საქმე "Bernh Larsen Holding AS and Others v. Norway"

საქმე „Bernh Larsen Holding AS and სხვები ნორვეგიის წინააღმდეგ“ ეხებოდა კომპანიას და ორ პირს, რომლებიც გაკოტრებულად გამოცხადდნენ და რომელთა პერსონალური ინფორმაცია, მათ შორის მათი სახელები, მისამართები, დაბადების თარიღები და ეროვნული საიდენტიფიკაციო ნომრები, გამოქვეყნდა საჯაროდ. ხელმისაწვდომი მონაცემთა ბაზა გაკოტრების პროცესის ფარგლებში. განმცხადებლები ამტკიცებდნენ, რომ მათი პირადი ინფორმაციის გამოქვეყნება არღვევდა მათ უფლებას, პატივი სცენ მათ პირად ცხოვრებას ადამიანის უფლებათა ევროპული კონვენციის მე-8 მუხლით. ადამიანის უფლებათა ევროპულმა სასამართლომ საბოლოოდ დაადგინა, რომ პერსონალური ინფორმაციის გამოქვეყნება არ იყო მათი პირადი ცხოვრების პატივისცემის უფლების დარღვევა, რადგან ის გამოქვეყნდა გაკოტრების პროცესის კონტექსტში, რომელიც იყო საჯარო ინტერესის საკითხი და არ იყო ზედმეტი ან ზედმეტი.

საქმე "Bărbulescu v. Romania"

საქმე „ბარბულესკუ რუმინეთის წინააღმდეგ“ ეხებოდა ინჟინერს, რომელიც გაათავისუფლეს სამსახურიდან მას შემდეგ, რაც მისმა დამსაქმებელმა შეაღწია მის სამუშაო ელფოსტის ანგარიშზე და აღმოაჩინა, რომ იგი იყენებდა მას პირადი შეტყობინებებისთვის, რაც აკრძალული იყო კომპანიის პოლიტიკით. ინჟინერმა გაასაჩივრა სამსახურიდან გათავისუფლება და ამტკიცებდა, რომ დამსაქმებლის მიერ მისი კომუნიკაციების მონიტორინგი არღვევდა ადამიანის უფლებათა ევროპული კონვენციის მე-8 მუხლის მიხედვით მის კონფიდენციალურობის უფლებას. ადამიანის უფლებათა ევროპულმა სასამართლომ საბოლოოდ დაადგინა, რომ ადგილი ჰქონდა მე-8 მუხლის დარღვევას, რადგან მონიტორინგი არ იყო საკმარისად შეზღუდული მოცულობითა და ხანგრძლივობით და ინჟინერი არ იყო წინასწარ ინფორმირებული, რომ მისი კომუნიკაციები შეიძლება მონიტორინგებულიყო.

საქმე “Digital Rights Ireland”

Digital Rights Ireland-ის საქმე იყო 2014 წელს ევროკავშირის იუსტიციის სასამართლოს მიერ განხილული საქმე, რომელიც ეხებოდა ევროკავშირის მონაცემთა შენახვის კანონების შესაბამისობას ფუნდამენტურ უფლებებთან. საქმე აღძრა Digital Rights Ireland-მა, კონფიდენციალურობის დამცველმა ჯგუფმა და ეხებოდა ევროკავშირის ორ დირექტივას, რომლებიც წევრ ქვეყნებს ავალდებულებდნენ, შეინარჩუნონ საკომუნიკაციო მონაცემები გარკვეული პერიოდის განმავლობაში. სასამართლომ დაადგინა, რომ დირექტივები იყო არასწორი, რადგან ისინი არღვევდნენ ფუნდამენტურ უფლებებს პირადი ცხოვრების პატივისცემასა და პერსონალური მონაცემების დაცვაზე ევროკავშირის ძირითადი უფლებების ქარტიით. სასამართლომ დაადგინა, რომ ასეთი მონაცემების შენახვა წარმოადგენს სერიოზულ ჩარევას ამ ფუნდამენტურ უფლებებში და რომ დირექტივები არ შეიცავს საკმარის გარანტიებს ამ მონაცემების ბოროტად გამოყენებისგან დასაცავად. გადაწყვეტილებამ ფაქტობრივად გააუქმა მონაცემთა შენახვის კანონები მთელს ევროკავშირში.

