პერსონალურ მონაცემთა დამუშავების პირობები

1. შესავალი

1.1. წინამდებარე დოკუმენტის მიზანია, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 36-ე მუხლის მოთხოვნების შესაბამისად, **დამუშავებისთვის პასუხისმგებელ პირსა** და **დამუშავებაზე უფლებამოსილ პირს** შორის წერილობით განისაზღვროს **პერსონალურ მონაცემთა** დამუშავების წესები და პირობები;

1.2. სს გაერთიანებული საფინანსო კორპორაცია (ს.ნ. 202175546), როგორც „საგადახდო სისტემისა და საგადახდო მომსახურების შესახებ“ საქართველოს კანონით გათვალისწინებული **საგადახდო სისტემის ოპერატორი**, იმ სახელშეკრულებო ურთიერთობებში, სადაც ის წარმოადგენს პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონით გათვალისწინებულ **დამუშავებაზე უფლებამოსილ პირს** (შემდგომში - **„სისტემის ოპერატორი**“ ან/და **დამუშავებაზე უფლებამოსილი პირი“**) მასზე გადაცემულ **პერსონალურ მონაცემებს** დაამუშავებს საქართველოს კანონმდებლობითა და წინამდებარე დოკუმენტით დადგენილი პირობების შესაბამისად.

2. ტერმინთა განმარტება

2.1. **დამუშავებაზე უფლებამოსილი პირი** – სისტემის ოპერატორი ან/და სს გაერთიანებული საფინანსო კორპორაცია;

2.2. **დამუშავებისთვის პასუხისმგებელი პირი** – კონტრაჰენტი;

2.3. **მხარე** - **დამუშავებისთვის პასუხისმგებელი პირი** ან **დამუშავებაზე უფლებამოსილი პირი** კონტექსტის შესაბამისად;

2.4. **მხარეები** - **დამუშავებისთვის პასუხისმგებელი პირი** და **დამუშავებისთვის უფლებამოსილი პირი** ერთად;

2.5. **პერსონალური მონაცემი (შემდგომ – 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;

2.6. **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;

2.7. **მონაცემთა 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;

2.8. **მონაცემთა სუბიექტი** – ნებისმიერი ფიზიკური პირი, რომლის შესახებ **მონაცემიც** მუშავდება;

2.9. **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;

2.10. **ხელშეკრულება** - მხარეთა შორის **სისტემის ოპერატორის** მომსახურების თაობაზე გაფორმებული ხელშეკრულება, რომლის ფარგლებშიც, სისტემის ოპერატორი წარმოადგენს პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონით გათვალისწინებულ **დამუშავებაზე უფლებამოსილ პირს**;

2.11. **ქვეკონტრაქტორი** - მესამე პირი, რომელიც **დამუშავებაზე უფლებამოსილი პირის** სახელით ან მის მიერ განსაზღვრული მიზნებით ახორციელებს **ხელშეკრულების** საფუძველზე, **დამუშავებისთვის პასუხისმგებელი პირისგან** მიღებულ **მონაცემთა დამუშავებას**;

2.12. **კანონი** - პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონი.

3. მონაცემთა დამუშავების მიზანი და საფუძველი

3.1. **პერსონალურ მონაცემთა დამუშავება** ხდება **მხარეთა** შორის გაფორმებული **ხელშეკრულებით** გათვალისწინებული მომსახურების გაწევის მიზნით. დაუშვებელია **ხელშეკრულებითა** და წინამდებარე დოკუმენტით განსაზღვრული მიზნებისგან განსხვავებული მიზნით **მონაცემთა** შემდგომი დამუშავება.

