოს შეღწევა, ინფორმაციის შეცვლა, წაშლა, გაზიარება. ასევე უსაფრთოხების მაღალი დონე საჭიროა იმისთვისაც, რომ თუნდაც ავტორიზირებულმა პირმა ვერ შეძლოს მონაცემების იმგვარი დამუშავება, რომელიც სცდება დამუშავების მიზნების და ამოცანების ფარგლებს.

14) რას გულისხმობს კომუნიკაციების კონფიდენციალურობა?

კომუნიკაციის კონფედენციალურობა ცალკე სტანდარტით (lex specialis) რეგულირდება. კომუნიკაციების კონფიდენციალობა გულისხმობს მოსმენის, მიყურადების, შენახვის, თვალთვალის, ასევე, კომუნიკაციასა და მეტამონაცემებზე მონიტორინგის პრინციპულად აკრძალვას. დირექტივა კრძალავს არასასურველ კომუნიკაციებსაც (ე.წ. spam-ს), გარდა იმ შემთხვევისა, როცა არსებობს მომხმარებლის თანხმობა, და ადგენს წესებს კომპიუტერებსა და მოწყობილობებზე ე.წ. „cookie ჩანაწერების“ (cookies) შენახვასთან მიმართებით. ეს ძირითადი უარყოფითი მოვალეობები მკაფიოდ მიუთითებს, რომ კომუნიკაციების კონფიდენციალობა მნიშვნელოვნად უკავშირდება პირადი ცხოვრების პატივისცემის უფლებას, რომელსაც ითვალისწინებს ქარტიის მე-7 მუხლი, და პერსონალურ მონაცემთა დაცვის უფლებას, გარანტირებულს ქარტიის მე-8 მუხლით.

15) რა არის პერსონალურ მონაცემთა უსაფრთხოების დარღვევის შესახებ შეტყობინების ვალდებულების მიზანი?

მონაცემების დამუშავებაზე სრულ პასუსხისმგებლობას უნდა იღებდეს დამმუშავებელი, იმის შესახებ რომ ინფორმაცია დამუშავდება კანონის დაცვით, არ მოხვდება არაავტორიზირებული პირის ხელში და არ დაექვემდებარება არასანქცირებულ გამოყენებას. თუმცა არსებობს შემთხვევები, როცა დამმუშავებელი ვერ იცავს პირად ინფორმაციას ამისგან. ამ დროს აუცილებლად უნდა მოხდეს შესაბამისი ორგანოების ინფორმირება და გადაეცეს ის შესაძლო უმცირესი ინფორმაცია, რომლის საშუალებითაც შესაძლოა მოხდეს გაჟონილი ინფორმაციის მიგნება და არაავტორიზებული წვდომისა და გაზიარების აღმოფხვრა. მაგ „მონაცემთა უსაფრთხოების დარღვევის ბუნება; მონაცემთა სუბიექტების კატეგორიები და რაოდენობა; დარღვევის მოსალოდნელი შედეგები; მონაცემთა დამმუშავებლის მიერ მიღებული ზომები დარღვევის აღმოსაფხვრელად ან მისი შედეგების შესამცირებლად. ამასთან ერთად აღნიშნულში უნდა იყოს იმ პირზე ინფორმაცია მითითებული, რომელსაც გადაეცემა აღნიშნული ინფორმაცია.

16) რა შემთხვევაში შეიძლება მიმღები იყოს მესამე პირი/მხარე

მონაცემთა მიმღები შეიძლება იყოს პირი, რომელიც არ არის დაკავშირებული მონაცემთა დამმუშავებელსა ან უფლებამოსილ პირთან (შესაბამისად, იგი მესამე პირად ჩაითვლება).

17) რა შემთხვევებშია მონაცემთა დამუშავება კანონიერი?

GDPR-ის თანახმად, მონაცემთა დამუშავება კანონიერია, თუ არსებობს:

- მონაცემთა სუბიექტის თანხმობა;
- ხელშეკრულების დადების საჭიროება;
- სამართლებრივი ვალდებულება;
- მონაცემთა სუბიექტის ან სხვა ფიზიკური პირის სასიცოცხლო ინტერესების დაცვის საჭიროება;
- საჯარო ინტერესში შემავალი ამოცანების შესრულების საჭიროება;
- მონაცემთა დამმუშავებლის ან მესამე პირის კანონიერი ინტერესების დაცვის საჭიროება, გარდა იმ შემთხვევისა, როდესაც მონაცემთა სუბიექტის უფლებები და ინტერესები აღემატება მათ.

18) მოკლედ ისაუბრეთ შემდეგ საქმეზე: K.H. and Others v. Slovakia (რომელი უფლების დარღვევაზეა საუბარი და რა დაადგინა სასამართლომ).

ამ საქმეში ბოშა ქალებმა, რომლებმაც მშობიაროზისას დახმარება მიიღეს აღმოსავლეთ სლოვაკეთის საავადმყოფოებისგან, ვეღარ შეძლეს დაორსულება. სასამართლომ საავადმყოფოებს მოსთხოვა სამედიცინო ჩანაწერების გადმოცემა, საავადმყოფოებმა ამ მოთხოვნაზე უარი განაცხადეს, იმ მიზეზით რომ შესაძლოა ჩანაწერები არასწორ ხელში ჩავარდნილიყო და ბოროტად ყოფილიყო გამოყენებული. ისინი არღვევდნენ ადამიანის უფლებათა ევროპული სასამართლოს (Ecthr) მე-8 მუხლს, რომლიც სახელმწიფოებს პოზიტიურად ავალდებულებს, პერსონას თავისი პირადი ინფორმაციის ასლები გაუზიაროს ან გონივრული მიზეზის შემთხვევაში უარი უთხრას მას. ამ კონკრეტულ შემთხვევაში კი უარისთვის მყარი მიზეზი არ არსებობდა.

19) რას გულისხმობს პერსონალური მონაცემების სამართლიანად დამუშავება?

- პერსონალური მონაცემები უნდა დამუშავდეს სამართლიანად. მონაცემთა სუბიექტი ინფორმირებული უნდა იყოს რისკების შესახებ, რათა დამუშავებას არ მოჰყვეს გაუთვალისწინებელი უარყოფითი შედეგები.
- დამმუშავებელმა მონაცემთა სუბიექტებსა და ფართო საზოგადოებას უნდა შეატყობინოს, რომ მონაცემებს ამუშავებს კანონიერად და გამჭვირვალედ. მან უნდა შეძლოს დადასტურება, რომ დამუშავებასთან დაკავშირებული საქმიანობა შეესაბამება GDPR-ს. დამუშავება არ უნდა განხორციელდეს საიდუმლოდ, ხოლო მონაცემთა სუბიექტებს უნდა ჰქონდეთ ინფორმაცია რისკების შესახებ. ამასთან, მონაცემთა დამმუშავებელმა შეძლებისდაგვარად სწრაფად უნდა შეასრულოს მონაცემთა სუბიექტის სურვილები, განსაკუთრებით, თუ ამ უკანასკნელის თანხმობა ქმნის მონაცემთა დაცვის სამართლებრივ საფუძველს.

