შპს ნუმუსი

პერსონალური მონაცემების დაცვისა და უსაფრთხოების პოლიტიკა

პროცედურა

შესაბამისობის დეპარტამენტი

6/25/2024

1. ზოგადი დებულებები

1.1. მიზანი და მოცულობა

მოცემული პერსონალური მონაცემების დაცვისა და უსაფრთხოების პოლიტიკა (შემდგომში „პერსონალურ მონაცემთა დაცვის პოლიტიკა“ ან „პოლიტიკა“) ძირითადად მიმართულია შპს ნუმუს-ს („კომპანია“) პერსონალური მონაცემების დაცვასთან, რომელსაც კომპანია ამუშავებს თანამშრომლებთან, კლიენტებთან ან მონაცემთა სხვა სუბიექტებთან თავის საქმიანობაში. პერსონალურ მონაცემთა დაცვის პოლიტიკა დანერგილია და ის მკაცრად უნდა დაიცვან კომპანიის თანამშრომლებმა ან/და ბიზნესპარტნიორებმა, როდესაც ისინი ამუშავებენ პერსონალურ მონაცემებს სამსახურებრივი მოვალეობების შესრულებისას. კომპანია აგროვებს, ინახავს და იყენებს პერსონალურ მონაცემებს თავის ყოველდღიურ საქმიანობაში. ამრიგად, პერსონალური მონაცემები მუშავდება კანონის ფარგლებში, ისეთ შემთხვევებში, როგორებიცაა: ინდივიდუალური შრომითი ხელშეკრულებების ან იურიდიული ან კომერციული შეთანხმების შესრულება, რომლის მხარესაც წარმოადგენს კომპანია; მარკეტინგული და სხვა მიზნებისთვის, მოქმედი რეგულაციების მოთხოვნების შესაბამისად.

პერსონალური მონაცემების დაცვის შესახებ კანონის მოთხოვნების შესაბამისად, ისევე როგორც მასთან დაკავშირებული კანონმდებლობის თანახმად, კომპანიისთვის უაღრესად მნიშვნელოვანია საკუთარი თანამშრომლების, მომხმარებლების სახელშეკრულებო პარტნიორების პერსონალური მონაცემების დაცვა.

აღნიშნულ პოლიტიკაში მოცემულია პერსონალურ მონაცემთა დაცვის მინიმალური მოთხოვნები და ინსტრუქცია. ეს დოკუმენტი ასევე წარმოადგენს პერსონალური მონაცემების კონფიდენციალურობისა და მთლიანობის შესანარჩუნებლად საჭირო ორგანიზაციულ-ტექნიკური ღონისძიებების მიღებისა და განხორციელების საფუძველს.

1.2. ვის ეხება პოლიტიკა

ეს პოლიტიკა განკუთვნილია და უნდა ეცნობოს შპს ნუმუსს ყველა შეილობილ კომპანიას, თანადამმუშავებელ კომპანიას, თანამშრომლებს, მიუხედავად მონაცემთა მდებარეობისა თუ მოწყობილობის ტიპისა, რომელზედაც ისინი ინახება. ამიტომ, პოლიტიკით გათვალისწინებული წესები უნდა დაიცვას და გამოიყენოს ყველა თანამშრომელმა, კონტრაქტორმა, შპს ნუმუსს-თან დაკავშირებულმა პირებმა და მესამე მხარეებმა, რომლებსაც აქვთ წვდომა კომპანიის მიერ შენახულ ან დამუშავებულ ინფორმაციაზე, ან/და IT სისტემებზე, რომლებიც გამოიყენება მათი შენახვისთვის და დამუშავებისთვის.

2. განმარტებები და შემოკლებები

კომპანია	შპს ნუმუს
ხელშეკრულება	ნებისმიერი ხელშეკრულება, რომლის ერთ-ერთ მხარეს წარმოადგენს კომპანია.
აქტივები	ნებისმიერი მატერიალური ან არამატერიალური აქტივი, რომელსაც ფლობს კომპანია.
ხელმისაწვდომობა	ნებისმიერმა საინფორმაციო სისტემამ თავისი მიზნის მისაღწევად უნდა დაუშვას ინფორმაციის ხელმისაწვდომობა, როდესაც ეს აუცილებელია. ამიტომ, ინფორმაციის შესანახად და დასამუშავებლად გამოყენებული საინფორმაციო სისტემები, უსაფრთხოების კონტროლი, რომელიც გამოიყენება მის დასაცავად და მასზე წვდომისთვის გამოყენებული საკომუნიკაციო არხები, სწორად უნდა მუშაობდეს.
ბიზნეს ერთეული	კომპანიის დეპარტამენტი, განყოფილება ან დანაყოფი, რომელიც ასახულია კომპანიის ორგანიზაციულ სქემაში (მაგ. მარკეტინგი, HR, ბუღალტერია, IT და ა.შ.).
კომპანიის მონაცემები/ინფორმაცია	მოიცავს, თუმცა არ შემოიფარგლება: კომპანიის მიერ წარმოებულ მონაცემებს/ინფორმაციას; მონაცემებს/ინფორმაციას, რომელზეც კომპანია ფლობს ინტელექტუალური საკუთრების უფლებებს; მონაცემებს/ინფორმაციას, რომელსაც კომპანია ფლობს ან ინახავს არქივებში; კომპანიიდან გაგზავნილ და კომპანიაში მიღებულ კომუნიკაციებს, განურჩევლად იმ მატარებლისა, რომელზეც ისინი ინახება, მაგ.: სისტემები, რომლებიც დაკავშირებულია კომპანიის კორპორატიულ მონაცემებთან ან სატელეფონო ქსელებთან; სისტემები, რომლებსაც მართავს კომპანია ან მესამე პირი კომპანიის სახელით; მობილური მოწყობილობები, რომლებიც გამოიყენება კომპანიის ქსელთან დასაკავშირებლად ან რომლებზეც ინახება კომპანიის მონაცემები; cloud სერვისებს, რომლებსაც მესამე მხარე ახორციელებს კომპანიის სახელით.

კომპიუტერი	ნებისმიერი კომპიუტერი ან ლეპტოპი, მობილური მოწყობილობა (მაგ. მობილური ტელეფონი, სმარტფონი, ტაბლეტი და ა.შ.), სერვერი ან/და სხვა შესაბამისი მოწყობილობა, რომელიც: i. გამოყენებულია მომსახურების შესრულებისას ii. შეიძლება გამოყენებულ იქნეს ქსელში ან ინფორმაციის მატარებელზე წვდომისთვის, ან iii. კონფიდენციალურ ინფორმაციაზე წვდომის ან მისი შენახვის საშუალებას იძლევა
კონფიდენციალური ინფორმაცია	ნებისმიერი ინფორმაცია, განურჩევლად ფორმატისა, რომელშიც ის წარმოდგენილია (მაგ. ზეპირად, ქაღალდზე ან სხვა არამატერიალურ ფორმატში), მათ შორის, მაგრამ არ შემოიფარგლება: მონაცემები, პერსონალური ინფორმაცია, ინტელექტუალური საკუთრება, პაროლები, ინფორმაცია კომპანიის მომხმარებლები, პროვაიდერების, პარტნიორებისა და პერსონალის შესახებ; ინფორმაცია კომპანიის პროდუქტების შესახებ, რომელიც ჯერ არ გასაჯაროვებულა. საგადახდო მომსახურების პროცესში განხორციელებული ტრანზაქციების, მათ შორის, მომხმარებლის ფულადი სახსრებისა და მასთან დაკავშირებული ინფორმაცია, აგრეთვე განხორციელებული ოპერაციის შესახებ (მათ შორის, ოპერაციის განხორციელების მცდელობის შემთხვევაში არსებული) ინფორმაცია;
კონფიდენციალურობა	ინფორმაციის უსაფრთხოების მოთხოვნების შესასრულებლად უზრუნველყოფა, რათა ის არ უნდა იყოს გამჟღავნებული საზოგადოებისთვის ან/და გადაცემული არაავტორიზებულ პირებზე, კომპანიებზე და არ უნდა იყოს გადაცემული/გამოყენებული ნებისმიერ არაავტორიზებულ პროცესებში.
ინფორმაციის საშუალება/მატარებელი	ინფორმაციის ნებისმიერი საშუალება/მატარებელი, მათ შორის, შემუშავება, ტესტირება, შედარებითი ანალიზი, დამხმარე აპლიკაციის ან ინფორმაციის მატარებლის შექმნა ან/და მხარდაჭერა, რომელზეც პროვაიდერს აქვს წვდომა კონტრაქტის მიხედვით ან რომელიც გამოიყენება სერვისების მიწოდებისთვის და შეიცავს ბიზნესთან დაკავშირებულ კონფიდენციალურ ან საკუთრებაში არსებულ ინფორმაციას.
ობიექტები	(ა) ნებისმიერი ოფისი, მონაცემთა ცენტრი და სხვა ლოკაცია (კომპანიის, კომპანიის ბიზნეს პარტნიორის, პროვაიდერის ან მესამე მხარის საკუთრებაში ან მართვაში), რომლებზეც კომპანიის კონფიდენციალურ ინფორმაციაზე, მედიასა თუ ქსელებზე წვდომა შეიძლება, ან (ბ) კომპანიის ნებისმიერი მუდმივი ან დროებითი დამუშავების ან შენახვის აქტივები.
საინფორმაციო ტექნოლოგიები IT	კომპანიის საინფორმაციო ტექნოლოგიები (IT) კომპანიასა და მის პერსონალს სთავაზობთ ტექნოლოგიური და დამხმარე სერვისების ფართო სპექტრს. IT პასუხისმგებელია კომპანიის ინფრასტრუქტურის უზრუნველყოფაზე საიმედო, მოქნილი და უსაფრთხო ინფრასტრუქტურის შექმნასა და ინფორმაციული ტექნოლოგიების სერვისების მიწოდებაზე.
ინფორმაციული უსაფრთხოების ინციდენტი	ინციდენტი არის კომპანიის ინფორმაციის უსაფრთხოების პოლიტიკის ან წინამძღვარე პოლიტიკის აშკარა ან ფარული დარღვევა: · სისტემაზე ან მის მონაცემებზე არაავტორიზებული წვდომის მოპოვების მცდელობები (წარუმატებელი ან წარმატებული); · მომსახურების არასასურველი შეწყვეტა ან შეჩერება; · სერვისის არასანქცირებული გამოყენება მონაცემების დამუშავების ან მათი შენახვის მიზნით; · ცვლილებები სისტემის ტექნიკაში, პროგრამულ უზრუნველყოფასა ან პროგრამული უზრუნველყოფის მახასიათებლებში მფლობელის ნებართვის, მითითების ან თანხმობის გარეშე.
უსაფრთხოების ინციდენტი, რომელიც გავლენას ახდენს მონაცემთა დაცვაზე	ინციდენტი - ნიშნავს პერსონალური მონაცემების უსაფრთხოების დარღვევას, რომელმაც გამოიწვია (შემთხვევით ან უკანონოდ) გაგზავნილი, შენახული ან სხვაგვარად დამუშავებული პერსონალური მონაცემების განადგურება, დაკარგვა, შეცვლა, მონაცემების უსაფრთხოების დარღვევა, მონაცემების შეგროვება/მოპოვება ან სხვაგვარი უნებართვო დამუშავება ან არასანქცირებული გამჟღავნება, ან მათზე არაავტორიზებული წვდომა. ამ გარემოებების აღმოჩენა ფაქტობრივად წარმოადგენს უსაფრთხოების ინციდენტის აღმოჩენას, რომელიც გავლენას ახდენს მონაცემთა დაცვაზე.
მთლიანობა	ინფორმაციის უსაფრთხოებაში მონაცემთა მთლიანობა ნიშნავს მონაცემთა სიზუსტისა და მთლიანობის შენარჩუნებას და უზრუნველყოფას მთელი სიცოცხლის ციკლის განმავლობაში (მონაცემების შეცვლა შეუძლებელია ავტორიზაციის ან გამჟღავნების გარეშე).
პერსონალი	კომპანიის ყველა თანამშრომელი, კონტრაქტორი, ქვეკონტრაქტორი და წარმომადგენელი, რომლებსაც აქვთ წვდომა ობიექტებზე, ქსელებზე, მედიაზე ან/და კონფიდენციალურ ან საკუთრებაში არსებულ ინფორმაციაზე.
პროდუქტი	მზა პროდუქტი ან პროგრამული კომპონენტი, ან პროდუქტი, რომელიც შექმნილია, დამზადებულია ან მიეწოდება კომპანიას.

