

სს „ნეო ქართული ბანკი“
პერსონალურ მონაცემთა დამუშავების პოლიტიკა

სარჩევი

1.	ზოგადი დებულებები.....	2
1.1.	მიზანი და ფარგლები.....	2
1.2.	ვინ ვართ ჩვენ.....	2
1.3.	მარეგულირებელი კანონმდებლობა.....	2
1.4.	ძირითადი ტერმინები.....	3
2.	პერსონალური მონაცემების კატეგორიები.....	4
2.1.	მონაცემთა ჯგუფები.....	4
2.2.	მონაცემთა დამუშავების სხვადასხვა შემთხვევები.....	5
3.	დამუშავების მიზნები, საფუძვლები და შენახვის ვადები.....	6
3.1.	სამართლებრივი საფუძვლები.....	6
3.2.	მონაცემთა დამუშავების ცხრილი.....	7
3.3.	პირდაპირი მარკეტინგი.....	9
3.4.	ავტომატური გადაწყვეტილებების მიღება (პროფაილინგი).....	9
4.	მესამე პირებისთვის მონაცემთა გაზიარება.....	10
4.1.	გაზიარების საფუძვლები.....	10
4.2.	მიმღებების კატეგორიები.....	10
4.3.	მონაცემთა საერთაშორისო გადაცემა.....	11
5.	მონაცემთა სუბიექტის უფლებები.....	12
5.1.	უფლებების ჩამონათვალი.....	12
5.2.	უფლებების განხორციელება.....	14
6.	ციფრული არხები და მზა ჩანაწერები (Cookies).....	14
6.1.	ონლაინ ბანკი / მობაილ ბანკი.....	14
6.2.	Cookies პოლიტიკა.....	14
7.	მონაცემთა შენახვის ვადები.....	15
8.	ინფორმაციული უსაფრთხოება.....	15
9.	კომუნიკაცია და საჩივრები.....	15

1. ზოგადი დებულებები

1.1. მიზანი და ფარგლები

წინამდებარე პერსონალურ მონაცემთა დამუშავების პოლიტიკა (შემდგომ - პოლიტიკა) განსაზღვრავს ბანკის მიდგომას პერსონალური მონაცემების დამუშავებასთან დაკავშირებით. დოკუმენტი ადგენს, თუ რა სახის პერსონალურ მონაცემებს ამუშავებს ბანკი, რა მიზნებისთვის, რა საშუალებებით, რა სამართლებრივი საფუძვლებზე დაყრდნობით, რა ვადით ინახავს და ვისთან აზიარებს მათ.

პოლიტიკა ვრცელდება ბანკის ყველა, მათ შორის პოტენციურ კლიენტზე, წინა სახელშეკრულებო ურთიერთობაში მყოფ კლიენტზე, ბენეფიციარ მესაკუთრეზე, მსესხებელზე, თავდებზე, უზრუნველყოფის საგნის მესაკუთრეზე, ყველა მომხმარებელსა თუ პარტნიორზე, ნებისმიერ პირზე, რომლის მონაცემებსაც ბანკი ამუშავებს.

1.2. ვინ ვართ ჩვენ

სს [ბანკის დასახელება] წარმოადგენს საქართველოს კანონმდებლობის შესაბამისად ლიცენზირებულ კომერციულ ბანკს. წინამდებარე პოლიტიკის მიზნებისთვის ბანკი მოქმედებს, როგორც პერსონალური მონაცემების დამმუშავებელი.

ბანკის საიდენტიფიკაციო კოდი: 404785372

იურიდიული მისამართი: 138ა, დავით აღმაშენებლის გამზირი, თბილისი, საქართველო]

ვებ-საიტი: www.ngbank.ge

ელ-ფოსტა: privacy@ngbank.ge

1.3. მარეგულირებელი კანონმდებლობა

ბანკი ამუშავებს პერსონალურ მონაცემებს, მათ შორის შემდეგი ნორმატიული აქტების შესაბამისად:

- საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“;
- საქართველოს კანონი „კომერციული ბანკების საქმიანობის შესახებ“
- საქართველოს კანონი „ფულის გათეთრებისა და ტერორიზმის დაფინანსების აღკვეთის ხელშეწყობის შესახებ“
- საქართველოს კანონი „საგადახდო სისტემისა და საგადახდო მომსახურების შესახებ“
- საქართველოს ეროვნული ბანკის ნორმატიული აქტები
- ევროპის კავშირის მონაცემთა დაცვის ზოგადი რეგლამენტი (GDPR).

1.4. ძირითადი ტერმინები

პოლიტიკაში გამოყენებულ ტერმინებს აქვს შემდეგი მნიშვნელობა:

- 1.4.1. **პერსონალური 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;
- 1.4.2. **მონაცემთა სუბიექტი** - ფიზიკური პირი, რომლის შესახებ მონაცემებსაც ბანკი ამუშავებს.
- 1.4.3. **დამუშავება** - მონაცემთა მიმართ შესრულებული ნებისმიერი მოქმედება, მათ შორის, მათი შეგროვება, მოპოვება, მათზე წვდომა, მათი ფოტოგადაღება, ვიდეომონიტორინგი 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;
- 1.4.4. **განსაკუთრებული კატეგორიის მონაცემი** - 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;
- 1.4.5. **მონაცემთა დამმუშავებელი** - ბანკი, რომელიც დამოუკიდებლად განსაზღვრავს მონაცემთა დამუშავების მიზანსა და საშუალებებს.
- 1.4.6. **ბიომეტრიული მონაცემი** - ტექნიკური საშუალებების გამოყენებით დამუშავებული, მონაცემთა სუბიექტის ფიზიკურ, ფიზიოლოგიურ ან ქცევის მახასიათებელთან (როგორიცაა, მაგალითად: სახის გამოსახულება, ხმის მახასიათებელი ან დაქტილოსკოპიური მონაცემები) დაკავშირებული მონაცემი, რომელიც მისი უნიკალური იდენტიფიცირების ან ვინაობის დადასტურების შესაძლებლობას იძლევა;
- 1.4.7. **პროფაილინგი** - მონაცემთა ავტომატური დამუშავების ნებისმიერი ფორმა, რომელიც გულისხმობს მონაცემების გამოყენებას ფიზიკურ პირთან დაკავშირებული გარკვეული პიროვნული მახასიათებლების შესაფასებლად, კერძოდ, იმ მახასიათებლების ანალიზსა და პროგნოზირებას, რომლებიც შეეხება ფიზიკური პირის მიერ სამუშაოს შესრულების ხარისხს, მის ეკონომიკურ მდგომარეობას, ჯანმრთელობას, პირად ინტერესებს, სანდოობას, ქცევას, ადგილსამყოფელს ან გადაადგილებას.

