

ელექტრონული საფულის კონფიდენციალურობის პოლიტიკა

მუხლი 1. ზოგადი დებულებები

- 1.1 წინამდებარე კონფიდენციალურობის პოლიტიკა განსაზღვრავს შპს „მულტიპრაიმ“-ის მიერ ელექტრონული საფულის მომსახურების ფარგლებში მომხმარებელთა პერსონალური მონაცემების შეგროვების, მოპოვების, გამოყენების, შენახვის, დაცვისა და კანონმდებლობით გათვალისწინებულ შემთხვევებში მესამე პირებისთვის გადაცემის წესებს.
- 1.2 წინამდებარე პოლიტიკა ვრცელდება ყველა მომხმარებელზე, რომელიც რეგისტრირდება, სარგებლობს ან ცდილობს ისარგებლოს კომპანიის ელექტრონული საფულის მომსახურებით.
- 1.3 პოლიტიკა ვრცელდება როგორც მომხმარებლის რეგისტრაციისა და იდენტიფიკაციის ეტაპზე, ისე ელექტრონული საფულის გამოყენების მთელი პერიოდის განმავლობაში.
- 1.4 კომპანიის მიერ პერსონალური მონაცემების დამუშავება ხორციელდება საქართველოს მოქმედი კანონმდებლობის, მათ შორის „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონისა და საგადახდო მომსახურების მარეგულირებელი კანონმდებლობის მოთხოვნების შესაბამისად.
- 1.5 წინამდებარე პოლიტიკის მიზანია მომხმარებლისთვის გასაგები და გამჭვირვალე ფორმით განისაზღვროს:
 - რა სახის პერსონალურ მონაცემებს ამუშავებს კომპანია
 - რა მიზნით და სამართლებრივი საფუძვლით ხდება მათი დამუშავება
 - როგორ გამოიყენება მონაცემები ელექტრონული საფულის მომსახურების გაწევისას
 - ვის შეიძლება გადაეცეს მონაცემები
 - რა ვადით ინახება მონაცემები
 - როგორ უზრუნველყოფს კომპანია მონაცემთა უსაფრთხოებას
 - რა უფლებები აქვს მომხმარებელს პერსონალურ მონაცემებთან დაკავშირებით

მუხლი 2. მონაცემთა დამუშავებისთვის პასუხისმგებელი პირი

- 2.1 პერსონალურ მონაცემთა დამუშავებისთვის პასუხისმგებელი პირია შპს „მულტიპრაიმ“

საიდენტიფიკაციო კოდი: 400397959

იურიდიული მისამართი: საქართველო, ქ. თბილისი, მთაწმინდის რაიონი, ვერცხლის ქ., №1

ელექტრონული ფოსტა: info@multiprime.ge

საკონტაქტო ტელეფონი: [+995 598 222 332](tel:+995598222332)

- 2.2 კომპანია პასუხისმგებელია მის მიერ დამუშავებული პერსონალური მონაცემების კანონიერ, სამართლიან და გამჭვირვალე დამუშავებაზე.
- 2.3 მომხმარებელს პერსონალური მონაცემების დამუშავებასთან დაკავშირებული საკითხების შესახებ შეუძლია მიმართოს კომპანიას ზემოაღნიშნული საკონტაქტო საშუალებებით.

მუხლი 3. ელექტრონული საფულის მომსახურების შესახებ

3.1 კომპანიის ელექტრონული საფულე წარმოადგენს კომპანიის მიერ მომხმარებლისთვის შეთავაზებულ ელექტრონულ მომსახურებას, რომლის მეშვეობითაც მომხმარებელს, შესაბამისი მომსახურების პირობების ფარგლებში, შეუძლია:

- ელექტრონული საფულის შექმნა და გამოყენება
- ელექტრონული საფულის შევსება
- ელექტრონული საფულიდან თანხის გადარიცხვა
- ელექტრონული საფულიდან თანხის გატანა
- საკუთარი ოპერაციების შესახებ ინფორმაციის მიღება
- კომპანიის მიერ შეთავაზებული სხვა შესაბამისი საგადახდო მომსახურებების გამოყენება

3.2 აღნიშნული მომსახურებების განხორციელების მიზნით კომპანია ამუშავებს მხოლოდ იმ მოცულობის პერსონალურ მონაცემებს, რომლებიც აუცილებელია შესაბამისი მომსახურების გაწევისთვის, კანონით გათვალისწინებული ვალდებულებების შესრულებისთვის ან სხვა შესაბამისი სამართლებრივი მიზნის მისაღწევად.