მომსახურება/სერვისები	კომპანიასა და მესამე მხარეს შორის დადებულ ხელშეკრულებაში, შეთანხმებაში ან საქმიანობის განრიგში განსაზღვრული სამუშაოები.
პროვაიდერი	კომპანია (მათ შორის მისი პერსონალი), რომელიც: i. ახორციელებს მომსახურებას ხელშეკრულების საფუძველზე ან/და ii. აქვს წვდომა კომპანიის ობიექტებზე, ქსელებზე, მედიაზე ან/და კონფიდენციალურ ან/და საკუთრებაში არსებულ ინფორმაციაზე.
სისტემური ადმინისტრატორი/მენეჯერი	ჯგუფი, რომელიც უზრუნველყოფს კომპანიის სისტემის ყოველდღიურ ტექნიკურ ფუნქციონირებას: მონაცემთა ბაზის მენეჯმენტს, პროგრამული უზრუნველყოფის გავრცელებას და განახლებას, ვერსიების კონტროლს, სარეზერვო ასლებს და აღდგენას, ვირუსებისგან დაცვას და შესაძლებლობების შესრულებას და დაგეგმვას. კომპანიაში ამ სერვისს უზრუნველყოფს IT დეპარტამენტი
მომხმარებელი	პირი, რომელიც იყენებს სარგებლობს კომპანიის მომსახურებით.
პერსონალური მონაცემები	წარმოადგენს ნებისმიერ ინფორმაციას, რომელიც ეხება იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს. იდენტიფიცირებადი ფიზიკური პირი არის ის, ვისი იდენტიფიცირებაც შესაძლებელია, პირდაპირ ან ირიბად, კერძოდ, ისეთი იდენტიფიკატორების გამოყენებით, როგორებიცაა: სახელი, გვარი, საიდენტიფიკაციო ნომერი, მდებარეობის მონაცემები, ონლაინ იდენტიფიკატორი ან ამ ფიზიკური პირის ფიზიკური, ფიზიოლოგიური, გენეტიკური, გონებრივი, ეკონომიკური, კულტურული ან სოციალური იდენტობის მახასიათებელი სპეციფიკური ერთი ან მეტი ფაქტორი.
იდენტიფიცირებული	როგორც წესი, ნიშნავს სახელით იდენტიფიცირებულს, მაგრამ იდენტიფიკაცია არ შემოიფარგლება პირის სახელითა და გვარით, არამედ „პერსონალური მონაცემების“ ტერმინი მოიცავს მონაცემთა სუბიექტის იდენტობის ყველა ელემენტს, როგორც ზემოთ იყო ჩამოთვლილი.
იდენტიფიცირებადი	ნიშნავს, რომ პირის იდენტიფიცირება შესაძლებელია იმ ელემენტების/მონაცემების ანალიზით, რომლებიც უკვე არის ხელმისაწვდომი ან მოიპოვება სხვა წყაროებიდან.
მონაცემთა სუბიექტი	არის ფიზიკური პირი, რომლის პერსონალურ მონაცემებს ამუშავებს კომპანია (მაგ.: თანამშრომლები, მომხმარებლები ან ბიზნესპარტნიორები – ფიზიკური პირები).
პერსონალური მონაცემების დამუშავება	ნიშნავს ნებისმიერ ოპერაციას ან ოპერაციების ერთობლიობას, რომელიც შესრულებულია პერსონალურ მონაცემებზე ან პერსონალურ მონაცემთა ჯგუფებზე, ავტომატური ან სხვა საშუალებებით, როგორიცაა შეგროვება, ჩაწერა, ორგანიზება, სტრუქტურირება, შენახვა, ადაპტაცია ან შეცვლა, მოძიება, კონსულტაცია, გამოყენება, გამჟღავნება, გავრცელება ან სხვაგვარად ხელმისაწვდომობა, ჩასწორება ან გაერთიანება, შეზღუდვა, წაშლა ან განადგურება და სხვა.
პერსონალური მონაცემების შენახვის სისტემა	პერსონალური მონაცემების ნებისმიერი სტრუქტურირებული ნაკრები, რომელიც ხელმისაწვდომია კონკრეტული კრიტერიუმების მიხედვით, იქნება ეს ცენტრალიზებული, დეცენტრალიზებული თუ განაწილებული ფუნქციონალური ან გეოგრაფიული ლოგიკით.
საჩივარი	ნიშნავს საჩივარს, განცხადებას, რომლითაც მონაცემთა სუბიექტი ახორციელებს პერსონალური მონაცემების დაცვის უფლებების რეალიზაციას მოქმედი რეგულაციებით.
ფსევდონიმიზირებული მონაცემები	ნიშნავს პერსონალური მონაცემების დამუშავებას ისე, რომ პერსონალური მონაცემები აღარ შეიძლება მიეკუთვნოს მონაცემთა კონკრეტულ სუბიექტს დამატებითი ინფორმაციის გამოყენების გარეშე, იმ პირობით, რომ ასეთი დამატებითი ინფორმაცია ინახება ცალკე და ექვემდებარება ტექნიკურ და ორგანიზაციულ ზომებს, რათა უზრუნველყოს, რომ პერსონალური მონაცემები არ მიეკუთვნებოდეს იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს.
მონაცემთა დეპერსონალიზაცია	მონაცემთა იმგვარი დამუშავება, როდესაც შეუძლებელია მონაცემთა სუბიექტთან მათი დაკავშირება ან ასეთი კავშირის დადგენა არაპროპორციულად დიდ ძალისხმევას, ხარჯებს ან/და დროს საჭიროებს.“ანონიმური მონაცემები არ წარმოადგენს პერსონალურ მონაცემებს.
დამუშავებისთვის პასუხისმგებელი პირი	არის ფიზიკური, კერძო ან საჯარო იურიდიული პირი, მათ შორის საჯარო ორგანოები, დაწესებულებები და მათი ტერიტორიული ერთეულები, რომელიც განსაზღვრავს პერსონალური მონაცემების დამუშავების მიზნებსა და საშუალებებს. უშუალოდ ან დამუშავებაზე უფლებამოსილი პირის მეშვეობით ახორციელებს მონაცემთა დამუშავებას

დამუშავებაზე უფლებამოსილი პირი	არის ფიზიკური, კერძო ან საჯარო იურიდიული პირი, რომელიც ამუშავებს პერსონალურ მონაცემებს კომპანიისთვის და კომპანიის სახელით. ეს შეიძლება იყოს კომპანიის პროვაიდერი ან მისი შვილობილი კომპანია, რომელსაც წვდომა აქვთ მონაცემთა სუბიექტების მონაცემებზე. მაგ.: სასწავლო სერვისის პროვაიდერი, სარეკლამო სააგენტო ან სხვა კომპანია, რომელიც ამუშავებს პერსონალურ მონაცემებს კომპანიის სახელით.
მონაცემთა თანადამმუშავებელი	კომპანიასთან ერთად დამუშავებისთვის პასუხისმგებელი პირი, რომელთან ერთადაც, მხარეები ერთობლივად განსაზღვრავენ მონავემთა დამუშავების მიზნებსა და საშუალებებს.
მონაცემთა მიმღები	შეიძლება იყოს საჯარო ორგანო ან სხვა ორგანო, რომელსაც გადაეცა პერსონალური მონაცემები, კანონმდებლობის შესაბამისად, მიუხედავად იმისა, წარმოადგენს მესამე მხარეს თუ არა.
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;

3. კომპანიის მიზნები

ამ პოლიტიკით, კომპანია მიზნად ისახავს:

- უზრუნველყოს პერსონალური მონაცემების დამუშავება იმ ლეგიტიმური მიზნების შესაბამისად, რისთვისაც ისინი შეგროვდა;

- უზრუნველყოს, რომ ყველა პერსონალური მონაცემი ადეკვატურად იყოს დაცული თავდასხმებისგან/საფრთხისგან, რათა უზრუნველყოფილი იყოს პერსონალური მონაცემების უსაფრთხოება;

- შექმნას პერსონალური მონაცემების დაცვის მოთხოვნებთან დაკავშირებული ინფორმირებულობის პროცესი, რათა ის ინტეგრირებულ იქნეს თანამშრომლების მიერ განხორციელებულ ყოველდღიურ საქმიანობაში; ასევე რათა უზრუნველყოს ყველა თანამშრომლის ინფორმირებულობა პროცედურების შესახებ, რომლებიც უნდა დაიცვან პერსონალური მონაცემების შეგროვების, ლეგიტიმური დამუშავების, გამჟღავნების, გადაცემის, შენახვის, დაარქივებისა და განადგურების დროს;

- უზრუნველყოს, რომ კომპანიის ყველა თანამშრომელმა გააცნობიეროს პერსონალური მონაცემების დაცვასთან დაკავშირებული პრაქტიკის მნიშვნელობა, ასევე საკუთარი ვალდებულებები, რომლებიც პერსონალური მონაცემების უსაფრთხოების დაცვასთანაა დაკავშირებული,;

- უზრუნველყოს, რომ ყველა ბიზნეს პარტნიორი, რომლებიც აგროვებენ, ინახავენ და ამუშავებენ პერსონალურ მონაცემებს კომპანიისთვის და კომპანიის სახელით, აკმაყოფილებდნენ და ახორციელებდნენ პერსონალური მონაცემების დაცვისა და უსაფრთხოების ადეკვატურ ზომებს. პერსონალური მონაცემები არავითარ შემთხვევაში არ უნდა იყოს გამჟღავნებული, შემთხვევით ან სხვაგვარად, არაუფლებამოსილ ადგილობრივ პირთან ან მესამე მხარესთან.

ამ პოლიტიკის ან კომპანიის არსებული ინსტრუქციების ნებისმიერმა დარღვევამ ან შეუსრულებლობამ, კერძოდ, პერსონალური მონაცემების განზრახ გამჟღავნებამ ნებისმიერი არაავტორიზებული პირისთვის ან მესამე მხარისთვის, შეიძლება გამოიწვიოს დისციპლინარული ან სხვა ადეკვატური ქმედებები.

პერსონალურ მონაცემებზე არასანქცირებული წვდომის ან გამჟღავნების, ან სხვა შემთხვევების შესახებ, უნდა ეცნობოს კომპანიის პერსონალური მონაცემების დაცვის ოფიცერს, იურიდიულ დეპარტამენტს, კომპანიის შესაბამისობის დეპარტამენტს ან კომპანიის ინფორმაციის უსაფრთხოების დეპარტამენტს, უმოკლეს ვადებში.

4. პერსონალური მონაცემები

კომპანიის მიერ განხორციელებულ საქმიანობაში შედის სხვადასხვა ტიპის ინფორმაცია, რომელიც ეხება: ფიზიკური პირების საიდენტიფიკაციო მონაცემებს, ბიზნეს ინფორმაციას და ინფორმაციას მომსახურების/პროდუქტის განვითარების, მარკეტინგისა და ბიზნეს გეგმების შესახებ, ინფორმაცია კლიენტების, ადამიანური რესურსების, კონსულტაციების, პარტნიორობის, კონტრაქტების, შერწყმისა და შესყიდვების შესახებ.

კონფიდენციალური მონაცემების ფართო სპექტრის გათვალისწინებით, რომელსაც კომპანია მართავს, მნიშვნელოვანია, რომ თანამშრომლებმა გაიგონ მათ მიერ დამუშავებული პერსონალური მონაცემების კატეგორია/კატეგორიები, რათა შეძლონ შესაბამისი მონაცემების დაცვის მოქმედი წესების და რისკების მართვის მეთოდების განსაზღვრა.

ეს პოლიტიკა განსაზღვრავს კომპანიის მიერ დამუშავებულ პერსონალურ მონაცემებს მისი ბიზნეს საქმიანობის ფარგლებში და მის შესრულების დროს, ამავდროულად ამ კატეგორიაში ხვდება კონფიდენციალური ინფორმაციაც.

