COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

სტრასბურგი, 7 ივნისი 2024

T-PD(2023)2rev6

პერსონალური მონაცემების ავტომატურ დამუშავებასთან დაკავშირებით ფიზიკურ პირთა დაცვის შესახებ კონვენციის საკონსულტაციო კომიტეტი

108-ე კონვენცია

სახელმძღვანელო დოკუმენტი ამომრჩეველთა რეგისტრაციისა და ავთენტიფიკაციის მიზნით პერსონალურ მონაცემთა დამუშავების შესახებ

www.coe.int/dataprotection

სარჩევი

1. შესავალი 1

2. ფარგლები და მიზანი 4

3. სახელმძღვანელოს მიზნებისათვის ტერმინთა განმარტება 4

4. 108+ კონვენციის გავრცელება ამომრჩეველთა პერსონალური მონაცემების გამოყენებაზე რეგისტრაციისა და ავთენტიფიკაციის დროს 6

4.1 მონაცემთა დამუშავების ლეგიტიმაცია და მონაცემთა ხარისხი ამომრჩეველთა რეგისტრაციისა და ავთენტიფიკაციისთვის (მუხლი 5) 6

4.2 განსაკუთრებული კატეგორიის მონაცემების (მათ შორის ბიომეტრიული მონაცემების) დამუშავება, რომელიც ცალსახად ახდენს პირის იდენტიფიცირებას ამომრჩეველთა რეგისტრაციისა და ავთენტიფიკაციის პროცესში (მუხლი 6) 9

4.3 მონაცემთა უსაფრთხოება და კონფიდენციალობა (მუხლი 7) 10

4.4 პერსონალური მონაცემების დამუშავების გამჭვირვალობა ამომრჩეველთა რეგისტრაციისა და ავთენტიფიკაციის პროცესში (მუხლი 8) 12

4.5 მონაცემთა სუბიექტის უფლებები (მუხლი 9) 13

4.6 დამატებითი ვალდებულებები და რეკომენდაციები არჩევნების მართვის ორგანოებისა და მონაცემთა დამუშავებისთვის პასუხისმგებელი პირებისთვის (მუხლი 10) 14

4.7 ამომრჩეველთა რეგისტრაციისა და ავთენტიფიკაციისათვის ბიომეტრიული მონაცემების დამუშავების დამატებითი ვალდებულებები 16

1. შესავალი

საარჩევნო პროცესის წარმართვისას, ნებისმიერმა სახელმწიფომ უნდა უზრუნველყოს, რომ მხოლოდ ხმის მიცემის უფლების მქონე პირები მოხვდნენ ოფიციალურ საარჩევნო რეესტრებში და შეძლონ საკუთარი ვინაობის დადასტურება. დროთა განმავლობაში სხვადასხვა დემოკრატიული ქვეყანა განსხვავებულ მეთოდებს იყენებდა ამომრჩეველთა სანდო და ზუსტი რეგისტრაციის ("Voter Registration") უზრუნველსაყოფად და ხმის მიცემის პროცესში მათი ავთენთიფიკაციისთვის ("Authentication"). განვითარებული დემოკრატიული ქვეყნებისთვის, ამომრჩეველთა რეგისტრაციისა და ავტორიზაციის სისტემები, როგორც წესი, ემყარება განსხვავებულ ინსტიტუციურ და ადმინისტრაციულ პრაქტიკას, რომელსაც ძლიერი ფესვები აქვს მათ პოლიტიკურ კულტურაში.

ბოლო წლების განმავლობაში, სხვადასხვა სახელმწიფომ დანერგა ამომრჩეველთა რეგისტრაციისა და ავთენტიფიკაციის ახალი მეთოდები, რომლებიც ბიომეტრიულ მონაცემებს ეყრდნობა. ეს ტენდენცია განპირობებულია სხვადასხვა ფაქტორით. გავრცელებული მოსაზრების თანახმად, ტექნოლოგიას შეუძლია გადაჭრას არჩევნებთან დაკავშირებული პრობლემური საკითხები. გლობალური ბიომეტრიული ინდუსტრია ხელს უწყობს ამომრჩეველთა რეგისტრაციისა და ავთენტიფიკაციის ახალ ფორმებს, რათა დამკვიდრდეს პრინციპი „ერთი ამომრჩეველი, ერთი ხმა", როგორც თავისუფალი და გამჭვირვალე არჩევნების განხორციელების წინაპირობა. „ციფრული იდენტობის" უნივერსალური უფლებების ხელშეწყობის მიზნით, მუშავდება სხვადასხვა საერთაშორისო ორგანიზაციების, ევროსაბჭოს სახელმძღვანელო დოკუმენტები.[1]

ციფრულ იდენტობასთან დაკავშირებული უფლებები და სახელმწიფო სერვისებზე უსაფრთხო ონლაინ წვდომა გლობალურ გამოწვევას წარმოადგენს. მოქალაქის ავთენტიფიკაციის ახალი ციფრული ფორმების დანერგვისას, ინდივიდის სამართლებრივი იდენტობის დასადასტურებლად, სახელმწიფო სერვისებზე წვდომის მიზნით, მიზანშეწონილი იქნება ამომრჩეველთა რეგისტრაციისა და ავთენტიფიკაციის პროცესში მსგავსი ტექნოლოგიის გამოყენება. ტენდენცია განსაკუთრებით შესამჩნევია განვითარებად ქვეყნებში.

დისტანციურად ხმის მიცემის ("remote voting") მექანიზმის დანერგვის მიზნით, რომლისთვისაც საჭიროა ავთენტიფიკაციის ახალი და განსხვავებული მეთოდები, ზოგიერთი სახელმწიფო საპილოტე რეჟიმში იყენებს მას. ამომრჩეველთა ერთიანი

[1] Council of Europe, Consultative Committee on the Convention for the protection of individuals with regard to the automatic processing of personal data, Guidelines on National Digital Identity. Strasbourg: Council of Europe (February 2023)

რეესტრისა და ამომრჩეველთა სიების შეგროვება და შენახვა შესაძლებელია სხვადასხვა გზით — როგორც ციფრული, ასევე არაციფრული მედიის გამოყენებით, ეროვნული ან ადგილობრივი ხელისუფლების მიერ.

არჩევნების ჩატარებისა და პერსონალურ მონაცემთა დამუშავების პრაქტიკას სხვადასხვა ადმინისტრაციული და ინსტიტუციური ფაქტორი აყალიბებს: საარჩევნო სისტემა; პარტიული სისტემა; ცენტრალურ და ადგილობრივ პარტიულ ორგანიზაციებს შორის ურთიერთობა; „პირველადი არჩევნების“ (“Primary Elections“) არსებობა; ხმის მიცემის სავალდებულო მოთხოვნები; რეფერენდუმის სიხშირე და სხვა.