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

Google Spain-ის საქმე ეხებოდა ესპანელ მამაკაცს, მარიო კოსტეა გონსალესს, რომელმაც მოითხოვა Google-ის წაშლა ძიების შედეგები, რომლებიც შეიცავდა ინფორმაციას ძველი დავალიანების შესახებ, რომელიც გადაჭრილი იყო. Google-მა უარი თქვა ძიების შედეგების წაშლაზე, ამიტომ კოსტეია გონსალესმა შეიტანა საჩივარი ესპანეთის მონაცემთა დაცვის სააგენტოში. საქმე საბოლოოდ მივიდა ევროპის მართლმსაჯულების სასამართლომდე, რომელმაც დაადგინა, რომ პირებს უფლება აქვთ მოითხოვონ ძიების შედეგების ამოღება, რომლებიც არაადეკვატური, შეუსაბამო ან აღარ არის რელევანტური, მაშინაც კი, თუ ინფორმაცია თავად არის ზუსტი და კანონიერად გამოქვეყნებული. სასამართლომ დაადგინა, რომ ეს „დავიწყების უფლება“ იყო ფუნდამენტური უფლება ევროკავშირის კანონმდებლობით და რომ საძიებო სისტემებს, როგორიცაა Google, აქვთ პასუხისმგებლობა დააბალანსონ კონფიდენციალურობის უფლება ინფორმაციის თავისუფლებასთან. საქმემ ევროკავშირში დავიწყების უფლება დაამყარა და შექმნა პრეცედენტი იმისა, თუ როგორ უნდა გაუმკლავდნენ საძიებო სისტემებს ძიების შედეგების წაშლის მოთხოვნებს.

საქმე „Franšek Ryneš“

ფრანსეკ რინესის საქმე იყო საქმე, რომელიც განიხილებოდა ევროპის იუსტიციის სასამართლოს მიერ 2010 წელს, ეხებოდა უპილოტო საჰაერო ხომალდების (დრონების) გამოყენებას კერძო პირების მიერ მტკიცებულებების შესაგროვებლად. საქმე ეხებოდა მამაკაცს, რომელმაც გამოიყენა კამერით აღჭურვილი დრონი ჩეხეთის რესპუბლიკაში ნარჩენების განთავსების ადგილის ფოტოსურათების გადასაღებად და შემდეგ გადასცა ფოტოები გარემოსდაცვით ორგანოებს უკანონო გადაყრის მტკიცებულებად. ნარჩენების განთავსების ადგილის ოპერატორმა რინესს უჩივლა კონფიდენციალურობის ხელყოფისთვის. საქმე საბოლოოდ მივიდა ევროპის იუსტიციის სასამართლომდე, რომელმაც დაადგინა, რომ თვითმფრინავების გამოყენება კერძო პირების მიერ მტკიცებულებების შესაგროვებლად არ იყო არსებითად უკანონო, მაგრამ ეს გამოყენება უნდა შეესაბამებოდეს ევროკავშირის მონაცემთა დაცვის კანონებს. სასამართლომ დაადგინა, რომ პირებს უნდა ჰქონდეთ ლეგიტიმური მიზეზი პერსონალური მონაცემების შესაგროვებლად დრონების გამოყენებისთვის და რომ შეგროვება უნდა იყოს შეგროვების მიზნის პროპორციული. საქმემ შექმნა პრეცედენტი იმისა, თუ როგორ შეიძლება დრონების გამოყენება მტკიცებულებების შესაგროვებლად ევროკავშირში კონფიდენციალურობისა და მონაცემთა დაცვის კანონების დაცვით.

საქმე „SWIFT“

SWIFT - ის საქმეში, ევროპულმა საბანკო ინსტიტუტმა დაიქირავა SWIFT - კომპანია მონაცემთა დამმუშავებლად. ინფორმაციას კომპანია ამერიკულ სერვერებზე ინახავდა. მოგვიანებით, სვიფტმა ეს ინფორმაცია ამერიკულ კომპანიებს გაუზიარა ისე, რომ საბანკო ინსტიტუტთან არ შეთანხმებულა. ქეისზე მომუშავე ჯგუფმა დაადგინა, რომ მიუხედავად იმისა, რომ ევროპულმა საბანკო ინსტიტუტმა არ იცოდა სვიფტის ქმედებების შესახებ, ამ საქმეში როგორც სვიფტი, ისე საბანკო ინსტიტუტი თანაბრად იყვნენ დამნაშავენი, ვინაიდან ინფორმაციის ერთობლივად დამუშავებისას, აუცილებელია პარტნიორმა კომპანიებმა ერთმანეთი აკონტროლონ.

