ევროპის პარლამენტისა და ევროპის საბჭოს 2016 წლის 27 აპრილის დირექტივა კომპეტენტური ორგანოების მიერ დანაშაულების პრევენციის, გამოძიების, დადგენის ან სისხლისსამართლებრივი დევნის, ან სასჯელთა აღსრულების მიზნით პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვის, მონაცემთა თავისუფალი მიმოცვლისა და საბჭოს 2008/977/ŽHA ჩარჩო გადაწყვეტილების გაუქმების შესახებ

ევროპის პარლამენტი და ევროკავშირის საბჭო,

ითვალისწინებენ რა ,,ევროკავშირის ფუნქციონირების შესახებ" ხელშეკრულებასა და ხელშეკრულების მე-16 მუხლის მე-2 ნაწილს,

ითვალისწინებენ რა ევროკომისიის წინადადებას,

ეროვნული პარლამენტებისათვის საკანონმდებლო აქტის პროექტის გადაგზავნის შემდეგ,

ითვალისწინებენ რა რეგიონების კომიტეტის[1] მოსაზრებას,

მოქმედებენ რა სტანდარტული საკანონმდებლო პროცედურის[2] ფარგლებში,

მხედველობაში იღებენ, რომ:

(1) ფიზიკური პირების დაცვა პერსონალური მონაცემების დამუშავებასთან მიმართებით ფუნდამენტური უფლებაა. ევროკავშირის ფუნდამენტური უფლებების ქარტიის (,,ქარტია") მე-8 მუხლის პირველი პუნქტითა და ,,ევროკავშირის ფუნქციონირების შესახებ" ხელშეკრულების მე-16 მუხლის პირველი პუნქტით გათვალისწინებულია, რომ ყველას აქვს მასთან დაკავშირებული პერსონალური მონაცემების დაცვის უფლება.

---

[1] OJ C 391, 18.12.2012, გვ. 127.

[2] ევროპარლამენტის 2014 წლის 12 მარტის პოზიცია (რომელიც ჯერ არ გამოქვეყნებულა ოფიციალურ ჟურნალში) და ევროპის საბჭოს პოზიცია 2016 წლის 8 აპრილის მოსმენაზე (ჯერ არ გამოქვეყნებულა ოფიციალურ ჟურნალში). ევროპარლამენტის 2016 წლის 14 აპრილის პოზიცია.

(2) პერსონალური მონაცემების დამუშავებასთან დაკავშირებით ფიზიკურ პირთა დაცვის პრინციპები და წესები, მათი მოქალაქეობის ან საცხოვრებელი ადგილის მიუხედავად, პატივს უნდა სცემდეს ამ პირთა ფუნდამენტურ უფლებებსა და თავისუფლებებს, განსაკუთებით მათ უფლებას პერსონალურ მონაცემთა დაცვაზე. წინამდებარე დირექტივის მიზანია თავისუფლების, უსაფრთხოებისა და მართლმსაჯულების სფეროს სრულყოფაში წვლილის შეტანა.

(3) სწრაფმა ტექნოლოგიურმა განვითარებამ და გლობალიზაციამ პერსონალურ მონაცემთა დაცვის სფეროში ახალი გამოწვევები შექმნა. პერსონალურ მონაცემთა შეგროვებისა და გაზიარების მოცულობა მნიშვნელოვნად გაიზარდა. ტექნოლიგია პერსონალური მონაცემების უპრეცედენტო მოცულობით დამუშავების შესაძლებლობას იძლევა ისეთი ღონისძიებების განსახორციელებლად, როგორიცაა დანაშაულების პრევენცია, გამოძიება, დადგენა, სისხლისსამართლებრივი დევნა ან სასჯელის აღსრულება.

(4) უნდა განხორციელდეს დანაშაულების პრევენციის, გამოძიების, დადგენის ან სისხლისსამართლებრივი დევნის, სასჯელების აღსრულების, ასევე, ევროკავშირის ტერიტორიაზე საზოგადოებრივი უსაფრთხოების წინააღმდეგ მიმართული საფრთხეებისაგან დაცვისა და პრევენციის მიზნით კომპეტენტურ ორგანოებს შორის პერსონალურ მონაცემთა თავისუფალი გადადინებისა და ამ მონაცემების მესამე სახელმწიფოებისათვის და საერთაშორისო ორგანიზაციებისათვის გადაცემის ხელშეწყობა ისე, რომ ამავდროულად, უზრუნველყოფილი იქნეს პერსონალურ მონაცემთა დაცვის მაღალი სტანდარტი. მოვლენათა ამგვარი განვითარება საჭიროებს ევროკავშირში პერსონალურ მონაცემთა დაცვის უფრო ძლიერი და თანმიმდევრული კანონმდებლობის შექმნას, რომელიც აღსრულების ძლიერი წესებითაა უზრუნველყოფილი.

(5) ევროპარლამენტისა და საბჭოს 95/46/EC დირექტივის[3] მოქმედება ვრცელდება წევრი სახელმწიფოების როგორც კერძო, ისე საჯარო სექტორის მიერ პერსონალურ მონაცემთა ყოველგვარ დამუშავებაზე. თუმცა, მისი მოქმედება არ ვრცელდება პერსონალურ მონაცემთა დამუშავებაზე ისეთი საქმიანობის პროცესში, რომელიც სცილდება

[3] ევროპარლამენტისა და ევროპის საბჭოს 1995 წლის 24 ოქტომბრის 95/46/EC დირექტივა პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვისა და მონაცემთა თავისუფალი გადადინების შესახებ (OJ L 281, 23.11.1995, გვ. 31).

ევროკავშირის კანომდებლობის მოქმედების ფარგლებს, როგორიცაა, მაგალითად, სისხლის სამართლის საქმეებზე სამართლებრივი დახმარებისა და საპოლიციო თანამშრომლობის სფეროში საქმიანობა.

(6) საბჭოს 2008/977/JHA ჩარჩო გადაწყვეტილების[4] მოქმედება ვრცელდება სისხლის სამართლის საქმეებზე სამართლებრივი დახმარებისა და საპოლიციო თანამშრომლობის სფეროზე. ხსენებული ჩარჩო გადაწყვეტილების მოქმედების სფერო შემოიფარგლება წევრ სახელმწიფოებს შორის გადაცემული ან სხვაგვარად ხელმისაწვდომი პერსონალური მონაცემების დამუშავებით.

(7) ფიზიკურ პირთა პერსონალური მონაცემების დაცვის თანმიმდევრული და მაღალი სტანდარტის უზრუნველყოფა და წევრი სახელმწიფოების კომპეტენტურ ორგანოებს შორის პერსონალური მონაცემების გაცვლის ხელშეწყობა გადამწყვეტი მნიშვნელობისაა სისხლის სამართლის საქმეებზე ეფექტიანი სამართლებრივი დახმარებისა და საპოლიციო თანამშრომლობის უზრუნველსაყოფად. ამისათვის, კომპეტენტური ორგანობის მიერ დანაშაულების პრევენციის, გამოძიების, დადგენის, სისხლისსამართლებრივი დევნის ან სასჯელების აღსრულების მიზნით, ასევე ევროკავშირის ტერიტორიაზე საზოგადოებრივი უსაფრთხოების წინააღმდეგ მიმართული საფრთხეებისაგან დაცვისა და პრევენციის მიზნებით პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა უფლებებისა და თავისუფლებების დაცვის სტანდარტი თანაბარი უნდა იყოს ყველა წევრ სახელმწიფოში. ევროკავშირის ტერიტორიაზე პერსონალურ მონაცემთა ეფექტიანი დაცვა საჭიროებს მონაცემთა სუბიექტების უფლებებისა და მონაცემთა დამმუშავებლების ვალდებულებების გაძლიერებას, ისევე როგორც მონიტორინგის შესაბამის უფლებამოსილებებს და წევრ სახელმწიფოებში პერსონალურ მონაცემთა დაცვის წესებთან შესაბამისობის უზრუნველყოფას.

(8) ,,ევროკავშირის ფუნქციონირების შესახებ" ხელშეკრულების მე-16 მუხლის მე-2 პუნქტი ავალდებულებს ევროპარლამენტსა და საბჭოს, განსაზღვრონ პერსონალური მონაცემების

[4] ევროპის საბჭოს 2008 წლის 27 ნოემბრის ჩარჩო გადაწყვეტილება 2008/977/JHA სისხლის სამარტლის საქმეებზე საპოლიციო და სამართლებრივი დახმარების ფარგლებში დამუშავებული პერსონალური მონაცემების დაცვის შესახებ (OJ L 350, 30.12.2008, გვ. 60).

დამუშავებასთან მიმართებით ფიზიკურ პირთა დაცვისა და პერსონალურ მონაცემთა თავისუფალი მოძრაობის წესები.

(9) აღნიშნული საფუძვლით ევროპარლამენტისა და საბჭოს (EU) 2016/679[5] რეგულაცია განსაზღვრავს პერსონალური მონაცემების დამუშავებისას ფიზიკურ პირთა დაცვისა და ევროკავშირის ტერიტორიაზე პერსონალურ მონაცემთა თავისუფალი გადადინების შესახებ ზოგად წესებს.

(10) მთავრობათშორისი კონფერენციის საბოლოო აქტზე თანდართულ ,,სისხლის სამართლის საქმეებზე სამართლებრივი დახმარებისა და საპოლიციო თანამშრომლობის სფეროში პერსონალურ მონაცემთა დაცვის" N21 დეკლარაციაში, რომლითაც დამტკიცდა ლისაბონის შეთანხმება, კონფერენციამ აღიარა, რომ ,,ევროკავშირის ფუნქციონირების შესახებ" ხელშეკრულების მე-16 მუხლზე დაყრდნობით, შესაძლოა, აუცილებელი გახდეს სისხლის სამართლის საქმეებზე სამართლებრივი დახმარებისა და საპოლიციო თანამშრომლობის სფეროში პერსონალური მონაცემების დაცვისა და მონაცემთა თავისუფალი გადადინების სპეციალური წესების შემუშავება აღნიშნული სფეროების სპეციფიური ბუნების გათვალისწინებით.

(11) შესაბამისად, ხსენებული სფეროები უნდა დარეგულირდს დირექტივით, რომელშიც განსაზღვრული იქნება კომპეტენტური ორგანოების მიერ დანაშაულების პრევენციის, გამოძიების, დადგენის, სისხლისსამართლებრივი დევნის, სასჯელების აღსრულების, ასევე, ევროკავშირის ტერიტორიაზე საზოგადოებრივი უსაფრთხოების წინააღმდეგ მიმართული საფრთხეებისაგან დაცვისა და პრევენციის მიზნით პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვის სპეციალური წესები, ამ საქმიანობის სპეციფიური ხასიათის გათვალისწინებით. ამგვარ კომპეტენტურ ორგანოებს შესაძლოა მიეკუთვნებოდნენ არამხოლოდ ისეთი საჯარო უწყებები, როგორებიცაა მართლმსაჯულების ორგანოები, პოლიცია ან სხვა სამართალდამცავი უწყებები, არამედ ნებისმიერი სხვა ორგანო ან უწყება, რომელსაც წევრი სახელმწიფოს კანონმდებლობით დაკისრებული აქვს წინამდებარე დირექტივის მიზნებისათვის საჯარო

[5] პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვის, მონაცემთა თავისუფალი გადადინებისა და 95/46/EC დირექტივის გაუქმების შესახებ ევროპარლამენტისა და ევროსაბჭოს 2016 წლის 27 აპრილის რეგულაცია (მონაცემთა დაცვის ძირითადი რეგულაცია) (იხ. ოფიციალურიჟურნალის პირველი გვერდი)

უფლებამოსილების განხორციელება. როდესაც ამგვარი უწყება ან ორგანო ამუშავებს პერსონალურ მონაცემებს წინამდებარე დირექტივის მიზნებისაგან განსხვავებული მიზნით, მასზე ვრცელდება (EU) 2016/679 რეგულაცის მოქმედება. შესაბამისად, (EU) 2016/679 რეგულაციის მოქმედება ვრცელდება ისეთ შემთხვევებზე, როდესაც უწყება ან ორგანო, აგროვებს პერსონალურ მონაცემებს სხვა მიზნებისათვის და შემდგომ ამუშავებს ამ მონაცემებს მასზე კანონით დაკისრებული მოვალეობის შესასრულებლად. მაგალითად, სისხლის სამართლის დანაშაულების გამოძიების, დადგენის ან სისხლის სამართლებრივი დევნის მიზნებისათვის ფინანსური დაწესებულებები ინახავენ მათ მიერ დამუშავებულ გარკვეულ მონაცემებს და აწვდიან მათ მხოლოდ კომპეტენტურ სახელმწიფო ორგანოებს კონკრეტულ შემთხვევებში და წევრი სახელმწიფოს კანონმდებლობის შესაბამისად. უწყება ან ორგანო, რომელიც ამგვარი უწყებების სახელით, ამ დირექტივის ფარგლებში ამუშავებს მონაცემებს, უნდა ემორჩილებოდეს სავალდებულო ხელშეკრულებას ან სამართლებრივ აქტს და იმ დებულებებს, რომლებიც წინამდებარე დირექტივის შესაბამისად ვრცელდება დამმუშავებლებზე. ამავდროულად, დამმუშავებლის მიერ წინამდებარე დირექტივის მოქმედების სფეროს გარეთ მონაცემთა დამუშავების მიზნებისათვის (EU) 2016/679 რეგულაციის გამოყენების წესი უცვლელი რჩება.

(12) პოლიციის ან სხვა სამართალდამცავი უწყებების საქმინობა ძირითადად მოიცავს დანაშაულების პრევენციას, გამოძიებას, დადგენას ან სისხლისსამართლებრივ დევნას, მათ შორის, ისეთ საპოლიციო საქმიანობას, როდესაც წინასწარ არ არის ცნობილი, ინციდენტი სისხლის სამართლის დანაშაულია თუ არა. ასეთი საქმიანობა შესაძლოა, ასევე, მოიცავდეს უფლებამოსილების განხორციელებას იძულებითი ზომების გამოყენებით, როგორებიცაა საპოლიციო საქმიანობა დემონსტრაციებზე, მასშტაბურ სპორტულ ღონისძიებებსა და ამბოხებისას. საქმიანობა, ასევე, მოიცავს მართლწესრიგის დაცვას, როგორც პოლიციაზე ან სხვა სამართალდამცავ უწყებაზე დასიკრებულ ამოცანას, რომელიც აუცილებელია საზოგადოებრივი უსაფრთხოებისა და საზოგადოების ფუნდამენტური ინტერესების წინააღმდეგ მიმართული საფრთხეებისაგან დასაცავად, რომლებმაც შეიძლება გამოიწვიონ სისხლის სამართლის დანაშაულის ჩადენა. წევრ სახელმწიფოებს უფლება აქვთ, კომპეტენტურ ორგანოებს დააკისრონ სხვა ამოცანების შესრულება, რომლებიც პირდაპირ დანაშაულების პრევენციის, გამოძიების, დადგენის, სისხლისსამართლებრივი დევნის ან სასჯელების აღსრულების მიზნით, ასევე, ევროკავშირის ტერიტორიაზე საზოგადოებრივი უსაფრთხოების წინააღმდეგ მიმართული საფრთხეებისაგან დაცვისა და პრევენციის

მიზნით არ ხორციელდება, იმ პირობით, რომ პერსონალურ მონაცემთა განსხვავებული მიზნებით დამუშავება, თუ ის ევროკავშირის კანონმდებლობის ფარგლებში ხორციელდება, ექვემდებარება (EU) 2016/679 რეგულაციის მოქმედების სფეროს.

(13) წინამდებარე დირექტივის მიზნებისათვის დანაშაული წარმოადგენს ევროკავშირის კანონმდებლობის ავტონომიურ კონცეფციას, როგორც ის განმარტებულია ევროკავშირის მართლმსაჯულების სასამართლოს ('მართლმსაჯულების სასამართლო') მიერ.

(14) ვინაიდან წინამდებარე დირექტივის მოქმედება არ ვრცელდება პერსონალურ მონაცემთა დამუშავებაზე ისეთი საქმიანობისას, რომელიც ევროკავშირის კანონმდებლობის იურისდიქციის ფარგლებს გარეთაა, ეროვნულ უსაფრთხოებასთან დაკავშირებული საქმიანობა, ეროვნულ უსაფრთხოებასთან დაკავშირებული უწყებების ან ქვედანაყოფების საქმიანობა და პერსონალურ მონაცემთა დამუშავება წევრი სახელმწიფოების მიერ ევროკავშირის ხელშეკრულების V ნაწილის მე-2 თავის იურისდიქციაში შემავალი საქმიანობის განხორციელებისას, არ უნდა ჩაითვალოს წინამდებარე დირექტივის იურისდიქციაში შემავალ საქმიანობად.

(15) ევროკავშირის მასშტაბით სამართლებრივად აღსრულებადი უფლებების მეშვეობით ფიზიკურ პირთა დაცვის ერთგვაროვანი სტანდარტის უზრუნველსაყოფად და კომპეტენტურ ორგანოებს შორის პერსონალურ მონაცემთა გაცვლის შემაფერხებელი განსხვავებების თავიდან ასაცილებლად, წინამდებარე დირექტივამ უნდა განსაზღვროს დანაშაულების პრევენციის, გამოძიების, დადგენის, სისხლისსამართლებრივი დევნის ან სასჯელების აღსრულების, ასევე, საზოგადოებრივი უსაფრთხოების წინააღმდეგ მიმართული საფრთხეებისაგან დაცვისა და პრევენციის მიზნით მონაცემთა დამუშავებისა და მონაცემთა თავისუფალი მიმოცვლის ჰამორნიზებული წესები. წევრი სახელმწიფოების კანონმდებლობის დირექტივასთან დაახლოებამ არ უნდა გამოიწვიოს პერსონალურ მონაცემთა დაცვის შესუსტება, არამედ პირიქით, უნდა უზრუნველყოს დაცვის მაღალი სტანდარტი ევროკავშირის მასშტაბით. წევრ სახელმწიფოებს არ ეკრძალებათ წინამდებარე დირექტივით კომპეტენტური ორგანოების მიერ პერსონალურ მონაცემთა დამუშავებისას მონაცემთა სუბიექტის უფლებებისა და თავისუფლებების დასაცავად განსაზღვრულ გარანტიებზე უფრო მაღალი გარანტიების დაწესება.

(16) წინამდებარე დირექტივა არ ზღუდავს ოფიციალური დოკუმენტების საზოგადოებისათვის ხელმისაწვდომობის პრინციპს. (EU) 2016/679 რეგულაციის თანახმად, საჯარო ინტერესის სფეროში განსახორციელებელი საქმიანობისათვის საჯარო უწყების ან საჯარო ან კერძო დაწესებულების ხელთ არსებულ ოფიციალურ დოკუმენტებში მოცემული პერსონალური მონაცემები შესაძლოა ამ ორგანოს ან დაწესებულების მიერ გასაჯაროვდეს ევროკავშირის ან იმ წევრი სახელმწიფოს კანონმდებლობის შესაბამისად, რომელიც ვრცელდება ამ ორგანოსა თუ უწყებაზე, იმისათვის, რომ დაცული იყოს ბალანსი ოფიციალურ დოკუმენტებთან საზოგადოების წვდომასა და პერსონალურ მონაცემთა დაცვის უფლებას შორის.

(17) წინამდებარე დირექტივით გარანტირებული დაცვა ვრცელდება ფიზიკურ პირებზე, მათი მოქალაქეობის ან საცხოვრებელი ადგილის მიუხედავად, მათი პერსონალური მონაცემების დამუშავებასთან მიმართებით.

(18) დარღვევის სერიოზული საფრთხის თავიდან ასაცილებლად, ფიზიკური პირების დაცვა ტექნოლოგიურად ნეიტრალური უნდა იყოს და არ უნდა იყოს დამოკიდებული გამოყენებულ ტექნიკებზე. ფიზიკურ პირთა დაცვა ვრცელდება ავტომატური და არაავტომატური საშუალებებით პერსონალურ მონაცემთა დამუშავებაზე, თუ პერსონალური მონაცემები ფაილური სისტემის ნაწილია ან მომავალში გახდება მისი ნაწილი. წინამდებარე დირექტივის მოქმედება არ ვრცელდება ფაილებზე, ფაილთა წყებებზე, ისევე როგორც მათ გარეკანებზე, რომლებიც არ არის სტრუქტურირებული კონკრეტული კრიუტერიუმის მიხედვით.

(19) ევროპარლამენტისა და საბჭოს (EC) No 45/2001 რეგულაციის[6] მოქმედება ვრცელდება ევროკავშირის დაწესებულებების, ორგანოების, ოფისებისა და სააგენტოების მიერ პერსონალური მონაცემების დამუშავებაზე. რეგულაცია (EC) No 45/2001 და ევროკავშირის სხვა სამართლებრივი აქტები, რომელთა მოქმედება ვრცელდება პერსონალურ მონაცემთა ამგვარ დამუშავებაზე მორგებულ უნდა იქნეს (EU) 2016/679 რეგულაციით განსაზღვრულ პრინციპებსა და წესებზე.

[6] ევროპარლამენტისა და ევროსაბჭოს 2000 წლის 18 დეკემბრის (EC) No 45/2001 რეგულაცია ევროკავშირის დაწესებულებებისა და უწყებების მიერ პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვისა და მონაცემთა თავისუფალი გადადინების შესახებ (OJ L 8, 12.1.2001,გვ. 1).

(20) წინამდებარე დირექტივა არ ზღუდავს წევრ სახელმწიფოებს, ეროვნულ სისხლის სამართლის საპროცესო კანონმდებლობაში განსაზღვრონ დამუშავების ოპერაციები და პროცედურები, რომლებიც უკავშირდება სასამართლოების და მართლმსჯულების სხვა ორგანოების მიერ პერსონალურ მონაცემთა დამუშავებას, კერძოდ კი იმ მონაცემებთან მიმართებით, რომლებსაც შეიცავს სასამართლოს გადაწყვეტილებები ან სისხლის სამართლის საპროცესო მოქმედებების ოქმები.

(21) მონაცემთა დამუშავების პრინციპები უნდა გავრცელდეს ნებისმიერ ინფორმაციაზე, რომელიც უკავშირდება იდინტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს. იმის დასადგენად, ფიზიკური პირი იდენტიფიცირებადია თუ არა, მხედველობაში უნდა იქნეს მიღებული ყველა ზომა, მაგალითად, როგორიცაა გადარჩევა, რომლის გამოყენებაც გონივრულად და დიდი ალბათობით მოხდება დამმუშავებლის ან სხვა პირის მიერ ფიზიკური პირის პირდაპირი ან არაპირდაპირი იდენტიფიცირებისათვის. იმის დასადგენად, მოხდება თუ არა ზომების გონივრულად და დიდი ალბათობით მიღება ფიზიკური პირის იდენტიფიცირბისათვის, მხედველობაში უნდა იქნეს მიღებული ყველა ობიექტური ფაქტორი, როგორიცაა იდენტიფიცირების ხარჯები და საჭირო დრო, იმ ტექნოლოგიისა და ტექნოლოგიური განვითარების გათვალისწინებით, რომელიც ხელმისაწვდომია დამუშავების პროცესში. შესაბამისად, მონაცემთა დამუშავების პრინციპები არ უნდა გავრცელდეს ანონიმურ ინფორმაციაზე, კერძოდ კი ინფორმაციაზე, რომელიც არ უკავშირდება იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს ან პერსონალურ მონაცემებზე, რომლებიც ანონიმურია იმ დონეზე, რომ მონაცემთა სუბიექტის იდენტიფიცირება აღარ არის შესაძლებელი.

(22) სახელმწიფო ორგანოები, რომელთაც გადაეცემა პერსონალური მონაცემები კანონმდებლობით დაკისრებული ოფიციალური დავალების შესაბამისად, როგორებიც არიან საგადასახადო და საბაჟო ორგანოები, ფინანსური დანაშაულის გამოძიების ქვედანაყოფები, დამოუკიდებელი ადმინისტრაციული ორგანოები ან ფინანსური ბაზრის ორგანოები, რომლებიც პასუხისმგებელნი არიან ფასიანი ქაღალდების ბაზრის რეგულირებასა და ზედამხედველობაზე, არ უნდა ჩაითვალონ მონაცემთა მიმღებად, თუ ისინი იღებენ პერსონალურ მონაცემებს, რომლებიც აუცილებელია საზოგადოებრივ ინტერესში შემავალი მოკვლევის განსახორციელებლად ევროკავშირის ან წევრი

სახელმწიფოს კანონმდებლობის შესაბამისად. სახელმწიფო ორგანოების თხოვნა მონაცემთა გადაცემის თაობაზე ყოველთვის უნდა იყოს წერილობითი, დასაბუთებული, იშვიათი და არ უნდა უკავშირდებოდეს მთლიან ფაილურ სისტემას ან არ უნდა იწვევდეს ფაილური სისტემების დაკავშირებას. მონაცემთა დამუშავება ამ საჯარო უწყებების მიერ უნდა შეესაბამებოდეს მონაცემთა დაცვის მოქმედ წესებს დამუშავების მიზნების შესაბამისად.

(23) გენეტიკური მონაცემები უნდა განიმარტოს, როგორც პერსონალური მონაცემები, რომლებიც უკავშირდება ფიზიკური პირის მემკვიდრეობით ან შეძენილ გენეტიკურ მახასიათებელს, რომელიც იძლევა უნიკალურ ინფორმაციას ფიზიკური პირის ფიზიოლოგიის, ან ჯანმრთელობის შესახებ და რომლის მიღებაც ხდება ფიზიკური პირის ბიოლოგიური ნიმუშის ანალიზის შედეგად, კერძოდ კი ქრომოსომული ანალიზის, დეზოქსირიბონუკლეინის მჟავის (დნმ), რიბონკულეინის მჟავის (რნმ) ანალიზის ან სხვა ელემენტის ანალიზის შედეგად, რომელიც იძლევა ექვივალენტური ინფორმაციის მოპოვების შესაძლებლობას. გენეტიკური ინფორმაციის კომპლექსურობისა და სენსიტიურობის გათვალისწინებით, არსებობს დამმუშავებლის მიერ მისი ბოროტად გამოყენებისა და ხელახლა გამოყენების მაღალი რისკი. აკრძალული უნდა იყოს ნებისმიერი დისკრიმინაცია გენეტიკური მახასიათებლების საფუძველზე.

(24) ჯანმრთელობასთან დაკავშირებულ მონაცემებში უნდა ჩაითვალოს ყველა მონაცემი, რომელიც ეხება მონაცემთა სუბიექტის ჯანმრთელობის მდგომარეობას და რომელიც ამჟღავნებს ინფორმაციას მონაცემთა სუბიექტის ფიზიკური ან ფსიქიკური ჯანმრთელობის წარსული, ამჟამინდილი ან მომავალი მდგომაროების შესახებ. მასში შედის ინფორმაცია ფიზიკური პირის შესახებ, რომელიც შეგროვებულია ჯანდაცვის მომსახურეობის მისაღებად რეგისტრაციის ან მომსახურეობის გაწევის დროს, როგორც ეს მითითებულია ევროპარლამენტისა და საბჭოს 2011/24/EU დირექტივაში[7]; ნომერი, სიმბოლო ან მონაცემი, რომელიც მიენიჭა ფიზიკურ პირს ჯანმრთელობის დაცვის მიზნებისათვის მისი უნიკალურად იდენტიფიცირებისათვის; ინფორმაცია, რომელიც წარმოიშვა სხეულის ორგანოს ან სხეულის ნივთიერების ტესტირების ან შემოწმების, მათ შორის გენეტიკური მონაცემების და ბიოლოგიური ნიმუშის შემოწმების შედეგად; და ნებისმიერი ინფორმაცია

[7] ევროპარლამენტისა და ევროსაბჭოს 2011 წლის 9 მარტის 2011/24/EU დირექტივა ტრანსსასაზღვრო ჯანდაცვისას პაციენტთა უფლებების გამოყენების შესახებ (OJ L 88, 4.4.2011, გვ. 45).

ფიზიკური პირის დაავადების, უუნარობის, დაავადების რისკის, სამედიცინო ისტორიის, ამბულატორიული მკურნალობის ან მისი ფიზიოლოგიური ან ბიოსამედიცინო მდგომარეობის შესახებ, მიუხედავად იმისა, თუ რა წყაროსგანაა მიღებული, მაგალითად თერაპევტისაგან თუ ჯანდაცვის სფეროს სხვა პროფესიონალისაგან, საავადმყოფოსაგან, სამედიცინო მოწყობილობიდან თუ ინვიტრო დიაგნოსტირების ტესტიდან.

(25) ყველა წევრი სახელმწიფო დაკავშირებულია საერთაშორისო კრიმინალური პოლიციის ორგანიზაციასთან (ინტერპოლი). თავისი მისიის შესასრულებლად, ინტერპოლი იღებს, ინახავს და ავრცელებს პერსონალურ მონაცემებს საერთაშორისო დანაშაულის პრევენციისა და მასთან ბრძოლისათვის კომპეტენტური ორგანოების დასახმარებლად. ამდენად, საჭიროა ევროკავშირსა და ინტერპოლს შორის თანამშრომლობის გაძლიერება პერსონალური მონაცემების ეფექტიანი გაცვლის ხელშეწყობის გზით და იმავდროულად პერსონალური მონაცემების ავტომატური დამუშავებისას ფუნდამენტური უფლებებისა და თავისუფლებების პატივისცემის უზრუნველყოფით. წინამდებარე დირექტივის, კერძოდ საერთაშორისო გადაცემასთან დაკავშირებული დებულებების მოქმედება ვრცელდება იმ შემთხვევებზე, როდესაც პერსონალური მონაცემების გადაცემა ხდება ევროკავშირიდან ინტერპოლში და იმ ქვეყნებში, რომლებსაც ჰყავთ წარმომადგენელი ინტერპოლში. წინამდებარე დირექტივა არ ზღუდავს საბჭოს 2005/69/JHA საერთო პოზიციაში[8] და საბჭოს 2007/533/JHA გადაწვეტილებაში[9] განსაზღვრულ კონკრეტულ წესებს.

(26) მონაცემთა ნებისმიერი დამუშავება კანონიერი, სამართლიანი და გამჭვირვალე უნდა იყოს ფიზიკურ პირებთან მიმართებაში. მონაცემები უნდა დამუშავდეს მხოლოდ კონკრეტული, კანონით განსაზღვრული მიზნებით. ეს დებულება არ უკრძალავს სამართალდამცავ ორგანოებს განახორციელონ ისეთი საქმიანობა, როგორიცაა ოპერატიულ-სამძებრო მოქმედებები ან ვიდეოთვალთვალი. ასეთი საქმიანობა შეიძლება განხორციელდეს დანაშაულების პრევენციის, გამოძიების, დადგენის, სისხლისსამართლებრივი დევნის ან სასჯელების აღსრულების მიზნით, ასევე საზოგადოებრივი უსაფრთხოების წინააღმდეგ მიმართული საფრთხეებისაგან დაცვისა და პრევენციის მიზნით, თუ ეს ღონისძიებები გათვალისწინებულია კანონით და წარმოადგენს

[8] ევროსაბჭოს 2005 წლის 24 იანვრის საერთო პოზიცია 2005/69/JHA გარკვეული მონაცემების ინტერპოლთან მიმოცვლის შესახებ (OJ L 27, 29.1.2005, გვ. 61).

[9] ევროსაბჭოს 2007 წლის 12 ივნისის 2007/533/JHA გადაწყვეტილება მეორე თაობის შენგენის საინფორმაციო სისტემის (SIS II) დაგერგვისა და გამოყენების შესახებ (OJ L 205, 7.8.2007, გვ. 63)

აუცილებელ და პროპორციულ ზომას დემოკრატიულ საზოგადოებაში და სათანადოდაა დაცული ფიზიკური პირების ლეგიტიმური ინტერესები. მონაცემთა დაცვისას სამართლიანი დამუშავების პრინციპი წარმოადგენს ქარტიის 47-ე მუხლითა და ადამიანის უფლებათა ევროპული კონვენციით განსაზღვრული სამართლიანი სასამართლოს ცნებისაგან განსხვავებულ ცნებას. ფიზიკურ პირებს უნდა ეცნობოთ იმ რისკების, წესების, გარანტიებისა და უფლებების შესახებ, რომლებიც დაკავშირებულია მათი პერსონალური მონაცემების დამუშავებასთან და როგორ უნდა განახორციელონ მათი უფლებები დამუშავებასთან დაკავშირებით. მონაცემთა დამუშავების კონკრეტული მიზნები უნდა იყოს მკაფიო და კანონიერი და განისაზღვროს მონაცემთა შეგროვების პროცესში. პერსონალური მონაცემები დამუშავების მიზნების ადეკვატური და შესაბამისი უნდა იყოს. განსაკუთრებით უზრუნველყოფილი უნდა იყოს, რომ შეგროვებული პერსონალური მონაცემები არ იყოს არაპროპორციული და არ იქნეს შენახული იმაზე მეტი ხნით ვიდრე ეს აუცილებელია მათი დამუშავების მიზნების მისაღწევად. პერსონალური მონაცემები უნდა დამუშავდეს მხოლოდ იმ შემთხვევაში, თუ დამუშავების მიზნის მიღწევა სხვა გზებით გონივრულად შეუძლებელია. იმისათვის, რომ უზრუნველყოფილი იყოს მონაცემთა მხოლოდ საჭირო დროით შენახვა, დამმუშავებლის მიერ უნდა განისაზღვროს ვადები, მონაცემთა წაშლისა ან პერიოდული გადახედვისთვის. წევრმა სახელმწიფოებმა უნდა განსაზღვრონ დაცვის სათანადო გარანტიები იმ პერსონალური მონაცემებისათვის, რომლებიც ინახება ხანგრძლივი ვადით საჯარო ინტერესით არქივირების, სამეცნიერო, სტატისტიკური ან ისტორიული მიზნებისათვის.

(27) დანაშაულების პრევენციის, გამოძიების და სისხლისამართლებრივი დევნის განხორციელების მიზნით კომპეტენტური ორგანოებისათვის აუცილებელია პერსონალური მონაცემების დამუშავება, რომლებიც შეგროვდა კონკრეტული დანაშაულების პრევენციის, გამოძიების და დადგენის კონტექსტში ამ კონკრეტული დანაშაულების სისხლისსამართლებრივი დევნის კონტექსტს მიღმა დანაშაულებრივ საქმიანობაზე წარმოდგენის შექმნის და სხვადასხვა გამოვლენილ დანაშაულს შორის კავშირის დასადგენად.

(28) დამუშავებასთან დაკავშირებული უსაფრთხოების უზრუნველსაყოფად და წინამდებარე დირექტივის დარღვევით განხორციელებული დამუშავების თავიდან ასაცილებლად, პერსონალური მონაცემები უნდა დამუშავდეს იმგვარად, რომ

უზრუნველყოფილი იყოს უსაფრთხოებისა და კონფიდენციალურობის სათანადო სტანდარტი, მათ შორის, თავიდან უნდა იქნეს აცილებული პერსონალურ მონაცემებთან ან დამუშავებისთვის გამოყენებულ მოწყობილობებთან უკანონო წვდომა ან მათი უკანონო გამოყენება იმგვარად, რომ გათვალისწინებულ იქნეს ტექნოლოგიების ხელმისაწვდომბა, იმპლემენტაციის ხარჯები პერსონალურ მონაცემებთან დაკავშირებული რისკებისა და დასამუშავებელ მონაცემთა ხასიათის გათვალისწინებით.