2. პერსონალური მონაცემების კატეგორიები

2.1. მონაცემთა ჯგუფები

ბანკი ამუშავებს, მათ შორის შემდეგი კატეგორიის პერსონალურ მონაცემებს:

2.1.1. საიდენტიფიკაციო / დოკუმენტური მონაცემები

სახელი, გვარი, დაბადების თარიღი და ადგილი, სქესი, პირადი ნომერი, პასპორტის ნომერი, ეროვნება, მოქალაქეობა, ხელმოწერა, ფინანსური ინფორმაცია და სხვა პირადი მონაცემები. ეს მონაცემები თავდაპირველად გამოიყენება კლიენტის პირველადი იდენტიფიკაციისა და “ივნობდე შენს კლიენტს” (KYC) და “ივნობდე შენს პარტნიორს” ვალდებულებების შესასრულებლად.

2.1.2. საკონტაქტო მონაცემები

ფაქტობრივი და იურიდიული მისამართი, ტელეფონის ნომერი(ები), ელექტრონული ფოსტის მისამართი და სხვა საკონტაქტო მონაცემი. ეს მონაცემები გამოიყენება კომუნიკაციისა და შეტყობინებების გაგზავნისთვის.

2.1.3. ფინანსური მონაცემები

ინფორმაცია შემოსავლის შესახებ (ხელფასი, ქირა, ბიზნეს შემოსავალი), ყოველთვიური ხარჯები, ქონება (უძრავი, მოძრავი), ვალდებულებები, საბანკო ანგარიშების ნაშთები, საკრედიტო ისტორია, ვადაგადაცილების ჩანაწერები, ინფორმაცია სხვა ფინანსური დაწესებულებებში გახსნილი ანგარიშების შესახებ და სხვა ფინანსური ინფორმაცია.

2.1.4. ტრანზაქციული მონაცემები

ბანკის ანგარიშის ნომერი, IBAN, განხორციელებული ოპერაციების ისტორია, საბარათო ოპერაციები, ინტერნეტ/მობაილ ბანკის ოპერაციები, გადარიცხვები, გადახდები, ანგარიშსწორების ორდერები და სხვა ტრანზაქციებთან დაკავშირებული ინფორმაცია.

2.1.5. სახელშეკრულებო მონაცემები

ინფორმაცია ბანკთან გაფორმებული ყველა ხელშეკრულების შესახებ: საკრედიტო ხელშეკრულება, სადეპოზიტო ხელშეკრულება, ხელშეკრულება საბანკო პროდუქტებით მომსახურების შესახებ, ბარათის გამოყენების წესები, ინდივიდუალური პირობები, ცვლილებები და დამატებები და სხვა ნებისმიერი შეთანხმება.

2.1.6. სოცო-დემოგრაფიული მონაცემები

განათლება, პროფესია და სამუშაო ადგილი, პოლიტიკური ან საზოგადოებრივი თანამდებობა, ოჯახური მდგომარეობა, სოციალური მდგომარეობა და სხვა სოცო-დემოგრაფიული მონაცემი.

2.1.7. ციფრული / ტექნოლოგიური მონაცემები

IP მისამართი, მოწყობილობის ID, ბრაუზერის ტიპი და ვერსია, ოპერაციული სისტემა, სესიის ჟურნალი (log files), cookies, ინტერნეტ / მობაილ ბანკის გამოყენების ქცევები, გეოლოკაცია და სხვა ტექნოლოგიური მონაცემი

2.1.8. ბიომეტრიული მონაცემები (განსაკუთრებული კატეგორია)

ხმის ბიომეტრიული ნიმუში (სატელეფონო მომსახურებისთვის), ვიდეო ბანკის სესიების ჩანაწერი, სახის ამოცნობის მონაცემები (მობაილ ბანკის ავთენტიფიკაცია), ქცევის ბიომეტრია. ეს მონაცემები მუშავდება მხოლოდ კლიენტის თანხმობის საფუძველზე, კანონმდებლობით გათვალისწინებულ შემთხვევებში.

2.1.9. AML/CFT / ფინანსური დანაშაულის მონაცემები

ინფორმაცია ფინანსური ოპერაციების მონიტორინგის შედეგად გამოვლენილ ექვმიტანილ ოპერაციებზე, ტრანზაქციების ავტომატური ანალიზის შედეგები, სანქციების სიებში შემოწმების შედეგები, სტატუსის ვერიფიკაცია, საექვო ტრანზაქციების ჩანაწერები და სხვა მსგავსი ტიპის ინფორმაცია.

2.1.10. საკომუნიკაციო მონაცემები

ბანკთან ზეპირი კომუნიკაციის ჩანაწერები (ქოლ-ცენტრი, ვიდეო ბანკი), ელ-ფოსტის და SMS/MMS კორესპონდენცია, ჩათ-ბოტის სესიების ჟურნალი, საჩივრები და მათ განხილვის ჩანაწერები, კლიენტის კმაყოფილების კვლევის შედეგები და სხვა მსგავსი მონაცემი.