საქმე „K.H. and Others v. Slovakia“

ამ საქმეში ბოშა ქალებმა, რომლებმაც მშობიარობისას დახმარება მიიღეს აღმოსავლეთ სლოვაკეთის საავადმყოფოებისგან, ვეღარ შეძლეს დაორსულება.

სასამართლომ საავადმყოფოებს მოსთხოვა სამედიცინო ჩანაწერების გადმოცემა, საავადმყოფოებმა ამ მოთხოვნაზე უარი განაცხადეს, იმ მიზეზით რომ შესაძლოა ჩანაწერები არასწორ ხელში ჩავარდნილიყო და ბოროტად ყოფილიყო გამოყენებული. ისინი არღვევდნენ Ecthr - ის მე 8 მუხლს, რომლიც სახელმწიფოებს პოზიტიურად ავალდებულებს, პერსონას თავისი პირადი ინფორმაციის ასლები გაუზიაროს ან გონივრული მიზეზის შემთხვევაში უარი უთხრას მას. ამ კონკრეტულ შემთხვევაში კი უარისთვის მყარი მიზეზი არ არსებობდა.

საქმე „Haralambie v. Romania“

საქმე ჰარალამბი რუმინეთის წინააღმდეგ ეხებოდა რუმინელ მამაკაცს, რომელიც ნასამართლევი იყო ორი ინდაურის ქურდობაში და მიესაჯა ორი წლით თავისუფლების აღკვეთა. მამაკაცი ამტკიცებდა, რომ მისი სასჯელი იყო არაპროპორციული და არღვევდა მის უფლებას სამართლიანი სასამართლოს შესახებ ადამიანის უფლებათა ევროპული კონვენციის მე-6 მუხლით. ადამიანის უფლებათა ევროპულმა სასამართლომ საბოლოოდ დაადგინა, რომ მამაკაცის სასჯელი მართლაც არაპროპორციული იყო და არღვევდა მის უფლებას სამართლიანი სასამართლოს შესახებ, რადგან სასჯელი არ შეესაბამება დანაშაულს. სასამართლომ დაადგინა, რომ სასჯელი გადაჭარბებული იყო შედარებით მცირე დანაშაულისთვის ორი ინდაურის ქურდობისთვის და რომ რუმინეთის ხელისუფლებამ სათანადოდ არ განიხილა შემამსუბუქებელი ფაქტორები, როგორიცაა მამაკაცის ასაკი და კრიმინალური ისტორიის ნაკლებობა. საქმემ შექმნა პრეცედენტი სისხლისსამართლებრივი სასჯელის დადგენისას პროპორციულობის მნიშვნელობისა და სასამართლოს მიერ სასჯელის დადგენისას ყველა შესაბამისი ფაქტორის გათვალისწინების აუცილებლობის შესახებ.

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

საქმე Smaranda Bara and Others v. Preşidentele Casei Naţionale de Asigurări de Sănătate and Casa Naţională de Administrare Fiscală (ANAF) ეხებოდა რუმინელი ექიმების ჯგუფს, რომლებიც გამოიძიეს საგადასახადო და ჯანმრთელობის დაზღვევის ორგანოებმა გადასახადებისა და სოციალური უზრუნველყოფის შენატანების სავარაუდო აცილების გამო. . ექიმები ამტკიცებდნენ, რომ ხელისუფლებამ დაარღვია მათი უფლება სამართლიანი სასამართლოს შესახებ და ადამიანის უფლებათა ევროპული კონვენციის მე-6 და მე-8 მუხლების მიხედვით პირადი ცხოვრების ხელშეუხებლობის უფლება. ადამიანის უფლებათა ევროპულმა სასამართლომ დაადგინა, რომ რუმინეთის ხელისუფლებამ დაარღვია ექიმების უფლება სამართლიანი სასამართლოს შესახებ, რადგან მათ არ მიაწოდეს სათანადო ინფორმაცია მათ წინააღმდეგ წაყენებული ბრალდებებისა და მტკიცებულებების შესახებ. სასამართლომ ასევე დაადგინა, რომ ხელისუფლებამ დაარღვია მათი პირადი ცხოვრების ხელშეუხებლობის უფლება, რადგან მათ ექიმებზე ფარული მეთვალყურეობა აწარმოეს ორდერის ან სხვა სამართლებრივი საფუძვლის გარეშე. საქმემ შექმნა პრეცედენტი სათანადო პროცესის და კონფიდენციალურობის დაცვის მნიშვნელობის შესახებ სამთავრობო ორგანოების მიერ გამოძიებებში და დევნაში.