3.2. **მონაცემთა დამუშავების** საფუძვლებია **კანონის** მე-5 მუხლის 1-ლი პუნქტის შემდეგი ქვეპუნქტები:

3.2.1. (ბ) **მონაცემთა დამუშავება** აუცილებელია **მონაცემთა სუბიექტთან** დადებული გარიგებით ნაკისრი ვალდებულების შესასრულებლად ან **მონაცემთა სუბიექტის** მოთხოვნით გარიგების დასადებად;

3.2.2. (გ) **მონაცემთა დამუშავება** გათვალისწინებულია კანონმდებლობით;

3.2.3. (დ) **მონაცემთა დამუშავება** საჭიროა **დამუშავებისთვის პასუხისმგებელი პირის** მიერ საქართველოს კანონმდებლობით მისთვის დაკისრებული მოვალეობების შესასრულებლად;

3.2.4. (ი) **მონაცემთა დამუშავება** აუცილებელია **დამუშავებისთვის პასუხისმგებელი პირის** ან მესამე პირის მნიშვნელოვანი ლეგიტიმური ინტერესების დასაცავად, გარდა იმ შემთხვევისა, თუ არსებობს **მონაცემთა სუბიექტის** (მათ შორის, არასრულწლოვანის) უფლებების დაცვის აღმატებული ინტერესი.

3.3. **სისტემის ოპერატორს** არ გადაეცემა **განსაკუთრებული კატეგორიის მონაცემები**, შესაბამისად **ხელშეკრულების** ფარგლებში არ ხდება **განსაკუთრებული კატეგორიის მონაცემის დამუშავება**.

4. მხარეთა უფლებები და ვალდებულებები

4.1. **მხარეები** ვალდებული არიან, მიიღონ **მონაცემთა დამუშავების** შესაძლო და თანამდევი საფრთხეების შესაბამისი ორგანიზაციული და ტექნიკური ზომები, რომლებიც უზრუნველყოფს **მონაცემთა** დაცვას **მონაცემთა** დაკარგვისგან, უკანონო დამუშავებისგან, მათ შორის, განადგურებისგან, წაშლისგან, შეცვლისგან, გამჟღავნებისგან ან გამოყენებისგან;

4.2. **დამუშავებისთვის პასუხისმგებელი პირი** ვალდებულია:

4.2.1. უზრუნველყოს **კანონით** გათვალისწინებული პრინციპებისა და მოთხოვნების დაცვა, მათ შორის, **მონაცემთა სუბიექტის** ინფორმირება მის შესახებ დამუშავებული **მონაცემების** თაობაზე, საჭიროების შემთხვევაში, უზრუნველყოს შესაბამისი თანხმობის მოპოვება;

4.2.2. **სისტემის ოპერატორს** მიაწოდოს სწორი **მონაცემები**, არ გადასცეს ისეთი **მონაცემები**, რომლებიც დამუშავებულია **კანონით** განსაზღვრული წესების დარღვევით. თავის მხრივ, **სისტემის ოპერატორი** ვალდებულია, სწორად აღრიცხოს მიღებული **მონაცემები**. ყოველგვარი პასუხისმგებლობა ზიანზე, რაც გამოწვეულია **კონტრაჰენტის** მიერ **მონაცემების** არაკანონიერად, **კანონით** დადგენილი პრინციპებისა და მოთხოვნების დაცვის გარეშე დამუშავებით, ეკისრება **დამუშავებისთვის პასუხისმგებელ პირს**;

4.2.3. **სისტემის ოპერატორს** გადასცეს მხოლოდ ის **მონაცემები**, რაც აუცილებელია **ხელშეკრულებით** გათვალისწინებული მომსახურების სრულად და ჯეროვნად შესრულებისთვის;

4.2.4. **სისტემის ოპერატორს** დაუყოვნებლივ, არაუგვიანეს ასეთი შემთხვევის დადგომიდან 48 (ორმოცდარვა) საათისა, აცნობოს ისეთი **ინციდენტის** შესახებ, რომელმაც შესაძლებელია გავლენა მოახდინოს **დამუშავებაზე უფლებამოსილი პირის** მიერ **ხელშეკრულებით** ნაკისრი ვალდებულებების შესრულებაზე;

4.2.5. გაუმართლებელი დაყოვნების გარეშე, დროულად უპასუხოს **დამუშავებაზე ფლებამოსილი პირის** მიერ წინამდებარე დოკუმენტიდან გამომდინარე წერილობით შეტყობინებებს.

