Digital Rights Ireland-ის საქმე

Digital Rights Ireland-ის საქმეში6 CJEU-მ იმსჯელა 2006/24/ EC დირექტივის საფუძვლიანობაზე პერსონალურ მონაცემთა და პირადი ცხოვრების პატივისცემის ფუნდამენტურ უფლებათა ჭრილში, რომელთაც განამტკიცებს ევროკავშირის ფუნდამენტურ უფლებათა ქარტია. დირექტივა საჯარო ელექტრონული კომუნიკაციებისა და საკომუნიკაციო ქსელების პროვაიდერებს ავალდებულებდა სატელეკომუნიკაციო მონაცემების შენახვას 2 წლამდე ვადით და მათ ხელმისაწვდომობას მძიმე დანაშაულთა პრევენციის, გამოძიებისა და დასჯის მიზნით. ეს ღონისძიება ეხებოდა მეტა, ადგილმდებარეობის განმსაზღვრელ და ისეთ მონაცემებს, რომლებიც საჭიროა გამომწერის ან მომხმარებლის იდენტიფიცირებისთვის და არ უკავშირდებოდა ელექტრონული კომუნიკაციის შინაარსს. CJEU-მ დაადგინა, რომ დირექტივა ზღუდავდა პერსონალურ მონაცემთა დაცვის ფუნდამენტურ უფლებას, „ვინაიდან იგი ასეთი მონაცემების დამუშავების შესაძლებლობას იძლევა,“7 ასევე, პირადი ცხოვრების პატივისცემის უფლებასაც.8 მთლიანობაში, დირექტივის საფუძველზე შენახული და ხელისუფლების კომპეტენტური ორგანოებისთვის ხელმისაწვდომი მონაცემები იძლევა „ძალიან ზუსტი დასკვნების გაკეთების შესაძლებლობას იმ ადამიანთა პირადი ცხოვრების შესახებ, ვისი მონაცემებიც შენახულია (მათ შორის, ყოველდღიური ჩვევების, მუდმივი ან დროებითი საცხოვრებლის, ყოველდღიური ან სხვა გადაადგილების, აქტივობების, სოციალური კავშირებისა და იმ გარემოს შესახებ, სადაც ხშირად იმყოფებიან“).9 ზემოაღნიშნული ორი უფლების შეზღუდვა იყო ფართო და განსაკუთრებულად მძიმე. CJEU-მ 2006/24/EC დირექტივა გაუქმებულად გამოაცხადა. სასამართლოს დასკვნით, მიუხედავად იმისა, რომ პერსონალურ მონაცემთა დაცვისა და პირადი ცხოვრების უფლებებზე დაწესებული შეზღუდვა ემსახურებოდა ლეგიტიმურ მიზანს, ეს იყო მძიმე შეზღუდვა და არ შემოიფარგლებოდა მხოლოდ მკაცრი საჭიროებით.

საქმე Bernh Larsen Holding AS and Others v. Norway

საქმე Bernh Larsen Holding AS and Others v. Norway140 შეეხებოდა სამი ნორვეგიული კომპანიის საჩივარს საგადასახადო ორგანოს გადაწყვეტილებასთან დაკავშირებით, რომლის მიხედვითაც მათ აუდიტორებისათვის უნდა გადაეცათ იმ სერვერზე განთავსებულ მონაცემთა ასლები, რომლითაც ეს კომპანიები ერთობლივად სარგებლობდნენ. ECtHR-მა დაადგინა, რომ ამ მოვალეობის დაკისრება განმცხადებლებზე იყო ჩარევა მათ საცხოვრებლისა და კორესპონდენციის პატივისცემის უფლებაში (მე-8 მუხლი). თუმცა, სასამართლოს განმარტებით, საგადასახადო ორგანოებს ეფექტიანი და სათანადო მექანიზმები ჰქონდათ ჩარევის ბოროტად გამოყენების ასაცილებლად: მათ განმცხადებელი კომპანიები წინასწარ, საკმაო დროით ადრე გააფრთხილეს; კომპანიების წარმომადგენლები ესწრებოდნენ შემოწმებას და ჰქონდათ თავიანთი არგუმენტების ადგილზე წარმოდგენის შესაძლებლობა, მასალები კი განადგურდებოდა საგადასახადო შემოწმების დასრულებისთანავე. ასეთ პირობებში, საჭირო იყო სამართლიანი წონასწორობის მიღწევა საპირისპირო ინტერესებს შორის. კერძოდ, ეფექტიანი შემოწმების საჯარო ინტერესი, საგადასახადო შეფასების მიზნებით, უნდა დაბალანსებულიყო განმცხადებელი კომპანიების „საცხოვრებლისა“ და „კორესპონდენციის“ უფლებასა და მათი თანამშრომლების პირადი ცხოვრების დაცვის ინტერესთან. სასამართლომ დაადგინა, რომ საქმეში კონვენციის მე-8 მუხლი არ დარღვეულა.

