დამტკიცებულია
შპს მოგო-ს დირექტორის 2024 წლის 01 აპრილის
Nr. 01/04 ბრძანებით

პერსონალურ მონაცემთა დაცვის პოლიტიკა

ვერსია 1.0

შინაარსი

1. ტერმინთა განმარტება

ბიზნეს პროცესის მფლობელი	კომპანიის მიერ დანიშნული და სათანადოდ უფლებამოსილი თანამშრომელი, რომელიც პასუხისმგებელია წინამდებარე პოლიტიკის მე-4 მუხლში მოცემულ კონკრეტულ მონაცემთა დამუშავებაზე და/ან დამუშავების მიზნებზე.
დირექტორი	კომპანიის მმართველი პირი
კლიენტი	ნებისმიერი ფიზიკური პირი, რომელიც იყენებს, იყენებდა კომპანიის სერვისებს ან გამოთქვამდა კომპანიის სერვისებით სარგებლობის განზრახვას.
კომპანია	შპს მოგო ს/კ:404468688
მაკონტროლებელი/ დამუშავებისთვის პასუხისმგებელი პირი	ფიზიკური პირი, იურიდიული პირი ან საჯარო დაწესებულება, რომელიც ინდივიდუალურად ან სხვებთან ერთად განსაზღვრავს მონაცემთა დამუშავების მიზნებსა და საშუალებებს, უშუალოდ ან დამუშავებაზე უფლებამოსილი პირის მეშვეობით ახორციელებს მონაცემთა დამუშავებას.
დამუშავებაზე უფლებამოსილი პირი	ფიზიკური პირი, იურიდიული პირი ან საჯარო დაწესებულება, რომელიც მონაცემებს ამუშავებს დამუშავებისთვის პასუხისმგებელი პირისთვის ან მისი სახელით. დამუშავებაზე უფლებამოსილ პირად არ მიიჩნევა დამუშავებისთვის პასუხისმგებელ პირთან შრომით ურთიერთობაში მყოფი ფიზიკური პირი.
კანონები მონაცემთა დაცვის შესახებ	„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, GDPR და სხვა ნორმატიული აქტები, რომლებიც არეგულირებენ პერსონალურ მონაცემთა დაცვას GDPR-ის შესაბამისად.
მონაცემთა სუბიექტი	კომპანიის თანამშრომელი ან კლიენტი, ისევე როგორც ნებისმიერი იდენტიფიცირებული ან იდენტიფიცირებადი ფიზიკური პირი, რომლის პერსონალური მონაცემები დამუშავებულია კომპანიის მიერ.
DPIA და/ან მონაცემთა დაცვაზე ზეგავლენის შეფასება	მონაცემთა დაცვაზე ზეგავლენისშეფასება, რომელიც განსაზღვრულია „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 31-ე და GDPR-ის 35-ე მუხლებით.
DPO	კომპანიის მიერ დანიშნული მონაცემთა დაცვის ოფიცერი.
DSR	მონაცემთა სუბიექტის მოთხოვნა, რომელიც მითითებულია წინამდებარე პოლიტიკის მე-8 მუხლში.
Eleving Group	Eleving Group S.A., რეგისტრირებული ლუქსემბურგის სავაჭრო და კომპანიების რეესტრში B 174457 ნომრით და მისი აფილირებული კომპანიები და შვილობილი კომპანიები.
თანამშრომელი	კომპანიაში შრომითი ხელშეკრულების საფუძველზე დასაქმებული ფიზიკური პირი.
GDPR	ევროპარლამენტისა და საბჭოს 2016 წლის 27 აპრილის რეგულაცია (EU) 2016/679 პერსონალური მონაცემების დამუშავების და ამ მონაცემების თავისუფალი მიმოცვლის თვალსაზრისით პირთა დაცვის შესახებ, რომელიც აუქმებს 95/46/EC დირექტივას.
საინფორმაციო სისტემა (IS)	პროგრამული უზრუნველყოფა, სისტემები, მონაცემთა ბაზები და სხვა საინფორმაციო რესურსები, რომლებიც გამოიყენება პერსონალური მონაცემების დამუშავების, შენახვისა და სხვა საქმიანობებისთვის.
ჟურნალის ფაილები	ფაილები, რომლებიც ინახავს მოვლენების, პროცესების, შეტყობინებების და სხვადასხვა პროგრამულ აპლიკაციებს, ოპერაციულ სისტემას და მონაცემთა ბაზებს შორის კომუნიკაციის რეესტრს (წვდომა, მონაცემთა

	შეყვანა, მონაცემთა ექსპორტი, ცვლილებები, მოქმედებები და ა.შ.).
პერსონალური მონაცემები	ნებისმიერი ინფორმაცია, რომელიც ეხება იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს (მონაცემთა სუბიექტს).
პერსონალური მონაცემებთან დაკავშირებული ინციდენტი	უსაფრთხოების დარღვევა, რომელიც იწვევს გადაცემული, შენახული ან სხვაგვარად დამუშავებული პერსონალური მონაცემების შემთხვევით ან უკანონო განადგურებას, შემთხვევით დაკარგვას, შეცვლას, უნებართვო გამჟღავნებას ან მათზე წვდომას (თითოეულ შემთხვევაში, როგორც ეს განსაზღვრულია GDPR-ით).
დამუშავება ან მონაცემთა დამუშავება	პერსონალური მონაცემებით შესრულებული ნებისმიერი ოპერაცია ან ოპერაციების ერთობლიობა, რომელიც ხორციელდება ავტომატური საშუალებებით ან მის გარეშე, როგორიცაა შეგროვება, რეგისტრაცია, ორგანიზაცია, სტრუქტურირება, შენახვა, ადაპტაცია ან შეცვლა, მოძიება, კონსულტაცია, გამოყენება, გამჟღავნება, გადაცემა, გავრცელება ან სხვაგვარად ხელმისაწვდომობა, გასწორება ან კომბინაცია, შეზღუდვა, წაშლა ან განადგურება.
განსაკუთრებული კატეგორიის მონაცემები	პერსონალური მონაცემები, რომლებიც ავლენს რასობრივ ან ეთნიკურ წარმომავლობას, პოლიტიკურ შეხედულებებს, რელიგიურ ან ფილოსოფიურ მრწამსს, ან პროფკავშირის წევრობას, და გენეტიკური მონაცემები, ბიომეტრიული მონაცემები, მონაცემები ჯანმრთელობის შესახებ ან მონაცემები ფიზიკური პირის სქესობრივი ცხოვრების ან სექსუალური ორიენტაციის შესახებ.
სამეთვალყურეო ორგანო	სახელმწიფო ორგანო ან დაწესებულება, რომელსაც აქვს უფლება, შეამოწმოს შესაბამისობის დაცვა მონაცემთა დაცვის სფეროში.
მესამე მხარე	მესამე მხარე (ფიზიკური ან იურიდიული პირი), რომელიც არის პერსონალური მონაცემების მიმღები, ჩართულია კომპანიის მიერ მონაცემთა დამუშავებაში, გარდა მონაცემთა სუბიექტის, მაკონტროლებლის, დამმუშავებლის და იმ პირებისა, რომლებიც კომპანიის უშუალო ნებართვით ავტორიზებულნი არიან, დაამუშაონ პერსონალური მონაცემები.