2.1.11. ღია წყაროს / საჯარო მონაცემები

ინფორმაცია საჯაროდ ხელმისაწვდომი წყაროებიდან, მათ შორის რეესტრებიდან, სასამართლო ჩანაწერები, სახელმწიფო სანქციების სიები და სხვა საჯაროდ ხელმისაწვდომი მონაცემი.

2.2. მონაცემთა დამუშავების სხვადასხვა შემთხვევები

2.2.1. არასრულწლოვანის მონაცემები

ბანკი არასრულწლოვანის პერსონალური მონაცემებს, მისი თანხმობის საფუძველზე, ამუშავებს თუ მან მიაღწია 16 წლის ასაკს. 16 წლამდე არასრულწლოვანის მონაცემების დამუშავება დასაშვებია მისი მშობლის ან სხვა კანონიერი წარმომადგენლის თანხმობით, გარდა კანონმდებლობით პირდაპირ გათვალისწინებული შემთხვევებისა.

არასრულწლოვანის განსაკუთრებული კატეგორიის მონაცემების დამუშავება დასაშვებია მხოლოდ მისი მშობლის ან სხვა კანონიერი წარმომადგენლის წერილობითი თანხმობის საფუძველზე, გარდა კანონმდებლობით პირდაპირ გათვალისწინებული შემთხვევებისა.

არასრულწლოვანის მონაცემების დამუშავებისას ბანკი ყველა შემთხვევაში ითვალისწინებს და იცავს არასრულწლოვანის საუკეთესო ინტერესებს. არასრულწლოვანის, მისი მშობლის ან სხვა კანონიერი წარმომადგენლის თანხმობა არ ჩაითვლება ნამდვილად, თუ მონაცემთა დამუშავება საფრთხეს უქმნის ან ზიანს აყენებს არასრულწლოვანის საუკეთესო ინტერესებს.

2.2.2. გარდაცვლილი პირის მონაცემები

ბანკი მონაცემთა სუბიექტის გარდაცვალების შემდეგ მის შესახებ პერსონალურ მონაცემებს დამუშავება ამუშავებს, მხოლოდ კანონმდებლობით განსაზღვრული მონაცემთა დამუშავების შესაბამისი საფუძვლის არსებობისას, აგრეთვე, თუ მონაცემთა დამუშავება აკრძალული არ არის მონაცემთა სუბიექტის მშობლის, შვილის, შვილიშვილის ან მეუღლის მიერ, გარდა იმ შემთხვევისა, როდესაც მონაცემთა სუბიექტმა გარდაცვალებამდე წერილობით აკრძალა მისი გარდაცვალების შემდეგ მის შესახებ მონაცემთა დამუშავება.

გარდაცვლილი პირის მონაცემების დამუშავება ასევე დასაშვებია, თუ მისი გარდაცვალებიდან გასულია 30 წელი ან მონაცემთა დამუშავება აუცილებელია მემკვიდრეობასთან დაკავშირებული უფლების განსახორციელებლად.

გარდაცვლილი პირის სახელის, გვარის, სქესის, დაბადებისა და გარდაცვალების თარიღების დამუშავება დასაშვებია ზემოაღნიშნული საფუძვლებისა და გარემოებების არსებობის მიუხედავად.

2.2.3. ბიომეტრიული მონაცემები

ბანკის მიერ ბიომეტრიული მონაცემების დამუშავება დასაშვებია მხოლოდ იმ შემთხვევაში, თუ ეს აუცილებელია ბანკის საქმიანობის განხორციელების, უსაფრთხოების, საკუთრების დაცვის, საიდუმლო ინფორმაციის გამჟღავნების თავიდან აცილების, ინფორმაციული უსაფრთხოებისა და კიბერუსაფრთხოების უზრუნველყოფის მიზნით და შესაბამისი მიზნის სხვა საშუალებით მიღწევა შეუძლებელია ან დაკავშირებულია არაპროპორციულად დიდ ძალისხმევასთან.

ბიომეტრიული მონაცემების დამუშავება ასევე დასაშვებია კანონით პირდაპირ გათვალისწინებულ სხვა შემთხვევებში და კანონმდებლობით დადგენილი წესითა და მიზნებისთვის.

2.2.4. ვიდეო მონიტორინგი

ბანკის შენობები და მომსახურების გაწევის ადგილები (მათ შორის ბანკომატი, სალარო) ექვემდებარება ვიდეო მონიტორინგს, რომლის მიზანია დანაშაულის თავიდან აცილება, მისი გამოვლენა, უსაფრთხოებისა და საკუთრების დაცვა, საიდუმლო ინფორმაციის დაცვა ან/და სხვა ლეგიტიმური ინტერესის სფეროსთვის მიკუთვნებული ამოცანების შესრულება.

3. დამუშავების მიზნები, საფუძვლები და შენახვის ვადები

3.1. სამართლებრივი საფუძვლები

ბანკი ამუშავებს პერსონალურ მონაცემებს შემდეგი სამართლებრივი საფუძვლებიდან ერთ-ერთის არსებობისას:

3.1.1. თანხმობა - კლიენტმა გამოხატა თანხმობა მონაცემთა დამუშავებაზე.

3.1.2. სახელშეკრულებო ვალდებულება - დამუშავება საჭიროა მხარეებს შორის დადებული ხელშეკრულების შესასრულებლად ან ხელშეკრულების გასაფორმებლად;

3.1.3. საკანონმდებლო ვალდებულება - დამუშავება გათვალისწინებულია კანონმდებლობით (მაგალითად, AML/CFT, სანქციების შესრულება, ანგარიშგება და სხვ.).