ბიომეტრიული მონაცემები წარმოადგენს განსაკუთრებული კატეგორიის მონაცემების ერთ-ერთ სახეს, რომელსაც დაცვის უფრო მაღალი სტანდარტი გააჩნია, რაც გამყარებულია საერთაშორისოსამართლებრივი მექანიზმებით, კერძოდ, ევროპის საბჭოს კონვენცია „პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ“ (ETS № 108), რომელიც განახლებულ იქნა ცვლილებათა ოქმით CETS № 223[2] ("კონვენცია 108+“). განსაკუთრებული კატეგორიის მონაცემების დამუშავებამ, შესაძლოა, მნიშვნელოვანი რისკი[3] გამოიწვიოს პირის პირადი ცხოვრების ხელშეუხებლობის უფლებისა და სხვა ძირითადი უფლებების დარღვევის თვალსაზრისით. წინამდებარე სახელმძღვანელოში განხილულია შემდეგი რისკები: ხმის მიცემის ფარულობა, ამომრჩეველთა დაშინება და დისკრიმინაცია, ამომრჩეველთა რეესტრში მონაცემების უსაფრთხოების დარღვევა, პოლიტიკური კამპანიების მიზნებისთვის ოფიციალური რეესტრის მონაცემების გამოყენება და ამომრჩეველთა რეგისტრაციასთან დაკავშირებული მონაცემთა ბაზების ინტეგრაცია მოსახლეობის ეროვნულ რეესტრებთან და კერძო მონაცემთა ბაზებთან.

108+ კონვენციის გამოყენების შესახებ სხვა სახელმძღვანელო დოკუმენტები, შესაძლოა, ასევე, ეხებოდეს ამომრჩეველთა რეგისტრაციისა და ავთენტიფიკაციის მიზნით პერსონალური მონაცემების დამუშავებას: პოლიტიკურ კამპანიას,[4]

[2] Council of Europe (2018), Convention for the protection of individuals with regard to the processing of personal data (2018) at: https://rm.coe.int/convention-108-for-the-protection-of-individuals (hereafter Convention 108+).
[3] Council of Europe (2018). Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data, at: https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-conventionfo/16808ac91a. Para 57.
[4] Council of Europe (2021). Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data. Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns. Strasbourg: Council of Europe (adopted 19 November 2021)

ხელოვნურ ინტელექტს[5] და სახის ამოცნობის ტექნოლოგიებს.[6] განსაკუთრებით აღსანიშნავია, რომ ეს სახელმძღვანელო დოკუმენტები აღიარებენ ციფრული იდენტობის უფლებების განვითარებას და ავსებენ კონვენციის საკონსულტაციო კომიტეტის მიერ 2023 წელს მიღებული ეროვნული ციფრული იდენტობის სახელმძღვანელო დოკუმენტებს.[7]

წინამდებარე სახელმძღვანელო მიემართება ოფიციალური საარჩევნო მართვის ორგანოებისა და სხვა ორგანოების ან ორგანიზაციების მიერ ამომრჩეველთა რეგისტრაციისა და ავთენტიფიკაციის მიზნით მონაცემთა შეგროვებასა და დამუშავებას. სახელმძღვანელოს თანახმად, მონაცემთა დამუშავებისთვის პასუხისმგებელი და დამუშავებაზე უფლებამოსილი პირები არ არიან პოლიტიკური პარტიები ან სხვა კამპანიის მხარდამჭერი ორგანიზაციები, არამედ ორგანიზაციები (მათ შორის, საარჩევნო მართვის ორგანოები ("EMBs")), რომლებიც პასუხისმგებელნი არიან ამომრჩეველთა რეგისტრაციის მიზნებისთვის პერსონალური მონაცემების დამუშავებაზე და უშუალოდ კენჭისყრის პროცესში ამომრჩეველთა ავთენტიფიკაციაზე.

სახელმძღვანელო დოკუმენტის მიზანია მონაცემთა დამუშავებისთვის პასუხისმგებელი პირებისთვის პრაქტიკული რჩევების მიწოდება იმის შესახებ, თუ როგორ უნდა იყოს უზრუნველყოფილი ამომრჩეველთა რეგისტრაციისა და ავთენტიფიკაციის სისტემების 108+ კონვენციასთან[8] შესაბამისობა, განსაკუთრებით კი მაშინ, როდესაც ინერგება ახალი ბიომეტრიული ტექნოლოგია. დოკუმენტში შემოთავაზებულია ერთგვარი ჩარჩო იმის გათვალისწინებით, რომ ინდივიდუალურ მარეგულირებლებს შეეძლებათ საკუთარი სახელმწიფოების უნიკალურ პოლიტიკურ, ინსტიტუციურ და კულტურულ პირობებზე მისი მორგება და შესაბამისობა.

შესაბამისად, სხვადასხვა იურისდიქციამ შესაძლოა მოისურვოს სახელმძღვანელო პრინციპების საკუთარ საარჩევნო სისტემებთან ადაპტირება. მათ, ასევე, შეიძლება შეიმუშაონ ამომრჩეველთა რეგისტრაციისა და ავთენტიფიკაციის შიდა პრაქტიკა,

---

[5] Council of Europe (2019). Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data. Guidelines on artificial intelligence and data protection. Strasbourg: Council of Europe (adopted 25 January 2019)

[6] Council of Europe (2021). Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data. Guidelines on Facial Recognition. Strasbourg: Council of Europe (adopted 2021)

[7] Council of Europe (2023). Consultative Committee on the Convention for the protection of individuals with regard to automatic processing of personal data. Guidelines on National Digital Identity. Council of Europe (adopted February 2023)

[8] Council of Europe (2018). Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data, at: <https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-conventionfo/16808ac91a>.

რომელიც შესაბამისი იქნება მათ შიდა პოლიტიკურ სისტემებთან და პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოების (DPAs) პასუხისმგებლობებთან, 108+ კონვენციის 15-ე მუხლის თანახმად.

2. ფარგლები და მიზანი

წინამდებარე სახელმძღვანელო დოკუმენტი შეეხება:

2.1 108+ კონვენციის მონაცემთა დაცვის პრინციპებს ამომრჩეველთა რეგისტრაციისა და ავთენტიფიკაციის მიზნით პერსონალური მონაცემების დამუშავების კონტექსტში;

2.2 მონაცემთა დამუშავებისთვის პასუხისმგებელ პირებს, რომლებიც ცალკეულ იურისდიქციაში პასუხისმგებელნი არიან ამომრჩეველთა რეესტრისა და სიების მართვაზე და, ასევე, აღნიშნული პირების მიერ დასაქმებულ მონაცემთა დამუშავებისთვის პასუხისმგებელ პირებს. მონაცემთა დამუშავებისთვის პასუხისმგებელი პირები არიან: ეროვნული და რეგიონული საარჩევნო მართვის ორგანოები (“EMBs”); ადგილობრივი, რეგიონული და მუნიციპალური ორგანოები, რომლებიც პასუხისმგებელნი არიან ამომრჩეველთა რეესტრისა და სიების მართვაზე;

2.3 მხოლოდ ამომრჩევლების (ან პოტენციური ამომრჩევლების) პერსონალური მონაცემების დამუშავებას. იგი არ ვრცელდება კანდიდატების, პოტენციური კანდიდატების ან თანამშრომლებისა და მოხალისეების პერსონალური მონაცემების დამუშავებაზე.

2.4 ხმის მიცემის რეგისტრაციასთან დაკავშირებულ მთლიან პროცესს და ხმის მიცემის ნებისმიერ ფორმას, როგორც პირადად და ფოსტით, ასევე ელექტრონულად.

3. სახელმძღვანელოს მიზნებისათვის ტერმინთა განმარტება

გარდა 108+ კონვენციის მე-2 მუხლით გათვალისწინებული განმარტებებისა, სახელმძღვანელოში გამოყენებულ ტერმინებს აქვთ შემდეგი მნიშვნელობა:

3.1 „კომპეტენტური საზედამხედველო ორგანოები“ — დამოუკიდებელი მარეგულირებელი უწყებები, რომლებსაც საარჩევნო მიზნებისთვის პერსონალური მონაცემების დამუშავებაზე ზედამხედველობის ფუნქცია გააჩნიათ და ახორციელებენ 108+ კონვენციის მე-15 მუხლით დადგენილ

უფლება-მოვალეობებს. პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოების (“DPAs”) გარდა, აღნიშნული, შესაძლოა, ასევე, მოიცავდეს სხვა ოფიციალურ მარეგულირებლებსაც.