2. პოლიტიკის მიზანი და მოქმედების სფერო

2.1. წინამდებარე პოლიტიკა ადგენს კომპანიის მიერ პერსონალური მონაცემების დამუშავების ზოგად წესებს. წინამდებარე პოლიტიკა სავალდებულოა ყველა თანამშრომლისთვის ან სხვა დაკავშირებული პირისთვის, რომლებსაც უშუალო დასაქმების ან სხვა თანამშრომლობითი მოვალეობების შესრულებისას აქვთ კონტაქტი კომპანიის მიერ შენახულ პერსონალურ მონაცემებთან.

2.2. წინამდებარე პოლიტიკა მიზნად ისახავს:

ა) დაადგინოს პერსონალური მონაცემების დამუშავების ზოგადი პრინციპები, მთლიანობის, კანონიერების, სიზუსტისა და ანგარიშვალდებულების პრინციპების ჩათვლით.

ბ) დააწესოს პერსონალური მონაცემების დაცვის სავალდებულო მოთხოვნები კომპანიის მიერ ამ მოთხოვნების შესრულების უზრუნველყოფის შესაძლებლობის გათვალისწინებით.

გ) შექმნას მონაცემთა დაცვისა და კონფიდენციალურობის დაცვის მართვის უსაფრთხო და კანონიერი სისტემა, რომელიც შეესაბამება მონაცემთა დაცვის შესახებ კანონებით დადგენილ მოთხოვნებს.

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

2.3. კომპანიის მენეჯმენტი უზრუნველყოფს წინამდებარე პოლიტიკის პერიოდულ გადასინჯვას.

2.4. პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებული საკითხები, რომელიც არ არის გათვალისწინებული წინამდებარე პოლიტიკით, წესრიგდება საქართველოს კანონმდებლობის შესაბამისად.

3. დაკავშირებული პროცედურები

3.1. წინამდებარე პოლიტიკა იკითხება კომპანიის სხვა პოლიტიკასა და პროცედურასთან ერთად, როგორიცაა:

ა) AML პროცედურა,

ბ) და სხვა პროცედურები ან პოლიტიკა, რომლებიც შეიძლება შეიცავდეს დებულებებს პერსონალური მონაცემების დამუშავების შესახებ ან პირდაპირ ან არაპირდაპირ ეხებოდეს მათ.

4. ბიზნეს პროცესის მფლობელი

4.1. კომპანია ნიშნავს პირს, რომელიც პასუხისმგებელია მონაცემთა კონკრეტულ დამუშავებაზე და/ან დამუშავების მიზნებზე კომპანიაში ან კომპანიის შესაბამის დეპარტამენტში ან ბიზნეს მიმართულებაში, რომლის ფუნქციები და ამოცანები მოიცავს, სხვებთან ერთად, მონაცემთა კონკრეტული დამუშავების ადმინისტრირებას, ზედამხედველობასა და კონტროლს და წინამდებარე პროცედურის დაცვის უზრუნველყოფას. ასეთი პირები ჩაითვლებიან ბიზნეს პროცესის მფლობელებად.

კომპანიას ასევე შეუძლია დანიშნოს კონკრეტული უფლებამოსილი წარმომადგენლები კონკრეტული სიტუაციის გათვალისწინებით, რათა მათ ეფექტურად მართონ და გადაჭრან კონკრეტული საკითხი ან სიტუაცია, როგორც ამას მოითხოვს წინამდებარე პროცედურა. მაგალითად, DSR-ების დამუშავებისა და მათზე რეაგირების შემთხვევაში.

5. პერსონალური მონაცემების დამუშავების პრინციპები და საფუძვლები

5.1. პერსონალური მონაცემების დამუშავებისას დაცული და უზრუნველყოფილი უნდა იყოს შემდეგი პრინციპები:

ა) კანონიერება, სამართლიანობა და გამჭვირვალობა. კომპანია პერსონალურ მონაცემებს ამუშავებს კანონიერად, სამართლიანად და გამჭვირვალედ მონაცემთა სუბიექტთან მიმართებაში. პერსონალური მონაცემები უნდა დამუშავდეს მხოლოდ იმ შემთხვევაში, თუ არსებობს მონაცემთა დაცვის შესახებ მოქმედი კანონებით დადგენილი ვალიდური სამართლებრივი საფუძველი. პერსონალური მონაცემების დამუშავებისას კომპანიამ უნდა უზრუნველყოს, რომ მონაცემთა სუბიექტისთვის ცნობილია, თუ როგორ და რა მიზნებისთვის დამუშავდება მისი პერსონალური მონაცემები, ასევე უნდა უზრუნველყოს მონაცემთა სუბიექტის უფლებების პატივისცემა.

ბ) მიზნის შეზღუდვა. კომპანია ამუშავებს პერსონალურ მონაცემებს კონკრეტული, აშკარა და ლეგიტიმური მიზნებისთვის. კომპანია მკაფიოდ აცხადებს და აღნიშნავს ამ მიზანს და ამუშავებს პერსონალურ მონაცემებს მხოლოდ იმდენ ხანს, რამდენიც საჭიროა ამ მიზნის შესასრულებლად. პერსონალური მონაცემები არ უნდა დამუშავდეს შეუთავსებელი მიზნებისთვის.

გ) მონაცემთა მინიმიზაცია. კომპანია შეაგროვებს პერსონალურ მონაცემებს, რომლებიც ადეკვატური და შესაბამისია იმ მიზანთან, რისთვისაც ისინი მუშავდება. მონაცემები უნდა დამუშავდეს მხოლოდ იმ მოცულობით, რომელიც აუცილებელია შესაბამისი ლეგიტიმური მიზნის მისაღწევად. მონაცემები იმ მიზნის თანაზომიერი უნდა იყოს, რომლის მისაღწევადაც ისინი მუშავდება.

დ) მონაცემთა სიზუსტე. შეგროვებული პერსონალური მონაცემები უნდა იყოს ზუსტი, განახლებული და კომპანიამ უნდა უზრუნველყოს არაზუსტი მონაცემების წაშლა ან განახლება, რათა ასახული იყოს რეალური სიტუაცია.

ე) შენახვის შეზღუდვა. კომპანია უზრუნველყოფს, რომ პერსონალური მონაცემები არ იქნება შენახული საჭიროზე მეტ ხანს, პერსონალური მონაცემების შენახვასთან დაკავშირებით მოქმედი სამართლებრივი ნორმების შესაბამისად, დამუშავების მიზნისა და ხანდაზმულობის ვადის გათვალისწინებით.