Bărbulescu v. Romania

საქმეში Bărbulescu v. Romania151 განმცხადებელი სამსახურიდან გაათავისუფლეს იმის გამო, რომ სამუშაო საათებში დამსაქმებლის ინტერნეტი შიდა რეგულაციების დარღვევით გამოიყენა. დამსაქმებელი ფარულ მონიტორინგს უწევდა დასაქმებულის კომუნიკაციებს და ჩანაწერები, რომლებიც მოიცავდა მხოლოდ პირადულ მესიჯებს, ეროვნულ დონეზე გამართულ სასამართლო პროცესზე წარმოადგინა. ECtHRმა, მას შემდეგ, რაც დაადგინა, რომ მე-8 მუხლი ვრცელდებოდა ასეთ მონაცემებზეც, ღია დატოვა კითხვა, თუ რამდენად უჩენდა დამსაქმებლის შემზღუდავი რეგულაციები განმცხადებელს პირადი ცხოვრების დაცვის გონივრულ მოლოდინს; თუმცა, ამავდროულად სასამართლომ დაადგინა, რომ დასაქმებულის ინსტრუქციები პირად სოციალურ ცხოვრებას სამუშაო ადგილზე ბოლომდე ვერ გამორიცხავდა. რაც შეეხება არსებით მხარეს, ხელშემკვრელ სახელმწიფოებს ფართო დისკრეცია ენიჭებათ შესაფასებლად, თუ რამდენად საჭიროა საკანონმდებლო ჩარჩოს შექმნა ისეთი პირობების დარეგულირებისათვის, რომელშიც დამსაქმებელს აქვს სამუშაო ადგილზე დასაქმებულის არაპროფესიული კომუნიკაციის გაკონტროლების უფლება - ელექტრონული თუ სხვა ფორმით. ამავდროულად, სახელმწიფო ორგანოებმა უნდა უზრუნველყონ, რომ დამსაქმებლის მიერ კორესპონდენციასა და სხვა კომუნიკაციაზე მონიტორინგის მიზნით დანერგილ ღონისძიებებს, მიუხედავად მათი მასშტაბისა და ხანგრძლივობისა, თან ახლდეს სათანადო და საკმარისი საშუალებები ბოროტად გამოყენებისგან დასაცავად. უაღრესად მნიშვნელოვანია პროპორციულობა და პროცედურული გარანტიები თვითნებობის წინააღმდეგ. ECtHR-მა გამოავლინა ასეთ პირობებისთვის საგულისხმო რამდენიმე ფაქტორი, მათ შორის, დასაქმებულზე მონიტორინგის ფარგლები და მის პირად ცხოვრებაში შეჭრის ხარისხი. კერძოდ, რა შედეგები ექნება ამგვარ ზომას დასაქმებულისთვის და რამდენად უზრუნველყოფილია დაცვის სათანადო საშუალებები. ამასთან, სახელმწიფო ორგანოების ძალისხმევით, დასაქმებულს, რომლის კომუნიკაციებზეც მონიტორინგი ხორციელდება, ხელი უნდა მიუწვდებოდეს სამართლებრივი დაცვის საშუალებაზე შესაბამისი სასამართლო ორგანოს წინაშე, რათა, სულ მცირე, არსებითად დადგინდეს წარმოდგენილი კრიტერიუმების დაცვის საკითხი და სადავო ღონისძიებათა კანონიერება. ამ საქმეში ECtHR-მა დაადგინა მე-9 მუხლის დარღვევა, რადგან სახელმწიფო ორგანოებმა სათანადოდ ვერ დაიცვეს განმცხადებლის პირადი ცხოვრებისა და კორესპონდენციის პატივისცემის უფლება; შედეგად, მათ ვერ შეძლეს ორი საპირისპირო ინტერესის სამართლიანად დაბალანსება.