4.3. **დამუშავებისთვის პასუხისმგებელი პირი** უფლებამოსილია:

4.3.1. მოსთხოვოს **სისტემის ოპერატორს** წინამდებარე დოკუმენტით დადგენილი პირობების შესრულება;

4.3.2. გონივრული ეჭვის არსებობისას, შეამოწმოს **დამუშავებაზე უფლებამოსილი პირისთვის** გადაცემული პერსონალური **მონაცემების დამუშავების** პროცესში გამოყენებული საშუალებებისა და სისტემების გამართულობა. ასევე, მათი ტექნიკური და ორგანიზაციული მახასიათებლების შესაბამისობა წინამდებარე დოკუმენტით დადგენილ უსაფრთხოების მოთხოვნებთან;

4.3.3. ჰქონდეს პირდაპირი კომუნიკაცია **დამუშავებაზე უფლებამოსილ პირთან** და მისცეს მას წერილობითი მითითებები **მონაცემების დამუშავების** პროცესთან დაკავშირებით.

4.4. **დამუშავებაზე უფლებამოსილი პირი** აცხადებს და გარანტიას იძლევა, რომ:

4.4.1. იმოქმედებს **მონაცემთა** დაცვის კანონმდებლობის შესაბამისად და უზრუნველყოფს **მონაცემთა სუბიექტების** უფლებების დაცვას;

4.4.2. შეზღუდავს **პერსონალურ მონაცემებთან** წვდომის უფლების მქონე პირთა წრეს და ასეთ უფლებას მიანიჭებს მხოლოდ იმ პირებს, რომელთაც წინასწარ აქვთ მიცემული შესაბამისი ინსტრუქციები **მონაცემთა** დაცვასთან მიმართებით და რომლებიც უშუალოდ საჭიროებენ **მონაცემებზე** წვდომას, გააზრებული აქვთ **მონაცემთა** კონფიდენციალურობის/უსაფრთხოების დაცვის ვალდებულება და უზრუნველყოფენ **მონაცემთა** საიდუმლოების დაცვას, მათ შორის, სამსახურებრივი უფლებამოსილების შეწყვეტის შემთხვევაში;

4.4.3. შეინახავს ჩანაწერებს მის მიერ **მონაცემებთან** მიმართებით წარმართული პროცესების თაობაზე;

4.4.4. **მონაცემთა სუბიექტის** მიერ, **მონაცემთა** წვდომის მოთხოვნასთან დაკავშირებით, იმუშავებს **კონტრაჰენტთან** ერთად, საკითხის გადასაწყვეტად;

4.4.5. პერსონალურ **მონაცემთა** არაავტორიზებული დამუშავების (მათ შორის შემთხვევითი ან უნებართვო გავრცელება, წვდომა, შეცვლა და განადგურება) აღსაკვეთად გაატარებს შესაბამის ტექნიკურ და ორგანიზაციულ ზომებს;

4.4.6. შეზღუდავს **პერსონალურ მონაცემებთან** წვდომის უფლების მქონე პირთა წრეს და ასეთ უფლებას მიანიჭებს მხოლოდ იმ პირებს, რომლებიც უშუალოდ საჭიროებენ **მონაცემებზე** წვდომას და რომელთაც ნაკისრი აქვთ **მონაცემთა** კონფიდენციალურობისა და უსაფრთხოების დაცვის ვალდებულება;