მუხლი 4. პერსონალური მონაცემების კატეგორიები

4.1 ელექტრონული საფულის მომხმარებლის შესახებ კომპანია შესაძლოა ამუშავებდეს შემდეგ მონაცემებს:

4.1.1 საიდენტიფიკაციო მონაცემები:

- სახელი
- გვარი
- დაბადების თარიღი
- მოქალაქეობა
- პირადი ნომერი ან სხვა საიდენტიფიკაციო ნომერი
- პირადობის დამადასტურებელი დოკუმენტი
- დოკუმენტის ნომერი
- დოკუმენტის გაცემის და მოქმედების ვადა
- დოკუმენტის გამცემი ორგანო
- კანონით დაშვებულ შემთხვევებში საიდენტიფიკაციო დოკუმენტის ასლი ან გამოსახულება
- მომხმარებლის ფოტოსურათი
- იდენტიფიკაციისა და ვერიფიკაციის პროცესის შესაბამისი მონაცემები

4.1.2 საკონტაქტო მონაცემები

- მობილური ტელეფონის ნომერი
- ელექტრონული ფოსტის მისამართი
- იურიდიული/ფაქტობრივი საცხოვრებელი მისამართი
- სხვა საკონტაქტო მონაცემები, როდესაც მათი დამუშავება აუცილებელია მომსახურების პირობებში

4.1.3 საქმიანობის შესახებ მონაცემები

კომპანია, კანონმდებლობით გათვალისწინებული მოთხოვნების შესაბამისად, შესაძლოა ამუშავებდეს:

- დასაქმების სტატუსს
- სამუშაო სფეროს
- სამუშაო ადგილს
- სამუშაო პოზიციას
- შემოსავლის შესახებ ინფორმაციას
- სხვა შესაბამის ინფორმაციას, რომელიც აუცილებელია მომხმარებლის იდენტიფიკაციისა და რისკის შეფასებისთვის

4.1.4 ფინანსური და საგადახდო მონაცემები

- ელექტრონული საფულის იდენტიფიკატორი
- საფულესთან დაკავშირებული ანგარიშის მონაცემები
- ოპერაციის თანხა
- ოპერაციის ვალუტა
- ოპერაციის თარიღი და დრო
- ოპერაციის ტიპი
- ოპერაციის სტატუსი
- გადამხდელის შესახებ შესაბამისი მონაცემები
- მიმღების შესახებ შესაბამისი მონაცემები
- ოპერაციის დანიშნულება
- თანხის შევსების მონაცემები
- თანხის გატანის მონაცემები
- ტრანზაქციის ისტორია

4.1.5 KYC/AML/CFT მონაცემები

საქართველოს მოქმედი კანონმდებლობითა და კომპანიის შესაბამისი ვალდებულებებით გათვალისწინებულ შემთხვევებში კომპანია შესაძლოა ამუშავებდეს:

- მომხმარებლის იდენტიფიკაციისა და ვერიფიკაციის მონაცემებს
- მომხმარებლის საქმიანობის შესახებ ინფორმაციას
- შემოსავლისა და შემოსავლის წყაროს შესახებ ინფორმაციას
- ქონების/ფულადი სახსრების წარმოშობის შესახებ ინფორმაციას

- მომხმარებლის რისკის შეფასებისთვის საჭირო მონაცემებს
- პოლიტიკურად აქტიური პირის (PEP) სტატუსთან დაკავშირებულ ინფორმაციას
- სანქციებთან დაკავშირებული შემოწმების მონაცემებს
- მომხმარებლის ბენეფიციარი მესაკუთრის შესახებ ინფორმაციას, როდესაც ასეთი მონაცემის დამუშავება საჭიროა
- ტრანზაქციის მონიტორინგის შედეგად მიღებულ ინფორმაციას
- საექვო ან უჩვეულო ოპერაციასთან დაკავშირებულ ინფორმაციას
- კანონმდებლობით გათვალისწინებულ სხვა შესაბამისობის მონაცემებს

4.1.6 ტექნიკური და ელექტრონული მონაცემები

ელექტრონული საფულისა და კომპანიის ვებგვერდის გამოყენებისას კომპანია შესაძლოა ამუშავებდეს:

- ა. IP მისამართს
- ბ. მოწყობილობის ტიპს
- გ. ოპერაციულ სისტემას
- დ. ბრაუზერის მონაცემებს
- ე. მოწყობილობის ტექნიკურ იდენტიფიკატორებს
- ვ. მომხმარებლის ავტორიზაციის მონაცემებს
- ზ. სისტემაში შესვლის თარიღსა და დროს
- თ. სისტემაში განხორციელებული მოქმედებების შესახებ ლოგებს
- ი. უსაფრთხოების მიზნით შექმნილ ტექნიკურ ჩანაწერებს

მუხლი 5. პერსონალური მონაცემების დამუშავების მიზნები

5.1 კომპანია პერსონალურ მონაცემებს ამუშავებს შემდეგი მიზნებისთვის:

- ა. მომხმარებლის რეგისტრაციისა და ელექტრონული საფულის შექმნისთვის
- ბ. მომხმარებლის იდენტიფიკაციისა და ვერიფიკაციისთვის
- გ. ელექტრონული საფულის მომსახურების გაწევისთვის
- დ. საფულის შევსების ოპერაციების განხორციელებისთვის
- ე. თანხის გადარიცხვის ოპერაციების განხორციელებისთვის
- ვ. თანხის გატანის ოპერაციების განხორციელებისთვის
- ზ. მომხმარებლის მიერ განხორციელებული ოპერაციების აღრიცხვისთვის
- თ. მომხმარებლისთვის ოპერაციის სტატუსისა და შესაბამისი ინფორმაციის მიწოდებისთვის

- ი. არაავტორიზირებული ოპერაციების გამოვლენისა და პრევენციისთვის
- კ. თაღლითობისა და თაღლითობის მცდელობის გამოვლენისა და პრევენციისთვის
- ლ. ფულის გათეთრებისა და ტერორიზმის დაფინანსების წინააღმდეგ ბრძოლის მოთხოვნების შესრულებისთვის
- მ. სანქციებთან დაკავშირებული მოთხოვნების შესრულებისთვის
- ნ. მომხმარებლის რისკის შეფასებისა და შესაბამისი ღონისძიებების განხორციელებისთვის
- ო. ინფორმაციული უსაფრთხოებისა და კიბერუსაფრთხოების უზრუნველყოფისთვის
- პ. მომხმარებლის საჩივრებისა და მოთხოვნების განხილვისთვის
- ჟ. მომსახურების ტექნიკური და ოპერაციული უზრუნველყოფისთვის
- რ. კანონმდებლობით დაკისრებული ვალდებულებების შესრულებისთვის
- ს. სასამართლოს, ზედამხედველი და სხვა უფლებამოსილი სახელმწიფო ორგანოების კანონიერი მოთხოვნების შესრულებისთვის
- ტ. კომპანიის კანონიერი ინტერესების დაცვისთვის, კანონით დაშვებულ ფარგლებში

მუხლი 6. მონაცემთა დამუშავების სამართლებრივი საფუძვლები

6.1 კომპანია პერსონალურ მონაცემებს ამუშავებს შესაბამისი სამართლებრივი საფუძვლის არსებობის შემთხვევაში

6.2 მონაცემთა დამუშავების სამართლებრივი საფუძველი შეიძლება იყოს:

- მომხმარებელთან ხელშეკრულების დადება ან ხელშეკრულებით გათვალისწინებული მომსახურების გაწევა
- კომპანიისთვის კანონით დაკისრებული ვალდებულებების შესრულება
- მომხმარებლის თანხმობა, როდესაც მონაცემთა დამუშავებისთვის თანხმობა

წარმოადგენს შესაბამის სამართლებრივ საფუძველს

• კომპანიის ან მესამე პირის მნიშვნელოვანი ლეგიტიმური ინტერესის დაცვა, კანონით დადგენილი წინაპირობების არსებობისას

- კანონმდებლობით გათვალისწინებული სხვა სამართლებრივი საფუძველი

6.3 იმ შემთხვევაში, როდესაც მონაცემთა დამუშავება ხორციელდება კანონით დაკისრებული ვალდებულებების შესასრულებლად, მომხმარებლის მიერ თანხმობის გამოხმაობა თავისთავად არ იწვევს კანონით სავალდებულო მონაცემთა დამუშავების შეწყვეტას

მუხლი 7. KYC და მომხმარებლის იდენტიფიკაცია

7.1 ელექტრონული საფულის გახსნამდე ან/და მომსახურების შესაბამის ეტაპზე კომპანია ახორციელებს მომხმარებლის იდენტიფიკაციასა და ვერიფიკაციას საქართველოს მოქმედი კანონმდებლობისა და კომპანიის შიდა პროცედურების შესაბამისად.