Bodil Lindqvist-ის186 საქმე

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

Bodil Lindqvist-ის საქმე შეეხებოდა ერთ-ერთ ინტერნეტგვერდზე სხვადასხვა ადამიანის იდენტიფიცირებას ისეთი საშუალებებით, როგორიცაა სახელი, ტელეფონის ნომერი და ინფორმაცია ჰობის შესახებ. CJEU-მ დაადგინა, რომ „ვებგვერდის მეშვეობით სხვადასხვა პიროვნებაზე მითითება და მათი იდენტიფიცირება სახელით ან სხვა საშუალებით, მონაცემთა დაცვის დირექტივის მე-3 მუხლის 1 პუნქტის ფარგლებში, არის „პერსონალური მონაცემების დამუშავება მთლიანად ან ნაწილობრივ ავტომატური საშუალებით“.

მონაცემთა ასეთი დამუშავება არ ხდება ცალსახად პირადი ან ოჯახური საქმიანობის შემთხვევაში, რომელზეც არ ვრცელდება ევროკავშირის მონაცემთა დაცვის წესები: ეს გამონაკლისი „უნდა განიმარტოს მხოლოდ იმ საქმიანობასთან მიმართებით, რომელიც ხორციელდება პიროვნების პირადი ან ოჯახური ცხოვრების ფარგლებში. ნათელია, რომ ეს არ ეხება პერსონალურ მონაცემთა დამუშავებას ინტერნეტში გამოქვეყნებისას, იმ მიზნით, რომ ისინი ადამიანთა განუსაზღვრელი რაოდენობისათვის იყოს ხელმისაწვდომი.

Franšek Ryneš-ის საქმე

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

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

SWIFT-ის საქმე

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

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

Google Spain-ის საქმეში განმცხადებელი, ესპანეთის მოქალაქე, მოითხოვდა Google-იდან ძველი საგაზეთო სტატიის ამოღებას მისი ფინანსური წარსულის შესახებ. CJEU-მ იმსჯელა, იყო თუ არა საძიებო სისტემის ოპერატორი Google მონაცემთა „დამმუშავებელი“, მონაცემთა დაცვის დირექტივის 2(დ) მუხლის თანახმად. 225 CJEU-მ გაითვალისწინა „დამმუშავებლის“ ფართო განსაზღვრება „მონაცემთა სუბიექტების ეფექტიანად და სრულად დაცვისათვის“226 და დაადგინა, რომ საძიებო სისტემის ოპერატორი განსაზღვრავდა საქმიანობის მიზნებსა და საშუალებებს და უზრუნველყოფდა ვებსაიტების გამომცემელთა მიერ ინტერნეტგვერდებზე ატვირთული მონაცემების ხელმისაწვდომობას ნებისმიერი მომხმარებლისათვის, რომელიც ძიებას ახორციელებს მონაცემთა სუბიექტის სახელით.227 შესაბამისად, CJEU-მ დაადგინა, რომ Google შეიძლება „დამმუშავებლად“ ჩაითვალოს.