- 3.1.4. საჯაროობა - მონაცემი საჯაროდ ხელმისაწვდომია ან მონაცემთა სუბიექტმა იგი საჯაროდ ხელმისაწვდომი გახადა;
- 3.1.5. სასიცოცხლო ინტერესი - მონაცემთა სუბიექტის ან სხვა პირის სიცოცხლის, ჯანმრთელობის ან სხვა სასიცოცხლო ინტერესის დაცვა.
- 3.1.6. საჯარო ინტერესი - მონაცემთა დამუშავება აუცილებელია მნიშვნელოვანი საჯარო ინტერესის დასაცავად;
- 3.1.7. საჯარო ინტერესის სფერო - მონაცემთა დამუშავება აუცილებელია საქართველოს კანონმდებლობით განსაზღვრული საჯარო ინტერესის სფეროსთვის მიკუთვნებული ამოცანების შესასრულებლად, მათ შორის, დანაშაულის თავიდან აცილების, დანაშაულის გამოძიების, სისხლისსამართლებრივი დევნის, მართლმსაჯულების განხორციელების, პატიმრობისა და თავისუფლების აღკვეთის აღსრულების, არასაპატიმრო სასჯელთა აღსრულებისა და პრობაციის, ოპერატიულ-სამძებრო საქმიანობის, საზოგადოებრივი უსაფრთხოების, მართლწესრიგის დაცვის, მათ შორის, ინფორმაციული უსაფრთხოებისა და კიბერუსაფრთხოების უზრუნველყოფის, მიზნებისთვის;
- 3.1.8. ლეგიტიმური ინტერესი - მონაცემთა დამუშავება აუცილებელია ბანკის ან მესამე პირის მნიშვნელოვანი ლეგიტიმური ინტერესების დასაცავად, გარდა იმ შემთხვევისა, თუ არსებობს მონაცემთა სუბიექტის (მათ შორის, არასრულწლოვანის) უფლებების დაცვის აღმატებული ინტერესი;
- 3.1.9. მომსახურების გაწევა - მონაცემთა დამუშავება აუცილებელია მონაცემთა სუბიექტის განცხადების განსახილველად, მისთვის მომსახურების გასაწევად.

3.2. მონაცემთა დამუშავების ცხრილი

ქვემოთ მოცემული ცხრილი განსაზღვრავს დამუშავების ძირითად კატეგორიებს:

პერსონალური მონაცემების კატეგორია	დამუშავების მიზანი, მათ შორის	სამართლებრივი საფუძველი	შენახვის ვადა
საიდენტიფიკაციო / დოკუმენტური მონაცემები	კლიენტის იდენტიფიკაცია, ანგარიშის გახსნა, KYC/AML შემოწმება	3.1.1 – 3.1.3, 3.1.4-3.1.9 პუნქტებით გათვალისწინებული ერთ-ერთი საფუძველი	15 წელი ურთიერთობის დასრულებიდან
საკონტაქტო მონაცემები	კომუნიკაცია, შეტყობინებების გაგზავნა, სახელშეკრულებო ვალდებულება	3.1.1-3.1.3, 3.1.8-3.1.9 პუნქტებით გათვალისწინებული ერთ-ერთი საფუძველი	15 წელი ურთიერთობის დასრულებიდან

ფინანსური მონაცემები	სესხის გაცემის გადაწყვეტილება, გადახდისუნარიანობის შეფასება, პორტფელის მართვა	3.1.1-3.1.3, 3.1.8-3.1.9 პუნქტებით გათვალისწინებული ერთ-ერთი საფუძველი	15 წელი ხელშეკრულების დასრულებიდან
ტრანზაქციული მონაცემები	საბანკო ოპერაციების განხორციელება, გადახდების მართვა, ანგარიშგება	3.1.1-3.1.3, 3.1.8-3.1.9 პუნქტებით გათვალისწინებული ერთ-ერთი საფუძველი	15 წელი ურთიერთობის დასრულებიდან
სახელშეკრულებო მონაცემები	ხელშეკრულებების მომზადება, დადება და შესრულება	3.1.1-3.1.3, 3.1.8-3.1.9 პუნქტებით გათვალისწინებული ერთ-ერთი საფუძველი	15 წელი ურთიერთობის დასრულებიდან
სოციო-დემოგრაფიული მონაცემები	კლიენტის სეგმენტაცია, პერსონალიზებული შეთავაზება, პროდუქტის შექმნა/განვითარება	3.1.1-3.1.3, 3.1.5. 3.1.8, 3.1.9 პუნქტებით გათვალისწინებული ერთ-ერთი საფუძველი	5 წელი ურთიერთობის დასრულებიდან
ციფრული / ტექნოლოგიური მონაცემები	კიბერ-უსაფრთხოება, თაღლითობის გამოვლენა, UX გაუმჯობესება	3.1.1-3.1.3, 3.1.8-3.1.9 პუნქტებით გათვალისწინებული საფუძველი	3 წელი მონაცემთა შეგროვებიდან
ბიომეტრიული: ხმის ჩანაწერი, სახის ამოცნობა (ვიდეო ბანკი, მობაილ ბანკი)	ავთენტიფიკაცია, დისტანციური სერვისი	3.1.1, 3.1.5, 3.1.7, 3.1.8 პუნქტებით გათვალისწინებული ერთ-ერთი საფუძველი	შესაბამისი მომსახურების შეწყვეტიდან 2 წელი
AML/CFT / ფინანსური დანაშაულის მონაცემები	ფულის გათეთრების, ტერორიზმის დაფინანსების, სანქციების შეუსაბამობის პრევენცია	3.1.3 პუნქტით გათვალისწინებული საფუძველი	15 წელი ურთიერთობის დასრულებიდან
საკომუნიკაციო: ზეპირი კომუნიკაცია (ჩაწერილი), ელ-ფოსტა, წერილი	საქმიანი ჩანაწერი, საჩივრების განხილვა, დავის გადაჭრა	3.1.2, 3.1.3, - 3.1.8, 3.1.9 პუნქტებით	15 წელი ურთიერთობის დასრულებიდან

		გათვალისწინებული ერთ-ერთი საფუძველი	
--	--	--	--

3.3. პირდაპირი მარკეტინგი

ბანკი ამუშავებს კლიენტის პერსონალურ მონაცემებს პირდაპირი მარკეტინგის მიზნებისთვის მხოლოდ კლიენტის წინასწარი, ნებაყოფლობითი თანხმობის საფუძველზე. მარკეტინგული კომუნიკაცია შეიძლება განხორციელდეს SMS, ელ-ფოსტა, Push-შეტყობინება, სატელეფონო ზარი ან/და სხვა საკომუნიკაციო არხებით.

