კვირა 1

- გაერო იცავს მე-8 მუხლს

- პერსონალური მონაცემების დაცვას უზრუნველყოფს დამოუკიდებელი ორგანიზაცია. პერსონალურ მონაცემთა დაცვის სამსახური

- ადამიანის უფლებათა ევროპული კონვენციის მე-8 მუხლის თანახმად, პერსონალურ მონაცემთა დაცვის უფლება ადამიანის პირადი და ოჯახური ცხოვრების, საცხოვრებლისა და მიმოწერის პატივისცემის უფლების ნაწილია

- დღესდღეობით, ევროპის საბჭოს 108-ე კონვენცია პირველი საერთაშორისო სამართლებლივი ინსტრუმენტია მონაცემთა დაცვის შესახებ, რომელსაც აქვს სავალდებულო ძალა. კონვენციის მოდერნიზაციის პროცესი დასრულდა CETS No. 223 შესწორების ოქმის მიღებით.

- ევროკავშირის კანონმდებლობის თანახმად, მონაცემთა დაცვა აღიარებულია დამოუკიდებელ ფუნდამენტურ უფლებად. მას განამტკიცებს ხელშეკრულება ევროკავშირის ფუნქციონირების შესახებ, კერძნობ, მისი მე-16 მუხლი, და ევროკავშირის ფუნდამენტურ უფლებათა ქარტიის მე-8 მუხლი

- ევროკავშირის კანონმდებლობაში მონაცემთა დაცვა პირველად მონაცემთა დაცვის დირექტივით დარეგულირდა 1995 წელს

- სწრაფი ტექნოლოგიური განვითარების გათვალისწინებით, ევროკავშირმა 2016 წელს ახალი კანონმდებლობა მიიღო ციფრულ ეპიქაში მონაცემთა დაცვის წესების ადაპტირებისათვის. 2018 წლის მაისში ძალაში შევიდა მონაცემთა დაცვის ზოგადი რეგულაცია, რომლითაც გაუქმნდა მონაცემთა დაცვის დირექტივა

- მონაცემთა დაცვის ზოგად რეგულაციასთან ერთად, ევროკავშირმა მიიღო კანონმდებლობა სახელმწიფო ორგანოების მიერ მონაცემთა დაცვის დამუშავებაზე სამართლის დასაცავად. დირექტივა (EU) 2016/680 ადგენს მონაცემთა დაცვის წესებსა და პრინციპებს პერსონალურ მონაცემთა დამუშავებაზე, რომლის მიზანია დანაშაულის პრევენცია, გამოძიება, დადგენა, სისხლისსამართლებრივი დევნა, ან სასჯელის აღსრულება.

- ევროპაში პერსონალურ მონაცემთა დაცვა დაიწყო 1970-იანი წლებიდან

- ევროკავშირის სამართლის სისტემაში, მონაცემთა დაცვა არის ფუნდამენტარული უფლებად აღიარებული, პირადი ცხოვრების პატივისცემისგან განცელკევებულად

- მე-8 მუხლის 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
- პირადი ცხოვრების ხელშეუხებლობის უფლება ეხება სიტუაციებს, რომლებიც საფრთხეს უქმის ადამიანის პირად ინტერესს, ანუ “პირად ცხოვრებას”

- პერსონალური ინფორმაციის შეგროვებისა და გამოყენების მარეგულირებელი სპეციფიკური წესების საჭიროებამ წარმოქმნა პირადი ცხოვრების ახალი კონცეფცია, რომელიც სხვადასხვა იურისდიქციაში ცნობილია, როგორც “საინფორმაციო პირადი ცხოვრება” ან “ინფორმაციული თვითთნგამორკვევის უფლება”. კონცეფციამ განაპირობა პერსონალურ მონაცემთა დაცვის სპეციალური სამართლებლივი რეგულაციების შემუშავება

გაერო

- გაერო პერსონალურ მონაცემთა დაცვას ფუნდამენტურ უფლებად არ მიიჩნევს

- UDHR-ს სავალდებულო იურიდიული ძალა არ გააჩნია, თუმცა აქვს ადამიანის უფლებათა საერთაშორისო სამართლის ფუძემდებლური ინსტრუმენტის მნიშვნელოვანი სტატუსი და გავლენა მოახდინა ადამიანის უფლებათა ინსტრუმენტების შექმნაზე ევროპაში

- ICCPR აცხადებს, რომ არავინ უნდა დაექვემდებაროს მის პირად და ოჯახურ ცხოვრებაში, საცხოვრებლის ან კორესპოდენციის ხელშეუხებლობაში თვითნებურ ან უკანონო ჩარევას ან ღირსებისა და რეპუტაციის უკანონო ხელყოფას

- ICCPR საერთაშორისო ხელშეკრულებაა, რომელიც ძალაში 1976 წელს შევიდა და რომელიც 169 ხელმომწერ მხარეს ავალდებულებს სამოქალაქო უფლებების, მათ შორის, პირადი ცხოვრების ხელშეუხებლობის უზრუნველყოფასა და დაცვას

- 2016-2017 წელს მიღებული რეზოლუციები გმობს სადაზვერვოს უფლებამოსილებებს და გმობს თვალთვალს

ევროპის 108-ე კონვენცია

- ინფორმაციული ტექნოლოგიების განვითარების გამო, 1981 წელს ხელმოსაწერად გაიხსნა კონცენცია პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ, 108-ე კონვენცია.

- 108-ე კონვენციას შესასრულებლად სავალდებულო ძალა აქვს იმ სახელმწიფოებისთვის, რომლებშის ის რატიფიცირებულია

- ეს დოკუმენტი იყო და რჩება სავალდებულო იურიდული ძალის მქონდე ერთადერთ საერთაშორისო ინსტრუმენტად მონაცემთა დაცვის სფეროში

- კონვენცია ვრცელდება ყველა სახის მონაცემთა დამუშავებაზე, როგორც კერძო, ისე საჯარო სექტორის, მათ შორის, მართლმსაჯულებისა და სამართალდამცველი ორგანოების მიერ

- იგი ადამიანის უფლებებს იცავს პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებული დარღვევებისგან

- პრინციპები შეეხება მონაცემთა სამართლიან და კანონიერ შეგროვებასა და ავტომატურ დამუშავებას კონკრეტული ლეგიტიმური მიზნებით, რაც ნიშნავს, რომ დაუშვებელია მათი გამოყენება სხვაგვარად, ან შენახვა იმაზე ხანგრძლივად, ვიდრე საჭიროა ამ მიზნების მისაღწევად. დებულებები შეეხება მონაცემთა ხარისხვაც. კერძნობდ, ისინი უნდა იყოს ადეკვატური, რელევანტური, ზომიერი და ზუსტი

- ასევე იგი იცავს ფიზიკური პირის უფლებებსაც, იცოდეს, თუ რა ინფორმაცია ინახება მასზე და საჭიროების შემთხვევაში მოითხოვოს მათი შესწორება

Digital Rights Ireland-ის საქმე:

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 პრავაიდერებს ავალდებულება სატელეკომუნიკაციო მონაცემების შენახვას 2 წლამდე ვადით და მათ ხელმისაწვდომობას მძიმე დანაშაულის პრევენციის, გამოძიებისა და დასჯის მიზნით. ეს ღონისძიება ეხებოდა მეტა, ადგილმდებარეობის განმსაზღვრელ და ისეთ მონაცემებს, რომლებიც საჭიროა გამოწერის 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.”

CJEU-მ დირექტივა გაუქმებულად გამოაცხადა. სასამართლოს დასკვნით, მიუხედავად იმისა, რომ პერსონალურ მონაცემთა დაცვისა და პირადი ცხოვრების უფლებაზე დაწესებული შეზღუდვა ემსახურებოდა ლეგიტიმურ მიზანს, ეს მძიმე შეზღუდბა და არ შემოიფარგლებოდა მხოლოდ მკაცრი საჭიროებებით.

კვირა 2

- მონაცემები პერსონალურია, თუ უკავშირდება იდენტიფიცირებულ ან იდენტიფიცირებად პირს – “მონაცემთა სუბიექტს”

- არის თუ არა პირი იდენტიფიცირებადი, ამის დასადგენად მონაცემთა დამმუშავებელმა ან სხვა სუბიექტმა უნდა გაითვალისწინოს ყველა

გონივრული საშუალება, რომელთა გამოყენებაც შესაძლებელია პიროვნების პირდაპირი ან ირიბი იდენტიფიცირებისთვის

- ნამდვილობის დადგენა არის პროცედურა, რომლითაც პირს შეუძლია დაადასტუროს გარკვეული ვინაობა და/ან უფლებამოსილება გარკვეული ქმედების განსახორციელებლად
- მონაცემები ანონიმურია, თუ აღარ უკავშირდება იდენტიფიცირებულ ან იდენტიფიცირებად პირს

- ფსევდონიმიზაცია არის ღონისძიება, რომელის გამოყენებითაც პერსონალური მონაცემები ვეღარ მიეწერება მონაცემთა სუბიექტს, დამატებითი ინფორმაციის გარეშე, რომელიც შენახულია ცალკე. “გასაღები” რომელიც მონაცემთა სუბიექტის ხელახლა იდენტიფიცირების შესაძლებლობას იძლევა, გამოყოფილად და უსაფრთხოდ უნდა იყოს დაცული. მონაცემები, რომლებმაც ფსევდონიმიზაციის პრეცესი გაიარა, პერსონალურ ინფორმაციას რჩება. ევროკავშირის სამართალში არ არსებობს “ფსევდონიმიზებულ მონაცემთა“ კონცეფცია

- მონაცემთა დაცვის პრინციპები და წესები არ ეხება ანონიმურ ინფორმაციას, მაგრამ ეხება ფსევდონიმიზებულ მონაცემებს

- პირს, რომლის მონაცემებიც მუშავდება, “მონაცემთა სუბიექტი” ეწოდება

- ევროპის მონაცემთა სამართალი, მხოლოდ ცოცხალ პირებს იცავს

- GDPR-ის თანახმად, პერსონალურ მონაცემად მიიჩნევა ნებისმიერი ინფორმაცია, რომელიც უკავშირდება იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს

- იურიდიული პირები სარგებლობენ დაცვის განსაკუთრებული დონით

- მოდერნიზებული 108-ე კონვენციის თანახმად, მონაცემთა დაცვა, ძირითადად, მოიცავს ფიზიკურ პირებს, თუმდა ხელმომწერმა სახელმწიფოებმა ის თავიანთ კანონმდებლობაში შეიძლება გაავრცელონ იურიდიულ პირებზეც

- ნებისმიერი ტიპის მონაცემი შეიძლება პერსონალურ ინფორმაციად ჩაითვალოს, თუ უკავშირდება იდენტიფიცირებულ ან იდენტიფიცირებად პირს

- მაგ, ხელმძღვანელის მიერ მუშაობის შეფასება, რომელიც მის პირად საქმეში ინახება, დასაქმებულის პერსონალური მონაცემია

- პერსონალური მონაცემი მოიცავს ინფორმაციას ადამიანის პირადი ცხოვრების, მათ შორის, პროფესიული და საზოგადოებრივი აქტივობების შესახებ

- EctHR-ის პრეცედენტული სამართალი ევროპული კონვენციის მე-8 მუხლთან დაკავშირებით ადასტურებს, რომ რთულია პირადი და პროფესიული ცხოვრების საკითხების ერთმანეთისგან გამიჯვნა

- ინფორმაცია პერსონალურ მონაცემებს შეიცავს, თუ მასში პირი: იდენტიფიცირებულია, ან იდენტიფიცირებადი; არ არის იდენტიფიცირებული,

მაგრამ შესაძლებელია ამ ინფორმაციის საფუძველზე მისი გამორჩევა, რაც იძლევა მონაცემთა სუბიექტის დადგენის შესაძლებლობას შემდგომი ძიების მეშვეობით

Bernh Larsen Holding AS and Others v. Norway

Bernh Larsen Holding AS and Others v. Norway შეეხებოდა სამი ნორვეგიული კომპანიის საჩივარს საგადასახადო ორგანოს გადაწყვეტილებასთან დაკავშირებით, რომლის მიხედვითაც მათ აუდიტოებისათვის უნდა გადაეცათ იმ სერვერზე განთავსებული მონაცემთა ასლები, რომლითაც ეს კომპანიები ერთობლივად სარგებლობდნენ. საქმეზე განილიხილეს მე-8 მუხლი. თუმცა, სასამართლოს განმარტებით, საგადასახადო ორგანოებს ეფექტიანი და სათანადო მექანიზმები ჰქონდათ ჩარევის ბოროტად გამოყენების ასაცილებლად: მათ განცხადებელი კომპანიების წარმომადგენლები ესწრებოდნენ შემოწმებისას და ჰქონდათ თავიანთი არგუმენტი ადგილზე წარმოდგენის შესაძლელობა, მასალები კი განადგურდებოდა საგადასახადო შემოწმების დასრულებისთანავე. სასამართლომ დაადგინა, რომ საქმეში კონვენციის მე-8 მუხლი არ დარღვეულა.