საქმე K.H. and Others v. Slovakia

პასუხი : ამ საქმეში ბოშა ქალებმა, რომლებმაც მშობიარობისას დახმარება მიიღეს აღმოსავლეთსლოვაკეთის 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

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

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

საქმეში Smaranda Bara and Others v. Preşidentele Casei Naţionale de Asigurări de Sănătate, Casa Naţională de Administrare Fiscală (ANAF)286 რუმინეთის ეროვნულმა საგადასახადო ორგანომ თვითდასაქმებულ პირთა შემოსავლების საგადასახადო მონაცემები გადასცა ჯანმრთელობის დაზღვევის ეროვნულ ფონდს, რის საფუძველზეც განისაზღვრა ჯანმრთელობის დაზღვევის გადასახადის ოდენობა. CJEU-მ იმსჯელა, უნდა ეცნობებინათ თუ არა მონაცემთა სუბიექტებისთვის დამმუშავებლის ვინაობა და მონაცემთა გადაცემის მიზანი მანამდე, სანამ მათ დაამუშავებდა ჯანმრთელობის დაზღვევის ეროვნული ფონდი. CJEU-მ დაადგინა: როდესაც წევრი სახელმწიფოს ერთი საჯარო ადმინისტრაციული ორგანო პერსონალურ მონაცემებს მეორე ასეთ უწყებას გადასცემს შემდგომი დამუშავებისთვის, საჭიროა მონაცემთა სუბიექტების ინფორმირება ამის შესახებ.

საქმე Y v. Turkey

საქმეში Y v. Turkey განმცხადებელს ჰქონდა აივ დადებითი სტატუსი. ვინაიდან საავადმყოფოში 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 პირდი ცხოვრების პატივისცემის უფლება. თუმცა, საავადმყოფოს პერსონალის უსაფრთხოების დაცვის საჭიროების გათვალისწინებით, სასამართლომ ამ ინფორმაციის გაზიარება განმცხადებლის უფლებების დარღვევად არ მიიჩნია.

