



სს “მისო ქართული კრედიტის” პერსონალურ მონაცემთა დაცვის პოლიტიკა

ნიკა ჩიქვილაძე
აღმასრულებელი დირექტორი

eSigned by:
ნიკა ჩიქვილაძე: a1aeba4c-27ce-492d-89c5-e2.....

Certified by Signify

2026 წელი, სექტემბერი
პირველადი რედაქცია 2024 წლის აგვისტო

შინაარსი

1. პერსონალურ მონაცემთა დაცვა	2
2. პოლიტიკის მიზანი და მოქმედების სფერო	2
3. ტერმინთა განმარტება	3
4. პერსონალურ მონაცემთა დამუშავების საფუძვლები	4
5. პერსონალურ მონაცემთა დამუშავების პრინციპები	5
6. პერსონალურ მონაცემთა კატეგორიები	5
7. არასრულწლოვანის მონაცემების დამუშავება	6
8. გარდაცვლილი პირის შესახებ მონაცემების დამუშავება	6
9. ვიდეო და აუდიოშემატების განხორციელება	6
10. კომპანიის ინტერნეტ ბანკით სარგებლობის წესი	6
11. პირდაპირი მარკეტინგი	7
12. მონაცემთა გადაცემა მესამე პირებისთვის	7
13. მონაცემთა სუბიექტის უფლებები	8
14. მონაცემების უსაფრთხოების უზრუნველყოფა	8
15. მონაცემთა შენახვის ვადები	9
16. ინციდენტზე რეაგირების წესი	9
17. დასკვნითი დებულებები	9
18. საკონტაქტო ინფორმაცია	10
19. პერსონალურ მონაცემთა დაცვის ოფიცერი	10

1. პერსონალურ მონაცემთა დაცვა

1.1. სს მისო “ქართული კრედიტის” (შემდგომში - “კომპანია”) პერსონალურ მონაცემთა დაცვის პოლიტიკა (შემდგომში - “პოლიტიკა”) ადგენს პერსონალური მონაცემების დამუშავების მიზნებს, ძირითად პრინციპებსა და წესებს და განსაზღვრავს მონაცემთა უსაფრთხოების უზრუნველსაყოფად დანერგილ ძირითად ზომებს;

1.2. სს მისო “ქართული კრედიტი” პატივს სცემს საქართველოს კანონმდებლობასა და საერთაშორისო სტანდარტებს ადამიანის უფლებათა დაცვის სფეროში. კომპანია პერსონალურ მონაცემთა დამუშავებას ახორციელებს “პერსონალურ მონაცემთა დაცვის შესახებ” საქართველოს კანონის შესაბამისად.

2. პოლიტიკის მიზანი და მოქმედების სფერო

2.1. წინამდებარე პოლიტიკა ადგენს კომპანიის მიერ პერსონალური მონაცემების დამუშავების ზოგად წესებს. პოლიტიკა ვრცელდება კომპანიის მომხმარებლებზე, თანამშრომლებზე, კონტრაქტორებზე და ყველა იმ პირზე, რომელთა მონაცემების მუშავდება კომპანიის მიერ,

ასევე, მონაცემთა მიმღებზე და იმ უფლებამოსილ პირებზე, რომლებიც კომპანიის სახელით ან/და მისთვის ამუშავებენ პერსონალურ მონაცემებს;

2.2. პოლიტიკის მიზანია პერსონალური მონაცემების დაცვის მაღალი სტანდარტის დანერგვა “პერსონალურ მონაცემთა დაცვის შესახებ” საქართველოს კანონისა და ევროკავშირის მონაცემთა დაცვის რეგულაციების გათვალისწინებით;

2.3. წინამდებარე პოლიტიკის მიზანია:

2.3.1. დაადგინოს პერსონალური მონაცემების დამუშავების ზოგადი პრინციპები, მთლიანობის, კანონიერების, სიზუსტისა და ანგარიშვალდებულების პრინციპების ჩათვლით;

2.3.2. დააწესოს პერსონალური მონაცემების დაცვის სავალდებულო მოთხოვნები კომპანიის მიერ ამ მოთხოვნების შესრულების უზრუნველყოფით;

2.3.3. შექმნას მონაცემთა დაცვისა და კონფიდენციალურობის დაცვის მართვის უსაფრთხო და კანონიერი სისტემა, რომელიც შეესაბამება მონაცემთა დაცვის შესახებ კანონით დადგენილ მოთხოვნებს;

2.3.4. უზრუნველყოს პერსონალური მონაცემების დამუშავების სფეროში არსებული საკითხების გადაწყვეტის ერთიანი და სისტემური მიდგომა.