ა) პერსონალური მონაცემები მოიცავს იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირთან დაკავშირებულ ნებისმიერ ინფორმაციას, მაგალითად, როგორებიცაა (თუმცა, არ შემოიფარგლება):

- სახელი, გვარი,
- მშობლებისა და ოჯახის წევრების ვინაობა (ქმარი/ცოლი, შვილები, მონაცემთა სუბიექტზე დამოკიდებულები),

- მისამართი (ფიზიკური ან იურიდიული),

- მონაცემები პირადობის დამადასტურებელი დოკუმენტებიდან, დაბადების მოწმობებიდან, ქორწინების მოწმობებიდან, მართვის მოწმობიდან, პასპორტიდან, ბინადრობის ნებართვიდან, აღნიშნული დოკუმენტების ასლებიდან და ა.შ.;

- მოქალაქეობა,

- განათლება, პროფესია, რეზიუმე, დიპლომების ასლები, საკვალიფიკაციო მოწმობების ასლები,

- პერსონალური მონაცემები ფინანსური მდგომარეობის შესახებ (მაგ. მონაცემები შემოსავლების, ყოველთვიური ხარჯების, მონაცემთა სუბიექტების საკუთრებაში არსებული აქტივების შესახებ, ლიზინგის ხელშეკრულებები, შეღავათები, ხელფასები, ბონუსი, მიზნების შესრულების ბონუსი),

- ფოსტა, ტელეფონის ნომერი,

- მომხმარებლის ანგარიშები კომპანიის აპლიკაციებისთვის,

- საბანკო მონაცემები (სახელფასო ანგარიში)

- მონაცემები შეძენილი ან შესასყიდი სერვისებისა და პროდუქტების შესახებ (მაგ. მონაცემები საწვავის სავარაუდო მოხმარების შესახებ, საწვავის ყოველთვიური ხარჯები, გამოყენებული საწვავის ტიპი, სადგური, სადაც მომხმარებლები იყენებენ დაგროვების ბარათს და ა.შ.),

- გეოლოკაციის მონაცემები (მაგ. სადგური, სადაც ისინი ავსებენ საწვავს, მარშრუტი სახლიდან სამსახურში და უკან, სამსახურში მგზავრობის და უკან დაბრუნების დრო),

- მონაცემები სამუშაო ადგილის შესახებ, მათ შორის დამსაქმებლის დასახელება და საიდენტიფიკაციო მონაცემები, სამუშაო ტელეფონის ნომერი, სამუშაო ელ-ფოსტა, თანამდებობა, განყოფილება, მენეჯერის სახელი, შიდა ID ნომერი, დასაქმების თარიღი/კომპანიიდან წასვლის თარიღი)

- მონაცემები დასაქმებულის სტატუსის შესახებ (ინდივიდუალური შრომითი ხელშეკრულების ნომერი და თარიღი, დაკავებული თანამდებობები, სამუშაო ადგილი, შიდა ID ნომერი, მიმდინარე სამუშაოს დაწყების თარიღი).

პერსონალური მონაცემები მოიცავს ინფორმაციას, რომელიც შეიძლება მოიძებნოს ნებისმიერი ფორმით, იქნება ეს ანბანური, რიცხვითი, გრაფიკული, ფოტოგრაფიული თუ აკუსტიკური, და შეიძლება მოიძებნოს ფიზიკურად (ქაღალდზე), ან ელექტრონულ ფორმატში (კომპიუტერის მეხსიერებაზე), ან თუნდაც ვიდეო და აუდიო ჩანაწერების სახით.

ბ) პერსონალური მონაცემების განსაკუთრებული კატეგორიები

განსაკუთრებული კატეგორიის მონაცემი არის მონაცემი, რომელიც ეხება პირის რასობრივ ან ეთნიკურ წარმომავლობას, პოლიტიკურ, რელიგიურ, ფილოსოფიურ ან მსგავს შეხედულებებს, პროფკავშირის წევრობას, ჯანმრთელობას ან სქესობრივ ცხოვრებას, აგრეთვე სისხლის სამართლის პროცესში პირის სტატუსს, ნასამართლობასთან დაკავშირებულ ინფორმაციას, დანაშაულის მსხვერპლად ცნობას, პატიმრობას და სასჯელის აღსრულებას.

ამავდროულად, განსაკუთრებული კატეგორიის მონაცემად მიიჩნევა ბიომეტრიული მონაცემი, რაც გულისხმობს მონაცემთა სუბიექტის როგორც ფიზიკურ და ფიზიოლოგიურ (მაგ. თითის ანაბეჭდი, სახის გამოსახულება, დეენემი), ისე ქცევის მახასიათებლებს (მაგ. სიარულის მანერა), რომელიც მისი უნიკალური იდენტიფიცირების ან ვინაობის დადასტურების შესაძლებლობას იძლევა.

განსაკუთრებული კატეგორიის მონაცემებია (თუმცა, არ შემოიფარგლება):

- მონაცემები პირის პოლიტიკური შეხედულების შესახებ,

5. კომპანიის მიერ განხორციელებული საქმიანობის ფარგლებში შესრულებული პერსონალური მონაცემების დამუშავების ძირითადი ოპერაციები და დამუშავების მიზანი

5.1. ძირითადი დამუშავების ოპერაციები/ოპერაციების ნაკრები შეიძლება შედგებოდეს შემდეგისგან:

- პერსონალური მონაცემების შეგროვება, ჩაწერა და ორგანიზება
- შეგროვებული პერსონალური მონაცემების შენახვა, და, შესაბამისად, ნებისმიერი ტიპის ინფორმაციის მატარებელზე შენახვა
- მათი ადაპტაცია, შეცვლა ან გამოყენება,
- პირადი მონაცემების მოპოვება
- გამჟღავნება მესამე პირებისთვის გადაცემის, გავრცელების ან სხვა გზით
- პერსონალური მონაცემების გაერთიანება ან დაკავშირება
- პერსონალური მონაცემების დაბლოკვა, წაშლა ან განადგურება.

5.2. პერსონალური მონაცემების დამუშავების მიზანი

მომხმარებლების, პოტენციური მომხმარებლების, მომხმარებელთა/პოტენციური მომხმარებლების კანონიერი წარმომადგენლების პერსონალური მონაცემები შეიძლება შეგროვდეს და გამოყენებულ იქნეს კონკრეტული აქტივობებისა და პროექტების განხორციელებისას, როგორებიცაა:

- კრედიტუნარიანობის შეფასება და საკრედიტო რისკის შეფასება კომპანიის მიერ მიწოდებული კონკრეტული პროდუქტებისთვის კომპანიის წინაშე დავალიანების ასანაზღაურებლად,

- ხელშეკრულებების გაფორმება და შესრულება, მათ შორის მომსახურების ხელშეკრულებები და სხვა ნებისმიერი ხელშეკრულება.

- სამართლებრივი ვალდებულების შესრულება, როგორიცაა ფისკალური ანგარიშ-ფაქტურების ან ქვითრების და საგადახდო/ინკასო დავალების გაცემა,

- მარკეტინგული საქმიანობის განხორციელება, საინფორმაციო ბიულეტენების ან სხვა კომერციული კომუნიკაციების გაგზავნით ელექტრონული ფოსტით, ტექსტური შეტყობინებით ან ფოსტით,

- მომხმარებლის პროფილის შესწავლა მორგებული შეთავაზებების გასაგზავნად,

- შიდა და გარე ღონისძიებების ორგანიზება,

- კომპანიის გარე პარტნიორების (როგორიცაა სარეკლამო სააგენტოები) მიერ განხორციელებული დამუშავების ოპერაციები,

- მომხმარებლებთან ხელშეკრულებების დადება – ფიზიკური პირები, რომლებიც სარგებლობენ კომპანიისა და მისი შვილობილი კომპანიების მომსახურებით.

- თანადამმუშავებლისთვის ინფორმაციის მიწოდება და მათგან მიღება.

თანამშრომლების პერსონალური მონაცემების შეგროვება და გამოყენება შესაძლებელია კომპანიის მიერ კონკრეტული აქტივობებისა და პროექტების განსახორციელებლად, როგორიცაა:

- რეკრუტინგის პროცესის განხორციელება,

- ინდივიდუალური შრომითი ხელშეკრულებების გაფორმება და შესრულება; ხელფასისა და სარგებლის გაღახდა; სამსახურში ყოფნასთან დაკავშირებული საქმიანობის განხორციელება; სასწავლო პროგრამების განხორციელება; სამუშაო ამოცანების შესასრულებლად საჭირო

აღჭურვილობის მართვა; მივლინებები; ყოველწლიური შვებულების ან სხვა ტიპის შვებულების დაგეგმვა და განხორციელება.

- საკანონმდებლო ვალდებულების შესრულება, როგორიცაა დასაქმებამდე სამედიცინო გამოკვლევის ჩატარება და შრომის ჯანმრთელობისა და უსაფრთხოების უზრუნველსაყოფად რეგულარული შემოწმების ჩატარება; შრომის ჯანმრთელობისა და უსაფრთხოების ფაილების შევსება; პროფესიული სწავლებისა და სასწავლო პროგრამების გავლა; რევიზიის რეესტრის შევსება; კანონით დადგენილი გადასახადების დაკავება და გადახდა; აპლიკაციის რეგლამენტით გათვალისწინებული შემწეობების გაღახდა.

- მონაცემთა მაკონტროლებლის კანონიერი ინტერესების განხორციელება; ვიდეომეთვალყურეობის შემთხვევაში აქტივებისა და პირების დაცვის უზრუნველყოფა; მონაცემთა დაკარგვის თავიდან აცილების მიზნით, საინფორმაციო სისტემების უსაფრთხოების უზრუნველყოფა;

- სპეციალიზებული კვლევების ჩატარება, როგორიცაა ხელფასის დონის გადახედვა, განვითარება და შრომითი ურთიერთობების გაუმჯობესება; მონაცემთა დამუშავების IT სისტემების შემუშავება, მათ შორის ხელფასის გაანგარიშება, ყოველწლიური შვებულების მართვა;

- კომპანიისთვის სხვა კომპეტენტური ორგანოებისა და ორგანოებისადმი ანგარიშგების განხორციელება და ა.შ.

- პროფესიული გამოცდილების განხილვა და ტრენინგი პროფესიული განვითარების პროგრამების შემუშავების მიზნით, პროფესიული და ტექნიკური ტესტების საფუძველზე,

- რელიგიური დღესასწაულების განსაზღვრა;

- დასაქმებულის შვილების ან ოჯახის სხვა წევრებისთვის ფულადი დანამატების გაანგარიშება ან გადახდა,

- შრომითი ურთიერთობისგან წარმოქმნილი მიანის ან კომპანიის მიერ მიყენებული მიანის ანაზღაურება; პერსონალური მონაცემების გაგზავნა კომპეტენტურ ორგანოებში,

- სტატისტიკური მიზნებისთვის.

6. პერსონალური მონაცემების გამოყენება

პერსონალური მონაცემების კატეგორიის მიუხედავად, მონაცემები უნდა იქნეს გამოყენებული მხოლოდ იმ მიზნისთვის, რისთვისაც ისინი შეგროვდა მონაცემთა სუბიექტებისგან (კომპანიის მომხმარებლები, არამომხმარებლები, თანამშრომლები ან კონტრაქტორები, პარტნიორები) და იმ პერიოდის განმავლობაში, რომელიც საჭიროა ამ მიზნების მისაღწევად, და, შესაბამისად, იმ

პერიოდის განმავლობაში, რომელიც საჭიროა კანონიერი ვალდებულების შესასრულებლად ან კომპანიის ინტერესების დასაცავად.

მაგალითად, როდესაც პერსონალური მონაცემების დამუშავება ხორციელდება მომხმარებლის მკაფიო და კონკრეტული თანხმობით (მაგ., შემთხვევა, როდესაც მომხმარებელი თანახმაა კომპანიის მიერ პერსონალური მონაცემების მარკეტინგული მიზნებისთვის დამუშავებაზე), მონაცემების დამუშავების მიზნები აღწერილი უნდა იყოს მონაცემთა სუბიექტის მიერ გამოთქმულ თანხმობაში.

ამავე მიზნით, კომპანიის მიერ პერსონალური მონაცემების დამუშავების ლეგიტიმურობის უზრუნველსაყოფად, იმ შემთხვევაში, თუ მონაცემთა სუბიექტი აუქმებს თანხმობას მისი მონაცემების დამუშავებაზე მარკეტინგული ან სხვა ლეგიტიმური მიზნებისთვის, რისთვისაც აუცილებელი იყო მისი წინასწარი თანხმობა, კომპანია უზრუნველყოფს პერსონალური მონაცემების წაშლას მოქმედი რეგულაციების შესაბამისად.

7. პერსონალურ მონაცემთა დაცვის ოფიცერი

კომპანიას ყავს მონაცემთა დაცვის ოფიცერი („მონაცემთა დაცვის ოფიცერი“), რომელიც ადეკვატურად და დროულად უნდა იყოს ჩართული პერსონალური მონაცემების დაცვასთან დაკავშირებულ ყველა ასპექტში.