7.2 KYC პროცესის ფარგლებში მომხმარებლისგან მოთხოვნილი ინფორმაციის მოცულობა განისაზღვრება მომსახურების, მომხმარებლის ტიპის, რისკის დონისა და კანონმდებლობით გათვალისწინებული მოთხოვნების შესაბამისად.

7.3. მომხმარებლისთვის მომსახურების გაწევა შესაძლოა შეჩერდეს ან შეიზღუდოს, თუ მომხმარებელი არ წარმოადგენს კანონით ან კომპანიის შესაბამისი პროცედურით გათვალისწინებულ ინფორმაციას ან დოკუმენტაციას.

7.4. კომპანია უფლებამოსილია გადაამოწმოს მომხმარებლის მიერ მიწოდებული ინფორმაცია შესაბამისი და კანონიერად ხელმისაწვდომი წყაროების გამოყენებით.

მუხლი 8. AML/CFT და სანქციებთან დაკავშირებული დამუშავება

8.1. კომპანია პერსონალურ მონაცემებს ამუშავებს ფულის გათეთრებისა და ტერორიზმის დაფინანსების წინააღმდეგ ბრძოლის, სანქციების შესრულებისა და სხვა შესაბამისობის მოთხოვნების უზრუნველყოფის მიზნით.

8.2. აღნიშნული მიზნით კომპანია უფლებამოსილია განახორციელოს მომხმარებლისა და შესაბამისი ოპერაციების შემოწმება კანონით დაშვებულ წყაროებში.

8.3. მომხმარებლის მონაცემები შესაძლოა გამოყენებულ იქნეს მომხმარებლის რისკის კატეგორიის განსაზღვრისა და შესაბამისი კონტროლის ღონისძიებების შესარჩევად.

8.4. კანონმდებლობით გათვალისწინებულ შემთხვევაში კომპანია უფლებამოსილია შესაბამისი ინფორმაცია გადასცეს უფლებამოსილ სახელმწიფო ორგანოს.

8.5. AML/CFT მიზნებისთვის დამუშავებული მონაცემების შენახვის ვადა განისაზღვრება შესაბამისი კანონმდებლობისა და კომპანიის მონაცემთა შენახვის წესების შესაბამისად.

მუხლი 9. ტრანზაქციების მონიტორინგი და თაღლითობის პრევენცია

9.1. მომხმარებლისა და მისი ოპერაციების უსაფრთხოების უზრუნველსაყოფად კომპანია იყენებს ტრანზაქციების მონიტორინგისა და თაღლითობის გამოვლენის/პრევენციის შესაბამის მექანიზმებს.

9.2. ამ მიზნით შესაძლოა დამუშავდეს:

- ოპერაციის მონაცემები;
- მომხმარებლის მოწყობილობის ტექნიკური მონაცემები;
- შესვლისა და ავტორიზაციის მონაცემები;
- მომხმარებლის მოქმედებების ისტორია;
- ოპერაციის გეოგრაფიული და ტექნიკური მახასიათებლები, როდესაც ასეთი მონაცემები მუშავდება;
- უსაფრთხოების სისტემის მიერ გამოვლენილი საეჭვო ქცევის ინდიკატორები.

9.3. შესაბამისი მონაცემების დამუშავება ხორციელდება თაღლითობის, უკანონო გამოყენებისა და არაავტორიზებული ოპერაციების პრევენციის მიზნით.