3. ტერმინთა განმარტება

წინამდებარე დოკუმენტში გამოყენებული ტერმინები მხოლოდ აღწერილობითია და განმარტებულია კომპანიის სამუშაო სპეციფიკიდან გამომდინარე. განმარტებები შესაბამისობაშია “პერსონალურ მონაცემთა დაცვის შესახებ” საქართველოს კანონთან და მათი ინტერპრეტირება კანონის საწინააღმდეგოდ დაუშვებელია.

პერსონალური მონაცემი (შემდგომში-“მონაცემი”) - ნებისმიერი ინფორმაცია, რომელიც იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს უკავშირდება. ფიზიკური პირი იდენტიფიცირებადია, როდესაც შესაძლებელია მისი იდენტიფიცირება პირდაპირ ან არაპირდაპირ, მათ შორის, სახელით, გვარით, საიდენტიფიკაციო ნომრით, გეოლოკაციის მონაცემებით, ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემებით, ფიზიკური, ფიზიოლოგიური, ფსიქიკური, ფსიქოლოგიური, გენეტიკური, ეკონომიკური, კულტურული ან სოციალური მახასიათებლით;

განსაკუთრებული კატეგორიის პერსონალური მონაცემები - მონაცემი, რომელიც უკავშირდება ფიზიკური პირის რასობრივ ან ეთნიკურ კუთვნილებას, პოლიტიკურ შეხედულებებს, რელიგიურ, ფილოსოფიურ ან სხვაგვარ მრწამსს, პროფესიული კავშირის წევრობას, ჯანმრთელობას, სქესობრივ ცხოვრებას, ბრალდებულის, მსჯავრდებულის, გამართლებულის ან დაზარალებულის სტატუსს სისხლის სამართლის პროცესში, მსჯავრდებას, ნასამართლობას, განრიდებას, ადამიანით ვაჭრობის (ტრეფიკინგის) ან „ქალთა მიმართ ძალადობის ან/და ოჯახში ძალადობის აღკვეთის, ძალადობის მსხვერპლთა დაცვისა და დახმარების შესახებ“ საქართველოს კანონის შესაბამისად დანაშაულის მსხვერპლად

ცნობას, პატიმრობას და მის მიმართ სასჯელის აღსრულებას, აგრეთვე ბიომეტრიულ და გენეტიკურ მონაცემებს, რომლებიც ფიზიკური პირის უნიკალური იდენტიფიცირების მიზნით მუშავდება;

მონაცემთა დამუშავება - მონაცემთა მიმართ შესრულებული ნებისმიერი მოქმედება, მათ შორის, მათი შეგროვება, მოპოვება, მათზე წვდომა, მათი ფოტოგადაღება, ვიდეო ან/და აუდიომონიტორინგი, ორგანიზება, დაჯგუფება, ურთიერთდაკავშირება, შენახვა, შეცვლა, აღდგენა, გამოთხოვა, გამოყენება, დაბლოკვა, წაშლა ან განადგურება, აგრეთვე მონაცემთა გამჟღავნება მათი გადაცემით, გასაჯაროებით, გავრცელებით ან სხვაგვარად ხელმისაწვდომად გახდომით;

მონაცემთა სუბიექტი - ნებისმიერი ფიზიკური პირი, რომლის შესახებაც მუშავდება მონაცემები;

მონაცემთა სუბიექტის თანხმობა - მონაცემთა სუბიექტის მიერ შესაბამისი ინფორმაციის მიღების შემდეგ მის შესახებ მონაცემთა კონკრეტული მიზნით დამუშავებაზე აქტიური მოქმედებით, წერილობით ან ზეპირად, თავისუფლად და მკაფიოდ გამოხატული ნება;

დამუშავებისთვის პასუხისმგებელი პირი - ფიზიკური პირი, იურიდიული პირი ან საჯარო დაწესებულება, რომელიც ინდივიდუალურად ან სხვებთან ერთად განსაზღვრავს მონაცემთა დამუშავების მიზნებსა და საშუალებებს, უშუალოდ ან დამუშავებაზე უფლებამოსილი პირის მეშვეობით ახორციელებს მონაცემთა დამუშავებას;