20) რას ნიშნავს პერსონალური მონაცემების გამჭვირვალედ დამუშავება?

- მონაცემთა დამუშავებამდე, დამმუშავებელმა მონაცემთა სუბიექტს უნდა შეატყობინოს დამუშავების მიზანი, დამმუშავებლის ვინაობა და მისამართი, სხვა დეტალებთან ერთად
- ინფორმაცია მონაცემთა დამუშავების შესახებ წარმოდგენილი უნდა იყოს გასაგები და მარტივი ენით, რათა მონაცემთა სუბიექტმა ადვილად გაიაზროს შესაბამისი წესები, რისკები, უსაფრთხოების ზომები და უფლებები. მონაცემთა სუბიექტს აქვს მათ მონაცემებზე წვდომის უფლება, დამუშავების ადგილის მიუხედავად.

21) რას გულისხმობს მიზნის შეზღუდვის პრინციპი?

- მონაცემთა დამუშავების მიზანი ნათლად უნდა განისაზღვროს დამუშავების დაწყებამდე.
- დაუშვებელია მონაცემთა შემდგომი დამუშავება იმგვარად, რომ არ შეესაბამებოდეს დამუშავების თავდაპირველ მიზანს. თუმცა, ამ კუთხით მონაცემთა დაცვის ზოგადი რეგულაცია ითვალისწინებს გარკვეულ გამონაკლის შემთხვევებს, საჯარო ან სამეცნიერო/ისტორიული კვლევის ინტერესებიდან, ანდა სტატისტიკური მიზნებიდან გამომდინარე.
- მიზნის შეზღუდვის პრინციპის არსი ის არის, რომ პერსონალური მონაცემები დამუშავდეს კონკრეტული, კარგად განსაზღვრული მიზნით და მხოლოდ თავდაპირველი მიზნის შესაბამისი დამატებითი, კონკრეტული ამოცანებით.

22) რა განსხვავებაა მონაცემთა მინიმიზაციისა და მონაცემთა სიზუსტის პრინციპებს შორის?

მონაცემთა მინიმიზაციის პრინციპი

- მონაცემები უნდა დამუშავდეს მხოლოდ იმ მოცულობით, რომელიც საჭიროა ლეგიტიმური მიზნის მისაღწევად.
- პერსონალურ მონაცემები უნდა დამუშავდეს მხოლოდ იმ შემთხვევაში, როდესაც დამუშავების მიზნის მიღწევა, გონივრულობის ფარგლებში, შეუძლებელია სხვა საშუალებებით.
- მონაცემთა დამუშავება არ უნდა იყოს არაპროპორციული ჩარევა კონკრეტულ ინტერესებში, უფლებებსა და თავისუფლებებში.

მონაცემთა სიზუსტის პრინციპი

- მონაცემთა დამმუშავებელი ვალდებულია, მონაცემთა სიზუსტის პრინციპი დანერგოს დამუშავების ყველა ოპერაციაში.
- არაზუსტი მონაცემები უნდა წაიშალოს, ან დაუყოვნებლივ გასწორდეს.
- შესაძლებელია, საჭირო გახდეს მონაცემთა რეგულარული შემოწმება და განახლება, სიზუსტის დასაცავად.

23) რას ნიშნავს შენახვის ვადის შეზღუდვის პრინციპი?

შენახვის ვადის შეზღუდვის პრინციპი გულისხმობს, რომ პერსონალური მონაცემები უნდა წაიშალოს, ან მოხდეს მათი ანონიმიზაცია, როგორც კი აღარ იქნება საჭირო იმ მიზნებისთვის, რომლებისთვისაც შეგროვდა.

24) რას გულისხმობს მონაცემთა უსაფრთხოების პრინციპი?

- პერსონალურ მონაცემთა უსაფრთხოებასა და კონფიდენციალობას უდიდესი მნიშვნელობა ენიჭება მონაცემთა სუბიექტებზე უარყოფითი გავლენის თავიდან ასაცილებლად.
- უსაფრთხოების ზომები შეიძლება იყოს ტექნიკური და/ან ორგანიზაციული.
- ფსევდონიმიზაცია არის პროცესი, რომელსაც შეუძლია პერსონალური მონაცემების დაცვა.
- უსაფრთხოების ზომის შესაბამისობა უნდა განისაზღვროს თითოეულ შემთხვევაში და რეგულარულად გადაიხედოს.

25) რა არის ანგარიშვალდებულების პრინციპი?

- ანგარიშვალდებულება მოითხოვს მონაცემთა დამმუშავებლისა და უფლებამოსილი პირის მიერ იმ ზომების აქტიურად და მუდმივად გატარებას, რომლებიც ხელს შეუწყობს და განამტკიცებს მონაცემთა დაცვას დამუშავების პროცესში
- მონაცემთა დამმუშავებელი და უფლებამოსილი პირი პასუხისმგებელნი არიან დამუშავების ოპერაციების შესაბამისობაზე მონაცემთა დაცვის კანონმდებლობასა და საკუთარ ვალდებულებებთან.
- დამმუშავებელმა, მონაცემთა სუბიექტის, საზოგადოებისა და საზედამხედველო ორგანოების წინაშე, ნებისმიერ დროს უნდა შეძლოს მონაცემთა დაცვის დებულებებთან შესაბამისობის დადასტურება. უფლებამოსილმა პირმა უნდა შეასრულოს სხვა გარკვეული ვალდებულებებიც, რომლებიც მკაცრად უკავშირდება ანგარიშვალდებულებას (მაგ.: დამუშავების ოპერაციების აღრიცხვა და მონაცემთა დაცვის ოფიცრის დანიშვნა).

26) რას ნიშნავს ნებაყოფლობითი თანხმობა?

თითქმის ყოველთვის, როდესაც ხდება სუბიექტის პერს. მონაცემების დამუშავების საჭიროება, საჭიროა მისგან თანხმობა. თანხმობა ნებაყოფლობითია, როცა „მონაცემთა სუბიექტს აქვს რეალური არჩევანის შესაძლებლობა და არ არსებობს მოტყუების, დაშინების, იძულების ან მნიშვნელოვანი უარყოფითი შედეგების საფრთხე, თუკი უარს იტყვის მის გაცემაზე.