მონაცემთა სუბიექტს შეუძლია ნებისმიერ დროს გამოიხმოს გაცემული თანხმობა, მონაცემთა მარკეტინგული მიზნებისთვის დამუშავებაზე.

მონაცემთა სუბიექტი ნებისმიერ შემთხვევაში მიიღებს სავალდებულო/სახელშეკრულებო შეტყობინებებს (ტარიფების ცვლილება, ახალი პირობები, ვადის გასვლის შეხსენება), რომელიც არ არის მიჩნეული მარკეტინგულ კომუნიკაციად.

3.4. ავტომატური გადაწყვეტილებების მიღება (პროფაილინგი)

ბანკი შეიძლება იყენებდეს ავტომატიზებულ გადაწყვეტილების მიღებას, მათ შორის პროფაილინგს, შემდეგი მიზნებისთვის:

- სასესხო განაცხადების გადაწყვეტა, მაგ: კრედიტუნარიანობის ავტომატური შეფასება;
- თაღლითობის გამოვლენა, მაგ: ტრანზაქციების ავტომატური მონიტორინგი;
- AML/CFT ოპერაციების მონიტორინგი, მაგ: საექვო ოპერაციების ალგორითმული ფილტრაცია;
- კლიენტის სეგმენტაცია, მაგ: პერსონალიზებული შეთავაზებების ფორმირება;
- პერსონიფიცირებული, კონკრეტულ მომხმარებელზე მორგებული პროდუქტების შექმნა;
- პერსონიფიცირებული, კონკრეტულ მომხმარებელზე მორგებული პროდუქტების შეთავაზება.

მონაცემთა სუბიექტს უფლება აქვს: (ა) მოითხოვოს ავტომატური გადაწყვეტილების ლოგიკის და შედეგების შესახებ განმარტება; (ბ) გააპროტესტოს ავტომატური გადაწყვეტილება; (გ) მოითხოვოს ადამიანის მონაწილეობით გადაწყვეტილების გადახედვა.

მონაცემთა სუბიექტს უფლება აქვს არ დაექვემდებაროს მხოლოდ ავტომატიზებულად, მათ შორის, პროფაილინგის საფუძველზე მიღებულ გადაწყვეტილებას, რომელიც სამართლებრივ ან სხვა სახის არსებითი მნიშვნელობის მქონე შედეგს წარმოშობს, გარდა იმ შემთხვევისა, როდესაც პროფაილინგის საფუძველზე გადაწყვეტილების მიღება:

- ეფუძნება მონაცემთა სუბიექტის მიერ აშკარად გამოხატულ თანხმობას;
- აუცილებელია ხელშეკრულების დასადებად, ან უკვე არსებული ხელშეკრულების შესასრულებლად;
- გათვალისწინებულია კანონით ან კანონის საფუძველზე გამოცემული კანონქვემდებარე ნორმატიული აქტით.

ავტომატიზებული გადაწყვეტილების მიღებისას განსაკუთრებული კატეგორიის მონაცემების გამოყენება დასაშვებია მხოლოდ თუ არსებობს შემდეგი ერთ-ერთი საფუძველი

- მონაცემთა სუბიექტმა განაცხადა წერილობითი თანხმობა ერთი ან რამდენიმე კონკრეტული მიზნით განსაკუთრებული კატეგორიის მონაცემთა დამუშავებაზე;
- განსაკუთრებული კატეგორიის მონაცემთა დამუშავება საჭიროა დანაშაულის თავიდან აცილების (მათ შორის, სათანადო ანალიტიკური კვლევის), დანაშაულის გამოძიების, სისხლისსამართლებრივი დევნის, მართლმსაჯულების განხორციელების, პატიმრობისა და თავისუფლების აღკვეთის აღსრულების, არასაპატიმრო სასჯელთა აღსრულებისა და პრობაციის, დროებითი მოთავსების იზოლატორში პირის განთავსების უზრუნველყოფის, უკანონო მიგრაციის წინააღმდეგ ბრძოლის, საერთაშორისო დაცვის განხორციელების, ადმინისტრაციულ სამართალდარღვევებზე რეაგირების, სამოქალაქო და სახანძრო უსაფრთხოების უზრუნველყოფის, ოპერატიულ-სამძებრო საქმიანობის, საზოგადოებრივი უსაფრთხოების ან/და მართლწესრიგის დაცვის (მათ შორის, შესაბამისი სამართალდამცავი ორგანოს ან სასამართლოს მიერ კრიმინოლოგიური კვლევის ჩატარების) მიზნებისთვის და ამ მონაცემთა დამუშავება გათვალისწინებულია შესაბამისი კანონით ან კანონითა და მის საფუძველზე გამოცემული კანონქვემდებარე ნორმატიული აქტით;
- განსაკუთრებული კატეგორიის მონაცემთა დამუშავება აუცილებელია მნიშვნელოვანი საჯარო ინტერესის დასაცავად,

და თუ იმავდროულად არსებობს მონაცემთა სუბიექტის უფლებების, თავისუფლებებისა და ლეგიტიმური ინტერესების დაცვის სათანადო გარანტიები.