Barbulescu v. Romania

საქმეში Barbulescu v. Romania 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. EttHR-მა დაადინა, რომ მე-8 მუხლი ვრცელდებოდა ასეთ მონაცემებზეც. საბოლოოდ, ამ საქმეში EctHR-მა დაადგინა, მე-8 მუხლის დარღვევა.

კვირა 3

განსაკუთრებული კატეგორიის პერსონალური მონაცემები (2.1.2)

- არსებობს პერსონალური მონაცემების კატეგორიები, რომლებიც თავიანთი ბუნებიდან გამომდინარე, დამუშავებისას შეიძლება რისკებს შეიცავდეს მონაცემთა სუბიექტისთვის.

- ისინი საჭიროებენ გაძლიერებულ დაცვას

- ამგვარ მონაცემებზე ვცრელდება აკრძალვის პრინციპი და მათუ დამუშავება კანონის თანახმად ნებადართულია მხოლოდ შეზღუდული რაოდენობით

- სენსიტიურ მონაცემებად მიიჩნევა ინფორმაცია:
    - რასისა და ეთნიკური წარმომავლობის შესახებ

    - პოლიტიკური, რელიგიური ან სხვა შეხედულებების შესახებ

    - პროფესიული კავშირის წევრობის შესახებ

- გენეტიკური და ბიომეტრიული მახასიათებლების შესახებ, რომელთა დამუშავებაც ხდება პიროვნების იდენტიფიცირების მიზნით

- პიროვნების ჯანმრთელობის მდგომარეობის, სქესობრივი ცხოვრების ან სექსუალური ორიენტაციის შესახებ

ნასამართლეობა და დანაშაულის ჩადენა

- მოდერნიზებული 108-ე კონვენცია მოიცავს პერსონალურ მონაცემებს დანაშაულის შესახებ

- მე-10 მუხლის თანახმად ასეთი მონაცემები უნდა დამუშავდეს მხოლოდ ოფიციალური ორგანოს კონტროლქვეშ, ან ევროკავშირისა თუ წევრი სახელმწიფოს საკონის თანახმად, რომელიც უზრუნველყოფს მონაცემთა სუბიექტის უფლებებისა და თავისუფლებების დაცვის სათანადო გარანტიებს

მონაცემთა დამუშავება (2.2)

- “მონაცემთა დამუშავება” გულისხმობს ნებისმიერ ქმედებას პერსონალური მონაცემების მიმართ

- ტერმინი “დამუშავება” მოიცავს ავტომატურ და არაავტომატურ დამუშავებას

- ევროკავშირის კანონმდებლობით, “დამუშავება” ასევე ეხება არაავტომატურ დამუშავებას სტრუქტურიზებულ ფაილურ სისტემაში

- ევროპის საბჭოს კანონმდებლობის მიხედვით, შესაძლებელია, “დამუშავების” ცნება, ეროვნული კანონმდებლობით, ვრცელდებოდეს მონაცემთა არაავტომატურ დამუშავებაზეც

- პერსონალურ მონაცემთა დამუშავება გულისხმობს ნებისმიერ ქმედებას, როგორიცაა, მაგალითად: შეგროვება, აღრიცხვა/ჩაწერა, ორგანიზება, სტრუქტურიზება, შენახვა, ადაპტაცია, ან შეცვლა, ამოღება, გაცნობა, გამოყენება, გამჟღავნება…

- Bodil Lindqvist-ის საქმე შეეხებოდა ერთ-ერთ ინტერნეტ გვედზე სხვადასხვა ადამიანის იდენტიფიცირებას სახელით ან სხვა საშუალებებით, როგორიცაა ტელეფონის ნომერი და ინფორმაცია ჰობის შესახებ. CJEU-მ დაადგინა: “ვებგვერდის მეშვეობით სხვადასხვა პიროვნებაზე მითითება და მათი იდენტიფიცირება ნებისმიერი საშუალებით არის პერსონალური მონაცემების მთლიანად ან ნაწილობრივ ავტომატური დამუშავება”

მონაცემთა ავტომატური დამუშავება (2.2.2)

- ევროკავშირის სამართალში მონაცემთა აბტომატური დამუშავება გულისხმობს ქმედებების, რომლებიც ხორციელდება “მონაცემთა მიმართ

სრულიად ან ნაწილობრივ აბტომატური საშუალებებით.” პრაქტიკაში ეს ნიშნავს, რომ პერსონალურ მონაცემთა ნებისმიერ სახით დამუშავებაზე ავტომატური საშუალებებით, კომპიუტერით, ტელეფონით ან როუტერით, ვრცელდება როგორც ევროკავშირის, ისე ევორპის საბჭოს მონაცემთა დაცვის წესები.

მონაცემთა არაავტომატური დამუშავება (2.2.3)

- 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 უზრუვენყოფს პერსონალურ მონაცემთა კატეგორიზაციას და მათზე ხელმისაწვდომობას გარკვეული კრიტერიუმების საფუძველზე. მაგალითად, თუ დამსაქმებელი აწარმოებს საქაღამდეს “დასაქმებულთა შვებულება”, რომელიც შეიცავს დეტალური ინფორმაციას მათ შესახებ, დალაგებულს ანბანის მიხედვით, ასეთი ფაილი ითვლება არაავტომატურ ფაილურ სისტემად, რომელზეც ვრცელდება ევროკავშირის მონაცემთა დაცვის წესები, რადგანაც:

- ფაილების სტრუქტურიზება შესაძლებელია იმგვარად, რომ მოხერხდეს ინფორმაციის სწრაფად და ადვილად მოძიება

- პერსონალური მონაცემების შენახვა საქაღალდეებში აიოლებს იმ შეზღუდვების აცილებას, რომელიც კანონმდებლობით გათვალისწინებულია მონაცემთა ავტომატური დამუშავებისთვის

- ევროკავშირის კანონმდებლობის თანახმად, მონაცემთა ავტომატური დამუშავების განმარტება ითვალისწინებს, რომ ავტომატურ ოპერაციებს შორის შეიძლება საჭირო გახდეს პერსონალური მონაცემების არაავტომატური გამოყენება

- “მონაცემთა დამუშავება” ნიშნავს ქმედებას ან ქმედებათა ერთობლიობას პერსონალური მონაცემების მიმართ, რომელიც ხორციელდება მათ სტრუქტურიზებულ წყებაზე და ხელმისაწვდომი ან დალაგებულია კონკრეტული კრიტერიუმების შესამაბისად

პერსონალურ მონაცემთა მომხმარებლები (2.3)

- ნებისმიერი პირო, რომელიც განსაზღვრავს სხვების პერსონალურ მონაცემთა დამუშავების საშუალებებსა და მიზნებს, არის “დამმუშავებელი”, მონაცემთა დაცვის კანონმდებლობის შესაბამისად; თუ ამ გადაწყვეტილებას ერთად რამდენიმე პირი იღებს, მათ “ერთობლივი დამმუშავებლები” ეწოდებათ

- “უფლებამოსილი პირი” არის ფიზიკური ან იურიდიული პირი, რომელიც პერსონალურ მონაცემებს ამუშავებს “დამმუშავებლის” სახელით

- უფლებამოსილი პირი დამმუშავებელი ხდება, თუ იგი განსაზღვრავს მონაცემთა დამუშავების საშუალებებსა და მიზნებს

- ნებისმიერი პირი, რომლისთვისაც მჟღავნდება პერსონალური მონაცემები, არის “მიმღები”

- “მესამე მხარე” არის ფიზიკური ან იურიდიული პირი, მონაცემთა სუბიექტის, დამმუშავებლის, უფლებამოსილი პირის ან იმ პირის გარდა, რომელსაც აქვს პერსონალურ მონაცემთა დამუშავების უფლება დამმუშავებლის ან უფლებამოსილი პირის პირდაპირი დავალებით;

- თანხმობა, როგორც პერსონალური მონაცემების დამუშავების სამართლებლივი საფუძველი, უნდა იყოს ნებაყოფლობითი, ინფორმირებული და კონკრეტული, და მკაფიოდ გამოხატავდეს დამუშავებაზე თანხმობის სურვილს, ნათლად დადასტურებულს აქტით.

- განსაკუთრებული კატეგორიის მონაცემთა დამუშავება ნებართვის საფუძველზე, საჭიროებს მკაფიოდ გამოხატულ თანხმობას

- დამუშავებაზე კონტროლი უნდა განახორციელოს მონაცემთა დამმუშავებელმა. ის ასევე პასუხისმგებელია სამართლებლივ საკითხებზეც

მონაცემთა დამმუშავებელი

- ევროკავშირის სამართალში მონაცემთა დამმუშავებელი არის პირი, რომელიც “დამოუკიდებლად ან სხვებთან ერთად განსაზღვრავს პერსონალურ მონაცემთა დამუშავების მიზნებსა და საშუალებებს”. დამმუშავებლის გადაწყვეტილება ადგენს, თუ რატომ და როგორ უნდა დამუშავდეს მონაცემები.

- ევროპის საბჭოს სამართალში, მოდერნიზებული 108-ე კონვენცია “დამმუშავებელს” განსაზღვრავს შემდეგნაირად: “ფიზიკური ან იურიდიული პირი, საჯარო უწყება, მომსახურების სააგენტო ან ორგანო, რომელსაც დამოუკიდებლად ან სხვებთან ერთად აქვს გადაწყვეტილების მიღების უფლებამოსილება მონაცემთა დამუშავების კუთხით”. ეს უფლებამოსილება შეეხება დამუშავების საშუალებებსა და მიზნებს.

ერთობლივი დამუშავება

- GDPR-ის თანახმად, თუ ორი ან მეტი დამმუშავებელი ერთობლივად განსაზღვრავს მონაცემთა დამუშავების მიზნებსა და საშუალებებს, ისინი ერთობლივ დამმუშავებლად მიიჩნევიან.