ვ) მთლიანობა და კონფიდენციალურობა. შესაბამისი ტექნიკური ან ორგანიზაციული ზომების გამოყენებით კომპანია უზრუნველყოფს პერსონალური მონაცემების დამუშავებას ისე, რომ უზრუნველყოფილი იყოს მონაცემების უსაფრთხოება, მათ შორის მათი დაცულობა არაავტორიზებული ან უკანონო დამუშავებისგან და შემთხვევითი დაკარგვისგან, განადგურებისგან ან დაზიანებისგან.

ზ) ანგარიშვალდებულება. კომპანია პასუხისმგებელია მონაცემთა დაცვის შესახებ კანონებთან, წინამდებარე პოლიტიკასთან და სხვა მოქმედ შიდა დოკუმენტებთან და პოლიტიკასთან შესაბამისობაზე, ასევე შეუძლია ამ შესაბამისობის დადასტურება.

5.2. კომპანიის საქმიანობის პროცესში მონაცემთა დამუშავება შესაძლებელია შემდეგი საფუძვლებიდან ერთ-ერთის არსებობის შემთხვევაში:

ა) მონაცემთა სუბიექტმა განაცხადა თანხმობა მის შესახებ მონაცემთა ერთი ან რამდენიმე კონკრეტული მიზნით დამუშავებაზე;

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

გ) მონაცემთა დამუშავება გათვალისწინებულია კანონმდებლობით;

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

ე) კანონმდებლობის თანახმად, მონაცემი საჯაროდ ხელმისაწვდომია ან მონაცემთა სუბიექტმა იგი საჯაროდ ხელმისაწვდომი გახადა;

ვ) მონაცემთა დამუშავება აუცილებელია მონაცემთა სუბიექტის ან სხვა პირის სასიცოცხლო ინტერესების დასაცავად, მათ შორის, ეპიდემიის მონიტორინგის ან/და მისი გავრცელების აღკვეთის, ჰუმანიტარული კრიზისების, ბუნებრივი და ადამიანის მოქმედებით გამოწვეული კატასტროფების სამართავად;

ზ) მონაცემთა დამუშავება აუცილებელია მნიშვნელოვანი საჯარო ინტერესის დასაცავად;

თ) მონაცემთა დამუშავება აუცილებელია საქართველოს კანონმდებლობით განსაზღვრული საჯარო ინტერესის სფეროსთვის მიკუთვნებული ამოცანების შესასრულებლად;

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;

კ) მონაცემთა დამუშავება აუცილებელია მონაცემთა სუბიექტის განცხადების განსახილველად (მისთვის მომსახურების გასაწევად).

6. პერსონალური მონაცემების კლასიფიკაცია

6.1. მონაცემთა დაცვის მოქმედი კანონების მოთხოვნების, პერსონალური მონაცემების უსაფრთხოების და და პერსონალურ მონაცემთა დამუშავების ზოგადი პრინციპების დაცვის უზრუნველსაყოფად აუცილებელი ტექნიკური და ორგანიზაციული უსაფრთხოების ზომების გათვალისწინებით კომპანია პერსონალურ მონაცემებს აჯგუფებს შემდეგ კატეგორიებად:

ა) საჯარო ინფორმაცია – ფართო საზოგადოებისთვის ან მესამე პირებისთვის უკვე ცნობილი ინფორმაცია, რომელიც ოფიციალურად გამოქვეყნებულია ან მიღებულია საჯაროდ ხელმისაწვდომი წყაროდან და არ წარმოადგენს პერსონალურ მონაცემებს. ასეთი ინფორმაციის გაზიარება არ მიაყენებს ზიანს კომპანიას ან მონაცემთა სუბიექტს. ასეთი ინფორმაცია არ ექვემდებარება წინამდებარე პროცედურას.

ბ) შიდა ინფორმაცია – პერსონალური მონაცემები, რომლებიც თავისუფლად არის ხელმისაწვდომი ყველა თანამშრომლისთვის, მაგრამ ავტორიზაციის გარეშე არ შეიძლება გამჟღავნებული იყოს მესამე პირებისთვის.

გ) შეზღუდული ინფორმაცია – პერსონალური მონაცემები, რომლებიც თავისუფლად არ არის ხელმისაწვდომი ყველა თანამშრომლისთვის და ხელმისაწვდომია მხოლოდ გარკვეული თანამშრომლებისთვის საჭიროებისამებრ და/ან მათი უშუალო სამუშაო მოვალეობების შესასრულებლად. შეზღუდული ინფორმაციის გამჟღავნებამ ან მათმა მოპარვამ შესაძლოა ზიანი მიაყენოს კომპანიას და/ან მონაცემთა სუბიექტს.

დ) საიდუმლო ინფორმაცია – პერსონალური მონაცემები, რომელიც შეიცავს სპეციალური კატეგორიის მონაცემებს ან მონაცემებს მონაცემთა სუბიექტის ნასამართლეობისა და სისხლისსამართლებრივი დანაშაულის შესახებ. საიდუმლო ინფორმაცია ხელმისაწვდომი უნდა იყოს მხოლოდ შეზღუდული და სათანადოდ უფლებამოსილი თანამშრომლებისთვის და კონკრეტული წერილობითი ავტორიზაციის საფუძველზე. საიდუმლო ინფორმაციის გამჟღავნებამ ან მათმა მოპარვამ შესაძლოა მნიშვნელოვანი ზიანი მიაყენოს კომპანიას და/ან მონაცემთა სუბიექტს.

6.2. წვდომა ინფორმაციაზე, რომელიც კლასიფიცირებულია, როგორც შეზღუდული ან საიდუმლო, უნდა ჰქონდეს თანამშრომლების შეზღუდულ რაოდენობას და მხოლოდ უშუალო სამსახურებრივი პასუხისმგებლობის საფუძველზე. ინფორმაცია, რომელიც კლასიფიცირებულია, როგორც შეზღუდული ან საიდუმლო, დაცული უნდა იყოს ტექნიკური და ორგანიზაციული უსაფრთხოების გაძლიერებული ზომებით.

7. პერსონალური მონაცემების დამუშავების ორგანიზაცია

მონაცემთა დამუშავების ჩანაწერები

7.1. კომპანია ინახავს და პერიოდულად ანახლებს ჩანაწერებს მის მიერ განხორციელებული პერსონალური მონაცემების დამუშავების შესახებ. ეს ჩანაწერები ხორციელდება GDPR-ის შესაბამისად და უნდა შეიცავდეს GDPR-ის 30-ე მუხლით გათვალისწინებულ ინფორმაციას. მონაცემთა დამუშვების ჩანაწერები ინახება და განახლდება შესაბამის სისტემაში.