დამუშავებაზე უფლებამოსილი პირი - ფიზიკური პირი, იურიდიული პირი ან საჯარო დაწესებულება, რომელიც მონაცემებს ამუშავებს დამუშავებისთვის პასუხისმგებელი პირისთვის ან მისი სახელით;

კომპანია - წინამდებარე პოლიტიკის მიზნებისთვის სს მისო ქართული კრედიტი, რომელიც ამუშავებს მონაცემებს, განსაზღვრავს მონაცემთა დამუშავების მიზნებსა და საშუალებებს, მეთოდებს, ფორმებს, ორგანიზაციულ და ტექნიკურ უსაფრთხოების ზომებს, ასევე მონაცემთა სუბიექტის უფლებების რეალიზების გზებს;

ვიდეომონიტორინგი - საჯარო ან კერძო სივრცეში განთავსებული/დამონტაჟებული ტექნიკური საშუალებების გამოყენებით ვიზუალური გამოსახულების მონაცემთა დამუშავება, კერძოდ, ვიდეოკონტროლი ან/და ვიდეოჩაწერა (გარდა ფარული საგამოძიებო მოქმედებისა);

მონაცემთა მიმღები - ფიზიკური პირი, იურიდიული პირი ან საჯარო დაწესებულება, რომელსაც მონაცემები გადაეცა, გარდა სახელმწიფო აუდიტის სამსახურისა;

ინციდენტი - მონაცემთა უსაფრთხოების დარღვევა, რომელიც იწვევს მონაცემების არამართლზომიერ ან შემთხვევით დაზიანებას, დაკარგვას, აგრეთვე უნებართვო

გამჟღავნებას, განადგურებას, შეცვლას, მათზე წვდომას, მათ შეგროვებას/მოპოვებას ან სხვაგვარ უნებართვო დამუშავებას;

კანონი - „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი.

4. პერსონალურ მონაცემთა დამუშავების საფუძვლები

4.1. პერსონალურ მონაცემთა დამუშავება დასაშვებია მხოლოდ “პერსონალურ მონაცემთა დაცვის შესახებ” საქართველოს კანონით გათვალისწინებული ერთ-ერთი საფუძვლით:

- მონაცემთა სუბიექტის თანხმობით;
- მონაცემთა სუბიექტთან დადებული გარიგებით ნაკისრი ვალდებულების შესასრულებლად ან მონაცემთა სუბიექტის მოთხოვნით გარიგების დასადავად;
- მონაცემთა დამუშავება გათვალისწინებულია კანონით;
- მონაცემთა დამუშავება საჭიროა დამუშავებისთვის პასუხისმგებელი პირის მიერ საქართველოს კანონმდებლობით ნაკისრი ვალდებულებების შესასრულებლად;
- მონაცემთა დამუშავება აუცილებელია ლეგიტიმური ინტერესების დასაცავად, გარდა იმ შემთხვევისა, როდესაც არსებობს მონაცემთა სუბიექტის უფლებების დაცვის აღმატებული ინტერესი.

4.2. კომპანიის მიერ მონაცემთა დამუშავება მოიცავს ავტომატური, ნახევრად ავტომატური ან არაავტომატური საშუალებების გამოყენებით მონაცემთა მიმართ შესრულებულ ნებისმიერ მოქმედებას, კერძოდ, მათ მონაცემთა სუბიექტისგან ან მესამე პირ(ებ)ისგან მოპოვებას, შეგროვებას ან სხვაგვარად დამუშავებას.

5. პერსონალურ მონაცემთა დამუშავების პრინციპები

5.1. კომპანია უზრუნველყოფს, რომ პერსონალური მონაცემების დამუშავება განხორციელდეს საქართველოს კანონის „პერსონალურ მონაცემთა დაცვის შესახებ“ მოთხოვნების შესაბამისად და შემდეგი პრინციპების დაცვით:

- მონაცემები უნდა დამუშავდეს სამართლიანად, კანონიერად და გამჭვირვალედ;
- მონაცემები უნდა შეგროვდეს და დამუშავდეს მხოლოდ კონკრეტული, მკაფიო და ლეგიტიმური მიზნებისთვის;
- მონაცემები უნდა იყოს ადეკვატური, რელევანტური და შემოიფარგლოს მხოლოდ იმით, რაც აუცილებელია დამუშავების მიზნებისათვის;
- მონაცემები უნდა იყოს ზუსტი და განახლებული; ნებისმიერი უზუსტობა უნდა წაიშალოს ან/და დაუყოვნებლივ გამოსწორდეს;
- მონაცემები არ უნდა ინახებოდეს იმაზე მეტი ხნით, ვიდრე აუცილებელია იმ მიზნების მისაღწევად, რისთვისაც ისინი მუშავდება;
- მონაცემები უნდა დამუშავდეს უსაფრთხოდ.