3.2 „საარჩევნო მართვის ორგანოები“ (“EMBs”) — ეროვნულ ორგანოები, რომლებიც პასუხისმგებელნი არიან არჩევნების უსაფრთხო და ეფექტიან განხორციელებაზე. არჩევნების დაფინანსების დებულებების შესრულებაზე და (საჭიროების შემთხვევაში) ამომრჩეველთა ეროვნული რეესტრის შემუშავებასა და მართვაზე, როგორც მონაცემთა დამუშავებისთვის პასუხისმგებელი პირები.

3.3 „ამომრჩეველთა რეგისტრაცია“ — ამომრჩეველთა რეესტრში შემავალი პირების შესახებ შესაბამისი ინფორმაციის შეგროვების, შეკრებისა და შენახვის პროცესი.

3.4 „ამომრჩეველთა რეესტრი“ — ხმის მიცემის უფლების მქონე ყველა პირის ერთიანი, ოფიციალური სია და ამ რეესტრებში დამუშავებული ძირითადი პერსონალური მონაცემები (დამოუკიდებელი ან კომბინირებული სახით, ცენტრალიზებული ან ფედერაციული სახით და ა.შ.).

3.5 „ამომრჩეველთა სიები“ — ყველა იმ პირის სია, რომლებიც რეგისტრირებულია კონკრეტულ საარჩევნო ოლქში.

3.6 „საარჩევნო ოლქი“ — განსაზღვრული რეგიონი, სადაც ამომრჩეველი რეგისტრირებულია ხმის მიცემის მიზნით.

3.7 „ამომრჩევლის ავთენტიფიკაცია“ — პროცესი, რომელიც გამოიყენება კონკრეტულ საარჩევნო ოლქში, ხმის მიცემის უფლების მქონე პირის შესამოწმებლად. ასევე, იმის დადასტურება, რომ ინდივიდს აქვს ხმის უფლება კონკრეტულ ოლქში კონკრეტულ არჩევნებზე.

3.8 „პოლიტიკური პარტია“ — ადამიანთა თავისუფალი გაერთიანება, რომლის ერთ-ერთი მიზანია საზოგადოებრივ საქმეთა მართვაში მონაწილეობა, მათ შორის, თავისუფალ და დემოკრატიულ არჩევნებზე კანდიდატების წარდგენის გზით.[9]

3.9 „ბიომეტრიული მონაცემები“ — პერსონალური მონაცემები, რომლებიც მიიღება მონაცემების სპეციფიკური ტექნიკური დამუშავების შედეგად და ეხება ინდივიდის ფიზიკურ, ბიოლოგიურ ან ფიზიოლოგიურ მახასიათებლებს. ბიომეტრიული მონაცემები მიიჩნევა განსაკუთრებული კატეგორიის მონაცემად.[10]

3.10 „ბიომეტრიული ნიმუში“ — ბიომეტრიული მონაცემების მახასიათებლები.

[9] Guidelines CDL-AD (2010))24 On Political Party Regulation by OSCE/ODIHR and Venice Commission.
[10] Explanatory report, para 58.

4. 108+ კონვენციის გავრცელება ამომრჩეველთა პერსონალური მონაცემების გამოყენებაზე რეგისტრაციისა და ავთენტიფიკაციის დროს

4.1 მონაცემთა დამუშავების ლეგიტიმაცია და მონაცემთა ხარისხი ამომრჩეველთა რეგისტრაციისა და ავთენტიფიკაციისთვის (მუხლი 5)

4.1.1 ამომრჩეველთა პერსონალური მონაცემები უნდა დამუშავდეს კანონიერად და 108+ კონვენციის მე-5 მუხლით დადგენილი პრინციპების შესაბამისად, მათ შორისაა, პროპორციულობის კანონიერების, სამართლიანობის, გამჭვირვალობის, მიზნის შეზღუდვის, მონაცემთა მინიმიზაციის, სიზუსტის და უსაფრთხოების პრინციპები. დამუშავება უნდა იყოს ლეგიტიმური მიზნის პროპორციული, რაც ასახავს საპირწონე უფლებებსა და თავისუფლებებს.

4.1.2 ამომრჩეველთა რეგისტრაციისა და ავთენტიფიკაციის ლეგიტიმური მიზანია უზრუნველყოს ხმის მიცემის უფლება ყველა ამომრჩევლისთვის საარჩევნო ოლქში. საჯაროდ ხელმისაწვდომ დოკუმენტებში აღნიშნული მიზნები და საშუალებები უნდა იყოს გაწერილი რაც შეიძლება ზუსტად და სრულად, გამჭვირვალობის პრინციპის შესაბამისად. ხოლო შემდგომი დამუშავება უნდა იყოს თავსებადი ზემოხსენებულ მიზნებთან, მე-5(4)(ბ) მუხლის შესაბამისად.

4.1.3 მონაცემთა მინიმიზაციის პრინციპის შესაბამისად, ამომრჩეველთა რეესტრებში და ამომრჩეველთა სიებში მონაცემები უნდა დამუშავდეს მხოლოდ იმ მოცულობით, რაც აუცილებელია ამომრჩეველთა რეგისტრაციისა და ავთენტიფიკაციისთვის (მუხლი 5(4)(გ)).

4.1.4 მოქმედ საარჩევნო კანონმდებლობაში „კანონით დადგენილი ლეგიტიმური საფუძველით“ (მუხლი 5(2)) პერსონალური მონაცემების შეგროვება უნდა იყოს ასახული. როდესაც საჯარო ინტერესი წარმოადგენს დამუშავების ლეგიტიმურ საფუძველს. აღნიშნული ინტერესი მკაფიოდ უნდა იყოს მითითებული კანონსა და “EMB”-ების, მონაცემთა დამუშავებისთვის პასუხისმგებელი სხვა პირების კონფიდენციალობის დაცვის პოლიტიკის დოკუმენტში.

4.1.5 როდესაც თანხმობა აუცილებელია ამომრჩეველთა რეგისტრაციისთვის (მუხლი 5(2)), პერსონალური მონაცემების დამუშავება უნდა ეფუძნებოდეს მონაცემთა სუბიექტის თავისუფალ, ინფორმირებულ და მკაფიო თანხმობას.