(29) პერსონალური მონაცემები უნდა შეგროვდეს კონკრეტული, მკაფიო და კანონიერი მიზნებისათვის წინამდებარე დირექტივის ფარგლებში და არ უნდა დამუშავდეს დანაშაულების პრევენციის, გამოძიების, დადგენის, სისხლისსამართლებრივი დევნის ან სასჯელების აღსრულების, ასევე, საზოგადოებრივი უსაფრთხოების წინააღმდეგ მიმართული საფრთხეებისაგან დაცვისა და პრევენციის მიზნებთან შეუთავსებელი მიზნით. თუ პერსონალურ მონაცემთა დამუშავება ხდება იმავე ან სხვა დამმუშავებლის მიერ წინამდებარე დირექტივის ფარგლებში, მათი შეგროვების მიზნისაგან განსხვავებული მიზნით, ამგვარი დამუშავება დასაშვებია იმ პირობით, თუ ეს გათვალისწინებულია საკანონმდებლო დებულებებით და აუცილებელი და პროპორციულია ახალ მიზანთან მიმართებით.

(30) მონაცემთა სიზუსტის პრინციპი გამოყენებული უნდა იქნეს დამუშავების ხასიათისა და მიზნების გათვალისწინებით. კერძოდ, სამართალწარმოების პროცესში ჩვენებები, რომლებიც შეიცავენ პერსონალურ მონაცემებს, ეფუძნებიან ფიზიკური პირების სუბიექტურ აღქმებს და მათი გადამოწმება ყოველთვის შესაძლებელი არ არის. შესაბამისად, სიზუსტის მოთხოვნა უნდა გავრცელდეს არა ჩვენების სიზუსტეზე, არამედ ჩვენების მიცემის ფაქტზე.

(31) სისხლის სამართლის საქმეებზე სამართლებივი დახმარებისას და საპოლიციო თანამშრომლობის სფეროში პერსონალური მონაცემების დამუშავებისათვის დამახასიათებელია სხვადასხვა კატეგორიის მონაცემთა სუბიექტებთან დაკავშირებული პერსონალური მონაცემების დამუშავება. ამდენად, საჭიროების შემთხვევაში და რამდენადაც ეს შესაძლებელია, მკვეთრად უნდა გაიმიჯნოს სხვადასხვა კატეგორიის მონაცემთა სუბიექტების პერსონალური მონაცემები, როგორებიცაა: ეჭვმიტანილები,

დანაშაულისათვის მსჯავრდებული პირები, დაზარალებულები და სხვა მხარეები, მაგალითად, მოწმეები; პირები, რომლებიც ფლობენ შესაბამის ინფორმაციას ან კონტაქტებს; და ეჭვმიტანილებთან ან მსჯავრდებულებთან დაკავშირებული პირები. ეს დებულება არ ზღუდავს ქარტიითა და ადამინის უფლებათა და ძირითად თავისუფლებათა ევროპული კონვენციით გარანტირებული უდანაშაულობის პრეზუმფციის უფლების გამოყენებას, როგორც ის განიმარტება მართლმსჯულების სასამართლოსა და ადამიანის უფლებათა ევროპული სასამართლოს პრაქტიკით.

(32) კომპეტენტურმა ორგანოებმა უნდა უზრუნველყონ, რომ არ მოხდეს არაზუსტი, არასრული ან განუახლებელი პერსონალური მონაცემების გადაცემა ან ისინი არ იყოს ხელმისაწვდომი. ფიზიკური პირების დაცვის, პერსონალურ მონაცემთა სიზუსტის, სრულყოფილების ან განახლებადობის, ასევე გადაცემული ან ხელმისაწვდომი პერსონალური მონაცემების სანდოობის მიზნით, კომპეტენტურმა ორგანოებმა უნდა უზუნველყონ, რამდენადაც ეს შესაძლებელია, რომ მონაცემთა გადაცემისას მიუთითონ აუცილებელი ინფორმაცია.

(33) როდესაც წინამდებარე დირექტივა მიუთითებს წევრი სახელმწიფოს კანონზე, სამართლებრივ საფუძველზე ან საკანონმდებლო ზომაზე, ეს აუცილებლად არ გულისხმობს პარლამენტის მიერ მიღებულ საკანომდებლო აქტს, წევრი სახელმწიფოს კონსტიტუციური წყობილების მოთხოვნების შეუზღუდავად. თუმცა, წევრი სახელმწიფოს კანონი, სამართლებრივი საფუძველი ან საკანონმდებლო ზომა უნდა იყოს მკაფიო და ზუსტი, ხოლო მისი გამოყენების შედეგები განჭვრეტადი, როგორც ამას მოითხოვს მართლმსაჯულების სასამართლოსა და ადამიანის უფლებათა ევროპული სასამართლოს პრაქტიკა. წევრი სახელმწიფოს კანონმდებლობა, რომელიც არეგულირებს პერსონალურ მონაცემთა დამუშავებას წინამდებარე დირექტივის ფარგლებში, სულ მცირე, უნდა შეიცავდეს მიზნებს, დასამუშავებელ პერსონალურ მონაცემებს, დამუშავების მიზნებს და პერსონალურ მონაცემთა მთლიანობისა და კონფიდენციალურობის შენარჩუნებისა და მონაცემთა განადგურების პროცედურებს, რითაც უზუნველყოფილი იქნება საკმარისი გარანტიები უფლების ბოროტად გამოყენებისა და თვითნებობის რისკების თავიდან ასაცილებლად.

(34) კომპეტენტური ორგანოების მიერ პერსონალურ მონაცემთა დამუშავება დანაშაულების პრევენციის, გამოძიების, დადგენის ან სისხლისსამართლებრივი დევნის, ასევე, საზოგადოებრივი უსაფრთხოების წინააღმდეგ მიმართული საფრთხეებისაგან დაცვისა და პრევენციის მიზნით უნდა მოიცავდეს ნებისმიერ ოპერაციას ან ოპერაციათა წყებას, რომელიც დასახელებული მიზნებით ხორციელდება პერსონალურ მონაცემებზე ან პერსონალურ მონაცემთა წყებაზე, როგორც ავტომატური, ისე სხვა საშუალებებით, როგორებიცაა შეგროვება, ჩაწერა, ორგანიზება, სტრუქტურირება, შენახვა, ადაპტირება ან შეცვლა, აღდგენა, გაცნობა, გამოყენება, დაწყობა ან კომბინირება, დაბლოკვა, წაშლა ან განადგურება. წინამდებარე დირექტივის წესები განსაკუთრებულად უნდა გავრცელდეს ამ დირექტივის მიზნებისათვის პერსონალაური მონაცემების ისეთი მიმღებისათვის გადაცემაზე, რომელიც არ არის ამ დირექტივის წევრი. ამგვარ მიმღებად ითვლება ფიზიკური ან იურიდიული პირი, საჯარო უწყება, სააგენტო ან ნებისმიერი სხვა ორგანო, რომელსაც კომპეტენტური ორგანო კანონიერად გადასცემს პერსონალურ მონაცემებს. როდესაც თავდაპირველად პერსონალური მონაცემები კომპეტენტური ორგანოს მიერ შეგროვდა წინამდებარე დირექტივის ერთ-ერთი მიზნისათვის, (EU) 2016/679 რეგულაციის მოქმედება გავრცელდება ამ მონაცემთა ისეთ დამუშავებაზე, რომელიც ხორციელდება წინადებარე დირექტივის მიზნებისაგან განსხვავებული მიზნით თუ ამგვარი დამუშავება ნებადართულია ევროკავშირის ან წევრი სახელმწიფოს კანონმდებლობით. განსაკუთრებით, (EU) 2016/679 რეგულაციის წესები უნდა გავრცელდეს პერსონალურ მონაცემთა გადაცემაზე იმ მიზნებისათვის, რომლებიც სცილდება წინამდებარე დირექტივის მოქმედების ფარგლებს. პერსონალურ მონაცემთა ისეთი მიმღების მიერ დამუშავებაზე, რომელიც არ წარმოადგენს კომპეტენტურ ორგანოს ან მისი მოვალეობების შემსრულებელს წინამდებარე დირექტივის მიზნებისათვის და რომელსაც კომპეტენტური ორგანოს მიერ კანონიერად გადაეცა პერსონალური მონაცემები, გავრცელდება (EU) 2016/679 რეგულაცია. წინამდებარე დირექტივის განხორციელებისას, წევრმა სახელმწიფოებმა დამატებით უნდა განსაზღვრონ (EU) 2016/679 რეგულაციის წესების გამოყენების საკითხი, მასში მოცემული პირობების გათვალისწინებით.

(35) დამუშავების კანონიერებისათვის, წინამდებარე დირექტივის საფუძველზე განხორციელებული დამუშავება აუცილებლი უნდა იყოს კომპეტენტური ორგანოს მიერ საჯარო ინტერესში შემავალი ამოცანების შესასრულებლად ევროკავშირის ან წევრი სახელმწიფოს კანონმდებლობის საფუძველზე დანაშაულების პრევენციის, გამოძიების,

დადგენის ან სისხლისამართლებრივი დევნის, ასევე საზოგადოებრივი უსაფრთხოების წინააღმდეგ მიმართული საფრთხეებისაგან დაცვისა და პრევენციის მიზნით. მითითებული საქმიანობა უნდა მოიცავდეს მონაცემთა სუბიექტის სასიცოცხლო ინტერესების დაცვას. კომპეტენტურ ორგანოებზე კანონით დაკისრებული ამოცანების - დანაშაულების პრევენციის, გამოძიების, დადგენის ან სისხლისამართლებრივი დევნის - შესრულება შესაძლებლობას აძლევს მათ, მოსთხოვონ, ან უბრძანონ ფიზიკურ პირებს, დაემორჩილონ მოთხოვნას. ასეთ შემთხვევაში, მონაცემთა სუბიექტის თანხმობა, როგორც მას განმარტავს (EU) 2016/679 რეგულაცია, არ უნდა წარმოადგენდეს კომპეტენტური ორგანოების მიერ მონაცემთა დამუშავების სამართლებრივ საფუძველს. როდესაც მონაცემთა სუბიექტი ვალდებულია დაემორჩილოს საკანონმდებლო მოთხოვნას, მას არ აქვს ნამდვილი და თავისუფალი არჩევანი. ამდენად, მონაცემთა სუბიექტის პასუხი არ შეიძლება ჩაითვალოს მისი სურვილის თავისუფალ გამოხატვად. ეს არ უკრძალავს წევრ სახელმწიფოებს, კანონმდებლობით განსაზღვრონ, რომ მონაცემთა სუბიექტს შეუძლია გამოხატოს თანხმობა მისი პერსონალური მონაცემების დამუშავებაზე წინამდებარე დირექტივის მიზნებისათვის, როგორიცაა სისხლის სამართლის საქმის გამოძიებისას დნმ ტესტირება ან სასჯელთა აღსრულებისას მისი ადგილმდებაროების მონიტორინგი ელექტრონული მოწყობილობით.

(36) წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ თუ ევროკავშირის ან წევრი სახელმწიფოს კანონმდებლობა, რომელიც ვრცელდება კომპეტენტურ ორგანოზე, ითვალისწინებს პერსონალურ მონაცემთა დამუშვებას კონკრეტული პირობებით და კონკრეტულ გარემოებებში, მაგალითად, ქცევის კოდექსების გამოყენებით, გადამცემმა კომპეტენტურმა ორგანომ უნდა შეატყობინოს ასეთი პერსონალური მონაცემების მიმღებს ამ პირობებისა და მათი დაცვის აუცილებლობის შესახებ. ამგვარი პირობები შეიძლება მოიცავდეს, მაგალითად, პერსონალური მონაცემების სხვა მიმღებისათვის შემდგომი გადაცემის ან მათი გადაცემის მიზნისაგან განსხვავებული მიზნით გამოყენების აკრძალვას, ან მონაცემთა სუბიექტის ინფორმირებას ინფორმაციის მიღების უფლების შეზღუდვის თაობაზე გადამცემი კომპეტენტური ორგანოს წინასწარი თანხმობის გარეშე. მითითებული მოვალეობები ასევე უნდა გვრცელდეს კომპეტენტური ორგანოების მიერ მესამე სახელმწიფოში არსებული მიმღებისათვის ან საერთაშორისო ორგანიზაციისათვის პერსონალურ მონაცემთა გადაცემაზე. წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ გადამცემმა კომპეტენტურმა ორგანომ ხსენებული პირობები არ გაავრცელოს სხვა წევრ

სახელმწიფოში არსებულ მიმღებზე ან “ევროკავშირის ფუნქციონირების შესახებ” ხელშეკრულების V ნაწილის მე-4 და მე-5 თავის საფუძველზე შექმნილ სააგენტოებზე, სამსახურებსა და უწყებებზე, გარდა იმ პირობებისა, რომლებიც ვრცელდება მონაცემთა მსგავს გადაცემაზე იმ კომპეტენტური ორგანოს წევრ სახელმწიფოში.

(37) პერსონალური მონაცემები, რომლებიც თავიანთი ბუნებით განსაკუთრებით სენსიტიურია ფუნამდენტურ უფლებებთან და თავისუფლებებთან მიმართებით, განსაკუთრებულად უნდა იყოს დაცული, ვინაიდან მათი დამუშავების კონტექტსმა შესაძლოა შექმნას ფუნდამენტური უფლებებისა და თავისუფლებების დარღვევის მნიშვნელოვანი საფრთხე. ამგვარ პერსონალურ მონაცემებს უნდა მიეკუთვნებოდეს მონაცემები, რომლებიც უკავშირდება რასობრივ ან ეთნიკურ წარმომავლობას. ამასთან, ტერმინი “რასობრივი წარმომავლობა” არ გულისხმობს, რომ ევროკავშირი იზიარებს თეორიებს, რომლებიც ცდილობენ დაამტკიცონ განსხვავებულობა ადამიანთა რასებს შორის. ამგვარი პერსონალური მონაცემები არ უნდა დამუშავდეს თუ არ არსებობს მონაცემთა სუბიექტის უფლებებისა და თავისუფლებების დაცვის კანონით გათვალისწინებული სათანადო გარანტიები და თუ ეს არ არის ნებადართული კანონით გათვალისწინებულ შემთხვევებში; თუ დამუშავება ჯერ არ არის ნებადართული ამგვარი კანონით, თუმცა დამუშავება აუცილებელია მონაცემთა სუბიექტის ან სხვა პირის სასიცოცხლო ინტერესების დასაცავად; ან დამუშავება უკავშირდება პერსონალურ მონაცემებს, რომლებიც მონაცემთა სუბიექტმა თავად გაასაჯაროვა მათი დამუშავების აშკარა აკრძალვის გარეშე. მონაცემთა სუბიექტის უფლებისა და თავისუფლებების დაცვის სათანადო გარანტიები შესაძლოა მოიცავდეს ამგავრი მონაცემების დამუშავების ნებართვას მხოლოდ ამავე ფიზიკურ პირთან დაკავშირებული სხვა მონაცემების დამუშავებისას, ადეკვატურად შეგროვებული მონაცემების უსაფრთხოების დაცვის შესაძლებლობას, კომპეტენტური ორგანოს თანამშრომლების მონაცემებთან დაშვების გამკაცრებულ წესებსა და მონაცემების გადაცემის აკრძალვას. ასეთი მონაცემების დამუშავება, კანონით, ასევე, დაშვებული უნდა იყოს თუ მონაცემთა სუბიექტმა აშკარა თანხმობა განაცხადა ისეთ დამუშავებაზე, რომელიც განსაკუთრებულად ზღუდავს მის უფლებებს. თუმცა, მონაცემთა სუბიექტის თანხმობა თავისთავად არ უნდა ქმნიდეს ასეთი სენსიტიური პერსონალური მონაცემების კომპეტენტური ორგანოების მიერ დამუშავების სამართლებრივ საფუძველს.

(38) მონაცემთა სუბიექტს უნდა ჰქონდეს უფლება, არ დაექვემდებაროს ისეთ გადაწყვეტილებას, რომელიც აფასებს მასთან დაკავშირებულ პერსონალურ ასპექტებს და რომელიც ეფუძნება მხოლოდ ავტომატურ დამუშავებას და რომელიც მონაცემთა სუბიექტისათვის წარმოშობს უარყოფით სამართლებრივ შედეგებს ან მნიშვნელოვან გავლენას ახდენს მასზე. ნებისმიერ შემთხვევაში ასეთი დამუშავება უნდა განხორციელდეს დაცვის შესაბამისი გარანტიებით, მათ შორის მონაცემთა სუბიექტისათვის კონკრეტული ინფორმაციის მიწოდებით და ადამიანური რესურსის ჩართვის მოთხოვნის უფლებით, ასევე, მისი აზრის გამოხატვის, ამგვარი შეფასების შედეგად მიღებული გადაწყვეტილების მიზეზების მოთხოვნისა და გადაწყვეტილების გასაჩივრების უფლებით. ქარტიის 21-ე და 52-ე მუხლებით დადგენილი პირობების თანახმად, იკრძალება პროფილირება, რომელიც იწვევს ფიზიკური პირების დისკრიმინაციას იმ პერსონალური მონაცემების საფუძველზე, რომლებიც თავიანთი ხასიათით განსაკუთრებით სენსიტიურია ფუნდამენტურ უფლებებსა და თავისუფლებებთან მიმართებაში.

(39) იმისათვის, რომ მონაცემთა სუბიექტმა შეძლოს თავისი უფლებების განხორციელება, ნებისმიერი ინფორმაცია, რომელიც მას მიეწოდება უნდა იყოს მარტივად ხელმისაწვდომი, მათ შორის დამმუშავებლის ვებ-გვერდზე და მარტივად აღსაქმელი, შესრულებული გასაგებ და მარტივ ენაზე. ასეთი ინფორმაცია მორგებული უნდა იყოს მოწყვლადი პირების, მაგალითად, ბავშვების საჭიროებებზე.

(40) უნდა შეიქმნას მექანიზმები, მათ შორის პერსონალურ მონაცემთა გამოთხოვის, ასევე, უფასოდ წვდომის, გასწორების, წაშლის ან მონაცემთა დაბლოკვის მექანიზმები, რომლებიც ხელს შეუწყობენ წინამდებარე დირექტივის საფუძველზე მიღებული დებულებებით გათვალისწინებული მონაცემთა სუბიექტის უფლებების განხორციელებას. დამმუშავებელი ვალდებულია, დაუყოვნებლივ უპასუხოს მონაცემთა სუბიექტის თხოვნას გარდა იმ შემთხვევისა, როდესაც დამმუშავებელი წინამდებარე დირექტივის შესაბამისად ზღუდავს მონაცემთა სუბიექტის უფლებებს. მეტიც, თუ მოთხოვნა აშკარად უსაფუძვლო ან გადაჭარბებულია, მაგალითად, როდესაც მონაცემთა სუბიექტი არაგონივრულად და განმეორებით ითხოვს ინფორმაციას ან როდესაც მონაცემთა სუბიექტი თავად ვნებს საკუთარ უფლებას ინფორმაციის მიღებაზე, მაგალითად, მცდარი ან შეცდომაში შემყვანი ინფორმაციის წარდგენით, დამმუშავებელს უნდა ჰქონდეს შესაძლებლობა, დააწესოს გონივრული საფასური ან უარი თქვას თხოვნის შესრულებაზე.

(41) როდესაც დამმუშავებელი მოითხოვს მონაცემთა სუბიექტის იდენტიფიცირებისათვის აუცილებელ დამატებით ინფორმაციას, ეს ინფორმაცია უნდა დამუშავდეს მხოლოდ ამ კონკრეტული მიზნისათვის და არ უნდა იქნეს შენახული უფრო მეტი ხნით, ვიდრე ეს საჭიროა აღნიშნული მიზნის მისაღწევად.

(42) მონაცემთა სუბიექტს უნდა მიეწოდოს, სულ მცირე, შემდეგი ინფორმაცია: დამმუშავებლის ვინაობა, დამუშავების მიმდინარეობა, დამუშავების მიზნები, საჩივრის წარდგენის უფლება და დამმუშავებლისაგან მონაცემებთან წვდომის, მათი შესწორების, წაშლის ან დაბლოკვის მოთხოვნის უფლების არსებობა. ეს ინფორმაცია შესაძლოა მიწოდებულ იქნეს კომპეტენტური ორგანოს ვებ-გვერდზე. დამატებით და კონკრეტულ შემთხვევებში უფლებების განხორციელების ხელშეწყობის მიზნით მონაცემთა სუბიექტს უნდა ეცნობოს დამუშავების სამართლებრივი საფუძვლისა და მონაცემების შენახვის ვადის შესახებ, თუ ამგვარი დამატებითი ინფორმაციის მიწოდება მონაცემთა დამუშავების კონკრეტული გარემოებების გათვალისწინებით, აუცილებელია მონაცემთა სუბიექტის მიმართ სამართლიანი დამუშავების უზრუნველსაყოფად.

(43) ფიზიკურ პირს უნდა ჰქონდეს მასთან დაკავშირებით შეგროვებულ მონაცემებთან წვდომის უფლება და ამ უფლების მარტივად და გონივრული ინტერვალებით განხორციელების შესაძლებლობა, იმისათვის, რომ ჰქონდეს ინფორმაცია დამუშავების შესახებ და შეამოწმოს მისი კანონიერება. შესაბამისად, თითოეულ მონაცემთა სუბიექტს უნდა ჰქონდეს უფლება, იცოდეს და მოიპოვოს ინფორმაცია, მონაცემთა დამუშავების მიზნების, დამუშავების ვადის და მონაცემთა მიმღების, მათ შორის მესამე სახელმწიფოში არსებული მიმღების, შესახებ. როდესაც ასეთი კომუნიკაცია მოიცავს ინფორმაციას მონაცემთა წარმომავლობის შესახებ, ამგვარმა ინფორმაციამ არ უნდა გაამჟღავნოს ფიზიკური პირების, განსაკუთრებით კონფიდენციალური წყაროების, ვინაობა. ამ უფლების განხორციელებისათვის საკმარისია, მონაცემთა სუბიექტს ჰქონდეს ამ მონაცემების სრული ჩამონათვალი წაკითხვად ფორმატში, ანუ სხვაგვარად, იმგვარ ფორმატში, რომელიც საშუალებას მისცემს მონაცემთა სუბიექტს, ჰქონდეს ინფორმაცია ამ მონაცემების შესახებ, გადაამოწმოს მათი სიზუსტე და წინამდებარე დირექტივის შესაბამისად დამუშავება წინამდებარე დირექტივით მისთვის მინიჭებული უფლებების

განსახორციელებლად. ასეთი ჩამონათვალი შესაძლოა წარდგენილ იყოს დამუშავებული მონაცემების ასლის სახით.

(44) წევრ სახელმწიფოებს უნდა შეეძლოთ იმგვარი საკანონმდებლო ზომების მიღება, რომლებიც შეაფერხებენ, შეზღუდავენ ან გამორიცხავენ მონაცემთა სუბიექტისათვის ინფორმაციის გადაცემას, ან მთლიანად ან ნაწილობრივ შეზღუდავენ მათ უფლებას მონაცემებთან წვდომაზე იმ მოცულობით, რამდენადაც ეს აუცილებელი და პროპორციულია დემოკრატიულ საზოგადოებაში, ფიზიკური პირების ფუნდამენტური უფლებისა და ლეგიტიმური ინტერესების სათანადოდ დაცვით, სამართლებრივი მოკვლევის, გამოძიების ან პროცედურებისათვის ხელის შეშლის თავიდან ასაცილებლად, დანაშაულების პრევენციის, გამოძიების, დადგენის ან სისხლისსამართლებრივი დევნის ან სასჯელების აღსრულების, ასევე, საზოგადოებრივი უსაფრთხოების წინააღმდეგ მიმართული საფრთხეებისაგან დაცვისა და პრევენციის შეფერხების თავიდან ასაცილებლად და სხვათა უფლებებისა და თავისუფლებების დასაცავად. დამმუშავებელმა კონკრეტული და ინდივიდუალური განხილვის წესით უნდა შეაფასოს თითოეული შემთხვევა, როდესაც მონაცემებთან წვდომის უფლება მთლიანად თუ ნაწილობრივ უნდა შეიზღუდოს.

(45) მონაცემთა სუბიექტს წერილობით უნდა განემარტოს მონაცემებთან ან ინფორმაციასთან წვდომაზე უარის ან ამ უფლების შეზღუდვის მიზეზი და მიღებული გადაწყვეტილების ფაქტორობივი და სამართლებრივი საფუძვლები.

(46) მონაცემთა სუბიექტის უფლებების ნებისმიერი შეზღუდვა უნდა შეესაბამებოდეს ქარტიასა და ადამიანის უფლებათა და ძირითად თავისუფლებათა ევროპულ კონვენციას, როგორც ეს არის განმარტებული მართლმსაჯულების სასამართლოსა და ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილებებში და განსაკუთრებით უნდა იყოს დაცული ამ უფლებებისა და თავისფლებების არსი.

(47) ფიზიკურ პირს უნდა ჰქონდეს უფლება, მოითხოვოს მასთან დაკავშირებული არაზუსტი პერსონალური მონაცემების გასწორება, განაკუთრებით, როდესაც ისინი ფაქტებს უკავშირდება და მონაცემთა წაშლის მოთხოვნის უფლება, როდესაც დამუშავება ეწინააღმდეგება წინამდებარე დირექტივას. თუმცა, მონაცემთა გასწორების უფლებამ

უარყოფითი გავლენა არ უნდა მოახდინოს, მაგალითად, მოწმის ჩვენების შინაარსზე. ფიზიკურ პირს ასევე უნდა ჰქონდეს უფლება, მოითხოვოს მონაცემთა დაბლოკვა, როდესაც ის სადავოდ ხდის მონაცემთა სიზუსტეს და მათი სიზუსტის დადგენა შეუძლებელია, ან როდესაც მონაცემთა შენახვა უნდა მოხდეს მტკიცებულებითი მიზნისათვის. პერსონალურ მონაცემთა წაშლის ნაცვლად მონაცემები უნდა დაიბლოკოს იმ განსაკუთრებულ შემთხვევაში, თუ არსებობს გონივრული ვარაუდი, რომ მათმა წაშლამ შესაძლოა უარყოფითი გავლენა მოახდინოს მონაცემთა სუბიექტის ლეგიტიმურ ინტერესებზე. ასეთ შემთხვევაში დაბლოკილი მონაცემები უნდა დამუშავდეს მხოლოდ იმ მიზნისთვის, რომლის გამოც არ მოხდა მათი წაშლა. პერსონალურ მონაცემთა დაბლოკვის მეთოდები შეიძლება მოიცავდეს, მათ შორის, შერჩეული მონაცემების სხვა დამუშავების სისტემაში გადატანას, მაგალითად, არქივირების მიზნებისათვის ან შერჩეულ მონაცემებთან წვდომის დაბლოკვას. ავტომატურ ფაილურ სისტემებში მონაცემების დაბლოკვის უზრუნველყოფა პრინციპში, უნდა მოხდეს ტექნიკური საშუალებებით. პერსონალურ მონაცემთა დაბლოკვის ფაქტი ფაილურ სისტემაში იმგვარად უნდა აღინიშნოს, რომ ცხადი გახდეს მათი დამუშავების შეზღუდვის ფაქტი. პერსონალურ მონაცემთა ამგვარი გასწორება ან წაშლა, ან მათი დაბლოკვა უნდა ეცნობოს მიმღებს, რომელსაც გადაეცა მონაცემები და იმ კომპეტენტურ ორგანოებს, რომლებისგანაც მოხდა არაზუსტი მონაცემების მოპოვება. ამასთან, დამმუშავებლემა თავი უნდა შეიკავონ ამგვარი მონაცემების შემდგომი გავრცელებისაგან.

(48) როდესაც დამმუშავებელი ზღუდავს მონაცემთა სუბეიქტის უფლებას ინფორმაციის მიღებაზე, მონაცემებთან წვდომაზე, გასწორებაზე, წაშლაზე ან მათ დაბლოკვაზე, მონაცემთა სუბიექტს უნდა ჰქონდეს უფლება, სთხოვოს ეროვნულ საზედამხედველო ორგანოს დამუშავების კანონიერების შემოწმება. მონაცემთა სუბიექტს უნდა ეცნობოს აღნიშნული უფლების შესახებ. როდესაც საზედამხედველო ორგანო მოქმედებს მონაცემთა სუბიექტის სახელით, მან მონაცემთა სუბიექტს უნდა აცნობოს, სულ მცირე ის, რომ ჩატარდა ყველა აუცილებელი შემოწმება ან განხილვა საზედამხედველო ორგანოს მიერ. ასევე, საზედამხედველო ორგანომ უნდა აცნობოს მონაცემთა სუბიექტს სასამართლოსათვის მიმართვის უფლების შესახებ.

(49) როდესაც პერსონალური მონაცემები მუშავდება სისხლის სამართლის საქმის გამოძიების ან სასამართლო განხილვის პროცესში, წევრმა სახელმწიფოებმა უნდა

უზუნრველყონ, რომ ინფორმაციის მოპოვების, მონაცემებთან წვდომის, გასწორების წაშლის ან დაბლოკვის უფლების განხორციელება მოხდეს ეროვნული საპროცესო კანონმდებლობის წესების შესაბამისად.

(50) უნდა განისაზღვროს დამმუშავებლის ვალდებულება და პასუხისმგებლობა დამმუშავებლის მიერ ან მისი სახელით პერსონალურ მონაცემთა ნებისმიერ დამუშავებაზე. კერძოდ, დამმუშავებელს უნდა დაევალოს სათანადო და ეფექტური ზომების მიღება და უნდა შეეძლოს დამუშავების წინამდებარე დირექტივასთან შესაბამისობის დემონსტრირება. ასეთი ზომები უნდა ითვალისწინებდეს დამუშავების ხასიათს, მოცულობას, კონტექსტსა და მიზნებს, ფიზიკური პირების უფლებებისა და თავისუფლებების დარღვევის რისკებს. დამმუშავებლის მიერ მიღებული ზომები უნდა მოიცავდეს მოწყვლად პირებთან, როგორებიც არიან ბავშვები, დაკავშირებული პერსონალური მონაცემების დამუშავებისას განსაკუთრებული დაცვის გარანტიების შემუშავებასა და განხორციელებას.

(51) მონაცემთა დამუშავებას, რომელმაც შეიძლება გამოიწვიოს ფიზიკური, მატერიალური ან არამატერიალური ზიანი, შესაძლოა მოჰყვეს ფიზიკური პირების უფლებებისა და თავისუფლებების სხვადასხვა ალბათობისა და სიმძიმის დარღვევა, განსაკუთრებით იმ შემთხვევაში, როდესაც მონაცემთა დამუშავებას შესაძლოა მოჰყვეს დისკრიმინაცია, ვინაობის მოპარვა ან თაღლითობა, ფინანსური დანაკარგი, რეპუტაციული ზიანი, პროფესიული უწყების მიერ დაცული პერსონალური მონაცემების კონფიდენციალურობის დარღვევა, ფსევდონიმიზირებული მონაცემების პირვანდელ მდგომარობაში უკანონო დაბრუნება ან ნებისმიერი სხვა მნიშვნელოვანი ეკონომიკური ან საზოგადოებრივი ზიანი; როდესაც მონაცემთა სუბიექტებს შესაძლოა ჩამოერთვათ მათი უფლებები ან თავისუფლებები ან პერსონალურ მონაცემებზე კონტროლის განხორციელების უფლება; როდესაც მუშავდება ისეთი პერსონალური მონაცემები, რომლებიც უკავშირდება რასობრივ ან ეთნიკურ წარმომავლობას, პოლიტიკურ შეხედულებებს, რელიგიურ ან ფილოსოფიურ მრწამსს ან პროფესიული კავშირის წევრობას; როდესაც პირის უნიკალურად იდენტიფიცირებისათვის მუშავდება გენეტიკური ან ბიომეტრიული მონაცემები; ან როდესაც მუშავდება ჯანმრთელობასთან, სქესობრივ ცხოვრებასთან ან სექსუალურ ორიენტაციასთან დაკავშირებული მონაცემები, ან მსჯავრდებასთან და დანაშაულთან, ან აღკვეთის ღონისძიებასთან დაკავშირებული მონაცემები; როდესაც

ფასდება პერსონალური ასპექტები, განსაკუთრებით, შრომის უნარებთან, ეკონომიკურ მდგომარეობასთან, ჯანმრთელობასთან, პიროვნულ უპირატესობებთან ან ინტერესებთან, სანდოობასა და ყოფაქცევასთან, ადგილმდებარეობასთან ან გადაადგილებასთან დაკავშირებული მონაცემების ანალიზი და განჭვრეტა პირადი პროფილების შექმნის ან გამოყენების მიზნით; როდესაც მუშავდება მოწყვლადი პირების, განსაკუთრებით ბავშვების პერსონალური მონაცემები; ან როდესაც მუშავდება დიდი მოცულობით პერსონალური მონაცემები და ეს გავლენას ახდენს დიდი რაოდენობით მონაცემთა სუბიექტებზე.

(52) რისკის ალბათობა და სიმძიმე უნდა დადგინდეს დამუშავების ხასიათის, მოცულობის, კონტექსტისა და მიზნების გათვალისწინებით. რისკის შეფასება უნდა მოხდეს ობიექტური შეფასების საფუძველზე, რომელიც დაადგენს, მოიაზრებს თუ არა მონაცემთა დამუშავების ოპერაციები მაღალ რისკს. მაღალი რისკი ნიშნავს მონაცემთა სუბიქტების უფლებებისა და თავისუფლებების დარღვევის კონკრეტულ რისკს.

(53) პერსონალური მონაცემების დამუშავებისას ფიზიკური პირების უფლებებისა და თავისუფლებების დაცვა საჭიროებს სათანადო ტექნიკური და ორგანიზაციული ზომების მიღებას, რათა უზრუნველყოფილი იყოს წინამდებარე დირექტივის მოთხოვნების შესრულება. ამგვარი ზომების განხორციელება არ უნდა იყოს დამოკიდებული მხოლოდ ეკონომიკურ ფაქტორებზე. წინამდებარე დირექტივასთან შესაბამისობის დემონსტრირებისათვის დამმუშავებელმა უნდა შეიმუშაოს შიდა პოლიტიკის დოკუმენტი და მიიღოს ზომები, რომლებიც განსაკუთრებულად იცავს ახალი პროდუქტის ან მომსახურების შექმნისას მონაცემთა დაცვის სტანდარტების გათვალისწინების პრინციპსა და პირველად პარამეტრად მონაცემთა დაცვის პრინციპს. როდესაც მონაცემთა დამმუშავებელს ჩატარებული აქვს მონაცემთა დაცვის ზეგავლენის შეფასება წინამდებარე დირექტივის შესაბამისად, მიღებული შედეგები მხედველობაში უნდა იქნეს მიღებული ხსენებული ზომებისა და პროცედურების შემუშავებისას. ეს ზომები შესაძლოა, მათ შორის, მოიცავდეს ფსევდონიმიზაციის გამოყენებას შეძლებისდაგვარად ადრეულ ეტაპზე. წინამდებარე დირექტივის მიზნებისათვის ფსევდონიმიზაცია შესაძლოა გამოყენებულ იქნეს როგორც საშუალება, რომელიც ხელს შეუწყობს თავისუფლების, უსაფრთხოებისა და მართლმსაჯულების სფეროში პერსონალურ მონაცემთა თავისუფალ გადადინებას.

(54) მონაცემთა სუბიექტების უფლებების დაცვა, ისევე როგორც დამმუშავებლისა და უფლებამოსილი პირების ვალდებულებები და პასუხისმგებლობა, ასევე, საზედამხედველო ორგანოების მიერ მონიტორინგის განხორციელება და ზომების მიღება საჭიროებს წინამდებარე დირექტივით გათვალისწინებული პასუხისმგებლობების მკაფიო განსაზღვრას, მათ შორის, როდესაც დამმუშავებელი დამუშავების მიზნებსა და საშუალებებს სხვა დამმუშავებლებთან ერთად განსაზღვრავს ან როდესაც მონაცემები დამმუშავებლის სახელით მუშავდება.