4.4.7. **პერსონალურ მონაცემებზე** შემთხვევითი ან უნებართვო წვდომის, ასეთი **მონაცემების** განადგურების, დაკარგვის, შეცვლის ან გასაჯაროვების შემთხვევაში, (**ინციდენტ**ი), დაუყოვნებლივ, თუმცა არაუგვიანეს ასეთი შემთხვევის დადგომიდან 48 (ორმოცდარვა) საათისა, შეატყობინებს მეორე მხარეს შემთხვევის შესახებ **ინციდენტის** გარემოებების, სახისა და დროის, ბუნებისა და გამჟღავნებული/მოპოვებული/დაზიანებული/წაშლილი/განადგურებული/დაკარგული/შეცვლილი პერსონალური **მონაცემების** მითითებით. ასევე, ასეთის შესაძლებლობის შემთხვევაში, მიაწოდებს ინფორმაციას **კონტრაჰენტს მონაცემთა** კატეგორიისა და ზუსტი ოდენობის თაობაზე და თუ რა ფორმით მოხდა პერსონალური **მონაცემების** მთლიანობის დარღვევა (**მონაცემების** სავარაუდო კატეგორიებისა და რაოდენობის, აგრეთვე იმ **მონაცემთა სუბიექტების** სავარაუდო კატეგორიებისა და რაოდენობის შესახებ, რომლებსაც **ინციდენტის** შედეგად შეექმნათ საფრთხე). შეტყობინება დამატებით უნდა შეიცავდეს პერსონალურ **მონაცემთა** დაცვაზე პასუხისმგებელი პირის საკონტაქტო **მონაცემს** და ინფორმაციას იმ საშუალების თაობაზე, რომლის მეშვეობითაც შესაძლებელია დამატებითი ცნობის მიღება. ამასთან, **კონტრაჰენტს** მიეწოდება ინფორმაცია იმის თაობაზე, მიმართა თუ არა **სისტემის ოპერატორმა** პერსონალური **მონაცემების** დაცვის ინსპექტორს **ინციდენტის** შესახებ, რა დროსაც ***კონტრაჰენტი*** უფლებამოსილია **სისტემის ოპერატორს** მოსთხოვოს, ხოლო **სისტემის ოპერატორი** უფლებამოსილია **კონტრაჰენტს** მიაწოდოს ის ნებისმიერი დამატებითი ინფორმაცია, რომელიც დაკავშირებულია **ინციდენტის** შესახებ პერსონალური **მონაცემების** დაცვის სამსახურთან კომუნიკაციასთან. **კონტრაჰენტს** ასევე მიეწოდება ინფორმაცია **ინციდენტით** გამოწვეული სავარაუდო ზიანის, მისი შემცირების ან აღმოფხვრის მიზნით **დამუშავებისთვის პასუხისმგებელი პირის** მიერ განხორციელებული ან დაგეგმილი ღონისძიებების შესახებ, ასევე, იმის შესახებ, კანონმდებლობით დადგენილი წესის შესაბამისად, იგეგმება თუ არა, **მონაცემთა სუბიექტისთვის** შესაბამისი შეტყობინების გაგზავნა;

4.4.8. დაუყოვნებლივ მიიღებს შესაბამის ზომებს **ინციდენტზე** დროული რეაგირებისა და მისი გამომწვევი მიზეზების აღმოფხვრისთვის და გატარებული ზომების შესახებ აცნობებს მეორე მხარეს;

4.4.9. არ გადასცემს **პერსონალურ მონაცემებს** საქართველოს ფარგლებს გარეთ, ხოლო იმ შემთხვევაში თუ **სისტემის ოპერატორის** საქმიანობა მოითხოვს **პერსონალური მონაცემების** საქართველოს ფარგლებს გარეთ გადაცემას, დაუყოვნებლივ შეატყობინებს ამის თაობაზე **კონტრაჰენტს**. ამასთან, ნებისმიერ შემთხვევაში მესამე პირისთვის **მონაცემთა** გადაცემა დასაშვებია, მხოლოდ იმ რწმუნებით, რომ **მონაცემი** გადაიცემა ისეთ ქვეყნებში, რომელიც საქართველოს კანონმდებლობით და GDPR რეგულაციების მოთხოვნის შესაბამისად, წარმოადგენს ე.წ. თეთრი სიის (Whitelist) ქვეყანას.