მონაცემთა დაცვის ოფიცერს აქვს მინიმუმ შემდეგი პასუხისმგებლობები:

(ა) მოთხოვნის შესაბამისად, კონსულტაცია გაუწიოს კომპანიას და, ასევე, იმ თანამშრომლებს, რომლებიც ახორციელებენ პერსონალური მონაცემების დაცვასთან დაკავშირებულ ვალდებულებებს;

(ბ) განახორციელოს მონაცემთა დაცვის შესახებ საკანონმდებლო დებულებებთან და კომპანიის პერსონალური მონაცემების დაცვის შესახებ პოლიტიკასთან შესაბამისობის მონიტორინგი, გაუწიოს დახმარება და გასცეს რეკომენდაციები კომპანიისთვის და მისი შიდა განყოფილებების თანამშრომლებისთვის მონაცემთა დაცვასთან დაკავშირებული ვალდებულებების შესრულების უზრუნველსაყოფად (მაგ. უსაფრთხოების ინციდენტების შემთხვევაში, უზრუნველყოს აუცილებელი დახმარება ზედამხედველობის ორგანოსა და მონაცემთა დაზარალებული სუბიექტების ინფორმირებაში);

(გ) უზრუნველყოს დახმარება პერსონალური მონაცემების დამუშავების ოპერაციების შიდა რეგულირებისთვის საჭირო შიდა პოლიტიკისა და პროცედურების შემუშავებაში;

(დ) კონსულტაცია გაუწიოს მონაცემთა დაცვაზე შეგავლენის შეფასების საკითხთან დაკავშირებით და უზრუნველყოს მისი ფუნქციონირების მონიტორინგი (მისცეს რჩევა პირადი მონაცემების ზემოქმედების შეფასების შემთხვევაში, რამდენად არის კომპანია ვალდებული შეასრულოს ეს შეფასება, ასევე უზრუნველყოს ამ შეფასებისთვის გამოსაყენებელი მეთოდოლოგია, საჭირო რესურსების არსებობა, უსაფრთხოების, ტექნიკური და ორგანიზაციული ზომების გამოყენება მონაცემთა სუბიექტის უფლებებისა და თავისუფლებების რისკების შესამცირებლად);

(ე) ის არის პერსონალური მონაცემების დაცვის საზედამხედველო ორგანოსთან ძირითადი საკონტაქტო პირი.

კომპანია ასაჯაროებს პერსონალურ მონაცემთა დაცვის ოფიცრის საკონტაქტო ინფორმაციას და აწვდის მას საზედამხედველო ორგანოს.

8. მონაცემთა დამუშავების საფუძვლები

ხშირ შემთხვევაში, პერსონალური მონაცემების შეგროვება და კომპანიის მიერ ასეთი მონაცემების შემდგომი დამუშავების ოპერაციები მიიღწევა მონაცემთა სუბიექტის აშკარა და ცალსახა თანხმობის საფუძველზე. როდესაც მონაცემთა სუბიექტის თანხმობაა საჭირო, კომპანია მონაცემთა სუბიექტს აწვდის სრულ, წინასწარ და ზუსტ ინფორმაციას, რათა მისი თანხმობა შეესაბამებოდეს თავისუფალი, კონკრეტული, ინფორმირებული და ცალსახა ნების გამოვლენის პირობებს.

ასევე არის შემთხვევები, როდესაც დამუშავების სამართლებრივი საფუძველი სხვაა, და არა თანხმობა, კერძოდ:

- ყოველთვის, როდესაც დამუშავება საჭიროა ხელშეკრულების გასაფორმებლად, რომლის მხარესაც მონაცემთა სუბიექტი წარმოადგენს, ან ხელშეკრულების გაფორმებამდე გარკვეული ნაბიჯების გადადგმა მონაცემთა სუბიექტის მოთხოვნით;

- როდესაც დამუშავება გათვალისწინებულია კანონით.

- როდესაც დამუშავება საჭიროა მონაცემთა სუბიექტის ან სხვა სუბიექტების სასიცოცხლო ინტერესების დასაცავად

- როდესაც დამუშავება საჭიროა იმ ამოცანის შესასრულებლად, რომელიც ემსახურება საჯარო ინტერესებს ან გამომდინარეობს საჯარო უფლებამოსილების პრეროგატივების განხორციელებიდან, რომელიც მინიჭებული აქვს დამუშავებისთვის პასუხისმგებელ პირს;

- როდესაც მონაცემების სუბიექტმა ეს ინფორმაცია საჯარო გახადა ან ისედაც მისაწვდომი იყო საჯაროდ.

- როდესაც მონაცემთა დამუშავება აუცილებელია საქართველოს კანონმდებლობით განსაზღვრული საჯარო ინტერესის სფეროსთვის მიკუთვნებული ამოცანების შესასრულებლად.

- როდესაც მონაცემების დამუშავება აუცილებელია მონაცემთა სუბიექტის განცხადების განსახილველად (მისთვის მომსახურების მიწოდების უზრუნველსაყოფად)

- როდესაც დამუშავება საჭიროა კომპანიის ან მესამე მხარის ლეგიტიმური ინტერესების განსახორციელებლად, რომელსაც ეს მონაცემები ეცნობა, იმ პირობით, რომ ასეთი ინტერესი არ აზიანებს მონაცემთა სუბიექტის ინტერესებს ან ფუნდამენტურ უფლებებსა და თავისუფლებებს.

სპეციალური კატეგორიის მონაცემების დამუშავება მკაცრად აკრძალულია, გარდა შემდეგი შემთხვევებისა:

- როდესაც მონაცემთა სუბიექტი პირდაპირ თანხმდება ასეთ დამუშავებაზე

- როდესაც დამუშავება საჭიროა კომპანიის ან მონაცემთა სუბიექტის მოვალეობების შესრულებისა და კონკრეტული უფლებების განხორციელების მიზნით, დასაქმების და სოციალური უზრუნველყოფის ან სოციალური დაცვის სფეროში.

- როდესაც დამუშავება საჭიროა მონაცემთა სუბიექტის ან ნებისმიერი სხვა სასიცოცხლოდ მნიშვნელოვანი სუბიექტის სიცოცხლის, ფიზიკური ხელშეუხებლობის ან ჯანმრთელობის ინტერესების დასაცავად, თუ მონაცემთა სუბიექტს ფიზიკური ან იურიდიული მიზეზებით არ შეუძლია შესაბამისი თანხმობის გამოხატვა.

- როდესაც დამუშავება ეხება მონაცემთა სუბიექტის მიერ ღიად გასაჯაროებულ მონაცემებს

- როდესაც დამუშავება საჭიროა სასამართლოში უფლების დადგენის, განხორციელების ან დაცვისთვის

- როდესაც დამუშავება საჭიროა პრევენციული მედიცინის, შრომის მედიცინის, თანამშრომლის შრომისუნარიანობის შეფასებისთვის, სამედიცინო დიაგნოზის დასადგენად, სამედიცინო ან სოციალური დახმარების ან სამედიცინო მკურნალობისთვის, პროფესიული კავშირის კანონის ან შიდა კანონმდებლობის საფუძველზე ან კლინიკური პერსონალის წევრთან დადებული

შეთანხმების საფუძველზე პროფესიულ საიდუმლოებაზე, ან სხვა სუბიექტის მიერ ან ზედამხედველობის ქვეშ, რომელიც ექვემდებარება ეკვივალენტურ საიდუმლოებას.

- როდესაც დამუშავება საჭიროა საზოგადოებრივი ინტერესის არქივის, სამეცნიერო და ისტორიული კვლევის ან სტატისტიკური მიზნებისთვის.

კომპანიის თანამშრომლებმა/პარტნიორებმა უნდა შეამოწმონ პერსონალური მონაცემების მოხვედრა ზემოხსენებულ კატეგორიებში და დაიცვან პერსონალური მონაცემები კანონმდებლობით გათვალისწინებული წესების თანახმად.

როდესაც კომპანია წარადგენს ახალ სერვისს, პროდუქტს ან ოპერაციულ პროცესს, რომელიც მოიცავს პერსონალური მონაცემების დამუშავებას, მათ უნდა მოითხოვონ ნებართვა პერსონალური მონაცემების დაცვასთან დაკავშირებით მონაცემთა დაცვის ოფიცრისგან.

9. მონაცემთა დამუშავების პრინციპები

კომპანიის თანამშრომლებმა, როგორც კომპანიის სახელით მონაცემთა დამუშავების პროცესში ჩართულმა პირებმა, უნდა დაიცვან პერსონალური მონაცემების დამუშავების კანონიერი პრინციპები, როგორც ეს მოცემულია მონაცემთა დაცვის კანონმდებლობით და როგორც ქვემოთ არის მითითებული.

ა) პერსონალური მონაცემების დამუშავების კანონიერების პრინციპი

მონაცემები უნდა დამუშავდეს კანონიერად, სამართლიანად და მონაცემთა სუბიექტის ღირსების შეულახავად. აღნიშნული პრინციპი მოითხოვს, რომ მონაცემების დამუშავების პროცესი თანხვედრაში იყოს კანონით დადგენილ წესებთან, მათ შორის, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით დადგენილ მოთხოვნებთან.

ბ) პერსონალური მონაცემების დამუშავების გამჭვირვალობის პრინციპი

მონაცემთა სუბიექტს წინასწარ უნდა ეცნობოს დასამუშავებელ პერსონალურ მონაცემებთან დაკავშირებით, დამუშავების მიზანსა და მისი სამართლებრივი საფუძვლების შესახებ; მაკონტროლებლის და დამმუშავებლების ვინაობის შესახებ; ასევე მაკონტროლებლის მიერ პერსონალური მონაცემების დამუშავების კანონიერი ინტერესის შესახებ. აუცილებლობის შემთხვევაში, ასეთი მონაცემების ნებისმიერი მიმღების ან მიმღებთა კატეგორიის შესახებ, აუცილებლობის შემთხვევაშ, კომპანიის განზრახვის შესახებ პერსონალური მონაცემები გადასცეს მესამე მხარეს ან საერთაშორისო ორგანიზაციას, თუ ყველა მოთხოვნილი მონაცენების მიწოდება აუცილებელს წარმოადგენს, და ასეთი მონაცემების წარდგენაზე უარის შედეგების შესახებ, იმ ვადების შესახებ რომლის მანძილზეც იქნება შენახული ასეთი პერსონალური მონაცემები ან, თუ შეუძლებელია, იმ კრიტერიუმების შესახებ, რომელიც ასეთი პერიოდის განსასაზღვრად გამოიყენება, გადაწყვეტილების მიღების ავტომატიზირებული პროცესის არსებობის შესახებ, პროფილების შექმნია ჩათვლით, ასევე, როგორც მინიმუმ, ასეთი შემთხვევებისთვის, ინფორმაცია გამოყენებული ლოგიკის, მოსალოდნელი შედეგებისა და ასეთი დამუშავების მნიშვნელოვნების შესახებ მონაცენების სუბიექტისთვის, მონაცემთა სუბიექტის უფლებების შესახებ, რომელიც მონაცემთა დაცვის სფეროშია კანონით გათვალისწინებული (ჩამონათვალი იხილეთ ქვემოთ, განყოფილებაში 10), ასევე იმ პირობების შესახებ, რომელთა დროსაც შეიძლება ისინი განხორციელდეს, ასევე სხვა ნებისმიერ ინფორმაციასთან დაკავშირებით, რომელიც თავად დამუშავების მიზანს შეეხება.

გამჭვირვალობის პრინციპიდან გამომდინარე, მონაცემთა სუბიექტებს - კლიენტებს/პოტენციურ კლიენტებს/თანამშრომლებს/პარტნიორებს - ეცნობებათ ადვილად გასაგები და მკაფიო ენით, რითაც ექნებათ პერსონალური მონაცემების დამუშავების ოპერაციებთან დაკავშირებულ ინფორმაციაზე წვდომის უფლება.