- ევროპის საბჭოს სამართლებლივი ჩარჩო უშვებს რამდენიმე დამმუშავებლის, ანუ ერთობლივი დამმუშავებლების არსებობას

- დამმუშავებლემბა სპეციალური შეთანხმებით უნდა განსაზღვრონ თავიანთი ვალდებულებები

- ერთობლივი დამუშავება განაპირობებს ერთობლივ პასუხისმგებლობას ამ საქმეზე. ევროკავშირის სამართლის ფარგლებში ეს ნიშნავს, რომ ერთობლივი დამუშავებისას გამოწვეული მთლიანი ზიანისთვის პასუხი შეიძლება თითოეულ დამმუშავებელს დაეკისროს, რათა მონაცემთა სუბიექტმა ეფექტიანი კომპენსაცია მიიღოს.

უფლებამოსილი პირი

- ევროკავშირის სამართალში უფლებამოსილი პირია ის, ვინც პერსონალურ მონაცემებს ამუშავებს დამმუშავებლის სახელით. უფლებამოსილი პირის საქმიანობა შეიძლება შემოიფარგლებოდეს კონკრეტული დავალებით/კონტექსტით, ან იყოს საკმაოდ ვრცელი და კომპექსური.

- ევროპის საბჭოს სამართალში უფლებამოსილი პირის მნიშვნელობა ევროკავშირის სამართლის მსგავსია

Bodil Lindqvist-ის საქმე

Bodil Lindqvist-ის საქმე შეეხებოდა ერთ-ერთ ინტერნეტგვერდზე სხვადასხვა ადამიანის იდენტიფიცირებას სახელით ან სხვა საშუალებით, როგორიცაა ტელეფონის ნომერი და ინფორმაცია ჰობის შესახებ. CJEU-მ დაადგინა: “ვებგვერდის მეშვეობით სხვადასხვა პიროვნებაზე მითითება და მათი იდენტიფიცირება სახელით ან სხვა საშუალებით, არის პერსონალური მონაცემების დამუშავება მთლიანად, ან ნაწილობრივ ავტომატური საშუალებით”

Google Spain SL, Google Inc. v. Agencia Espanola de Proteccion de Datos (AEPD), Mario Costaja Gonzalez

საქმეში Google Spain SL, 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 ამოსაჭებად. CJEU-მ იმსჯელა და დაადგინა, რომ ამგვარი ქმედება არის “დამუშავება”, მიუხედავად იმისა, რომ საძიებო სისტემის ოპერატორი იმავე ოპერაციებს ახორციელებს სხვა ტიპის ინფორმაციის მიმართ და უკანასკლენს არ განარჩევს პერსონალური მონაცემებისგან.

Frantisek Rynes-ის საქმე

Frantisek Rynes-ის საქმეში ბატონმა რეინეშმა უსაფრთხოების მიზნით სახლში დამონტაჟებული CCTV სისტემის გამოყენებით დააფიქსირა იმ ორი ადამიანის გამოსახულება, რომლებმაც დანჯრები ჩაუმსხვრიეს. ვიდეოჩანაწერი შემდგომ გადაეცა პოლიციას და წარდგენილი იყო სასამართლო პროცესზე. CJEU-მ დაადგინა: “ვინაიდან ვიდეოთვალთვალი მოიცავს საჯარო სივრცეს და. შესაბამისად, მონაცემთა დამუშავება პიროვნების პირადი სივრციდან გარეთ არის მიმართული, იგი ვერ ჩაითვლება ცალსახად “პირად ან ოჯახურ საქმიანობად””

SWIFT-ის საქმე

ე.წ SWIFT-ის საქმეში ევროპიულმა საბანკო ინსტიტუტებმა თავდაპირველად SWIFT დაიქირავეს, როგორც დამმუშავებელი, საბანკო ტრანზაქციების

პროცესში მონაცემთა გადასაცემად. SWIFT-მა ეს მონაცემები, რომლებიც აშშ-ში მდებარე კომპიუტერულ სერვერებზე ინახებოდა, აშშ-ს სახაზინო დეპარტამენტს გაუზიარა – ისე, რომ დამქირავებლისგან პირდაპირი მითითება არ მიუჭია. 29-ე მუხლის სამუშაო ჯგუფმა იმსჯელა შექმნილი სიტუაციის კანონიერებაზე და დაადგინა, რომ SWIFT და მისი დამქირავებელი ევროპული საბანკო ინსტიტუტები იყვნენ ერთობლივი დამმუშავებლები, რომელთაც ევროპელი მომხმარებლის წინაშე ეკისრებოდათ პასუხისმგებლობა მათი მონაცემების აშშ-ს მთავრიბოსთვის გამჟღავნებაზე.

კვირა 4

მონაცემთა მიმღები და მესამე მხარე/პირი

- მესამე მხარე/პირი განსხვავდება მონაცემთა დამმუშავებლისა და უფლებამოსილი პირისგან. GDPR-ის თანახმად, ეს “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.”

- მაგალითად, იმ ორგანიზაციის თანამშრომელი, რომელიც არ არის მონაცემთა დამმუშავებელი – მაშინაც კი, თუ იმავე ჯგუფს ან კომპანიას ეკუთვნის – “მესამე პირად” ჩაითვლება

- მაგალითად, იმ ბანკის ფილიალი, რომელიც მომხმარებელთა ანგარიშებს ამუშავებს, ცენტრალური ფილიალის პირდაპირი უფლებამოსილების ფარგლებში, “მესამე პირად” არ მიიჩნევა

- “მიმღები” ფართო ცნებაა და მხოლოდ “მესამე პირს” არ მოიცავს. GDPR-ის თანახმად, მონაცემთა მიმღები “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)

თანხმობა (2.4)

- თანხმობა, როგორც პერსონალურ მონაცემთა დამუშავების სამართლებლივი საფუძველი, უნდა იყოს ნებაყოფლობითი, ინფორმირებული და კონკრეტული და მკაფიოდ გამოხატავდეს დამუშავებაზე თანხმობის სურვილს

- განსაკუთრებული კატეგორიის მონაცემთა დამუშავება საჭიროებს მკაფიოდ გამოხატულ თანხმობას

- თანხმობა უნდა იყოს მკაფიოდ გამოხატული და დგინდებოდეს მონაცემთა სუბიექტის ნებაყოფლობითი, კონკრეტული და ინფორმირებული სურვილი მის მონაცემთა დამუშავების შესახებ

- მონაცემთა სუბიექტი უფლებამოსილია, ნებისმიერ დროს გამოითხოვოს თანხმობა

- წერილობითი განცხადების კონტექსტში, რომელიც სხვა საკითხებსაც მოიცავს, თანხმობაზე მოთხოვნა უნდა იყოს მკაფიო, მარტივი ენით დაწერილი, გასაგები და ადვილად ხელმისაწვდომი, თანხმობა კი ნათლად იყოს გამოყოფილი სხვა საკითხებისგან; თუ ეს განაცხადი არღვევს GDPR-ს, მას არ ექნება შესასრულებლად სავალდებულო ძალა

დამუშავების კანონიერების, სამართლიანობისა და გამჭირვალობის პრინციპები (3.1)

- კანონიერების, სამართლიანობისა და გამჭირვალობის პრინციპები ვრცელდება მონაცემთა ნაბისმიერი სახლის დამუშავებაზეც

- GDPR-ის თანახმად, მონაცემთა დამუშავება კანონიერია, თუ არსებობს:
    - მონაცემთა სუბიექტის თანხმობა;

    - ხელშეკრულების დადების საჭიროება;

    - სამართლებლივი ვალდებულება;

    - მონაცემთა სუბიექტის ან სხვა ფიზიკური პირის საციცოცხლო 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 მეთ.

- პერსონალური მონაცემები უნდა დამუშავდეს სამართლიანად
    - მონაცემთა სუბიექტი ინფორმირებული უნდა იყოს რისკების შესახებ, რათა დამუშავებას არ მოჰყვეს გაუთვალისწინებელი უარყოფითი შედეგები

- პერსონალური მონაცემები უნდა დამუშავდეს გამჭირვალედ.
    - 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

K.H and Others v. Slovakia

საქმეში K.H and Others v. Slovakia განმცხადებლებს ბოშური წარმოშობის ქალებს – აღმოსავლეთ სლოვაკიაში მდებარე ორ საავამდყოფოში გაუწიეს სამედიცინო მომსახურება ორსულობისა და მშობიარობის დროს. ამის შემდეგ, მიუხედავად არაერთი მცდელობისა ვერცერთმა მათგანვა ვერ შეძლო დაორსულება. ეროვნულმა სასამართლოებმა საავადმყოფოებს მოსთვოვეს, 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 ბოროტად გამოყენების საფრთხე. სახელმწიფომ საკმარისად მყარი მიზეზებით ვერ დაასაბუთა თავისი უარი, განმცხადებლებს ჰქონდათ წვდომა მათი ჯანმრთელობის შესახებ ინფორმაციაზე. სასამართლომ საქმეში დაადგინა მე-8 მუხლის დარღვევა, რაც გულისხმობს, რომ ნებისმიერ ადამიანს აქვს თავის პირად მონაცემებზე წვდომის უფლება.

Haralambie v. Romania

საქმეში Haralambie v. Romania განმცხადებლის მოთვონა მის შესახებ საიდუმლო სამსახურის ხელთ არსებული ინფორმაციის ხელმისაწვდომობაზე მხოლოდ 5 წლის შემდეგ დააკმაყოფილეს. EctHR-მა კიდევ ერთხელ ხაზგასმით აღნიშნა, რომ პირებს, რომლებიც საჯარო უწყებების ხელთ არსებულ პერსონალური ფაილების სუბიექტები არიან, აქვთ ამ ფაილებზე წვდომის სასიცოცხლო ინტერესი და ხელისუფლებას ევალებოდა შესაბამისი ეფექტიანი პროცედურის უზრუნვეყოფა.
სასამართლომ საქმეში დაადგინა კონვენციის მე-8 მუხლის დარღვევა.

Smaranda Bara and Others v. Presidentele Casei Nationale de Asigurari de Sanatate, Casa Nationala de Administrare Fiscala (Anaf)

საქმეში Smaranda Bara and Others v. Presidentele Casei Nationale de Asigurari de Sanatate, Casa Nationala de Administrare Fiscala (Anaf) რუმინეთის ეროვნულმა საგადასახადო ორგანომ თვითდასაქმებულთ პირდა შემოსავლების საგადასახადო მონაცემები გადასცა ჯანმრთელობის დაზღვევის ეროვნულ ფონდს, რის საფუძველზეც განისაზღვრა ჯანმრთელობის დაზღვევის გადასახადის ოდენობა. CJEU-მ იმსჯელა, უნდა ეცნობებინათ თუ არა მონაცემთა სუბიექტებისათვის 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 სუბიექტის ინფორმირება ამის შესახებ.

კვირა 5

3.2 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 შემთვევებსაც, საჯარო ან სამედიცინო/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

- მონაცემთა დამუშავების ნებისმიერ ახალ მიზანს, რომელიც თავდაპირველ ამოცანას არ შეესაბამება, უნდა ჰქონდეს სამართლებლივი საფუძველი. იგი ვერ დაეყრდნობა იმ ფაქტს, რომ მონაცემთა მიღება-დამუშავება დავდაპირველად მოხდა სხვა კანონიერ კანონიერი მიზნის საფუძველზე. კანონიერი დამუშავება, თავის მხრივ, შემოიფარგლება მხოლოდ საწყისი მიზნით და ნებისმიერი ახალი ამოცანა საჭიროებს ცალკე სამართლებლივ საფუძველს. მაგალითად, პერსონალურ მონაცემთა მესამე პირისათვის გამჟავნება ახალი მიზნებით გულდასმით უნდა განიხილონ, რაგან ასეთი გამჟღავნება შეიძლება საჭიროებდეს დამატებით სამართლებლივ საფუძველს, რომელიც მონაცემთა გროვების საFუძვლისგან განსხვავდება
- მონაცემების გამოყენება სტატისტიკისთვის, არ საჭიროებს დამატებით საფუძვლებს, რადგან სტატისტიკა შეესაბამება თავდაპირველ მიზანს. ამიტომ არ არის საჭირო მონაცემთა სუბიექტის თანხმობა

3.3 მონაცემთა მინიმიზაციის პრინციპი

- მონაცემები უნდა დამუშავდეს მხოლოდ იმ მოცულობით, რომელიც საჭიროა ლეგიტიმური მიზნის მისაღწევად.