(55) უფლებამოსილი პირის მიერ მონაცემთა დამუშავება უნდა რეგულირდებოდეს სამართლებრივი აქტით, მათ შორის ხელშეკრულებით, რომელიც ბოჭავს უფლებამოსილ პირს დამმუშავებლის წინაშე და ითვალისწინებს მხოლოდ დამმუშავებლისაგან მიღებული მითითებების საფუძველზე მოქმედებას. უფლებამოსილმა პირმა მხედველობაში უნდა მიიღოს ახალი პროდუქტის ან მომსახურების შექმნისას მონაცემთა დაცვის სტანდარტების გათვალისწინების პრინციპი და პირველად პარამეტრად მონაცემთა დაცვის პრინციპი.

(56) წინამდებარე დირექტივასთან შესაბამისობის დემონსტრირებისათვის დამმუშავებელმა ან უფლებამოსილმა პირმა უნდა აღრიცხოს მისი პასუხისმგებლობის ქვეშ არსებული ყველა კატეგორიის დამუშავების ოპერაციები. თითოეული დამმუშავებელი და უფლებამოსილი პირი ვალდებული უნდა იყოს, ითანამშრომლოს საზედამხედველო ორგანოსთან და მოთხოვნისამებრ მიაწოდოს აღრიცხული ჩანაწერები დამუშავების ოპერაციების მონიტორინგის მიზნით. დამმუშავებელს ან უფლებამოსილ პირს, რომლებიც მონაცემებს ამუშავებენ არაავტომატური დამუშავების სისტემებში შემუშავებული უნდა ჰქონდეთ დამუშავების კანონიერების დემონსტრირების, თვითმონიტორინგისა და მონაცემთა მთლიანობისა და უსაფრთხოების დემონსტრირების ისეთი ეფექტური მეთოდები, როგორიცაა ლოგირება ან აღრიცხვის სხვა ფორმები.

(57) ლოგები შენახულ უნდა იქნეს ავტომატური დამუშავების სისტემებში განხორციელებული სულ მცირე ისეთი დამუშავების ოპერაციებისათვის, როგორებიცაა, მონაცემთა შეგროვება, შეცვლა, გაცნობა და გამჟღავნება, მათ შორის გადაცემა, კომბინირება ან წაშლა. უნდა მოხდეს იმ ადამიანების ვინაობის ლოგირება, რომლებიც გაეცნენ ან გაამჟღავნეს მონაცემები და ვინაობის მონაცემებიდან შესაძლებელი უნდა იყოს

დამუშავების საფუძვლის დადგენა. ლოგების გამოყენება უნდა მოხდეს მხოლოდ დამუშავების კანონიერების შემოწმების, თვით-მონიტორინგის, მონაცემთა მთლიანობისა და უსაფრთხოების უზრუნველსაყოფად და სისხლის სამართლოს საქმეების წარმოებისათვის. თვითმონიტორინგი, ასევე, გულისხმობს კომპეტენტური ორგანოების შიდა დისციპლინურ პროცედურებს.

(58) დამმუშავებლის მიერ უნდა განხორციელდეს მონაცემთა დაცვის ზეგავლენის შეფასება როდესაც დამუშავების ოპერაციები მათი ხასიათის, მოცულობისა და მიზნების გათვალისწინებით დიდი ალბათობით გამოიწვევს მონაცემთა სუბიექტების უფლებებისა და თავისუფლებების დარღვევის მაღალ რისკს. ზეგავლენის შეფასება უნდა მოიცავდეს ზომებს, დაცვის გარანტიებსა და მექანიზმებს, რომლებიც გამიზნულია პერსონალურ მონაცემთა დასაცავად და წინამდებარე დირექტივასთან შესაბამისობის დემონსტრირებისათვის. ზეგავლენის შეფასებამ უნდა მოიცვას დამუშავების ოპერაციების შესაბამისი სისტემები და პროცესები და არა ინდივიდულური შემთხვევები.

(59) მონაცემთა სუბიექტების უფლებებისა და თავისუფლებების ეფექტური დაცვის უზრუნველსაყოფად დამმუშავებელმა ან უფლებამოსილმა პირმა კონკრეტულ შემთხვევებში დამუშავების დაწყებამდე უნდა გაიაროს კონსულტაცია საზედამხედველო ორგანოსთან.

(60) უსაფრთხოების უზრუნველსაყოფად და წინამდებარე დირექტივის დარღვევით განხორციელებული დამუშავების თავიდან ასაცილებლად დამმუშავებელმა ან უფლებამოსილმა პირმა უნდა შეაფასონ რისკები, რომლებიც თან ახლავს დამუშავებას და ამ რისკების შესამცირებლად მიიღონ ზომები, როგორიცაა დაშიფრვა. ასეთი ზომები უნდა უზუნველყოფდნენ უსაფრთხოების სათანადო სტანდარტს, მათ შორის, კონფიდენციალურობას და ითვალისწინებდნენ არსებულ ვითარებას, იმპლემენტაციის ხარჯებს რისკებთან და დასაცავი პერსონალური მონაცემების ხასიათთან მიმართებით. მონაცემთა უსაფრთხოების რისკების შეფასებისას მხედველობაში უნდა იქნეს მიღებული ის რისკები, რომლებიც ახლავს მონაცემთა დამუშვებას, როგორებიცაა შემთხვევითი ან უკანონო განადგურება, დაკარგვა, შეცვლა ან უკანონო გამჟღავნება ან გადაცემულ, შენახულ ან სხვაგვარად დამუშავებულ პერსონალურ მონაცემებთან უკანონო წვდომა, რამაც თავის მხრივ შესაძლოა გამოიწვიოს ფიზიკური, მატერიალური ან არამატერიალური

ზიანი. დამმუშავებელმა და უფლებამოსილმა პირმა უნდა უზრუნველყონ, რომ პერსონალურ მონაცემთა დამუშავება არ ხორციელდებოდეს არაუფლებამოსილი პირის მიერ.

(61) პერსონალურ მონაცემთა უსაფრთხოების ინციდენტმა, თუ მასზე რეაგირება არ მოხდა სათანადოდ და დროულად, შესაძლოა გამოიწვიოს ფიზიკური პირებისათვის ფიზიკური, მატერიალური ან არამატერიალური ზიანის მიყენება, როგორიცაა მათ პერონალურ მონაცემებზე კონტროლის დაკარგვა, ან მათი უფლებების შეზღუდვა, დისკრიმინაცია, ვინაობის მოპარვა ან თაღლითობა, ფინანსური დანაკარგი, ფსევდონომიზირებული მონაცემების პირვანდელ მდგომარეობაში უნებართვო დაბრუნება, რეპუტაციული ზიანი, პროფესიული საიდუმლოებით დაცული პერსონალური მონაცემების კონფიდენციალურობის დარღვევა, ან სხვა მნიშვნელოვანი ეკონომიკური ან სოციალური უაყოფითი შედეგი. ამდენად, როგორც კი დამმუშავებლისათვის ცნობილი გახდება პერსონალურ მონაცემთა უსაფრთხოების ინციდენტის შესახებ, დამმუშავებელმა დაუყოვნებლივ, ხოლო შესაძლებლობის შემთხვევაში - ინციდენტის დადგენიდან არაუგვიანს 72 საათისა, უნდა შეატყობინოს ინციდენტის შესახებ საზედამხედველო ორგანოს, გარდა იმ შემთხვევისა, როდესაც დამმუშავებელს შეუძლია ანგარიშვალდებულების პრინციპის შესაბამისად დაამტკიცოს, რომ პერსონალურ მონაცემთა უსაფრთხოების ინციდენტი დიდი ალბათობით არ გამოიწვევს ფიზიკური პირების უფლებებისა და თავისუფლებების დაღვევის რისკს. თუ ამგვარი შეტყობინების გაგზავნა 72 საათის განმავლობაში შეუძლებელია, შეტყობინებას უნდა ახლდეს დაგვიანების მიზეზები და ინფორმაციის მიწოდება დასაშვებია ეტაპობრივად შემდგომი დაყოვნების გარეშე.

(62) ფიზიკურ პირებს დაუყოვნებლივ უნდა ეცნობოთ იმ შემთხვევების შესახებ, როდესაც პერსონალურ მონაცემთა უსაფრთხოების ინციდენტი დიდი ალბათობით გამოიწვევს ფიზიკური პირების უფლებებისა და თავისუფლებების დარღვევის მაღალ რისკს იმისათვის, რომ მათ სათანადო ზომების მიღების შესაძლებლობა მიეცეთ. მიწოდებული ინფორმაცია უნდა აღწერდეს პერსონალურ მონაცემთა უსაფრთხოების ინციდენტის ხასიათს და შეიცავდეს რეკომენდაციას ფიზიკური პირებისათვის შესაძლო უარყოფითი შედეგების შესამცირებლად. მონაცემთა სუბიექტებს ინფორმაცია უნდა მიეწოდოთ როგორც კი ეს გონივრულად შესაძლებელი იქნება, საზედამხედველო ორგანოსთან

მჭიდრო თანამშრომლობის ფარგლებში და ამ უკანასკნელის ან სხვა შესაბამისი ორგანოს მიერ მიცემული მითითებების დაცვით. მაგალითად, ზიანის მყისიერი რისკის შემცირება საჭიროებს მონაცემთა სუბიექტისათვის სწრაფად შეტყობინებას, თუმცა, საჭირო ზომების გატარება იმავე ინციდენტის გაგრძელების ან მსგავსი ინციდენტის წინააღმდეგ ამართლებს შეტყობინების დაყოვნებას. როდესაც სამსახურებრივი ან სამართლებრივი მოკვლევის, გამოძიების ან პროცედურებისათვის ხელის შეშლის თავიდან აცილება, დანაშაულების პრევენციის, გამოძიების, დადგენის ან სისხლისსამართლებრივი დევნის ან სისხლის სამართლის სასჯელების აღსრულების, ასევე, საზოგადოებრივი უსაფრთხოების წინააღმდეგ მიმართული საფრთხეებისაგან დაცვისა და პრევენციისათვის ხელის შეშლის თავიდან აცილება, ან სხვათა უფლებებისა და თავისუფლებების დაცვა შეუძლებელია ფიზიკური პირებისათვის პერსონალურ მონაცემთა უსაფრთხოების ინციდენტის შესახებ შეტყობინების დაყოვნების ან შეზღუდვის გარეშე, ასეთი შეტყობინება, შესაძლოა, გამონაკლის შემთხვევებში, არ განხორციელდეს.

(63) დამმუშავებელმა უნდა დანიშნოს პირი, რომელიც მას დახმარებას გაუწევს წინამდებარე დირექტივის საფუძველზე მიღებულ დებულებებთან შესაბამისობის შიდა მონიტორინგში, გარდა იმ შემთხვევისა, როდესაც წევრი სახელმწიფო გადაწყვეტს, რომ პასუხისმგებლობისაგან გაათავისუფლოს სასამართლოები და მართლმასჯულების სხვა ორგანოები, როდესაც ისინი მოქმედებენ სასამართლო უფლებამოსილების ფარგლებში. მითითებული პირი შესაძლოა იყოს დამმუშავებელთან დასაქმებული მუშაკი, რომელმაც გაიარა სპეციალური გადამზადება პერსონალურ მონაცემთა დაცვის კანონმდებლობასა და პრაქტიკაში ამ სფეროში საექსპერტო ცოდნის მისაღებად. საექსპერტო ცოდნის საჭირო დონის დადგენა უნდა განხორციელდეს მონაცემთა დამუშავების ოპერაციებისა და დამმუშავებლის მიერ დამუშავებული პერსონალური მონაცემებისათვის საჭირო დაცვის გათვალისწინებით. მისი ამოცანები შესაძლოა შესრულდეს როგორც ნახევარ ისე სრულ განაკვეთზე. მონაცემთა რამდენიმე დამმუშავებელს შეუძლია დანიშნოს ერთი მონაცემთა დაცვის ოფიცერი მათი ორგანიზაციული სტრუქტურისა და ზომის გათვალისწინებით, მაგალითად, ცენტრალური ქვედანაყოფების მიერ საერთო რესურსების გამოყენების შემთხვევაში. ხსენებული პირი შესაძლოა, ასევე, დაინიშნოს სხვა პოზიციებზე შესაბამისი დამმუშავებლის სისტემის შემადგენლობაში. ოფიცერი უნდა დაეხმაროს დამმუშავებელსა და დასაქმებულებს, რომლებიც ამუშავებენ მონაცემებს, მონაცემთა დაცვის ვალდებულებებთან შესაბამისობის შესახებ მათი ინფორმირებისა და მათთვის

კონსულტაციის გაწევის გზით. მონაცემთა დაცვის ოფიცრებს უნდა შეეძლოთ მათი მოვალეობებისა და ამოცანების დამოუკიდებლად შესრულება წევრი სახელმწიფოს კანონმდებლობის შესაბამისად.

(64) წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ მონაცემთა მესამე სახელმწიფოში ან საერთაშორისო ორგანიზაციაში გადაგზავნა განხორციელდეს მხოლოდ მაშინ, როდესაც ეს აუცილებელია დანაშაულების პრევენციის, გამოძიების, დადგენის, სისხლისსამართლებრივი დევნის ან სასჯელების აღსრულების მიზნით, ასევე ევროკავშირის ტერიტორიაზე საზოგადოებრივი უსაფრთხოების წინააღმდეგ მიმართული საფრთხეებისაგან დაცვისა და პრევენციის მიზნით და როდესაც მესამე სახელმწიფოში არსებული მონაცემთა დამმუშავებელი ან საერთაშორისო ორგანიზაცია კომპეტენტური ორგანოა წინამდებარე დირექტივის მიზნებისათვის. მონაცემთა გადაცემა უნდა განხორციელდეს მხოლოდ კომპეტენტური ორგანოების მიერ, რომლებიც მოქმედებენ როგორც დამმუშავებლები, გარდა იმ შემთხვევისა, როდესაც უფლებამოსილ პირებს აქვთ მკაფიო მითითება, გადასცენ მონაცემები დამმუშავებლების სახელით. ასეთი გადაცემა შესაძლოა განხორციელდეს, როდესაც კომისია გადაწყვეტს, რომ მესამე სახელმწიფო ან საერთაშორისო ორგანიზაცია უზრუნველყოფს დაცვის ადეკვატურ სტანდარტს, ან როდესაც წარმოდგენილია დაცვის სათანადო გარანტიები ან როდესაც არსებობს საგამონაკლისო წესი კონკრეტული შემთხვევებისათვის. როდესაც პერსონალური მონაცემების გადაცემა ხორციელდება ევროკავშირიდან მესამე სახელმწიფოში არსებული დამმუშავებლების, უფლებამოსილი პირების ან სხვა მიმღებისათვის ან საერთაშორისო ორგანიზაციისათვის, ფიზიკური პირების წინამდებარე დირექტივით გარანტირებულ დაცვის სტანდარტს საფრთხე არ უნდა შეექმნას, მათ შორის მესამე სახელმწიფოდან ან საერთაშორისო ორგანიზაციიდან იმავე ან სხვა მესამე სახელმწიფოში არსებული დამმუშავებლის ან უფლებამოსილი პირისათვის ან საერთაშორისო ორგანიზაციისათვის პერსონალურ მონაცემთა შემდგომი გადაცემისას.

(65) როდესაც პერსონალურ მონაცემთა გადაცემა ხდება წევრი სახელმწიფოდან მესამე სახელმწიფოში ან საერთაშორისო ორგანიზაციაში, ასეთი გადაცემა უნდა განხორციელდეს მხოლოდ მას შემდეგ, რაც წევრი სახელმწიფო რომლისგანაც მოხდა მონაცემთა მოპოვება, გასცემს ნებართვას გადაცემაზე. სამართალდამცავ ორგანოებს შორის ეფექტიანი თანამშრომლობის ინტერესები საჭიროებს, რომ

კომპეტენტურ ორგანოს შეეძლოს შესაბამისი პერსონალური მონაცემების გადაცემა მესამე სახელმწიფოს ან საერთაშორისო ორგანიზაციისათვის ამგვარი წინასწარი ნებართვის გარეშე, როდესაც წევრი სახელმწიფოს საზოგადოებრივი უსაფრთხოების ან წევრი სახელმწიფოს ძირითადი ინტერესების წინააღმდეგ მიმართული საფრთხის ხასიათი იმგვარია, რომ შეუძლებელია წინასწარი ნებართვის მოპოვება. წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ გადაცემასთან დაკავშირებული ნებისმიერი სპეციალური პირობის შესახებ ეცნობოთ მესამე სახელმწიფოებს ან საერთაშორიო ორგანიზაციებს. პერსონალური მონაცემების შემდგომ გადაცემაზე წინასწარი ნებართვა უნდა გაიცეს იმ კომპეტენტური ორგანოს მიერ, რომელმაც განახორციელა თავდაპირველი გადაცემა. მონაცემთა შემდგომი გადაცემის შესახებ თხოვნაზე გადაწყვეტილების მიღებისას კომპეტენტურმა ორგანომ, რომელმაც თავდაპირველად განახორციელა მონაცემთა გადაცემა, მხედველობაში უნდა მიიღოს ყველა რელევანტური ფაქტორი, მათ შორის დანაშაულის სიმძიმე, ის პირობები და მიზნები, როლებითაც მოხდა მონაცემთა თავდაპირველი გადაცემა, სასჯელის აღსრულების ხასიათი და პირობები, იმ მესამე სახელმწიფოში ან საერთაშორისო ორგანიზაციაში პერსონალურ მონაცემთა დაცვის სტანდარტები, რომელშიც უნდა განხორციელდეს მონაცემთა შედგომი გადაცემა. კომპეტენტურ ორგანოს, რომელმაც მოახდინა მონაცემთა თავდაპირველი გადაცემა, უნდა შეეძლოს სპეციალური პირობების დაწესება მონაცემთა შედმგომ გადაცემაზე. ამგვარი სპეციალური პირობები შესაძლოა აღიწეროს, მაგალითად, ქცევის კოდექსებში.

(66) კომისიას აქვს შესაძლებლობა, მიიღოს გადაწყვეტილება, რომელიც მთელს ევროკავშირზე გავრცელდება და რომელიც დაადგენს, რომ კონკრეტულ მესამე სახელმწიფოებს, მესამე სახელმწიფოს ტერიტორიას ან ერთ ან მეტ კონკრეტულ სექტორს ან საერთასორისო ორგანიზაციას აქვთ მონაცემთა დაცვის სათანადო სტანდარტი და ამ გადაწყვეტილებით უზრუნველყოფილი იქნება სამართლებრივი სიცხადე და ერთგვაროვნება ევროკავშირის მასშტაბით იმ მესამე სახელმწიფოების ან საერთაშორისო ორგანიზაციების მიმართ, რომლებსაც შეუძლიათ დაცვის ამგვარი სტანდარტის უზრუნველყოფა. ასეთ შემთხვევებში პერსონალურ მონაცემთა გადაცემა ამ ქვეყნებში

უნდა მოხდეს ყოველგვარი სპეციალური ნებართვის გარეშე, გარდა იმ შემთხვევისა, როდესაც სხვა წევრმა სახელმწიფომ, რომლისგანაც მოხდა მონაცემთა მოპოვება, უნდა გამოხატოს თანხმობა გადაცემაზე.

(67) იმ ფუნდამენტური ღირებულებების შესაბამისად, რომლებზეც დაფუძნებულია ევროკავშირი, კერძოდ კი ადამიანის უფლებათა დაცვის ღირებულებების შესაბამისად, მესამე სახელმწიფოს, ამ სახელმწიფოში არსებული ტერიტორიის ან ერთი ან მეტი კონკრეტული სექტორის შეფასებისას კომისიამ მხედველობაში უნდა მიიღოს, რამდენად უზრუნველყოფს მესამე სახელმწიფო კანონის უზენაესობას, მართლმსაჯულების ხელმისაწვდომობას, ისევე როგორც ადამიანის უფლებათა საერთაშორისო ნორმებსა და სტანდარტებს, მისი ზოგადი და სექტორული კანონმდებლობა, მათ შორის საზოგადოებრივ უსაფრთხოებასთან, თავდაცვასთან, ეროვნულ უსაფრთხოებასთან და საზოგადოებრივ წესრიგთან დაკავშირებული კანომდებლობა და სისხლის სამართლის კანონმდებლობა. მესამე სახელმწიფოში არსებული ტერიტორიის ან ერთი ან მეტი კონკრეტული სექტორის მიმართ შესაბამისობის გადაწყვეტილების მიღებისას მხედველობაში უნდა იქნეს მიღებული მკაფიო და ობიექტური კრიტერიუმები, როგორიცაა დამუშავების კონკრეტული ოპერაციები და მესამე სახელმწიფოში მოქმედი შესაბამისი სამართლებრივი სტანდარტებისა და კანონმდებლობის მოქმედების სფერო. მესამე სახელმწიფოს უნდა ჰქონდეს გარანტიები, რომლებიც უზრუნველყოფენ მონაცემთა დაცვის ადეკვატურ სტანდარტს, რომელიც ევროკავშირში არსებული სტანდარტის ექვივალენტურია, განსაკუთრებით, როდესაც მონაცემები მუშავდება ერთ ან მეტ კონკრეტულ სექტორში. მესამე სახელმწიფომ განსაკუთრებით უნდა უზრუნველყოს მონაცემთა დაცვაზე დამოუკიდებელი ზედამხედველობა, წევრი სახელმწიფოების მონაცემთა დაცვის ორგანოებთან თანამშრომლობა და მონაცემთა სუბიექტები უზუნველყოფილები უნდა იყვნენ ეფექტური და განხორციელებადი უფლებებით და დარღვეული უფლების აღდგენის ეფექტური ადმინისტრაციული და სასამართლო საშუალებებით.

(68) მესამე სახელმწიფოს ან საერთაშორისო ორგანიზაციის მიერ ნაკისრი საერთაშორისო ვალდებულებების გარდა, კომისიამ უნდა გაითვალისწინოს მესამე სახელმწიფოს ან საერთაშორისო ორგანიზაციის მრავალმრხრივ ან რეგიონულ სისტემებში მონაწილეობიდან გამომდინარე ვალდებულებები, განსაკუთრებით კი მონაცემთა

დაცვასთან მიმართებით, ასევე, ამ ვალდებულებების შესრულება. განსაკუთრებით უნდა იქნეს მიღებული მხედველობაში პერსონალურ მონაცემთა ავტომატური დამუშვებისას ფიზიკურ პირთა დაცვის ევროპის საბჭოს 1981 წლის 28 იანვრის კონვენციასა და მის დამატებით ოქმთან მესამე სახელმწიფოს მიერთება. მესამე სახელმწიფოებში ან საერთაშორისო ორგანიზაციებში მონაცემთა დაცვის სტანდარტების შეფასებისას კომისიამ კონსტულტაცია უნდა გაიაროს ევროპის მონაცემთა დაცვის საბჭოსთან, რომელიც (EU) 2016/679 რეგულაციით არის შექმნილი ("საბჭო"). კომისიამ ასევე მხედველობაში უნდა მიიღოს ნებისმიერი შესაბამისობის გადაწყვეტილება, რომელიც (EU) 2016/679 რეგულაციის 45-ე მუხლის შესაბამისად არის მიღებული.

(69) კომისიამ ზედამხედველობა უნდა გაუწიოს მესამე სახელმწიფოში, მესამე სახელმწიფოს ტერიტორიაზე ან კონკრეტულ სექტორში არსებული დაცვის სტანდარტების შესახებ მიღებული გადაწყვეტილების ფუნქციონირებას. თავის ადეკვატურობის გადაწყვეტილებებში, კომისიამ უნდა განსაზღვროს მათი ფუნქციონირების პერიოდული გადასინჯვის მექანიზმი. პერიოდული გადასინჯვა უნდა მოხდეს მესამე სახელმწიფოსთან ან საერთაშორისო ორგანიზაციასთან კონსულტაციის შედეგად და მხედველობაში უნდა იქნეს მიღებული მესამე სახელმწიფოში ან საერთაშორისო ორგანიზაციაში არსებული ყველა რელევანტური ფაქტორი.

(70) კომისიას, ასევე, უნდა შეეძლოს დაადასტუროს, რომ მესამე სახელმწიფო, ამ სახელმწიფოში არსებული ტერიტორია, კონკრეტული სექტორი ან საერთაშორისო ორგანიზაცია ვეღარ უზრუნველყოფს მონაცემთა დაცვის სათანადო სტანდარტს. შედეგად, პერსონალურ მონაცემთა გადაცემა ასეთ მესამე სახელმწიფოში ან საერთაშორისო ორგანიზაციაში უნდა აიკრძალოს ვიდრე არ შესრულდება წინამდებარე დირექტივით მონაცემთა გადაცემასთან დაკავშირებული დაცვის სათანადო გარანტიები და გამონაკლისები კონკრეტული სიტუაციებისათვის. უზრუნველყოფილი უნდა იყოს კომისიას და მესამე სახელმწიფოს ან საერთაშორისო ორგანიზაციას შორის ამგვარი კონსულტაციების პროცედურები. კომისიამ გონივრულ ვადაში უნდა შეატყობინოს მესამე სახელმწიფოს ან საერთაშორისო ორგანიზაციას მიზეზების შესახებ და დაიწყოს მასთან კონსულტაციები მდგომარეობის გამოსწორების მიზნით.

(71) მონაცემთა გადაცემა, რომელიც არ ხორციელდება შესაბამისობის გადაწყვეტილების საფუძველზე, დასაშვები უნდა იყოს მხოლოდ იმ შემთხვევაში, თუ სამართლებრივად სავალდებულო ხასიათის დოკუმენტში წარმოდგენილია დაცვის სათანადო გარანტიები, რომლებიც უზრუნველყოფენ პერსონალურ მონაცემთა დაცვას ან როდესაც დამმუშავებელმა შეაფასა მონაცემთა გადაცემასთან დაკავშირებული ყველა გარემოება და აღნიშნული შეფასების საფუძველზე მიიჩნევს, რომ პერსონლურ მონაცემთა დაცვასთან დაკავშირებული სათანადო გარანტიები სახეზეა. ამგვარი სამართლებრივად სავალდებულო დოკუმენტები, შესაძლოა, იყოს სამართლებრივად სავალდებულო ორმხრივი შეთანხმებები, რომლებიც დაიდო და სრულდება წევრი სახელმწიფოს მიერ და რომლებიც შეიძლება აღსრულდეს მათი მონაცემთა სუბიექტების მიერ. დოკუმენტი უნდა უზრუნველყოფდეს მონაცემთა დაცვის მოთხოვნებთან შესაბამისობასა და მონაცემთა სუბიექტების უფლებების დაცვას, მათ შორის ეფექტური ადმინისტრაციული ან სასამართლო დაცვის უფლებას. მონაცემთა გადაცემასთან დაკავშირებული ყველა გარემოების შეფასებისას დამმუშავებელს უნდა შეეძლოს, გაითვალისწონოს ევროპოლისა და ევროჯასტის მიერ მესამე სახელმწიფოსთან დადებული თანამშრომლობის შეთანხმებები, რომლებიც იძლევა მონაცემთა გადაცემის შესაძლებლობას. დამმუშავებელმა, ასევე, უნდა გაითვალისწინოს ის ფაქტი, რომ პერსონალურ მონაცემთა გადაცემა მოხდება კონფიდენციალურობის და კონკრეტული მიზნით დამუშავების პრინციპის დაცვით, რაც უზრუნველყოფს, რომ პერსონალური მონაცემები არ დამუშავდება გადაცემის მიზნისგან განსხვავებული მიზნით. ასევე, დამმუშავებელმა მხედველობაში უნდა მიიღოს, რომ პერსონალურ მონაცემთა გადაცემა არ უნდა მოხდეს სიკვდლით დასჯის ან ნებისმიერი ფორმის სასტიკი და არაადამიანური სასჯელის მოსათხოვად ან აღსასრულებლად. მართალია, მითითებული პირობები მონაცემთა გადაცემისათვის შეიძლება საკმარის გარანტიებად ჩაითვალოს, თუმცა დამმუშავებელს უნდა შეეძლოს დამატებითი გარანტიების მოთხოვნა.

(72) თუ არ არსებობს შესაბამისობის გადაწყვეტილება ან დაცვის სათანადო გარანტიები, გადაცემა ან გადაცემის კატეგორია შესაძლოა განხორციელდეს მხოლოდ სპეციალურ შემთხვევებში, თუ ეს აუცილებელია მონაცემთა სუბიექტის ან სხვა პირის სასიცოცხლო ინტერესების დასაცავად ან მონაცემთა სუბიექტის ლეგიტიმური ინტერესების დასაცავად, თუ ეს გათვალისწინებულია გადამცემი წევრი სახელმწიფოს კანონმდებლობით; წევრი სახელმწიფოს ან მესამე სახელმწიფოს საზოგადოებრივი უსაფრთხოების წინააღმდეგ

მიმართული მყისიერი და არსებითი საფრთხის პრევენციისათვის; ინდივიდუალურ შემთხვევებში დანაშაულთა პრევენციის, გამოძიების, დადგენის ან სისხლისსამართლებრივი დევნის ან სასჯელის აღსრულების, ასევე, საზოგადოებრივი უსაფრთხოების წინააღმდეგ მიმართული საფრთხისაგან დაცვის და პრევენციის მიზნებით; ან ინდივიდუალურ შემთხვევაში სამართლებრივი მოთხოვნების დასადგენად, განსახორციელებლად ან დასაცავად. ჩამოთვლილი გამონაკლისების ინტერპრეტაცია უნდა მოხდეს მკაცრად და არ უნდა ხდებოდეს პერსონალურ მონაცემთა ხშირი, მასობრივი და სტრუქტურიზებული გადაცემა, ან დიდი რაოდენობით მონაცემთა გადაცემა. გადაცემული მონაცემების რაოდენობა მკაცრად უნდა შეიზღუდოს მხოლოდ აუცილებელი მონაცემებით. მონაცემთა ამგვარი გადაცემა უნდა აღირიცხოს და დოკუმენტები მოთხოვნისამებრ გადაეცეს საზედამხედველო ორგანოს გადაცემის კანონიერებაზე ზედამხედველობის განსახორციელებლად.

(73) კანონით დაკისრებული ამოცანების შესასრულებლად რელევანტური ინფორმაციის გაცვლის მიზნით წევრი სახელმწიფოების კომპეტენტური ორგანოები იყენებენ სისხლის სამართლის საქმეებზე სასამართლო თანამშრომლობისა და საპოლიციო თანამშრომლობის სფეროში მესამე სახელმწიფოებთან დადებულ ორმხრივ ან მრავალმხრივ საერთაშორისო შეთანხმებებს. ძირითადად ეს ხდება ამ დირექტივის მიზნებისათვის მესამე სახელმწიფოში არსებული კომპეტენტური ორგანოს მეშვეობით ან სულ მცირე მასთან თანამშრომლობით, ხანდახან ორმხრივი ან მრავალმხრივი საერთაშორისო შეთანხმების არარსებობის პირობებში. თუმცა, სპეციალურ ინდივიდუალურ შემთხვევებში რეგულარული პროცედურა, რომელიც მესამე სახელმწიფოში ამგვარ ორგანოსთან კონტაქტის დამყარებას მოითხოვს, შესაძლოა, არაეფექტური ან არამართებული იყოს, განსაკუთრებით თუ გადაცემა ვერ განხორციელდება დროულად ან იმიტომ, რომ მესამე სახელმწიფოს კომპეტენტური ორგანო არ იცავს კანონის უზენაესობის პრინციპს ან ადამიანის უფლებათა საერთაშორისო ნორმებსა და სტანდარტებს. ამდენად, წევრი სახელმწიფოს კომპეტენტურ ორგანოებს შეუძლიათ პერსონალური მონაცემები პირდაპირ მესამე სახელმწიფოში არსებულ მიმღებს გადასცენ. ეს შეიძლება მოხდეს იმ შემთხვევაში თუ არსებობს პერსონალურ მონაცემთა გადაცემის სასწრაფო საჭიროება იმ პირის სიცოცხლის გადასარჩენად, რომელსაც ემუქრება დანაშაულის მსხვერპლად ქცევის საფრთხე ან დანაშაულის, მათ შორის ტერორიზმის მყისიერი პრევენციის ინტერესებისათვის. მაშინაც თუკი კომპეტენტურ ორგანოებსა და მესამე სახელმწიფოში

არსებულ მიმღებს შორის მონაცემთა გადაცემა მოხდება კონკრეტულ ინდივიდუალურ შემთხვევებში, წინამდებარე დირექტივა უნდა ითვალისწინებდეს ამგვარი შემთხვევების მარეგულირებელ პირობებს. ეს დებულებები არ უნდა ჩაითვალოს გამონაკლისად სისხლის სამართლის საქმეებზე სასამართლო თანამშრომლობისა და საპოლიციო თანამშრომლობის სფეროში დადებული რომელიმე ორმხრივი ან მრავალმხრივი საერთაშორისო შეთანხმებისაგან. ეს დებულებები გამოყენებულ უნდა იქნეს წინამდებარე დირექტივის სხვა წესებთან ერთად, განსაკუთრებით დამუშავების კანონიერების და V თავის წესებთან ერთად.

(74) როდესაც პერსონალური მონაცემები საზღვრებს მიღმა გადადინდება, გაზრდილი საფრთხე შესაძლოა შეექმნას ფიზიკური პირების მიერ მონაცემთა დაცვის უფლებების განხორციელების შესაძლებლობას ამ მონაცემების უკანონო გამოყენების ან გამჟღავნებისაგან საკუთარი თავის დასაცავად. ამავდროულად, საზედამხედველო ორგანოებმა შესაძლოა აღმოაჩინონ, რომ ვერ განიხილავენ საჩივრებს და ვერ ატარებენ გამოძიებას მათ საზღვრებს მიღმა განხორციელებულ საქმიანობაზე. მათი მცდელობა, ითანამშრომლონ ტრანსსასაზღვრო კონტექსტში შესაძლოა, ასევე, შეფერხდეს არასაკმარისი პრევენციული ან მაკორექტირებელი უფლებამოსილებების და განსხვავებული სამართლებრივი რეჟიმების გამო. ამდენად, საჭიროა მონაცემთა დაცვის საზედამხედველო ორგანოთა შორის მჭიდრო თანამშრომლობის გაღრმავება უცხოელ პარტნიორებთან ინფორმაციის გაცვლაში დახმარების მიზნით.

(75) წევრ სახელმწიფოებში ისეთი საზედამხედველო ორგანოების შექმნა, რომელთაც შეუძლიათ თავიანთი ფუნქციების სრულიად დამოუკიდებლად შესრულება, პერსონალური მონაცემების დამუშავებისას ფუზიკურ პირთა დაცვის არსებითი კომპონენტია. საზედამხედველო ორგანოებმა უნდა მოახდინონ წინამდებარე დირექტივის შესაბამისად მიღებული დებულებების გამოყენებაზე ზედამხედველობა და ხელი შეუწყონ მათ ერთგვაროვან გამოყენებას ევროკავშირის მასშტაბით იმისათვის, რომ დაიცვან ფიზიკური პირები მათი პერსონალური მონაცემების დამუშავებისას. ამ მიზნით საზედამხედველო ორგანოებმა უნდა ითანამშრომლონ ერთმანეთთან და კომისიასთან.

(76) წევრ სახელმწიფოებს უფლებათ აქვთ (EU) 2016/679 რეგულაციის საფუძველზე უკვე შექმნილ საზედამხედველო ორგანოს დააკისრონ წინამდებარე დირექტივის მიხედვით შესაქმნელი საზედამხედველო ორგანოს ამოცანების შესრულება.

(77) წევრ სახელმწიფოებს უფლება აქვთ, შექმნან ერთზე მეტი საზედამხედველო ორგანო, რომელიც შეესაბამება მათ კონსტიტუციურ, ორგანიზაციულ და ადმინისტრაციულ სტრუქტურას. თითოეული საზედამხედველო ორგანო უზრუნველყოფილი უნდა იყოს ფინანსური და ადამიანური რესურსით, სამუშაო სივრცითა და ინფრასტრუქტურით, რომლებიც აუცილებელია მისი ამოცანების ეფექტურად შესრულებისათვის, მათ შორის ევროკავშირის მასშტაბით არსებულ საზედამხედველო ორგანოებთან ურთიერთდახმარებასა და თანამშრომლობასთან დაკავშირებული ამოცანების შესასრულებლად. თითოეულ საზედამხედველო ორგანოს უნდა ჰქონდეს დამოუკიდებელი წლიური ბიუჯეტი, რომელიც შესაძლოა მთლიანი სახელმწიფო ან ეროვნული ბიუჯეტის ნაწილი იყოს.