თანხმობა არ უნდა იქნას მიღებული „დუმილის, უმოქმედობის ან წინასწარ დადასტურების ფორმით“.[11]

4.1.6 თუ კანონით არ არის აკრძალული, ამომრჩეველს შეუძლია ნებისმიერ დროს გამოიხმოს თანხმობა.[12]

4.1.7 მიზნის შეზღუდვის პრინციპი (მუხლი 5(4)(ბ)) გულისხმობს, რომ პერსონალური მონაცემები უნდა შეგროვდეს აშკარა, განსაზღვრული და ლეგიტიმური მიზნებისთვის და არ გამჟღავნდეს მიზნებთან შეუთავსებელი გზით. ამომრჩეველთა დასარეგისტრირებლად დამუშავებული პერსონალური მონაცემები არ უნდა იქნას გამოყენებული სხვა მიზნებისთვის, თუ არ არსებობს კანონით დადგენილი ლეგიტიმური საფუძველი. განსაკუთრებით, კი არ უნდა იქნას გამოყენებული „გაურკვეველი, არაზუსტი ან ბუნდოვანი მიზნებისთვის“.[13] „თავსებადი გამოყენების“ შეფასებისას კონცეფციამ არ უნდა შეარყიოს მონაცემთა დამუშავების გამჭვირვალობა, სამართლებრივი სიცხადე, განჭვრეტადობა ან სამართლიანობა.[14]

4.1.8 ამომრჩეველთა პერსონალური მონაცემები არ უნდა დამუშავდეს იმგვარად, რომ ამომრჩეველს ჰქონდეს „მოულოდნელობის, შეუსაბამობის ან სხვაგვარად არასათანადოობის“ განცდა.[15]

4.1.9 პოლიტიკური ორგანიზაციებისა მათი კანდიდატების მიერ “EMB”-ისგან ამომრჩეველთა ოფიციალური სიის კანონიერად მოპოვების შემთხვევაში, აუცილებელია, რომ კანონით განისაზღვროს, თუ ვის აქვს აღნიშნულ მონაცემებზე წვდომის უფლება, მიზნობრიობა და ხანგრძლივობა. ამომრჩეველთა სიების უნდა გაზიარდეს მხოლოდ ამომრჩეველთან საარჩევნო კამპანიის განხორციელების მიზნით, მონაცემთა სხვა მიზნებისთვის გამოყენება დაუშვებელია და გათვალისწინებულია შესაბამისი სანქცია.

4.1.10 პერსონალური მონაცემების შემცველი ოფიციალური რეესტრების შემდგომი დამუშავება ან მესამე პირებთან გაზიარება, დაუშვებელია კანონით გათვალისწინებული საფუძვლის გარეშე. ერთიან ოფიციალურ სიაში სახელები და მისამართები არ უნდა იყოს შერწყმული სხვა

[11] Explanatory report, para 42. In most societies, voter registers are derived from mandatory national and/or local population registers. Individual consent is, therefore, overridden by the legitimate basis laid down by law of the voter register. Some jurisdictions do, however, permit voters to remove their names and addresses from voter registers for legitimate reasons.

[12] Explanatory report, para. 45.

[13] Explanatory report, para 48.

[14] Explanatory report, para 49.

[15] Explanatory report, para. 49.

პერსონალურ მონაცემებთან, რომლებიც შეგროვებულია პოლიტიკური პარტიების ან კამპანიის ორგანიზატორების მიერ.

4.1.11 პერსონალური მონაცემების დამუშავება, სტატისტიკური მიზნებისთვის, ხმის მიცემის ტენდენციებზე დემოგრაფიული ან გეოგრაფიული ცვლადების მიხედვით ჩვეულებრივ ჩაითვლება „თავსებად მიზნად“, თუ არსებობს დამატებითი გარანტიები პერსონალური მონაცემების დაცვის უზრუნველსაყოფად, (მაგ.: მონაცემთა ანონიმიზაციის ან ფსევდონიმიზაცია).[16] ამგვარმა დამუშავებამ არ უნდა შელახოს ხმის მიცემის საიდუმლოება და არ უნდა იქნეს გამოწვეული ამომრჩეველთა ინტერესებში, უფლებებსა და თავისუფლებებში არაპროპორციული ჩარევა.

4.1.12 დაუშვებელია რაიმე სახის ზეწოლა ამომრჩეველზე ან პოტენციურ ამომრჩეველზე რეგისტრაციისთვის პერსონალური მონაცემების გაზიარების მიზნით, გარდა დემოკრატიულ პროცესში მონაწილეობის წახალისება.[17]

4.1.13 როდესაც “EMB”-ები იღებენ პერსონალურ მონაცემებს სხვადასხვა ორგანოებისგან (როგორიცაა: საგადასახადო ორგანოები ან მოსახლეობის რეესტრი), მონაცემები უნდა დამუშავდეს მხოლოდ ლეგიტიმური საფუძვლითა და განსაზღვრული მიზნით. მონაცემები უნდა იყოს შენახული ამომრჩეველთა რეგისტრაციის ან/და რეესტრის განახლების მიზნების შესაბამისი ხანგრძლივობით.

4.1.14 “EMB”-ებმა განსაკუთრებული ყურადღება უნდა დაუთმონ ახალგაზრდების პერსონალურ მონაცემების დამუშავების საკითხებს აშშ-ს იმ შტატებში, სადაც 18 წლამდე ასაკის პირებს აქვთ ხმის მიცემის უფლება, კონვენციის მე-15 მუხლის (ე) პუნქტის შესაბამისად.[18]

4.1.15 “EMB”-ებს ეკისრებათ პასუხისმგებლობა, უზრუნველყონ ზუსტი, სრული და საჭიროების შემთხვევაში, განახლებული პერსონალური მონაცემები.

4.1.16 “EMB”-ებმა არ უნდა გაუზიარონ ამომრჩეველთა მონაცემები სხვა ორგანიზაციებს დასამუშავებლად, თუნდაც გაერთიანებული ფორმით, გარდა იმ შემთხვევისა, როდესაც არსებობს მონაცემთა დამუშავებისთვის პასუხისმგებელი და დამუშავებაზე უფლებამოსილი პირების ურთიერთობა რაიმე სამართლებრივი საფუძვლის გარეშე.

4.1.17 წინამდებარე პუნქტები უნდა იყოს განმარტებული არჩევნების საიდუმლოების საყოველთაოდ აღიარებული პრინციპის შესაბამისად და არ უნდა არღვევდეს საჯარო ინფორმაციის ხელმისაწვდომობის შიდა ნორმებს.

[16] Explanatory report, para 50.
[17] Explanatory report, para. 42
[18] Explanatory report, para. 125.

4.2 განსაკუთრებული კატეგორიის მონაცემების (მათ შორის ბიომეტრიული მონაცემების) დამუშავება, რომელიც ცალსახად ახდენს პირის იდენტიფიცირებას ამომრჩეველთა რეგისტრაციისა და ავთენტიფიკაციის პროცესში (მუხლი 6)

4.2.1 კონვენციის მე-6(1) მუხლის მიხედვით, პერსონალური მონაცემები, რომლებიც შეეხება „პოლიტიკურ მოსაზრებებს“, მიეკუთვნება განსაკუთრებული კატეგორიის მონაცემებს. ამომრჩეველის ხმის მიცემის, ადგილმდებარეობის და ხმის მიცემის მეთოდის შესახებ მონაცემებით პოტენციურად შეიძლება გამჟღავნდეს ინდივიდთა პოლიტიკური მოსაზრებები.

4.2.2 108+ კონვენციის 6(1) მუხლის თანახმად, „რასობრივი ან ეთნიკური წარმომავლობის, პოლიტიკურ შეხედულებების, პროფკავშირის წევრობის, რელიგიური ან სხვა შეხედულებების, ჯანმრთელობის ან სექსუალურ ცხოვრების შესახებ პერსონალური მონაცემების გამჟღავნება დაიშვება მხოლოდ მაშინ, როდესაც შესაბამისი გარანტიები გათვალისწინებულია კანონით და ამავდროულად ავსებს კონვენციით განმტკიცებულ გარანტიებს“.[19]

4.2.3 მე-6 მუხლის პირველი პუნქტის თანახმად, „ბიომეტრიული მონაცემები, რომლითაც შესაძლებელია პირის იდენტიფიცირება“, ასევე განეკუთვნება განსაკუთრებული კატეგორიის მონაცემს, რომლის „დამუშავება დასაშვებია მხოლოდ კანონით განსაზღვრული სათანადო გარანტიების არსებობის შემთხვევებში, რაც ავსებს კონვენციას“ (იხ. 4.7 ქვემოთ)).