European Commission v. Federal Republic of Germany

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

European Commission v. Republic of Austria

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

European Commission v. Hungary

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

Weltimmo-ს საქმე

Weltimmo-ს საქმეში510 CJEU-მ იმსჯელა ეროვნული საზედამხედველო ორგანოების კომპეტენციებზე, მათი იურისდიქციის გარეთ შექმნილ ორგანიზაციებთან დაკავშირებით. Weltimmo სლოვაკეთში რეგისტრირებული კომპანიაა, რომელიც უნგრეთში არსებული უძრავი ქონების ყიდვა-გაყიდვის ვებგვერდს მართავს. რეკლამის დამკვეთებმა უნგრეთის მონაცემთა დაცვის საზედამხედველო ორგანოში შეიტანეს საჩივარი მონაცემთა დაცვის შიდასახელმწიფოებრივი კანონმდებლობის დარღვევაზე, რის შედეგადაც საზედამხედველო ორგანომ Weltimmo-ს ჯარიმა დააკისრა. კომპანიამ ჯარიმა გაასაჩივრა ეროვნულ სასამართლოში, რომელმაც CJEU-ს მიმართა და სთხოვა დადგენა, აძლევდა თუ არა ევროკავშირის მონაცემთა დაცვის დირექტივა წევრი სახელმწიფოს საზედამხედველო ორგანოს მონაცემთა დაცვის ეროვნული კანონმდებლობის გამოყენების უფლებას იმ კომპანიასთან მიმართებით, რომელიც სხვა წევრ ქვეყანაში იყო დარეგისტრირებული.CJEU-მ განმარტა, რომ მონაცემთა დაცვის დირექტივის მე-4 მუხლის 1 (ა) პუნქტი წევრ სახელმწიფოს აძლევს უფლებას, მონაცემთა დაცვის საკუთარი კანონმდებლობა გამოიყენოს სხვა წევრ სახელმწიფოში რეგისტრირებული დამმუშავებლის მიმართ, თუკი ის „შესაბამისი წევრი სახელმწიფოს ტერიტორიაზე სტაბილურად ორგანიზებული დაწესებულების მეშვეობით, რეალურად ეწევა თუნდაც მინიმალურ ეფექტიან საქმიანობას მონაცემთა დამუშავების კუთხით.“ CJEU-მ აღნიშნა, რომ მის ხელთ არსებულ ინფორმაციაზე დაყრდნობით, Weltimmo-ს საქმიანობა უნგრეთში რეალური და ეფექტიანი გახლდათ, რადგან კომპანიის წარმომადგენელი ამ ქვეყანაში სლოვაკეთის კომპანიათა რეესტრში უნგრული მისამართით იყო დარეგისტრირებული; ასევე, მას უნგრეთში ჰქონდა საბანკო ანგარიში და საფოსტო ყუთი და უნგრულ ენაზე დაწერილ აქტივობებს ახორციელებდა. ეს ინფორმაცია მიუთითებდა დაწესებულების რეალურად არსებობაზე, რის გამოც Weltimmo-ს აქტივობებზე ვრცელდებოდა უნგრეთის მონაცემთა დაცვის კანონმდებლობა და საზედამხედველო ორგანოს იურისდიქცია. თუმცა, CJEU-მ ეროვნულ სასამართლოს მიანდო ამ ინფორმაციის გადამოწმება, კერძოდ: თუ ეროვნული სასამართლო დაადგენდა, რომ Weltimmo-ს უნგრეთში ჰქონდა დაწესებულება, უნგრეთის საზედამხედველო ორგანოს ექნებოდა ჯარიმის დაკისრების უფლებამოსილება; სასამართლოს მიერ საპირისპირო გადაწყვეტილების მიღების შემთხვევაში, კომპანიაზე გავრცელდებოდა იმ წევრი სახელმწიფოს კანონმდებლობა, სადაც კომპანია რეგისტრირებული იყო. ვინაიდან საზედამხედველო ორგანოების უფლებამოსილება უნდა განხორციელდეს სხვა წევრი სახელმწიფოების ტერიტორიულ სუვერენიტეტთან შესაბამისობაში, ამ საქმეში უნგრეთის საზედამხედველო ორგანოს არ ჰქონდა ჯარიმის დაკისრების უფლება. თუმცა, რაკი მონაცემთა დაცვის დირექტივა ითვალისწინებდა საზედამხედველო ორგანოებს შორის თანამშრომლობის ვალდებულებას, უნგრეთის საზედამხედველო ორგანოს შეეძლო, სლოვაკეთის ასეთივე ორგანოსთვის ეთხოვა აღნიშნული საკითხის გარკვევა, სლოვაკეთის კანონმდებლობის დარღვევის დადგენა და მისივე სამართლით გათვალისწინებული სანქციების დაკისრება.

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 მოხდედ არაპრპორციული ჩარევა და მინიმაზაციის გამოყენება ძირითად შემთხვევაში, მხოლოდ მაშინ ხდება, როცა დამუშავების სხვა საშუალება არ არის.

**12)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

**13) 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

**14)  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. **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.

1. **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.

1. **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.

1. **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.

1. **რა არის პერსონალურ მონაცემთა უსაფრთხოების დარღვევის შესახებ 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.

1. **განმარტეთ მონაცემთა დამმუშავებელი**

**პასუხი :** მონაცემთა დამმუშავებელია პირი, რომელიც განსაზღვრავს თუ როგორ მუშავდება სხვა პერსონების პერს.ინფორმაციის დამუშავება, დამუშავების საშუალებები და მიზნები. პერს. ინფორმაცია შეიძლება დამუშავდეს ერთი ან ერთზე მეტი პირი, როდესაც ინფორმაციას 1 ზე მეტი პირი ამუშავებს, ამას ეწოდება ერთობლივი დამუშავება

1. **რას გულისხმობს მონაცემთა დამუშავების სამართლიანობის პრინციპი?**

**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. **ჩამოთვალეთ განსაკუთრებული კატეგორიის პერსონალური მონაცემები**

**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. **რა განსხვავებაა მონაცემთა არაავტომატურ და ავტომატურ დამუშავებას შორის?**