27) რას გულისხმობს ინფორმირებული თანხმობა?

მონაცემთა სუბიექტს მისი მონაცემების დამუშავებისას ხშირად უწევს მნიშვნელოვანი გადაწყვეტილებების მიღება. როდესაც ის ასეთ მდგომარეობაში აღმოჩნდება, სუბიექტი უნდა იყოს ინფორმირებული ყველა დეტალის შესახებ იმ გადაწყვეტილების გარშემო რომელზეც მოეთხოვება პასუხის გაცემა. როგორიცაა დამუშავებული მონაცემების ბუნება, მათი შესაძლო მიმღებები და მონაცემთა სუბიექტების უფლებები. ყოველივე ეს სუბიექტისთვის მკაფიო, გასაგები ენით უნდა იყოს ახსნილი. სუბიექტი უნდა იყოს ინფორმირებული როგორც დამუშავებაზე დადებით, ისევე უარყოფით პასუხის გაცემის შემთხვევაში გამოწვეულ შედეგებზე.

28) რა ტიპის გადაწყვეტილება მიიღო სასამართლომ საქმეში Y v. Turkey და რატომ?

განმცხადებელს ჰქონდა აივ დადებითი სტატუსი. კონკრეტული სიტუაციის შემდეგ, მისი საავადმყოფოში გადაყვანა გახდა საჭირო, სადაც ექიმებს მისი აივ სტატუსის გაცხადება მოუწიათ, რადგან განმაცხადებელი აღნიშნულ მომენტში უგონოდ იყო. განმცხადებელმა კი განცხადება გააკეთა იმიტომ, რომ არ სურდა, მისი აივ სტატუსი გასაჯაროებულიყო.

ამ საქმეში სასამართლომ განმცხადებლის უფლებები დარღვეულად არ სცნო, ვინაიდან განმაცხადებელი აღნიშნულ მომენტში უგონოდ იყო, საავადმყოფოს პერსონალს კი გადაუდებელი დახმარების გასაწევად მისი აივ სტატუსის გაცხადება დასჭირდა.

GDPR-ის მე-6 მუხლის თანახმად, სუბიექტის განსაკუთრებული კატეგორიის პერს. მონაცემების დამუშავება დაშვებულია იმ შემთხვევაში, თუ ეს მის სასიცოცხლო ინტერესებს იცავს. □ოწრედ ეს მუხლი გახდა საჩივრის გაბათილების საფუძველი.

29) რასნიშნავს თანხმობის გამოთხოვის უფლება?

მონაცემთა სუბიექტს პერს. ინფორმაციის დამუშავების ნებისმიერ ეტაპზზე უნდა შეეძლოს საკუთარი ინფორმაციის გამოთხოვა/დამუშავებაზე უარის თქმა. ეს არის მონაცემთა კანონიერი დამუშავების ერთ - ერთი ფუნდამენტური პრინციპი.

30) როგორია კონკრეტული და მკაფიო თანხმობა?

კონკრეტული - თანხმობა უნდა მიემართებოდეს კონკრეტული დამუშავების მიზანს, რომელიც ნათლად და მკაფიოდ არის აღწერილი. ეს მჭიდროდ უკავშირდება თანხმობის

მიზანზე მონაცემთა სუბიექტისათვის მიწოდებული ინფორმაციის ხარისხს. ასეთ კონტექსტში მისი გონივრული მოლოდინები შესაბამისია.
მკაფიო - ყველა თანხმობა უნდა იყოს მკაფიო, კერძოდ, გამოირიცხოს ყოველგვარი გონივრული ეჭვი, რამდენად სურდა მონაცემთა სუბიექტს, გამოეხატა თანხმობა საკუთარი მონაცემების დამუშავებაზე. მაგალითად, მონაცემთა სუბიექტის მხრიდან უმოქმედობა არ აღნიშნავს მკაფიო თანხმობას.

31) დამოუკიდებელი ორგანოს მიზანი?

ევროკავშირის ფუნდამენტურ უფლებათა ქარტიის მე-8 მუხლი არა მხოლოდ განამტკიცებს პერსონალურ მონაცემთა დაცვის უფლებას, არამედ განსაზღვრავს მასთან დაკავშირებულ ძირითად ღირებულებებსაც. ქარტიის თანახმად, პერსონალურ მონაცემთა დამუშავება უნდა იყოს სამართლიანი, ხორციელდებოდეს კონკრეტული მიზნებით, შესაბამისი პირის თანხმობით ან ლეგიტიმური საფუძვლით, რომელსაც ადგენს კანონმდებლობა. ადამიანებს ხელი უნდა მიუწვდებოდეთ თავიანთ პერსონალურ მონაცემებზე და ჰქონდეთ მათი გასწორების შესაძლებლობა, პერსონალურ მონაცემთა დაცვის უფლებასთან შესაბამისობას კი აკონტროლებდეს დამოუკიდებელი ორგანო.

მონაცემთა დაცვის წესების შესრულებას აკონტროლებს დამოუკიდებელი ორგანო. საქართველოში პეროსნალურ მოანაცემთა დაცვის მარეგურილებელი კანონმდებლობის შესრულებასა და მონაცემთა დამუშავების კანონიერებაზე ზედამხედველობას, დამოუკიდებელი საზედამხედველო ორგანო, **პერსონალურ მონაცემთა სამსახური** ახორციელებს. ეს ორგანო:

- გაგიწევთ კონსულტაციას
- მოახდენს მყისიერ რეგაირებას და განიხლავს თქვენს განცხადებას ობიექტურად და მიუკერძოებლად
- შეამოწმებს მონაცემთა დამუშვების კანონიერებას
- დარღვევის აღმოჩენის შემთხვევაში მოახდენს მყისიერ რეაგირებას.

საქმეები

1) Y v. Turkey

განმცხადებელს ჰქონდა აივ დადებითი სტატუსი. კონკრეტული სიტუაციის შემდეგ, მისი საავადმყოფოში გადაყვანა გახდა საჭირო, სადაც ექიმებს მისი აივ სტატუსის გაცხადება მოუწიათ, რადგან განმაცხადებელი აღნიშნულ მომენტში უგონოდ იყო. განმცხადებელმა კი განცხადება გააკეთა იმიტომ, რომ არ სურდა, მისი აივ სტატუსი გასაჯაროებულიყო.