4.2.4 ამომრჩეველთა რეგისტრაციის კონტექსტში აღსანიშნავია, რომ ინფორმაციამ ინდივიდის მიერ კონკრეტულ არჩევნებზე ხმის მიცემის შესახებ, შესაძლოა გაამჟღავნოს მისი პოლიტიკური შეხედულებები. კენჭისყრის ისტორიის აღრიცხვა, ასევე, წარმოადგენს ინფორმაციას, რომლის საფუძველზე შესაძლებელია პირის პოლიტიკური შეხედულებების იდენტიფიცირება. აღნიშნული განეკუთვნება პერსონალურ მონაცემს, რომელიც 108+ კონვენციის მიხედვით განსაკუთრებული კატეგორიის მონაცემებში მოიაზრება.

4.2.5 ზოგიერთ ქვეყანაში პირს, შესაძლოა, კანონით შეეზღუდოს ხმის მიცემის უფლება ნასამართლობის ან გონებრივი შესაძლებლობების გამო. აღნიშნულიც, მე-6(1) მუხლის შესაბამისად, წარმოადგენს განსაკუთრებული კატეგორიის მონაცემებს.

[19] Convention 108+, Article 6

4.2.6 პოლიტიკური მოსაზრებების შესახებ პერსონალური მონაცემების დამუშავებამ, შესაძლოა, გამოიწვიოს ამომრჩეველთა დისკრიმინაცია და დაშინების მცდელობა. იმის ცოდნამ, თუ ვინ მისცა ან არ მისცა ხმა (ზოგიერთ სოციუმში), შესაძლოა, იქონიოს გავლენა სახელმწიფო სერვისების წვდომის უზრუნველყოფაზე. ამომრჩეველთა ჯგუფების ანალიზს, კლასიფიკაციას და პროფაილინგს გეოგრაფიული და/ან დემოგრაფიული ფაქტორების მიხედვით, შეიძლება, ჰქონდეს დისკრიმინაციული ეფექტი[20]. ასეთი განსაკუთრებული კატეგორიის მონაცემების დამუშავება მოითხოვს გარანტიებს, რომლებიც შეამცირებს რისკებს და დაიცავს ამომრჩეველთა უფლებებს, ინტერესებსა და თავისუფლებებს.

4.2.7 "EMB"-ებმა არ უნდა გაამჟღავნონ პერსონალური მონაცემები მესამე პირებთან, თუ აღნიშნული არ არის შიდა კანონმდებლობით ნებადართული და სათანადო გარანტიები არ არის გათვალისწინებული მონაცემებისა და პირთა პირადი ცხოვრების ხელშეუხებლობის უფლების დასაცავად. "EMB"-ებმა მესამე პირებს არ უნდა გაუზიარონ ამომრჩეველთა რეგისტრაციასთან დაკავშირებული მონაცემები (მათ შორის, მონაცემთა ბროკერებს) მონეტიზაციის მიზნით ან ხელახლა დამუშავდეს იგი, ანონიმური ან არაიდენტიფიცირებული მონაცემების რეალიზაციისთვის.

4.3 მონაცემთა უსაფრთხოება და კონფიდენციალობა (მუხლი 7)

4.3.1 შესაბამისი უსაფრთხოების ღონისძიებების გამოყენება ამომრჩეველთა რეგისტრაციის თითოეულ ეტაპზე სასიცოცხლოდ მნიშვნელოვანია. უსაფრთხოების ზომების მიღებისას გათვალისწინებული უნდა იყოს მონაცემთა უსაფრთხოების თანამედროვე მეთოდები და ტექნოლოგიები. გამოყენებული ღონისძიებები, ასევე, შესაბამისი უნდა იყოს რისკის სიმძიმესთან და ალბათობასთან.[21]

4.3.2 მონაცემთა დამუშავებამდე რისკის შეფასებამ ("Risk assessment") უნდა განსაზღვროს, არის თუ არა მონაცემები დაცული არაავტორიზებული მოდიფიკაციისგან ან განადგურებისგან.

4.3.3 რისკების შეფასების მიზანია უსაფრთხოების მაღალი სტანდარტების დანერგვა მონაცემთა დამუშავების მთელი ციკლის განმავლობაში. ამგვარი

[20] Council of Europe, The Protection of individuals with regard to automatic processing of personal data in the context of profiling. Recommendation CM/REC (2010) 13 (November 23, 2010)

[21] Explanatory report, para 63.

შეფასებები უნდა შემუშავდეს აუცილებლობის, პროპორციულობისა და მონაცემთა დაცვის ფუნდამენტური პრინციპების გათვალისწინებით. მნიშვნელოვანია, შეფასდეს რისკების მთელი რიგი, ფიზიკური წვდომა მონაცემებზე, ქსელში წვდომა მოწყობილობებსა და მონაცემებზე და სათანადო სარეზერვო და დაარქივების პროცედურები.

4.3.4 არჩევნების დროს ამომრჩეველთა ავთენტიფიკაცია ხშირად მოიაზრებს ამომრჩევლების შესახებ მონაცემების გაზიარებას მოხალისეებთან, კონტრაქტორებთან და თანამშრომლებთან. "EMB"-ებმა უნდა მიიღონ უსაფრთხოების შესაბამისი ზომები, რათა უზრუნველყონ პერსონალური მონაცემების დაცვა შემთხვევითი ან არაავტორიზებული წვდომისგან, განადგურებისგან, დაკარგვისგან, გამოყენებისგან, მოდიფიკაციისა ან გამჟღავნებისგან.

4.3.5 უსაფრთხოების ზომები უნდა ითვალისწინებდეს შემდეგ საკითხებს: კონფიდენციალობისა და უსაფრთხოების შესახებ სწავლება (ტრენინგი); წვდომის კონტროლი ("access control"); კონფიდენციალობის შესახებ შეთანხმება; ფიზიკური წვდომის კონტროლი იმ ადგილებსა და აღჭურვილობაზე, სადაც ინახება ამომრჩეველთა რეესტრი ან სიები; უსაფრთხოების ზომების მდგრადობის გადამოწმების მექანიზმები (ყალბი სახელით შემოწმება); ბიომეტრიული მონაცემების სხვა პერსონალური მონაცემებისგან განცალკევებით შენახვა; მონაცემთა უსაფრთხოებასთან დაკავშირებული მოქმედების ჟურნალის წარმოება.

4.3.6 საარჩევნო პროცესებთან დაკავშირებით "EMB"-ებმა უნდა გადაამზადონ თითოეული თანამშრომელი და მოხალისე, რა დროსაც ხაზი უნდა გაესვას კონფიდენციალობისა და მონაცემთა უსაფრთხოების ზომების მნიშვნელობას. საგულისხმოა, რომ თითოეულ თანამშრომელსა და მოხალისეს კონფიდენციალობის დაცვის ვალდებულება გააჩნია. ასევე, ამომრჩეველთა რეესტრი და ამომრჩეველთა სიები მკაცრად უნდა გაკონტროლდეს.