ინფორმაციის შეტყობინება, რომელიც მიმართულია მონაცემთა სუბიექტ(-ებ-)ისადმი მათი პერსონალური მონაცემების დამუშავებასთან დაკავშირებით, უნდა მოიცავდეს საკონტაქტო პუნქტებს, სადაც მათ შეუძლიათ განცხადების წარდგენა, შემდეგნაირად:

- მომხმარებლის/პოტენციური მომხმარებლის, ბიზნესპარტნიორების, თანამშრომლების, ფიზიკური პირების მიერ წარმოდგენილი განაცხადები შეიძლება წარდგენილი იქნეს კომპანიის რეგისტრირებულ ოფისებში, ელექტრონული ფოსტის მეშვეობით, მისამართზე: info@paybox.ge;

როდესაც მონაცემთა სუბიექტი, რომლის მონაცემებიც მუშავდება, ითხოვს ინფორმაციას მისი მონაცემების დამუშავების შესახებ, დეპარტამენტი, რომელიც იღებს ასეთ განცხადებას, ითხოვს მონაცემთა დაცვის ოფიცრის აზრს.

კომპანიამ უნდა უპასუხოს ნებისმიერ ასეთ განაცხადს მისი მიღებიდან მაქსიმუმ 10 დღის განმავლობაში, მონაცემთა დაცვის კანონების დებულებების შესაბამისად. ეს ვადა განსაკუთრებულ შემთხვევებში და სათანადო დასაბუთებით შეიძლება გაგრძელდეს არაუმეტეს 10 სამუშაო დღით, რის შესახებაც მონაცემთა სუბიექტს დაუყოვნებლივ უნდა ეცნობოს

მონაცემთა სუბიექტის პრეტენზია/მოთხოვნა განიხილება მონაცემთა სუბიექტის განაცხადების განხილვის სპეციფიკური პროცედურის შესაბამისად.

გ) მონაცემებთა დამუშავების მიზნის შეზღუდვის პრინციპი

მონაცემები უნდა შეგროვდეს/მოპოვებული უნდა იქნეს მხოლოდ კონკრეტული, მკაფიოდ განსაზღვრული და ლეგიტიმური მიზნებისთვის. დაუშვებელია მონაცემთა შემდგომი დამუშავება სხვა, მონაცემთა დამუშავების თავდაპირველ მიზანთან შეუთავსებელი მიზნით.

თუ მონაცემები უნდა დამუშავდეს მათი შეგროვების/მოპოვების მიზნისგან განსხვავებული მიზნით და დამუშავება მონაცემთა სუბიექტის თანხმობით ან კანონის საფუძველზე არ ხორციელდება, მონაცემთა შეგროვების/მოპოვების მიზნისგან განსხვავებული მიზნით მონაცემთა დამუშავების საკითხის გადაწყვეტისას დამუშავებისთვის პასუხისმგებელმა პირმა უნდა გაითვალისწინოს შემდეგი გარემოებები:

- არსებობს თუ არა მონაცემთა შეგროვების/მოპოვების თავდაპირველ მიზანსა და შემდგომ მიზანს შორის კავშირი;

- მონაცემთა შეგროვებისას/მოპოვებისას დამუშავებისთვის პასუხისმგებელ პირსა და მონაცემთა სუბიექტს შორის არსებული ურთიერთობის ხასიათი;

- აქვს თუ არა მონაცემთა სუბიექტს მის შესახებ მონაცემთა შემდგომი დამუშავების გონივრული მოლოდინი;

- ხორციელდება თუ არა განსაკუთრებული კატეგორიის მონაცემთა დამუშავება;

- მონაცემთა სუბიექტისთვის შესაძლო შედეგები, რომლებიც შეიძლება თან ახლდეს მონაცემთა შემდგომ დამუშავებას;

- მონაცემთა ტექნიკური და ორგანიზაციული უსაფრთხოების ზომების არსებობა.

დ) პერსონალური მონაცემების დამუშავების პროპორციულობის პრინციპი

პერსონალური მონაცემები უნდა დამუშავდეს მხოლოდ იმ მოცულობით, რომელიც აუცილებელია შესაბამისი ლეგიტიმური მიზნის მისაღწევად. მონაცემები იმ მიზნის თანაზომიერი უნდა იყოს, რომლის მისაღწევადაც ისინი მუშავდება.

ზემოაღნიშნულიდან გამომდინარე, კომპანია ამუშავებს პერსონალურ მონაცემებს გონივრულად, მხოლოდ იმ მოცულობით, რაც აუცილებელია შესაბამისი დამუშავების მიზნისთვის.

პერსონალური მონაცემების დამუშავებამდე კომპანია, მისი შესაბამისი განყოფილებების (მაგ. მარკეტინგის დეპარტამენტის) მიერ, მონაცემთა დაცვის ოფიცრის თანხმობით, განსაზღვრავს არის თუ არა, და რამდენად საჭიროა პერსონალური მონაცემების დამუშავება იმ მიზნის მისაღწევად, რისთვისაც შეგროვდა ეს მონაცემები.

ე) კანონიერი შენახვის ვადის გასვლის შემდეგ მონაცემთა წაშლის პრინციპი

მონაცემები შეიძლება შენახულ იქნეს მხოლოდ იმ ვადით, რომელიც აუცილებელია მონაცემთა დამუშავების შესაბამისი ლეგიტიმური მიზნის მისაღწევად. იმ მიზნის მიღწევის შემდეგ, რომლისთვისაც მუშავდება მონაცემები, ისინი უნდა წაიშალოს, განადგურდეს ან შენახული უნდა იქნეს დეპერსონალიზებული ფორმით, გარდა იმ შემთხვევისა, თუ მონაცემთა დამუშავება განსაზღვრულია კანონით ან/და კანონის შესაბამისად გამოცემული კანონქვემდებარე ნორმატიული აქტით და მონაცემთა შენახვა აუცილებელი და პროპორციული ზომაა დემოკრატიულ საზოგადოებაში აღმატებული ინტერესების დასაცავად.

რაც შეეხება პერსონალური მონაცემების დაარქივების საკითხს, ისინი უნდა ინახებოდეს კომპანიის სისტემებში დამუშავების ლეგიტიმური მიზნების განსახორციელებლად, დამუშავების მიზნისთვის საჭირო დროით ან მოქმედი კანონმდებლობით გათვალისწინებული პერიოდით, რომელიც პერსონალური მონაცემების თითოეული კატეგორიისთვის ცალ-ცალკე არის განსაზღვრული. შენახვის ვადა: თანამშრომლების შემთხვევაში 5 წელი, პარტნიორებისა და მომხმარებლების შემთხვევაში 15 წელი.

მაგალითად, რაც შეეხება მონაცემთა სუბიექტების ვიდეომასალას მიღებული მაკონტროლებლის ლოკაციებიდან, ვიდეომეთვალყურეობის სისტემის საშუალებით მიღებული მონაცემები ინახება დამუშავების მიზნისთვის საჭირო ვადის პროპორციულად, მაგრამ არაუმეტეს 30 დღისა, რის შემდეგაც ისინი უნდა განადგურდეს (წაიშალოს). გამონაკლისის სახით, მაგალითად, კანონით პირდაპირ რეგულირებულ ან სრულიად გამართლებულ შემთხვევებში (მაგ. უსაფრთხოების ინციდენტის შემთხვევა), ზემოაღნიშნული ვადა შეიძლება გაგრძელდეს კანონით აუცილებელი და დაშვებული ვადით და მონაცემთა დაცვის ოფიცრის თანხმობის საფუძველზე.

კომპანიამ უნდა შეინახოს კლიენტის/პოტენციური კლიენტების/თანამშრომლების/ბიზნეს პარტნიორების მიერ გამოხატული თანხმობის დამადასტურებელი საბუთი, თუ მათი პერსონალური მონაცემების დამუშავება ხდება ასეთი თანხმობით.

პერსონალური მონაცემები არ უნდა ინახებოდეს იმაზე მეტი ხნით, ვიდრე საჭიროა ან დაწესებულია პერსონალური მონაცემების დამუშავების მიზნებით. მონაცემთა შენახვის ვადის გაგრძელება მოხდება მხოლოდ მონაცემთა დაცვის ოფიცრის თანხმობით.

ლეგიტიმური დამუშავებისა და შენახვის მიზნების დასრულების და პერსონალური მონაცემების შემცველი მონაცემების/დოკუმენტების არქივის კანონიერი ვადის გასვლის შემდეგ, თუ მონაცემთა სუბიექტი არ დათანხმდა შემდგომ დამუშავებაზე და მასზე არ ვრცელდება მონაცემთა დაცვის კანონმდებლობით გათვალისწინებული არცერთი გამონაკლისი, განხორციელდება შემდეგი ქმედება:

- პერსონალური მონაცემები უნდა წაიშალოს ჩანაწერებიდან/IT აპლიკაციების სისტემებიდან ან

- უნდა განხორციელდეს ჩანაწერებში/IT აპლიკაციების სისტემებში არსებული პერსონალური მონაცემების დეპერსონალიზაცია, რაც ნიშნავს იმას, რომ ისინი უნდა გარდაიქმნას ანონიმურ მონაცემებად, საიდანაც შეუძლებელი იქნება კონკრეტული მონაცემთა სუბიექტის ვინაობის იდენტიფიცირება;

- ბეჭდურ დოკუმენტებზე არსებული მონაცემები უნდა განადგურდეს საიდუმლო დოკუმენტებისთვის (მაგ., კონფიდენციალური/შეზღუდული დოკუმენტების) განკუთვნილი სპეციალური დამქუცმაცებლების გამოყენებით.

ვ) პერსონალური მონაცემების დამუშავების სიზუსტის პრინციპი

პერსონალური მონაცემები უნდა იყოს ზუსტი და, საჭიროების შემთხვევაში, განახლებული. კომპანია მიიღებს ყველა საჭირო ზომას, რათა დარწმუნდეს, რომ ნებისმიერი პერსონალური მონაცემი, რომელიც არაზუსტია, დაუყოვნებლივ წაიშალოს ან ჩასწორდეს, დამუშავების ლეგიტიმური მიზნის შესაბამისად.

ზ) პერსონალური მონაცემების კონფიდენციალურობის პრინციპი და მონაცემთა უსაფრთხოება

კომპანიამ უნდა მიიღოს ყველა ტექნიკური და ორგანიზაციული ზომა, რომელიც საჭიროა პერსონალური მონაცემების ადეკვატური უსაფრთხოების უზრუნველსაყოფად, რათა თავიდან აიცილოს არასანქცირებული/არაუფლებამოსილი წვდომა, უნებართვო ან უკანონო დამუშავება, არაავტორიზებული გამჟღავნება, მათ შორის მათი შემთხვევითი დაკარგვა, განადგურება ან დაზიანება.

კომპანიაში არსებობს დოკუმენტირებული ავტორიზაციისა და დამტკიცების პროცესი ნებისმიერ ინფორმაციაზე, რომელიც ითვლება პერსონალურად, წვდომის მინიჭების, შენარჩუნებისა და წაშლისთვის. ამიტომ, თანამშრომლისთვის წვდომის უფლების მინიჭების მიზნით, ადამიანური რესურსების დეპარტამენტი უგზავნის მოთხოვნას IT დეპარტამენტს ახალი თანამშრომლის დასაქმებისთანავე, მისი სამუშაო აღწერილობიდან გამომდინარე. წვდომა მიენიჭება თანამშრომლის უშუალო ხელმძღვანელის თანხმობის საფუძველზე.

არსებული თანამშრომლისთვის მოთხოვნა IT სისტემებზე წვდომის შესახებ უნდა შეასრულოს უშუალო უფროსმა, სამუშაოს აღწერილობიდან გამომდინარე, ხოლო წვდომას ანიჭებს IT დეპარტამენტი.

თ) პასუხისმგებლობის პრინციპი პერსონალური მონაცემების დამუშავებისას

კომპანია პასუხისმგებელია მონაცემთა დამუშავებისას ზემოთ ჩამოთვლილი პრინციპების დაცვისთვის და მან უნდა შეძლოს მათთან შესაბამისობის დასაბუთება.

ყველა ტექნიკური და ორგანიზაციული ღონისძიება უნდა იქნას გამოყენებული, რათა თავიდან იქნას აცილებული პერსონალურ მონაცემებზე არასანქცირებული წვდომა, არაავტორიზებული და უკანონო დამუშავება, პერსონალური მონაცემების უნებართვო გამჟღავნება და განადგურება, შეცვლა ან შემთხვევითი დაკარგვა.

11. დამუშავებული მონაცემთა სუბიექტების უფლებები

კომპანია ამუშავებს ფიზიკური პირების, როგორიცაა თანამშრომლები, კლიენტები/პოტენციური კლიენტები, კლიენტების/პოტენციური კლიენტების კანონიერი წარმომადგენლები, პარტნიორები, კონტრაქტორები, მესამე მხარეები, ბიზნეს პარტნიორები, მათი წარმომადგენლები და სხვა სუბიექტები (მონაცემთა სუბიექტები) პერსონალურ მონაცემებს.