ამ საქმეში სასამართლომ განმცხადებლის უფლებები დარღვეულად არ სცნო, ვინაიდან განმაცხადებელი აღნიშნულ მომენტში უგონოდ იყო, საავადმყოფოს პერსონალს კი გადაუდებელი დახმარების გასაწევად მისი აივ სტატუსის გაცხადება დასჭირდა.

GDPR-ის მე-6 მუხლის თანახმად, სუბიექტის განსაკუთრებული კატეგორიის პერს. მონაცემების დამუშავება დაშვებულია იმ შემთხვევაში, თუ ეს მის სასიცოცხლო ინტერესებს იცავს. □ოწრედ ეს მუხლი გახდა საჩივრის გაბათილების საფუძველი.

2) Digital Rights Ireland-ის საქმე

მაგალითი: Digital Rights Ireland-ის საქმეში CJEU-მ იმსჯელა 2006/24/ EC დირექტივის საფუძვლიანობაზე პერსონალურ მონაცემთა და პირადი ცხოვრების პატივისცემის ფუნდამენტურ უფლებათა ჭრილში, რომელთაც განამტკიცებს ევროკავშირის ფუნდამენტურ უფლებათა ქარტია. დირექტივა საჯარო ელექტრონული კომუნიკაციებისა და საკომუნიკაციო ქსელების პროვაიდერებს ავალდებულებდა სატელეკომუნიკაციო მონაცემების შენახვას 2 წლამდე ვადით და მათ ხელმისაწვდომობას მძიმე დანაშაულთა პრევენციის, გამოძიებისა და დასჯის მიზნით. ეს ღონისძიება ეხებოდა მეტა, ადგილმდებარეობის განმსაზღვრელ და ისეთ მონაცემებს, რომლებიც საჭიროა გამომწერის ან მომხმარებლის იდენტიფიცირებისთვის და არ უკავშირდებოდა ელექტრონული კომუნიკაციის შინაარსს. CJEU-მ დაადგინა, რომ დირექტივა ზღუდავდა პერსონალურ მონაცემთა დაცვის ფუნდამენტურ უფლებას, „ვინაიდან იგი ასეთი მონაცემების დამუშავების შესაძლებლობას იძლევა, ასევე, პირადი ცხოვრების პატივისცემის უფლებასაც. მთლიანობაში, დირექტივის საფუძველზე შენახული და ხელისუფლების კომპეტენტური ორგანოებისთვის ხელმისაწვდომი მონაცემები იძლევა „ძალიან ზუსტი დასკვნების გაკეთების შესაძლებლობას იმ ადამიანთა პირადი ცხოვრების შესახებ, ვისი მონაცემებიც შენახულია (მათ შორის, ყოველდღიური ჩვევების, მუდმივი ან დროებითი საცხოვრებლის, ყოველდღიური ან სხვა გადაადგილების, აქტივობების, სოციალური კავშირებისა და იმ გარემოს შესახებ, სადაც ხშირად იმყოფებიან). ზემოაღნიშნული ორი უფლების შეზღუდვა იყო ფართო და განსაკუთრებულად მძიმე. CJEU-მ 2006/24/EC დირექტივა გაუქმებულად გამოაცხადა. სასამართლოს დასკვნით, მიუხედავად იმისა, რომ პერსონალურ მონაცემთა დაცვისა და პირადი ცხოვრების უფლებებზე დაწესებული შეზღუდვა ემსახურებოდა ლეგიტიმურ მიზანს, ეს იყო მძიმე შეზღუდვა და არ შემოიფარგლებოდა მხოლოდ მკაცრი საჭიროებით.

3) საქმე Bernh Larsen Holding AS and Others v. Norway

მაგალითი: საქმე Bernh Larsen Holding AS and Others v. Norway140 შეეხებოდა სამი ნორვეგიული კომპანიის საჩივარს საგადასახადო ორგანოს გადაწყვეტილებასთან დაკავშირებით, რომლის მიხედვითაც მათ აუდიტორებისათვის უნდა გადაეცათ იმ სერვერზე განთავსებულ მონაცემთა ასლები, რომლითაც ეს კომპანიები ერთობლივად სარგებლობდნენ.

ECtHR (ადამიანის უფლებათა ევროპული სასამართლო)-მა დაადგინა, რომ ამ მოვალეობის დაკისრება განმცხადებლებზე იყო ჩარევა მათ საცხოვრებლისა და კორესპონდენციის პატივისცემის უფლებაში (მე-8 მუხლი). თუმცა, სასამართლოს განმარტებით, საგადასახადო ორგანოებს ეფექტიანი და სათანადო მექანიზმები ჰქონდათ ჩარევის ბოროტად გამოყენების ასაცილებლად: მათ განმცხადებელი კომპანიები წინასწარ, საკმაო დროით ადრე გააფრთხილეს; კომპანიების წარმომადგენლები ესწრებოდნენ შემოწმებას და ჰქონდათ თავიანთი არგუმენტების ადგილზე წარმოდგენის შესაძლებლობა, მასალები კი განადგურდებოდა საგადასახადო შემოწმების დასრულებისთანავე. ასეთ პირობებში, საჭირო იყო სამართლიანი წონასწორობის მიღწევა საპირისპირო ინტერესებს შორის. კერძოდ, ეფექტიანი შემოწმების საჯარო ინტერესი, საგადასახადო შეფასების მიზნებით, უნდა დაბალანსებულიყო განმცხადებელი კომპანიების „საცხოვრებლისა“ და „კორესპონდენციის“ უფლებასა და მათი თანამშრომლების პირადი ცხოვრების დაცვის ინტერესთან. სასამართლომ დაადგინა, რომ საქმეში კონვენციის მე-8 მუხლი არ დარღვეულა.