7.2. კომპანია პასუხისმგებელია მონაცემთა დამუშვების ჩანაწერების შენახვასა და ზედამხედველობაზე და ამ მიზნით მან უნდა მიიღოს კონსულტაცია პერსონალურ მონაცემთა დაცვის ოფიცრისგან.

7.3. მონაცემთა ახალი დამუშვების დაწყებამდე (მაგალითად, ახალი სერვისის მიწოდება, კლიენტის დამატებითი შეფასების განხორციელება, ახალი IT სისტემის დანერგვა), კომპანია:

ა) განსაზღვრავს მონაცემთა დამუშვებას, მის ფარგლებს, მიზანს;

ბ) ადგენს, ვინ არის მონაცემთა დამუშვების ბიზნეს პროცესის მფლობელი;

გ) იწყებს მონაცემთა დამუშვების შეფასებას შესაბამისი სისტემის გამოყენებით, სადაც ბიზნეს პროცესის მფლობელი აწვდის დეტალებს მონაცემთა დამუშვების შესახებ და საბოლოოდ წარმოადგენს აუცილებელ შეფასებებს, მაგალითად, ლეგიტიმური ინტერესის შეფასებას და DPIA-ს ზღვრულ შეფასებას.

დ) მონაცემთა დამუშვების შეფასებას დასამტკიცებლად წარუდგენს ბიზნეს პროცესის მფლობელის უშუალო მენეჯერს ან, ალტერნატიულად, გუნდის წევრს, რომელიც უფლებამოსილია, განიხილოს კონკრეტული მონაცემთა დამუშვება ან საბჭოს.

7.4. დამუშავება ხორციელდება კომპანიის ან/და მონაცემების დამმუშავებლის ობიექტში (დამმუშავებელთან დადებული წინასწარი წერილობითი შეთანხმების საფუძველზე) ან ნებისმიერ სხვა ადგილას, კომპანიის ინსტრუქციის შესაბამისად.

7.5. პერსონალური მონაცემების ელექტრონული ფორმით დამუშავება უნდა განხორციელდეს მხოლოდ იმ საინფორმაციო სისტემების გამოყენებით, რომლებიც იდენტიფიცირებულია და განთავსებულია კომპანიის ჩანაწერებში და მისი კონტროლის ქვეშაა, გარდა იმ შემთხვევებისა, როდესაც დამუშავება ხორციელდება დამმუშავებლის მიერ.

მონაცემთა დაცვაზე ზეგავლენის შეფასების (DPIA) ჩატარება

7.6. თუ 7.3 ნაწილში მითითებული მონაცემთა დამუშვების შეფასების შემდეგ, კომპანია გამოავლენს, რომ მონაცემთა დამუშვება შეიძლება ჩაითვალოს მაღალ რისკად, ანუ დამუშავების ტიპმა, კერძოდ, ახალი ტექნოლოგიების გამოყენებამ, დამუშავების ბუნების, ფარგლების, კონტექსტისა და მიზნების გათვალისწინებით, შესაძლოა მაღალი რისკის ქვეშ დააყენოს ფიზიკური პირების უფლებები და თავისუფლებები, კომპანია განახორციელებს DPIA-ს.

7.7. კომპანია DPIA-ს ახორციელებს შესაბამისი სისტემის გამოყენებით:

ა) DPIA-ს შეფასების ფორმების მორგება მონაცემთა დაცვის შესახებ მოქმედი კანონების, გაიდლაინების შესაბამისად და პერსონალურ მონაცემთა დაცვის ოფიცერთან კონსულტაციით.

ბ) შეფასების დანერგვა, რომელიც ივსება ბიზნეს პროცესის მფლობელის მიერ. ბიზნეს პროცესის მფლობელი, საჭიროების შემთხვევაში, აწვდის საჭირო ინფორმაციას, განმარტებებს და დოკუმენტაციას შეფასების განსახორციელებლად.

გ) DPIA-ს განხილვა და დამტკიცება. დამტკიცება უნდა დასრულდეს ბიზნეს პროცესის მფლობელის უშუალო მენეჯერის ან, ალტერნატივის სახით, გუნდის წევრის მიერ,

რომელიც უფლებამოსილია განიხილოს მონაცემთა კონკრეტული დამუშვება ან საბჭოს მიერ.

7.8. თუ შეფასების შემდეგ ცხადი გახდება, რომ პერსონალური მონაცემების დაცვის დამატებითი ზომების არარსებობის შემთხვევაში, მონაცემთა დამუშვება მონაცემთა სუბიექტის უფლებებსა და თავისუფლებებს მაღალი რისკის დააყენებს, კომპანიამ უნდა აცნობოს მონაცემთა დამუშვების სამეთვალყურეო ორგანოს და გაიაროს კონსულტაცია დამუშავების შესაბამისი გარემოებების შესახებ. კომპანიამ სამეთვალყურეო ორგანოს უნდა მიაწოდოს:

ა) კომპანიისა და დამუშავების მონაწილე დამმუშავებლების პასუხისმგებლობის აღწერა, კერძოდ, საწარმოთა ჯგუფის ფარგლებში დამუშავების მიზნით;

ბ) მონაცემთა დამუშვების მიზნები და საშუალებები;

გ) GDPR-ის შესაბამისად მონაცემთა სუბიექტების უფლებებისა და თავისუფლებების დასაცავად გათვალისწინებული ზომები და გარანტიები;

დ) პერსონალურ მონაცემთა დაცვის ოფიცრის საკონტაქტო მონაცემები;

ე) გაფორმებული DPIA; და

ვ) ზედამხედველობის ორგანოს მიერ მოთხოვნილი ნებისმიერი სხვა ინფორმაცია.

7.9. კომპანია ინახავს გაფორმებულ DPIA-ებს, ხოლო შესაბამისი ბიზნეს პროცესის მფლობელი პერიოდულად განიხილავს რისკების გამკლავების გეგმას მონაცემთა სუბიექტების უფლებებისა და თავისუფლებების გამოვლენილი რისკების შესამცირებლად.

პერსონალური მონაცემების გაზიარება, გამჟღავნება და გადაცემა

7.10. პერსონალურ მონაცემებს კომპანია გაუზიარებს მხოლოდ სხვა მაკონტროლებლებს, დამმუშავებლებს ან იმ მესამე მხარეებს, რომლებთანაც კომპანიამ დადო მონაცემთა გაზიარების წინასწარი წერილობითი შეთანხმება მონაცემთა დაცვის მოქმედი კანონების შესაბამისად ან იმ შემთხვევაში, თუ მოთხოვნილია მოქმედი კანონებითა და რეგულაციებით. მაგალითად:

ა) პერსონალური მონაცემები შეიძლება გაზიარებული იქნას მაკონტროლებლებთან და დამმუშავებლებთან, რომლებთანაც კომპანიამ დადო მონაცემთა დამუშავების ხელშეკრულება;

ბ) კომპანიამ მიიღო წერილობითი მოთხოვნა სახელმწიფო ან სამთავრობო ორგანოსგან კონკრეტული პერსონალური მონაცემების გამჟღავნების შესახებ და კომპანია კანონიერად ვალდებულია, შეასრულოს ეს მოთხოვნა.