მონაცემთა სუბიექტების უფლებები, სხვა ყველაფერთან ერთად, მოიცავს შემდეგს:

ა) მონაცემთა დამუშავების შესახებ ინფორმაციის და ასლის მიღების უფლება:

მონაცემთა სუბიექტს აქვს უფლება იყოს ინფორმირებული პერსონალური მონაცემების შეგროვებისა და გამოყენების შესახებ. ეს ნიშნავს, რომ მოთხოვნისამებრ, კომპანიამ უნდა მიაწოდოს დეტალები იმის თაობაზე, თუ რომელ პერსონალურ მონაცემებს ამუშავებს, რა მიზნით და საფუძვლით, როგორ აგროვებს, რა ვადით ინახავს, ვის გადასცემს მონაცემთა სუბიექტის პერსონალურ მონაცემებს და ა.შ. მონაცემთა სუბიექტს, ასევე უფლება აქვს, მიიღოს კომპანიისგან იმ პერსონალური მონაცემების ასლი, რომელიც მუშავდება მოქმედი კანონმდებლობის შესაბამისად.

მონაცემთა სუბიექტს აქვს უფლება მიიღოს შეტყობინება მისი პერსონალური მონაცემების დამუშავების შესახებ, დამუშავების მიზანსა და სამართლებრივი საფუძვლების, დამუშავების ვადის, დამუშავებისთვის პასუხისმგებელი პირისა და დამუშავებაზე უფლებამოსილი პირის შესახებ; დამუშავებისთვის პასუხისმგებელი პირის მიერ მონაცემების დამუშავების კანონიერი ინტერესის შესახებ; წარმოადგენს თუ არა პერსონალური მონაცემების მიწოდება კანონიერ ან სახელშეკრულებო ვალდებულებას მოვალეობების შესასრულებლად; ვალდებულია თუ არა მონაცემთა სუბიექტი მიაწოდოს პერსონალური მონაცემები და რა შესაძლო შედეგს გამოიწვევს ამ მოვალეობის შეუსრულებლობა; პერსონალური მონაცემების შენახვის ვადა ან, თუ ამის წინასწარ განსაზღვრა შეუძლებელია, ინფორმაცია იმ კრიტერიუმების შესახებ, რომლებიც გამოიყენება ამ ვადის დასადგენად.

მონაცემთა სუბიექტს აქვს უფლება ჰქონდეს ინფორმაცია მონაცემთა მიმღების ან მონაცემთა მიმღებთა კატეგორიების შესახებ;

ბ) მონაცემთა გასწორების, განახლებისა და შევსების უფლება:

თუ კომპანიის მიერ დამუშავებული მონაცემები არასწორი, არასრული ან არაზუსტია, მონაცემთა სუბიექტს შეუძლია მოითხოვოს მონაცემების გასწორება, განახლება ან/და შევსება და კომპანიას მიაწოდოს ამისათვის აუცილებელი ინფორმაცია.

მონაცემთა დამუშავების შეწყვეტის, წაშლის ან განადგურების უფლება:

მონაცემთა სუბიექტს უფლება აქვს კომპანიას მოსთხოვოს მის შესახებ მონაცემთა დამუშავების (მათ შორის, პროფაილინგის) შეწყვეტა, წაშლა ან განადგურება.

გ) მონაცემთა დაბლოკვის უფლება:

მონაცემთა სუბიექტს შეუძლია მოითხოვოს მონაცემთა დაბლოკვა (დამუშავების შეზღუდვა), როდესაც პერსონალური მონაცემების სიზუსტე სადავოა მონაცემთა სუბიექტის მხრიდან ან ითხოვს მონაცემთა დამუშავების შეწყვეტას, წაშლას ან განადგურებას, იმ პერიოდის განმავლობაში, რომელიც შესაძლებლობას მისცემს კომპანიას გადაამოწმოს პერსონალური მონაცემების სიზუსტე და განიხილოს მოთხოვნა; როდესაც დამუშავება უკანონოა, თუმცა, მონაცემთა სუბიექტი უარს აცხადებს პერსონალური მონაცემების წაშლაზე და, სანაცვლოდ, ითხოვს მონაცემების დაბლოკვას; როდესაც არსებობს მონაცემების მტკიცებულებად გამოყენების მიზნით შენახვის აუცილებლობა.

დ) მონაცემთა გადატანის უფლება:

მონაცემთა სუბიექტს აქვს უფლება მოითხოვოს სტრუქტურიზებული, საზოგადოდ გამოყენებადი და მანქანურად წაკითხვადი ფორმატით მიიღოს მის მიერ მიწოდებული მონაცემები ან მოითხოვოს ამ მონაცემთა სხვა დამუშავებისთვის პასუხისმგებელი პირისთვის გადაცემა. კომპანია უფლებამოსილია უარი განაცხადოს მონაცემთა სუბიექტის მოთხოვნის დაკმაყოფილებაზე, თუ აღნიშნული ტექნიკურად შეუძლებელია.

მონაცემთა გადაცემის უფლება (მათთან დაკავშირებული და მაკონტროლებლისთვის მიწოდებული სტრუქტურირებული ფორმატით, უკვე გამოყენებული და ავტომატურად წაკითხული, და ასეთი მონაცემების სხვა მაკონტროლებელთან გაგზავნის უფლება) თუ დამუშავება ეფუძნება მონაცემთა სუბიექტის თანხმობას ან შეთანხმებას და დამუშავება ხდება ავტომატური გზით:

ამ შემთხვევაში, პერსონალური მონაცემების გადაცემა უნდა იყოს დაცული და უსაფრთხო ისეთი ტექნიკური პროცედურების განხორციელებით, რომლებიც მიზნად ისახავს ადეკვატურად და უსაფრთხოდ უზრუნველყოფილ იქნეს გადაცემა, ასევე შენარჩუნდეს მონაცემთა კონფიდენციალურობა და მთლიანობა. გადაადგილების უფლების გამოყენება მიანს არ უნდა აყენებდეს მონაცემთა სუბიექტის სხვა უფლებებს (მაგ. წვდომის უფლებას).

მონაცემთა სუბიექტის მიერ გადაცემის უფლების განხორციელება არ გულისხმობს კომპანიის მოვალეობას, წაშალოს მონაცემთა სუბიექტის პერსონალური მონაცემები მაშინაც კი, თუ, მაგალითად, მონაცემთა სუბიექტი აღარ არის კომპანიის კლიენტი. ამ შემთხვევაში მონაცემთა შენახვის ვადა დგინდება სხვა კონკრეტული სამართლებრივი საფუძვლების გათვალისწინებით.

ე) უფლება კომპანიისგან წერილობითი განმარტების შესახებ:

მოთხოვნილი ინფორმაცია კომპანიის მიერ დამუშავებულ პერსონალურ მონაცემებთან დაკავშირებით; (დათარიღებული და ხელმოწერილი) განცხადების წარდგენის შემდეგ, განაცხადის შეტანიდან 10 დღის ვადაში, ასევე, იგივე ვადაში მიიღოს კომპანიის გადაწყვეტილება იმ მოთხოვნებთან დაკავშირებით, რომლითაც ხორციელდებოდა ყველა სხვა ზემოაღნიშნული კანონიერი უფლება.

ვ) ავტომატიზებულ ინდივიდუალურ გადაწყვეტილებასთან დაკავშირებული უფლებები:

მონაცემთა სუბიექტს აქვს უფლება არ დაექვემდებაროს მხოლოდ ავტომატიზებულად, მათ შორის, პროფაილინგის საფუძველზე, მიღებულ გადაწყვეტილებას, გარდა იმ შემთხვევისა, როდესაც პროფაილინგის საფუძველზე გადაწყვეტილების მიღება: (ა) ეფუძნება მონაცემთა სუბიექტის აშკარად გამოხატულ თანხმობას; (ბ)აუცილებელია მხარეთა შორის ხელშეკრულების დასადებად ან ხელშეკრულების შესასრულებლად; (გ) გათვალისწინებულია კანონით ან კანონის საფუძველზე დელეგირებული უფლებამოსილების ფარგლებში გამოცემული კანონქვემდებარე ნორმატიული აქტით.

მონაცემთა სუბიექტს აქვს უფლება მიიღოს შეტყობინება გადაწყვეტილების ავტომატიზებული პროცესის არსებობის შესახებ, პროფაილინგის ჩათვლით, ასევე, როგორც მინიმუმ, მიიღოს ინფორმაცია აღნიშნული სისტემის მუშაობის ლოგიკის, მონაცემთა სუბიექტისთვის ამგვარი დამუშავების მოსალოდნელი შედეგებისა და მნიშვნელობის შესახებ.

მონაცემთა სუბიექტის აქვს უფლება არ გამოვიდეს პროფაილინგის ობიექტის როლში (მონაცემთა ავტომატიზირებული დამუშავება რომელიმე ფიზიკურ პირთან დაკავშირებული პერსონალური საკითხების შეფასებით, განსაკუთრებით მონაცემთა სუბიექტის სამსახურთან, ფინანსურ მდგომარეობასთან, ჯანმრთელობასთან, პირად პრეფერენციებთან ან ინტერესებთან, სანდოობასთან ან ქცევასთან, მდებარეობასთან ან მოგზაურობებთან დაკავშირებული გარკვეული საკითხების განხილვის ან განჭვრეტის მიზნით) როდესაც ეს იწვევს სამართლებრივ შედეგს მონაცემთა სუბიექტზე ან ანალოგიურად და მნიშვნელოვნად ახდენს მასზე გავლენას.

ნებისმიერ შემთხვევაში, პროფაილინგი უნდა იყოს ადეკვატური გარანტიების ობიექტი (კონკრეტული შეტყობინება მონაცემთა სუბიექტისთვის და მათი პროცესში ჩარევის უფლება; აზრის გამოხატვის უფლება; გარკვეული შეფასების შემდეგ მიღებული გადაწყვეტილების განმარტების მიღების უფლება; ასევე გადაწყვეტილების გასაჩივრების უფლება).

პროფაილინგი არ უნდა ეხებოდეს ბავშვებს.

კომპანიამ, თუ ის აპირებს პროფაილინგის გამოყენებას, უნდა მიიღოს ადეკვატური ტექნიკური და ორგანიზაციული ზომები, რათა, კერძოდ, უზრუნველყოს პერსონალური მონაცემების უზუსტობის გამომწვევი ფაქტორების გამოსწორება და მინიმუმამდე დაიყვანოს შეცდომების რისკი, ისე დაიცვას პერსონალური მონაცემები, რომ გაითვალისწინოს პოტენციური საფრთხეები, რომლებიც მონაცემთა სუბიექტის ინტერესებთან და უფლებებთანაა, ასევე დაიწყოს ზემოქმედების შემოწმების განხილვა.

ზ) თანხმობის გამოხმობის უფლება:

მონაცემთა სუბიექტს თანხმობის გამოხმობა შეუძლია ნებისმიერ დროს, თუ აღნიშნული არ ეწინააღმდეგება კანონმდებლობის მოთხოვნებს. თანხმობის გამოხმობა არ იწვევს თანხმობის გამოხმობამდე და თანხმობის ფარგლებში წარმოშობილი სამართლებრივი შედეგების გაუქმებას. მონაცემთა სუბიექტს აქვს უფლება, მოითხოვოს ინფორმაცია თანხმობის გამოხმობის შესაძლო შედეგების შესახებ.

თ) გასაჩივრების უფლება:

მონაცემთა სუბიექტს აქვს უფლება მიმართოს საქართველოს პერსონალურ მონაცემთა დაცვის სამსახურს ან/და სასამართლოს. კომპანია იყენებს ადეკვატურ სტანდარტებს, რათა უზრუნველყოს ზემოაღნიშნული უფლებების დაცვა.

კომპანიის თანამშრომლებმა და პარტნიორებმა უნდა გამოიყენონ ყველა ძალისხმევა, რათა არ მოხდეს პერსონალური მონაცემების შეგროვება და დამუშავება, გარდა აბსოლუტურად აუცილებელი დამტკიცებული კანონიერი მიზნებისთვის.

მონაცემთა სუბიექტებს შეუძლიათ გამოიყენონ ეს უფლებები წინამდებარე პოლიტიკის შესაბამისი ნაწილის მიხედვით განაცხადის წარდგენით და ასეთი განაცხადები დამუშავებული უნდა იქნეს მონაცემთა დაცვის ოფიცრის მიერ, მონაცემთა სუბიექტების უფლებების განხორციელების პოლიტიკის შესაბამისად.