- პერსონალური 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

- უნდა დამუშავდეს მხოლოდ ისეთი მონაცემები, რომლებიც “შესაბამისი და რელევატურია, მოცულობა კი არ აჭარბებდეს მიზანს, რისთვისაც ისინი შეგროვდა და/ან დამუშავდა”. დამუშავებისთვის შერჩეულ მონაცემთა კატეგორიები საჭირო უნდა იყოს დამუშავების ოპერაციების გაცხადებული მიზნის მისაღწევად, ხოლო დამმუშავებელი მკაცრად შეიძრუდოს მხოლოდ იმ მონაცემთა შეგროვებით, რომლებიც პირდაპირ შეესაბამება კონკრეტულ მიზანს

3.4 მონაცემთა სიზუსტის პრინციპი
- მონაცემთა დამმუშავებელი ვალდებულია, მონაცემთა სიზუსტის პრინციპი დანერგოს დამუშავების ყველა ოპერაციაში

- არაზუსტი მონაცემები უნდა წაიშალოს, ან დაუყონებლივ გასწორდეს

- შესაძლებელია, საჭირო გახდესმონაცემთა რეგულარული შემოწმება და განახლება, სიზუსტის დასაცავად

- ზოგიერთ სიტუაციაში, არსებობს მონაცემთა განახლებისა და სიზუსტის შემოწმების აბსოლიტური საჭიროება, იმ პოტენციური ზიანის გამო, რომელიც შეიძლება არაზუსტმა მონაცემებმა მოუტანოს მონაცემთა სუბიექტს

3.5 შენახვის ვადის შეზღუდვის პრინციპი

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

- GDPR-ის 108-ე მოდერნიზებული კონვენციის მე-5 მუხლის 4(ე) ქვეპუნქტის თანახმად, პერსონალური მონაცემები "უნდა შეინახონ ისეთი ფორმით, რომელიც იძლევა მონაცემთა სუბიექტის იდენტიფიცირების შესაძლებლობას არაუმეტეს იმ დროით, რომელიც აუცილებელია მონაცემთა დამუშავების მიზნებისთვის". შესაბამისად, აღნიშნული მიზნების მიღწევისთანავე საჭიროა მონაცემთა წაშლა ან ანონიმიზება

3.6 მონაცემთა უსაფრთხოების პრინციპი

- პერსონალურ მონაცემთა უსაფრთხოებასა და კონფიდენციალობას უდიდესი მნიშვნელობა ენიჭება მონაცემთა სუბიექტზე უარყოფითი გავლენის თავიდან ასაცილებად

- უსაფრთხოების ზომები შეიძლება იყოს ტექნიკური და/ან ორგანიზაციული

- ფსევდონიმიზაცია არის პროცესი, რომელსაც შეუძლია პრსონალური მოანცემების დაცვა

- უსაფრთხოების ზომების შესაბამისობა უნდა განისაზღვროს თითოეულ შემთხვევაში და რეგულარულად გადაიხედოს

3.7 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 განონმდებლობისა და საკუთარ ვალდებულებებთან

- დამმუშავებელმა, მონაცემთა სუბიექტს, საზოგადოებისა და საზედამხედველო ორგანოების წინაშე, ნებისმიერ დროს უნდა შეძლოს მონაცემთა დაცვის დებულებებთან შესაბამისობის დადასტურება. უფლებამოსილმა პირდა უნდა შეასრულოს სხვა გარკვებული ვალდებულებებიც, რომელიც მკაცრად უკავშირდება ანგარიშვალდებულებას მაგ: დამუშავების ოპერაციების აღრიცხვა და მონაცემთა დაცვის ოფიცრის დანიშვნა

კვირა 9

(კვირა 6 აღდგომის გამო გაცდა, კვირა 7 ხათუნას მიზეზის გამო და კვირა 8 შუალედურები იყო ხდ)

4.1 კანონიერი დამუშავების წესები

- პერსონალურ მონაცემთა კანონიერი დამუშავება უნდა აკმაყოფილებდეს შემდეგ კრიტერიუმებს:

- ხორციელდებოდეს მონაცემთა სუბიექტის თანხმობის საფუძველზე

- ითვალისწინებდეს სახელშეკრულებო ურთიერთობას

- საჭირო იყოს მონაცემთა დამმუშავებლის სამართლებლივი ვალდებულების შესასრულებლად

- მოითხოვდეს მონაცემთა სუბიექტის ან სხვა პირის სასიცოცხლო ინტერესები

- აუცილებელი იყოს საჯარო ინტერესის სფეროში შემავალი ამოცანების შესასრულებლად

- განაპირობებდეს მონაცემთა დამმუშავებლის ან მესამე პირის კანონიერი ინტერესები, მხოლოდ იმ შემთხვევაში, თუ ამ ინტერესებს არ გადაწონის მონაცემთა სუბიექტის ინტერესები ან ფუნდამენტური უფლებები

- განსაკუთრებული კატეგორიის პერსონალური მონაცემების კანონიერ დამუშავებაზე ვცრელდება სპეციალური, უფრო მკაცრი რეჟიმი

თანხმობა

- ევროპის საბჭოს სამართალში, თანხმობაზე მიუთითებს მოდერნიზებული 108-ე კონვენციის 5(2) მუხლი; ასევე EctHR-ის პრეცენტენტული სამართალი და ევროპის საბჭოს რამდენიმე რეკომენდაცია

- ევროკავშირის სამართალში თანხმობა, როგორც მონაცემთა კანონიერი დამუშავების საფუძველი, მკაცრად არის დადგენილი GDPR-ის მე-6 მუხლით. მასზე მკაფიოდ მიუთითებს ქარტიის მე-8 მუხლიც

- უნდა იყოს ნებაყოფლობითი/თავისუფალი

- უნდა იყოს ინფორმირებული

- უნდა იყოს კონკრეტული

- მკაფიო

- არასწრულწლოვანისგან თანხმობის მიღების სპეციალურ წესებს საინფორმაციო საზოგადოების მომსახურებასთან დაკავშირებთი, მათ ადგენს რეგულაციის მ-8 მუხლი

ნებაყოფლობითი/თავისუფალი თანხმობა

- მოდერნიზებული 108-ე კონვენციის ფარგლებში, მონაცემთა სუბიექტის თანხმობა უნდა “იყოს გამიზნული არჩევანის ნებაყოფლობითი გამოხატულება”

- 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”

- ამ კუთხით, ევროკავშირის სამართალში აღნიშნულია, რომ თანხმობა არ მიიჩნევა ნებაყოფლობითად, თუ “მონაცემთა სუბიექტს არ აქვს რეალური და

თავისუფალი არჩევანის საშუალება, არ შეუძლია უარის თქმა ან თანხმობის გამოთხოვა ისე, რომ არ გახდეს მისთვის საზიანო”.

- ნებაყოფლობითი თანხმობა ეჭვქვეშ დგება, როდესაც, გარკვეული სუბორიენტაციის მიხედვით, მონაცემთა დამმუშავებლისა (თანხმობის მიმღები) და მონაცემთა სუბიექტის (თანხმობის გამცემი) შორის მნიშვნელოვანი ეკონომიკური ან სხვა სახის დისბალანსია. ამის ტიპიური მაგალითია დამსაქმებლის მიერ პერსონალურ მონაცემთა დამუშავება დასაქმებულთან ურთიერთობის კონტექსტში

- მაგალითი: ერთ-ერთი მსხვილი კომპანია აპირებს საკუთარი თანამშრომლების ცნობარის შედგებას, სადაც წარმოდგენილი იქნება მათი სახელი, ინფორმაცია სამსახურეობრივი ფუნქციების შესახებ და სამსახურეობრივი მისამართები. ცნობარი იქნება მხოლოდ და მხოლოდ კომპანიის შიდა კომუნიკაციის გასაუმჯობესებლად. კადრების განყოფილების ხელმძღვანელმა წარმოადგინა წინადადება ცნობარში თანამშრომელთა ფოტოების შეტანის შესახებ, რაც გააიოლებს შეხვედრაზე კოლეგების იდენტიფიცირებას. დასაქმებულთა წარმომადგენლების მოთხოვნით, სურთაბი ცხობარში უნდა შეიტანონ მოლოდ დასაქმებულთა ნებართვის საფუძველზე.

- ასეთ ვითარებაში, დასაქმებულის თანხმობა უნდა ჩაითვალოს სამართლებრივ საფუძვლად ცნობარში ფოტოების დამუშავებისთვის, ვინაიდან შეგვიძლია ვივარაუდოთ, რომ საკუთარი ფოტოს გამოქვეყნებაზე უარი დასაქმებულს უარყოფით შედეგს არ მოუტანს

ინფორმირებული თანხმობა

- მონაცემთა სუბიექტს გადაწყვეტილების მიღებამდე საკმარისი ინფორმაცია უნდა ჰქონდეს. ინფორმირებული თანხმობა ძირითადად მოიცავს იმ საკითხის ზუსტ და მარტივ აღწერას, რომელზეც იგი მოითხოვება.

- “შესაბამის პირს მკაფიო და გასაგები ფორმით უნდა მიეწოდოს ზუსტი და სრული ინფორმაცია ყველა საჭირო საკითხზე, როგორიცაა დამუშავებული მონაცემების ბუნება, მათი შესაძლო მიმღებები და მონაცემთა სუბიექტის უფლებები”. ინფორმირებული თანხმობისთვის შესაბამის პირს უნდა ეცნობოს დამუშავებაზე უარის თქმის შედეგებიც

- GDPR და მოდერნიზებული 108-ე კონვენციის განმარტებითი ბარათი მოიცავს ამ ცნების განმარტებას. GDPR-ის შესავალ ნაწილში აღნიშნულია “ინფორმირებული თანხმობა ნიშნავს, რომ მონაცემთა სუბიექტისთვის ცნობილი უნდა იყოს, სულ მცირე, დამმუშავებლის ვინაობა და დამუშავების მიზანი”.