6. პერსონალურ მონაცემთა კატეგორიები

6.1. კომპანია პერსონალურ მონაცემებს ამუშავებს მხოლოდ კონკრეტული, წინასწარ განსაზღვრული და ლეგიტიმური მიზნებისთვის, მონაცემთა მინიმიზაციის პრინციპის დაცვით;

6.2. **დასაქმებულების, სტაჟიორებისა და დასაქმების მსურველი პირები:** მონაცემთა დამუშავების წესი რეგულირდება “დასაქმებულთა პერსონალურ მონაცემთა დაცვის პოლიტიკით,” რომელიც სავალდებულო წესით ეცნობა დასაქმებულსა და დასაქმების მსურველ პირებს.

6.3. **კლიენტები და კონტრაქტები:** მუშავდება მხოლოდ ის მონაცემები, რომლებიც აუცილებელია სახელშეკრულებო ვალდებულებების შესრულების, მომსახურების გაწევისა და საგადასახადო კანონმდებლობის მოთხოვნათა დასაკმაყოფილებლად, კერძოდ:

- **საიდენტიფიკაციო მონაცემები:** სახელი, გვარი, დაბადების თარიღი, პირადი ნომერი/პასპორტის ნომერი, საინდეტიფიკაციო მონაცემის გაცემის თარიღი/გამცემი ორგანო, მოქალაქეობა;
- **საკონტაქტო მონაცემები:** ტელეფონის ნომერი, მისამართი, ელ.ფოსტა;
- **ფინანსური მონაცემები:** ფინანსური მდგომარეობა, საკრედიტო ისტორია, კრედიტუნარიანობა, შემოსავლების შესახებ ინფორმაცია, საბანკო ანგარიშის ნომერი, ანგარიშზე განხორციელებული შემოსავალი/გასავალი, ინფორმაცია მოვალეთა რეესტრიდან;
- **საჯაროდ ხელმისაწვდომი ინფორმაცია:** ინფორმაცია, რომელსაც კომპანია მოიპოვებს პირის შესახებ საჯაროდ განთავსებული, კანონიერად ხელმისაწვდომი ბაზებიდან;
- **ოჯახის წევრის შესახებ:** საიდენტიფიკაციო და საკონტაქტო მონაცემები.

7. არასრულწლოვანის მონაცემების დამუშავება

7.1. არასრულწლოვანი პირის შესახებ მონაცემები მუშავდება “პერსონალურ მონაცემთა დაცვის შესახებ” საქართველოს კანონის მოთხოვნების შესაბამისად.

8. გარდაცვლილი პირის შესახებ მონაცემების დამუშავება

8.1. გარდაცვლილი პირის შესახებ მონაცემები მუშავდება „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მოთხოვნების შესაბამისად.

8.2. კომპანია გარდაცვლილი პირის შესახებ მონაცემებს ამუშავებს სადაზღვევო კომპანიის მიერ სიცოცხლის დაზღვევის ხელშეკრულებით ნაკისრი ვალდებულების შესრულების მიზნით. აღნიშნული მიზნით მუშავდება შემდეგი მონაცემები:

- გარდაცვლილი პირის სახელი, გვარი, პირადი ნომერი, სქესი, ასაკი;
- გარდაცვალების ცნობა;
- ფორმა 100 და ფორმა 106;
- ექსპერტიზის დასკვნა (ასეთის არსებობის და სადაზღვევო კომპანიის მოთხოვნის შემთხვევაში).

- სხვა დამატებითი დოკუმენტაცია, რომელსაც მოითხოვს სადაზღვეო კომპანია და ქართულ კრედიტს გარდაცვლილი პირის უფლებამონაცვლე/ოჯახის წევრი თავად წარუდგენს.