7.11. პერსონალური მონაცემების გაზიარებამდე ან გადაცემამდე, ბიზნეს პროცესის მფლობელმა უნდა უზრუნველყოს, რომ:

ა) პერსონალური მონაცემების გაზიარებისა და გადაცემის პირობები შეესაბამება კომპანიის პოლიტიკასა და წინამდებარე პროცედურას;

ბ) მაკონტროლებელს ან დამმუშავებელს აქვს უნარი, უზრუნველყოს ადეკვატური ტექნიკური და ორგანიზაციული უსაფრთხოების ზომები და ისინი უზრუნველყოფენ უსაფრთხოების მინიმუმ იმავე დონეს, როგორიცაა კომპანიის შიდა ინფორმაციის დაცვის პროცედურა და/ან ზოგადად მიღებული დარგობრივი უსაფრთხოების ზომები;

გ) მიმღები მხარე აკმაყოფილებს „პერსონალურ მონაცემთა დაცვის შესახებ“საქართველოს კანონის მე-5 თავით გათვალისწინებულ პირობებს..

7.12. აკრძალულია პერსონალური მონაცემების კოპირება/ასლის გადაღება და/ან გადატანა გარე მყარ დისკებზე, თუ ეს არ არის სპეციალურად ავტორიზებული საბჭოს ან სხვა სათანადოდ უფლებამოსილი თანამშრომლების მიერ.

7.13. თუ შესაძლებელია მოცემულ სიტუაციაში, კომპანია აზიარებს პერსონალურ მონაცემებს დაშიფრული ფორმით და იცავს გაზიარებულ ინფორმაციას არაავტორიზებული წვდომისგან პაროლების გამოყენებით ან წვდომის კონტროლის უზრუნველყოფით.

7.14. აკრძალულია თანამშრომლების პირადი ანგარიშების გამოყენება (მაგალითად,პირადი ელ.ფოსტის ანგარიშები) პერსონალური მონაცემების ან კომპანიის ნებისმიერი სხვა ინფორმაციის გასაზიარებლად.

7.15. მატერიალური ფაილები, რომლებიც შეიძლება შეიცავდეს პერსონალურ მონაცემებს, ინახება დაცულ საცავში, მაგალითად, ჩაკეტილ სივრცეში ოფისში, სადაც წვდომა უზრუნველყოფილია მხოლოდ ავტორიზებული თანამშრომლებისთვის.

7.16. კომპანია იცავს სუფთა მაგიდის პოლიტიკას, რომელიც უზრუნველყოფს, რომ ყველა დოკუმენტი, რომელიც შეიძლება შეიცავდეს პერსონალურ მონაცემებს, ამოღებული უნდა იქნას იმ ადგილებიდან, სადაც მათზე წვდომა დასაშვებია არაავტორიზებული პირებისთვის, და ინახებოდეს დაცულ კარადებში ან სხვა სივრცეებში. მაგალითად, ასეთი დოკუმენტები არ უნდა დარჩეს უყურადღებოდ თანამშრომლის მაგიდაზე.

პერსონალური მონაცემების შენახვა

7.17. პერსონალურ მონაცემთა დამუშავების ყველა ტიპისა და პერსონალური მონაცემების ტიპისთვის კომპანია ადგენს შენახვის კონკრეტულ პერიოდს. კომპანია ინახავს მონაცემებს მხოლოდ იმ ვადით, რომელიც საჭიროა იმ მიზნების მისაღწევად, რისთვისაც აღნიშნული მონაცემები შეგროვდა, მათ შორის და არამხოლოდ, ნებისმიერი სამართლებრივი, მარეგულირებელი, საგადასახადო, სააღრიცხვო, ან ანგარიშგებასთან დაკავშირებულ მოთხოვნათა დაკმაყოფილების მიზნებისათვის.

7.18. შენახვის ვადის განსაზღვრისას, კომპანია:

ა) იცავს მოქმედ კანონებსა და რეგულაციებს,

ბ) იცავს მონაცემთა მინიმიზაციის პრინციპს,

გ) უზრუნველყოფს შენახული პერსონალური მონაცემების შესაბამის ტექნიკურ და ორგანიზაციულ უსაფრთხოების ზომებს, კომპანიის ინფორმაციის დაცვის პროცედურების შესაბამისად.

7.19. შენახვის ვადები პერიოდულად უნდა იქნას გადასინჯული და შესწორდეს მონაცემთა დამუშავების ხელახალი შეფასების დროს და მოქმედ საკანონმდებლო ნორმებსა და რეგულაციებში შეტანილი ნებისმიერი ცვლილების შემდეგ.

7.20. შენახვის ვადების შეფასებისას და განსაზღვრისას კომპანიამ უნდა გაითვალისწინოს შემდეგი მოსაზრებები:

ა) პერსონალური მონაცემები ინახება მანამ, სანამ ისინი საჭირო იქნება მონაცემთა დამუშავების მიზნის შესასრულებლად;

ბ) პერსონალური მონაცემები ინახება მოქმედი კანონებითა და რეგულაციებით დადგენილი ვადით;

გ) პერსონალური მონაცემები ინახება ხანდაზმულობის ვადის გასვლამდე, რათა დაცული იქნას კომპანიის კანონიერი უფლებები და ინტერესები საკუთარი თავის დაცვისა და სამართლებრივი დავის შემთხვევაში მტკიცებულებების მიწოდების თვალსაზრისით;

დ) პერსონალური მონაცემები არ უნდა წაიშალოს ფაილებიდან ან დოკუმენტებიდან, თუ ამან შეიძლება გავლენა მოახდინოს ფაილის ან დოკუმენტის იურიდიულ ხასიათსა და ძალაზე, მაგალითად, გახადოს იგი ბათილი ან არააღსრულებადი.

პერსონალური მონაცემების წაშლა

7.21. პერსონალური მონაცემების დამუშავების დასრულებისას ან კონკრეტული პერსონალური მონაცემების შენახვის ვადის ამოწურვისას, კომპანია წაშლის ან ანონიმურად აქცევს ან,

კანონიერი საჭიროების შემთხვევაში, გადაიტანს პერსონალურ მონაცემებს შესაბამის არქივში (შპს მოგოს შემთხვევაში კერძო კომპანია). თუ პერსონალური მონაცემები დამუშავებულია მატერიალური ფორმით, დოკუმენტები განადგურდება იმგვარად, რომ უზრუნველყოფილი იყოს ინფორმაციის აღდგენის შეუძლებლობა. მონაცემთა კონკრეტული დამუშვების ბიზნეს პროცესის მფლობელი პასუხისმგებელია ამ პუნქტში განსაზღვრული შესაბამისობის უზრუნველყოფაზე.