12. კომპანიის მიერ განხორციელებული ტექნიკური და ორგანიზაციული ღონისძიებები, რათა უზრუნველყოს მონაცემთა „კონფიდენციალურობა სისტემურად დაგეგმარებისას“ (Privacy by Design) და “კონფიდენციალურობა პირველადი პარამეტრების დონეზე” (Privacy by Default)

კომპანია იღებს ვალდებულებას დაიცვას მონაცემთა სუბიექტების პერსონალური მონაცემები, რომლებიც დამუშავდა როგორც მათთან, ასევე ნებისმიერ სხვა ფიზიკურ პირთან ურთიერთქმედების შედეგად.

დამუშავების ბუნების, მოცულობის, წყობისა და მიზნების გათვალისწინებით, ასევე მონაცემთა სუბიექტების უფლებებისა და თავისუფლებების გათვალისწინებით, კომპანია ახორციელებს ადეკვატურ ტექნიკურ და ორგანიზაციულ ზომებს, რათა უზრუნველყოს და შეძლოს იმის დემონსტრირება, რომ პერსონალური მონაცემების დამუშავება ხდება საქართველოს მოქმედი კანონმდებლობის შესაბამისად. ასეთი ზომები პერიოდულად განიხილება მონაცემთა დაცვის ოფიცრის, IT დირექტორატის, შიდა კონტროლის სასამართლო ექსპერტიზისა და უსაფრთხოების, შესაბამისობისა და ბიზნეს ინფორმაციის სისტემის მფლობელის მიერ და უნდა განახლდეს მიმდინარე მოქმედი მოთხოვნების შესაბამისად.

იმის მიხედვით, თუ რა გავლენა შეიძლება მოახდინოს პერსონალური მონაცემების დამუშავების ასეთმა ოპერაციამ, კომპანია იღებს მონაცემთა დაცვისა და უსაფრთხოების სპეციალურ ზომებს და კომპანიის თანამშრომლებმა/პარტნიორებმა უნდა უზრუნველყონ უსაფრთხოების ასეთი მოთხოვნების ეფექტურად დაცვა მათი პროფესიული საქმიანობისას. ასეთი დაცვის ზომები პერიოდულად უნდა შემოწმდეს შესაბამისი მოვალეობების მქონე პირების მიერ (მაგ. ინფორმაციის უსაფრთხოება) და უნდა მოხდეს მათი ეფექტურობის მონიტორინგი და შემოწმება.

ამიტომ, დამუშავების ტიპის, მოცულობის, წყობისა და მიზნების გათვალისწინებით, იმ შემთხვევაში, თუ კონკრეტული მონაცემების ტიპის დამუშავება, განსაკუთრებით ახალი ტექნოლოგიების გამოყენებით, გამოიწვევს მონაცემთა სუბიექტების უფლებებისა და თავისუფლებების მაღალ რისკს, კომპანიის თანამშრომლებმა, რომლებიც პასუხისმგებელნი არიან პერსონალური მონაცემების დამუშავებაზე თავიანთი მოვალეობების შესაბამისად, დამუშავებამდე უნდა შეაფასონ პერსონალური მონაცემების დაცვაზე გავლენა. ერთიანი შეფასება შეიძლება გამოყენებულ იქნეს მსგავსი დამუშავების ოპერაციების ერთობლიობაზე, რომელიც შეიცავს ანალოგიურად მაღალ რისკებს. ასეთ შემთხვევებში მიზანშეწონილია მოითხოვოთ მონაცემთა დაცვის ოფიცრის აზრი.

კომპანიის თანამშრომლებმა უნდა უზრუნველყონ მონაცემთა დაცვის ოფიცრისგან მიღებული რეკომენდაციების შესრულება კომპანიის სახელით განხორციელებული მონაცემთა დამუშავების ოპერაციების დროს.

ასევე გასათვალისწინებელია, რომ მონაცემთა დამუშავების ოპერაციებისთვის, რომლებიც შეიცავს მონაცემთა სუბიექტების ფუნდამენტურ უფლებებთან და თავისუფლებებთან დაკავშირებულ მაღალ რისკს, კომპანიამ უნდა დაადგინოს ასეთი რისკები და შეაფასოს ისინი პერსონალური მონაცემებთა დაცვაზე ზეგავლენის შეფასების გზით - აცნობოს აღნიშნული ინფორმაცია პერსონალური მონაცემების დაცვის ოფიცერს. ასეთი მიმოხილვის დროს განსაკუთრებით უნდა შეფასდეს მსგავსი რისკის წარმოშობა, ტიპი, სპეციფიკა და სერიოზულობა.

თუ მონაცემთა დაცვაზე ზეგავლენის შეფასების პროცესში, ტექნიკური და ორგანიზაციული ღონისძიებების განხორციელების შემდეგაც კი აღმოჩნდება, რომ რისკი რჩება მაღალ დონეზე, კომპანიამ ასევე წინასწარ უნდა მიმართოს პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს.

ამ მოვალეობების შესასრულებლად, დამუშავებაში ჩართულმა ან მონაწილე დეპარტამენტ(-ებ-)მა უნდა დანიშნოს პირი, რომელიც პასუხისმგებელი იქნება მონაცემთა დაცვაზე ზეგავლენის

შეფასებაზე და უნდა დარწმუნდეს, რომ ამ პირს გააჩნია სათანადო ცოდნა ასეთი განხილვის განსახორციელებლად შიდა წესების და მარეგულირებელი კანონის დაცვით.

ტექნიკური და ორგანიზაციული ზომების ფარგლებში, კომპანიის ნებისმიერმა თანამშრომელმა, რომელიც პასუხისმგებელია IT აღჭურვილობასა და პერსონალური მონაცემების დაცვასა და უსაფრთხოებაზე, ყოველთვის უნდა გაითვალისწინოს პერსონალური მონაცემების დაცვის ადეკვატური კონტროლის აღსრულება, მათ შორის, შეუზღუდავად, თანამშრომლების/პარტნიორების უსაფრთხო და კონტროლირებადი წვდომა პერსონალურ მონაცემებზე, ასევე კომპანიის მონაცემთა ბაზებზე, IT სისტემებსა თუ აპლიკაციებზე.

ა) მონაცემებზე წვდომის ავტორიზაციასთან დაკავშირებული საკითხები

პერსონალური მონაცემები უნდა ინახებოდეს დაცულ გარემოში, ხოლო წვდომა უნდა შემოიფარგლოს მხოლოდ იმ თანამშრომლებითა და პარტნიორებით, რომლებსაც აქვთ წვდომის უფლება კომპანიის სისტემებსა და აპლიკაციებზე.

მხოლოდ ის პერსონალი, რომელიც საჭიროებს პერსონალურ მონაცემებზე წვდომას სამუშაო ამოცანების შესასრულებლად, უფლებამოსილია იქონიოს წვდობა კომპანიის მონაცემთა ბაზებზე, სისტემებზე („ცოდნის საჭიროების“ პრინციპი).

კომპანიის თანამშრომლებმა და პარტნიორებმა, რომლებმაც მიიღეს მონაცემთა ბაზებზე წვდომის ავტორიზაცია ან ფლობენ ადმინისტრაციულ უფლებებს მათზე, ისევე როგორც IT სისტემებსა და აპლიკაციებზე, ასეთის არსებობის შემთხვევაში, რომლებზეც ინახება ეს მონაცემთა ბაზები, რეგულარულად უნდა მიიღონ მონაწილეობა ტრენინგ-პროგრამებში პერსონალური მონაცემების დაცვისა და უსაფრთხოების საკითხებზე.

ბ) პერსონალურ მონაცემთა ბაზებისთვის ავტორიზებული პერსონალის ავთენტიფიკაცია

პერსონალური მონაცემების შემცველ/შემნახველ სისტემებსა და აპლიკაციებზე წვდომა შეიძლება მიენიჭოს მხოლოდ ავტორიზებული პირის იდენტიფიცირებისა და ავტორიზაციის შემდეგ, მომხმარებლის სახელისა და პაროლის საფუძველზე. თუ პაროლი წარუმატებლად იქნა შეყვანილი, ან არ არსებობს წვდომის ავტორიზაცია, პერსონალური მონაცემების შემცველ ჩანაწერებზე წვდომა უნდა იყოს აკრძალული.

კომპანიის თანამშრომლებმა/პარტნიორებმა არ უნდა გაუმჟღავნონ მომხმარებლის სახელი და პაროლი სხვას. თუ ისინი ეჭვობენ, რომ მესამე მხარემ აღმოაჩინა მათი პაროლი ასეთ ჩანაწერებზე წვდომისთვის, დაუყოვნებლივ უნდა განახორციელონ პაროლის შეცვლა. ასეთ შემთხვევაში, თანამშრომელმა უნდა აცნობოს და გაიაროს კონსულტაცია მონაცემთა დაცვის ოფიცერთან.

კომპანიის სისტემებსა და აპლიკაციებში საიდენტიფიკაციო პაროლები მომხმარებელმა პერიოდულად უნდა შეცვალოს, როგორც კი ის მიიღებს ავტომატურ შეტყობინებას პაროლის ვადის გასვლის შესახებ.

გ) ავტორიზებული მომხმარებლების სიის განახლება

მონაცემთა ბაზებზე წვდომის უფლების მქონე პერსონალის სია რეგულარულად უნდა განახლდეს, რითაც უზრუნველყოფილი იქნება ამ სიის მინიმუმამდე დაყვანა, „ცოდნის აუცილებლობის“ პრინციპის გამოყენებით.

ნებისმიერ თანამშრომელს/პარტნიორს, რომელიც ტოვებს კომპანიას ან გადადის კომპანიის სხვა განყოფილებაში, გაუუქმდება ჩანაწერების სისტემებზე/IT აპლიკაციებზე წვდომის უფლება იმ შემთხვევაში, თუ ის აღარ არის საჭირო სამუშაო ამოცანების შესასრულებლად.

დ) პერსონალური მონაცემების გადაცემა

პერსონალური მონაცემები უნდა იყოს გადაცემული მხოლოდ სრული უსაფრთხოებით; ნებისმიერი პერსონალური მონაცემების გადაცემა კომპანიის გარეთ, რომელიც არ ექვემდებარება მონაცემთა დაცვის ოფიცრის მიერ დამტკიცებულ პროცედურებს უნდა განხორციელდეს მხოლოდ მისი წინასწარი თანხმობით. აღნიშნული შესაძლებელია განხორციელდეს საკანონმდებლო მოთხოვნების შესაბამისად.

კომპანიამ უნდა უზრუნველყოს უსაფრთხოების ზომები პერსონალური მონაცემების გადაცემის შემთხვევაში, მათ შორის ტექნიკური აპლიკაციებითა და გადაწყვეტილებებით, რათა თავიდან

იქნას აცილებული მონაცემების დაკარგვა, და უზრუნველყოფილ იქნეს მონაცემთა მთლიანობისა და კონფიდენციალურობის დაცვის ვალდებულება, GDPR-ის მოთხოვნების შესაბამისად.

ე) პერსონალური მონაცემების უსაფრთხო შენახვა

პერსონალური მონაცემები უნდა ინახებოდეს დაცულ გარემოში, რომელიც მოიცავს ლოგიკურ (ავტორიზაცია, ავთენტიფიკაცია, დაშიფვრა და წვდომის პაროლი), და ასევე ფიზიკურ (შეზღუდული წვდომა მონაცემთა შენახვის სერვერზე და აღჭურვილობაზე) უსაფრთხოებას. ასევე, შესაბამისი ყურადღება ექცევა უძრავი ქონების ფიზიკურ უსაფრთხოებას, სადაც კომპანია ახორციელებს თავის საქმიანობას და ინახავს პერსონალური მონაცემების შემცველ დოკუმენტებს.

ვ) სარეზერვო ასლების შექმნა

სარეზერვო ასლები უნდა კეთდებოდეს დისკზე, ყოველდღიურად, 21-დღიანი შენახვის ვადით. პერსონალური მონაცემების შემცველი მონაცემთა ბაზების/აპლიკაციების აღდგენა უნდა ხდებოდეს მონაცემთა დაცვის ოფიცრის თანდასწრებით („4 თვალის პრინციპი“) და უნდა იყოს დოკუმენტირებული.