4.4.10. მხოლოდ განსაზღვრულ შემთხვევებში და **კონტრაჰენტის** წინასწარი წერილობითი თანხმობის შესაბამისად, **პერსონალური მონაცემების დამუშავების** პროცესში ჩართავს **ქვეკონტრაქტორებს,** რომლებსაც სათანადოდ ექნებათ დანერგილი შესაბამისი უსაფრთოხების მექანიზმები და რომლებზეც ყოველგვარი შეზღუდვის გარეშე გავრცელდება წინამდებარე შეთანხმებით განსაზღვრული პირობები. **მონაცემთა დამუშავების** პროცესში **ქვეკონტრაქტორის** ჩართვა არ ათავისუფლებს **სისტემის ოპერატორს** ნაკისრი ვალდებულებებისაგან.

5. მონაცემების დამუშავების შეწყვეტა და განადგურება

5.1. **სისტემის ოპერატორი** მისთვის გადაცემულ **პერსონალურ მონაცემებს** ამუშავებს **ხელშეკრულების** მოქმედების ვადის განმავლობაში და ინახავს **ხელშეკრულების** მოქმედების ან/და კანონმდებლობით დადგენილი ვადით. **პერსონალური მონაცემების დამუშავება** და შენახვა შეიძლება შეწყდეს კანონმდებლობით ან/და ამ შეთანხმებით გათვალისწინებული პირობების შესაბამისად.

5.2. იმ შემთხვევაში, თუ **მონაცემთა სუბიექტი** მოითხოვს **მონაცემთა დამუშავების** შეწყვეტას, კანონმდებლობით გათვალისწინებული სხვა უფლებების რეალიზებას (თანხმობის გამოხმობა, **მონაცემთა** გაცნობა და ასლის მიღება, გასწორება, განახლება, დამატება, შევსება, დაბლოკვა, **მონაცემთა დამუშავების** შეწყვეტა, წაშლა, გადატანა, განადგურება და სხვა) ან/და ინფორმაციას **მონაცემთა დამუშავების** თაობაზე, **სისტემის ოპერატორი** დაუყოვნებლივ, მაგრამ არაუგვიანეს მეორე სამუშაო დღეს, შეატყობინებს **კონტრაჰენტს** და დაელოდება **კონტრაჰენტის** მითითებას.

5.3. **სისტემის ოპერატორის** მიერ საქმიანობის შეწყვეტის ან/და **ხელშეკრულების** შეწყვეტის შემთხვევაში, **სისტემის ოპერატორი** დაუყოვნებლივ დაუბრუნებს **კონტრაჰენტს** და აღდგენის შესაძლებლობის გარეშე წაშლის/გაანადგურებს მისთვის გადაცემულ **პერსონალურ მონაცემებს** და მათ ასლებს. **კონტრაჰენტი** უფლებამოსილია, **სისტემის ოპერატორს** მოსთხოვოს **მონაცემთა** წაშლის დადასტურება. წინამდებარე მუხლი არ ვრცელდება ისეთ ინფორმაციაზე, რომლის შენახვის უფლებას/ვალდებულებას **სისტემის ოპერატორს** მოქმედი კანონმდებლობა ანიჭებს/უდგენს.