7.22. ბიზნეს პროცესის მფლობელმა უნდა უზრუნველყოს, რომ 7.23 პუნქტში მითითებული მოთხოვნა შესრულდეს ნებისმიერი დამმუშავებლის მიერ, რომელთანაც გაზიარებულია შესაბამისი პერსონალური მონაცემები.

7.23. კომპანია უზრუნველყოფს, რომ ნებისმიერი რესურსი (IS ან აპარატურა), რომელიც შეიძლება შეიცავდეს პერსონალურ მონაცემებს, განკარგული იქნას უსაფრთხოდ და კომპანიის ინფორმაციის დაცვის პროცედურების შესაბამისად.

8. მონაცემთა სუბიექტის მოთხოვნის მართვა

მონაცემთა სუბიექტის მოთხოვნის (DSR) მართვის ზოგადი წესები

8.1. კომპანია უზრუნველყოფს მონაცემთა სუბიექტის უფლებების შესრულებას და იცავს თავის სამართლებრივ ვალდებულებებს DSR-ებზე რეაგირებით და მოთხოვნილი ინფორმაციის მიწოდებით მონაცემთა დაცვის შესახებ მოქმედი კანონებისა და წინამდებარე პროცედურის შესაბამისად.

8.2. DSR-ების მიღებისა და დამუშავებისას კომპანიამ უნდა (ა) განახორციელოს ქვემოთ ჩამოთვლილი ნაბიჯები და (ბ) უზრუნველყოს კონკრეტულ DSR-ზე რეაგირების განსაზღვრული წესების დაცვა. კომპანია:

ა) აცნობებს DPO-ს და უზრუნველყოფს, რომ DPO-ს აქვს ყველა საჭირო ინფორმაცია და რესურსი, რათა დაეხმაროს კომპანიას DSR-ზე რეაგირებაში. კომპანია უზრუნველყოფს DSR-ების განხილვას, მართვას და პასუხის გაცემას კომპანიისა და DPO-ს უფლებამოსილი წარმომადგენლის მიერ.

ბ) უზრუნველყოფს მონაცემთა სუბიექტის იდენტიფიცირებას და საჭიროების შემთხვევაში ითხოვს დამატებით ინფორმაციას, რომელიც შეიძლება საჭირო გახდეს მონაცემთა სუბიექტის იდენტიფიკაციისთვის.

გ) ადგენს, შეიცავს თუ არა DSR საჭირო ინფორმაციას, რომელიც საჭიროა კომპანიის მიერ განხილვისა და რეაგირებისთვის. მაგალითად, საჭიროების შემთხვევაში, განმარტავს, რა ინფორმაციის მიღება სურს მონაცემთა სუბიექტს და/ან რომელი უფლების გამოყენება სურს მონაცემთა სუბიექტს.

დ) პასუხის მომზადებისას კომპანია ამოწმებს თავის IS და სხვა აქტივებს, ფაილების საცავებსა და მონაცემთა ბაზებს (ელექტრონულ და ფიზიკურ), რათა შეძლოს, რომ მონაცემთა სუბიექტს მიაწოდოს ზუსტი და ნამდვილი ინფორმაცია. საჭიროების შემთხვევაში, კომპანია მიმართავს მონაცემთა დამუშავების ჩანაწერებს, რათა დაადგინოს მაკონტროლებლები, დამმუშავებლები ან მესამე მხარეები, რომლებმაც შესაძლოა მიიღეს პერსონალური მონაცემები.

ე) უზრუნველყოფს, რომ DSR-ის კონკრეტულ მოთხოვნებს იცავენ კომპანიის მაკონტროლებლები და დამმუშავებლები, თუ ეს გონივრულად მოითხოვება. მაგალითად, კომპანია უზრუნველყოფს, რომ წაშლის უფლების შემთხვევაში, პერსონალური მონაცემები წაიშლება ან ანონიმური გახდება ასევე კომპანიის დამმუშავებლების მიერ.

ვ) განიხილავს DSR-ს და ამუშავებს მას მონაცემთა სუბიექტისგან საფასურის მოთხოვნის გარეშე. კომპანია უფლებამოსილია უარი განაცხადოს მოთხოვნის დაკმაყოფილებაზე, თუ აღნიშნული ტექნიკურად შეუძლებელია ან გაუმართლებლად დიდ ძალისხმევას საჭიროებს.

ვ) გასცემს პასუხს არასათანადო დაყოვნების გარეშე და მიღებიდან სულ მცირე 1 თვის ვადაში. თუ ამ ვადაში პასუხის გაცემა შეუძლებელია, კომპანიას შეუძლია გააგრძელოს ვადა კიდევ ორი თვით, DSR-ების სირთულისა და რაოდენობის გათვალისწინებით.

დ) აღრიცხავს და არეგისტრირებს ყველა მიღებულ DSR-ს, რითაც უზრუნველყოფს DSR-ების მართვას, პასუხების მომზადების ვადების კონტროლს, ასევე საშუალებას აძლევს კომპანიას, გამოვლინდეს არაგონივრული DSR-ები, რომლებზეც შეიძლება დაწესდეს საფასური.

8.3. კომპანია მიიღებს DSR-ებს მატერიალური ან ელექტრონული ფორმით. თუ DSR წარდგენილია წერილობითი ფორმით, კომპანია უზრუნველყოფს, რომ მას ხელს აწერდეს მონაცემთა სუბიექტი. თუ DSR წარდგენილია მონაცემთა სუბიექტის წარმომადგენლის მიერ, DSR ასევე უნდა შეიცავდეს მინდობილობას ან სხვა იურიდიულად ქმედით დოკუმენტს, რომელიც ადასტურებს წარმომადგენლობის უფლებას.

8.4. DSR-ზე პასუხს კომპანია გასცემს ელექტრონული ფორმით, გარდა იმ შემთხვევებისა, როდესაც მონაცემთა სუბიექტმა ნათლად მოითხოვა პასუხის სხვა ფორმატში მიწოდება, მაგალითად, წერილობითი ფორმით ან მონაცემთა სუბიექტის ელექტრონული ფოსტის მისამართი არ არის ცნობილი და არ არის მითითებული DSR-ში.