9. ვიდეო და აუდიომონიტორინგის განხორციელება

- 9.1. ვიდეომონიტორინგი მიმდინარეობს კომპანიის შიდა და გარე სივრცეში პირის უსაფრთხოების, საკუთრებისა და კონფიდენციალური ინფორმაციის დაცვის მიზნით;
- 9.2. ვიდეომონიტორინგი მიმდინარეობს მხოლოდ იმ სივრცეებში, სადაც ეს აუცილებელია დასახული მიზნების მისაღწევად. დაუშვებელია მონიტორინგი იქ, სადაც პირს აქვს პირადი ცხოვრების დაცულობის გონივრული მოლოდინი;
- 9.3. აუდიომონიტორინგი მიმდინარეობს სატელეფონო მომსახურების სრულყოფისა და გაუმჯობესების მიზნით;
- 9.4. ვიდეომონიტორინგისა და აუდიომონიტორინგის განხორციელების ტექნიკური პირობები, ჩანაწერების შენახვის ვადები და მათზე წვდომის წესი განსაზღვრულია კომპანიის შიდა დოკუმენტით - „ვიდეომონიტორინგისა და აუდიომონიტორინგის განხორციელების წესი“.

10. პირდაპირი მარკეტინგი

- 10.1. მონაცემთა დამუშავება პირდაპირი მარკეტინგის მიზნით შეიძლება განხორციელდეს მხოლოდ მონაცემთა სუბიექტის თანხმობის შემთხვევაში;
- 10.2. მონაცემთა სუბიექტის სახელის, გვარის, მისამართის, ტელეფონის ნომრისა და ელექტრონული ფოსტის მისამართის გარდა, პირდაპირი მარკეტინგის მიზნით სხვა მონაცემების დამუშავებისთვის აუცილებელია მონაცემთა სუბიექტის წერილობითი თანხმობა;
- 10.3. მონაცემთა სუბიექტს უფლება აქვს ნებისმიერ დროს გამოიხმოს თანხმობა მისი პერსონალური მონაცემების პირდაპირი მარკეტინგის მიზნით დამუშავების შესახებ;
- 10.4. კომპანია ვალდებულია, შეწყვიტოს პირდაპირი მარკეტინგის მიზნით მონაცემთა დამუშავება მონაცემთა სუბიექტის შესაბამისი მოთხოვნის მიღებიდან არაუგვიანეს 7 სამუშაო დღისა;
- 10.5. მონაცემთა სუბიექტი უფლებამოსილია, მოითხოვოს პირდაპირი მარკეტინგის მიზნით მონაცემთა დამუშავების შეწყვეტა იმავე ფორმით, რომლითაც პირდაპირი მარკეტინგი ხორციელდება;
- 10.6. კომპანია ვალდებულია მონაცემთა სუბიექტის მიერ მონაცემთა დამუშავებაზე თანხმობა და თანხმობის გამოხმობა აღრიცხოს და შეინახოს პირდაპირი მარკეტინგის განხორციელების ვადით და პირდაპირი მარკეტინგის განხორციელების შეწყვეტიდან 1 წლის განმავლობაში.

11. მონაცემთა გადაცემა მესამე პირებისთვის

11.1 კომპანიამ, კონკრეტული დავალების შესასრულებლად, შესაძლებელია პერსონალური მონაცემები გაუზიაროს მესამე პირებს იმ შემთხვევაში, თუ იგი ძირითადი საქმიანობის ფარგლებში იყენებს სხვა პროვაიდერების მომსახურებას. ასეთი მომსახურება შეიძლება მოიცავდეს:

- ვებ-ინსტრუმენტების ან/და აპლიკაციების დიზაინსა და მიმდინარე საექსპლუატაციო მომსახურებას;
- IT სერვისის პროვაიდერების მომსახურებას, რომლებიც უზრუნველყოფენ აპლიკაციის ან ინფრასტრუქტურის (მაგ., „cloud“) სერვისებს;
- იურიდიულ, აუდიტორულ და სხვა პროფესიულ მომსახურებას, რომელსაც კომპანიას აწვდიან იურისტები, ნოტარიუსები, მინდობილი პირები, აუდიტორული კომპანიები და სხვ.

11.2. კომპანია უფლებამოსილია მონაცემთა სუბიექტის პერსონალური მონაცემები გადასცეს საგამომიებო უწყებას, შრომის ინსპექციასა თუ სხვა სახელმწიფო/ადმინისტრაციულ ორგანოებს, რომლებიც უფლებამოსილი არიან, მოითხოვონ სუბიექტთან დაკავშირებული ინფორმაციის გაზიარება;

11.3. პერსონალური მონაცემების მესამე პირებისთვის გადაცემა ხორციელდება მხოლოდ საქართველოს მოქმედი კანონმდებლობისა და მონაცემთა დაცვის მოთხოვნების შესაბამისად.