(78) საზედამხედველო ორგანოები უნდა ექვემდებარებოდნენ კონტროლის ან ზედამხედველობის დამოუკიდებელ მექანიზმებს მათ ფინანსურ ხარჯვასთან დაკავშირებით, იმ პირობით, რომ ამგვარი ფინანსური კონტროლი ზიანს არ მიაყენებს მათ დამოუკიდებლობას.

(79) ზოგადი პირობები, რომლებსაც საზედამხედველო ორგანოს წევრი ან წევრები უნდა აკმაყოფილებდნენ, წევრი სახელმწიფოს კანონმდებლობით უნდა განისაზღვროს და უნდა უზრუნველყოფდეს, რომ წევრებს ნიშნავდეს პარლამენტი, მთავრობა, ან წევრი სახელმწიფოს მეთაური მთავრობის, მთავრობის წევრის, პარლამენტის ან მისი პალატის, ან დამოუკიდებელი ორგანოს წარდგინების საფუძველზე, რომელსაც წევრი სახელმწიფოს კანონმდებლობით აკისრია გამჭვირვალე პროცედურების საფუძველზე დანიშვნის უფლებამოსილება. საზედამხედველო ორგანოს დამოუკიდებლობის უზრუნველსაყოფად მისმა წევრმა ან წევრებმა უნდა იმოქმედონ ეთიკურად, თავი შეიკავონ ქმედებისგან, რომელიც შეუთავსებელია მათ მოვალეობებთან და თანამდებობაზე ყოფნის განმავლობაში არ დაიკავონ შეუთავსებელი პოზიცია, როგორც ანაზღაურებადი, ისე არაანაზღაურებადი. საზედამხედევლო ორგანოს დამოუკიდებლობის უზრუნველსაყოფად მისი

თანამშრომლების შერჩევა უნდა მოხდეს საზედამხედველო ორგანოს მიერ და ამ პროცესში შესაძლოა ჩაერთოს წევრი სახელმწიფოს მიერ უფლებამოსილი დამოუკიდებელი ორგანო.

(80) მართალია, წინამდებარე დირექტივის მოქმედება ვრცელდება სასამართლოებსა და მართლმსაჯულების სხვა ორგანოების საქმიანობაზე, საზედამხედველო ორგანოს უფლებამოსილება არ უნდა გავრცელდეს პერსონალურ მონაცემთა დამუშავებაზე, როდესაც სასამართლოები მოქმედებენ სასამართლო უფლებამოსილების ფარგლებში, იმისათვის, რომ დაცული იყოს მოსამართლეთა დამოუკიდებლობა მათ მიერ სასამართლო ამოცანების შესრულებისას. ეს გამონაკლისი უნდა გავრცელდეს მხოლოდ სასამართლო საქმეების განხილვაზე და არა სხვა საქმიანობაზე, რომელშიც შესაძლოა ჩართული იყოს მოსამართლე წევრი სახელმწიფოს კანონმდებლობის შესაბამისად. ამასთან, წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ საზედამხედველო ორგანოს კომპეტენცია არ გავრცელდეს მართლმსაჯულების სხვა ორგანოების მიერ პერსონალურ მონაცემთა დამუშავებაზე, როდესაც ისინი მართლმსაჯულების ფუნქციას ასრულებენ, მაგალითად, პროკურატურა. ნებისმიერ შემთხვევაში წინამდებარე დირექტივასთან სასამართლოებისა და მათლმსაჯულების სხვა დამოუკიდებელი ორგანოების შესაბამისობა ექვემდებარება დამოუკიდებელ ზედამხედველობას ქარტიის მე-8 მუხლის მე-3 პუნქტის შესაბამისად.

(81) თითოეულმა საზედამხედველო ორგანომ უნდა განიხილოს მონაცემთა სუბიექტების მიერ შეტანილი საჩივრები და გამოიძიოს საკითხი ან გადაუგზავნოს საჩივარი კომპეტენტურ საზედამხედველო ორგანოს. საჩივრის საფუძველზე ჩატარებული გამოძიება, რომელიც შესაძლოა სასამართლოს გადასინჯვის საგანი იყოს, უნდა ჩატარდეს იმ მოცულობით, რომელიც საჭიროა კონკრეტულ შემთხვევაში. საზედამხედველო ორგანომ გონივრულ ვადაში უნდა შეატყობინოს მონაცემთა სუბიექტს საჩივრის განხილვის შედეგების შესახებ. თუ საქმე საჭიროებს დამატებით გამოძიებას ან სხვა საზედამხედველო ორგანოსთან კოორდინირებას, მონაცემთა სუბიექტს უნდა მიეწოდოს შუალედური ინფორმაცია.

(82) “ევროკავშირის ფუნქციონირების შესახებ” ხელშეკრულებისა და მართლმსაჯულების სასამართლოს განმარტებების შესაბამისად ევროკავშირის მასშტაბით წინამდებარე დირექტივის შესრულების ეფექტური, სანდო და ერთგვაროვანი ზედამხედველობის უზრუნველსაყოფად, საზედამხედველო ორგანოებს ყველა წევრ სახელმწიფოში ერთნაირი

ამოცანები და ეფექტური უფლებამოსილებები უნდა ჰქონდეთ, მათ შორის საგამოძიებო, მაკორექტირებელი და საკონსულტაციო უფლებამოსილებები, რომლებიც მათი ამოცანების შესასრულებლად აუცილებელ საშუალებებს წარმოადგენს. თუმცა, მათი უფლებამოსილება არ უნდა უშლიდეს ხელს სისხლის სამართლის პროცესის წესებს, მათ შორის გამოძიებას და დანაშაულების სისხლისსამართლებივ დევნას, ან სასამართლოს დამოუკიდებლობას. წევრი სახელმწიფოს კანონმდებლობით საპროკურორო ორგანოების უფლებამოსილებების შეუზღუდავად, საზედამხედველო ორგანოებს, ასევე, უნდა ჰქონდეთ წინამდებარე დირექტივის დარღვევების შესახებ სასამართლო ორგანოების ინფომირების ან სამართალწარმოებაში ჩართვის უფლებამოსილება. საზედამხედველო ორგანოების უფლებამოსილებები უნდა განხორციელდეს ევროკავშირის და წევრი სახელმწიფოს კანონმდებლობით განსაზღვრული პროცედურული გარანტიების შესაბამისად, მიუკერძოებლად, სამართლიანად და გონივრულ ვადაში. თითოეული ზომა უნდა იყოს სათანადო, აუცილებელი და პროპორციული წინამდებარე დირექტივასთან შესაბამისობის უზრუნველსაყოფად, უნდა ითვალისწინებდეს თითოეული ინდივიდუალური საქმის გარემოებებს, პატივს უნდა სცემდეს თითოეული პირის უფლებას, გამოთქვას საკუთარი აზრი, ვიდრე მისთვის საზიანო კონკრეტული ზომა იქნება მიღებული და არ უნდა იწვევდეს ზედმეტ ხარჯს და დაინტერესებული პირისათვის გადამეტებული დისკომფორტის მიყენებას. ტერიტორიაზე შესვლის საგამოძიებო უფლებამოსილებების გამოყენება უნდა განხორციელდეს წევრი სახელმწიფოს სპეციალური მოთხოვნების შესაბამისად, როგორიცაა წინასწარი სასამართლო ნებართვის მოპოვების მოთხოვნა. სამართლებრივად სავალდებულო გადაწყვეტილების გადასინჯვა უნდა მოხდეს სასამართლოს მიერ იმ საზედამხედველო ორგანოს წევრ სახელმწიფოში, რომელმაც გამოიტანა გადაწყვეტილება.

(83) საზედამხედველო ორგანოებმა ერთმანეთთან უნდა ითანამშრომლონ თავიანთი ამოცანების შესრულებისას და ორმხივი დახმარება აღმოუჩინონ ერთმანეთს იმისათვის, რომ უზრუნველყონ წინამდებარე დირექტივის შესაბამისად მიღებული დებულებების ერთგვაროვანი გამოყენება და აღსრულება.

(84) საბჭომ ხელი უნდა შეუწყოს ევროკავშირის მასშტაბით წინამდებარე დირექტივის ერთგვაროვან გამოყენებას, მათ შორის კომისიისათვის კონსულტაციების გაწევისა და

ევროკავშირის ტერიტორიაზე საზედამხედველო ორგანოთა თანამშრომლობის წახალისების გზით.

(85) თითოეულ მონაცემთა სუბიექტს უნდა ჰქონდეს უფლება, შეიტანოს საჩივარი ერთ საზედამხედველო ორგანოში და უფლება, გამოიყენოს სამართლებრივი დაცვის ეფექტური საშუალება ქარტიის 47-ე მუხლის შესაბამისად, როდესაც მონაცემთა სუბიექტი მიიჩნევს, რომ წინამდებარე დირექტივის შესაბამისად მიღებული დებულებებით გათვალისწინებული მისი უფლებები დაირღვა, ან საზედამხედველო ორგანო არ ახორციელებს რეაგირებას საჩივარზე და სრულად ან ნაწილობრივ არ დააკმაყოფილებს, დაუშვებლად ცნობს საჩივარს ან არ იღებს ზომებს, როდესაც ასეთი ზომები აუცილებელია მონაცემთა სუბიექტის უფლებების დასაცავად. საჩივრის საფუძველზე ჩატარებული გამოძიება, რომელიც შესაძლოა სასამართლოს გადასინჯვის საგანი იყოს, უნდა ჩატარდეს იმ მოცულობით, რომელიც საჭიროა კონკრეტულ შემთხვევაში. საზედამხედველო ორგანომ გონივრულ ვადაში უნდა შეატყობინოს მონაცემთა სუბიექტს საჩივრის განხილვის მიმდინარეობისა და შედეგების შესახებ. თუ საქმე საჭიროებს დამატებით გამოძიებას ან სხვა საზედამხედველო ორგანოსთან კოორდინირებას, მონაცემთა სუბიექტს უნდა მიეწოდოს შუალედური ინფორმაცია. საჩივრის წარდგენის პროცედურის ხელშეწყობისათვის, თითოეულმა საზედამხედველო ორგანომ უნდა მიიღოს სათანადო ზომები, მათ შორის შეიმუშაოს საჩივრის ფორმა, რომლის შევსება ელექტრონულადაც არის შესაძლებელი, კომუნიკაციის სხვა ფორმების შეუზღუდავად.

(86) თითოეულ ფიზიკურ თუ იურიუდიულ პირს უნდა ჰქონდეს საზედამხედველო ორგანოს სამართლებრივი შედეგის მომტანი გადაწყვეტილების წინააღმდეგ ეროვნულ სასამართლოში სამართლებრივი დაცვის ეფექტური საშუალების გამოყენების უფლება. ეს გადაწყვეტილება შესაძლოა ეხებოდეს საზედამხედველო ორგანოს მიერ საგამოძიებო, მაკორექტირებელი და სანებართვო უფლებამოსილებების განხორციელებას და საჩივრების დაკმაყოფილებაზე უარის თქმას ან მათ დაუშვებლად ცნობას. ამასთან, ეს უფლება არ ვრცელდება საზედამხედველო ორგანოს მიერ გამოყენებულ სხვა ზომებზე, რომელთაც არ აქვთ სამართლებრივად სავალდებულო ხასიათი, როგორებიცაა საზედამხედველო ორგანოს მოსაზრება ან რჩევა. სამართალწარმოება საზედამხედველო ორგანოს წინააღმდეგ უნდა მიმდინარეობდეს იმ წევრი სახელმწიფოს სასამართლო ორგანოებში, რომელშიც დაფუძნებულია საზედამხედევლო ორგანო და უნდა წარიმართოს წევრი სახელმწიფოს

კანონმდებლობის შესაბამისად. სასამართლომ უფლებამოსილება, მათ შორის დავასთან დაკავშირებული ყველა ფაქტობრივი და სამართლებრივი საკითხის გამოკვლევის უფლებამოსილება სრულად უნდა განახორციელოს.

(87) როდესაც მონაცემთა სუბიექტი თვლის, რომ წინამდებარე დირექტივით გათვალისწინებული მისი უფლებები დაირღვა, მას უნდა ჰქონდეს უფლება, მისი უფლებების დაცვა დაავალოს ორგანიზაციას, რომლის მიზანი პერსონალურ მონაცემთა დაცვასთან მიმართებით მონაცემთა სუბიექტების ინტერესების დაცვაა და რომელიც წევრი სახელმწიფოს კანონმდებლობის შესაბამისად უფლებამოსილია სუბიექტის სახელით საზედამხედველო ორგანოში შეიტანოს საჩივარი და გამოიყენოს სამართლებრივი დაცვის საშუალების უფლება. მონაცემთა სუბიექტის წარმომადგენლობის უფლება არ ზღუდავს წევრი სახელმწიფოს საპროცესო კანონმდებლობას, რომელიც შესაძლოა მოითხოვდეს ეროვნული სასამართლოების წინაშე მონაცემთა სუბიექტის სავალდებულო წარმომადგენლობას ადვოკატის მიერ, როგორც ეს განსაზღვრულია საბჭოს 77/249/EEC დირექტივით[10].

(88) ნებისმიერი ზიანი, რომელიც შესაძლოა პირს მიადგეს წინამდებარე დირექტივის საფუძველზე მიღებული დებულებების დარღვევით განხორციელებული დამუშავების შედეგად, უნდა ანაზღაურდეს დამმუშავებლის ან წევრი სახელმწიფოს კანონმდებლობით განსაზღვრული სხვა კომპეტენტური ორგანოს მიერ. ზიანის კონცეფციას ფართო ინტერპრეტაცია უნდა მიეცეს მართლმსაჯულების სასამართლოს პრაქტიკის გათვალისწინებით იმგვარად, რომ სრულად იყოს ასახული წინამდებარე დირექტივის მიზნები. ზიანის ანაზღაურების მოთხოვნის განხორციელება უნდა მოხდეს ევროკავშირის ან წევრი სახელმწიფოს კანონმდებლობის სხვა დარღვევებით გამოწვეული ზიანის მოთხოვნის უფლების შეუზღუდავად. როდესაც საუბარია უკანონო დამუშავებაზე ან დამუშავებაზე, რომელიც ეწინააღმდეგება წინამდებარე დირექტივის შესაბამისად მიღებულ დებულებებს, მასში, ასევე, იგულისხმება დამუშავება, რომელიც ეწინააღმდეგება წინამდებარე დირექტივის შესაბამისად მიღებულ საიმპლემენტაციო აქტებს. მონაცემთა სუბიექტებმა მიყენებული ზიანისათვის უნდა მიიღონ სრული და ეფექტური კომპენსაცია.

---

[10] ევროსაბჭოს 1977 წლის 22 მარტის 77/249/EEC დირექტივა ადვოკატების მიერ მომსახურეობის თავისუფალი გაწევის უფლების განხორციელების ხელშეწყობის თაობაზე (OJ L 78, 26.3.1977, გვ . 17).

(89) ნებისმიერ ფიზიკურ ან იურიდიულ პირს, იქნება ის კერძო თუ საჯარო სამართლის სუბიექტი, უნდა დაეკისროს სახდელი წინამდებარე დირექტივის დარღვევისათვის. წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ სახდელები იყოს ეფექტური, პროპორციული და შემაკავებელი ეფექტის მქონე და მიიღონ ყველა ზომა ამ სახდელების აღსასრულებლად.

(90) წინამდებარე დირექტივის აღსრულების ერთიანი პირობების უზრუნველსაყოფად, კომისიას უნდა მიენიჭოს საიმპლემენტაციო უფლებამოსილება მესამე სახელმწიფოს, ამ სახელმწიფოს ტერიტორიის ან კონკრეტული სექტორის ან საერთაშორისო ორგანიზაციის მიერ დაცვის ადეკვატურ სტანდარტთან, ურთიერთდახმარების ფორმატსა და პროცედურებთან, საზედამხედველო ორგანოებს, ასევე, საბჭოსა და საზედამხედველო ორგანოებს შორის ინფორმაციის ელექტრონულ გაცვლასთან მიმართებით. ეს უფლებამოსილებები უნდა განხორციელდეს ევროპის პარლამენტისა და საბჭოს (EU) No 182/2011 რეგულაციის[11] შესაბამისად.

(91) მესამე სახელმწიფოს, ამ სახელმწიფოს ტერიტორიის ან კონკრეტული სექტორის ან საერთაშორისო ორგანიზაციის მიერ დაცვის ადეკვატურ სტანდარტთან, ურთიერთდახმარების ფორმატსა და პროცედურებთან, საზედამხედველო ორგანოებს, ასევე, საბჭოსა და საზედამხედველო ორგანოებს შორის ინფორმაციის ელექტრონულ გაცვლასთან დაკავშირებული საიმპლემენტაციო აქტების მიღებისათვის უნდა განისაზღვროს გადასინჯვის პროცედურა, თუ ამ აქტებს მოქმედების ზოგადი სფერო აქვთ.

(92) მესამე სახელმწიფოს, ამ სახელმწიფოს ტერიტორიასთან, კონკრეტულ სექტორთან ან საერთაშორისო ორგანიზაციასთან დაკავშირებით, რომლებიც დადასტურებულად ვეღარ უზრუნველყოფენ მონაცემთა დაცვის სათანადო სტანდარტს კომისიამ უნდა მიიღოს დაუყოვნებლივ აღსრულებადი საიმპლემენტაციო აქტები თუ ამას გადაუდებელი აუცილებლობა მოითხოვს.

---

[11] ევროპარლამენტისა და ევროსაბჭოს 2011 წლის 16 თებერვლის (EU) No 182/2011 რეგულაცია, რომელიც ადგენს კომისიის მიერ საიმპლემენტაციო უფლებამოსილების განხორციელების წევრი სახელმწიფოების მხრიდან კონტროლის მექანიზმების წესებსა და ზოგად პრინციპებს (OJ L 55, 28.2.2011, გვ. 13).

(93) თუ წინამდებარე დირექტივის მიზნები, კერძოდ, ფიზიკური პირების ფუნდამენტური უფლებებისა და თავისუფლებების დაცვა, პერსონალურ მონაცემთა დაცვის უფლება და ევროკავშირის ტერიტორიაზე კომპეტენტური ორგანოების მიერ პერსონალური მონაცემების თავისუფალი გაცვლის უზრუნველყოფა, ვერ ხორციელდება წევრი სახელმწიფოების მიერ და ქმედების მასშტაბის ან შედეგების გამო შესაძლოა ევროკავშირის დონეზე უკეთ განხორციელდეს, ევროკავშირის ხელშეკრულების მე-5 მუხლით განსაზღვრული სუბსიდიარობის პრინციპის შესაბამისად, ევროკავშირს შეუძლია მიიღოს სათანადო ზომები. ხსენებულ მუხლში განსაზღვრული პროპორციულობის პრინციპის შესაბამისად, წინამდებარე დირექტივა არ გამოიყენება იმაზე მეტად, ვიდრე ეს აუცილებელია ამ მიზნების მისაღწევად.

(94) ევროკავშირის სამართლებრივ აქტებში მოცემული პერსონალურ მონაცემთა დაცვის კონკრეტული დებულებები სისხლის სამართლის საქმეებზე სამართლებრივი დახმარებისა და საპოლიციო თანამშრომლობის სფეროში, რომლებიც ძალაში წინამდებარე დირექტივის მიღებამდე შევიდა და არეგულირებს წევრ სახელმწიფოებს შორის დამუშავებას და წევრი სახელმწიფოს უფლებამოსილი ორგანოების მიერ წინამდებარე დირექტივის ფარგლებში არსებული ხელშეკრულებების შესაბამისად შექმნილ საინფორმაციო სისტემებთან წვდომას, ძალაში რჩება. ესენია, მაგალითად, საბჭოს 2008/615/JHA გადაწყვეტილების[12] შესაბამისად მიღებული სპეციალური დებულებები, რომლებიც პერსონალურ მონაცემთა დაცვას ეხება, ან ევროკავშირის წევრ სხელმწიფოებს შორის სისხლის სამართლის საქმეებზე ურთიერთდახმარების შესახებ კონვენციის 23-ე მუხლი[13]. ვინაიდან ქარტიის მე-8 მუხლისა და “ევროკავშირის ფუნქციონირების შესახებ” ხელშეკრულების მე-16 მუხლის მოთხოვნაა ევროკავშირის მასშტაბით პერსონალურ მონაცემთა დაცვის ფუნდამენტური უფლების ერთგვაროვნად დაცვა, კომისიამ უნდა შეაფასოს, წინამდებარე დირექტივასა და მის მიღებამდე მიღებულ სამათლებრივ აქტებს შორის ურთიერთობა, რომლებიც არეგულირებენ წევრ სახელმწიფოებს შორის მონაცემთა დამუშავებას ან წევრი სახელმწიფოების უფლებამოსილი ორგანოების მიერ საერთაშორისო ხელშეკრულებების

[12] ევროსაბჭოს 2008 წლის 23 ივნისის 2008/615/JHA გადაწყვეტილება ტრანსასაზღვრო თანამშრომლობის გაძლიერების შესახებ, განსაკუთრებით ტერორიზმისა და ტრანსნაციონალური დანაშაულის წინააღმდეგ ბრძოლაში (OJ L 210, 6.8.2008, გვ. 1).

[13] საბჭოს 2000 წლის 29 მაისის აქტი, რომელიც ევროკავშირის შესახებ ხელშეკრულების 34-ე მუხლის შესაბამისად ამტკიცებს ევროკავშირის წევრ სახელმწიფოებს შორის სისხლის სამართლის საქმეებზე ურთიერთდახმარების კონვენციას (OJ C 197, 12.7.2000, გვ 1).

შესაბამისად შექმნილ საინფორმაციო სისტემებთან წვდომას, იმისათვის, რომ იმსჯელოს ამ სპეციალური დებულებების წინამდებარე დირექტივასთან შესაბამისობაში მოყვანის საჭიროებაზე. საჭიროების შემთხვევაში, კომისიამ უნდა წარმოადგინოს შემოთავაზებები პერსონალური მონაცემების დამუშვებასთან დაკავშირებული ერთგვაროვანი სამართლებრივი რეგულაციების უზრუნველყოფის მიზნით.

(95) ევროკავშირში პერსონალურ მონაცემთა სრულყოფილი და ერთგვაროვანი დაცვის უზრუნველსაყოფად, საერთაშორისო შეთანმებები, რომლებიც წევრმა სახელმწიფოებმა წინამდებარე დირექტივის ძალაში შესვლამდე დადეს და რომლებიც შეესაბამება ევროკავშირის შესაბამის კანომდებლობას მითითებულ თარიღამდე, უნდა დარჩეს ძალაში მათში ცვლილებების შეტანამდე, მათ ჩანაცვლებამდე ან გაუქმებამდე.

(96) წევრ სახელწიფოებს უნდა მიეცეს წინამდებარე დირექტივის ძალაში შესვლიდან არაუმეტეს ორი წლის ვადა მისი ტრანსპოზიციისათვის. დამუშავება, რომელიც უკვე მიმდინარეობს მოყვანილ უნდა იქნეს წინამდებარე დირექტივასთან შესაბამისობაში მისი ძალაში შესვლიდან ორი წლის ვადაში. თუმცა, თუ დამუშავება შეესაბამება წინამდებარე დირექტივის ძალაში შესვლამდე მოქმედ ევროკავშირის კანომდებლობას, წინამდებარე დირექტივის მოთხოვნა, რომელიც შეეხება საზედამხედველო ორგანოს წინასწარ კონსულტაციას, არ გავრცელდება დამუშავების იმ ოპერაციებზე, რომლებიც უკვე მიმდინარეობს ამ თარიღისათვის იმის გათვალისწინებით, რომ თავიანთი ხასიათიდან გამომდინარე ეს მოთხოვნები უნდა დაკმაყოფილდეს დამუშავების დაწყებამდე. თუ მითითებულ ვადამდე შემუშავებული ავტომატური დამუშავების სისტემებთან დაკავშირებული ლოგირების ვალდებულებების შესასრულებლად წევრი სახელმწიფოები ისარგებლებენ იმპლემენტაციის უფრო ხანგრძლივი ვადით, რომელიც იწურება წინამდებარე დირექტივის ძალაში შესვლიდან შვიდი წლის შემდეგ, დამმუშავებელს ან უფლებამოსილ პირს შემუშავებული უნდა ჰქონდეთ დამუშავების კანონიერების დემონსტრირებისთვის ეფექტური მეთოდები, როგორიცაა, ლოგირება ან აღრიცვის სხვაგვარი ფორმები, თვითმონიტორინგისა და მონაცემთა უსაფრთხოების და მთლიანობის უზრუნველსაყოფად.

(97) წინამდებარე დირექტივა არ ზღუდავს სექსუალური ძალადობის, ბავშვთა სექსუალური ექსპლუატაციისა და ბავშვთა პორნოგრაფიასთან ბრძოლისაკენ მიმართულ

რეგულაციებს, რომლებიც განსაზღვრულია ევროპის პარლამენტისა და საბჭოს 2011/93/EU დირექტივით[14].

(98) ჩარჩო გადაწყვეტილება 2008/977/JHA ძალადაკარგულად ცხადდება.

(99) თავისუფლების, უსაფრთხოებისა და მართლმსაჯულების სფეროში გაერთიანებული სამეფოსა და ირლანდიის პოზიციასთან დაკავშირებული "ევროკავშირის შესახებ" ხელშეკრულებისა და "ევროკავშირის ფუნქციონირების შესახებ" ხელშეკრულების N21 ოქმის მე-6 მუხლის შესაბამისად, გაერთიანებული სამეფო და ირლანდია არ არიან შეზღუდულები წინამდებარე დირექტივის წესებით, რომლებიც შეეხება წევრ სახელმწიფოთა მიერ პერსონალური მონაცემების დამუშავებას "ევროკავშირის ფუნქციონირების შესახებ" ხელშეკრულების მე-3 ნაწილის V კარის მე-4 ან მე-5 თავების იურისდიქციაში შემავალი საქმიანობის განხორციელებისას, სადაც გაერთიანებული სამეფო და ირლანდია არ არიან შეზღუდულები სისხლის სამართლის საქმეებზე სასამართლო და საპოლიციო თანამშრომლობის ფორმების მარეგულირებელი წესებით, რომლებიც მოითხოვენ "ევროკავშირის ფუნქციონირების შესახებ" ხელშეკრულების მე-16 მუხლის შესაბამისად მიღებულ დებულებებთან შესაბამისობას.

(100) დანიის პოზიციასთან დაკავშირებული "ევროკავშირის შესახებ" ხელშეკრულებისა და "ევროკავშირის ფუნქციონირების შესახებ" ხელშეკრულების N22 ოქმის მე-2 და მე-2ა მუხლების შესაბამისად, დანია არ არის შეზღუდული წინამდებარე დირექტივის წესებით და არ არის ვალდებული გამოიყენოს ეს წესები, რომლებიც შეეხება წევრ სახელმწიფოთა შორის პერსონალური მონაცემების დამუშავებას "ევროკავშირის ფუნქციონირების შესახებ" ხელშეკრულების მე-3 ნაწილის V კარის მე-4 ან მე-5 თავების იურისდიქციაში შემავალი საქმიანობის განხორციელებისას. იმის გათვალისწინებით, რომ "ევროკავშირის ფუნქციონირების შესახებ" ხელშეკრულების მესამე ნაწილის V კარის შესაბამისად, წინამდებარე დირექტივა ეფუძნება შენგენის კანონების და ნორმატიული აქტების კრებულს, ოქმის მე-4 მუხლის შესაბამისად დანიამ წინამდებარე დირექტივის მიღებიდან

[14] ევროპარლამენტისა და საბჭოს 2011 წლის 13 დეკემბრის 2011/93/EU დირექტივა არასრულწლოვნებზე სექსუალური ძალადობისა და სექსუალური ექსპლუატაციის, ასევე ბავშვთა პორნოგრაფიის წინააღმდეგ ბრძოლის შესახებ, რომელმაც ჩაანაცვლა საბჭოს ჩარჩო გადაწყვეტილება 2004/68/JHA (OJ L 335, 17.12.2011, გვ. 1).

ექვსი თვის ვადაში უნდა გადაწყვიტოს მისი ეროვნულ კანომდებლობაში იმპლემენტაციის საკითხი.

(101) რაც შეეხება ისლანდიასა და ნორვეგიას, წინამდებარე დირექტივა წარმოადგენს შენგენის კანონების და ნორმატიული აქტების კრებულის დებულებების გაგრძელებას, როგორც ეს გათვალისწინებულია ევროკავშირის საბჭოსა და ისლანდიის რესპუბლიკას და ნორვეგიის სამეფოს შორის გაფორმებული შეთანხმებით, რომელიც შეეხება მითითებული ორი სახელმწიფოს ასოცირებას შენგენის კანონებისა და ნორმატიული აქტების კრებულის იმპლემენტაციით, გამოყენებითა და განვითარებით[15].

(102) რაც შეეხება შვეიცარიას, წინამდებარე დირექტივა წარმოადგენს შენგენის კანონების და ნორმატიული აქტების კრებულის დებულებების გაგრძელებას, როგორც ეს გათვალისწინებულია ევროკავშირს, ევროკავშირის საზოგადოებასა და შვეიცარიის კონფედერაციას შორის გაფორმებული შეთანხმებით, რომელიც შეეხება შვეიცარიის კონფედერაციის ასოცირებას შენგენის კანონებისა და ნორმატიული აქტების კრებულის იმპლემენტაციით, გამოყენებითა და განვითარებით[16].

(103) რაც შეეხება ლიხტენშტეინს, წინამდებარე დირექტივა წარმოადგენს შენგენის კანონების და ნორმატიული აქტების კრებულის დებულებების გაგრძელებას, როგორც ეს გათვალისწინებულია ევროკავშირის, ევროკავშირის საზოგადოებას, შვეიცარიის კონფედერაციასა და ლიხტენშტეინის საგრაფოს შორის გაფორმებული ოქმით, რომელიც შეეხება შვეიცარიის კონფედერაციის ასოცირებას შენგენის კანონებისა და ნორმატიული აქტების კრებულის იმპლემენტაციით, გამოყენებითა და განვითარებით[17].

(104) წინამდებარე დირექტივა იცავს ფუნდამენტურ უფლებებსა და ქარტიით აღიარებულ პრინციპებს, როგორც ეს გათვალისწინებულია “ევროკავშირის ფუნქციონირების შესახებ” ხელშეკრულებით, კერძოდ, პირადი და ოჯახური ცხოვრების უფლებას, პერსონალურ მონაცემთა დაცვის უფლებას, ეფექტური სამართლებრივი დაცვის უფლებას და სამართლიანი სასამართლოს უფლებას. ამ უფლებების შეზღუდვა შეესაბამება ქარტიის

---

15 OJ L 176, 10.7.1999, გვ. 36.
16 OJ L 53, 27.2.2008, გვ. 52.
17 OJ L 160, 18.6.2011, გვ. 21.

52-ე მუხლის პირველ ნაწილს, ვინაიდან შეზღუდვა აუცილებელია ევროკავშირის ძირითადი ამოცანების შესასრულებლად ან სხვა პირების უფლებებისა და თავისუფლებების დასაცავად.

(105) განმარტებითი დოკუმენტების შესახებ წევრი სახელმწიფოებისა და კომისიის 2011 წლის 28 სექტემბრის ერთობლივი პოლიტიკური დეკლარაციის შესაბამისად, წევრი სახელმწიფოები იღებენ ვალდებულებას, დასაბუთებულ შემთხვევებში მათ მიერ მიღებული ტრანსპოზიციის ზომების შესახებ შეტყობინებას დაურთონ ერთი ან მეტი დოკუმენტი, რომელშიც განმარტებულია დირექტივის კომპონენტებსა და ეროვნულ სტანდარტზე მიღებულ ტრანსპოზიციის ზომების შესაბამის ნაწილებს შორის კავშირი. წინამდებარე დირექტივასთან მიმართებით, კანონმდებელი ამგვარი დოკუმენტების გადაცემას გამართლებულად მიიჩნევს.

(106) (EC) No 45/2001 რეგულაციის 28-ე მუხლის მე-2 ნაწილის შესაბამისად, ევროპის მონაცემთა დაცვის საზედამხედველო ორგანოსთან მოხდა წინასწარი კონსულტაციის გავლა და მან წარმოადგინა 2012 წლის 7 მარტით დათარიღებული მოსაზრება[18].

(107) წინამდებარე დირექტივა არ ზღუდავს წევრ სახელმწიფოებს სისხლის სამართლის საქმის წარმოებისას განახორციელონ მონაცემთა სუბიექტების უფლება ინფორმაციის მიღებაზე, მონაცემებთან წვდომასა და მათ გასწორებაზე ან წაშლაზე და მონაცემთა დაბლოკვაზე, ან შეზღუდონ ეს უფლებები ეროვნული სისხლის სამართლის საპროცესო კანონმდებლობით.

იღებენ წინამდებარე დირექტივას:

თავი I

ზოგადი დებულებები

მუხლი 1

დირექტივის საგანი და მიზნები

1. წინამდებარე დირექტივა განსაზღვრავს კომპეტენტური ორგანოების მიერ დანაშაულის პრევენციის, გამოძიების, დადგენის ან სისხლისსამართლებრივი დევნის, სასჯელთა აღსრულების, ასევე, საზოგადოებრივი უსაფრთხოების წინააღმდეგ მიმართული

[18] OJ C 192, 30.6.2012, გვ. 7.

საფრთხეებისაგან დაცვის მიზნებისათვის პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვის წესებს.

2. წინამდებარე დირექტივის შესაბამისად, წევრმა სახელმწიფოებმა:

(ა) უნდა დაიცვან ფიზიკური პირების ფუნდამენტური უფლებები და თავისუფლებები და განსაკუთრებით პერსონალურ მონაცემთა დაცვის უფლება; და

(ბ) უზრუნველყონ, რომ ევროკავშირის მასშტაბით კომპეტენტურ ორგანოებს შორის პერსონალურ მონაცემთა გაცვლა, როდესაც ამგვარი გაცვლა აუცილებელია ევროკავშირის ან წევრი სახელმწიფოს კანომდებლობით, არ შეიზღუდოს ან აიკრძალოს პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვასთან დაკავშირებული მიზეზით.

3. წინამდებარე დირექტივა არ ზღუდავს წევრ სახელმწიფოებს წინამდებარე დირექტივით კომპეტენტური ორგანოების მიერ პერსონალური მონაცემების დამუშავებისას ფიზიკურ პირთა უფლებებისა და თავისუფლებების დასაცავად განსაზღვრულ გარანტიებზე უფრო მაღალი გარანტიების გასნაზღვრისაგან.

მუხლი 2

მოქმედების სფერო

1. წინამდებარე დირექტივის მოქმედება ვრცელდება კომპეტენტური ორგანოების მიერ პირველი მუხლის პირველი ნაწილით განსაზღვრული მიზნებით პერსონალურ მონაცემთა დამუშავებაზე.

2. წინამდებარე დირექტივის მოქმედება ვრცელდება პერსონალურ მონაცემთა მთლიანად ან ნაწილობრივ ავტომატური საშუალებებით დამუშავებაზე, ასევე, იმ პერსონალური მონაცემების არაავტომატური ან ნახევრადავტომატური საშუალებებით დამუშავებაზე, რომლებიც წარმოადგენენ ფაილური სისტემის ნაწილს ან განკუთვნილია იმისათვის, რომ წარმოადგენდნენ ფაილური სისტემის ნაწილს.

3. წინამდებარე დირექტივის მოქმედება არ ვრცელდება პერსონალური მონაცემების დამუშავებაზე:

(ა) ისეთი საქმიანობის პროცესში, რომელიც სცილდება ევროკავშირის კანომდებლობის იურისდიქციის ფარგლებს;

(ბ) ევროკავშირის ორგანოების, უწყებების, სამსახურებისა და სააგენტობის მიერ.