4.3.7 "EMB"-ებმა სულ მცირე უნდა შეატყობინონ კომპეტენტურ საზედამხედველო ორგანოებს, 108+ კონვენციით განსაზღვრული მონაცემების დარღვევის შესახებ, რამაც შეიძლება, შეზღუდოს ამომრჩეველთა უფლებები და ძირითადი თავისუფლებები 108+ კონვენციის 7(2) მუხლის შესაბამისად. შეტყობინება უნდა მოიცავდეს ინფორმაციას დარღვევის უარყოფითი შედეგების შემცირების ზომების შესახებ.[22]

4.3.8 როდესაც ამომრჩეველთა რეგისტრაციასთან დაკავშირებული მონაცემები მუშავდება მომსახურების მიმწოდებლების მიერ (მესამე პირი), ისინი უნდა

[22] Explanatory report, para 66.

განისაზღვრონ მოქმედი კანონმდებლობის შესაბამისად. “EMB”-ები, როგორც დამუშავებისთვის პასუხისმგებელი პირები მუდმივად უნდა აცნობიერებდნენ თავიანთ პასუხისმგებლობებს. მათ უნდა შეეძლოთ იმის დადასტურება, რომ დამუშავებაზე უფლებამოსილი პირები ასრულებენ ვალდებულებებს მე-7(1) მუხლის შესაბამისად, რა შემთხვევაშიც აღნიშნული შესაძლებელია (კონვენციის მე-10 მუხლი).

4.4 პერსონალური მონაცემების დამუშავების გამჭვირვალობა ამომრჩეველთა რეგისტრაციისა და ავთენტიფიკაციის პროცესში (მუხლი 8)

4.4.1 საარჩევნო პროცესის თითოეულ ეტაპზე, პერსონალური მონაცემები უნდა დამუშავდეს სამართლიანად და გამჭვირვალედ, ამომრჩეველთა შესაძლო მანიპულირების თავიდან არიდების მიზნით.

4.4.2 ამომრჩეველთა რეესტრის შესაბამისად, “EMB”-ებმა უნდა მიაწოდონ ამომრჩეველს შემდეგი ინფორმაცია: ორგანიზაციის სახელი, იურიდიული მისამართი; პერსონალური მონაცემების დამუშავების სამართლებრივი საფუძველი; დამუშავებული პერსონალური მონაცემების კატეგორიები და მათი გაზიარების მიზეზები; და თუ როგორ შეუძლია ამომრჩეველს საკუთარი უფლებებით სარგებლობა.

4.4.3 როდესაც არსებული სახელმწიფო რეესტრებიდან ამომრჩეველთა რეესტრი იქმნება (მაგ.: მოსახლეობის მონაცემთა ბაზები, საგადასახადო ან აღწერის ჩანაწერები), მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს არ მოეთხოვება ფიზიკური პირების ინფორმირება, თუ დამუშავება ცალსახად ნებადართულია კანონით, ან თუ მათი შეტყობინება მოითხოვს არაპროპორციულ ძალისხმევას.[23]

4.4.4 იმ ქვეყნებში, სადაც ამომრჩეველთა რეგისტრაცია დამოუკიდებლად არის ინიცირებული, პირებს რეგისტრაციის დროს უნდა ჰქონდეთ ინფორმაცია იმის შესახებ, თუ როგორ იქნება გამოყენებული მათი პერსონალური მონაცემები, დამუშავების მიზნები და ნებისმიერი დამუშავებაზე უფლებამოსილი პირის ვინაობა, რომლებსაც შესაძლოა, ჰქონდეთ წვდომა მონაცემებზე.

4.4.5 იმ ქვეყნებში, სადაც ამომრჩეველთა რეგისტრაციის პროცესს მოხალისეები ან/და თანამშრომლები ახორციელებენ „საყოფაცხოვრებო დონეზე“ (“household level”), პირებს მკაფიოდ უნდა განემარტოთ მონაცემთა შეგროვების მიზანი და რეგისტრაციის სამართლებრივი საფუძველი.

[23] Convention 108+, Article 8(3)

4.4.6 “EMB”-ების კონფიდენციალობის პოლიტიკა უნდა იყოს ადვილად ხელმისაწვდომი, წაკითხვადი, გასაგები და შესაბამისი პირებისთვის ადაპტირებული.[24] კომუნიკაციის მეთოდები არ უნდა ზღუდავდეს სამართლიანი დამუშავებისთვის საჭირო განმარტებებს, მაგრამ არც გადაჭარბებული უნდა იყოს. „მრავალშროვანი კონფიდენციალობის შეტყობინებების“ (“Layered privacy notices”) მიზანია ზუსტი ინფორმაციის საჭიროებისამებრ გაერთიანება.

4.4.7 ამომრჩეველთა რეგისტრაციასთან დაკავშირებული მონაცემების დამუშავება, ასევე, უნდა შეესაბამებოდეს შიდა ეროვნულ და საჯარო წყაროებიდან ხელმისაწვდომ კანონმდებლობას.

4.4.8 ანგარიშვალდებულებისა და გამჭვირვალობის უზრუნველსაყოფად, პერსონალური მონაცემების დამუშავების ტექნოლოგიის შესყიდვასთან დაკავშირებული დოკუმენტაცია საჯაროდ ხელმისაწვდომი უნდა იყოს. საარჩევნო ტექნოლოგიების სერვისების ხელშეკრულებები მკაფიოდ უნდა ასახავდეს კომპანიის მიერ მონაცემებზე წვდომის ფარგლებს და გარანტიებს მათი უსაფრთხოებისა და სათანადო დამუშავების უზრუნველსაყოფად.

4.5 მონაცემთა სუბიექტის უფლებები (მუხლი 9)

4.5.1 მონაცემთა სუბიექტებს მათი მოთხოვნის საფუძველზე, გონივრულ ვადაში, ზედმეტი დაყოვნებისა და ხარჯების გარეშე შეუძლიათ, მიიღონ ამომრჩეველთა რეესტრში ან ამომრჩეველთა სიაში მათთან დაკავშირებული პერსონალური მონაცემების დამუშავების პროცესებზე დასტური, არსებული ინფორმაცია მათი წყაროსა და შენახვის პერიოდის შესახებ, კონვენციის 9(1)(ბ) მუხლის შესაბამისად. მონაცემთა სუბიექტებს უფლება აქვთ, მოთხოვნისთანავე მიიღონ ინფორმაცია, თუ როგორ იქნა მოპოვებული მათი პერსონალური მონაცემები ამომრჩეველთა რეესტრისთვის და რა წყაროდან.

4.5.2 მონაცემთა სუბიექტებს არაზუსტი, ძველი ან არასრული ინფორმაციის გამოსწორების ან/და წაშლის უფლება უნდა ჰქონდეთ, კონვენციის 9(1) მუხლის „ე“ ქვეპუნქტის შესაბამისად.[25]

4.5.3 მონაცემთა სუბიექტი უფლებამოსილია, არ დაექვემდებაროს გადაწყვეტილებას, რომელიც მონაცემთა მხოლოდ ავტომატურ

[24] Explanatory report, para. [12.]
[25] Explanatory report, para. 72.

დამუშავებაზე დაყრდნობით მიიღება და წარმოშობს სამართლებრივ ან სხვა მნიშვნელოვან შედეგებს მისთვის.