11.4. კომპანია პასუხისმგებელია პერსონალური მონაცემების დაცვაზე კანონმდებლობით დადგენილი სტანდარტების შესაბამისად. კომპანია არ აგებს პასუხს მესამე პირების ისეთი უკანონო ქმედებების შედეგად დამდგარ ზიანზე, რომლებიც სცდება კომპანიის კონტროლის ფარგლებს და მიუხედავად გონივრული უსაფრთხოების ზომების მიღებისა, შეუძლებელი იყო მათი პრევენცია.

12. მონაცემთა სუბიექტის უფლებები

12.1. მონაცემთა სუბიექტი სარგებლობს “პერსონალურ მონაცემთა დაცვის შესახებ” საქართველოს კანონის მე-3 თავით გათვალისწინებული უფლებებით, რომლებიც მოიცავს, მაგრამ არ შემოიფარგლება შემდეგით:

- **წვდომის უფლება** - მიიღოს ინფორმაცია, თუ რა პერსონალური მონაცემები მუშავდება და რა მიზნით, მათ შორის ინფორმაცია ვიდეო მონიტორინგის განმახორციელებელი პირის, მონიტორინგის მიზნისა და სამართლებრივი საფუძვლის შესახებ.
- **შესწორების/განახლების უფლება** - მოითხოვოს არაზუსტი ან არასრული მონაცემების შესწორება ან განახლება;
- **წაშლის უფლება** („დავიწყების უფლება“) - მოითხოვოს მონაცემების წაშლა, თუ მათი დამუშავება აღარარის საჭირო მიზნის მისაღწევად ან თანხმობა გაუქმებულია, გარდა კანონით დადგენილი გამონაკლისებისა;
- **დამუშავების შეზღუდვის უფლება** - მოითხოვოს მონაცემთა დამუშავების შეზღუდვა კანონით განსაზღვრულ შემთხვევებში;

- თანხმობის გამოხმობის (უარის თქმის) უფლება - გამოიხმოს გაცემული თანხმობა.
- უფლებების დარღვევის შემთხვევაში მიმართოს სახელმწიფო აუდიტის სამსახურს ან სასამართლოს.

13. მონაცემების უსაფრთხოების უზრუნველყოფა

13.1. კომპანიის მიერ მიღებულია შესაბამისი ორგანიზაციული და ტექნიკური ზომები ელექტრონულად და ფიზიკურად არსებული მონაცემების კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის უზრუნველსაყოფად.

13.2. კომპანიაში აღირიცხება ელექტრონული ფორმით არსებული მონაცემების მიმართ შესრულებული ყველა მოქმედება (მათ შორის, ინციდენტების შესახებ, მონაცემთა შეგროვების, შეცვლის, მათზე წვდომის, მათი გამჟღავნების (გადაცემის), დაკავშირებისა და წაშლის თაობაზე ინფორმაციის). არაელექტრონული ფორმით არსებულ მონაცემთა დამუშავებისას, კი, აღირიცხება მონაცემთა გამჟღავნებასთან ან/და ცვლილებასთან დაკავშირებული ყველა მოქმედება (მათ შორის, ინციდენტების შესახებ ინფორმაციის).

13.3. კომპანიის ხელმძღვანელობასა და წარმომადგენლობაზე უფლებამოსილი პირის აქტით, კომპანიის თანამშრომლების უფლებამოსილების შესაბამისად, განისაზღვრება პერსონალურ მონაცემებზე წვდომის ფარგლები (მონაცემების კატეგორიის მითითებით).

13.4. იმ შემთხვევაში თუ კომპანია განახორციელებს მონაცემების მესამე პირებისთვის გადაცემას, მათ შორის, ინფორმაციის სხვა ქვეყნის რეზიდენტი პირ(ებ)ისათვის გადაცემას, კომპანია უზრუნველყოფს პერსონალურ მონაცემთა გადაცემის შესახებ შესაბამისი ხელშეკრულების გაფორმებას, რომლითაც კანონმდებლობით გათვალისწინებული მოთხოვნების შესაბამისად, განისაზღვრება მიმღები მხარის ვალდებულებები პერსონალურ მონაცემების დაცვის უზრუნველსაყოფად.