მუხლი 3

ტერმინთა განმარტება

წინამდებარე დირექტივის მიზნებისათვის:

(1) ‘პერსონალური მონაცემი’ ნიშნავს ნებისმიერ ინფორმაციას, რომელიც უკავშირდება იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს (‘მონაცემთა სუბიექტს’); იდენტიფიცირებადია ფიზიკური პირი, რომლის იდენტიფიცირება შესაძლებელია პირდაპირ ან არაპირდაპირ ისეთ იდენტიფიკატორზე მითითებით, როგორიცაა პირადი ნომერი, ლოკაციის მონაცემი, ონლაინ იდენტიფიკატორი ან ფიზიკური პირის მახასიათებელი ერთი ან მეტი ფიზიკური, ფიზიოლოგიური, გენეტიკური, ფსიქოლოგიური, ეკონომიკური, კულტურული ან სოციალური ნიშანი;

(2) ‘დამუშავება’ ნიშნავს პერსონალური მონაცემების ან მონაცემთა წყების მიმართ შესრულებულ მოქმედებას ან მოქმედებათა ერთობლიობას, როგორც ავტომატური ისე არაავტომატური საშუალებებით, როგორიცააა შეგროვება, ჩაწერა, ორგანიზება, სტრუქტურირება, შენახვა, ადაპტაცია ან შეცვლა, აღდგენა, გაცნობა, გამოყენება, გამჟღავნება მონაცემთა გადაცემის, გავრცელების ან სხვაგვარად ხელმისაწვდომად გახდომის გზით, დაჯგუფება ან კომბინირება, შეზღუდვა, წაშლა ან გადანგურება;

(3) ‘დამუშვების შეზღუდვა’ ნიშნავს შენახული პერსონალური მონაცემების მონიშვნას მომავალში მათი შემდგომი დამუშავების შეზღუდვის მიზნით;

(4) ‘პროფილირება’ ნიშნავს პერსონალურ მონაცემთა ავტომატური დამუშავების ნებისმიერ ფორმას, რომელიც მოიცავს პერსონალური მონაცემების გამოყენებას ფიზიკურ პირთან დაკავშირებული ცალკეული პიროვნული ასპექტების შეფასებისათვის, კერძოდ, ამ ფიზიკური პირის შრომითი უნარების, ეკონომიკური მდგომარეობის, ჯანმრთელობის, უპირატესობების, ინტერესების, სანდოობის, ქცევის, ლოკაციის ან გადაადგილების ანალიზის ან წინასწარ განსაზღვრისთვის;

(5) ‘ფსევდონიმიზაცია’ ნიშნავს მონაცემთა იმგვარად დამუშავებას, რომ შეუძლებელი იყოს პერსონალურ მონაცემთა დაკავშირება კონკრეტულ მონაცემთა სუბიექტთან დამატებითი ინფორმაციის გამოყენების გარეშე იმ პირობით, რომ ასეთი დამატებითი ინფორმაცია შეინახება განცალკევებულად და გატარებულია ტექნიკური და ორგანიზაციული ზომები იმის უზრუნველსაყოფად, რომ შეუძლებელი იყოს პერსონალური მონაცემების დაკავშირება იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირთან;

(6) ‘ფაილური სისტემა’ ნიშნავს მონაცემთა სტრუქტურიზებულ წყებას, რომელშიც ისინი ხელმისაწვდომია კონკრეტული კრიტერიუმის მიხედვით, ცენტრალიზებულად,

დეცენტრალიზებულად, ან გადანაწილებულია ფუნქციური თუ გეოგრაფიული საფუძვლით.

(7) 'კომპეტენტური ორგანო' ნიშნავს:

ა) ნებისმიერ საჯარო უწყებას, რომლის კომპეტენციაში შედის დანაშაულების თავიდან აცილება, გამოძიება, დადგენა ან სისხლისსამართლებრივი დევნა, ან სასჯელის აღსრულება, ასევე, საზოგადოებრივი უსაფრთხოების წინააღმდეგ მიმართული საფრთხეებისაგან დაცვა და მათი პრევენცია; ან

(ბ) ნებისმიერ სხვა ორგანოს ან უწყებას, რომლისთვის წევრ სახელმწიფოს მინდობილი აქვს დანაშაულების თავიდან აცილება, გამოძიება, დადგენა ან სისხლისსამართლებრივი დევნა, ან სასჯელის აღსრულება, ასევე, საზოგადოებრივი უსაფრთხოების წინააღმდეგ მიმართული საფრთხეებისაგან დაცვა და მათი პრევენცია;

(8) 'დამმუშავებელი' ნიშნავს კომპეტენტურ ორგანოს, რომელიც ინდივიდუალურად ან სხვებთან ერთად განსაზღვრავს პერსონალურ მონაცემთა დამუშავების მიზნებსა და საშუალებებს; თუ დამუშავების მიზნები და საშუალებები განსაზღვრულია ევროკავშირის ან მისი წევრი სახელმწიფოს კანონმდებლობით, მონაცემთა დამმუშავებელი ან მისი წარდგენის კონკრეტული კრიტერიუმები შეიძლება განისაზღვროს ევროკავშირის ან მისი წევრი სახელმწიფოს კანონმდებლობით;

(9) "უფლებამოსილი პირი' ნიშნავს ფიზიკურ ან იურიდიულ პირს, საჯარო უწყებას, სააგენტოს ან სხვა ორგანოს, რომელიც ამუშავებს პერსონალურ მონაცემებს მონაცემთა დამმუშავებლის სახელით;

(10) 'მიმღები' ნიშნავს ფიზიკურ ან იურიუდიულ პირს, საჯარო უწყებას, სააგენტოს ან სხვა ორგანოს, რომელსაც გადაეცემა პერსონალური მონაცემები, მიუხედავად იმისა მესამე პირია თუ არა; თუმცა, საჯარო უწყებები, რომლებმაც შესაძლოა მიიღონ პერსონალური მონაცემები კონკრეტული გამოძიების მიმდინარეობის ფარგლებში წევრი სახელმწიფოს კანონმდებლობის შესაბამისად, არ ჩაითვლებიან მიმღებად; ამ საჯარო უწყებების მიერ მონაცემთა დამუშავება უნდა შეესატყვისებოდეს მონაცემთა დაცვის შესაბამის წესებს მათი დამუშავების მიზნების შესაბამისად;

(11) 'პერსონალურ მონაცემთა უსაფრთხოების ინციდენტი' ნიშნავს უსაფრთხოების ინციდენტს, რომელმაც გამოიწვია გადაცემული, შენახული ან სხვაგვარად დამუშავებული მონაცემების შემთხვევითი ან უკანონო განადგურება, დაკარგვა, შეცვლა, უნებართვო გამჟღავნება, ან მათზე უნებართვო წვდომა;

(12) 'გენეტიკური მონაცემი' ნიშნავს პერსონალურ მონაცემს, რომელიც დაკავშირებულია ფიზიკური პირის შეძენილ ან მემკვიდრეობით მიღებულ გენეტიკურ მახასიათებელთან, რომელიც ამ ფიზიკური პირის ბიოლოგიური ნიმუშის ანალიზის შედეგად იძლევა უნიკალურ ინფორმაციას ფიზიკური პირის ფიზიოლოგიის ან ჯანმრთელობის შესახებ;

(13) 'ბიომეტრიული მონაცემი' ნიშნავს კონკრეტული ტექნიკური დამუშავების შედეგად მიღებულ პერსონალურ მონაცემს, რომელიც დაკავშირებულია ფიზიკური პირის ფიზიკურ, ფიზიოლოგიურ ან ქცევით მახასიათებლებთან, რომლებიც იძლევა ამ ფიზიკური პირის უნიკალურად იდენტიფიცირების შესაძლებლობას, მაგალითად სახის გამოსახულება ან დაქტილოსკოპიური მონაცემები.

(14) 'ჯანმრთელობასთან დაკავშირებული მონაცემი' ნიშნავს ფიზიკური პირის ფიზიკურ ან ფსიქიკურ ჯანმრთელობასთან დაკავშირებულ პერსონალურ მონაცემს, მათ შორის ინფორმაციას სამედიცინო მომსახურეობის გაწევის შესახებ, რომელიც იძლევა ინფორმაციას პირის ჯანმრთელობის მდგომარეობის შესახებ.

(15) 'საზედამხედველო ორგანო' ნიშნავს დამოუკიდებელ საჯარო უწყებას, რომელიც შექმნილია წევრი სახელმწიფოს მიერ 41-ე მუხლის შესაბამისად;

(16) 'საერთაშორისო ორგანიზაცია' ნიშნავს საერთაშორისო საჯარო სამართლით რეგულირებად ორგანიზაციას და მის დაქვემდებარებაში მყოფ ორგანოებს ან ნებისმიერ სხვა ორგანოს, რომელიც შექმნილია ორ ან მეტ სახელმწიფოს შორის დადებული შეთანხმებით ან მის საფუძველზე.

თავი II

პრინციპები

მუხლი 4

პერსონალური მონაცემების დამუშავებასთან დაკავშირებული პრინციპები

1. წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ პერსონალური მონაცემები:

(ა) დამუშავდეს კანონიერად და სამართლიანად;

(ბ) შეგროვდეს კონკრეტული, მკაფიო და კანონიერი მიზნისათვის და არ დამუშავდეს ამ მიზანთან შეუთავსებელი მიზნით;

(გ) იყოს დამუშავების მიზნის ადეკვატური, შესაბამისი და პროპორციული;

(დ) იყოს ზუსტი და საჭიროების შემთხვევაში განახლდეს; ყველა გონივრული ზომა უნდა იქნეს მიღებული, რომ უზრუნველყოფილი იყოს არაზუსტი მონაცემების დაუყოვნებლივ წაშლა ან განადგურება, მათი დამუშავების მიზნების გათვალისწინებით;

ე) შენახულ იქნეს ისეთი, ფორმით, რომელიც მონაცემთა სუბიექტის იდენტიფიცირების შესაძლებლობას იძლევა არაუმეტეს იმ ვადით, რაც აუცილებელია მათი დამუშავების მიზნის მისაღწევად;

ვ) დამუშავდეს იმგვარად, რომ უზრუნველყოფილი იყოს პერსონალურ მონაცემთა სათანადო უსაფრთხოება და მათი დაცვა უნებართვო ან უკანონო დამუშავების, შემთხვევითი დაკარგვის, განადგურების ან დაზიანებისაგან, სათანადო ტექნიკური და ორგანიზაციული ზომების გამოყენებით.

2. იმავე ან სხვა მონაცემთა დამმუშავებლის მიერ პირველი მუხლის პირველი პუნქტით გათვალისწინებული მიზნებისაგან განსხვავებული მიზნით მონაცემთა დამუშავება დასაშვებია მხოლოდ იმ შემთხვევაში თუ:

(ა) მონაცემთა დამმუშავებელი უფლებამოსილია დაამუშაოს ასეთი პერსონალური მონაცემები ამგვარი მიზნით ევროკავშირის ან მისი წევრი ქვეყნის კანონმდებლობის შესაბამისად და

(ბ) ევროკავშირის ან მისი წევრი ქვეყნის კანონმდებლობის შესაბამისად დამუშავება აუცილებელი და თავდაპირველი მიზნისგან განსხვავებული მიზნის პროპორციულია;

3. იმავე ან სხვა დამმუშავებლის მიერ დასაშვებია პირველი მუხლის პირველი პუნქტის მიზნებისათვის მონაცემთა დამუშავება საჯარო ინტერესების შესაბამისად არქივირების, სამეცნიერო, სტატისტიკური ან ისტორიული მიზნებისათვის, მონაცემთა სუბიექტების უფლებებისა და თავისუფლებების დაცვის სათანდო გარანტიებით.

4. დამმუშავებელი პასუხისმგებელია ამ მუხლის პირველ, მე-2 და მე-3 პუნქტებთან შესაბამისობაზე და უნდა შეეძლოს მათთან შესაბამისობის დემონსტრირება.

მუხლი 5

შენახვის ვადები და გადასინჯვა

წევრმა სახელმწიფოებმა უნდა უზრუნველყონ პერსონალურ მონაცემთა წაშლის სათანადო ვადების განსაზღვრა და პერსონალური მონაცემების შენახვის საჭიროების პერიოდული გადასინჯვა. პროცედურული ზომებით უზრუნველყოფილი უნდა იყოს ამ ვადების სათანადოდ დაცვა.

მუხლი 6

განსხვავება მონაცემთა სუბიექტების სხვადასხვა კატეგორიებს შორის

წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ მონაცემთა დამმუშავებელმა საჭიროებისამებრ და შეძლებისდაგვარად მკაფიოდ განასხვავონ ერთმანეთისაგან სხვადასხვა კატეგორიის მონაცემთა სუბიექტების პერსონალური მონაცემები, როგორებიც არიან:

(ა) პირები, რომელთა მიმართაც არსებობს საფუძვლიანი ეჭვი, რომ მათ ჩაიდინეს დანაშაული ან აპირებენ დანაშაულის ჩადენას;

(ბ) დანაშაულისათვის მსჯავრდებული პირები;

(გ)) დანაშაულის შედეგად დაზარალებულები ან პირები, რომელთა მიმართაც არსებობს კონკრეტული ფაქტები, რომლებიც იძლევიან ვარაუდის საფუძველს, რომ ისინი შესაძლოა იყვნენ დანაშაულის შედეგად დაზარალებულები; და

(დ) დანაშაულთან დაკავშირებული სხვა მხარეები, როგორებიც არიან დანაშაულთან დაკავშირებით დაკითხვაზე ან შემდგომ სისხლისამართლებრივ პროცედურებზე გამოსაძახებელი პირები ან პირები, რომლებიც შესაძლოა ფლობდნენ ინფორმაციას დანაშაულის შესახებ, ან (ა) და (ბ) ქვეპუნქტებში მითითებული ადამიანების საკონტაქტო ან მათთან კავშირში მყოფი პირები.

მუხლი 7

განსხვავება პერსონალურ მონაცემსა და პერსონალური მონაცემის ხარისხის შემოწმებას შორის

1. წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ მოხდეს ფაქტებზე დაფუძნებული პერსონალური მონაცემების განსხვავება პერსონალური მონაცემებისაგან, რომლებიც პირად შეფასებებს ეფუძნება.

2. წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ კომპეტენტურმა ორგანოებმა მიიღონ ყველა გონივრული ზომა არაზუსტი, არასრული ან განუახლებელი მონაცემების გადაცემის ან ხელმისაწვდომობის თავიდან ასაცილებლად. ამ მიზნით თითოეულმა კომპეტენტურმა ორგანომ, რამდენადაც ეს შესაძლებელია, უნდა შეამოწმოს პერსონალური მონაცემების ხარისხი მათ გადაცემამდე ან ხელმისაწვდომად გახდომამდე. რამდენადაც შესაძლებელია, პერსონალურ მონაცემთა ყოველი გადაცემისას უნდა მიეთითოს აუცილებელი ინფორმაცია, რომელიც შესაძლებლობას მისცემს მიმღებ კომპეტენტურ ორგანოს, შეაფასოს პერსონალურ მონაცემთა სიზუსტის, სრულყოფილებისა და სანდოობის ხარისხი და განახლებულობის ფარგლები.

3. თუ დადგინდება, რომ მოხდა არაზუსტი პერსონალური მონაცემების გადაცემა ან მონაცემთა გადაცემა იყო უკანონო, აღნიშნულის შესახებ დაუყოვნებლივ უნდა შეატყობინო მონაცემთა მიმღებს. ასეთ შემთხვევაში, პერსონალური მონაცემები უნდა გასწორდეს ან წაიშალოს ან მათი დამუშავება უნდა შეიზღუდოს მე-16 მუხლის შესაბამისად.

მუხლი 8

დამუშავების კანონიერება

1. წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ მონაცემთა დამუშავება ჩაითვალოს კანონიერად მხოლოდ იმ შემთხვევაში თუ ის აუცილებელია კომპეტენტური ორგანოს მიერ პირველი მუხლის პირველი პუნქტით განსაზღვრული ამოცანის შესასრულებლად და დამუშავების საფუძველი გათვალისწინებულია ევროკავშირის ან მისი წევრი სახელმწიფოს კანონმდებლობით.

2. წევრი სახელმწიფოს კანონმდებლობა, რომელიც არეგულირებს დამუშავებას მოცემული დირექტივის ფარგლებში, უნდა განსაზღვრავდეს, სულ მცირე, დამუშავების დანიშნულებას, დასამუშავებელ მონაცემებსა და დამუშავების მიზნებს.

მუხლი 9

დამუშავების კონკრეტული პირობები

1. კომპეტენტური ორგანოების მიერ პირველი მუხლის პირველი პუნქტით გათვალისწინებული მიზნებისათვის შეგროვებული მონაცემები არ უნდა დამუშავდეს პირველი მუხლის პირველი პუნქტისაგან განსხვავებული მიზნით გარდა იმ შემთხვევისა, როდესაც ასეთი დამუშავება ნაბადართულია ევროკავშირის ან მისი წევრი სახელმწიფოს კანონმდებლობით. როდესაც მონაცემები მუშავდება ამგვარი განსხვავებული მიზნებით, მათზე გავრცელდება (EU) 2016/679 რეგულაციის დებულებები, გარდა იმ შემთხვევისა, როდესაც დამუშავება ხორციელდება ისეთი საქმიანობის ფარგლებში, რომელზეც არ ვრცელდება ევროკავშირის კანონმდებლობა.

2. როდესაც კომპეტენტური ორგანოები წევრი სახელმწიფოს კანონმდებლობის შესაბამისად ასრულებენ პირველი მუხლის პირველი პუნქტის მიზნებისაგან განსხვავებულ ფუნქციებს, ასეთი მიზნებით დამუშავებაზე გავრცელდება (EU) 2016/679 რეგულაცია, მათ შორის საჯარო ინტერესების შესაბამისად არქივირების, სამეცნიერო ან ისტორიულ-კვლევითი ან სტატისტიკური მიზნებით დამუშავებაზე, გარდა იმ

შემთხვევისა, როდესაც დამუშავება ხორციელდება ისეთი საქმიანობის ფარგლებში, რომელზეც არ ვრცელდება ევროკავშირის კანონმდებლობა.

3. თუ ევროკავშირის ან მისი წევრი სახელმწიფოს კანონმდებლობა, რომელიც ვრცელდება მონაცემთა გადამცემ კომპეტენტურ ორგანოზე, ითვალისწინებს მონაცემთა დამუშავების კონკრეტულ პირობებს, წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ მონაცემთა გადაცემა კომპეტენტურმა ორგანოებმა შეატყობინონ პერსონალურ მონაცემთა მიმღებს ამ პირობებისა და მათი შესრულების სავალდებულო მოთხოვნის შესახებ.

4. წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ მონაცემთა გადამცემმა კომპეტენტურმა ორგანომ არ გაავრცელოს მე-3 პუნქტით გათვალისწინებული მოთხოვნები სხვა წევრ სახელმწიფოებში არსებულ მონაცემთა მიმღებზე, ან სააგენტოებზე, უწყებებზე და ორგანოებზე, რომლებიც შექმნილია ევროკავშირის ფუნქციონირების ხელშეკრულების მე-5 კარის მე-4 და მე-5 თავების შესაბამისად, გარდა იმ შემთხვევისა, როდესაც ეს პირობები ვრცელდება მონაცემთა ამგვარ გადაცემაზე გადამცემი წევრი სახელმწიფოს შიგნით.

მუხლი 10

განსაკუთრებული კატეგორიის მონაცემთა დამუშავება

პირის რასობრივ ან ეთნიკურ წარმომავლობასთან, პოლიტიკურ შეხედულებებთან, რელიგიურ ან ფილოსოფიურ მრწამსთან, პროფესიული კავშირის წევრობასთან დაკავშირებული მონაცემების დამუშავება, გენეტიკური მონაცემების და ბიომეტრიული მონაცემების დამუშავება პირის უნიკალურად იდენტიფიცირების მიზნისათვის, ჯანმრთელობასთან დაკავშირებული მონაცემების ან ფიზიკური პირის სქესობრივ ცხოვრებასთან ან სექსუალურ ორიენტაციასთან დაკავშირებული მონაცემების დამუშავება დასაშვებია მხოლოდ იმ შემთხვევაში, თუ ეს აუცილებელია, მიღებულია მონაცემთა სუბიექტის უფლებებისა და თავისუფლებების დაცვის სათანადო ზომები და დამუშავება:

(ა) ნებადართულია ევროკავშირის ან წევრი სახელმწიფოს კანონმდებლობით;

(ბ) საჭიროა მონაცემთა სუბიექტის ან სხვა ფიზიკური პირის სასიცოცხლო ინტერესების დასაცავად; ან

(გ) დაკავშირებულია მონაცემებთან, რომლებიც მონაცემთა სუბიექტმა თავად გაასაჯაროვა მათი დამუშავების აშკარა აკრალვის გარეშე.

მუხლი 11

ავტომატური ინდივიდუალური გადაწყვეტილების მიღება

წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ გადაწყვეტილება, რომელიც მხოლოდ ავტომატური დამუშავების შედეგადაა მიღებული, მათ შრის პროფილირება, რომელიც მონაცემთა სუბიექტისათვის წარმოშობს უარყოფით შედეგს ან მნიშვნელოვან გავლენას ახდენს მასზე, აიკრძალოს, გარდა იმ შემთხვევისა, როდესაც ეს დაშვებულია ევროკავშირის ან წევრი სახელმწიფოს კანონმდებლობით, რომელიც ვრცელდება მონაცემთა დამმუშავებელზე და რომელიც უზრუნველყოფს მონაცემთა სუბიექტის უფლებებისა და თავისუფლებების დაცვის სათანადო გარანტიებს, სულ მცირე, მონაცემთა დამმუშავებლის მხრიდან ადამიანური რესურსის გამოყენების მოთხოვნის უფლებას.

2. ამ მუხლის პირველ პუნქტში მითითებული გადაწყვეტილებების მიღება არ უნდა მოხდეს მე-10 მუხლით გათვალისწინებული განსაკუთრებული კატეგორიის მონაცემთა დამუშავების საფუძველზე, გარდა იმ შემთხვევისა, როდესაც მიღებულია მონაცემთა სუბიექტის უფლებების, თავისუფლებებისა და ლეგიტიმური ინტერესების დაცვის სათანადო ზომები.

3. პროფილირება, რომლის შედეგადაც ადგილი აქვს ფიზიკური პირების დისკრიმინაციას მე-10 მუხლში მითითებული განსაკუთებული კატეგორიის მონაცემების საფუძველზე, დაუშვებელია, ევროკავშირის კანონმდებლობის შესაბამისად.

თავი III

მონაცემთა სუბიექტის უფლებები

მუხლი 12

კომუნიკაცია და მონაცემთა სუბიექტის უფლებების განხორციელების საშუალებები

1. წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ მონაცემთა დამმუშავებელმა მიიღოს გონივრული ზომები მონაცემთა სუბიექტისათვის მე-13 მუხლით გათვალისწინებული ინფორმაციის მისაწოდებლად და მე-11, მე-14, მე-18 და 31-ე მუხლებთან მიმართებით განახორციელოს მასთან ნებისმიერი კომუნიკაცია, რომელიც დაკავშირებულია მონაცემთა დამუშავებასთან მკაფიო, გასაგები და იოლად ხელმისაწვდომი ფორმით, ნათელი და მარტივი ენის გამოყენებით. ინფორმაცია წარდგენილი უნდა იყოს ნებისმიერი სათანადო საშუალებით, მათ შორის ელექტრონულად. როგორც წესი, მონაცემთა დამმუშავებელმა ინფორმაცია უნდა გასცეს იმავე ფორმით, რა ფორმითაც მიიღო მოთხოვნა.

2. წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ მონაცემთა დამმუშავებლებმა ხელი შეუწყონ მონაცემთა სუბუექტის მე-11 მუხლით და მე-14-მე-18 მუხლებით გათვალისწინებული უფლებების განხორციელებას.

3. წევრმა სახელმწიფოებმა უნდა უზრუნველონ, რომ მონაცემთა დამმუშავებელმა წერილობითი ფორმით დაუყოვნებლივ შეატყობინოს მონაცემთა სუბიექტს მისი მოთხოვნის განხილვის შედეგები.

4. წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ მე-13 მუხლის საფუძველზე ინფორმაციის წარდგენა და მე-11 მუხლით და მე-14-მე-18 მუხლებით გათვალისწინებული ნებისმიერი კომუნიკაცია ან მიღებული ზომა განხორციელდეს უფასოდ. იმ შემთხვევაში, თუ მონაცემთა სუბიექტის მოთხოვნები აშკარად უსაფუძვლო ან გადაჭარბებულია, განსაკუთრებით კი თუ ერთი და იგივე მოთხოვნა განმეორებითი ხასიათისაა, მონაცემთა დამმუშავებელი უფლებამოსილია:

(ა) დააწესოს გონივრული საფასური ინფორმაციის წარდგენის, კომუნიკაციის ან მოთხოვნილი ზომის მიღების ადმინისტრაციული ხარჯის გათვალისწინებით; ან

(ბ) უარი თქვას მოთხოვნის შესრულებაზე;

დამმუშავებელს ეკისრება მოთხოვნის აშკარა უსაფუძვლობის ან გადაჭარბების დემონსტრირების მტკიცების ტვირთი.

5. თუ მონაცემთა დამმუშავებელს გონივრული ეჭვი აქვს მე-14 ან მე-16 მუხლებით გათვალისწინებული მოთხოვნის წარმდგენი ფიზიკური პირის ვინაობის მიმართ, მონაცემთა დამმუშავებელი უფლებამოსილია, მოითხოვოს დამატებითი ინფორმაციის წარდგენა, რომელიც აუცილებელია მონაცემთა სუბიექტის ვინაობის დასადასტურებლად.

მუხლი 13

ინფორმაცია, რომელიც ხელმისაწვდომი უნდა იყოს მონაცემთა სუბიექტისათვის ან უნდა გადაეცეს მონაცემთა სუბიექტს

1. წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ მონაცემთა დამმუშავებელმა მონაცემთა სუბიექტისათვის ხელმისაწვდომი გახადოს, სულ მცირე, შემდეგი ინფორმაცია:

(ა) მონაცემთა დამმუშავებლის ვინაობა და საკონტაქტო მონაცემები;

(ბ) მონაცემთა დაცვის ოფიცრის საკონტაქტო მონაცემები, ასეთის არსებობის შემთხვევაში;

(გ) მონაცემთა დამუშავების მიზნები, რომლებისთვისაც მუშავდება პერსონალური მონაცემები;

დ) საზედამხედველო ორგანოსათვის საჩივრით მიმართვის უფლება და საზედამხედველო ორგანოს საკონტაქტო მონაცემები;

(ე) ინფორმაცია მონაცემთა სუბიექტთან დაკავშირებულ მონაცემებთან წვდომის, მათი გასწორების, წაშლის ან დამუშავების შეზღუდვის მოთხოვნის დამმუშავებლისათვის წარდგენის უფლების არსებობის შესახებ.

2. გარდა პირველი პუნქტით გათვალისწინებული ინფორმაციისა, წევრმა სახელმწიფოებმა კანონმდებლობით უნდა უზრუნველყონ, რომ მონაცემთა დამმუშავებელმა მონაცემთა სუბიექტს კონკრეტულ შემთხვევებში გადასცეს შემდეგი დამატებითი ინფორმაცია მისი უფლებების განსახორციელებლად:

(ა) დამუშავების სამართლებრივი საფუძველი;

(ბ) მონაცემთა შენახვის ვადა, ან თუ ასეთი ვადის განსაზღვრა შეუძლებელია, კრიტერიუმი, რომლებიც გამოიყენება ვადის დასადგენად;

(გ) შესაძლებლობის შემთხვევაში, პერსონალური მონაცემების მიმღებთა კატეგორიები, მათ შორის მესამე სახელმწიფოებსა და საერთასორისო ორგანიზაციებში;

(დ) საჭიროების შემთხვევაში დამატებითი ინფორმაცია, განსაკუთრებით, თუ მონაცემების შეგროვება ხდება მონაცემთა სუბიექტის ინფორმირებულობის გარეშე.

3. წევრ სახელმწიფოებს უფლება აქვთ, მიიღონ ისეთი საკანონმდებლო ზომები, რომლებიც აფერხებს, ზღუდავს ან გამორიცხავს მე-2 პუნქტის შესაბამისად მონაცემთა სუბიექტისათვის ინფორმაციის გადაცემას მხოლოდ იმ შემთხვევაში და იმ პირობით, რომ ასეთი ზომები წარმოადგენს აუცილებელ და პროპორციულ ზომას დემოკრატიულ საზოგადოებაში და სათანადოდ იქნება გათვალისწინებული დაინტერესებული ფიზიკური პირის ფუნდამენტური უფლებები და ლეგიტიმური ინტერესები, შემდეგი მიზნებისათვის:

(ა) ოფიციალური ან სამართლებრივი მოკვლევისათვის, გამოძიებისათვის ან პროცედურებისათვის ხელის შეშლის პრევენციის მიზნით;

(ბ) დანაშაულის პრევენციის, დადგენის, გამოძიების ან სისხლისსამართლებრივი დევნის ან სასჯელის აღსრულებისათვის ხელის შეშლის თავიდან ასაცილებლად;

(გ) საზოგადოებრივი უსაფრთხოების დასაცავად;

(დ) ეროვნული უსაფრთხოების დასაცავად;

(ე) სხვათა უფლებებისა და თავისუფლებების დასაცავად;

4. წევრ სახელმწიფოებს შუძლიათ, მიიღონ სამართლებრივი ზომები იმისათვის, რომ განსაზღვრონ დამუშავების კატეგორიები, რომლებზეც მთლიანად ან ნაწილობრივ ვრცელდება მე-3 პუნქტის რომელიმე ქვეპუნქტი.

მუხლი14

მონაცემებთან წვდომის უფლება

მე-15 მუხლის შეზღუდვების გათვალისწინებით, წევრმა სახელმწოფებმა უნდა უზრუნველყონ, რომ მონაცემთა სუბიექტს ჰქონდეს უფლება, მონაცემთა დამმუშავებლისაგან მიიღოს დადასტურება, მუშავდება თუ არა მისი პერსონალური მონაცემები, ხოლო დამუშავების შემთხვევაში ჰქონდეს წვდომა პერსონალურ მონაცემებსა და შემდეგ ინფორმაციაზე:

(ა) დამუშავების მიზნები და სამართლებრივი საფუძვლები;

(ბ) დამუშავებულ პერსონალურ მონაცემთა კატეგორიები;

(გ) მონაცემთა მიმღების ვინაობა ან მიმღებთა კატეგორიები, რომელთაც გადაეცათ პერსონალური მონაცემები, განსაკუთრებით თუ მიმღები მესამე სახელმწიფო ან საერთაშორისო ორგანიზაციაა;

(დ) შესაძლებლობის შემთხვევაში მონაცემთა შენახვის დადგენილი ვადა, ან თუ ეს შეუძლებელია, კრიტერიუმები, რომლებიც გამოიყენება ვადის დასადგენად;

(ე) მონაცემთა სუბიექტთან დაკავშირებული პერსონალური მონაცემების გასწორების, წაშლის ან მათი დამუშავების შეზღუდვის მოთხოვნის მონაცემთა დამმუშავებლისათვის წარდგენის უფლების არსებობა:

(ვ) საზედამხდველო ორგანოსათვის საჩივრით მიმართვის უფლების არსებობა და საზედამხედველო ორგანოს საკონტაქტო მონაცემები;

(ზ) დამუშავების პროცესში მყოფი პერსონალური მონაცემები და ნებისმიერი ხელმისაწვდომი ინფორმაცია მათი წარმომავლობის შსახებ.

მუხლი 15

მონაცემებთან წვდომის უფლების შეზღუდვა

1. წევრ სახელმწიფოებს უფლება აქვთ, მიიღონ ისეთი საკანონმდებლო ზომები, რომლებიც მთლიანად ან ნაწილობრივ ზღუდავს მონაცემთა სუბიექტის უფლებას მონაცემებთან წვდომაზე მხოლოდ იმ შემთხვევაში და იმ პირობით, თუ მთლიანი ან ნაწილობრივი შეზღუდვა წარმოადგენს აუცილებელ და პროპორციულ ზომას

დემოკრატიულ საზოგადოებაში და სათანადოდაა დაცული ფიზიკური პირის ფუნდამენტური უფლებები და ლეგიტიმური ინტერესები შემდეგი მიზნებისათვის:

(ა) ოფიციალური ან სამართლებრივი მოკვლევისათვის, გამოძიებისათვის ან პროცედურებისათვის ხელის შეშლის თავიდან ასაცილებლად;

(ბ) დანაშაულის პრევენციის, დადგენის, გამოძიების ან სისხლისსამართლებრივი დევნის ან სასჯელის აღსრულების შეფერხების თავიდან ასაცილებლად;

(გ) საზოგადოებრივი უსაფრთხოების დასაცავად;

(დ) ეროვნული უსაფრთხოების დასაცავად;

(ე) სხვათა უფლებებისა და თავისუფლებების დასაცავად.

2. წევრ სახელმწიფოებს უფლება აქვთ, მიიღონ საკანონმდებლო ზომები იმისათვის, რომ განსაზღვრონ დამუშავების კატეგორიები, რომლებზეც მთლიანად ან ნაწილობრივ ვრცელდება პირველი პუნქტის ა-ე ქვეპუნქტები.

3. პირველი და მე-2 პუნქტებით გათვალისწინებულ შემთხვევებში წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ დამმუშავებელმა მონაცემთა სუბიექტს დაუყოვნებლივ წერილობითი ფორმით შეატყობინოს მის მოთხოვნაზე უარის თქმის ან მონაცემებთან წვდომის შეზღუდვის, ასევე უარის თქმისა და შეზღუდვის მიზეზების შესახებ. ინფორმაციის მიწოდება არ არის სავალდებულო თუ მისი მიწოდება ხელს შეუშლის პირველი პუნქტით გათვალისწინებული მიზნების მიღწევას. წევრმა სახელმწიფოებმა უნდა უზრუნრველყონ, რომ დამმუშავებელმა მონაცემთა სუბიექტს შეატყობინოს საზედამხედველო ორგანოსთვის საჩივრით მიმართვის უფლების ან დარღვეული უფლების სასამართლო წესით აღდგენის შესაძლებლობის შესახებ.

4. წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ დამმუშავებელმა დოკუმენტურად აღრიცხოს ის ფაქტობრივი და სამართლებრივი მიზეზები, რომლებიც საფუძვლად დაედო გადაწყვეტილებას. ეს ინფორმაცია ხელმისაწვდომი უნდა გახდეს საზედამხედველო ორგანოებისათვის.

მუხლი 16

პერსონალურ მონაცემთა გასწორების ან წაშლისა და მონაცემთა დამუშავების შეზღუდვის უფლება

1. წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ მონაცემთა სუბიექტს ჰქონდეს უფლება, დამმუშავებლისაგან დაუყოვნებლივ მოითხოვოს მასთან დაკავშირებული არასწორი პერსონალური მონაცემების გასწორება. დამუშავების მიზნების

გათვალისწინებით წევრმა სახელმწიფოებმა უნდა უზრუნველყონ მონაცემთა სუბიექტის უფლება, მოითხოვოს არასრული პერსონალური მონაცემების შევსება, მათ შორის, დამატებითი განაცხადის წარდგენის გზით.