1. **რა ტიპის პერსონალური მონაცემები შეიძლება მივიჩნიოთ განსაკუთრებული კატეგორიის პერსონალურ მონაცემებად?**

პასუხი : 108 - მოდერნიზებული კოვნვენციის მე - 8 და GDPR - ის მე - 6 ე მუხლის თანახმად, განსაკუთრებული კატეგორიის პერსონალურ მონაცემებში იგულისხმება ისეთი მონაცემები, რომლებიც შეიცავენ ინფორმაციას სუბიექტის : რასის, ეთნიკურობის, პოლიტიკური და ფილოსოფიური შეხედულებების, სქესობრივი და პირის ორიენტაციის შესახებ

1. **რას გულისხმობს მონაცემთა ავტომატური დამუშავება?**

პასუხი : მონაცემთა ავტომატურ დამუშავებაში მოიაზრება ისეთი დამუშავება, რომელიც ცოცხალ დამმუშავებელს არ მოითოვს, მაგალითად კომპიუტერები, ტელეფონები, აპლიკაციები, საძიებო სისტემები, სამეთვალყურეო კამერები და ა.ს.შ

1. **რას ნიშნავს მონაცემთა არაავტომატური დამუშავება?**

პასუხი : არაავტომატური დამუშავებისას პერსონალური მონაცემები ინახება სპეციალურად მოწყობილ სტრუქტურირებულ მონაცემთა ბაზაში, დაცულ საქაღალდეში და სხვა მსგავს კონსტრუქციებში. არაავტომატურ დამუშავებაში საკვანძო და მნიშვნელოვანია ის ფაქტი, რომ მონაცემები ინახება დაცულ შემნახველ სისტემაში და მასზე წვდომა არ ეძლევა ყველას, მხოლოდ გარკვეული კრიტერიუმების მქონეებს.

1. **რა განსხვავებაა მონაცემთა დამმუშავებელსა და უფლებამოსილ პირს შორის?**

პასუხი : მონაცემთა დამამუშავებელი საზღვრავს პერს. მონაცემების შეგროვების მიზანს, ქმნის მონაცემთა შემნახველ სტრუქტურას, მენეჯმენტს უწევს ინფორმაციის მიღებისა და დამუშავების პროცესებს. ისინი მეტად პასუხისმგებელნი არიან კანონის წინაშე და მათთვის აუცილებელია მონაცემთა აღრიცხვის ყველა ეტაპის აღწერა.

დამმუშავებელი შეიძლება იყოს ერთი პიროვნება/ორგანიზაცია ან ერთზე მეტი (ერთობლივი დამამუშავებელი).

უფლებამოსილი პირი ძირითად შემთხვევაში დამმუშავებლისგან იღებს პერსონალურ მონაცემზე წვდომას (ოფიციალური თანხმობის თანხლებით) ის იღებს დავალებებს დამმუშავებლისგან. მისი დავალება შეიძლება იყოს მცირე და მარტივი ან დიდი და კომპლექსური. მონაცემთა დამმუშავებელი შეიძლება იყოს როგორც ფიზიკური პირი, ასევე სხვა ორგანიზაცია.

1. **რას ნიშნავს მონაცემთა ერთობლივი დამუშავება?**

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

1. **რა შემთხვევაში შეიძლება მიმღები იყოს მესამე პირი/მხარე**

პასუხი : მიმღები ფართ ცნებაა. მიმღები შეიძლება იყოს ნებისმიერი, რომელსაც გადაეცემა პერსონალური ინფორმაცია, მათ შორის იმ შემთხვევაშიც თუ ის მესამე პირია.