4.5.4 მოთხოვნის საფუძველზე მონაცემთა სუბიექტებს უფლება აქვთ, დაყოვნებისა და ხარჯების გარეშე მოითხოვონ მონაცემთა დამუშავების საფუძვლის შესახებ ინფორმაცია მაშინ, როდესაც დამუშავების შედეგებს გავლენა აქვს მათზე (მუხლი 9(1)(გ)). მაგალითად, როდესაც მონაცემთა სუბიექტებს უარი ეთქვათ რეგისტრაციაზე ან ამოიღეს ამომრჩეველთა რეესტრიდან (ასაკობრივი, გონებრივი შესაძლებლობების ან ნასამართლობის გამო), მათ უფლება აქვთ სათანადო წესით ინფორმირებულნი იყვნენ გადაწყვეტილების მიღების მიზეზების შესახებ.

4.5.5 მონაცემთა სუბიექტებს უფლება აქვთ, გაასაჩივრონ მონაცემთა დამუშავება "EMB"-სა ან კომპეტენტურ ორგანოში, გარდა იმ შემთხვევისა, როდესაც დამუშავებისთვის პასუხისმგებელი პირი წარმოადგენს დამუშავების ლეგიტიმურ საფუძველს, რომელიც გადაწონის მონაცემთა სუბიექტის ინტერესებს ან უფლებებსა და ძირითად თავისუფლებებს (მუხლი 9(1) (დ)). ამომრჩეველთა ზუსტი რეგისტრაციისა და ავთენტიფიკაციის უზრუნველყოფა შესაძლოა, იყოს ლეგიტიმური საფუძველი.

4.5.6 მონაცემთა სუბიექტების უფლების დარღვევის შემთხვევაში, პირი უფლებამოსილია მიმართოს მოქმედი კანონმდებლობით გათვალისწინებულ ღონისძიებებს.

4.5.7 საზედამხედველო ორგანოს დახმარებით მონაცემთა სუბიექტი უფლებამოსილია, განახორციელოს საკუთარი უფლებები (მუხლი 9(1)(ზ)).

4.6 დამატებითი ვალდებულებები და რეკომენდაციები არჩევნების მართვის ორგანოებისა და მონაცემთა დამუშავებისთვის პასუხისმგებელი პირებისთვის (მუხლი 10)

4.6.1 ანგარიშვალდებულების პრინციპი გულისხმობს, რომ მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირმა და საჭიროების შემთხვევაში, დამუშავებაზე უფლებამოსილმა პირმა უზრუნველყოს დამუშავების პროცესის მონაცემთა დაცვის პრინციპებთან და კანონმდებლობასთან შესაბამისობა.

4.6.2 "EMB"-ებმა და დამუშავებაზე უფლებამოსილმა ნებისმიერმა პირმა უნდა აწარმოონ ჩანაწერები პერსონალური მონაცემების მოპოვებისა და დამუშავების პროცესის შესახებ. საჭიროებისამებრ, დამუშავებისთვის პასუხისმგებელი პირსა და დამუშავებაზე უფლებამოსილი პირს შორის

დადებულ ხელშეკრულებაში მკაფიოდ უნდა იყოს ასახული მათი პასუხისმგებლობის საკითხი მონაცემთა დამუშავების სახეობის მიხედვით (მუხლი 10(1)).

4.6.3 სხვა ღონისძიებები ("Measures") შეიძლება მოიცავდეს შიდა პროცესუალური ნორმების შექმნასა და თანამშრომელთა გადამზადებას (ტრენინგი). "EMB"-ებმა უნდა განსაზღვრონ პერსონალურ მონაცემთა დაცვის ოფიცერი, რომელიც პასუხისმგებელი იქნება 108+ კონვენციით გათვალისწინებულ მონაცემთა დაცვის პრინციპებთან შესაბამისობის შემოწმებასა და ზედამხედველობაზე[26].

4.6.4 "EMB"-ებმა უნდა გამოიკვლიონ და შეაფასონ მონაცემთა დამუშავების სავარაუდო ზეგავლენა ამომრჩევლის უფლებებსა და ძირითად თავისუფლებებზე, რაც უნდა განხორციელდეს მონაცემთა შეგროვებამდე და დამუშავების პროცესის დაწყებამდე. მათ უნდა წარმართონ პროცესი იმგვარად, რომ თავიდან იქნას არიდებული ამომრჩეველთა უფლებების შეზღუდვის მინიმალური რისკიც კი (მუხლი 10(2)).

4.6.5 მონაცემთა დაცვაზე ზეგავლენის შეფასებებმა უნდა შეისწავლოს დამუშავების ზეგავლენა მონაცემთა სუბიექტების უფლებებზე, ასევე, განიხილოს, არის თუ არა დამუშავების კონკრეტული ქმედება დემოკრატიული ღირებულებებისა და დემოკრატიული არჩევნების ერთიანობის ინტერესებში.

4.6.6 "EMB"-ებმა უნდა წაახალისონ და განამტკიცონ პერსონალურ მონაცემთა დაცვის კულტურა ორგანიზაციაში, როგორც საარჩევნო პროცესების განმავლობაში, ასევე შემდგომ პერიოდშიც.

4.6.7 არჩევნების ჩატარების საუკეთესო პრაქტიკის პროაქტიულ მითითებებს გადამწყვეტი მნიშვნელობა აქვს. ადამიანის უფლებების რისკების სრულად გაგება არ შემოიფარგლება არჩევნების განმავლობაში მხოლოდ ცალკეული საჩივრების განხილვით.

4.6.8 პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოებს, მათი კომპეტენციის ფარგლებში, შეუძლიათ დახმარება გაუწიონ "EMB"-ებს. საზედამხედველო ორგანოებს ღირებული ცოდნა და გამოცდილება გააჩნიათ მონაცემთა დაცვის კულტურის დანერგვასა და პირადი ცხოვრების ხელშეუხებლობის პრაქტიკულ დაცვაში. მათ შეუძლიათ მონაცემთა დაცვის შესახებ ზოგადი წესები საარჩევნო კონტექსტზე მოარგონ.

4.6.9 მიუხედავად იმისა, რომ წინამდებარე სახელმძღვანელო დოკუმენტების იმპლემენტაცია ადგილობრივი პოლიტიკური კონტექსტის მიხედვით განხორციელდება, აღნიშნულ პროცესში შესაძლოა, საჭირო გახდეს

[26] Explanatory report, para. 87.

საზედამხედველო ორგანოებს შორის თანამშრომლობა. გლობალური ბიომეტრიული ინდუსტრიის გავლენა "ეროვნულ და საერთაშორისო დონეზე მუდმივ ყურადღებას მოითხოვს EMB"-ებისა და ზედამხედველობის ორგანოებისგან.

4.7 ამომრჩეველთა რეგისტრაციისა და ავთენტიფიკაციისათვის ბიომეტრიული მონაცემების დამუშავების დამატებითი ვალდებულებები

4.7.1 ბიომეტრიული მონაცემები წარმოიქმნება კონკრეტული ტექნიკური დამუშავების შედეგად, რომელიც ეხება ინდივიდის ფიზიკურ, ბიოლოგიურ ან ფიზიოლოგიურ მახასიათებლებს, რაც პირის უნიკალურ იდენტიფიკაციისა ან/და ავთენტიფიკაციის საშუალებას იძლევა. ბიომეტრიული მონაცემები, რომელიც გამოიყენება მონაცემთა სუბიექტის იდენტიფიცირებისთვის, 108+ კონვენციის მე-6 მუხლის მიხედვით, წარმოადგენს განსაკუთრებული კატეგორიის მონაცემებს.

4.7.2 პერსონალური მონაცემები, რომლებიც დაკავშირებულია პოლიტიკურ შეხედულებებთან, ასევე, განიხილება განსაკუთრებული კატეგორიის პერსონალურ მონაცემად, კონვენციის მე-6 მუხლის შესაბამისად.