2. წევრმა სახელმწიფოებმა უნდა დაავალდებულონ მონაცემთა დამმუშავებელი, დაუყოვნებლივ წაშალოს პერსონალური მონაცემები და უზუნრველყონ, რომ მონაცემთა სუბიექტს ჰქონდეს უფლება, დამმუშავებლისაგან მოითხოვოს მასთან დაკავშირებული პერსონალური მონაცემების დაუყოვნებლივ წაშლა, როდესაც დამუშავება ეწინააღმდეგება მე-4, მე-8 ან მე-10 მუხლით დადგენილ დებულებებს, ან როდესაც პერსონალური მონაცემები უნდა წაიშალოს მონაცემთა დამმუშავებლის მიერ მისთვის კანონმდებლობით დაკისრებული მოვალეობების შესასრულებლად;

3. წაშლის ნაცვლად მონაცემთა დამმუშვებელმა უნდა დაბლოკოს მონაცემები როდესაც:

(ა) მონაცემთა სუბიექტი სადავოდ ხდის მონაცემების სიზუსტეს და მათი სიზუსტის ან უზუსტობის დადგენა შეუძლებელია; ან

(ბ) მონაცემები შენახულ უნდა იქნეს მტკიცებულებად გამოყენების მიზნისათვის.

თუ მონაცემები დაბლოკოლია ამ პუნქტის (ა) ქ/პუნქტის შესაბამისად, დამმუშავებელმა შეზღუდვის მოხსნამდე უნდა აცნობოს მონაცემთა სუბიექტს დაბლოკვის შესახებ მიღებული გადაწყვეტილების გაუქმების თაობაზე.

4. წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ დამმუშავებელმა წერილობით შეატყობინოს მონაცემთა სუბიექტს მონაცემთა გასწორების, წაშლის ან დაბლოკვის უფლების შეზღუდვის და ამ შეზღუდვის მიზეზის შესახებ. წევრ სახელმწიფოებს უფლება აქვთ მიიღონ ისეთი საკანონმდებლო ზომები, რომლებიც მთლიანად ან ნაწილობრივ ზღუდავს მონაცემთა სუბიექტის უფლებას მონაცემებთან წვდომაზე მხოლოდ იმ შემთხვევაში და იმ პირობით, თუ მთლიანი ან ნაწილობრივი შეზღუდვა წარმოადგენს აუცილებელ და პროპორციულ ზომას დემოკრატიულ საზოგადოებაში და სათნადოდაა დაცული ფიზიკური პირის ფუნდამენტური უფლებები და ლეგიტიმური ინტერესები შემდეგი მიზნებისათვის:

(ა) თავიდან იქნეს აცილებული ოფიციალური ან სამართლებრივი მოკვლევისათვის, გამოძიებისათვის ან პროცედურებისათვის ხელის შეშლა;

(ბ) თავიდან იქნეს აცილებული დანაშაულის პრევენციის, დადგენის, გამოძიების ან სისხლისსამართლებრივი დევნის ან სასჯელის აღსრულების შეფერხება;

(გ) საზოგადოებრივი უსაფრთხოების დასაცავად;

(დ) ეროვნული უსაფრთხოების დასაცავად;

(ე) სხვათა უფლებებისა და თავისუფლებების დასაცავად.

სახელმწიფოებმა უნდა უზრუნველყონ, რომ დამმუშავებელმა მონაცემთა სუბიექტს შეატყობინოს საზედამხედველო ორგანოსათვის საჩივრით მიმართვის უფლების ან დარღვეული უფლების სასამართლო წესით აღდგენის შესაძლებლობის შესახებ.

5. წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ დამმუშავებელმა არაზუსტი მონაცემების გასწორების შესახებ შეატყობინოს კომპეტენტურ ორგანოს, რომელიც წარმოადგენდა არაზუსტი პერსონალური მონაცემების წყაროს.

6. თუ პერსონალური მონაცემები გასწორდა, წაიშალა ან დაიბლოკა პირველი, მე-2 და მე-3 პუნქტების შესაბამისად, წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ დამმუშავებელმა შეატყობინოს მონაცემთა მიმღებს, ხოლო მიმღებმა უნდა გაასწოროს, წაშალოს ან დაბლოკოს მათი პასუხისმგებლობის ქვეშ არსებული პერსონალური მონაცემები.

მუხლი 17

მონაცემთა სუბიექტის მიერ უფლებების განხორციელება და საზედამხედველო ორგანოს მიერ შემოწმება

1. მე-13 მუხლის მე-3 პუნქტით, მე-15 მუხლის მე-3 პუნქტით და მე-16 მუხლის მე-4 პუნქტით დადგენილ შემთხვევებში წევრმა სახელმწიფოებმა უნდა მიიღონ ზომები, იმისათვის, რომ უზრუნველყოფილი იყოს მონაცემთა სუბიექტის მიერ მისი უფლებების საზედამხედველო ორგანოს მეშვეობით განხორციელება.

2. წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ დამმუშავებელმა შეატყობინოს მონაცემთა სუბიექტს მისი უფლებების საზედამხევდელო ორგანოს მეშვეობით განხორციელების შესაძლებლობის შესახებ პირველი პუნქტის შესაბამისად.

3. თუ ადგილი აქვს პირველი პუნქტით დადგენილი უფლების განხორციელებას, საზედამხედველო ორგანომ უნდა შეატყობინოს მონაცემთა სუბიექტს სულ მცირე ის, რომ საზედამხედველო ორგანომ ჩაატარა ყველა საჭირო შემოწმება ან განხილვა. საზედამხედველო ორგანომ ასევე უნდა შეატყობინოს მონაცემთა სუბიექტს დარღვეული უფლების სასამართლოს წესით აღდეგნის უფლების შესახებ.

მუხლი 18

მონაცემთა სუბიექტის უფლებები სისხლის სამართლის საქმის გამოძიებისას და პროცესში

თუ პერსონალურ მონაცემებს შეიცავს განაჩენი ან საქმის გამოძიების ან წარმოებისას დამუშავებული სისხლის სამართლის საქმე, სახელწიფოებს უფლება აქვთ, რომ მე-13, მე-14 და მე-16 მუხლებით გათვალისწინებული უფლებების განხორციელება მოხდეს წევრი სახელმწიფოს კანონმდებლობის შესაბამისად.

თავი IV

დამმუშავებელი და უფლებამოსილი პირი

ნაწილი 1

ზოგადი ვალდებულებები

მუხლი 19

დამმუშავებლის ვალდებულებები

1. დამუშავების ხასიათის, მოცულობის, კონტექსტის და მიზნების, ასევე ფიზიკური პირების უფლებებისა და თავისუფლებების შელახვის რისკების გათვალისწინებით წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ მონაცემთა დამმუშავებელმა მიიღოს სათანადო ტექნიკური და ორგანიზაციული ზომები, რომ შეძლოს მონაცემთა დამუშავების წინამდებარე დირექტივასთან შესაბამისობის დემონსტრირება. ეს ზომები საჭიროებისამებრ უნდა გადაისინჯოს და განახლდეს.

2. პირველი პუნქტით გათვალისწინებული ზომები უნდა მოიცავდეს დამმუშავებლის მიერ მონაცემთა დამუშავების პოლიტიკის შემუშავებას, თუ ეს დამუშავების ოპერაციების პროპორციულია.

მუხლი 20

მონაცემთა დაცვის სტანდარტების გათვალისწინება ახალი პროდუქტის ან მომსახურების შექმნისას და მონაცემთა დაცვა როგორც პირველადი პარამეტრი

1. წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ მონაცემთა დამმუშავებელმა თანამედროვე მეთოდების, ხარჯების, დამუშავების ხასიათის, მოცულობის და მიზნების, ასევე დამუშავების შედეგად მონაცემთა სუბიექტის უფლებებისა და თავისუფლებების დარღვევის განსხვავებული და სხვადასხვა სიმძიმის რისკების გათვალისწინებით, მონაცემთა დამუშავების საშუალებების განსაზღვრამდე და უშუალოდ დამუშავების პროცესში დანერგოს ისეთი ტექნიკური და ორგანიზაციული ზომები, როგორიცაა ფსევდონიმიზაცია, რომელიც უზრუნველყოფს მონაცემთა დამუშავების პრინციპების (როგორიცაა მონაცემთა მინიმიზაცია_ეფექტურ იმპლემენტაციას და მოახდინოს დაცვის

საჭირო გარანტიების ინტეგრირება დამუშავების პროცესში წინამდებარე დირექტივის მოთხოვნებთან შესაბამისობისა და მონაცემთა სუბიექტების უფლებების დაცვისათვის.

2. წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ მონაცემთა დამმუშავებლის მიერ შემუშავებული ტექნიკური და ორგანიზაციული ზომები უზრუნველყოფდნენ პირველად პარამეტრად მხოლოდ იმ მონაცემების დამუშავებას, რაც აუცილებელია მონაცემთა დამუშავების კონკრეტული მიზნის მისაღწევად. ეს ვალდებულება ვრცელდება შეგროვებული პერსონალური მონაცემების რაოდენობაზე, დამუშავების მოცულობაზე, შენახვის ვადასა და მათ ხელმისაწვდომობაზე. კერძოდ, ასეთი ზომები პირველად პარამეტრად უნდა უზრუნველყოფდნენ, რომ ფიზიკური პირის მოქმედების გარეშე პერსონალური მონაცემები არ გახდეს ხელმისაწვდომი ფიზიკურ პირთა განუსაზღვრელი წრისთვის.

მუხლი 21

თანადამმუშავებლები

1. როდესაც მონაცემთა დამუშავების მიზნებსა და საშუალებებს ორი ან მეტი დამმუშავებელი ერთობლივად განსაზღვრავს, წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ ისინი იყვნენ მონაცემთა თანადამმუშავებლები. თანადამმუშავებლებმა გამჭვირვალედ უნდა განსაზღვრონ მათი ვალდებულებები ამ დირექტივასთან შესაბამისობის კუთხით, მათ შორის მონაცემთა სუბიექტის უფლებების განხორციელებასთან და მე-13 მუხლით გათვალისწინებული ინფორმაციის წარდგენის ვალდებულებასთან დაკავშირებით, შეთანხმების ფორმით, გარდა იმ შემთხვევისა, როდესაც დამმუშავებლების შესაბამისი ვალდებულებები დადგენილია ევროკავშირის ან წევრი სახელმწიფოს კანონმდებლობით, რომელიც ვრცელდება დამმუშავებლებზე. შეთანხმება უნდა განსაზღვრავდეს საკონტაქტო პირს მონაცემთა სუბიექტებისათვის. წევრ სახელმწიფოებს უფლება აქვთ, განსაზღვრონ, რომელი დამმუშავებელი შეასრულებს მონაცემთა სუბიექტისათვის საკონტაქტო პირის ფუნქციას მათი უფლებების განხორციელების მიზნით.

2. მიუხედავად პირველი პუნქტით გათვალისწინებული შეთანხმების პირობებისა, წევრ სახელმწიფოებს უფლება აქვთ, ნება დართონ მონაცემთა სუბიექტს, განახორციელოს წინამდებარე დირექტივის შესაბამისად მიღებული დებულებებით გათვალისწინებული მისი უფლებები თითოეულ თანადამმუშავებელთან ინდივიდულაურად ან მის წინააღმდეგ.

მუხლი 22

უფლებამოსილი პირი

1. როდესაც დამუშავება დამმუშავებლის სახელით უნდა განხორციელდეს, წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ დამმუშავებელმა გამოიყენოს მხოლოდ ისეთი უფლებამოსილი პირი, რომელიც წარმოადგენს საკმარის გარანტიებს სათანადო ტექნიკური და ორგანიზაციული ზომების იმპლემენტაციისათვის იმგვარად, რომ დამუშავება შესაბამისობაში იყოს წინამდებარე დირექტივის მოთხოვნებთან და უზრუნველყოფდეს მონაცემთა სუბიექტის უფლებების დაცვას.

2. წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ უფლებამოსილმა პირმა დამუშავების პროცესში დამმუშავებლის წინასწარი კონკრეტული ან ზოგადი წერილობითი ნებართვის გარეშე არ ჩართოს დამუშავებაში სხვა უფლებამოსილი პირი. ზოგადი წერილობითი თანხმობის შემთხვევაში, უფლებამოსილი პირი ვალდებულია შეატყობინოს დამმუშავებელს სხვა უფლებამოსილი პირის დამატებასთან ან ჩანაცვლებასთან დაკავშირებული დაგეგმილი ცვლილების შესახებ, რითაც დამმუშავებელს მისცემს ასეთი ცვლილებების გაპროტესტების შესაძლებლობას.

3. წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ უფლებამოსილი პირის მიერ მონაცემთა დამუშავება რეგულირდებოდეს ხელშეკრულებით ან ევროკავშირის ან მისი წევრი სახელმწიფოს კანონმდებლობით განსაზღვრული სხვა სამართლებრივი აქტით, რომელიც უფლებამოსილი პირისათვის დამმუშავებელთან მიმართებით შესასრულებლად სავალდებულოა და რომელშიც გაწერილია დამუშავების საკითხი, ხანგრძლივობა, პერსონალურ მონაცემთა სახეები და მონაცემთა სუბიექტების კატეგორიები, ასევე დამმუშავებლის ვალდებულებები და უფლებამოსილებები. ხელშეკრულება ან სხვა სამართლებრივი აქტი კერძოდ უნდა ითვალისწინებდეს, რომ უფლებამოსილი პირი:

(ა) იმოქმედებს მხოლოდ დამმუშავებლის დავალების საფუძველზე;

(ბ) უზრუნველყოფს, რომ იმ პირებს, რომლებიც უშუალოდ მონაწილეობენ მონაცემთა დამუშავებაში, აღებული ჰქონდეთ კონფიდენციალურობის დაცვის ვალდებულება ან ეკისრებოდეთ კონფიდენციალურობის დაცვის შესაბამისი კანონისმიერი ვალდებულება;

(გ) სათანადო საშუალებების გამოყენებით დაეხმარება დამმუშავებელს მონაცემთა სუბიექტის უფლებებთან დაკავშირებული დებულებების შესრულების უზრუნველყოფაში;

(დ) მონაცემების დამუშავებასთან დაკავშირებული მომსახურების გაწევის შემდეგ, დამმუშავებლის არჩევანით, წაშლის ან დაუბრუნებს დამმუშავებელს პერსონალურ მონაცემებს და წაშლის მასთან არსებულ ასლებს, თუ ევროკავშირის ან წევრი სახელმწიფოს კანონმდებლობით პერსონალურ მონაცემთა შენახვა არ არის გათვალისწინებული;

(ე) მონაცემთა დამმუშავებელს მიაწვდის ყველა ინფორმაციას, რომელიც აუცილებელია ამ მუხლით დადგენილ ვალდებულებებთან შესაბამისობის დემონსტრირებისათვის;

(ვ) შეასრულებს სხვა უფლებამოსილი პირის დამუშავებაში ჩართვასთან დაკავშირებით მე-2 და მე-3 პუნქტებით გათვალისწინებულ პირობებს.

4. მე-3 პუნქტით გათვალისწინებული ხელშეკრულება ან სხვა სამართლებრივი აქტი უნდა გაფორმდეს წერილობით, მათ შორის ელექტრონულად.

5. თუ წინამდებარე დირექტივის დარღვევით უფლებამოსილი პირი თავად განსაზღვრავს დამუშავების მიზნებსა და საშუალებებს, ეს უფლებამოსილი პირი ჩაითვლება დამმუშავებლად ამ დამუშავებასთან მიმართებით.

მუხლი 23

დამუშავება დამმუშავებლის ან უფლებამოსილი პირის ნებართვით

წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ ნებისმიერმა პირმა, რომელიც დამმუშავებლის ან უფლებამოსილი პირის სახელით მოქმედებს და აქვს წვდომა პერსონალურ მონაცემებზე, ეს მონაცემები დაამუშაოს მხოლოდ დამმუშავებლის დავალების საფუძველზე, გარდა იმ შემთხვევისა, როდესაც დამუშავების ვალდებულება ევროკავშირის ან წევრი სახელმწიფოს კანონმდებლობით აკისრია.

მუხლი 24

მონაცემთა დამუშავების აღრიცხვა

1. წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ დამმუშავებელმა აღრიცხოს მისი პასუხისმგებლობის ქვეშ არსებული დამუშავების ყველა კატეგორიები. რეესტრი უნდა შეიცავდეს ყველა შემდეგ ინფორმაციას:

(ა) დამმუშავებლის, თანადამმუშავებლის, ასეთის არსებობის შემთხვევაში და მონაცემთა დაცვის ოფიცრის დასახელება და საკონტაქტო მონაცემები;

(ბ) დამუშავების მიზნები;

(გ) მონაცემთა მიმღების კატეგორიები, რომელთაც გადაეცათ ან გადეცემათ მონაცემები, მათ შორის ის მიმღებნი, რომლებიც მესამე სახელმწიფოებში იმყოფებიან და საერთაშორისო ორგანიზაციები;

(დ) მონაცემთა სუბიექტის კატეგორიებისა და პერსონალური მონაცემების კატეგორიების აღწერა;

(ე) ინფორმაცია პროფილირების შესახებ, ასეთის გამოყენების შემთხვევაში;

(ვ) მესამე სახელმწიფოს ან საერთაშორისო ორგანიზაციისათვის მონაცემთა გადაცემის კატეგორიები, ასეთი გადაცემის შემთხვევაში;

(ზ) დამუშავების, მათ შორის, მონაცემთა გადაცემის, სამართლებრივი საფუძველი, რომლისთვისაც გროვდება მონაცემები;

(თ) შესაძლებლობის შემთხვევაში, სხვადასხვა კატეგორიის პერსონალური მონაცემების წაშლის ვადები;

(ი) შესაძლებლობის შემთხვევაში, 29-ე მუხლის პირველი პუნქტით გათვალისწინებული უსაფრთხოების ტექნიკური და ორგანიზაციული ზომების ზოგადი აღწერა.

2. წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ უფლებამოსილმა პირმა აწარმოოს დამმუშავებლის სახელით განხორციელებული ყველა კატეგორიის დამუშავების რეესტრი, რომელიც შეიცავს:

(ა) უფლებამოსილი პირის ან პირების, თითოეული დამმუშავებლის, რომლის სახელითაც მოქმედებს უფლებამოსილი პირი და მონაცემთა დაცვის ოფიცრის (ასეთის არსებობის შემთხვევაში) დასახელებას და საკონტაქტო მონაცემებს;

(ბ) თითეული დამმუშავებლის სახელით განხორციელებული დამუშავების კატეგორიებს;

(გ) ინფორმაციას დამმუშავებლის პირდაპირი დავალების საფუძველზე პერსონალური მონაცემების მესამე სახელწმიფოში ან საერთაშორისო ორგანიზაციაში გადაცემის შესახებ, მათ შორის, ინფორმაციას მესამე სახლემწიფოს ან საერთაშორისო ორგანიზაციის დასახელების შესახებ;

(დ) შესაძლებლობის შემთხვევაში 29-ე მუხლის პირველი პუნქტით გათვალისწინებული უსაფრთხოების ტექნიკური და ორგანიზაციული ზომების ზოგად აღწერას.

3. პირველი და მე-2 პუნქტებით გათვალისწინებული რეესტრი უნდა აღირიცხოს წერილობით, მათ შორის ელექტრონულად.

დამმუშავებელი და უფლებამოსილი პირი ვალდებულია რეესტრის მონაცემები მიაწოდოს საზედამხედველო ორგანოს მისი მოთხოვნისამებრ.

მუხლი 25

ლოგირება

1. წევრმა სახელმწიფოებმა უნდა უზრუნრველყონ, რომ შენახულ იქნეს სულ მცირე შემდეგი დამუშავების ოპერაციების ლოგები ავტომატური დამუშვების სისტემებში: მონაცემთა შეგროვება, შეცვლა, გაცნობა, გადაცემა, მათ შორის საერთაშორისო გადაცემა, კომბინირება და წაშლა. მონაცემთა გაცნობისა და გადაცემის ლოგები შესაძლებლობას უნდა იძლეოდეს, რომ დადგინდეს ასეთი ოპერაციების საფუძველი, თარიღი და დრო, და რამდენადაც ეს შესაძლებელია, იმ პირის ვინაობა, რომელიც გაეცნო მონაცემებს ან განახორციელა მათი გადაცემა, ასევე ამ პერსონალურ მონაცემთა მიმღების ვინაობა.

2. ლოგების გამოყენება დასაშვებია მხოლოდ დამუშავების კანონიერების შემოწმების, თვითმონიტორინგის, მონაცემთა მთლიანობისა და უსაფრთხოების უზრუნველყოფის და სისხლის სამართლის პროცესის მიზნებისათვის.

3. მონაცემთა დამმუშავებელმა და უფლებამოსილმა პირმა მოთხოვნისამებრ უნდა უზრუნველყონ საზედამხედველო ორგანოს წვდომა ლოგებზე.

მუხლი 26

საზედამხედველო ორგანოსთან თანამშრომლობა

წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ მონაცემთა დამმუშავებელმა და უფლებამოსილმა პირმა მოთხოვნისამებრ ითანამშრომლონ საზედამხედველო ორგანოსთან მისი ამოცანების შესრულებაში.

მუხლი 27

მონაცემთა დაცვის ზეგავლენის შეფასება

1. როდესაც გარკვეული ტიპის დამუშავება, განსაკუთრებით ახალი ტექონოლოგიების გამოყენებით, დამუშავების ხასიათის, მოცულობის, კონტექსტისა და მიზნების გათვალისწინებით, დიდი ალბათობით გამოიწვევს ფიზიკური პირების უფლებებისა და თავისუფლებების დარღვევის მაღალ რისკს, წევრმა სახელმწიფოებმა უნდა უზუნრველყონ, რომ დამუშავების დაწყებამდე დამმუშავებელმა ჩაატაროს დაგეგმილი დამუშვების ოპერაციების მონაცემთა დაცვაზე ზეგავლენის შეფასება.

2. პირველი პუნქტით გათვალისწინებული შეფასება უნდა შეიცავდეს, სულ მცირე, დამუშავების დაგეგმილი ოპერაციების აღწერას, მონაცემთა სუბიექტების უფლებებისა და თავისუფლებების დარღვევის რისკების შეფასებას, ამ რისკების დარეგულირების ზომებს,

დაცვის გარანტიებს, უსაფრთხოების ზომებსა და მექანიზმებს პერსონალური მონაცემების დაცვის და წინამდებარე დირექტივასთან შესაბამისობის დემონსტრირების მიზნით, მონაცემთა სუბიექტებისა და სხვა დაინტერესებული პირების უფლებებისა და ლეგიტიმური ინტერესების გათვალისწინებით.

მუხლი 28

წინასწარი კონსულტაცია საზედამხედველო ორგანოსთან

1. წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ დამმუშავებელმა ან უფლებამოსილმა პირმა გაიაროს კონსულტაცია საზედამხედველო ორგანოსთან იმ დამუშვების დაწყებამდე, რომელიც ახალი ფაილური სისტემის ნაწილი უნდა გახდეს, იმ შემთხვევებში როდესაც:

(ა) 27-ე მუხლით გათვალისწინებული მონაცემთა დაცვის ზეგავლენის შეფასება მიუთითებს, რომ დამუშვება გამოიწვევს მაღალ რისკს დამმუშავებლის მიერ რისკის შემცირების მიზნით მისაღები ზომების არარსებობის შემთხვევაში;

(ბ) დამუშავების გარკვეული ტიპი, განსაკუთრებით ახალი ტექნოლოგიების, მექანიზმების, ან პროცედურების გამოყენებით, შეიცავს მონაცემთა სუბიექტების უფლებებისა და თავისუფლებების დარღვევის მაღალ რისკს.

2. წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ საზედამხედველო ორგანოსთან კონსულტაცია განხორციელდეს ეროვნული პარლამენტის მიერ დასამტკიცებელი, დამუშავებასთან დაკავშირებული საკანონმდებლო წინადადების შემუშავებისას ან ამგვარი საკანონმდებლო ზომის საფუძველზე მისაღები მარეგულირებელი ზომის შემუშავებისას.

3. წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ საზედამხედველო ორგანოს ჰქონდეს უფლება, განსაზღვოს იმ დამუშავების ოპერაციების სია, რომლებთან დაკავშირებითაც სავალდებულოა წინასწარი კონსულტაციის გავლა პირველი პუნქტის შესაბამისად.

4. წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ დამმუშავებელმა მიაწოდოს საზედამხედველო ორგანოს მონაცემთა დამუშავების ზეგავლენის შეფასება 27-ე მუხლის შესაბამისად და მოთხოვნისამებრ სხვა ინფორმაციაც, რომელიც შესაძლებლობას მისცემს საზედამხედველო ორგანოს, შეაფასოს დამუშავების შესაბამისობა და კერძოდ კი

მონაცემთა სუბიექტის პერსონალური მონაცემების დაცვის რისკები და შესაბამისი დაცვის გარანტიები.

5. იმ შემთხვევაში თუ საზედამხედველო ორგანოს აზრით, ამ მუხლის პირველი პუნქტით გათვალისწინებული დაგეგმილი დამუშავება დაარღვევს წინამდებარე დირექტივის შესაბამისად მიღებულ დებულებებს, კერძოდ კი იმ შემთხვევაში თუ დამმუშავებელმა არასაკმარისად მოახდინდა რისკის იდენტიფიცირება ან შემცირება, წევრმა სახელმწიფომ უნდა უზრუნველყოს, რომ საზედამხედველო ორგანომ, კონსულტაციის თხოვნით მომართვიდან 6 კვირის განმავლობაში გაუწიოს დამმუშავებელს, ხოლო ასეთის არსებობის შემთხვევაში უფლებამოსილ პირს, წერილობითი კონსულტაცია და გამოიყენოს 47-ე მუხლით გათვალისწინებული ნებისმიერი უფლებამოსილება. ეს ვადა შეიძლება გაგრძელდეს ერთი თვით, დაგეგმილი დამუშავების სირთულის გათვალისწინებით. საზედამხედველო ორგანომ უნდა აცნობოს დამმუშავებელს, ხოლო ასეთის არსებობის შემთხვევაში უფლებამოსილ პირსაც, ვადის ამგვარი გაგრძელების შესახებ კონსულტაციის შესახებ მოთხოვნის მიღებიდან ერთი თვის განმავლობაში და შეატყობინოს გაგრძელების მიზეზების შესახებ.

ნაწილი 2

პერსონალურ მონაცემთა უსაფრთხოება

მუხლი 29

დამუშავების უსაფრთხოება

1. წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ მონაცემთა დამმუშავებელმა თანამედროვე მეთოდების, ხარჯების, დამუშავების ხასიათის, მოცულობის და მიზნების, ასევე მონაცემთა სუბიექტის უფლებებისა და თავისუფლებების დარღვევის განსხვავებული და სხვადასხვა სიმძიმის რისკების გათვალისწინებით, მიიღონ სათანადო ტექნიკური და ორგანიზაციული ზომები, რომლებიც რისკის შესაბამის უსაფრთხოებას უზრუნველყოფენ, განსაკუთრებით, მე-10 მუხლით გათვალისწინებული განსაკუთრებული კატეგორიის მონაცემების დამუშავებასთან მიმართებით.

2. ავტომატურ დამუშავებასთან მიმართებით თითოეულმა წევრმა სახელმწიფომ უნდა უზრუნველყოს, რომ დამმუშავებელმა ან უფლებამოსილმა პირმა რისკების შეფასების შემდეგ მიიღოს ზომები:

(ა) დამუშავებისათვის გამოყენებულ მოწყობილობაზე არაუფლებამოსილი პირებისთვის დაშვების აღსაკვეთად (‘მოწყობილობაზე დაშვების კონტროლი’);

(ბ) მონაცემთა მატარებლის წაკითხვის, ასლის გადაღების, შეცვლის ან წაშლის პრევენციისთვის (‘მონაცემთა მატარებლის კონტროლი’);

(გ) პერსონალურ მონაცემთა უკანონო შევსების, შენახული პერსონალური მონაცემების დათვალიერების, შეცვლის ან წაშლის პრევენციისთვის (‘შენახვის კონტროლი’);

(დ) მონაცემთა გადასაცემი მოწყობილობების გამოყენებით არაუფლებამოსილი პირების მიერ ავტომატური დამუშავების სისტემების გამოყენების პრევენციისთვის (‘მოხმარებლის კონტროლი’);

(ე) ავტომატური დამუშავების სისტემის გამოყენებაზე უფლებამოსილების მქონე პირების მიერ მხოლოდ იმ მონაცემებთან წვდომის უზრუნველსაყოფად, რომელზეც მათ აქვთ დაშვების უფლებამოსილება (‘მონაცემებთან დაშვების კონტროლი’);

(ვ) უზრუნველყოს იმ ორგანოების იდენტიფიცირებისა და დადგენის შესაძლებლობა, რომლებსაც გადაეცა ან შესაძლოა გადაეცეს მონაცემები ან რომლებისთვისაც მონაცემები ხელმისაწვდომი გახდა მონაცემთა გადასაცემი მოწყობილობის მეშვეობით (‘კომუნიკაციის კონტროლი’);

(ზ) უზრუნველყოს იმ მონაცემთა იდენტიფიცირება და დადგენა, რომელთა შეყვანაც მოხდა ავტომატური დამუშავების სისტემებში და ვინ და როდის მოახდინა პერსონალური მონაცემების შეყვანა (‘შეყვანის კონტროლი’);

(თ) პერსონალური მონაცემების გადაცემისას ან მონაცემთა მატარებლის ტრანსპორტირებისას მოახდინოს პერსონალურ მონაცემთა უკანონო წაკითხვის, ასლის გადაღების, შეცვლის ან წაშლის პრევენცია (‘ტრანსპორტირების კონტროლი’);

(ი) შეფერხების შემთხვევაში უზრუნველყოს დაყენებული სისტემების აღდგენა (‘აღდგენა’);

(კ) უზრუნველყოს სისტემის ფუნქციების მუშაობა, ფუნქციების სავარაუდო ხარვეზების შეტყობინება (‘სანდოობა’) და უზრუნველყოს, რომ შენახული პერსონალური მონაცემების დაზიანება შეუძლებელია სისტემის გაუმართავი ფუნქციონირების გზით (‘მთლიანობა’)

მუხლი 30

მონაცემთა უსაფრთხოების ინციდენტის შეტყობინება საზედამხედველო ორგანოსათვის

1. წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ პერსონალურ მონაცემთა უსაფრთხოების ინციდენტის შემთხვევაში დამმუშავებელი დაუყოვნებლივ, ხოლო შესაძლებლობის შემთხვევაში ინციდენტის გამოვლენიდან არაუგვიანეს 72 საათისა, შეატყობინებს საზედამხედველო ორგანოს ინციდენტის შესახებ გარდა იმ შემთხვევისა,

როდესაც ნაკლებად სავარაუდოა, რომ პერსონალურ მონაცემთა უსაფრთხოების ინციდენტი შეუქმნის საფრთხეს ფიზიკური პირების უფლებებსა და თავისუფლებებს. თუ საზედამხედველო ორგანოს შეტყობინება არ გაეგზავნა 72 საათის განმავლობაში, მას თან უნდა ახლდეს შეფერხების გამომწვევი მიზეზები.

2. უფლებამოსილმა პირმა უნდა შეატყობინოს დამმუშავებელს პერსონალურ მონაცემთა უსაფრთხოების ინციდენტის გამოვლენიდან დაუყოვნებლივ.

3. პირველი პუნქტით გათვალისწინებული შეტყობინება სულ მცირე უნდა:

(ა) აღწერდეს პერსონალურ მონაცემთა უსაფრთხოების ინციდენტის ხასიათს, მათ შორის თუ შესაძლებელია დაინტერესებული მონაცემთა სუბიექტების კატეგორიებსა და დაახლოებით რაოდენობას და პერსონალური მონაცემების კატეგორიებსა და დაახლოებით რაოდენობას;

(ბ) შეიცავდეს ინფორმაციას მონაცემთა დაცვის ოფიცრის ან სხვა საკონტაქტო პირის (რომლისგანაც მეტი ინფორმაციის მოპოვებაა შესაძლებელი) სახელის და საკონტაქტო მონაცემების შესახებ;

(გ) აღწერდეს პერსონალური მონაცემების უსაფრთხოების ინციდენტის მოსალოდნელ შედეგებს;

(დ) აღწერდეს დამმუშავებლის მიერ პერსონალურ მონაცემთა უსაფრთხოების დარღვევის ინციდენტის აღმოსაფხვრელად მიღებულ ან შემოთავაზებულ ზომებს, მათ შორის, შესაძლებლობის შემთხვევაში, მოსალოდნელი უარყოფითი შედეგების შემცირების ზომებს;

4. იმ შემთხვევაში თუ ინფორმაციის ერთიანად მიწოდება შეუძლებელია, ინფორმაციის მიწოდება დასაშვებია ეტაპობრივად შემდგომი დაყოვნების გარეშე.

5. წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ დამმუშავებელმა დოკუმენტურად აღრიცხოს პირველი პუნქტით გათვალისწინებული პერსონალურ მონაცემთა უსაფრთხოების ნებისმიერი ინციდენტი, პერსონალური მონაცემების უსაფრთხოების ინციდენტთან დაკავშირებული ფაქტები, მისი შედეგები და მისი აღმოფხვრის მიზნით მიღებული ზომები. ხსენებული დოკუმენტაცია შესაძლებლობას უნდა აძლევდეს საზედამხედველო ორგანოს, შეამოწმოს წინამდებარე მუხლთან შესაბამისობა.

6. იმ შემთხვევაში თუ პერსონალურ მონაცემთა უსაფრთხოების ინციდენტი მოიცავს პერსონალურ მონაცემებს, რომელთა გადაცემა სხვა წევრი სახელმწიფოს დამმუშავებელმა მოახდინა ან რომლებიც გადაეცა სხვა წევრი სახელმწიფოს დამმუშავებელს, წევრმა

სახელმწიფოებმა უნდა უზრუნველყონ, რომ ამ წევრი სახელმწიფოს დამმუშავებელს დაუყოვნებლივ ეცნობოს აღნიშნულის თაობაზე.

მუხლი 31

პერსონალურ მონაცემთა უსაფრთხოების ინციდენტის შეტყობინება მონაცემთა სუბიექტისათვის

1. თუ პერსონალური მონაცემების უსაფრთხოების ინციდენტი დიდი ალბათობით გამოიწვევს ფიზიკური პირების უფლებებისა და თავისუფლებების დარღვევის მაღალ რისკს, წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ დამმუშავებელმა დაუყოვნელივ შეატყობინოს პერსონალურ მონაცემთა უსაფრთხოების ინციდენტი მონაცემთა სუბიექტს.

2. მონაცემთა სუბიექტისათვის მიწოდებული, პირველი პუნქტით გათვალისწინებული შეტყობინება გასაგები და მარტივი ენით უნდა აღწერდეს პერსონალურ მონაცემთა უსაფრთხოების ინციდენტის ხასიათს, და შეიცავდეს, სულ მცირე, 30-ე მუხლის მე-3 პუნქტის (ბ), (გ) და (დ) ქვეპუნქტებით გათვალისწინებულ ინფორმაციასა და ზომებს.

3. მონაცემთა სუბიექტისათვის პირველი პუნქტით გათვალისწინებული შეტყობინების მიწოდება არ არის სავალდებულო თუ სახეზეა ერთ-ერთი შემდეგი პირობა:

(ა) დამმუშავებელმა მიიღო უსაფრთხოების სათანადო ტექნიკური და ორგანიზაციული ზომები და ეს ზომები გამოყენებულ იქნა იმ პერსონალურ მონაცემებთან მიმართებით, რომელთა მიმართაც განხორციელდა პერსონალურ მონაცემთა უსაფრთხოების ინციდენტი, კერძოდ ისეთი ზომები, როგორიცაა, დაშიფრვა, რომელიც პერსონალურ მონაცემებს მიუწვდომელს ხდის ნებისმიერი პირისათვის რომელიც არ არის უფლებამოსილი, ჰქონდეს მათზე წვდომა;

(ბ) დამმუშავებელმა მიიღო შესაბამისი ზომები, რომლებიც უზრუნველყოფენ, რომ მონაცემთა სუბიექტების უფლებებისა და თავისუფლებების შელახვის პირველი პუნქტით გათვალისწინებული მაღალი რისკი არ მატერიალიზდება;

(გ) შეტყობინება მოითხოვს არაპროპორციულ ძალისხმევას. ასეთ შემთხვევაში შეტყობინება უნდა მოხდეს საჯაროდ ან სხვა მსგავსი თანაბრად ეფექტური საშუალებით, რომლითაც მონაცემთა სუბიექტები მიიღებენ ინფორმაციას.