- მონაცემთა დამმუშავებელმა მონაცემთა სუბიექტს უნდა შეატყობინოს გადაცემასთან დაკავშირებული რისკები, შესაბამისობაზე გადაწყვეტილებასა და სათანადო დაცვის ზომების არარსებობის გამო

კონკრეტული თანხმობა

- იმისათვის, რომ თანხმობას ჰქონდეს კანონიერი ძალა, უნდა მიემართებოდეს კონკრეტული დამუშავების მიზანს, რომელიც ნათლად და მკაფიოდ არის აღწერილი. ეს მჭიდროდ უკავშირდება თანხმის მიზანზე მონაცემთა სუბიექტისთვის მიწოდებული ინფორმაციის ხარისხს

მკაფიო თანხმობა

- 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

- მაგალითად, ეს შეიძლება იყოს “ჩვენი სერვისების გამოყენებით, თქვენ ეთანხმებით პერსონალურ მონაცემთა დამუშავებას”. ასეთ შემთხვევაში მონაცემთა დამმუშავებელმა უნდა იზრუნველყოს, რომ მომხმარებელი ასეთ განაცხადს დაეთანხმება ინდივიდუალურად და არაავტომატურად

- თუ თანხმობა გაიცემა წერილობითი ფორმით, კონტრაქტის ფარგლებში, პერსონალურ მონაცემთა დამუშავებაზე თანხმობა ცალკე უნდა განისაზღვროს და, ნებისმიერ შემთხვევაშიმ “არსებობდეს უსაფრთხოების ზომები, რომელიც უზრუნველყოფს თანხმობის გაცემას და მისი მასშტაბის გაცნობიერებას მონაცემთა სუბიექტის მხრიდან”

თანხმობის მოთხოვნა ბავშვების შემთხვევაში

- GDPR ბავშვებისთვის განსაკუთრებულ დაცას ითვალისწინებს საინფორმაციო საზოგადოების მომსახურების კონტექსტში, ვინაიდან “მათთვის შეიძლება ნაკლებად იყოს ცნობილი რისკები, შედეგები, დაცვის მექანიზმები და უფლებები, რომელიც უკავშირდება პერსონალური მონაცემების დამუშავებას”

- ევროკავშირის სამართალში, როდესაც საინფორმაციო საზოგადოების მომსახურების მიმწოდებელი ამუშავებს 16 წლამდე პირთა პერსონალურ მონაცემებს თანხმობის საფუძველზე, ასეთი დამუშავება კანონიერად ჩაითვლება “მხოლოდ იმ შემთხვევაში, თუ თანხმობა გაცემულია/დამუშავება ნებადართულია მშობლის უფლების მქონე პირის მიერ”

თანხმობის ნებმისიერ დროს გამოთხოვნის უფლება

- GDPR აწესებს თანხმობის ნებისმიერ დროს გამოთხოვნის ზოგად უფლებას. მონაცემთა სუბიექტს ეს უფლება უნდა განემარტოს თანხმობის გაცემამდე, მისი რეალიზება კი შეეძლოს ნებისმიერ დროს და საკუთარი შეხედულებისამებრ.

- მონაცემთა სუბიექტი არ არის ვალდებული, ახსნას, თუ რატომ გამოითხოა თანხმობა.

- გამოთხოვამ არ უნდა გამოიწვიოს რაიმე უარყოფითი შედეგი, გარდა იმ სარგებლის შეწყვეტისა, რომელიც უკავშირდებოდა მონაცემთა გამოყენებას სუბიექტის მიერ გამოხატულ თანხმობის საფუძველზე;

- ასევე, გამოთხოვა ისეთივე მარტივი უნდა იყოს, როგორც გაცემა

- თანხმობა-გამოთხოვის შესაძლებლობა რაიმე ზიანის გარეშე, ან გამოთხოვა არ არის ისეთივე ადვილი, როგორც მისი გამოხატვა

Y v. Turkey

საქმეში Y v. Turkey განმცხადებელს ჰქონდა აივ დადებითი სტატუსი. ვინაიდან სააბადმყოფოში მიყვანისას იგი უგონოდ იყო, კლინიკის პერსონალს სასწრაფო დახმარების ექიმებმა დაუდასტურეს პაციენტის აივ დადებითი სტატუსი. განმცხადებელი EctHR-ის წინაშე აცხადებდა, რომ ამ ინფორმაციის გამჟღავნებით დაირღვა მისი პირადი ცხოვრების პატივისცემის უფლება. თუმცა, საავადმყოფოს პერსონალის უსაფრთხოების დაცვის საჭიროების გათვალისწინებით, სასამართლომ ამ ინფორმაციის გაზიარება განმცხადებლის უფლებების დარღვევად არ მიიჩნია.

კვირა 10

განსაკუთრებული კატეგორიის მონაცემთა დამუშავება

- ზოგადად, განსაკუთრებული კატეგორიის მონაცემების დამუშავება აკრძალულია, თუმცა არსებობს გამონაკლისი შემთხვევების ამომწურავი ჩამონათვალი, რომელიც წარმოდგენილია რეგულაციის მე-9 მუხლის მე-2 პუნქტში. ესენია:

- არსებობს მონაცემთა სუბიექტის მკაფიო თანხმობა დამუშავებაზე

- მონაცემებს ამუშავებს არაკომერციული ორგანიზაცია, კერძოდ, კანონიერი საქმიანობისას პოლიტიკური, ფილოსოფიური, რელიგიური ან პროფესიული კავშირის მიზნებით და იმ პირობით, რომ დამუშავება ეხება მხოლოდ მის მოქმედ ან ყოფილ წევრებს, რომლებთაც მუდმივი კავშირი აქვთ ორგანიზაციასთან, მისი ამონაცებიდან გამომდინარე

- დამუშავება მოიცავს ისეთ მონაცემებს, რომლებიც თვითონ სუბიექტმა საჯაროდ გამოაქვეყნა

- დამუშავება აუცილებელია შემდეგი მიზნებისთვის:
    - დამმუშავებლის ან მონაცემთა სუბიექტის მოვალეობებისა და კონკრეტული უფლებების განხორციელება, დასაქმების, სოციალური უსაფრთოების ან სოციალური დაცვის კონტექსტში

    - მონაცემთა სუბიექტის ან სხვა ფიზიკური პირის სასიცოცხლო ინტერესების დაცვა (როდესაც მონაცემთა სუბიექტს არ შეუძლია თანხმობის გაცემა)

    - სამართლებლივი მოთხოვნის დადგენა, შესრულება ან დაცვა; ანდა სასამართლო საქმისწევრობა

    - პრევენციული მედიცინა ან შრომითი უსაფრთხოების დაცვა: დასაქმებულის სამუშაო შესაძლებლობათა შეფასება; სამედიცინო დიაგნოზის დასმა; ჯანდაცვა ან სოციალური დაცვა; ასევე, აღნიშნული სფეროსა და შესაბამისი მომსახურების მართვა ევროკავშირის ან წევრი სახელმწიფოს კანონმდებლობისა თუ სამედიცინო სფეროს სპეციალისტთან დადებული ხელშეკრულების საფუძველზე;

- საჯარო ინტერესებისათვის არქივირება, სამეცნიერო/ისტორიული კვლევა ან სტატისტიკის წარმოება

- საჯარო ინტერესი საზოგადოებრივი ჯანდაცვის სფეროში

- მნიშვნელოვანი საჯარო ინტერესი

მონაცემთა სუბიექტის მკაფიო თანხმობა

- ევროკავშირის კანონმდებლობაში მონაცემთა კანონიერი დამუშავების უპირველესი პირობა – როგორც განსაკუთრებული კატეგორიის, ისე სხვა მონაცემებისთვის – არის მონაცემთა სუბიექტის თანხმობა. განსაკუთრებული კატეგორიის მონაცემების შემთხვევაში, ასეთი თანხმობა უნდა იყოს მკაფიო. ამავდროულად, ევროკავშირის ან წევრი სახელმწიფოს კანონმდებლობა შეიძლება ადგენდეს, რომ განსაკუთრებული კატეგორიის მონაცემთა დამუშავების აკრძალვას მონაცემთა სუბიექტი ვერ შეეწინააღმდეგება (მაგ: როდესაც დამუშავება მონაცემთა სუბიექტს უჩვეულო საფრთხეს უქმნის)

მონაცემთა სუბიექტის სასიცოცხლო ინტერესები

- ევროკავშირის კანონმდებლობით, განსაკუთრებული კატეგორიის მონაცემები, სხვა ტიპის მონაცემთა მსგავსად, შეიძლება დამუშავდეს მონაცემთა სუბიექტის ან სხვა ფიზიკური პირის სასიცოცხლო ინტერესების გამო.

- პერსონალური მონაცემების დამუშავება შესაძლებელია სხვა პირის სასიცოცხლო ინტერესის საფუძველზე, თუ "დამუშავება ცალსახად ვერ მოხდება სხვა სამართლებლივი საფუძვლით."

- ზოგ შემთხვევაში, შესაძლოა, პერსონალურ მონაცემთა დამუშავება იცავდეს როგორც ცალკეული პირის, ისე საჯარო ინტერესებს (მაგ: როცა დამუშავება ხდება ჰუმანიტარული მიზნებით)

საქველმოქმედო ან არაკომერციული ორგანიზაციები

- პერსონალურ მონაცემთა დამუშავება ნებადართულია ფონდების, ასოციაციების ან სხვა არაკომერციული ორგანიზაციების კანონიერი საქმიანობის ფარგლებშიც, რომლებსაც პოლიტიკური, ფილოსოფიური, რელიგიური ან პროფესიული კავშირის მიზნები აქვთ. ამავდროულად, დამუშავება უნდა ეხებოდეს მხოლოდ და მხოლოდ ამ ორგანიზაციის მოქმედ ან ყოფილ წევრებს, ან ვისაც მასთან რეგულარული კონტაქტი აქვს. ასეთი ორგანიზაციების მიერ განსაკუთრებული კატეგორიის მონაცემების გამჟღავნება მონაცემთა სუბიექტის თანხმობის გარეშე დაუშვებელია

მონაცემთა სუბიექტის მიერ ცალსახად საჯაროდ გამოქვეყნებული მონაცემები

- GDPR-ის მე-9 (ე) მუხლის თანახმად, დამუშავება არ იკრძალება თუ იგი ეხება მონაცემთა სუბიექტის მიერ ცალსახად საჯაროდ გამოქვეყნებულ პერსონალურ მონაცემებს.

- რეგულაცია არ განმარტავს "მონაცემთა სუბიექტის მიერ ცალსახად საჯაროდ გამოქვეყვებულ მონაცემებს", ვინაიდან ეს გამონაკლისია განსაკუთრებული კატეგორიის მონაცემთა დამუშავებაზე დაწესებული

აკრძალვისგან, თუმცა მისი შინაარსი უნდა გავიგოთ, როგორც მონაცემთა სუბიექტის მიერ საკუთარი მონაცემების განზრახ გამოქვეყნება საჯაროდ.

- ამრიგად, თუ ტელევიზიით გადაიცემა სათვალთვალო კამერტიდან ამოღებული ვიდეოჩანაწერი, სადაც ჩანს, როგორ დაშავდა მეხანძრე შენობის ევაკუაციისას, ეს ვერ ჩაითვლება მეხანძრის მიერ ცალსახად საჯაროდ გამოქვეყნებულ მონაცემებად.

- მეორე მხრივ, თუ მეხანძრე გადაწყვეტს, რომ ინციდენტის შესახებ ინფორმაცია, ვიდეომასალა და ფოტოები განათავსოს საჯარო ვებგვერდზე, ეს მისი მხრიდან იქნება წინასწარგანზრახული, ნათლად გამოხატული მოქმედება პერსონალურ მონაცემთა საჯაროდ გამოსაქვეყნებლად.