**პასუხი :** მონაცემთა ავტომატურ დამუშავებაში მოიაზრება ისეთი დამუშავება,

რომელიც ცოცხალ დამმუშავებელს არ მოითოვს, მაგალითად კომპიუტერები,

ტელეფონები, აპლიკაციები, საძიებო სისტემები, სამეთვალყურეო კამერები და

ა.ს.შ

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. **რას ნიშნავს მონაცემთა დამუშავება?**

პასუხი :

მონაცემთა დამუშავება არის ნებისმიერი ქმედება, რომელიც პერსონალური მონაცემების მიმართ ხორციელდება: შეგროვება, ჩაწერა, შენახვა, გამოყენება, გამჟღავნება, ფოტოზე აღბეჭდვა, მესამე პირისთვის გადაცემა, გავრცელება, წაშლა, განადგურება და სხვა.

1. **რა განსხვავებაა მონაცემთა მიმღებსა და მესამე პირს შორის?**

პასუხი :

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

მესამე მხარე/ პირი - ეს არის ფიზიკური, იურიდიული ან ორგანიზაციის წარმომადგენელი პირი/ორგანიზაცია, რომელსაც აქვს პირდაპირი უფლება - დამმუშავებელი ორგანიზაციის, პერს. ინფორმაციის მფლობელი ფიზიკური პირის ან უფლებამოსილი პირის მიერ - დაამუშავოს ინფორმაცია.

მონაცემთა მიმღებია - ორგანიზაციის წარმომადგენელი, ფიზიკური ან იურიდიული პირი, სააგენტოს ან უწყისის წარმომადგენელი, რომელსაც არ აქვს კავშირი მონაცემთა დამამუშავებელ ან მესამე პირთან - ან პირიქით უკავშირდება მას (მაგალითად, როგორც დამამუშავებელი ორგანიზაციის სხვა უწეყების ან დეპარტამენტის წარმომადგენელი)

1. **რას გულისხმობს მონაცემთა უსაფრთხოების მაღალი დონის უზრუნველყოფა?**

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.

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.

1. **რა არის მონაცემთა დაცვის ოფიცრის ფუნქცია?**

პასუხი :

მონაცემთა დაცვის ოფიცერი პირია, რომელიც ინფორმაციის დამამუშავებელ ორგანიზაციას აწვდის ინფორმაციას იმის შესახებ, თუ რამდენად შეესაბამება მათ მიერ ჩატარებული დამუშავების პროცესი მონაცემთა დამუშავების შესაბამის წესებსა და კანონებს. ის ერთგვარი „ხიდია“ მონაცემთა დამმუშავებელს, მის ზედამხედველ ორგანიზაციებსა და იმ სუბიექტს შორის, ვისი პერსონალური ინფორმაციის დამუშავებაც ხდება. მონაცემთა ოფიცერს აქვს ვალდებულება, უზრუნველყოს რომ პირის პერსონალური ინფორმაცია მუშავდება კონვენციის მიერ გამოცემული კანონის თანახმად, დამამუშავებელი ორგანიზაციის მიერ

1. **რას ნიშნავს მონაცემთა დაცვის რისკების შეფასება?**

პასუხი :

მაშინ როდესაც მონაცემთა დამამუშავებელი ორგანიზაციები ამუშავებენ პირის პერსონალურ ინფორმაციას, იქმნება საფრთხე, რომ ეს ინფორმაცია შეიძლება გაიჟონოს, გადაკეთდეს, არაავტორიზებულ პირთა ხელში მოხვდეს და ასე შემდეგ...

სწორედ ამიტომ, როგორც ევროპის საბჭო, ისე ევროკავშირი ავალდებულებს მონაცემთა დაცვის შესახებ კანონმდებლობის ხელის მომწერებს, რომ შეაფასონ ის რიკები, რომლებიც ზემოხსენებულმა საფრთხეება შეიძლება შეუქმნან პირის ძირეულ თავისუფლებას. პირველ რიგში, უნდა შეფასდეს რისკები, ამის შემდეგ კი უნდა იქნას შემუშავებული ისეთი მოდელი, რომელიც მაქსიმალურად მოახდენს რისკების თავიდან აცილებას.