4. მესამე პირებისთვის მონაცემთა გაზიარება

4.1. გაზიარების საფუძვლები

ბანკი მონაცემთა სუბიექტის პერსონალურ მონაცემებს მესამე პირებს გაუზიარებს მხოლოდ:

- კლიენტის წინასწარი თანხმობით;
- პროდუქტების შექმნის, შეთავაზების და განვითარების მიზნით;
- მომსახურების გაწევის მიზნით;
- კანონმდებლობით გათვალისწინებულ შემთხვევებში (სასამართლო, საგამოძიებო ორგანო, საბანკო მარეგულირებელი);
- სახელშეკრულებო ვალდებულების შესრულებისთვის (მომსახურების გაწევა მოითხოვს მონაცემების გაზიარებას);
- ბანკის ლეგიტიმური ინტერესის დაცვის მიზნით (დავის გადაწყვეტა, დავალიანების მართვა და სხვა).

4.2. მიმღებების კატეგორიები

ბანკმა შესაძლოა გაუზიაროს პერსონალური მონაცემები მათ შორის, შემდეგ მიმღებ სუბიექტებს:

- საქართველოს ეროვნული ბანკი - ზედამხედველობის პროცესში, ანგარიშგების მიზნით;
- სსიპ ფინანსური მონიტორინგის სამსახური - ზედამხედველობის პროცესში, AML/CFT ანგარიშგების მიზნით;

- საქართველოს შინაგან საქმეთა სამინისტრო / პროკურატურა - კანონდებლობით განსაზღვრულ შემთხვევები;
- საქართველოს საგადასახადო ორგანოები - კანონდებლობით განსაზღვრულ შემთხვევებში, მათ შორის CRS/FATCA ვალდებულებების შესრულებისას;
- საკრედიტო საინფორმაციო ბიურო(ები) - კანონდებლობით განსაზღვრულ შემთხვევებში;
- საერთაშორისო და ლოკალური საგადახდო სისტემები (Visa, Mastercard, ადგილობრივი სისტემები) - ტრანზაქციების დამუშავების, ბარათით მომსახურების მიზნით;
- საკორესპოდენტო/შუამავალი ბანკები - საერთაშორისო გადარიცხვების განხორციელების მიზნით;
- სადაზღვევო კომპანიები - სადაზღვევო პროდუქტით მომსახურების მიზნით;
- IT/ტექნოლოგიური სერვის-პროვაიდერები (Cloud, კიბერ-უსაფრთხოება) - მომსახურების გაწევის მიზნით, ბანკის ფუნქციონირების მიზნით;
- იურიდიული, აუდიტორული, საკონსულტაციო ორგანიზაციები - პროფესიული მომსახურების მიღების მიზნით;
- ბანკის მშობელი, შვილობილი და დაკავშირებული კომპანიები - მომსახურების გაწევის მიზნით.

მონაცემები მესამე პირებს გადაეცემათ იმ გარემოებებში, რომ დაცული იქნება კანონმდებლობით დადგენილი ყველა მოთხოვნა და ამასთან, ასეთი პირები იკისრებენ მონაცემთა სათანადო წესით დამუშავების ვალდებულებას.

4.3. მონაცემთა საერთაშორისო გადაცემა

ბანკი შეიძლება გადასცემდეს პერსონალურ მონაცემებს საქართველოს გარეთ, კერძოდ:

- SWIFT ქსელით საერთაშორისო გადარიცხვების განხორციელებისას.
- EEA/UK-ში მდებარე Cloud-პროვაიდერებით სარგებლობისას.
- GDPR/UK GDPR სუბიექტებთან, FATCA/CRS ვალდებულების შესრულებისას.
- მომსახურების გაწევის მიზნით და სხვ.

ბანკის მიერ პერსონალური მონაცემების სხვა სახელმწიფოსა და საერთაშორისო ორგანიზაციისთვის გადაცემა დასაშვებია მხოლოდ “პერსონალურ მონაცემთა დაცვის შესახებ” საქართველოს კანონმდებლობით განსაზღვრული მოთხოვნების დაცვით და იმ შემთხვევაში, თუ შესაბამის სახელმწიფოში ან საერთაშორისო ორგანიზაციაში უზრუნველყოფილია მონაცემთა დაცვისა და მონაცემთა სუბიექტის უფლებების დაცვის სათანადო გარანტიები.

სათანადო გარანტიების არარსებობის შემთხვევაშიც მონაცემთა გადაცემა დასაშვებია კანონმდებლობით პირდაპირ გათვალისწინებულ შემთხვევებში, მათ შორის, თუ გადაცემა გათვალისწინებულია საქართველოს საერთაშორისო ხელშეკრულებით ან შეთანხმებით, შესაბამისი კანონმდებლობით ან ნორმატიული აქტით, მონაცემთა სუბიექტის ინფორმირებული წერილობითი თანხმობით, აუცილებელია მისი სასიცოცხლო ინტერესების დასაცავად ან მნიშვნელოვანი საჯარო ინტერესის უზრუნველსაყოფად.

მონაცემთა გადაცემა ასევე დასაშვებია, თუ ბანკი უზრუნველყოფს მონაცემთა დაცვის სათანადო გარანტიებს მონაცემთა მიმღებ შესაბამის სახელმწიფოსთან, საჯარო დაწესებულებასთან, იურიდიულ ან ფიზიკურ პირთან ან საერთაშორისო ორგანიზაციასთან დადებული ხელშეკრულებით. ასეთ

შემთხვევაში მონაცემთა გადაცემა ხორციელდება მხოლოდ სახელმწიფო აუდიტის სამსახურის შესაბამისი ნებართვის მიღების შემდეგ, ხოლო შეთანხმება უნდა შეიცავდეს სავალდებულო სამართლებრივი ძალის მქონე და შესასრულებელ პირობებს.

მონაცემთა საერთაშორისო გადაცემისას ბანკი უზრუნველყოფს მონაცემთა უსაფრთხო გადაცემისთვის აუცილებელი ორგანიზაციული და ტექნიკური ზომების მიღებას.