მუხლი 10. ავტომატიზებული დამუშავება და პროფაილინგი

- 10.1. კომპანია შესაძლოა იყენებდეს ავტომატიზებულ ტექნიკურ საშუალებებს მომხმარებლის რისკის შეფასების, ტრანზაქციების მონიტორინგის, თაღლითობის გამოვლენისა და უსაფრთხოების უზრუნველყოფის მიზნით.
- 10.2. ავტომატიზებული დამუშავების გამოყენების შემთხვევაში იგი განხორციელდება საქართველოს მოქმედი კანონმდებლობის მოთხოვნების შესაბამისად.
- 10.3. იმ შემთხვევაში, თუ კანონმდებლობა მომხმარებლისთვის დამატებითი უფლებების უზრუნველყოფას ითვალისწინებს ავტომატიზებულ გადაწყვეტილებასთან ან პროფაილინგთან დაკავშირებით, კომპანია უზრუნველყოფს შესაბამისი უფლებების განხორციელების შესაძლებლობას.

მუხლი 11. პერსონალური მონაცემების მესამე პირებისთვის გადაცემა

- 11.1. კომპანია მომხმარებლის მონაცემებს მესამე პირს გადასცემს მხოლოდ შესაბამისი სამართლებრივი საფუძვლის არსებობის შემთხვევაში.
- 11.2. მონაცემები შესაძლოა გადაეცეს:
- საქართველოს ეროვნულ ბანკს;
 - სხვა უფლებამოსილ საზედამხედველო ორგანოებს;
 - საქართველოს კანონმდებლობით უფლებამოსილ სახელმწიფო ორგანოებს;
 - სასამართლოსა და კანონით უფლებამოსილ სხვა ორგანოებს;
 - საგადახდო მომსახურებაში ჩართულ ბანკებსა და სხვა საგადახდო მომსახურების პროვაიდერებს, როდესაც ეს აუცილებელია კონკრეტული ოპერაციის განსახორციელებლად;
 - ტექნოლოგიურ/ტექნიკურ მომსახურების მიმწოდებლებს;
 - იდენტიფიკაციისა და ვერიფიკაციის მომსახურების მიმწოდებლებს;
 - თაღლითობის პრევენციისა და მონიტორინგის მომსახურების მიმწოდებლებს;
 - აუდიტორებსა და პროფესიულ მომსახურების მიმწოდებლებს, შესაბამისი სამართლებრივი საფუძვლის არსებობის შემთხვევაში;
 - სხვა პირებს, როდესაც მონაცემთა გადაცემა პირდაპირ არის გათვალისწინებული კანონით ან აუცილებელია მომხმარებლის მიერ მოთხოვნილი მომსახურების განსახორციელებლად.

11.3. კომპანია მესამე პირებთან ურთიერთობისას იღებს შესაბამის ზომებს პერსონალური მონაცემების კონფიდენციალურობისა და უსაფრთხოების უზრუნველსაყოფად.

მუხლი 12. პერსონალური მონაცემების შენახვა

- 12.1. კომპანია პერსონალურ მონაცემებს ინახავს მხოლოდ იმ ვადით, რომელიც აუცილებელია შესაბამისი მიზნის მისაღწევად ან განსაზღვრულია მოქმედი კანონმდებლობით.
- 12.2. იმ მონაცემების მიმართ, რომელთა შენახვაც კანონმდებლობით არის სავალდებულო, კომპანია უზრუნველყოფს შესაბამისი სამართლებრივი ვადის დაცვას.

12.3. ელექტრონული საფულის მომხმარებლის მონაცემები შესაძლოა ინახებოდეს მომსახურების დასრულების/საფულის დახურვის შემდეგაც, თუ მათი შენახვა აუცილებელია:

- კანონით დაკისრებული ვალდებულების შესასრულებლად;
- AML/CFT მოთხოვნების შესასრულებლად;
- საგადასახადო ან საბუღალტრო მოთხოვნების შესასრულებლად;
- სასამართლო ან სამართლებრივი დავის მიზნებისთვის;
- თაღლითობის ან სხვა უკანონო ქმედების გამოძიებისა და პრევენციისთვის;
- კომპანიის კანონიერი ინტერესების დასაცავად.

12.4. მონაცემთა შენახვის კონკრეტული ვადა განისაზღვრება შესაბამისი სამართლებრივი მოთხოვნებისა და კომპანიის შიდა მონაცემთა შენახვის პოლიტიკის შესაბამისად.

12.5. შენახვის ვადის გასვლის შემდეგ კომპანია უზრუნველყოფს მონაცემთა წაშლას, განადგურებას ან სხვა კანონით დაშვებული ფორმით დამუშავების შეწყვეტას, გარდა იმ შემთხვევისა, როდესაც მონაცემთა შემდგომი შენახვა სხვა სამართლებრივი საფუძვლით არის აუცილებელი.