4) საქმე Bărbulescu v. Romania

მაგალითი: საქმეში Bărbulescu v. Romania151 განმცხადებელი სამსახურიდან გაათავისუფლეს იმის გამო, რომ სამუშაო საათებში დამსაქმებლის ინტერნეტი შიდა რეგულაციების დარღვევით გამოიყენა. დამსაქმებელი ფარულ მონიტორინგს უწევდა დასაქმებულის კომუნიკაციებს და ჩანაწერები, რომლებიც მოიცავდა მხოლოდ პირადულ მესიჯებს, ეროვნულ დონეზე გამართულ სასამართლო პროცესზე წარმოადგინა. ECtHRმა, მას შემდეგ, რაც დაადგინა, რომ მე-8 მუხლი ვრცელდებოდა ასეთ მონაცემებზეც, ღია დატოვა კითხვა, თუ რამდენად უჩენდა დამსაქმებლის შემზღუდავი რეგულაციები განმცხადებელს პირადი ცხოვრების დაცვის გონივრულ მოლოდინს; თუმცა, ამავდროულად სასამართლომ დაადგინა, რომ დასაქმებულის ინსტრუქციები პირად სოციალურ ცხოვრებას სამუშაო ადგილზე ბოლომდე ვერ გამორიცხავდა. რაც შეეხება არსებით მხარეს, ხელშემკვრელ სახელმწიფოებს ფართო დისკრეცია ენიჭებათ შესაფასებლად, თუ რამდენად საჭიროა საკანონმდებლო ჩარჩოს შექმნა ისეთი პირობების დარეგულირებისათვის, რომელშიც დამსაქმებელს აქვს სამუშაო ადგილზე დასაქმებულის არაპროფესიული კომუნიკაციის გაკონტროლების უფლება - ელექტრონული თუ სხვა ფორმით. ამავდროულად, სახელმწიფო ორგანოებმა უნდა უზრუნველყონ, რომ დამსაქმებლის მიერ კორესპონდენციასა და სხვა კომუნიკაციაზე მონიტორინგის მიზნით დანერგილ ღონისძიებებს, მიუხედავად მათი მასშტაბისა და ხანგრძლივობისა, თან ახლდეს სათანადო და საკმარისი საშუალებები ბოროტად გამოყენებისგან დასაცავად. უაღრესად მნიშვნელოვანია პროპორციულობა და პროცედურული გარანტიები თვითნებობის წინააღმდეგ. ECtHR-მა გამოავლინა ასეთ პირობებისთვის საგულისხმო რამდენიმე ფაქტორი, მათ შორის, დასაქმებულზე მონიტორინგის ფარგლები და მის პირად ცხოვრებაში შეჭრის ხარისხი. კერძოდ, რა შედეგები ექნება ამგვარ ზომას დასაქმებულისთვის და რამდენად უზრუნველყოფილია დაცვის სათანადო საშუალებები.

ამასთან, სახელმწიფო ორგანოების ძალისხმევით, დასაქმებულს, რომლის კომუნიკაციებზეც მონიტორინგი ხორციელდება, ხელი უნდა მიუწვდებოდეს სამართლებრივი დაცვის საშუალებაზე შესაბამისი სასამართლო ორგანოს წინაშე, რათა, სულ მცირე, არსებითად დადგინდეს წარმოდგენილი კრიტერიუმების დაცვის საკითხი და სადავო ღონისძიებათა კანონიერება. ამ საქმეში ECtHR-მა დაადგინა მე-9 მუხლის დარღვევა, რადგან სახელმწიფო ორგანოებმა სათანადოდ ვერ დაიცვეს განმცხადებლის პირადი ცხოვრებისა და კორესპონდენციის პატივისცემის უფლება; შედეგად, მათ ვერ შეძლეს ორი საპირისპირო ინტერესის სამართლიანად დაბალანსება.

5) Criminal proceedings Against Bodil Lindqvist

მაგალითი: Bodil Lindqvist-ის186 საქმე შეეხებოდა ერთ-ერთ ინტერნეტგვერდზე ადამიანების იდენტიფიცირებას სახელით ან სხვა საშუალებებით, როგორიცაა ტელეფონის ნომერი და ინფორმაცია ჰობის შესახებ. CJEU-მ დაადგინა: „მითითება იმ ფაქტზე, რომ პიროვნებამ დაიზიანა ფეხი და ნახევარ განაკვეთზე მუშაობს სამედიცინო მიზეზების გამო, პერსონალური მონაცემია ჯანმრთელობის შესახებ.“

6) Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González

საქმეში Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González199 ბატონმა გონზალეზმა მოითხოვა, Google-ის საძიებო სისტემიდან წაეშალათ ან შეეცვალათ კავშირი მის სახელსა და იმ ორ საგაზეთო სტატიას შორის, რომლებიც აანონსებდნენ უძრავი ქონების აუქციონის გამართვას სოციალური უსაფრთხოების დავალიანების ამოსაღებად. CJEU-მ განაცხადა: „ინტერნეტის ავტომატური, მუდმივი და სისტემატური შესწავლის პროცესში, ინტერნეტში გამოქვეყნებული ინფორმაციის მოსაძიებლად, საძიებო სისტემის ოპერატორი „აგროვებს“ მონაცემებს, რომლებსაც შემდგომ „აღადგენს“, „იწერს“ და „ალაგებს“ ინდექსაციის პროგრამების ფრგლებში, „ინახავს“ სერვერებზე და, საჭიროებისას, „ამჟღავნებს“ მას; ასევე, უზრუნველყოფს მასზე „წვდომას“ თავისი მომხმარებლებისათვის, საძიებო შედეგების ჩამონათვალის ფორმით.“200 CJEU-მ დაასკვნა, რომ ამგვარი ქმედება არის „დამუშავება“, მიუხედავად იმისა, რომ საძიებო სისტემის ოპერატორი იმავე ოპერაციებს ახორციელებს სხვა ტიპის ინფორმაციის მიმართ და ამ უკანასკნელს არ განარჩევს პერსონალური მონაცემებისაგან.“

7) František Ryneš-ის საქმე

მონაცემთა დამუშავების კონცეფცია

მაგალითები: František Ryneš-ის საქმეში ბატონმა რეინეშმა, სახლში უსაფრთხოების მიზნით დამონტაჟებული CCTV სისტემის გამოყენებით დააფიქსირა იმ ორი ადამიანის გამოსახულება, რომლებმაც ფანჯრები ჩაუმსხვრიეს. CJEU-მ დაადგინა, რომ ვიდეოთვალთვალი, რომელიც მოიცავდა პერსონალურ მონაცემთა ჩაწერა-შენახვას,მონაცემთა ავტომატური დამუშავებაა, რაზეც ვრცელდება ევროკავშირის

მონაცემთა დაცვის კანონმდებლობა. საქმეში Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni194 ბატონი მანი ითხოვდა თავისი პერსონალური მონაცემების წაშლას სარეიტინგო კომპანიის რეესტრიდან, რომელიც მის სახელს უკავშირებდა უძრავი ქონების ლიკვიდირებულ კომპანიას, რითაც ზიანდებოდა მისი რეპუტაცია. CJEU-მ დაადგინა, რომ „ინფორმაციის ტრანსკრიფციით გადმოცემით, რეესტრში შენახვითა და გადაცემით (მესამე მხარის მოთხოვნის საფუძველზე), რეესტრის შენახვაზე/დაცვაზე პასუხისმგებელი ორგანო „ამუშავებს პერსონალურ მონაცემებს“. შესაბამისად, იგი „დამმუშავებელია“.