1. **რა შემთხვევებშია მონაცემთა დამუშავება კანონიერი?**

პასუხი : თუ გვაქვს მონაცემთა სუბიექტის თანხმობა, თუ საჭიროა რომ საჯარო ინტერესში შემავალი ამოცანა შესრულდეს, იმ შემთხვევაში თუ მონაცემთა სუბიექტის ფიზიკური ან სხვა სასიცოცხლო ინტერესების დაცვაა საჭირო.

1. **რას გულისხმობს პერსონალური მონაცემების სამართლიანად დამუშავება?**

პასუხი : თუ გვაქვს დასამუშავებელი სუბიექტისგან თანხმობა (განსაკუთრებული კატეგორიის მონაცემთა დამუშავება საჭიროებს მკაფიოდ გამოხატულ თანხმობას.), პროცესი მიმდინარეობს გამჭირვალედ, სუბიექტთან გაცხადებულია დამუშავების მიზნები, ფორმები, პერიოდი და ა.ს.შ - დეტალები. მონაცემთა სუბიექტს ნებისმიერ დროს უნდა შეეძლოს ნებისმიერ დროს გამოიხმოს თანხმობა. თანხმობა უნდა გადმოიცეს ნათლად, ისე, რომ არ წარმოშვას რაიმე ეჭვი მონაცემთა სუბიექტის განზრახვასთან დაკავშირებით.

1. **რას ნიშნავს პერსონალური მონაცემების გამჭვირვალედ დამუშავება?**

პასუხი : მონაცემების დამუშავებამდე სუბიექტს უნდა შეატყობინონ დამუშავების მიზანი, ვინაობა, მისამართი და სხვა დეტალები შესაბამის ფორმატში (საჭიროების შემთხვევაში ეს ყოველივე ბავშვისთვის გასაგებ ენაზეც კი შესაძლოა გახდეს წარმოდგენილი). სუბიექტისგან მიღებული უნდა იყოს მკაფიო თანხმობა, რომელიც ასევე შეიძლება ელექტრონულ ან წერილობით ფორმატშიც ჩაითვალოს ვალიდურად. სუბიექტებს კი თანხმობის შემდეგ შეუძლიათ მოითხოვონ პროაქტიულად შემდეგი ინფორმაცია : თუ რამდენ ხანს გაგრძელდება დამუშავება, პროცედურის მიზნები, ინფორმაცია გამოყენებული საშუალებების შესახებ და ა.ს.შ

1. **რას გულისხმობს მიზნის შეზღუდვის პრინციპი?**

პასუხი : მიზნის შეზღუდვის არსი შემდეგია : პერს. მონაცემები უნდა დამუშავდეს მხოლოდ წინასწარ განსაზღვრული მიზნების შესაბამისი ინფორმაციით ან თავდაპირველი მიზნის დამატებითი მიზნებით. აუცილებლია რომ ეს მიზნები იყოს გამჭირვალე, მკაფიო და გასაგები, ვინაიდან გამჭირვალობა მიზნის შეზღუდვის პრინციპში აუცილებელი და ფუნდამენტური პრინციპია ევროპულ სამართალში

1. **რა განსხვავებაა მონაცემთა მინიმიზაციისა და მონაცემთა სიზუსტის პრინციპებს შორის?**

პასუხი : მიზნის შეზღუდვის პრინციპისგან განსხვავებით, მონაცემთა მინიმიზაციისას

მონაცემები უნდა დამუშავდეს მხოლოდ ლეგიტიმურ ფარგლებში, დაუშვებელია რომ მოხდეს არაპრპორციული ჩარევა და მინიმაზაციის გამოყენება ძირითად შემთხვევაში, მხოლოდ მაშინ ხდება, როცა დამუშავების სხვა საშუალება არ არის.

1. **რას ნიშნავს შენახვის ვადის შეზღუდვის პრინციპი?**

პასუხი : მონაცემთა შენახვის ვადის შეზღუდვა მოისაზრებს იმას, რომ დამუშავებული პირადი მონაცემები უნდა შეინახოს მხოლოდ იმ დროს განმავლობაში, რომელშიც საჭიროა დამუშავების მიზნის მისაღწევად ან როგორც GDPR-ის მე-5 მუხლის 1(ე) და მოდერნიზებული 108-ე კონვენციის მე-5 მუხლის მეოთხე პუნქტიშია აღწერილი - : „იქამდე, სანამ პირის იდენტიფიცირებისთვის საჭირო მონაცემი გვაძლევს საშუალებას რომ პირი იდენტიფიცირდეს კონკრეტული მიზნებისთვის“