მუხლი 13. მონაცემთა უსაფრთხოება

13.1. კომპანია იღებს შესაბამის ტექნიკურ და ორგანიზაციულ ზომებს მომხმარებელთა პერსონალური მონაცემების დასაცავად.

13.2. უსაფრთხოების ღონისძიებები მოიცავს, მათ შორის:

- მომხმარებლის ავტორიზაციასა და ავთენტიფიკაციას;
- წვდომის უფლებების შეზღუდვას;
- პერსონალურ მონაცემებზე წვდომის კონტროლს;
- სისტემური მოქმედებების აღრიცხვას;
- ტექნიკური სისტემების მონიტორინგს;
- უსაფრთხოების ინციდენტების გამოვლენასა და მართვას;
- მონაცემთა დაცვის შესაბამის ტექნიკურ საშუალებებს;
- თანამშრომლების მიერ მონაცემებზე წვდომის პრინციპების განსაზღვრას;
- კონფიდენციალურობის ვალდებულებების დაწესებას;
- სხვა შესაბამის ტექნიკურ და ორგანიზაციულ ღონისძიებებს.

13.3. მომხმარებლის ავტორიზაციის მონაცემები დაცულია კომპანიის მიერ შესაბამისი უსაფრთხოების მექანიზმების გამოყენებით.

13.4. მომხმარებელი ვალდებულია არ გადასცეს მესამე პირს საკუთარი ავტორიზაციის მონაცემები, პაროლი, ერთჯერადი კოდი ან სხვა უსაფრთხოების მონაცემი.

მუხლი 14. მომხმარებლის უფლებები

14.1. მომხმარებელს, საქართველოს კანონმდებლობით დადგენილ ფარგლებში, უფლება აქვს:

- მიიღოს ინფორმაცია იმის შესახებ, მუშავდება თუ არა მის შესახებ პერსონალური მონაცემები;
- მიიღოს ინფორმაცია დამუშავებული მონაცემების შესახებ;
- მიიღოს ინფორმაცია მონაცემთა დამუშავების მიზნისა და სამართლებრივი საფუძვლის შესახებ;
- მიიღოს ინფორმაცია მონაცემთა წყაროს შესახებ;
- მიიღოს ინფორმაცია მონაცემთა შენახვის ვადის ან მისი განსაზღვრის კრიტერიუმების შესახებ;
- მიიღოს ინფორმაცია მონაცემთა მიმღების ან მიმღებთა კატეგორიების შესახებ;
- მოითხოვოს არაზუსტი მონაცემების გასწორება;
- კანონით გათვალისწინებულ შემთხვევაში მოითხოვოს მონაცემთა დამუშავების შეწყვეტა, წაშლა ან განადგურება;
- კანონით გათვალისწინებულ შემთხვევაში მოითხოვოს მონაცემთა დამუშავების შეზღუდვა;
- კანონით გათვალისწინებულ შემთხვევაში ისარგებლოს მონაცემთა გადატანის უფლებით;
- კანონით გათვალისწინებულ შემთხვევაში გამოიხმოს თანხმობა;
- გაასაჩივროს პერსონალური მონაცემების დამუშავებასთან დაკავშირებული დარღვევა კანონით დადგენილი წესით.

14.2. მომხმარებლის უფლებების განხორციელება არ ზღუდავს კომპანიის უფლებას, შეინახოს მონაცემები იმ მოცულობითა და ვადით, რაც კანონით არის სავალდებულო.

მუხლი 15. თანხმობის გამოხმობა

15.1. როდესაც მონაცემთა დამუშავება ეფუძნება მომხმარებლის თანხმობას, მომხმარებელს უფლება აქვს კანონით დადგენილი წესით ნებისმიერ დროს გამოიხმოს თანხმობა.

15.2. თანხმობის გამოხმობა არ მოქმედებს თანხმობის საფუძველზე მის გამოხმობამდე განხორციელებული მონაცემთა დამუშავების კანონიერებაზე.

15.3. თუ კონკრეტული მონაცემების დამუშავება სხვა სამართლებრივი საფუძვლითაც არის აუცილებელი, თანხმობის გამოხმობა არ იწვევს ასეთი მონაცემების დამუშავების ავტომატურ შეწყვეტას.