8) SWIFT-ის საქმე

მაგალითი: ე.წ. SWIFT-ის საქმეში ევროპულმა საბანკო ინსტიტუტებმა თავდაპირველად SWIFT დაიქირავეს, როგორც დამმუშავებელი, საბანკო ტრანზაქციების პროცესში მონაცემთა გადასაცემად. SWIFT-მა ეს მონაცემები, რომლებიც აშშ-ში მდებარე კომპიუტერულ სერვერზე ინახებოდა, აშშ-ს სახაზინო დეპარტამენტს გაუზიარა - ისე, რომ დამქირავებლებისგან (ევროპული საბანკო ინსტიტუტებისგან) პირდაპირი მითითება არ მიუღია. 29-ე მუხლის სამუშაო ჯგუფმა იმსჯელა შექმნილი სიტუაციის კანონიერებაზე და დაადგინა, რომ SWIFT და მისი დამქირავებელი ევროპული საბანკო ინსტიტუტები იყვნენ ერთობლივი დამმუშავებლები, რომელთაც ევროპელი მომხმარებლების წინაშე ეკისრებოდათ პასუხისმგებლობა მათი მონაცემების აშშ-ს მთავრობისთვის გამჟღავნების გამო.

9) საქმე K.H. and Others v. Slovakia

დამუშავების სამართლიანობა - კანონიერების გარდა, ევროკავშირისა და ევროპის საბჭოს მონაცემთა დაცვის კანონმდებლობა მოითხოვს პერსონალურ მონაცემთა სამართლიან დამუშავებასაც. სამართლიანი დამუშავების პრინციპი, ძირითადად, აწესრიგებს ურთიერთობას მონაცემთა დამმუშავებელსა და მონაცემთა სუბიექტს შორის.

მაგალითი: საქმეში K.H. and Others v. Slovakia განმცხადებლებს - ბოშური წარმოშობის ქალებს - აღმოსავლეთ სლოვაკეთში მდებარე ორ საავადმყოფოში გაუწიეს სამედიცინო მომსახურება ორსულობისა და მშობიარობის დროს. ამის შემდეგ, მიუხედავად არაერთი მცდელობისა, ვერცერთმა მათგანმა ვერ შეძლო დაორსულება. ეროვნულმა სასამართლოებმა საავადმყოფოებს მოსთხოვეს, განმცხადებლებისა და მათი წარმომადგენლებისათვის დაერთოთ ნება, გაცნობოდნენ სამედიცინო ჩანაწერებს და გაეკეთებინათ წერილობითი ამონაწერები, თუმცა მათ არ დააკმაყოფილეს მოთხოვნა დოკუმენტების ასლის გადაღებაზე. მიზეზად დაასახელეს დოკუმენტების ბოროტად გამოყენების საფრთხე. ECHR-ის მე-8 მუხლი სახელმწიფოებს უდგენს პოზიტიურ ვალდებულებას, რომელიც მოიცავს მონაცემთა სუბიექტის ხელმისაწვდომობას თავისი მონაცემების ასლებზე. სახელმწიფომ უნდა განსაზღვროს პერსონალურ მონაცემთა ფაილების ასლად გადაღების პირობები ან, მყარი მიზეზების არსებობისას, მონაცემთა სუბიექტს უარი უთხრას ამაზე. განმცხადებლების შემთხვევაში, ეროვნული სასამართლოები ასლების გადაღებაზე უარს ამართლებდნენ შესაბამისი ინფორმაციის

ბოროტად გამოყენებისგან დაცვით. თუმცა, ECtHR-მა ვერ დაინახა, როგორ გამოიყენებდნენ ბოროტად განმცხადებლები მათ შესახებ ინფორმაციას, თუკი ექნებოდათ წვდომა მთლიან სამედიცინო მასალებზე. ამასთან, ბოროტად გამოყენების პრევენცია შესაძლებელია სხვა საშუალებებით, რომლებიც არ გულისხმობს ასლის გადაღებაზე უარის თქმას (მაგ.: იმ პირთა წრის დავიწროება, რომლებსაც აღნიშნულ მასალებზე წვდომის უფლება აქვთ). სახელმწიფომ საკმარისად მყარი მიზეზებით ვერ დაასაბუთა თავისი უარი, განმცხადებლებს ჰქონოდათ წვდომა მათი ჯანმრთელობის შესახებ ინფორმაციაზე. სასამართლომ საქმეში დაადგინა მე-8 მუხლის დარღვევა.

10) საქმე Haralambie v. Romania

დამუშავების გამჭვირვალობა - ევროკავშირისა და ევროპის საბჭოს მონაცემთა დაცვის სამართალი მოითხოვს, რომ პერსონალური მონაცემები „მონაცემთა სუბიექტთან მიმართებით გამჭვირვალედ“ დამუშავდეს.

მაგალითი: საქმეში Haralambie v. Romania განმცხადებლის მოთხოვნა მის შესახებ საიდუმლო სამსახურის ხელთ არსებული ინფორმაციის ხელმისაწვდომობაზე მხოლოდ 5 წლის შემდეგ დააკმაყოფილეს. ECtHRმა კიდევ ერთხელ ხაზგასმით აღნიშნა, რომ პირებს, რომლებიც საჯარო უწყებების ხელთ არსებული პერსონალური ფაილების (პირადი საქმის) სუბიექტები არიან, აქვთ ამ ფაილებზე წვდომის სასიცოცხლო ინტერესი და ხელისუფლებას ევალებოდა შესაბამისი ეფექტიანი პროცედურის უზრუნველყოფა. ECtHR-მა მიიჩნია, რომ არც გადაცემული ფაილების რაოდენობა და არც არქივის სისტემაში არსებული ხარვეზები არ ამართლებდა განმცხადებლის მოთხოვნის დაკმაყოფილებას 5 წლის შემდეგ. ხელისუფლებამ განმცხადებელი ვერ უზრუნველყო ეფექტიანი პროცედურით - გონივრულ ვადაში მიეღო წვდომა თავის პერსონალურ ფაილებზე. სასამართლომ საქმეში დაადგინა კონვენციის მე-8 მუხლის დარღვევა.

11) საქმე Smaranda Bara and Others v. Preşidentele Casei Naţionale de Asigurări de Sănătate, Casa Naţională de Administrare Fiscală (ANAF)

დამუშავების გამჭვირვალობა - ევროკავშირისა და ევროპის საბჭოს მონაცემთა დაცვის სამართალი მოითხოვს, რომ პერსონალური მონაცემები „მონაცემთა სუბიექტთან მიმართებით გამჭვირვალედ“ დამუშავდეს.