- უნდა აღინიშნოს, რომ მონაცემთა გამოქვეყნება არის არა თანხმობა, არამედ ნებართვა განსაკუთრებული გატეგორიის მონაცემთა დამუშავების შესახებ

- დამუშავებული პერსონალური მონაცემების გამოქვეყნება მონაცემთა სუბიექტის მიერ დამმუშავებელს არ ათავისუფლებს მონაცემთა დაცვის კანონმდებლობით გათვალისწინებული ვალდებულებებისგან (მაგ: მიზნის შეზღუდვის პრინციპი კვლავ ვრცელდება პერსონალურ მონაცემებზე მიუხედავად იმისა, რომ ეს მონაცემები საჯაროდ ხელმისაწვდომია)

სამართლებლივი მოთხოვნები

- GDPR-ის თანახმად, განსაკუთრებული კატეგორიის მონაცემთა დამუშავება ნებადართულია, თუ ეს აუცილებელია სამართლებლივი მოთხოვნების დასადგენად, შესასრულებლად, ან დასაცავად სასამართლო საქმიანობის დროს, ან ადმინისტრაციული პროცედურისა თუ დავის არასასამართლო გზით მოგვარებისას. ასეთ შემთხვევაში დამუშავება რელევანტური უნდა იყოს კონკრეტული სამართლებლივი მოთხოვნის შესრულებისა თუ დაცვისთვის და მას ითხოვდეს სამართლებლივი დავის ერთ-ერთი მხარე

- საკუთარი ფუნქციების განხორციელების პროცესში, სასამართლოს აქვს განსაკუთრებული კატეგორიის მონაცემთა დამუშავების უფლება სამართლებლივი დავის გადაწყვეტის კონტექსტში. ამ ტიპის მონაცემთა მაგალითებია: გენეტიკური ინფორმაცია მამომის ან დედობის დადგენისას; და ჯანმრთელობის მდგომარეობა, როდესაც მტკიცებულებათა ნაწილი ეხება მსხვერპლებისთვის მიყენებული ზიანის დეტალებს

მნიშვნელოვანი საჯარო ინტერესი

- GDPR-ის მე-9 მუხლის 2(ზ) პუნქტის თანახმად, წევრ სახელმწიფოებს უფლება აქვთ, დაადგინონ დამატებითი გარემოებები, სადაც დაშვებულია განსაკუთრებული კატეგორიის მონაცემთა დამუშავება, თუ კი:

- ეს აუცილებელია მნიშვნალოვანი საჯარო ინტერესიდან გამომდინარე

- გათვალისწინებულია ევროპული ან ეროვნული კანონმდებლობით

- ევროპული ან ეროვნული კანონმდებლობა პროპორციულია, პატივს სცემს მონაცემთა დაცვის უფლებას და ითვალისწინებს სათანადო და

კონკრეტულ ღონისძიებებს მონაცემთა სუბიექტის ფუნდამენტური უფლებებისა და ინტერესების დასაცავად

- ამის თვალსაჩინო მაგალითია ჯანდაცვის ფაილური სისტემა

- ასეთ სისტემაში ნებადართულია ჯანდაცვის სფეროს პროცესიონალთა მიერ პაციენტის მკურნალობის პროცესში შეგროვებულ მონაცემებზე უფრო ფართო წვდომა ჯანდაცვის სხვა პროვაიდერებისთვის, რომელიც იმავე პაციენტს ემსახურება

განსაკუთრებული კატეგორიის მონაცემთა დამუშავების სხვა საფუძვლები

- GDPR-ის თანახმად, განსაკუთრებული კატეგორიის მონაცემთა დამუშავება შესაძლებელია, თუ ის აუცილებელია შემდეგი მიზნებიდან გამომდინარე:

- პრევენციული ან ოკუპაციური მედიცინა, ანდა შრომითი უსაფრთხოების დაცვა; დასაქმებულის სამუშაო შესაძლებლობათა შეფასება; სამედიცნო დიაგნოზის დასმა; ჯანდაცვა ან სოციალური დაცვა; ასევე, აღნიშნული სფეროსა და შესაბამისი მომსახურების მართვა ევროკავშირის ან მისი წევრი სახელმწიფოს კანონმდებლობის, ან სამედიცინო სფეროს სპეციალისტთან დადებული ხელშეკრულების საფუძველზე

- საზოგადოებრივ ჯანმრთელობასთან დაკავშირებული საჯარო ინტერესი, როგორიცაა, მაგალითად: დაცვა ჯანმრთელობის სერიოზული საერთაშორისო საფრთხეებისგან; მაღალხარისხიანი და უსაფრთხო ჯანდაცვის მომსახურების, სამედიცინო პროდუქტებისა და მოწყობილობების უზრუნველყოფა ევროკავშირის ან წევრი სახელმწიფოს კანონმდებლობის საფუძველზე, რომელშიც გათვალისწინებულია სათანადო ზომები მონაცემთა სუბიექტის უფლებებისა და თავისუფლებების დასაცავად

- არქივირება, სამეცნიერო/ისტორიული კვლევა ან სტატისტიკის წარმოება ევროკავშირის ან წევრი სახელმწიფოს კანონმდებლობის შესაბამისად. იგი უნდა იყოს დასახული მიზნის პროპორციული, პატივს სცემდეს მონაცემთა დაცვის უფლებას და ითვალისწინებდეს სათანადო და კონკრეტულ ზომებს მონაცემთა დაცვის სუბიექტის ფუნდამენტურ უფლებებისა და ინტერესების დასაცავად

ეროვნული კანონმდებლობით გათვალისწინებული დამატებითი პირობები

- GDPR-ის თანახმად, წევრ სახელმწიფოებს უფლება აქვთ, შემოიღონ ან შეინარჩუნონ დამატებითი პირობები, მათ შორის, შეზღუდვები გენეტიკურ, ბიომეტრიულ ან ჯანმრთელობასთან დაკავშირებულ მონაცემთა დამუშავებაზე

კვირა 11

დამუშავების უსაფრთხოების წესები (4.2)

- დამუშავების უსაფრთხოების წესები მონაცემთა დამმუშავებელსა და უფლებამოსილ პირს ავალდებულებს შესაბამისი ტექნიკური და ორგანიზაციული ზომების დანერგვას დამუშავების პროცესში ნებისმიერი უნებართვო ჩარევის პრევენციისთვის

- მონაცემთა უსაფრთხოების აუცილებელი დონე განისაზღვრება შემდეგი ფაქტორებით:

- ბაზარზე ხელმისაწვდომი უსაფრთხოების ზომები ნებისმიერი ტიპის დამუშავებისთვის

- ხარჯები

- საფრთვე, რომელსაც დამუშავება უქმნის მონაცემთა სუბიექტის ფუნდამენტურ უფლებებსა და თავისუფლებებს

- პერსონალური მონაცემების კონფიდენციალობა იმ ზოგადი პრინციპების ნაწილია, რომელსაც აღიარებს მონაცემთა დაცვის ზოგადი რეგულაცია

- როგორც ევროკავშირის, ისე ევროპის საბჭოს სამართალში, დამმუშავებელს, პერსონალურ მონაცემთა დამუშავების პროცესში, ეკისრება გამჭირვალეობისა და ანგარიშვალდებულების ზოგადი ვალდებულება, კერძოდ, მონაცემთა უსაფრთხოების დარღვევებთან დაკავშირებით.

- ასეთ შემთხვევაში, მონაცეMთა დამმუშავებელი ვალდებულია, უსაფრთხოების დარღვევის შესახებ შეატყობინოს საზედამხედველო ორგანოებს, გარდა იმ შემთხვევისა, როცა ნაკლებია რისკი, რომ ეს დარღვევა შელახავს ფიზიკურ პირთა უფლებებსა და თავისუფლებებს

- აუცილებელია მონაცემთა სუბიექტის ინფორმირებაც პერსონალურ მონაცემთა უსაფრთხოების დარღვევაზე, თუკი სავარაუდოა, რომ დარVევა მნიშვნელოვან საფრთხე შეუქმნის ფიზიკურ პირთა უფლებებსა და თავისუფლებებს

მონაცემთა უსაფრთხოების ელემენტები (4.2.1)

- ევროკავშირის კანონმდებლობის შესაბამისი დებულებების თანახმად:
“უახლესი ტექნოლოგიების, განხორციელების ხარჯების, დამუშავების ბუნების, მოცულობის, კონტექსტისა და მიზნების, ასევე, მონაცემთა სუბიექტის უფლებებისა და თავისუფლებებისათვის სავარაუდო საფრთხეების გათვალისწინებით, მონაცემთა დამმუშავებელმა და უფლებამოსილმა პირმა უნდა მიიღონ რისკების შესაბამისი ტექნიკური და ორგანიზაციული ზომები უსაფრთხოების უზრუნველსაყოფად”

- ეს ზომები მოიცავს შემდეგ ასპექტებს:

- პერსონალურ მონაცემთა ფსებდონიმიზაცია და დაშიფვრა

- დამუშავების სისტემებისა და სერვისების მუდმივი კონფიდენციალობა, ხელშეუხებლობა, ხელმისაწვდომობა და მოქნილობა

- ფიზიკური ან ტექნიკური ინციდენტის შემთხვევაში, პერსონალურ მონაცემთა წვდომისა და ხელმისაწვდომობის დროული აღდგენა

- დამუშავების უსაფრთხოების ტექნიკურ და ორგანიზაციულ საშუალებათა ეფექტიანობის რეგულარული შემოწმება და შეფასება

ევროპის საბჭოს კანონმდებლობა შეიცავს მსგავს დებულებას:

"თითოეულმა მხარემ უნდა უზრუნველყოს, რომ მონაცემთა დამმუშავებელი და, საჭიროების შემთხვევაში, უფლებამოსილი პირი, მიიღებენ უსაფრთხოების სათანადო ზომებს ისეთი რისკების აღმოსაფხვრელად, როგორიცაა შემთხვევითი ან არასანქცირებული წვდომა პერსონალურ მონაცემებზე, მათი განადგურება, დაკარგვა, გამოყენება, შეცვლა ან გამჟღავდება"

- ევროკავშირისა და ევროპის საბჭოს სამართალში მონაცემთა უსაფრთხოების დარღვევა, რამაც შესაძლოა გავლენა იქონიოს ფიზიკური პირის უფლებებისა და თავისუფლებებზე, დამმუშავებელს ავალდებულებს დარღვევის შეტყობინებას საზედამხედველო ორგანოსთვის

- მონაცემთა უსაფრთხოება არ მიიღწევა მხოლოდ სათანადო აღჭურვილობის – ტექნოლოგიური და პროგრამული უზრუნველყოფის – დანრგვით, იგი ასევე საჭიროებს შესაბამის შიდა ორგანიზაციულ წესებს. ასეთი შიდა წესები, საუკეთესო შემთხვევაში, უნდა ითვალისწინებდეს ქვემოთ ჩამოთვლილ საკითხება:

- ყველა თანამშრომლისათვის ინფორმაციის რეგულარული მიწოდება მონაცემთა უსაფრთხოების წესებისა და მონაცემთა დაცვის კანონმდებლობით გათვალისწინებული ვალდებულებების, განსაკუთრებით, კონფიდენციალობის პირობების შესახებ

- მონაცემთა დამუშავების საკითხებში პასუხისმგებლობის მკაფიო გადანაწილება და უფლებამოსილებათა ნათლად ჩამოყალიბება, განსაკუთრებით, როცა მიიღება გადაწყვეტილება პერსონალურ მონაცემთა დამუშავებაზე, ასევე, მესამე პირების ან მონაცემთა სუბიექტისთვის გადაცემაზე

- პერსონალურ მონაცემთა გამოყენება მხოლოდ უფლებამოსილ პირთა მიერ დადგენილი ინსტრუქციების ან ზოგადი წესების შესაბამისად

- დაცვა მონაცემთა დამმუშავებლის ან უფლებამოსილი პირის ადგილმდებარეობასა და ტექნიკურ თუ პროგრამულ უზრუნველყოფაზე წვდომისაგან

- პერსონალურ მონაცემებზე წვდომის ნებართვის გაცემა მხოლოდ უფლებამოსილი პირის მიერ და შესაბამისი დოკუმენტაციის საფუძველზე

- ელექტრონული საშუალებებით პერსონალურ მონაცემებზე წვდომის ავტომატიზებული წესები (პროტოკოლი) და შიდა საზედამხედველო ორგანოს მიერ მათი რეგულარული შემოწმება