5.4. პერსონალურ **მონაცემთა დამუშავებასთან** დაკავშირებული ვალდებულებები ძალაში რჩება **მხარეთა** შორის სახელშეკრულებო ურთიერთობის შეწყვეტის შემდეგაც იმ ვადით, რა ვადითაც **მხარე** ინარჩუნებს წვდომას მეორე მხარის მიერ მისთვის გადაცემულ **პერსონალურ მონაცემებზე**. წინამდებარე დათქმა არ უნდა იქნას მიჩნეული **სისტემის ოპერატორის** უფლებად, შეინარჩუნოს წვდომა **ხელშეკრულების** საფუძველზე მიღებულ **პერსონალურ მონაცემებზე** სახელშეკრულებო ურთიერთობის დასრულების შემდეგ. **სისტემის ოპერატორი** ვალდებულია, სახელშეკრულებო ურთიერთობის დასრულებიდან გონივრულ ვადაში, მაგრამ არაუგვიანეს 30 დღისა დააბრუნოს და აღდგენის შესაძლებლობის გარეშე წაშალოს/გაანადგუროს მისთვის **კონტრაჰენტის** მიერ გადაცემული **პერსონალური მონაცემები** და მათი ასლები, გარდა წინამდებარე შეთანხმებით ან **ხელშეკრულებით** პირდაპირ გათვალისწინებული შემთხვევებისა. ამ პუნქტით გათვალისწინებული წაშლის ვალდებულება, არ ვრცელდება ისეთ ინფორმაციაზე, რომლის შენახვის ვალდებულება დადგენილია მოქმედი კანონმდებლობით ან **სისტემის ოპერატორს** გააჩნია **მონაცემთა დამუშავების** სხვა საფუძველი.

6. ინფორმაციული სისტემების უსაფრთხოება

6.1. **მონაცემთა** უსაფრთხოების დაცვის მიზნით, **სისტემის ოპერატორს** მიღებული აქვს შემდეგი ორგანიზაციული და ტექნიკური ზომები:

6.1.1. ორგანიზაცია ფლობს საერთაშორისოდ აღიარებულ უსაფრთხოების სერტიფიკატებს, როგორიც არის PCI DSS, PCI PIN, PCI 3 DS, ISO27001, ISO22301 და რეგულარულად გადის დამოუკიდებელ აუდიტს, რათა შეინარჩუნოს ნდობისა და გამჭირვალობის მაღალი დონე;

6.1.2. აღნიშნული სერტიფიკატები ადასტურებს, რომ **სისტემის ოპერატორის** ინფრასტრუქტურა, **მონაცემთა დამუშავებისა** და გადაცემის პროცესები დანერგილია უსაფრთხოების მაღალი სტანდარტების (საერთაშორისო დონეზე აღიარებული სტანდარტების) დაცვით;

6.1.3. **სისტემის ოპერატორის** უსაფრთხოების სისტემა დაფუძნებულია მრავალდონიან დაცვის მექანიზმებზე, მათ შორის **მონაცემთა** შიფრაციაზე, წვდომის მკაცრ კონტროლზე და უწყვეტ

მონიტორინგზე, რაც უზრუნველყოფს მომხმარებელთა **მონაცემების** კონფიდენციალურობისა და ოპერაციების სრულ დაცვას;

6.1.4. პერსონალური **მონაცემების** შესანახად და დასამუშავებლად არსებობს იზოლირებული გარემო, რომელიც ძირითადი ინფრასტრუქტურისგან გამოყოფილია დამოუკიდებელი Firewall-ით და გარემოს Firewall-ზე წვდომების დაშვება, კონტროლდება შესაბამისი უფლებამოსილი პირების მიერ. იზოლირებულ გარემოში მოთავსებულ ინფორმაციასთან წვდომა ხორციელდება ე.წ. ტერმინალ სერვერების (Jump Server) საშუალებით.

6.1.5. **სისტემის ოპერატორი** უზრუნველყოფს გარემოს მთლიანობის/წვდომადობის მონიტორინგს. გარემოში მოთავსებულ სერვერებზე ხორციელდება განახლებების მონიტორინგი;

6.1.6. სადაც შესაძლებელია **პერსონალური მონაცემები** ინახება დაშიფრული სახით ძლიერი შიფრაციის ალგორითმების გამოყენებით;

6.1.7. იზოლირებულ გარემოსთან წვდომა ხდება დაცული მეთოდით, დაშიფრული კომუნიკაციით და უსაფრთხო პროტოკოლის გამოყენებით;

6.1.8. იზოლირებული გარემოსთვის არსებობს პაროლების პოლიტიკა, რომელიც განსაზღვრავს პაროლის სირთულეს, ცვლილების დროს და ისტორიას;