ამის შემდეგ უნდა მოხდეს პირადი ინფორმაციის წაშლა ან მათი ანონიმიზაცია

1. **რას გულისხმობს მონაცემთა უსაფრთხოების პრინციპი?**

ეს პრინციპი მოითხოვს ორგანიზაციისგან, რომ დამუშავებული პერ. ინფორმაცია სპეციალურად სტრუქტურირებულ შემნახველში შეინახოს და მასზე წვდომა მხოლოდ ავტორიზებულ პირებს ჰქონდეთ. ასეთი სტურქტურის შექმნისას აუცილებელია ყურადღება მიექცეს ისეთ დეტალებს როგორიცაა უახლესი დაცვის ტექნოლოგიები და მათი რისკის წყაროები, რათა არ მოხდეს ამ სტრუქტურაზე უკანონო წვდომა, მონაცემების წაშლა, ცვლილება და ა.ს.შ

1. **რა არის ანგარიშვალდებულების პრინციპი?**

პაუხი : ეს პრინციპი ავალებს მონაცემთა დამმუშავებელს, რომ მუდმივად გაატაროს ის ზომები, რომლებიც დაეხმარება მათ მონაცემთა დაცვაში. ვინაიდან დამმუშავებელი ვალდებულია მუდმივად იცავდეს პერს. ინფორმაციას და ანგარიშვალდებულია, მუდმივად იყენებდეს პერს. მონაცემთა დაცვაში არსებულ სტანდარტებს.

1. **რას ნიშნავს ნებაყოფლობითი თანხმობა?**

**პასუხი** : თითქმის ყოველთვის, როდესაც ხდება სუბიექტის პერს. მონაცემების დამუშავების საჭიროება, საჭიროა მისგან თანხმობა. აუცილებელია რომ ეს თანხმობა იყოს ნებაყოფლობითი. 108 კონვენციის თანახმად - თავისუფალი ნებისყოფა უნდა იყოს გამიზნული და ზეწოლის გარეშე მიღებული. თანხმობის გაცემის ან არ გაცემის შემთხვევაში, სუბიექტს არ უნდა ექმნებოდეს მაჟორული პრობლემა.

1. **რას გულისხმობს ინფორმირებული თანხმობა?**

**პასუხი** : მონაცემთა სუბიექტს მისი მონაცემების დამუშავებისას ხშირად უწევს მნიშვნელოვანი გადაწყვეტილებების მიღება. როდესაც ის ასეთ მდგომარეობაში აღმოჩნდება, სუბიექტი უნდა იყვეს ინფორმირებული ყველა დეტალის შესახებ იმ გადაწყვეტილების გარშემო რომელზეც მოეთხოვება პასუხის გაცემა. ყოველივე ეს სუბიექტისთვის მკაფიო, გასაგები ენით უნდა იყვეს ახსნილი. სუბიექტი უნდა იყოს ინფორმირებული როგორც დამუშავებაზე დადებით, ისევე უარყოფით პასუხის გაცემის შემთხვევაში გამოწვეულ შედეგებზე.

1. **რას ნიშნავს თანხმობის გამოთხოვის უფლება?**

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

1. **როგორია კონკრეტული და მკაფიო თანხმობა?**

**პასუხი** : როდესაც სუბიექტის მხრიდან ხდება მონაცემთა დამუშავებაზე თანხმობის გაცემა საჭირო, აღნიშნულითანხმობა უნდა იყოს მკაფიო, გასაგები, უნდა გამორიცხავდეს ნებისმიერ გონივრულ ეჭვს, თანხმობის მიღების ფორმატი ისე უნდა იყოს განსაზღვრული, რომ გარანტირებული იყვეს შემდეგი ფაქტი - სუბიექტი გააზრებულად აცხადებს თანხმობას და არა ავტომატურად. უმოქმედობა სუბიეექტისგან არ აღნიშნავს მკაფიო თანხმობას!.

1. **შეიძლება თუ არა ზოგადად განსაკუთრებული კატეგორიის მონაცემების დამუშავება?**

**პასუხი :** არა, გარდა გამონაკლისი შემთხვევებისა, როცა პირის განსაკუთრებული კატეგორიის მონაცემების დამუშავება აუცილებელია მისივე სასიცოცხლო ინტერესებისთვის ან მნიშვნელოვანი საჯარო ინტერესებისთვის.