სარეზერვო ასლებზე წვდომა კონტროლირებადი პროცესია, რომელიც ექვემდებარება შიდა აუდიტს.

ზ) მონაცემთა თანადამმუშავებელი

კომპანიის მიერ პერსონალური მონაცემების დამუშავების შემთხვევაში კომპანიამ უნდა უზრუნველყოს, რომ მათ ასევე განახორციელონ ადეკვატური ტექნიკური და ორგანიზაციული ზომები მონაცემთა უსაფრთხოების სათანადო დონის უზრუნველსაყოფად. მათ შორის, მათთან გაფორმებული ხელშეკრულებების ფარგლებში უნდა იყოს ჩადებული ისეთი პუნქტები, რომლებიც დაკავშირებულია მონაცემთა უსაფრთხოების მინიმალურ მოთხოვნებთან გამოვლენილი ადეკვატური ტექნიკური და ორგანიზაციული ზომების მიმართებაში.

ასეთი ზომები შეიძლება შეიცავდეს, თუმცა, არ შემოიფარგლება:

ა) ღონისძიებებს, რომლებიც ეხება პერსონალური მონაცემების რაოდენობის შემცირებას ფილტრაციისა და წაშლის გზით, სენსიტუირობის შემცირება გარდაქმნის გზით, მონაცემთა დაგროვების შემცირება, წვდომის შეზღუდვა, მონაცემთა ტიპის იდენტიფიკაციის შესაძლებლობის შემცირება კომპანიის ინსტრუქციების შესაბამისად.

ბ) მიკვლევადობასთან დაკავშირებულ ღონისძიებებს – მიკვლევადობისა და ჟურნალის მართვის პოლიტიკის არსებობა მისი შენარჩუნებით მონაცემთა დამუშავების მთელი ოპერაციების განმავლობაში, მაგრამ არანაკლებ 2 წლის განმავლობაში.

გ) ღონისძიებებს, რომლებიც ეხება დამმუშავებლებსა და ქვეკონტრაქტორებს შორის ურთიერთობებს – მონაცემთა უნებართვო წვდომის რისკის შემცირების პოლიტიკისა და პროცესების არსებობა.

დ) ზომებს დამმუშავებლის მიერ პერსონალური მონაცემების წაშლის, დეპერსონალიზაციის ან/და დაბრუნების მიზნით დამუშავების დასრულების შემდეგ მაკონტროლებლის სახელით, გარდა შემთხვევებისა, როდესაც არსებობს კანონიერი მოთხოვნა ასეთი პერსონალური მონაცემების შენახვის შესახებ მისი დამუშავების დასრულების შემდეგაც კი.

13. დამუშავების უსაფრთხოება. მონაცემთა დაცვა და უსაფრთხოების ინციდენტები

კომპანიამ უნდა განახორციელოს მათი ბიზნესისთვის დამახასიათებელი ტექნიკური და ორგანიზაციული ღონისძიებები, მათ შორის, საჭიროების შემთხვევაში:

- ჩანაწერების სისტემებისა და IT აპლიკაციების, სადაც ინახება პერსონალური მონაცემები, უწყვეტი კონფიდენციალურობის, მთლიანობის, ხელმისაწვდომობისა და მდგრადობის უზრუნველყოფა,

- ფიზიკური ან ტექნიკური ინციდენტის შემთხვევაში პერსონალური მონაცემების ხელმისაწვდომობისა და მათზე ხელმისაწვდომობის აღდგენის დროული შესაძლებლობა;

- პერსონალური მონაცემების ფსევდონიმიზაცია და დაშიფვრა ან ასეთი მონაცემების დეპერსონალიზაცია;

- შემოწმების, შეფასების და ტექნიკური და ორგანიზაციული ზომების ეფექტურობის შეფასების პერიოდული პროცესი პერსონალური მონაცემების დამუშავების უსაფრთხოების უზრუნველყოფის მიზნით.

- კომპანიის IT სისტემებზე/აპლიკაციებზე წვდომა მხოლოდ ავტორიზებული, სწორი პაროლის მქონე მომხმარებლებისთვის.

IT სისტემების ნებისმიერი ინციდენტი, რომელიც მნიშვნელოვან გავლენას ახდენს კომპანიის კლიენტების ან მონაცემთა სხვა სუბიექტების პერსონალურ მონაცემებზე, ითვლება მაღალი რისკის ინციდენტად.

პერსონალური მონაცემების უსაფრთხოების ინციდენტის შემთხვევაში, ასევე განიხილება კომპანიის მიერ მიღებული ინფორმაციის უსაფრთხოების პოლიტიკის დებულებები (მათ შორის შესაბამისი დანართები).

პერსონალური მონაცემების უსაფრთხოების ინციდენტების შედეგები მონაცემთა სუბიექტზე (კლიენტზე/სუბიექტზე/დასაქმებულზე) შეიძლება იყოს: ფიზიკური, მატერიალური და მორალური ზიანი, დისკრიმინაცია, პირადი მონაცემების მოპარვა ან თაღლითობა, რეპუტაციის კომპრომეტირება, პროფესიული საიდუმლოების ქვეშ ნაფიცი პირადი მონაცემების კონფიდენციალურობის დაკარგვა, ან რაიმე სხვა მნიშვნელოვანი ან სოციალური უპირატესობა, მათ შორის, მათ პირად მონაცემებზე სრული კონტროლის დაკარგვა.

პირადი მონაცემების უსაფრთხოების ინციდენტების მაგალითები:

- ლეპტოპის ან გარე დისკების, რომლებიც შეიცავს კლიენტების პერსონალურ მონაცემებს, მოპარვა ან დაკარგვა;

- წვდომა იმ კლიენტების პერსონალურ მონაცემებზე, რომლებმაც ისარგებლეს მობილური აპლიკაციის/საიტის საშუალებით რეგისტრაციის მომსახურებით, აპლიკაციაში არსებული მოწყვლადობის გამოყენებით;

- მნიშვნელოვანი ინფორმაციის შემცველი ელექტრონული წერილი, გაგზავნილი სხვა ადრესატთან, ვიდრე თავდაპირველად იყო დაგეგმილი და ა.შ.

- კომპანიის ინტრანეტზე უნებართვო წვდომა;

- პირადი მონაცემების გადაცემა პირადი ელექტრონული ელ-ფოსტის საშუალებით.

თუ IT უსაფრთხოების ინციდენტი გავლენას მოახდენს პერსონალურ მონაცემებზე, კომპანიის თანამშრომლის IT განყოფილებამ, რომელმაც მიიღო ინფორმაცია ასეთი ინციდენტის შესახებ, დაუყოვნებლივ უნდა აცნობოს მონაცემთა დაცვის ოფიცერს, რათა ამ უკანასკნელმა განიხილოს კომპანიის მიერ გადასადგმელი დაუყოვნებელი ნაბიჯები, როგორიცაა პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს ინფორმირება ინციდენტის შესახებ, ინციდენტის აღმოჩენიდან 72 საათის განმავლობაში, იმ შემთხვევაში, თუ არსებობს მონაცემთა სუბიექტების ძირითადი უფლებებისა და თავისუფლებებისთვის მნიშვნელოვანი ზიანის მიყენების საშუალო ან მაღალი რისკი.

მონაცემთა დაცვის ოფიცერი, აგზავნის პერსონალური მონაცემების დამუშავების ზედამხედველობის ორგანოში შეტყობინებას შემდეგი ინფორმაციით:

- ინციდენტის გარემოებების, სახესა და დროის თაობაზე.

- აღწერს პერსონალური მონაცემების უსაფრთხოების დარღვევის ხასიათს, მათ შორის, სადაც ეს შესაძლებელია: მონაცემთა შესაბამისი სუბიექტების კატეგორიებსა და სავარაუდო რაოდენობას, აგრეთვე შესაბამის პერსონალურ მონაცემებზე ჩანაწერების კატეგორიებსა და სავარაუდო რაოდენობას;

- აცნობებს მონაცემთა დაცვის ოფიცრის სახელს და საკონტაქტო მონაცემებს ან სხვა საკონტაქტო პუნქტს, სადაც დამატებითი დეტალების მიღება არის შესაძლებელი;

- აღწერს პერსონალური მონაცემების უსაფრთხოების დარღვევის სავარაუდო შედეგებს;

- აწვდის ინფორმაციას იმის შესახებ ინციდენტის შესახებ შეატყობინოს მონაცემთა სუბიექტს.

- აღწერს ინციდენტის შედეგად დამდგარ სავარაუდო ზიანს, ასევე, კომპანიის მიერ გატარებულ ან შემოთავაზებულ ღონისძიებებს პერსონალური მონაცემების უსაფრთხოების დარღვევის გამოსასწორებლად, მათ შორის, საჭიროების შემთხვევაში, ნებისმიერი პოტენციური ნეგატიური ეფექტის შესამცირებელ ზომებს.

ასევე, ინფორმაცია ნებისმიერი სხვა ტიპის ინციდენტზე, რომელმაც შეიძლება გავლენა იქონიოს კომპანიის მიერ დამუშავებულ პერსონალურ მონაცემებზე, უნდა მიეწოდოს მონაცემთა დაცვის ოფიცერს ან განიხილოს პერსონალური მონაცემების დაცვის კანონმდებლობის შესაბამისად.

ისეთი უსაფრთხოების ინციდენტის დადგომის შემთხვევაში, რომელმაც შეიძლება გამოიწვიოს ფიზიკური პირების უფლებებისა და თავისუფლებების მაღალი რისკიანობა, კომპანიამ, გედმეტი შეფერხების გარეშე, უნდა აცნობოს დაზარალებულ პირს ასეთი ინციდენტისა და შესაბამისი ზეგავლენის შესახებ.

14. ტრენინგი პერსონალური მონაცემების დაცვისა და უსაფრთხოების შესახებ

თანამშრომლებს ტრენინგები უტარდებათ შესაბამისობის, მონაცემთა დაცვის ოფიცრის, ინფორმაციის უსაფრთხოების სამსახურის მიერ პერსონალური მონაცემების დაცვისა და უსაფრთხოების სფეროში პროფესიული ტრენინგების გზით, შიდა/გარე სპეციალიზებული პერსონალის მეშვეობით, პერიოდულად და საჭიროების შემთხვევაში.

თანამშრომლებს არ აქვთ უფლება დაამუშავონ, გაამჟღავნონ, გადასცენ მესამე პირებს, დაუშვან პერსონალურ მონაცემებზე წვდომა ან გამოიყენონ პერსონალური ინფორმაცია ავტორიზებულის გარდა სხვა მიზნით, და სამუშაო ამოცანების კანონიერი შესრულების ფარგლებს გარეთ.

15. შესაბამისობა, დისციპლინარული პროცედურები

პერსონალური მონაცემების კონფიდენციალურობის დაკარგვა ან დარღვევა არის სერიოზული დარღვევა და ამან შეიძლება გამოიწვიოს სასამართლო პროცესის დაწყება კომპანიის წინააღმდეგ. ამიტომ, კომპანიის IT სისტემებში პერსონალური მონაცემების ყველა მომხმარებელი უნდა შეესაბამებოდეს იმ პოლიტიკას და ინსტრუმენტებს, რომლებიც შემოთავაზებულია ამ პოლიტიკის აღსრულებისთვის, ისევე როგორც კომპანიის ინფორმაციის უსაფრთხოების პოლიტიკას.

კომპანიის ყველა თანამშრომელი, კონსულტანტი და კონტრაქტორი უნდა იყოს უშუალოდ ინფორმირებული ამ და დამხმარე პოლიტიკის არსებობის შესახებ, ასევე პრაქტიკის კოდექსებისა და სახელმძღვანელო პრინციპების შესახებ.

ამ პოლიტიკის ნებისმიერი დარღვევა თანამშრომლების მიერ გამოიწვევს მათ დისციპლინარულ პასუხისმგებლობას და ასევე, დარღვევის შედეგად მიყენებული ზიანის ანაზღაურების რეგრესის წესით მოთხოვნას, თუ დადასტურდა რომ თანამშრომელი მონაწილეობდა ან/და ახორციელდებდა პოლიტიკით გათვალისწინებული ვალდებულებების დარღვევას.

ნებისმიერმა პირმა, რომელსაც აქვს ინფორმაცია ან ეჭვობს ამ პოლიტიკის დარღვევას, დაუყოვნებლივ უნდა შეატყობინოს ფაქტები მონაცემთა დაცვის ოფიცერს შემდეგ ელ. ფოსტაზე: info@numus.ge;