მუხლი 16. პერსონალური მონაცემების უსაფრთხოების ინციდენტი

16.1. პერსონალური მონაცემების უსაფრთხოების ინციდენტის გამოვლენის შემთხვევაში კომპანია მოქმედებს საქართველოს მოქმედი კანონმდებლობის შესაბამისად.

16.2. კომპანია იღებს შესაბამის ზომებს:

- ინციდენტის იდენტიფიცირებისთვის;
- ინციდენტის გავრცელების/განვითარების შეჩერებისთვის;

- მონაცემთა შემდგომი უკანონო დამუშავების თავიდან ასაცილებლად;
- ინციდენტის შედეგების შესამცირებლად;
- კანონით გათვალისწინებულ შემთხვევაში შესაბამისი ორგანოსთვის შეტყობინების განსახორციელებლად;
- კანონით გათვალისწინებულ შემთხვევაში მონაცემთა სუბიექტისთვის ინფორმაციის მისაწოდებლად.

მუხლი 17. მომხმარებლის მოთხოვნის წარდგენა

17.1. პერსონალურ მონაცემებთან დაკავშირებული მოთხოვნის წარდგენა

მომხმარებელს შეუძლია:

- ელექტრონული ფოსტა: info@multiprime.ge
- მისამართი: საქართველო, ქ. თბილისი, მთაწმინდის რაიონი, ვერცხლის ქ., №1
- ტელეფონი: [+995 598 222 332](tel:+995598222332)

17.2. მოთხოვნის განხილვის მიზნით კომპანიამ შესაძლოა განახორციელოს მომხმარებლის იდენტიფიკაცია, რათა თავიდან იქნეს აცილებული მონაცემებზე არაუფლებამოსილი წვდომა.

17.3. მომხმარებლის მოთხოვნა განიხილება საქართველოს მოქმედი კანონმდებლობით დადგენილი წესისა და ვადების შესაბამისად.

მუხლი 18. კონფიდენციალურობის პოლიტიკის ურთიერთკავშირი სხვა დოკუმენტებთან

18.1. წინამდებარე პოლიტიკა წარმოადგენს ელექტრონული საფულის მომხმარებლის პერსონალური მონაცემების დამუშავების ძირითად საინფორმაციო დოკუმენტს.

18.2. წინამდებარე პოლიტიკა უნდა განიხილებოდეს კომპანიის:

- ელექტრონული საფულის გამოყენების პირობებთან;
- მომხმარებელთან დადებულ ჩარჩო-ხელშეკრულებასთან;
- AML/CFT პოლიტიკასა და პროცედურებთან;
- მომხმარებლის იდენტიფიკაციისა და ვერიფიკაციის პროცედურებთან;
- თაღლითობის მონიტორინგის პროცედურებთან;
- ინფორმაციული უსაფრთხოების შესაბამის დოკუმენტებთან;
- საჩივრების განხილვის პროცედურასთან ერთობლიობაში.

18.3. წინამდებარე დოკუმენტი არ ცვლის მომხმარებელთან გაფორმებულ ხელშეკრულებას და არ განსაზღვრავს ელექტრონული საფულის მომსახურების საფასურებს, ლიმიტებს ან სხვა კომერციულ პირობებს.

მუხლი 19. კონფიდენციალურობის პოლიტიკის ცვლილება

19.1. კომპანია უფლებამოსილია განაახლოს ან შეცვალოს წინამდებარე პოლიტიკა:

- კანონმდებლობის ცვლილების შემთხვევაში;

- მარეგულირებელი მოთხოვნების ცვლილების შემთხვევაში;
- ელექტრონული საფულის ფუნქციონალის ცვლილების შემთხვევაში;
- მონაცემთა დამუშავების პროცესების ცვლილების შემთხვევაში;
- უსაფრთხოების ან ტექნოლოგიური გარემოს ცვლილების შემთხვევაში.

19.2. განახლებული ვერსია გამოქვეყნდება კომპანიის ვებგვერდზე და/ან ელექტრონულ საფულეში.

19.3. მნიშვნელოვანი ცვლილებების შემთხვევაში კომპანია მომხმარებელს მიაწვდის შესაბამის ინფორმაციას კანონმდებლობით გათვალისწინებული წესით.

19.4. პოლიტიკის თითოეულ ვერსიას მიენიჭება შესაბამისი ვერსიის ნომერი და ძალაში შესვლის თარიღი.