DSR-ებზე რეაგირების კონკრეტული წესები

<u>წვდომის უფლება</u>

8.5. თუ მონაცემთა სუბიექტმა მოითხოვა დადასტურება იმის შესახებ, ამუშავებს თუ არა კომპანია მის პერსონალურ მონაცემებს, კომპანია ვალდებულია:

ა) მიაწოდოს მონაცემთა სუბიექტს GDPR-ის მე-15 მუხლით მოთხოვნილი ინფორმაცია, კონკრეტულად (ა) მისი პერსონალური მონაცემების დამუშავების მიზნები, (ბ) შესაბამისი პერსონალური მონაცემების კატეგორიები, (გ) აღნიშნული პერსონალური მონაცემების მიმღებები, მათ შორის მიმღებები მესამე ქვეყნებში, (დ) პერსონალური მონაცემების შენახვის პერიოდი, (ე) ინფორმაცია მონაცემთა სუბიექტის უფლებების შესახებ და (ვ) ავტომატიზირებული გადაწყვეტილების მიღების არსებობა, პროფილირების ჩათვლით, და ინფორმაცია ლოგიკის შესახებ, თუ ეს შესაძლებელია;

ბ) მიაწოდოს მონაცემთა სუბიექტს შესაბამისი პერსონალური მონაცემების ასლი იმგვარად, რომ ამავდროულად უზრუნველყოს, რომ მონაცემთა სხვა სუბიექტების პერსონალური მონაცემები არ გამჟღავნდება.

<u>შესწორების უფლება</u>

8.6. თუ მონაცემთა სუბიექტმა მოითხოვა თავისი პერსონალური მონაცემების შესწორება და გასწორება, კომპანიამ უნდა:

ა) შეასწოროს და/ან შეცვალოს პერსონალური მონაცემები, როგორც ამას მოითხოვს მონაცემთა სუბიექტი და მიაწოდოს ამის დასტური მონაცემთა სუბიექტს.

<u>წაშლის უფლება</u>

თუ მონაცემთა სუბიექტმა მოითხოვა თავისი პერსონალური მონაცემების წაშლა, კომპანია წაშლის ან ანონიმურს გახდის შესაბამის პერსონალურ მონაცემებს, თუ GDPR-ის მე-17 მუხლის თანახმად, ვრცელდება რომელიმე ქვემოთ ჩამოთვლილი პირობა:

ა) პერსონალური მონაცემები აღარ არის საჭირო იმ მიზნებისთვის, რისთვისაც ისინი დამუშავდა;

ბ) მონაცემთა სუბიექტმა გააუქმა თანხმობა, რომელსაც დამუშავება ეფუძნებოდა ან აღარ არსებობს პერსონალური მონაცემების დამუშავების სამართლებრივი საფუძველი;

გ) პერსონალური მონაცემები დამუშავდა კომპანიის ლეგიტიმური ინტერესებიდან გამომდინარე, მაგრამ მონაცემთა სუბიექტი ეწინააღმდეგება ასეთ დამუშავებას და კომპანიას არ წარმოუდგენია ასეთი დამუშავების აღმატებული ლეგიტიმური საფუძველი;

დ) პერსონალური მონაცემები დამუშავდა უკანონოდ;

ე) მოქმედი კანონებით ან რეგულაციებით მოთხოვნილია, რომ კომპანიამ წაშალოს პერსონალური მონაცემები.

8.7. კომპანია უარს იტყვის პერსონალური მონაცემების წაშლაზე, თუ პერსონალური მონაცემები საჭიროა კომპანიისთვის მოქმედი სამართლებრივი ვალდებულების შესასრულებლად, პერსონალური მონაცემები საჭიროა არქივის მიზნებისთვის საჯარო ინტერესებიდან გამომდინარე ან საჭიროა სამართლებრივი პრეტენზიების ჩამოყალიბების, განხორციელების ან დაცვისთვის.

<u>დამუშავების შეზღუდვის უფლება</u>

8.8. თუ ვრცელდება რომელიმე ქვემოთ ჩამოთვლილი პირობა, მონაცემთა სუბიექტს შეუძლია მოსთხოვოს კომპანიას პერსონალური მონაცემების დამუშავების შეზღუდვა:

ა) მონაცემთა სუბიექტი ეჭვქვეშ აყენებს პერსონალური მონაცემების სიზუსტეს და სთხოვს კომპანიას, შეწყვიტოს აღნიშნული პერსონალური მონაცემების დამუშავება გარკვეული ვადით, რაც კომპანიას მონაცემების სიზუსტის გადამოწმების საშუალებას მისცემს;

ბ) დამუშავება იყო უკანონო, მაგრამ მონაცემთა სუბიექტი ითხოვს, კომპანიამ შეინახოს მონაცემები და შეზღუდოს დამუშავება;

გ) კომპანიას აღარ სჭირდება პერსონალური მონაცემები მისი დამუშავების მიზნით, მაგრამ მონაცემთა სუბიექტი ითხოვს ინფორმაციის შენახვას სამართლებრივი პრეტენზიების დადგენისა და დაცვისათვის;

დ) მონაცემთა სუბიექტმა გააპროტესტა დამუშავება, რომელიც ეფუძნება კომპანიის ლეგიტიმურ ინტერესებს და მიმდინარეობს შემოწმება, აჭარბებს თუ არა კომპანიის კანონიერ საფუძვლები მონაცემთა სუბიექტის კანონიერ უფლებებს.

8.9. თუ მოქმედებს ზემოაღნიშნული პირობები, კომპანია ზღუდავს კონკრეტული პერსონალური მონაცემების დამუშავებას, როგორც ამას მონაცემთა სუბიექტი ითხოვს.

8.10. კომპანიას შეუძლია გააგრძელოს შეზღუდული პერსონალური მონაცემების შენახვა და ნებისმიერი სხვა დამუშავება ნებადართულია მხოლოდ იმ შემთხვევაში, თუ მონაცემთა სუბიექტმა განაცხადა თანხმობა ან ეს საჭიროა კომპანიის სამართლებრივი პრეტენზიების ან სხვა მიზნების დადგენისა და დაცვისათვის, როგორც ეს მითითებულია GDPR-ის მე-18(2) მუხლში.

8.11. თუ კომპანია მოხსნის შეზღუდვას რაიმე მიზნით, იგი წინასწარ წერილობით აცნობებს მონაცემთა სუბიექტს.

<u>მონაცემთა პორტაბელურობის უფლება</u>

8.12. თუ მონაცემთა სუბიექტი ითხოვს კომპანიისთვის მის მიერ მიწოდებული თავისი პერსონალური მონაცემების მიღებას, კომპანია ვალდებულია:

ა) დაადგინოს, არის თუ არა შესაძლებელი მოთხოვნილი პერსონალური მონაცემების ექსპორტი და ექვემდებარება თუ არა პორტაბელურობის მოთხოვნებს, ანუ, შესაბამისი პერსონალური მონაცემები დამუშავდა მონაცემთა სუბიექტის თანხმობის საფუძველზე თუ მონაცემთა სუბიექტთან ხელშეკრულების გაფორმების მიზნით და დამუშავდა ავტომატიზირებული საშუალებებით.