- მონაცემთა ავტომატიზებული წვდომის გარდა, სხვა ფორმების საგულდაგულოდ დოკუმენტირებაც, მონაცემთა გაცემის უკანონო ფორმათა არარსებობის საჩვენებლად

კონფიდენციალობა (4.2.2)

- ევროკავშირის კანონმდებლობაში GDPR პერსონალურ მონაცემთა კონფიდენციალობას ზოგადი პრინციპის ნაწილად მიიჩნევს. საჯაროდ ხელმისაწვდომი ელექტორნული საკომუნიკაციო მომსახურების მიმწოდებლებს მოეთხოვებათ კონფიდენციალობისა და მომსახურების უსაფრთხოების დაცვა

- მე-5 მუხლის 1(ვ) პინტქის თანახმად, პერსონალური მონაცემები უნდა დამუშავდეს იმგვარად, რომ სათანადო ტექნიკური ან ორგანიზაციული ზომების მეშვეობით, უზრუნველყონ მათი უსაფრთხოება. მონაცემები დაცული უნდა იყოს უკანონო და არაუფლებამოსილი პირების მხრიდან დამუშავების, დაკარგვის, განადგურების ან დაზიანებისგან

- 32-ე მუხლის თანახმად, მონაცემთა დამმუშავებელმა და უფლებამოსილბა პირმა უნდა მიიღონ საბარაუდო რისკების შესაბამისი ტექნიკური და ორგანიზაციული ზომები, უსაფრთხოების მაღალი დონის უზრუნველსაყოფად. ეს ზომები მოიაცევს 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. GDPR-ის 28-ე მუხლის თანახმად, მონაცემთა დამმუშავებელსა და უფლებამოსილ პირს შორის არსებული საბალდებულო ძალის მქონე კონტრაქტი უნდა ითვალისწინებდეს უფლებამოსილი პირის პასუხისმგებლობას, უზრუნველყოს კონფიდენციალობის ან კანონით განსაზღვრული შესაბამისი ვალდებულებების შესრულება დამუშავებაზე პასუხისმგებელ პირთა მხრიდან

- კონფიდენციალობის ვალდებულება არ ვრცელდება, თუ მონაცემებს მოიპოვებს კერძო პირი და არა მონაცემთა დამმუშავებლის ან უფლებამოსილი პირის თანამშრომელი.

- ასეთ დროს GDPR-ის 32-ე და 28-ე მუხლები არ მოქმედებს, რადგან კერძო პირთა მიერ პერსონალური მონაცემების გამოყენება მთლიანად სცდება რეგულაციის მოქმედების სფეროს, თუკი ის ხვდება ე.წ ოჯახური გამონაკლისის ფარგლებში. ოჯახური გამონაკლისი გულისხმობს, პერსონალური მონაცემების გამოყენებას “ფიზიკური პირის მიერ, ცალსახად პირადი ან ოჯახური საქმიანობის ფარგლებში”.

- ე.წ ოჯახური გამონაკლისი არ ვრცელდება: პერსონალურ მონაცემთა გამოქვეყნებაზე ინტერნეტში, როდესაც მონაცემების მიმღებთა რაოდენობა შეუზღუდავია; და მონაცემთა დამუშავებაზე, რომელსაც აქვს პროფესიული ან კომერციული ასპექტები

- კონფიდენციალობის კიდევ ერთი ასპექტია “კომუნიკაციის კონფიდენციალობა”, რომელიც სპეციალური ნორმით (lex specialis) რეგულირდება. ელექტრონულ სივრცეში პირადი ცხოვრების შესახებ

დირექტივით გათვალისწინებული სპეციალური წესები, რომლებიც მიზნად ისახავს ელექტრონული კომუნიკაციების კონფიდენციალობას, წევრ სახელმწიფოებს ავალდებულებს, რომ ნებისმიერ პირს, გარდა მომხმარებლებისა, აუკრძალონ კომუნიკაციებისა და ამასთან დაკავშირებული მეტამონაცემების მოსმენა, მიყურადება, შენახვა ან სხვა სახის წვდომა თუ მონიტორინგი, მომხმარებელთა თანხმობის გაერეშე.

- ეროვნული კანონმდებლობა შესაძლოა უშვებდეს გარკვეულ გამონაკლისებს მხოლოდ და მხოლოდ ეროვნული უსაფრთხოების, თავდაცვის, ასევე, დანაშაულის პრევენციისა და გამოვლენის მიზნებით, თუკი ასეთი ზომები აუცილებელია და დასახული მიზნის პროპორციული

- ევროპის საბჭოს სამართალში კონფიდენციალობის ვალდებულებას მოიცავს მონაცემთა უსაფრთხოების ცნება, რომელსაც განსაზღვრავს მოდერინიზებული 108-ე კონვენციის მე-7 მუხლის პირველი პუნქტი

- უფლებამოსილი პირების შემთხვევაში კონფიდენციალობის დაცვა ნიშნავს, რომ მათ ეკრძალებათ მონაცემთა გამჟღავნება მესამე პირების ან სხვა მიმღებთათვის, შესაბამისი ნებართვის გარეშე; მონაცემთა დამმუშავებლის ან უფლებამოსილი პირის თანამშრომლებისათვის კი ეს ცნება გულისხმობს პერსონალური მონაცემების გამოყენებას მხოლოდ უფლებამოსილი ხელმძღვანელი პირების ინსტრუქციათა შესაბამისად

შეტყობინება პერსონალურ მონაცემთა უსაფრთხოების დარღვევის შესახებ (4.2.3)

- ასეთი დარღვევა გულისმობს გადაცემული, შენახული, ან სხვაგვარად დამუშავებული პერსონალური მონაცემების შემთხვევით ან უკანონო განადგურებას, დაკარგვას, შეცვლას, უკანონო გამჟღავნებას ან არასანქცირებულ წვდომას.

- თანამედროვე ტექნოლოგიები, როგორიცაა დაშიფვრა, ხელს უწყობს მონაცემთა დაცვას, თუმცა მონაცემები მაინც შეიძლება დაზიანდეს

- ევროპის საბჭოს მოდერნიზებული 108-ე კონვენციის თანახმად, ხელშემკვრელმა მხარეებმა მონაცემთა დამმუშავებლებს უნდა დააკისრონ ვალდებულება, რომ უსაფრთხოების დარღვევისას, სულ მცირე “დაუყონებლივ” გაუგზავნონ შეტყობინება კომპეტენტურ კომპეტენტურ საზედამხედველო ორგანოს, თუკი ამ ფაქტმა შეიძლება მნიშვნელოვნად შელახოს მონაცემთა სუბიექტის უფლებები

- ევროკავშირის კანონმდებლობით, თუ კი მონაცემები საფრთხეშია, დამმუშავებელმა ეს წერილობით უნდა ამცნოს მონაცემთა სუბიექტებს 72 საათის განმავლობაში. თუ კი ეს ვერ ხერხდება დადგენილ დროში, მაშინ მოგვიანებით გაგზავნილ წერილში დეტალურად უნდა აიხსნას, თუ რატომ ვერ მოხერხდა თავის დროზე მონაცემთა სუბიექტების გაფრთხილება.

კვირა 12

წესები ანგარიშვალდებულებისა და შესაბამისობის ხელშეწყობაზე (4.3)

- პერსონალურ მონაცემთა დამუშავების პროცესში ანგარიშვალდებულების უზრუნველსაყოფად, მონაცემთა დამმუშავებელი და უფლებამოსილი პირი ვალდებულნი არიან, აწარმოონ ჩანაწერები საკუთარი მოვალეობების ფარგლებში შესრულებულ სამუშაოზე და, მოთხოვნის შემთხვევაში, გადასცენ საზედამხედველო ორგანოებს

- შესაბამისობის ხელშესაწყობად, მონაცემთა დაცვის ზოგადი რეგულაცია ითვალისწინებს რამდენიმე ინსტრუმენტს:

- მონაცემთა დაცვის ოფიცრის დანიშვნა გარკვეულ სიტუაციებში

- როდესაც სავარაუდოა, რომ კონკრეტული ტიპის დამუშავება სერიოზულ საფრთხეს შეუქმნის ფიზიკურ პირთა უფლებებსა და თავისუფლებებს, დამმუშავებელს დაევალოს მონაცემთა დაცვის რისკების შეფასება

- წინასწარი კონსულტაციის გავლა შესაბამის საზედამხედველო ორგანოსგან, თუკი მონაცემთა დაცვის რისკების შეფასების თანახმად, დამუშავება შექმნის შეუქცევად საფრთხეებს, რომელთა აღმოფხვრაც შეუძლებელია

- მონაცემთა დამმუშავებლისა და უფლებამოსილი პირის ქცევის კოდექსის შექმნა, რომელიც დეტალურად მიმოიხილავს რეგულაციის გამოყენებას დამუშავების სხვადასხვა სფეროში

- სერტიფიცირების მექანიზმები, მონაცემთა დაცვის ბეჭდები და ნიშნები

- ევროპის საბჭოს კანონმდებლობა მსგავს ინსტუმენტებს ითვალისწინებს მოდერნიზებულ 108-ე კონვენციასთან შესაბამისობის მხრივაც

- ანგარიშვალდებულების პრინციპი განსაკუთრებით მნიშვნელოვანია ევროპაში მონაცემთა დაცვის წესების აღსრულებისათვის. დამმუშავებელი პასუხისმგებელია მონაცეMთა დაცვის წესებთან შესაბამისობაზე და უნდა შეძლოს დადასტურება, რომ უზრუნველყოფს მას. ანგარიშვალდებულება მხოლოდ დარღვევის შემდგომ არ უნდა გააქტიურდეს, მონაცემთა დამმუშავებელს ეკისრება პროაქტიული ვალდებულება, რომ მონაცემთა მართვის შესაბამისი პრინციპები დაიცვას დამუშავების ყველა ეტაპზე. მონაცემთა დაცვის ეროვნული კანონმდებლობა დამმუშავებელს ავალდებულებს სათანადო ტექნიკური და ორგანიზაციული ზომების შემუშავებას, რათა შეძლოს დადასტურება, რომ დამუშავება ხორციელდება კანონის შესაბამისად. ესენია: მონაცემთა დაცვის ოფიცრების დანიშვნა, დამუშავებასთან დაკავშირებული ჩანაწერებისა და დოკუმენტაციის შენახვა და მონაცემთა დაცვის რისკების შეფასება.

მონაცემთა დაცვის ოფიცერი (4.3.1)

- მონაცემთა დაცვის ოფიცერი (DPO) არის პირი, რომელიც დამმუშავებელ ორგანოზაციას აწვდის რჩევებს მონაცემთა დაცვის წესებთან შესაბამისობაზე. ის “ანგარიშვალდებულების ქვაკუთხედია”, ვინაიდან ხელს უწყობს შესაბამისობას და, ამავდროულად, მოქმედებს, როგორც შუამავალი

საზედამხედველო ორგანოებს, მონაცემთა სუბიექტებსა და დამნიშნავ ორგანოზაციას შორის.