4. თუ მონაცემთა დამმუშავებელს არ შეუტყობინებია მონაცემთა სუბექტისათვის პერსონალურ მონაცემთა უსაფრთხოების ინციდენტის შესახებ, საზედამხედველო ორგანო, პერსონალურ მონაცემთა უსაფრთხოების ინციდენტის მიერ მაღალი რისკის გამოწვევის

დიდი ალბათობის გათვალისწინებით, უფლებამოსილია, დაავალოს დამმუშავებელს შეტყობინების მიწოდება, ან უფლება აქვს დაადგინოს, რომ მე-3 პუნქტით გათვალისწინებული პირობა შესრულებულია.

5. მონაცემთა სუბიექტისათვის ამ მუხლის პირველი პუნქტით გათვალისწინებული შეტყობინების მიწოდება შეიძლება გადაიდოს, შეიზღუდოს ან არ მოხდეს მე-13 მუხლის მე-3 პუნქტით გათვალისწინებული პირობებითა და საფუძვლებით.

ნაწილი 3

მონაცემთა დაცვის ოფიცერი

მუხლი 32

მონაცემთა დაცვის ოფიცრის დანიშვნა

1. წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ დამმუშავებელმა დანიშნოს მონაცემთა დაცვის ოფიცერი. წევრ სახელმწიფოებს უფლება აქვთ, ამ ვალდებულებისაგან გამონაკლისის სახით გაათავისუფლონ სასამართლოები და მართლმსაჯულების სხვა დამოუკიდებელი ორგანოები, როდესაც ისინი მოქმედებენ სასამართლო უფლებამოსილების ფარგლებში.

2. მონაცემთა დაცვის ოფიცერი უნდა დაინიშნოს მისი პროფესიული უნარების, პერსონალურ მონაცემთა დაცვის კანონმდებლობისა და პრაქტიკის ექსპერტული ცოდნისა და 34-ე მუხლით განსაზღვრული ამოცანების შესრულების უნარის საფუძველზე.

3. რამდენიმე კომპეტენტური ორგანოსთვის დასაშვებია მონაცემთა დაცვის ერთი ოფიცრის დანიშვნა, ამ ორგანოების ორგანიზაციული სტრუქტურისა და ზომის გათვალისწინებით.

4. წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ დამმუშავებელმა საჯაროდ გამოაქვეყნოს მონაცემთა დაცვის ოფიცრის საკონტაქტო მონაცემები და მიაწოდოს ისინი საზედამხედველო ორგანოს.

მუხლი 33

მონაცემთა დაცვის ოფიცრის სტატუსი

1. წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ დამმუშავებელმა მოახდინოს მონაცემთა დაცვის ოფიცრის სათანადო და დროული ჩართვა პერსონალური მონაცემების დაცვასთან დაკავშირებულ ნებისმიერ საკითხში.

2. დამმუშავებელი უნდა დაეხმაროს მონაცემთა დაცვის ოფიცერს 34-ე მუხლით გათვალისწინებული ამოცანების შესრულებაში, რა დროსაც უნდა მოხდეს ოფიცრისათვის ამ ამოცანების შესასრულებლად და საექსპერტო ცოდნის შესანარჩუნებლად აუცილებელი რესურსების გამოყოფა და პერსონალურ მონაცემებთან და დამუშვების ოპერაციებთან მისი წვდომის უზრუნველყოფა.

მუხლი 34

მონაცემთა დაცვის ოფიცრის ამოცანები

წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ დამმუშავებელმა მონაცემთა დაცვის ოფიცერს მიანიჭოს, სულ მცირე, შემდეგი ამოცანების შესრულების უფლებამოსილება:

(ა) დამმუშავებლის და მასთან დასაქმებულების (რომლებიც ახორციელებენ მონაცემთა დამუშავებას) ინფორმირება წინამდებარე დირექტივის, ევროკავშირის ან წევრი სახელმწიფოს მონაცემთა დაცვის დებულებებით გათვალისწინებული მათი ვალდებულებების შესახებ;

(ბ) წინამდებარე დირექტივასთან, ევროკავშირის ან წევრი სახელმწიფოს მონაცემთა დაცვის დებულებებთან, პერსონალური მონაცემების დაცვის საკითხზე დამმუშავებლის მიერ შემუშავებული პოლიტიკის დოკუმენტთან შესაბამისობის მონიტორინგი, მათ შორის, პასუხისმგებლობის განაწილება, დამუშავების ოპერაციებში ჩართული თანამშრომლების ცნობიერების ამაღლება, გადამზადება და დაკავშირებული აუდიტი;

(გ) მოთხოვნისამებრ კონსულტაციის გაწევა მონაცემთა დაცვის ზეგავლენის შეფასებასთან მიმართებით და მისი შესრულების მონიტორინგი 27-ე მუხლის შესაბამისად;

(დ) საზედამხედველო ორგანოსთან თანამშრომლობა;

(ე) დამუშავებასთან დაკავშირებულ ნებისმიერ საკითხზე საზედამხედველო ორგანოსთან საკონტაქტო პირის ფუნქციის შესრულება, მათ შორის 28-ე მუხლით გათვალისწინებული წინასწარი კონსულტაციისას და საჭიროებისამებრ საზედამხედველო ორგანოსთან კონსულტაციის გავლა ნებისმიერ სხვა საკითხზე.

თავი V

პერსონალურ მონაცემთა მესამე სახელმწიფოსთვის ან საერთაშორისო ორგანიზაციისათვის გადაცემა

მუხლი 35

პერსონალურ მონაცემთა გადაცემის ზოგადი პრინციპები

1. წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ კომპეტენტური ორგანოების მიერ დამუშავების პროცესში მყოფი ან მესამე სახელმწიფოს ან საერთაშორისო ორგანიზაციისათვის გადაცემის შემდგომ დასამუშავებელი, მათ შორის შემდგომი გადაცემისათვის განკუთვნილი პერსონალური მონაცემების გადაცემა განხორციელდეს წინამდებარე დირექტივის დებულებების საფუძველზე მიღებული ეროვნული დებულებების შესაბამისად და მხოლოდ იმ შემთხვევაში თუ სახეზეა ამ თავით გათვალისწინებული პირობები, კერძოდ:

(ა) გადაცემა აუცილებელია პირველი მუხლის პირველი პუნქტით გასნაზღვრული მიზნებისათვის;

(ბ) პერსონალური მონაცემები გადაეცემა მესამე სახელმწიფოში ან საერთაშორისო ორგანიზაციაში ისეთ დამმუშავებელს, რომელიც კომპეტენტურია პირველი მუხლის პირველი პუნქტის მიზნებისათვის;

(გ) როდესაც პერსონალური მონაცემების გადაცემა ან მათზე წვდომა ხორციელდება სხვა წევრი სახელმწიფოდან, აღნიშნულ წევრ სახელმწიფოს გაცემული უნდა ჰქონდეს წინასწარი ნებართვა გადაცემაზე მისი ეროვნული კანონმდებლობის შესაბამისად;

(დ) კომისიას მიღებული აქვს შესაბამისობის გადაწყვეტილება 36-ე მუხლის თანახმად ან ასეთი გადაწყეტილების არარსებობის შემთხვევაში წარმოდგენილია, ან არსებობს 37-ე მუხლის შესაბამისი სათანადო გარანტიები, ან 36-ე მუხლით გათვალისწინებული შესაბამისობის გადაწყვეტილებისა და 37-ე მუხლის შესაბამისი სათანადო გარანტიების არარსებობის შემთხვევაში, კონკრეტულ სიტუაციებზე ვრცელდება 38-ე მუხლით გათვალისწინებული გამონაკლისები; და

(ე) მონაცემთა სხვა მესამე სახელწმიფოსა ან საერთაშორისო ორგანიზაციისათვის შემდგომი გადაცემის შემთხვევაში კომპეტენტური ორგანო, რომელმაც განახორციელა თავდაპირველი გადაცემა ან იმავე წევრი სახელმწიფოს სხვა კომპეტენტური ორგანო თანხმობას გასცემს შემდგომ გადაცემაზე მას შემდეგ, რაც გაითვალისწინებს ყველა შესაბამის ფაქტორს, მათ შორის დანაშაულის სიმძიმეს, მონაცემთა თავდაპირველი გადაცემის მიზანს და მონაცემთა დაცვის მდგომარეობას მესამე სახელმწიფოში ან საერთაშორისო ორგანიზაციაში, რომელშიც ხორციელდება პერსონალური მონაცემების შემდგომი გადაცემა.

2. წევრმა სახელწმიფოებმა უნდა უზრურველყონ, რომ სხვა წევრი სახელმწიფოს წინასწარი თანხმობის გარეშე პირველი პუნქტის (გ) ქვეპუნქტის შესაბამისად მონაცემთა გადაცემა განხორციელდეს მხოლოდ იმ შემთხვევაში თუ პერსონალური მონაცემების გადაცემა

აუცილებელია წევრი სახელმწიფოს ან მესამე ქვეყნის საზოგადოებრივი უსაფრთხოების ან წევრი სახელმწიფოს არსებითი ინტერესების წინააღმდეგ მიმართული მყისიერი და სერიოზული საფრთხის თავიდან ასაცილებლად და თუ წინასწარი თანხმობის მოპოვება დროულად შეუძლებელია. უწყება, რომელიც პასუხისმგებელია წინასწარი თანხმობის გაცემაზე დაუყოვნებილვ უნდა იქნეს ინფორმირებული.

3. ამ თავის ყველა დებულება გამოყენებული უნდა იქნეს იმისათვის, რომ უზრუნველყოფილი იყოს ფიზიკური პირების დაცვის წინამდებარე დირექტივით დადგენილი გარანტიები.

მუხლი 36

გადაცემა შესაბამისობის გადაწყვეტილების საფუძველზე

1. წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ პერსონალური მონაცემების მესამე სახელმწიფოს ან საერთაშორისო ორგანიზაციისათვის გადაცემა დასაშვები იყოს თუ კომისიას გადაწყვეტილი აქვს, რომ მესამე სახელმწიფო, ტერიტორია ან ერთი ან მეტი კონკრეტული სექტორი მესამე სახელმწიფოში, ან საერთაშორისო ორგანიზაცია უზრუნველყოფს დაცვის შესაბამის სტანდარტს. ასეთი გადაცემა არ საჭიროებს სპეციალურ ნებართვას.

2. დაცვის სტანდარტის შესაბამისობის შეფასებისას, კომისიამ განსაკუთრებით უნდა მიიღოს მხედველობაში შემდეგი ელემენტები:

(ა) კანონის უზენაესობა, ადამიანის ფუნდამენტური უფლებებისა და თავისუფლებების პატივისცემა, შესაბამისი კანონმდებლობა, როგორც ზოგადი, ისე სექტორული, მათ შორის საზოგადოებრივ უსაფრთხოებასთან, თავდაცვასთან, ეროვნულ უსაფრთხოებასთან და სისხლის სამართალთან დაკავშირებული კანონმდებლობა, ასევე საჯარო უწყებების წვდომა პერსონალურ მონაცემებთან, ისევე როგორც ასეთი კანონმდებლობის აღსრულება, მონაცემთა დაწვის წესები, პროფესიული რეგულაციები და უსაფრთხოების ზომები, მათ შორის სხვა მესამე სახელმწიფოს ან საერთაშორისო ორგანიზაციისათვის მონაცემთა შემდგომი გადაცემის წესები, რომლებიც მოქმედებს იმ სახელმწიფოსა თუ საერთაშორისო ორგანიზაციაში, სასამართლო პრაქტიკა, აგრეთვე მონაცემთა სუბიექტების ეფექტური და განხოციელებადი უფლებები და მონაცემთა იმ სუბიექტების ეფექტური ადმინისტრაციული და სამართლებრივი დაცვის საშუალებები, რომელთა მონაცემების გადაცემაც ხორციელდება;

(ბ) ერთი ან მეტი საზედამხედველო ორგანოს არსებობა და მისი ეფექტური ფუნქციონირება მესამე სახელმწიფოში ან იმ შემთხვევაში, როდესაც მას ექვემდებარება საერთაშორისო ორგანიზაცია, მონაცემთა დაცვის წესებთან შესაბამისობის უზრუნველყოფის აღსრულების უფლებამოსილებით, მათ შორის აღსრულების ადეკვატური უფლებამოსილებით, მონაცემთა სუბიექტებისათვის მათი უფლებების განხორციელებაში დახმარებისა და კონსულტაციის გაწევის უფლებამოსილებითა და წევრი სახელმწიფოების საზედამხედველო ორგანოებთან თანამშრომლობის უფლებამოსილებით; და

(გ) მესამე სახელმწიფოს ან საერთაშორისო ორგანიზაციის მიერ ნასიკისრი საერთაშორისო ვალდებულებები, ან სხვა სამართლებრივად ხელშემკვრელი კონვენციებიდან ან ინსტრუმენტებიდან, ასევე პერსონალური მონაცემების დაცვასთან დაკავშირებული მრავალმხრივ ან რეგიონალურ სისტემებში მისი ჩართულობიდან გამომდინარე სხვა ვალდებულებები.

3. დაცვის სტანდარტის შესაბამისობის შეფასების შემდეგ კომისია უფლებამოსილია, აქტის იმპლემენტაციის გზით გადაწყვიტოს, რომ მესამე სახელმწიფო, ტერიტორია ან ერთი ან მეტი კონკრეტული სექტორი მესამე სახელმწიფოში, ან საერთაშორისო ორგანიზაცია უზრუნველყოფს დაცვის ადეკვატურ სტანდარტს ამ მუხლის მე-2 პუნქტის მიზნებისათვის. საიმპლემენტაციო აქტი უნდა ადგენდეს გადაწყვეტილების პერიოდული, სულ მცირე, ყოველ ოთხ წელიწადში გადასინჯვის მექანიზმს, რომლის დროსაც მხედველობაში უნდა იქნეს მიღებული ყველა შესაბამისი განვითარება მესამე სახელმწიფოსა თუ საერთაშორისო ორგანიზაციაში. საიმპლემენტაციო აქტი უნდა ადგენდეს მის ტერიტორიულ და სექტორულ გავრცელებას და ასეთის არსებობის შემთხვევაში, ახდენდეს ამ მუხლის მე-2 პუქნტის (ბ) ქვეპუნქტით განსაზღვრული საზედამხედველო ორგანოს იდენტიფიცირებას. საიმპლემენტაციო აქტი მიიღება 58-ე მუხლის მე-2 ნაწილით განსაზღვრული შემოწმების პროცედურის შესაბამისად.

4. კომისია მუდმივმოქმედ რეჟიმში უნდა დააკვირდეს მესამე ქვეყნებსა და საერთაშორისო ორგანიზაციებში არსებულ სიახლეებს, რომლებსაც შეუძლიათ გავლენა მოახდინონ მე-3 პუნქტის შესაბამისად მიღებული გადაწყვეტილებების ფუნქციონირებაზე.

5. თუ გამოვლინდება, მათ შორის ამ მუხლის მე-3 პუნქტით გათვალისწინებული გადახედვის პროცედურის შემდეგ, რომ მესამე სახელმწიფო, ტერიტორია ან ერთი ან მეტი კონკრეტული სექტორი მესამე სახლემწიფოში ან საერთაშორისო ორგანიზაცია ვეღარ უზრუნველყოფს დაცვის ადეკვატურ სტანდარტს ამ მუხლის მე-2 პუნქტის

მიზნებისათვის, კომისიამ საჭირო მოცულობით უნდა გააუქმოს, შეასწოროს ან შეაჩეროს ამ მუხლის მე-3 პუნქტით გათვალისწინებული გადაწყვეტილება საიმპლემენტაციო აქტების მეშვეობით, რომელთაც არ აქვთ უკუქცევითი ძალა. საიმპლემენტაციო აქტი მიიღება 58-ე მუხლის მე-2 ნაწილით განსაზღვრული შემოწმების პროცედურის შესაბამისად. გადაუდებლობის სათანადოდ დასაბუთებული იმპერატიული საფუძვლების არსებობისას, კომისიამ დაუყოვნებლივ უნდა მიიღოს აღსრულებადი საიმპლემენტაციო აქტები 58-ე მუხლის მე-3 პუნქტით დადგენილი პროცედურის შესაბამისად.

6. მე-5 პუნქტის შესაბამისად მიღებული გადაწყვეტილების გამომწვევი მდგომარეობის გამოსწორების მიზნით კომისიამ უნდა გამართოს კონსულტაციები მესამე ქვეყანასთან ან საერთაშორისო ორგანიზაციასთან.

7. წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ მე-5 პუნქტის შესაბამისად მიღებულმა გადაწყვეტილებამ ხელი არ შეუშალოს 37-ე და 38-ე მუხლების შესაბამისად პერსონალური მონაცემების გადაცემას მესამე ქვეყანაში, მესამე ქვეყნის ტერიტორიაზე ან მის ერთ ან მეტ კონკრეტულ სექტორში ან საერთაშორისო ორგანიზაციაში.

8. კომისიამ ევროკავშირის ოფიციალურ ჟურნალში და თავის ვებ-გვერდზე უნდა გამოაქვეყნოს იმ მესამე სახელმწიფოების, მათი ტერიტორიების ან ერთი ან მეტი კონკრეტული სექტორების, ან საერთაშორისო ორგანიზაციების სია, რომლებიც კომისიის გადაწყვეტილებით არ უზრუნველყოფენ ან ვეღარ უზრუნველყოფენ დაცვის ადეკვატურ სტანდარტს.

მუხლი 37

გადაცემა სათანადო გარანტიების საფუძველზე

1. 36-ე მუხლის მე-3 პუნქტის საფუძველზე მიღებული გადაწყვეტილების არარსებობის შემთხვევაში წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ პერსონალური მონაცემების გადაცემა მესამე ქვეყნისათვის ან საერთაშორისო ორგანიზაციისათვის შესაძლებელი იყოს იმ შემთხვევაში როდესაც:

(ა)სამართლებრივად სავალდებულო ძალის მქონე ინსტრუმენტით უზრუნველყოფილია პერსონალურ მონაცემთა დაცვის სათანადო გარანტიები;;

ბ) დამმუშავებელმა შეაფასა პერსონალური მონაცემების გადაცემასთან დაკავშირებული გარემოებები და დაადგინა, რომ სახეზეა პერსონალური მონაცემების დაცვის სათანადო გარანტიები.

2. დამმუშავებელმა უნდა შეატყობინოს საზედამხედველო ორგანოს პირველი პუნქტის (ბ) ქვეპუნქტის საფუძველზე განხორციელებული გადაცემების კატეგორიების შესახებ.

3. თუ გადაცემა ხორციელდება პირველი პუქნტის (ბ) ქვეპუნქტის საფუძველზე, ასეთი გადაცემა დოკუმენტურად უნდა აღირიცხოს და დოკუმენტები მოთხოვნისამებრ ხელმისაწვდომი უნდა იყოს საზედამხედველო ორგანოსთვის, მათ შორის გადაცემის თარიღი და დრო, მიმღები კომპეტენტური ორგანო, გადაცემის დასაბუთება და გადაცემული პერსონალური მონაცემები.

მუხლი 38

გამონაკლისები კონრკეტული გარემოებებისათვის

1. 38-ე მუხლის საფუძველზე მიღებული შესაბამისობის გადაწყვეტილების ან 37-ე მუხლის შესაბამისად დადგენლი გარანტიების არარსებობის შემთხვევაში, წევრმა სახელწმიფოებმა უნდა უზრუნველყონ, რომ პერსონალური მონაცემების გადაცემა მესამე ქვეყნისათვის ან საერთაშორისო ორგანიზაციისათვის ან გადაცემის გარკვეული კატეგორიები შესაძლებელი იყოს მხოლოდ იმ შემთხვევაში თუ გადაცემა აუცილებელია:

(ა) მონაცემთა სუბიექტის ან სხვა პირის სასიცოცხლო ინტერესების დასაცავად;

(ბ) მონაცემთა სუბიექტის ლეგიტიმური ინტერესების დასაცავად, როდესაც ეს გათვალისწინებულია მონაცემთა გადამცემი სახელმწიფოს კანონმდებლობით;

(გ) წევრი სახელმწიფოს ან მესამე ქვეყნის საზოგადოებრივი უსაფრთხოების წინააღმდეგ მიმართული მყისიერი და მნიშვნელოვანი საფრთხის თავიდან ასაცილებლად;

(დ) ინდივიდუალურ შემთხვევებში პირველი მუხლის პირველი პუნქტით დადგენილი მიზნების მისაღწევად;

(ე) პირველი მუხლის პირველი პუნქტით დადგენილ მიზნებთან დაკავშირებული სამართლებრივი მოთხოვნების დასადგენად, განსახორციელებლად ან დასაცავად.

2. პერსონალურ მონაცემთა გადაცემა დაუშვებელია თუ გადამცემი კომპეტენტური ორგანო დაადგენს, რომ დაინტერესებული მონაცემთა სუბიექტების ფუნდამენტური უფლებები და თავისუფლებები აღემატება გადაცემის პირველი პუნქტის (დ) და (ე) ქვეპუნქტებით დადგენილ საჯარო ინტერესს.

3. როდესაც გადაცემას საფუძვლად უდევს პირველი პუნქტი, ასეთი გადაცემა დოკუმენტურად უნდა აღირიცხოს და დოკუმენტები მოთხოვნისამებრ ხელმისაწვდომი უნდა იყოს საზედამხედველო ორგანოსთვის, მათ შორის გადაცემის თარიღი და დრო,

მიმღები კომპეტენტური ორგანო, გადაცემის დასაბუთება და გადაცემული პერსონალური მონაცემები.

მუხლი 39

პერსონალურ მონაცემთა გადაცემა მესამე სახელმწიფოში არსებული მიმღებისათვის

1. როგორც გამონაკლისი 35-ე მუხლის პირველი პუნქტის (ბ) ქვეპუნქტისაგან, ამ მუხლის მე-2 პუნქტით გათვალისწინებული რომელიმე საერთაშორისო შეთანხმების შეუზღუდავად, წევრი სახელმწიფოები უფლებამოსილები არიან, უზრუნველყონ, რომ მე-3 მუხლის მე-7 პუნქტის (ა) ქვეპუნქტით განსაზღვრულ კომპეტენტურ ორგანოებს შეეძლოთ, კონკრეტულ და ინდივიდუალურ შემთხვევებში პირდაპირ გადასცენ პერსონალური მონაცემები მესამე სახელმწიფოში არსებულ მიმღებს მხოლოდ იმ შემთხვევაში თუ შესრულებულია წინამდებარე დირექტივის ყველა დებულება და ყველა ჩამოთვლილი პირობა:

(ა) გადაცემა მკაცრად აუცილებელია გადამცემი კომპეტენტური ორგანოს მიერ ევროკავშირის ან წევრი სახელმწიფოს კანონით განსაზღვრული ამოცანის შესასრულებლად პირველი მუხლის პირველი პუნქტით დადგენილი მიზნებისათვის;

(ბ) გადამცემმა კომპეტენტურმა ორგანომ დაადგინა, რომ დაინტერესებული მონაცემთა სუბიექტების ფუნდამენტური უფლებები და თავისუფლებები არ აღემატება საჯარო ინტერესს, რომლითაც გამოწვეულია კონკრეტული გადაცემა;

(გ) გადამცემი ორგანო მიიჩნევს, რომ მესამე სახელმწიფოს იმ ორგანოსათვის მონაცემთა გადაცემა, რომელიც პირველი მუხლის პირველი პუნქტის მიზნებისათვის კომპეტენტურად ითვლება, არაეფექტური ან შეუსაბამოა, განსაკუთრებით თუ გადაცემა ვერ მოხდება დროულად;

(დ) მესამე სახელმწიფოს ორგანოს, რომელიც პირველი მუხლის პირველი პუნქტის მიზნებისათვის კომპეტენტურად ითვლება, დაუყოვნებლივ მიეწოდა ინფორმაცია, გარდა იმ შემთხვევისა როდესაც ასეთი შეტყობინება არაეფექტური ან შეუსაბამოა;

(ე) გადამცემი კომპეტენტური ორგანო შეატყობინებს მიმღებს იმ კონკრეტულ მიზანს ან მიზნებს, რომლის ფარგლებშიც უნდა მოხდეს მონაცემთა დამუშავება, თუ ამგვარი დამუშავება აუცილებელია.

2. პირველი პუნქტით გათვალისწინებული საერთაშორისო შეთანხმება შეიძლება იყოს ნებისმიერი ორმხრივი ან მრავალმხრივი საერთაშორისო შეთანხმება, რომელიც ძალაშია

წევრ სახელმწიფოებსა და მესამე სახელმწიფოებს შორის სისხლის სამართლის საქმეებზე სამართლებრივი თანამშრომლობის ან საპოლიციო თანამშრომლობის სფეროში.

3. გადამცემმა კომპეტენტურმა ორგანომ უნდა შეატყობინოს საზედამხედველო ორგანოს ამ მუხლის შესაბამისად განხორციელებული გადაცემის შესახებ.

4. როდესაც გადაცემა პირველი პუნქტის საფუძველზე ხორციელდება, ის დოკუმენტურად უნდა აღირიცხოს.

მუხლი 40

საერთაშორისო თანამშრომლობა პერსონალურ მონაცემთა დაცვისათვის

მესამე სახელმწიფოებთან და საერთაშორისო ორგანიზაციებთან მიმართებით კომისიამ და წევრმა სახელმწიფოებმა უნდა მიიღონ სათანადო ზომები იმისათვის, რომ:

(ა) განავითარონ საერთაშორისო თანამშრომლობის მექანიზმები პერსონალურ მონაცემთა დაცვის კანონმდებლობის ეფექტური აღსრულების უზრუნველსაყოფად;

(ბ) უზრუნველყონ საერთაშორისო ურთიერთდახმარება პერსონალურ მონაცემთა დაცვის კანონმდებლობის აღსრულებისას, მათ შორის შეტყობინების, საჩივრების გადამისამართების, საგამოძიებო თანამშრომლობისა და ინფორმაციის გაცვლის საშუალებით, რისთვისაც სახეზე უნდა იყოს პერსონალურ მონაცემთა და სხვა ფუნდამენტური უფლებების და თავისუფლებების დაცვის სათანადო გარანტიები;

(გ) ჩართონ შესაბამისი მხარეები დისკუსიასა და ღონისძიებებში, რომლებიც მიმართულია პერსონალურ მონაცემთა დაცვის კანომდებლობის აღსრულებისას საერთაშორისო თანამშრომლობის გაღრმავებისაკენ;

(დ) ხელი შეუწყონ პერსონალურ მონაცემთა დაცვის კანომდებლობისა და პრაქტიკის დოკუმენტების გაცვლას, მათ შორის, მესამე სახელმწიფოსთან იურისდიქციულ კოლიზიასთან დაკავშირებით.

თავი VI

დამოუკიდებელი საზედამხედველო ორგანოები

ნაწილი 1

დამოუკიდებელი სტატუსი

მუხლი 41

საზედამხედველო ორგანო

1. თითოეულმა წევრმა სახელმწიფომ უნდა უზრუნველყოს, რომ ერთი ან მეტი საჯარო საზედამხედველო ორგანო ზედამხედველობას უწევდეს წინამდებარე დირექტივის დებულებების შესრულებას დამუშავებასთან დაკავშირებით ფიზიკური პირების ფუნდამენტური უფლებებისა და თავისუფლებების დასაცავად და პეროსონალური მონაცემების ევროკავშირის ტერიტორიაზე თავისუფალი გადადინების ხელშესაწყობად (‘საზედამხედველო ორგანო;).

2. თითოეულმა საზედამხედველო ორგანომ წვლილი უნდა შეიტანოს წინამდებარე დირექტივის ევროკავშირის მასშტაბით ერთგვაროვან გამოყენებაში. ამ მიზნით საზედამხედველო ორგანოებმა უნდა ითანამშრომლონ ერთმანეთთან და კომისიასთან VII თავით დადგენილი წესით.

3. წევრი სახელმწიფოები უფლებამოსილნი არიან, უზრუნველყონ, რომ ევროკავშირის (EU) 2016/679 რეგულაციით დადგენილი საზედამხედველო ორგანო იყოს წინამდებარე დირექტივით განსზღვრული საზედამხედველო ორგანო და შეასრულოს საზედამხედველო ორგანოს ამ მუხლის პირველი პუნქტით გათვალისწინებული ამოცანები.

4. თუ წევრ სახელმწიფოში შექმნილია ერთზე მეტი საზედამხედველო ორგანო, წევრმა სახელმწიფომ უნდა განსაზღვროს საზედამხედველო ორგანო, რომელიც წარმოადგენს ამ უწყებებს 51-ე მუხლით გათვალისწინებულ საბჭოში.

მუხლი 42

დამოუკიდებლობა

1. ყოველმა წევრმა სახელმწიფომ უნდა უზრუნველყოს, რომ თოთოეული საზედამხედველო ორგანო ამ დირექტივის შესაბამისად თავისი ამოცანების შესრულებისას და უფლებამოსილებების განხორციელებისას მოქმედებდეს სრულიად დამოუკიდებლად.

2. წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ მათი საზედამხედველო ორგანოების წევრი ან წევრები ამ დირექტივის შესაბამისად თავიანთი ამოცანების შესრულებისას და უფლებამოსილებების განხორციელებისას ინარჩუნებდნენ თავისუფლებას გარეშე, პირდაპირი ან არაპირდაპირი ზეწოლისაგან და არ ითხოვდნენ და არ იღებდნენ მითითებებს არავისგან.

3. წევრი სახელმწიფოების საზედამხედველო ორგანოების წევრებმა თავი უნდა შეიკავონ ნებისმიერი მოქმედებისაგან, რომელიც შეუთავსებელია მათ მოვალეობებთან და

თანამდებობაზე ყოფნის განმავლობაში არ უნდა დაიკავონ შეუთავსებელი ანაზღაურებადი თუ არაანაზღაურებადი თანამდებობა.

4. თითოეულმა წევრმა სახელმწიფომ უნდა უზრუნველყოს, რომ ყოველი საზედამხედველო ორგანო უზრუნველყოფილი იყოს ადამიანური, ტექნიკური და ფინანსური რესურსებით, შენობით და ინფრასტრუქტურით, რომელიც აუცილებელია მისი ამოცანების და უფლებამოსილებების ეფექტური განხორციელებისათვის, მათ შორის იმ ამოცანების და უფლებამოსილებების, რომლებიც ურთიერთდახმარების, თანამშრომლობის და საბჭოში მონაწილეობის კონტექსტში უნდა განხორციელდეს.

5. ყოველმა წევრმა სახელწმიფომ უნდა უზრუნველყოს, რომ თითოეული საზედამხედველო ორგანო ირჩევდეს საკუთარ თანამშრომლებს და ჰყავდეს საკუთარი თანამშრომლები, რომლებიც ექსკლუზიურად ექვემდებარებიან საზედამხედველო ორგანოს წევრის ან წერვების მითითებებს.

6. ყოველმა წევრმა სახელმწიფომ უნდა უზრუნველყოს, რომ თითოეული საზედამხედველო ორგანო ექვემდებარებოდეს ფინანსურ კონტროლს, რომელიც უარყოფითად არ იმოქმედებს მის დამოუკიდებლობაზე და უზრუნველყოს, რომ მას ჰქონდეს განცალკევებული წლიური ბიუჯეტი, რომელიც შესაძლოა იყოს საერთო სახელმწიფო ან ეროვნული ბიუჯეტის ნაწილი.

მუხლი 43

ზოგადი მოთხოვნები საზედამხედველო ორგანოს წევრებისათვის

1. წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ მათი საზედამხედველო ორგანოების თითოეული წევრი ინიშნებოდეს გამჭვირვალე პროცედურით:

— პარლამენტის მიერ;

— მთავრობის მიერ;

— სახელმწიფოს მეთაურის მიერ; ან

— დამოუკიდებელი ორგანოს მიერ, რომელსაც წევრი სახელმწიფოს კანონმდებლობით მინიჭებული აქვს მისი დანიშვნის უფლებამოსილება.

2. თითოეულ წევრს უნდა ჰქონდეს კვალიფიკაცია, გამოცდილება და უნარები, განსაკუთრებით პერსონალურ მონაცემთა დაცვის სფეროში, რომლებიც აუცილებელია მისი ამოცანების შესასრულებლად და უფლებამოსილებების განსახორციელებლად.

3. წევრს უფლებამოსილება შეუწყდება თანამდებობაზე ყოფნის ვადის გასვლისას, გადადგომისას ან პენსიაზე გასვლისას წევრი სახელმწიფოს კანონმდებლობის შესაბამისად.

4. წევრის თანამდებობიდან გათავისუფლება დასაშვებია მხოლოდ მნიშვნელოვანი გადაცდომის შემთხვევაში ან თუ წევრი აღარ აკმაყოფილებს მისი მოვალეობების შესასრულებლად საჭირო მოთხოვნებს.

მუხლი 44

საზედამხედველო ორგანოს შექმნის წესები

1. თითოეულმა წევრმა სახელმწიფომ უნდა უზრუნველყოს, რომ კანონმდებლობით გათვალისწინებული იყოს ყველა შემდეგი დებულება:

(ა)საზედამხედველო ორგანოს შექმნა;

(ბ) კვალიფიკაცია და დასაშვებობის პირობები, რომლებიც საჭიროა თითოეული საზედამხედველო ორგანოს წევრად დანიშვნისთვის;

(გ) თითოეული საზედამხედველო ორგანოს წევრის ან წევრების დანიშვნის წესები და პროცედურები;

(დ) თითოეული საზედამხედველო ორგანოს წევრის ან წევრების თანამდებობაზე გამწესების არანაკლებ ოთხწლიანი ვადა, გარდა 2016 წლის 6 მაისის შემდგომი პირველი დანიშვნისა, რომელიც შესაძლოა მოხდეს უფრო ნაკლები ვადით, თუ ეს აუცილებელია საზედამხედველო ორგანოს დამოუკიდებლობის დასაცავად ეტაპობრივი დანიშვნის პროცედურის მეშვეობით;

(ე) შესაძლებელია თუ არა საზედმხედველო ორგანოს წევრის ან წევრების რამდენიმე ვადით დანიშვნა და თუ შესაძლებელია, რამდენჯერ;

(ვ) თითოეული საზედამხედველო ორგანოს წევრის ან წევრების და თანამშრომლების მოვალეობების მარეგულირებელი დებულებები, თანამდებობაზე ყოფნისას და შემდგომში შეუფერებელი მოქმედებების, თანამდებობების დაკავების და შემოსავლების აკრძალვა და წესები, რომლებიც არეგულირებენ დასაქმების შეწყვეტას.

2. თითოეული საზედამხედველო ორგანოს წევრი ან წევრები და თანამშრომლები ევროკავშირის ან წევრი სახელმწიფოს კანონმდებლობის შესაბამისად უნდა იცავდნენ პროფესიულ საიდუმლოებას როგორც თანამდებობაზე ყოფნის დროს, ისე შემდეგაც ნებისმიერ კონფიდენციალურ ინფორმაციასთან მიმართებით, რომელიც მათთვის გახდება ცნობილი მათი ამოცანების შესრულებისას ან უფლებამოსილებების განხორციელებისას. თანამდებობაზე ყოფნის პერიოდში პროფესიული საიდუმლოების დაცვის ვალდებულება განსაკუთრებით უნდა გავრცელდეს ფიზიკური პირების მიერ წინამდებარე დირექტივის დარღვევის შესახებ განცხადების გაკეთებაზე.