მაგალითი: საქმეში Smaranda Bara and Others v. Preşidentele Casei Naţionale de Asigurări de Sănătate, Casa Naţională de Administrare Fiscală (ANAF) რუმინეთის ეროვნულმა საგადასახადო ორგანომ თვითდასაქმებულ პირთა შემოსავლების საგადასახადო მონაცემები გადასცა ჯანმრთელობის დაზღვევის ეროვნულ ფონდს, რის საფუძველზეც განისაზღვრა ჯანმრთელობის დაზღვევის გადასახადის ოდენობა. CJEU-მ იმსჯელა, უნდა ეცნობებინათ თუ არა მონაცემთა სუბიექტებისთვის დამმუშავებლის ვინაობა და მონაცემთა გადაცემის მიზანი მანამდე, სანამ მათ დაამუშავებდა ჯანმრთელობის დაზღვევის ეროვნული ფონდი. CJEU-მ დაადგინა: როდესაც წევრი სახელმწიფოს ერთი საჯარო ადმინისტრაციული ორგანო პერსონალურ მონაცემებს მეორე

ასეთ უწყებას გადასცემს შემდგომი დამუშავებისთვის, საჭიროა მონაცემთა სუბიექტების ინფორმირება ამის შესახებ.

დამუშავების გამჭვირვალობა - ევროკავშირისა და ევროპის საბჭოს მონაცემთა დაცვის სამართალი მოითხოვს, რომ პერსონალური მონაცემები „მონაცემთა სუბიექტთან მიმართებით გამჭვირვალედ“ დამუშავდეს.

12) European Commission v. Federal Republic of Germany

დამოუკიდებლობა - ევროკავშირისა და ევროპის საბჭოს სამართალი საზედამხედველო ორგანოებს ავალდებულებს სრული დამოუკიდებლობით მოქმედებას თავიანთი ფუნქციებისა და უფლებამოსილებების განხორციელებისას

მაგალითები: European Commission v. Federal Republic of Germany498 ევროპულმა კომისიამ CJEU-ს მიმართა თხოვნით, რათა დაედგინა, რომ გერმანიამ მონაცემთა დაცვაზე პასუხისმგებელი ორგანოებისათვის „სრული დამოუკიდებლობის“ მოთხოვნა და მასზე დაკისრებული ვალდებულებები ვერ შეასრულა მონაცემთა დაცვის დირექტივის 28-ე მუხლის პირველი პუნქტის შესაბამისად. კომისიის აზრით, ის, რომ გერმანიამ საზედამხედველო ორგანოები, რომლებიც სხვადასხვა ფედერალურ ერთეულში (Länder) პერსონალურ მონაცემთა დამუშავებას აკონტროლებდნენ, სახელმწიფო კონტროლქვეშ მოაქცია, ეწინააღმდეგებოდა დამოუკიდებლობის მოთხოვნას მონაცემთა დაცვის კანონმდებლობასთან შესაბამისობის მიზნით. CJEU-მ ხაზგასმით აღნიშნა, რომ ცნება „სრული დამოუკიდებლობით“ უნდა განიმარტოს [28-ე მუხლის პირველი პუნქტის] ფორმულირების, ასევე, ევროკავშირის მონაცემთა დაცვის კანონმდებლობის მიზნებისა და სტრუქტურის საფუძველზე.499 CJEU-მ ხაზი გაუსვა, რომ საზედამხედველო ორგანოები პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებული უფლებების „დამცველები“ არიან. ამრიგად, მათი შექმნა წევრ სახელმწიფოში მიჩნეულია „ფიზიკურ პირთა დაცვის მნიშვნელოვან კომპონენტად პერსონალურ მონაცემთა დამუშავებისას.“500 CJEU-ს დასკვნით, „მოვალეობების შესრულებისას, საზედამხედველო ორგანოები ობიექტურად და მიუკერძოებლად უნდა მოქმედებდნენ. საამისოდ ისინი თავისუფალნი უნდა იყვნენ ნებისმიერი გარე ზემოქმედებისგან, მათ შორის, სახელმწიფო ორგანოთა პირდაპირი ან არაპირდაპირი გავლენისგან.“ 501 სასამართლომ ასევე დაადგინა, რომ „სრული დამოუკიდებლობა“ უნდა განიმარტოს EDPS-ის დამოუკიდებლობიდან გამომდინარე, რაც განსაზღვრულია ევროკავშირის ინსტიტუტების მონაცემთა დაცვის რეგულაციით. ამ რეგულაციის თანახმად, დამოუკიდებლობის კონცეფცია გულისხმობს, რომ EDPS-მა არ მოითხოვოს/მიიღოს ინსტრუქციები რომელიმე პირისგან. შესაბამისად, CJEU-მ დაადგინა, რომ საზედამხედველო ორგანოები გერმანიაში - სახელმწიფო ორგანოების მხრიდან კონტროლის გამო - არ იყვნენ სრულად დამოუკიდებელნი ევროკავშირის მონაცემთა დაცვის კანონმდებლობის მიხედვით

13) European Commission v. Republic of Austria

დამოუკიდებლობა - ევროკავშირისა და ევროპის საბჭოს სამართალი საზედამხედველო ორგანოებს ავალდებულებს სრული დამოუკიდებლობით მოქმედებას თავიანთი ფუნქციებისა და უფლებამოსილებების განხორციელებისას

საქმეში European Commission v. Republic of Austria502 CJEU-მ იმავე პრობლემებს გაუსვა ხაზი, ამჯერად ავსტრიის მონაცემთა დაცვის საზედამხედველო ორგანოს (მონაცემთა დაცვის კომისია, DSK) გარკვეული წევრებისა და თანამშრომლების დამოუკიდებლობასთან მიმართებით. სასამართლომ განმარტა: ის ფაქტი, რომ ფედერალური კანცელარია საზედამხედველო ორგანოს უზრუნველყოფდა სამუშაო ძალით, ევროკავშირის მონაცემთა დაცვის კანონმდებლობით გათვალისწინებულ დამოუკიდებლობის მოთხოვნას ასუსტებდა. CJEU-მ ასევე დაადგინა, რომ კანცელარიის უფლება, ნებისმიერ დროს ყოფილიყო ინფორმირებული DSK-ის საქმიანობის შესახებ, უგულებელყოფდა საზედამხედველო ორგანოს სრული დამოუკიდებლობის მოთხოვნას.