ბ) თუ პირობები დაკმაყოფილებულია, მიაწოდოს მოთხოვნილი პერსონალური მონაცემები სტრუქტურირებულ, ჩვეულებრივ გამოყენებად და მანქანურად წაკითხვად ფორმატში (*.xml, *.doc, *.csv) მონაცემთა სუბიექტს ან სხვა სუბიექტს მონაცემთა სუბიექტის მოთხოვნით.

გ) ასეთ DSR-ზე რეაგირებისას არ გაამჟღავნოს მონაცემთა სხვა სუბიექტების პერსონალური მონაცემები და უზრუნველყოს პერსონალური მონაცემების გადაცემა ტექნიკური და ორგანიზაციული უსაფრთხოების შესაბამისი ზომების

უზრუნველყოფით, მათ შორის, მონაცემთა გაზიარების დაცული ქსელების გამოყენებით ან პაროლით დაცვის გამოყენებით.

გაპროტესტების უფლება

8.13. თუ მონაცემთა სუბიექტმა გააპროტესტა თავისი პერსონალური მონაცემების დამუშავება, კომპანიამ უნდა შეაფასოს, ეფუძნებოდა თუ არა შესაბამისი პერსონალური მონაცემების დამუშავება კომპანიის კანონიერ ინტერესებს, ამ სამართლებრივ საფუძველზე დაფუძნებული პროფილირების ჩათვლით. თუ დამუშავების სამართლებრივი საფუძველი არ არის კანონიერი ინტერესები, DSR-ი უარყოფილი იქნება.

8.14. თუ დამუშავების სამართლებრივი საფუძველია ლეგიტიმური ინტერესები, კომპანიამ, DPO-სთან თანამშრომლობით, უნდა შეაფასოს, არსებობს თუ არა დამუშავების დამაჯერებელი ლეგიტიმური საფუძველი, რომელიც აჭარბებს მონაცემთა სუბიექტის ინტერესებს, უფლებებსა და თავისუფლებებს და/ან (ბ)) საჭიროა თუ არა პერსონალური მონაცემები კომპანიისთვის სამართლებრივი პრეტენზიების ჩამოყალიბების, განხორციელების ან დაცვისათვის. თუ ეს შეფასებები არ შეესაბამება სიმართლეს, პერსონალური მონაცემები აღარ დამუშავდება კონკრეტული მიზნით.

8.15. იმ შემთხვევაში, თუ კომპანიის კანონიერი ინტერესია პირდაპირი მარკეტინგი, კომპანია არ ახორციელებს 8.15-ე პუნქტში დადგენილ შეფასებას და წყვეტს პერსონალური მონაცემების დამუშავებას ამ მიზნით.

გადაწყვეტილების ავტომატიზირებულ მიღებაზე, მათ შორის პროფილირებაზე არ დაქვემდებარების უფლება

8.16. მონაცემთა სუბიექტს შეუძლია მოითხოვოს, რომ არ დაექვემდებაროს გადაწყვეტილების ავტომატიზირებულ მიღებას პროფილირების ჩათვლით, თუ გადაწყვეტილების მიღების პროცესი დაფუძნებულია მხოლოდ ავტომატიზირებულ დამუშავებაზე, პროფილირების ჩათვლით, რაც იწვევს სამართლებრივ ან მსგავს მნიშვნელოვან გავლენას მონაცემთა სუბიექტზე. ასეთ შემთხვევაში კომპანია წყვეტს ასეთი ავტომატიზირებული გადაწყვეტილების მიღებას მონაცემთა კონკრეტულ სუბიექტთან დაკავშირებით, თუ ეს გადაწყვეტილება:

ა) არ არის აუცილებელი მონაცემთა სუბიექტსა და კომპანიას შორის ხელშეკრულების დასადებად ან შესასრულებლად ან მონაცემთა სუბიექტის აშკარა თანხმობის საფუძველზე. ასეთ შემთხვევაში კომპანია უარყოფს DSR-ს, მაგრამ უზრუნველყოფს მონაცემთა სუბიექტის უფლებების, თავისუფლებებისა და ლეგიტიმური ინტერესების დაცვას, მათ შორის, იმ პირობით, რომ კომპანიის უფლებამოსილი წარმომადგენელი განიხილავს გადაწყვეტილებას.

ბ) არ არის ნებადართული მოქმედი კანონმდებლობით ან რეგულაციებით.

9. თანამშრომელთა ტრენინგი

9.1. კომპანია ჩაატარებს თანამშრომლების რეგულარულ ტრენინგს და აცნობებს თანამშრომლებს წინამდებარე პოლიტიკისა და სხვა პროცედურების ან პოლიტიკის შესახებ, რომლებიც შეიძლება შესაბამისი იყოს წინამდებარე პოლიტიკის მიზნების შესასრულებლად.

9.2. თანამშრომელთა ტრენინგი შეიძლება ჩატარდეს ინდივიდუალურად (თანამშრომლის სამსახურში მიღების პროცესში) ან ჯგუფურად.

9.3. საჭიროების შემთხვევაში, კომპანიას შეუძლია, ჩაატაროს ტრენინგი, რომელიც ორიენტირებულია კონკრეტულ თემაზე ან საკითხზე, რითაც ხელს შეუწყობს წინამდებარე პროცედურის მიზნების მიღწევას და კომპანიის შესაბამისობას მონაცემთა დაცვის შესახებ მოქმედ კანონებთან.

9.4. ტრენინგის შემდეგ, თანამშრომლებისგან შესაძლოა მოთხოვნილი იქნას ტრენინგის თემის შესახებ ცოდნის შემოწმების ტესტის შევსება. თუ თანამშრომელი არ მიიღებს მონაწილეობას ტესტის შევსებაში, ან ვერ შეავსებს ტესტს, მას მოეთხოვება ტესტის ხელახლა ჩაბარება.

10. ცვლილებები პოლიტიკაში

10.1. წინამდებარე პოლიტიკაში ცვლილებების შეტანა და მისი განახლება შესაძლებელია რეგულარულად და ნებისმიერი ცვლილება უნდა დამტკიცდეს დირექტორის ბრძანების საფუძველზე. დირექტორს ეკისრება საერთო პასუხისმგებლობა წინამდებარე პოლიტიკის შესრულების ზედამხედველობაზე.

10.2. წინამდებარე პოლიტიკას გაეცნობა ყველა თანამშრომელი სამსახურში მიღების დროს. პოლიტიკა ნებისმიერ დროს ხელმისაწვდომია კომპანიის პერსონალის მართვის სისტემაში.

10.3. წინამდებარე პოლიტიკაში ცვლილებების შეტანის შემთხვევაში, თანამშრომლებს ცვლილებების შესახებ ეცნობებათ უმოკლეს ვადაში, მაგრამ არა უგვიანეს 1 თვისა შესწორებული პოლიტიკის მიღებიდან.

10.4. წინამდებარე პოლიტიკიდან გადახვევა შესაძლებელია მხოლოდ დირექტორის წინასწარი წერილობითი თანხმობით.