ნაწილი 2

კომპეტენცია, ამოცანები და უფლებამოსილებები

მუხლი 45

კომპეტენცია

1. თითოეულმა წევრმა სახელმწიფომ უნდა უზრუნველყოს, რომ თითოეულ საზედამხედველო ორგანოს ჰქონდეს მასზე დაკისრებული ამოცანების შესრულების და მისთვის მინიჭებული უფლებამოსილებების განხორციელების კომპეტენცია, წინამდებარე დირექტივის შესაბამისად თავისი წევრი სახელმწიფოს ტერიტორიაზე.

2. თითოეულმა წევრმა სახელმწიფომ უნდა უზრუნველყოს, რომ არც ერთ საზედამხედველო ორგანოს არ ჰქონდეს სასამართლოების მიერ დამუშავებაზე ზედამხედველობის კომპეტენცია, როდესაც ისინი მოქმედებენ სასამართლო უფლებამოსილების ფარგლებში. წევრი სახელმწიფოები უფლებამოსილნი არიან, უზრუნველყონ, რომ მათ საზედამხედველო ორგანოს არ ჰქონდეს სხვა დამოუკიდებელი მართლმსაჯულების ორგანოების მიერ მონაცემთა დამუშავებაზე ზედამხედველობის კომპეტენცია, როდესაც ისინი მოქმდებენ სასამართლო უფლებამოსილებს ფარგლებში.

მუხლი 46

ამოცანები

1. თითეულმა წევრმა სახელმწიფომ უნდა უზრუნველყოს, რომ მის ტერიტორიაზე ყოველი საზედამხდველო ორგანო:

(ა) ზედამხედველობას უწევდეს და აღასრულებდეს წინამდებარე დირექტივის შესაბამისად მიღებული დებულებების და მათი საიმპლემენტაციო ღონისძიებების შესრულებას;

(ბ) ამაღლებდეს საზოგადოების ცნობიერებასა და ხელს უწყობდეს დამუშავებასთან დაკავშირებული რისკების, წესების, დაცვის გარანტიებისა და უფლებების გააზრებას;

(გ) წევრი სახლემწიფოს კანონმდებლობის შესაბამისად კონსულტაციას უწევდეს ქვეყნის პარლამენტს, მთავრობასა და სხვა უწყებებს იმ საკანონმდებლო და ადმინისტრაციულ ზომებზე, რომლებიც უკავშირდება დამუშავებასთან მიმართებით ფიზიკური პირების უფლებებისა და თავისუფლებების დაცვას;

(დ) ხელს უწყობდეს დამმუშავებლებისა და უფლებამოსილი პირების ცნობიერების ამაღლებას წინამდებარე დირექტივით გათვალისწინებული მათი მოვალეობების შესახებ;

(ე) მოთხოვნისამებრ, აწვდიდეს ინფორმაციას ნებისმიერ მონაცემთა სუბიექტს წინამდებარე დირექტივით გათვალისწინებული მათი უფლებების განხორციელების თაობაზე და საჭიროების შემთხვევაში, ამ მიზნით თანამშრომლობდეს სხვა წევრი სახელმწიფოს საზედამხედველო ორგანოებთან;

(ვ) განიხილავდეს მონაცემთა სუბიექტის, უწყების, ორგანიზაციის ან ასოციაციის საჩივრებს 55-ე მუხლის შესაბამისად და საჭირო ფარგლებში იძიებდეს საჩივრის საგანს და მომჩივანს გონივრულ ვადაში ატყობინებდეს გამოძიების მიმდინარეობისა და შედეგების შესახებ, განსაკუთრებით იმის შესახებ, რომ საჭიროა შემდგომი გამოძიება ან კოორდინირება სხვა საზედამხედველო ორგანოსთან ერთად;

(ზ) მე-17 მუხლის შესაბამისად ამოწმებდეს დამუშავების კანონიერებას და ამავე მუხლის მე-3 პუნქტის შესაბამისად გონივრულ ვადაში აცნობებდეს მონაცემთა სუბიექტს შემოწმების შედეგების ან მიზეზების შესახებ, რომელთა გამოც შემოწმება არ განხორციელებულა.

(თ) წინამდებარე დირექტივის ერთგვაროვანი გამოყენებისა და აღსრულების უზრუნველყოფის მიზნით თანამშრომლობდეს სხვა საზედამხედველო ორგანოებთან, მათ შორის ინფორმაციის გაცვლის და ორმხრივი თანამშრომლობის გაწევის გზით;

(ი) ატარებდეს გამოძიებას წინამდებარე დირექტივის შესრულებაზე, მათ შორის სხვა საზედამხედველო ორგანოდან ან საჯარო უწყებიდან მიღებული ინფორმაციის საფუძველზე;

(კ) ახორციელებდეს რელევანტური სიახლეების მონიტორინგს, რამდენადაც მათ შეიძლება გავლენა ჰქონდეთ პერსონალურ მონაცემთა დაცვაზე, კერძოდ კი საინფორმაციო და საკომუნიკაციო ტექნოლოგიების განვითარებას;

(ლ) გასცემდეს კონსულტაციას 28-ე მუხლით გათვალისწინებული დამუშავების ოპერაციებზე; და

(მ) ხელს უწყობდეს საბჭოს საქმიანობას;

2. თითოეულმა საზედამხედველო ორგანომ ხელი უნდა შეუწყოს პირველი პუნქტის (ვ) ქვეპუნქტით გათვალისწინებული საჩივრების წარდგენას ისეთი ზომების მეშვეობით, როგორიცაა საჩივრის ფორმის უზრუნველოფა, რომლის შევსება ელექტრონულადაც არის შესაძლებელი, კომუნიკაციის სხვა გზების გამორიცხვის გარეშე;

3. თითოეული საზედამხედველო ორგანოს ამოცანების შესრულება უფასო უნდა იყოს მონაცემთა სუბიექტებისა და მონაცემთა დაცვის ოფიცრისათვის.

4. თუ თხოვნა აშკარად დაუსაბუთებელი ან გადაჭარბებულია, განსაკუთრებით იმიტომ, რომ მისი წარდგენა ხდება მუდმივად, საზედამხედველო ორგანოს უფლება აქვს, დააწესოს გონივრული საფასური ადმინისტრაციული ხარჯების გათვალისწინებით, ან უარი თქვას თხოვნის შესრულებაზე. საზედამხედველო ორგანოს ეკისრება მტკიცების ტვირთი, რომ თხოვნა აშკარად დაუსაბუთებელი ან გადაჭარბებულია.

მუხლი 47

უფლებამოსილებანი

1. თითოეულმა წევრმა სახელმწიფომ კანონმდებლობით უნდა უზრუნველყოს, რომ თითოეულ საზედამხედველო ორგანოს ჰქონდეს ეფექტური საგამოძიებო უფლებამოსილება. ამ უფლებამოსილებებში, სულ მცირე, უნდა შედიოდეს დამმუშავებლის და უფლებამოსილი პირისაგან დამუშავების პროცესში მყოფ პერსონალურ მონაცემებზე და მისი ამოცანების შესასრულებლად აუცილებელ ყველა ინფორმაციაზე წვდომის მოპოვების უფლებამოსილება.

2. თითოეულმა წევრმა სახელმწიფომ კანონმდებლობით უნდა უზრუნველყოს, რომ თითოეულ საზედამხედველო ორგანოს ჰქონდეს კანონის აღსრულების მიზნით გამოყენებული ეფექტური ღონისძიებები, როგორებიცაა, მაგალითად:

(ა) დამმუშავებლის ან უფლებამოსილი პირის გაფრთხილება, რომ დამუშავების დაგეგმილი ოპერაციები დიდი ალბათობით გამოიწვევენ წინამდებარე დირექტივის შესაბამისად მიღებული დებულებების დარვევას;

(ბ) დამმუშავებლის ან უფლებამოსილი პირისათვის დავალების მიცემა, რომ წინამდებარე დირექტივის შესაბამისად მიღებულ დებულებებთან შესაბამისობაში მოიყვანონ დამუშავების ოპერაციები, საჭიროების შემთხვევაში კონკრეტული გზით და კონკრეტულ ვადაში, კერძოდ, მე-16 მუხლის შესაბამისად პერსონალურ მონაცემთა გასწორების, წაშლის ან მონაცემთა დაბლოკვის შესახებ დავალების მიცემით;

(გ) დროებითი ან მუდმივი შეზღუდვის, მათ შორის დამუშავების აკრძალვის დაკისრება;

3. თითოეულმა წევრმა სახელმწიფომ კანონმდებლობით უნდა უზრუნველყოს, რომ თითოეულ საზედამხედველო ორგანოს გააჩნდეს ეფექტური საკონსულტაციო უფლებამოსილება, რომ კონსულტაცია გაუწიოს დამმუშავებელს 28-ე მუხლით გათვალისწინებული წინასწარი კონსულტაციის პროცედურისას და საკუთარი ინიციატივით ან მოთხოვნისამებრ მიაწოდოს მოსაზრებები პარლამენტს, მთავრობას ან ეროვნული კანონმდებლობის შესაბამისად სხვა საჯარო დაწესებულებებს და უწყებებს, ისევე მიაწოდოს მოსაზრებები საზოგადოებას პერსონალური მონაცემების დაცვასთან დაკავშირებულ ნებისმიერ საკითხზე.

4. საზედამხედველო ორგანოს მიერ წინამდებარე მუხლით მისთვის მინიჭებული უფლებამოსილებების განხორციელება სათანადოდ უნდა იყოს დაცული, დაცვის ეფექტური სასამართლო და პროცესუალური საშუალებებით, როგორც ეს ევროკავშირის და წევრი სახელმწიფოს კანონმდებლობითაა განსაზღვრული, ქარტიის შესაბამისად.

5. თითოეულმა წევრმა სახელმწიფომ კანონმდებლობით უნდა უზრუნველყოს, რომ თითოეულ საზედამხედველო ორგანოს, ჰქონდეს უფლებამოსილება, წინამდებარე დირექტივის საფუძველზე მიღებული დებულებების დარღვევების საკითხი წარუდგინოს სასამართლო ორგანოებს და საჭიროების შემთხვევაში, წინამდებარე დირექტივის შესაბამისად მიღებული დებულებების აღსრულების მიზნით დაიწყოს სამართალწარმოება ან ჩაერთოს მასში.

მუხლი 48

სამართალდარღვევათა შეტყობინება

წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ კომპეტენტურმა ორგანოებმა შეიმუშაონ ეფექტური მექანიზმები წინამდებარე დირექტივის დარღვევის კონფიდენციალურად შეტყობინებისათვის.

მუხლი 49

საქმიანობის ანგარიშები

თითოეულმა საზედამხედველო ორგანომ უნდა მოამზადოს თავისი საქმიანობის წლიური ანგარიში, რომელიც შეიძლება შეიცავდეს შეტყობინების სახით მიღებული სამართალდარღვევების და დაკისრებული სანქციების ტიპების სიას. ანგარიშები უნდა წარედგინოს სახელმწიფოს პარლამენტს, მთავრობას და სხვა უწყებებს წევრი სახელმწიფოს

კანონმდებლობის შესაბამისად. ანგარიშები ხელმისაწვდომი უნდა იყოს საზოგადოებისათვის, კომისიისა და საბჭოსთვის.

თავი VII

თანამშრომლობა

მუხლი 50

ურთიერთდახმარება

1. თითოეულმა სახელმწიფომ უნდა უზრუნველყოს, რომ მათმა საზედამხედველო ორგანოებმა ერთმანეთს მიაწოდონ შესაბამისი ინფორმაცია და გაუწიონ ურთიერთდახმარება წინამდებარე დირექტივის ერთგვაროვანი შესრულებისა და გამოყენებისათვის და შეიმუშაონ ერთმანეთთან ეფექტური თანამშრომლობის ზომები. ურთიერთდახმარება უნდა მოიცავდეს ინფორმაციის შესახებ თხოვნისა და საზედამხედველო ფუნქციის შესრულების თხოვნების გაცვლას ისეთ საკითხებზე, როგორიცაა კონსულტაციის გაწევა, ინსპექტირებისა და გამოძიების ჩატარება.

2. თითოეულმა წევრმა სახელმწიფომ უნდა უზრუნველყოს, რომ თითოეულმა საზედამხედველო ორგანომ მიიღოს ყველა სათანადო ზომა სხვა საზედამხედველო ორგანოს თხოვნის შესასრულებლად დაუყოვნებილივ და მისი მიღებიდან არაუგვიანეს 1 თვისა. ასეთი ზომები შესაძლოა მოიცავდეს გამოძიების მიმდინარეობის შესახებ შესაბამისი ინფორმაციის გადაგზავნას.

3. დახმარების თხოვნა უნდა შეიცავდეს ყველა აუცილებელ ინფორმაციას, მათ შორის, თხოვნის მიზანსა და მიზეზებს. გაგზავნილი ინფორმაცია შეიძლება გამოყენებული იქნეს მხოლოდ იმ მიზნისთვის, რომლისთვისაც მოხდა მისი გამოთხოვა.

4. თხოვნის მიმღებმა საზედამხედველო ორგანომ უარი არ უნდა თქვას თხოვნის შესრულებაზე, გარდა იმ შემთვევისა თუ:

(ა) მას არ გააჩნია კომპეტენცია თხოვნაში მითითებულ საკითხზე ან არ არის უფლებამოსილი, მიიღოს მოთხოვნილი ზომები;

(ბ) თხოვნის შესრულება ეწინააღმდეგება წინამდებარე დირექტივას ან წევრი სახელმწიფოს კანონმდებლობას, რომლის შესრულებაც სავალდებულოა თხოვნის მიმღები საზედამხედველო ორგანოსთვის.

5. თხოვნის მიმღებმა საზედამხედველო ორგანომ უნდა შეატყობინოს თხოვნის წარმდგენ საზედამხედველო ორგანოს შედეგების ან თხოვნის საპასუხოდ მიღებული ზომების

მიმდინარეობის შესახებ. თხოვნის მიმღებმა საზედამხედველო ორგანომ უნდა დაასაბუთოს თხოვნის შესრულებაზე უარი მე-4 პუნქტის შესაბამისად.

6. თხოვნის მიმღება ორგანომ, როგორც წესი, სხვა საზედამხედველო ორგანოს მიერ მოთხოვნილი ინფორმაცია უნდა წარადგინოს ელექტრონულად, სტანდარტიზებული ფორმატის გამოყენებით.

7. თხოვნის მიმღებმა საზედამხედველო ორგანოებმა არ უნდა დააწესონ საფასური ნებისმიერი ზომისათვის, რომელიც მათ მიიღეს ურთიერთდახმარების შესახებ თხოვნის საფუძველზე. საზედამხედველო ორგანობი შეიძლება შეთანხმდნენ ერთმანეთისათვის კონკრეტული დანახარჯების ანაზღაურების დაკისრებაზე, რომელიც საგამონაკლისო შემთხვევებში ურთიერთდახმარების გაწევითაა გამოწვეული.

8. კომისია უფლებამოსილია საიმპლემენტაციო აქტებით დააზუსტოს ამ მუხლით გათვალისწინებული ურთიერთდახმარების ფორმატი და პროცედურები და საზედამხედველო ორგანოებს, ასევე საზედამხედველო ორგანოებსა და საბჭოს შორის ინფორმაციის ელექტრონულად გაცვლის წესები. მითითებული საიმპლემენტაციო აქტები მიღებული უნდა იყოს 58-ე მუხლის მე-2 პუნქტით გათვალისწინებული შემოწმების პროცედურის შესაბამისად.

მუხლი 51

საბჭოს ამოცანები

1. ევროკავშირის (EU) 2016/679 რეგულაციით შექმნილმა საბჭომ უნდა შეასრულოს დამუშავებასთან დაკავშირებული ყველა ჩამოთვლილი ამოცანა წინამდებარე დირექტივის ფარგლებში:

(ა) კონსულტაცია გაუწიოს კომისიას ევროკავშირში პერსონალურ მონაცემთა დაცვასთან დაკავშირებულ ნებისმიერ საკითხზე, მათ შორის წინამდებარე დირექტივის ნებისმიერი ცვლილების პროექტზე;

(ბ) საკუთარი ინიციატივით, თავისი წევრების ან კომისიის თხოვნით განიხილოს წინამდებარე დირექტივის გამოყენებასთან დაკავშირებული ნებისმიერი საკითხი და გამოაქვეყნოს სახელმძღვანელო, რეკომენდაციები და საუკეთესო გამოცდილება წინამდებარე დირექტივის ერთგვაროვანი გამოყენების ხელშეწყობის მიზნით;

(გ) საზედამახედველო ორგანოებისათვის მოამზადოს სახელმძღვანელო 47-ე მუხლის პირველი და მე-3 პუნქტებით გათვალისწინებული ზომების გამოყენების საკითხზე;

(დ) გამოაქვეყნოს სახელმძღვანელო, რეკომენდაციები და საუკეთესო გამოცდილება ამ პუნქტის (ბ) ქვეპუნქტის შესაბამისად პერსონალურ მონაცემთა უსაფრთხოების დარღვევის ინციდენტის და 30-ე მუხლის პირველი და მე-2 პუნქტებით გათვალისწინებული დაუყოვნებლივი შეტყობინების განსამარტად და კონკრეტული გარემოებების დასადგენად, რომლებშიც დამმუშავებელს ან უფლებამოსილ პირს ეკისრებათ პერსონალურ მონაცემთა უსაფრთხოების დარღვევის ინციდენტის შეტყობინების ვალდებულება;

(ე) გამოსცეს სახელმძღვანელო, რეკომენდაციები და საუკეთესო გამოცდილება ამ პუნქტის (ბ) ქვეპუნქტის შესაბამისად იმ გარემოებების შესახებ, რომელთა დადგომის შემთხვევაშიც პერსონალურ მონაცემთა უსაფრთხოების ინციდენტი დიდი ალბათობით შეუქმნის საფრთხეს ფიზიკური პირების უფლებებსა და თავისუფლებებს, როგორც ეს მითითებულია 31-ე მუხლის პირველ პუნქტში;

(ვ) შეამოწმოს (ბ) და (გ) ქვეპუნქტებში მითითებული სახელმძღვანელოების, რეკომენდაციებისა და საუკეთესო გამოცდილების პრაქტიკაში გამოყენება;

(ზ) კომისიას მიაწოდოს მოსაზრება მესამე ქვეყანაში, ტერორიაზე ან მესამე ქვეყნის რამდენიმე კონკრეტულ სექტორში ან საერთაშორისო ორგანიზაციაში დაცვის სათანადო სტანდარტების შესაფასებლად, მათ შორის იმის შესაფასებლად, რომ მესამე ქვეყანა, ტერიტორია ან მესამე ქვეყნის რამდენიმე კონკრეტული სექტორი ან საერთაშორისო ორგანიზაცია ვეღარ უზრუნველყოფს დაცვის სათანადო სტანდარტს;

(თ) ხელი შეუწყოს საზედამხედველო ორგანოებს შორის თანამშრომლობას და ინფორმაციისა და საუკეთესო გამოცდილების ეფექტურ ორმხრივ და მრავალმხრივ გაცვლას;

(ი) ხელი შეუწყოს საზედამხედველო ორგანოებს შორის, საჭიროების შემთხვევაში - მესამე ქვეყნების საზედამხედველო ორგანოებთან და საერთაშორისო ორგანიზაციებთან გადამზადების პროგრამებისა და თანამშრომლების გაცვლას;

კ) ხელი შეუწყოს მსოფლიოს ქვეყნების საზედამხედველო ორგანოებს შორის მონაცემთა დაცვის კანონმდებლობასა და პრაქტიკაზე ცოდნისა და დოკუმენტების გაცვლას.

პირველი პუნქტის (ზ) ქვეპუნქტთან მიმართებით კომისიამ უნდა მიაწოდოს საბჭოს ყველა საჭირო დოკუმენტაცია, მათ შორის მიმოწერა მესამე სახელმწიფოს მთავრობასთან, მესამე ქვეყნის ტერიტორიასთან, კონკრეტულ სექტორთან ან საერთაშორისო ორგანიზაციასთან.

2. თუ კომისია საბჭოსგან ითხოვს რჩევას, ის უფლებამოსილია, დაადგინოს ვადა საკითხის გადაუდებლობის გათვალისწინებით.

3. საბჭომ თავისი მოსაზრებები, სახელძღვანელოები, რეკომენდაციები და საუკეთესო გამოცდილება უნდა მიაწოდოს კომისიას და 58-ე მუხლის პირველი ნაწილით გათვალისწინებულ კომიტეტს და უზრუნველყოს მათი საჯაროდ გამოქვეყნება.

4. კომისიამ უნდა შეატყობინოს საბჭოს იმ ზომების შესახებ, რომლებიც მიიღო საბჭოს მოსაზრებების, სახელძღვანელოების, რეკომენდაციებისა და საუკეთესო გამოცდილების გამოქვეყნების შემდეგ.

თავი VIII

სამართლებრივი დაცვის საშუალებები, პასუხისმგებლობა და სახდელები

მუხლი 52

საზედამხედველო ორგანოსთვის საჩივრით მიმართვის უფლება

1. ნებისმიერი სხვა ადმინისტრაციული ან სამართლებრივი დაცვის საშუალების შეუზღუდავად, წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ მონაცემთა ყველა სუბიექტს ჰქონდეს საზედამხედველო ორგანოსათვის საჩივრით მიმართვის უფლება თუ მონაცემთა სუბიექტი მიიჩნევს, რომ მასთან დაკავშირებული პერსონალური მონაცემების დამუშავება ეწინააღმდეგება წინამდებარე დირექტივის საფუძველზე მიღებულ დებულებებს.

2. წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ საზედამხედველო ორგანომ, რომელმაც მიიღო საჩივარი, დაუყოვნებლივ მიაწოდოს ის კომპეტენტურ საზედამხედველო ორგანოს თუ საჩივარი მიიღო საზედამხედველო ორგანომ, რომელიც 45-ე მუხლის პირველი პუნქტის შესაბამისად არ წარმოადგენს კომპეტენტურ ორგანოს. მონაცემთა სუბიექტს უნდა ეცნობოს საჩივრის გადაგზავნის შესახებ.

3. წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ საჩივრის მიმღებმა ორგანომ მოთხოვნისამებრ მონაცემთა სუბიექტს გაუწიოს დამატებითი დახმარება.

4. საზედამხედველო ორგანომ მონაცემთა სუბიექტს უნდა შეატყობინოს საჩივრის განხილვის მიმდინარეობისა და შედეგების შესახებ, მათ შორის, აცნობოს 53-ე მუხლის შესაბამისად სამართლებრივი დაცვის საშუალების გამოყენების შესაძლებლობის შესახებ.

მუხლი 53

საზედამხედველო ორგანოს წინააღმდეგ დაცვის ეფექტური სამართლებრივი საშუალების გამოყენების უფლება

1. ნებისმიერი სხვა ადმინისტრაციული ან არასამართლებრივი დაცვის საშუალების შეუზღუდავად, წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ ფიზიკურ ან იურიდიულ პირს ჰქონდეს საზედამხედველო ორგანოს სამართლებრივად სავალდებულო გადაწყვეტილების წინააღმდეგ ეფექტური სამართლებრივი დაცვის საშუალების გამოყენების უფლება.
2. ნებისმიერი სხვა ადმინისტრაციული ან არასამართლებრივი დაცვის საშუალების შეუზღუდავად, მონაცემთა სუბიექტს უნდა ჰქონდეს სამართლებრივი დაცვის ეფექტური საშუალების გამოყენების უფლება, როდესაც საზედამხედველო ორგანო, რომელიც 45-ე მუხლის პირველი ნაწილის შესაბამისად კომპეტენტურია, არ განიხილავს საჩივარს ან სამი თვის ვადაში არ შეატყობინებს მონაცემთა სუბიექტს 52-ე მუხლის შესაბამისად წარდგენილი საჩივრის განხილვის მიმდინარეობის ან შედეგების შესახებ.
3. წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ საზედამხედველო ორგანოების წინააღმდეგ სამართალწარმოება დაიწყოს იმ წევრი სახელმწიფოს სასამართლოში, რომელშიც საზედამხედველო ორგანოა განთავსებული.

მუხლი 54

დამმუშავებლის ან უფლებამოსილი პირის წინააღმდეგ დაცვის ეფექტური სამართლებრივი საშუალების გამოყენების უფლება

ნებისმიერი სხვა ადმინისტრაციული ან არასამართლებრივი დაცვის საშუალების შეუზღუდავად, მათ შორის, 52-ე მუხლის შესაბამისად საზედამხედველო ორგანოსათვის საჩივრით მიმართვის უფლების შეუზღუდავად, წევრმა სახელმწიფოებმა უნდა უზუნველყონ, რომ მონაცემთა სუბიექტს ჰქონდეს დაცვის ეფექტური სამართლებრივი საშუალების გამოყენების უფლება თუ მონაცემთა სუბიექტი მიიჩნევს, რომ წინამდებარე დირექტივის საფუძველზე მიღებული დებულებებით გათვალისწინებული მისი უფლებები დაირღვა მისი პერსონალური მონაცემების ამ დებულებების დარღვევით დამუშავების პროცესში.

მუხლი 55

მონაცემთა სუბიექტის წარმომადგენელი

წევრმა სახელმწიფოებმა საპროცესო კანონმდებლობის შესაბამისად უნდა უზრუნველყონ, რომ მონაცემთა სუბიექტს ჰქონდეს უფლება, არაკომერციულ უწყებას, ორგანიზაციას ან ასოციაციას, რომელიც წევრი სახელმწიფოს კანონმდებლობის შესაბამისადაა შექმნილი,

აქვს წესდებით გათვალისწინებული და საჯარო ინტერესებში შემავალი მიზნები და მომღვაწეობს მონაცემთა სუბიექტების უფლებებისა და თავისუფლებების დაცვის სფეროში, მიანიჭოს უფლება, მისი სახელით შეიტანოს საჩივარი და ისარგებლოს 52-ე, 53-ე და 54-ე მუხლებით გათვალისწინებული უფლებებით.

მუხლი 56

კომპენსაციის მიღების უფლება

წევრმა სახელმწიფოებმა უნდა უზრუნველყონ, რომ ნებისმიერ პირს, რომელსაც მიადგა მატერიალური ან არამატერიული ზიანი მონაცემთა უკანონო დამუშავების ან წინამდებარე დირექტივის საფუძველზე მიღებული ეროვნული დებულებების დარღვევის შედეგად, ჰქონდეს კომპენსაციის მიღების უფლება იმ ზიანისათვის, რომელიც დამმუშავებლისგან ან წევრი სახელმწიფოს კანონმდებლობის შესაბამისად განსაზღვრული კომპეტენტური ორგანოს ქმედებით მიადგა.

მუხლი 57

სახდელები

წევრმა სახელმწიფოებმა უნდა განსაზღვრონ სახდელების დადების წესი წინამდებარე დირექტივის შესაბამისად მიღებული დებულებების დარვევებისათვის და მიიღონ ყველა აუცილებელი ზომა მათ აღსასრულებლად. დადგენილი სახდელები უნდა იყოს ეფექტური, პროპორციული და ჰქონდეს შემაკავებელი ეფექტი.

თავი IX

საიმპლემენტაციო აქტები

მუხლი 58

კომიტეტის პროცედურა

1. კომისიას დახმარებას უწევს კომიტეტი, რომელიც შექმნილია (EU) 2016/679 რეგულაციის 93-ე მუხლის შესაბამისად. ხსენებული კომიტეტი წარმოადგენს კომიტეტს (EU) No 182/2011 რეგულაციის მიზნებისათვის.
2. წინამდებარე პუნქტზე მითითების შემთხვევაში, მოქმედებს (EU) No 182/2011 რეგულაციის მე-5 მუხლი.
3. წინამდებარე პუნქტზე მითითების შემთხვევაში, მოქმედებს (EU) No 182/2011 რეგულაციის მე-8 და მე-5 მუხლები.

თავი X

დასკვნითი დებულებები

მუხლი 59

2008/977/JHA ჩარჩო გადაწყვეტილების გაუქმება

1. 2018 წლის 6 მაისიდან 2008/977/JHA ჩარჩო გადაწყვეტილება ძალადაკარგულია.

2. პირველი პუნქტით გათვალისწინებულ გადაწყვეტილებაზე გაკეთებული მითითებანი უნდა ჩაითვალოს წინამდებარე დირექტივაზე მითითებად.

მუხლი 60

ევროკავშირის ძალაში შესული სამართლებრივი აქტები

ევროკავშირის სამართლებრივ აქტებში მოცემული პერსონალურ მონაცემთა დაცვის კონკრეტული დებულებები სისხლის სამართლის საქმეებზე სამართლებრივი დახმარებისა და საპოლიციო თანამშრომლობის სფეროში, რომლებიც ძალაში 6 მაისს ან მანამდე შევიდა და არეგულირებს წევრ სახელმწიფოებს შორის დამუშავებას და წევრი სახელმწიფოს უფლებამოსილი ორგანოების მიერ წინამდებარე დირექტივის ფარგლებში არსებული ხელშეკრულებების შესაბამისად შექმნილ საინფორმაციო სისტემებთან წვდომას, ძალაში რჩება.

მუხლი 61

მიმართება სისხლის სამართლის საქმეებზე სამართლებრივი დახამრებისა და საპოლიციო თანამშრომლობის სფეროში მანამდე გაფორმებულ საერთაშორისო შეთანხმებებთან

საერთაშორისო შეთანხმებები, რომლებიც შეეხება პერსონალურ მონაცემთა გადაცემას მესამე სახელმწიფოს ან საერთაშორისო ორგანიზაციისათვის, რომლებიც წევრმა სახელმწიფოებმა 2016 წლის 6 მაისამდე გააფორმეს და რომლებიც მითითებულ თარიღამდე შეესაბამებოდა ევროკავშირის კანონმდებლობას, რჩება ძალაში მათ შეცვლამდე, ჩანაცვლებამდე ან გაუქმებამდე.

მუხლი 62

კომისიის ანგარიშები

1. 2022 წლის 6 მაისისათვის და შემდგომ ყოველ მეოთხე წელს კომისიამ ევროპარლამენტსა და ევროსაბჭოს უნდა წარუდგინოს ანგარიში წინამდებარე დირექტივის შეფასებისა და შემოწმების შესახებ. ანგარიშები საჯაროდ უნდა გამოქვეყნდეს.

2. პირველ პუნქტში მითითებულ შეფასებასა და შემოწმებასთან მიმართებით კომისიამ განსაკუთრებულად უნდა შეამოწმოს პერსონალური მონაცემების მესამე სახელმწიფოებისა და საერთაშორისო ორგანიზაციებისათვის გადაცემასთან დაკავშირებული მე-5 თავის გამოყენება და ფუნქციონირება, განსაკუთრებით კი 36-ე მუხლის მე-3 პუნქტისა და 39-ე მუხლის შესაბამისად მიღებული გადაწყვეტილებები.

3. პირველი და მე-2 პუნქტის მიზნებისათვის კომისია უფლებამოსილია წევრი სახელმწიფოებისაგან და საზედამხედველო ორგანოებისაგან მოითხოვოს ინფორმაცია.

4. პირველი და მე-2 პუნქტებით გათვალისწინებული შეფასებებისა და შემოწმების განხორციელებისას, კომისიამ მხედველობაში უნდა მიიღოს ევროპის პარლამენტის, ევროპის საბჭოს და სხვა შესაბამისი უწყებებისა და წყაროების პოზიციები და დასკვნები.

5. აუცილებლობის შემთხვევაში კომისიამ უნდა მოახდინოს წინამდებარე დირექტივის ცვლილების ინიცირება, განსაკუთრებით ინფრორმაციული ტექნოლოგიებისა და ინფორმაციული საზოგადოების განვითარების გათვალისწინებით.

6. 2019 წლის 6 მაისისათვის კომისიამ უნდა გადასინჯოს ევროკავშირის სხვა სამართლებრივი აქტები, რომლებიც არეგულირებენ კომპეტენტური ორგანოების მიერ დამუშავებას პირველი მუხლის პირველი პუნქტის მიზნებისავის, მათ შორის მე-60 მუხლით გათვალისწინებული აქტები იმისათვის, რომ მოახდინოს მათი წინამდებარე დირექტივასთან შესაბმისობაში მოყვანა და საჭიროების შემთხვევაში წარადგინოს მათი შეცვლის ინიციატივა წინამდებარე დირექტივის ფარგლებში პერსონალურ მონაცემთა დაცვის ერთგვაროვანი მიდგომების უზრუნველსაყოფად.

მუხლი 63

ტრანსპოზიცია

1. 2018 წლის 6 მაისისათვის წევრმა სახელმწიფოებმა უნდა მიიღონ და გამოაქვეყნონ კანონები, რეგულაციები და ადმინისტრაციული დებულებები, რომლებიც აუცილებელია წინამდებარე დირექტივასთან შესაბამისობის უზრუნველსაყოფად. მათ უნდა მიაწოდონ კომისიას მიღებული დებულებების ტექსტები. დებულებების გამოყენება უნდა მოხდეს 2018 წლის 6 მაისიდან. როდესაც წევრი სახელმწიფოები მიიღებენ ხსენებულ დებულებებს, ისინი უნდა შეიცავდნენ მითითებას წინამდებარე დირექტივაზე ან უნდა ახლდეთ ასეთი

მითითება ოფიციალური გამოქვეყნებისას. წევრმა სახელმწიფოებმა თავად უნდა განსაზღვრონ, როგორ უნდა გაკეთდეს ასეთი მითითება.

2. როგორც გამონაკლისი პირველი პუნქტისაგან, წევრ სახლემწიფოს უფლება აქვს, საგამონაკლისო წესით, უზრუნველყოს, რომ ავტომატური დამუშავების სისტემები, რომლებიც დაინერგა 2016 წლის 6 მაისამდე 25-ე მუხლის პირველ პუნქტთან შესაბამისობაში იქნეს მყვანილი 2023 წლის 6 მაისამდე, თუ ეს არაპროპორციულ ძალისხმევას საჭიროებს.

3. როგორც გამონაკლისი წინამდებარე მუხლის პირველი და მე-2 პუნქტებიდან, წევრ სახელმწიფოს უფლება აქვს, საგამონაკლისო წესით, ავტომატური დამუშავების სისტემა 25-ე მუხლის პირველ პუნქტთან შესაბამისობაში მოიყვანოს, როგორც ეს მითითებულია ამ მუხლის მე-2 პუნქტში, კონკრეტული ვადის განმავლობაში ამ მუხლის მე-2 პუნქტში მითითებული ვადის გასვლის შემდეგ თუ სხვაგვარად მნიშვნელოვანი დაბრკოლებები შეექმნება ამ კონკრეტული ავტომატური დამუშავების სისტემის მუშაობას. წევრმა სახელმწიფომ უნდა შეატყობინოს კომისიას ხსენებული დაბრკოლებების საფუძვლებისა და კონკრეტული ვადის შესახებ, რომლის განმავლობაშიც ის ავტომატური დამუშვების სისტემას მოიყვანს 25-ე მუხლის პირველ პუნქტთან შესაბამისობაში. ეს კონკრეტული ვადა ნებისმიერ შემთხვევაში არ უნდა გადასცდეს 2026 წლის 6 მაისს.

4. წევრმა სახელმწიფოებმა უნდა მიაწოდონ კომისიას ეროვნული კანონმდებლობის ძირითადი დებულებების ტექსტი, რომელიც მიღებულია წინამდებარე დირექტივით გათვალისწინებულ სფეროში.

მუხლი 64

ძალაში შესვლა

წინამდებარე დირექტივა ძალაში შედის ევროკავშირის ოფიციალურ ჟურნალში მისი გამოქვეყნებიდან მეორე დღეს.

მუხლი 65

ადრესატები

წინამდებარე დირექტივის ადრესატებს წევრი სახელმწიფოები წარმოადგენენ.

დადებულია ბრიუსელში, 2016 წლის 27 აპრილს

ევროპარლამენტის სახელით

პრეზიდენტი

მ. შულცი

საბჭოს სახელით

პრეზიდენტი

ჯ.ა. ჰენის-პლეშარტი