1. **რა შემთხვევაში მიიჩნევა მონაცემთა სუბიექტის მიერ მონაცემები**

**ცალსახად საჯაროდ  გამოქვეყნებულად?**

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

**21)შესაძლოა თუ არა სამართლებრივი მოთხოვნის საფუძველზე**

**განსაკუთრებული კატეგორიის მონაცემების დამუშავება?**

**პასუხი :**  მხოლოდ ისეთ შემთხვევაში, რომელშიც დაცული უნდა იყოს მოდერნიზებული 108-ე კონვენციის პირობები - კერძოდ, კანონმდებლობის მიერ გათვალისწინებული უსაფრთხოების სათანადო ზომები შეესაბამებოდეს კონვენციის სხვა დებულებებს.

რაც შეეხება ისეთ განს. მონაცემებს, როგორიცაა პირის (სენსიტიური) რელიგიური, სექსუალური, გენეტიკური და ბიომეტრიული მონაცემების დამუშავება არ შეიძლება, გარდა შემთხვევებისა როცა დამმუშავებელმა თავისი ნებინ გაასაჯორვა ინფორმაცია, საჭიროა მისი დასაქმებისათვის, პირის სასიცოცხლო ან მნიშვნელოვანი საჯარო ინტერესებისათვისაა საჭირო.

1. **რას გულისხმობს მნიშვნელოვანი საჯარო ინტერესის საფუძველზე**

**განსაკუთრებული კატეგორიის მონაცემების დამუშავება?**

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

**22)მონაცემთა სუბიქეტის სასიცოცხლო ინტერესის გათვალისწინებით შეიძლება თუ არა განსაკუთრებული კატეგორიის მონაცემების დამუშავება?**

**პასუხი :** თუ მონაცემთა სუბიექტის სასიცოცხლო ინტერესებს საფრთხე ემუქრება და თვით მონაცემთა სუბიექტს არ აქვს საშუალება, განაცხადოს თანხმობა (უგონოდაა, მიუწვდომელია, არ იმყოფება საღ გონებაზე და ა.ს.შ) შესაძლებელია.

**23) რას გულისხმობს უსაფრთხოების უზრუნველყოფის ტექნიკური ზომები?**

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

**24)რას ნიშნავს უსაფრთხოების უზრუნველყოფის ორგანიზებული ზომები?**

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

**25)რა არის უსაფრთხოების მაღალი დონის უზრუნველყოფის მიზანი?**

პასუხი : მე - 5 მუხლის მიხედვით, ინფორმაცია ისე უნდა დამუშავდეს, რომ მასში უცხო პირმა ვერ შეძლოს შეღწევა, ინფორმაციის შეცვლა, წაშლა, გაზიარება. ასევე უსაფრთოხების მაღალი დონე საჭიროა იმისთვისაც, რომ თუნდაც ავტორიზირებულმა პირმა ვერ შეძლოს მონაცემების იმგვარი დამუშავება, რომელიც სცდება დამუშავების მიზნების და ამოცანების ფარგლებს.

**26)რას გულისხმობს კომუნიკაციების კონფიდენციალურობა?**

პასუხი : კომუნიკაციის კონფედენციალურობა ცალკე სტანდარტით რეგულირდება.

აღნიშნული ნორმა - სტანდარტი წევრ სახელმწიფოებს უკრძალავს ყველა პირს, გარდა მომხმარებლისა, მისთვის მიყურადებას, მისი თანხმობის გარეშე მისი პირადი ინფორმაციისა და კომუნიკაციების ჩაწერას, შენახვას, გაზიარებას და ა.ს.შ. (გარდა გამონაკლისი შემთხვევებისა, როცა აღნიშნულის გაკეთება ხალხის დიდი მასების ინტერესის ან ეროვნული უსაფრთოხების დაცვისთვისაა საჭირო) აღნიშნული ვრცელდება ასევე საჯარო სივრცეებში განთავსებულ ინფორმაციაზე და OTT - სერვისებზეც.

**26)რა არის პერსონალურ მონაცემთა უსაფრთხოების დარღვევისშესახებ შეტყობინების ვალდებულების მიზანი?**

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