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 დამოუკიდებელო 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 თვითონგამორკვევის 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 კერძნო, 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, გამოძIებისა და დასჟის 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 შესაძლევებია 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 მუხსლთან 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 სახელIთ 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 დოს 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