სხვა სახელმწიფოსა და საერთაშორისო ორგანიზაციისთვის გადაცემული მონაცემების მესამე მხარისთვის შემდგომი გადაცემა დასაშვებია მხოლოდ იმ შემთხვევაში, თუ იგი ემსახურება თავდაპირველ მიზნებს და აკმაყოფილებს კანონმდებლობით განსაზღვრულ მონაცემთა გადაცემის საფუძვლებსა და მონაცემთა დაცვის სათანადო გარანტიებს.

5. მონაცემთა სუბიექტის უფლებები

5.1. უფლებების ჩამონათვალი

საქართველოს კანონმდებლობის შესაბამისად, კლიენტს (მონაცემთა სუბიექტს) გააჩნია შემდეგი უფლებები:

უფლება	შინაარსი	გამოხმაურების ვადა
ინფორმაციის მიღება	უფლება იცოდეს, თუ რა მონაცემები მუშავდება, რა მიზნით, რა საფუძველით, მონაცემთა შეგროვების/ მოპოვების წყარო, შენახვის ვადა ან ვადის განსაზღვრის კრიტერიუმი	10 სამუშაო დღე
ინფორმაციის მიღება	უფლება იცოდეს საკუთარი უფლებები, მონაცემთა გადაცემის სამართლებრივი საფუძველი და მიზნები, აგრეთვე ინფორმაცია მონაცემთა დაცვის სათანადო გარანტიების შესახებ, თუ მონაცემები გადაეცემა სხვა სახელმწიფოს ან საერთაშორისო ორგანიზაციას;	10 სამუშაო დღე
ინფორმაციის მიღება	უფლება იცოდეს მონაცემთა მიმღების ვინაობა ან მონაცემთა მიმღებების კატეგორიები, მათ შორის, ინფორმაცია მონაცემთა გადაცემის საფუძვლისა და მიზნის თაობაზე, თუ მონაცემები მესამე პირს გადაეცემა;	10 სამუშაო დღე
ინფორმაციის მიღება	უფლება იცოდეს ავტომატიზებული დამუშავების, მათ შორის, პროფაილინგის შედეგად მიღებული გადაწყვეტილების და იმ ლოგიკის შესახებ, რომელიც გამოიყენება ამგვარი	10 სამუშაო დღე

	გადაწყვეტილების მისაღებად, აგრეთვე მონაცემთა დამუშავებაზე მისი გავლენისა და დამუშავების მოსალოდნელი/სავარაუდო შედეგის თაობაზე.	
წვდომა მონაცემებზე	მონაცემების გაცნობა, უსასყიდლოდ ასლის მიღება ელექტრონული ან წერილობითი ფორმით	10 სამუშაო დღე
გასწორება, განახლება, შევსება	მცდარი, არაზუსტი, არასრული მონაცემების გასწორების, განახლების, შევსების მოთხოვნა.	10 სამუშაო დღე
დამუშავების შეწყვეტა, წაშლა, განადგურება	მონაცემების დამუშავების შეწყვეტის, წაშლის, განადგურების მოთხოვნა	10 სამუშაო დღე
მონაცემთა ხელმისაწვდომობის შეზღუდვა	მონაცემთა საჯაროდ ხელმისაწვდომი ფორმით დამუშავების შემთხვევაში მონაცემთა ხელმისაწვდომობის შეზღუდვა ან/და მონაცემთა ასლების ან მონაცემებთან დამაკავშირებელი ინტერნეტბმულის წაშლა.	10 სამუშაო დღე
მონაცემთა დაბლოკვის უფლება	სადაოა სიზუსტე, ნამდვილობა, აღარ არის საჭირო დამუშავება, დამუშავება უკანონოა, მიმდინარეობს განხილვა, არსებობს მტკიცებულებად შენახვის აუცილებლობა	3 სამუშაო დღე
მონაცემთა გადატანის უფლება	მანქანით წასაკითხი ფორმით მონაცემების გადაცემა (სადაც ეს ტექნიკურად განხორციელებადია).	10 სამუშაო დღე
თანხმობის გამოთხოვა (მარკეტინგი)	პირდაპირი მარკეტინგის მიზნით დამუშავებაზე უარის თქმა	7 სამუშაო დღე (მარკეტინგი)
გაცემული თანხმობის გამოხმობა	თანხმობის საფუძველზე მონაცემთა დამუშავების შეწყვეტის მოთხოვნა, ნებისმიერ დროს, ყოველგვარი განმარტების გარეშე.	10 სამუშაო დღე
ავტომატური გადაწყვეტილების გაპროტესტება	ადამიანის ჩარევით ავტომატიზებული გადაწყვეტილების გადახედვის მოთხოვნა.	10 სამუშაო დღე

ინფორმაციის მიღების, მონაცემებზე წვდომის, მონაცემთა გაცნობის, ან/და ასლის მიღებისთვის განსაზღვრული 10 დღიანი ვადა შესაძლოა გაგრძელდეს განსაკუთრებულ შემთხვევებში და სათანადო დასაბუთებით არაუმეტეს 10 სამუშაო დღით, რის შესახებაც მონაცემთა სუბიექტს ეცნობება დაუყოვნებლივ.

მონაცემთა სუბიექტს უფლება აქვს, ნებისმიერ დროს, ყოველგვარი განმარტების ან დასაბუთების გარეშე გამოიხმოს მის მიერ გაცემული თანხმობა. ბანკი უზრუნველყოფს მონაცემთა სუბიექტის მოთხოვნის შესრულებას კანონმდებლობის ფარგლებში და იმ შემთხვევაში, თუ არ არსებობს მონაცემთა დამუშავების სხვა საფუძველი გარდა თანხმობისა. თანხმობის გაუქმება არ ახდენს გავლენას სხვა სამართლებრივი საფუძვლებით მონაცემთა დამუშავების უფლებაზე.