13) European Commission v. Hungary

დამოუკიდებლობა - ევროკავშირისა და ევროპის საბჭოს სამართალი საზედამხედველო ორგანოებს ავალდებულებს სრული დამოუკიდებლობით მოქმედებას თავიანთი ფუნქციებისა და უფლებამოსილებების განხორციელებისას

საქმეში European Commission v. Hungary503 სასამართლომ აკრძალა შიდასახელმწიფოებრივ დონეზე არსებული მსგავსი პრაქტიკა, რომელიც საზედამხედველო ორგანოს სამუშაო ძალის დამოუკიდებლობაზე ახდენდა გავლენას. მან აღნიშნა: „მოთხოვნა [...], რომ თითოეულმა საზედამხედველო ორგანომ შეძლოს მასზე დაკისრებულ მოვალეობათა სრული დამოუკიდებლობით შესრულება, მოიცავს შესაბამისი წევრი სახელმწიფოს ვალდებულებას, ამ უწყებას მისცეს უფლებამოსილების ვადის სრულ ამოწურვამდე მუშაობის საშუალება.“ CJEU-მ ასევე დაადგინა, რომ „პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს უფლებამოსილების ვადის ნაადრევი შეწყვეტით, უნგრეთმა ვერ შეასრულა 95/46/EC დირექტივით გათვალისწინებული ვალდებულებები [...]“.

13) Weltimmo-ს საქმე

კომპეტენცია და უფლებამოსილება - ევროკავშირის კანონმდებლობაში GDPR ითვალისწინებს საზედამხედველო ორგანოთა კომპეტენციებსა და ორგანიზაციულ სტრუქტურას და ადგენს მოთხოვნას, რომ ისინი იყვნენ კომპეტენტურნი და ჰქონდეთ რეგულაციით გათვალისწინებული ფუნქციების შესასრულებლად საჭირო უფლებამოსილება.

მაგალითი: Weltimmo-ს საქმეში510 CJEU-მ იმსჯელა ეროვნული საზედამხედველო ორგანოების კომპეტენციებზე, მათი იურისდიქციის გარეთ შექმნილ ორგანიზაციებთან დაკავშირებით. Weltimmo სლოვაკეთში რეგისტრირებული კომპანიაა, რომელიც უნგრეთში არსებული უძრავი ქონების ყიდვა-გაყიდვის ვებგვერდს მართავს. რეკლამის დამკვეთებმა უნგრეთის მონაცემთა დაცვის საზედამხედველო ორგანოში შეიტანეს საჩივარი მონაცემთა

დაცვის შიდასახელმწიფოებრივი კანონმდებლობის დარღვევაზე, რის შედეგადაც საზედამხედველო ორგანომ Weltimmo-ს ჯარიმა დააკისრა. კომპანიამ ჯარიმა გაასაჩივრა ეროვნულ სასამართლოში, რომელმაც CJEU-ს მიმართა და სთხოვა დადგენა, აძლევდა თუ არა ევროკავშირის მონაცემთა დაცვის დირექტივა წევრი სახელმწიფოს საზედამხედველო ორგანოს მონაცემთა დაცვის ეროვნული კანონმდებლობის გამოყენების უფლებას იმ კომპანიასთან მიმართებით, რომელიც სხვა წევრ ქვეყანაში იყო დარეგისტრირებული.

CJEU-მ განმარტა, რომ მონაცემთა დაცვის დირექტივის მე-4 მუხლის 1 (ა) პუნქტი წევრ სახელმწიფოს აძლევს უფლებას, მონაცემთა დაცვის საკუთარი კანონმდებლობა გამოიყენოს სხვა წევრ სახელმწიფოში რეგისტრირებული დამმუშავებლის მიმართ, თუკი ის „შესაბამისი წევრი სახელმწიფოს ტერიტორიაზე სტაბილურად ორგანიზებული დაწესებულების მეშვეობით, რეალურად ეწევა თუნდაც მინიმალურ ეფექტიან საქმიანობას მონაცემთა დამუშავების კუთხით.“ CJEU-მ აღნიშნა, რომ მის ხელთ არსებულ ინფორმაციაზე დაყრდნობით, Weltimmo-ს საქმიანობა უნგრეთში რეალური და ეფექტიანი გახლდათ, რადგან კომპანიის წარმომადგენელი ამ ქვეყანაში სლოვაკეთის კომპანიათა რეესტრში უნგრული მისამართით იყო დარეგისტრირებული; ასევე, მას უნგრეთში ჰქონდა საბანკო ანგარიში და საფოსტო ყუთი და უნგრულ ენაზე დაწერილ აქტივობებს ახორციელებდა. ეს ინფორმაცია მიუთითებდა დაწესებულების რეალურად არსებობაზე, რის გამოც Weltimmo-ს აქტივობებზე ვრცელდებოდა უნგრეთის მონაცემთა დაცვის კანონმდებლობა და საზედამხედველო ორგანოს იურისდიქცია. თუმცა, CJEU-მ ეროვნულ სასამართლოს მიანდო ამ ინფორმაციის გადამოწმება, კერძოდ: თუ ეროვნული სასამართლო დაადგენდა, რომ Weltimmo-ს უნგრეთში ჰქონდა დაწესებულება, უნგრეთის საზედამხედველო ორგანოს ექნებოდა ჯარიმის დაკისრების უფლებამოსილება; სასამართლოს მიერ საპირისპირო გადაწყვეტილების მიღების შემთხვევაში, კომპანიაზე გავრცელდებოდა იმ წევრი სახელმწიფოს კანონმდებლობა, სადაც კომპანია რეგისტრირებული იყო. ვინაიდან საზედამხედველო ორგანოების უფლებამოსილება უნდა განხორციელდეს სხვა წევრი სახელმწიფოების ტერიტორიულ სუვერენიტეტთან შესაბამისობაში, ამ საქმეში უნგრეთის საზედამხედველო ორგანოს არ ჰქონდა ჯარიმის დაკისრების უფლება. თუმცა, რაკი მონაცემთა დაცვის დირექტივა ითვალისწინებდა საზედამხედველო ორგანოებს შორის თანამშრომლობის ვალდებულებას, უნგრეთის საზედამხედველო ორგანოს შეეძლო, სლოვაკეთის ასეთივე ორგანოსთვის ეთხოვა აღნიშნული საკითხის გარკვევა, სლოვაკეთის კანონმდებლობის დარღვევის დადგენა და მისივე სამართლით გათვალისწინებული სანქციების დაკისრება.