6.1.9. იზოლირებულ გარემოს სერვერებზე ადმინ მომხმარებლების პაროლები დანაწევრებულია მინიმუმ ორ ნაწილად და ინახება სხვადასხვა მფლობელთან, უსაფრთხო მეთოდის გამოყენებით;

6.1.10. იზოლირებულ გარემოს სერვერებზე წვდომები იმართება privileged access management system (PAM) - ით;

6.1.11. გარემოზე წვდომის დაშვებისას ხორციელდება მომხმარებლის ორ ნაბიჯიანი ავთენტიფიკაცია (ე.წ. Two Step Authentication);

6.1.12. იზოლირებული გარემო არ არის ინტერნეტიდან წვდომადი, იზოლირებულ გარემოს სერვერებზე ხორციელდება ლოგირება, ლოგი ინახება ცენტრალიზებულად და საჭიროების შემთხვევაში, შესაძლებელია მოხდეს მისი გამოყენება **ინციდენტის** ან ხარვეზის გამოკვლევის პროცესში;

6.1.13. პერსონალური **მონაცემების** შესანახად დასამუშავებლად ან გადასაცემად არ გამოიყენება ღრუბლოვანი გარემო (Remote storage, Cloud Service);

6.1.14. სისტემის ოპერატორი უზრუნველყოფს, რომ დეველოპმენტის ან ტესტირების ფარგლებში პერსონალური **მონაცემების** გამოყენებისას, ხდებოდეს ინფორმაციის ცვლილება ისეთი სახით, რომ ვერ ხდებოდეს პიროვნების პირდაპირი ან ირიბი იდენტიფიცირება;

6.1.15. ხანდაზმულობით ან სპეციალური მოთხოვნით ინფორმაციის განადგურებისას გამოიყენება შრედერი ან ცეცხლი.

7. მხარეების პასუხისმგებლობა

7.1. **მხარეები** იღებენ ვალდებულებას აუნაზღაურონ ერთმანეთს მათ მიერ წინამდებარე დოკუმენტით დადგენილი პირობების სრულად ან ნაწილობრივ შეუსრულებლობის ან არაჯეროვნად შესრულების შედეგად მიყენებული ზიანი, კანონმდებლობითა და **ხელშეკრულებით** დადგენილი წესით. ზიანის ანაზღაურება **მხარეებს** არ ათავისუფლებს შეთანხმებით ნაკისრი ვალდებულებების შესრულებისაგან;

7.2. **სისტემის ოპერატორის** პასუხისმგებლობა შემოიფარგლება პირდაპირი, რეალური ზიანით, რომელიც მიადგა **კონტრაჰენტს სისტემის ოპერატორის** ბრალეული ქმედების შედეგად, რაც პირდაპირ და უშუალო კავშირშია დამდგარ ზიანთან და არ მოიცავს არაპირდაპირ ზიანს ან/და მიუღებელ შემოსავალს.

8. დასკვნითი დებულებები

8.1. **კონტრაჰენტის** მიერ **სისტემის ოპერატორისთვის პერსონალური მონაცემების** გადაცემა ხორციელდება კანონმდებლობით გათვალისწინებული მიზნებისა და საფუძვლების შესაბამისად;

8.2. **კონტრაჰენტი პერსონალური მონაცემების** შენახვასა და დამუშავებას განახორციელებს შიდა პროცედურებისა და მოქმედი კანონმდებლობით დადგენილი ვადების შესაბამისად;

8.3. **სისტემის ოპერატორი/კონტრაჰენტი** ვალდებულია, **მხარეებს** შორის დავის წარმოშობის შემთხვევაში მოთხოვნისთანავე გადასეს **მხარეს** მის ხელთ არსებული **მონაცემები**;

8.4. **კონტრაჰენტი** უფლებამოსილია, შემოწმების მიზნით, **სისტემის ოპერატორს** მოსთხოვოს შესაბამისი ინფორმაციისა და დოკუმენტაციის წარდგენა.