5.2. უფლებების განხორციელება

უფლებების განსახორციელებლად მონაცემთა სუბიექტს შეუძლია:

- ეწვიოს ბანკის ნებისმიერ ფილიალს;
- გაგზავნოს განცხადება ელ-ფოსტაზე: privacy@ngbank.ge
- გამოიყენოს ონლაინ ბანკი ან მობაილ ბანკი;
- დაუკავშირდეს ბანკის ქოლ-ცენტრს

ბანკი უზრუნველყოფს მონაცემთა სუბიექტის მიერ დაფიქსირებული საკითხის განხილვასა და გადაწყვეტას, არაუგვიანეს კანონმდებლობით განსაზღვრულ ვადებში

კლიენტს ასევე შეუძლია საჩივრით მიმართოს საქართველოს პერსონალურ მონაცემთა დაცვის სამსახურს - <https://pdp.sao.ge/ka>

6. ციფრული არხები და მზა ჩანაწერები (Cookies)

6.1. ონლაინ ბანკი / მობაილ ბანკი

ბანკის ელექტრონული პლატფორმებით სარგებლობისას (ინტერნეტ/მობაილ ბანკი) შეიძლება დამუშავდეს:

- მოწყობილობის ID, მოდელი, ბრენდი, სახელი, OS ვერსია და აპლიკაციის ვერსია.
- სესიის ხანგრძლივობა, გვერდების ნავიგაცია, ოპერაციების ჟურნალი.
- IP მისამართი, გეოლოკაცია
- ტელეფონის კონტაქტების სია;
- სხვა მონაცემები მომსახურების გაწევის და უსაფრთხოების უზრუნველყოფის მიზნით.

იმ შემთხვევაში, თუ მონაცემთა სუბიექტი იყენებს ფოტოსურათს დიჯიტალ არხებში, ფოტოსურათი ხილვადი იქნება გადარიცხვების ფუნქციონალით სარგებლობისას, მესამე პირებისთვის.

6.2. Cookies პოლიტიკა

ბანკის ვებ-გვერდი იყენებს ე.წ. "მზა ჩანაწერებს" (Cookies) შემდეგი კატეგორიებით:

- სავალდებულო (Essential) Cookies - საიტის ფუნქციონირებისთვის, თანხმობას არ საჭიროებს.

- ფუნქციური (Functional) Cookies - სამომხმარებლო გამოცდილების გაუმჯობესებისთვის;
- ანალიტიკური (Analytics) Cookies - ვიზიტორების ქცევის ანონიმური ანალიზის, ვებ-საიტის გაუმჯობესებისთვის.
- მარკეტინგული (Marketing) Cookies - პერსონალიზებული რეკლამისთვის.

კლიენტს შეუძლია მართოს Cookie პარამეტრები ბანკის ვებ-საიტზე გამოჩენილი Cookie Banner-ის მეშვეობით. Cookies-ის სრული პოლიტიკა ხელმისაწვდომია ბანკის ვებ-გვერდზე.

7. მონაცემთა შენახვის ვადები

ბანკი ინახავს პერსონალურ მონაცემებს იმ ვადის განმავლობაში, რაც სულ მცირე განსაზღვრულია კანონმდებლობით ან/და არსებობს კონკრეტული საფუძველი მონაცემთა შენახვის. მონაცემთა შენახვის ვადების შესახებ ძირითადი ინფორმაცია მოცემულია წინამდებარე პოლიტიკაში, იმ შემთხვევაში, თუ პოლიტიკა არ ფარავს ინფორმაციას ყველა ტიპის მონაცემის შენახვის ვადის თაობაზე, მონაცემთა სუბიექტმა უნდა მიმართოს ბანკის პერსონალურ მონაცემთა დაცვის ოფიცერს.

8. ინფორმაციული უსაფრთხოება

მომხმარებელთა პერსონალური მონაცემების დაცვის მიზნით, ბანკს დანერგილი აქვს ინფორმაციული უსაფრთხოების საუკეთესო სტანდარტები და სისტემები. ბანკი, რისკზე დაფუძნებული მიდგომით, მათ შორის იყენებს:

- როლებზე დაფუძნებულ წვდომასა და მინიმალური პრივილეგიის პრინციპს;
- მომხმარებელთა და თანამშრომელთა უფლებამოსილებები მართვის პრინციპს;
- ძლიერ ავთენტიფიკაციას;
- მონაცემთა დაცვას შენახვისა და გადამცემისას, მათ შორის შესაბამის შემთხვევებში დაშიფვრას;
- მოქმედებების აღრიცხვას, უსაფრთხოების ჟურნალებსა და მონიტორინგს;
- ქსელური, სისტემური და საბოლოო მოწყობილობების დაცვის ზომებს;
- უსაფრთხო კონფიგურაციას, განახლებებსა და მოწყვლადობების მართვას;
- სარეზერვო ასლებს, აღდგენისა და უწყვეტობის მექანიზმებს;
- ფიზიკური დოკუმენტებისა და მატარებლების დაცულ შენახვისა და განადგურების წესებს;
- თანამშრომელთა კონფიდენციალურობის ვალდებულებებსა და რეგულარულ ცნობიერების ამაღლებას;
- უსაფრთხოების ზომების პერიოდულ შეფასებას, ტესტირებასა და გაუმჯობესებას.

9. კომუნიკაცია და საჩივრები

ბანკს ჰყავს პერსონალურ მონაცემთა დაცვის ოფიცერი (DPO)

მონაცემთა დაცვასთან დაკავშირებულ ნებისმიერ საკითხზე კლიენტს შეუძლია მიმართოს ბანკის DPO-ს:

სახელი გვარი: მარიამ მაისურაძე,

ელ-ფოსტა: privacy@ngbank.ge

მისამართი: 138ა, აღმაშენებლის გამზირი, თბილისი, საქართველო

ზედამხედველობის ორგანო

კლიენტს ასევე შეუძლია საჩივრით მიმართოს:

საქართველოს სახელმწიფო აუდიტის სამსახური

მისამართი: 0105 თბილისი, ნ. ვაჩნაძის ქ. №7

ვებ-საიტი: <https://pdp.sao.ge/ka>

ელ-ფოსტა: sao@sao.ge