4.7.3 განსაკუთრებული კატეგორიის მონაცემების დამუშავება დასაშვებია მხოლოდ მაშინ, როდესაც კანონით შესაბამისი გარანტიებია გათვალისწინებული, რომელიც ავსებს 108+ კონვენციას.[27]

4.7.4 ბიომეტრიული იდენტიფიკაციის ავტომატური ფორმების ინტეგრაცია ამომრჩეველთა ბაზაში რისკებს უქმნის პირთა პირადი ცხოვრების ხელშეუხებლობას და ამომრჩეველთა დემოკრატიულ უფლებებს.[28]

4.7.5 ადამიანის უფლებებისა და ფუნდამენტური თავისუფლებების დარღვევის რისკების გათვალისწინებით, მიზანშეწონილია, რომ პოლიტიკურმა პარტიებმა გულდასმით შეაფასონ ამომრჩეველთა რეგისტრაციისა და ავთენტიფიკაციის მიზნით იდენტიფიკაციის ავტომატური ბიომეტრიული ფორმების დანერგვის აუცილებლობა, აგრეთვე, უზრუნველყონ, რომ აღნიშნული განხორციელდეს მხოლოდ აუცილებლობის შემთხვევაში. ამგვარი სისტემები უნდა დაინერგოს მხოლოდ მაშინ, როდესაც იდენტიფიკაციისა და ავთენტიფიკაციის სხვა არსებული ფორმები აშკარად არაზუსტი ან შეუსაბამოა.

[27] Convention 10, Art 6. 2.
[28] Guidelines on facial recognition, p. 5

4.7.6 ამომრჩეველთა რეგისტრაციისა და ავთენტიფიკაციის მიზნებისთვის ბიომეტრიის ავტომატური გამოყენება უნდა ეყრდნობოდეს შესაბამის სამართლებრივ საფუძველს, კერძოდ: უნდა განისაზღვროს ბიომეტრიის სპეციფიკური დანიშნულება; გამოყენებული კონკრეტული ტექნოლოგიისა და ალგორითმის მინიმალური სანდოობისა და სიზუსტის სტანდარტები (როგორიცაა: ცრუ დადებითი და ცრუ უარყოფითი შეცდომის კოეფიციენტები); გამოყენებული ბიომეტრიული ნიმუშის შენახვის პერიოდი; საზედამხედველო ორგანოს წინასწარი კონსულტაციის მოთხოვნა; ბიომეტრიული ნიმუშის გამოყენებისა და გაზიარების მიკვლევადობა; დადგენილი გარანტიები და რისკები, რომლებიც განსაკუთრებული კატეგორიის მონაცემთა დამუშავებით შეიძლება წარმოიშვას მონაცემთა სუბიექტის ინტერესების, უფლებებისა და ძირითადი თავისუფლებების შეზღუდვის რისკი, კერძოდ, დისკრიმინაციის რისკი.[29]

4.7.7 იდენტიფიკაციის ბიომეტრიული ფორმების გამოყენება უნდა განხორციელდეს მხოლოდ ამომრჩეველთა რეგისტრაციისა და ავთენტიფიკაციის მიზნებისთვის. დაუშვებელია მათი დამუშავება რასობრივი, ეთნიკური წარმომავლობის, ასაკის, ჯანმრთელობის ან სხვა სოციალური გარემოებების დასადგენად.

4.7.8 დაუშვებელია ამომრჩეველთა რეგისტრაციისა და ავთენტიფიკაციის მიზნებისთვის ციფრული სურათების გამოყენება, რომლებიც ინტერნეტში ან სოციალურ მედიაში იქნა განთავსებული/გადაღებული ვიდეოსათვალთვალო კამერის საშუალებით.[30]

4.7.9 დაუშვებელია ბიომეტრიული მონაცემების გაზიარება პოლიტიკურ პარტიებთან, პოლიტიკურ კანდიდატებთან, კამპანიის ორგანიზაციებთან ან სხვა მესამე პირებთან. ამომრჩეველთა რეგისტრაციისთვის დამუშავებულ ბიომეტრიულ მონაცემებზე წვდომა შესაძლოა, ჰქონდეს მხოლოდ "EMB"-ს ან მათი სახელით მოქმედ დამუშავებაზე უფლებამოსილ პირებს.

4.7.10 ბიომეტრიული ტექნოლოგიების შემქმნელებმა და მწარმოებლებმა უნდა მიიღონ შესაბამისი ღონისძიებები, რათა უზრუნველყონ, რომ ამგვარი მონაცემების დამუშავება განხორციელდეს მხოლოდ მაშინ, როდესაც უზრუნველყოფილია მონაცემთა უსაფრთხოების ზომები და გარანტიები. მე-5 მუხლის თანახმად, დაცულია მისი სიზუსტე, რაც გულისხმობს სისტემების მუდმივად შემოწმებას რაიმე სახის უთანასწორობის აღმოფხვრის მიზნით, განსაკუთრებით კი ეთნიკური, ასაკისა და სქესის

[29] Guidelines on facial recognition, p. 7.
[30] Guidelines on facial recognition, p. 9.

ნიშნით. აღნიშნულში ასევე იგულისხმება ბიომეტრიული პროდუქტის ან მომსახურების წარმოების პროცესში მონაცემთა მეტად დაფარვის პრიორიტეტის პრინციპების საწყის მეთოდად გამოყენებას ("data protection by design principles").

4.7.11 ბიომეტრიული ტექნოლოგიების შემქმნელებმა და მწარმოებლებმა უნდა შეისწავლონ მონაცემთა დამუშავებაზე ზეგავლენა მონაცემთა დამუშავების დაწყებამდე. მათ უნდა უზრუნველყონ ტექნიკური და ორგანიზაციული ზომები, დამუშავების პროცესის ყველა ეტაპზე პერსონალური მონაცემების დაცვის მიზნით.

4.7.12 ბიომეტრიული ტექნოლოგიის შესყიდვასთან დაკავშირებული დოკუმენტაცია უნდა იყოს საჯაროდ ხელმისაწვდომი. კერძო კომპანიებმა, რომლებიც უზრუნველყოფენ ამგვარი საარჩევნო ტექნოლოგიის მიწოდებას, უარი უნდა თქვან კომერციული საიდუმლოების დაცვაზე და სრულად გასაჯაროვდეს მათი ტექნოლოგიები სისტემის ფუნქციებისა და შესაძლებლობების ფართო გაგების მიზნით. საარჩევნო ტექნოლოგიებთან დაკავშირებული ხელშეკრულებები უნდა მოიცავდეს კომპანიის შესახებ დეტალურ ინფორმაციას და შესაბამის გარანტიებს მონაცემთა უსაფრთხოებისა და სათანადო მართვის უზრუნველსაყოფად.

4.7.13 კონვენციის მე-15 მუხლის მე-3 პუნქტის შესაბამისად, საზედამხედველო ორგანოებთან უნდა იქნეს გავლილი კონსულტაციები საარჩევნო პროცესში ამომრჩეველთა რეგისტრაციისა და ავთენტიფიკაციის მიზნით. ბიომეტრიული ტექნოლოგიის დანერგვის შესახებ მოსაზრებების წარსადგენად. აღსანიშნავია, რომ კონსულტაციები უნდა იქნეს გავლილი წინასწარ, ამომრჩეველთა ბიომეტრიული რეგისტრაციის სქემების დანერგვამდე.