14. მონაცემთა შენახვის ვადები

15.1. კომპანია პერსონალურ მონაცემებს ინახავს მხოლოდ იმ ავდით, რაც აუცილებელია მათი დამუშავების კონკრეტული მიზნის მისაღწევად, ან განსაზღვრულია შესაბამისი კანონმდებლობით:

- **ვიდეომონიტორინგის ჩანაწერები:** ინახება 30 კალენდარული დღის განმავლობაში;
- **აუდიომონიტორინგის ჩანაწერები:** ინახება 2 წლის განმავლობაში;
- **დასაქმებულთან, სტაჟიორთან და დასაქმების მსურველ პირთან დაკავშირებული დოკუმენტაციის შენახვის ვადები** განისაზღვრება “დასაქმების მსურველი პირების, დასაქმებულების, სტაჟიორებისა და ყოფილი დასაქმებულების პერსონალურ მონაცემთა დაცვის პოლიტიკის” შესაბამისად;
- **სახელშეკრულებო და ფინანსური დოკუმენტაცია:** ინახება ხელშეკრულების შეწყვეტიდან 6 წლის განმავლობაში;
- **შემოსული განცხადებები:** საქმისწარმოების ვადით;

- უბედურ შემთხვევებთან/ინციდენტებთან დაკავშირებული პერსონალური მონაცემები ინახება მოკვლევის შიდა პროცედურით განსაზღვრული შემდეგი ვადით:

ა) საშუალო სიმძიმის უბედური შემთხვევა - 5 წელი;

ბ) მძიმე უბედური შემთხვევა - 7 წელი;

გ) ფატალური უბედური შემთხვევა - 10 წელი;

დ) მასობრივი უბედური შემთხვევა - 15 წელი.

15.2. შენახვის ვადის გასვლის შემდეგ, კომპანია უზრუნველყოფს მონაცემთა შეუქცევად განადგურებას მექანიკური გზით.

15. ინციდენტზე რეაგირების წესი

16.1. დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია აღრიცხოს ინციდენტი, დამდგარი შედეგი, მიღებული ზომები და ინციდენტის აღმოჩენიდან არაუგვიანეს 72 საათისა მის შესახებ წერილობით ან ელექტრონულად შეატყობინოს სახელმწიფო აუდიტის სამსახურს, გარდა იმ შემთხვევისა, როდესაც ნაკლებად სავარაუდოა, რომ ინციდენტი მნიშვნელოვან ზიანს გამოიწვევს ან/და მნიშვნელოვან საფრთხეს შეუქმნის ადამიანის ძირითად უფლებებსა და თავისუფლებებს.

16.2. კომპანია უზრუნველყოფს ინციდენტების შესახებ ინფორმაციის აღრიცხვას კანონმდებლობით დადგენილი წესით.

16. დასკვნითი დებულებები

17.1. წესები და პირობები, რომლებიც არ არის განსაზღვრული წინამდებარე დოკუმენტით, რეგულირდება საქართველოს კანონმდებლობის შესაბამისად;

17.2. პოლიტიკის დოკუმენტი გადაიხედება საჭიროების მიხედვითან პერსონალურ მონაცემთა დამუშავების მარეგულირებელი კანონმდებლობის მნიშვნელოვანი ცვლილების დროს.

17. საკონტაქტო ინფორმაცია

18.1. მონაცემთა სუბიექტი უფლებამოსილია ნებისმიერ დროს მიმართოს ორგანიზაციას წინამდებარე პოლიტიკასთან დაკავშირებული, მისთვის საჭირო ინფორმაციის მიღების მიზნით, საკონტაქტო ტელეფონის ნომერი: (+995 32)2 -500-100 ელ-ფოსტა: info@geocredit.ge

18. პერსონალურ მონაცემთა დაცვის ოფიცერი

კომპანიას ჰყავს პერსონალურ მონაცემთა დაცვის ოფიცერი, რომელიც უზრუნველყოფს პერსონალურ მონაცემთა დამუშავების პროცესების შესაბამისობას პერსონალურ მონაცემთა დაცვის კანონმდებლობასთან. საკუთარ საქმიანობაში დამოუკიდებელია და ექვემდებარება მმართველობის უმაღლეს რგოლს.

შპს “უსაფრთხო მონაცემთა გადაწყვეტილებები” (ს/კ: 405805384)

საკონტაქტო ინფორმაცია: anatavkhelidze@safedata.ge