- GDPR-ის თანახმად, მონაცემთა დაცვის ოფიცრის დანიშვნა სავალდებულოა 3 ძირითად შემთხვევაში: როდესაც მონაცემებს ამუშავებს სახელმწიფო უწყება ან ორგანო' მონაცემთა დამმუშავებლის ან უფლებამოსილი პირის ძირითადი საქმიანობა მოიცავს მონაცემთა სუბიექტის რეგულარულ და სისტემატიურ მონიტორინგს ფართო მასშტაბებით; მათი ძირითადი საქმიანობაა განსაკუთრებული კატეგორიის მონაცემთა ფართომასშტაბიანი დამუშავება

- მონაცემთა დაცვის ოფიცრის დანიშვნა არ არის სავალდებულო, ორგანიზაციებს შეუძლიათ დანიშნონ თავიანთ კომპანიებში, თუმცა რეგულაცია წევრ სახელმწიფოში გარდა 3 ძირითადი კატეგორიისა აძლევს საშუალებას, რომ მონაცემთა დაცვის ოფიცრის დანიშვნა სხვა ორგანიზაციებშიც სავალდებულო იყოს

- მონაცემთა დაცვასთან დაკავშირებულ ყველა საკითხში. მაგალითად, მონაცემთა დაცვის ოფიცერი უნდა მონაწილეობდეს რჩევების მიცემაში რისკების შეფასების შესახებ, ასევე დამუშავებასთან დაკავშირებული ჩანაწერების წარმოებაში. ორგანიზაცია ვალდებულია ოფიცერი უზრუნველყოს ყველა საჭირო საშუალებით

- GDPR-ის მიხედვით, მონაცემთა დაცვის ოფიცერი, უნდა იყოს დამოუკიდებელი და დამუშავების პროცესში არ მიიღოს ინსტრუქციები დამმუშავებლისგან, ან უფლებამოსილი პირისგან. მათ შორის, არც უმაღლესი რგოლის წარმომადგენლებისგან

- შეუძლებელია ოფიცრის სამსახურიდან დათხოვნა ან დასჯა მოვალეობის შესრულების გამო

დამუშავების საქმიანობის აღრიცხვა (4.3.2)

- ევროკავშირის კანონმდებლობით, მონაცემთა დამმუშავებელი ან მისი წარმომადგენელი ვალდებულია, აღრიცხოს მისი უფლებამოსილების ფარგლებში განხორციელებული ნებისმიერი დამუშავება. ამ ვალდებულების მიზანია, საჭიროების შემთხვევაში, საზედამხედველო ორგანომ მიიღოს დამუშავების კანონიერების დასადგენას საჭირო დოკუმენტები

- ჩანაწერები უნდა შეიცავდეს შემდეგ ინფორმაციას:

- მონაცემთა დამმუშავებლის, ერთობლივი დამმუშავებლის, დამმუშავებლის წარმომადგენლის, ან მონაცემთა დაცვის ოფიცრის სახელი და საკონტაქტო ინფორმაცია

- დამუშავების მიზნები

- მონაცემთა სუბიექტის და პერსონალურ მონაცემთა კატეგორიები

- მონაცემთა მიმღების კატეგორიები, ვისთვისაც გამჟღავნდა/გამჟღავნდება პერსონალური მონაცემები

- ინფორმაცია მესამე სახელმწიფოს ან საერთაშორისო ორგანოზაციისთვის მონაცემთა გადაცემის შესახებ

- თუ შესაძლებელია, სხვადასხვა კატეგორიის პერსონალურ მონაცემთა წაშლის ვადები; ასევე, დამუშავების უსაფრთხოებისთვის შემუშავებული ტექნიკური და ორგანიზაციული ზომების ზოგადი აღწერილობა

- აღრიცხვის ვალდებულება არ ვრცელდება იმ საწარმოზე, სადაც დასაქმებულია 250-ზე ნაკლები ადამიანი

- თუ საზედამხედველო ორგანო მოითხოვს ჩანაწერებზე წვდომას, მონაცემთა დამმუშავებელი და უფლებამოსილი პირი ვალდებულნი არიან, ითანამშრომლონ მასთან და წარუდგინონ ჩანაწერები

კვირა 13

ძირითადი საკითხები:

- დამოუკიდებელი ზედამხედველობა მონაცემთა დაცვის ევროპული კანონმდებლობის ძირითადი კომპონენტია, გათვალისწინებული ქარტიის მე-8 მუხლის მე-3 პუნქტით

- მონაცემთა ეფექტიანად დაცვისათვის, საჭიროა დამოუკიდებელი საზედამხედველო ორგანოს შექმნა ეროვნული კანონმდებლობის საფუძველზე

- საზედამხედველო ორგანო უნდა მოქმედებდეს სრული დამოუკიდებლობით, რაც გარანტირებული იქნება სადამფუძვებლო კანონით და აისახება საზედამხედველო ორგანოს სპეციალურ ორგანიზაციულ სტრუქტურაში

- საზედამხედველო ორგანოს აქვს კონკრეტული უფლებამოსილებები და ამოცანები, მათ შორის:

  - შიდასახემწიფოებრივ დონეზე მონაცემთა დაცვის კონტროლი და ხელშეწყობა

  - კონსულტაცია მონაცემთა სუბიექტებისა და დამმუშავებლებისათვის, ასევე, ხელისუფლებისა და მთალიანად საზოგადოებისთვის

  - საჩივრების/განცხადებების განხილვა და მონაცემთა სუბიექტის დახმარება მონაცემთა დაცვის უფლების შესაძლო დარღვევებისას

  - დამმუშავებლებისა და უფლებამოსილი პირების ზედამხედველობა

- საზედამხედველო ორგანოებს, საჭიროების შემთხვევაში, აქვთ ჩარევის უფლებამოსილბაც, კერძნოდ:

  - მონაცემთა დამმუშავებლისა და უფლებამოსილი პირის გაფრთხილება, საყვედურის გამოცხადება ან დაჯარიმება

- მონაცემთა შესწორებაზე, დაბლოკვასა ან წაშლაზე ბრძანების გაცემა

- მონაცემთა დამუშავების აკრძალვა ან ადმინისტრაციული ჯარიმის დაკისრება

- საქმის სასამართლოსთვის გადაცემა

- ხშირად პერსონალურ მონაცემთა დამუშავებაში მონაწილეობენ სხვადასხვა სახელმწიფოში მყოფი მონაცემთა დამმუშავებლები, უფლებამოსილი პირები და მონაცემთა სუბიექტები. შესაბამისად, საზედამხედველო ორგანოებს მოეთხოვებათ საერთაშორისო საკითხებზე თანამშრომლობა, რაც უზრუნველყოფს ფიზიკურ პირთა ეფექტიან დაცვას ევროპაში

- ევროკავშირში მონაცემთა დაცვის ზოგადი რეგულაცია ადგენს “ერთი ფანჯრის პრინციპს” მონაცემთა დამუშავების საერთაშორისო შემთხვევებისთვის. ზოგიერთი კომპანია ახორციელებს საერთაშორისო დამუშავებას, რადგან მონაცემები მუშავდება სხვადასხვა წევრ სახელმწიფოში მდებარე დაწესებულებათა საქმიანობის კონტექსტში, ან ეს პროცესი მნიშვნელოვან გავლენას ახდენს რამდენიმე წევრ ქვეყანაში მცხოვრებ მონაცემთა სუბიექტებზე. ასეთი მექანიმის ფარგლებში, კომპანიებს მხოლოდ ერთ ეროვნულ საზედამხედველო ორგანოსთან მოუწევთ ურთიერთობა.

- თანამშრომლებისა და თანმიმდევრულობის მექანიზმი ხელს უწყობს კონკრეტულ საქმეში მონაწილე საზედამხედველო ორგანოთა კოორდინირებული მიდგომის დანერგვას. ძირითადი ან ერთი დაწესებულების წამყვანი საზედამხედველო ორგანო კონსულტაციას გადის და გადაწყვეტილების პროექტს წარუდგენს სხვა შესაბამის საზედამხედველო ორგანოებს

- ევროპის საბჭოს კანონმდებლობის მიხედვით, პერსონალურ მონაცემთა დამუშავების კონტექსტში ფიზიკურ პირთა უფლებებისა და თავისუფლებების დასაცავად, დამოუკიდებელი საზედამხედველო ორგანოს არსებობა აუცილებელია. ვინაიდან მონაცემთა დამუშავება ფართოდ გავრცელებული ფენომენია და მისი აღქმა სულ უფრო და უფრო რთულდება ფიზიკური პირებისთვის, საზედამხედველო ორგანოები ციფრული ეპიქის დამკვირვებლები (watchdogs) არიან.

დამოუკიდებლობა (5.1)

- ევროკავშირისა და ევროპის საბჭოს სამართალი საზედამხედველო ორგანოებს ავალდებულებს სრული დამოუკიდებლობით მოქმედებას თავიანთი ფუნქციებისა და უფლებამოსილებების განხორციელებისას. საზედამხედველო ორგანოს, ასევე, მისი წევრებისა და თანამშრომლების დამოუკიდებლობას პირდაპირი და ირიბი გარე გავლენისგან, ფუნდამენტური მნიშვნელობა აქვს მონაცემთა დაცვის საკითხებზე ობიექტირუი გადაწყვეტილების მიღებისათვის.

საქმე:
European Commission v. Federal Republic of Germany

European Commission v. Federal Republic of Germany ევროპულმა კომისიამ CJEU-ს მიმართა თხოვნით, რათა დაედგინა, რომ გერმანიამ მონაცემთა დაცვაზე პასუხისმგებელი ორგანოებისთვის "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 (Lander) პერსონალურ მონაცემთა დამუშავებას აკონტროლებენ, სახემწიფო კონტროლქვეშ მოაქცია, ეწინააღმდეგებოდა დამოუკიდებლობის მოთხოვნას მონაცემთა დაცვის კანონმდებლობასთან შესაბამისობის მიზნით.

CJEU-მ ხაზგასმით აღნიშნა, რომ ცნება "სრული დამოუკიდებლობა" უნდა განიმარტოს ფორმულირების, ასევე ევროკავშირის მონაცემთა დაცვის კანონმდებლობის მიზნებისა და სტრუქტურის საფუძველზე. CJEU-მ ხაზი გაუსვა, რომ საზედამხედველო ორგანოები პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებული უფლებების "დამცველები" არიან. ამრიგად, მათი შექმნა წევრ სახელმიფოში მიჩნეულია "ფიზიკურ პირთა დაცვის მნიშვნელოვან კომპონენტად პერსონალურ მონაცემთა დამუშავებისას". CJEU-ს დასკვნით "მოვალეობების შესრულებისას, საზედამხედველო ორგანოები ობიექტურად და მიუკერძოებლად უნდა მოქმედებენ. საამისოდ, ისინი თავისუფალნი უნდა იყვნენ ნებისმიერი გარე ზემოქმედებისგან, მათ შორის, სახელმწიფო ორგანოთა პირდაპირი ან არაპირდაპირი გავლენისგან".

სასამართლომ ასევე დაადგინა, რომ "სრული დამოუკიდებლობა" უნდა განიმარტოს EDPS-ის დამოუკიდებლობისგან გამომდინარე, რაც განსაზღვრულია ევროკავშირის ინსტიტუტების მონაცემთა დაცვის რეგულაციით. ამ რეგულაციის თანახმად, დამოუკიდებლობის კონცეფცია გულისხმობს, რომ EDPSმა 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.

საქმეში European Commission v. Republic of Austria CJEU-მ იმავე პრობლემებს გასვა ხაზი, ამჯერად ავსტრიის მონაცემთა დაცვის საზედამხედველო ორგანოს (მონაცემთა დაცვის კომისია, DSK) გარკვებული 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 DSKის საქმიანობის შესახებ, უგულებელყოფდა საზედამხედველო ორგანოს სრული დამოუკიდებლობის მოთხოვნას.

საქმეში European Commission v. Hungary სასამართლომ აკრძალა შიდასახელმწიფოებრივ დონეზე არსებული მსგავსი პრაქტიკა, რომელიც საზედამხედველო ორგანოს სამუშაო ძალის დამოუკიდებლობაზე ახდენდა გავლებას. 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 ნაადრები შეწყვეტით.”